



Étude révision de l'architecture EasyGov : Architecture cible d'intégration pour les portails de prestations administratives

AWK Group AG

Janvier 2022



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'économie,
de la formation et de la recherche DEFR
Secrétariat d'Etat à l'économie SECO
Direction de la promotion économique

Impressum

Editeur

Secrétariat d'État à l'économie SECO, Direction de la promotion économique, Secteur Politique PME

Mandant de l'étude

Martin Godel, Leiter KMU-Politik SECO und Auftraggeber EasyGov

Markus Pfister, Gruppenleiter E-Government für KMU und Stv. Auftraggeber EasyGov

Comité de pilotage

Alexandra Collm, Leiterin Bereich Kunden, Direktion für Organisation und Informatik Stadt Zürich

David De Groot, Mitglied Planungsausschuss eGov-CH, Canton du Jura

Hansjörg Hänggi, Planungsausschuss eGov-CH, Verantwortlicher E-Government Kanton Baselstadt

Marcel Kessler, Projektleiter Umsetzungsplan, Geschäftsstelle E-Government Schweiz

Andreas Spichiger, Auftraggeber UZ14, Leiter Bereich Architektur Bundeskanzlei

Groupe d'experts

Philipp Achermann, Leiter Unternehmensarchitektur, Kanton Bern

Nils Blattner, IT-Architekt, Kanton Basellandschaft

Urs Brunner, Teamleiter ZSservices, Staatskanzlei Kanton Zürich

Vojto Elias, Business Analyst Cyber Administration, Canton de Vaud

Pascal Graf, Programmleiter EasyGov, SECO

Giovanni Groppo, ICT-Architekt Schwerpunkt Fachanwendungen, Stadtverwaltung Zürich

Daniel Krebs, Leiter Digital Services, UVEK

David Lehmann, Verantwortlicher Entwicklung und Betrieb ePortal, BIT

Oldrich Milde, Unternehmensarchitekt WBF

Matthieu Overney, IT-Architekt und technischer Leiter iGovPortal, Canton de Fribourg

Jörg Pietschmann, IT-Unternehmensarchitekt, Kanton Luzern

Willy Reinhardt, Leiter Centre de compétences architecture et intégration à la Direction des systèmes d'information, VD

René Staudenmann, Identity and Access Management, BIT

Jürg Umhang, GS EFD, ePortal

Lukas Weibel, Leiter Business Engineering und Projekte, Kanton ZH

Jürg Wüst, Unternehmensarchitekt, BK

Andreas Zeltner, Leiter Gruppe Strategische Projekte, KSTA ZH

Auteurs

Peter Neidel, Projektleiter (AWK)

Olivier Thyès (AWK)

AWK Group AG

Laupenstrasse 4, CH - 3008 Berne

Tél.: +41 58 411 95 00

www.awk.ch

info@awk.ch

Management Summary

Situation initiale et objectif de l'étude

Les citoyens et les entreprises souhaitent de plus en plus profiter des prestations des autorités publiques par voie numérique. Outre le confort accru pour les utilisateurs grâce à un échange avec les autorités fédérales, cantonales et communales sans rupture de média, les prestations fournies numériquement peuvent être proposés par les autorités de manière plus flexible, plus efficace et de meilleure qualité.

Le développement du guichet unique pour les prestations administratives destiné aux entreprises sous le nom de EasyGov.swiss est un projet stratégique de la cyberadministration suisse. La présente étude porte sur la mesure M1 de l'objectif de mise en œuvre OMO1 du plan de mise en œuvre de la cyberadministration suisse pour la période législative 2020-2023 : Réalisation d'une étude examinant l'architecture du portail sous l'angle de la faisabilité de l'intégration des prestations fédérales, cantonales et communales, avec la participation des acteurs concernés. Dans un premier temps, une architecture cible d'intégration générale pour les portails de prestations administratives sera élaborée, ce qui permettra de préparer un projet de norme eCH. Ensuite, dans une deuxième étape, on évaluera quelles adaptations d'EasyGov sont nécessaires pour répondre à l'architecture cible globale (analyse des écarts - ne fait pas partie de cette version de l'étude).

Démarche

L'examen de l'architecture a été mené en étroite coordination avec le comité de planification de l'organisation Cyberadministration suisse. L'architecture cible d'intégration a été développée de manière itérative dans une série d'ateliers avec des représentants de tous les niveaux fédéraux.

Principales conclusions concernant l'architecture cible d'intégration

1. Image cible

Le point de départ de l'image cible a été une précédente évaluation des besoins, qui a permis de mettre en évidence des points faibles concrets du point de vue de l'utilisateur/du client et de l'autorité/de l'exploitant du portail :

- L'utilisateur préfère pouvoir tout faire avec un seul login à partir d'un seul portail et ne pas avoir à saisir quoi que ce soit deux fois
- L'exploitant du portail ne veut pas négocier/implémenter l'architecture et les interfaces individuellement pour chaque intégration (de prestations administratives externes)

Pour répondre aux points faibles mentionnés, il faut avant tout un dénominateur commun conceptuel et, sur cette base, un degré suffisant d'interopérabilité des données. L'image cible est donc :

La normalisation doit permettre l'interopérabilité des données et des processus nécessaires à l'interaction des portails de prestations administratives.

2. Conception de l'architecture cible d'intégration

Les différents sujets de normalisations, dérivés des points faibles, ont été spécifiés sous la forme d'exigences pour une future norme, qui restent autant que possible neutres sur le plan technologique.

- Dans le périmètre : Domaines de données interopérables, Responsabilités, Processus d'interface
- Hors du périmètre : Détermination de la technologie, Domaines de données spécifiques aux prestations

Les résultats suivants ont été définis :

- Cadre d'interopérabilité technologiquement neutre : il définit la manière dont un niveau suffisant d'interopérabilité des données peut être atteint au niveau des interfaces pour faire face aux points faibles. Cela comprend entre autres la manière dont les différentes entités (telles que utilisateur, prestation administrative, droit de gestion) sont identifiées et de quelle façon les données correspondantes doivent être conçues de manière interopérable (données de base interopérables). Le cadre d'interopérabilité définit également les systèmes d'identification à utiliser (p. ex. registre IDE).
- Modèles d'intégration et interfaces nécessaires : grâce aux deux modèles d'intégration "implémentation" et "intégration", un portail de prestations administratives peut intégrer de deux manières différentes une prestation administrative mise à disposition en externe. Les exigences d'interface correspondantes ont été spécifiées.
 - Dans le cas de l'**implémentation** (ou intégration complète), le portail de prestations administratives utilise des interfaces avec un système métier interne d'une autorité afin de reproduire intégralement la transaction correspondante. Dans ce cas, une structure de processus de communication généraux a été spécifiée, sur la base de laquelle des contenus spécifiques aux prestations sont transmis (c'est-à-dire une séquence réglementée de messages entre les systèmes).
 - Dans le cas de l'**intégration** (ou intégration partielle), une implémentation externe existante d'une démarche administrative est utilisée, de sorte que la transmission de la session utilisateur (au moyen d'une authentification unique) vers le portail de prestations externe est spécifiée en vue d'une future normalisation.

3. Recommandations pour la suite de la procédure

L'architecture cible d'intégration pour les portails de prestations administratives développée dans cette étude doit être mise en œuvre étape par étape. La feuille de route est divisée en phases, de sorte que les étapes d'extension facultatives peuvent être décidées à une date ultérieure.

La norme à élaborer dans une première phase doit supporter les deux modèles d'intégration et renoncer, dans la mesure du possible, à des composants d'infrastructure centraux. La norme à créer est basée sur le principe "Peer-2-Peer", afin de pouvoir réutiliser les implémentations existantes et d'obtenir des résultats rapides. Dans les étapes ultérieures, des composants centraux pourront être introduits en fonction des besoins, afin de permettre un haut degré d'interopérabilité et une mise en œuvre simple des futures intégrations.

Le processus de la mise en œuvre planifiée de l'architecture cible d'intégration sous la forme d'une ou plusieurs normes doit être dirigé par l'organisation "Administration Numérique Suisse" (ANS). Une fois la normalisation effectuée, il est recommandé de mettre en œuvre des projets pilotes impliquant des autorités de différents niveaux fédéraux.

Liste des changements

Version	Date	Changement	Auteur
0.01 - 0.05	10.09.2020	Initialisation, élaboration ébauche jusqu'à et y compris le chapitre 2.3	Peter Neidel, Corinne Kuhn
0.08	29.09.2020	Intégration du retour d'information de l'atelier du comité d'experts du 18.09.2020 et examen.	Peter Neidel, Alexander Zurkinden
0.09-0.10	14.10.2020	Intégration du retour d'information du comité d'experts sur la révision du 29.09. jusqu'à et y compris le Ch. 2.3, ébauche pour le Ch. 2.4 Image cible	Peter Neidel, Alexander Zurkinden
0.11-0.12	20.10.2020	Définition des images cibles, intégration de nouveaux commentaires du comité d'experts.	Peter Neidel, Alexander Zurkinden
0.13	27.10.2020	Intégration du retour d'information de l'atelier du comité d'experts du 22.10.20, ainsi que finalisation du chapitre sur l'image cible comme base pour la révision circulaire par le comité d'experts.	Peter Neidel, Alexander Zurkinden
0.15	19.11.2020	Intégration du retour d'information de la révision circulaire du comité d'experts jusqu'au chapitre sur l'image cible, ainsi que formulation des défis en préparation de l'atelier du comité d'experts du 25.11.2020.	Peter Neidel, Alexander Zurkinden
0.16-0.17	04.12.2020	Intégration du retour d'information de l'atelier du comité d'experts du 25.11.2020	Peter Neidel, Alexander Zurkinden
0.18	16.12.2020	Préparation de l'atelier du comité d'experts du 16.12.2020. Intégration de l'évaluation des variantes de solutions.	Peter Neidel, Alexander Zurkinden
0.19	06.01.2021	Intégration du retour d'information de l'atelier du comité d'experts du 16.12.2020	Peter Neidel, Alexander Zurkinden
0.20	04.02.2021	Intégration du retour d'information de l'atelier du comité d'experts du 18.01.2021	Peter Neidel
0.21	16.02.2021	Intégration des résultats de la révision de la v0.20, informations sur le SNA (HF-2)	Peter Neidel, Olivier Thyes
0.22	06.03.2021	Feedback des ateliers du comité d'experts du 1.3.2021 et du 30.3.2021. Refactoring du chapitre 2.1 pour intégrer la base conceptuelle clarifiée.	Peter Neidel, Olivier Thyes
0.23	18.04.2021	Retour d'information de l'atelier du comité d'experts du 30.3.2021 ainsi que de la révision ultérieure. Chapitre 2.5.1 Sujets de normalisation Chapitre 2.5.4 Gouvernance informatique	Peter Neidel, Olivier Thyes
0.24-0.25	16.07.2021	Révision du chapitre 2.5.4, nouveau chapitre 2.7, ébauche du résumé	Olivier Thyes
0.25-0.29	04.08.2021	Restructuration de l'étude après l'achèvement des ateliers, formulation des sujets de normalisation ainsi que finalisation d'une version révisable V1.	Peter Neidel
0.30-0.31	11.08.2021	Résumé Correction des annexes, vérification les références	Olivier Thyes, Peter Neidel

Version	Date	Changement	Auteur
		Compléter les abréviations et le glossaire Compléter les décisions et l'accomplissement des besoins	
0.89	18.08.2021	Compléter le chapitre 2.5 Prêt pour la révision	Olivier Thyès, Peter Neidel
0.90	20.08.2021	Correction des problèmes liés aux références et aux notes de bas de page	Olivier Thyès
0.91	15.09.2021	Révision après le premier examen par le comité d'experts	Peter Neidel, Olivier Thyès
0.92	03.11.2021	Révision après de nouvelles clarifications bilatérales et une deuxième révision, couverture détaillée des besoins.	Peter Neidel, Olivier Thyès
0.93	17.12.2021	Finalisation et envoi au mandant pour examen final avant acceptation par le comité de pilotage	Peter Neidel, Olivier Thyès
0.94	12.01.2022	Intégration des constatations du mandant, nouveau Management Summary, diverses petites modifications.	Peter Neidel, Olivier Thyès
1.0	18.01.2022	Version finale pour acceptation par le comité de pilotage	Peter Neidel, Olivier Thyès

Documents référencés

No	Document	Description	Lien
[1]	Mandat d'initialisation du projet		Lien
[2]	eCH-0039	Interface de cyberadministration	Lien
[3]	eCH-0044	Norme concernant les données Echange d'identifications de personnes	Lien
[4]	eCH-0058	Norme d'interface – Cadre d'annonce	Lien
[5]	eCH-0084	UPI Declaration Interface	Lien
[6]	eCH-0085	UPI Query Interface	Lien
[7]	eCH-0086	UPI Compare Interface	Lien
[8]	eCH-0088	Règles relatives à la description des démarches administratives en Suisse («Règles de description eCH pour les démarches administratives»)	Lien
[9]	eCH-0090	Enveloppe sedex	Lien
[10]	eCH-0107	Principes de conception pour la gestion de l'identité et de l'accès (IAM)	Lien
[11]	eCH-0158	Conventions de modélisation BPMN pour l'administration publique	Lien
[12]	eCH-0123	Architecture de la cyberadministration suisse: Distribution	Lien
[13]	eCH-0124	Architecture de la cyberadministration suisse: Production	Lien
[14]	eCH-0126	Concept cadre «Administration interconnectée en Suisse»	Lien
[15]	eCH-0138	Concept organisationnel pour la description et la documentation de tâches, prestations, processus et structures d'accès de l'administration publique en Suisse	Lien
[16]	eCH-0177	Modèle d'information pour le déroulement d'une affaire dans une administration interconnectée en Suisse	Lien

No	Document	Description	Lien
[17]	EIF brochure	The new European Interoperability Framework	Lien
[18]	Étude portail du DFF 1.0	Examine les exigences techniques d'une future solution de portail du DFF et formule des solutions possibles.	Lien
[19]	Plan de mise en œuvre 2020-2023	Plan de mise en œuvre 2020-2023 de la cyberadministration Suisse	Lien
[20]	EIRA	European Interoperability Reference Architecture	Lien
[21]	eCH-0170	Modèle de qualité pour l'authentification des sujets	Lien
[22]	eCH-0171	Modèle de qualité de la confirmation de valeur d'attribut concernant l'eID	Lien
[23]	LSIE	Loi fédérale sur les services d'identification électronique (LSIE)	Lien
[24]	eCH-0074	Représentation graphique des processus d'affaires - Utilisation du BPMN du point de vue administratif	Lien
[25]	eCH-0242	Modélisation des règles d'affaires	Lien
[26]	SB000	Stratégie informatique de la Confédération 2020-2023	Lien
[27]	eCH-0070	Inventaire des prestations de l'administration publique suisse («Inventaire des prestations eCH»)	Lien
[28]	eCH-0097	Norme concernant les données Identification des entreprises	Lien
[29]	eCH-0098	Norme concernant les données des entreprises	Lien
[30]	eCH-0108	Norme concernant les données Registre des entreprises	Lien
[31]	eCH-0224	Modèles d'architecture Identity Federation impliquant un Broker	Lien
[32]	eCH-0225	Identity Federations impliquant un Broker – Implémentation avec OIDC	Lien
[33]	GSVB ausländische Unternehmen UID BUR	BK/DTI: Studie ausländische Unternehmen im UID/BUR (V1 vom 29.04.2021) – version française non disponible	
[34]	API-Architektur Bund	BK/DTI: Konzept zur API-Architektur im Bund (V0.9 vom 23.07.2021) – version française non disponible	
[35]	eCH-0147	Groupe de messages GEVER	Lien
[36]	Image cible E-ID	Document de travail concernant le projet d'identité électronique (e-ID)	Lien
[37]	Rapport de base ANS	Rapport de base concernant l'Administration numérique suisse	Lien
[38]	Requête client PP	Amtlich einfach - Lebenslagen Bürger - version française non disponible	Lien
[39]	Requête client PM	Amtlich einfach - Lebenslagen Unternehmen - version française non disponible	Lien
[40]	EasyGov Architecture du système	EasyGov Systemarchitektur (V1.13 vom 1.11.2021) – version française non disponible	Lien
[41]	Stratégie Suisse numérique	Stratégie Suisse numérique (Septembre 2018) Stratégie Suisse numérique (Septembre 2020)	Lien Lien

Abréviations utilisées

Abréviation	Signification
1FA	Authentification à un facteur
2FA	Authentification à deux facteurs

Abréviation	Signification
A2A	D'administration à administration
A2B	De l'administration à l'entreprise
A2C	De l'administration au citoyen
AC	Assurance-chômage
AFC	Administration fédérale des contributions
ANS	Administration numérique suisse
API	Application Programming Interface
AVS	Assurance-vieillesse et survivants
CDC	Centrale de compensation
ChF	Chancellerie fédérale
DFF	Département fédéral des finances
EIF	European Interoperability Framework
FI	Fournisseur d'identités
GCDC	Gestion commune des données de base de la Confédération
IAM	Identity and Access Management
IDE	Numéro d'identification des entreprises
IU	Interface utilisateur
LoA	Level of Assurance
LPD	Loi fédérale sur la protection des données
LSAdr	Loi sur le service des adresses
NAVS13	Numéro AVS à 13 chiffres
OFAG	Office fédéral de l'agriculture
OFIT	Office fédéral de l'informatique et de la télécommunication
OFS	Office fédéral de la statistique
OMO	Objectif de mise en œuvre
P2P	Peer-to-Peer
PAMS	Polymorphic Access Management System
PF	Point faible
PM	Personne morale
PP	Personne physique
RFC	Request For Change
SEA	Search Engine Advertising
SECO	Secrétariat d'Etat à l'économie
SEO	Search Engine Optimization
SIPD	Sûreté de l'information et de protection des données
SLA	Service Level Agreement
SLO	Single Logout
SNA	Service national des adresses
SSO	Single Sign On
TCR	Tâches, compétences et responsabilités
TIC	Technologies de l'information et de la communication
TNI	Transformation numérique et gouvernance de l'informatique (secteur de la ChF)
TOGAF	The Open Group Architecture Framework
UPI	Unique Person Identification
UX	User Experience (expérience utilisateur)

Table des matières

Management Summary	2
<i>Liste des changements.....</i>	<i>4</i>
<i>Documents référencés</i>	<i>5</i>
<i>Abréviations utilisées</i>	<i>6</i>
0 Résumé	11
0.1 Situation initiale et objectif de l'étude	11
0.2 Démarche	12
0.3 Résultats Étape 1: Architecture cible d'intégration pour les portails de prestations administratives	12
0.3.1 Fondement conceptuel.....	12
0.3.2 Image cible	16
0.3.3 Conception de l'architecture cible d'intégration.....	17
0.3.3.1 Sujets de normalisation.....	17
0.3.3.2 Cadre d'interopérabilité	17
0.3.3.3 Interfaces	18
0.3.4 Recommandations pour la suite de la procédure	20
0.4 Résultats Étape 2: Analyse des écarts d'EasyGov	21
1 Situation initiale et objectif de l'étude	22
1.1 Niveaux politique et légal	22
1.2 Objectifs de l'«Administration numérique suisse»	22
1.3 Objectif de mise en œuvre UZ1 de la cyberadministration suisse	23
2 Architecture cible d'intégration pour les portails de prestations administratives	25
2.1 Analyse de la situation des portails de prestations administratives d'un point de vue logique	25
2.1.1 Vue du processus d'une prestation administrative.....	25
2.1.2 Le portail de prestations comme canal d'accès numérique	31
2.1.3 Structure fonctionnelle d'un portail de prestations.....	33
2.1.4 Paysage des portails de prestations.....	37
2.1.5 Modèle d'information des termes les plus importants.....	44
2.1.6 Modèles d'intégration pour la représentation des démarches administratives	49
2.2 Exigences pour le domaine des portails de prestations du point de vue commercial	53
2.2.1 Conditions cadres.....	53
2.2.2 Besoins.....	54
2.2.2.1 Catégorisation selon la déclaration de Tallinn sur la cyberadministration.....	55
2.2.2.2 Structuration de la détermination des besoins	55
2.2.2.3 Besoins concernant l'intégration des prestations administratives.....	57
2.2.2.4 Besoins en matière d'authentification et d'autorisation.....	58

2.2.2.5	Besoins en matière de communication client - autorité	59
2.2.2.6	Besoins en matière d'interface utilisateur (UI)	60
2.2.2.7	Besoins en matière de marche des affaires des prestations administratives 61	
2.2.2.8	Besoins en matière de SIPD.....	63
2.2.2.9	Besoins en matière de mise en œuvre et d'exploitation.....	63
2.2.2.10	Répartition des besoins par catégories	64
2.2.3	Délimitations	65
2.2.4	Attentes en matière de qualité de l'architecture cible	65
2.3	Principes architecturaux	66
2.3.1	Considération préliminaire: Interoperability Principles du EIF.....	66
2.3.2	Principes architecturaux pour l'architecture cible	69
2.4	Image cible.....	71
2.5	Développement de l'architecture cible d'intégration	76
2.5.1	Sujets de normalisation	77
2.5.1.1	Cadre d'interopérabilité	77
2.5.1.1.1	Modèle d'information.....	79
2.5.1.1.2	Identification des prestations	81
2.5.1.1.3	Identification des requêtes client	81
2.5.1.1.4	Identification des clients et gestion des données de base	82
2.5.1.1.5	Métadonnées des processus pour les démarches administratives et les transactions.....	85
2.5.1.1.6	Compte utilisateur	86
2.5.1.1.7	Aperçu sommaire du cadre d'interopérabilité	90
2.5.1.2	Interface "démarche administrative↔traitement des transactions"	92
2.5.1.3	Interface pour l'intégration des démarches administratives implémentées en externe	98
2.5.1.3.1	Authentification unique (SSO)	99
2.5.1.3.2	Synchronisation du contexte	107
2.5.1.3.3	Déconnexion unique (SLO)	110
2.5.1.3.4	Canal de retour pour la démarche administrative (statut, notifications officielles, documents de résultats)	110
2.5.1.4	Aperçu du flux de données des interfaces	111
2.5.1.5	Responsabilité des interfaces.....	113
2.5.2	Sujets relatifs à la SIPD	115
2.5.2.1	Identification des besoins de protection.....	115
2.5.2.2	Excursus: Exigences de l'autorité en matière de SIPD.....	115
2.5.2.3	Excursus: Exigences en matière de SIPD pour le portail de prestations... 117	
2.5.3	Questions légales	118
2.5.4	Gouvernance informatique	118
2.5.4.1	Gouvernance informatique dans le contexte de l'architecture cible d'intégration.....	118
2.5.4.2	Exigences en matière de gouvernance informatique.....	119
2.6	Couverture des besoins	120
2.7	Recommandations pour la suite des opérations.....	123

2.7.1	Feuille de route pour la mise en œuvre.....	123
2.7.2	Recommandations d'action	125
3	Analyse des écarts entre l'architecture actuelle d'EasyGov et l'architecture cible d'intégration.....	127
3.1	Écarts identifiées	127
3.2	Planification grossière pour l'élimination des écarts	127
4	Annexes.....	127
	<i>Liste des figures.....</i>	<i>191</i>
	<i>Liste des tableaux.....</i>	<i>193</i>

Note: Le masculin générique choisi dans cette étude fait référence simultanément aux identités masculines, féminines et autres. Pour une meilleure lisibilité, l'utilisation des formes masculines et féminines est supprimée. Toutes les identités de genre sont explicitement incluses, dans la mesure où les déclarations l'exigent.

0 Résumé

0.1 Situation initiale et objectif de l'étude

Les citoyens et les entreprises souhaitent de plus en plus profiter des prestations des autorités publiques par voie numérique. Outre le confort accru pour les utilisateurs grâce à un échange avec les autorités fédérales, cantonales et communales sans rupture de média, les prestations fournies numériquement peuvent être proposés par les autorités de manière plus flexible, plus efficace et de meilleure qualité.

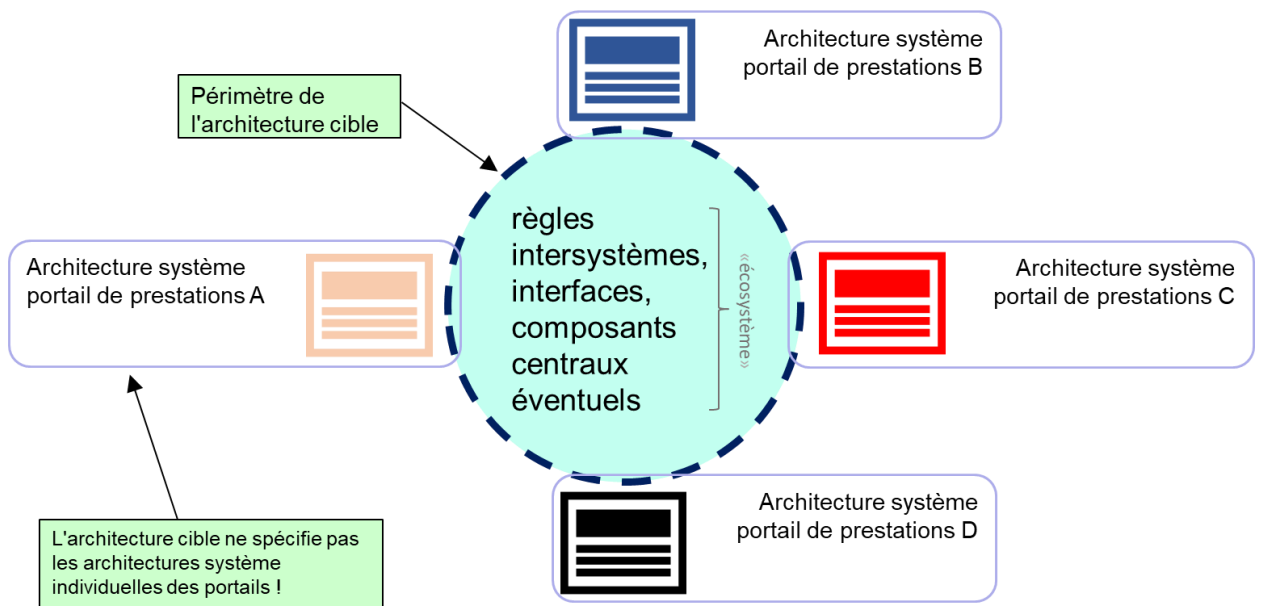
Diverses organisations et stratégies contribuent à la mise en œuvre de la transformation numérique à tous les niveaux de la Confédération, comme l'organisation "Administration Numérique Suisse" et la stratégie informatique de la Confédération. Les bases légales sont la loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités et la loi sur l'allégement des coûts de la réglementation pour les entreprises.

Le développement du guichet unique pour les prestations administratives destiné aux entreprises sous le nom de EasyGov.swiss est un projet stratégique de la cyberadministration suisse. Le plan de mise en œuvre définit deux mesures pour la période législative 2020-2023 en rapport avec l'objectif de mise en œuvre 1 (OMO1):

- M1: Réalisation d'une étude examinant l'architecture du portail sous l'angle de la faisabilité de l'intégration des prestations fédérales, cantonales et communales, avec la participation des acteurs concernés
- M2: Intégration dans EasyGov de prestations administratives cantonales destinées aux entreprises, si plusieurs cantons souhaitent cette intégration

La présente étude porte sur la mesure M1 "Examen de l'architecture". Dans un premier temps, une architecture cible d'intégration **générale** pour les portails de prestations administratives destinés aux personnes morales et physiques sera élaborée, ce qui permettra de préparer un projet de norme eCH. Ensuite, dans une deuxième étape, on évaluera quelles adaptations d'EasyGov sont nécessaires pour répondre à l'architecture cible globale (analyse des écarts).

L'architecture cible d'intégration souhaitée pour les portails de prestations administratives ne se concentre pas sur les architectures des portails individuels, mais plutôt sur un "écosystème" interportails qui régule l'interaction et améliore l'interopérabilité, voir le graphique suivant:



0.2 Démarche

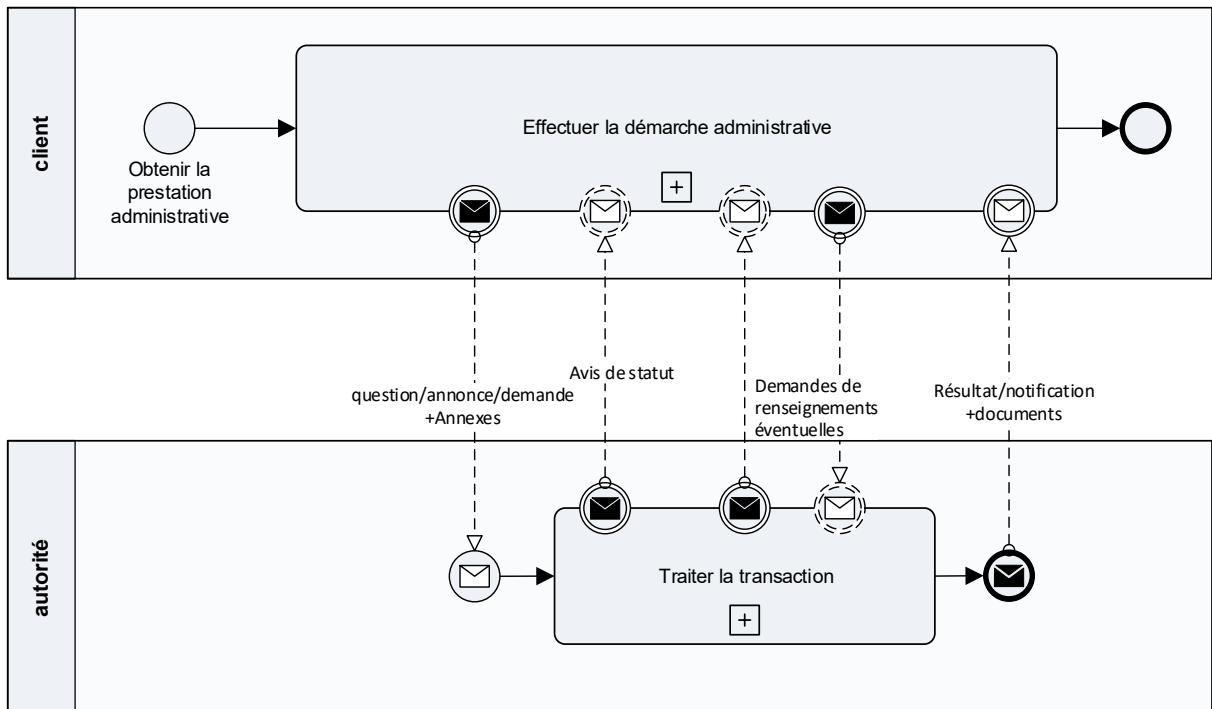
L'examen de l'architecture a été mené en étroite coordination avec le comité de planification de l'organisation Cyberadministration suisse. L'architecture cible d'intégration a été développée de manière itérative dans une série d'ateliers avec des représentants de tous les niveaux fédéraux:

- Représentants de l'administration fédérale: ChF, TNI, DFF, DEFR, DETEC
- Représentants cantonaux de la cyberadministration
- Représentants cantonaux de l'architecture TIC, y compris iGovPortal
- Représentants des villes, notamment de la ville de Zurich
- Direction opérationnelle E-Government Suisse

0.3 Résultats Étape 1: Architecture cible d'intégration pour les portails de prestations administratives

0.3.1 Fondement conceptuel

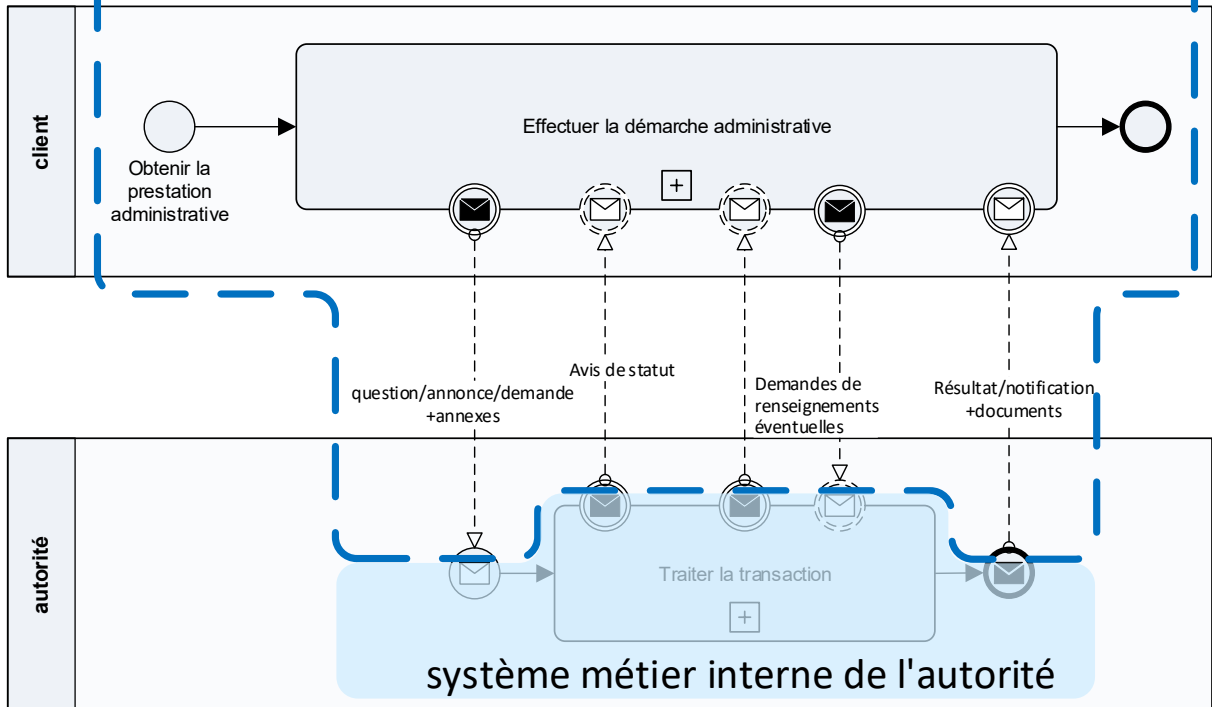
Une prestation administrative (électronique) peut être représentée de manière très abstraite comme des processus fonctionnant en parallèle du côté du client et de l'autorité:



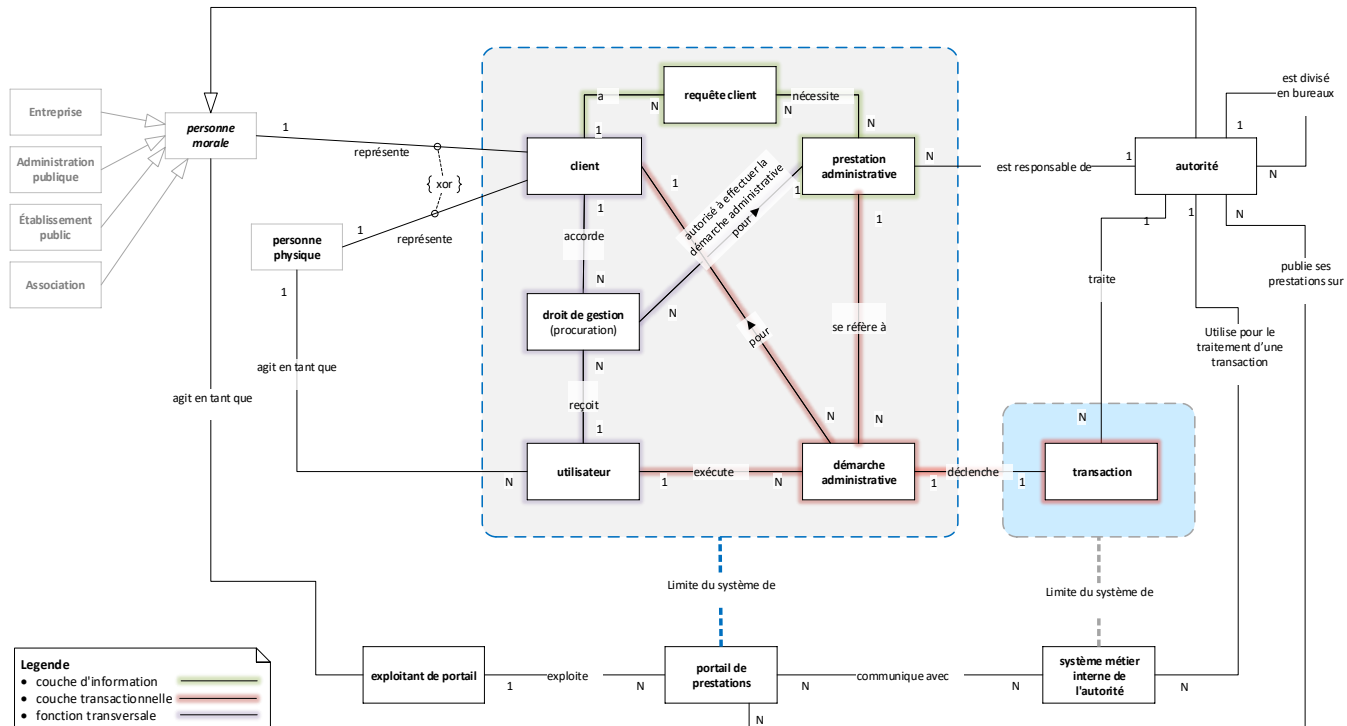
À l'aide d'un portail de prestations administratives (ou portail de prestations), un exploitant de portail offre des prestations administratives au client. Il représente un canal d'accès pour le client à une ou plusieurs démarches administratives. Le portail de prestations communique avec le système métier¹ de l'autorité compétente dans lequel le traitement des transactions a lieu. Un portail de prestations peut être compris comme le front-end client qui supporte l'interface entre le client et l'autorité:

¹ Du point de vue du portail, le système métier interne de l'autorité peut également être considéré comme un back-end. Comme ceci est lié à la perspective, il n'est pas mentionné en tant que tel dans cette étude.

périmètre portail de prestations



Sur la base de la considération liée au processus et de l'utilisation habituelle du langage dans le secteur, les termes les plus importants d'un point de vue architectural dans le contexte des portails de prestations administratives ont été reliés dans un modèle d'information:



(Représentation agrandie en format paysage à l'Annexe B)

Notes:

- Les deux zones colorées indiquent le périmètre du portail de prestations et du système métier interne de l'autorité, respectivement.

- Les entités bordées de gris dans la figure le sont à titre d'illustration. Par exemple, il est montré que soit une personne morale (par exemple sous la forme d'une société), soit une personne physique apparaît en tant que client. Cette dernière peut également interagir avec le portail de prestations de l'autorité en tant qu'utilisateur.

En général, les fonctionnalités suivantes sont nécessaires pour la représentation numérique des prestations administratives (voir la légende du modèle d'information ci-dessus)

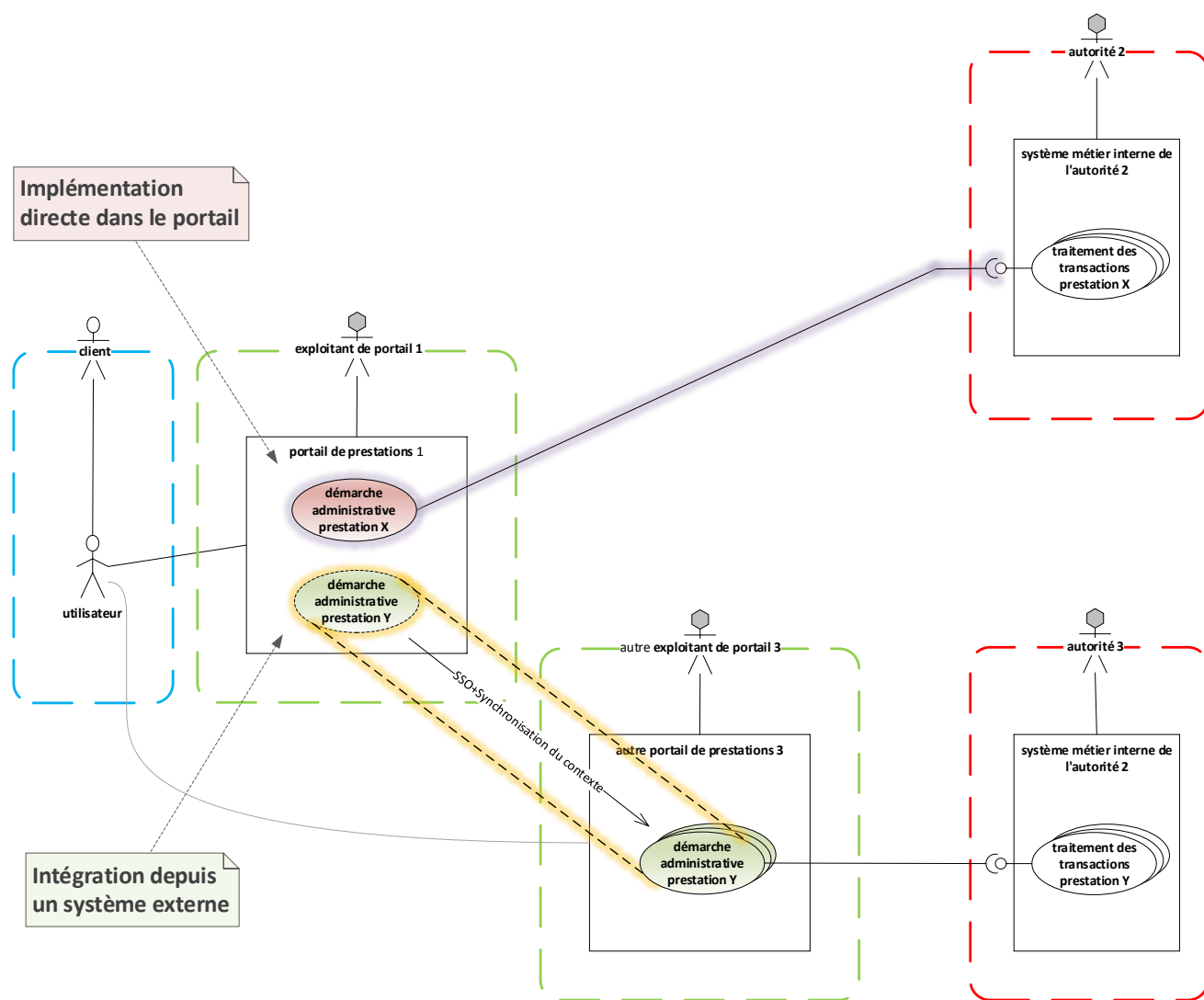
- Couche d'information: Aperçu de la gamme des prestations administratives et orchestration des prestations plus complexes au moyen d'assistants numériques (par exemple, la création d'une entreprise).
- Fonctions transversales: p.ex. compte utilisateur, gestion des autorisations, compte client, statut des démarches administrative, notifications officielles, stockage des documents.
- Couche transactionnelle: démarche administrative (utilisation de la prestation administrative)

Les modèles d'intégration suivants se retrouvent généralement dans la pratique au niveau de la couche transactionnelle en ce qui concerne la conception du système:

- Modèle d'intégration 1: **Implémentation** de la démarche administrative **directement** dans le portail via une interface avec le système métier interne de l'autorité.
- Modèle d'intégration 2: **Intégration** d'une démarche administrative **externe** via redirection SSO.

Note: Dans cette version française de l'étude, nous utilisons le terme "intégration" pour désigner le modèle d'intégration 2. Cela peut prêter à confusion. Les auteurs considèrent toutefois que cette traduction est la plus appropriée pour le terme allemand "Einbindung".

L'architecture cible d'intégration est basée sur ces deux modèles d'intégration. Ils peuvent également se présenter sous une forme mixte, comme l'illustre le graphique suivant en utilisant un portail fictif comme exemple:



0.3.2 Image cible

Le point de départ de l'image cible était une précédente évaluation des besoins, au cours de laquelle les points faibles suivants se sont manifestés:

- Point faible 1: L'utilisateur préfère pouvoir tout faire avec un seul login à partir d'un seul portail et ne pas avoir à saisir quoi que ce soit deux fois, et attend une orchestration des prestations nécessaires adaptées à sa requête particulière.

Deux autres points faibles apparaissent dans les efforts des exploitants de portails pour répondre à ce besoin par des offres intégratives en implémentant des démarches administratives de différentes responsabilités ou en les intégrant à partir d'autres systèmes:

- Point faible 2: L'exploitant du portail ne veut pas négocier/implémenter l'architecture et les interfaces individuellement pour chaque intégration.
- Point faible 3: L'exploitant du portail ne veut pas implémenter des interfaces individuelles pour le traitement des transactions de chaque démarche administrative. Ceci s'applique également à l'autorité.

Pour résoudre les points faibles mentionnés, il faut avant tout un dénominateur commun conceptuel et, sur cette base, un degré suffisant d'interopérabilité des données. L'image cible est donc:

La normalisation doit permettre l'interopérabilité des données et des processus nécessaires à l'interaction des portails de prestations administratives.

0.3.3 Conception de l'architecture cible d'intégration

Dans le sens de l'image cible, l'architecture d'intégration est grossièrement développée. Dans ce contexte, "grossièrement" signifie que les domaines à régler sont définis et que des stipulations fondamentales sont exprimées, mais qu'aucune spécification détaillée n'est faite. Les exigences sont formulées quant à ce que la normalisation souhaitée doit réaliser concrètement et à quoi doit ressembler le cadre logique de cette normalisation.

0.3.3.1 Sujets de normalisation

Les différents sujets sont spécifiés sous la forme d'exigences pour une future norme, qui restent autant que possible neutres sur le plan technologique.

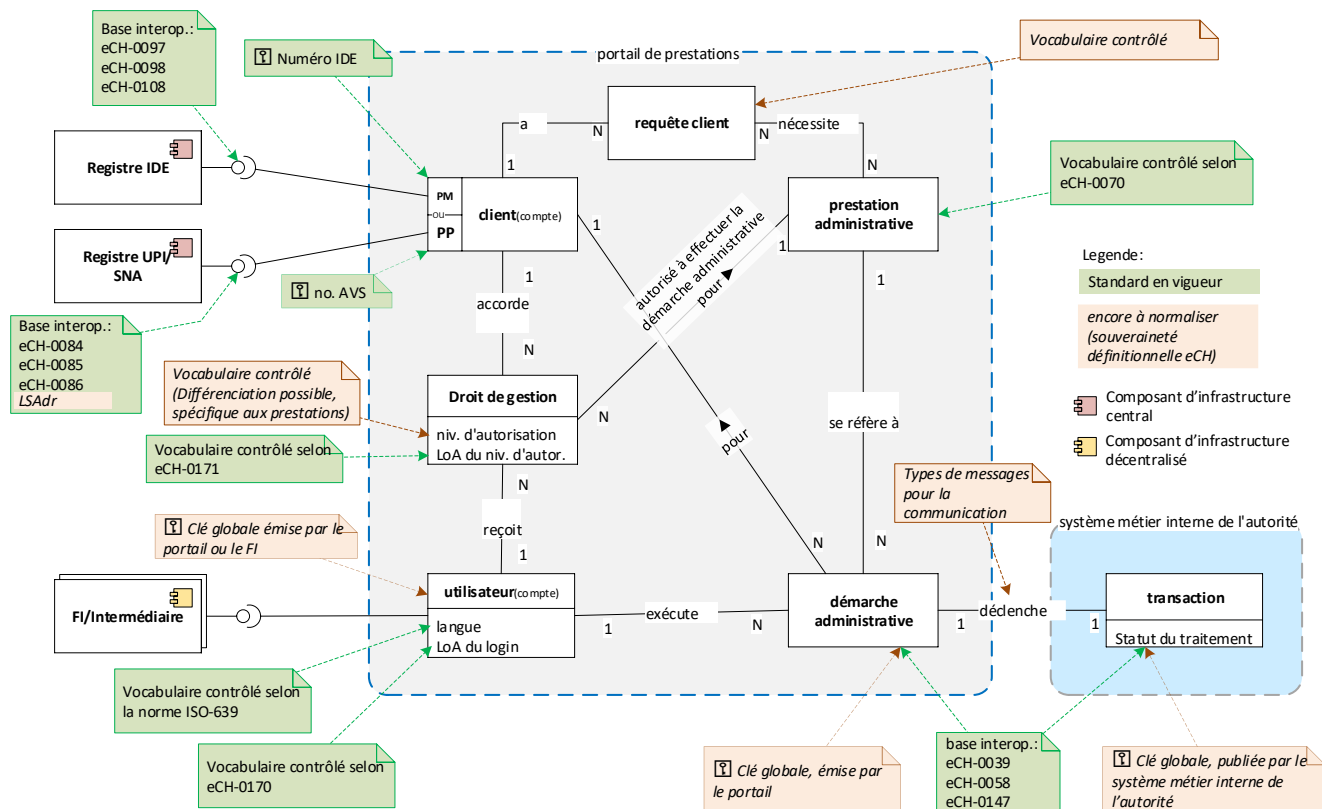
- Dans le périmètre:
 - Domaines de données interopérables (par exemple, les identifiants)
 - Responsabilités (souveraineté de définition, souveraineté des données)
 - Processus d'interface
- Hors du périmètre:
 - Détermination de la technologie (par exemple, protocole, système de bus éventuel)
 - Domaines de données spécifiques aux prestations

0.3.3.2 Cadre d'interopérabilité

Afin de remédier aux trois points faibles mentionnés dans l'image cible, un degré suffisant d'interopérabilité des données au niveau des interfaces est avant tout nécessaire. Le cadre d'interopérabilité se définit en ce sens sur la base du modèle d'information présenté ci-dessus:

- Systèmes d'identification et vocabulaire contrôlé
- Définition des données de base interopérables

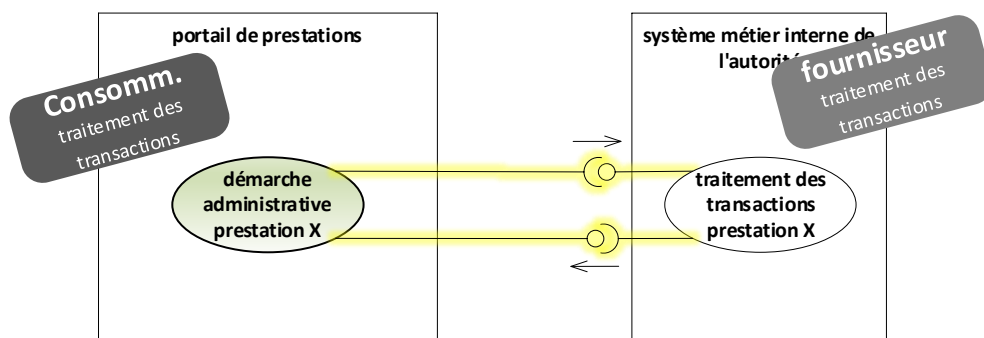
La figure suivante situe les éléments du cadre d'interopérabilité dans le modèle d'information:



0.3.3.3 Interfaces

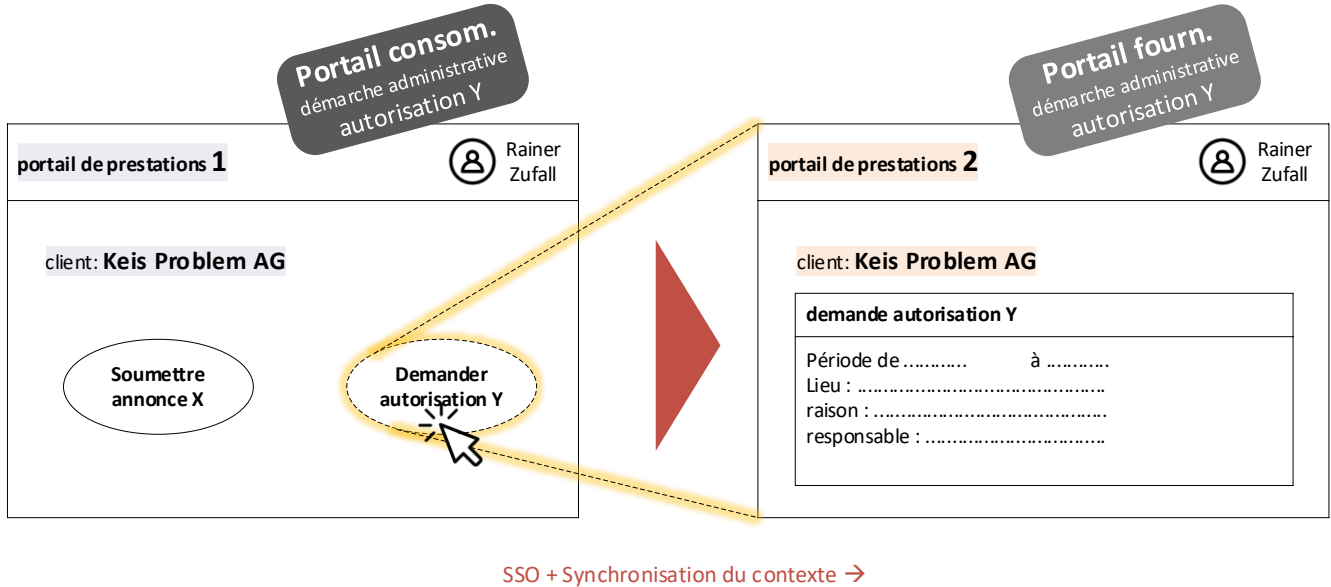
Sur la base du cadre d'interopérabilité, les interfaces associées aux deux modèles d'intégration sont normalisées pour répondre aux points faibles 2 et 3. Les deux modèles d'intégration, à leur tour, supportent le développement de portails inter-autorités axés sur des segments de clientèle spécifiques au sens du point faible 1/1a.

Pour l'interface **démarche administrative ↔ traitement des transactions** du modèle d'intégration 1, un cadre de processus de communication généraux est spécifié à la suite de la considération précédente liée au processus dans la section 0.3.1, sur la base duquel les contenus spécifiques à la prestation sont transmis. Ces modules peuvent également être utilisés pour cartographier les caractéristiques spécifiques du flux de la procédure, telles que les sous-processus, le transfert de la procédure ou l'initiation de processus du côté des autorités.



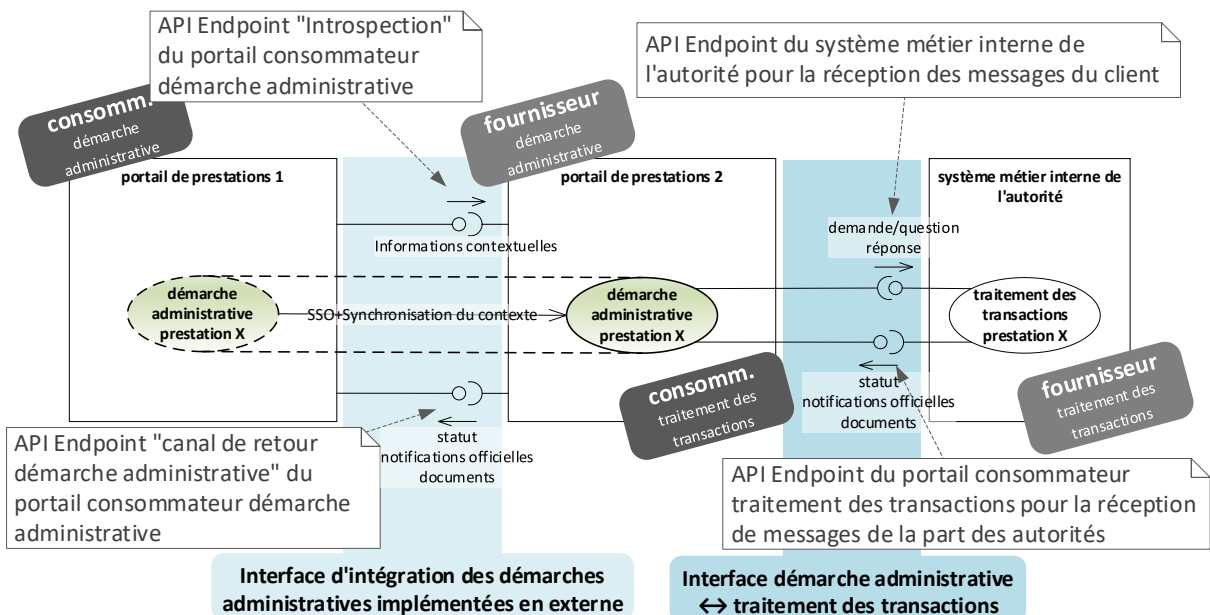
Un élément essentiel de l'interface d'intégration des démarches administratives implémentées en externe du modèle d'intégration 2 est la redirection, c'est-à-dire le transfert de la session utilisateur du portail vers le système externe ou le portail fournisseur au moment de l'exécution. Pour que l'utilisateur puisse continuer à travailler de manière transparente lorsqu'il passe à la démarche administrative intégrée (et implémentée sur un autre portail), le transfert ou la redirection doit s'accompagner d'une authentification unique (SSO) et d'une synchronisation

du contexte. Les processus d'interface nécessaires sont nommés et spécifiés à un niveau logique. En plus de traiter la démarche administrative, ils transfèrent également le contexte de la démarche administrative dans le portail consommateur vers le portail du fournisseur (le contexte étant composé du login utilisateur correspondant, de la sélection du client et du droit de gestion associé). Ce principe est illustré dans la figure suivante:



Des scénarios illustrent le fonctionnement de l'interface dans les constellations A) fournisseur d'identité partagé et B) confiance bilatérale entre pairs (peer-to-peer trust). Puisque B) peer-to-peer trust représente une solution découplée du fournisseur d'identité, elle est finalement préférée à A).

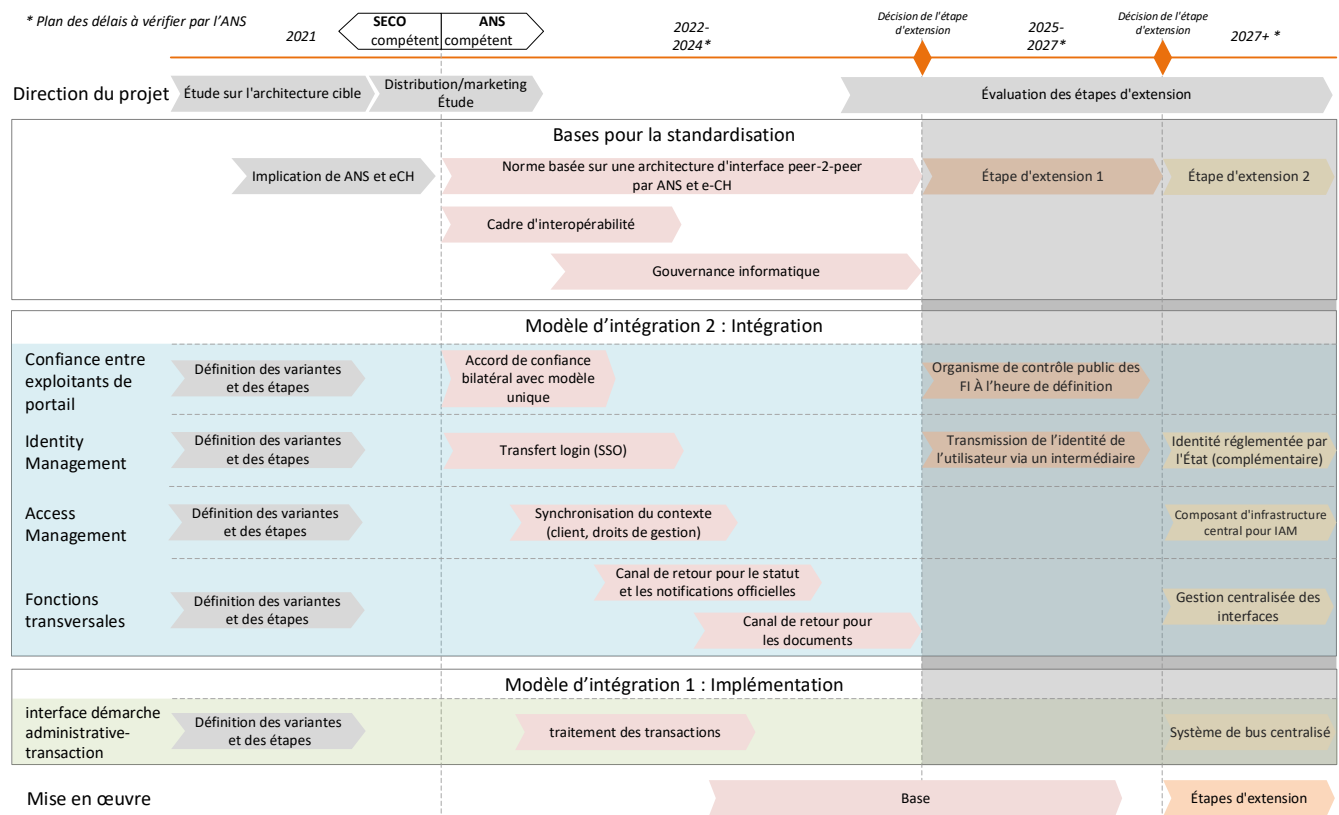
Le graphique suivant montre l'image globale des interfaces décrites à l'aide de l'exemple d'une démarche administrative intégrée via peer-to-peer trust, dont l'implémentation dans le portail fournisseur communique avec le système métier interne de l'autorité compétente qui se trouve derrière:



Enfin, l'ébauche de l'architecture cible d'intégration pour les deux interfaces précise que la souveraineté de définition de leur conception appartient au fournisseur respectif au-delà de la normalisation. Dans le cas du modèle d'intégration 1, il s'agit du système métier interne à l'autorité, dans le cas du modèle d'intégration 2, du portail fournisseur.

0.3.4 Recommandations pour la suite de la procédure

L'architecture cible d'intégration pour les portails de prestations administratives développée dans cette étude doit être mise en œuvre étape par étape. La feuille de route est divisée en phases, de sorte que les étapes d'extension facultatives peuvent être décidées à une date ultérieure.



(Représentation agrandie en format paysage à l'Annexe C)

Le processus de la mise en œuvre planifiée de l'architecture cible d'intégration sous la forme d'une ou plusieurs normes doit être dirigé par l'organisation "Administration Numérique Suisse" (ANS). Dans un premier temps, l'ANS doit examiner la feuille de route de mise en œuvre et initialiser des groupes de travail pour l'établissement d'une norme et la création de la base légale. Afin de pouvoir fonder la normalisation sur des valeurs empiriques, la mise en œuvre de projets pilotes avec la participation des autorités à tous les niveaux fédéraux est recommandée.

Le SECO, en tant que mandant de cette étude, participe à l'ambition de l'ANS "une identification numérique reconnue par toutes les autorités est établie" (voir rapport de base [37]) et apporte une contribution importante à l'étude.

0.4 Résultats Étape 2: Analyse des écarts d'EasyGov

Une deuxième version ultérieure de cette étude permettra d'évaluer quelles adaptations dans EasyGov sont nécessaires pour répondre à l'architecture cible d'intégration (analyse des écarts).

1 Situation initiale et objectif de l'étude

Les citoyens et les entreprises souhaitent de plus en plus profiter des prestations des autorités publiques par voie numérique. Outre le confort accru pour les utilisateurs grâce à un échange avec les autorités fédérales, cantonales et communales sans rupture de média, les prestations fournies numériquement peuvent être proposés par les autorités de manière plus flexible, plus efficace et de meilleure qualité.

L'élaboration de cette étude est basée sur les conditions cadres décrites ci-dessous.

1.1 Niveaux politique et légal

Afin d'offrir les prestations administratives de manière flexible et efficace, la mise à disposition numérique via des portails de prestations administratives est nécessaire. La base légale de cette démarche est notamment:

- l'art. 3 al. 3 LOGA, selon lequel l'activité de l'administration vise à atteindre les objectifs fixés et répond aux critères d'une bonne gestion
- La loi fédérale sur l'utilisation de moyens électroniques pour l'exécution des tâches des autorités (en consultation depuis le 11.12.2020).
- La loi sur l'allègement des coûts de la réglementation pour les entreprises (en consultation depuis le 28.4.2021)
- En outre, les recommandations du CDF issues de l'audit " Synergies potentielles des portails informatiques fédéraux - Chancellerie fédérale – TNI". Les motions actuelles à cet égard sont, par exemple, Mo. 20.4726 Glättli, qui donne un aperçu des initiatives politiques actuelles.

1.2 Objectifs de l'«Administration numérique suisse»

Selon le rapport de base [37] , l'objectif de l'organisation nouvellement créée «Administration numérique suisse» (ANS) est le suivant (extrait): "[le projet ANS] vise à renforcer durablement la collaboration tant verticale qu'horizontale aux trois échelons étatiques". Le rapport sur l'agenda de l'ANS décrit notamment les ambitions suivantes:

- Un canal numérique est établi entre la population et l'administration
- Le potentiel d'automatisation et de simplification au profit de l'économie est pleinement exploité
- Une identification numérique reconnue par toutes les autorités est établie

Dans le contexte de l'«Administration numérique suisse », des aspects du renforcement de la coopération entre les niveaux de l'administration dans la transformation numérique sont abordés.

Au niveau fédéral, la stratégie informatique de la Confédération² contribue également à la mise en œuvre des stratégies du Conseil fédéral, notamment la stratégie Suisse numérique et la stratégie de cyberadministration.

Des axes stratégiques et des domaines d'action ont été définis à cette fin. Ces axes stratégiques sont coordonnés avec la stratégie «Suisse numérique», la stratégie nationale de protection contre les cyber-risques, la stratégie suisse de cyberadministration et le rapport final du DFF et de la Conférence des gouvernements cantonaux sur le projet «Administration numérique».

Dans le cadre de l'axe stratégique C, les domaines d'action C1 (Pratiquer la focalisation sur les clients et donner l'exemple en la matière) et C2 (Fournir des portails et des interfaces)³ sont pertinents dans le contexte de cette étude: les prestations administratives sont mises à la disposition des utilisateurs via des portails (homme à machine) et/ou des interfaces électroniques (machine à machine). Les portails et interfaces partagés existent afin de fournir des prestations plus rapidement, de manière plus rentable et avec moins de risques.

En principe, les prestations administratives électroniques devraient être proposées de manière "intégrale": normalisées, réutilisables, conçues de manière transversale, interopérables.

1.3 Objectif de mise en œuvre UZ1 de la cyberadministration suisse

Le développement du guichet unique pour les prestations administratives destiné aux entreprises sous le nom de EasyGov.swiss est un projet stratégique de la cyberadministration suisse et faisait partie du plan stratégique 2016 - 2019, où le projet était répertorié sous le titre "Portail administratif destiné aux entreprises". Cet objectif s'inscrit dans le cadre de la stratégie précédente et de la stratégie prévue pour la "Suisse numérique" (voir [41], chapitre 4.6: "les obstacles administratifs doivent être encore réduits et les échanges entre entreprises et les autorités centralisés").

EasyGov fait également partie du plan de mise en œuvre de la cyberadministration suisse pour la période législative 2020-2023. L'objectif de mise en œuvre "Développer le portail EasyGov.swiss" est défini dans le cadre de l'objectif stratégique " Développer des offres numériques en matière d'interaction et de participation à l'échelle nationale", voir [19]⁴.

En outre, deux mesures sont définies pour atteindre l'objectif de mise en œuvre "Développer le portail EasyGov.swiss" (OMO1):

- M1: Réalisation d'une étude examinant l'architecture du portail sous l'angle de la faisabilité de l'intégration des prestations fédérales, cantonales et communales, avec la participation des acteurs concernés.
- M2: Intégration dans EasyGov de prestations administratives cantonales destinées aux entreprises, si plusieurs cantons souhaitent cette intégration.

² https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/strategie-planung/ikt-strategie_bund_2020-2023.html

³ Dans le cadre du domaine de mesure "C2 Fournir des portails et des interfaces", l'architecture API de la Confédération [34] est notamment en cours de développement.

⁴ S'applique généralement à la présente étude: le numéro entre crochets renvoie à la section "Documents référencés" au début.

Cette étude porte sur la mesure M1 "Examen de l'architecture". Les responsables de la cyberadministration dans les cantons souhaitent en particulier une révision de l'architecture - notamment en ce qui concerne la sécurité de la planification, la protection des investissements et la promotion des prestations de cyberadministration à tous les niveaux fédéraux - afin d'examiner en détail dans une étude la faisabilité de l'intégration des prestations cantonales et communales sur EasyGov et inversement, c'est-à-dire l'intégration des prestations d'EasyGov sur les portails cantonaux.

Dans un premier temps, une architecture cible **générale** et globale pour le domaine des portails de prestations administratives⁵ sera développée. Ensuite, dans une deuxième étape, on évaluera quelles adaptations sont nécessaires dans le portail EasyGov pour répondre à l'architecture cible globale (analyse des écarts).

Les objectifs suivants en découlent:

- Formulation d'une architecture cible d'intégration grossière pour les portails de prestations administratives sur la base d'une évaluation des besoins.
 - Développement systématique selon TOGAF⁶:
 - Architecture d'entreprise (objets d'entreprise, processus, mise à disposition des prestations de l'autorité)
 - Architecture technique du système d'information (objets de données, applications/services, interfaces, canaux de transmission, responsabilités)
 - Prise en compte de l'interopérabilité⁷ des identités (personnes physiques, personnes morales) et de leurs autorisations
 - Proposition de l'architecture cible comme ébauche d'une norme eCH
 - Forme une sous-architecture de l'OMO14 / M2 "Définition de l'architecture globale de la mise en œuvre de la stratégie suisse de cyberadministration 2020–2023."⁸
 - Peut être utilisé comme objectif pour UZ14 / M4 "Réalisation d'un projet pilote d'intégration de services en ligne dans divers portails Internet."⁸

⁵ Les portails de prestations administratives sont des applications accessibles au public (par exemple, une application à page unique, une application mobile, etc.) avec lesquelles un exploitant de portail offre au client un canal d'accès numérique à une ou plusieurs prestations administratives dans le cadre de la cyberadministration. Il représente le front-end client d'une prestation administrative. Voir également les explications des termes au chapitre 2.1.5, Tableau 1.

⁶ Voir l'Annexe G.C pour un ancrage de TOGAF

⁷ L'EIF [17] définit l'interopérabilité comme suit: *Interoperability is the ability of organisations (= public administration units or any entity acting on their behalf, or EU institutions or bodies) to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these organisations, through the business processes they support, by means of the exchange of data between their ICT systems.*

⁸ Se réfère à l'objectif de mise en œuvre 14 "Élaborer et gérer l'architecture de la cyberadministration compte tenu du plan de mise en œuvre stratégique", voir [19]

- Analyse des écarts entre l'état actuel et l'état cible de l'architecture du portail EasyGov par rapport à l'architecture cible interportails.
- Une planification grossière pour éliminer les lacunes d'EasyGov

Important: l'architecture cible d'intégration grossière prévue pour les portails de prestations administratives ne se concentre pas sur les architectures de système des portails individuels, mais plutôt sur un "écosystème" interportails qui régule l'interaction et améliore l'interopérabilité⁷, voir la Figure 1.

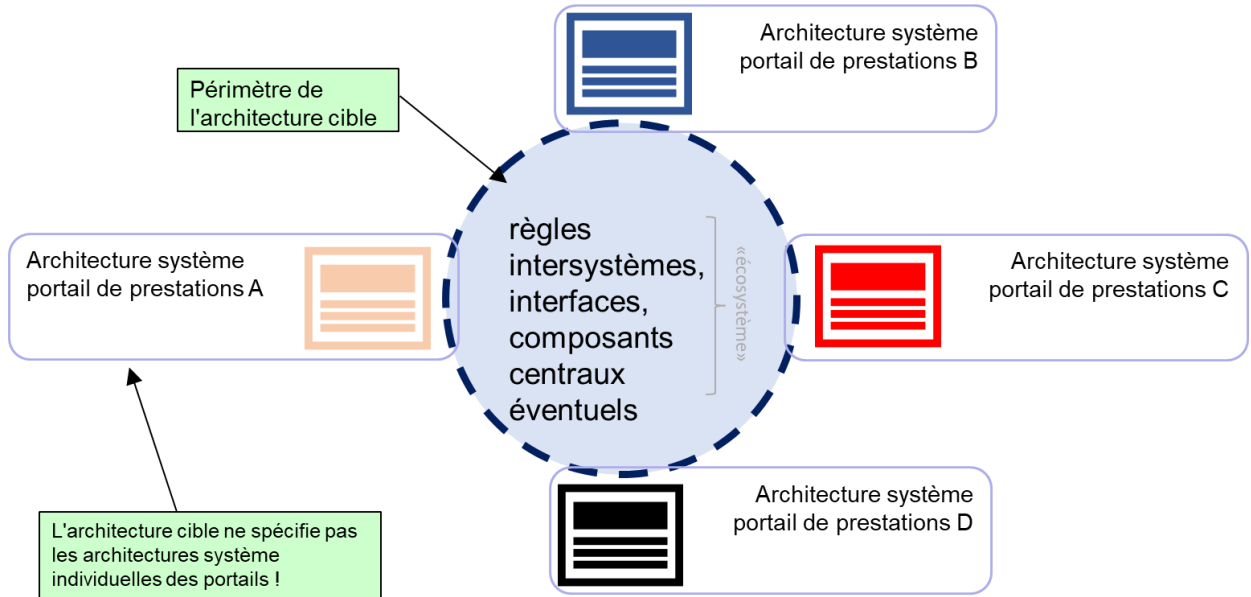


Figure 1: Périmètre de l'architecture cible d'intégration (représentation schématique)

2 Architecture cible d'intégration pour les portails de prestations administratives

2.1 Analyse de la situation des portails de prestations administratives d'un point de vue logique

La première étape consiste à identifier les composants essentiels des portails de prestations administratives (ci-après appelés portails de prestations) afin d'obtenir une base conceptuelle pour les chapitres suivants.

