

Studie Architekturreview EasyGov: Integrations-Sollarchitektur für Behördenleistungsportale

AWK Group AG

Januar 2022



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF
Staatssekretariat für Wirtschaft SECO
Direktion für Standortförderung

Impressum

Herausgeber

Staatssekretariat für Wirtschaft SECO, Direktion für Standortförderung, Ressort KMU-Politik

Auftraggeber

Martin Godel, Leiter KMU-Politik SECO und Auftraggeber EasyGov

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

Projektausschuss

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

David De Groot, Mitglied Planungsausschuss eGov-CH, Kanton 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

Fachausschuss

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

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, Kanton Freiburg

Jörg Pietschmann, IT-Unternehmensarchitekt, Kanton Luzern

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

Autoren

Peter Neidel, Projektleiter (AWK)

Olivier Thyès (AWK)

AWK Group AG

Laupenstrasse 4, CH - 3008 Bern

Tel.: +41 58 411 95 00

www.awk.ch

info@awk.ch

Management Summary

Ausgangslage und Ziel der Studie

Bürger, Bürgerinnen und Unternehmen möchten Behördenleistungen zunehmend digital beziehen. Nebst dem Komfortgewinn für die Benutzer durch einen medienbruchfreien Austausch mit Behörden von Bund, Kantonen und Gemeinden, können digital zur Verfügung gestellte Behördenleistungen flexibler, effizienter und in höherer Qualität durch die Behörden angeboten werden.

Der Aufbau des One-Stop-Shops für Behördenleistungen für Unternehmen unter dem Namen EasyGov.swiss ist ein strategisches Projekt von E-Government Schweiz. Die vorliegende Studie behandelt Massnahme M1 des Umsetzungsziels UZ1 des Umsetzungsplans von E-Government Schweiz für die Legislaturperiode 2020-2023: Architekturreview betreffend Machbarkeit der Integration von Bundes-, kantonalen und kommunalen Leistungen unter Einbezug der relevanten Akteure in einer Studie erstellen. Dazu soll in einem ersten Schritt eine übergreifende, grobe Integrations-Sollarchitektur für Behördenleistungsportale erarbeitet werden, welche den Entwurf eines eCH-Standards vorbereitet. Anschliessend soll in einem zweiten Schritt beurteilt werden, welche Anpassungen an EasyGov notwendig sind, um der übergreifenden Sollarchitektur gerecht zu werden (Gap-Analyse – nicht Bestandteil dieser Version der Studie).

Vorgehen

Der Architekturreview wurde in enger Abstimmung mit dem Planungsausschuss von E-Government Schweiz durchgeführt. Die Integrations-Sollarchitektur wurde iterativ in einer Workshop-Reihe zusammen mit Vertretern aller föderalen Ebenen erarbeitet.

Wichtigste Erkenntnisse zur Integrations-Sollarchitektur

1. Zielbild

Ausgangspunkt für das Zielbild war eine vorausgegangene Bedürfniserhebung, bei der sich aus den Perspektiven User/Kunde und Behörde/Portalbetreiber konkrete Pain Points herauskristallisierten:

- Der User möchte mit einem Login von einem Portal alles erledigen und nichts doppelt erfassen müssen
- Der Portalbetreiber möchte nicht für jede Integration (von externen Behördenleistungen) individuell Architektur und Schnittstellen verhandeln/umsetzen

Um den genannten Pain Points zu begegnen braucht es vor allem einen konzeptuellen gemeinsamen Nenner und - darauf aufbauend - ein ausreichendes Mass an Dateninteroperabilität. Das Zielbild lautet deshalb:

Die Standardisierung soll die für das Zusammenwirken der Behördenleistungsportale nötige Daten- und Prozessinteroperabilität ermöglichen.

2. Entwurf der Integrations-Sollarchitektur

Die einzelnen Standardisierungsthemen – abgeleitet von den Pain-Points – wurden in Form von Anforderungen an einen zukünftigen Standard spezifiziert, die so weit wie möglich Technologie-neutral gehalten wurden.

- In-Scope: interoperable Datenbereiche, Verantwortlichkeiten, Schnittstellen-Prozesse
- Out-of-Scope: Festlegung der Technologie, leistungsspezifische Datenbereiche

Im Ergebnis wurden definiert:

- Der **technologieneutrale Interoperabilitätsrahmen**: dieser legt fest, wie ein ausreichendes Mass an Dateninteroperabilität auf Ebene der Schnittstellen erreicht werden kann, um den Pain-Points zu begegnen. Dies beinhaltet unter anderem, wie die unterschiedlichen Entitäten (wie z.B. User, Behördenleistung, Bewirtschaftungsrecht) identifiziert werden und auf welche Art die dazugehörigen Daten interoperabel zu gestalten sind (interoperable Kerndaten). Auch ist im Interoperabilitätsrahmen definiert, welche Identifikationssysteme genutzt werden sollen (z.B. UID-Register).
- Die **Integrationsmuster** samt den nötigen Schnittstellen: dank der beiden Integrationsmuster «Implementation» und «Einbindung» kann ein Behördenleistungsportal eine extern zur Verfügung gestellte Behördenleistung auf zwei unterschiedliche Arten integrieren. Die entsprechenden Schnittstellenanforderungen wurden spezifiziert.
 - Im Fall der **Implementation** (oder Vollintegration) nutzt das Behördenleistungsportal Schnittstellen zu einem internen Fachsystem einer Behörde, um den entsprechenden Geschäftsfall vollumfänglich abzubilden. Für diesen Fall wurde ein Gerüst aus allgemeinen Kommunikationsprozessen spezifiziert, auf deren Basis leistungsspezifische Inhalte übermittelt werden (d.h. eine geregelte Abfolge von Meldungen zwischen den Systemen).
 - Im Fall der **Einbindung** (oder Teilintegration) wird eine bestehende, externe Implementierung eines Behördengangs genutzt, sodass u.a. die Weiterleitung der Usersession (mittels Single Sign-on) auf das entsprechende, externe Behördenleistungsportal für eine künftige Standardisierung spezifiziert wird.

3. Empfehlungen für das weitere Vorgehen

Die in dieser Studie entwickelte Integrations-Sollarchitektur für Behördenleistungsportale soll schrittweise umgesetzt werden. Die Roadmap ist in Phasen eingeteilt, sodass zu einem späteren Zeitpunkt über optionale Ausbauschritte entschieden werden kann.

Der in einer ersten Phase zu erarbeitende Standard soll die beiden Integrationsmuster unterstützen und dabei wo immer möglich auf zentrale Infrastrukturkomponenten verzichten. Der zu schaffende Standard beruht auf dem Prinzip «Peer-2-Peer», damit bestehende Implementierungen weitergenutzt und schnelle Ergebnisse erreicht werden können. In späteren Ausbauschritten können je nach Bedarf zentrale Komponenten eingeführt werden, um ein höheres Mass an Interoperabilität und eine entsprechende einfache Umsetzbarkeit künftiger Integrationen zu ermöglichen.

Den Prozess zur geplanten Umsetzung der Integrations-Sollarchitektur in Form eines oder mehrerer Standards sowie der Prüfung allfälliger zentraler Infrastrukturkomponenten soll die Organisation «Digitale Verwaltung Schweiz» (DVS) führen. Nach erfolgter Standardisierung wird die Umsetzung von Pilotprojekten mit Einbezug von Behörden unterschiedlicher föderaler Ebenen empfohlen.

Änderungsverzeichnis

Version	Datum	Änderung	Autor
0.01 - 0.05	10.09.2020	Initialisierung, Ausarbeitung Entwurf bis einschliesslich Kap. 2.3	Peter Neidel, Corinne Kuhn
0.08	29.09.2020	Aufnahme Rückmeldungen Fachausschuss Workshop vom 18.09.2020, sowie Review	Peter Neidel, Alexander Zurkinder
0.09-0.10	14.10.2020	Einarbeitung Rückmeldung Fachausschuss zum Review vom 29.09. bis einschliesslich Kap. 2.3, Entwurf für Kap. 2.4 Zielbild	Peter Neidel, Alexander Zurkinder
0.11-0.12	20.10.2020	Definition der Zielbilder, Einarbeitung weiterer Rückmeldungen des Fachausschusses.	Peter Neidel, Alexander Zurkinder
0.13	27.10.2020	Einarbeitung der Rückmeldungen aus dem Fachausschuss-Workshop vom 22.10.20, sowie Finalisierung des Kapitels Zielbild als Basis für den Zirkularreview durch den Fachausschuss.	Peter Neidel, Alexander Zurkinder
0.15	19.11.2020	Einarbeitung der Rückmeldungen aus dem Fachausschuss-Zirkularreview bis Kapitel Zielbild, sowie Formulierung der Herausforderungen als Vorbereitung auf den Fachausschuss-Workshop vom 25.11.2020.	Peter Neidel, Alexander Zurkinder
0.16-0.17	04.12.2020	Einarbeitung der Rückmeldungen aus dem Fachausschuss-Workshop vom 25.11.2020	Peter Neidel, Alexander Zurkinder
0.18	16.12.2020	Vorbereitung Fachausschuss-Workshop vom 16.12.2020. Einarbeitung Evaluation Lösungsvarianten	Peter Neidel, Alexander Zurkinder
0.19	06.01.2021	Einarbeitung der Rückmeldungen aus dem Fachausschuss-Workshop vom 16.12.2020	Peter Neidel, Alexander Zurkinder
0.20	04.02.2021	Einarbeitung der Rückmeldungen aus dem Fachausschuss-Workshop vom 18.01.2021	Peter Neidel
0.21	16.02.2021	Einarbeitung der Befunde aus dem Review der v0.20, Informationen zu NAD (HF-2)	Peter Neidel, Olivier Thyes
0.22	06.03.2021	Rückmeldungen aus FA-WS vom 1.3.2021 sowie vom 30.3.2021. Refactoring des Kapitels 2.1 zur Einarbeitung der präzisierten konzeptuellen Basis	Peter Neidel, Olivier Thyes
0.23	18.04.2021	Rückmeldungen aus FA-WS vom 30.3.2021 resp. dem anschliessenden Review. Kapitel 2.5.1 Standardisierungsthemen Kapitel 2.5.4 IT-Governance	Peter Neidel, Olivier Thyes
0.24-0.25	16.07.2021	Überarbeitung Kapitel 2.5.4, Kapitel 2.7 neu, Entwurf Management Summary	Olivier Thyes
0.25-0.29	04.08.2021	Refactoring der Studie nach Abschluss der FA-WS, Ausformulierung der Standardisierungsthemen sowie Finalisierung zum Review fähigen Entwurf V1	Peter Neidel
0.30-0.31	11.08.2021	Management Summary Bereinigung Anhänge, Prüfung Verweise Ergänzung Abkürzungen und Glossar Ergänzung Entscheide und Bedürfnisabdeckung	Olivier Thyes, Peter Neidel
0.89	18.08.2021	Ergänzung Kapitel 2.5 Bereit zum Review	Olivier Thyes, Peter Neidel

Version	Datum	Änderung	Autor
0.90	20.08.2021	Behebung Probleme mit Verweisen und Fussnoten	Olivier Thyès
0.91	15.09.2021	Überarbeitung nach 1. Review durch den Fachausschuss	Peter Neidel, Olivier Thyès
0.92	03.11.2021	Überarbeitung nach weiteren bilateralen Abklärungen und 2. Review, Bedürfnisabdeckung detailliert, Übersetzung ins Französisch	Peter Neidel, Olivier Thyès
0.93	17.12.2021	Finalisierung und Versand an den Auftraggeber zur finalen Prüfung	Peter Neidel, Olivier Thyès
0.94	12.01.2022	Einarbeitung Befunde des Auftraggebers, neues Management Summary, diverse kleine Änderungen.	Peter Neidel, Olivier Thyès
1.0	18.01.2022	Finale Version zur Abnahme durch den Projekt-ausschuss	Peter Neidel, Olivier Thyès