2.1.1 Vue du processus d'une prestation administrative

Malgré l'abondance des prestations administratives fédérales, cantonales ou communales (voir [27]), les modèles typiques suivants peuvent être identifiés en accord avec le modèle de phase de la procédure administrative présenté dans eCH-0126 [14] et les types de prestations mentionnés dans eCH-0138 [15]:

- Procédure d'autorisation (par exemple, permis de construire)

- Procédure d'annonce (par exemple, procédure d'annonce pour les activités lucratives de courte durée des ressortissants de l'UE/AELE)
- Procédure de demande (par exemple, demande de confirmation de résidence ou de naturalisation)
- Procédure d'enregistrement (par exemple, l'enregistrement de la TVA)
- Procédure de déclaration (par exemple, déclaration de TVA)
- Prestations d'information (par exemple, information sur le recouvrement des créances)

La procédure d'autorisation se révèle être la plus complexe. Il suit le schéma suivant: un client⁹ (personne morale ou physique) soumet une demande pour une prestation spécifique de l'autorité et déclenche ainsi une transaction dans l'autorité concernée. L'autorité traite la demande et communique au client un message réponse sur le statut du traitement ou toute question. Au cours du traitement, il peut être nécessaire d'obtenir des éclaircissements ou l'approbation d'autres autorités. Après un examen approfondi des documents de demande, l'autorité communique le résultat (positif ou négatif) au client à la fin de la procédure¹⁰, par exemple sous la forme d'un permis ou d'une décision.

⁹ Le terme client est décrit plus en détail dans le modèle d'information, chapitre 2.1.5

¹⁰ Dans certains cas, un transfert vers un autre bureau d'une administration a lieu pendant la procédure, ce qui fait que le client reçoit le résultat de la procédure de ce bureau. C'est le cas, par exemple, des procédures d'autorisation de travail des ressortissants de pays tiers dans les villes de Berne, Thoun ou Bienne. La demande doit d'abord être soumise à l'Office de l'économie du canton de Berne, qui est responsable de la décision préliminaire. L'Office transfère ensuite la procédure à l'autorité compétente en matière de migration. En général, la responsabilité incombe au canton, mais dans le cas où le lieu de travail est Berne, Thoun ou Bienne, c'est la commune qui est responsable. Le client reçoit le résultat de la procédure de cette autorité et non de celle où la demande a été initialement introduite.

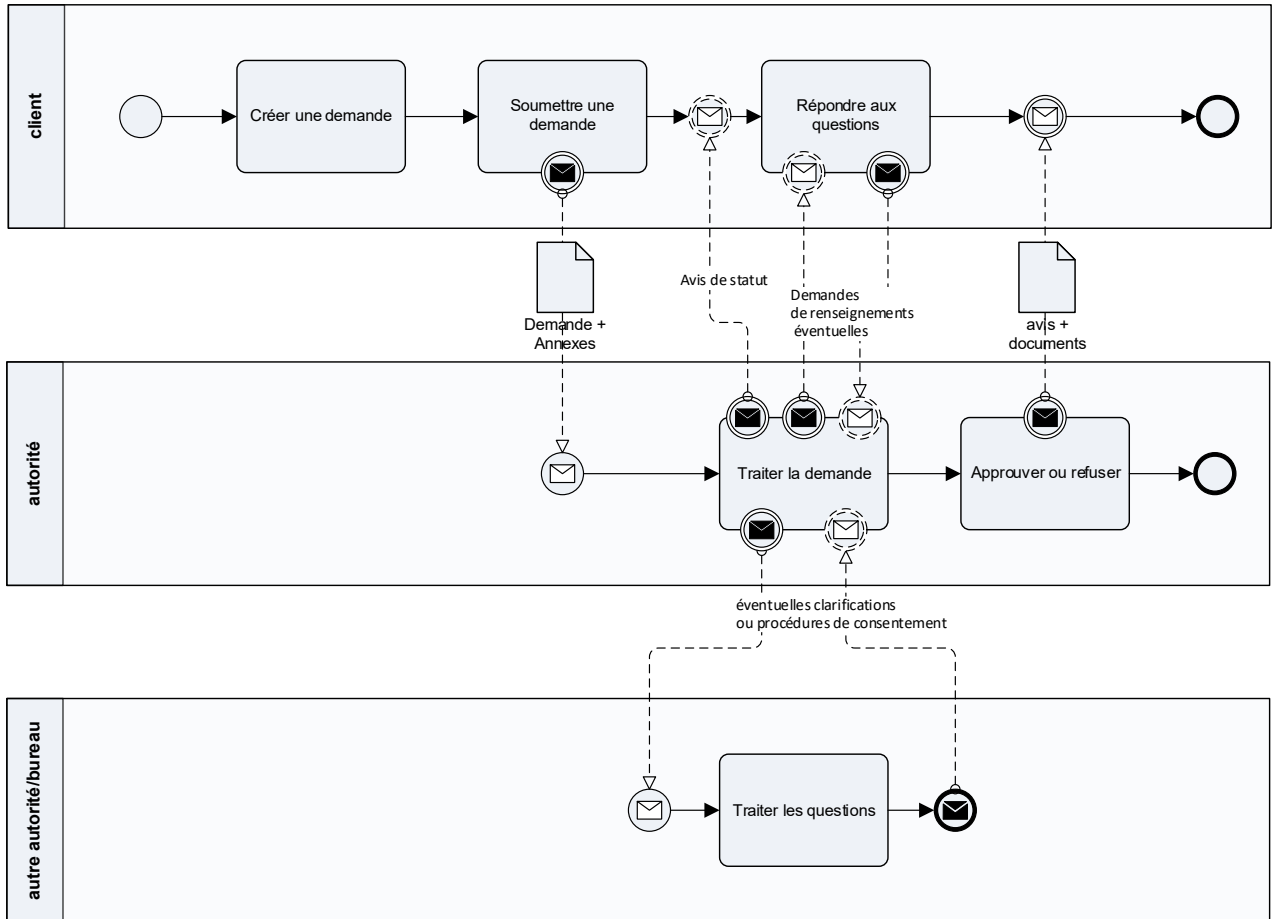


Figure 2: Flux général d'une procédure d'autorisation (diagramme BPMN)

La procédure d'annonce est comparativement la moins complexe. Il s'agit d'une procédure à sens unique. Au lieu d'une autorisation, une annonce obligatoire (par exemple, le démarrage d'un travail) doit être soumise. Le client envoie les informations requises à l'autorité compétente, qui achève la procédure pour lui. Pour l'autorité concernée, l'annonce déclenche une autre transaction, qui peut donner lieu à des mesures supplémentaires (par exemple, des contrôles distincts).

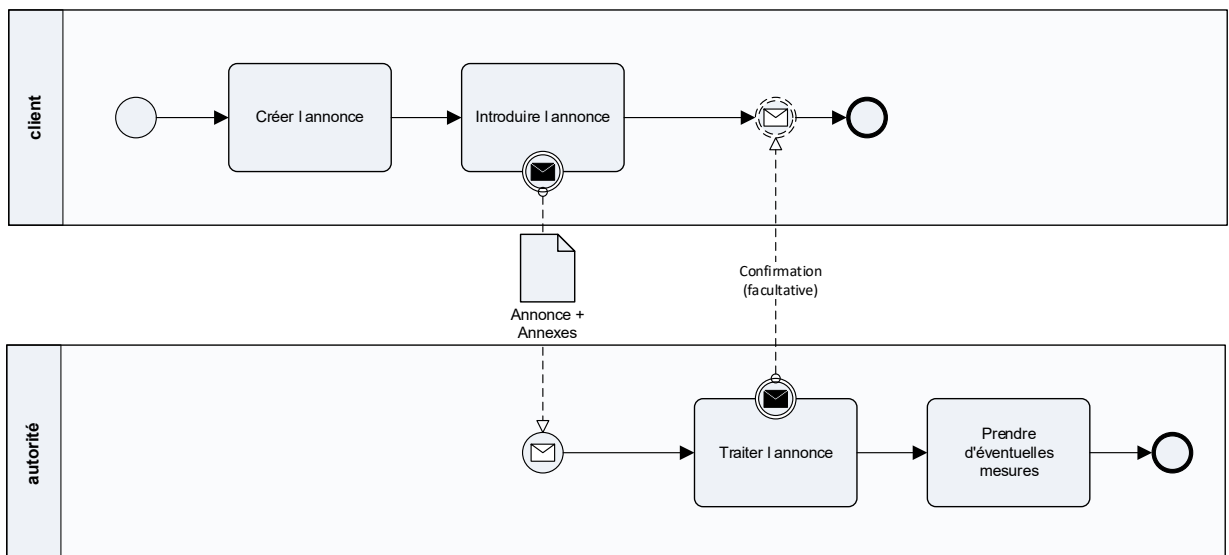


Figure 3: Flux général d'une procédure d'annonce (diagramme BPMN)

Les autres procédures mentionnées se situent entre ces deux points extrêmes. Ainsi, les procédures d'annonce, de demande, d'enregistrement et de déclaration représentent chacune un sous-ensemble de la procédure d'autorisation.

En termes abstraits, le traitement d'une prestation administrative peut être résumé comme un processus côté client et un processus côté autorité. Conformément à la terminologie diffusée par les normes eCH 0088, 0126 [14] et 0138 [15], le processus côté client est appelé **démarche administrative** et le processus côté autorité est appelé **transaction**.

Note: Pour le traitement des transactions par les autorités compétentes, les délais doivent être respectés conformément aux délais prescrits par la loi. Ceci n'est pas représenté dans les diagrammes BPMN de la Figure 2 et de la Figure 3 pour des raisons de clarté, car elles ne sont pas pertinentes pour la suite.

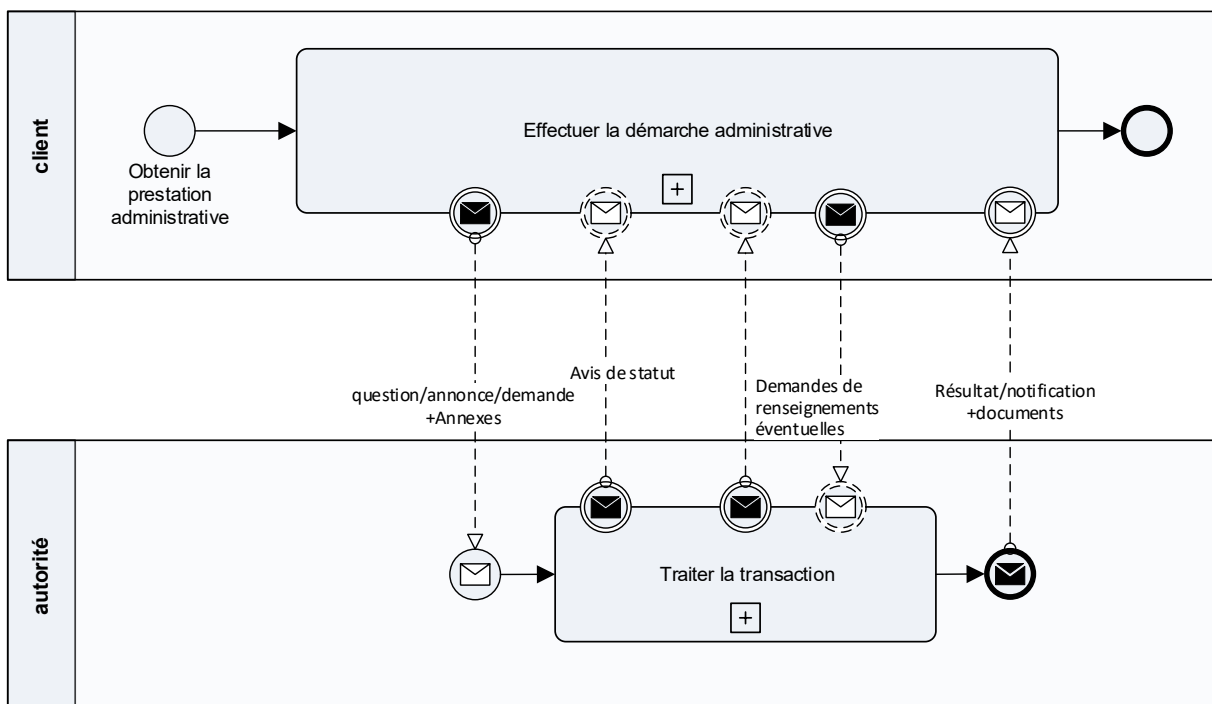


Figure 4: Abstraction du traitement d'une prestation administrative en tant que processus fonctionnant en parallèle du côté du client et de l'autorité

Dans des cas particuliers - comme déjà mentionné dans la précédente Figure 2 - d'autres bureaux de la même autorité ou d'une autre autorité peuvent être impliqués dans le traitement des transactions. Il existe deux modèles pour cela:

- Sous-processus (voir Figure 5)
- Transfert de la procédure (voir Figure 6)

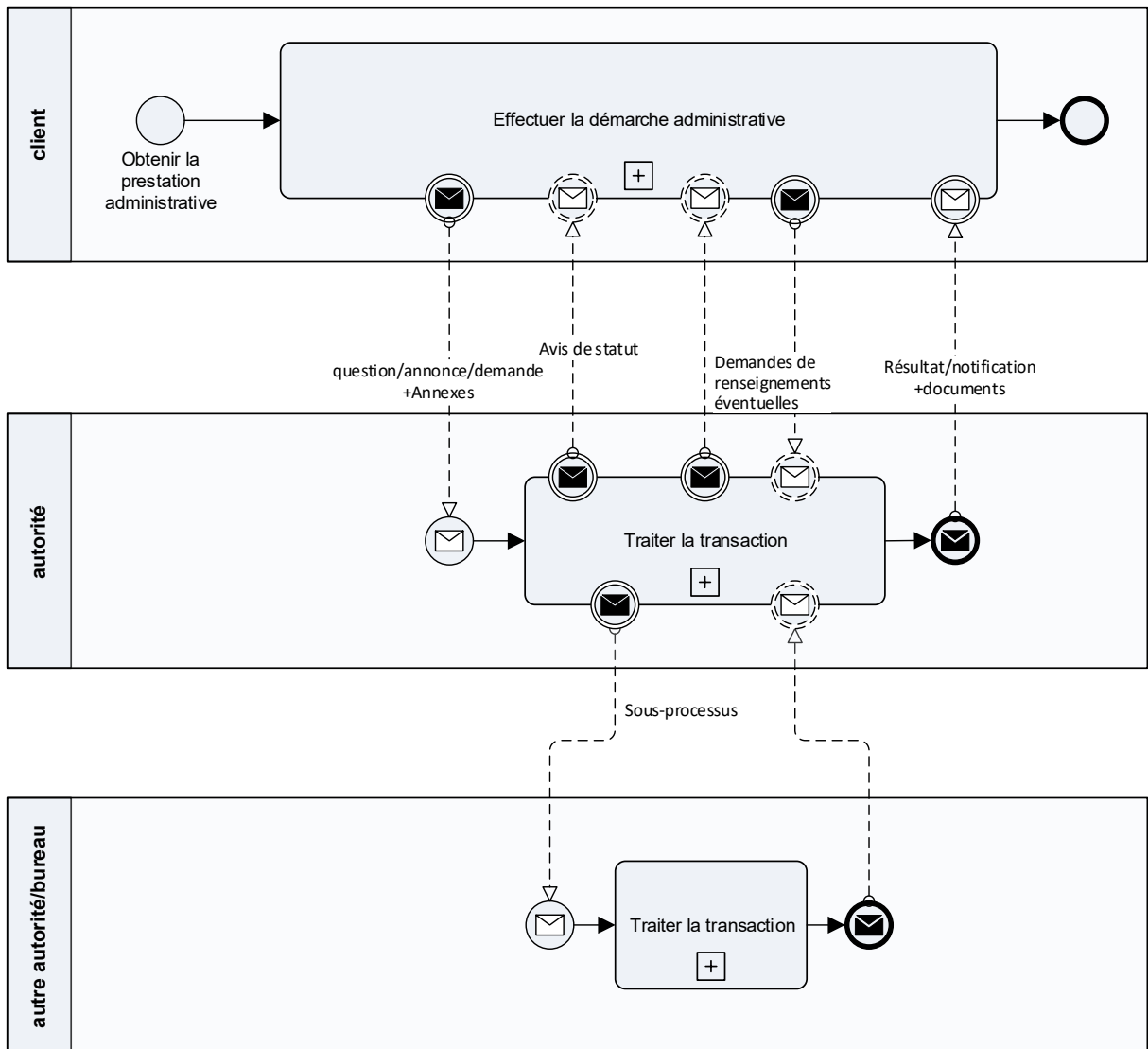


Figure 5: Implication d'une autre autorité/d'un autre bureau dans le traitement des transactions selon le modèle de sous-processus

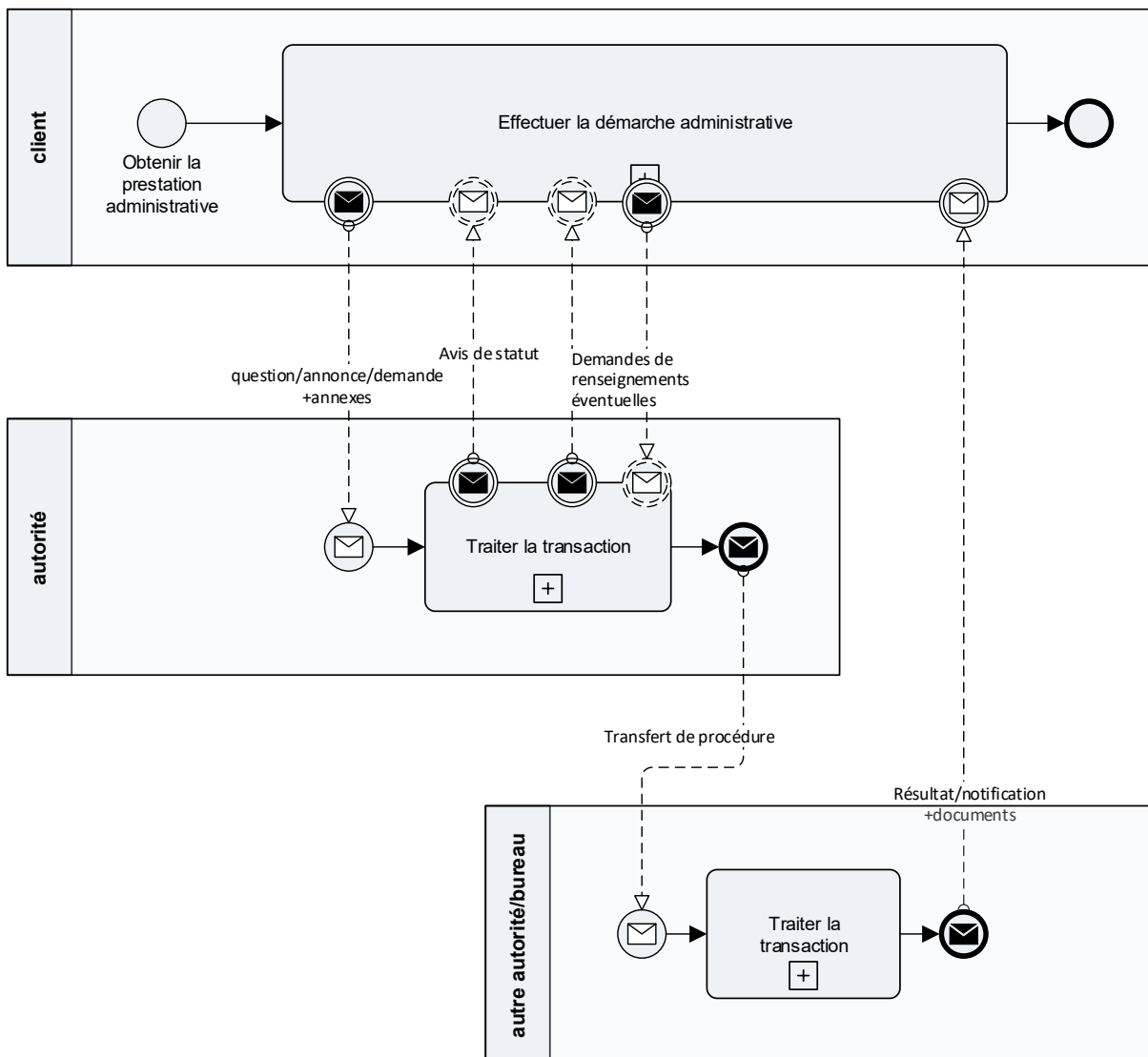


Figure 6: Implication d'une autre autorité/d'un autre bureau dans le traitement des transactions selon le modèle de **transfert de la procédure**

Alors que dans le premier modèle de sous-processus, les autres bureaux impliqués n'apparaissent pas directement envers le client, dans le second modèle de transfert de la procédure, le client est confronté à un changement de responsabilités.

Note: Dans le contexte de cette étude, l'accent est mis sur des prestations administratives qui ne peuvent être obtenus de manière anonyme et qui sont liées à une transaction. Ainsi, les prestations d'information utilisables de manière anonyme en libre-service (comme par exemple un calculateur d'impôts) n'en font pas partie, de même que les prestations qui ne déclenchent pas de transaction au sein de l'autorité (comme par exemple l'outil de gestion des parts de contingent concernant une autorisation générale d'importation délivrée par l'OFAG¹¹). Le premier cas relève de la couche d'information

¹¹ Voir <https://www.ekontingente.admin.ch/ekontingente/#/info/info-page/public/-1>

introduite au chapitre 2.1.3, le second peut être supporté par le modèle d'intégration 2 (intégration) introduit au chapitre 2.1.6, malgré l'exclusion mentionnée ci-dessus.

2.1.2 Le portail de prestations comme canal d'accès numérique

À l'aide d'un portail de prestations¹², un exploitant de portail offre des prestations administratives au client au niveau numérique (voir la Figure 7¹³). Il représente un canal d'accès pour le client à une ou plusieurs démarches administratives. L'autorité elle-même peut également faire office d'exploitant de portail (voir la Figure 8). De même, un exploitant de portail ou l'autorité elle-même peut être client d'une autre prestation sur un autre portail.

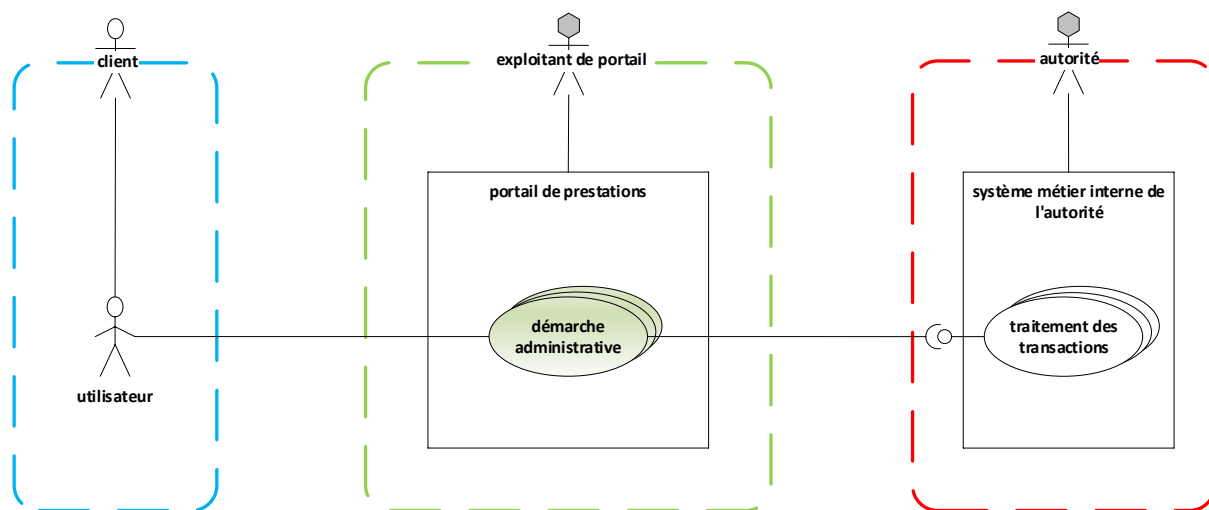


Figure 7: Portail de prestations comme canal d'accès numérique à une ou plusieurs prestations de l'autorité pour le client (diagramme Use-Case UML)

¹² Parfois aussi appelé "plate-forme". Voir l'explication des termes dans le Tableau 1, chapitre 2.1.5

¹³ Dans ces illustrations et dans toutes les illustrations ultérieures, des relations entre le client, l'exploitant de portail et l'autorité, le code couleur suivant s'applique aux acteurs: client = bleu, exploitant de portail = vert, autorité = rouge. Tous les éléments situés dans une case de couleur sont sous la responsabilité de l'acteur correspondant.

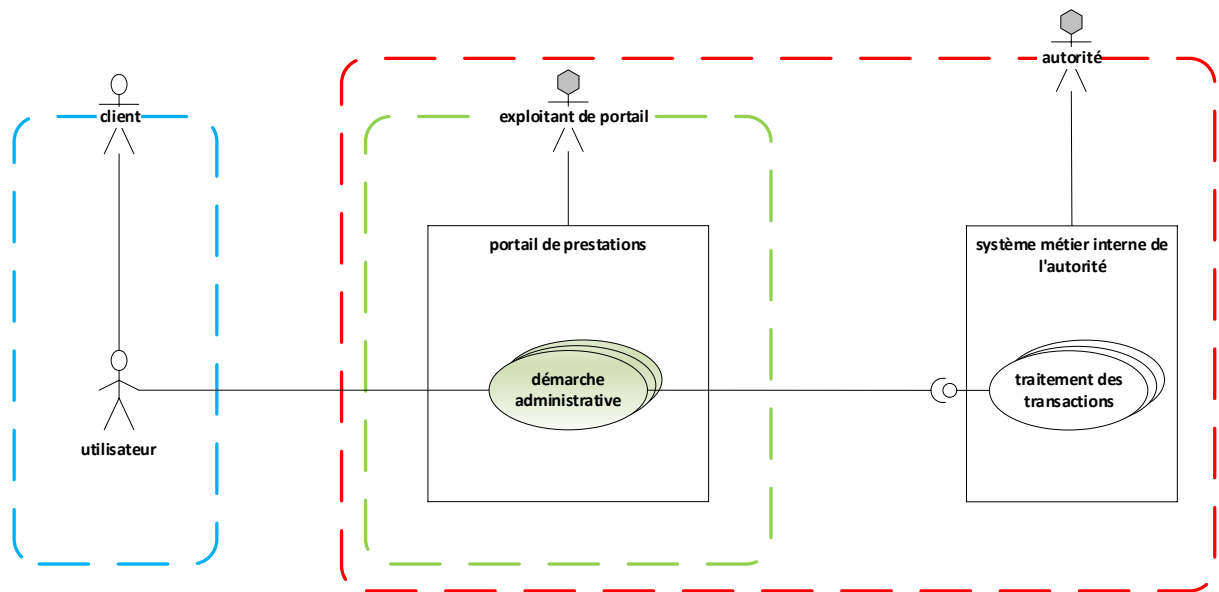


Figure 8: L'exploitant du portail peut aussi être l'autorité elle-même

Du point de vue de l'utilisateur, un portail de prestations en soi ne fait que représenter les besoins du client ainsi que toute communication entre lui et l'autorité concernée et n'intervient pas dans les processus internes de l'autorité. Selon la Figure 4 cela correspond aux relations du client avec l'autorité. Dans ce cadre, le portail de prestations communique avec le système métier interne de l'autorité compétente, qui prend en charge le traitement des transactions. La Figure 9 ci-dessous illustre cette délimitation:

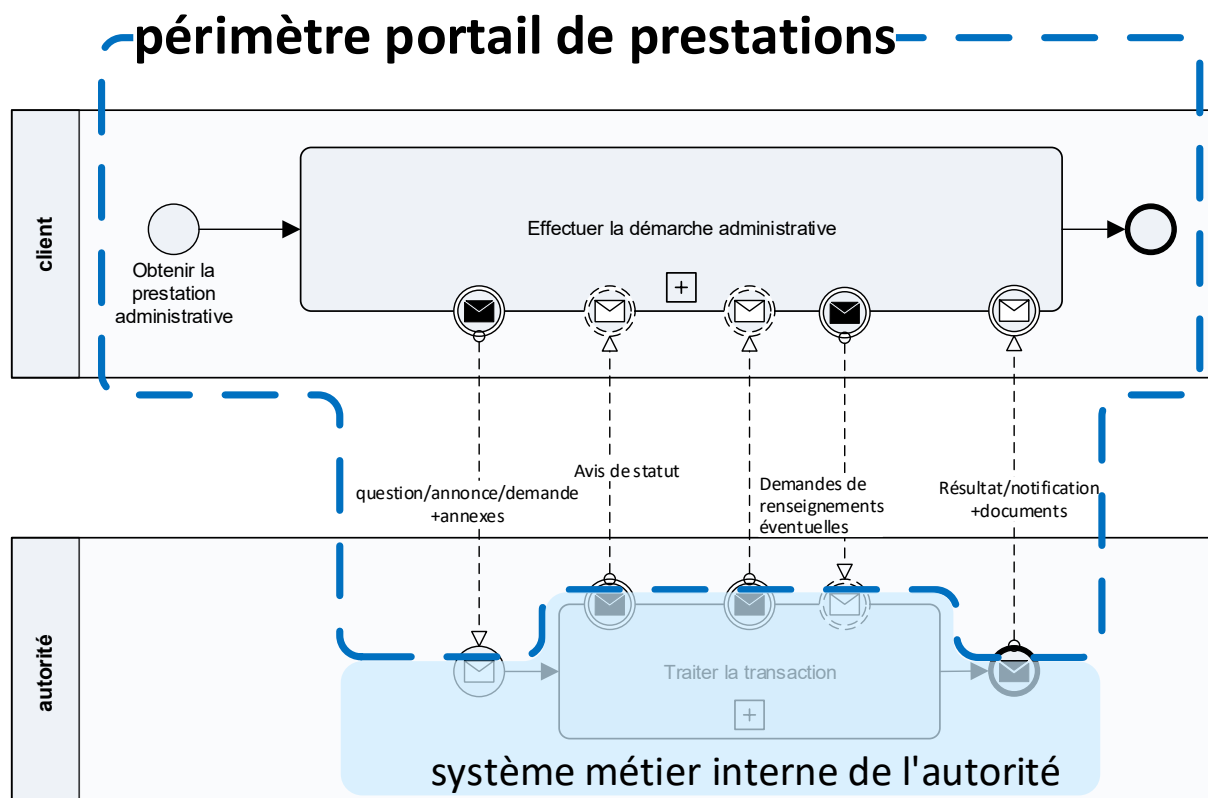


Figure 9: Délimitation du périmètre d'un portail de prestations au processus côté client. En revanche, les processus internes à l'autorité sont pris en charge par le système métier de l'autorité.

Un portail de prestations peut être compris comme un front-end client¹⁴ qui, au sens de la Figure 9, prend en charge l'interface entre le client et l'autorité. Le terme "client" doit être considéré comme un terme abstrait au sens d'un sujet de droit, qui peut représenter une personne morale ou physique. Dans tous les cas, la règle suivante s'applique: la démarche administrative numérique est effectuée par un utilisateur du portail de prestations qui agit pour le compte du client. Dans le cas de "client = personne physique", les rôles de client et d'utilisateur sont généralement remplis par la même personne physique (mais parfois non, par exemple lorsque le conseiller fiscal effectue la déclaration fiscale pour son client).

2.1.3 Structure fonctionnelle d'un portail de prestations

Outre la représentation pure et simple du processus officiel, un portail de prestations peut également fournir une assistance au client, en particulier à la question suivante: "J'ai XX en tête, quels prestations sont pertinents pour cela? Quelle autorité en est responsable? Pour différencier ce niveau de la prestation réelle de l'autorité, on adopte la terminologie utilisée dans [18], qui distingue la couche d'information et la couche transactionnelle. La couche d'information présente l'offre de prestations de l'autorité, sous quelque forme que ce soit, tandis que la

¹⁴ Voir également la définition de frontend/backend dans le glossaire à l'Annexe A. Du point de vue du client, le portail de prestations est le frontend et le système métier interne de l'autorité est le backend.

couche transactionnelle décrit le traitement de la prestation, c'est-à-dire de la démarche administrative correspondante. Suivant l'exemple de la Figure 9 précédente, la Figure 10 suivante situe les deux couches du point de vue du processus:

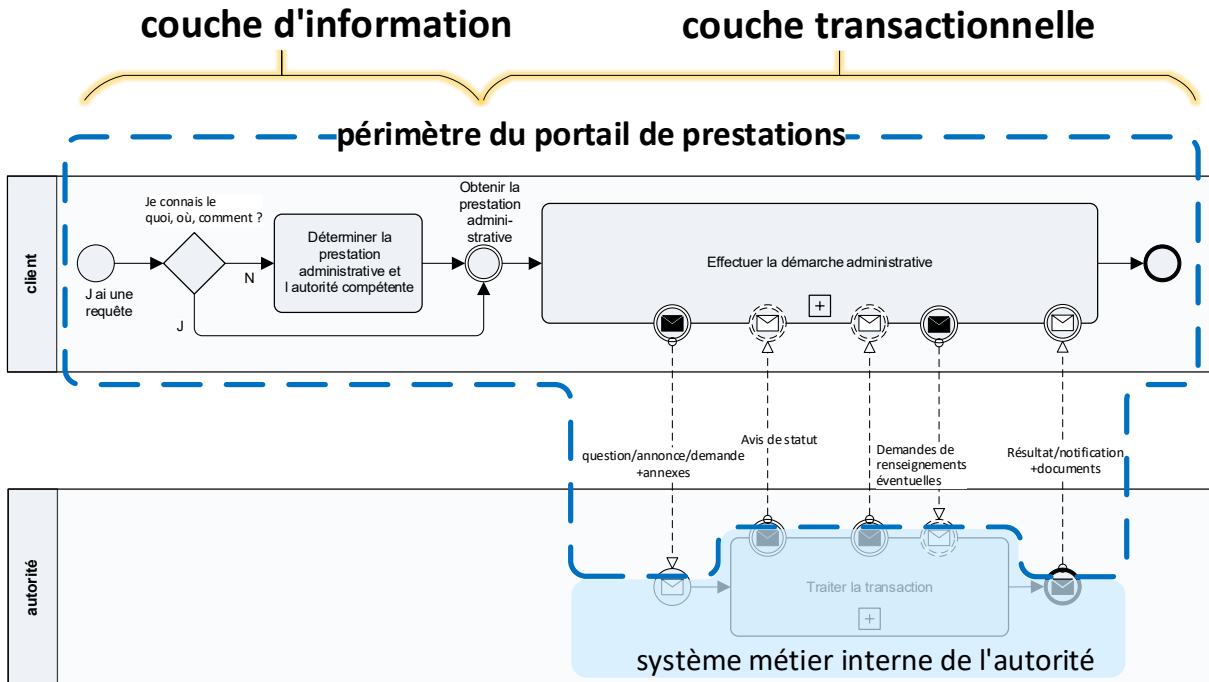


Figure 10: Emplacement des couches d'information et transactionnelle du point de vue du processus

Enfin, la couche d'information sert à guider l'utilisateur vers une prestation spécifique, pour laquelle il peut finalement lancer une démarche administrative dans la couche transactionnelle. Les clients administratifs demandent et obtiennent des prestations administratives sur la base de requêtes qui reflètent des situations de vie spécifiques (par exemple, un mariage, un déménagement) ou des situations professionnelles (par exemple, la création d'une entreprise)¹⁵. Comme l'illustre la Figure 11, une orchestration de prestations peut être proposée à cette fin. Cette orchestration conduit l'utilisateur d'une telle requête au moyen d'un assistant à travers toutes les prestations obligatoires et facultatives pertinentes - pratiquement sur un "fil". Un exemple en est la représentation de la création d'une entreprise dans EasyGov, qui guide l'utilisateur pas à pas à travers les formalités et enregistrements nécessaires (registre du commerce, AVS, TVA, etc.).

¹⁵ Une vue d'ensemble des situations de vie ou professionnelles typiques peut être trouvée dans [38] et [39].

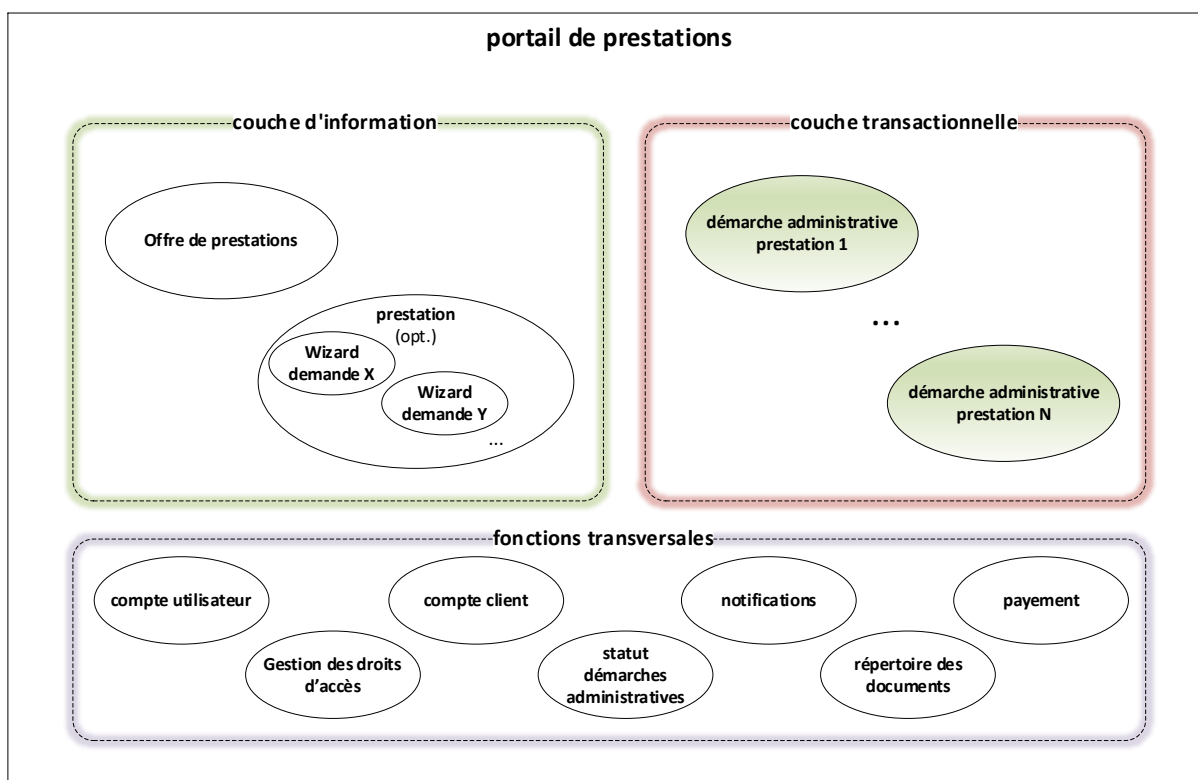


Figure 11: Structure fonctionnelle de base d'un portail de prestations

En outre, la Figure 11 montre qu'un portail de prestations peut contenir un certain nombre de fonctions transversales qui sont utilisées dans les deux couches. Les fonctions transversales typiques sont, par exemple:

- Compte utilisateur
- Gestion des autorisations
- Compte client¹⁶
- Etat des démarches administratives
- Notifications officielles
- Stockage des documents

L'étendue des fonctions transversales varie selon l'éventail des portails de prestations existants. Par exemple, il existe des portails où la couche d'information n'est pas réalisée en grande partie dans le portail lui-même, mais sur le site Web de l'autorité concernée. Dans ce cas, la couche d'information n'a pas de fonctions transversales au sens susmentionné. On peut interpréter de

¹⁶ Parfois également appelé gestion des données de base (clients) ou gestion des partenaires commerciaux. Pour la clarification des synonymes, voir le glossaire sous 4

la même manière les couches transactionnelles réalisées sous forme de formulaires électroniques sans état¹⁷, qui n'ont pas non plus de fonctions transversales.

En définitive, on constate que dans les portails de prestations existants, la portée des trois niveaux logiques - couche d'information, couche transactionnelle et fonctions transversales - varie en fonction de leur orientation spécifique. Le schéma suivant illustre cette diversité à l'aide d'exemples.

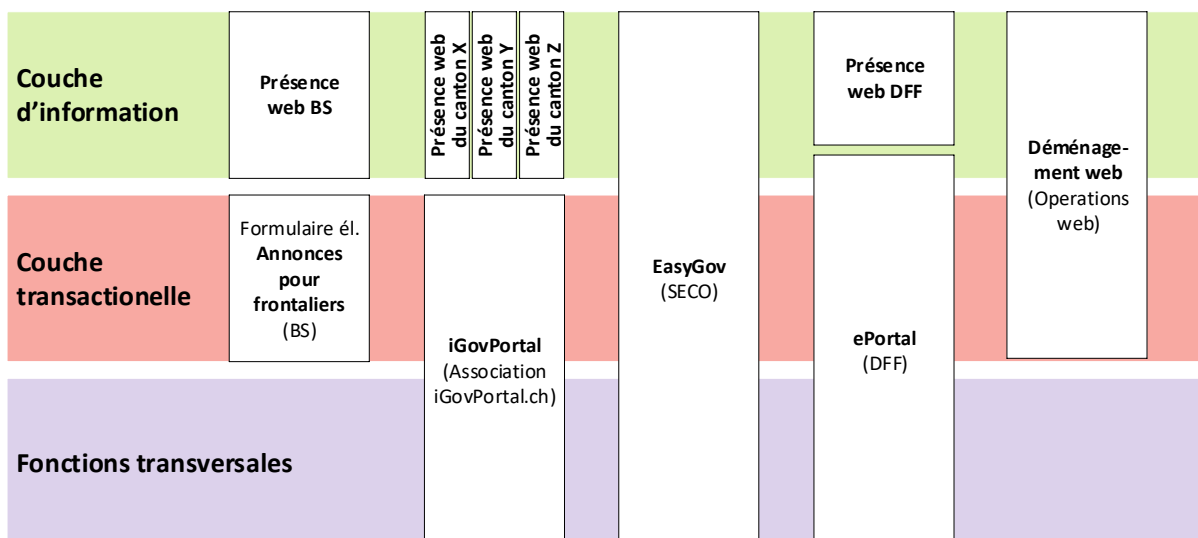


Figure 12: Diverses caractéristiques des couches dans les portails de prestations existants

En outre, l'exemple du ePortal fédéral exploité par l'OFIT¹⁸ présenté à la Figure 12 montre que les différentes couches peuvent également être réparties sur plusieurs sous-systèmes. Cela permet de séparer les responsabilités: Alors que l'ePortal est développé par l'OFIT et relève de la responsabilité de ce dernier, les démarches administratives sont réalisées par les offices responsables respectifs, comme l'application portail métier "Décompte TVA easy" qui relève de la responsabilité de l'AFC. Les institutions concernées travaillent ensemble en tant que communauté d'exploitants de portail.

¹⁷ Voir le glossaire à l'Annexe A

¹⁸ Voir <https://eportal.admin.ch>

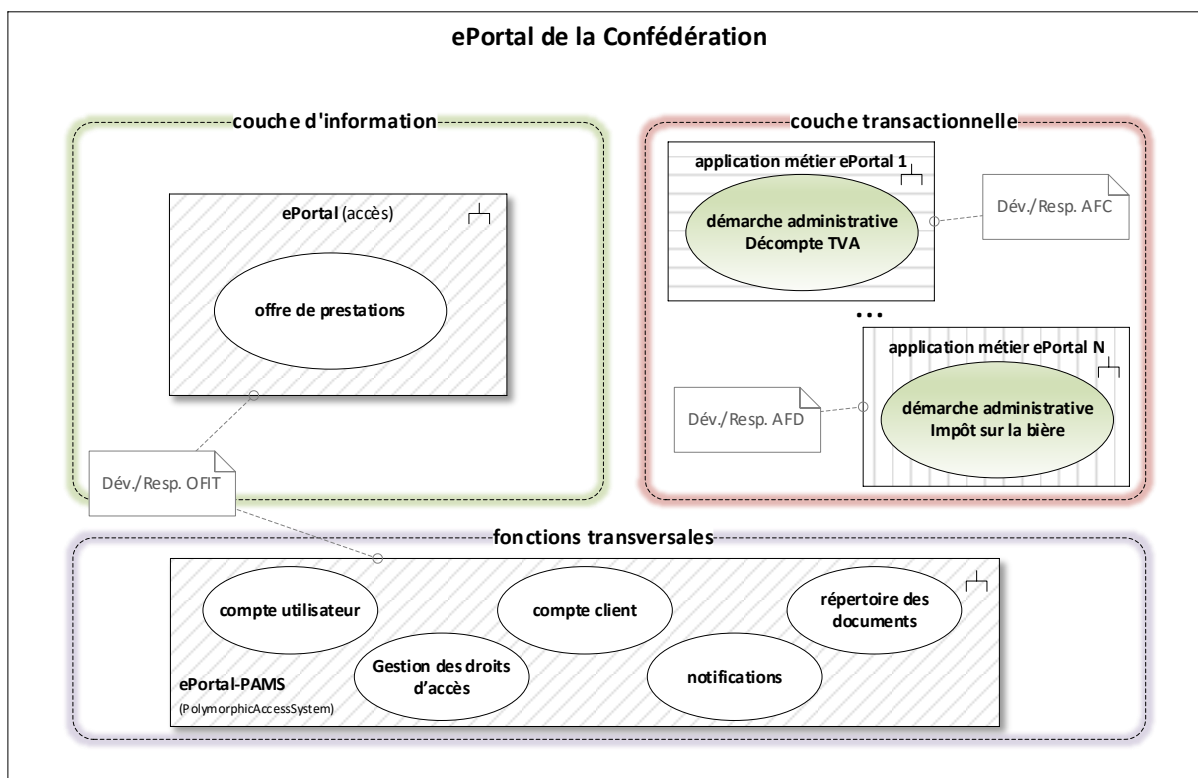


Figure 13: Structure de l'ePortal avec des sous-systèmes distribués sous différentes responsabilités

2.1.4 Paysage des portails de prestations

Les portails de prestations existants ou en cours de création en Suisse ont généralement été créés indépendamment les uns des autres et représentent chacun un ensemble spécifique de prestations administratives. Cet ensemble est basé sur l'orientation du contenu des portails, qui peut être soit se concentrer sur

- (A) le portefeuille d'une autorité (voir Figure 14, p. ex. guichet en ligne du canton SG, guichet virtuel du canton FR, ePortal fédéral).
- ou (B) les besoins spécifiques d'un groupe-cible de clients (voir Figure 15, par exemple EasyGov pour les entreprises).
- ou (C) un hybride des deux.

Dans chaque cas, l'orientation du portail de prestations respectif se reflète dans sa couche d'information.

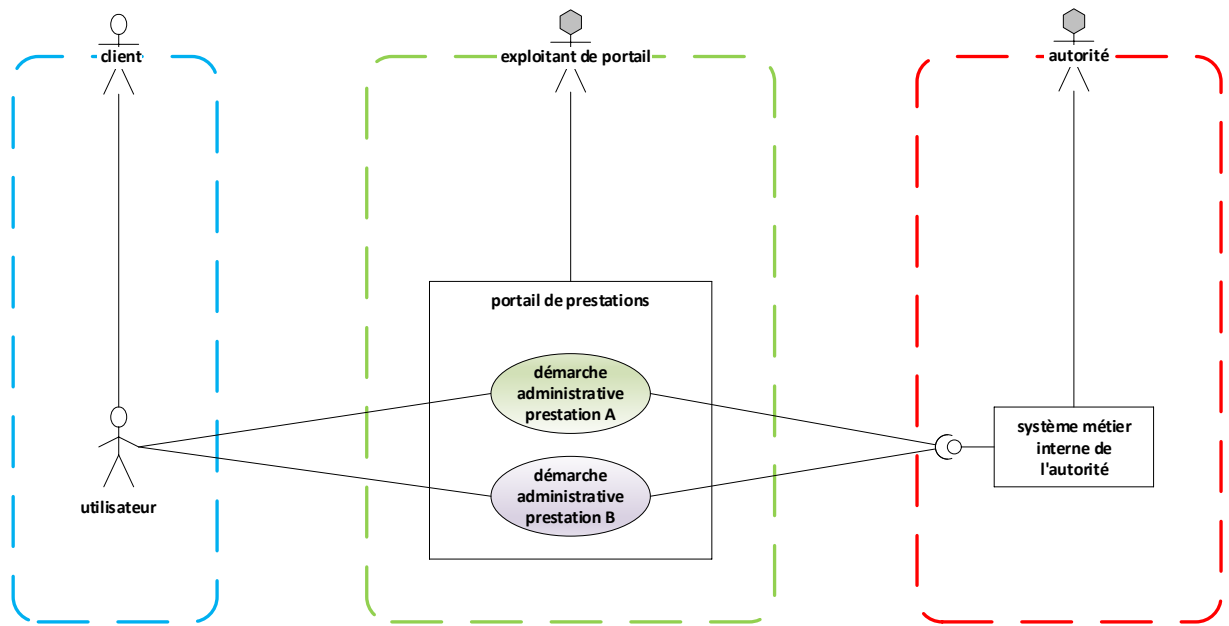


Figure 14: Portail de prestations axé sur le portefeuille d'une autorité (A): le portail présente le portefeuille de prestations offertes par une autorité spécifique.

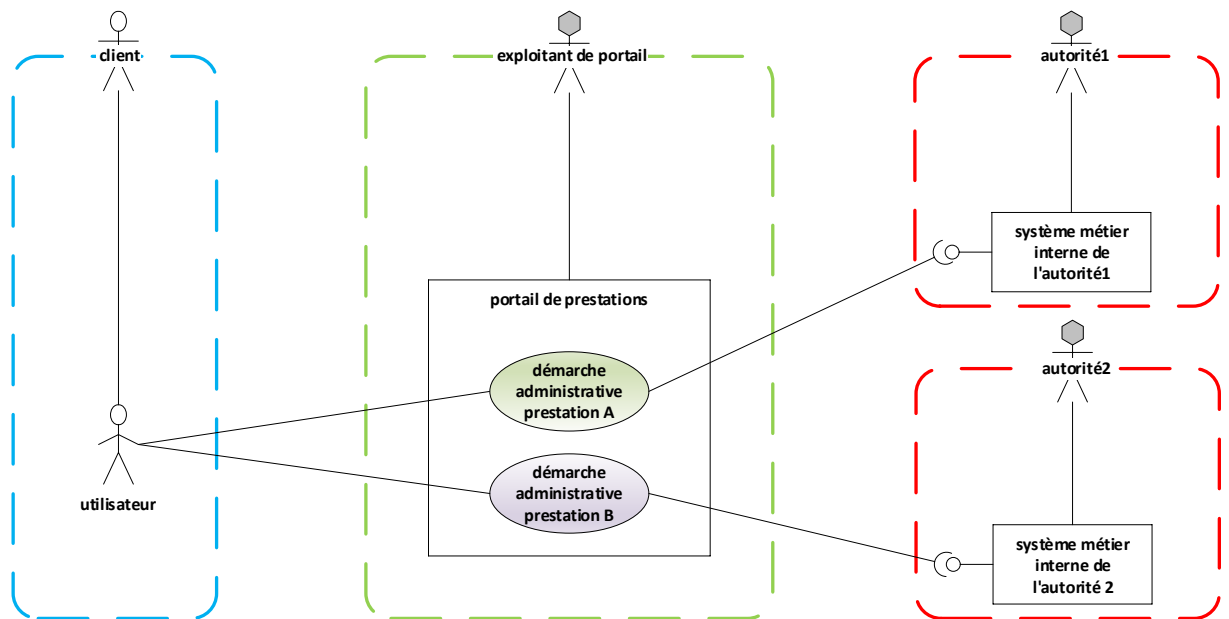


Figure 15: Portail de prestations (B) adapté aux besoins d'un groupe-cible de clients spécifique: le portail représente l'ensemble des prestations pertinentes pour le groupe-cible de clients. Ces prestations peuvent provenir de différentes autorités.

L'orientation en fonction des besoins des clients (B) peut également se manifester par le fait qu'une prestation administrative cantonale ou communale est offerte indépendamment de la compétence concrète (par exemple les inscriptions au registre du commerce pour les entreprises dans EasyGov), de sorte que du point de vue de l'utilisateur, la prestation apparaisse de la même façon, indépendamment de la compétence réelle (B'). Dans ce cas, la connaissance de

la responsabilité respective est implémentée dans le portail. Sur cette base, la communication est dirigée vers le système métier de l'autorité cantonale ou communale effectivement responsable.

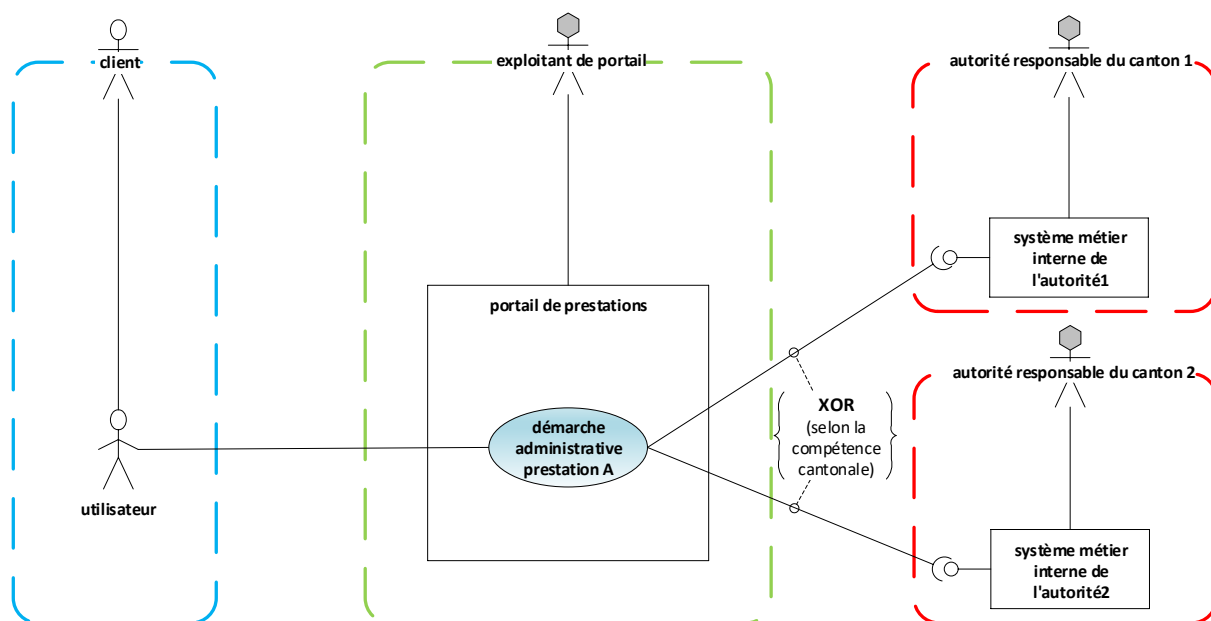


Figure 16: Encapsulation de la responsabilité spécifique d'une prestation administrative cantonale/communale par une offre globale (B')

Une variante de mise en œuvre de la forme mixte (C) est un portail qui est équipé de toutes les fonctionnalités de base nécessaires à un portail (couche d'information et fonctions transversales). Ces fonctionnalités de base peuvent être développées et exploitées par une seule organisation. Sur la base des fonctionnalités de base disponibles, les autorités intéressées peuvent ensuite développer leurs propres offres et les proposer sur le portail sans avoir à développer à nouveau les fonctionnalités de base à chaque fois. Cela crée un portail avec des offres de plusieurs autorités.

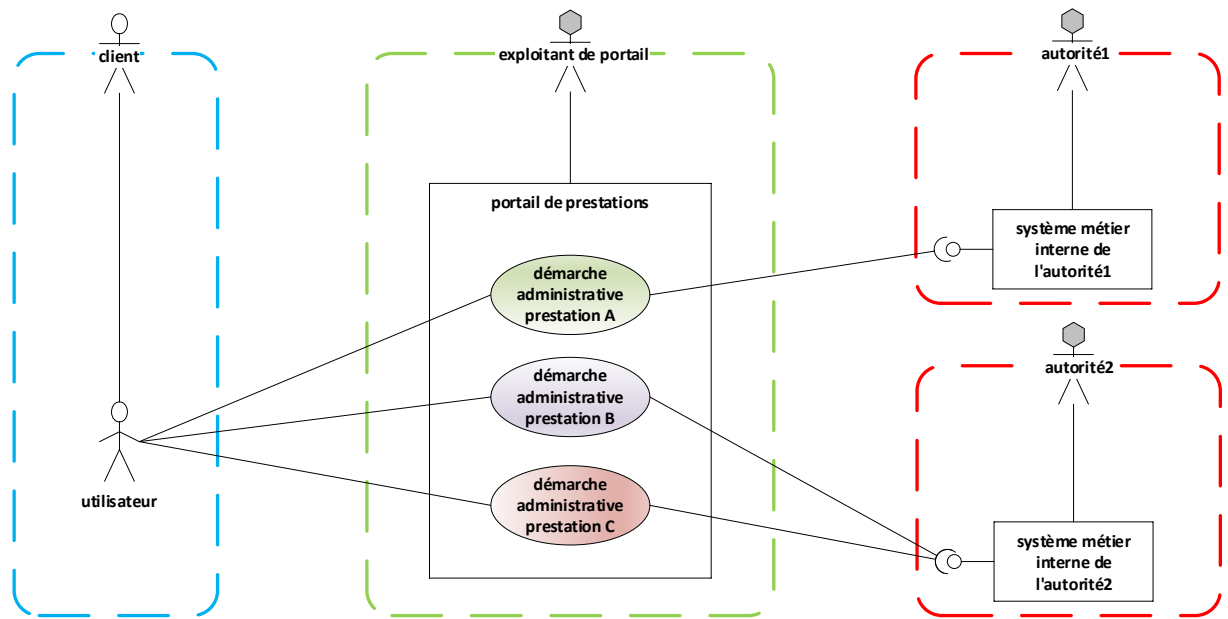


Figure 17: Forme mixte (C) de (A) et (B)

En raison des diverses orientations des portails de prestations - en particulier ceux qui sont orientés vers la demande (B) - les ensembles respectifs se chevauchent partiellement, c'est-à-dire que certaines prestations ne sont pas exclusivement représentées sur un portail, mais individuellement sur différents portails. Ce cas est illustré dans la Figure 18 suivante.

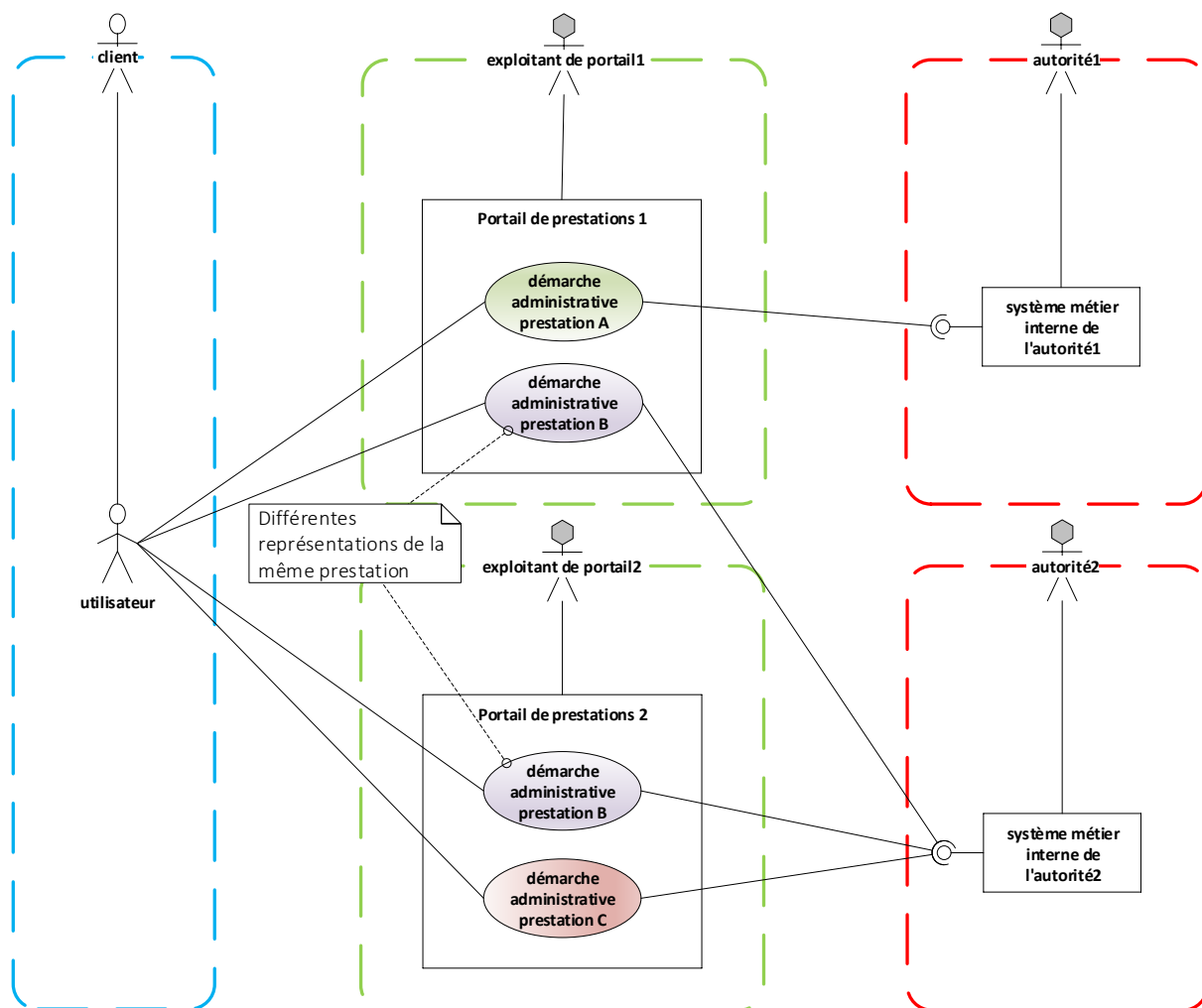


Figure 18: Représentation individuelle d'une prestation administrative sur différents portails

Le modèle des représentations individuelles d'une prestation sur différents portails, motivé par les besoins des clients, présente à la fois des avantages et des inconvénients.

Avantages:

- Un portail peut se concentrer exclusivement sur les besoins d'un groupe cible de clients - du point de vue du client, la variante préférée est (B).
- En permettant au groupe de clients visé par le portail d'obtenir toutes les prestations nécessaires des autorités en un seul endroit, les avantages suivants s'offrent à lui:
 - Support du principe «Once-Only» pour toutes les démarches administratives disponibles dans le portail.
 - Enregistrement sur un seul portail
 - Orchestration de prestations relatives à une situation de vie ou d'affaires
 - Le groupe de clients connaît le portail et ses caractéristiques d'application, et peut donc utiliser le portail plus facilement et plus rapidement.

- Le groupe de clients ne doit pas se rendre sur le portail approprié en fonction de ses besoins et de ses responsabilités, mais tous ses besoins sont couverts en un seul endroit et il n'a pas à se soucier des responsabilités.
- Pour les démarches administratives avec exécution cantonale, la question de la compétence cantonale peut déjà être clarifiée au sein du portail et le processus correct peut ensuite être proposé.

Inconvénients:

- Chaque implémentation de la démarche administrative doit être mise à jour séparément pour refléter toute modification des exigences de l'autorité compétente.
- L'expertise nécessaire pour représenter une démarche administrative est généralement vaste et n'est disponible qu'indirectement auprès de l'exploitant de portail. (Sauf si l'exploitant de portail fait partie de l'autorité, comme illustré dans la Figure 8).
- Les représentations individuelles et séparées de démarches administratives numériques existantes contredisent le principe économique de la réutilisation (sauf pour des démarches administratives cantonales existantes sans attribution de compétence ni transaction de bout en bout)

Afin de pouvoir utiliser les avantages tout en évitant les inconvénients, il est également possible pour les portails de réutiliser les démarches administratives qui ont déjà été mises en œuvre sur un autre portail. Cela signifie qu'un portail intègre une démarche administrative qui est mise en œuvre sur une couche transactionnelle qui existe ailleurs (voir la construction exemplaire illustrée à la Figure 19, où le portail de prestations A ne met pas en œuvre lui-même la démarche administrative "Prestation 3", mais l'intègre à partir du portail de prestations B). C'est ainsi, par exemple, que l'inscription de la TVA est mis en œuvre dans EasyGov: au lieu d'un développement propriétaire, l'implémentation existante de l'AFC a été intégrée.

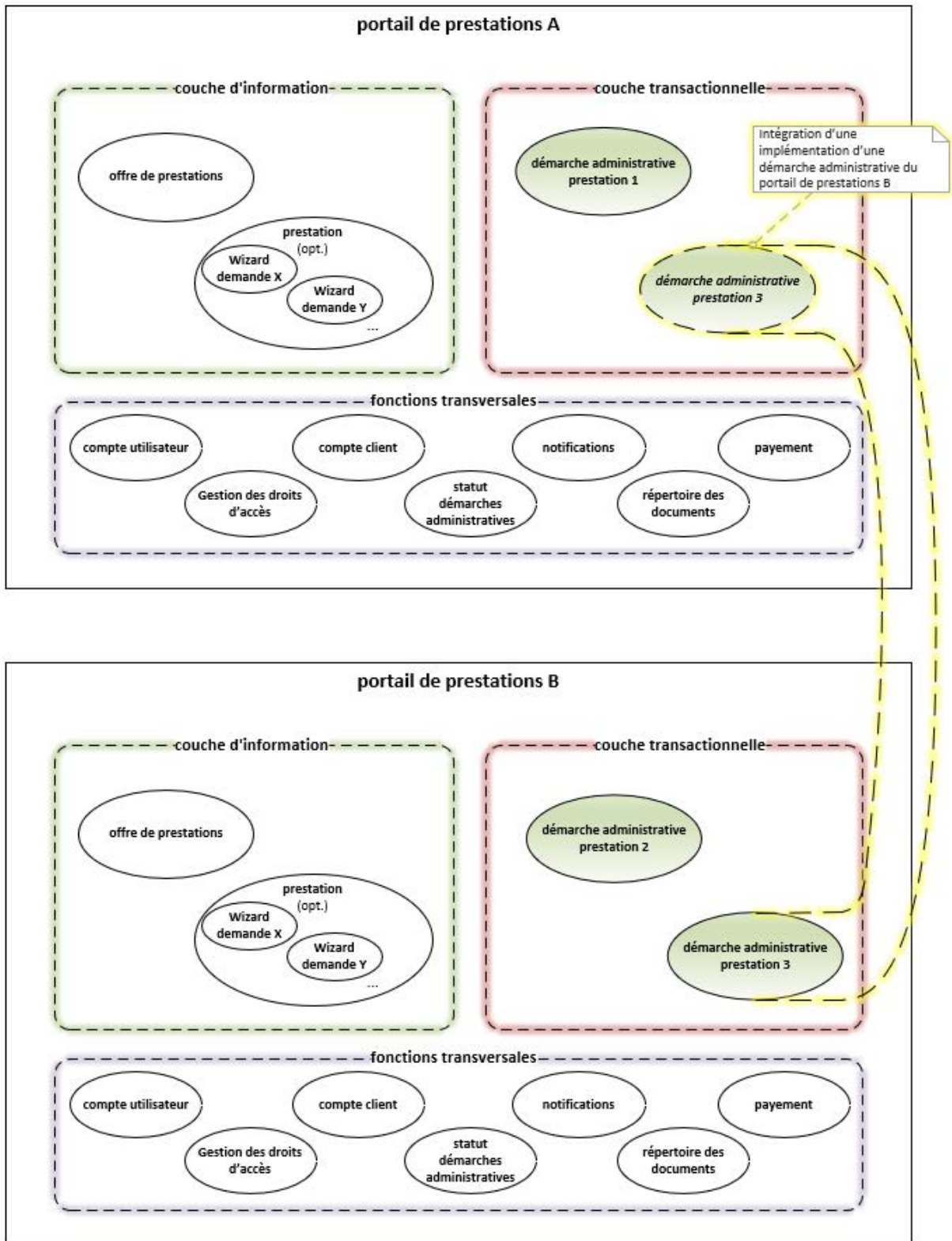


Figure 19: Intégration d'une implémentation existante d'une démarche administrative dans un autre portail

Les modèles d'intégration techniques possibles ne sont pas examinés ici pour le moment (cela sera fait au chapitre 2.1.6) ; il faut seulement noter que l'intégration se fait actuellement par le biais d'interfaces individuelles et qu'elle est donc complexe en conséquence. Cette situation est notamment compliquée par les différences conceptuelles entre les systèmes de portail. En définitive, cette circonstance est l'un des principaux moteurs de la présente étude. La grande complexité qui en résulte doit être maîtrisée et, si possible, réduite progressivement.

2.1.5 Modèle d'information des termes les plus importants

Les concepts élaborés dans les sections précédentes sont maintenant reliés dans un modèle d'information.

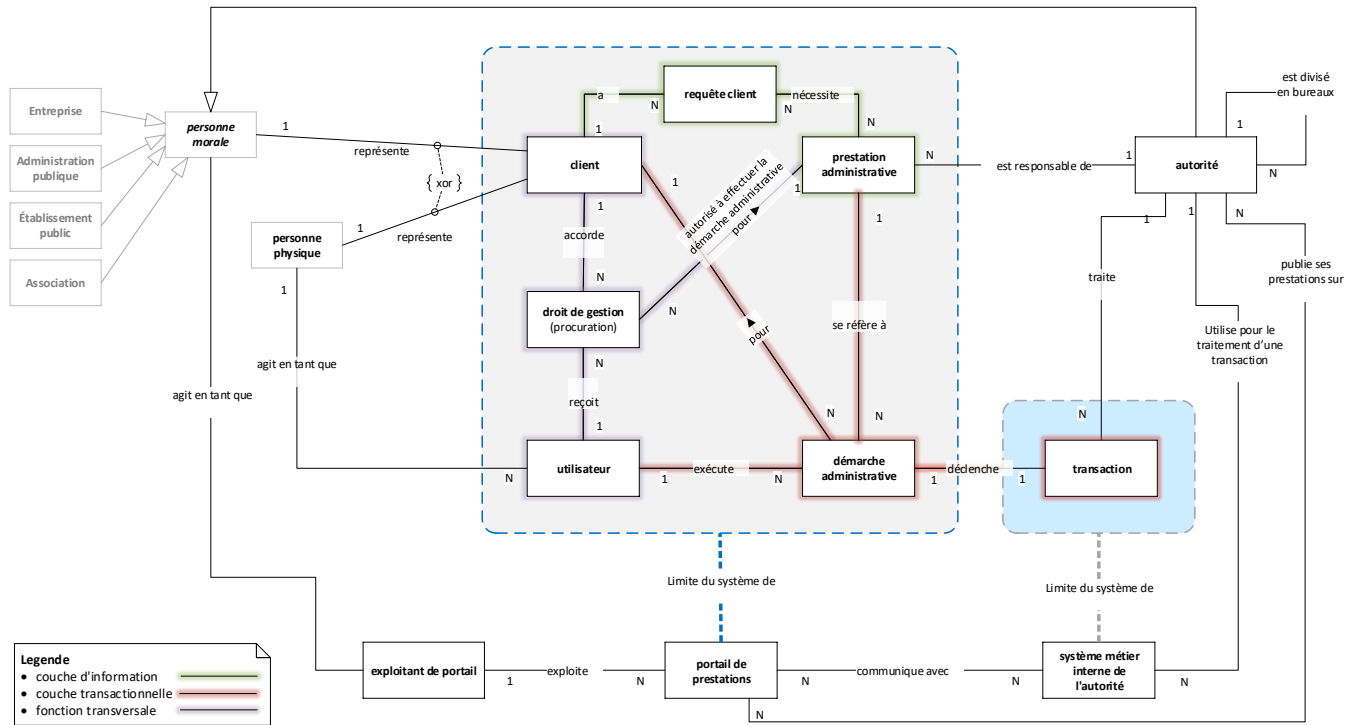


Figure 20: Modèle d'information pour les portails de prestations (diagramme de classe UML, pour une représentation agrandie, voir l'Annexe B)

Notes:

- Les deux zones colorées indiquent l'étendue du périmètre du portail de prestations et du système métier interne de l'autorité, respectivement.
- Les entités représentées en gris dans la figure le sont à titre d'illustration. Par exemple, il est montré que soit une personne morale (par exemple sous la forme d'une société), soit une personne physique apparaît en tant que client. Cette dernière peut également interagir avec le portail de prestations en tant qu'utilisateur. Les illustrations en gris ne sont pas expliquées plus loin.
- Le modèle d'information s'écarte en certains points du modèle formulé dans la norme eCH-0177 [16]. On sait que cette dernière présente des faiblesses, et la révision de la norme est prévue.

Tableau 1: Explication des entités représentées dans le modèle d'information

Entité ou terme	Description
Autorité	Une organisation de droit public qui exerce des fonctions d'État souveraines en Suisse. Les autorités peuvent exister au niveau communal, cantonal ou fédéral et appartenir aux pouvoirs législatif, exécutif ou judiciaire.