Referenzierte Dokumente

Nr.	Dokument	Beschreibung	Link
[1]	Projektinitialisierungsauftrag		Link
[2]	eCH-0039	E-Government-Schnittstelle für Dossiers und Dokumente	Link
[3]	eCH-0044	Datenstandard Austausch von Personenidentifikationen	Link
[4]	eCH-0058	Schnittstellenstandard Meldungsrahmen	Link
[5]	eCH-0084	UPI Declaration Interface	Link
[6]	eCH-0085	UPI Query Interface	Link
[7]	eCH-0086	UPI Compare Interface	Link
[8]	eCH-0088	Vorgaben zur Beschreibung von Behördengängen in der Schweiz	Link
[9]	eCH-0090	Sedex Umschlag	Link
[10]	eCH-0107	Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM)	Link
[11]	eCH-0158	BPMN-Modellierungskonventionen für die öffentliche Verwaltung	Link
[12]	eCH-0123	Architektur E-Government Schweiz: Vertrieb	Link
[13]	eCH-0124	Architektur E-Government Schweiz: Produktion	Link
[14]	eCH-0126	Architektur E-Government Schweiz: Rahmenkonzept „Vernetzte Verwaltung Schweiz“ (Langversion)	Link
[15]	eCH-0138	Rahmenkonzept zur Beschreibung und Dokumentation von Aufgaben, Leistungen, Prozessen und Zugangsstrukturen der öffentlichen Verwaltung der Schweiz	Link
[16]	eCH-0177	Informationsmodell zur Geschäftsabwicklung in einer vernetzten Verwaltung Schweiz	Link
[17]	EIF brochure	The new European Interoperability Framework	Link
[18]	EFD Portal Studie 1.0	Untersucht fachliche Anforderungen an eine zukünftige Portallösung des EFD und formuliert Lösungsansätze	Link
[19]	Umsetzungsplan 2020-2023	E-Government Schweiz Umsetzungsplan 2020–2023	Link
[20]	EIRA	European Interoperability Reference Architecture	Link

Nr.	Dokument	Beschreibung	Link
[21]	eCH-0170	Qualitätsmodell zur Authentifizierung von Subjekten	Link
[22]	eCH-0171	Qualitätsmodell der Attributwertbestätigung zur eID	Link
[23]	BGEID	Bundesgesetz über elektronische Identifizierungsdienste	Link
[24]	eCH-0074	Grundsätze zur grafischen Modellierung von Geschäftsprozessen	Link
[25]	eCH-0242	Modellierung von Geschäftsregeln	Link
[26]	SB000	IKT-Strategie des Bundes 2020-2023	Link
[27]	eCH-0070	Inventar der Leistungen der öffentlichen Verwaltung der Schweiz ("Leistungsinventar CH")	Link
[28]	eCH-0097	Datenstandard Unternehmensidentifikation	Link
[29]	eCH-0098	Datenstandard Unternehmensdaten	Link
[30]	eCH-0108	Datenstandard Unternehmensregister	Link
[31]	eCH-0224	Vermittlerbasierte Identity Federation Architekturmodelle	Link
[32]	eCH-0225	Vermittlerbasierte Identity Federations – Implementierung mit OIDC	Link
[33]	GSVB ausländische Unternehmen UID BUR	BK/DTI: Studie ausländische Unternehmen im UID/BUR (V1 vom 29.04.2021)	
[34]	API-Architektur Bund	BK/DTI: Konzept zur API-Architektur im Bund (V0.9 vom 23.07.2021)	
[35]	eCH-0147	Nachrichtengruppe GEVER	Link
[36]	Zielbild E-ID	Diskussionspapier zum «Zielbild E-ID»	Link
[37]	Grundlagenbericht DVS	Grundlagenbericht «Digitale Verwaltung Schweiz»	Link
[38]	Kundenanliegen NP	Amtlich einfach - Lebenslagen Bürger	Link
[39]	Kundenanliegen JP	Amtlich einfach - Lebenslagen Unternehmen	Link
[40]	EasyGov SysArch	EasyGov Systemarchitektur v1.13 TC, Stand 1.11.2021	Link
[41]	Strategie Digitale Schweiz	Strategie Digitale Schweiz (September 2018) Strategie Digitale Schweiz (September 2020)	Link Link

Verwendete Abkürzungen

Abkürzung	Bedeutung
1FA	Ein-Faktor-Authentifizierung
2FA	Zwei-Faktor-Authentifizierung
A2A	Administration to Administration, womit gemäss [17] Interaktionen zwischen öffentlichen Verwaltungen gemeint sind, auch G2G genannt
A2B	Administration to Business, womit gemäss [17] Interaktionen zwischen öffentlichen Verwaltungen und juristischen Personen gemeint sind, auch G2B genannt
A2C	Administration to Citizen, womit gemäss [17] Interaktionen zwischen öffentlichen Verwaltungen und natürlichen Personen gemeint sind, auch G2C genannt
ADG	Adressdienstgesetz (Bundesgesetz über das nationale System zur Abfrage von Adressen natürlicher Personen)
AHV	Alters- und Hinterlassenenversicherung
AHVN13	13-stellige AHV-Nummer
AKV	Aufgaben, Kompetenzen und Verantwortlichkeiten
ALV	Arbeitslosenversicherung

Abkürzung	Bedeutung
API	Application Programming Interface
BIT	Bundesamt für Informatik und Telekommunikation
BFS	Bundesamt für Statistik
BLW	Bundesamt für Landwirtschaft
BK	Bundeskanzlei
DSG	Datenschutzgesetzgebung
DTI	Digitale Transformation und IKT-Lenkung (Bereich der BK)
DVS	Digitale Verwaltung Schweiz
EFD	Eidgenössisches Finanzdepartement
EIF	European Interoperability Framework
ESTV	Eidgenössische Steuerverwaltung
GSVB	Gemeinsame Stammdatenverwaltung Bund
IAM	Identity and Access Management
IdP	Identitätsprovider
IKT	Informations- & Kommunikationstechnik
ISDS	Informationssicherheit und den Datenschutz
JP	Juristische Person
LoA	Level of Assurance
NAD	Nationaler Adressdienst
NP	Natürliche Person
P2P	Peer-to-Peer
PAMS	Polymorphic Access Management System
PP	Pain Point
RFC	Request For Change
SEA	Search Engine Advertising
SECO	Staatsekretariat für Wirtschaft
SEO	Search Engine Optimization
SLA	Service Level Agreement
SLO	Single Logout
SSO	Single Sign On
TOGAF	The Open Group Architecture Framework
UI	User Interface
UID	Unternehmensidentifikationsnummer
UPI	Unique Person Identification
UX	User Experience
UZ	Umsetzungsziel
ZAS	Zentrale Ausgleichsstelle

Inhaltsverzeichnis

Management Summary	2
<i>Änderungsverzeichnis</i>	<i>4</i>
<i>Referenzierte Dokumente</i>	<i>5</i>
<i>Verwendete Abkürzungen.....</i>	<i>6</i>
0 Zusammenfassung.....	11
0.1 Ausgangslage und Ziel der Studie.....	11
0.2 Vorgehen	12
0.3 Ergebnisse Schritt1: Integrations-Sollarchitektur für Behördenleistungsportale 12	
0.3.1 Konzeptuelles Fundament.....	12
0.3.2 Zielbild.....	16
0.3.3 Entwurf der Integrations-Sollarchitektur.....	17
0.3.3.1 Standardisierungsthemen	17
0.3.3.2 Interoperabilitätsrahmen	17
0.3.3.3 Schnittstellen.....	18
0.3.4 Empfehlungen für das weitere Vorgehen.....	20
0.4 Ergebnisse Schritt 2: Gap-Analyse EasyGov.....	21
1 Ausgangslage und Ziel der Studie.....	22
1.1 Politische und gesetzliche Ebene	22
1.2 Zielsetzung «Digitale Verwaltung Schweiz».....	22
1.3 Umsetzungsziel UZ1 von E-Government Schweiz	23
2 Integrations-Sollarchitektur für Behördenleistungsportale	25
2.1 Situationsanalyse von Behördenleistungsportalen aus logischer Sicht	25
2.1.1 Prozesssicht einer Behördenleistung	25
2.1.2 Behördenleistungsportal als digitaler Zugangskanal.....	31
2.1.3 Funktionelle Struktur eines Behördenleistungsportals.....	33
2.1.4 Portallandschaft der Behördenleistungsportale	36
2.1.5 Informationsmodell der wichtigsten Begriffe.....	43
2.1.6 Integrationsmuster für die Abbildung von Behördengängen	48
2.2 Bedürfnisse an die Domäne Behördenleistungsportale aus Business-Sicht	52
2.2.1 Rahmenbedingungen.....	52
2.2.2 Bedürfnisse	53
2.2.2.1 Kategorisierung gemäss Tallinn-Deklaration zum E-Government.....	54
2.2.2.2 Strukturierung der Bedürfniserhebung.....	54
2.2.2.3 Bedürfnisse bezüglich der Integration von Behördenleistungen	55
2.2.2.4 Bedürfnisse bezüglich Authentisierung und Autorisierung.....	56
2.2.2.5 Bedürfnisse bezüglich Kommunikation Kunde – Behörde	57
2.2.2.6 Bedürfnisse bezüglich Präsentation (UI)	58
2.2.2.7 Bedürfnisse bezüglich Geschäftsabwicklung von Behördenleistungen.....	59
2.2.2.8 Bedürfnisse bezüglich ISDS.....	61

2.2.2.9	Bedürfnisse bezüglich der Umsetzung und des Betriebes	61
2.2.2.10	Verteilung der Bedürfnisse nach Kategorien.....	62
2.2.3	Abgrenzungen	63
2.2.4	Qualitätserwartungen an die Sollarchitektur	63
2.3	Architekturprinzipien	64
2.3.1	Vorbetrachtung: Interoperability Principles des EIF	64
2.3.2	Architekturprinzipien zur Sollarchitektur.....	67
2.4	Zielbild.....	69
2.5	Entwicklung der Integrations-Sollarchitektur	74
2.5.1	Standardisierungsthemen.....	75
2.5.1.1	Interoperabilitätsrahmen	75
2.5.1.1.1	Informationsmodell	77
2.5.1.1.2	Identifikation Behördenleistung	79
2.5.1.1.3	Identifikation Kundenanliegen.....	79
2.5.1.1.4	Identifikation Kunde und Stammdatenmanagement	79
2.5.1.1.5	Prozessmetadaten von Behördengang und Geschäftsfall	83
2.5.1.1.6	Userkonto	84
2.5.1.1.7	Zusammenfassende Übersicht Interoperabilitätsrahmen	88
2.5.1.2	Schnittstelle Behördengang↔Geschäftsfallbearbeitung	90
2.5.1.3	Schnittstelle zur Einbindung extern implementierter Behördengänge.....	96
2.5.1.3.1	Single Sign On (SSO).....	97
2.5.1.3.2	Kontextsynchronisation	105
2.5.1.3.3	Single Logout (SLO).....	108
2.5.1.3.4	Rückkanal für den Behördengang (Status, behördliche Benachrichtigungen, Ergebnisdokumente)	108
2.5.1.4	Schnittstellen-Datenfluss im Überblick	109
2.5.1.5	Schnittstellen-Verantwortung.....	111
2.5.2	ISDS-Themen	113
2.5.2.1	Identifizierung des Schutzbedarfs	113
2.5.2.2	Exkurs: ISDS-Anforderungen der Behörde	113
2.5.2.3	Exkurs: ISDS-Anforderungen an das Behördenleistungsportal.....	115
2.5.3	Rechtliche Fragen.....	116
2.5.4	IT-Governance	116
2.5.4.1	IT-Governance im Kontext der Integrations-Sollarchitektur	116
2.5.4.2	Anforderungen an die IT-Governance.....	117
2.6	Bedürfnisabdeckung	117
2.7	Empfehlungen für das weitere Vorgehen.....	121
2.7.1	Umsetzungs-Roadmap.....	121
2.7.2	Handlungsempfehlungen	123
3	Gapanalyse Ist-Architektur EasyGov bezüglich Integrations-Sollarchitektur	125
3.1	Identifizierte Gaps	125
3.2	Grobplanung zur Gap-Beseitigung	125
4	Anhänge	125

<i>Abbildungsverzeichnis</i>	185
<i>Tabellenverzeichnis</i>	187

Hinweis: Das in dieser Studie gewählte generische Maskulinum bezieht sich zugleich auf die männliche, die weibliche und andere Geschlechteridentitäten. Zur besseren Lesbarkeit wird auf die Verwendung männlicher und weiblicher Sprachformen verzichtet. Alle Geschlechteridentitäten werden ausdrücklich mitgemeint, soweit die Aussagen dies erfordern.

0 Zusammenfassung

0.1 Ausgangslage und Ziel der Studie

Bürger, Bürgerinnen und Unternehmen möchten Behördenleistungen zunehmend digital beziehen. Nebst dem Komfortgewinn für die Benutzer durch einen medienbruchfreien Austausch mit Behörden von Bund, Kantonen und Gemeinden, können digital zur Verfügung gestellte Behördenleistungen flexibler, effizienter und in höherer Qualität durch die Behörden angeboten werden.

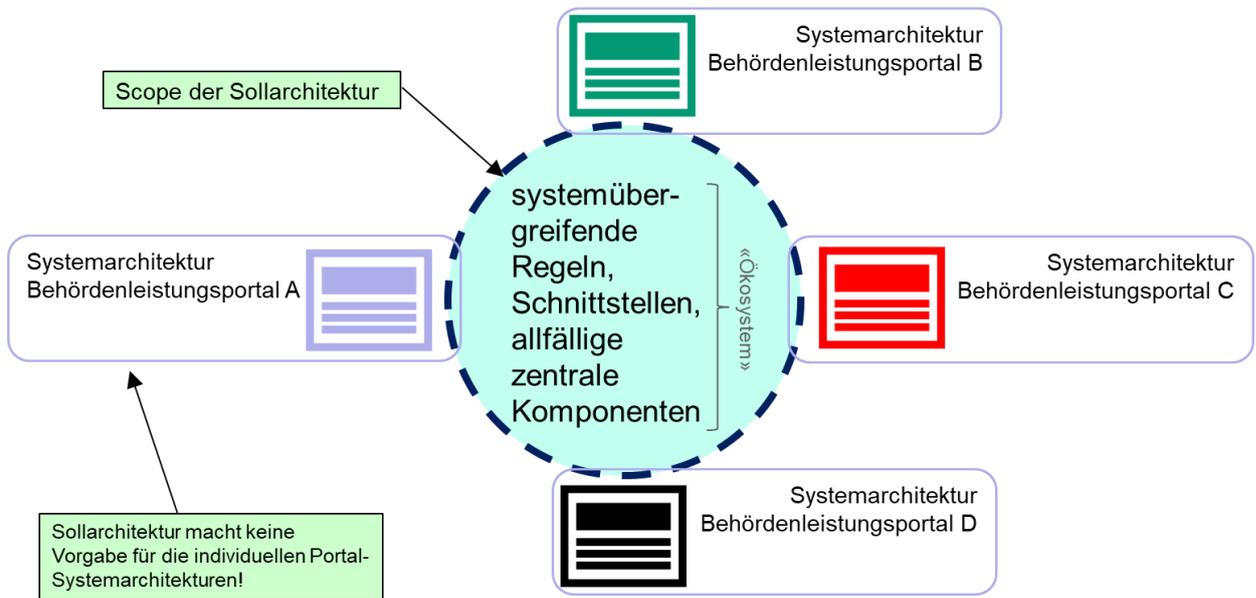
Verschiedene Organisationen und Strategien tragen zur Umsetzung der digitalen Transformation auf allen föderalen Ebenen bei, so beispielsweise die Organisation «Digitale Verwaltung Schweiz» und die IKT-Strategie des Bundes. Die Rechtsgrundlagen bilden unter anderem das Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben und das Unternehmensentlastungsgesetz.

Der Aufbau des One-Stop-Shops für Behördenleistungen für Unternehmen unter dem Namen EasyGov.swiss ist ein strategisches Projekt von E-Government Schweiz. Der Umsetzungsplan definiert für die Legislaturperiode 2020-2023 Umsetzungsziel 1 (UZ1) zwei Massnahmen:

- M1: Architekturreview betreffend Machbarkeit der Integration von Bundes-, kantonalen und kommunalen Leistungen unter Einbezug der relevanten Akteure in einer Studie erstellen.
- M2: Integration von kantonalen Behördenleistungen für Unternehmen, die von mehreren Kantonen gewünscht werden, auf EasyGov sicherstellen.

Die vorliegende Studie behandelt Massnahme M1 «Architekturreview». Dazu soll in einem ersten Schritt eine **generelle** übergreifende Integrations-Sollarchitektur für Behördenleistungsportale für juristische und natürliche Personen erarbeitet werden, welche den Entwurf eines eCH-Standards vorbereitet. Anschliessend soll in einem zweiten Schritt beurteilt werden, welche Anpassungen an EasyGov notwendig sind, um der übergreifenden Sollarchitektur gerecht zu werden (Gap-Analyse).

Die angestrebte Integrations-Sollarchitektur für Behördenleistungsportale fokussiert nicht auf die Systemarchitekturen einzelner Portale, sondern vielmehr auf ein portalübergreifendes "Ökosystem", welches das Zusammenspiel regelt und die Interoperabilität verbessert, siehe folgende Grafik:



0.2 Vorgehen

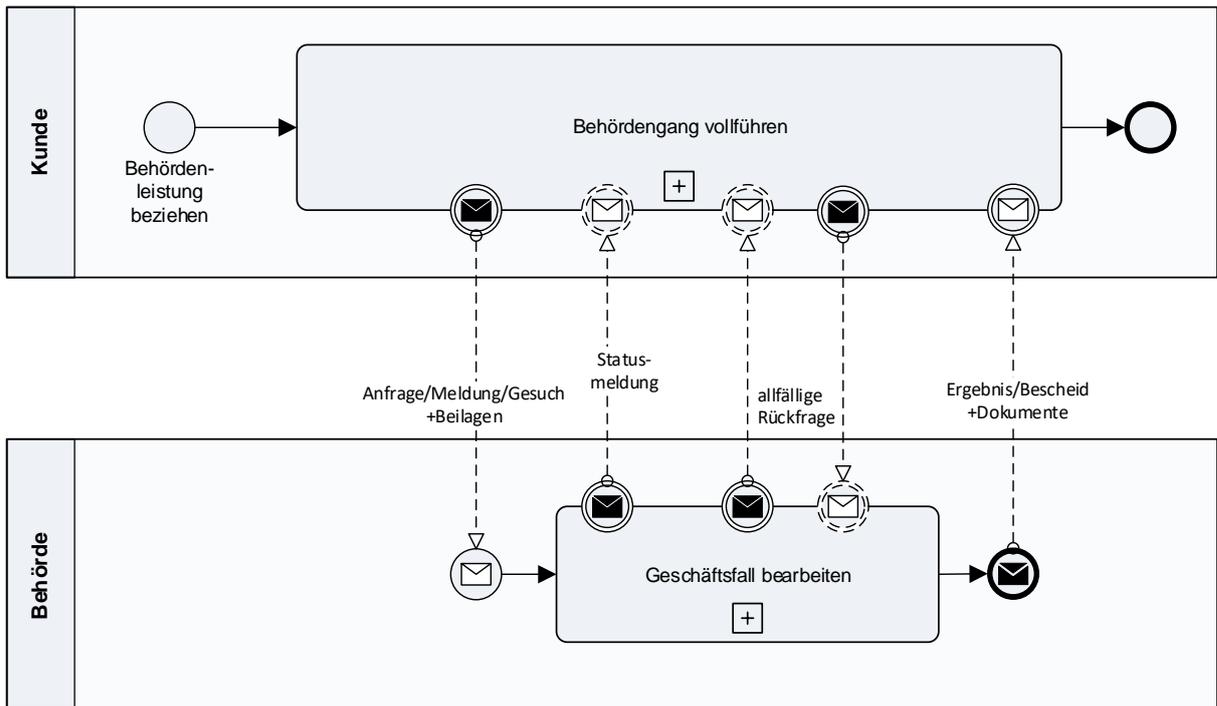
Der Architekturreview wurde in enger Abstimmung mit dem Planungsausschuss von E-Government Schweiz durchgeführt. Die Integrations-Sollarchitektur wurde iterativ in einer Workshop-Reihe zusammen mit Vertretern aller föderalen Ebenen erarbeitet:

- Vertreter Bundesverwaltung: BK, ISB, EFD, WBF, UVEK
- Kantonale Vertreter E-Government
- Kantonale Vertreter ICT-Architektur, inkl. iGovPortal
- Vertreter von Städten, insb. Stadt Zürich
- Geschäftsstelle E-Government Schweiz

0.3 Ergebnisse Schritt1: Integrations-Sollarchitektur für Behördenleistungsportale

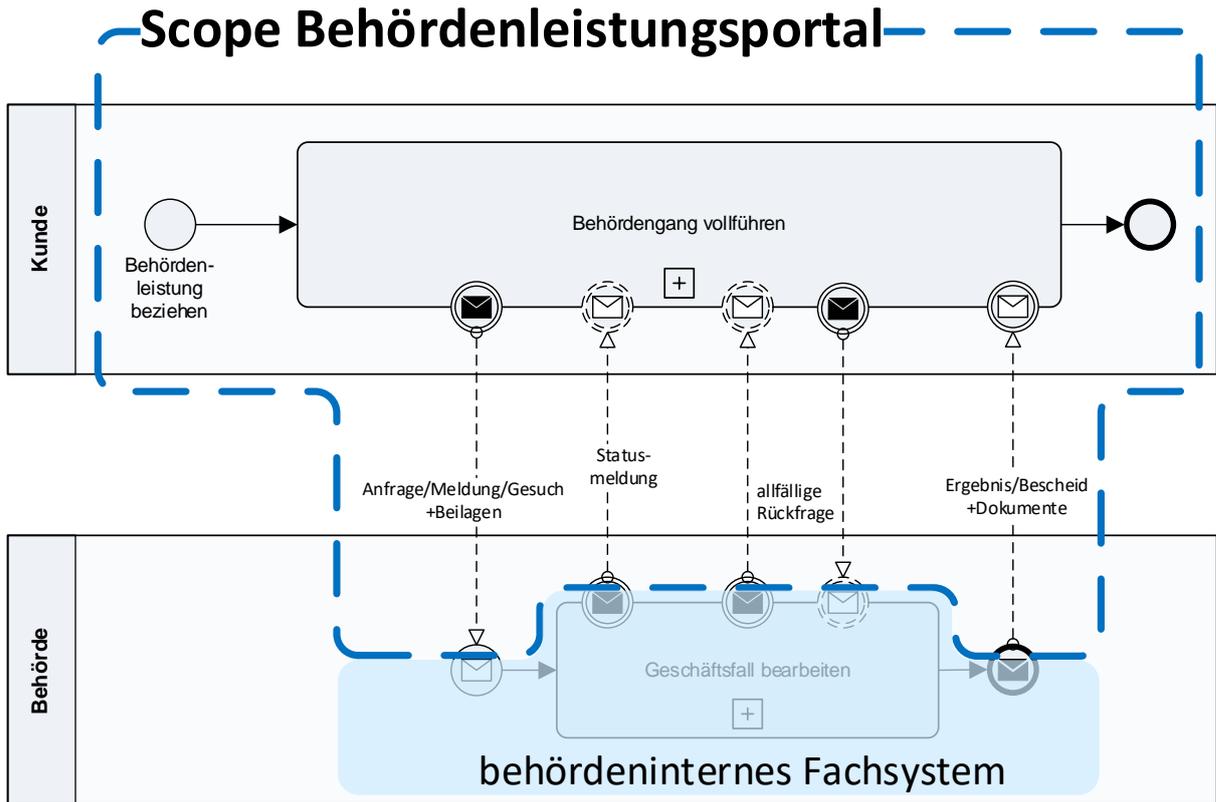
0.3.1 Konzeptuelles Fundament

Eine Behördenleistung kann stark abstrahiert als parallel auf Kunden- und Behördenseite laufende Prozesse dargestellt werden:

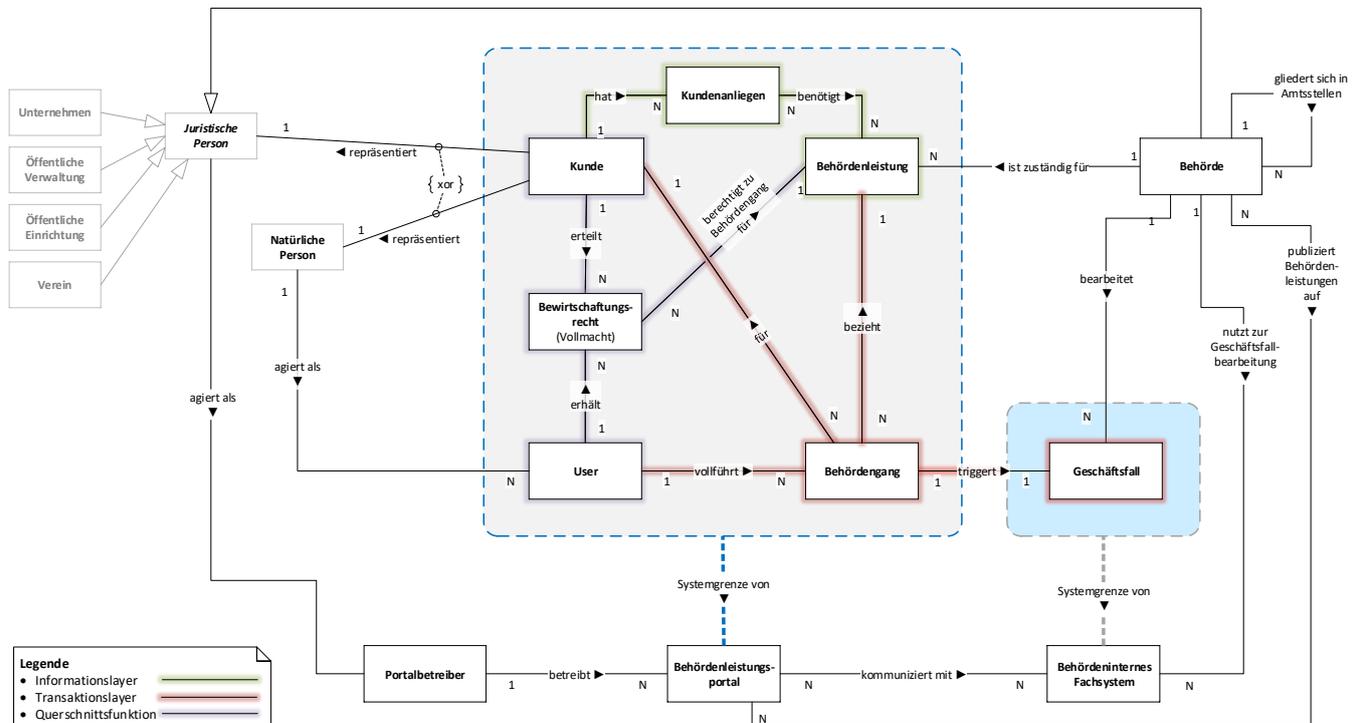


Mit Hilfe eines Behördenleistungsportals bietet ein Portalbetreiber Behördenleistungen dem Kunden auf digitaler Ebene an. Es stellt einen Zugangskanal für den Kunden auf ein oder mehrere Behördengänge dar. Das Behördenleistungsportal kommuniziert mit dem Fachsystem¹ der zuständigen Behörde, in dem die Geschäftsbearbeitung stattfindet. Ein Behördenleistungsportal kann als Kunden-Front-End verstanden werden, welches die Schnittstelle zwischen Kunde und Behörde unterstützt:

¹ Aus Sicht des Portals kann das behördeninterne Fachsystem auch als Back-End aufgefasst werden. Da dies an die Perspektive gebunden ist, wird es in dieser Studie nicht so bezeichnet.



Ausgehend von der prozessualen Betrachtung und des branchenüblichen Sprachgebrauchs wurden die aus Architektursicht wichtigsten Begriffe im Kontext von Behördenleistungsportalen in einem Informationsmodell in Beziehung gebracht:



(Vergrößerte Darstellung im Querformat in Anhang B)

Hinweise:

- Die beiden farbig hinterlegten Flächen umreißen jeweils den inhaltlichen Scope von Behördenleistungsportal bzw. behördeninternem Fachsystem
- Die in der Abbildung grau umrandeten Entitäten dienen der Illustration. So wird z.B. aufgezeigt, dass als Kunde entweder eine juristische Person (z.B. in Form eines Unternehmens) oder eine natürliche Person auftritt. Letztere kann zusätzlich auch als User mit dem Behördenleistungsportal interagieren.

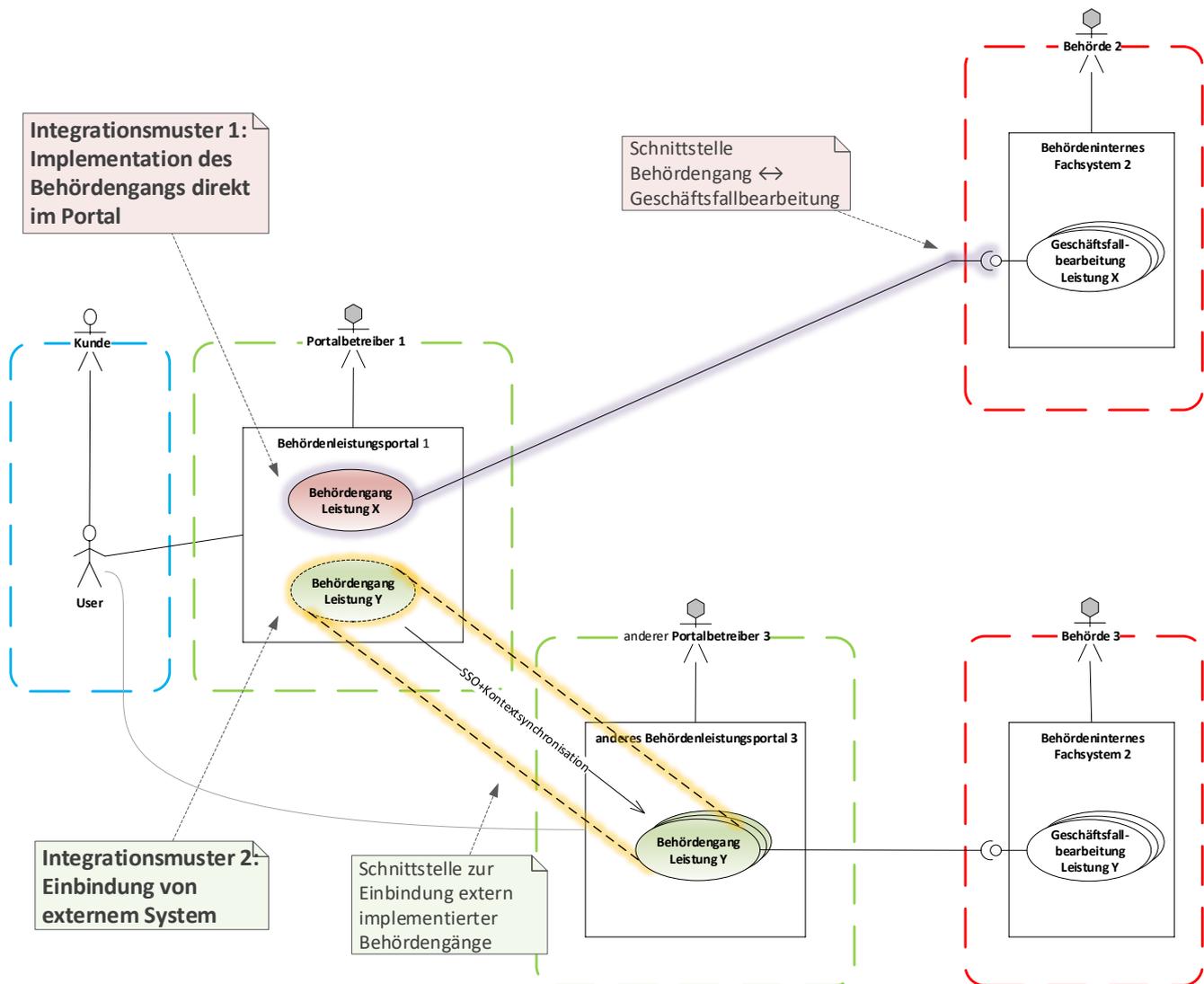
Typischerweise werden für die digitale Abbildung von Behördenleistungen folgende Funktionalitäten benötigt (siehe Legende im obigen Informationsmodell)

- Informationslayer: Übersicht des Leistungsangebots (Behördenleistungen) und Orchestrierung von komplexeren Behördenleistungen mittels Wizards (z.B. Unternehmensgründung)
- Querschnittsfunktionen: Userkonto, Berechtigungsmanagement, Kundenkonto, Status der Behördengänge, Benachrichtigungen von Behörden, Dokumentenablage
- Transaktionslayer: Behördengang (Bezug der Behördenleistung)

Folgende Integrationsmuster sind auf Stufe Transaktionslayer hinsichtlich des Systemzuschnitts typischerweise in der Praxis anzutreffen:

- Integrationsmuster 1: **Implementation** des Behördengangs **direkt** im Portal via Schnittstelle zum behördeninternen Fachsystem
- Integrationsmuster 2: **Einbindung** eines **extern** implementierten Behördengangs via SSO-Weiterleitung

Die Integrations-Sollarchitektur baut auf diesen beiden Integrationsmustern auf. Sie können auch als Mischform auftreten, wie nachfolgende Grafik exemplarisch an einem fiktiven Portal veranschaulicht:



0.3.2 Zielbild

Ausgangspunkt für das Zielbild war eine vorausgegangene Bedürfniserhebung, bei der sich folgende Pain Points herauskristallisierten:

- Pain Point 1: Der User möchte am liebsten mit einem Login von einem Portal alles erledigen und nichts doppelt erfassen müssen und erwartet eine auf sein jeweiliges Anliegen ausgerichtete Orchestrierung der dafür nötigen Behördenleistungen

In dem Bemühen der Portalbetreiber, diesem Bedürfnis durch integrative Angebote Rechnung zu tragen, indem sie Behördengänge verschiedener Zuständigkeiten implementieren oder von anderen Systemen einbinden, ergeben sich zwei weitere Pain Points:

- Paint Point 2: Der Portalbetreiber möchte nicht für jede Einbindung individuell Architektur und Schnittstellen verhandeln/umsetzen
- Paint Point 3: Der Portalbetreiber möchte nicht für jeden Behördengang individuelle Schnittstellen zur Geschäftsfallbearbeitung implementieren, dies gilt umgekehrt auch für die Behörde

Um die genannten Pain Points zu beheben, braucht es vor allem einen konzeptuellen gemeinsamen Nenner und - darauf aufbauend - ein ausreichendes Mass an Dateninteroperabilität. Das Zielbild lautet deshalb:

Die Standardisierung soll die für das Zusammenwirken der Behördenleistungsportale nötige Daten- und Prozessinteroperabilität ermöglichen.