Entité ou terme	Description
	<p>Notes:</p> <ul style="list-style-type: none"> • Les tâches de l'État peuvent être confiées à un organisme public comme à une organisation privée. • La division hiérarchique en unités organisationnelles (également appelées bureaux) n'est pas davantage différenciée par le terme autorité. Le terme désigne une unité organisationnelle, quel que soit le niveau hiérarchique auquel elle se situe et quel que soit le nombre d'unités subordonnées ou supérieures qu'elle comporte.
Client	<p>Entité juridique pour laquelle une prestation administrative est utilisée. Il s'agit soit d'une personne morale, soit d'une personne physique (ou d'un groupe de personnes) qui a une obligation légale ou un droit à une prestation. Le client est représenté dans le portail par un compte client. Afin de simplifier les transactions A2B et A2C, des dispositions légales concernant les identifiants uniques des clients ont été établies en Suisse. Pour les personnes morales, il s'agit de l'IDE¹⁹, pour les personnes physiques, du numéro d'assuré (NAVS13)²⁰.</p> <p>Remarque: le terme partenaire commercial, qui provient de l'environnement SAP, est aussi couramment utilisé comme synonyme de client. Il convient également de mentionner le terme de données de base, qui est parfois utilisé comme synonyme de données clients. Ces synonymes et d'autres sont énumérés dans le glossaire (voir Annexe A).</p>
Couche d'information	<p>Domaine fonctionnel d'un portail de prestations qui donne à l'utilisateur une vue d'ensemble des prestations administratives disponibles (offre de prestations) et le conduit à la prestation requise. Comme l'illustre la Figure 11, une orchestration de prestations peut également être proposée, qui guide l'utilisateur à travers toutes les prestations obligatoires et facultatives pertinentes pour une requête spécifique du client au moyen d'un assistant (wizard). C'est le cas, par exemple, lors de la création d'une entreprise dans EasyGov, qui guide l'utilisateur pas à pas dans les formalités et enregistrements nécessaires (registre du commerce, AVS, TVA, etc.). La couche d'information peut également s'étendre au-delà du portail de prestations, jusqu'à la présence sur le web de l'autorité concernée.</p>
Couche transactionnelle	<p>Domaine fonctionnel permettant de traiter une prestation administrative. Cela comprend à la fois la démarche administrative du client dans le portail et le traitement des transactions dans le système métier interne de l'autorité (voir Figure 10).</p>

¹⁹ L'IDE est délivré aux entreprises par le registre IDE de l'OFS, le terme entreprise étant défini au sens large comme une entité active dans l'économie suisse. Voir <https://www.bfs.admin.ch/bfs/fr/home/registres/registre-entreprises/numero-identification-entreprises.html>

²⁰ Voir <https://www.bfs.admin.ch/bfs/fr/home/registres/service-national-adresses.html> et <https://www.egovernment.ch/fr/umsetzung/schwerpunktplan/aufbau-nationaler-adressdienste/>

Entité ou terme	Description
Démarche administrative	<p>Du point de vue du client, la démarche administrative est un processus qui comprend toutes les activités et étapes procédurales nécessaires pour obtenir une prestation administrative. Elle reflète le point de vue du bénéficiaire de la prestation sur la procédure administrative officielle. Les étapes du processus sont complémentaires à celles du traitement des transactions du côté de l'autorité.</p> <p>On peut distinguer les étapes suivantes du processus:</p> <ul style="list-style-type: none">• Initiation de la procédure par le client (par exemple, une demande)• Dans le cadre de la phase de traitement:<ul style="list-style-type: none">- Le client peut être contacté plusieurs fois par les autorités, par exemple pour fournir des informations ou des documents.- Réception de la prestation par le client dans le cadre de l'ouverture (remise) d'une décision officielle (par exemple, l'octroi d'un permis de construire).• Conclusion de la procédure. Lors de la remise de la prestation, soit la procédure est terminée pour le client, soit le client peut faire appel d'une décision impopulaire des autorités (une nouvelle procédure dès la phase "Initiation" est lancée lorsque l'appel est soumis).
Droit de gestion (procuration)	<p>Le droit de gestion représente une procuration qui, au sens juridique, autorise un représentant à agir au nom du sujet de droit - c'est-à-dire le client. Sur le portail de prestations cette procuration autorise un utilisateur à gérer le compte client concerné et à effectuer des démarches administratives pour une prestation administrative spécifique, l'autorisation pouvant être graduée (par exemple, consultation, modification, soumission, Superuser).</p> <p>L'octroi et l'administration des droits de gestion relèvent de la responsabilité du client ou du représentant autorisé par le client. En pratique, après un processus d'autorisation²¹ préalable, l'utilisateur initial d'un client se voit accorder un droit de gestion général de Superuser "pouvant tout faire" (quasi une autorisation collective). Ce droit lui donne accès à toutes les prestations ainsi qu'à la gestion des autorisations (voir besoin [B-10]).</p>
Exploitant de portail	<p>Entreprise ou organisation qui, en tant que prestataire de services, met un portail de prestations à la disposition de l'autorité en tant que bénéficiaire de services. Il peut également s'agir d'un bureau de l'autorité elle-même ou d'un prestataire privé.</p>

²¹ Dans le cadre de la procédure d'autorisation, le client confirme par écrit que l'utilisateur en question est autorisé à mener des activités officielles pour le compte du client.

Entité ou terme	Description
Fonction transversale	Terme collectif désignant les fonctions générales du portail qui sont utilisées à la fois dans les couches d'information et transactionnelle: par exemple, compte d'utilisateur, gestion des droits d'accès, compte client, statut des démarches administratives, notifications officielles, répertoire des documents, paiement, etc.
Portail de prestations administratives	<p>Application accessible au public (par exemple, application à page unique, application mobile, etc.) avec laquelle l'exploitant de portail offre au client un canal d'accès numérique à une ou plusieurs prestations administratives dans le cadre de la cyberadministration. Il s'agit de du front-end client pour des prestations administratives numériques. Le frontend est exploité par des utilisateurs dûment autorisés. Les fonctions d'un portail de prestations peuvent être divisées logiquement en couche d'information, fonctions transversales et couche transactionnelle. Dans la couche transactionnelle du portail, la démarche administrative côté client est mise en œuvre, mais aucun processus d'autorité interne (voir la Figure 10).</p> <p>Notes:</p> <ul style="list-style-type: none"> • Le terme "plateforme" est aussi couramment utilisé comme synonyme de portail de prestations. Toutefois, ce terme est également utilisé dans d'autres contextes (par exemple, système d'exploitation, Cloud, développement de logiciels, voir Wikipedia) et n'est donc pas utilisé plus avant dans le contexte de l'étude. • Pour certains portails (par exemple l'ePortal de la Confédération), la couche transactionnelle est mise en œuvre de manière modulaire dans des applications portail métier spécialisées (voir chapitre 2.1.6). • Le contenu de la couche d'information varie d'un portail à l'autre en fonction de son orientation. La gamme s'étend d'une simple liste des prestations offertes par les autorités jusqu'à de vastes orchestrations.
Prestation administrative	Prestation publique (activité A2A, A2B ou A2C) qu'une autorité offre au client (PP ou PM) dans le cadre de ses compétences, conformément au mandat de l'État. L'utilisation se fait par le biais d'une démarche administrative côté client, la mise à disposition de la prestation par le biais du traitement des transactions côté autorité.
Requête client	<p>Une requête client fait référence à la raison ou à l'élément déclencheur d'avoir recours à une prestation administrative. Dans le cas des clients PP, on parle également de "situation de vie", dans le cas des clients PM également de "situation commerciale" (voir eCH-0126 [14]et eCH-0138 [15])²².</p> <p>Exemple: un agriculteur veut employer temporairement une personne étrangère (par exemple de l'UE) comme ouvrier de récolte et se comporter en</p>

²² La définition suit la proposition d'Alexander Kämpfer (ChF).

Entité ou terme	Description
	<p>toute légalité. Par conséquent, cet agriculteur doit obtenir plusieurs prestations auprès des autorités (enregistrement de l'emploi en raison du quota de libre circulation, enregistrement de l'assurance sociale, enregistrement de l'assurance accident, enregistrement de l'impôt à la source, éventuellement d'autres).</p> <p>Une compilation systématique des requêtes client peut être trouvée pour PP dans [38] et pour PM dans [39].</p>
Système métier interne de l'autorité	<p>Une ou plusieurs applications métier qui prennent en charge le traitement des transactions d'une ou plusieurs prestations administratives. Les utilisateurs sont exclusivement des employés de l'autorité respective.</p> <p>Du point de vue d'un portail de prestations, le système métier interne de l'autorité peut être associé en tant que back-end.</p>
Transaction/ Traitement des transactions	<p>Processus qui est déclenché dans l'autorité compétente à la suite d'une démarche administrative (c'est-à-dire lorsque le client a recours à une prestation administrative). Le traitement des transactions comprend toutes les activités et les étapes de la procédure qui sont nécessaires, du point de vue de l'autorité, pour la fourniture d'une prestation. Il reflète le point de vue du prestataire sur la procédure administrative. Les étapes du processus sont complémentaires à celles de la démarche administrative du côté du client. Le traitement des transactions peut être assuré dans son ensemble par un ou plusieurs bureaux.</p> <p>En règle générale, un système métier interne de l'autorité prend en charge le traitement des transactions.</p>
Utilisateur	<p>Personne physique qui utilise activement le portail de prestations via une interface utilisateur (IU)^{23,24} et effectue ainsi des démarches administratives pour un client spécifique. L'utilisateur est représenté dans le portail par un compte utilisateur, qui est lié à des fonctions de sécurité pour l'authentification et l'autorisation. L'authentification fait référence à l'accès au système, l'autorisation aux droits de gestion spécifiques au client.</p>

Pour les autres termes utilisés dans cette étude, veuillez-vous référer au glossaire de l'Annexe A.

²³ Une personne physique peut avoir plusieurs utilisateurs ou comptes d'utilisateurs. À l'inverse, on suppose qu'il y a exactement une personne derrière un utilisateur, car la distribution d'informations d'identification n'est généralement pas légale.

²⁴ En principe, une machine peut également représenter un utilisateur. Toutefois, ce point est exclu ici car le contexte est délibérément limité à l'interface utilisateur, les portails de prestations étant construits pour des utilisateurs humains. Les interfaces machines sont traitées ailleurs, voir la Figure 29 et la Figure 30.

2.1.6 Modèles d'intégration pour la représentation des démarches administratives

Enfin, il convient de montrer quels modèles d'intégration peuvent être abstraits de la pratique pour la représentation des démarches administratives.

- Modèle d'intégration 1: **Implémentation** de la démarche administrative directement dans le portail²⁵
- Modèle d'intégration 2: **Intégration** d'une démarche administrative mise en œuvre en externe²⁶

Le premier modèle correspond à une mise en œuvre (généralement un développement individuel) de la démarche administrative directement dans le portail. Dans ce cas, la démarche administrative d'une prestation spécifique est entièrement représentée dans le portail, et la mise en œuvre est donc la responsabilité de l'exploitant du portail²⁷. La communication requise entre la démarche administrative et le traitement des transactions selon la Figure 9 (chapitre 2.1.2) est gérée via une interface depuis le portail vers le système métier interne de l'autorité, qui est appelée interface "démarche administrative ↔ traitement des transactions". Comme l'illustre la Figure 21 ci-dessous, le système métier interne de l'autorité fonctionne comme le fournisseur (du service «traitement des transactions»), tandis que le portail fonctionne comme le consommateur, puisque la mise en œuvre de la démarche administrative utilise le service de traitement des transactions.

Le rôle de fournisseur du traitement des transactions ne doit pas être compris comme servant un seul portail consommateur. Il est plutôt possible de servir plusieurs portails consommateur, qui mettent en œuvre la démarche administrative pour la prestation en question. La Figure 22 suivante illustre ce cas: l'utilisateur peut effectuer la démarche administrative pour la prestation X sur le portail 1 ainsi que sur le portail 2. Le portail 1 pourrait, par exemple, être le guichet en ligne de l'autorité en question et le portail 2 un portail spécifique au client, tel que EasyGov.

²⁵ Dans l'environnement EasyGov, le terme "intégration complète" est aussi couramment utilisé à cette fin.

²⁶ Dans l'environnement EasyGov, le terme "intégration partielle" est aussi couramment utilisé à cette fin.

²⁷ Il peut également s'agir de l'autorité elle-même, voir la Figure 8.

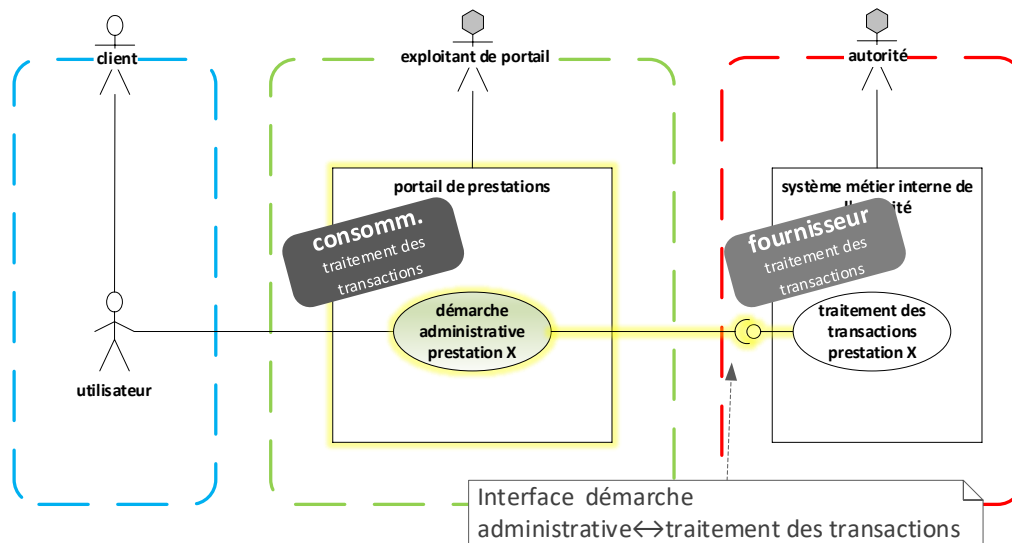


Figure 21: Modèle d'intégration 1 - Implémentation de la démarche administrative directement dans le portail

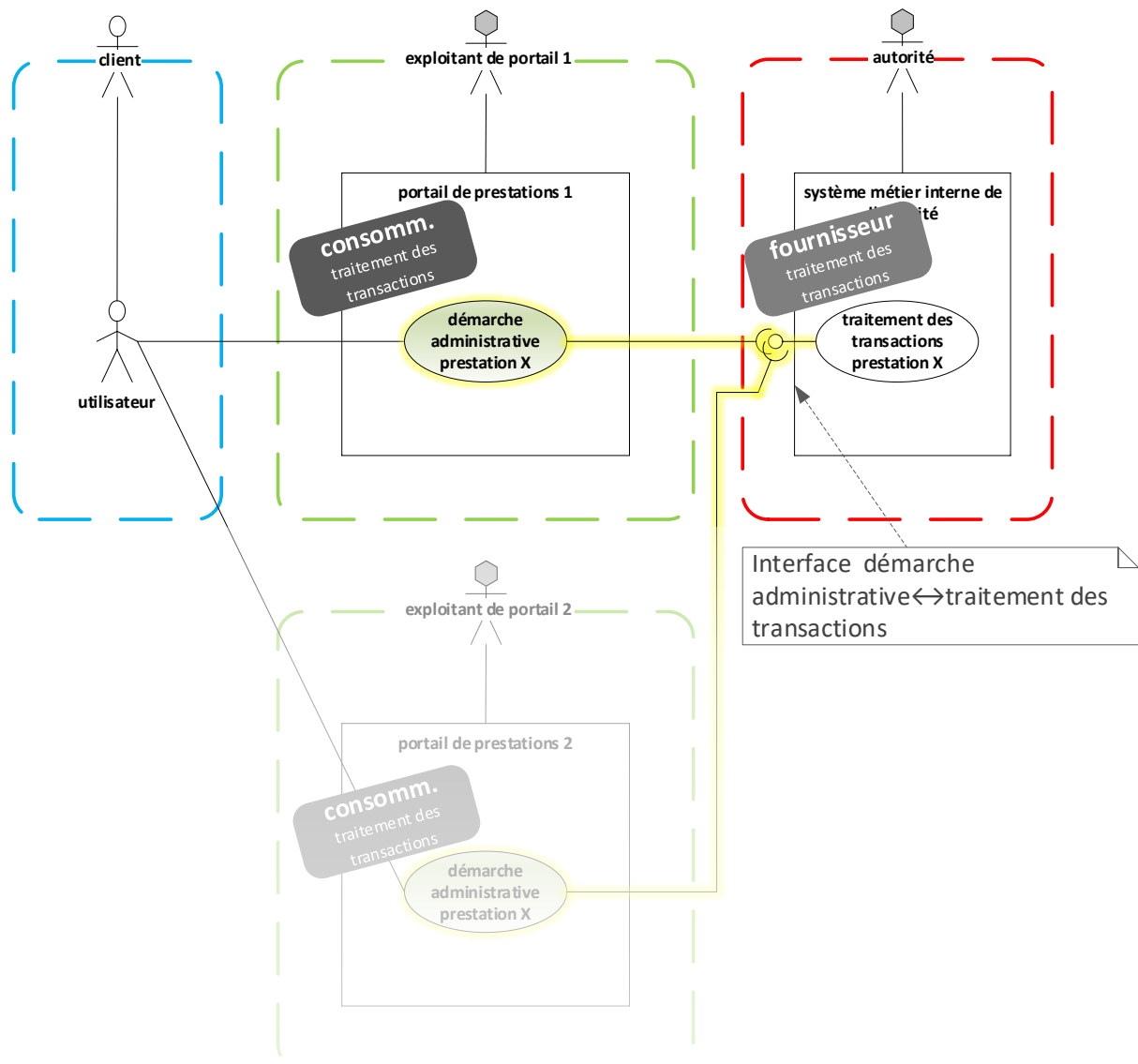


Figure 22: Le modèle d'intégration 2 permet également l'utilisation de plusieurs portails consommateur.

Un cas particulier du modèle d'intégration 1 est celui où un portail de prestations sert d'environnement d'exécution ou de cadre/plateforme réutilisable (par exemple, iGovPortal, ePortal de la Confédération²⁸) pour les prestations administratives. Cela signifie qu'il offre la fonctionnalité transversale nécessaire, sur la base de laquelle des démarches administratives concrètes peuvent être mis en œuvre en tant qu'application portail métier (quasi comme un add-in) ou configurées en composants préfabriqués. Cette approche permet à une autorité d'offrir ses prestations sous sa propre responsabilité, sans avoir à exploiter ou à développer son propre portail. En fin de compte, cependant, le principe du modèle d'intégration 1 demeure, c'est pourquoi les cas particuliers ne nécessitent pas de considération différenciée du point de vue de l'architecture cible d'intégration.

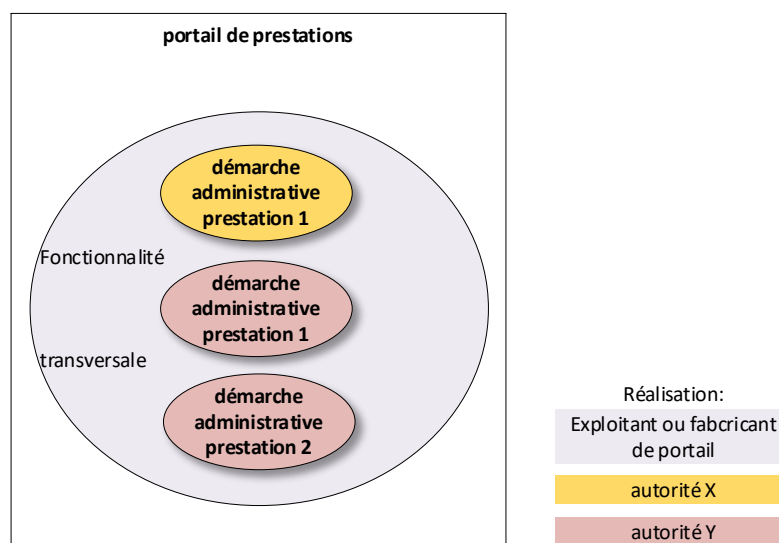


Figure 23: Cas particulier du modèle d'intégration 1: un portail de prestations fournit un environnement/cadre d'exécution pour des prestations l'autorité sur lequel les autorités mettent en œuvre leurs prestations en tant qu'application portail métier ou les configurent en composants préfabriqués.

Contrairement à l'implémentation directe dans le portail, il est également possible d'intégrer une implémentation existante d'un système externe. Cette constellation est soutenue par le deuxième modèle d'intégration. Il permet la réutilisation d'une démarche administrative implémenté dans un autre portail, comme le montre le chapitre 2.1.4/Figure 19. Cette approche qui est particulièrement utile pour la mise en œuvre d'une offre de prestations orchestrée. Comme l'illustre la Figure 24 suivante, cet autre portail (à droite) fonctionne comme un fournisseur, car il fournit au sens d'un service la démarche administrative complète, y compris l'interface utilisateur, la logique commerciale et le stockage des données. Le portail intégrant

²⁸ D'un point de vue externe, le l'ePortal et les applications portail métier qu'il contient constituent un système de portail au sens de la Figure 23. En interne, il existe un écosystème de composants centraux (par exemple, PAMS, service de notification, etc. ainsi que l'ePortal lui-même) et d'applications portail métier qui interagissent dans une architecture de microservices.

la prestation (à gauche) est le consommateur de l'implémentation de la démarche administrative en s'"accrochant"²⁹ en un endroit approprié. L'utilisateur "saute" du portail du consommateur à celui du fournisseur, le contexte de la session étant également transféré en arrière-plan afin que l'utilisateur puisse continuer à travailler de manière transparente sur le portail du fournisseur (comme illustré à la Figure 34 ci-dessous). Cela signifie notamment que la transition s'accompagne d'une authentification unique (SSO) et d'une synchronisation du contexte (sélection de la prestation et du client, droits de gestion). Pour le portail consommateur, l'interface "démarche administrative ↔ traitement des transactions" (voir le modèle d'intégration 1 ci-dessus) reste cachée ; elle ne joue aucun rôle dans le modèle d'intégration 2.

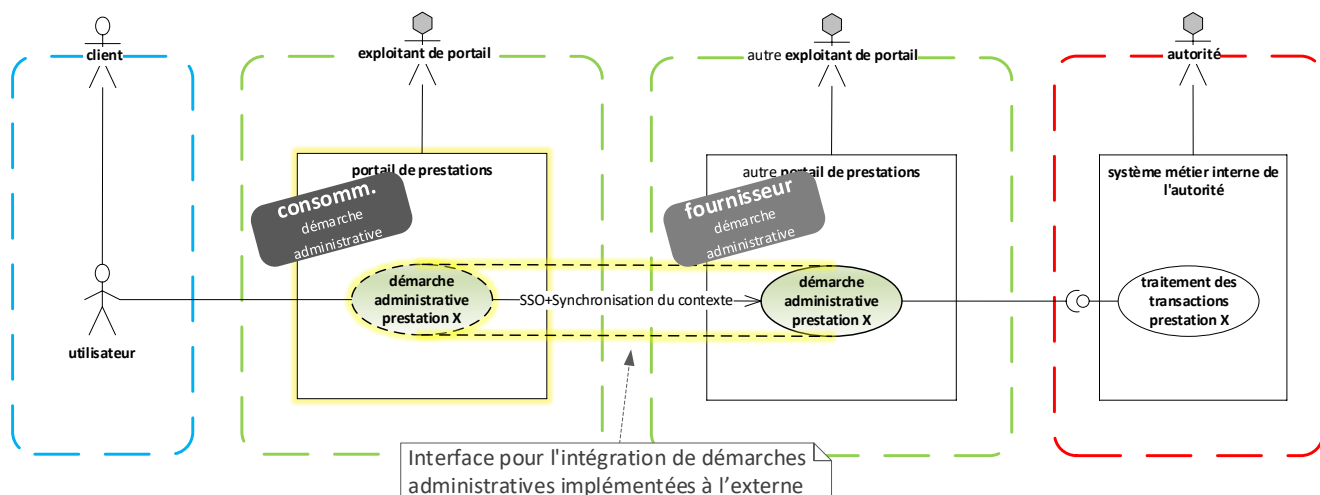


Figure 24: Modèle d'intégration 2 - Intégration d'une démarche administrative implémentée en externe

Dans la pratique, les modèles d'intégration mentionnés sont souvent combinés. Un portail peut implémenter directement une démarche administrative (selon le modèle d'intégration 1) et en intégrer un autre en externe (modèle d'intégration 2). Un exemple d'une telle forme mixte est EasyGov, qui, à l'origine, ne contenait que des démarches administratives directement implémentées, mais qui utilise de plus en plus la possibilité d'intégration dans une extension ultérieure.

La Figure 25 suivante illustre la forme mixte à l'aide de l'exemple d'un portail de prestations fictif 1, que

- la démarche administrative « prestation X » directement implémentée utilise l'interface "démarche administrative ↔ traitement des transactions" du système métier interne 2 de l'autorité responsable de la prestation,
- il intègre la prestation Y de l'autre portail 3,

²⁹ Cette déclaration doit être comprise indépendamment de la technologie. Le fait que l'intégration technique se fasse par le biais d'une redirection, de composants web, d'iFrame ou d'autres moyens similaires n'a aucune incidence sur le principe.

- l'utilisateur peut exécuter la démarche administrative "prestation Y" sur le portail 1 ainsi que sur l'autre portail 3, qui implémente la démarche administrative derrière l'intégration.

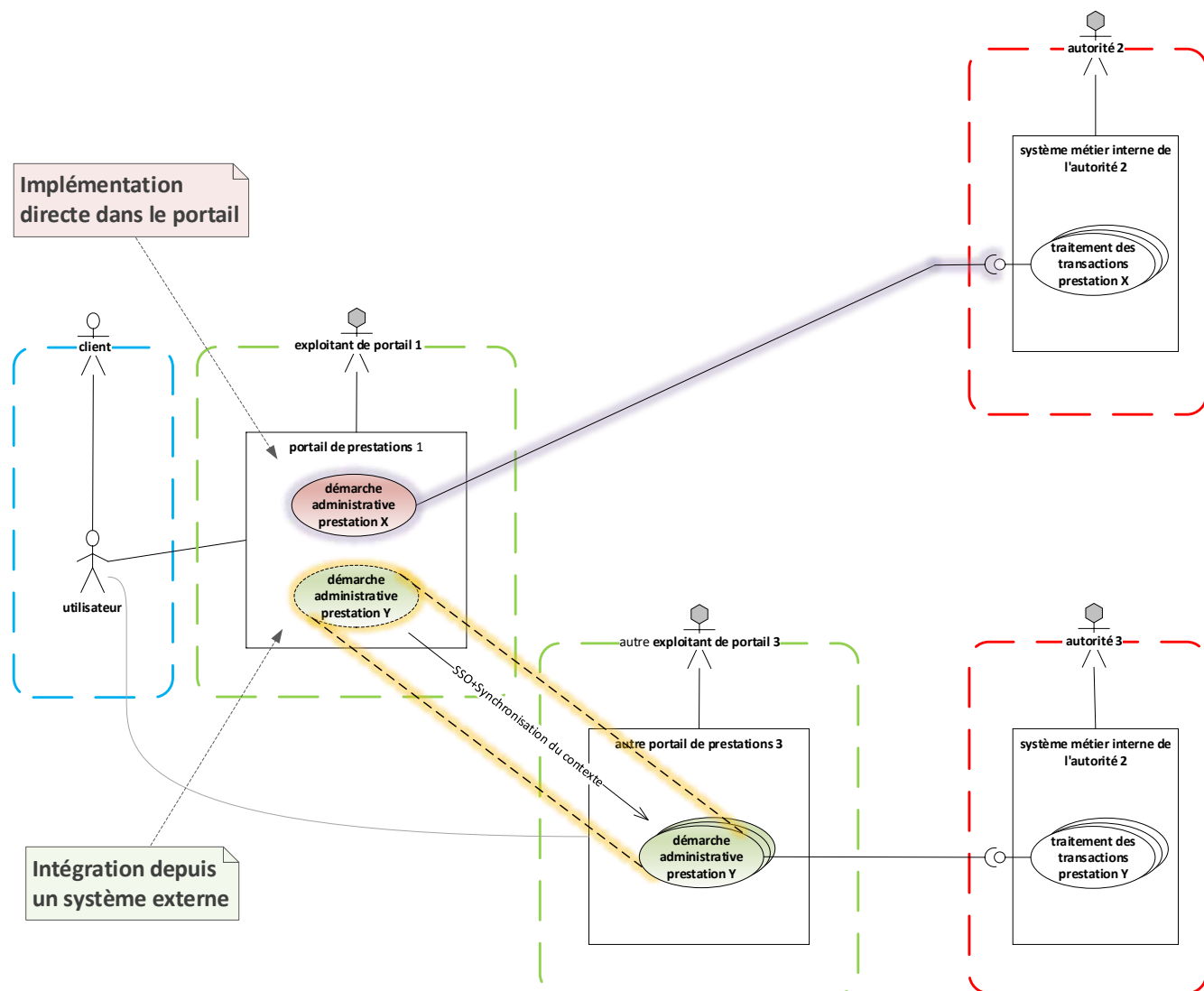


Figure 25: Forme mixte - le portail représente les démarches administratives selon les deux modèles d'intégration 1 et 2

Note: Dans cette version française de l'étude, nous utilisons le terme "intégration" pour désigner le modèle d'intégration 2. Cela peut prêter à confusion. Les auteurs considèrent toutefois que cette traduction est la plus appropriée pour le terme allemand "Einbindung".

2.2 Exigences pour le domaine des portails de prestations du point de vue commercial

2.2.1 Conditions cadres

Les conditions cadres suivantes pour le développement de l'architecture cible peuvent être déduites à la fois du mandat d'initialisation du projet et de l'évaluation des besoins (voir 2.2.2

Tableau 2: Conditions cadres pour le développement de l'architecture cible

Non.	Titre	Cadre de travail
[F-1]	Normes eCH	<p>L'architecture cible est développée en tenant compte de eCH-0123 [12], eCH-0124 [13] et eCH-0177 [16]. En cas de divergences, des RFC (Request for Changes) sont rédigés à l'attention d'eCH.</p> <p>La modélisation des processus et des règles d'affaires doit être conforme à ces normes:</p> <ul style="list-style-type: none">• eCH-0074 Principes de modélisation graphique des processus d'affaires, version 2.2 (2020) [24]• eCH-0158 Conventions de modélisation BPMN pour l'administration publique, version 1.2 (2020) [11]• eCH-0242 Modélisation des règles d'affaires, version 1.0 (2020) [25]
[F-2]	Solutions ISA ²	Les solutions ISA ² ³⁰ suivantes sont envisagées: Core Public Service Vocabulary Application Profile ³¹ (CPSV-AP) et The New European Interoperability Framework (EIF) [17].
[F-3]	Personnes physiques et morales	La proposition architecturale est valable pour les prestations destinées aux personnes morales et aux personnes physiques.
[F-4]	Focalisation A2C	L'accent est mis sur l'interface client-autorité (A2B, A2C). Les systèmes métier respectifs sont responsables des processus d'autorité internes.
[F-5]	Exigences en matière d'architecture UX	Les exigences architecturales résultant des besoins liés à l'UX (expérience utilisateur) doivent être prises en compte, mais les besoins de l'UX eux-mêmes ne sont pas pertinents.
[F-6]	Accessibilité	Selon les exigences légales, l'accessibilité doit être garantie.

2.2.2 Besoins

Les sections suivantes 2.2.2.3 à 2.2.2.9 résument les besoins qui ont été identifiés pour le domaine des portails de prestations. Ceux-ci se réfèrent à la numérisation des prestations administratives et ont été élaborés dans un premier temps au moyen d'une enquête auprès des membres du comité de pilotage. Ils ont ensuite été complétés par les souhaits d'autres acteurs du Conseil d'architecture de la cyberadministration suisse (mentionnés lors de la réunion du 11

³⁰ Interoperability solutions for public administrations, businesses and citizens: https://ec.europa.eu/isa2/solutions_en

³¹ https://ec.europa.eu/isa2/solutions/core-public-service-vocabulary-application-profile-cpsv-ap_en

août 2020). Enfin, les besoins ont été vérifiés et finalisés en plusieurs itérations avec le comité de pilotage et le groupe technique.

Afin d'obtenir une meilleure vue d'ensemble des besoins, ceux-ci ont été classés selon la déclaration de Tallinn sur la cyberadministration et affectés à différents thèmes. En outre, pour chaque besoin, il est indiqué pour quels acteurs il est pertinent. Cette catégorisation se trouve à la fin de ce chapitre (chapitre 2.2.2.10).

Note: Nous parlons délibérément de besoins et non d'exigences, car leurs formulations orientées vers les parties prenantes ne correspondent pas à l'attente de qualité des exigences détaillées (à partir desquelles des cas de test peuvent être dérivés, par exemple). Le catalogue des besoins sert plutôt de base et d'inspiration pour la formulation de l'image cible. En ce sens, le chapitre 2.6 évaluera finalement dans quelle mesure les besoins des parties prenantes sont couverts par l'image cible.

2.2.2.1 Catégorisation selon la déclaration de Tallinn sur la cyberadministration

Le conseiller fédéral Ueli Maurer a signé la déclaration de Tallinn sur la cyberadministration³² avec les gouvernements de l'UE et de l'AELE en 2017. Les objectifs de la déclaration sont conformes à la stratégie suisse de cyberadministration adoptée par la Confédération, les cantons et les communes. Les principes de Tallinn sont énumérés ci-dessous. La mise en œuvre cohérente de ces principes offre à la population et à l'économie une infrastructure publique numérique à l'épreuve du temps.³³

Tableau 3: Principes de la déclaration de Tallinn sur la cyberadministration

T1	Digital by default, inclusiveness and accessibility	Numérique par défaut, inclusif et accessible
T2	Once-only	Saisie unique des données par l'utilisateur (et non récurrente à chaque démarche administrative)
T3	Trustworthiness and security	Fiabilité et sécurité
T4	Openness and transparency	Ouverture et transparence
T5	Interoperability by default	Interopérabilité par défaut

2.2.2.2 Structuration de la détermination des besoins

Dans l'enquête mentionnée au chapitre 2.2.2, les parties prenantes ont été invitées à identifier les besoins sous différents angles.

Les perspectives ont été dérivées des acteurs identifiés dans les considérations précédentes - en particulier les chapitres 2.1.4 et 2.1.5:

- Utilisateur

³² Voir https://ec.europa.eu/newsroom/document.cfm?doc_id=47559

³³ De <https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaefte?AffairId=20193686>

- Client (personnes physiques et morales)
- Autorité
- Exploitant de portail

Une fois la détermination des besoins terminée, les nombreuses contributions ont été condensées et classées par catégories. Le résultat est documenté dans les chapitres suivants 2.2.2.3 à 2.2.2.9. Pour chaque besoin, il est indiqué pour quel acteur il est pertinent ou de quel acteur il émane. Les commentaires originaux se trouvent à l'Annexe G.F.

2.2.2.3 Besoins concernant l'intégration des prestations administratives

Tableau 4: Besoins concernant l'intégration des prestations administratives

No	Titre	Besoin	Tallinn	Besoin de...
[B-1]	Interopérabilité des systèmes	Les prestations administratives peuvent être intégrées dans différents portails (portail global, municipalité, canton, Confédération) / soutien de différents modèles d'intégration (eCH). En d'autres termes, selon [EIF-6], les prestations administratives doivent être accessibles via différents canaux ou portails afin que l'utilisateur puisse choisir le canal qui répond le mieux à ses besoins.	T2, T5	Tous
[B-2]	Interopérabilité des données	Les différents portails de prestations et les systèmes sources pertinents doivent pouvoir échanger des données par voie électronique. L'échange de données doit donc être standardisé (norme eCH) et compréhensible - à la fois A2C et A2B.	T5	Autorité, exploitant de portail
[B-3]	Offrir des services de base	Les services de base et les infrastructures de portail existants peuvent être utilisés pour faciliter la mise en place par les pouvoirs publics de nouvelles offres d'administration en ligne.	T2	Autorité, exploitant de portail
[B-4]	Répertoire de métadonnées	Un répertoire central de toutes les prestations administratives, y compris les spécifications nécessaires à l'intégration, doit être disponible.	T4, T5	Autorité, exploitant de portail
[B-5]	Intégration des systèmes existants sans impact sur d'autres systèmes	Il doit être possible d'intégrer les solutions existantes des différents niveaux administratifs de la Confédération, des cantons et des communes, ainsi que des différents fabricants de ces solutions, en mode "runtime", c'est-à-dire sans arrêter et démarrer l'ensemble du système, pour autant que ces solutions tiennent compte des normes d'interface convenues.	T5	Autorité, exploitant de portail

2.2.2.4 Besoins en matière d'authentification et d'autorisation

Tableau 5: Besoins en matière d'authentification et d'autorisation

No	Titre	Besoin	Tallinn	Besoin de...
[B-6]	Authentification unique (SSO)	L'utilisateur ne doit se connecter qu'une seule fois pour utiliser les prestations administratives (même pour plusieurs clients). S'il possède plusieurs noms d'utilisateur (identités logiques, par exemple un pour ses démarches administratives en tant que personne physique et un pour les démarches qu'il effectue en tant que personne physique agissant pour une personne morale), ceux-ci peuvent être fusionnés et liés dans l'authentification unique. Le niveau de confiance (LoA, par exemple 2FA) ou les contrôles de sécurité initiaux (par exemple la vérification par courrier électronique) utilisés dans le processus doivent être acceptés par toutes les prestations administratives, quel que soit le système sur lequel elles sont effectuées.	T2	Utilisateur
[B-7]	Identités multiples utilisables	Il doit être possible d'utiliser diverses identités électroniques existantes pour le login (par exemple eID, SwissID, TrustID ou d'autres identités telles que Facebook, Google avec une portée réduite des services).	T3	Utilisateur
[B-8]	LoA différencié	Une prestation administrative ne doit pas exiger de l'utilisateur un niveau de connaissance plus élevé que nécessaire (par exemple, l'offre d'information peut être consultée sans authentification).	T3	Utilisateur, Autorité
[B-9]	Signature électronique	Les signatures nécessaires doivent être couvertes autant que possible par le niveau de confiance (LoA) et peuvent donc être omises. Ceci est soumis à la vérification prouvable de l'identité authentifiée que l'utilisateur est réellement qu'il prétend être. Pour cela, les fondements non seulement techniques mais aussi juridiques sont déterminants. Dans les cas où cela n'est pas possible, il doit être possible d'utiliser une signature électronique.	T3	Utilisateur, Autorité

[B-10]	Gérer soi-même les droits de gestion	Le client (ou l'utilisateur qui le représente) doit pouvoir gérer les droits de gestion des employés de l'entreprise et des personnes physiques en mode self-service. À cette fin, il convient de fournir un aperçu des droits accordés.	T3	Client
[B-11]	Procuration standardisée	Dans le cadre de l'interopérabilité des portails de prestations, l'objectif doit être de développer et de proposer une procuration légale standardisée, qui ne doit être établie qu'une seule fois par le client pour un utilisateur spécifique. L'utilisateur doit alors être en mesure d'effectuer toutes les démarches administratives interopérables à tous les niveaux fédéraux pour le client.	T2, T5	Utilisateur, Client

2.2.2.5 Besoins en matière de communication client - autorité

Tableau 6: Besoins en matière de communication client - autorité

No	Titre	Besoin	Tallinn	Besoin de...
[B-12]	Contact facile avec l'autorité	En cas de questions du point de vue du client, ce dernier (ou l'utilisateur qui le représente) peut facilement et spontanément, par voie numérique ou analogique, contacter l'autorité compétente et lui faire part de ses retours. Il existe un processus de support clairement défini.	T4	Tous
[B-13]	Communication sécurisée et juridiquement contraignante entre l'autorité et le client	L'autorité doit pouvoir communiquer avec des clients individuels (par exemple, demander des documents, poser des questions) et avec des groupes entiers de clients (par exemple, pour communiquer des informations générales) d'une manière juridiquement contraignante et sûre. ³⁴	T3	Autorité

³⁴ Sûre signifie ici: Appropriée au cas d'utilisation et conforme à la norme actuelle d'utilisation du papier par la poste.

2.2.2.6 Besoins en matière d'interface utilisateur (UI)

Tableau 7: Besoins d'interface utilisateur (UI)

No	Titre	Besoin	Tallinn	Besoin de...
[B-14]	Personnaliser la vue sur les prestations de l'autorité	L'utilisateur doit pouvoir personnaliser sa vue des prestations administratives disponibles (par exemple: langue, signets/raccourcis pour les prestations fréquemment utilisées).	T1	Utilisateur
[B-15]	Aide dans la variété des prestations administratives	L'utilisateur doit se voir proposer une vue thématique inter-autorités afin de trouver facilement les prestations administratives. Un vocabulaire uniforme doit être disponible pour toutes les prestations, par exemple pour la description des prestations. Si nécessaire, une norme du point de vue de l'utilisateur peut être appliquée pour le classement des sujets resp. des transactions.	T4	Utilisateur
[B-16]	Prestations administratives accessibles à partir d'un seul point d'entrée	Si possible, le client peut bénéficier des prestations administratives qui le concernent à partir d'un seul point d'entrée (portail). (Remarque: cela ne signifie pas qu'il ne peut y avoir qu'un seul portail de prestations).	T1	Utilisateur

2.2.2.7 Besoins en matière de marche des affaires des prestations administratives

Tableau 8: Besoins en matière de traitement des affaires

No	Titre	Besoin	Tallinn	Besoin de...
[B-17]	Once-only	Le client (ou l'utilisateur qui le représente) souhaite ne devoir saisir les données qu'une seule fois pour toutes les autorités (principe once-only inter-autorités) ³⁵ . Lorsqu'elles sont disponibles, les données sont obtenues à partir d'un registre ou d'un service de base. Si des données spécifiques ne sont pas encore disponibles pour toutes les autorités, elles doivent être saisies une fois.	T2, T5	Utilisateur, client
[B-18]	Transparence du traitement des transactions	Le client (ou l'utilisateur qui le représente) doit pouvoir s'informer de l'état d'avancement du traitement des transactions de ses démarches administratives en cours et achevées: État d'avancement du traitement, responsabilité, notifications/questions éventuelles, résultat. Il s'ensuit que le traitement des transactions par les autorités doit être traçable et transparent.	T1, T3, T4	Utilisateur, client
[B-19]	Les transactions classiques peuvent également être suivies	[B-18] s'applique indépendamment du fait que la transaction respective ait été initiée numériquement ou via un processus officiel analogique classique. (C'est-à-dire que dans ce dernier cas, l'autorité devrait en plus mettre en place la démarche administrative au niveau numérique).	T1	Client, Autorité
[B-20]	Traitement des transactions sans rupture de médias	Le client peut effectuer ses démarches administratives auprès des autorités de manière entièrement électronique (sans rupture de médias). Cela s'applique en particulier à l'interface avec le traitement des transactions de l'autorité concernée.	T1	Tous

³⁵ De même, les autorités ont également le besoin pour "Once-Only" dans le traitement des transactions. Ce besoin est déjà abordé par le projet OMO9 de la cyberadministration suisse "Mettre en place une gestion transversale des données de base des autorités " et n'est pas traité plus avant dans cette étude.

[B-21]	Processus guidé	Dans la mesure du possible, les démarches administratives doivent être uniformes dans toute la Suisse, avec le moins d'interactions possible, et doivent être auto-expliquatives (processus guidé).	T1	Utilisateur, client
[B-22]	Offre pour les entreprises sans IDE	Les démarches administratives doivent également être proposées aux entreprises sans IDE (c'est-à-dire aux entreprises en phase de démarrage ou étrangères) - dans la mesure du raisonnable.	T1	Client, Autorité
[B-23]	L'autorité conserve le contrôle de ses prestations	L'autorité doit conserver le contrôle de ses prestations (contenu, processus et présentation).	T1	Autorité
[B-24]	Identification proactive des besoins des clients par le biais du portail de prestations	L'identification proactive des besoins des clients par le biais du portail de prestations doit faire partie intégrante des portails de prestations. Le client doit être pris en charge où et quand il a besoin d'une prestation. Par exemple, des prestations telles que le renouvellement d'un abonnement ou d'un passeport doivent être automatiquement déclenchées par les autorités à l'expiration de la validité, mais il peut aussi s'agir d'une reconnaissance des besoins plus complexe. En outre, le client doit être informé des autres fonctions des autorités qui le concernent.	T1	Client, Autorité

2.2.2.8 Besoins en matière de SIPD

Tableau 9: Besoins concernant l'ISDS

No	Titre	Besoin	Tallinn	Besoin de...
[B-25]	Garantie SIPD	La sûreté de l'information et la protection des données doivent être garanties.	T3	Tous
[B-26]	Transparence concernant l'utilisation des données	Le client doit pouvoir savoir où se trouvent ses données, quelles autorités y ont accès et dans quel but.	T3	Utilisateur, client
[B-27]	Disponibilité de l'ensemble du système	La disponibilité de l'ensemble des systèmes concernés est déterminée et garantie par l'autorité, en tenant compte de la demande du client. Le client doit pouvoir s'informer sur les pannes en cours ainsi que sur les travaux de maintenance prévus.	T1	Tous

2.2.2.9 Besoins en matière de mise en œuvre et d'exploitation

Tableau 10: Besoins concernant les conditions cadres de mise en œuvre

No	Titre	Besoin	Tallinn	Besoin de...
[B-28]	Efficacité économique	L'architecture cible doit tenir compte des aspects économiques de tous les partenaires impliqués.	T5	Client, autorité, exploitant de portail
[B-29]	Qualité du développement futur	... tels que la fiabilité, la maintenabilité et la portabilité	-	Exploitant de portail

2.2.2.10 Répartition des besoins par catégories

La Figure 26 ci-dessous visualise les contributions originales non condensées de l'enquête sur les besoins (voir Annexe G.F) selon la structuration décrite au chapitre 2.2.2.2. On peut constater ce qui suit:

- Tous les principes de la déclaration de Tallinn sur la cyberadministration semblent être suffisamment couverts par les besoins.
- L'accent est mis sur les catégories de l'intégration des prestations administratives, du traitement des transactions et de la SIPD.
- La catégorie de la présentation (UI) n'est couverte que par trois besoins. Cependant, cela est considéré comme suffisant pour l'objectif architectural de l'étude.
- Les perspectives des acteurs sont réparties de manière assez équilibrée.

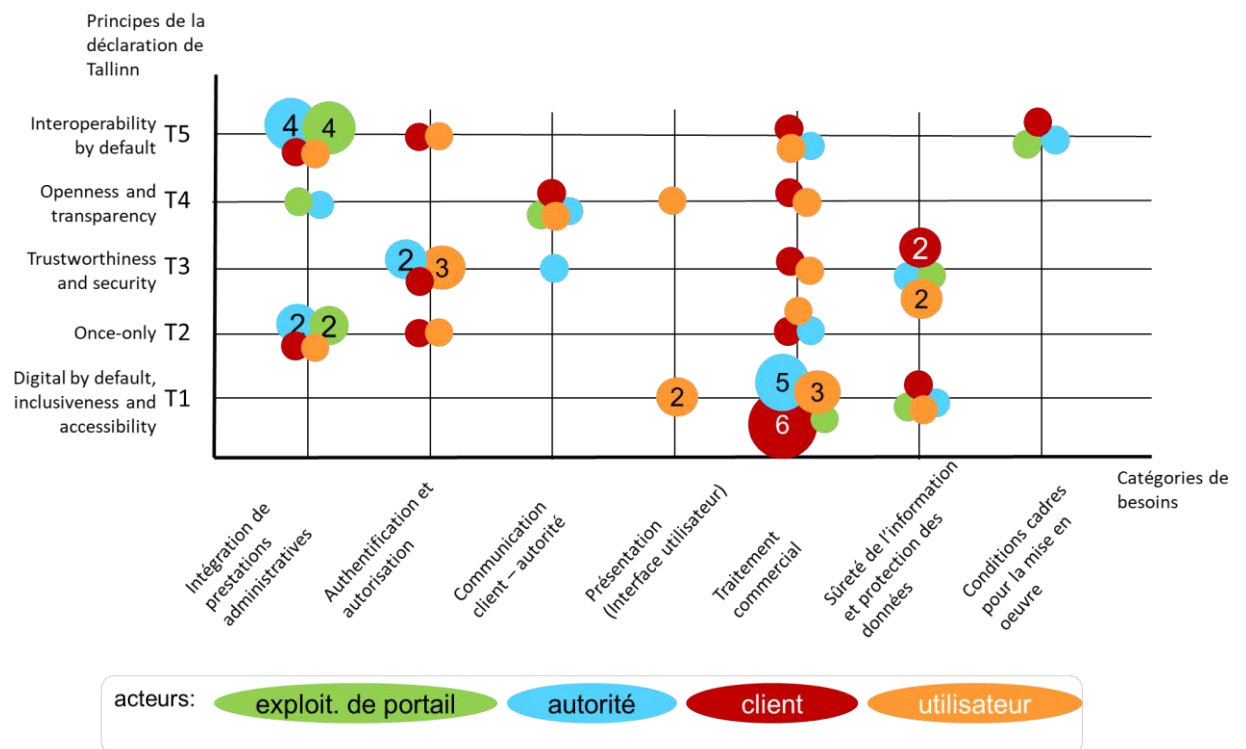


Figure 26: Catégorisation des besoins par Tallinn, thèmes et acteurs (la taille des bulles représente le nombre de mentions)

2.2.3 Délimitations

Les besoins suivants sortent du périmètre de la présente étude et ont été explicitement délimités:

Tableau 11: Délimitations du périmètre de l'architecture cible

Non.	Titre	Délimitation
[A-1]	UX	Seuls les sujets UX pertinents pour l'architecture sont pris en compte. Les besoins supplémentaires dans le domaine de l'UX sont explicitement délimités.
[A-2]	Processus d'autorité internes	L'architecture cible est axée sur la couverture des prestations administratives pour les clients et les utilisateurs. Les processus et les systèmes métier internes de l'autorité sont hors du périmètre, tout comme la communication et les interfaces entre les différents bureaux. (Voir également la Figure 9)
[A-3]	Focalisation	L'architecture cible d'intégration pour les portails de prestations requise dans la mesure M1 (voir chapitre 1) est développée indépendamment d'EasyGov. Seule l'analyse des écarts prévue à l'étape M2 porte sur EasyGov.
[A-4]	Financement	Les questions relatives au financement (par exemple, pour la réalisation d'un portail de prestations) sortent du périmètre de cette étude.
[A-5]	TCR	Les responsabilités structurelles sont grossièrement définies dans cette étude, voir chapitre 2.5. Cependant, la manière dont ces responsabilités sont mises en œuvre et vécues dans la pratique sort du périmètre de cette étude. (TCR: tâches, compétences, responsabilités)
[A-6]	Interfaces	Seules les interfaces externes entre les différentes responsabilités sont pertinentes en termes d'interopérabilité. Les interfaces internes ne présentent pas d'intérêt et ne seront pas étudiées dans cette étude.

Note: Les délimitations se réfèrent à la présente étude. Ils peuvent très bien devenir obsolètes dans les activités en aval (voir chapitre 2.7).

2.2.4 Attentes en matière de qualité de l'architecture cible

Lors de l'évaluation des besoins (voir chapitre 2.2.2), outre les besoins réels, des attentes qualitatives ont également été exprimées concernant l'architecture d'intégration souhaitée pour les portails de prestations. Elles sont énumérées ci-dessous. Conformément à la note placée à la fin du chapitre 2.2.2, il convient de noter ici qu'il s'agit d'attentes et non d'exigences précises. Ces attentes donnent une idée des facteurs "mous" qui déterminent principalement l'acceptation de l'architecture cible par les parties prenantes.

Tableau 12: Attentes en matière de qualité pour l'architecture cible

Non.	Besoin de	Besoin de...
[Q-1]	Concept ouvert, facilement extensible.	Exploitant de portail, autorité
[Q-2]	Simplicité technique de l'intégration / "Bring your own service" doit être très facile à mettre en œuvre / Modèles d'intégration adéquats (coûts / avantages) / Flexibilité.	Autorité
[Q-3]	Soutenir les différentes maturités de mise en œuvre des communes en matière de principes de numérisation (ex: si le principe du "Once-Only" est appliqué, la mise en œuvre prendra un certain temps).	Autorité
[Q-4]	Implication de toutes les parties prenantes / engagement de toutes les parties prenantes envers la solution.	Exploitant de portail, autorité
[Q-5]	Aucun compromis politique, des solutions purement factuelles.	Exploitant de portail, autorité
[Q-6]	Soutien des institutions correspondantes (eCH).	Exploitant de portail, autorité
[Q-7]	Lorsque des normes sont définies, il faut s'assurer qu'elles sont respectées et mises en œuvre.	Exploitant de portail

2.3 Principes architecturaux

2.3.1 Considération préliminaire: Interoperability Principles du EIF

En conséquence de la condition cadre incorporée par le mandat d'initialisation du projet [1] ([F-2], voir chapitre 2.2.1), les "interoperability principles" énumérés dans le document "The New European Interoperability Framework " (EIF) [17] au chapitre 2 ont été analysés. Le Tableau 13 ci-dessous montre comment ces principes sont appliqués dans l'étude. Le EIF est référencé par la déclaration de Tallinn (voir 2.2.2.1).

Tableau 13: Traitement des *Interoperability Principles* du EIF dans l'étude

Non.	Titre	Recommandations			Conséquences pour le développement de l'architecture cible
		pertinent	partiellement pertinent	non pertinent	
[EIF-1]	Subsidiarity and proportionality	Ensure that national interoperability frameworks and interoperability strategies are aligned with the EIF and, if needed, tailor and extend them to address the national context and needs.			Ce principe est à l'origine du principe architectural [P-1]. En outre, la condition-cadre [F-2] suit une idée analogue.
[EIF-2]	Openess	Publish the data you own as open data unless certain restrictions apply.			Non pertinent pour l'architecture cible actuelle.
		Ensure a level playing field for open source software and demonstrate active and fair consideration of			Hors du périmètre de l'étude (voir les délimitations [A-3] et [A-4]). L'architecture cible crée un cadre <i>conceptuel</i>

Non.	Titre	Recommandations			Conséquences pour le développement de l'architecture cible
		pertinent	partiellement pertinent	non pertinent	
		using open source software, taking into account the total cost of ownership of the solution.			pour le développement des portails de prestations.
		Give preference to open specifications, taking due account of the coverage of functional needs, maturity and market support and innovation.			Correspond à la condition du cadre [F-1].
[EIF-3]	Transparency	Ensure internal visibility and provide external interfaces for European public services.			Le développement de l'architecture cible est une mesure au sens de la recommandation. En outre, les normes et services de base existants sont identifiés dans le cadre de l'architecture cible et leur utilisation éventuelle est vérifiée.
[EIF-4]	Reusability	Reuse and share solutions and cooperate in the development of joint solutions when implementing European public services.			La mise en place du groupe d'experts responsable de cette architecture cible avec une orientation vers tous les niveaux fédéraux est une mesure au sens de la recommandation.
		Reuse and share information and data when implementing European public services, unless certain privacy or confidentiality restrictions apply.			L'inclusion de l'architecture cible dans la norme publique eCH (voir la condition-cadre [F-1]) est une mesure au sens de la recommandation.
[EIF-5]	Technological neutrality and data portability	Do not impose any technological solutions on citizens, businesses and other administrations that are technology-specific or disproportionate to their real needs.			Ce principe est à l'origine du principe architectural [P-2].
		Ensure data portability, namely that data is easily transferable between systems and applications supporting the implementation and evolution of European public services without unjustified restrictions, if legally possible.			Correspond au besoin [B-2].
[EIF-6]	User-centricity	Use multiple channels to provide the European public service, to ensure that users can select the channel that best suits their needs.			Correspond au besoin [B-1].
		Provide a single point of contact in order to hide internal administrative complexity and facilitate users' access to European public services.			Correspond au besoin [B-16].
		Put in place mechanisms to involve users in analysis, design, assessment and further development of European public services.			Le catalogue des besoins collectés au cours de l'étude (voir 2.2.2) implique la perspective du client et de l'utilisateur. C'est un instantané. Cependant, l'implication continue des clients - comme le recommande l'EIF - n'entre pas dans le périmètre de l'étude (voir la délimitation [A-1]).

Non.	Titre	Recommandations			Conséquences pour le développement de l'architecture cible
		pertinent	partiellement pertinent	non pertinent	
		As far as possible under the legislation in force, ask users of European public services once-only and relevant-only information.			La première partie (once-only) est conforme à l'exigence [B-17]. La deuxième partie relève de la responsabilité de l'autorité respective.
[EIF-7]	Inclusion and accessibility	Ensure that all European public services are accessible to all citizens, including persons with disabilities, the elderly and other disadvantaged groups. For digital public services, public administrations should comply with e-accessibility specifications that are widely recognised at European or international level.			Correspond à la condition cadre [F-6].
[EIF-8]	Security and privacy	Define a common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.			Correspond au besoin [B-25].
[EIF-9]	Multilingualism	Use information systems and technical architectures that cater for multilingualism when establishing a European public service. Decide on the level of multilingualism support based on the needs of the expected users.			Correspond à la condition cadre [F-6] et au besoin [B-14]
[EIF-10]	Administrative simplification	Simplify processes and use digital channels whenever appropriate for the delivery of European public services, to respond promptly and with high quality to users' requests and reduce the administrative burden on public administrations, businesses and citizens.			Le développement de l'architecture cible est une mesure au sens de la recommandation.
[EIF-11]	Preservation of information	Formulate a long-term preservation policy for information related to European public services and especially for information that is exchanged across borders.			Fait référence à l'accessibilité et au stockage des fichiers. C'est la responsabilité de l'autorité. Les processus d'autorité internes sont en dehors du périmètre de l'étude, voir la délimitation [A-2].
[EIF-12]	Assessment of Effectiveness and Efficiency	Evaluate the effectiveness and efficiency of different interoperability solutions and technological options considering user needs, proportionality and balance between costs and benefits.			Les images cibles et les variantes de solutions développées dans le cadre de l'étude sont évaluées par rapport au catalogue des besoins (procédure standard HERMES). Le processus d'évaluation ne s'arrête pas là, mais accompagne constamment les mesures qui vont au-delà de l'étude.

2.3.2 Principes architecturaux pour l'architecture cible

Les principes architecturaux formulés ici fournissent une orientation pour le développement de l'architecture cible. Attention, il ne s'agit pas de conditions cadres (elles ont déjà été compliées au chapitre 2.2.1). Les principes architecturaux servent plutôt d'orientation dans le processus de développement, en particulier lorsqu'il s'agit de choisir entre des alternatives aussi mauvaises les unes que les autres³⁶. Contrairement aux conditions cadres, ce qui suit s'applique donc aux principes architecturaux:

- "Moins, c'est plus"
- La formulation peut également laisser place à l'interprétation

Tableau 14: Principes d'architecture pour l'architecture cible

Non.	Titre	Description	Conséquences pour le développement de l'architecture cible
[P-1]	Réutiliser avant de créer soi-même	Dans la mesure du possible, donnez la priorité aux solutions éprouvées plutôt qu'à la création de solutions propres. Cela signifie également qu'il faut utiliser les normes autant que possible.	Pour un problème donné, il faut d'abord rechercher les solutions existantes et les analyser pour déterminer leur potentiel de réutilisation.
[P-2]	Le concept avant la technologie	Traiter les problèmes principalement au niveau conceptuel. Le niveau technologique n'est pas au premier plan, mais la faisabilité doit être assurée.	Limitation - dans la mesure du possible et du raisonnable - aux spécifications conceptuelles, évitement des dépendances vis-à-vis de technologies ou de fabricants spécifiques. Toutefois, des recommandations techniques sont souhaitées.
[P-3]	L'architecture d'intégration avant l'architecture du système	L'architecture cible d'intégration susmentionnée pour les portails de prestations ne se concentre pas sur les architectures de systèmes des portails individuels, mais plutôt sur un "écosystème" interportails qui régule l'interaction et améliore l'interopérabilité, voir la Figure 1.	Orientation vers les interfaces, aussi peu de spécifications que possible pour les architectures de systèmes individuels, celles-ci devant néanmoins être libres.
[P-4]	La décentralisation avant la centralisation	... afin de ne pas entraver le développement agile du paysage des portails. En raison de la complexité des prestations administratives à tous les niveaux fédéraux, une solution centrale n'est de facto pas non plus possible.	Des spécifications centrales sont indispensables, mais celles-ci ne devraient aller que jusqu'à ce qui est nécessaire pour l'interopérabilité.

³⁶ Proverbial: "Le choix entre la peste et le choléra".

[P-5]	Les besoins des utilisateurs/clients ³⁷ avant ceux des autorités et des exploitants de portail	Lors de l'évaluation des variantes de solutions, accorder plus de poids aux besoins des utilisateurs/clients qu'à ceux des autorités et des exploitants de portail. Ce principe est clairement conditionné par l'application de la déclaration de Tallinn ³⁸ , voir chapitre 2.2.2.1.	Il se peut que la satisfaction des attentes des utilisateurs se heurte aux lois, réglementations, etc. locales (par exemple, la protection des données ou les réglementations informatiques). Ces conflits doivent être clarifiés autant que possible dans le cadre de l'étude.
[P-6]	Se concentrer sur les aspects indépendants des autorités	Éviter que l'architecture cible dépende d'aspects spécifiques aux prestations administratives afin de permettre l'adoption de règles générales.	L'architecture cible fait abstraction des aspects généraux et des aspects spécifiques aux prestations et ne régit que les premiers.
[P-7]	Couplage faible	Fait référence à un faible degré d'interdépendance entre plusieurs composants ou systèmes.	Les systèmes qui relèvent de responsabilités différentes doivent être couplés de manière souple dans la mesure du possible.

³⁷ Voir également l'étude nationale sur la cyberadministration <https://www.egov.ch/fr/dokumentation/etude-nationale-2019/>

³⁸ Voir la vision de la déclaration de Tallinn sur la cyberadministration, page 3 de la déclaration, http://ec.europa.eu/newsroom/document.cfm?doc_id=47559.

<p>[P-8]</p>	<p>Utilisation d'initiatives fédérales pertinentes</p>	<p>La mise en œuvre réussie des projets de la Confédération peut être anticipée. Par projets de la Confédération, on entend ce qui suit:</p> <ul style="list-style-type: none">• Les lois et projets fédéraux qui se trouvent dans le processus législatif au moment de la préparation de cette étude et qui ne sont donc pas encore entrés en vigueur. La modification de la loi sur l'AVS concernant l'utilisation plus large du numéro AVS par les autorités³⁹, mais aussi la LMETA⁴⁰ et la LACRE⁴¹ sont notamment pertinentes.• Projets initiés au niveau fédéral qui n'ont pas encore été mis en œuvre au moment de la préparation de cette étude. Il convient de mentionner ici, par exemple, les objectifs de mise en œuvre selon le plan de mise en œuvre 2021 - 2023 de la cyberadministration suisse [19] et le document de discussion sur l'"image cible de l'e-ID" [36]. <p>Il s'agit d'atteindre les objectifs suivants:</p> <ul style="list-style-type: none">• L'architecture cible doit rester à jour le plus longtemps possible et ne pas devenir obsolète et inutile en raison de projets de la Confédération mise en œuvre dans un avenir prévisible.• Les projets de la Confédération mis en œuvre devraient être renforcés par le traitement de celles-ci dans l'architecture cible et par une utilisation généralisée de l'architecture.	<p>L'architecture cible peut (mais ne doit pas) anticiper l'entrée en vigueur des lois fédérales prévues et pertinentes et la mise en œuvre réussie des projets pertinents au niveau fédéral et les utiliser en conséquence, le cas échéant, aux fins de l'architecture.</p>
--------------	--	---	--

2.4 Image cible

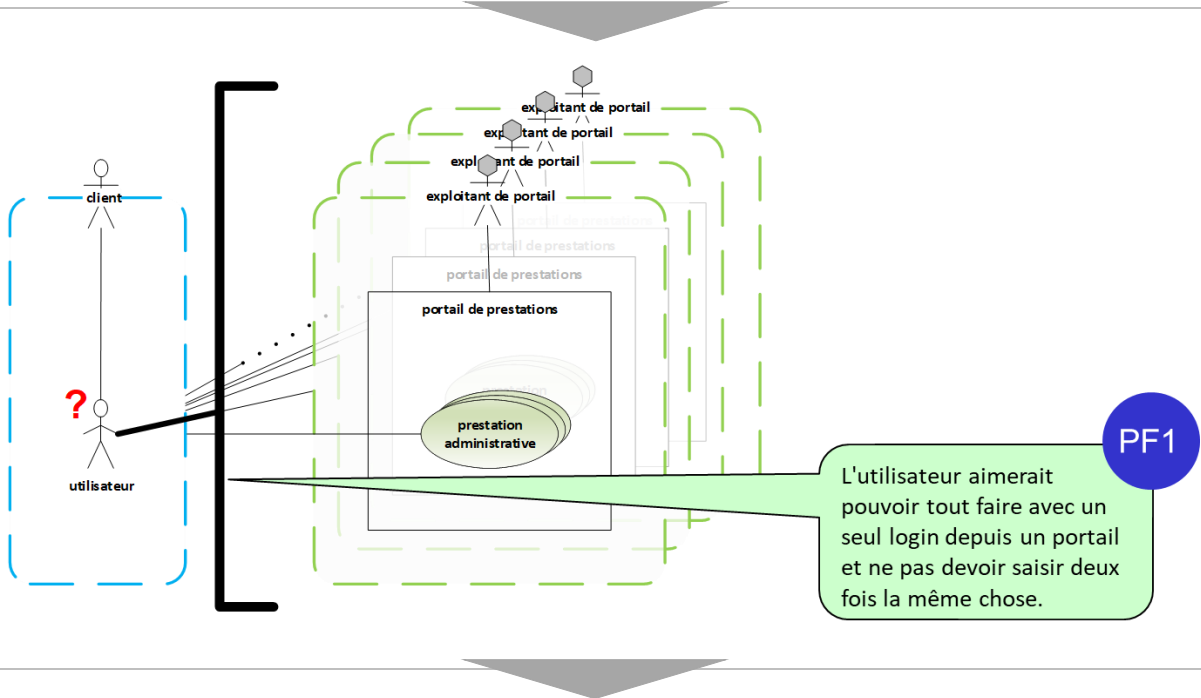
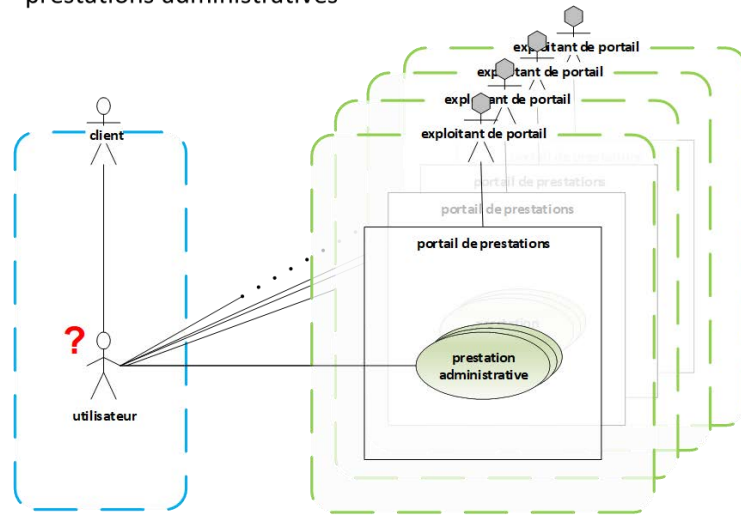
L'image cible découle des besoins identifiés au chapitre 2.2.2. Les points focaux de ces besoins peuvent être résumés en points faibles (PF), comme l'illustrent les schémas suivants. Compte tenu du principe architectural [P-5], les besoins de l'utilisateur/client sont placés au premier plan.

³⁹ Voir <https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaefte?AffairId=20190057>

⁴⁰ Voir <https://www.admin.ch/gov/fr/accueil/documentation/communiqués.msg-id-81580.html>

⁴¹ Voir <https://www.admin.ch/gov/fr/accueil/documentation/communiqués.msg-id-83285.html>

Les utilisateurs sont confrontés à une variété de portails et différentes prestations administratives



PF1

L'utilisateur aimerait pouvoir tout faire avec un seul login depuis un portail et ne pas devoir saisir deux fois la même chose.