0.3.3 Entwurf der Integrations-Sollarchitektur

Im Sinne des Zielbildes wird die Integrations-Sollarchitektur grob entwickelt. "Grob" bedeutet dabei, es werden die zu regelnden Themenbereiche abgesteckt und darin fundamentale Festlegungen getroffen, aber es erfolgt keine detaillierte Spezifikation. Es werden Anforderungen formuliert, was die angestrebte Standardisierung konkret leisten soll und wie das logische Gerüst dazu aussieht.

0.3.3.1 Standardisierungsthemen

Die einzelnen Themen werden in Form von Anforderungen an einen zukünftigen Standard spezifiziert, die so weit wie möglich Technologie-neutral gehalten sind.

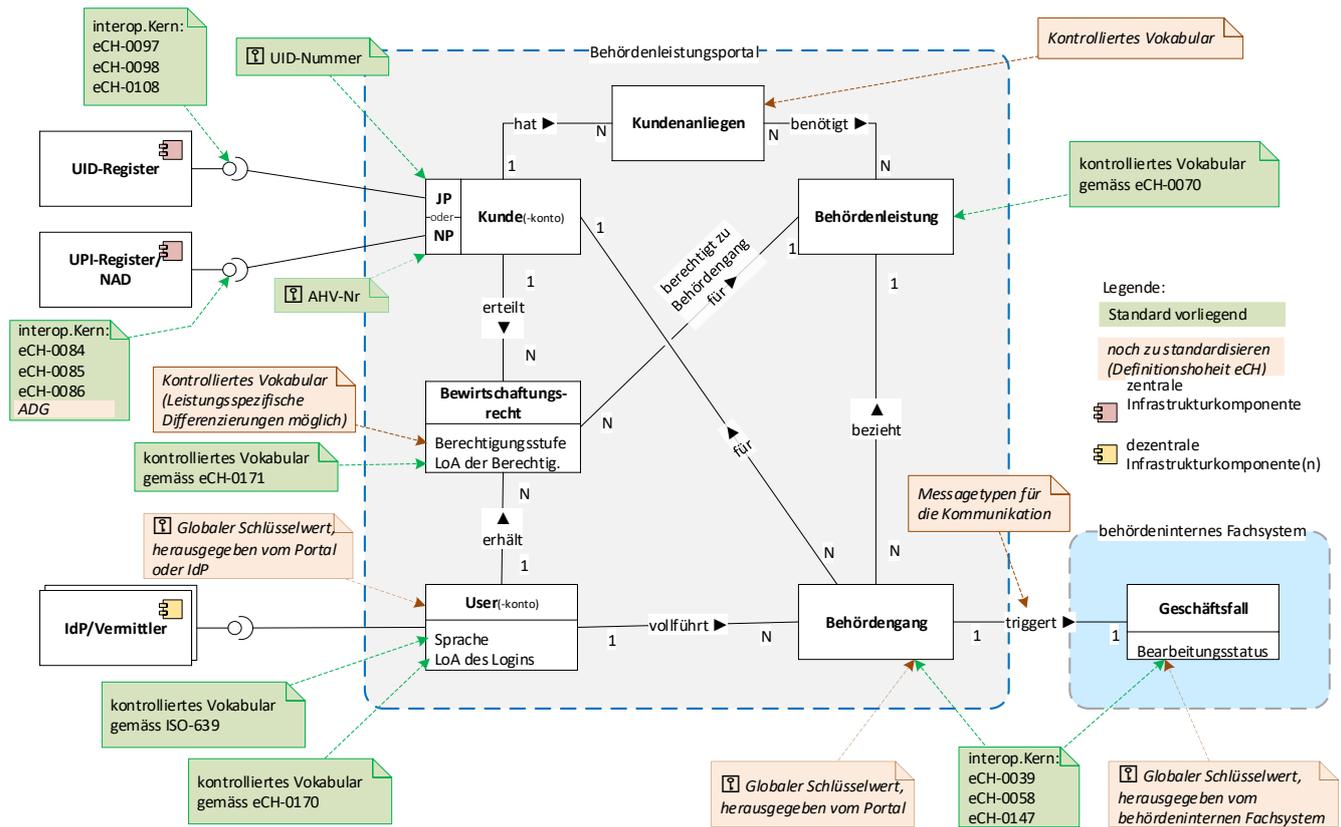
- In-Scope:
 - interoperable Datenbereiche (z.B. Identifikatoren)
 - Verantwortlichkeiten (Definitionshoheit, Datenhoheit)
 - Schnittstellen-Prozesse
- Out-of-Scope:
 - Festlegung der Technologie (z.B. Protokoll, allfälliges Bus-System)
 - leistungsspezifische Datenbereiche

0.3.3.2 Interoperabilitätsrahmen

Um den im Zielbild genannten drei Pain Points zu begegnen, braucht es vor allem ein ausreichendes Mass an Dateninteroperabilität auf Ebene der Schnittstellen. Der Interoperabilitätsrahmen definiert in diesem Sinne auf der Basis des oben gezeigten Informationsmodells:

- Identifikationssysteme und kontrolliertes Vokabular
- Festlegung der interoperablen Kerndaten

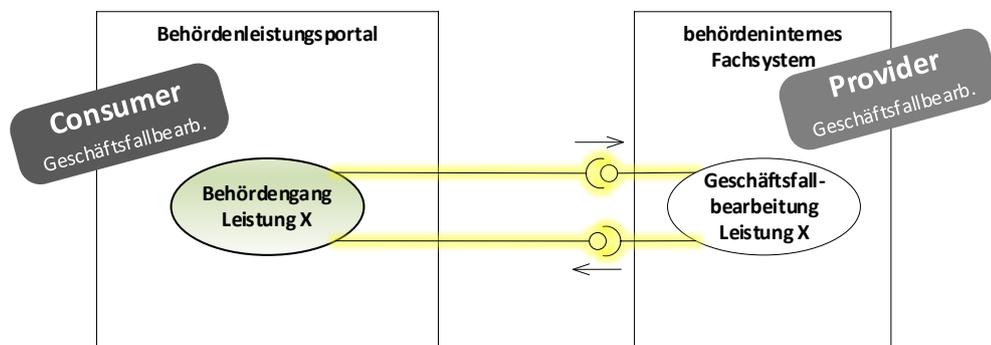
Das folgende Bild verortet die Elemente des Interoperabilitätsrahmens im Informationsmodell:



0.3.3.3 Schnittstellen

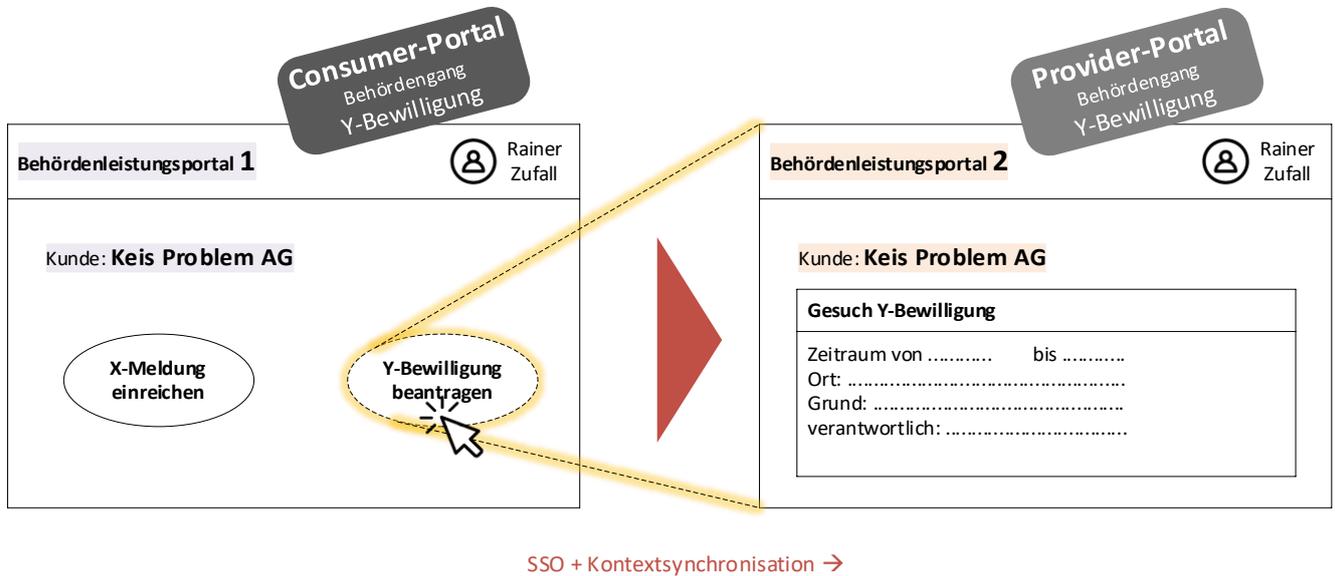
Auf dem Interoperabilitätsrahmen aufbauend werden die mit den beiden Integrationsmustern verbundenen Schnittstellen standardisiert, um Pain Point 2 und 3 zu begegnen. Beide Integrationsmuster unterstützen wiederum im Sinne von Pain Point 1/1a den Aufbau von behördenübergreifenden Portalen, die auf dedizierte Kundensegmente fokussieren.

Für die **Schnittstelle Behördengang ↔ Geschäftsfallbearbeitung** des Integrationsmusters 1 wird der vorausgehenden prozessualen Betrachtung in Abschnitt 0.3.1 folgend ein Gerüst aus allgemeinen Kommunikationsprozessen spezifiziert, auf deren Basis leistungsspezifische Inhalte übermittelt werden. Mit diesen Bausteinen können auch Besonderheiten im Verfahrensablauf wie Subprozess, Verfahrenweitergabe oder behördenseitiger Prozessanstoß abgebildet werden.



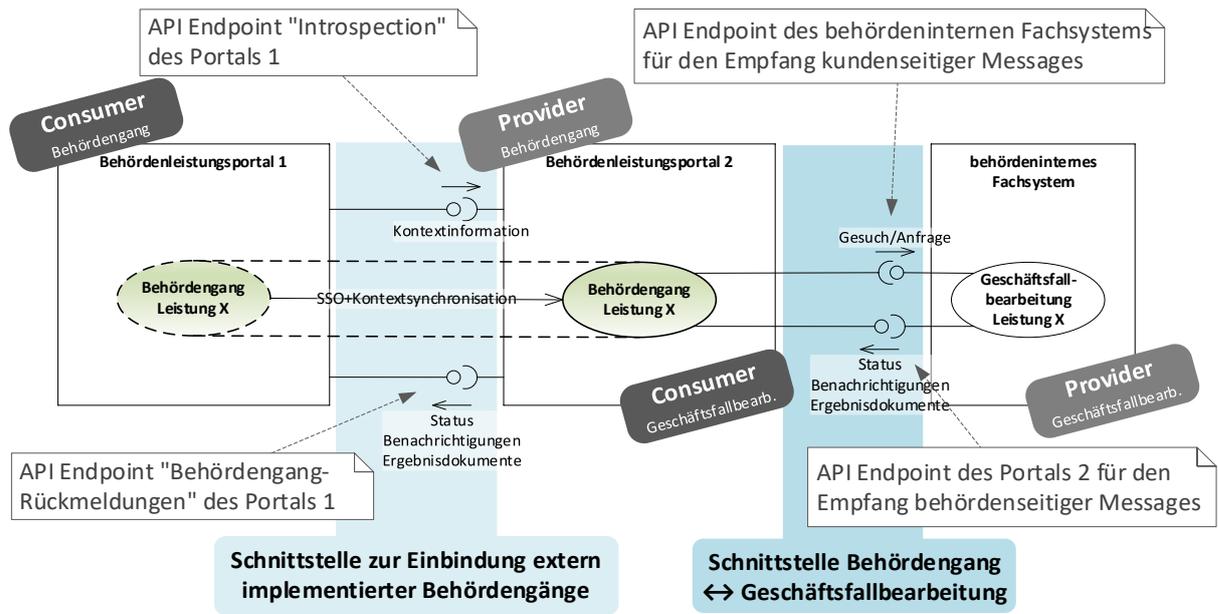
Wesentliches Element der **Schnittstelle zur Einbindung extern implementierter Behördengänge** des Integrationsmusters 2 ist die Weiterleitung, d.h. die Übertragung der Usersession vom Portal auf das externe System bzw. Provider-Portal zur Laufzeit. Damit der User beim Sprung in den eingebetteten – auf einem anderen Portal implementierten – Behördengang nahtlos

weiterarbeiten kann, muss die Übertragung bzw. Weiterleitung mit Single Sign On (SSO) und Kontextsynchronisation einhergehen. Es werden die dazu nötigen Schnittstellenprozesse benannt und auf logischer Ebene spezifiziert, die neben der Behördengang-Adressierung auch den Kontext des Behördengangs im Consumer-Portal, bestehend aus korrespondierendem User-Login, Kundenselektion und dazugehörigem Bewirtschaftungsrecht auf das Provider-Portal übertragen, wie folgendes Bild illustriert:



Es werden Szenarien aufgezeigt, wie die Schnittstelle in der Konstellation A) Gemeinsamer Identitätsprovider und in der Konstellation B) bilaterale Peer-to-Peer Trust funktioniert. Da B) Peer-to-Peer Trust eine vom Identitätsprovider entkoppelte Lösung darstellt, wird diese gegenüber A) letztlich präferiert.

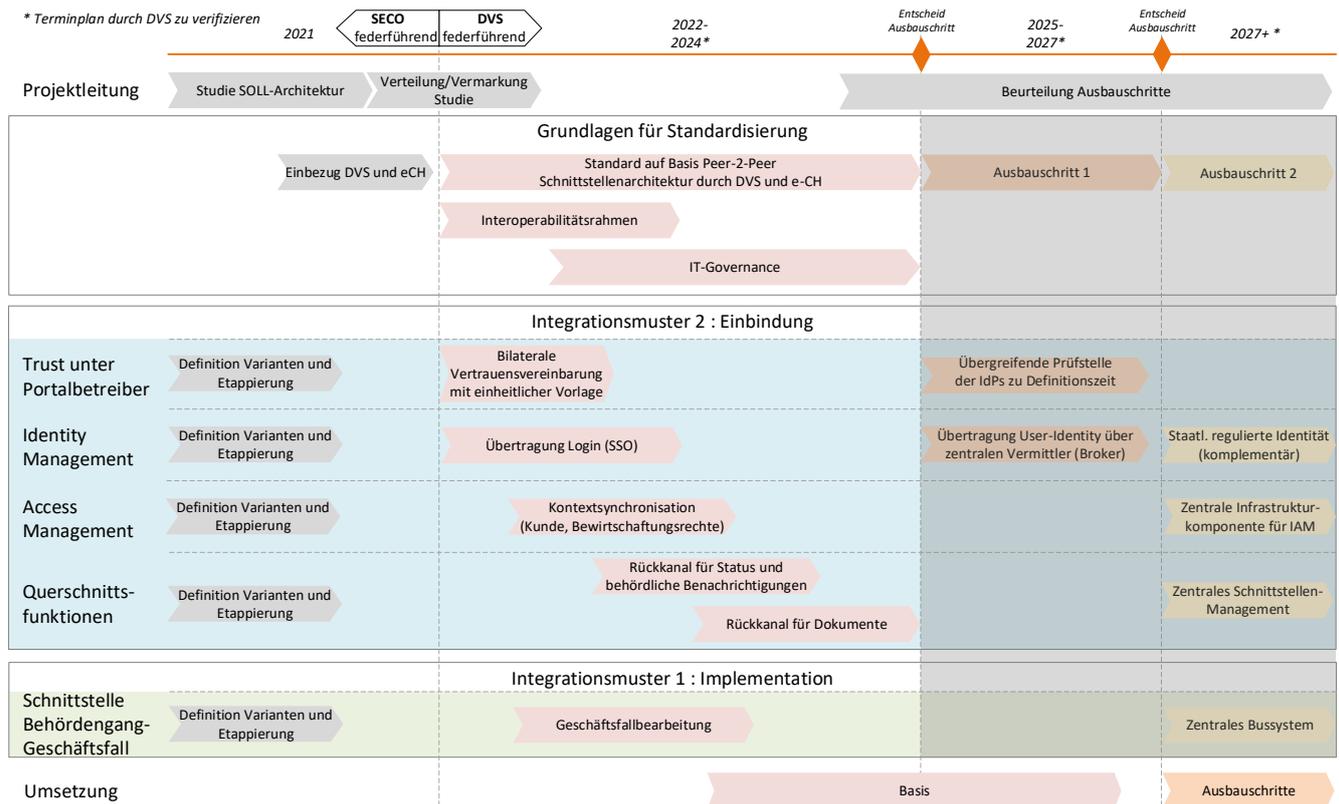
Die nachfolgende Grafik zeigt das Gesamtbild der beschriebenen Schnittstellen am Beispiel eines per Peer-to-Peer Trust eingebundenen Behördengangs, dessen Implementation im Provider-Portal mit dem dahinterstehenden zuständigen behördeninternen Fachsystem kommuniziert:



Abschliessend trifft der Entwurf der Integrations-Sollarchitektur für beide Schnittstellen die Festlegung, dass die Definitionshoheit zu deren Ausgestaltung über die Standardisierung hinaus beim jeweiligen Provider liegt. Im Fall von Integrationsmuster 1 betrifft das das behördeninterne Fachsystem, im Fall von Integrationsmuster 2 das Provider-Portal.

0.3.4 Empfehlungen für das weitere Vorgehen

Die in dieser Studie entwickelte Integrations-Sollarchitektur für Behördenleistungsportale soll schrittweise umgesetzt werden. Die Roadmap ist in Phasen eingeteilt, sodass zu einem späteren Zeitpunkt über optionale Ausbauschritte entschieden werden kann.



(Vergrößerte Darstellung im Querformat in Anhang D)

Den Prozess zur geplanten Umsetzung der Integrations-Sollarchitektur in Form eines oder mehrerer Standards soll die Organisation «Digitale Verwaltung Schweiz» (DVS) führen. In einem ersten Schritt soll die DVS die Umsetzungs-Roadmap prüfen und Arbeitsgruppen für die Etablierung eines Standards und die Schaffung der Rechtsgrundlagen initialisieren. Um die Standardisierung auf Erfahrungswerten abstützen zu können, wird die Umsetzung von Pilotprojekten mit Einbezug von Behörden auf allen föderalen Ebenen empfohlen.

Das SECO als Auftraggeber dieser Studie beteiligt sich an der DVS-Ambition «Behördenübergreifende digitale Identifikation ist etabliert» (siehe Grundlagenbericht [37]) und liefert mit der Studie einen wichtigen Input.

0.4 Ergebnisse Schritt 2: Gap-Analyse EasyGov

In einer folgenden zweiten Version dieser Studie wird beurteilt, welche Anpassungen an EasyGov notwendig sind, um der Integrations-Sollarchitektur gerecht zu werden (Gap-Analyse).

1 Ausgangslage und Ziel der Studie

Bürger, Bürgerinnen und Unternehmen möchten Behördenleistungen zunehmend digital beziehen. Nebst dem Komfortgewinn für die Benutzer durch einen medienbruchfreien Austausch mit Behörden von Bund, Kantonen und Gemeinden, können digital zur Verfügung gestellte Behördenleistungen flexibler, effizienter und in höherer Qualität durch die Behörden angeboten werden.

Die Erstellung der vorliegenden Studie basiert auf den in der Folge beschriebenen Rahmenbedingungen.

1.1 Politische und gesetzliche Ebene

Um Behördenleistungen flexibel und effizient anzubieten, ist die digitale Bereitstellung über Behördenleistungsportale notwendig. Die Rechtsgrundlagen bilden dabei insbesondere:

- Art. 3 Abs. 3 RVOG, wonach die Verwaltung nach den Grundsätzen der Zweckmässigkeit und der Wirtschaftlichkeit handeln soll
- Das Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (seit 11.12.2020 in Vernehmlassung)
- Das Unternehmensentlastungsgesetz (seit 28.4.2021 in Vernehmlassung)
- Ergänzend die EFK-Empfehlungen aus der Prüfung «Synergiepotenziale bei IT-Portalen des Bundes - Bundeskanzlei – DTI». Aktuelle Motionen dazu sind z.B. Mo. 20.4726 Glättli, die einen Übersicht über die laufenden politischen Vorstösse gibt.

1.2 Zielsetzung «Digitale Verwaltung Schweiz»

Die Zielsetzung der neu geschaffenen Organisation «Digitale Verwaltung Schweiz» (DVS) lautet gemäss der Grundlagenbericht [37] wie folgt (Auszug): «Die vertikale und die horizontale Zusammenarbeit sollen über alle drei Staatsebenen hinweg nachhaltig gestärkt werden». Im Bericht zur Agenda DVS werden unter anderem die folgenden Ambitionen beschrieben:

- Digitaler Kanal zwischen Bevölkerung und Verwaltung ist etabliert
- Potenzial zur Automatisierung und Vereinfachung für die Wirtschaft ist ausgeschöpft
- Behördenübergreifende digitale Identifikation ist etabliert

Im Kontext der «Digitalen Verwaltung Schweiz» werden Aspekte der Stärkung in der Zusammenarbeit unter den Staatsebenen bei der digitalen Transformation behandelt.

Auf Bundesebene leistet zudem die IKT-Strategie des Bundes² Beiträge zur Umsetzung der Strategien des Bundesrats, insbesondere der Strategie Digitale Schweiz und der E-Government-Strategie.