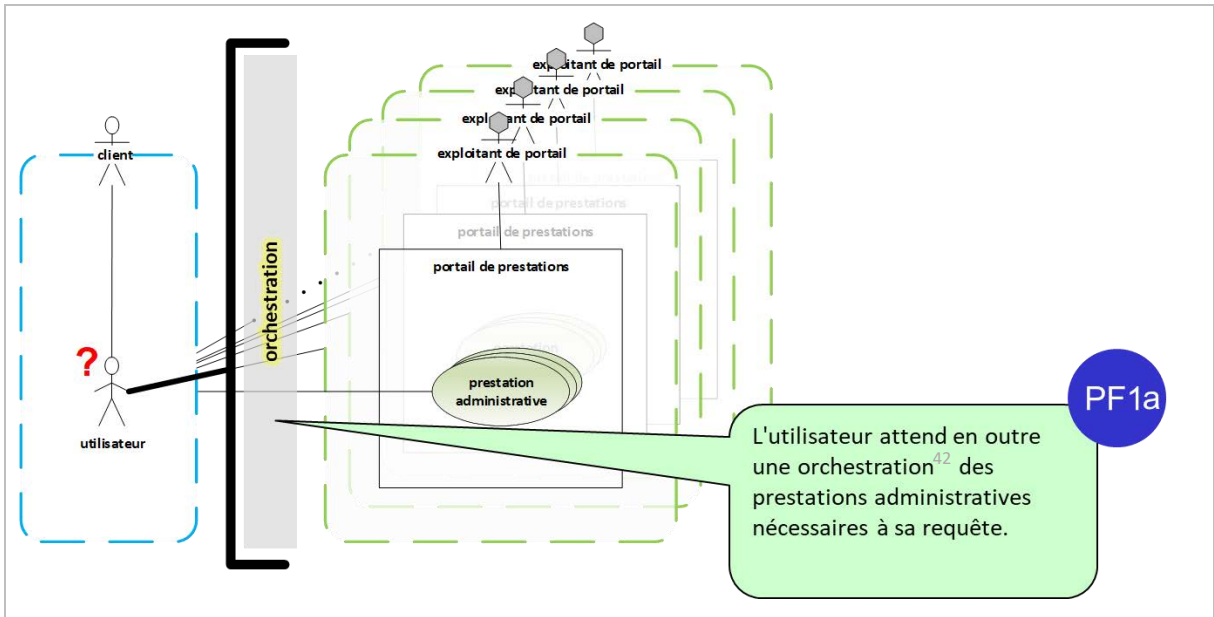
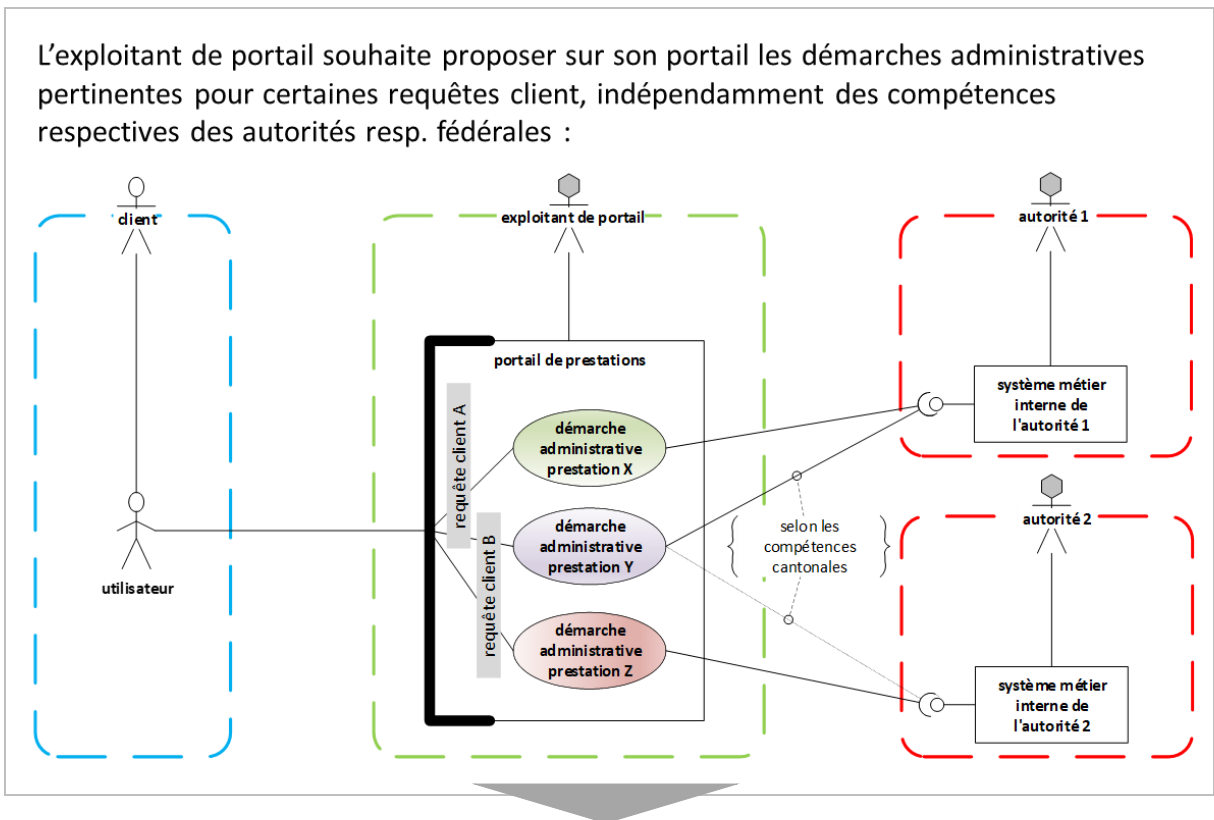
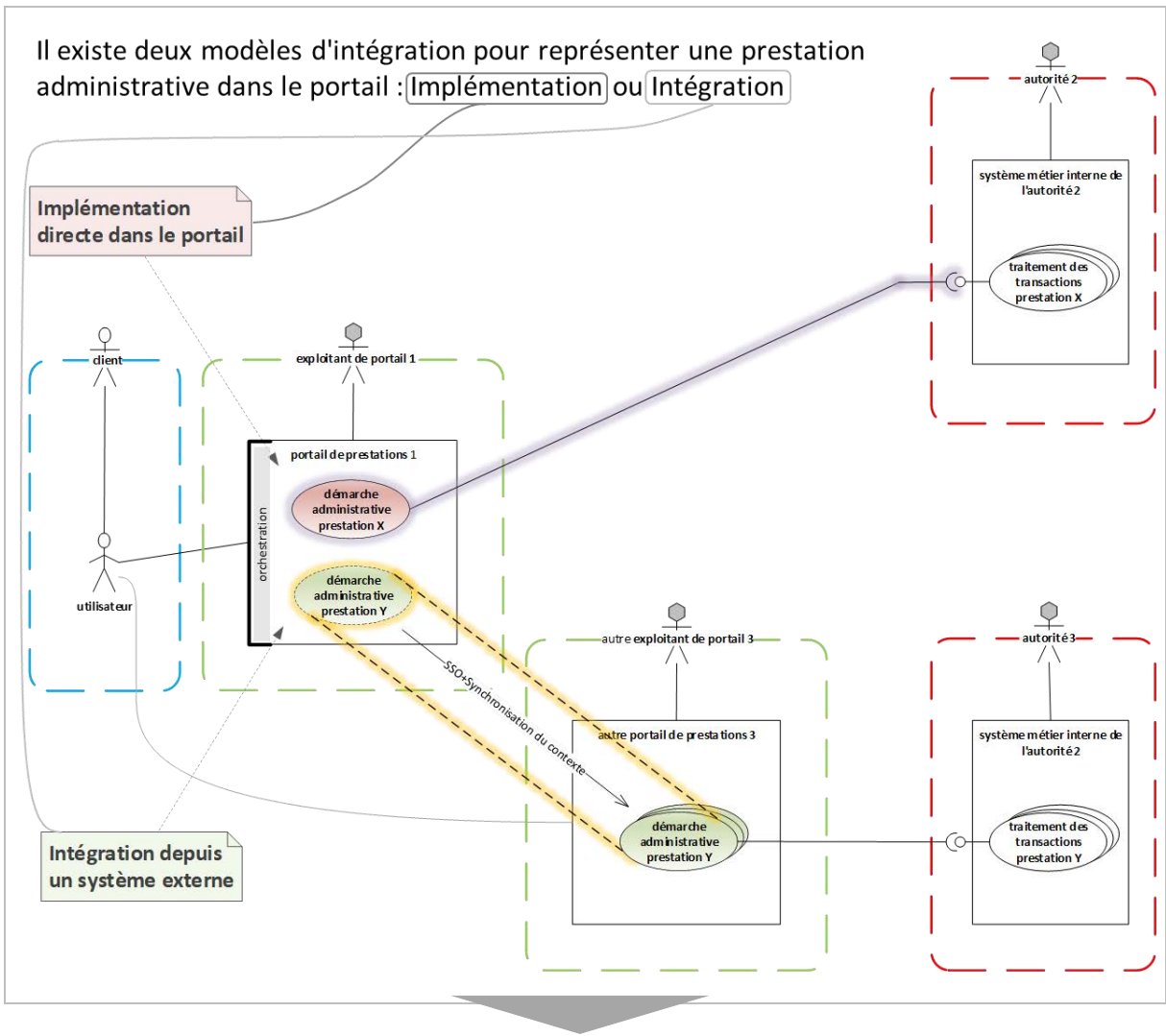


Figure 27: Séquence d'images pour le point faible 1

Les efforts des exploitants de portail pour prendre en compte ce point faible PP1 ou PP1a par le biais d'offres intégratives (voir l'Annexe E) font apparaître d'autres points faibles:





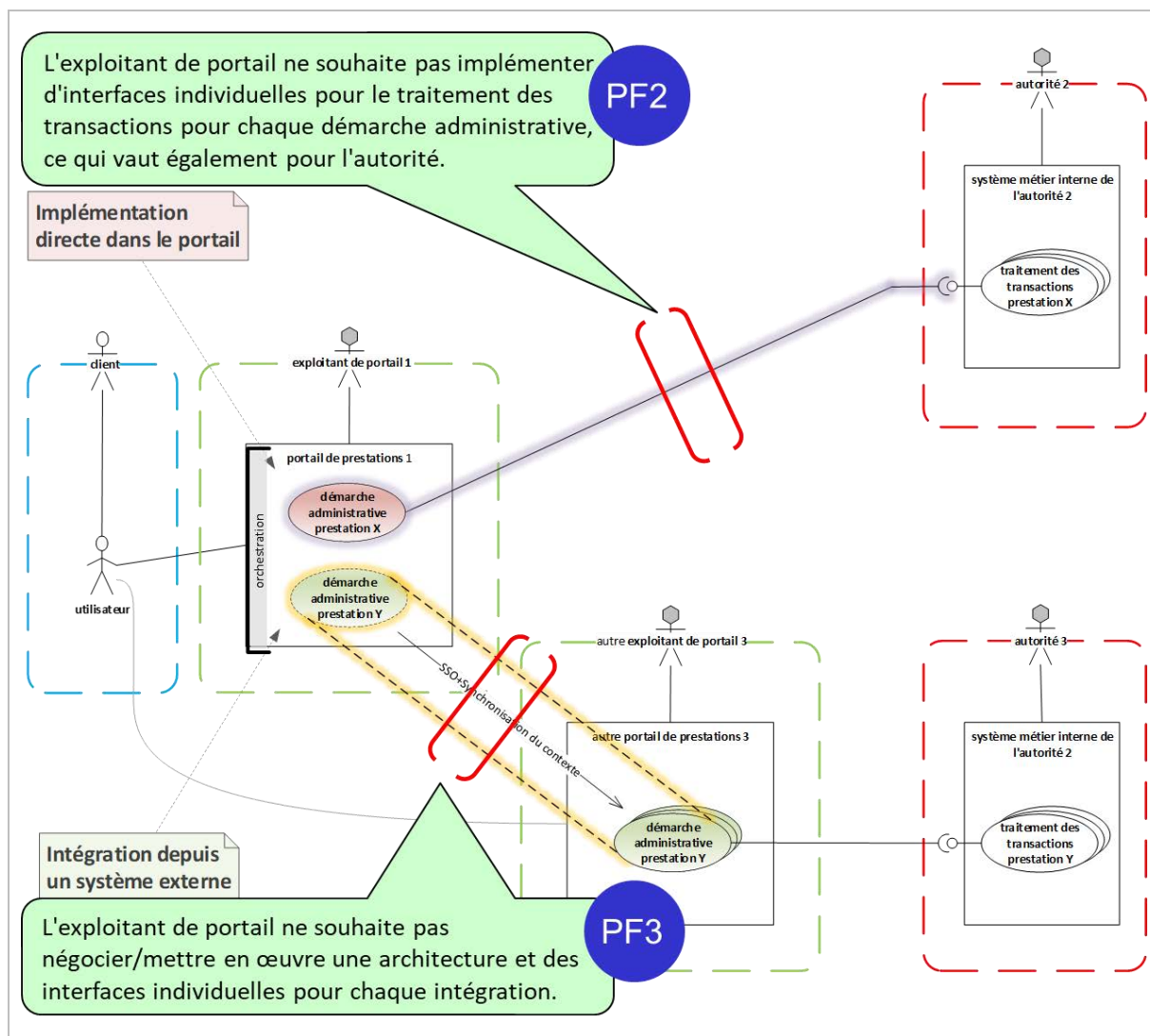


Figure 28: Séquence d'images pour les points faibles 2 et 3

Pour résoudre ces problèmes, il faut un degré suffisant d'interopérabilité des données au niveau des interfaces, ce qui suppose une base conceptuelle globale. A partir de cette considération, les points faibles conduisent à l'image cible des **sujets de normalisation**:

⁴² L'orchestration signifie que le portail guide l'utilisateur à travers les prestations administratives pertinentes, par exemple en alignant les procédures nécessaires de l'autorité moyennant un assistant/wizard (voir Figure 11).



- Définition d'un cadre d'interopérabilité (voir les exigences selon le chapitre 2.5.1.1)
 - Modèle d'information global
 - Mise en place de systèmes d'identification et d'un vocabulaire contrôlé
 - Définition et délimitation des données de base interoperables



- Standardisation de l'interface démarche administrative ↔ traitement des transactions (modèle d'intégration 1 selon le chapitre 2.1.6 et exigences selon le chapitre 2.5.1.2).
 - Cadre des processus de communication généraux (non spécifiques aux prestations)
 - Transmission du statut du traitement, des notifications officielles, des documents de résultats



- Standardisation de l'interface pour l'intégration des démarches administratives implémentées en externe (modèle d'intégration 2 selon le chapitre 2.1.6 et exigences selon 2.5.1.3).
 - Processus d'exécution lors de l'appel d'une démarche administrative intégrée
 - Spécification des positions de confiance nécessaires

En résumé, l'image cible est:

La normalisation prévue devrait permettre l'interopérabilité des données et des processus nécessaires à l'interaction entre les portails de prestations.

2.5 Développement de l'architecture cible d'intégration

Dans ce chapitre, l'architecture cible d'intégration est développée grossièrement dans le sens de l'image cible décrite ci-dessus au chapitre 2.4 (et des points faibles correspondants PP1 à PP3). Dans ce contexte, "grossièrement" signifie que les domaines à régler sont définis et que des stipulations fondamentales sont faites, mais qu'aucune spécification détaillée n'est faite. Les exigences sont formulées quant à ce que la normalisation souhaitée doit réaliser concrètement et à quoi doit ressembler le cadre logique de cette normalisation.

Notes:

- Conformément à l'objectif énuméré au chapitre 1, la profondeur de détail des considérations suivantes ne va que jusqu'à préparer le terrain pour l'élaboration d'une norme eCH.
- L'architecture cible d'intégration a été développée avec le groupe d'experts du projet, composé de représentants de tous les niveaux fédéraux, dans le cadre de dix ateliers d'une demi-journée (voir l'Annexe G.A et l'Annexe G.B). Les défis à résoudre ont été identifiés et travaillés étape par étape sous la forme de décisions de variantes. Le processus argumentatif et la justification des décisions individuelles sont documentés dans l'Annexe G.E.

- La question de savoir dans quelle mesure l'architecture cible d'intégration développée couvre les besoins identifiés est évaluée au chapitre 2.6.

2.5.1 Sujets de normalisation

Les différents sujets sont spécifiés sous la forme d'exigences [REQ-n] qui, dans l'intérêt de la viabilité future, sont maintenues aussi neutres que possible sur le plan technologique, conformément au principe d'architecture [P-2]. Par conséquent, l'accent est mis principalement sur les aspects techniques généraux qui sont également pertinents pour toutes les prestations administratives possibles.

- Dans le périmètre:
 - Domaines de données interopérables (par exemple, les identifiants)
 - Responsabilités (souveraineté de définition, souveraineté des données)
 - Processus d'interface
- Hors du périmètre:
 - Détermination de la technologie (par exemple, protocole, système de bus éventuel)
 - Domaines de données spécifiques aux prestations

Le point de vue "dans le périmètre/hors du périmètre" tient compte de l'image cible décrite au chapitre 2.4, à savoir que la normalisation est axée sur des données et des processus d'interface interopérables, c'est-à-dire non spécifiques à une prestation.

2.5.1.1 Cadre d'interopérabilité

Les deux points suivants sont supposés dans ce domaine:

- Les besoins centraux [B-6] et [B-7], ainsi que
- L'exigence de l'IAM selon laquelle l'identité numérique et l'identifiant du client sont deux choses différentes. Le premier est utilisé pour authentifier⁴³ les utilisateurs, le second est utilisé pour identifier les clients⁴⁴.

Sur la base de ces deux points, l'exigence suivante résulte:

[REQ-1] Un utilisateur peut utiliser le même login (c'est-à-dire l'identité numérique) pour bénéficier des prestations administratives pour plusieurs clients (PP et/ou PM). En même temps, un utilisateur peut utiliser différentes identités numériques pour s'inscrire.

La Figure 29 illustre la relation suivante entre l'utilisateur et le client, tirée de [REQ-1]: Une personne physique apparaissant sous une identité numérique est représentée en tant

⁴³ Voir <https://fr.wikipedia.org/wiki/Authentification>

⁴⁴ Voir <https://fr.wikipedia.org/wiki/Identifiant>

qu'utilisateur dans un portail de prestations. De même, un client (de l'autorité) géré dans un portail de prestations représente une personne morale ou physique qui est désignée de manière unique par un identifiant défini en externe.

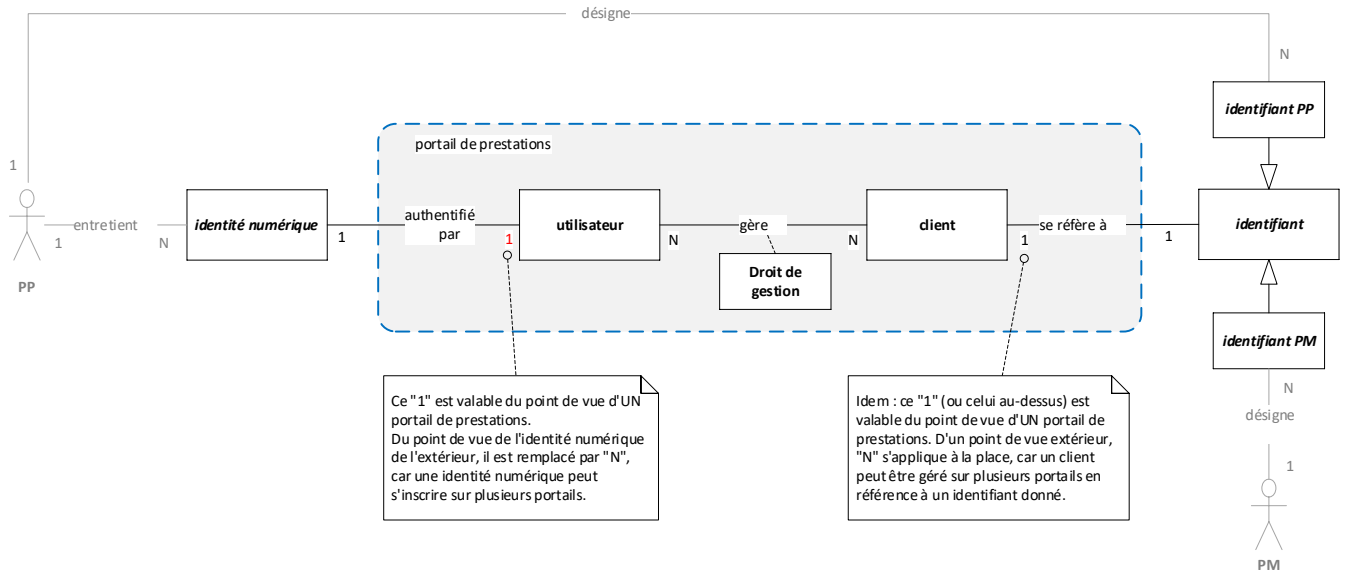


Figure 29: Un portail de prestations utilise une identité numérique⁴⁵ définie en externe pour l'authentification des utilisateurs, tandis qu'il identifie les clients à l'aide d'un identifiant⁴⁶ défini en externe.

Le diagramme suivant, Figure 30, illustre les constellations possibles et la manière dont elles doivent être mises en correspondance conformément à [REQ-1].

- La personne "Rainer Zufall" utilise deux identités numériques portées par des fournisseurs d'identité différents (FI1 et FI2) sur le portail de prestations X⁴⁷ et possède deux comptes d'utilisateur en conséquence (xu1 et xu2). Tous deux sont autorisés pour son client PP du même nom, qui est identifié par le numéro d'assuré correspondant⁴⁶. Il peut donc gérer un seul et même compte client avec les deux identités numériques.
- Rainer Zufall et Inge Borg utilisent tous deux une de leurs identités numériques pour se connecter à différents portails.
- Grâce à son identité numérique chez FI1, l'utilisateur "Rainer Zufall" ne gère pas seulement le client PP qui le représente sur le portail de prestations X, mais l'utilise également pour mener des affaires d'autorité pour son entreprise "Keis-Problem AG", qui est identifiée par son IDE.

⁴⁵ Le cas où différentes identités numériques peuvent être encapsulées par un service intermédiaire interposé entre le fournisseur d'identité et le portail n'est pas abordé initialement dans l'image cible. À cet égard, veuillez-vous référer à [Herausforderung-1] dans l'Annexe G.D

⁴⁶ Pour la question de savoir quels identifiants spécifiques de quels fournisseurs devraient être utilisés, veuillez-vous référer à [Herausforderung-2] dans l'Annexe G.D

⁴⁷ En supposant que le portail X utilise plusieurs fournisseurs d'identité.

- Le client NP "Rainer Zufall" peut être géré indépendamment sur les deux portails. La personne "Inge Borg" peut le faire sur les portails de prestations X et Y, la personne "Inge Borg" uniquement sur X. Le client PP géré est identifié dans chaque cas par le même identifiant unique (dans l'exemple, on suppose le numéro d'assuré).

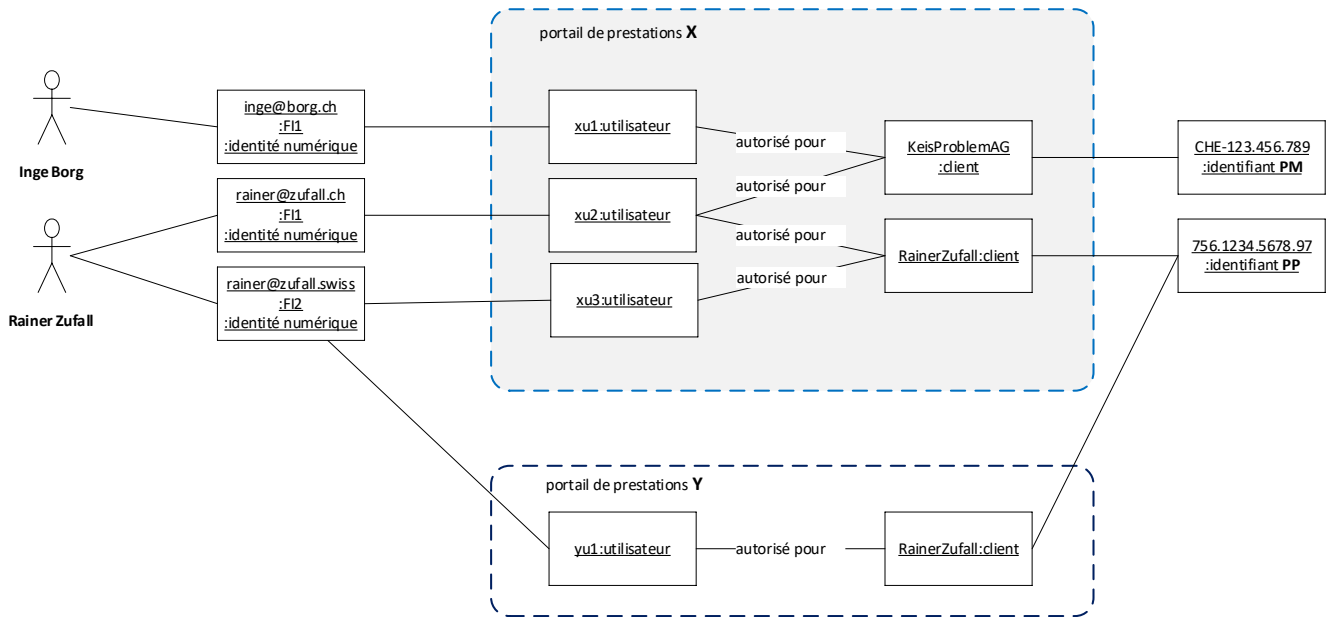


Figure 30: Illustration [REQ-1] à l'aide d'un contexte exemplaire (diagramme d'objet UML)

2.5.1.1.1 Modèle d'information

Le modèle d'information établi au chapitre 2.1.5 prend déjà en compte l'exigence [REQ-1]. Il peut donc être utilisé comme base pour le cadre d'interopérabilité.

[REQ-2] La base conceptuelle du cadre d'interopérabilité est le modèle d'information décrit au chapitre 2.1.5.

Sur la base du modèle d'information, il est possible de montrer de manière différenciée pour quelles informations les deux interfaces abordées nécessitent de l'interopérabilité (voir Figure 31). Par exemple, pour l'interface destinée à l'intégration des démarches administratives implémentées en externe (voir le modèle d'intégration 2 au chapitre 2.1.6), la prestation administrative ne joue pas de rôle, car la sélection de la prestation est effectuée dans le portail consommateur et la démarche administrative pertinente est adressée directement dans le portail fournisseur externe (voir le chapitre 2.5.1.2). Pour l'interface "démarche administrative ↔ traitement des transactions", en revanche, il n'est pas pertinent de savoir quel utilisateur a effectué la démarche administrative et avec quel droit, car cela n'est pas pertinent pour le traitement des transactions. Ce dernier requiert plutôt les données du client.

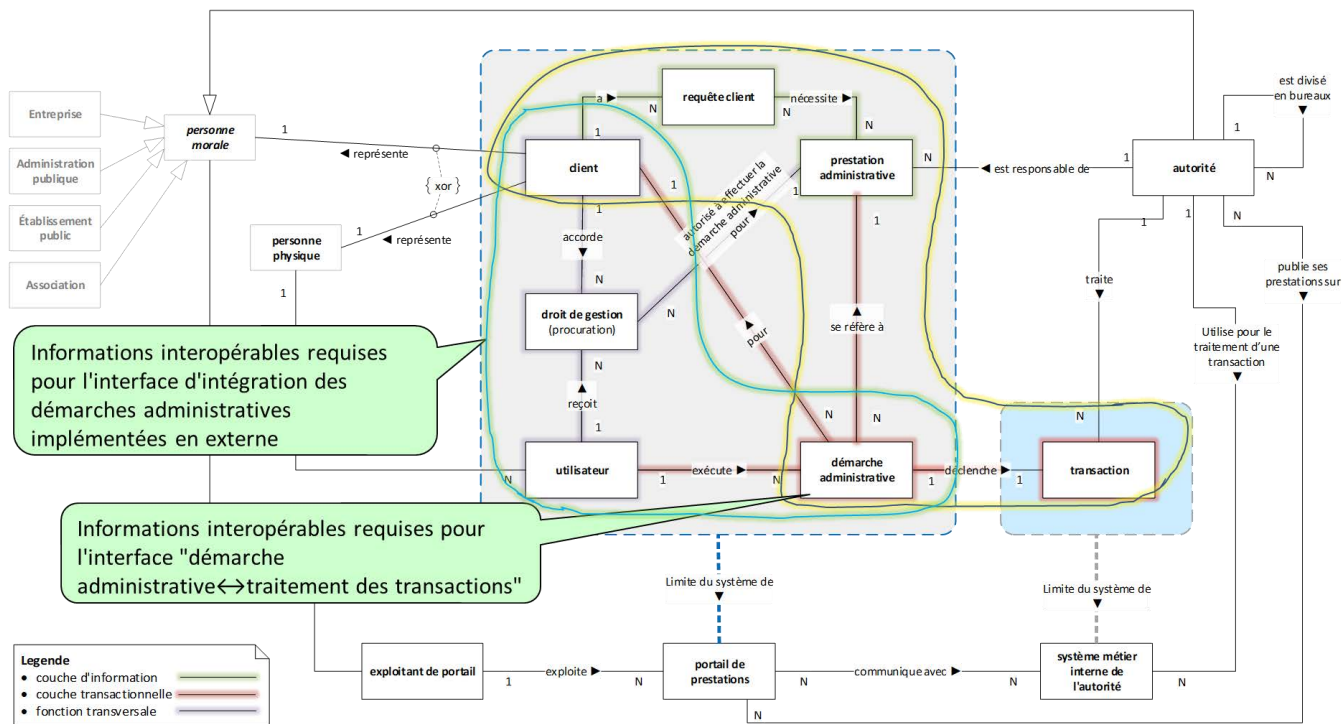


Figure 31: Localisation des exigences d'interopérabilité dans le modèle d'information

[REQ-3] Une base interopérable est définie pour les entités du modèle d'information.

Cette base interopérable est limitée à la partie des données qui, en raison des exigences d'interface spécifiées dans les chapitres 2.5.1.2 et 2.5.1.3 suivants, doit être comprise sémantiquement de la même manière par les systèmes concernés (portails et systèmes métiers internes des autorités) des deux côtés. Il s'agit principalement d'identifiants (par exemple, l'ID du client) et de vocabulaire contrôlé (par exemple, transaction.statut_traitement). En revanche, les contenus qui vont au-delà relèvent de la partie non interopérable. Pour un éventuel transfert d'interface, cette partie non standardisée devrait faire l'objet d'un accord individuel entre les partenaires concernés. Cela concerne par exemple les données spécifiques aux prestations.

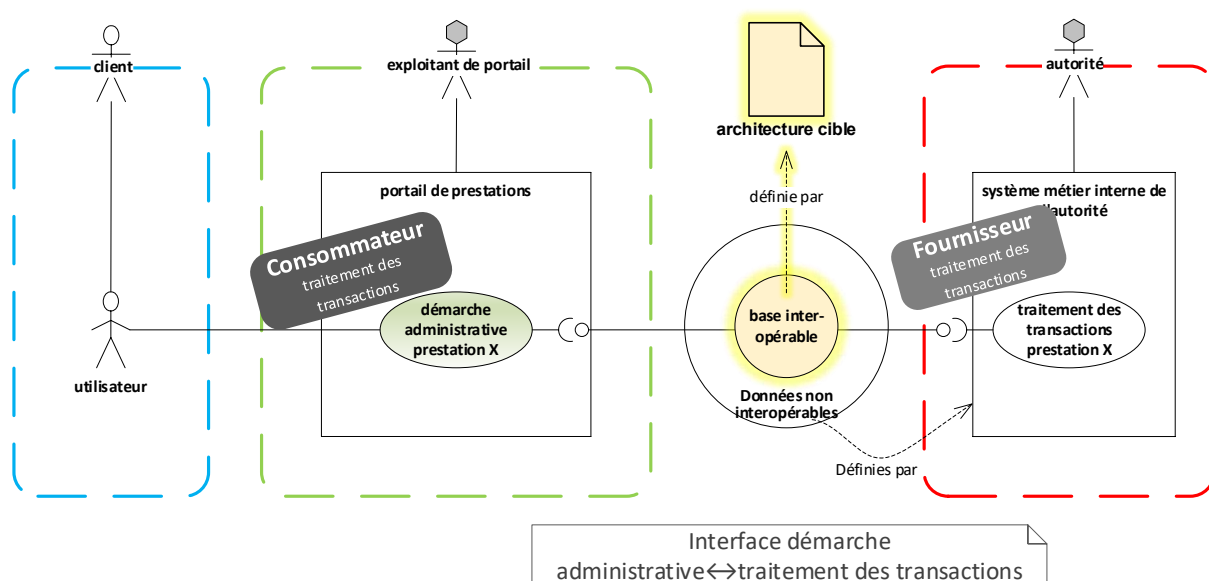


Figure 32: Illustration de la base interopérable à l'aide de l'exemple de l'interface "démarche administrative ↔ traitement des transactions" (modèle d'intégration 1).

2.5.1.1.2 Identification des prestations

[REQ-4] Pour l'identification ou le référencement d'une prestation administrative, l'inventaire des prestations de l'administration publique suisse eCH-0070 [27] fait foi.

Les références de prestations doivent être codées selon la spécification de la norme eCH-0070. Selon la Figure 35 c'est le cas pour les entités suivantes:

- Démarche administrative: référence à la prestation reçue
- Droit de gestion: référence à la prestation pour laquelle l'utilisateur en question est autorisé à gérer une démarche administrative pour le client respectif.

Le catalogue de prestations représente un vocabulaire contrôlé, dont la définition incombe à l'association eCH.

Remarque: la différenciation des prestations pratiquée actuellement dans la norme eCH-0070 semble très hétérogène. Ainsi, par exemple, pour les inscriptions au registre du commerce, outre le type d'inscription (formes juridiques, signataires autorisés, ...), une différenciation est faite entre nouvelle inscription, mutation, radiation. En revanche, ce n'est pas le cas pour les prestations dans le domaine des permis de travail. Par exemple, l'indication ID=1128 ("autorisation frontalière pour les ressortissants de l'UE/AELE (permis G CE/AELE)") ne semble pas suffisamment précise, car dans la pratique, on distingue nouvelle délivrance, prolongation, réattribution, transformation, changement de nom, changement d'emploi, etc.

2.5.1.1.3 Identification des requêtes client

[REQ-5] Actuellement, il n'existe pas de vocabulaire contrôlé pour les requêtes client. Si cela devait changer à l'avenir, il faudrait en tenir compte dans le cadre d'interopérabilité.

2.5.1.1.4 Identification des clients et gestion des données de base

Pour une identification interopérable des clients, il faut un système d'identification qui existe indépendamment du portail. Les registres d'État (tels que le [registre IDE](#)) ou les services de base⁴⁸ qui peuvent être référencés par les portails de prestations s'y prêtent. En outre, les données de base associées à l'identifiant respectif, que les registres détiennent également, s'appliquent à tous les portails.

En raison du traitement administratif différent entre les personnes morales (PM) et les personnes physiques (PP), les clients PM et PP sont considérés différemment.

2.5.1.1.4.1 Client PM

[REQ-6] Le numéro d'identification des entreprises IDE est utilisé pour identifier ou référencer un client PM.

La structure de l'IDE est définie par la norme eCH-0097 [28]. L'OFS gère le registre IDE pour l'attribution, la gestion et l'utilisation correctes de l'IDE⁴⁹. Selon les informations de l'OFS, les entreprises étrangères, c'est-à-dire les entreprises non domiciliées en Suisse, pourront également obtenir un IDE à l'avenir⁵⁰.

[REQ-7] Les portails de prestations utilisent le registre IDE comme système principal pour la base interopérable des données de base des clients PM.

Cela ne signifie pas que les portails de prestations ne doivent pas détenir de données de base sur les clients. L'exigence stipule simplement que la souveraineté des données (au sens de la vérité officielle) appartient au registre.

Les portails de prestations peuvent utiliser un service web pour la récupération électronique des données du registre IDE⁵¹. La structure des données est basée sur eCH-0108 [30], qui est elle-même basée sur eCH-0097 [28] et eCH-0098 [29].

[REQ-8] La base interopérable des données de base du client PM correspond à l'enregistrement "organisationType" défini au chapitre 3.2 dans eCH-0108 [30].

Cet enregistrement comprend les données qui peuvent être consultées publiquement dans le registre IDE.

Le processus de mise en correspondance des données de base entre le registre principal IDE et les portails de prestations est examiné au chapitre 2.5.1.1.4.3.

⁴⁸ Dans le cadre de cette étude, seul le terme "registre" sera utilisé dans ce qui suit. En principe, cela inclut également les services de base.

⁴⁹ Base légale: Loi fédérale sur le numéro d'identification des entreprises ([LIDE](#)), Ordonnance sur le numéro d'identification des entreprises ([OIDE](#))

⁵⁰ Ceci est déjà pris en compte dans les dernières versions des normes pertinentes eCH-0097 [28], eCH-0098 [29] et eCH-0108 [30]. Selon [33], la mise en œuvre dans le registre IDE lui-même devrait avoir lieu à l'horizon de la fin de 2022.

⁵¹ Voir <https://www.bfs.admin.ch/bfs/fr/home/registres/registre-entreprises/numero-identification-entreprises/registre-ide/interfaces-ide.assetdetail.11007266.html>

2.5.1.1.4.2 Client PP

[REQ-9] Le numéro d'assuré NAVS13 doit être utilisé pour identifier ou référencer un client PP.

La base légale est fournie par la loi sur l'AVS⁵² modifiée. Le processus argumentatif menant à la décision du groupe technique en faveur du NAVS13 comme identificateur PP par rapport aux autres alternatives peut être retracé dans l'Annexe G.D, [Herausforderung-2] (= défi-2).[Herausforderung-2] La question des options possibles pour l'identification des PP étrangères y est également abordée.

La gestion de l'identifiant numéro AVS dans le registre central des assurés des assurances sociales fédérales et la communication du numéro AVS en dehors du domaine AVS sont effectuées par la base de données UPI de la CdC⁵³. Les services UPI sont disponibles pour des interrogations automatiques de la base de données UPI. Leur interface externe est spécifiée par les normes eCH-0084 [5], eCH-0085 [6] et eCH-0086 [7]. L'accès est limité aux utilisateurs systématiques du numéro AVS. Toutefois, cette exigence est remplie par les portails de prestations en tant que tels.

Cependant, la base de données UPI ne peut pas fournir de données d'adresse. Cette tâche incombe plutôt au futur système central de données de référence⁵⁴ "Service national des adresses" (SNA)⁵⁵ respectivement fait l'objet du projet OMO10⁵⁶ dans le plan de mise en œuvre 2021-2023 de la cyberadministration suisse [19]. Le SNA obtient les données d'adresse des bureaux d'enregistrement et des registres de la population et se base également sur le numéro d'assuré. Elle peut donc être considérée comme un complément à la base de données UPI du point de vue des données de base des PP (voir Annexe G.D, [Herausforderung-2]).

[REQ-10] Les portails de prestations utilisent la base de données UPI ainsi que le SNA⁵⁷ comme système principal pour la base interopérable des données de base des clients PP.

Le processus de mise en correspondance des données de base entre les systèmes principaux et les portails de prestations est examiné au chapitre 2.5.1.1.4.3.

[REQ-11] La base interopérable des données de base du client PP correspond aux caractéristiques d'identité (nom, prénom, date de naissance, lieu de naissance, sexe, nationalité, etc.) qui peuvent être interrogées à partir de la base de données UPI conformément à la norme eCH-0084 [5], ainsi qu'aux données d'adresse qui peuvent être

⁵² Base légale: Loi modifiée sur l'AVS <https://www.fedlex.admin.ch/eli/fga/2020/2693/fr>

⁵³ Voir <https://www.zas.admin.ch/zas/fr/home/partenaires-et-institutions-/unique-person-identification--upi-.html>

⁵⁴ Contrairement au registre IDE, le SNA ne fait pas autorité sur le plan juridique, c'est pourquoi il est qualifié de système de données de référence et non de registre.

⁵⁵ Voir <https://www.bfs.admin.ch/bfs/fr/home/registres/service-national-adresses.html>

⁵⁶ Voir <https://www.egovernment.ch/fr/umsetzung/schwerpunktplan/aufbau-nationaler-adressdienste>

⁵⁷ Les prérequis juridiques relatives à l'accès au SNA par le biais des portails de prestations doivent encore être clarifiées dans le cadre du projet SNA.

interrogées à partir du SNA (adresse de résidence, adresse de service, commune d'établissement ou de résidence)^{55, 58, 59}.

Les informations relatives à l'état civil et aux relations avec d'autres PP (conjoints, etc.), qui sont gérées dans le registre d'état civil Infostar⁶⁰, ne peuvent pas être incluses dans la base interopérable des données de base des PP tant qu'il n'existe pas d'option d'interrogation utilisable pour les portails de prestations.

Les portails peuvent également collecter d'autres identifiants PP dans certains cas. Ceci est obligatoire, par exemple, si une personne étrangère n'a pas encore de numéro AVS (voir Annexe G.D, [Herausforderung-2]). C'est pourquoi, selon la norme eCH-0044 [3], plusieurs identifiants peuvent également être détenus et transmis.

2.5.1.1.4.3 Alignement des données de base interopérables des clients entre le portail et le registre principal

Conformément aux exigences [REQ-7] et [REQ-10] susmentionnées, la base interopérable des données de base des clients PM resp. PP détenues dans un portail de prestations doit suivre le statut des données des registres spécifiés. Afin d'éviter les conflits potentiels pour d'éventuels problèmes de cohérence, la règle suivante doit être appliquée:

[REQ-12] Les portails de prestations sont chargés de faire correspondre le statut des données au registre correspondant.

Cela signifie qu'en cas de mutation, ni un processus de réplication automatique ni un déclenchement de la propagation des données ne sont nécessaires de la part des registres concernés. Les portails doivent plutôt détecter toute différence entre l'état de leurs données et celui du registre lui-même. À cette fin, les services UPI fournissent la fonction de comparaison spécifiée dans la norme eCH-0086 [7]. Cette vérification ne doit pas nécessairement être effectuée de manière proactive. Il suffit généralement que le contrôle de la mise à jour des données de base d'un client ne soit effectué que lorsqu'un utilisateur autorisé accède au compte client en question (par exemple pour effectuer une démarche administrative). Le portail peut visualiser les divergences pour l'utilisateur et lui proposer des fonctions de réconciliation manuelle registre → portail⁶¹.

⁵⁸ Statut de l'avant-projet LSAdr: https://www.fedlex.admin.ch/fr/consultation-procedures/ended/2019#https://fedlex.data.admin.ch/eli/dl/proj/6019/57/cons_1

⁵⁹ Pour les registres officiels de personnes, les nomenclatures (ou le vocabulaire contrôlé) de l'OFS sont applicables, voir <https://www.bfs.admin.ch/bfs/fr/home/registres/registre-personnes/harmonisation-registres/nomenclatures.html>

⁶⁰ Voir <https://www.bj.admin.ch/bj/fr/home/gesellschaft/zivilstand.html> et <https://de.wikipedia.org/wiki/Infostar>

⁶¹ Exemple EasyGov: Lors de l'accès à un compte client, en cas de divergence entre les données de base de l'entreprise dans le portail et le registre IDE, un avis est affiché indiquant que celles-ci ne correspondent pas au statut actuel dans le registre IDE et l'utilisateur peut lancer une mise à jour.

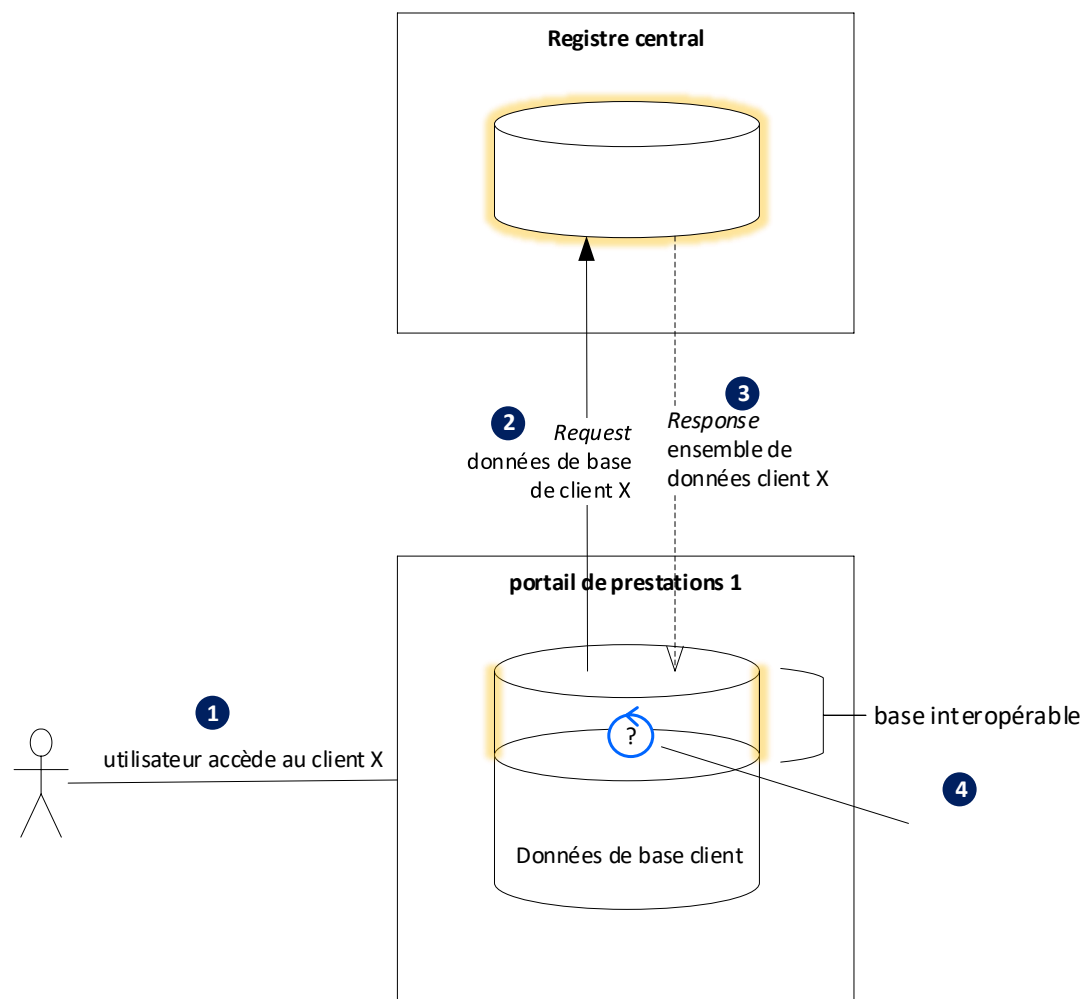


Figure 33: Mise en correspondance de la base interopérable d'une fiche client dans un portail de prestations

Nonobstant, ce qui suit s'applique spécifiquement au cas PP: la norme eCH-0212 (annonces de mutations UPI à des tiers) décrit la diffusion des mutations NAVS13 dans le registre UPI aux tiers que la CdC envoie à tous les clients qui ont souscrit. Les mutations traitées sont celles qui modifient le statut du numéro d'assuré ou les attributs démographiques d'une personne dans UPI.

2.5.1.1.5 Métadonnées des processus pour les démarches administratives et les transactions

Comme l'illustre déjà la Figure 32, une base interopérable doit être définie pour l'échange de données via l'interface "démarche administrative ↔ traitement des transactions" (décrite dans le chapitre suivant 2.5.1.2). Cet échange de données est décrit ici à l'avance pour les métadonnées des processus de communication généraux (non spécifiques à une prestation) (voir la Figure 36 au chapitre 2.5.1.2).

[REQ-13] Les métadonnées des processus de communication généraux (non spécifiques à une prestation) constituent la base interopérable et fournissent une structure et un vocabulaire contrôlé (par exemple, le statut du traitement) aux schémas définis dans eCH-0039 [2], eCH-0058 [4] et eCH-0147 [35].

[REQ-14] Pour identifier une démarche administrative au-delà de la limite du système du portail de prestations concerné, ce dernier doit fournir une valeur clé⁶² permanente et globale.

[REQ-15] Pour identifier une transaction au-delà de la limite du système du portail de prestation concerné, ce dernier doit fournir une valeur clé⁶² permanente et globale.

Les spécifications du chapitre 2.5.1.1.2 sont appliquées pour le référencement de la prestation utilisée.

Le contenu spécifique à la prestation s'appuie sur la base décrite. Différentes normes eCH définissent déjà les schémas de données et les vocabulaires contrôlés correspondants pour les différents domaines (eCH-0006 (catégories d'étrangers), eCH-0007 (communes), eCH-0008 (états et territoires), eCH-0010 (adresse postale), eCH-0011 (données concernant les personnes), eCH-0021 (données complémentaires relatives aux personnes), eCH-0046 (contacts), eCH-0119 (E-Tax Filing), eCH-0129 (référencement d'objets), eCH-0229 (déclarations d'impôts des personnes morales)). En fin de compte, les spécifications spécifiques aux prestations restent toutefois réservées aux domaines spécialisés respectifs.

2.5.1.1.6 Compte utilisateur

Un élément essentiel de l'intégration d'une démarche administrative implémentée en externe (modèle d'intégration 2, voir chapitre 2.1.6) est la redirection, c'est-à-dire le transfert de la session utilisateur du portail vers le système externe ou le portail fournisseur au moment de l'exécution. Pour que l'utilisateur puisse continuer à travailler de manière transparente lorsqu'il passe à la démarche administrative embarquée - implémentée sur un autre portail - au sens de [REQ-1] et de la dernière partie de l'exigence [B-6], la redirection doit être accompagnée d'une authentification unique (SSO) et d'une synchronisation du contexte. Cela signifie qu'en plus de l'adressage de la démarche administrative et du login de l'utilisateur, le contexte de la démarche administrative du portail consommateur, constitué de la sélection du client et du droit de gestion associé, doit être créé de manière analogue sur le portail fournisseur (voir l'illustration de la Figure 34).

⁶² Une valeur clé globale peut être formée, par exemple, selon le modèle <clé locale>@<URL du système émetteur> ou par une GUID.

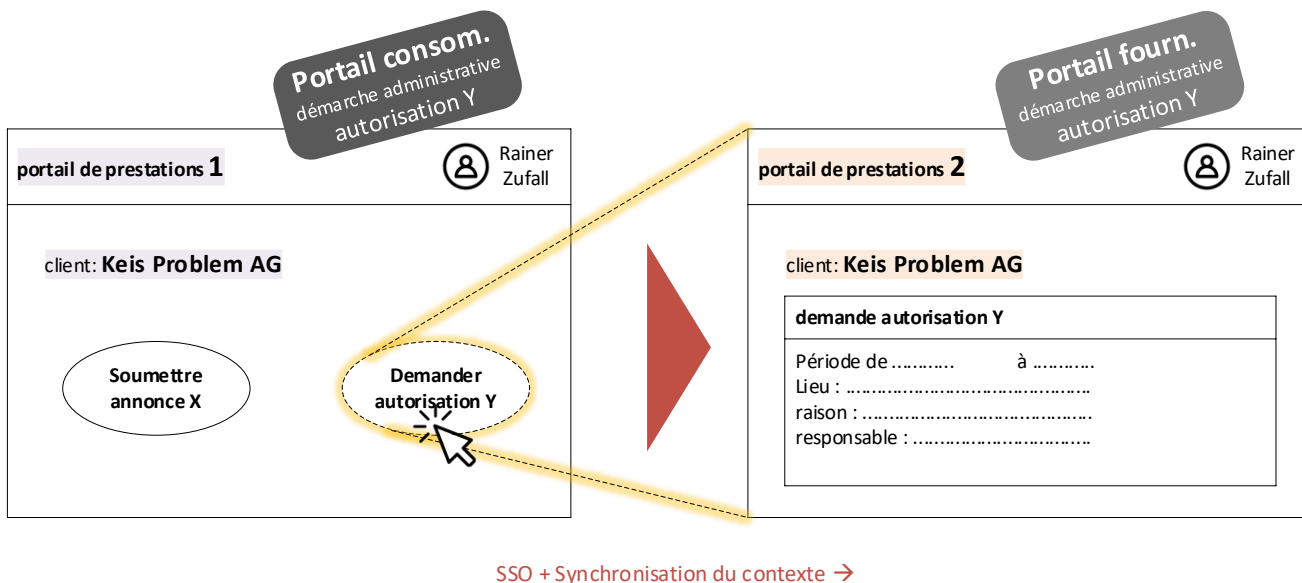


Figure 34: Établissement du contexte de session lors de l'appel de la démarche administrative "Demande d'autorisation Y" dans le portail fournisseur en conformité avec le contexte du portail consommateur au moyen de SSO + synchronisation du contexte

Pour une telle synchronisation du contexte, outre l'identification interopérable du client déjà évoquée (voir 2.5.1.1.4), il faut une interopérabilité de l'identification de l'utilisateur, des paramètres, du LoA du login ainsi que du droit de gestion. Ce point est traité dans les sections suivantes 2.5.1.1.6.1 et 2.5.1.1.6.4, les positions de confiance nécessaires dans le chapitre 2.5.1.3.

2.5.1.1.6.1 Identification

Pendant le transfert, le portail fournisseur doit d'abord ouvrir une session pour le compte utilisateur correspondant (voir la description du processus au chapitre 2.5.1.3). L'affectation de l'utilisateur associé du portail consommateur au portail fournisseur doit être basée sur une caractéristique d'identité unique, c'est-à-dire un identifiant émis par le portail consommateur. Peu importe que l'identifiant de l'utilisateur provienne du portail consommateur lui-même ou qu'il provienne de son fournisseur d'identité. L'important est que l'identifiant délivré puisse être distingué sans ambiguïté au niveau global.

[REQ-16] Pour identifier un utilisateur au-delà de la frontière du système du portail de prestations concerné, ce dernier doit fournir une valeur clé permanente et globalement unique⁶².

2.5.1.1.6.2 Paramètres (profil utilisateur)

Un transfert sans heurts dans l'intégration décrite à la Figure 34 exige, au sens du besoin [B-14], que le profil de l'utilisateur soit prolongé de manière analogue⁶³ dans le portail fournisseur.

⁶³ Les positions de confiance nécessaires sont traitées au chapitre 2.5.1.3.

Par exemple, si l'utilisateur a choisi l'italien comme langue dans le portail consommateur, la page de renvoi adressée dans le portail fournisseur doit également apparaître en italien.

[REQ-17] La base interopérable de paramètres dans le profil utilisateur comprend au moins le nom, le prénom et le paramètre de langue de l'utilisateur.

[REQ-18] Le vocabulaire contrôlé selon la norme ISO 639-1⁶⁴ est utilisé pour le réglage de la langue.

2.5.1.1.6.3 LoA du login

De même, aucun autre LoA ne peut s'appliquer sur le portail fournisseur que sur le portail consommateur. Le LoA du login documente la mesure dans laquelle on peut faire confiance à la personne réelle derrière l'utilisateur authentifié pour être réellement la personne qu'elle prétend être. Plus le processus d'enregistrement est approfondi (par exemple, avec une vérification supplémentaire de l'identité) et plus l'authentification est forte (par exemple, 2FA au lieu de 1FA), plus le degré de confiance est élevé.

[REQ-19] Pour le LoA du login, les niveaux de confiance définis dans eCH-0170 [21] sont utilisés comme vocabulaire contrôlé.

Tableau 15: Modèle de niveau de confiance LoA selon eCH-0170 [21]

Niveau LoA	Description
LoA 1	Pas ou peu de confiance
LoA 2	Faible confiance
LoA 3	Confiance considérable
LoA 4	Confiance élevée

Les niveaux de confiance individuels du modèle eCH-0170 [21] font référence à des combinaisons de force d'authentification et de qualité du processus d'enregistrement.

2.5.1.1.6.4 Droit de gestion

En outre, une transition transparente dans l'intégration décrite à la Figure 34 exige que le droit de gestion nécessaire à la démarche administrative sélectionnée du client concerné soit également accordé dans le portail fournisseur^{63,65}. Si, par exemple, l'utilisateur a fait appel à la démarche administrative "autorisation Y" intégrée dans le portail consommateur sur la base de son droit de gestion avec le niveau d'autorisation "Déposant", il doit aussi disposer précisément de ce droit dans le portail fournisseur, ni plus ni moins.

L'appel d'une démarche administrative intégrée nécessite le droit de gestion de l'utilisateur pour le client concerné pour cette démarche administrative.

⁶⁴ Voir https://fr.wikipedia.org/wiki/Liste_des_codes_ISO_639-1

⁶⁵ Le droit de gestion nécessaire doit avoir existé en soi dans le portail consommateur, sinon l'utilisateur n'aurait pas pu choisir la démarche administrative.

[REQ-20] La base interopérable du droit de gestion comprend au moins le niveau d'autorisation.

[REQ-21] Un vocabulaire contrôlé - qui doit encore être défini par une norme eCH - est utilisé pour le niveau d'autorisation.

À ce stade, le Tableau 16 illustre un exemple d'un tel modèle de niveau d'autorisation, qui est orienté vers les modèles pratiqués dans les portails de prestations actuels, qui, de manière intéressante, sont largement similaires.

Tableau 16: Modèle de niveau d'autorisation exemplaire⁶⁶

Niveau d'autorisation	Description
Traiter	Permet le traitement des démarches administratives pour un client spécifique
Soumettre	Permet de soumettre des demandes/requêtes/annonces d'une prestation administrative spécifique pour un client spécifique
Superuser	Permet d'accorder des droits de gestion pour traiter des transactions pour un client spécifique. L'octroi de ce niveau d'autorisation à un utilisateur nécessite une procuration écrite du client selon laquelle la personne derrière l'utilisateur peut gérer le compte du client sans restriction. Ceci ne s'applique pas au cas "le client PP et l'utilisateur représentent la même personne".

La question de savoir dans quelle mesure un tel vocabulaire contrôlé à l'échelle du portail resp. un modèle de niveau d'autorisation peut être clairement mis en correspondance avec les fonctionnalités d'autorisation spécifiques au portail⁶⁷ est abordée dans [Herausforderung-4] à l'Annexe G.D.

De la même manière que pour le LoA du login discuté dans le chapitre précédent 2.5.1.1.6.3, le portail fournisseur a besoin que le portail consommateur indique le niveau de confiance (LoA) du niveau d'autorisation transmis, qui documente la qualité du processus d'attribution des droits.

[REQ-22] Pour l'indication du LoA d'un droit de gestion, les niveaux de qualité définis dans la norme eCH-0171 [22] pour les confirmations de valeurs d'attributs sont appliqués comme vocabulaire contrôlé.

Les niveaux de qualité individuels spécifiés par la norme eCH-0171 [22] (voir le Tableau 17) se rapportent aux valeurs d'attribut des identités numériques (telles que la date de naissance) et quantifient la qualité du processus de la collecte. Le modèle de niveau est également applicable

⁶⁶ Attention: L'exemple ne doit pas être compris comme un projet de norme pour le modèle d'autorisation.

⁶⁷ Par exemple, "peut consulter les rendez-vous liés à la démarche administrative X, mais ne peut pas les reporter".

pour spécifier le LoA du niveau d'autorisation, d'autant plus que celle-ci peut également être comprise comme une valeur d'attribut au sens large.

Tableau 17: Niveaux de qualité selon la norme eCH-0171 [22]

Niveau de qualité	Description
1 - faible	Au niveau 1, la confiance dans la valeur d'attribut prétendue ou confirmée est minimale. On utilise ce niveau de confiance lorsque le risque associé à la valeur d'attribut utilisée est minime. Un grand nombre d'autorités d'attributs délivrent des confirmations de valeur d'attribut de ce niveau et aucune ou très peu d'exigences ne leur sont imposées.
2 - moyen	Au niveau 2, il existe une certaine confiance dans la valeur d'attribut prétendue ou confirmée. On utilise ce niveau de confiance lorsque le risque associé à la valeur d'attribut utilisée est modéré. Des processus et contrôles fondamentaux sont respectés, mais il n'y a pas de surveillance externe générale de l'autorité d'attributs. Les confirmations de valeur d'attribut de ce niveau suffisent pour le traitement d'affaires simples.
3 - élevé	Au niveau 3, la confiance dans la valeur d'attribut prétendue ou confirmée est élevée. On utilise ce niveau de confiance lorsque le risque associé à la valeur d'attribut utilisée est élevé. Les processus et contrôles mis en œuvre font l'objet de surveillance et vérifications par un service externe. Les attributs de ce niveau suffisent pour le traitement d'affaires moyennement critiques.
4 - très élevé	Au niveau 4, la confiance dans la valeur d'attribut prétendue ou confirmée est très grande. On utilise ce niveau de confiance lorsque le risque associé à la valeur d'attribut utilisée est très élevé. Les processus et contrôles mis en œuvre sont prescrits par la législation. Les confirmations de valeur d'attribut de ce niveau suffisent pour le traitement de toutes les affaires possibles.

Il convient également de noter que la norme eCH-0107 [10] définit les processus de base pour la gestion et l'octroi des droits d'accès.

Compte tenu de la nécessité [B-11], il est en outre noté:

[REQ-23] Pour les niveaux d'autorisation qui nécessitent une procuration (voir l'exemple "Superuser" dans le Tableau 16 ci-dessus), une procuration standard - à définir - juridiquement résiliente est utilisée et reconnue dans l'ensemble du portail.

2.5.1.1.7 Aperçu sommaire du cadre d'interopérabilité

Le Tableau 18 ci-dessous résume les différents éléments du cadre d'interopérabilité:

Tableau 18: Résumé du cadre d'interopérabilité

Entité	Système dirigeant	Identifica- tion	Base interopérable
Démarche administrative	Portail sur lequel s'effectue la démarche administrative ⁶⁸	Valeur clé globale ⁶⁹	Métadonnées des processus conformément aux normes eCH-0039 [2] et eCH-0058 [4] Types de messages pour la communication avec la transaction complémentaire (voir [REQ-33]) selon une norme encore à créer
Prestation administrative	eCH-0070	Vocabulaire contrôlé	
Droit de gestion	Client (physique), représenté par un superuser autorisé ⁷⁰		Niveau d'autorisation (selon une norme à créer) et son LoA (vocabulaire contrôlé selon eCH-0171 [22])
Transaction	Système métier interne de l'autorité sur lequel la transaction est traitée	Valeur clé globale ⁶⁹	Métadonnées des processus conformément aux normes eCH-0039 [2] et eCH-0058 [4] Types de messages pour la communication avec la transaction complémentaire (voir [REQ-33]) selon une norme encore à créer
(compte) Client PM	Registre IDE	IDE	Correspondant au contenu du registre IDE accessible publiquement (base eCH-0097 [28], eCH-0098 [29], eCH-0108 [30])
Requête client	Future norme eCH	Vocabulaire contrôlé	
(compte) Client PP	Registre UPI/SNA	NAVS13	Correspondant au contenu du registre UPI accessible pour les portails de prestations (selon eCH-0084 [5], eCH-0085 [6], eCH0086 [7]) et le SNA (selon la LSAdr).

⁶⁸ Dans le cas du modèle d'intégration 1 (implémentation, voir Figure 21), il s'agit du portail consommateur, tandis que dans le modèle d'intégration 2 (intégration, voir Figure 24), il s'agit du portail fournisseur.

⁶⁹ Une valeur clé globale peut être formée, par exemple, selon le modèle <clé locale>@<URL du système émetteur> ou par un GUID

⁷⁰ Parfois également appelé administrateur client

(compte) Utilisateur	FI/intermédiaire du portail sur lequel l'utilisateur s'est connecté ⁷¹	Valeur clé globale ⁶⁹	Paramétrage de la langue (vocabulaire contrôlé selon ISO-639) et LoA du login (vocabulaire contrôlé selon eCH-0170 [21])
--------------------------------	---	----------------------------------	--

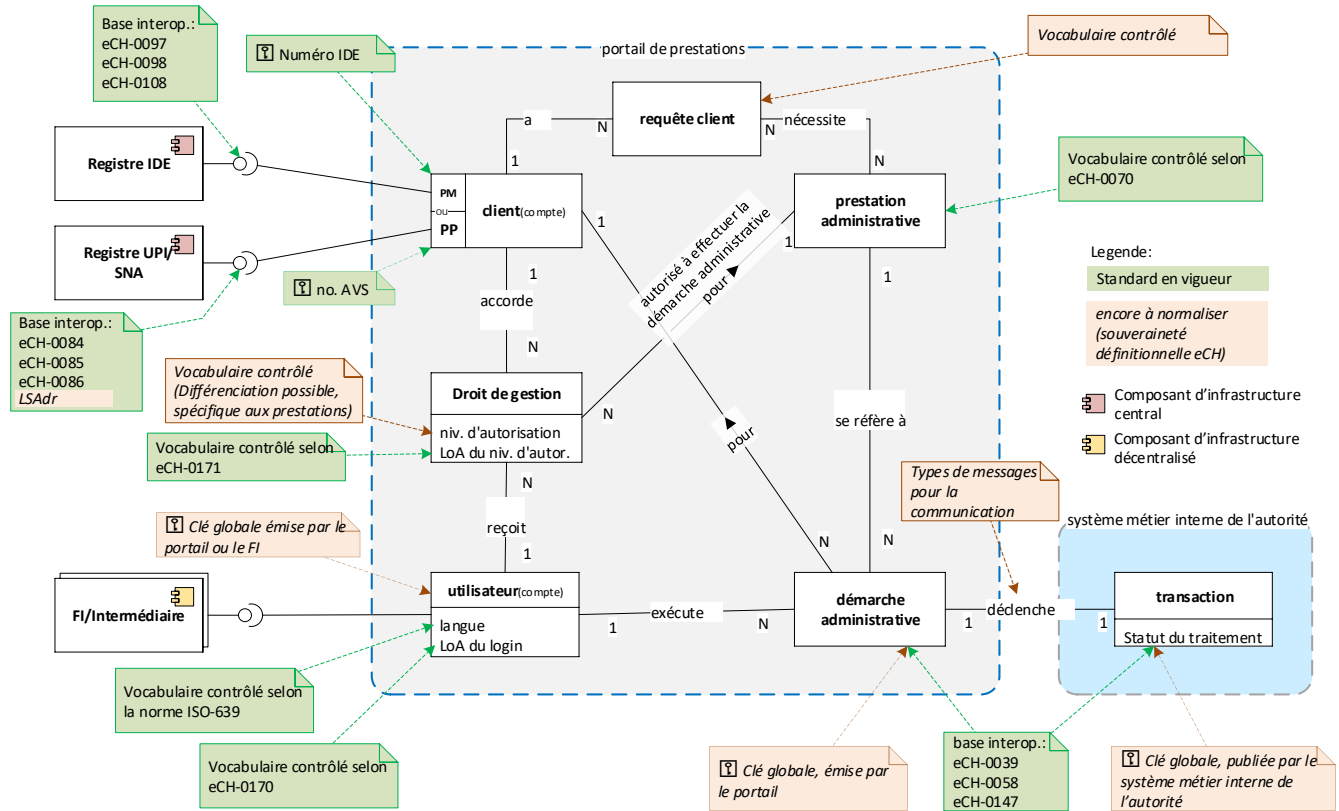


Figure 35: Situation du cadre d'interopérabilité dans le modèle d'information

2.5.1.2 Interface "démarche administrative ↔ traitement des transactions"

En principe, l'interface entre la démarche administrative et le traitement des transactions (voir le modèle d'intégration 1 au chapitre 2.1.6) peut être formulée de manière globale pour les portails selon les prémisses suivantes:

- Abstraction du contenu spécifique de la prestation administrative concernée
- Concentration sur les processus généraux de communication qui ont été élaborés au chapitre 2.1.1

⁷¹ Il s'agit du portail consommateur pour le modèle d'intégration 1 (implémentation, voir Figure 21) et le modèle d'intégration 2 (intégration, voir Figure 24).

La motivation est de briser et de découpler en grande partie les dépendances mutuelles des interfaces entre le portail de prestations et le système métier interne de l'autorité. Cela conduit - conformément au principe architectural [P-7] de couplage faible - à la définition suivante:

[REQ-24] L'architecture cible d'intégration définit les processus de communication généraux (non spécifiques à prestation) pour l'échange de données entre le portail de prestations et le système métier interne de l'autorité, sur la base desquels le contenu spécifique à la prestation respectif est transmis. Cela comprend:

- Transmission des demandes, questions et pièces jointes du client à l'autorité
- Messages de statut de l'autorité au client
- Notifications (précisions/information/rappel) de l'autorité au client et vice versa toute réponse du client à l'autorité
- Transmission du résultat de la procédure (décision/documents) de l'autorité au client

Les processus de communication généraux (non spécifiques aux prestations) sont au cœur de la normalisation de l'interface démarche administrative ↔ traitement des transactions

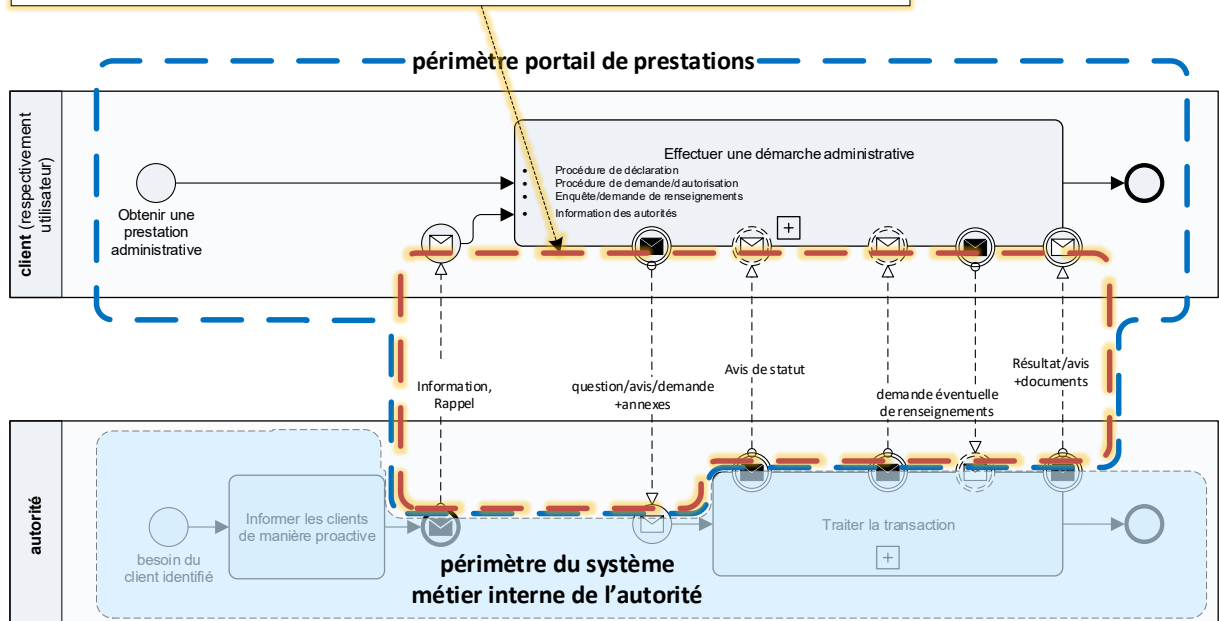


Figure 36: L'architecture cible d'intégration spécifie les processus de communication généraux (non spécifiques à une prestation) entre le portail de prestations et le système métier interne de l'autorité

[REQ-25] Pour les processus de communication, les métadonnées de processus spécifiées au chapitre 2.5.1.1.5 sont toujours fournies comme informations d'en-tête.

[REQ-26] En outre, la requête client doit être communiquée, si elle est connue⁷².

En plus:

[REQ-27] La communication doit être ciblée, c'est-à-dire qu'un message envoyé par un client spécifique dans un portail doit non seulement être reçu par le système métier interne de l'autorité compétente adressée, mais aussi être attribué à ce client.

[REQ-28] Il en va de même dans le sens inverse. Un message envoyé par le système métier interne de l'autorité à ce client doit être reçu dans le portail dans lequel la démarche administrative initiale a été effectuée et affecté à cette démarche administrative dans le compte client concerné.

Remarque: les deux dernières exigences sont déjà prises en charge par les normes eCH définies dans [REQ-13].

[REQ-29] En vertu du principe de couplage faible, les documents doivent être transmis intégralement sous forme de fichier et non de lien⁷³. Cette dernière solution entraînerait une dépendance vis-à-vis de l'hôte du lien.

[REQ-30] En cas de notification officielle proactive de l'autorité vers le client (par exemple, rappel d'une obligation d'annonce, déclenchement ultérieur de la démarche administrative électronique après un contact physique classique au sens de [B-19]), il doit être possible pour l'autorité de déclencher une démarche administrative avec le client.

[REQ-31] En raison des procédures spéciales mentionnées au chapitre 2.1.1, sous-processus et transfert de procédures (voir Figure 5 et Figure 6), l'interface de communication doit également être en mesure de mettre en correspondance des processus imbriqués.

[REQ-32] En conséquence des deux exigences [REQ-28] et [REQ-31], le modèle d'information suivant, qui a été affiné pour entités "démarche administrative" et "transaction", est utilisé comme base pour les processus d'interface:

⁷² Actuellement, en raison de l'absence d'un vocabulaire contrôlé (voir 2.5.1.1.3), ces informations peuvent au mieux être transmises sous forme de texte libre dans le champ de commentaire de l'en-tête (voir eCH-0058 [4]).

⁷³ Nonobstant, une autorité peut - par exemple pour des raisons légales - transmettre des documents via des plateformes reconnues (telles que IncaMail ou PrivaSphere) ou par voie postale. Cette responsabilité incombe en dernier ressort à l'autorité.

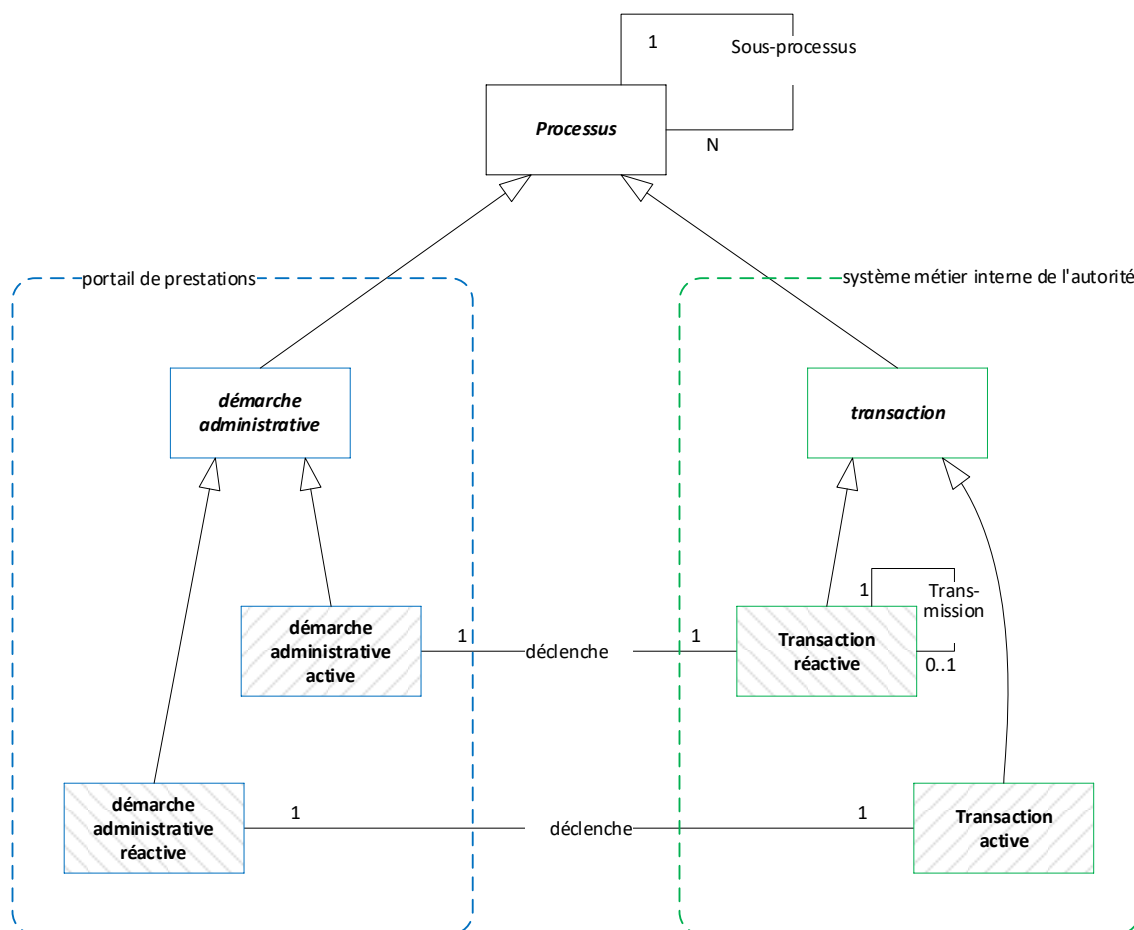


Figure 37: Modèle d'information des processus d'interface "démarche administrative ↔ traitement des transactions"

- La démarche administrative et la transaction peuvent tous deux instancier des sous-processus.
- Selon le côté qui donne le déclenchement initial, on distingue - par rapport à la paire complémentaire que constituent la démarche administrative et la transaction - un processus d'action et un processus de réaction.
- Le cas particulier du transfert de processus (voir la Figure 6 du chapitre 2.1.1) est pris en charge par la relation de référence supplémentaire "transfert" dans le cas de la transaction réactive.