Dazu wurden Strategische Stossrichtungen und Massnahmenbereiche definiert. Die Stossrichtungen sind mit der Strategie Digitale Schweiz, der Nationalen Strategie zum Schutz vor Cyber-

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

Risiken und der E-Government-Strategie Schweiz sowie dem Schlussbericht EFD/KdK zum Projekt Digitale Verwaltung abgestimmt.

Innerhalb der Stossrichtung C sind die Massnahmenbereichen C1 (Kundenorientierung leben und vorleben) und C2 (Portale und Schnittstellen bereitstellen)³ im Kontext dieser Studie von Belang: Behördenleistungen werden den Nutzenden über Portale (Mensch zu Maschine) und/oder elektronische Schnittstellen (Maschine zu Maschine) zur Verfügung gestellt. Es bestehen gemeinsam genutzte Portale und Schnittstellen, um Leistungen schneller, kostengünstiger und mit geringeren Risiken erbringen zu können.

Grundsätzlich sollen digitale Behördenleistung «Integral» angeboten werden: standardisiert, wiederverwendet, übergreifend gestaltet, interoperabel.

1.3 Umsetzungsziel UZ1 von E-Government Schweiz

Der Aufbau des One-Stop-Shops unter dem Namen EasyGov.swiss ist ein strategisches Projekt von E-Government Schweiz und war Bestandteil des Schwerpunktplans 2016 – 2019, wo das Projekt unter dem Titel "Transaktionsportal für die Wirtschaft" geführt wurde. Die Zielsetzung ist abgestimmt mit der bisherigen und der geplanten Strategie "Digitale Schweiz" (siehe [41], Kapitel 4.6: "administrative Hürden sind weiter abzubauen und der Austausch zwischen den Unternehmen und Behörden ist zentral abzuwickeln").

Auch für die Legislaturperiode 2020-2023 bildet EasyGov Teil des Umsetzungsplans von E-Government Schweiz. So ist unter dem strategischen Ziel «Digitale Interaktions- und Partizipationsangebote national ausbauen» das Umsetzungsziel «EasyGov.swiss ausbauen» festgelegt, siehe [19]⁴.

Weiter sind zur Erreichung des Umsetzungsziels «EasyGov.swiss ausbauen» (UZ1) zwei Massnahmen definiert:

- M1: Architekturreview betreffend Machbarkeit der Integration von Bundes-, kantonalen und kommunalen Leistungen unter Einbezug der relevanten Akteure in einer Studie erstellen.
- M2: Integration von kantonalen Behördenleistungen für Unternehmen, die von mehreren Kantonen gewünscht werden, auf EasyGov sicherstellen.

Die vorliegende Studie behandelt Massnahme M1 «Architekturreview». Insbesondere die E-Government-Verantwortlichen der Kantone wünschen - namentlich im Hinblick auf Planungssicherheit, Investitionsschutz und Förderung der E-Government-Angebote aller föderalen Stufen - einen Architekturreview, um u.a. die Machbarkeit der Integration von kantonalen und kommunalen Leistungen auf EasyGov sowie auch umgekehrt, d.h. die Integration von Leistungen aus EasyGov auf kantonalen Portalen, in einer Studie eingehend zu prüfen.

³ Im Rahmen des Massnahmenbereichs «C2 Portale und Schnittstellen bereitstellen» wird u.a. die API-Architektur Bund [34] erarbeitet.

⁴ Gilt generell für die vorliegende Studie: Ziffer in eckiger Klammer bezieht sich auf den Abschnitt "Referenzierte Dokumente" am Anfang

Dazu soll in einem ersten Schritt eine **generelle** übergreifende Sollarchitektur für die Domäne Behördenleistungsportale⁵ erarbeitet werden. Anschliessend soll in einem zweiten Schritt beurteilt werden, welche Anpassungen an EasyGov notwendig sind, um der übergreifenden Sollarchitektur gerecht zu werden (Gap-Analyse).

Daraus leiten sich die folgenden Ziele ab:

- Formulierung einer groben Integrations-Sollarchitektur für Behördenleistungsportale auf der Grundlage einer Bedürfnisabklärung.
 - Systematische Erarbeitung gemäss TOGAF⁶:
 - Geschäftsarchitektur (Geschäftsobjekte, Prozesse, Erbringung der Behördenleistungen)
 - Technische Informationssystemarchitektur (Datenobjekte, Applikationen/Services, Schnittstellen, Übertragungskanäle, Zuständigkeiten)
 - Betrachtung der Interoperabilität⁷ von Identitäten (natürliche, juristische Personen) und deren Berechtigungen
 - Vorschlag der Sollarchitektur als Entwurf eines eCH-Standards
 - Bildet eine Teilarchitektur von UZ14 / M2 "Gesamtarchitektur zur Umsetzung der E-Government-Strategie Schweiz 2020–2023 definieren."⁸
 - Kann als Vorgabe für UZ14 / M4 "Pilotprojekt zur Integration von E-Services in verschiedenen Portalen umsetzen"⁸ verwendet werden.
- Gapanalyse bezüglich Ist-/Sollzustand der Architektur von EasyGov im Vergleich zur portalübergreifenden Sollarchitektur
- Grobplanung zur Beseitigung der Gaps in EasyGov

Wichtig: Die angestrebte grobe Integrations-Sollarchitektur für Behördenleistungsportale fokussiert wohlgermerkt nicht auf die Systemarchitekturen einzelner Portale, sondern vielmehr auf ein portalübergreifendes "Ökosystem", welches das Zusammenspiel regelt und die Interoperabilität⁷ verbessert, siehe Abbildung 1.

⁵ Unter Behördenleistungsportale werden öffentlich zugängliche Applikationen (z.B. Single Page Application, mobile App, etc.) verstanden, mit welchen ein Portalbetreiber im Rahmen des E-Governments dem Kunden einen digitalen Zugangskanal für eine oder mehrere Behördenleistungen bietet. Es stellt das Kunden-Front-End einer Behördenleistung dar. Siehe dazu auch Begriffserläuterungen in Kapitel 2.1.5, Tabelle 1.

⁶ Siehe Anhang G.C für eine Verankerung von TOGAF

⁷ Das EIF [17] definiert Interoperabilität wie folgt: *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 Bezieht sich auf Umsetzungsziel 14 "E-Government-Architektur für den strategischen Umsetzungsplan erarbeiten und führen", siehe [19]

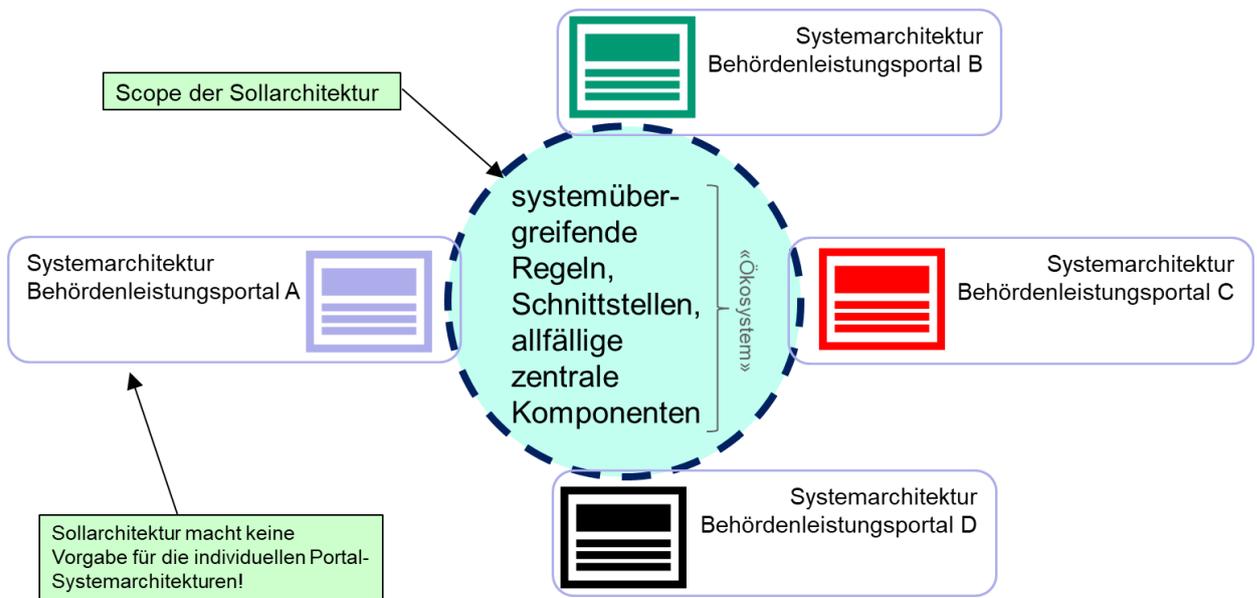


Abbildung 1: Scope der angestrebten Integrations-Sollarchitektur (schematische Darstellung)

2 Integrations-Sollarchitektur für Behördenleistungsportale

2.1 Situationsanalyse von Behördenleistungsportalen aus logischer Sicht

Im ersten Schritt geht es darum, die wesentlichen Bestandteile von Behördenleistungsportalen zu identifizieren, um ein begriffliches Fundament für die späteren Kapitel zu bekommen.

2.1.1 Prozesssicht einer Behördenleistung

Trotz der Fülle von Bundes-, kantonalen oder kommunalen Behördenleistungen (siehe [27]) lassen sich im Einklang mit dem in eCH-0126 [14] aufgezeigten Phasenmodell des Verwaltungsverfahrens und den in eCH-0138 [15] genannten Leistungstypen folgende typische Muster erkennen:

- Bewilligungsverfahren (z.B. Baubewilligung)
- Meldeverfahren (z.B. Meldeverfahren für kurzfristige Erwerbstätigkeit von Staatsangehörigen EU/EFTA)
- Antragsverfahren (z.B. Antrag auf eine Wohnsitzbestätigung oder zur Einbürgerung)
- Anmeldeverfahren (z.B. Anmeldung zur Mehrwertsteuer)
- Deklarationsverfahren (z.B. Mehrwertsteuerabrechnung)
- Informationsleistung (z.B. Betriebsauskunft)

Das Bewilligungsverfahren sticht als das komplexeste hervor. Es läuft nach dem folgenden Muster ab: Ein Kunde⁹ (juristische oder natürliche Person) stellt ein Gesuch zu einer bestimmten Behördenleistung und löst damit einen Geschäftsfall in der betreffenden Behörde aus. Die Behörde bearbeitet das Gesuch und kommuniziert Rückmeldungen zum Bearbeitungsstand oder allfällige Rückfragen an den Kunden zurück. Bei der Bearbeitung können allfällige Abklärungen/Zustimmungen von anderen Amtsstellen nötig sein. Nach eingehender Prüfung der Gesuchsunterlagen übermittelt die Behörde am Ende des Verfahrens¹⁰ dem Kunden das Ergebnis (positiv oder negativ), z.B. in Form einer Bewilligung oder eines Bescheids.