[REQ-33] L'interface prend en charge deux types de messages pour la paire complémentaire que constituent la démarche administrative et la transaction, quel que soit le côté du déclenchement (voir la Figure 38 suivante et la Figure 39 correspondante):

- Message initial
- Message réponse

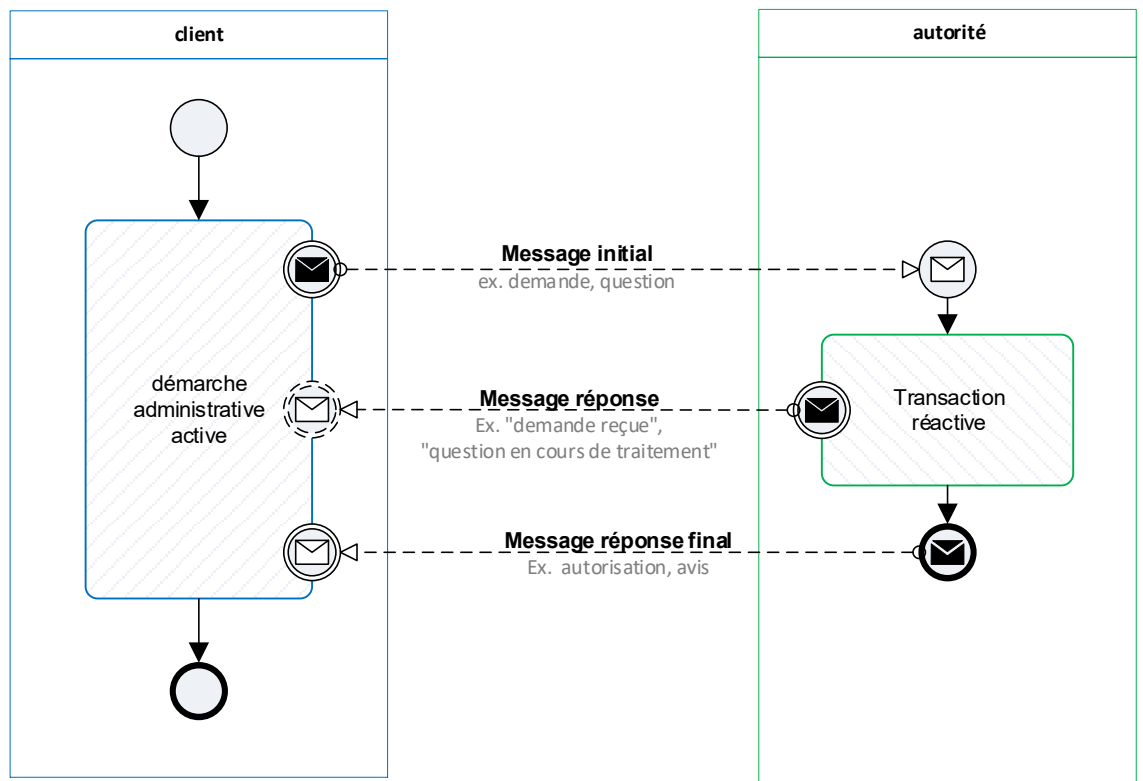


Figure 38: Modèle de processus d'interface "démarche administrative ↔ traitement des transactions" dans le cas "Déclenchement par le client"

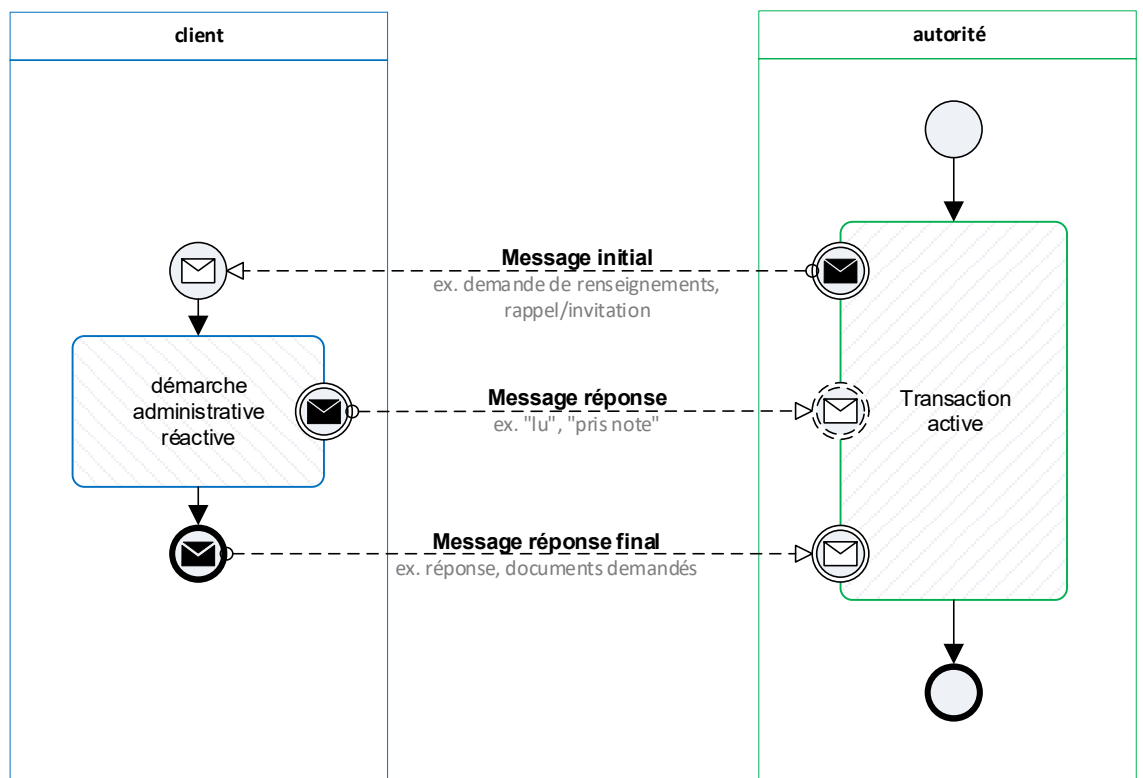


Figure 39: Modèle de processus d'interface "démarche administrative ↔ traitement des transactions" dans le cas "Déclenchement par l'autorité"

Le scénario suivant illustre le cadre logique des exigences formulées ci-dessus [REQ-24] à [REQ-33]:

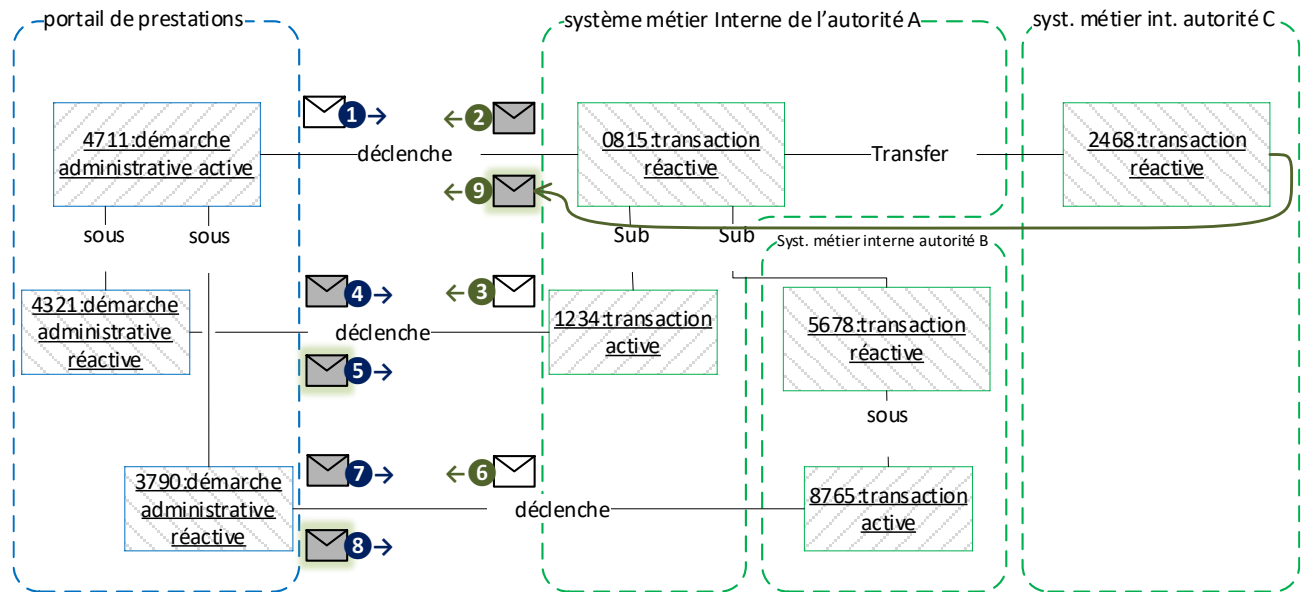


Figure 40: Scénario des processus d'interface entre la démarche administrative et le traitement des transactions conformément aux exigences pertinentes

Dans le portail de prestations, une démarche administrative est effectuée, au cours de laquelle une demande remplie est envoyée par message initial au système métier interne de l'autorité publique A ①. Dans le processus, l'ID de la démarche administrative 4711 est également transmis par le portail. En réponse à la réception du message, le système métier de l'autorité A crée une transaction et lui donne l'ID 0815. Chaque fois que le statut du traitement change, le système de l'autorité A envoie un message réponse du statut au portail ②, qui attribue cette information à la démarche administrative initiale 4711 de l'autorité sur la base des métadonnées fournies et note également l'ID de la transaction complémentaire. Entre-temps, une question se pose à l'autorité, c'est pourquoi une requête de précision est envoyée au client. Cela déclenche un cas de sous-transaction avec l'ID 1234, dans laquelle la requête au client est transmise au portail ③. Le portail associe le message à la démarche administrative originale en utilisant les métadonnées fournies et crée une sous-démarche administrative 4321. Dès qu'un utilisateur autorisé par le client prend connaissance de la requête dans le portail, un message réponse du statut est envoyé à l'autorité A, qui l'affecte à la transaction complémentaire 1234 ④. Enfin, la réponse à la requête est enregistrée du côté du client et envoyée avec un message réponse final (concernant le sous-processus). Le système métier de l'autorité récepteur A l'affecte à son tour à la transaction 1234 ⑤. En outre, un sous-processus de la procédure a lieu auprès de l'autre autorité B, pour laquelle une communication avec le client a lieu dans la même logique ⑥ ⑦ ⑧. Enfin, on suppose que la procédure est transmise à l'autorité C, dont le système métier interne crée par conséquent une transaction avec l'ID 2468 et envoie enfin le message réponse final au portail à la fin de la procédure ⑨.

Pour le scénario décrit, les points d'accès API présentés dans la Figure 41 sont nécessaires.

[REQ-34] Le portail de prestations, en tant que consommateur du traitement des transactions, fournit un point d'accès API pour recevoir des messages de l'autorité.

[REQ-35] En tant que fournisseur du traitement des transactions, le système métier interne de l'autorité fournit un point d'accès API pour recevoir les messages des clients.

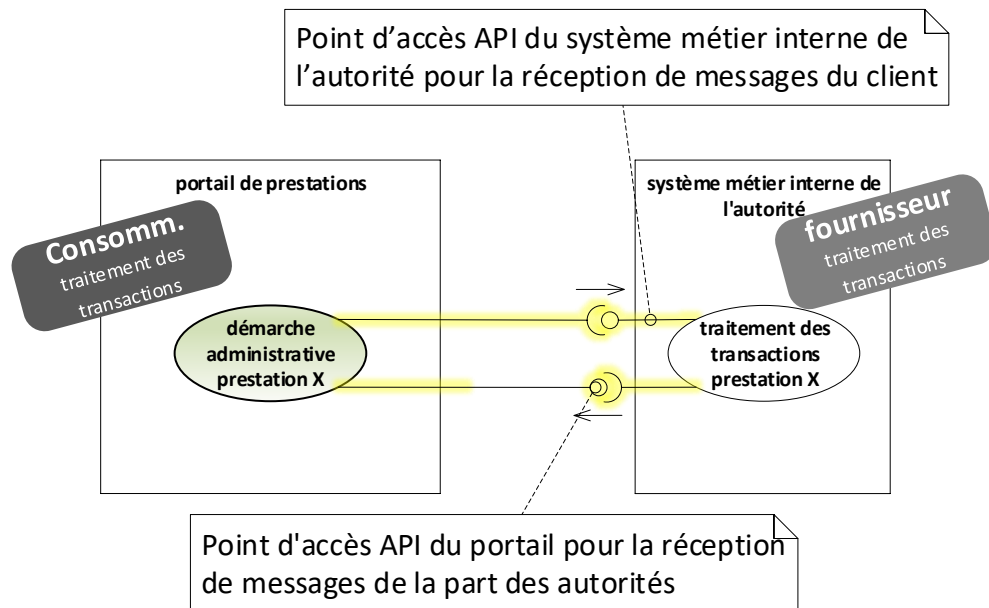


Figure 41: Points d'accès API de l'interface "démarche administrative ↔ traitement des transactions"

En général, les messages entrants dans un compte client peuvent être consultés par les utilisateurs autorisés. Un portail de prestations peut également offrir à l'utilisateur une fonction de notification instantanée (par exemple, via message électronique ou SMS), qui l'informe des nouveaux messages qu'il peut consulter. Toutefois, une telle fonction ne doit pas être réglementée par l'architecture cible d'intégration, mais relève de la responsabilité de l'exploitant du portail concerné (fonction transversale).

Il existe deux options de base pour la mise en œuvre technique de l'interface:

- Système de bus: un service d'infrastructure central tel que Sedex fournit la couche de transport.
- API: L'autorité fournit une API pour les portails.

Les avantages et les inconvénients de ces deux options sont analysés dans [Herausforderung-5], Annexe G.D. En définitive, les deux options permettent de répondre aux exigences d'interface ci-dessus. Dans tous les cas, les exigences de sécurité (voir chapitre 2.5.2) doivent être respectées.

2.5.1.3 Interface pour l'intégration des démarches administratives implémentées en externe

L'interface d'intégration des démarches administratives implémentées en externe est l'élément essentiel du modèle d'intégration 2 (voir chapitre 2.1.6).

[REQ-36] L'interface d'intégration des démarches administratives implémentées en externe comprend - comme l'a déjà montré la Figure 34 au chapitre 2.5.1.1.6 - la redirection du portail consommateur vers le portail fournisseur. Il faut d'abord effectuer le SSO (voir 2.5.1.3.1), puis établir de la même manière le contexte de la démarche administrative sur le portail fournisseur (voir 2.5.1.3.2).

[REQ-37] Lorsqu'il fait des allers-retours (de redirection), l'utilisateur doit rester dans la même fenêtre de navigateur afin de ne pas être conscient du changement de système

physique. Toutefois, des changements perceptibles dans la conception de l'interface utilisateur peuvent être acceptés.

[REQ-38] Lors du retour du portail fournisseur au portail consommateur, l'utilisateur doit arriver dans le même contexte qu'avant le saut.

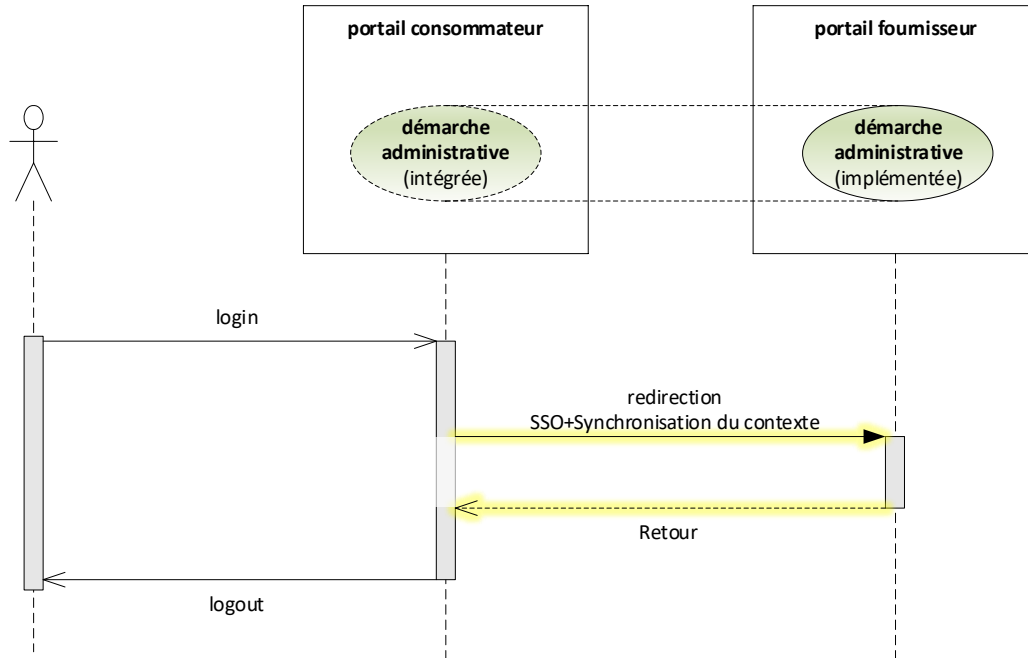


Figure 42: L'intégration d'une démarche administrative implémentée en externe comprend la redirection aller et retour.

2.5.1.3.1 Authentification unique (SSO)

Fondamentalement, il y a deux constellations à considérer:

- A) Service d'identité partagé: les portails consommateur et fournisseur utilisent le même FI/intermédiaire⁷⁴
- B) Confiance entre pairs (P2P trust): les portails consommateur et fournisseur utilisent différents FI/intermédiaires

Le premier cas A) est illustré à la Figure 43 dans le scénario suivant.

Prologue: L'utilisateur se connecte au portail consommateur ❶, qui délègue l'authentification à son fournisseur d'identité⁷⁵ (FI) ❷. En cas d'authentification réussie, le FI émet un *Identity Token*⁷⁶ et le transmet au portail consommateur ❸. Ce dernier vérifie d'abord auprès du FI, au

⁷⁴ Un intermédiaire (tel que eIAM de l'administration fédérale) peut proposer plusieurs FI, voir également le glossaire à l'Annexe A

⁷⁵ Qu'il s'agisse d'un fournisseur d'identité unique ou d'un intermédiaire de plusieurs fournisseurs d'identité n'est pas pertinent pour le scénario.

⁷⁶ Les aspects technologiques (format et support de l'*Identity Token*, type de cryptage, etc.) sont laissés de côté dans la représentation, car ils ne sont pas pertinents d'un point de vue logique.

moyen de la signature, que le *token* provient bien du FI ④. Ce n'est qu'ensuite que le portail consommateur établit une session connectée pour le compte utilisateur avec l'ID local "4711"⁷⁷, qui est attribué à l'ID "1234" transmis dans l'*Identity Token* ⑤. S'il n'y a pas de compte d'utilisateur pour cet ID dans la table de correspondance (*mapping*) pertinente, il sera nouvellement créé et stocké dans la table. Dans tous les cas, l'utilisateur se trouve maintenant dans une session connectée du portail consommateur, dans laquelle il appellera à un moment donné la démarche administrative intégrée depuis le portail fournisseur.

SSO: Lors de redirection, l'*Identity Token* (provenant du FI) est également transmis au portail fournisseur ⑥⁷⁸. Le portail fournisseur établit ensuite une session connectée pour le compte utilisateur (existant ou nouvellement créé in situ) avec l'identifiant local 0815 ⑦ ⑧. Ceci est effectué selon le même modèle tel que pratiqué dans le portail consommateur au cours des étapes ④ et ⑤. L'utilisateur continue à travailler de manière transparente dans sa fenêtre de navigation sur le portail fournisseur et effectue la démarche administrative prévue ⑨.

⁷⁷ Dans l'intérêt de la lisibilité, les valeurs d'identification exemplaires sont courtes.

⁷⁸ Le protocole de transmission n'est pas pertinent. D'un point de vue logique, il importe peu que cela se fasse par le biais de paramètres d'URL ou d'*Identity Token*, par exemple.

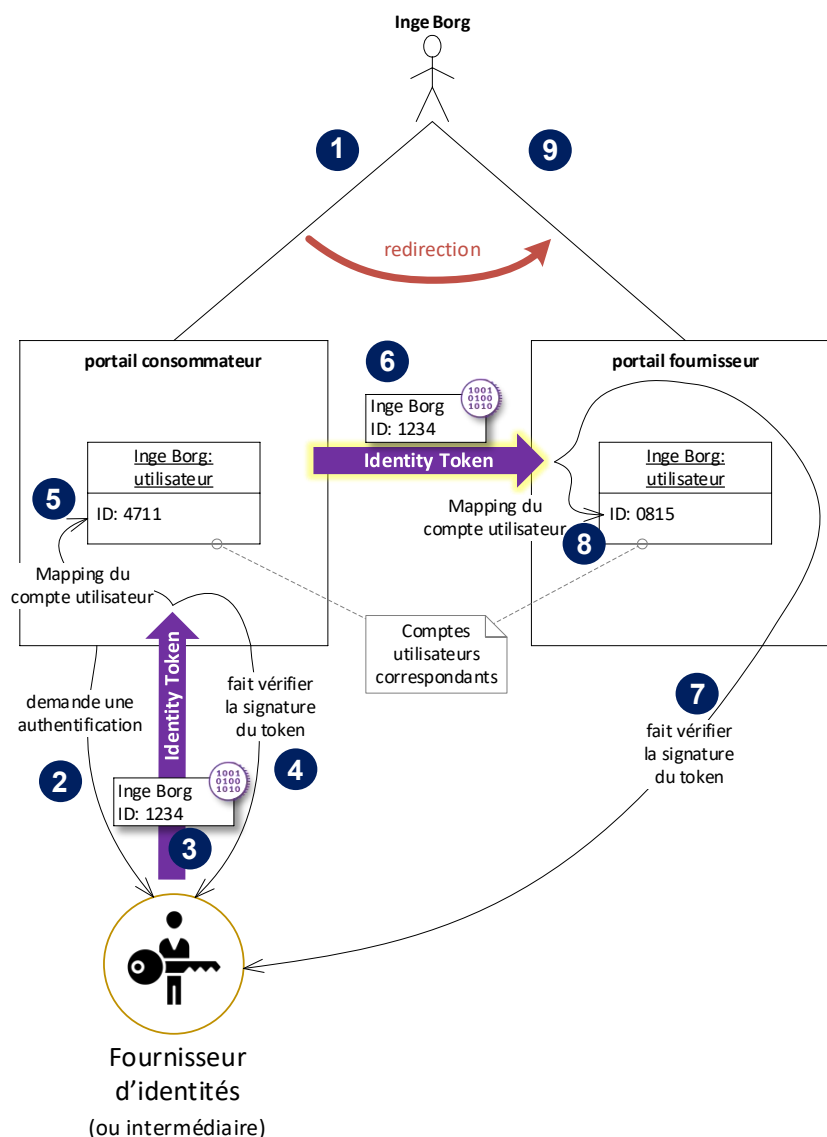


Figure 43: Scénario SSO avec fournisseur d'identité partagé

La Figure 44 montre le retour. Après avoir terminé la démarche administrative sur le portail fournisseur, l'utilisateur retourne à la dernière page du portail consommateur ⑩. Habituellement, l'état du login resp. l'Identity Token est conservé dans un cookie. Sinon, le portail consommateur doit restaurer la session pour le compte utilisateur existant avec l'identifiant local 0815 selon le même schéma que celui pratiqué dans le portail consommateur aux étapes ④ et ⑤. Dans tous les cas, il rétablit l'état initial au moment du saut ⑪ ⑫. L'utilisateur est maintenant de retour dans le portail consommateur, où il peut continuer à gérer le compte client concerné ou effectuer d'autres activités ⑬.

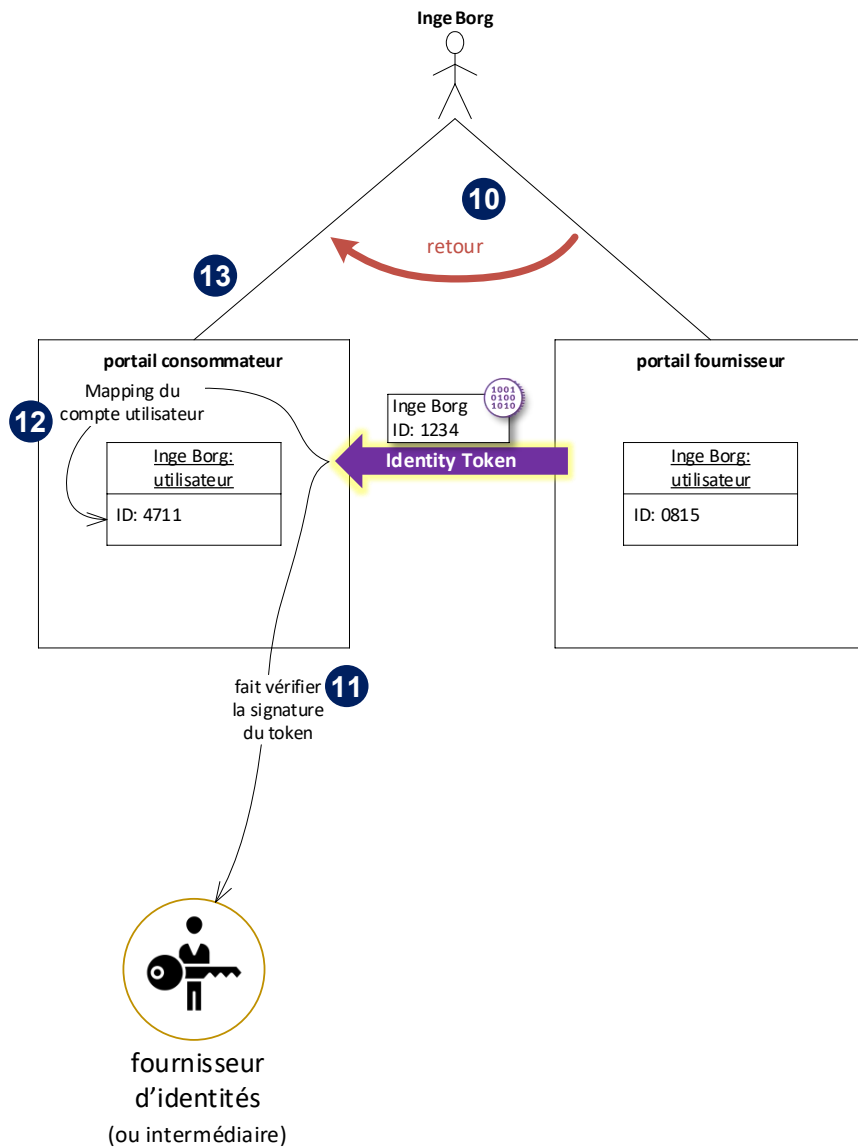


Figure 44: Retour dans un scénario SSO avec FI partagé

Contrairement au premier cas, le deuxième cas B) incarne une approche décentralisée de la confiance entre pairs (P2P trust). La Figure 45 montre un scénario exemplaire:

Tout d'abord, l'utilisateur se trouve sur le portail consommateur. La procédure allant du login à l'appel de la démarche administrative intégrée ①-⑤ est exactement la même que celle décrite dans le prologue ci-dessus pour le premier cas A). Cependant, cela reste caché pour le portail fournisseur et il est également sans importance de savoir avec quel FI le portail consommateur coopère. Lors de la redirection, seul un *Access Token*⁷⁹ est transmis au portail fournisseur ⑥⁷⁸. Cet *Access Token* autorise⁸⁰ le portail fournisseur à demander les informations

⁷⁹ Le terme *Access Token* remonte aux normes OAuth 2.0 et OpenID connect (OIDC)

⁸⁰ L'autorisation peut être limitée dans le temps pour des raisons de sécurité

d'identité au portail consommateur ⑦. Ce dernier fournit un *Introspection*⁸¹ *API Endpoint* correspondant, qui renvoie les informations d'identité souhaitées en réponse (*Response*) à la demande (*Request*) du portail fournisseur. Que les informations d'identité contiennent l'identifiant provenant du FI ou celui du compte utilisateur n'a aucune importance. Il est seulement important que [REQ-16] soit respecté, c'est-à-dire que l'ID identifie de manière unique le compte utilisateur au niveau global. Avec ces informations, le portail fournisseur peut créer une session connectée pour le compte utilisateur (existant ou nouvellement créé in situ) avec l'identifiant local 0815 ⑧. Ceci s'effectue selon le même schéma que celui pratiqué dans le portail consommateur aux étapes ④ et ⑤. L'utilisateur continue à travailler de manière transparente dans sa fenêtre de navigation sur le portail fournisseur et effectue la démarche administrative prévue ⑨.

Après avoir terminé la démarche administrative sur le portail fournisseur, l'utilisateur retourne à la dernière page du portail consommateur. Le retour est similaire au scénario décrit ci-dessus pour le cas A): habituellement, l'état du login resp. le Security Token a été conservé dans un cookie dans le portail consommateur. Dans le cas contraire, le portail consommateur doit restaurer la session selon le même schéma pour le compte utilisateur existant avec l'identifiant local 0815 (tel que pratiqué dans le portail grand public aux étapes ④ et ⑤ de la Figure 45). Dans tous les cas, il rétablit l'état initial au moment du saut.

⁸¹ Le terme *Introspection Endpoint* remonte à la norme OAuth 2.0. La norme eCH-0225 [32] montre également au chapitre 10.3 comment l'*Introspection Endpoint* doit être conçu

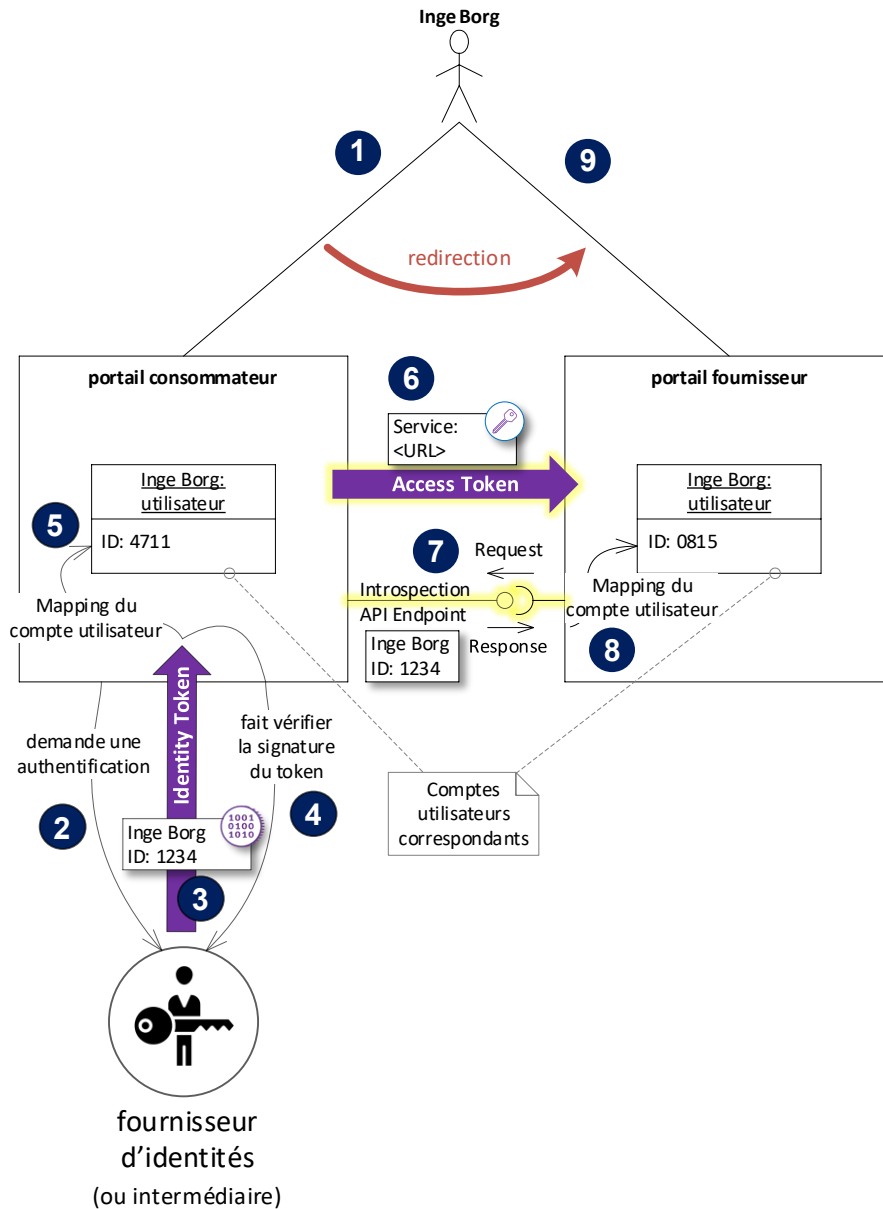


Figure 45: Scénario SSO avec confiance bilatérale entre pairs (P2P trust)

La question de savoir laquelle des deux constellations présentées, A) ou B), doit être privilégiée a fait l'objet de discussions intenses lors des ateliers du groupe d'experts (voir [Herausforderung-3] dans l'Annexe G.D). En conséquence, le modèle décentralisé B) P2P trust a été recommandé, en tenant compte des principes d'architecture [P-4] et [P-7], car il **dissocie** la question du FI de l'interface d'intégration des démarches administratives implémentées en externe. Du point de vue du portail fournisseur, il importe peu de savoir quel(s) FI ou intermédiaire(s) le portail consommateur utilise en coulisse, car cela est entièrement encapsulé par l'interface. De cette façon, le modèle P2P permet la flexibilité nécessaire à l'interopérabilité au-delà des frontières fédérales, ainsi que l'inclusion de fournisseurs d'identité étrangers. L'approche B) P2P trust est donc reprise en conséquence dans la feuille de route de mise en œuvre (voir 2.7.1). L'approche A) peut être utilisée dans des cas exceptionnels si les portails consommateur et fournisseur utilisent de toute façon le même service d'identité (par exemple, les portails basés sur l'eIAM/les applications métiers de la Confédération).

Les deux variantes ont en commun:

[REQ-39] Sur la base de l'identifiant transmis par le portail consommateur pour le compte utilisateur, le compte correspondant est sélectionné dans le portail fournisseur (ou créé in situ s'il n'existe pas encore).

[REQ-40] Au moins les informations suivantes sont transmises du portail consommateur au portail fournisseur: ID du compte utilisateur (voir 2.5.1.1.6.1), paramètres du profil (voir 2.5.1.1.6.2), LoA du login (voir 2.5.1.1.6.3)

[REQ-41] Lors du retour du portail fournisseur vers le portail du consommateur, ce dernier doit rétablir l'état original qui existait immédiatement avant la redirection vers le portail fournisseur. Pour ce faire, le portail consommateur doit enregistrer entre-temps les paramètres contextuels correspondants (par exemple, la page de saut, le choix du client et du service).

Il y a une différence entre les deux variantes en ce qui concerne le compte utilisateur correspondant créé dans le portail fournisseur: dans le cas A) (FI partagé), l'utilisateur peut se connecter directement au portail fournisseur avec ce compte correspondant ; dans le cas B) (P2P trust), cependant, cela n'est pas possible car aucun login n'est attribué au compte utilisateur correspondant.

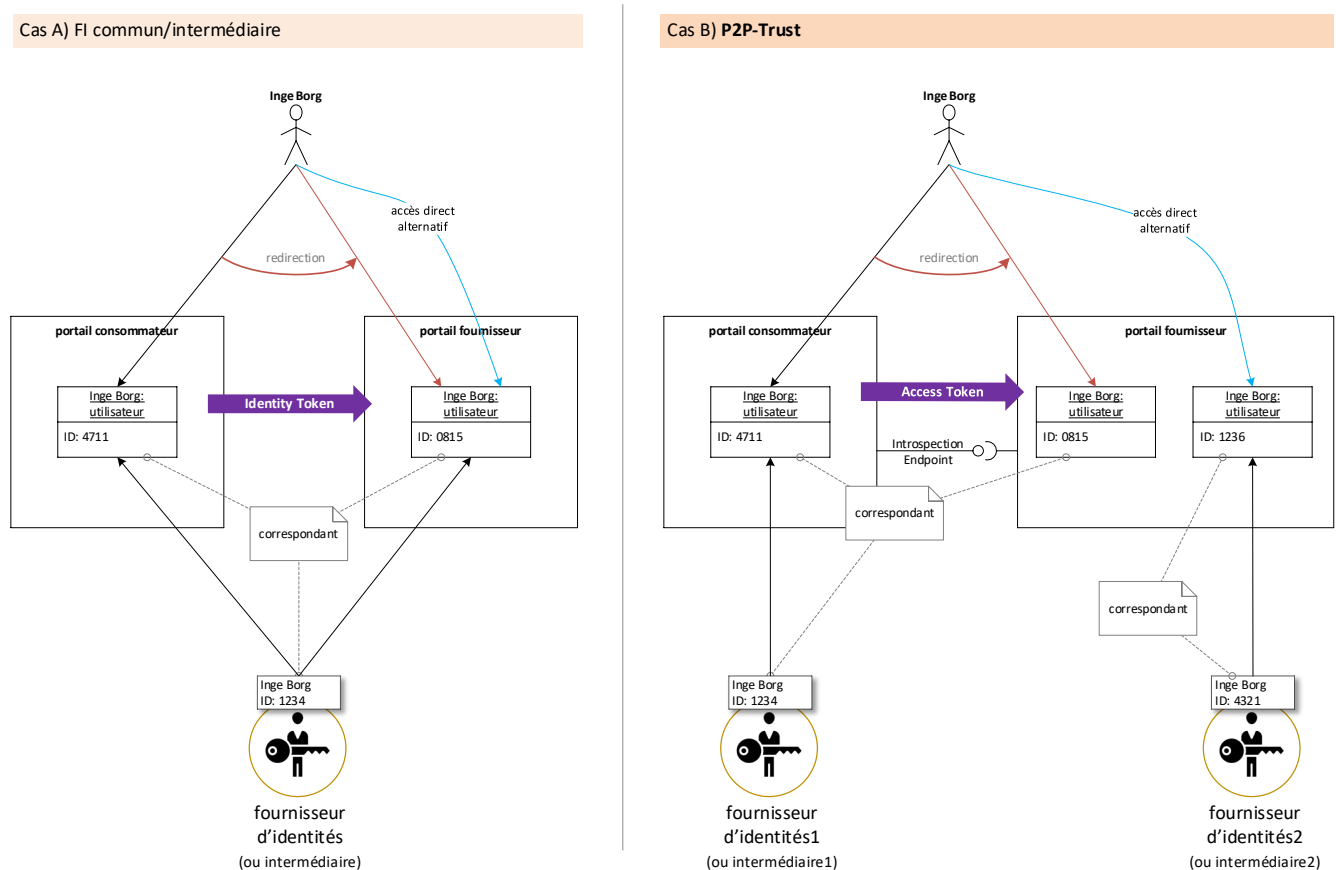


Figure 46: Différence entre les cas A) et B) en ce qui concerne la redirection et l'accès direct alternatif

Le LoA du login est d'une importance particulière. Dans le cas B) (P2P trust), le portail fournisseur doit faire confiance au portail consommateur pour que la valeur transmise corresponde aux faits. Cette question peut être explicitement réglée et vérifiée dans un accord de confiance

mutuel. En outre, il est concevable qu'un organisme de contrôle de l'État certifie les éditeurs de valeurs de LoA (lors du temps de définition). Sur présentation d'un tel certificat, l'accord bilatéral ne serait pas nécessaire. Cette idée est reprise dans la feuille de route de mise en œuvre (voir 2.7.1).

Note: Dans le cas A) (service d'identité partagé), la question de la confiance est également pertinente pour la relation entre le FI/l'intermédiaire et les portails connectés. Toutefois, cela sort du cadre de l'architecture cible d'intégration.

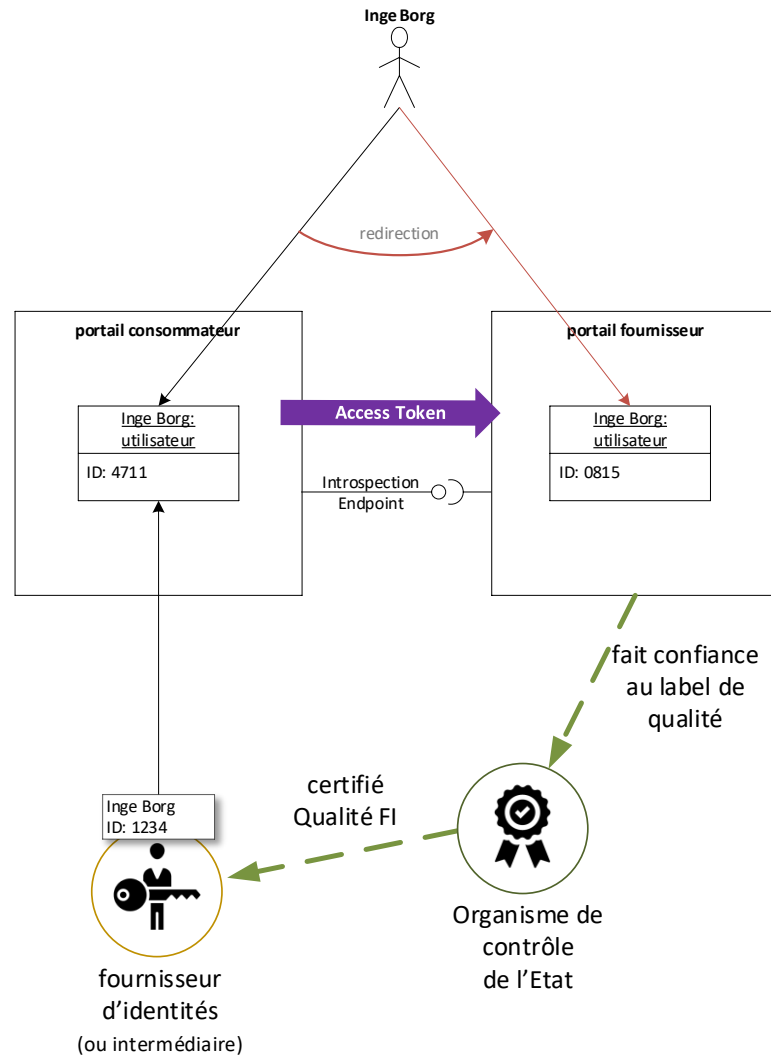


Figure 47: Un organisme de contrôle de l'Etat simplifie la position de confiance par rapport à la LoA du login au moyen d'une certification.

Le LoA du login requis pour une démarche administrative⁸² est défini par l'autorité responsable de la prestation respective.

⁸² Attention, risque de confusion: le LoA du login et le droit de gestion sont des choses différentes. Le premier décrit un niveau de confiance, le second un droit explicitement accordé par le client.

[REQ-42] Le portail fournisseur est chargé de veiller à ce que le LoA du login minimal fixé pour la démarche administrative concernée soit respecté.

Toutefois, afin d'éviter des conflits de conformité inutiles, il est recommandé que le portail consommateur relie déjà l'appel de la démarche administrative intégrée au LoA requis.

2.5.1.3.2 Synchronisation du contexte

Comme déjà expliqué au chapitre 2.5.1.1.6 et illustré à la Figure 34, outre le SSO et le login de l'utilisateur, le contexte de la démarche administrative doit également être synchronisé entre les portails impliqués au moment du saut depuis le portail consommateur vers le portail fournisseur (le contexte consistant en la sélection du client et le droit de gestion associé). À cette fin, les informations nécessaires doivent d'abord être transmises via l'interface lors de la redirection conformément au cadre d'interopérabilité:

[REQ-43] Au moins les informations suivantes sont transmises du portail consommateur au portail fournisseur: prestation administrative (vocabulaire contrôlé selon le chapitre 2.5.1.1.2) auquel la démarche administrative adressée fait référence, ID du client (voir chapitre 2.5.1.1.4) pour lequel la démarche administrative doit être effectuée, droit de gestion (vocabulaire contrôlé selon le chapitre 2.5.1.1.6.4), LoA du droit de gestion (voir [REQ-22] au chapitre 2.5.1.1.6.4). Si une démarche administrative existante a été adressée dans le portail consommateur, son ID (voir [REQ-14] au chapitre 2.5.1.1.5) doit également être transmis.

[REQ-44] En outre, la requête client doit être communiquée, si elle est connue⁷².

[REQ-45] La transmission est effectuée avec les informations SSO décrites dans [REQ-40].

Cela signifie que pour le cas SSO A) (FI partagé) décrit dans le chapitre précédent 2.5.1.3.1, le portail consommateur ajoute les informations mentionnées dans [REQ-43] dans un *Context Token*. Dans le cas du SSO B) (P2P trust), l'*Introspection API Endpoint* fournit le complément du contexte.

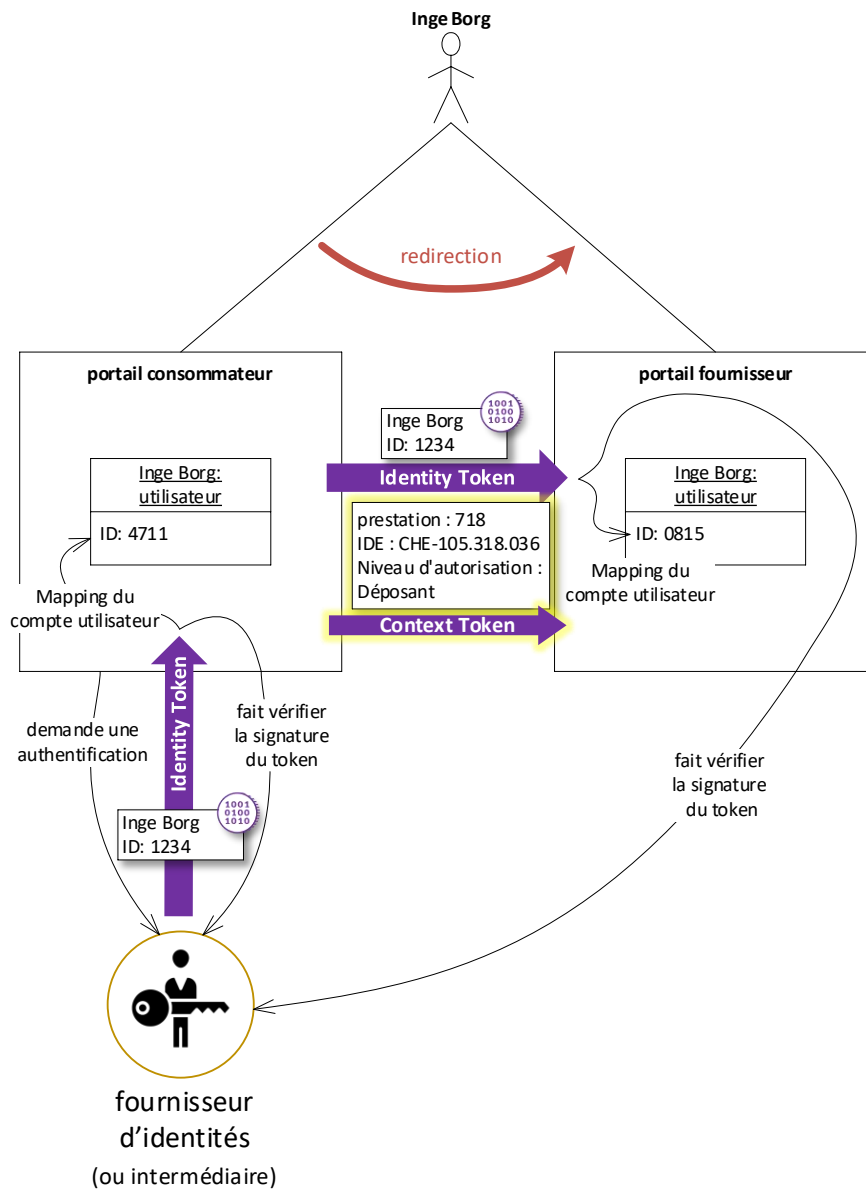


Figure 48: Transmission des informations du contexte dans le cas A) via le *Context Token* en complément du *Identity Token* (comparer avec la Figure 43)

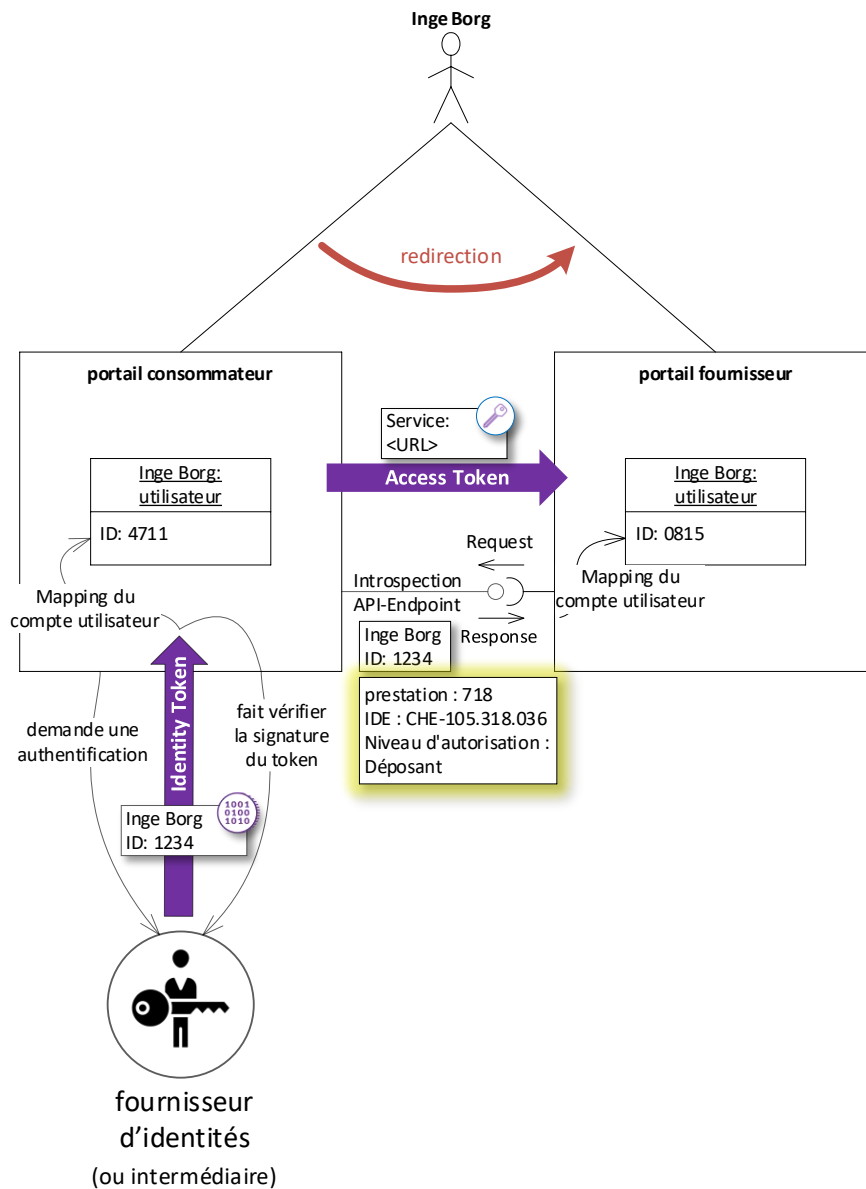


Figure 49: Transmission des informations contextuelles dans le cas B) en tant qu'ajout à la réponse du point de terminaison de l'API d'introspection (comparer la Figure 45)

[REQ-46] Sur la base des informations du contexte transmises, le portail fournisseur établit son contexte comme suit:

- Sélection du compte client adressé. Si celui-ci n'existe pas, il est créé in situ. Dans ce cas, les données de base sont obtenues à partir du registre correspondant (voir 2.5.1.1.4.3).

- Reprise temporaire du niveau d'autorisation transmis de l'utilisateur concerné pour la prestation/le client concernés dans le portail fournisseur pendant la durée de vie de la session⁸³.
- Navigation vers la page de démarrage de la démarche administrative adressée en mettant l'accent sur le compte client adressé ainsi que sur la fonctionnalité correspondant au niveau d'autorisation.

Une condition préalable est que le portail fournisseur fasse confiance aux droits de gestion attribués dans le portail consommateur. La qualité des processus d'attribution et d'autorisation dans le portail consommateur (documenté par le LoA du droit de gestion) doit répondre aux exigences du portail fournisseur.

[REQ-47] Le portail fournisseur doit s'assurer qu'il n'accepte les droits de gestion transmis par le portail consommateur que s'ils ont un certain LoA minimal.

Afin de faciliter les accords de confiance à cet égard, la certification du LoA des droits de gestion par un organisme de contrôle de l'Etat serait envisageable, comme dans le cas du LoA du login (voir les explications dans la dernière partie du chapitre 2.5.1.3.1 ainsi que la Figure 47).

2.5.1.3.3 Déconnexion unique (SLO)

[REQ-48] Dans tout scénario de SSO, le SLO doit être assuré.

Cela signifie que la déconnexion doit avoir lieu à la fois sur le portail consommateur et sur le portail fournisseur. Si, par exemple, l'utilisateur est sur le portail fournisseur et se déconnecte, l'état du login sur le portail consommateur doit également être résilié. Cela s'applique également à l'inverse: si l'utilisateur se déconnecte sur le portail consommateur, toute session initiée via SSO sur le portail fournisseur doit également être terminée. Si l'utilisateur a appelé plusieurs démarches administratives intégrées dans le portail consommateur, toutes les sessions liées sur les portails fournisseur respectifs doivent être terminées.

2.5.1.3.4 Canal de retour pour la démarche administrative (statut, notifications officielles, documents de résultats)

Dans le sens de la revendication de [REQ-37] (voir chapitre 2.5.1.3), suite aux besoins [B-18] et [B-24], toute information sur le statut (à la fois sur la démarche administrative elle-même et sur le traitement des transactions) et les documents de résultats ainsi que d'éventuelles notifications officielles (par exemple, le renouvellement d'un passeport dû) devraient également être visibles pour les démarches administratives intégrées dans le portail consommateur. Ce n'est pas une obligation (l'utilisateur peut consulter les informations sur le portail fournisseur en rappelant la démarche administrative concernée), mais c'est certainement souhaitable du

⁸³ Le droit de gestion ne doit pas être persisté de manière permanente dans le portail fournisseur via l'interface, car sinon des incohérences peuvent apparaître dans la manière dont le droit en question continue d'exister dans le portail fournisseur (après le retrait des droits dans le portail consommateur).

point de vue de l'utilisateur, car cela serait autrement moins pratique que les démarches administratives implémentées.

[REQ-49] Le portail consommateur fournit un *API Endpoint* qui permet au portail fournisseur de transmettre au portail consommateur les messages réponse relatifs à une démarche administrative.

[REQ-50] Les messages réponse comprennent aussi bien des informations sur le statut et des documents de résultats de la démarche administrative ainsi que des notifications proactives de l'autorité au client (par exemple, renouvellement d'un passeport dû).

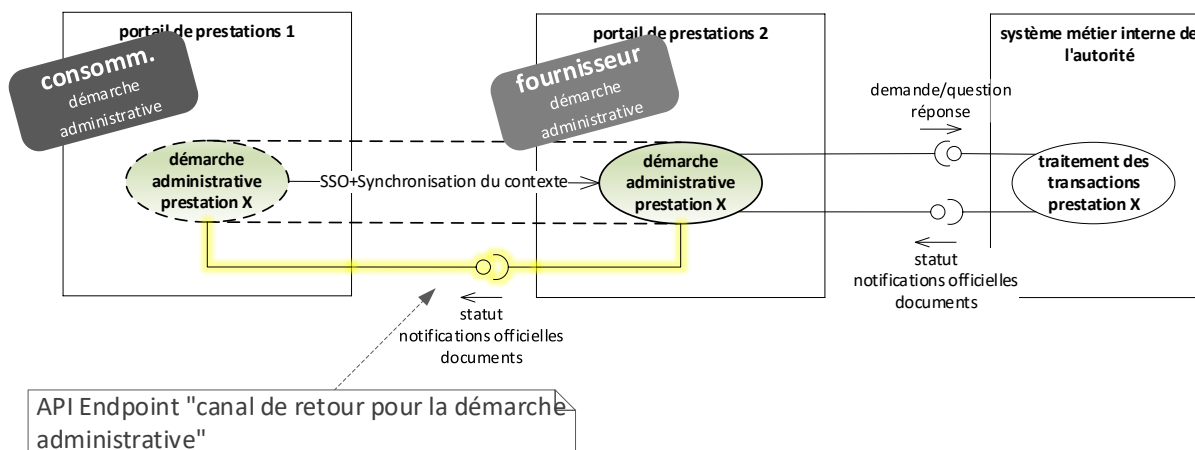


Figure 50: API endpoint pour les messages réponse pour la démarche administrative dans le cadre de l'interface pour l'intégration des démarches administratives implémentées en externe

2.5.1.4 Aperçu du flux de données des interfaces

En résumé, le flux de données des deux interfaces décrites dans les chapitres précédents 2.5.1.2 et 2.5.1.3 est illustré par l'image globale exemplaire présentée à la Figure 51. Celle-ci contient le portail de prestations 1 avec une démarche administrative intégrée par le portail de prestations 2, dont l'implémentation dans le portail de prestations 2 communique via l'interface "démarche administrative ↔ traitement des transactions" avec le système métier interne de l'autorité compétente qui se trouve derrière.

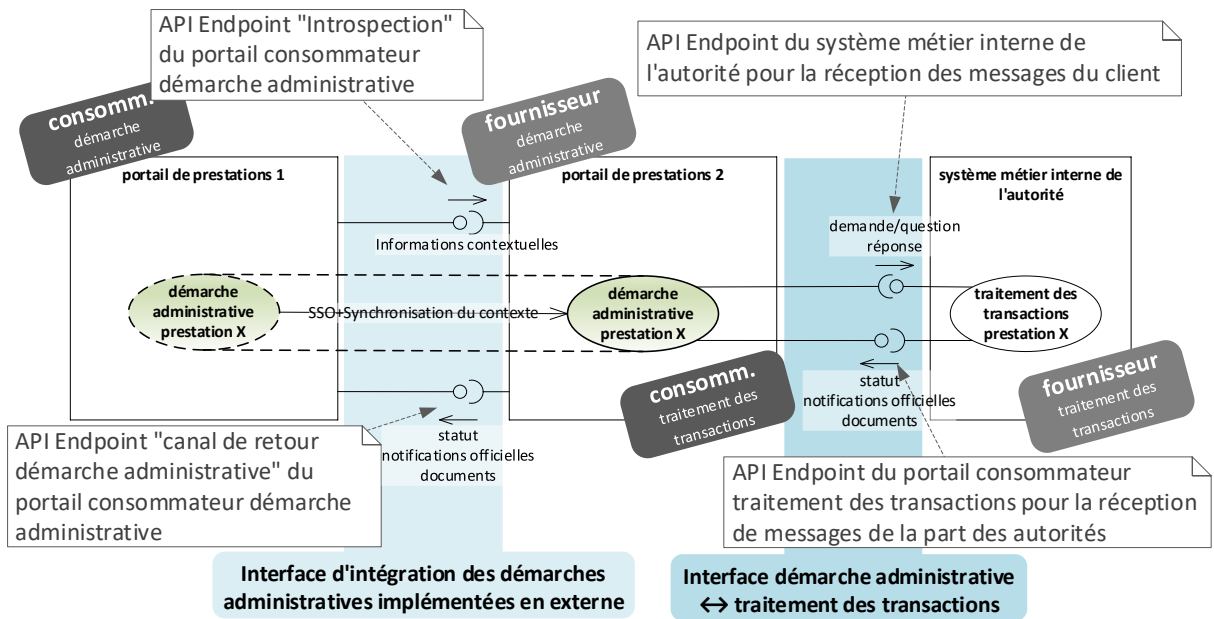


Figure 51: Image globale d'une démarche administrative intégrée avec, derrière, l'interface encapsulée par le portail fournisseur vers le système métier interne de l'autorité.

La Figure 52 montre le flux de données différencié pour les différents domaines du cadre d'interopérabilité, la base interopérable respective étant délimitée de manière schématique. L'illustration montre clairement quelles interfaces transmettent quels domaines. Le diagramme montre également que l'origine du flux de la base interopérable des données de base des clients se trouve dans le registre compétent, qui est interrogé à la fois par le portail de prestations 1 et le portail de prestations 2 (voir le chapitre 2.5.1.1.4.3). Les données obtenues à partir des registres sont donc toujours déterminantes pour les portails de prestations. L'interface entre les deux portails ne transmet que l'identifiant du client.

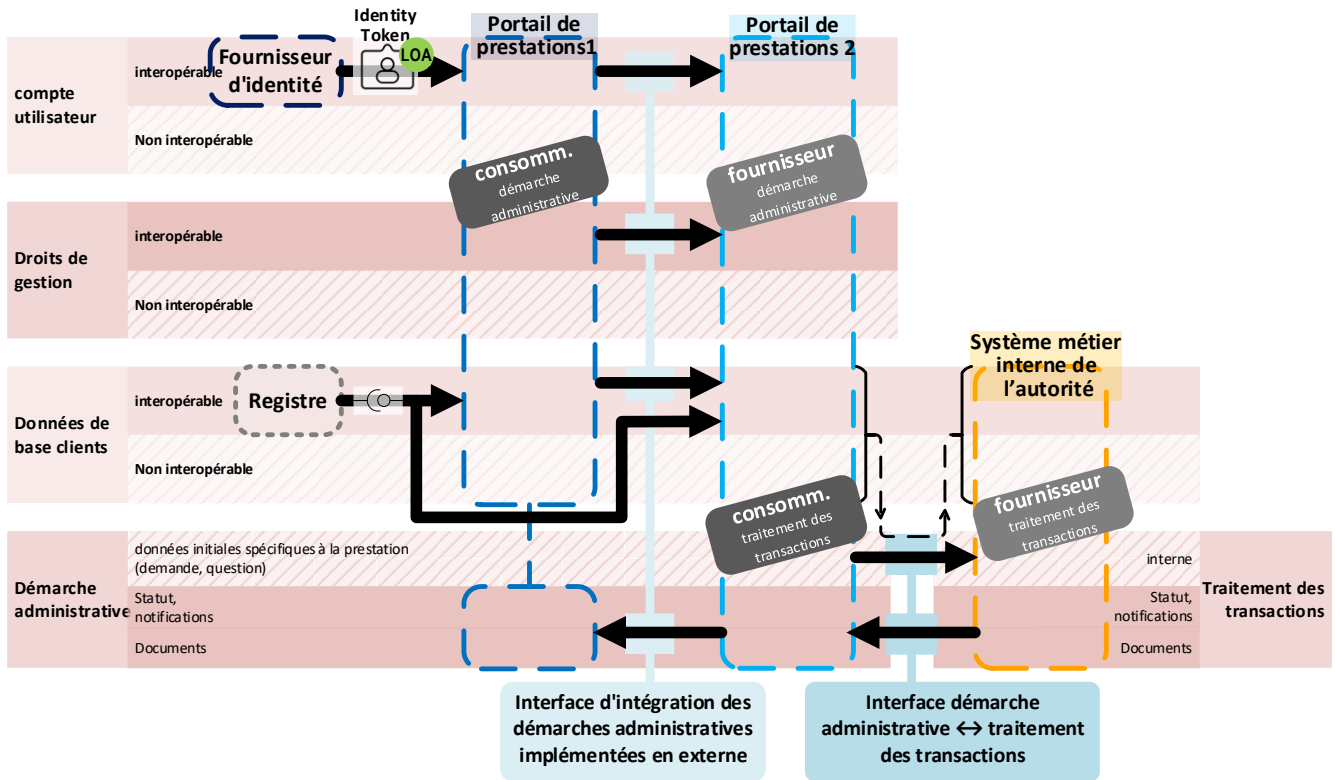


Figure 52: Aperçu du flux de données des interfaces

2.5.1.5 Responsabilité des interfaces

Afin d'éviter des dépendances circulaires (comme le montre la Figure 53), la responsabilité (c'est-à-dire la souveraineté de définition) des interfaces entre deux systèmes doit être dans une seule main.

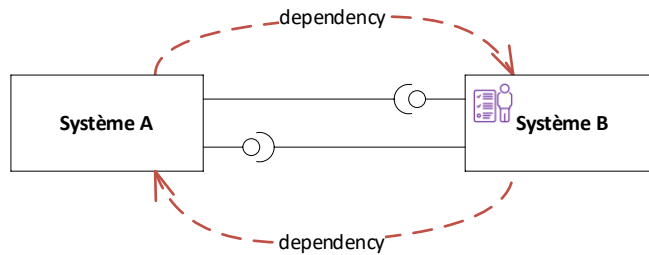


Figure 53: Dépendance circulaire due à la responsabilité distribuée des interfaces

En ce qui concerne les différents *API Endpoints* des interfaces abordées aux chapitres 2.5.1.2 et 2.5.1.3, cela signifie que la responsabilité des *Endpoints* respectifs doit être entièrement attribuée soit au consommateur, soit au fournisseur de la démarche administrative ou du

traitement des transactions⁸⁴. Suite à la discussion au sein du groupe technique, cette question a été tranchée en faveur du fournisseur. Par conséquent, les dispositions suivantes s'appliquent:

[REQ-51] La responsabilité de l'interface "démarche administrative ↔ traitement des transactions" (voir 2.5.1.2) incombe au système métier de l'autorité compétent respectif.

[REQ-52] La responsabilité de l'interface d'intégration des démarches administratives implémentées en externe (voir 2.5.1.3) incombe au portail fournisseur concerné.

En relation avec les normes pertinentes, l'analyse des dépendances est la suivante:

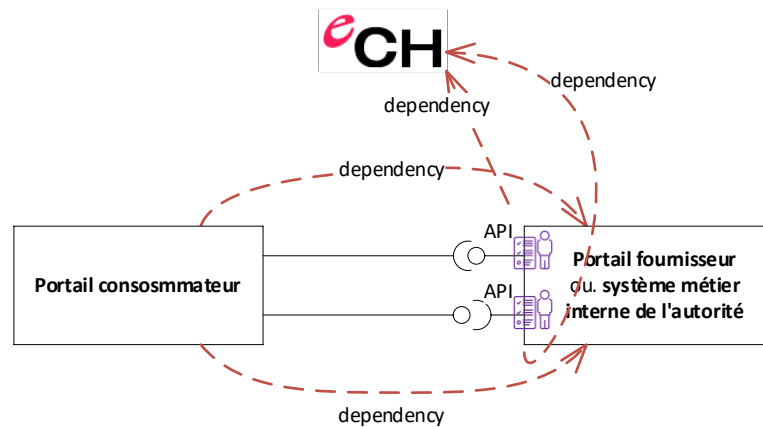


Figure 54: Dépendances claires entre les systèmes grâce à la définition et à la normalisation des responsabilités

Dans le cadre de la responsabilité des interfaces, les choses suivantes, entre autres, doivent être réglementées:

[REQ-53] Lors de la mise en œuvre de l'interface, le traitement des exceptions (*Exception handling*) doit être assuré au niveau technique.⁸⁵

[REQ-54] Lors de la mise en œuvre de l'interface d'intégration des démarches administratives implémentées en externe, il faut tenir compte du "droit à l'oubli" (*Right to forget*). Cela signifie, par exemple, qu'une suppression de compte sur le portail consommateur doit être⁸⁶ suivie dans le portail fournisseur.

Enfin, il convient de se référer au document "API-Architektur Bund" [34], qui systématise, entre autres, les options de conception technique et organisationnelle pour la mise en œuvre d'une

⁸⁴ Le rôle de l'interface (actif/réactif) et la direction du flux de données n'ont pas d'importance.

⁸⁵ À titre d'exemple, il est fait référence à la norme eCH-0090 2.0 [9], qui prévoit cela pour la communication Sedex.

⁸⁶ Ceci s'applique à chaque démarche administrative intégrée. Si, par exemple, le portail consommateur intègre une démarche administrative du portail fournisseur A et une démarche administrative d'un autre portail fournisseur B, alors une suppression de compte sur le portail consommateur doit être suivie dans le portail A ainsi que dans le portail B.

API. L'interface "démarche administrative↔traitement des transactions" (voir 2.5.1.2) représente un cas d'utilisation classique d'une API au sens de l'architecture API fédérale.

2.5.2 Sujets relatifs à la SIPD

Lors de l'intégration d'une prestation administrative par le biais d'un portail de prestations, les informations sont échangées et traitées au-delà des frontières de l'autorité. En fonction des exigences de protection des données échangées et de la prestation fournie par l'autorité, certaines exigences en matière de sûreté de l'information et de protection des données doivent être respectées.

[REQ-55] Le portail de prestations doit veiller à ce que l'utilisateur et les clients qu'il représente bénéficient d'une protection appropriée en matière de TIC lorsqu'ils utilisent une prestation administrative.

2.5.2.1 Identification des besoins de protection

Les besoins de protection dépendent essentiellement de deux facteurs:

- Les prestations administratives intégrées par le portail de prestations et les exigences correspondantes en matière de sûreté de l'information et de protection des données de l'autorité (vue externe) - voir l'excursus à ce sujet au chapitre 2.5.2.2.
- Les données des utilisateurs collectées, traitées et stockées par le portail de prestations lui-même et les fonctions transversales fournies (vue interne) - voir l'excursus à ce sujet au chapitre 2.5.2.3.

[REQ-56] Lors de l'intégration d'une nouvelle prestation administrative (vue externe) et lors de la mise à disposition d'une nouvelle fonction transversale (vue interne), l'exploitant du portail de prestations doit évaluer si des modifications sont apportées aux besoins de protection et mettre en œuvre les mesures nécessaires.

Cela doit se faire selon la procédure de sécurité habituelle en Suisse⁸⁷. La responsabilité de ce processus, ainsi que de la création et de la mise en œuvre d'un éventuel concept SIPD, incombe à l'exploitant du portail de prestations.

[REQ-57] L'exploitant doit également décider s'il veut mettre en œuvre des exigences SIPD individuelles par prestation administrative ou des exigences SIPD d'application générale pour toutes les prestations administratives intégrées.

2.5.2.2 Excursus: Exigences de l'autorité en matière de SIPD

Il est de la responsabilité de l'autorité qui rend une prestation disponible pour l'intégration de définir les conditions pour l'intégration de sa prestation dans un portail (voir l'Annexe F, [Domaine d'intérêt-2], "Konzeption"). Cela inclut également les exigences SIPD pour le portail de prestations (vue externe).

Les exigences en matière de SIPD dépendent notamment des facteurs suivants:

⁸⁷ <https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren.html>

- Type de procédure: par exemple, annonce, demande, enregistrement, déclaration, autorisation
- Données à échanger et à traiter: par exemple, données personnelles, données accessibles au public.
- Criticité de la prestations administratives en termes de disponibilité

L'autorité peut avoir des exigences en matière de SIPD différentes par modèle d'intégration. Le tableau suivant donne une estimation approximative de la nécessité d'augmenter les exigences par modèle d'intégration.

Tableau 19: Évaluation des facteurs de risque en matière de SIPD en fonction du modèle d'intégration

Facteur de risque	Évaluation et exigences
Confidentialité	<p>Du point de vue de la confidentialité, <i>l'intégration</i> est préférable à <i>l'implémentation</i>.</p> <p>Dans le cas de <i>l'intégration</i>, le portail consommateur ne fait que mettre les données nécessaires sur les utilisateurs et les clients à la disposition du portail fournisseur, où se déroule ensuite la démarche administrative. Inversement, le portail fournisseur ne peut renvoyer que des métadonnées sur la démarche administrative, par exemple le statut de la démarche administrative.</p> <p>Dans le cas de <i>l'implémentation</i>, le portail consommateur doit recevoir toutes les données pertinentes du système métier interne de l'autorité, qui sont générées pendant l'exécution de la démarche administrative (par exemple, des documents). Par conséquent, des exigences de protection accrues doivent être appliquées si des données personnelles particulièrement sensibles sont transmises. Les mesures possibles sont le cryptage du canal de transport ou des données, une augmentation de LoA.</p> <p>Lors de la détermination des exigences en matière de confidentialité, il faut également tenir compte des différentes réglementations possibles en matière de protection des données.</p>
Disponibilité	<p>Du point de vue de la disponibilité, <i>l'implémentation</i> est préférable à <i>l'intégration</i>.</p> <p>Dans les deux cas, en cas de défaillance du portail utilisé par l'utilisateur, la transaction peut toujours être traitée par l'autorité ou par le système métier interne de l'autorité.</p> <p>Dans le cas de <i>l'intégration</i>, la disponibilité doit être évaluée comme plus faible car les portails consommateur et fournisseur peuvent tous deux tomber en panne.</p>
Intégrité	<p>Dans les deux cas (<i>intégration</i> et <i>implémentation</i>), l'authenticité, l'exactitude et l'intégrité des données échangées doivent être garanties.</p> <p>Étant donné que des documents sont généralement aussi échangés dans le cas de <i>l'implémentation</i>, les effets de la non-intégrité des données peuvent être évalués comme plus graves. Ainsi, des mesures accrues</p>

	doivent être prises pour protéger l'intégrité des données en cas de l'implémentation.
Traçabilité	Dans les deux cas, il doit être possible de prouver les opérations de travail dans le portail. Les exigences de traçabilité ne diffèrent pas en fonction du modèle d'intégration.

Le modèle d'intégration le plus approprié en matière de SIPD dépend de la pondération des facteurs de risque. Une recommandation générale ne peut être faite.

2.5.2.3 Excursus: Exigences en matière de SIPD pour le portail de prestations

Indépendamment des prestations administratives intégrées, le portail de prestations doit remplir certaines exigences SIPD généralement applicables (vue interne). Dans le chapitre 2.2.2.8, les besoins en matière de SIPD identifiés dans le cadre de cette étude ont été décrits. Ces besoins sont complétés par d'autres exigences.

Tableau 20: Exigences en matière de SIPD

Exigence	Description
Garantie SIPD	La sûreté de l'information et la protection des données doivent être garanties.
Transparence concernant l'utilisation des données	Le client doit pouvoir savoir où se trouvent ses données et quelles autorités y accèdent et à quelles fins. La suppression des données doit également être garantie conformément aux dispositions légales.
Disponibilité de l'ensemble du système	Le portail de prestations doit être en mesure de respecter les objectifs de disponibilité (SLA). Dans le cas du modèle d'intégration 2 (intégration), cela s'applique aux portails fournisseur et consommateur.
Une vision holistique de la sûreté	La sûreté ne doit pas seulement être considérée en termes de technologie/systèmes, mais aussi en termes de processus lui-même, dans sa représentation à travers la totalité des systèmes (par exemple, que se passe-t-il après une défaillance d'un système?).
Prendre en compte la législation sur la protection des données (LPD)	L'échange de données dans le domaine de la cyberadministration doit fondamentalement respecter la législation applicable en matière de protection des données. L'obligation de préserver le secret de fonction (art. 320 CP et art. 22 al. 1 de la Loi sur le personnel de la Confédération) peut également être liée à la sûreté de l'information. En fonction des prestations offertes, d'autres secrets peuvent également être touchés. Il convient de tenir compte des différentes réglementations en matière de protection des données selon le canton (conformité).
N'utiliser que les données personnelles requises	Seules les données à caractère personnel nécessaires à l'accomplissement de la démarche administrative doivent être échangées et conservées.

Aucune atténuation LoA	Le niveau de confiance (LoA) requis par la démarche administrative intégrée (en cas d'intégration) ou par la transaction (en cas d'implémentation) ne doit pas être affaibli par le portail consommateur.
Traçabilité des changements	Des précautions doivent être prises pour que les données ne puissent être consultées et modifiées que par des personnes autorisées avant, pendant et après la transmission. Des outils tels qu' <i>Audit-trail</i> doivent être utilisés pour garantir la traçabilité des modifications.
Sécurité juridique et caractère contraignant	L'échange d'informations entre l'autorité et le client doit être juridiquement sûr et contraignant. Cela se fait généralement par le biais du cryptage et de la signature.

Ces exigences doivent être prises en compte dans la normalisation (voir 2.5.1).

2.5.3 Questions légales

Un portail de prestations n'a pas besoin d'une base légale spécifique pour intégrer une prestation administrative, car il s'agit uniquement d'un système de transmission vers l'autorité effectivement responsable. Le portail ne modifie pas le traitement des transactions ni leurs responsabilités. Les bases légales spécifiques au sujet sont appliquées par l'autorité compétente respective.

Toutefois, le portail de prestations doit indiquer de manière transparente à l'utilisateur que, pour des raisons techniques, le transfert de certaines données (notamment les données d'identification de l'utilisateur) à l'autorité responsable est nécessaire pour bénéficier des prestations. Cela doit être explicitement communiqué dans les conditions d'utilisation du portail de prestations.

2.5.4 Gouvernance informatique

Jusqu'à présent, dans cette étude, nous nous sommes concentrés sur le développement de l'architecture cible d'intégration pour les portails de prestations. Dans ce chapitre, nous nous concentrons sur la gestion ou l'administration des ressources liées à l'architecture cible d'intégration: la gouvernance informatique.

2.5.4.1 Gouvernance informatique dans le contexte de l'architecture cible d'intégration

La gouvernance informatique, dans le contexte de l'architecture cible d'intégration, régit la gestion des ressources (personnel, processus, infrastructure, informations) qui sont liées aux composants intersystèmes et sont pertinentes pour l'interopérabilité (selon les sujets de normalisation 2.5.1.1 à 2.5.1.3). Cela inclut également l'architecture cible d'intégration, qui doit être développée en fonction des besoins.

[REQ-58] L'Administration numérique suisse (ANS) ou une institution à déterminer disposant des compétences nécessaires doit assumer la responsabilité globale de la gouvernance informatique et la responsabilité de l'orientation stratégique (selon l'Annexe F, [Fokusbereich-1]). L'ANS peut déléguer la responsabilité d'autres domaines de la gouvernance informatique et du respect des exigences correspondantes à des partenaires ou autorités appropriés.

[REQ-59] Dans le cadre des travaux de normalisation, il convient de préciser les exigences en matière de gouvernance informatique et de définir des responsabilités claires pour les sous-domaines.

2.5.4.2 Exigences en matière de gouvernance informatique

Pour déduire les exigences de la gouvernance informatique, nous nous référons aux 5 domaines d'intérêt de la gouvernance informatique:

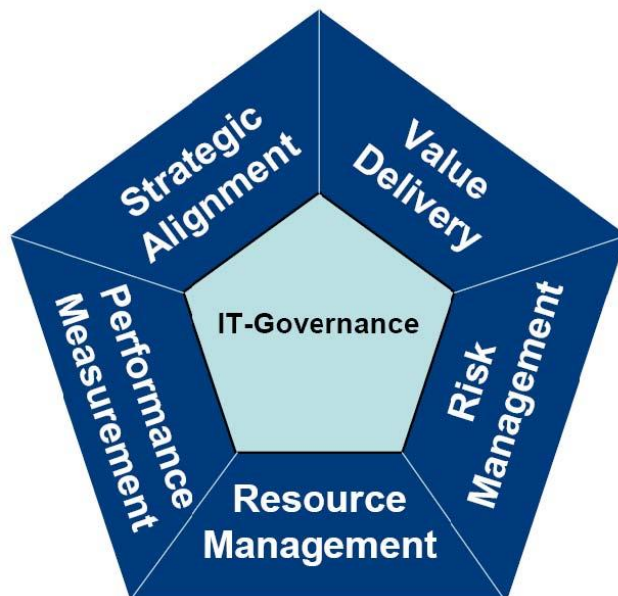


Figure 55: Domaines d'intérêt de la gouvernance informatique

Dans le contexte de la cyberadministration, nous définissons les domaines d'intérêt comme suit:

- [Domaine d'intérêt-1]** *Strategic Alignment*: veiller à ce que la stratégie de la cyberadministration soit prise en compte et que les principes de cyberadministration, les normes eCH et les bases légales soient appliqués.
- [Domaine d'intérêt-2]** *Value Delivery*: assurer la continuité des prestations avec un niveau élevé de rentabilité sur l'ensemble du cycle de vie, y compris le développement de l'architecture cible d'intégration.
- [Domaine d'intérêt-3]** *Risk Management*: assurer la sensibilisation aux risques, l'identification, la mesure, l'évaluation, la surveillance et la minimisation, promouvoir la prévention des erreurs.
- [Domaine d'intérêt-4]** *Resource Management*: utilisation responsable des fonds publics afin d'utiliser les ressources (personnel, processus, infrastructures, informations) de la manière la plus efficace possible. Une réglementation claire des responsabilités (RACI) au sein des différentes organisations.
- [Domaine d'intérêt-5]** *Performance Measurement*: suivi et contrôle de la fourniture des prestations tout au long du cycle de vie.

Dans l'Annexe F, les exigences sont formulées pour les 5 domaines d'intérêt (Allemand: Fokusbereiche).

2.6 Couverture des besoins

Le tableau suivant permet de contrôler et de suivre la mise en œuvre des besoins à travers l'architecture cible d'intégration.

Tableau 21: Traitement et mise en œuvre des besoins du chapitre 2.2.2 dans le développement de l'image cible au chapitre 2.4 et de l'architecture cible au chapitre 2.5

No	Titre	Traitement/mise en œuvre
[B-1]	Interopérabilité des systèmes	Les modèles d'intégration 1 (implémentation) et 2 (intégration) décrits au chapitre 2.1.6 permettent l'intégration de prestations administratives sur différentes plateformes de portail.
[B-2]	Interopérabilité des données (échange standardisé de données)	Le cadre d'interopérabilité (voir 2.5.1.1, en particulier 2.5.1.1.5) constitue la base de l'échange standardisé de données entre les portails de prestations et les systèmes métier internes des autorités (A2B et A2C).
[B-3]	Offrir des services de base (infrastructure cyberadministration)	L'architecture cible postule que les FI et les registres administrés publiquement (registre IDE, registre UPI et SNA) sont des services de base. Voir en particulier [REQ-6]-[REQ-12], [REQ-39]-[REQ-40]
[B-4]	Répertoire de métadonnées (répertoire central des prestations administratives, y compris les spécifications d'intégration)	[[REQ-4] est basé sur l'inventaire des prestations administratives conformément à la norme eCH-0070 [27]. L'interface "démarche administrative↔traitement des transactions" spécifiée au chapitre 2.5.1.2 constitue la base pour offrir une prestation administrative sous la forme d'une API. L'architecture cible ne prévoit pas de répertoire central d'API, car cela fait déjà l'objet de l'OMO14.
[B-5]	Intégration des systèmes existants sans impact sur d'autres systèmes	La responsabilité de l'interface du côté du fournisseur définie au chapitre 2.5.1.5 crée des dépendances clairement dirigées entre les systèmes impliqués et empêche ainsi les effets secondaires incontrôlables.
[B-6]	Authentification unique (pour plusieurs prestations administratives, éventuellement via différents systèmes / plusieurs clients PP/PM)	Le cadre d'interopérabilité (voir 2.5.1.1) constitue la base du SSO requis en ce qui concerne les comptes clients multiples, notamment par le biais du modèle d'information. Cela facilite le SSO spécifié au chapitre 2.5.1.3.1. Voir également [REQ-1], [REQ-2], [REQ-16], [REQ-39]
[B-7]	Identités multiples utilisables	Ceci est indiqué si le portail concerné utilise un intermédiaire (relève de la responsabilité de l'exploitant de portail concerné). Pour le cadre d'interopérabilité (voir 2.5.1.1), il importe peu que ce soit le cas ou non.

No	Titre	Traitement/mise en œuvre
[B-8]	LoA différencié (pas plus que nécessaire pour la prestation administrative)	Voir [REQ-19], [REQ-42]
[B-9]	Signature électronique (via LoA ou explicite)	Signature liée à un LoA du login (minimal): voir [REQ-19], [REQ-42] Explicite ⁸⁸ : la signature est liée au(x) document(s) ou enregistrement(s) électronique(s) à signer.
[B-10]	Gérer soi-même les droits de gestion (client)	Soutenu par [REQ-20], [REQ-21], [REQ-22]. L'architecture cible d'intégration suppose une administration décentralisée des droits de gestion. C'est-à-dire qu'ils sont attribués localement dans le portail concerné. Dans le cas de la synchronisation du contexte (voir chapitre 2.5.1.3.2), le droit de gestion correspondant est temporairement transmis du consommateur au fournisseur.
[B-11]	Procuration standardisée	Voir [REQ-23]
[B-12]	Contact facile avec l'autorité	Supporté par la définition de l'interface "démarche administrative↔traitement des transactions" (voir chapitre 2.5.1.2), voir notamment [REQ-24] et la Figure 37
[B-13]	Communication sécurisée et juridiquement contraignante entre l'autorité et le client	Cet aspect est examiné au chapitre 2.5.2.3 (SIPD). Concerne principalement le trafic de données via l'interface "démarche administrative↔traitement des transactions" (voir chapitre 2.5.1.2)
[B-14]	Personnaliser la vue sur les prestations administratives	La fonctionnalité à cet égard est spécifique au portail et relève de la responsabilité de l'exploitant du portail concerné. Dans le cas du modèle d'intégration 2 (intégration), la portabilité des principaux paramètres de l'utilisateur est prise en charge par le cadre d'interopérabilité - en particulier [REQ-17], [REQ-18].
[B-15]	Aide à la variété des prestations administratives (+ vocabulaire uniforme pour toutes les prestations)	Cet aspect a été analysé dans Annexe G.D, [Herausforderung-6]. La mise en œuvre de ce besoin relève de la responsabilité des OMO6 et OMO7.
[B-16]	Prestations administratives accessibles à partir d'un seul point d'entrée	Les modèles d'intégration 1 et 2 resp. les sujets de normalisation (voir le chapitre 2.5.1) constituent la base de la création de portails inter-autorités axés sur des segments de clients spécifiques.

⁸⁸ Cette partie du besoin vise un aspect hors du périmètre de l'étude.

No	Titre	Traitement/mise en œuvre
[B-17]	Once-Only	Garanti pour la base des données interopérable des entités inter-prestations (voir [REQ-3] et la Figure 33), mais pas au-delà.
[B-18]	Transparence du traitement des transactions	Est supporté par le cadre d'interopérabilité concernant les métadonnées de processus (voir chapitre 2.5.1.1.5) des interfaces spécifiées (voir chapitre 2.5.1.2 et 2.5.1.3), spécifiquement par les informations de statut transmises.
[B-19]	Les transactions classiques peuvent également être suivies	Supporté par l'interface "démarche administrative ↔ traitement des transactions" (voir chapitre 2.5.1.2), spécifiquement [REQ-30].
[B-20]	Traitement des transactions sans rupture de médias	Supporté par l'interface "démarche administrative ↔ traitement des transactions" (voir chapitre 2.5.1.2), notamment [REQ-24].
[B-21]	Processus guidé (transactions aussi uniformes que possible dans toute la Suisse)	Exclusion: Les aspects métiers tels que le désir d'une gestion uniforme des processus dans toute la Suisse concerne la conception d'une démarche administrative. Cependant, cela relève du domaine de responsabilité d'un portail de prestations individuel, qui est en dehors du périmètre de l'architecture cible d'intégration. Indépendamment de cela, le modèle d'intégration 2 (intégration) (voir chapitre 2.1.6) permet de réutiliser l'implémentation existante d'une démarche administrative, ce qui répond au besoin d'uniformité.
[B-22]	Offre pour les entreprises sans IDE	Ce besoin est déjà couvert par les possibilités existantes du registre IDE. Toutes les entreprises existantes en reçoivent un tel identifiant automatiquement (entreprises inscrites au registre du commerce) ou peuvent en demander un (entreprises étrangères), voir chapitre 2.5.1.1.4.1.
[B-23]	L'autorité conserve le contrôle de ses prestations	Ce principe est respecté en réglementant la responsabilité des interfaces (voir chapitre 2.5.1.5) au niveau de l'architecture cible d'intégration.
[B-24]	Identification proactive des besoins des clients par le biais du portail de prestations	Une distinction doit être faite ici: A) Un événement externe déclenche une requête client dans le contexte duquel le client veut/doit utiliser une prestation administrative. B) Un événement externe déclenche une action proactive de l'autorité, qui comprend l'information/la demande/... à des clients spécifiques. Le cas A est principalement à répertorier dans la couche d'information. La requête client en question

No	Titre	Traitement/mise en œuvre
		est prise en compte dans le cadre d'interopérabilité (voir 2.5.1.1.3) et communiquée via les interfaces (voir [REQ-26] et [REQ-44]). Le cas B est pris en charge par la définition de l'interface "démarche administrative↔traitement des transactions" (voir chapitre 2.5.1.2), voir notamment la Figure 37.
[B-25]	Garantie SIPD	Traité au chapitre 2.5.2, qui spécifie les exigences nécessaires.
[B-26]	Transparence concernant l'utilisation des données	Ce sujet relève de la compétence de l'OMO13 (voir [19]) et n'est donc pas traité plus avant dans l'étude.
[B-27]	Disponibilité de l'ensemble du système	Traité au chapitre 2.5.2.3, qui spécifie les exigences nécessaires.
[B-28]	Efficacité économique	Les sujets de normalisation spécifiés (voir 2.5.1) simplifient la complexité de la représentation des prestations administratives sur les portails et contribuent ainsi à une plus grande efficacité économique.
[B-29]	Qualité du développement futur	Les sujets de normalisation spécifiés (voir 2.5.1) simplifient la complexité de la représentation des prestations administratives sur les portails et contribuent ainsi à une meilleure qualité du développement futur. En outre, la gouvernance nécessaire est décrite au chapitre 2.5.4.

2.7 Recommandations pour la suite des opérations

L'architecture cible d'intégration pour les portails de prestations développée dans cette étude doit être mise en œuvre étape par étape. La feuille de route de mise en œuvre suivante montre une voie possible à cet égard.

2.7.1 Feuille de route pour la mise en œuvre

La mise en œuvre de la normalisation de l'interopérabilité des portails de prestations se fera par étapes.

Principes de la feuille de route

- Les étapes s'appuient les unes sur les autres et doivent avoir une taille raisonnable afin que les normes initiales et la mise en œuvre basée sur celles-ci puissent être disponibles rapidement.
- La normalisation de la synchronisation du contexte dans le modèle d'intégration 2 (intégration) doit être réalisée en 4 étapes selon l'ordre de priorité suivant:
 1. Compte utilisateur (identification de l'utilisateur, profil utilisateur, LoA) et identification du client
 2. Droit de gestion

3. Canal de retour pour le statut de la démarche administrative et les notifications officielles
4. Canal de retour pour les documents

La normalisation des interfaces pour le modèle d'intégration 1 (implémentation) peut se faire en parallèle avec les étapes 1 et 2. Dans les deux cas, la normalisation doit se baser sur les normes eCH existantes dans la mesure du possible.

- L'accès aux registres n'est pas abordé dans la feuille de route, car les interfaces correspondantes existent déjà (p. ex. UPI, IDE) ou sont en cours de développement (p. ex. SNA).
- Le SECO a été chargé de créer l'architecture cible d'intégration et de réaliser cette étude. L'ANS est chargée d'élaborer les normes requises et de les mettre en œuvre en coordination avec les autorités et d'autres partenaires.

Architecture d'interfaces pour l'approche "confiance entre pairs" (P2P trust)

Dans un premier temps, une approche de confiance entre pairs (P2P trust) doit être envisagée pour la synchronisation du contexte entre les portails consommateur et fournisseur. Dans le même temps, une relation de confiance bilatérale doit être créée entre les partenaires d'intégration sur la base d'un accord uniforme dans toute la Suisse. Les avantages de cette approche sont une mise en œuvre simplifiée avec un degré de liberté relativement élevé de la part des portails et des risques relativement faibles, car il est possible de s'appuyer sur des implémentations existantes pour la plupart.

Étapes d'extension possibles

Après la mise en œuvre des 4 étapes de normalisation mentionnées et d'autres décisions nécessaires concernant le contenu, d'autres étapes d'extension pourraient par exemple être envisagées. L'objectif d'une première étape d'extension peut être l'élimination des accords bilatéraux par l'introduction d'un organisme de contrôle de l'État pour la certification des émetteurs d'identités numériques et de droits de gestion (voir les explications dans la dernière partie des chapitres 2.5.1.3.1 et 2.5.1.3.2 ainsi que la Figure 47) et, par conséquent, un processus d'intégration simplifié. Dans une autre étape d'extension possible, des composants d'infrastructure centraux peuvent être introduits (par exemple, un intermédiaire central des identités des utilisateurs, un composant IAM central) afin de réduire le nombre total d'interfaces et d'augmenter la réutilisabilité des systèmes. Dès qu'une identité électronique réglementée par l'État sera disponible, elle pourra être utilisée en complément d'autres identités numériques - dans le sens d'une amélioration du principe Once-Only.

La feuille de route de mise en œuvre peut être résumée comme suit (vue agrandie en format paysage à l'Annexe C):

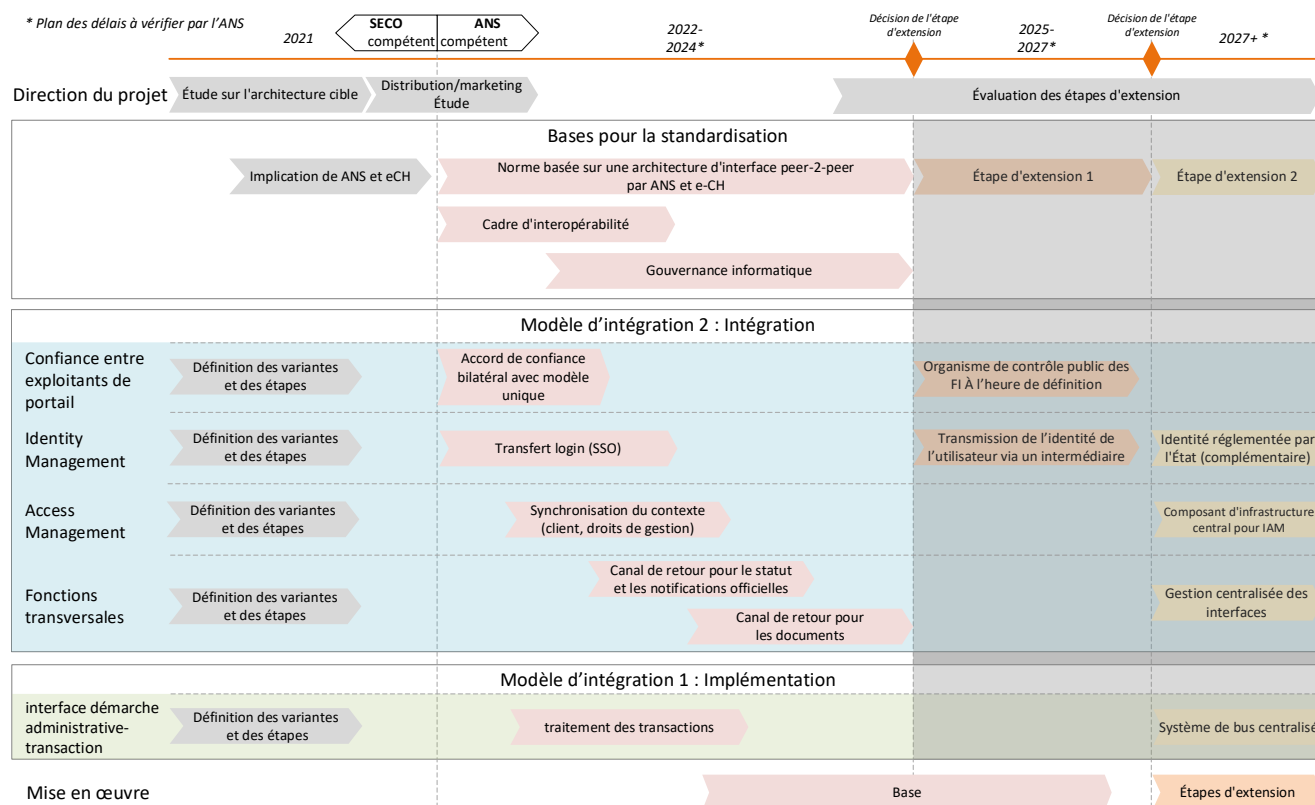


Figure 56: Feuille de route pour la mise en œuvre de la normalisation

Le SECO, en tant que mandant de cette étude, participe à l'ambition de l'ANS "une identification numérique reconnue par toutes les autorités est établie" (voir rapport de base [37]) et apporte une contribution importante grâce à l'étude.

2.7.2 Recommandations d'action

L'organisation "Administration numérique suisse" (ANS) est chargée de mettre en œuvre l'architecture cible d'intégration sous la forme d'une ou plusieurs normes. L'ANS est créé pour piloter la transformation numérique du système fédéral. Elle favorise la transformation numérique des administrations en Suisse et est conçue comme une plateforme politique qui fixe des normes⁸⁹. Elle reprendra les tâches de la cyberadministration suisse et de la Conférence suisse sur l'informatique (CSI).

Recommandations d'action à l'attention de l'ANS et d'autres parties prenantes:

Tableau 22: Mesures recommandées sous la responsabilité du SECO

Mesure	Résultat
Distribution de l'étude aux autorités intéressées	-

⁸⁹ "Plateforme politique qui fixe des normes" conformément au rapport final d'octobre 2019 (<https://www.admin.ch/gov/fr/accueil/documentation/communiqués.msg-id-76798.html>) et aux résolutions de la séance plénière de la CdC du 27.03.2021 et du Conseil fédéral du 03.04.2021.

Analyse des écarts entre l'architecture cible d'intégration et les intégrations d'easyGov avec des cas d'utilisation concrets (par exemple, les permis de travail dans le cadre de la loi sur l'immigration).	Version 2.0 de l'étude
Proposer des solutions pour les écarts identifiés	Version 2.0 de l'étude

Tableau 23: Mesures recommandées sous la responsabilité de l'ANS

Mesure	Résultat
Examen de la feuille de route de mise en œuvre	Achèvement de la feuille de route et lancement des premières mesures.
Mise en place d'un groupe de travail pour la normalisation	Pilotage et coordination avec les partenaires concernant l'établissement ou la modification d'une ou plusieurs normes pour les portails de prestations interopérables.
Développement d'une norme ou de plusieurs normes pour les portails de prestations (confiance entre pairs)	Normes eCH Prise en compte de l'orientation client, y compris l'élaboration d'un annuaire des prestations administratives à tous les niveaux fédéraux.
Mise en place d'un groupe de travail pour les aspects légaux	Création de la base légale pour l'intégration des prestations administratives à tous les niveaux fédéraux. Focalisation sur les dispositions relatives à la protection des données. Concrétisation des exigences légales pour l'accès aux registres et aux services de base (ex. UPI, SNA) Clarification des possibilités de déclaration donnant force obligatoire d'une norme.
Développement d'une procuration légale standardisée	Procuration légale standardisée, qui ne doit être émise qu'une seule fois par le client pour un utilisateur spécifique pour toutes les démarches administratives interopérables.
Initialisation de projets pilotes impliquant les autorités à tous les niveaux fédéraux (par exemple iGovPortal, EasyGov, DETEC, ePortal)	Mise en œuvre des travaux de normalisation
Clarification de la gouvernance informatique	Guide de la gouvernance informatique Clarification des responsabilités (RACI) et souveraineté de définition Spécification des exigences

Évaluation régulière du besoin de normalisation et de la mise en œuvre éventuelle d'étapes d'extension (selon la feuille de route de mise en œuvre)	Recommandation concernant l'étape d'extension
---	---

3 Analyse des écarts entre l'architecture actuelle d'EasyGov et l'architecture cible d'intégration.

Une deuxième version de cette étude évalue quelles adaptations à EasyGov sont nécessaires pour répondre à l'architecture cible d'intégration (analyse des écarts).

3.1 Ecart identifiés

Les écarts sont identifiés dans la 2ème version de cette étude.

3.2 Planification grossière pour l'élimination des écarts

La planification sommaire a lieu dans le cadre de la 2e version.

4 Annexes

Les annexes ne sont pas traduites. Exceptions: glossaire et figures utilisées dans le texte principal. Veuillez également trouver à l'Annexe H un glossaire allemand → français pour les principaux termes utilisés dans cette étude.

Annexe A Glossaire

Terme	Définition / Explication
Application métier	Une <i>application métier</i> met en correspondance des processus métier et gère généralement des données ou des informations qui représentent une valeur commerciale.
Application portail métier	<i>Application métier</i> accessible via un <i>portail de prestations</i> , qui représente une ou plusieurs <i>démarches administratives</i> (voir Figure 13, chapitre 2.1.3).
Autorité	Une organisation de droit public qui exerce des fonctions d'État souveraines en Suisse. Les <i>autorités</i> peuvent exister au niveau communal, cantonal ou fédéral et appartenir aux pouvoirs législatif, exécutif ou judiciaire. Voir également le Tableau 1 du chapitre 2.1.5
Back-end et front-end	Les termes <i>back-end</i> et <i>front-end</i> sont utilisés dans les technologies de l'information en relation avec une division en couches. En principe, le <i>front-end</i> est plus proche de l'entrée utilisateur (UI) et le <i>back-end</i> est plus proche du traitement. Voir aussi https://en.wikipedia.org/wiki/Front-end_and_back-end Note: La distinction entre les couches logiques back-end et front-end n'est pas la même que la différenciation technique entre client et serveur. Le front-end et le back-end peuvent avoir des composants client et serveur.
Client	Entité juridique pour laquelle une <i>prestation administrative</i> est utilisée. Il s'agit soit d'une personne morale, soit d'une personne physique (ou d'un groupe de personnes) qui a une obligation légale ou un droit à une prestation. Voir également le Tableau 1 du chapitre 2.1.5
Compte client	Représentation du <i>client</i> dans le <i>portail</i> . En plus de leurs données de base, les <i>notifications officielles</i> , les <i>démarches administratives</i> et les <i>droits de gestion</i> sont gérés dans le contexte du <i>compte client</i> .
Compte utilisateur	Représentation de l' <i>utilisateur</i> dans le <i>portail</i> . Outre leurs données de base, les informations d'identification et les paramètres (par exemple la langue) sont gérés dans le contexte du <i>compte utilisateur</i> .
Couche d'information	Domaine fonctionnel d'un <i>portail de prestations</i> qui donne à l' <i>utilisateur</i> une vue d'ensemble des <i>prestations administratives</i> disponibles (offre de prestations) et le conduit à la prestation requise Voir également le Tableau 1 du chapitre 2.1.5
Couche transactionnelle	Domaine fonctionnel permettant de traiter une <i>prestation administrative</i> . Cela comprend à la fois la <i>démarche administrative</i> du client dans le portail et le <i>traitement des transactions</i> dans le <i>système métier interne de l'autorité</i> .

	Voir également le Tableau 1 du chapitre 2.1.5
Démarche administrative	<p>Du point de vue du <i>client</i>, la <i>démarche administrative</i> est un processus qui comprend toutes les activités et étapes procédurales nécessaires pour obtenir une <i>prestation administrative</i>. Elle reflète le point de vue du bénéficiaire de la prestation sur la procédure administrative officielle. Les étapes du processus sont complémentaires à celles du <i>traitement des transactions</i> du côté de l'<i>autorité</i>.</p> <p>Voir également le Tableau 1 du chapitre 2.1.5</p>
Droit de gestion	<p>Le <i>droit de gestion</i> représente une <i>procuration</i> qui, au sens juridique, autorise un représentant à agir au nom du sujet de droit - c'est-à-dire le <i>client</i>. Sur le <i>portail de prestations</i> cette <i>procuration</i> autorise un utilisateur à gérer le <i>compte client</i> concerné et à effectuer des <i>démarches administratives</i> pour une <i>prestation administrative</i> spécifique, l'autorisation pouvant être graduée (par exemple, consultation, modification, soumission, Superuser).</p> <p>L'octroi et l'administration des <i>droits de gestion</i> relèvent de la responsabilité du <i>client</i> ou du représentant autorisé par le client. L'objectif doit être de développer et d'offrir une procuration légale standardisée, qui ne doit être émise qu'une seule fois par le client pour un utilisateur spécifique pour toutes les démarches administratives interopérables.</p> <p>Voir également le Tableau 1 du chapitre 2.1.5</p>
Exploitant de portail	<p>Entreprise ou organisation qui, en tant que prestataire de services, met un <i>portail de prestations</i> à la disposition de l'<i>autorité</i> en tant que bénéficiaire de services.</p> <p>Voir également le Tableau 1 du chapitre 2.1.5</p>
Fonction transversale	<p>Terme collectif désignant les fonctions générales du portail qui sont utilisées à la fois dans les <i>couches d'information</i> et <i>transactionnelle</i>.</p> <p>Voir également le Tableau 1 du chapitre 2.1.5</p>
Fournisseur d'identité (FI)	<p>Émetteur et gestionnaire d'<i>identités numériques</i>. Un <i>FI</i> fournit un service d'authentification et agit comme un système d'accès pour les <i>portails de prestations</i>. Exemples:</p> <ul style="list-style-type: none"> • CH-Login (eIAM de la Confédération) • FED login (eIAM de la Confédération) • BE-Login (Canton de Berne) • E-ID (future option d'identification électronique réglementée par l'État sur une base légale [23] et document de discussion sur l'image cible de l'E-ID [36])
Front-End	Voir <i>back-end</i>
Gestion des données clients	Domaine fonctionnel pour la création/enregistrement, la modification ou la suppression d'un <i>compte client</i>

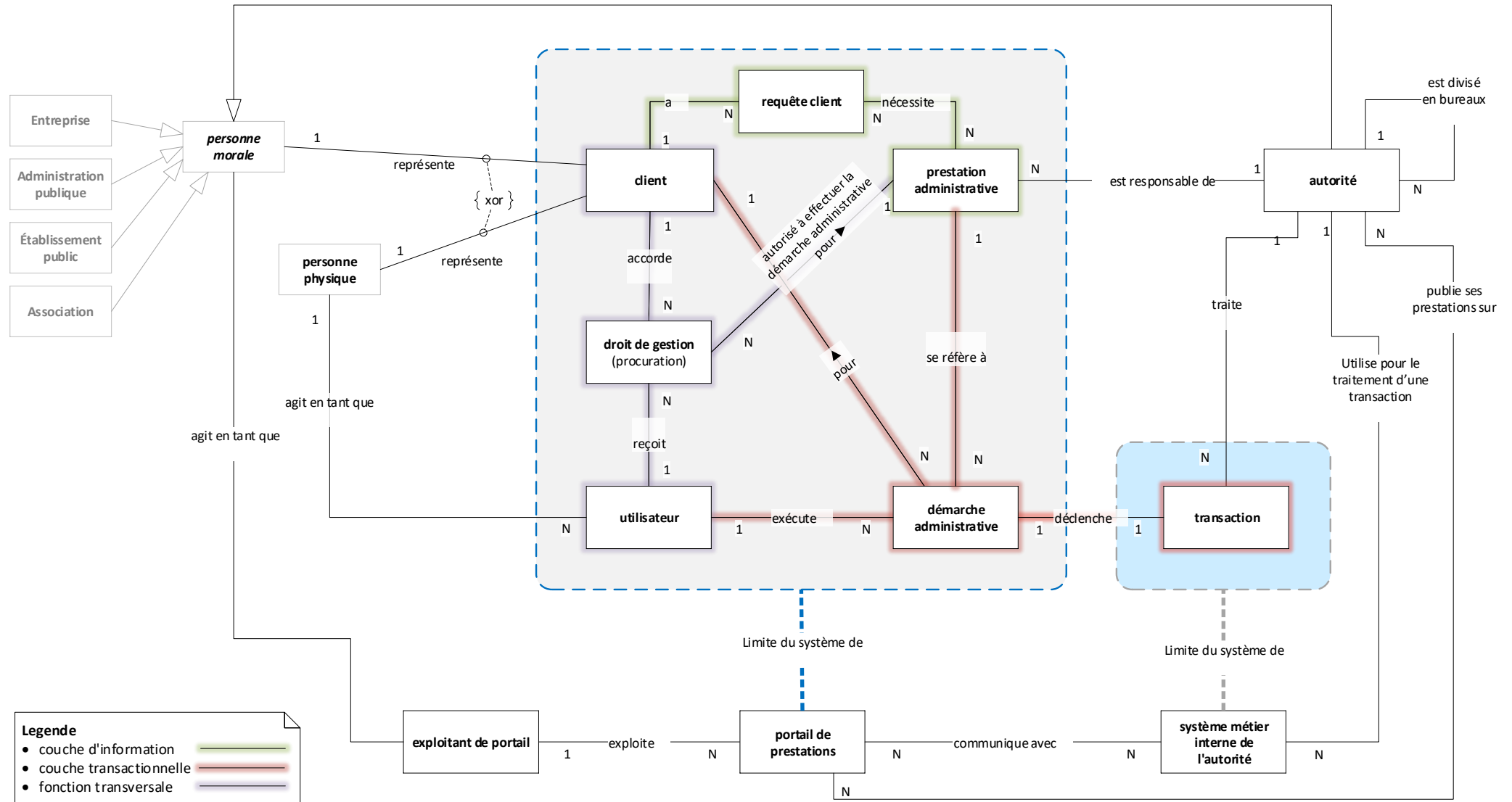
Gestion des données de base clients	Synonyme de <i>gestion des données clients</i>
Gestion des partenaires commerciaux	Synonyme de <i>gestion des données clients</i>
Identifiant	<p>Une chaîne de caractères exploitable par une machine qui identifie de manière unique une entité ou un objet commercial dans un espace de noms. Exemple d'identifiant de client:</p> <ul style="list-style-type: none"> • <i>client</i> PM → IDE • <i>client</i> PP → Numéro d'assuré (numéro AVS)
Identité électronique	Synonyme d' <i>identité numérique</i>
Identité numérique	Représentation d'une personne physique dans le monde numérique associée à une preuve d'identité électronique, délivrée et gérée par des <i>fournisseurs d'identité</i> . Une <i>identité numérique</i> permet l'accès aux <i>portails</i> . Le <i>fournisseur d'identité</i> peut également être le <i>portail</i> lui-même.
Intermédiaire	<p>Service d'infrastructure qui permet à un portail de prestations d'utiliser les identités numériques de différents FI. L'intermédiaire encapsule les différents FI et agit lui-même comme FI devant le portail.</p> <p>Selon la norme eCH-0107 [10], un intermédiaire fournit des services communs, tels que la gestion des métadonnées, la découverte du FI, la mise en relation des identités ou l'authentification et la transformation de la confirmation des attributs, à tous les autres fournisseurs de services IAM et aux parties utilisatrices d'une fédération d'identité. Un intermédiaire peut éventuellement comprendre un CSP. En outre, il convient de se référer aux normes eCH 0224 [31] et 0225 [32], qui décrivent plus en détail une fédération d'identité basée sur un intermédiaire.</p>
LoA (Level of Assurance / niveau de confiance)	<p>Ce terme désigne les niveaux de sécurité de l'authentification pour les transactions de cyberadministration. Elles décrivent le degré de certitude quant à la réalité de l'identité de l'utilisateur. La norme eCH-00170 [21] définit le modèle de niveau suivant pour le LoA du login:</p> <ul style="list-style-type: none"> • Niveau 1: Peu ou pas de confiance dans la validité de l'identité revendiquée. • Niveau 2: Faible confiance dans la validité de l'identité revendiquée. • Niveau 3: confiance considérable dans la validité de l'identité revendiquée. • Niveau 4: confiance élevée dans la validité de l'identité revendiquée. <p>L'utilisation des <i>prestations administratives</i> est généralement liée à un certain niveau de <i>LoA</i>.</p>

<p>Modèles d'intégration</p>	<p>Les <i>modèles d'intégration</i> "implémentation" et "intégration" sont des fonctionnalités de la manière dont les <i>portails de prestations</i> intègrent les prestations disponibles en externe (voir chapitre 2.1.6).</p> <p>Lors de l'implémentation, la <i>démarche administrative</i> pour une prestation spécifique est entièrement représentée dans le portail. Le terme "intégration complète" est également utilisé à cet effet.</p> <p>L'intégration consiste à incorporer une implémentation existante d'un système externe en la réutilisant. Les termes "intégration partielle" ou "saut" sont également utilisés à cet effet.</p> <p>Note: Dans cette version française de l'étude, nous utilisons le terme "intégration" pour désigner le modèle d'intégration 2. Cela peut prêter à confusion. Les auteurs considèrent toutefois que cette traduction est la plus appropriée pour le terme allemand "Einbindung".</p>
<p>Notification officielle</p>	<p>Message <i>autorité</i> → <i>client</i>, par exemple:</p> <ul style="list-style-type: none"> • Statut sur le traitement des <i>transactions</i> • Demande de preuves supplémentaires • Rappel du respect d'un délai <p>L'Annexe C présente une systématisation détaillée des notifications officielles adoptées à partir de l'ePortal.</p>
<p>Orchestration</p>	<p>Combinaison de plusieurs <i>prestations administratives</i> en un paquet global dans le but de regrouper les <i>prestations</i> pertinentes par rapport à une <i>requête client</i>. L'<i>orchestration</i> signifie notamment que le <i>portail</i> guide l'<i>utilisateur</i> à travers les <i>prestations</i> pertinentes en enchaînant les <i>démarches administratives</i> nécessaires (par exemple, dans un assistant/wizard) ou en proposant des connexions croisées (par exemple, l'obligation d'inscription préalable à l'emploi pour une demande de permis de travail pour les ressortissants de pays tiers).</p>
<p>Partenaire commercial</p>	<p>Terme couramment utilisé dans l'environnement SAP qui, selon le portail d'aide SAP, inclut les "personnes morales ou physiques avec lesquelles votre entreprise entretient des relations commerciales". Dans le cas des <i>prestations administratives</i>, le <i>partenaire commercial</i> est synonyme de <i>client</i>.</p>
<p>Plate-forme</p>	<p>Synonyme de <i>portail de prestations</i></p>
<p>Portail</p>	<p>Mot court pour <i>portail de prestations</i></p>
<p>Portail de prestations administratives / Portail de prestations</p>	<p>Application accessible au public (par exemple, application à page unique, application mobile, etc.) avec laquelle l'<i>exploitant de portail</i> offre au <i>client</i> un canal d'accès numérique à une ou plusieurs <i>prestations administratives</i> dans le cadre de la cyberadministration. Il s'agit de du <i>front-end client</i> pour des <i>prestations administratives</i> numériques. Le frontend est exploité par des <i>utilisateurs</i> dûment autorisés.</p> <p>Voir également le Tableau 1 du chapitre 2.1.5</p>


Prestation	Abréviation de <i>prestation administrative</i>
Prestation administrative	<p>Prestation publique (activité A2A, A2B ou A2C) qu'une autorité offre au <i>client</i> (PP ou PM) dans le cadre de ses compétences, conformément au mandat de l'État. L'utilisation se fait par le biais d'une <i>démarche administrative</i> côté client, la mise à disposition de la prestation par le biais du <i>traitement des transactions</i> côté autorité.</p> <p>Voir également le Tableau 1 du chapitre 2.1.5</p>
Procuration	Base juridique pour l'octroi d'un <i>droit de gestion</i>
Registre	Registre officiel dans lequel une collecte et une identification systématiques sont effectuées sur un groupe d'objets (par exemple, des entreprises).
Requête client	<p>Une requête client fait référence à la raison ou à l'élément déclencheur d'avoir recours à une <i>prestation administrative</i>. Dans le cas des clients PP, on parle également de "situation de vie", dans le cas des clients PM également de "situation commerciale" (voir eCH-0126 [14] et eCH-0138 [15]).</p> <p>Voir également le Tableau 1 du chapitre 2.1.5</p>
Sans état (stateless)	Un composant <i>sans état</i> "oublie" toutes les données de la transaction après l'entrée/le traitement/la sortie. Il ne contient que la logique commerciale de la transaction et ne fait aucune gestion des données. Voir aussi https://fr.wikipedia.org/wiki/Protocole_sans_%C3%A9tat
Souveraineté de définition	Responsabilité de la définition de spécifications, de règles ou d'interfaces ou similaires, qui sont appliquées au <i>temps d'exécution</i> . La <i>souveraineté de définition</i> s'exerce au <i>temps de définition</i> .
Souveraineté des données	Rôle prépondérant d'une institution dans la gestion des données. Le système utilisé par cette institution à cette fin est le système principal (tel que les registres d'Etat) pour les données concernées. Ce n'est que dans le système principal que ces données peuvent être modifiées, tous les autres systèmes concernés les reprennent.
Système métier interne de l'autorité	<p>Une ou plusieurs <i>applications métier</i> qui prennent en charge le <i>traitement des transactions</i> d'une ou plusieurs <i>prestations administratives</i>. Les utilisateurs sont exclusivement des employés de l'autorité respective.</p> <p>Du point de vue d'un <i>portail de prestations</i>, le <i>système métier interne de l'autorité</i> peut être associé en tant que <i>back-end</i>.</p> <p>Voir également le Tableau 1 du chapitre 2.1.5</p>
Temps d'exécution	Période de temps pendant laquelle les systèmes "vivent" de manière productive conformément à leur objectif.
Temps de définition	Période de temps pendant laquelle un système ou une spécification informatique - tel qu'un vocabulaire contrôlé - est en cours de développement, de mise en place et de configuration et n'est donc pas encore productif ou contraignant.

Transaction / Traitement des transactions	<p>Processus qui est déclenché dans l'<i>autorité</i> compétente à la suite d'une <i>démarche administrative</i> (c'est-à-dire lorsque le <i>client</i> a recours à une <i>prestation administrative</i>). Le <i>traitement des transactions</i> comprend toutes les activités et les étapes de la procédure qui sont nécessaires, du point de vue de l'autorité, pour la fourniture d'une prestation. Il reflète le point de vue du prestataire sur la procédure administrative. Les étapes du processus sont complémentaires à celles de la <i>démarche administrative</i> du côté du <i>client</i>.</p> <p>Voir également le Tableau 1 du chapitre 2.1.5</p>
Utilisateur	<p>Personne physique qui utilise activement le <i>portail de prestations</i> via une interface utilisateur et effectue ainsi des <i>démarches administratives</i> pour un <i>client</i> spécifique.</p> <p>Voir également le Tableau 1 du chapitre 2.1.5</p>

Annexe B Modèle d'information en vue agrandie au format paysage



Annexe C Systématisation des notifications officielles



Arten von Notifikationen

	Typ 1	Typ 2a	Typ 2b	Typ 2c	Typ 3	Typ 4
	Kommunikation, einweg	Kommunikation, einweg	Kommunikation, mit Rückantwort	Kommunikation mit Rückantwort – Start durch Benutzer	Kommunikation über mehrere User	Chat
Art	asynchron	asynchron	asynchron	asynchron	asynchron	Synchron Ausserhalb Betriebszeiten / User offline: Antwort als Typ 1 oder 2a
Zweck	Information an einen registrierten Benutzer senden. z.B. Information zum Geschäftsfall oder Zustellen von Dokumenten	Information an einen registrierten Benutzer senden. z.B. Information zum Geschäftsfall oder Zustellen von Dokumenten	Information an einen registrierten Benutzer senden bei der eine Rückantwort erforderlich oder gewünscht ist. z.B. fehlende Dokumente einfordern	Benutzer kann eine Frage zu einem Geschäftsfall stellen	Einfordern von Informationen durch Bund beim Vertreter des Benutzers – Vertreter wiederum kontaktiert den Benutzer	<ul style="list-style-type: none"> - Fragen / fachlicher Support innerhalb von Fachapplikationen klären - Benutzer beraten, mit welcher Fachapplikation
Auslöser	Portal / Service (System)	Portal / Service (System)	Portal / Service (System)	Benutzer	Portal / Service (System)	Benutzer
Inhalte	«SMS-charakter»	«Mailcharakter» ohne Rückantwort	«Mailcharakter» mit Rückantwort	«Mailcharakter» mit Rückantwort	«Mailcharakter»	Kurzauskunft
Anzeige in	Postfach des Portals		Postfach des Portals	Postfach des Portals	Fachapplikation	Portal

Eidgenössisches Finanzdepartement EFD
Generalsekretariat EFD

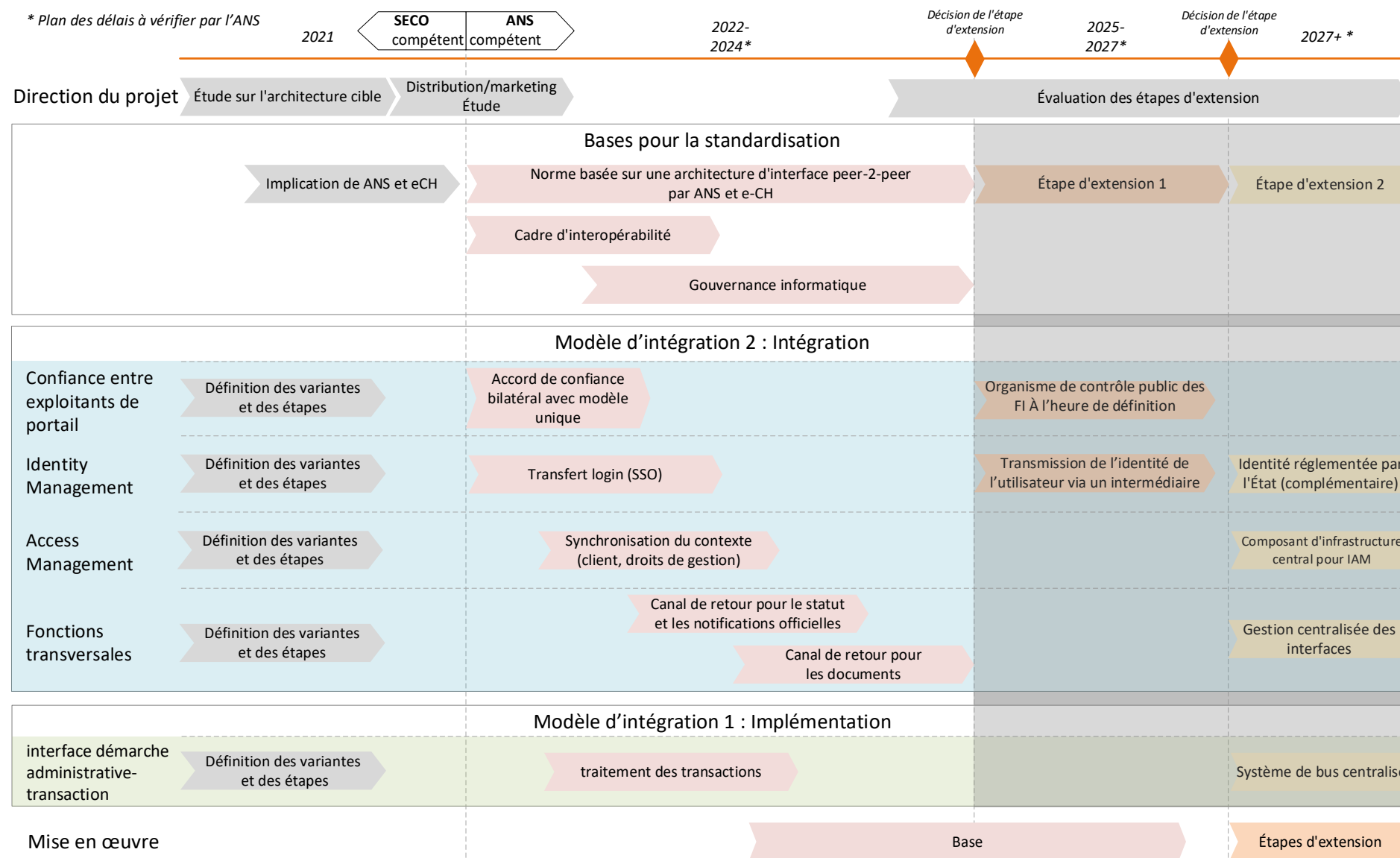
ABB Portal 31.03.2020 / ePortal / J. Umhang

19

(Quelle: Beitrag im Architekturboard Bund vom 31. März 2020 seitens EFD/ePortal)

Annexe D Feuille de route de mise en œuvre en vue élargie au format paysage

* Plan des délais à vérifier par l'ANS



Annexe E Thèses sur l'image cible de la représentation intégrative de prestations administratives sur des portails

Aus dem Bedürfnis [B-16] folgt zunächst: Ein Behördenleistungsportal muss einem User die für ihn relevanten Behördenleistungen zugänglich machen können. Es ist dabei jedoch egal, ob diese aus technischer Sicht wirklich in dem Portal implementiert sind oder das dem User nur so erscheint.

Es gestaltet sich infolge der unterschiedlichen User- bzw. Kundenbedürfnisse schwierig, alle Behördenleistungen der Schweiz auf einem einzigen zentralen Portal anzubieten, das allen Anforderungen aller Stakeholdergruppen gerecht wird. Hinzu kommt, dass die föderale Struktur der Schweiz diesen zentralen Ansatz nicht begünstigt. In Konsequenz dieser Überlegung sei folgendes Zielbild formuliert:

[These-1] Ein Behördenleistungsportal kann einem User⁹⁰ die für ihn relevanten Behördenleistungen digital zugänglich machen, auch wenn diese nicht in diesem, sondern in einem anderen System primär implementiert sind⁹¹.

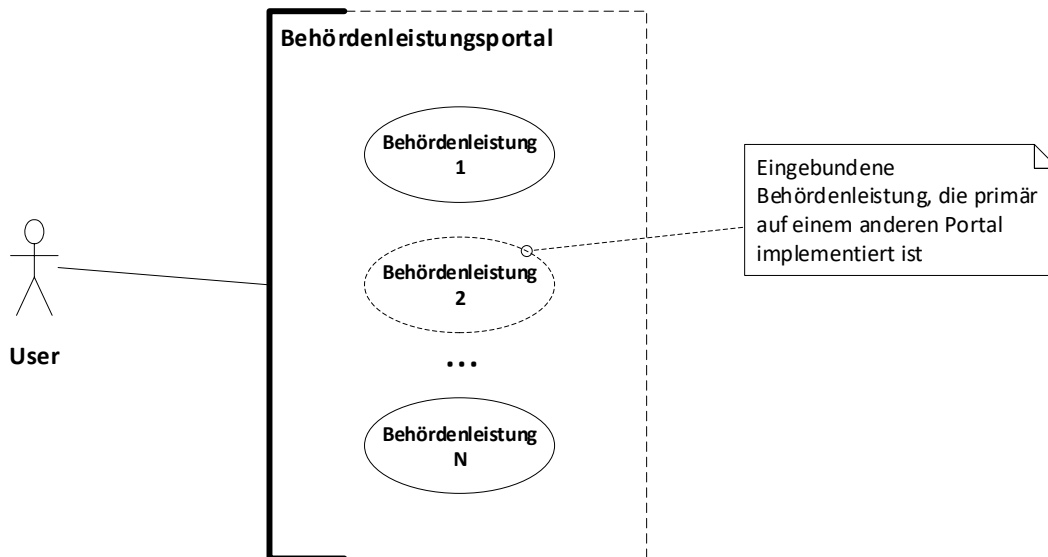


Abbildung 57: Ein Behördenleistungsportal bietet dem User die für ihn relevanten Behördenleistungen an, egal auf welchem System sie primär implementiert sind [These-1] (UML Use Case Diagramm)

Es fragt sich jedoch, was unter "relevante" Behördenleistungen zu verstehen ist. Dies kann einerseits vom Kontext des Kundentyps abhängen, der auf den Kunden zutreffend ist, in dessen

⁹⁰ Wie schon im Informationsmodell, Kapitel 2.1.5 klargestellt, wird der Fall betrachtet, dass hinter dem User eine natürliche Person steht. Der Fall User = IT-System wird bei der Entwicklung des Zielbilds aus der User-Perspektive nicht betrachtet, da IT-Systeme (noch) keine Interessen verfolgen, sondern nur deren Betreiber.

⁹¹ Beispiel EasyGov: Die Mehrwertsteueranmeldung ist in EasyGov zugänglich, obwohl sie effektiv in einem System der ESTV implementiert ist. Diese Anmeldung ist in EasyGov eingebettet.

Namen/Auftrag der User agiert⁹². Andererseits kann aber auch das Leistungsangebot einer bestimmten Behörde als relevant erachtet werden. Letztlich ist festzustellen:

- Es gibt – je nach Blickwinkel – mannigfaltige Sets als relevant erachteter Behördenleistungen
- Sets an relevanten Behördenleistungen können sich überlappen

Diese Feststellung führt zu einem weiteren Aspekt des Zielbilds:

[These-2] Behördenleistungsportale präsentieren gemäss ihrer Ausrichtung vielfältige Sets an Behördenleistungen, die sich aus portalübergreifender Sicht überlappen können. Auf welches Set an Behördenleistungen ein Portal ausgerichtet ist, liegt in der Verantwortung des jeweiligen Portalbetreibers.

⁹² Gilt auch, wenn im Falle einer natürlichen Person Kunde und User identisch sind (z.B. Bürger, Selbständige)

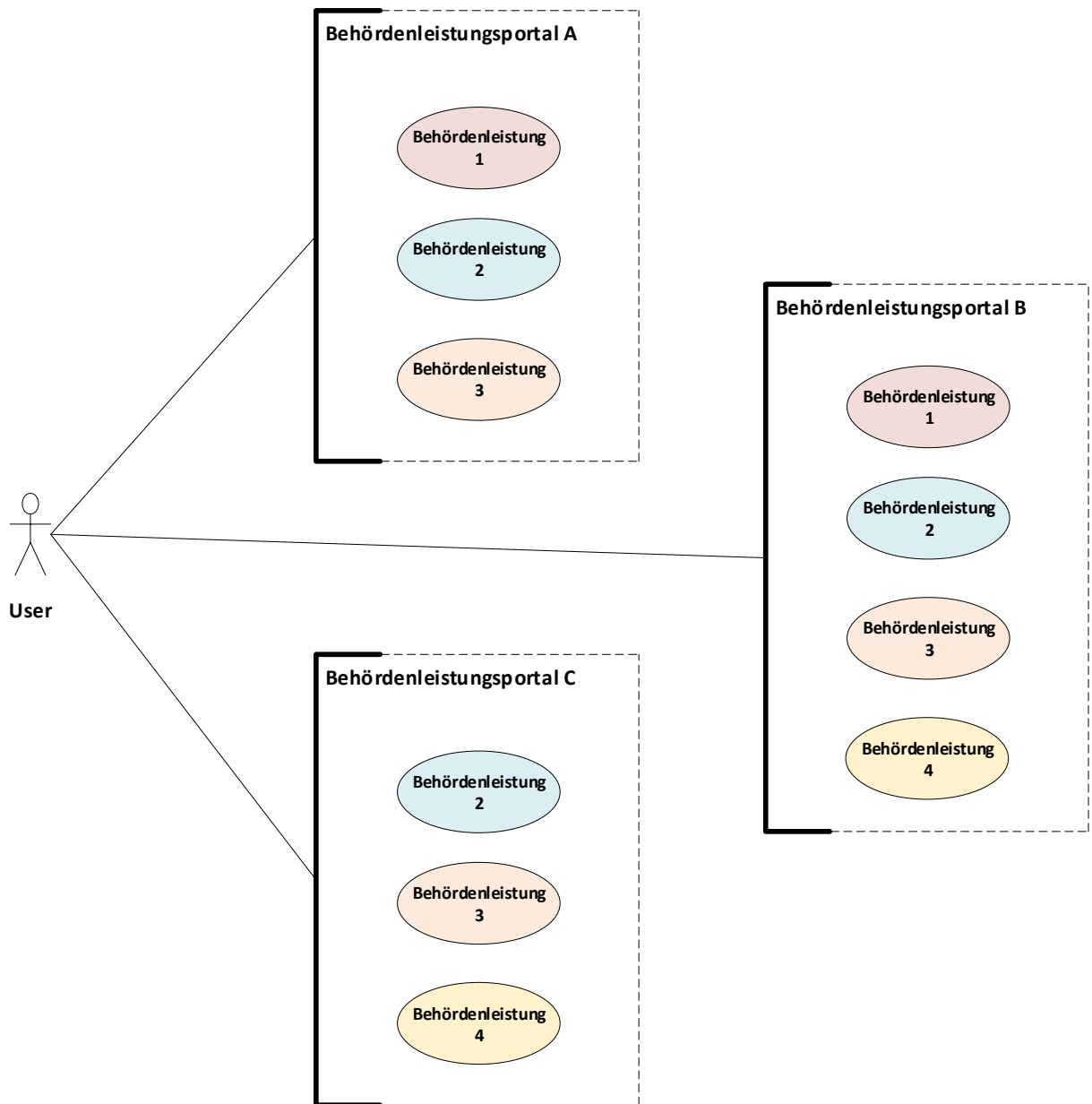


Abbildung 58: Behördenleistungsportale präsentieren überlappende Sets an Leistungen [These-2]

Gemäss Bedürfnis [B-1] bzw. [EIF-6] muss der Zugang zu den relevanten Behördenleistungen über verschiedene Portale möglich sein, damit der User jenes auswählen kann, das seinen Bedürfnissen am besten gerecht wird. Wie die folgende Überlegung zeigt, können diese Bedürfnisse auch persönlicher Art sein: Im Blick auf die Vertrautheit der User im Umgang mit Behördenleistungen sei von einer Bandbreite zwischen folgenden Extrempunkten ausgegangen:

- User "Keine-Ahnung"
 - Wird infolge irgendeines kundenseitigen Auslösers damit konfrontiert, einen Behördengang zu absolvieren, den er noch nie oder nur selten gemacht hat
 - Weiss nicht (mehr), wo man was wie erledigt und welche Behörde zuständig ist
- User "Weiss-Bescheid"

- Kennt sich in der Vielfalt von Behördenleistungen aus
- Weiss, wo man was wie erledigt und welche Behörde zuständig ist
- Möchte wiederkehrende Behördengänge effizient erledigen

Es ist anzunehmen, dass der User "Keine Ahnung" gemäss Bedürfnis [B-15] einen ausführlichen Informationslayer und gemäss Bedürfnis [B-21] viele Hilfestellungen im Transaktionslayer erwartet und somit eher ein Behördenleistungsportal bevorzugt, welches auf den Typ des von ihm vertretenen Kunden ausgerichtet ist (z.B. KMU, Bienenzüchter, Pensionäre, etc.). User "Weiss-Bescheid" wird hingegen vermutlich eher Behördenleistungsportalen mit schlankem oder gar keinem Informationslayer zuneigen und Hilfestellungen im Transaktionslayer als unnötig oder bremsend empfinden. Als Beispiel seien folgend drei unterschiedliche Gestaltungsbedürfnisse zur Anwendung «Steuer ausfüllen» illustriert:

- eine Treuhänderin, die pro Steuerperiode hunderte von Steuererklärungen ausfüllt
- eine Person, die einmal jährlich die Steuererklärung ausfüllt
- eine blinde Person

Letztlich führt diese Überlegung zu der Feststellung, dass jegliche Ausrichtung eines Behördenleistungsportals seine Berechtigung hat. Das Zielbild darf diesbezüglich keine Beschränkungen implizieren. Es ist vielmehr zu unterstützen, dass eine Behördenleistung auf mehreren Portalen unterschiedlich gestaltet sein kann (siehe Abbildung 59). Im Einklang mit dem Informationsmodell (N:N-Beziehung zwischen Behördenleistung und Behördenleistungsportal, siehe Figure 20) sei für das Zielbild ergänzt:

[These-3] Eine Behördenleistung kann auf mehreren Portalen unabhängig voneinander verschieden präsentiert werden.

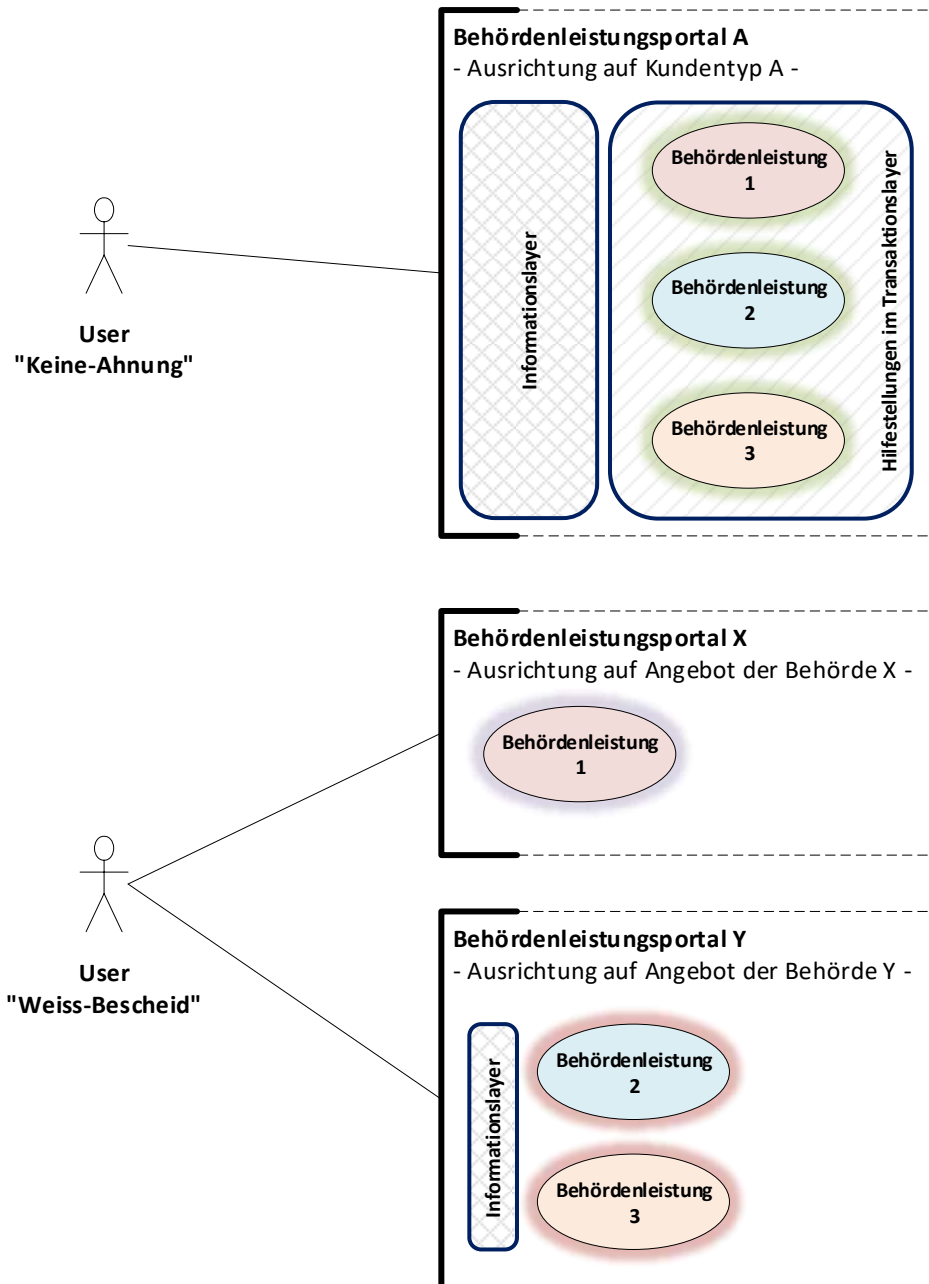


Abbildung 59: Abbildung von Behördenleistungen auf verschieden ausgerichteten Portalen in jeweils individuellem Design (verbildlicht durch die verschiedenen farblichen Umrandungen der Ovale) [These-3]

Annexe F Exigences en matière de gouvernance informatique

Zu den in Kapitel 2.5.4.2 erwähnten Fokusbereiche der IT-Governance werden nun Anforderungen formuliert.

[Fokusbereich-1] *Strategic Alignment*: Sicherstellen, dass die E-Government Strategie berücksichtigt wird und E-Government Prinzipien, eCH-Standards und Rechtsgrundlagen angewendet werden

Es gilt ein strategisches Fundament zu legen und anzuwenden, welches es allen Akteuren im Umfeld von E-Government erlaubt, auf ein gemeinsames Ziel hinzuarbeiten: Die Interoperabilität zwischen Behördenleistungsportalen mittels Standardisierung zu ermöglichen.

[REQ-60] Die DVS soll federführend und in Abstimmung mit Partnern und Behörden auf dieses Ziel hinarbeiten. Die DVS übernimmt dabei eine Koordinations- und Steuerungsrolle, der Verein eCH zeichnet verantwortlich für die Standardisierung und die eOperations Schweiz AG übernimmt die Beschaffung und den Betrieb von Behördenübergreifenden Systemen.

[REQ-61] Der zu etablierende Standard soll wo immer möglich auf bestehenden eCH-Standards aufbauen.

[REQ-62] Die DVS soll den Standard auf allen föderalen Ebenen fördern. Die Behörden sollen über die Vorteile der Interoperabilität zwischen Portalen und die Anwendung von Standards informiert und überzeugt werden.

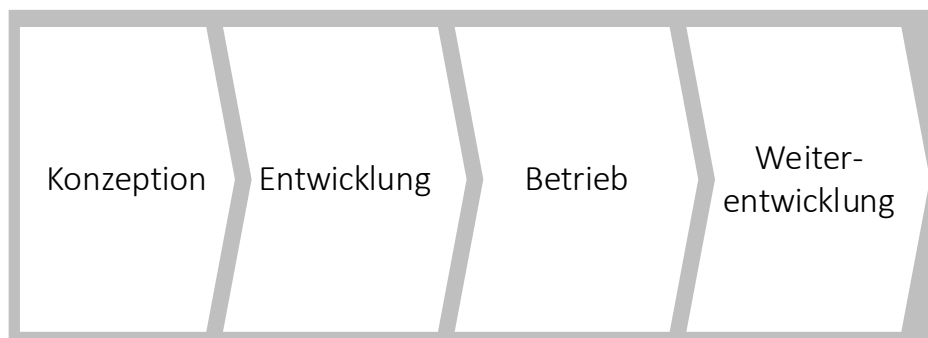
[REQ-63] Die DVS soll Konkurrenzsituationen vermeiden (z.B. Einführung und Betrieb unterschiedlicher Lösungen im Bereich IAM).

[REQ-64] Die DVS soll klären, ob und wie eine Verbindlicherklärung des neu zu schaffenden Standards möglich ist (z.B. mittels Unternehmensentlastungsgesetz oder andere Rechtsgrundlagen).

[Fokusbereich-2] *Value Delivery*: Gewährleistung der Kontinuität der Leistungen mit einer hohen Wirtschaftlichkeit über den gesamten Life-Cycle, inklusive Weiterentwicklung der Integrations-Sollarchitektur

Die Behördenleistungsportale sollen Behördenleistungen stets in hoher Qualität und mit einem wirtschaftlichen Einsatz von Steuergeldern zur Verfügung stellen.

Die Anforderungen an den Fokusbereich *Value Delivery* werden in folgende Life-Cycle Phasen beschrieben:



Konzeption

Die Definitionshoheit über Daten, Prozesse und Prinzipien, welche für die Integration einer Behördenleistung von Bedeutung sind, soll beim Provider der Behördenleistung liegen.

[REQ-65] Im Zuge der Standardisierung soll festgehalten werden, welche Merkmale der zu integrierenden Behördenleistung der Provider vorab definieren muss. Dazu zählen: Schnittstellen-Prozesse, Interoperable Datenbereiche, Unterstützte Technologien, Anbindungsbedingungen (beispielsweise minimal geforderter Level-of-Assurance (LoA) für die Nutzung der Behördenleistung), Anforderungen an den Datenschutz, Performanceanforderungen, Vertragliche Verpflichtungen.

Gleichzeitig muss der Provider auch gewisse Pflichten erfüllen, wie beispielsweise die Sicherstellung von gleich hohen Performanceanforderungen (SLA) und die Berücksichtigung von Standards.

Entwicklung

[REQ-66] Bei der Entwicklung und Bewertung von Softwareprodukten sollen Qualitätskriterien gemäss ISO 250xx berücksichtigt werden

[REQ-67] Bei der Weiterentwicklung ist stets auf die Rückwärtskompatibilität zu achten inkl. Grace Period während der ältere Schnittstellenversionen unterstützt werden

[REQ-68] Bei der Entwicklung von Benutzeroberflächen (UI) sollen nach Möglichkeit gleiche UX-Prinzipien angewendet werden. Dies bezieht sich insbesondere auf den Bedienkomfort (z.B. Anzahl Bedienschritte, Navigation, etc.), nicht auf das Look & Feel.

[REQ-69] Alle für eine Integration relevante Systeme müssen in drei Umgebungen zur Verfügung stehen: Test, Abnahme und Produktion. Dies betrifft alle Systemkomponenten (Front-End, Back-End, etc.) der involvierten Partner (Consumer und Provider) im Transaktionslayer.

[REQ-70] Zur Verifizierung von Entwicklungen sollen Pilotprojekte über die drei föderalen Ebenen hinweg durchgeführt werden.

Betrieb

[REQ-71] Die Verfügbarkeit muss sowohl von Provider- wie auch von Consumer-Seite gewährleistet werden (SLA). Allfällige in einer späteren Phase zentral zur Verfügung gestellte Infrastrukturkomponenten müssen die Verfügbarkeit ebenfalls garantieren.

[REQ-72] Im Fall eines Systemausfalls innerhalb der gesamten Systemkette soll der Behörden-gang zu einem späteren Zeitpunkt nahtlos fortgesetzt werden können (z.B. durch Speicherung des Benutzerkontextes).

[REQ-73] Alle involvierten Organisationen sollen nach Möglichkeit eine gleich hohe Verfügbarkeit garantieren (z.B. zeitliche Verfügbarkeit des Servicedesks). Eine garantierte Verfügbarkeit des Gesamtsystems wird nicht angestrebt, da diese von der Komplexität her kaum zu steuern wäre.

[REQ-74] Der Support muss für den User nachvollziehbar geregelt sein: das Consumer-Portal muss immer die erste Anlaufstelle für den User sein (1st Level). Für den 2nd Level Support ist der Betreiber der integrierten Behördenleistung verantwortlich.

Weiterentwicklung

[REQ-75] DVS soll verantwortlich für die Change-Management Prozesse der interoperablen Schnittstellen sein

[REQ-76] Veränderungen sollen zeitnah an alle Akteure kommuniziert werden, insbesondere bei der Einführung und Verbindlichkeitserklärung von Standards.

[Fokusbereich-3] *Risk Management*: Risikobewusstsein und –minimierung sicherstellen, Fehlervermeidung fördern

[REQ-77] Interoperable Schnittstellen und Infrastrukturkomponenten sollen etappierte gemäss einer Roadmap eingeführt werden

[REQ-78] Zentrale Infrastrukturkomponenten sollen erst in späteren Ausbausritten vorgesehen werden

Risiken im Zusammenhang mit Informationssicherheit und Datenschutz (ISDS) wurden im Kapitel 2.5.2 näher beleuchtet.

[Fokusbereich-4] *Resource Management*: Verantwortungsbewusster Umgang mit öffentlichen Geldern, um Ressourcen (Personal, Prozesse, Infrastruktur, Information) möglichst effizient einzusetzen. Klare Regelung der Verantwortlichkeiten (RACI) innerhalb verschiedener Organisationen

[REQ-79] Die personellen und finanziellen Ressourcen sollen effizient und zum richtigen Zeitpunkt eingesetzt werden.

[REQ-80] Jedes Portal / jede Behörde muss die Kosten für die Umsetzung von neuen Schnittstellen grundsätzlich selbst übernehmen. Investitionszyklen der Akteure (z.B. Kantone) müssen berücksichtigt werden.

[REQ-81] Es soll möglichst transparent bezüglich der Verwendung der Ressource 'Daten' gehandelt werden: Jeder Kunde (im Sinne von JP oder NP, aber auch des Portal-Benutzers) soll sich im Rahmen der gesetzlichen Möglichkeiten informieren können, welche Daten gespeichert werden, wo und wie lange die Daten gespeichert werden und welche Behörden für welchen Zweck darauf zugreifen können. Es gilt aus Komplexitätsgründen abzuwägen, welche Informationen zur Verfügung gestellt werden können.

[Fokusbereich-5] *Performance Measurement*: Verfolgung und Überwachung der Leistungserbringung über den gesamten Life-Cycle

[REQ-82] Die DVS soll definieren, welche Performanceindikatoren (KPI) durch die Leistungserbringer regelmässig geprüft werden müssen.

[REQ-83] Service-Provider sollen mittels SLA dazu verpflichtet werden, bestimmte Leistungskriterien zu garantieren.

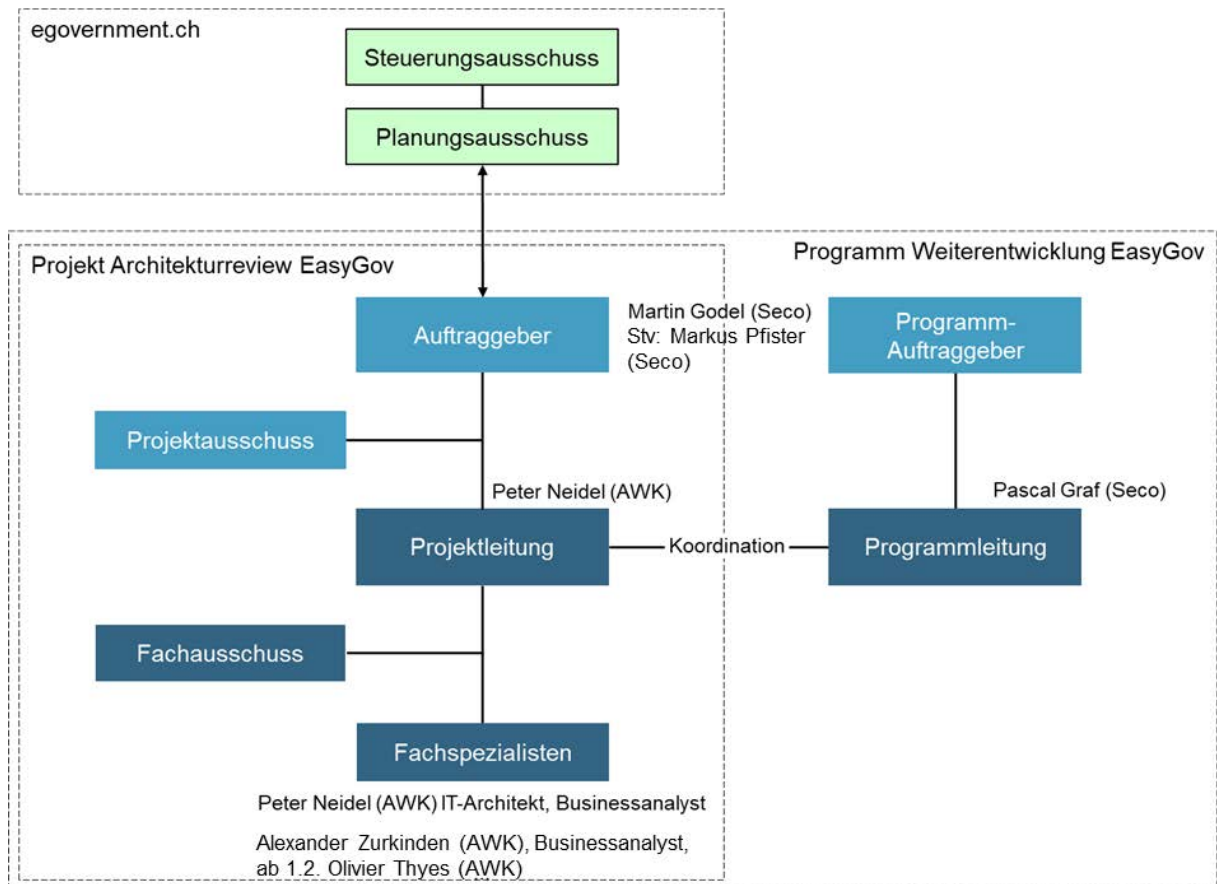
Annexe G Détails sur la mise en œuvre du projet

Annexe G.A Projektsetup

Der Architekturreview wurde in enger Abstimmung mit dem Planungsausschuss von E-Government Schweiz durchgeführt.

Die Einbindung der Stakeholder für den Architekturreview erfolgte differenziert:

- Im Projektausschuss für die strategische Ebene (Ziele und daraus abgeleitete geschäftliche Anforderungen strategischer und rechtlicher Natur)
- Im Fachausschuss für die Geschäfts- bzw. IT-Ebene (Ziele, Anforderungen an Geschäfts- und Technologiearchitekturen operativer Natur)



Der Projektausschuss war wie folgt besetzt:

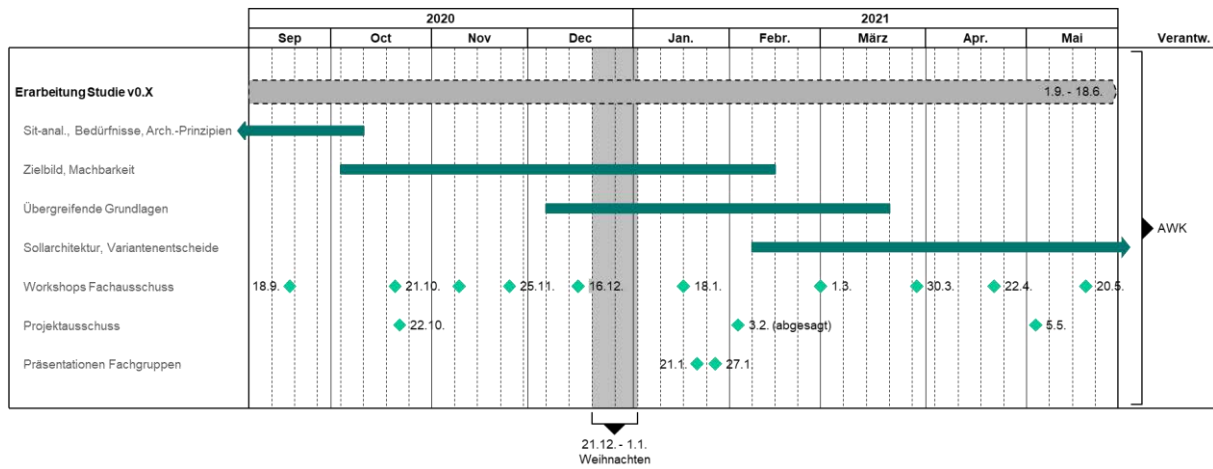
- Alexandra Collm, Leiterin Bereich Kunden, Direktion für Organisation und Informatik Stadt Zürich
- David De Groote, Mitglied Planungsausschuss eGov-CH, Kt. Jura
- Hansjörg Hänggi, Planungsausschuss eGov-CH, E-Government Verantwortlicher Kt. Baselstadt
- Marcel Kessler, Projektleiter Umsetzungsplan, Geschäftsstelle E-Government Schweiz
- Andreas Spichiger, Auftraggeber UZ14, Leiter Bereich Architektur, BK

Der Fachausschuss war wie folgt besetzt (teils wechselnde Teilnehmer):

- Philipp Achermann, Leiter Unternehmensarchitektur, Kanton Bern
- Nils Blattner, IT-Architekt, Kanton Basellandschaft
- Urs Brunner, Teamleiter ZSservices, Staatskanzlei Kanton Zürich
- Vojto Elias, Business Analyst Cyber Administration, Kanton Waadt
- Giovanni Groppo, ICT-Architekt Schwerpunkt Fachanwendungen, Stadtverwaltung Zürich
- Daniel Krebs, Leiter Digital Services, UVEK
- David Lehmann, Verantwortlicher Entwicklung und Betrieb ePortal, BIT
- Oldrich Milde, Unternehmensarchitekt WBF
- Matthias Overney, IT-Architekt und technischer Leiter iGovPortal, Kanton Freiburg
- Jörg Pietschmann, IT-Unternehmensarchitekt, Kanton Luzern
- Willy Reinhardt, Leiter Centre de compétences architecture et intégration à la Direction des systèmes d'information, VD
- Staudenmann René, Identity and Access Management, BIT
- Jürg Umhang, GS EFD, ePortal
- Lukas Weibel, Leiter Business Engineering und Projekte, Kt. ZH
- Jürg Wüst, Unternehmensarchitekt, BK
- Andreas Zeltner, Leiter Gruppe Strategische Projekte, KSTA ZH

Annexe G.B Vorgehensweise und Termine

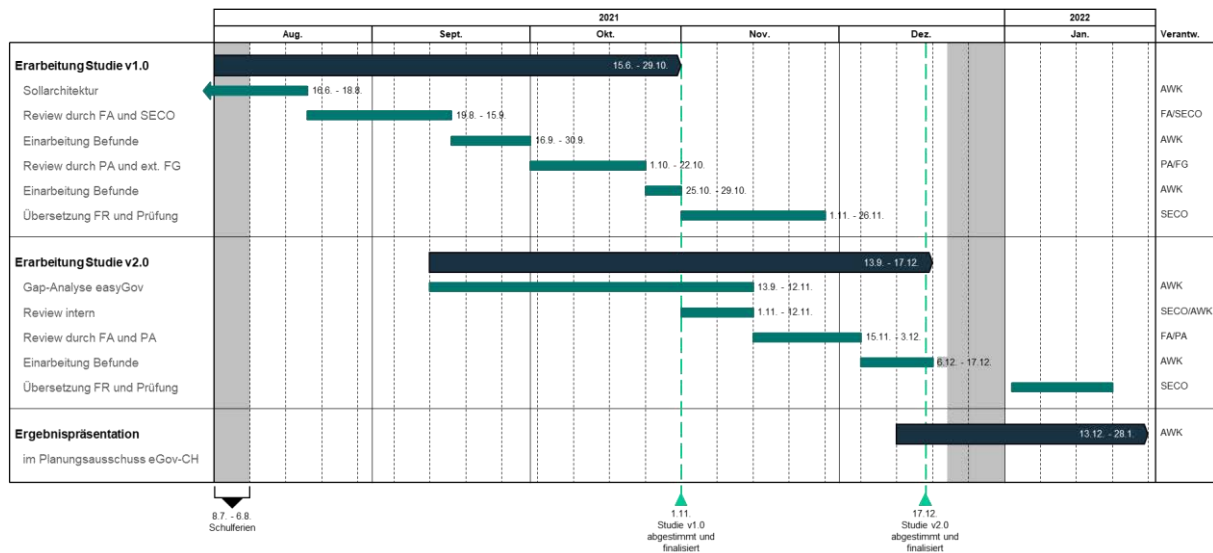
Die Integrations-Sollarchitektur wurde iterativ in einer Workshop-Reihe zusammen mit dem Fachausschuss gemäss folgendem Terminplan erarbeitet:



Zusätzlich zu den Workshops haben fortlaufend bilaterale Abklärungen mit Mitgliedern des Fachausschusses und diversen Experten stattgefunden.

Parallel dazu wurde die Studie sukzessive entwickelt, regelmässig durch den Fachausschuss revidiert und die Befunde anschliessend eingearbeitet. Das Vorhaben und der zu dem Zeitpunkt aktuelle Stand wurde den Fachgruppen SEAC⁹³ am 21.1.2021 sowie der Interkantonalen Fachgruppe E-Government⁹⁴ am 27.1.2021 präsentiert. Beide Fachgruppen waren im Fachausschuss vertreten sowie im gesamthaften Review der Studie eingebunden.

Das Review der Studie und die Erstellung der Version 2 erfolgten gemäss folgendem Zeitplan:



⁹³ Siehe <https://www.ech.ch/de/node/36639>

⁹⁴ Siehe <https://www.egovernment.ch/de/organisation/fachgruppe-egovernment-schweiz>

Annexe G.C Verankerung von TOGAF

Die Erarbeitung dieser Studie erfolgt systematisch gemäss TOGAF. Für ein klareres Verständnis zum Vorgehen gemäss TOGAF im Rahmen dieser Studie sind nachfolgend relevante Informationen aufgeführt.

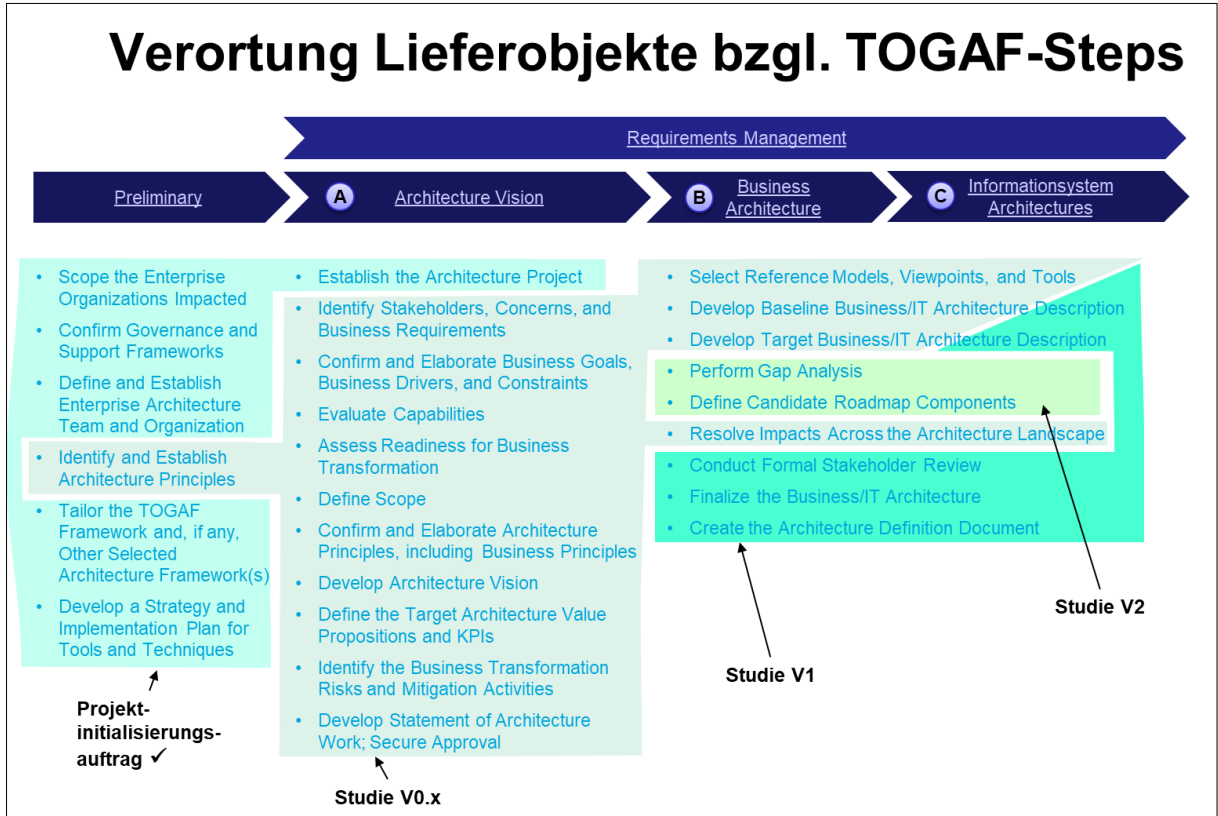


Abbildung 60: Verortung Lieferobjekte bezüglich TOGAF-Steps

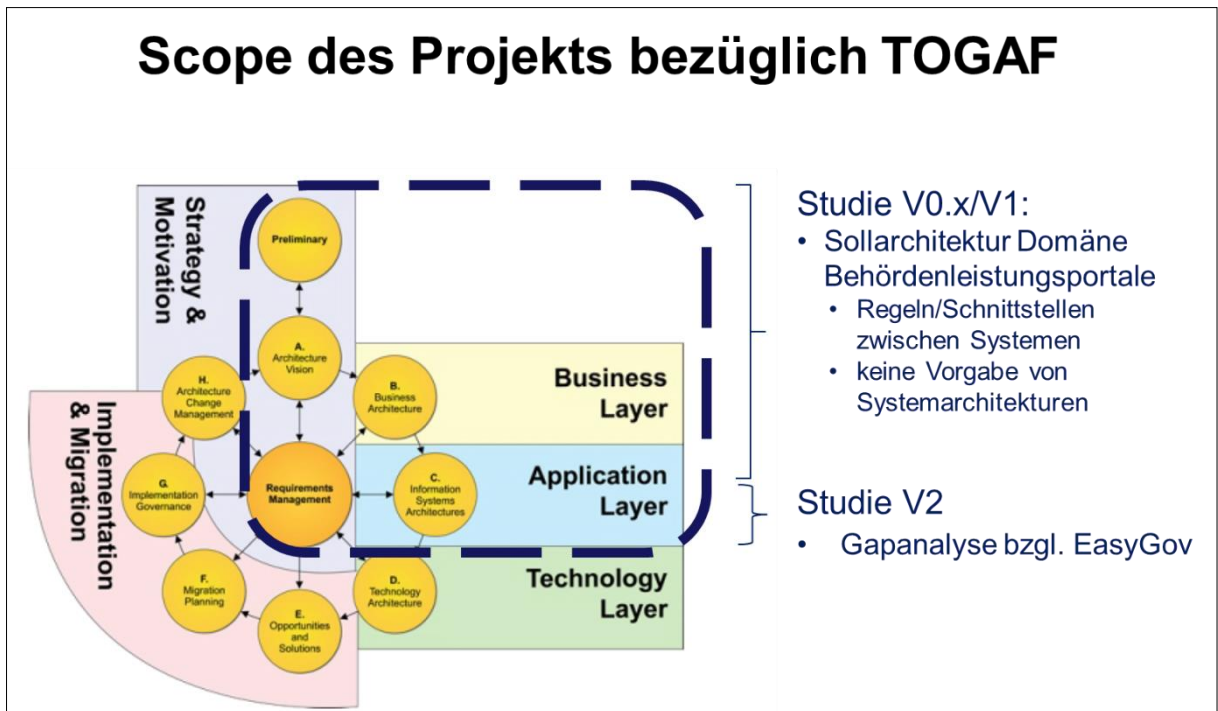


Abbildung 61: Scope des Projekts bezüglich TOGAF

Weitere Informationen zu TOGAF können auf der offiziellen Seite der «the Open Group», die den TOGAF Standard definiert, gefunden werden:

<https://pubs.opengroup.org/architecture/togaf9-doc/arch/index.html>

Annexe G.D Evaluation von Lösungsansätzen bezüglich zu lösender Herausforderungen

Zur Umsetzung des in Kapitel 2.4 beschriebenen Zielbildes in eine Sollarchitektur stellen sich verschiedene Herausforderungen. Im Zuge der Ausarbeitung dieser Studie wurden diverse Herausforderungen identifiziert, die einen hohen Einfluss auf den Lösungsraum haben. Zu Beginn der Architekturentwicklung wurden geeignete Lösungsansätze evaluiert.

Wichtig: Einige der in diesem Anhang formulierten Empfehlungen und Entscheide wurden zu einem späteren Zeitpunkt wieder revidiert. Ebenso hat sich die Systematisierung gegen Ende geändert. Im Interesse der Nachvollziehbarkeit wird die Betrachtung der Herausforderungen gleichwohl in diesem Anhang belassen, obwohl die Ergebnisse nicht 1:1 in die Anforderungen an die Standardisierung einfließen.

[Herausforderung-1] Der User-Zugang erfolgt mittels einer portalübergreifend definierten digitalen Identität. Welche digitalen Identitäten sollen verwendet werden? Kommen verschiedene Identitätsprovider in Betracht, ist ein Portalbetreiber diesbezüglich mit einer heterogenen und sich dynamisch entwickelnden Schnittstellenwelt konfrontiert, was den Bedürfnissen [B-28] "Wirtschaftlichkeit" und [B-29] "Weiterentwicklungsqualität" zuwider läuft.

Lösungsansätze:

- (A) Standard für die Schnittstelle Identitätsprovider ↔ Behördenleistungsportal kreieren, wobei auf bestehenden Standards und Protokollen (z.B.: SAML, OAUTH/OIDC, LDAP,...) aufgebaut wird.
- (B) Auf Vermittlerdienste (gemäss des im eCH-0107 [10] beschriebenen Hub-'n'-Spoke Identity Federation Modells welches in den eCH-Standards 0224 [31] und 0225 [32] näher detailliert wird) setzen, die die von [Herausforderung-1] beschriebene Komplexität vor dem Behördenleistungsportal kapseln. Darüber hinaus können Vermittler auch Mappingdienste von verschiedenen digitalen Identitäten einer Person leisten. Der Vermittler muss dabei nicht zwingend ein dem Portal externer Dienst sein. Es kann z.B. auch ein lizenziertes Software Produkt sein, welches direkt auf dem Portal eingesetzt wird. Unabhängig der gewählten Nutzungsvariante des Vermittlerdienstes ist es wichtig, dass das Portal die Verantwortung über die durch den Vermittler akzeptierten Identitätsprovider behält. So kann das Portal z.B. im Fall, dass es mit der Leistung eines

Identitätsproviders nicht einverstanden ist, diesen im Vermittler von der Liste der möglichen Provider ausschliessen.

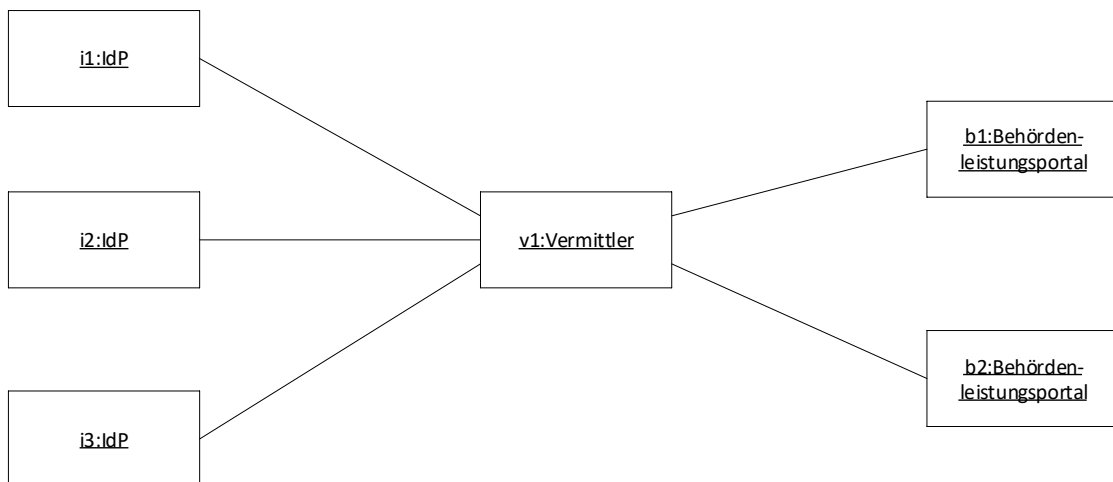


Abbildung 62: Vermittlerdienst zwischen IdPs und Behördenleistungsportalen

- (C) Nur staatlich regulierte elektronische Identifizierungsmöglichkeiten verwenden. Grundlage dafür ist das E-ID-Gesetz [23] (BGEID^{95, 96}), welches u.a. vorsieht,
 - dass zwar mehrere Identitätsprovider die E-ID anbieten dürfen, aber gemäss Artikel 18 diese sämtliche ausgegebenen E-IDs verarbeiten müssen, ungeachtet dessen, von welchem IdP bzw. E-ID-System diese primär verwaltet werden (Interoperabilität). Folglich muss ein Behördenleistungsportal nur mit einem E-ID-System bzw. IdP zusammenarbeiten.
 - dass Identitätsprovider der E-ID einer staatlichen Anerkennung bedürfen sowie jede E-ID, die für das geforderte Sicherheitsniveau ausgestellt wurde, durch Behörden oder anderen Stellen, die öffentliche Aufgaben erfüllen, akzeptiert wird. Daraus ergibt sich ein Zusatznutzen: Dem mit einer einzelnen E-ID verbundenen Sicherheitsniveau/LoA kann ein Portalbetreiber folglich vorbehaltlos vertrauen, was [REQ-42][REQ-39] entgegenkommt.
 - dass mit der E-ID eine E-ID-Registrierungsnummer verbunden ist. Daraus ergibt sich ein weiterer Zusatznutzen: Die E-ID bietet neben der digitalen Identität

⁹⁵ Es ist klar, dass mit der Einführung der E-ID eine Transitionsphase verbunden sein wird. Es ist jedoch anzunehmen, dass am Ende dieser Phase die "kritische Masse" an Anwendern erreicht ist und das initiale Henne-Ei-Problem "E-ID nicht anwendbar, da zu wenig Nutzer überwunden" ist.

⁹⁶ Am 7.3.2021 hat sich die schweizerische Bevölkerung gegen das BGEID [23] entschieden. Das Bundesamt für Justiz arbeitet zurzeit an einem Aussprachepapier für den Bundesrat bezüglich weiteren Vorgehens in Sachen E-ID. Am 19.5.2021 wurde an der E-ID Initialisierungskonferenz des Verein(s) Schweizerische Städte- und Gemeinde-Informatik (SSGI) ein mögliches Vorgehen für eine interkantonal standardisierte E-ID präsentiert: https://ssgi.ch/media/Initialisierungskonferenz_AGr_eID.pdf

auch einen Identifikator für ein allfälliges NP-Kundenkonto (siehe [Herausforderung-2]).

- o dass die E-ID allen potenziellen Usern, also sowohl In- als auch Ausländern⁹⁷ offensteht.

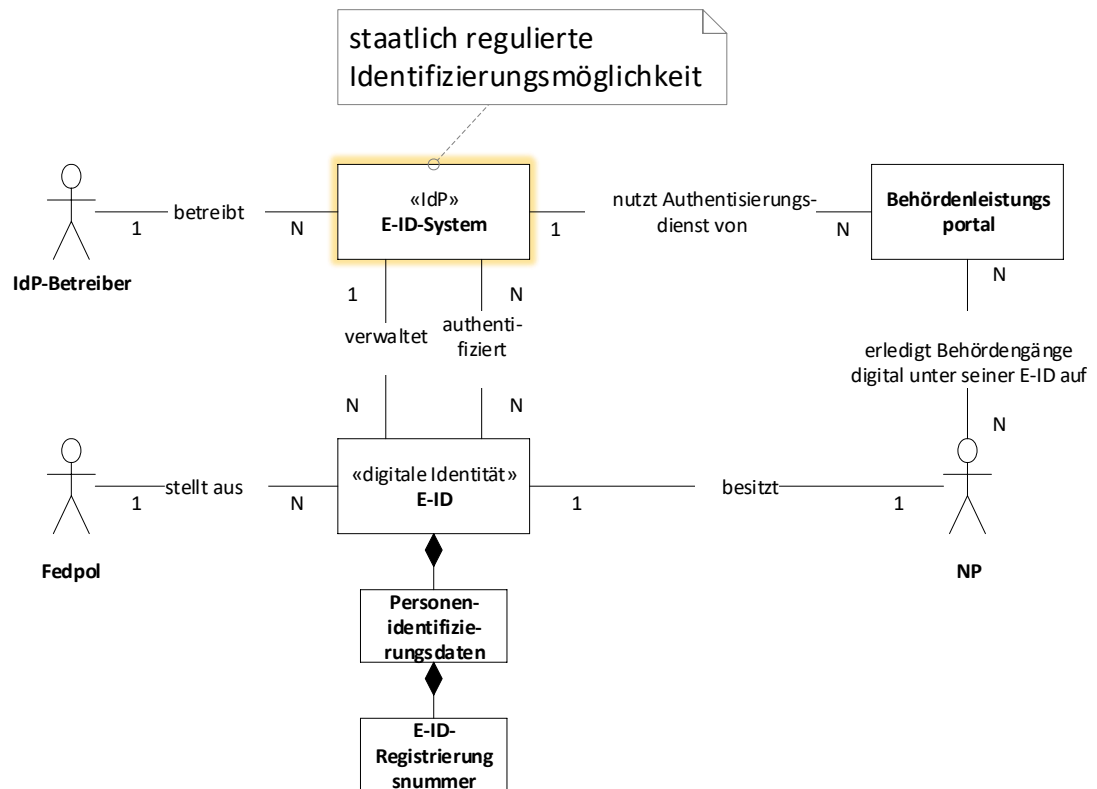


Abbildung 63: Aussagen des BGEID⁹⁸ [23] aus der Strukturperspektive

Darüber hinaus sagt die Botschaft zum Bundesgesetz über elektronische Identifizierungsdienste⁹⁹:

- o Das schweizerische Konzept ist grundsätzlich EU- bzw. eIDAS-konform.
- o In der eIDAS-Verordnung und den entsprechenden technischen Standards werden Rahmenbedingungen spezifiziert, die garantieren, dass die Interoperabilität zwischen den einzelnen länderspezifischen Systemen gewahrt wird. Das Konzept für die E-ID-Systeme nach diesem Gesetz richtet sich nach diesen internationalen Regelungen, sodass die schweizerischen E-ID auch im internationalen Kontext eingesetzt werden könnten. Der

⁹⁷ Die E-ID können auch durch Ausländerinnen und Ausländer beantragt werden, sofern sie zum Zeitpunkt der Ausstellung der E-ID im Besitz eines gültigen, nach Artikel 13 Absatz 1 des Ausländer- und Integrationsgesetzes vom 16. Dezember 2005 anerkannten Ausweispapiers sind oder über eine gültige Legitimationskarte nach der Gaststaatgesetzgebung verfügen, oder deren Identität zum Zeitpunkt der Ausstellung der E-ID in einem besonderen Identifizierungsverfahren verlässlich festgestellt werden konnte.

⁹⁸ <https://www.admin.ch/opc/de/federal-gazette/2019/6567.pdf>

⁹⁹ siehe <https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2018/1524/de/pdf-x/fedlex-data-admin-ch-eli-fga-2018-1524-de-pdf-x.pdf>

hier vorgeschlagene Rahmen für die Anerkennung von E-ID-Systemen und die Anerkennung der IdP ist so ausgestaltet, dass eine spätere gegenseitige Anerkennung der E-ID-Systeme zwischen der Schweiz und der EU (nach der eIDAS Verordnung) oder einzelner EU-Mitglied- oder Drittstaaten (Anm. d. A.: z.B. USA oder Grossbritannien) möglich bleibt. Zur Umsetzung wären Staatsverträge notwendig.

- *Alle Mitgliedstaaten werden verpflichtet, überall dort, wo sie für den Zugang zu Behördendiensten eine E-ID verlangen, auch jede ausländische E-ID aus jedem notifizierten System zuzulassen (Art. 6 eIDAS-Verordnung).*

Es kann also davon ausgegangen werden, dass ein E-ID-System als staatlich regulierte elektronische Identifizierungsmöglichkeit – gemäss diesbezüglicher Staatsverträge - auch ausländische E-ID akzeptieren wird, also miteinander interoperabel sind.

Eine exklusive Nutzung von E-ID-Systemen als staatlich regulierte elektronische Identifizierungsmöglichkeit steht allerdings folgendem Bedürfnis entgegen:











- [B-25] «Gewährleistung ISDS (bezüglich Risiko gläserner Bürger)»: Hier ist zu berücksichtigen, dass sich das Projekt UZ13 mit der Förderung der Nachvollziehbarkeit der Verwendung von persönlichen Daten durch die Verwaltung befasst, wodurch das Vertrauen der Bürger in die Datenhaltung und -verarbeitung gestärkt und somit das Bedürfnis der «Gewährleistung ISDS (bezüglich Risiko gläserner Bürger)» begünstigt wird. Da diese Thematik bereits durch das Projekt UZ13 abgedeckt wird, muss die Entwicklung der Sollarchitektur vorerst nicht weiter darauf eingehen. Allerdings befindet sich UZ13 aktuell erst in der Initialisierungsphase. So ist damit zu rechnen, dass aus den späteren potenziellen UZ13-Ergebnissen noch Anforderungen an die Sollarchitektur entstehen.

Andererseits ist eine exklusive Nutzung einer staatlich regulierten elektronische Identifizierungsmöglichkeit – d.h. eines E-ID-Systems - folgenden Bedürfnissen zuträglich:

- [B-3] «Angebot Basisdienste»: Es werden zukünftig bestehende Basisdienste genutzt.
- [B-6] «Single Sign On»: Eine staatlich regulierte elektronische Identifizierungsmöglichkeit vereinfacht massgeblich die Umsetzung von Single Sign On.
- [B-7] «Mehrere Identitäten verwendbar»: Gemäss BGEID ist es einer NP nicht untersagt, mehrere E-IDs zu unterhalten. Jede E-ID wäre mit je einem Account auf dem Behördenleistungsportal verknüpft und dies mit möglicherweise unterschiedlichen Bewirtschaftungsrechten. In Anbetracht des Ziels des Bundes der Einführung und entsprechenden Förderung einer einheitlichen elektronischen Identität, sowie der Umsetzung des Projekts UZ13, ist fraglich, ob das aufgeführte Bedürfnis nach der Etablierung der E-ID weiter Bestand hat.
- [B-9] «Elektronische Signatur»: Die staatlich regulierte elektronische Identifizierungsmöglichkeit gewährleistet, dass der hinter einer E-ID stehende User auch wirklich die Person ist, die sie vorgibt zu sein. Damit kann grundsätzlich der Bedarf nach einer handschriftlichen Signatur entfallen.
- [B-28] «Wirtschaftlichkeit»: Die exklusive Nutzung einer staatlich regulierten elektronischen Identifizierungsmöglichkeit verringert die Komplexität im

Gegensatz zum gegenteiligen Fall und unterstützt somit das Bedürfnis nach Wirtschaftlichkeit.

Tabelle 24: Evaluation Lösungsvarianten [Herausforderung-1]

	Variante A	Variante B	Variante C
Potential zur Befriedigung der Herausforderung	 Einheitliche IdP-Schnittstelle infolge Standard	 IdP-Vielfalt wird durch einen Vermittlerdienst gekapselt.	  Infolge Interoperabilität der E-ID muss nur die Schnittstelle zu einem IdP realisiert werden. Darüber hinaus bieten sich mehrere Zusatznutzen.
Wirtschaftlichkeit	 Aufgrund Eigenkreation tief, keine Nachnutzung.	 Nachnutzung etablierter Services	 Nutzung einer gegebenen Infrastruktur. Es muss nur mit einem IdP zusammengearbeitet werden.
Machbarkeit	 Aufgrund Eigenkreation und Komplexität unsicher.	 Gut, da auf etablierte Services gesetzt wird.	 Gut, da auf eine gesetzliche Grundlage aufgebaut wird. Jedoch ist mit einer nicht zu vernachlässigenden Transitionsphase zur Einführung und Etablierung der E-ID zu rechnen.
Auswirkung auf Sollarchitektur	Ausarbeitung und Etablierung neuer Standards.	Behandlung der Einbindung eines Vermittler-Services.	Behandlung der Einbindung eines IdPs.
Zusammenfassende Beurteilung	Gegenüber den anderen Varianten mit vielen Unsicherheiten und erheblichen Mehraufwänden verbunden.	Durchwegs positive Evaluation.	Insgesamt positive Evaluation, darüberhinaus Zusatznutzen.

Empfehlung: Im Ergebnis der Evaluation scheidet Variante A im Einklang mit Architekturprinzip [P-1] (Nachnutzung vor Eigenkreation) aus. Variante B und Variante C erscheinen zwar in der Evaluationstabelle zunächst fast gleichwertig, aber gemäss Architekturprinzip [P-7] (Unterstützung Vorhaben des Bundes), sowie den aufgeführten Zusatznutzen, ist Variante C zu bevorzugen.

Entscheid¹⁰⁰: Variante C wird umgesetzt.

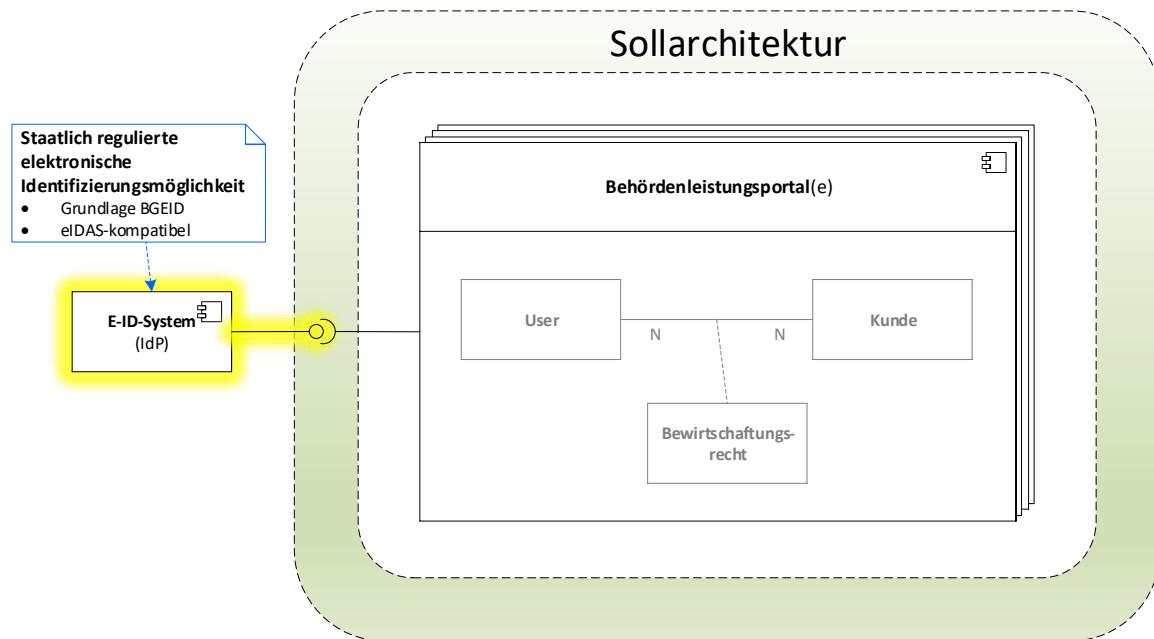


Abbildung 64: Die Nutzung eines E-ID-Systems als staatlich regulierte elektronische Identifizierungsmöglichkeit ist ein Schlüsselement der Sollarchitektur

Konsequenz des Entscheides: Der Besitz einer E-ID ist für User eine Voraussetzung zur Nutzung von E-Government Angeboten in Portalen, die auf der vorliegenden Architektur basieren. Im Umkehrschluss bedeutet dies, dass Personen, die nicht im Besitze einer E-ID sind, von der Nutzung von E-Government Angebote auf solchen Portalen als User ausgeschlossen wären. Diese Beschränkung wurde unter Berücksichtigung des Ergebnisses der Lösungsvarianten Evaluation, sowie dem Architekturprinzip [P-8], bewusst in Kauf genommen.

Hinweise:

- Der im BGEID Art. 12 Absatz 2 vorgesehene Fall "Alternativer Zugang bei Sicherheitsniveau *niedrig* ohne E-ID" wird im Kapitel 2.5.1.1 behandelt. In diesem Fall wird nur eine eingeschränkte Funktionalität gefordert.
- Transitionsfragen⁹⁵ bezüglich der Verfügbarkeit von E-ID-Systemen als staatlich regulierte elektronische Identifizierungsmöglichkeit sind noch zu klären.

[Herausforderung-2] Gemäss [REQ-1] braucht es für NP und JP jeweils einen für Behördenleistungen nutzbaren Kunden-Identifikator, die möglichst von entsprechenden Registerdiensten unterstützt werden.

¹⁰⁰ siehe Annexe G.E

Für den JP-Bereich besteht die Lösung der Herausforderung bereits mit der gesetzlich verankerten UID¹⁰¹ und dem dazu gehörigen Register¹⁰², welches vom BFS betrieben wird und einen Webservice umfasst, der für Portale maschinelle Abfragen gemäss der Standards eCH-0097, eCH-0098, eCH-0108 und eCH-0116 ermöglicht. Diese Standards wurden kürzlich überarbeitet (publiziert 26.11.2020, Implementierung im UID-System per Ende 2022), infolgedessen die UID allen potenziellen JP-Kunden offen steht¹⁰³.

Die Frage ist, wie eine analoge Lösung für den NP-Bereich im Einklang mit dem bei [Herausforderung-1] getroffenen Entscheid für die E-ID als staatlich regulierte elektronische Identifizierungsmöglichkeit aussehen kann.

Lösungsansätze:

- (A) Verwendung der vom BGEID [23] vorgesehenen E-ID-Registrierungsnummer als NP-Kundenidentifikator. Gemäss BGEID Art. 21 darf diese von E-ID-verwendenden Diensten (darunter würden Behördenleistungsportale fallen) zur Identifizierung von Personen verwendet werden und ist auch gemäss Art. 22 von Behörden zu akzeptieren. Damit würde auch die eigenhändige¹⁰⁴ Eröffnung eines NP-Kundenkontos erleichtert: Da der digitalen Identität E-ID die E-ID-Registrierungsnummer als Attribut anhängt, kann für diese Registrierungsnummer das NP-Kundenkonto ohne weiteren Nachweis eröffnet werden. Dies da verbürgt ist, dass die hinter der digitalen Identität stehende Person tatsächlich die ist, auf die sich das Kundenkonto beziehen soll. Dies gilt gleichermassen für die Bewirtschaftung des NP-Kundenkontos: Ein User erhält für sein NP-Kundenkonto, d.h. welches auf die mit der E-ID-Identität verknüpften E-ID-Registrierungsnummer geführt wird, automatisch Administrationsrechte. (Zusätzlich kann er/sie natürlich anderen Usern Bewirtschaftungsrechte erteilen.) Allerdings gibt es keine Aussicht auf ein auf der E-ID-Registrierungsnummer basierendes NP-Register. Die Vorgaben des Bundes bezüglich eines NP-Registers basieren auf der Versichertennummer (siehe Variante (B)). Allerdings kann ein E-ID-Identitätsdienst die der E-ID hinterlegten Identitätsmerkmale wie Namen, Vornamen, Geburtsdatum, Geschlecht, Geburtsort, Staatsangehörigkeit und AHV-Nummer liefern. Das sind aber vergleichsweise nur wenig Informationen und nur im Falle der eigenhändigen¹⁰⁴ Eröffnung/Bewirtschaftung eines NP-Kundenkontos von Belangen.
- (B) Verwendung der Versichertennummer (AHV-Nummer). Die Versichertennummer wird heute insbesondere in den Sozialversicherungen als Personenidentifikator verwendet. Mit der Anpassung des AHV-Gesetzes¹⁰⁵ dürfen Behörden im Rahmen ihrer gesetzlichen Aufgaben neu generell die AHV-Nummer verwenden. In der Regel verfügen

¹⁰¹ Bundesgesetz über die Unternehmens-Identifikationsnummer <https://www.admin.ch/opc/de/official-compilation/2010/4989.pdf>

¹⁰² UID-Register@BFS <https://www.uid.admin.ch/>. Der UID-Webservice umfasst u.a. die Funktionen Unternehmen (bzw. UID-Einheit) suchen, Detaildaten abfragen, Unternehmen registrieren/mutieren/löschen.

¹⁰³ Nunmehr können auch ausländischen Unternehmen eine UID beantragen, wobei sie ihre nationale ID angeben müssen.

¹⁰⁴ Eigenhändig bedeutet, dass die hinter User und Kunde stehende NP identisch ist. Dies ist im Gegensatz dazu bei einer treuhänderischen Eröffnung/Bewirtschaftung eines Kundenkontos nicht der Fall. Deshalb ist bei einer treuhänderischen Eröffnung ein Onboardingprozess - analog wie bei JP - nötig.

¹⁰⁵ Siehe <https://www.fedlex.admin.ch/eli/fga/2020/2693/de>

potenzielle NP-Kunden über eine Versichertennummer¹⁰⁶. Ausnahmen ergeben sich in folgenden Fällen:

- Wenn die Versichertennummer erst im Verlaufe des Verfahrens zugeteilt wird und deshalb bei der Gesuchstellung noch nicht vorliegt (z.B. bei der Gesuchstellung für eine Arbeitsbewilligung eines Ausländers)
- oder bei Aufenthalts- und Grenzgängerbewilligungen für Aufenthalte unter 4 Monaten sowie Kurzaufenthaltsbewilligungen¹⁰⁷.

Analog zu Variante (A) ist eine eigenhändige Eröffnung¹⁰⁴ bzw. Bewirtschaftung eines NP-Kundenkontos ohne weiteren Nachweis möglich, da ein Portal analog Variante (A) die Versichertennummer vom E-ID-Identitätsservices als verbürgtes Attribut abfragen kann. Im Gegensatz zur Variante (A) gibt es bei Variante (B) jedoch die Möglichkeit eines Registers in Form der von der ZAS betriebenen UPIServices¹⁰⁸. Dieser Webservice ermöglicht auf der Versichertennummer basierende Abfragen auf die in der UPI-Datenbank gespeicherten Identitätsmerkmale (Name, Vorname, Geburtsdatum, ...). Allerdings kann diese keine Adressdaten liefern. Das ist vielmehr Aufgabe des zukünftigen zentralen Referenzdatensystems¹⁰⁹ Nationaler Adressdienst (NAD)¹¹⁰ bzw. Gegenstand des Projekts UZ10¹¹¹ im Umsetzungsplan 2021-2023 von E-Government Schweiz [19]. Der NAD basiert ebenfalls auf der Versichertennummer und bezieht die Adressdaten von den zahlreichen Meldeämtern und ZEMIS, wobei der Bezug mindestens 4x jährlich erfolgen soll. Im Unterschied zum öffentlichen UID-Webservice¹¹² stehen die Services von UPI und NAD jedoch nur Behörden zur Verfügung.

- (C) Weitere Identifikatoren, wie kantonale oder ausländische zulassen. Bei der Eröffnung eines NP-Kundenkontos braucht es jedoch dabei in jedem Fall einen Onboardingprozess, da diese Angaben durch das Portal nicht nachprüfbar sind. Weiterhin ist - und wird nach aller Wahrscheinlichkeit - für diese Identifikatoren kein allgemeines Register verfügbar sein.

Tabelle 25: Evaluation Lösungsvarianten [Herausforderung-2]

¹⁰⁶ Die AHV-Nummer wird jeder in der Schweiz wohnhaften Person oder jeder Person, deren gewöhnlicher Aufenthalt sich in der Schweiz befindet, zugeteilt. Ausserdem wird sie auch an Personen zugeteilt, die im Ausland wohnhaft sind und Beiträge bezahlen oder Leistungen beziehen. Falls erforderlich können Anträge zur Zuteilung der AHV-Nummer sowohl von Organen, welche die AHV durchführen wie auch von systematischen Benutzern, die zur Nutzung der AHV-Nummer berechtigt sind, auch ausserhalb der AHV beantragt werden (siehe ¹⁰³ bzw. https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/cc/63/837_843_843/20210101/de/pdf-a/fedlex-data-admin-ch-eli-cc-63-837_843_843-20210101-de-pdf-a.pdf). Wer letztlich alles eine AHV-Nummer zugeteilt bekommt, ist in ¹⁰⁵ klar umrissen.

¹⁰⁷ Siehe https://www.zas.admin.ch/dam/zas/de/dokumente/Partenaires%20et%20institutions/NAVS13/Attribution-du-NAVS13-circonstances_D.pdf.download.pdf/Attribution-du-NAVS13-circonstances_D.pdf










¹⁰⁸ Siehe <https://www.zas.admin.ch/zas/de/home/partenaires-et-institutions/-unique-person-identification--upi-/upiservices.html>

¹⁰⁹ Siehe <https://www.egovernment.ch/de/dokumentation/rechtliche-fragen/register/personenregister/>

¹¹⁰ Siehe <https://www.bfs.admin.ch/bfs/de/home/register/nationaler-adressdienst.html>

¹¹¹ Siehe <https://www.egovernment.ch/de/umsetzung/umsetzungsziele/nationaler-adressdienst/>

¹¹² Die Bekanntgabe der Daten über den öffentlichen UID-Webservice unterliegt den Bestimmungen von Art. 11 UIDG

	Variante A	Variante B	Variante C
Potential zur Befriedigung der Herausforderung	 Da die Nutzung der E-ID-Registrierungsnummer freiwillig ist, wird sie nicht so stark verbreitet sein wie die Versichertennummer. Andererseits kann jeder eine E-ID bekommen, d.h. auch Ausländer ohne Aufenthaltsstatus. Es besteht kein nationales NP-Register, welches auf der E-ID-Registrierungsnummer basiert.	 Eine grosse Mehrheit der Schweizer Portalnutzenden ist im Besitze der Versichertennummer ¹⁰⁶ . Diese ist in der Verwaltung weit verbreitet. Andererseits ist sie bei Ausländern nicht immer verfügbar ¹⁰⁷ . Zudem sollen mit dem erwähnten UPI-Register bzw. Nationalen Adressdienst auf der Versichertennummer basierende Referenzdienste zur Verfügung stehen.	 Diese Variante schliesst kein Kundensegment aus. Allerdings führt sie zu einer hohen Heterogenität in Bezug auf die verwendeten Indikatoren. Es besteht kein nationales NP-Register, welches auf weiteren Identifikatoren, wie der Versichertennummer, basiert, zur Verfügung steht.
Wirtschaftlichkeit	 Vorhandenes Identifikationsmerkmal der E-ID des Users	 Weitverbreiteste Identifikationsnummer. Zudem ist zusammen mit der Verwendung des E-ID Service für Portale mit systematischer Verwendung der Versichertennummer die Überprüfung des Identifikators sichergestellt.	 Starke Heterogenität führt zu einem hohen Aufwand, zusätzlich ist ein Onboardingprozess notwendig. Zusatznutzen zu Verwendung der Varianten A und B begrenzt.
Machbarkeit	 Vorhandenes Identifikationsmerkmal der E-ID des Users	 Da bereits vielen Fachsystemen bekannt und durch diese genutzt, kein grosser Aufwand zur Einführung. Mit der Gesetzesanpassung weiter gefördert und verbreitert.	 Machbar, jedoch führt eine starke Heterogenität zu einem hohen Aufwand
Auswirkung auf Sollarchitektur	Behandlung der E-ID-Registrierungsnummer als Identifikator	Behandlung der Versichertennummer als Identifikator	Behandlung einer Beispiel-ID als Identifikator.
Zusammenfassende Beurteilung	Die E-ID-Registrierungsnummer ist integraler Bestandteil des E-ID-Services, welcher als Identitätsprovider genutzt wird.	Die Versichertennummer ist der weitverbreiteste und genutzte Identifikator der Schweiz. Die Akzeptanz ist entsprechend hoch, die Hürden zur Nutzung entsprechend tief. Zudem gibt es auf der Versichertennummer basierende	Allenfalls sind für einige Portale neben der Identifikatoren der Varianten A und B weitere notwendig. Die Integration ist jedoch mit einem entsprechenden Mehraufwand verbunden.

Infrastrukturdienste bzw. sind
in Planung.

Empfehlung: Die Versichertennummer (B) soll - wenn immer möglich - als zwingenden, interoperablen NP-Kundenidentifikator unterstützt werden. Dies kann bei in der Schweiz wohnhaften NP angewendet werden. Die E-ID-Registrierungsnummer (A) (und allenfalls auch die Registrierungsnummer einer ausländischen eIDAS-kompatiblen E-ID) soll als optionaler Kundenidentifikator zum Zuge kommen, wenn der NP (noch) keine AHV-Nr zugeteilt wurde. Das betrifft z.B. Ausländer ohne Aufenthaltstitel. Dadurch kompensieren sich Vor- und Nachteile der beiden Identifikatorsysteme gegenseitig. Zusätzlich können weitere Identifikatoren (C) hinterlegt werden (z.B. Partner-ID der ESTV für die Verrechnungssteuer von Ausländer, ZEMIS-NR. des SEM für Erstanträge von Arbeitsbewilligungen). In letzterem Fall ist allerdings keine Interoperabilität möglich, d.h. die Leistung kann nur im primären Portal bezogen werden.

Auf Basis der Versichertennummer (AHVN13) werden die Infrastrukturdienste UPI und NAD zur Verfügung stehen, mit dessen Hilfe Behördenleistungsportale Stammdaten von NP-Kunden abgleichen können. Bei Bedarf kann ein Portal die Versichertennummer des E-ID-Identitätsservice als verbürgtes Attribut abfragen. Die Identifikation von nicht in der Schweiz wohnhaften NP erfolgt über die E-ID-Registrierungsnummer.

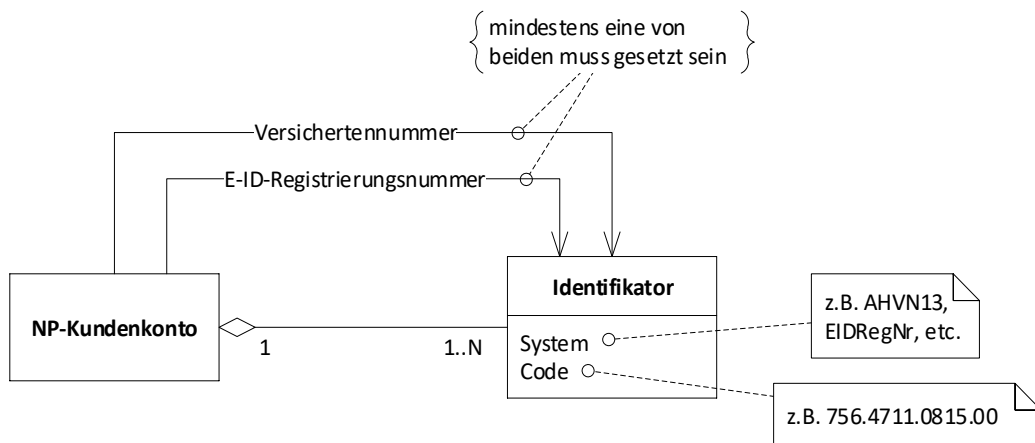


Abbildung 65: In einem NP-Kundenkonto können mehrere Identifikatoren hinterlegt werden, mindestens jedoch die Versichertennummer, optional die E-ID-Registrierungsnummer

Tabelle 26: Entscheidungsbaum bezüglich der Verfügbarkeit von Versichertennummer und/oder E-ID-Registrierungsnummer zur Verwendung als Identifikator bei der Eröffnung eines NP-Kundenkontos

Situation NP-Kunde mit der hinter dem User stehenden Per- son identisch?	in der Schweiz ge- meldet?	Verfügbarer Identifikator für Eröffnung NP-Kunden- konto		Kommentar
		Versicher- ten-num- mer	E-ID-Regist- rierungs- nummer	
Ja (eigenhändige Er- öffnung)	Ja	Ja	Ja	
	Nein	Nein	Ja	
	Ja	Ja	Evtl.	

Nein (treuhänderische Eröffnung)	Nein	Nein	Evtl.	Eröffnung nicht möglich, sofern NP-Kunde keine E-ID hat
----------------------------------	------	------	-------	---

Entscheid¹⁰⁰: Variante (B) wird umgesetzt und zwingend für Kunden, welche in der Schweiz wohnhaft sind. Varianten (A) und (C) je nach Wohnort (CH oder Ausland) des Kunden optional.

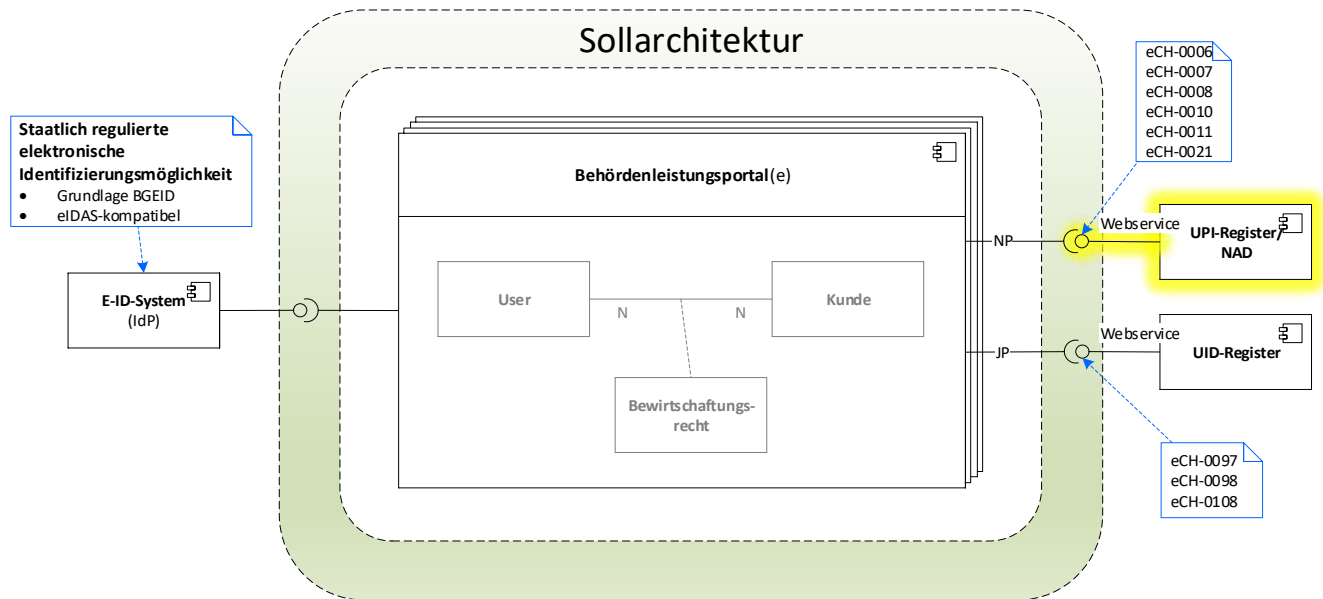


Abbildung 66: Die Nutzung des UPI-Registers und des entstehenden NAD für NP ist neben dem existierenden UID-Register für JP ein weiteres Schlüsselement der Sollarchitektur

[Herausforderung-3] Kapitel 2.5.1.3.2 sieht eine portalübergreifende Übertragbarkeit von Bewirtschaftungsrechten vor, die für das Integrationsmuster 'Einbindung' eine essenzielle Bedeutung hat. Dabei soll die Änderung eines Bewirtschaftungsrechts, die auf einem Portal vorgenommen wurde, sofort auf allen betroffenen Portalen wirksam werden. Es darf im Bereich der Bewirtschaftungsrechte zwischen verschiedenen Portalen keine Inkonsistenz geben. Aufgrund der verteilten Verantwortlichkeiten zwischen den verschiedenen Portalen kann die gegenseitige Akzeptanz von der Sollarchitektur nicht einfach vorgegeben werden.

Lösungsansätze:

- (A) Peer-to-Peer Trust: Standard zum Einrichten und Betrieb einer Vertrauensbeziehung zwischen 2 Portalen kreieren (prozessuale und technische Komponente). Dazu ist wahrscheinlich eine juristische Grundlage nötig.

- (B) Zentraler Infrastrukturdienst: Etablierung eines Service, der portalübergreifend die Bewirtschaftungsrechte¹¹³ für die Kundenkonten managt. Ein solcher Infrastrukturdienst fungiert für Behördenleistungs-portale als zentrale Rechteverwaltung (siehe Abbildung 67), indem er eine Schnittstelle mit Funktionen/Methoden nach diesem exemplarischen Muster anbietet:
 - Bewirtschaftungsrecht abfragen
 - Bewirtschaftungsrecht verwalten
 - Create (allenfalls in Verbindung mit einem Onboarding-Prozess)
 - Update
 - Delete

Diese Methoden wären mit folgenden Eingangsparametern verbunden:

- Identifikator der digitalen Identität
- Kundenidentifikator
- Identifikator der Behördenleistung

Die Datenhoheit über die (Kunden-)Bewirtschaftungsrechte liegt bei der zentralen Rechteverwaltung. Für den Portal-User bleibt diese Tatsache jedoch verborgen, denn die Verwaltung der Bewirtschaftungsrechte bezüglich eines bestimmten Kundenkontos durch einen von diesem Kunden bevollmächtigten User kann von irgendeinem Portal erfolgen. Aus dieser Sicht handelt es sich scheinbar um eine dezentrale Verwaltung, tatsächlich erfolgt dies aber unter der Haube zentral. Somit ist gewährleistet, dass die Rechteverwaltung in Verantwortung des jeweiligen Kunden geschieht. Dies gilt ungeachtet dessen, ob der zentrale Infrastrukturdienst für die Verwaltungsfunktionen eine API oder eine ins Portal einbindbare UI anbietet.

Per Status quo gibt es bereits Systeme, die die genannten Anforderungen unterstützen. Beispiele sind:

- PAMS¹¹⁴ vom BIT. Dieser als Microservice angebotene Dienst arbeitet eng mit dem IdP-Vermittlerdienst eIAM zusammen, da PAMS die Identitäten von eIAM bezieht. Sowohl eIAM als auch PAMS stehen als Standardservice des BITs Bund, Kantonen und Gemeinden zur Verfügung.
- IAM-System der ALV. Dieses arbeitet ebenfalls mit eIAM zusammen.







Beide stellen IAM-Systeme mit einem Vermittler im Sinne von Abbildung 62 und einer angeschlossenen Rechteverwaltung dar.

Tabelle 27: Evaluation Lösungsvarianten [Herausforderung-3]

Variante A	Variante B
------------	------------

¹¹³ Die Begriffsbestimmung "Bewirtschaftungsrecht" wurde in Kapitel 2.1.5 vorgenommen.

¹¹⁴ Polymorphic Access Management System, siehe https://www.eiam.admin.ch/pages/fl/eiamglossary!pub_de.html?&l=de&l=de#d139

Potential zur Befriedigung der Herausforderung	 Standard schafft klare Rahmenbedingungen	 Löst das Problem der Herausforderung im Kern ¹¹⁵
Wirtschaftlichkeit	 Rahmenbedingung verringert Initialaufwand seitens Portalbetreiber. Im Vergleich zu B hoher Initialaufwand.	 Nutzung einer zentralen Verantwortlichkeit entlastet Portalbetreiber. Die Betriebskosten werden über alle nutzenden Portalbetreiber verteilt.
Machbarkeit	 Machbar. Durchsetzung/Akzeptanz des Standards jedoch nicht garantiert.	 Es bestehen bereits geeignete IAM-Systeme.
Auswirkung auf Sollarchitektur	Ausarbeitung und Etablierung neuer Standards.	Evaluation eines Infrastrukturdienstes und dessen Einbindung in die Sollarchitektur
Zusammenfassende Beurteilung	Neuer Standard muss erarbeitet werden, Akzeptanz nicht garantiert. Widerspricht Architekturprinzip Nachnutzung vor Eigenkreation.	Die Aufgabe des zentralen Infrastrukturdienstes kann ein bestehendes IAM-System erfüllen.

Empfehlung: Im Sinne von Variante B im Rahmen der Studie Anforderungen an ein IAM-System spezifizieren und als zentrale Infrastrukturkomponente in die Sollarchitektur integrieren (siehe Abbildung 68). Die Aufgabe zur Umsetzung, d.h. Evaluation und Betrieb eines geeigneten zentralen IAM-Systems bei der Digitalen Verwaltung Schweiz¹¹⁶ (DVS) platzieren.

Zusatznutzen: Ein IAM-System mit einer Vermittlerkomponente wie eIAM an Bord kann die E-ID-Transitionsphase⁹⁵ unterstützen, da es die Frage des Identifizierungssystems kapselt.

Entscheid¹⁰⁰: Variante (B) wird umgesetzt.

¹¹⁵ Eine direkte Anmeldung auf Provider-Portal führt zum selben Userkonto wie via Weiterleitung vom Consumer-Portal

¹¹⁶ <https://www.egov.ch/de/umsetzung/umsetzungsziele/aufbau-der-organisation-digitale-verwaltung-schweiz-dvs/>

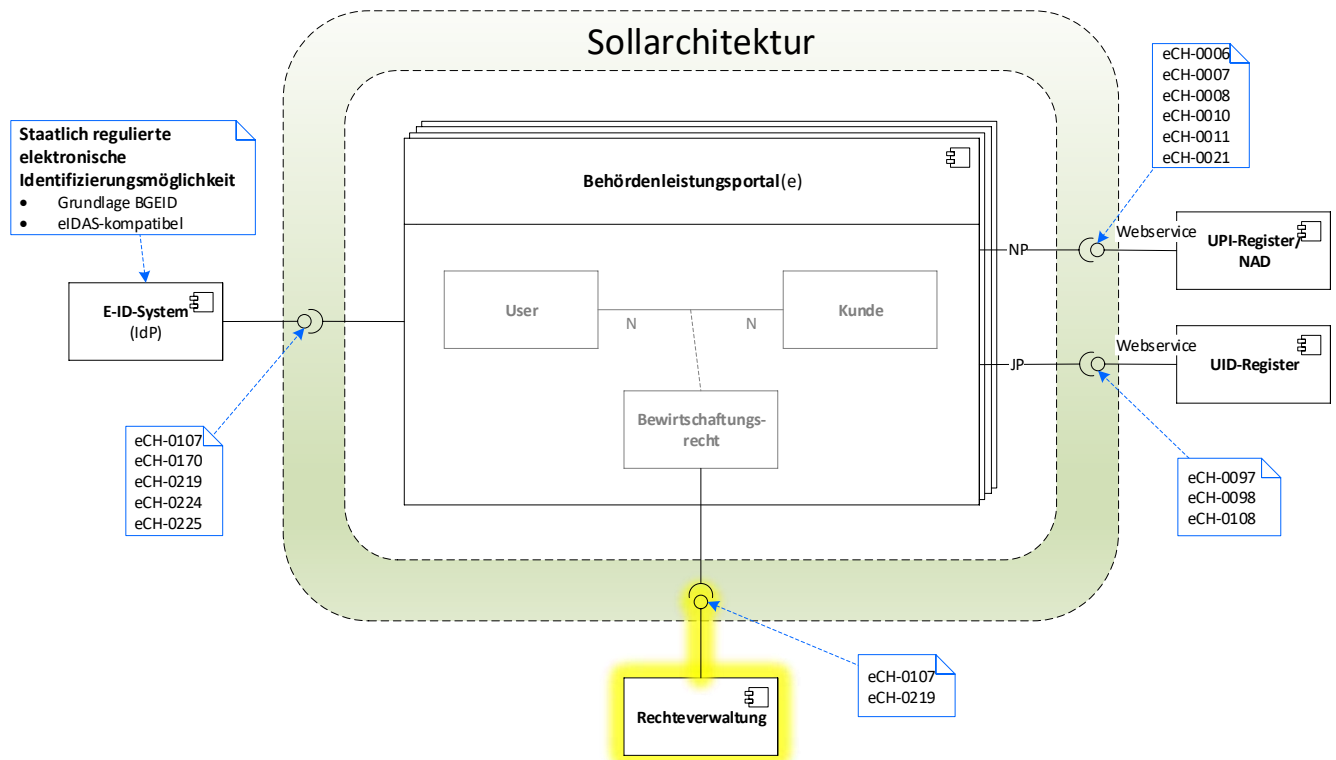


Abbildung 67: Die Nutzung eines zentralen Infrastrukturdienstes für die Verwaltung der Bewirtschaftungsrechte ist ein weiteres Schlüsselement der Sollarchitektur

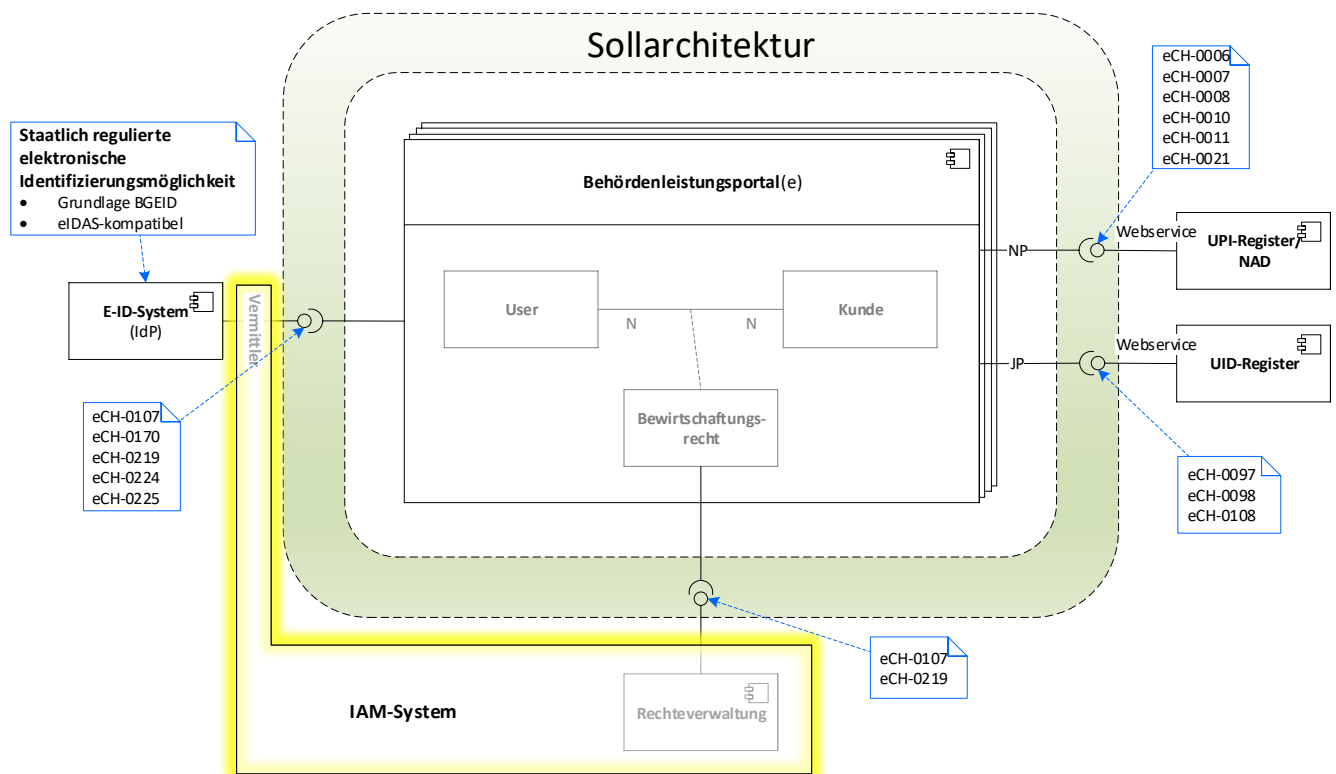


Abbildung 68: Ein geeignetes IAM-System kann die Aufgabe der zentralen Rechteverwaltung übernehmen und bringt darüber hinaus noch einen Vermittler ins Spiel

[Herausforderung-4] Bei der Formulierung des unter 2.5.1.1.6.3 geforderten portalübergreifenden Bewirtschaftungsrechtemodells stellt sich die Frage, inwieweit dabei individuelle Anforderungen von einzelnen Portalen oder Behörden berücksichtigt werden können (z.B. von der kantonalen Amtsstelle X oder der Gemeinde Y). Wenn man allen individuellen Anforderungen gerecht werden will, wird vermutlich eine so hohe Komplexität entstehen, die das Bewirtschaftungsrechtemodell zu schwerfällig und damit unpraktikabel werden lässt.

Lösungsansätze:

- (A) Anwendung eines Schalenmodells:
 - Von Sollarchitektur definierter portalübergreifender interoperabler Bereich
 - Übergreifend definierter, behördenleistungsspezifischer Bereich der nur im Kontext einer bestimmten Behördenleistung interoperabel ist. Die diesbezügliche Verantwortlichkeit müsste pro Behördenleistung von den betreffenden Fachstellen gesamthaft wahrgenommen werden.
 - Individueller Bereich in bilateraler Verantwortung zwischen Betreiber und Behörde

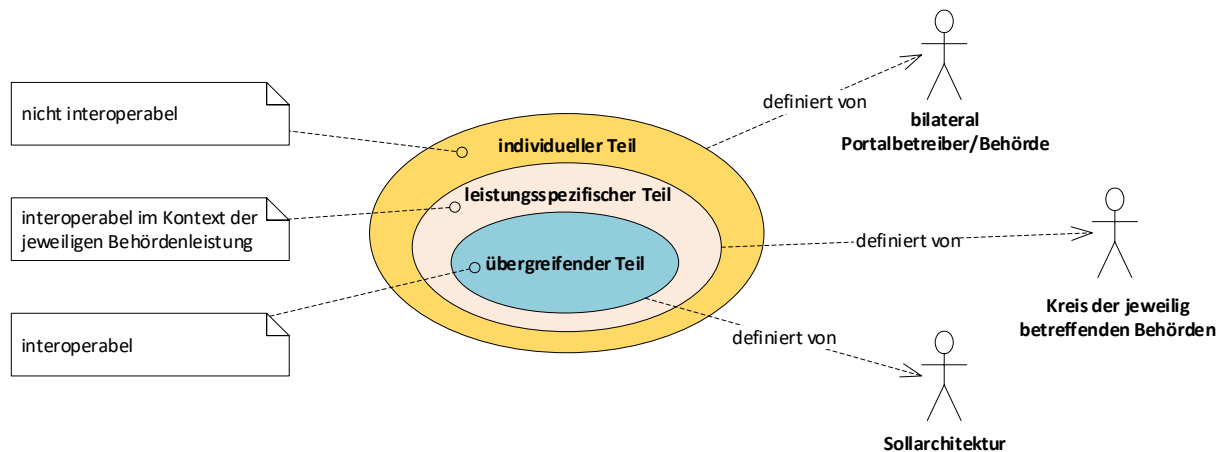


Abbildung 69: Muster eines Schalenmodells für ein Bewirtschaftungsrechtemodell

- (B) Anwendung eines weiteren Schalenmodells, wobei nur ein geregelter und ein nicht geregelter Teil unterschieden wird. Für den nicht geregelten Teil wird ein auf dem geregelten Teil aufbauendes Metamodell vorgegeben, um eine Ordnung herzustellen. Die Semantik selbst ist derweil frei wählbar.

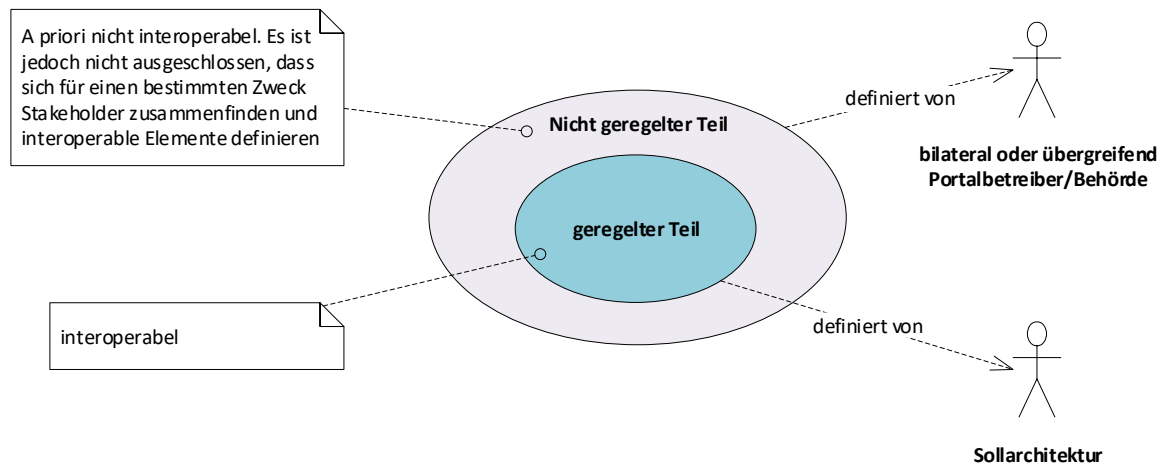


Abbildung 70: Muster eines Berechtigungsmodells mit einem geregelten und einem ungeregelten Teil

Bei beiden Varianten sind relevante Standards/Referenzkataloge wie der eCH-0070 (Leistungsinventar eGov CH) zur Identifikation von Leistungen einzubeziehen.

Tabelle 28: Evaluation Lösungsvarianten [Herausforderung-4]

	Variante A	Variante B
Potential zur Befriedigung der Herausforderung	😊 Einheitliche Basis infolge Standard, auf der individuelle Lösungen gedeihen können	😊 Einheitliche Lösung infolge Standard
Wirtschaftlichkeit	😞 Aufgrund Eigenkreation per se tief, keine Nachnutzung.	😞 Aufgrund Eigenkreation per se tief, keine Nachnutzung.
Machbarkeit	😞 Aufgrund höherer Komplexität schwieriger als (B). Abgrenzung zwischen leistungsspezifischen und individuellem Teil in der Praxis kaum durchsetzbar	😊 Erscheint im Vergleich zu (A) einfacher, da weniger Abstraktionsebenen.
Auswirkung auf Sollarchitektur	Ausarbeitung und Etablierung eines Standards.	Ausarbeitung und Etablierung eines Standards.
Zusammenfassende Beurteilung	Neuer Standard muss erarbeitet werden. Aufgabe erscheint komplexer als bei (B).	Neuer Standard muss erarbeitet werden. Aufgabe erscheint einfacher als bei (A).

Empfehlung: Variante (B) ist zu bevorzugen, da deren Lösung einfacher erscheint. Im Sinne des Architekturprinzips "Nachnutzung vor Eigenkreation" soll dabei auf relevante Standards/Referenzkataloge wie der eCH-0070 (Leistungsinventar eGov CH) aufgebaut werden.

Entscheid¹⁰⁰: Variante (B) wird umgesetzt.

[Herausforderung-5] Die Bedürfnisse [B-13] und [B-25] sowie die enorme Vielzahl an potentiellen behördeninternen Fachsystemen setzen ein Transportsystem voraus, das Daten zielgerichtet an bestimmte portalseitige Empfänger geschützt und sicher¹¹⁷ übermitteln kann.



Abbildung 71: Geschütztes Transportsystem für den zielgerichteten Datenaustausch bzw. die bidirektionale Kommunikation zwischen Behördenleistungsportalen und behördeninternen Fachsystemen

Hinweis: Diese Herausforderung betrifft die Schnittstelle Behördengang↔Geschäftsfallbearbeitung (siehe 2.5.1.2) und nicht den Datenaustausch zwischen Portalen. Dieser Schnittstelle liegt aus Prozesssicht ein asynchroner Nachrichtenaustausch zugrunde. Die Herausforderung kann ausserdem die Schnittstelle zwischen Portal-Fachanwendung und behördeninternem Fachsystem betreffen, allerdings ist auf dieser Stufe eine Interoperabilität in der Regel nicht notwendig, da beide Komponenten oft innerhalb der gleichen Behörde angesiedelt sind und somit tendenziell proprietäre Schnittstellen eingesetzt werden (z.B. SAP).

Das geschützte Transportsystem zielt in erster Linie darauf ab, Meldungen im Zusammenhang mit Behördengängen zwischen Portal und behördeninternem Fachsystem sicher und bidirektional zu übertragen. Dies auf eine synchrone oder asynchrone Art und Weise. Es können aber durchaus weitere Anwendungsfälle in Betracht gezogen werden, sodass das geschützte Transportsystem als allgemeingültiges Medium für den Austausch von Daten zwischen Portal und behördeninternem Fachsystem betrachtet werden kann.

Lösungsansätze:

- (A) Zentraler Infrastrukturdienst: Ein zentraler Infrastrukturdienst übernimmt die Vermittlerrolle zwischen dem Portal und dem behördeninternen Fachsystem für den sicheren Austausch von Daten. Dabei werden diverse Aspekte vor und während des Datenaustauschs geregelt: Kommunikationsmatrix (welche Systeme dürfen untereinander kommunizieren), wie muss die Authentisierung erfolgen (z.B. OAuth), nach welchem Muster erfolgt der Datenaustausch (z.B. synchron vs. asynchron), welche Datenformate

¹¹⁷ Die diesbezüglichen ISDS-Anforderungen werden im Kapitel 2.5.2 geklärt.

(z.B. XML) und -protokolle (z.B. sFTP) werden angewendet, etc. Folgende Möglichkeiten sind für diesen Zweck denkbar, sind hier aber lediglich als Beispiele aufgeführt und nicht abschliessend:

- Sedex: Sedex steht für secure data exchange und ist eine Dienstleistung des Bundesamts für Statistik BFS. Die Plattform ist für den sicheren asynchronen Datenaustausch zwischen Organisationseinheiten konzipiert. Sedex erfüllt die umfangreichen Anforderungen an ein sicheres Transportmedium im Bereich eGovernment. In spezifischen Fällen erfolgt auch ein synchroner Datenaustausch¹¹⁸. Die Plattform ist hochverfügbar (99.8%), genügt hohen Anforderungen an die Sicherheit sowie Nachvollziehbarkeit und wird von über 6'800 Organisationseinheiten für die Datenübermittlung verwendet. Im Jahr 2018 wurden ca. 17.6 Millionen Meldungen via sedex übermittelt. Sedex wird fortlaufend weiterentwickelt, die aktuelle Client Software wurde im August 2020 veröffentlicht¹¹⁹. Für die Nutzung von Sedex für den vorliegenden Zweck müssten allenfalls gewisse Elemente weiterentwickelt werden. Sedex hat gewisse Einschränkungen, insbesondere in Bezug auf Supportzeiten und der Flexibilität bei der Weiterentwicklung.
- Enterprise Service Bus (ESB): Ein Enterprise Service Bus besteht aus einem Kommunikationsbus, über den Nachrichten ausgetauscht werden können. Dienste verbinden ihre Dienstschnittstellen über Endpunkte mit dem Bus. Dienstanutzer kommunizieren mit einem Dienstanbieter, indem sie mit dem Dienstanbieter über den Bus Nachrichten austauschen. Ein API-getriebener ESB stellt Anbietern und Nutzern plattformsspezifische Schnittstellen (z.B. REST-APIs) zur Verfügung, um Services zu implementieren und aufzurufen.

In der Bundesverwaltung wird beispielsweise im Rahmen von FISCAL-IT von der ESTV eine ESB-Infrastruktur auf Basis eines API Gateways der Firma WSO eingesetzt, der für REST-basierte Zugriffe geeignet ist. Der Bus übermittelt Nachrichten zwischen den angeschlossenen Systemen in Form von GDC-XML Dokumenten. Insofern ist XML die «native» Sprache des ESB. Es wird kein SOA-Ansatz verwendet, sondern eine Architektur mit Micro Services, welche für Web-Lösungen sehr viel besser geeignet ist.

¹¹⁸ siehe <https://www.bfs.admin.ch/bfs/de/home/register/personenregister/sedex/synchron.html>

¹¹⁹ Siehe <https://www.bfs.admin.ch/bfs/de/home/register/personenregister/sedex.html>

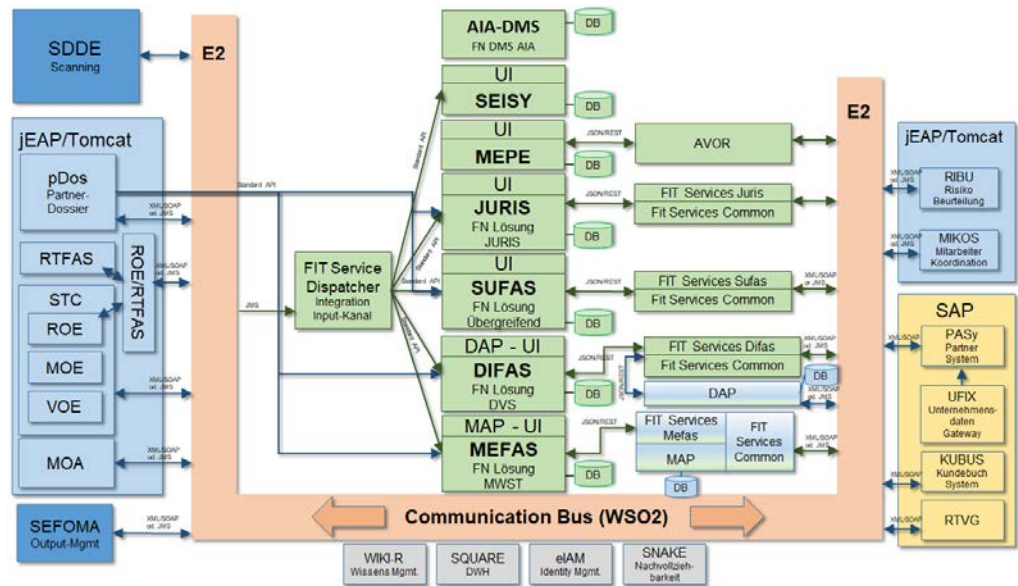


Abbildung 72: Beispiel einer Verwendung eines ESB auf Basis des WSO2 API Gateways bei FISCAL-IT

Der WSO2 API-Manager ist eine Komplettlösung vom Entwurf eines APIs, über das Deployment bis zur Pflege einer Developer Community. Das Produkt von WSO2 besteht aus einer Reihe von Bausteinen speziell für das API Management, die auf der WSO2 Middleware Plattform aufsetzen wie z.B. der API Store oder API Publisher. Einige Funktionen wie z.B. Analytics sind die der WSO2 Plattform oder kommen vom WSO2 ESB. Im API Publisher können APIs erstellt, neue Versionen erzeugt, Statistiken eingesehen und Subscriptions verwaltet werden. Das API Gateway ist mit dem WSO2 Enterprise Service Bus realisiert. WSO2 nennt seine API Gateway Komponente API Microgateway. Ein Microgateway arbeitet autonom und kann Anfragen weiterleiten, ohne dafür eine zentrale Management Komponente um Erlaubnis zu fragen. Die Erzeugung und Validierung von Access Tokens (z.B. OAuth2) übernimmt der Key Manager. Die API Gateways können sich für die Validierung mit dem Key Manager verbinden.







- (B) Peer-to-Peer Trust: Standard kreieren mit übergreifenden Festlegungen (vor allem in den Bereichen Transportprotokoll und Security) ohne einen konkreten zentralen Infrastrukturdienst festzulegen. Es bietet sich eher die Anwendung von Webservices an.

Beide Varianten unterstützen sowohl asynchrone als auch synchrone Kommunikation. Für die Schnittstelle Behördengang ↔ Geschäftsfallbearbeitung macht eher eine asynchrone Kommunikation Sinn, aber es sind durchaus auch Fälle denkbar, die für synchrone Kommunikation prädestiniert sind. So könnte man den Status der behördlichen Bearbeitung eines Geschäftsfalls auf zwei Arten übermitteln:

- Asynchron: Bei einem Statuswechsel sendet das behördeninterne Fachsystem der Behörde eine Nachricht an das Portal (so wie in Figure 36 dargestellt).
- Synchron: Das Portal fragt bei Bedarf den Status vom Fachsystem live ab.

Tabelle 29: Evaluation Lösungsvarianten [Herausforderung-5]

Variante A	Variante B
------------	------------

Potential zur Befriedigung der Herausforderung	 Es bestehen diverse, weit verbreitete und etablierte zentrale Lösungen, die genau dem Zweck im Sinne der Herausforderung dienen.	 Im Unterschied zu (A) besteht keine Abhängigkeit zu einem zentralen Infrastrukturdienst, sondern gibt lediglich eine fundamentale Spezifikation vor. Dies ermöglicht mehr Agilität und Spielraum für individuelle Anforderungen.
Wirtschaftlichkeit	 Die Kosten teilen sich über alle Teilnehmer auf. Die Umsetzung und der Betrieb kann je nach Lösung sehr komplex ausfallen.	 Im Gegensatz zu (A) liegt der Wiederverwendungsgrad deutlich tiefer, da die Anforderungen auf mehreren Systemen redundant umzusetzen sind. Zudem muss der Standard erst ausgearbeitet werden.
Machbarkeit	 Es stehen einsatzfähige Lösungen bereit. Die Lösung muss durch eine Organisation wie z.B. das BIT als zentraler Infrastrukturdienst für Behörden auf allen föderalen Ebenen angeboten werden. Dies ist heute zum Teil der Fall.	 Hohe Umsetzungstiefe: Standard muss erst ausgearbeitet werden. Implementierungen sind noch zu realisieren.
Auswirkung auf Sollarchitektur	Behandlung der Einbindung einer zentralen Infrastrukturkomponente. Allfällige Einflussnahme auf die Weiterentwicklung von bestehenden Lösungen wie z.B. Sedex.	Ausarbeitung und Etablierung eines Standards.
Zusammenfassende Beurteilung	Bestehende und weit verbreitete Lösungen, welche genau diese Herausforderung lösen können.	Neuer Standard muss erarbeitet werden, Akzeptanz nicht garantiert. Widerspricht Architekturprinzip Nachnutzung vor Eigenkreation.

Empfehlung: Im Sinne von Variante A im Rahmen der Studie Anforderungen an ein geschütztes Transportsystem spezifizieren und als zentrale Infrastrukturkomponente in die Sollarchitektur integrieren. Die Aufgabe zur Umsetzung, d.h. Evaluation und Betrieb eines geeigneten zentralen Transportsystems bei der Digitalen Verwaltung Schweiz (DVS) platzieren. Grundsätzlich können mehrere zentrale Infrastrukturkomponenten eingesetzt werden, je nach Bedürfnissen der Portale und behördeninternen Fachsysteme (z.B. Sedex und ESB).

Entscheid: Variante (A) wird umgesetzt.

[Herausforderung-6] In Bezug auf die aus Bedürfnis [B-15] resultierende Frage "Wie findet der User «Keine Ahnung» effizient die für sein Anliegen passende Behördenleistung?" verbleibt die Herausforderung, wie der User das für ihn bzw. sein Anliegen geeignete Behördenleistungsportal findet, bzw. wie die portalübergreifende Sollarchitektur diesen Use-Case unterstützt.

In dieser Frage steckt die Teilfrage "Welche Behördenleistungen sind für mich relevant?". Die Beantwortung dieser Frage leitet sich entweder aus dem jeweiligen Anliegen bzw. Themenkontext des Users (z.B. Bauprojekt) ab oder folgt aus dessen vertretenen Kundentyp bzw. Kundensegment (z.B. Unternehmen). Behördenleistungsportale sind in diesem Sinne gemäss 2.1.4

eher themenorientiert ausgerichtet oder wollen eher ganz bestimmte Kundensegmente ansprechen. In der Regel ist es eine Mischung aus beidem, weshalb es erlaubt sein muss, dass Ausrichtungen sich überlappen und Behördenleistungen verschieden präsentiert werden. Dies auch aus der Überlegung heraus, dass sich bereits Kundensegmente überlappen, da es mannigfaltige Kriterien zur Aufteilung gibt. Weiterhin folgt aus der Überlegung, dass es keine zentrale generelle Beantwortung der in der Herausforderung genannten Frage geben kann.

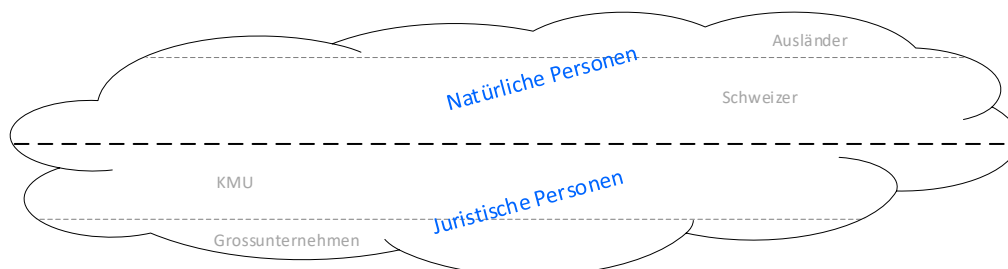


Abbildung 73: Kundensegmentierung Beispiel 1

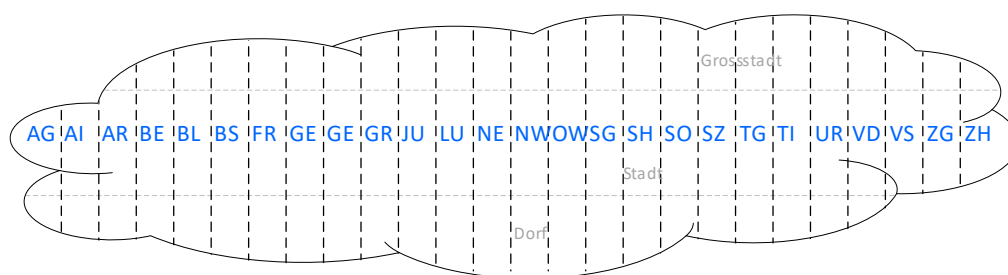


Abbildung 74: Kundensegmentierung Beispiel 2

Lösungsansätze:

- (A) Portale machen sich durch entsprechendes Marketing (z.B. mittels Search Engine Advertising SEA oder Search Engine Optimization SEO) bei der Kundengruppe bekannt, für welche sie Behördendienstleistungen anbieten. Dabei wird angestrebt, dass ein potenzieller User das für ihn geeignete Portal kennt, welches ihm bei seinem Anliegen am besten hilft.
- (B) Definition von zentralen Portalen, die ein bestimmtes Kundensegment per Dekret umfassend bedient (wie das z.B. die Motion Sollberger¹²⁰ für die Kundengruppe Unternehmen vorschlägt). Dies schliesst wohlgermerkt nicht aus, dass weitere Portale Angebote für das gleiche Kundensegment machen dürfen. Wenn z.B. eine unternehmensrelevante Leistung im Sinne der Motion Sollberger¹²⁰ auf EasyGov anzubieten ist, schliesst das nicht aus, dass sie auch auf einem kantonalen Portal angeboten werden kann.
- (C) Portalübergreifende Unterstützung der themenorientierten Suche nach Behördenleistungen in gängigen Suchmaschinen (z.B. Google oder Bing). Der Gedanke ist hierbei, dass Keywords für SEO-relevante Website-Tags (z.B. Bildbeschreibung, Seitenbeschreibung, Seitentitel) portalübergreifend definiert werden, so dass Suchmaschinen

¹²⁰ Siehe https://www.wbf.admin.ch/wbf/de/home/dokumentation/nsb-news_list.msg-id-78870.html

portalneutral qualitativ gleichmässige Trefferlisten hervorbringen. Die Entwicklung eines solchen portalübergreifenden Keyword-Katalogs setzt ein fachliches Modell voraus, das noch zu entwickeln wäre¹²¹. Dabei ist zu beachten, dass erstens portalübergreifende Keywords nicht exklusiv beansprucht werden können, eine isolierte Anwendung ist daher nicht möglich. Zweitens gilt es zu beachten, dass die Logik der Suchmaschinen jederzeit Anpassungen erfahren können, sie sind von einer Schweizer Vorgabe nicht steuerbar.

- (D) Aufbau oder Nutzung von bestehenden themenorientierten zentralen Landingpages, von denen der User zur jeweiligen Behördenleistung bzw. zum passenden Portal findet. Dies ist in zwei Varianten denkbar:
 - (D-1) Redaktionell verwaltete Landingpages nach dem Muster ch.ch, welche im Sinne eines zustandslosen Informationslayers auf die jeweiligen Behördenleistungen verlinken (siehe auch Figure 12). Hierzu sind keine Vorgaben seitens der portalübergreifenden Sollarchitektur nötig. Es können auch vorhandene Angebote (ch.ch¹²² oder auch Angebote aus der Privatwirtschaft) genutzt werden. ch.ch dient gemäss UZ7¹²³ als Anknüpfungspunkt bei Google und ist Einstiegsseite und verbindendes Element in der Landschaft der tausenden von Verwaltungsangeboten. ch.ch setzt dabei auf eine konsequente Suchmaschinenoptimierung. Damit wird Lösungsvariante C bereits durch eine auf die SEO-Aspekte spezialisierte Organisation, zentral für alle Verwaltungsangebote, die sich dieser bestehenden Lösung anschliessen, umgesetzt.
 - (D-2) Automatische vertikale Suchmaschine¹²⁴. Auf der Grundlage einer zentralen Vorgabe von generalisierten Elementen/Strukturen für den Informationslayer können Anbieter von Behördenleistungen Informationen zur Verfügung stellen, die dann von einer zentralen Webseite in einer schweizweiten Zusammenstellung verwertet werden und User bei der Selektion durch geeignete Suchlogiken unterstützt. Allerdings setzt dieser Ansatz ein entsprechendes fachliches Modell voraus. Dies müsste erst entwickelt werden, was wiederum diesbezüglich verwertbare Anforderungen voraussetzt¹²¹.

Hinweis: Zu diesem Lösungsansatz gibt es bereits Aktivitäten:

- Der Standard eCH-0049 definiert "Themenkataloge zur Gliederung des Leistungsangebots der öffentlichen Verwaltung der Schweiz aus der Perspektive von Leistungsbezügern", sowohl für die Belange von natürlichen als auch von juristischen Personen. Ergänzend dazu spezifiziert der Standard eCH-0141 "Vorgaben zur Beschreibung und Gliederung des Leistungsangebots der öffentlichen Verwaltung der Schweiz aus der Perspektive von Leistungsbezügern (Themenkataloge)". Diese Standards haben sich jedoch in der Praxis nicht bewährt, da die

¹²¹ Solch ein Unterfangen müsste in einer separaten Studie oder Arbeit geleistet werden.

¹²² Der Prozess zur Aufnahme einer Portal Referenz in ch.ch startet mit einer entsprechenden Kontaktaufnahme, siehe auch: <https://www.ch.ch/de/kontaktformular/>





¹²³ Siehe https://www.egovernment.ch/index.php/download_file/1747/3410/, Kapitel 3.1.7 «UZ7: Behördenübergreifende E-Information und Betrieb des neuen ch.ch etablieren»

¹²⁴ siehe https://de.wikipedia.org/wiki/Vertikale_Suchmaschine









beabsichtigte Leistungsbezüger-Perspektive eher aus der behördlichen Sicht gestaltet wurde. Der Standard ist deshalb als "veraltet" deklariert und befindet sich in Überarbeitung. Dabei wird der umgekehrte Ansatz verfolgt: Auf Basis der Userbedürfnisse und Suchintentionen wird eine Leistungsstruktur entwickelt.

- Der Standard eCH-0070 "Leistungsinventar eGov CH" definiert eine Struktur zur einheitlichen Beschreibung von Behördenleistungen und offeriert einen auf dieser Basis erstellten Katalog aller Schweizer Behördenleistungen. Der Reifegrad dieses Standards steht allerdings noch auf "Experimentell".
- Die Standards eCH-0073 "Vorgaben zur Beschreibung von Leistungen der öffentlichen Verwaltung der Schweiz" und eCH-0088 "Vorgaben zur Beschreibung von Behördengängen in der Schweiz" stehen über dem eCH-0070 und definieren Beschreibungsmerkmale von Behördenleistungen.
- Der Standard eCH-0138 "Rahmenkonzept zur Beschreibung und Dokumentation von Aufgaben, Leistungen, Prozessen und Zugangsstrukturen der öffentlichen Verwaltung der Schweiz" liefert die konzeptionellen Grundlagen für die oben genannten Standards eCH-0049, eCH-0010, eCH-0073, eCH-0088 und eCH-0141.
- Der Standard eCH-0123 "Architektur E-Government Schweiz: Vertrieb" [12] macht konzeptionelle Aussagen zur Präsentation (im Sinne von "Vermarktung") von Behördenleistungen.
- Im Rahmen des Umsetzungsplans 2020-2023 [19] von E-Government Schweiz läuft das Projekt UZ6¹²⁵ "Nutzerfreundlichkeit der elektronischen Behördenleistungen verbessern" und ergänzend dazu das Projekt UZ7¹²³ "Behördenübergreifende E-Information und Betrieb des neuen ch.ch etablieren".

Tabelle 30: Evaluation Lösungsvarianten [Herausforderung-6]

	Variante A	Variante B	Variante C	Variante D
Potential zur Befriedigung der Herausforderung	 <p>Bedienung vielfältiger Kundensegmente durch die Kraft des Marktes. Vielfalt bedeutet jedoch auch vielfältige Präsentationen (Vokabular, Strukturen). Infolge der Marktselektion können sich Quasi-Standards bilden.</p>	 <p>Bedienung des betreffenden Kundensegments mit klarer Struktur und einheitlicher Präsentation/ Philosophie. Zentral protegiertes Portal verzerrt jedoch im Vergleich zu A den Wettbewerb um Userakzeptanz. Letztlich kann der Ansatz aber nur</p>	 <p>Theoretisch umfassende Bedienung aller Kundensegmente möglich.</p>	 <p>Theoretisch umfassende Bedienung aller Kundensegmente möglich, inkl. integraler Umsetzung von Lösungsvariante C durch ch.ch</p>

¹²⁵ Siehe https://www.egovernment.ch/index.php/download_file/1747/3410/, Kapitel 3.1.6 «UZ6: Nutzerfreundlichkeit der elektronischen Behördenleistungen verbessern»

		einzelne (und nicht alle denkbaren) Kundensegmente (vergl. Abbildung 73, Abbildung 74) abdecken.		
Wirtschaftlichkeit	 Im Vergleich zu B hohe Marketingausgaben für einzelne Portale. Aus übergreifender Sicht redundante Investitionen nicht vermeidbar.	 Im Vergleich zu A geringe Marketingaufwände für protegierte Portale. Aus übergreifender Sicht Vermeidung redundanter Investitionen.	 Hoher Initialaufwand infolge Komplexität des nötigen fachlichen Modells, kontinuierliche Pflege nötig.	 Hohe Wirtschaftlichkeit, falls auf eine bestehende Lösung wie ch.ch gesetzt wird.
Machbarkeit	 Status quo, jedoch aus Sicht der Herausforderung noch lange nicht am Ende der Entwicklung. Langer Weg zum Ziel im Vergleich zu B.	 Ohne politische Unterstützung aufgrund der föderalen Struktur der Schweiz schwierig durchsetzbar. Infolge Motion Sollberger ¹²⁰ Realisierung jedoch für JP (EasyGov) wahrscheinlich. In diesem Fall kurzer Weg zum Ziel im Vergleich zu A.	 Durch spezialisierte Organisationen machbar. Nachteil: die SEO ist nicht isolierbar und nicht zentral steuerbar. Diesem Nachteil kann jedoch mit entsprechendem Aufwand begegnet werden.	 Standards bereits realisiert (Anwendung durch ch.ch), allerdings mit aus Usersicht noch nicht vollständig befriedigendem Ergebnis. Deshalb Weiterentwicklung im Rahmen von UZ6 und UZ7.
Auswirkung auf Sollarchitektur	Zielbilder unterstützen diesen Ansatz, keine zusätzlichen Auswirkungen.	wie A.	Zusätzliche Anforderung: Definition eines leistungsübergreifenden Keywordkatalogs.	Keine direkten Auswirkungen, da Weiterentwicklung durch eCH und UZ6 und UZ7 erfolgt. Allenfalls könnten sich daraus Anforderungen an die Sollarchitektur ergeben.
Zusammenfassende Beurteilung	Ohnehin gegeben, keine Massnahmen nötig.	B kann A nicht ersetzen, sondern nur optional auf A aufsetzen. Insofern kein Widerspruch zum Architekturprinzip [P-4].	Google als de facto Standard zur Suche von Leistungen im Internet muss in einer Lösung berücksichtigt werden. Der Aufbau dieser Lösung ist jedoch aufwendig und bedarf spezifisches Knowhow.	Diese Variante wurde bereits durch spezifische Angebote (z.B. ch.ch) umgesetzt. Diese Angebote setzen dabei integral auch die Lösungsvariante C um.

Empfehlung: Alle Lösungsvarianten haben ihre Berechtigung und können parallel umgesetzt werden.

Variante B ergänzt optional Variante A. Beide stehen im Einklang mit den Zielbildern (insbesondere denen in Kapitel 2.1.2 und 2.1.6), es ergibt sich keine Einschränkung des Lösungsraums.

Die Zielbilder unterstützen sowohl Variante A und B. Die Entwicklung der Sollarchitektur in Kapitel 2.5 muss in diesem Sinne diese beiden Varianten ermöglichen.

Variante C bedingt sehr spezifisches Know-how und erscheint für eine Umsetzung aufwendig. Gleichzeitig ist diese Variante, da Google der de facto Standard zur Suche von Leistungen im Internet ist, eine effektive Massnahme und entsprechend möglichst zu berücksichtigen. Deshalb wird diese Variante von den E-Government Schweiz-Projekten UZ6¹²⁵ und UZ7¹²³, die zum Ziel die Förderung des ch.ch-Portal haben, verfolgt. ch.ch ist ein bestehendes Angebot, das der Variante D entspricht. Da die Projekte UZ6/UZ7 das Thema bereits im Sinne von Variante C und D bearbeiten, muss diese Studie keine Aufwände in dieser Richtung machen.

Entscheid¹⁰⁰: Alle Lösungsvarianten können umgesetzt werden.

Annexe G.E Entscheide

Entscheid	Beschreibung	Entscheider	Termin
Projektziele	Die Projektziele wurden genehmigt	Projektaus- schuss	5.5.2020
Fokus Schnittstelle Kunde - Behörde	Der Scope der Soll-Architektur ist die Schnittstelle zwischen Kunde und Behörde. Behördeninterne Prozesse sind nicht Inhalt des Scopes	Projektaus- schuss	5.5.2020
Abgrenzung UX	Architekturrelevante UX-Themen sollen als Bedürfnis aufgenommen werden. Wichtig ist, dass die Abgrenzung die Architekturrelevanz ist.	Projektaus- schuss	5.5.2020
Erweiterung Scope	Verankerung der getroffenen Scope-Erweiterungen in den Projektzielen: <ul style="list-style-type: none"> • Machbarkeit Integration von <i>Bundes-</i>, kantonalen und kommunalen Leistungen • Sollarchitektur <i>für die Domäne Behördenleistungsportale</i> • Gapanalyse sowie Grobplanung <i>bezüglich EasyGov</i> 	Projektaus- schuss	27.8.2020
Verlängerung Planung	Verlängerung Projektende um ein Jahr auf Ende 2021	Projektaus- schuss	27.8.2020
E-ID als digitale Identität	Es soll voll und ausschliesslich auf die E-ID als staatlich regulierte Identifizierungsmöglichkeit setzen	Fachausschuss	16.12.2020
Anwendung eines Schalenmodells mit einem geregelten und einem nicht geregelten Teil	Individuelle Anforderungen von einzelnen Portalen oder Behörden können bei der Formulierung eines portalübergreifenden Bewirtschaftungsrechtemodells berücksichtigt werden. Dabei können ein geregelter, interoperabler Teil und ein nicht interoperabler Teil angewendet werden.	Fachausschuss	18.1.2021
Versichertennummer als führender Kundenidentifikator	Die Versichertennummer gilt als führender und zwingender Kundenidentifikator. Die E-ID-Registrierungsnummer wie auch weitere Identifikatoren können zugelassen werden. Die Registerdienste UPI und NAD sollen	Fachausschuss	1.3.2021

	auf Basis der Versichertennummer genutzt werden.		
Zentrale Infrastrukturkomponente für die portalübergreifende Übertragbarkeit von Bewirtschaftungsrechten	Es sollen Anforderungen an ein IAM-System spezifiziert und dieses als zentrale Infrastrukturkomponente in die Sollarchitektur integriert werden. Die Evaluation eines geeigneten Systems soll durch die Digitale Verwaltung Schweiz (DVS) erfolgen.	Fachausschuss	1.3.2021
Zentrale Infrastrukturkomponente für ein geschütztes Transportsystem	Es sollen Anforderungen an ein geschütztes Transportsystem spezifiziert und dieses als zentrale Infrastrukturkomponente in die Sollarchitektur integriert werden. Die Evaluation eines geeigneten Systems soll durch die Digitale Verwaltung Schweiz (DVS) erfolgen.	Fachausschuss	1.3.2021
Unterschiedliche Varianten zur Auffindung von Behördenleistungen	Zur Auffindung der für den User relevanten Behördenleistungen können unterschiedliche Varianten umgesetzt werden. Alle Lösungsvarianten können umgesetzt werden.	Fachausschuss	1.3.2021
Berücksichtigung von zwei Integrationsmuster	Folgende Integrationsmuster werden berücksichtigt: Integrationsmuster 1: Implementation des Behördengangs direkt im Portal Integrationsmuster 2: Einbindung eines extern implementierten Behördengangs	Fachausschuss	22.4.2021
Gemeinsame Domain Policy	Es wird festgehalten, dass als Standard eine gemeinsame Domain Policy definiert wird, die bei DVS umgesetzt, für verbindlich erklärt und gepflegt wird.	Fachausschuss	22.4.2021
Nicht ausschliesslich auf E-ID setzen	Es soll nicht ausschliesslich auf die E-ID als digitale Identität gesetzt werden. Die E-ID soll komplementär zu anderen Identitäten zum Einsatz kommen, sobald sie verfügbar ist. Der entsprechende Entscheid vom 16.12.2020 wird revidiert.	Projektausschuss	5.5.2021

Peer-to-Peer Trust Schnittstellenarchitektur	In einer ersten Phase der Standardisierung soll auf eine Peer-to-Peer Trust, also dezentrale Schnittstellenarchitektur fokussiert werden.	Projektausschuss	17.5.2021
Dezentral vor zentral	Die Entscheide zu zentralen Infrastrukturkomponenten werden zugunsten eines in einer ersten Phase dezentralen Ansatzes revidiert.	Projektausschuss	17.5.2021
Empfehlung zur Technologie	Die Anforderungen an die Standardisierung sind auf konzeptioneller Ebene zu formulieren und nicht auf technischer. Die Festlegung der Technologie greift zu weit. Eine Empfehlung zur Technologie ist jedoch angebracht und soll abgegeben werden.	Fachausschuss	24.6.2021
Definitionshoheit	Die Schnittstellen-Verantwortung (Definitionshoheit) liegt in der Hand des Providers des Behördengangs resp. des Geschäftsfalls	Fachausschuss	24.6.2021
Etappierte Roadmap	Es soll eine etappierte Roadmap mit Ausbausritten über Peer-to-Peer Trust hinaus umgesetzt werden. Die Entscheide zu den Ausbausritten erfolgen zu einem späteren Zeitpunkt.	Fachausschuss	24.6.2021
Kostenübernahme	Jedes Portal ist für die Implementierung der Schnittstelle und der damit verbundenen Kosten selbst verantwortlich.	Fachausschuss	24.6.2021
Abnahme der Studie	Die Studie in der Version 1.0 wurde abgenommen	Projektausschuss	4.2.2022

Annexe G.F Input des Projektausschusses bezüglich der Bedürfnisse

I. Bedürfnisse aus Sicht Kunde (z.B. Unternehmen, Privatperson)

Input von Alexandra Collm

- Möchte so viele Dienstleistungen wie möglich im Self-Service Modus direkt beziehen/ausführen können
- Möchte die Dienstleistungen auch unterwegs (mobil) nutzen können
- Möchte Transparenz haben, welche Daten wo liegen, welche Behördenstellen für welchen Zweck darauf zugreifen und sicher sein, dass der Datenschutz eingehalten ist.
- Möchte immer wissen, welche Leistungen er/sie wo beziehen kann und direkt dorthin gelangen
- Möchte geeignet unterstützt werden, wenn er/sie wiederkehrende Fälle abwickelt und wiederkehrende Dinge sofort ausführen können.
- Möchte "seine" personalisierte Sicht auf die Leistungen der Amtsstellen pflegen können.
- Möchte eine vollständige Sicht auf alle Leistungen, die für ihn / sie im aktuellen Kontext relevant sind
- Möchte die Berechtigungen der Unternehmensmitarbeitenden im Self-Service Modus pflegen können.
- Möchte mit demselben Login Leistungen für verschiedene Unternehmen abwickeln können und am besten auch für private Geschäfte.
- Möchte immer wissen, bei welcher Behörde er/sie gerade ist, aber auch wissen, dass er/sie dieser Behörde Vertrauen kann (Stichwort: wechselnde Look&Feels, Bin ich noch am richtigen Ort?, Qualitätslabel)
- Möchte die Übersicht über alle Mitteilungen und Aktivitäten im Zusammenhang mit Behördengängen nicht verlieren (Stichwort: Mitteilungen, Rückfragen, Aktivitäten). Was muss ich wo tun?
- Möchte je nach Wissenstand nicht mit Informationen überladen werden und sich bei Bedarf vertieft informieren können. Zusatz-Informationen sollen auch redundanzfrei sein (Pro Behördenleistung muss klar sein, welche Behörde die Informationshoheit hat und die Informationen pflegt).
- Erwartet, dass die Informationen und Wordings auf verschiedenen Behördenstufen (Bund/Kanton/Gemeinden) stimmig aufeinander abgestimmt sind.
- Hat hohe und immer steigende Erwartungen an die Benutzerfreundlichkeit, Übersichtlichkeit, Verständlichkeit, Auffindbarkeit und Bedienbarkeit.
- Wünschen sich einen themenorientierten Zugang und nicht bloss einen leistungsbezogenen Zugang
- Der Weg von der Google Suche bis zum Aufruf des gesuchten Online Services bei der relevanten Behörde soll kurz und ohne Umwege sein (< 3-4 "Klicks away").

- Worauf habe ich Zugriff und worauf nicht, sollte früh ersichtlich sein (Grobautorisierung)
- Möchte barrierefreien Zugang zu den Leistungen auf allen gängigen Geräten haben.

Input von Andreas Spichiger

- Kunde kann für ihn relevante Amtsgänge einfach finden. (T1)
- Kunde kann alle für ihn relevanten Amtsgänge vollständig elektronisch abwickeln. (T1)
- Die Amtsgänge sind für den Kunden einfach zugänglich (accessibility). (T1)
- Ein Single Point of Contact SPOC kümmert sich um alle Probleme in der Interaktion zwischen Behörden. (T1)
- Kunde muss Daten nur einmal erfassen (behördenübergreifendes Once-Only-Prinzip). (T2)
- Ein einheitliches CI erhöht die Zufriedenheit mit der Lösung und stärkt das Vertrauen in die Lösung. (T3)
- Eine Person kann alle Amtsgänge mit einer eID erledigen. Sie darf aber auch mehrere separate eID einsetzen. (T3)
- Single-sign on funktioniert auf der Basis einer eID portal-übergreifend. (T3)
- Ein Amtsgang verlangt von der Person keinen höheren LOA-Level als notwendig. (T3)
- Ein Amtsgang führt den Kunden – auch behördenübergreifend – transparent durch den Prozess. (T4)
- Eine Person kann jederzeit Transparenz über die Verwendung von ihren eigenen Personendaten erlangen. (T4)
- Amtsgänge sind so geschnitten und umgesetzt, dass der Kunde mit möglichst wenigen Interaktionen seine Pflichten erledigen kann. (T5)
- Amtsgänge sind über einfache, standardisierte Schnittstellen zugänglich. (T5)

Input von David De Groote

- Le citoyen doit avoir un point de contact unique où il retrouve l'historique de ses transactions, ses messages, ses documents, ses processus «en cours», etc... peu importe sur quelle plateforme de base le processus a été exécuté.
- Le citoyen doit pouvoir utiliser son identité électronique habituelle (SwissID, TrustID ou toute autre eID reconnue) ou encore tout autre identité publique (Facebook, Google, etc.) tout en réduisant le niveau de prestations.
- Processus sans rupture de média
- Multilingues (FR/DE/EN, ...)
- Intégration qui permette l'accessibilité AA des prestations intégrées
- Consentement éclairé lorsque des données sont transférées d'une plateforme à une autre
- Transparence envers l'utilisation des données (OMO13: Élaborer un modèle de traçabilité de l'utilisation des données personnelles)

Input von Marcel Kessler

- Möchte für ihn relevante Amtsgänge möglichst an einem Ort (Plattform) finden/abwickeln und möchte sich dazu nur einmal einloggen
- Möchte keine Daten doppelt erfassen (behördenübergreifendes Once-Only-Prinzip)
- Wünscht, dass er – auch behördenübergreifend – durch den Prozess geführt wird
- Will über den Stand der Bearbeitung informiert sein (ist eventuell schon im Vorpunkt)
- Muss den Entry-Point kennen und ihm vertrauen.
- Will eventuell die Möglichkeit haben, bei Schwierigkeiten eine Ansprechperson ohne Aufwand zu kontaktieren

Input von Hansjörg Hänggi

- Möchte für ihn relevante Amtsgänge möglichst an einem Ort (Plattform) finden/abwickeln und möchte sich dazu nur einmal einloggen
- Möchte keine Daten doppelt erfassen (behördenübergreifendes Once-Only-Prinzip)
- Wünscht, dass er – auch behördenübergreifend – durch den Prozess geführt wird
- Möchte über den Stand seiner Anträge, Gesuche informiert sein
- Möchte sehen wer für seinen Antrag, Gesuch zuständig ist
- Möchte fehlende Daten über die gleiche Plattform nachreichen können
- Möchte mit dem zuständigen Amt online kommunizieren (Offline Chat)
- Möchte das Ergebnis seines Gesuchs, Antrags auf dem Portal abholen
- Möchte über wichtige Ereignisse seinen Antrag betreffend informiert sein
- Einfache Bedienbarkeit der Prozesse
- Es ist dem Kunden immer klar wer für ihn zuständig ist und verantwortlich für die Leistungserbringung.
- Er möchte die gleiche Leistung in unterschiedlichen Kantonen mit den gleichen Prozessen abwickeln.
- Der Zugang zum Portal und Kantonalen, Gemeinde und Städte Leistungen erfolgt mit einem Account / Password

II. Bedürfnisse aus Sicht Behörde (Bund, Kanton oder Gemeinde)

Input von Alexandra Collm

- Wollen ihre Leistungen digital anbieten
- Möchten dabei die Kontrolle über ihre Behördenleistung behalten (fachlich und betrieblich)
- Würden gerne eine bestehende Portalinfrastruktur nutzen (vor allem aus Kostengründen/Durchgängigkeit/Einfachheit)
- Würden gerne Unternehmen nur noch digital bewirtschaften (Digital Only) – und private nach dem Digital First Prinzip.

- White-Labeling: Die Leistungen sollen im CI/CD der Gemeinde bereits auf easyGov geeignet erkennbar sein, damit der Sprung / Wechsel in die Gemeinde keine Irritationen auslöst.
- Möchte verschiedene Integrationspatttern nutzen können.
- Gemeinden und Kantone digitalisieren dieselbe Behördenleistung unterschiedlich. Die unterschiedlichen Ansätze sollen unterstützt werden. Eine Leistung kann unterschiedlich in Teilprozesse "geschnitten" sein. Beispiel:
- Leistung passt 1:1 auf die Leistung, die im easygov Portal angeboten wird.
- Gemeinde hat für die Leistung zwei Teilprozesse (Erstanmeldung und jährlich wiederkehrende Erneuerungsmeldung)
- Gemeinde hat mehrere Leistungen in einem Unterportal zusammengefasst
- Leistung setzt sich aus einem Online Teil und einen noch nicht digitalisierten Kanal zusammen
- Leistung involviert mehrere Amtsstellen (innerhalb der Gemeinde oder auch ausserhalb)
- Möchte den Benutzer/Die Benutzerin nahtlos auf Behördenleistungen der eigenen und anderer Amtsstellen weiterleiten / hinweisen können.
- Möchte keine Auswirkungen auf eigenen Webauftritt / CI/CD.
- Möchte auch funktionsfähig bleiben, wenn das zentrale Portal ausfallen sollte.
- Kontaktaufnahme im Falle von Fragen bei der korrekten Behörde und Regelung der Weiterleitung von fehlgeleiteten Kontaktanfragen. Am liebsten eine zentrale Anlaufstelle.
- Rückmeldungen zu den eigenen Leistungen sollen den Weg zur relevanten Behörde finden.
- Wünschen sich einen Werbekanal und Informationskanäle für neu eingeführte Services
- Möchte auch Services anbieten können, während das Unternehmen noch in der Gründungsphase ist und noch keine UID hat (unverifizierte Unternehmen)
- Möchte auch Services für Privatpersonen anbieten können (Beispiel Bestellen Betriebsregisterauszug für sich selbst oder für Dritte).
- Zentrale Register sollen vollständig und zeitnah aktuell sein, damit keine Übergangslösungen notwendig werden (Bsp: BUR Daten sind nicht aktuell genug, um die Grundgebühren für neue Firmen für die Abfallentsorgung zu erheben).
- Community, um Verbesserungsvorschläge unkompliziert einspeisen zu können.

Input von Andreas Spichiger

- Behörde bietet alle Leistungen per default digital an. (T1)
- Behörde kann Interaktion mit Kunden auf ein Minimum reduzieren. (T1)
- Behörde kann andere Leistungen (eigene, anderer Behörden und Dritter) einfach einbinden. (T5)

- Ein aktuelles Verzeichnis verzeichnet alle Behördenleistungen mit den für die Integration notwendigen Metadaten. (T5)
- Behörden-übergreifend werden gemeinsame Stammdaten hoher Qualität genutzt (bedingt gemeinsam genutzte Identifikatoren wie z.B. AHV#). (T2, T5)
- Support-Organisation (1st, 2nd, 3rd) kann einfach integriert werden. (T5)
- Personen verfügen über eine eID hoher Qualität. (T3)
- Die Erbringung der Behördenleistung erfolgt in (hoheitlichen) Auftrag der Behörde. (T4)
- Die Behörde kann mit möglichst geringem Ressourceneinsatz einen möglichst hohen Impact erreichen. (Effektivität, Effizienz)

Input von David De Groote

- Processus sans rupture de média aussi pour l'administration!

Input von Marcel Kessler

- Möchten auf verschiedene Weisen, aber standardisiert ihre Fachapplikationen einbinden
- Möchte die Möglichkeit haben den Kunden zu kontaktieren, wenn nötig
- Möchte, dass Prozesse automatisch ablaufen, aber (wie schon erwähnt) kontrollierbar bleiben (tracing?)
- Möchte, dass alternativ-Eingaben auch in den digitalen Prozess eingebunden werden können

Input von Hansjörg Hänggi

- Wollen ihre Leistungen digital anbieten
- Möchten dabei die Kontrolle über ihre Behördenleistung behalten (fachlich und betrieblich)
- Wollen keine Medienbrüche in den Prozessen
- Hohe Qualität der gelieferten Informationen
- Können mit dem Kunden sicher kommunizieren (Unterlagen nachfordern, Fragen stellen...)
- Status der Bearbeitung wird automatisiert an den Kunden weitergeleitet
- Leistung kann auf zentralem Portal aufgerufen werden aber auch im jeweiligen Behördenumfeld (Gemeinde, Stadt, Kanton, Bund)

III. Bedürfnisse aus Sicht Portalanbieter (z. B. EasyGov, ePortal oder Kanton X)

Input von Alexandra Collm

- Möchte das Nutzenversprechen vollständig (d. h. mit allen relevanten Behördenleistungen) ausfüllen
- Möchte den Integrationsaufwand und die technische Komplexität in Grenzen halten
- Würde einen Standard zur Interoperabilität von digitalen Behördendiensten (bzw. -Applikationen) begrüßen

- Eigenentwicklungen sollen im Self-service Modus unkompliziert und rasch in easygov aufgeschaltet werden können. (Rasch heisst: "sofort", wenn sich neue Leistung an Minimalset von Standards hält)
- Wünschen sich einen vollständigen schweizweiten Referenz-Leistungskatalog mit allen Behördenleistungen (inkl. der Gemeindeleistungen).
- Wünschen sich einen schweizweiten Standard (oder vermutlich besser Empfehlungen) für Namens- und Begriffsdefinitionen, sowie Formulierungen zu Leistungskatalogen
- Möchte nicht ausgebremst werden, beim Etablieren eigener / neuer Online Leistungen
- Möchte möglichst wenig an bestehenden und etablierten Online Lösungen anpassen müssen und diese einfach integrieren können.
- Möchte bereits existierende Portale weiter nutzen.
- Möchte eine klare verbindliche Roadmap haben, um beurteilen zu können, welche Services wann im zentralen Portal angeboten werden und welche in einem lokalen Portal entwickelt werden sollen (Vermeidung von Doppelspurigkeiten)
- Möchte einen hohen Entkoppelungsgrad und stabile Schnittstellen (Parallelbetrieb bei grösseren Änderungen notwendig)
- Glaubte nur an eine Lösung, wenn alle Portale mit einer einheitlichen Identifikation arbeiten können (Stichwort E-ID und eCH-0170).
- Standardprodukte für Gemeindelösungen und Individualentwicklungen sollen einfach integrierbar sein und Hersteller brauchen klare Richtlinien, Guidelines, Schnittstellen...
- Möchte klare Abgrenzungen haben, was zentral und was auf behördenseitigen Portalen zu lösen ist.
- Klare definierte Verantwortlichkeiten und Ansprechpersonen
- Das Portal sieht ein Rollenmodell Individuum welches für mehrere Unternehmung und als Privatperson unterwegs ist vor.

Input von Andreas Spichiger

- Portalanbieter will den Integrationsaufwand (politisch, rechtlich, organisatorisch, semantisch und technisch) tief halten. -> Behördenleistungen sind interoperabel ausgestaltet. (T5)
- Portalanbieter will vertrauenswürdige und verlässliche Behörden als Leistungserbringer integrieren. (T3)
- Portalanbieter will einen schlanken Betrieb. (T5)
- Portalanbieter will hohe Transparenz in der Abwicklung eines Amtsgeschäfts. (T4)

Input von David De Groote

- Les portails nationaux, cantonaux, etc. doivent pouvoir s'échanger des données sur la base d'un standard eCH (documents, cas d'affaires, messages, historique de transactions, Etc.)
- Des API doivent être disponibles sur les back-ends métiers liés aux prestations administratives

Input von Marcel Kessler

- Möchte das Nutzenversprechen vollständig (d. h. mit allen relevanten Behördenleistungen) ausfüllen
- Möchte den Integrationsaufwand und die technische Komplexität in Grenzen halten
- Verlangt einen Standard zur Interoperabilität von digitalen Behördendiensten (bzw. -Applikationen) begrüßen
- Möchte, dass es allen Beteiligten klar ist, wer der Prozess-Owner ist und somit Ansprechperson
- Möchte einen klaren Help-Desk bzw. Supportprozess

Input von Hansjörg Hänggi

- Möchte das Nutzenversprechen vollständig (d. h. mit allen relevanten Behördenleistungen) ausfüllen
- Möchte den Integrationsaufwand und die technische Komplexität in Grenzen halten
- Fordert einen Standard zur Interoperabilität von digitalen Behördendiensten (bzw. -Applikationen) und arbeitet mit an der Gestaltung einer eCH-Norm
- Das Portal lässt sich Stand-Alone betreiben, das Front-End lässt sich auch in anderen Portalplattformen einbinden (Gemeinde, Kanton)
- User Support Prozesse sind standardisiert und mit den beteiligten Partnern abgestimmt

IV. Weitere Bedürfnisse und Erfolgsfaktoren

Input von Alexandra Collm

- Auch BenutzerInnen mit einer niedrigen Vertrauensstufe (unverifizierte Benutzer mit Username Passwort) sollen das Portal für unkritische Behördenleistungen nutzen können.
- Alle Leistungen müssen auch im nicht eingeloggten Zustand durchsucht werden können.
- Governance und Finanzierung sollen klar geregelt sein und die Ansprüche der Stakeholder (Bund, Kantone, kleine und grosse Gemeinden) sollen berücksichtigt werden.
- Allgemeine Funktionen sollen nicht von den Gemeinden finanziert werden müssen. Gemeinden sollen die Möglichkeit haben, Spezialanforderungen einzubringen und es soll sichergestellt sein, dass diese in nützlicher Frist umgesetzt werden.
- Wie soll mit Leistungen umgegangen werden, die sowohl für Unternehmen als auch für Privatpersonen angeboten werden (Bsp: Betreibungsregisterauszug)?
- Wird easygov in Zukunft neben Unternehmensservices auch Leistungen für Privatpersonen generell unterstützen?
- Gute und durchgängige User Journey's
- Vollständigkeit der Dienstleistungen
- Adäquate Integrationspattern (Kosten / Nutzen)/ Flexibilität
- Tiefe Kosten

- Unterstützung durch entsprechende Institutionen (eCH)
- Breite Kommunikation
- Vor allem in der ersten Phase: Reaktionszeiten und Kurze Durchlaufzeiten für Integration von Services
- Unterstützung unterschiedlicher Umsetzungsreife von Gemeinden für Digitalisierungsgrundsätze (Bsp: Wenn Once-Only kommt, dann wird die Umsetzung einige Zeit in Anspruch nehmen)

Input von Andreas Spichiger

- Internationale Integrierbarkeit
- Föderierte Portale -> es wird immer viele andere geben ... -> Alle lokalen Basisdienste basieren auf einer föderierten Architektur
- Offenes, einfach erweiterbares Konzept
- Bring your own Service muss sehr einfach umsetzbar sein

Input von David De Groote

- Mise en place d'outils nationaux qui doivent permettre de mettre à disposition des prestations administratives 100% digitales:
 - Services de base (service de paiement, éditeur de formulaires, scanner mobile, etc...)
 - Kit de développement national de prestations administratives
 - Look & Feel national de prestations administratives (tout en étant adaptable au couleurs cantonales)
- Intégration transparente pour le citoyen (le citoyen doit savoir en permanence où il se trouve)
- Simplicité technique de l'intégration
- Coûts raisonnables d'intégration
- Si des standards sont définis, il faut s'assurer qu'ils soient suivis et mis en oeuvre.

Input von Marcel Kessler

- Soll kongruent mit der Architektur E-Government sein
- Die Bedürfnisse des Tracings (Konzept zur Nachvollziehbarkeit der Verwendung persönlicher Daten) sollen miteinfließen
- Verständlichkeit
- Einfachheit (wenn möglich)
- Weitere Unterlagen, die helfen bei der Umsetzung

Input von Hansjörg Hänggi

- Anbindung auch bundesinterner Applikationen die für die Prozesse relevant sind (funktional und zeitnah).

- Ein Anlaufpunkt für die Wirtschaft für ihre relevanten Dienstleistungen der Behörden
- Durchgängigkeit der Prozesse
- Transparenz über die verarbeiteten und gespeicherten Daten
- Zugriff auf alte Gesuche, Wiederverwendung derselben
- Einbezug aller Stakeholder
- Commitment aller Beteiligten für die Lösung
- Keine politischen Kompromisse, rein sachliche Lösungen
- Eine durchgehende Authentifizierungslösung
- Akzeptanz und Integration der Partnersysteme
- Diskussion auf Augenhöhe.

Annexe H Glossaire allemand → français

Begriff in Deutsch	Termes en français
Anfrage	question
Anliegen	requête
API Endpoint	point d'accès API
Architekturreview	révision de l'architecture
Auftraggeber	mandant
Authentifikation	authentification
Back-End	back-end
Bedürfniserfüllung	accomplissement des besoins
Behörde	autorité
Behördengang(e)	démarche(s) administrative(s)
Behördengang↔Geschäftsfallbearbeitung	démarche administrative↔traitement des transactions
Behördeninternes Fachsystem	système métier interne de l'autorité
Behördenleistung(en)	prestation(s) administrative(s)
Behördenleistungsportal(e)	portail(s) de prestations administratives / portail de prestations
behördliche Benachrichtigung	notification officielle
Benachrichtigung(en)	notification(s)
Berechtigungsmanagement	gestion des droits d'accès
Berechtigungsstufe	niveau d'autorisation
Bescheid	avis
Bewirtschaftungsrecht	droit de gestion
Consumer-Portal	portail consommateur
Datenhoheit	souveraineté des données
Definitionshoheit	souveraineté définitionnelle
Definitionszeit	heure de définition
Digitale Identität	identité numérique
Dokumentenablage	répertoire des documents
E-Government-Strategie Schweiz	stratégie suisse de cyberadministration
Einbindung	intégration
Elektronische Identität	identité électronique

Fachanwendung	application métier
Fachausschuss	comité d'experts
Fachsystem	système métier
Front-End	front-end
Geschäftsfall (-bearbeitung)	traitement des transactions
Geschäftspartner	partenaire commercial
Geschäftspartnerverwaltung	gestion des partenaires commerciaux
Gesuch	demande
Identifikator	identifiant
Identitätsprovider (IdP)	fournisseur d'identités (FI)
IKT-Strategie des Bundes	stratégie informatique de la Confédération
Implementation	implémentation
implementieren	Implémenter
Informationslayer	couche d'information
Informationsmodell	modèle d'information
Initialmeldung	message initial
Integrationsmuster	modèle d'intégration
Integrations-Sollarchitektur	architecture cible d'intégration
Integrations-Sollarchitektur	architecture cible d'intégration
Interoperabilitätsrahmen	cadre d'interopérabilité
Interoperabler Kern	base interopérable
IT-Governance	gouvernance informatique
Kontextsynchronisation	synchronisation du contexte
Kunde	client
Kundenanliegen	requête client
Kundendatenverwaltung	gestion des données clients
Kundenkonto	compte client
Kundenstammdatenverwaltung	gestion des données de base des clients
Laufzeit	temps d'exécution
Leistung	prestation
Leistungsangebot	offre de prestations
LoA (Level of Assurance)	LoA (Level of Assurance / niveau de confiance)
Login	login

Lose Kopplung	couplage faible
Management Summary	résumé exécutif
Meldung (Initialmeldung, Rückmeldung)	message (message initial, message réponse)
Orchestrierung	orchestration
Payment	payement
Peer-to-Peer Trust	confiance entre pairs / P2P trust
Plattform	plate-forme
Portal	portail
Portalbetreiber	exploitant de portail
Portal-Fachanwendung	application portail métier
Projektausschuss	comité de pilotage
Projektinitialisierungsauftrag	mandat d'initialisation du projet
Provider-Portal	portail fournisseur
Querschnittsfunktion(en)	fonction(s) transversale(s)
Register	registre
Rückkanal	canal de retour
Rückmeldung	message réponse
Schlüsselwert	valeur clé
Scope	périmètre
Single Logout	déconnexion unique
Single Sign-On	authentification unique
SSO-Weiterleitung	redirection SSO
Stammdaten	données de base
Standardisierungsthemen	sujets de normalisation
Systemarchitektur	architecture du système
Transaktionslayer	couche transactionnelle
Umsetzungs-Roadmap	feuille de route de mise en œuvre
User	utilisateur
Userkonto	compte utilisateur
Verbindlicherklärung	déclaration donnant force obligatoire
Verfahren	procédure
Vertrauensgrad (LoA)	niveau de confiance (LoA)
(beiderseitige) Vertrauensvereinbarung	accord de confiance (mutuel)

Vollmacht	procuration
Weitergabe	transfert
zustandslos	sans état / stateless

Liste des figures

Figure 1: Périmètre de l'architecture cible d'intégration (représentation schématique)	25
Figure 2: Flux général d'une procédure d'autorisation (diagramme BPMN)	27
Figure 3: Flux général d'une procédure d'annonce (diagramme BPMN).....	28
Figure 4: Abstraction du traitement d'une prestation administrative en tant que processus fonctionnant en parallèle du côté du client et de l'autorité	28
Figure 5: Implication d'une autre autorité/d'un autre bureau dans le traitement des transactions selon le modèle de sous-processus	29
Figure 6: Implication d'une autre autorité/d'un autre bureau dans le traitement des transactions selon le modèle de transfert de la procédure	30
Figure 7: Portail de prestations comme canal d'accès numérique à une ou plusieurs prestations de l'autorité pour le client (diagramme Use-Case UML).....	31
Figure 8: L'exploitant du portail peut aussi être l'autorité elle-même.....	32
Figure 9: Délimitation du périmètre d'un portail de prestations au processus côté client. En revanche, les processus internes à l'autorité sont pris en charge par le système métier de l'autorité.	33
Figure 10: Emplacement des couches d'information et transactionnelle du point de vue du processus	34
Figure 11: Structure fonctionnelle de base d'un portail de prestations	35
Figure 12: Diverses caractéristiques des couches dans les portails de prestations existants ...	36
Figure 13: Structure de l'ePortal avec des sous-systèmes distribués sous différentes responsabilités	37
Figure 14: Portail de prestations axé sur le portefeuille d'une autorité (A): le portail présente le portefeuille de prestations offertes par une autorité spécifique	38
Figure 15: Portail de prestations (B) adapté aux besoins d'un groupe-cible de clients spécifique: le portail représente l'ensemble prestations pertinentes pour le groupe-cible de clients. Ces prestations peuvent provenir de différentes autorités	38
Figure 16: Encapsulation de la responsabilité spécifique d'une prestation administrative cantonale/communale par une offre globale (B')	39
Figure 17: Forme mixte (C) de (A) et (B)	40
Figure 18: Représentation individuelle d'une prestation administrative sur différents portails ..	41
Figure 19: Intégration d'une implémentation existante d'une démarche administrative dans un autre portail	43
Figure 20: Modèle d'information pour les portails de prestations (diagramme de classe UML, pour une représentation agrandie, voir l'Annexe B).....	44
Figure 21: Modèle d'intégration 1 - Implémentation de la démarche administrative directement dans le portail.....	50
Figure 22: Le modèle d'intégration 2 permet également l'utilisation de plusieurs portails consommateur.....	50
Figure 23: Cas particulier du modèle d'intégration 1: un portail de prestations fournit un environnement/cadre d'exécution pour des prestations l'autorité sur lequel les autorités mettent en œuvre leurs prestations en tant qu'application portail métier ou les configurent en composants préfabriqués.	51
Figure 24: Modèle d'intégration 2 - Intégration d'une démarche administrative implémentée en externe	52
Figure 25: Forme mixte - le portail représente les démarches administratives selon les deux modèles d'intégration 1 et 2.....	53

Figure 26: Catégorisation des besoins par Tallinn, thèmes et acteurs (la taille des bulles représente le nombre de mentions)	64
Figure 27: Séquence d'images pour le point faible 1	73
Figure 28: Séquence d'images pour les points faibles 2 et 3	75
Figure 29: Un portail de prestations utilise une identité numérique définie en externe pour l'authentification des utilisateurs, tandis qu'il identifie les clients à l'aide d'un identifiant défini en externe.	78
Figure 30: Illustration [REQ-1] à l'aide d'un contexte exemplaire (diagramme d'objet UML) ..	79
Figure 31: Localisation des exigences d'interopérabilité dans le modèle d'information	80
Figure 32: Illustration de la base interopérable à l'aide de l'exemple de l'interface "démarche administrative↔traitement des transactions" (modèle d'intégration 1).	81
Figure 33: Mise en correspondance de la base interopérable d'une fiche client dans un portail de prestations	85
Figure 34: Établissement du contexte de session lors de l'appel de la démarche administrative "Demande d'autorisation Y" dans le portail fournisseur en conformité avec le contexte du portail consommateur au moyen de SSO + synchronisation du contexte	87
Figure 35: Situation du cadre d'interopérabilité dans le modèle d'information.....	92
Figure 36: L'architecture cible d'intégration spécifie les processus de communication généraux (non spécifiques à une prestation) entre le portail de prestations et le système métier interne de l'autorité	93
Figure 37: Modèle d'information des processus d'interface "démarche administrative↔traitement des transactions"	95
Figure 38: Modèle de processus d'interface "démarche administrative↔traitement des transactions" dans le cas "Déclenchement par le client"	96
Figure 39: Modèle de processus d'interface "démarche administrative↔traitement des transactions" dans le cas "Déclenchement par l'autorité "	96
Figure 40: Scénario des processus d'interface entre la démarche administrative et le traitement des transactions conformément aux exigences pertinentes	97
Figure 41: Points d'accès API de l'interface "démarche administrative↔traitement des transactions"	98
Figure 42: L'intégration d'une démarche administrative implémentée en externe comprend la redirection aller et retour.	99
Figure 43: Scénario SSO avec fournisseur d'identité partagé	101
Figure 44: Retour dans un scénario SSO avec FI partagé.....	102
Figure 45: Scénario SSO avec confiance bilatérale entre pairs (P2P trust)	104
Figure 46: Différence entre les cas A) et B) en ce qui concerne la redirection et l'accès direct alternatif	105
Figure 47: Un organisme de contrôle de l'Etat simplifie la position de confiance par rapport à la LoA du login au moyen d'une certification.....	106
Figure 48: Transmission des informations du contexte dans le cas A) via le <i>Context Token</i> en complément du <i>Identity Token</i> (comparer avec la Figure 43)	108
Figure 49: Transmission des informations contextuelles dans le cas B) en tant qu'ajout à la réponse du point de terminaison de l'API d'introspection (comparer la Figure 45).....	109
Figure 50: <i>API endpoint</i> pour les messages réponse pour la démarche administrative dans le cadre de l'interface pour l'intégration des démarches administratives implémentées en externe	111
Figure 51: Image globale d'une démarche administrative intégrée avec, derrière, l'interface encapsulée par le portail fournisseur vers le système métier interne de l'autorité.	112
Figure 52: Aperçu du flux de données des interfaces	113
Figure 53: Dépendance circulaire due à la responsabilité distribuée des interfaces.....	113

Figure 54: Dépendances claires entre les systèmes grâce à la définition et à la normalisation des responsabilités.....	114
Figure 55: Domaines d'intérêt de la gouvernance informatique	119
Figure 56: Feuille de route pour la mise en œuvre de la normalisation	125
Abbildung 57: Ein Behördenleistungsportal bietet dem User die für ihn relevanten Behördenleistungen an, egal auf welchem System sie primär implementiert sind [These-1] (UML Use Case Diagram)	137
Abbildung 58: Behördenleistungsportale präsentieren überlappende Sets an Leistungen [These-2]	139
Abbildung 59: Abbildung von Behördenleistungen auf verschiedenen ausgerichteten Portalen in jeweils individuellem Design (verbildlicht durch die verschiedenen farblichen Umrandungen der Ovale) [These-3]	141
Abbildung 60: Verortung Lieferobjekte bezüglich TOGAF-Steps	148
Abbildung 61: Scope des Projekts bezüglich TOGAF	149
Abbildung 62: Vermittlerdienst zwischen IdPs und Behördenleistungsportalen	151
Abbildung 63: Aussagen des BGEID [23] aus der Strukturperspektive	152
Abbildung 64: Die Nutzung eines E-ID-Systems als staatlich regulierte elektronische Identifizierungsmöglichkeit ist ein Schlüsselement der Sollarchitektur	155
Abbildung 65: In einem NP-Kundenkonto können mehrere Identifikatoren hinterlegt werden, mindestens jedoch die Versichertennummer, optional die E-ID-Registrierungsnummer	159
Abbildung 66: Die Nutzung des UPI-Registers und des entstehenden NAD für NP ist neben dem existierenden UID-Register für JP ein weiteres Schlüsselement der Sollarchitektur ...	160
Abbildung 67: Die Nutzung eines zentralen Infrastrukturdienstes für die Verwaltung der Bewirtschaftungsrechte ist ein weiteres Schlüsselement der Sollarchitektur	163
Abbildung 68: Ein geeignetes IAM-System kann die Aufgabe der zentralen Rechteverwaltung übernehmen und bringt darüber hinaus noch einen Vermittler ins Spiel	163
Abbildung 69: Muster eines Schalenmodells für ein Bewirtschaftungsrechtmodell	164
Abbildung 70: Muster eines Berechtigungsmodells mit einem geregelten und einem unregulierten Teil	165
Abbildung 71: Geschütztes Transportsystem für den zielgerichteten Datenaustausch bzw. die bidirektionale Kommunikation zwischen Behördenleistungsportalen und behördeninternem Fachsystemen	166
Abbildung 72: Beispiel einer Verwendung eines ESB auf Basis des WSO API Gateways bei FISCAL-IT	168
Abbildung 73: Kundensegmentierung Beispiel 1	170
Abbildung 74: Kundensegmentierung Beispiel 2	170

Liste des tableaux

Tableau 1: Explication des entités représentées dans le modèle d'information	44
Tableau 2: Conditions cadres pour le développement de l'architecture cible.....	54
Tableau 3: Principes de la déclaration de Tallinn sur la cyberadministration	55
Tableau 4: Besoins concernant l'intégration des prestations administratives.....	57
Tableau 5: Besoins en matière d'authentification et d'autorisation	58
Tableau 6: Besoins en matière de communication client - autorité	59
Tableau 7: Besoins d'interface utilisateur (UI)	60
Tableau 8: Besoins en matière de traitement des affaires	61
Tableau 9: Besoins concernant l'ISDS	63
Tableau 10: Besoins concernant les conditions cadres de mise en œuvre.....	63

Tableau 11: Délimitations du périmètre de l'architecture cible	65
Tableau 12: Attentes en matière de qualité pour l'architecture cible	66
Tableau 13: Traitement des <i>Interoperability Principles</i> du EIF dans l'étude	66
Tableau 14: Principes d'architecture pour l'architecture cible	69
Tableau 15: Modèle de niveau de confiance LoA selon eCH-0170 [21].....	88
Tableau 16: Modèle de niveau d'autorisation exemplaire.....	89
Tableau 17: Niveaux de qualité selon la norme eCH-0171 [22].....	90
Tableau 18: Résumé du cadre d'interopérabilité.....	91
Tableau 19: Évaluation des facteurs de risque en matière de SIPD en fonction du modèle d'intégration	116
Tableau 20: Exigences en matière de SIPD	117
Tableau 21: Traitement et mise en œuvre des besoins du chapitre 2.2.2 dans le développement de l'image cible au chapitre 2.4 et de l'architecture cible au chapitre 2.5 ...	120
Tableau 22: Mesures recommandées sous la responsabilité du SECO	125
Tableau 23: Mesures recommandées sous la responsabilité de l'ANS	126
Tabelle 24: Evaluation Lösungsvarianten [Herausforderung-1].....	154
Tabelle 25: Evaluation Lösungsvarianten [Herausforderung-2].....	157
Tabelle 26: Entscheidungsbaum bezüglich der Verfügbarkeit von Versichertennummer und/oder E-ID-Registrierungsnummer zur Verwendung als Identifikator bei der Eröffnung eines NP-Kundenkontos.....	159
Tabelle 27: Evaluation Lösungsvarianten [Herausforderung-3].....	161
Tabelle 28: Evaluation Lösungsvarianten [Herausforderung-4].....	165
Tabelle 29: Evaluation Lösungsvarianten [Herausforderung-5].....	168
Tabelle 30: Evaluation Lösungsvarianten [Herausforderung-6].....	172

Secrétariat d'État à l'économie SECO

Direction de la promotion économique

Secteur Politique PME

Holzikofenweg 36, 3003 Berne

Tél. +41 58 462 28 71

www.seco.admin.ch, www.kmu.admin.ch