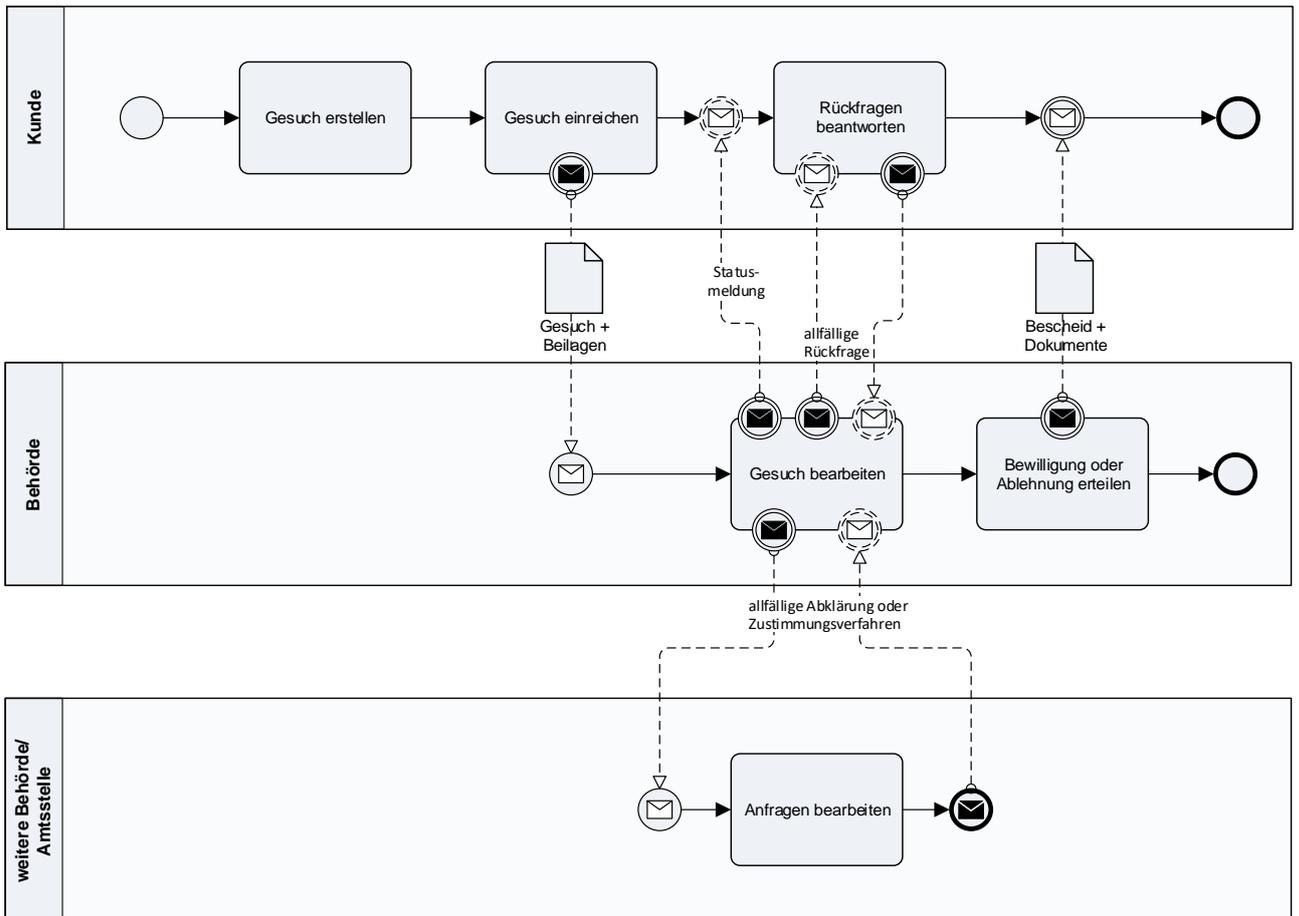


Abbildung 2: Allgemeiner Ablauf eines Bewilligungsverfahrens (BPMN-Diagramm)

Das Meldeverfahren weist vergleichsweise die geringste Komplexität auf. Hierbei handelt es sich um ein One Way-Verfahren. Statt einer Bewilligung ist eine obligatorische Meldung (z.B.

⁹ Der Begriff Kunde wird im Informationsmodell, Kapitel 2.1.5 näher beschrieben.

¹⁰ In manchen Fällen findet während des Verfahrens eine Übergabe an eine andere Amtsstelle statt, infolgedessen der Kunde das Verfahrensergebnis von dieser erhält. Dies ist zum Beispiel bei Bewilligungsverfahren zur Erwerbstätigkeit Drittstaatsangehörige in der Stadt Bern, Thun oder Biel der Fall. Das Gesuch ist zunächst beim Amt für Wirtschaft des Kantons Bern einzureichen, welches für den arbeitsmarktlichen Vorentscheid zuständig ist. Anschliessend übergibt das Amt das Verfahren an die zuständige Migrationsbehörde. Üblicherweise verbleibt dabei die Zuständigkeit im Kanton, im Falle des Arbeitsorts Bern, Thun oder Biel ist jedoch die Kommune zuständig. Der Kunde erhält das Verfahrensergebnis von dieser Behörde und nicht von jener, wo er das Gesuch ursprünglich eingereicht hat.

Arbeitsaufnahme) abzugeben. Der Kunde übermittelt der zuständigen Behörde die geforderten Informationen, womit für ihn der Vorgang erledigt ist. Für die betreffende Behörde löst die Meldung einen weiteren Geschäftsfall aus, der weitere Massnahmen nach sich ziehen kann (z.B. gesonderte Kontrollen).

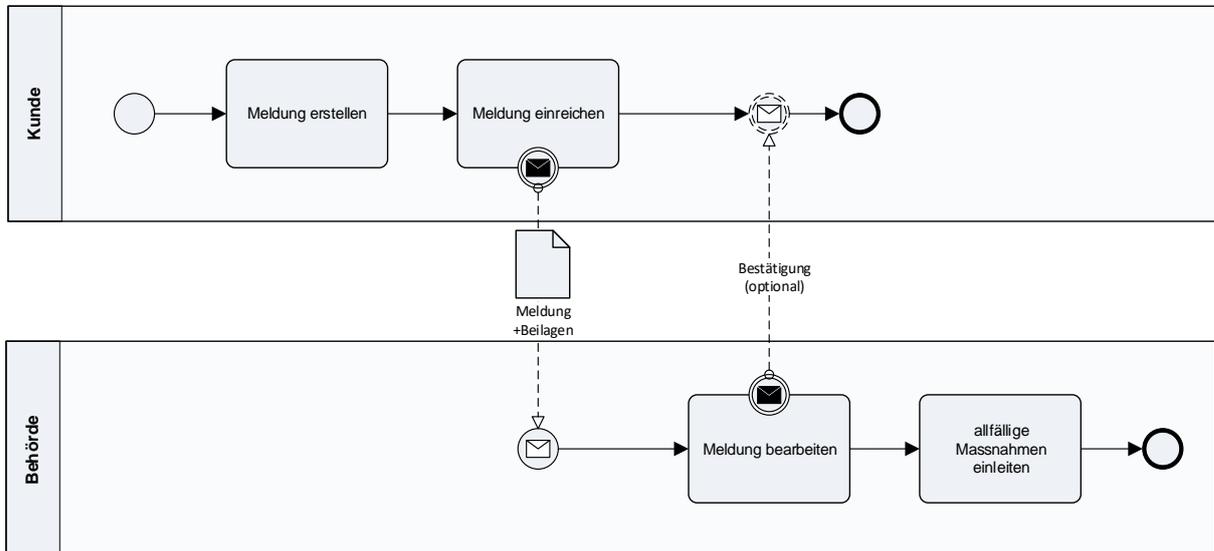


Abbildung 3: Allgemeiner Ablauf eines Meldeverfahrens (BPMN-Diagramm)

Die anderen genannten Verfahren liegen zwischen diesen beiden Extrempunkten. Somit stellen Melde-, Antrags-, Anmeldungs- und Deklarationsverfahren jeweils ein Subset des Bewilligungsverfahrens dar.

Abstrahierend lässt sich die Abwicklung einer Behördenleistung auf einen kunden- und einen behördenseitigen Prozess zusammenfassen. In Anlehnung an die von den eCH-Standards 0088, 0126 [14] und 0138 [15] propagierte Begrifflichkeit wird dabei der kundenseitige Prozess als **Behördengang** und der behördenseitige Prozess als **Geschäftsfall** bezeichnet.

Hinweis: Für die Bearbeitung von Geschäftsfällen durch die zuständigen Behörden sind zeitliche Vorgaben gemäss gesetzlich vorgegebenen Fristen einzuhalten. Dies ist in den BPMN-Diagrammen

Abbildung 2 und Abbildung 3 im Interesse der Übersichtlichkeit nicht dargestellt, da es für die weiteren Betrachtungen nicht von Belang ist.

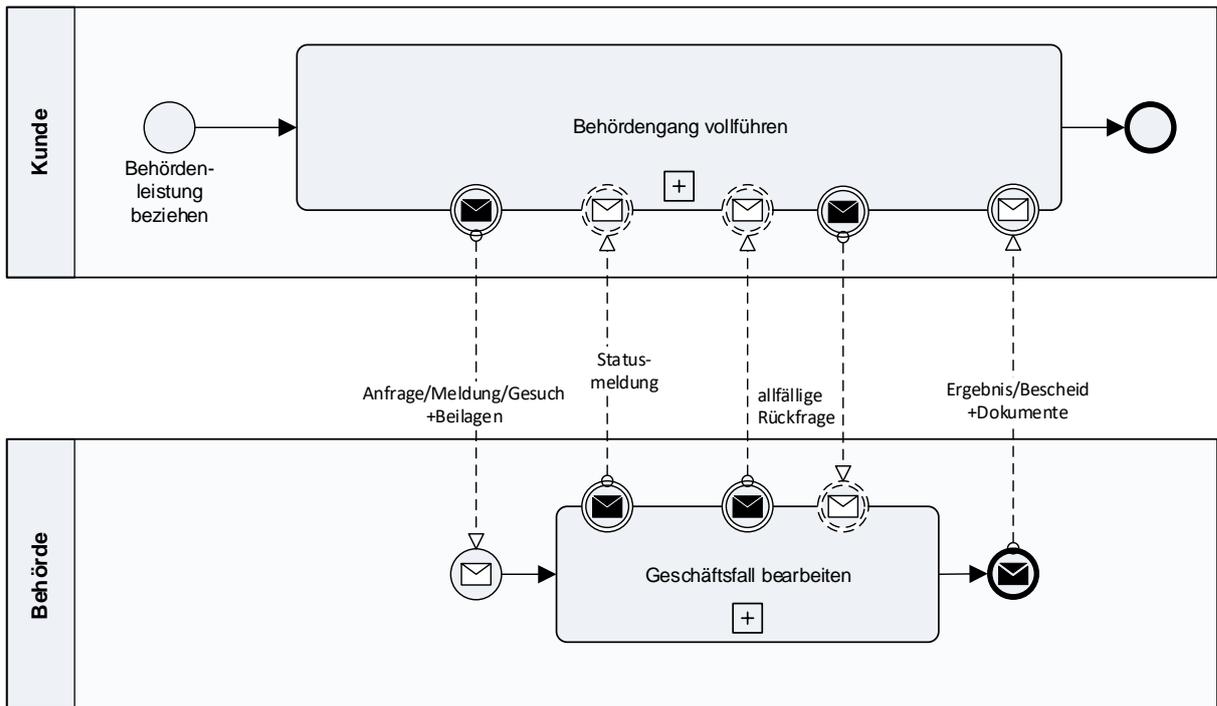


Abbildung 4: Abstraktion der Abwicklung einer Behördenleistung als parallel auf Kunden- bzw. Behördenseite laufende Prozesse

In speziellen Fällen können - wie bereits auf der vorangegangenen

Abbildung 2 angedeutet - auf Behördenseite weitere Amtsstellen der gleichen oder einer anderen Behörde in die Bearbeitung des Geschäftsfalls involviert sein. Dafür gibt es zwei Muster:

- Subprozess (siehe Abbildung 5)
- Verfahrensübergabe (siehe Abbildung 6)

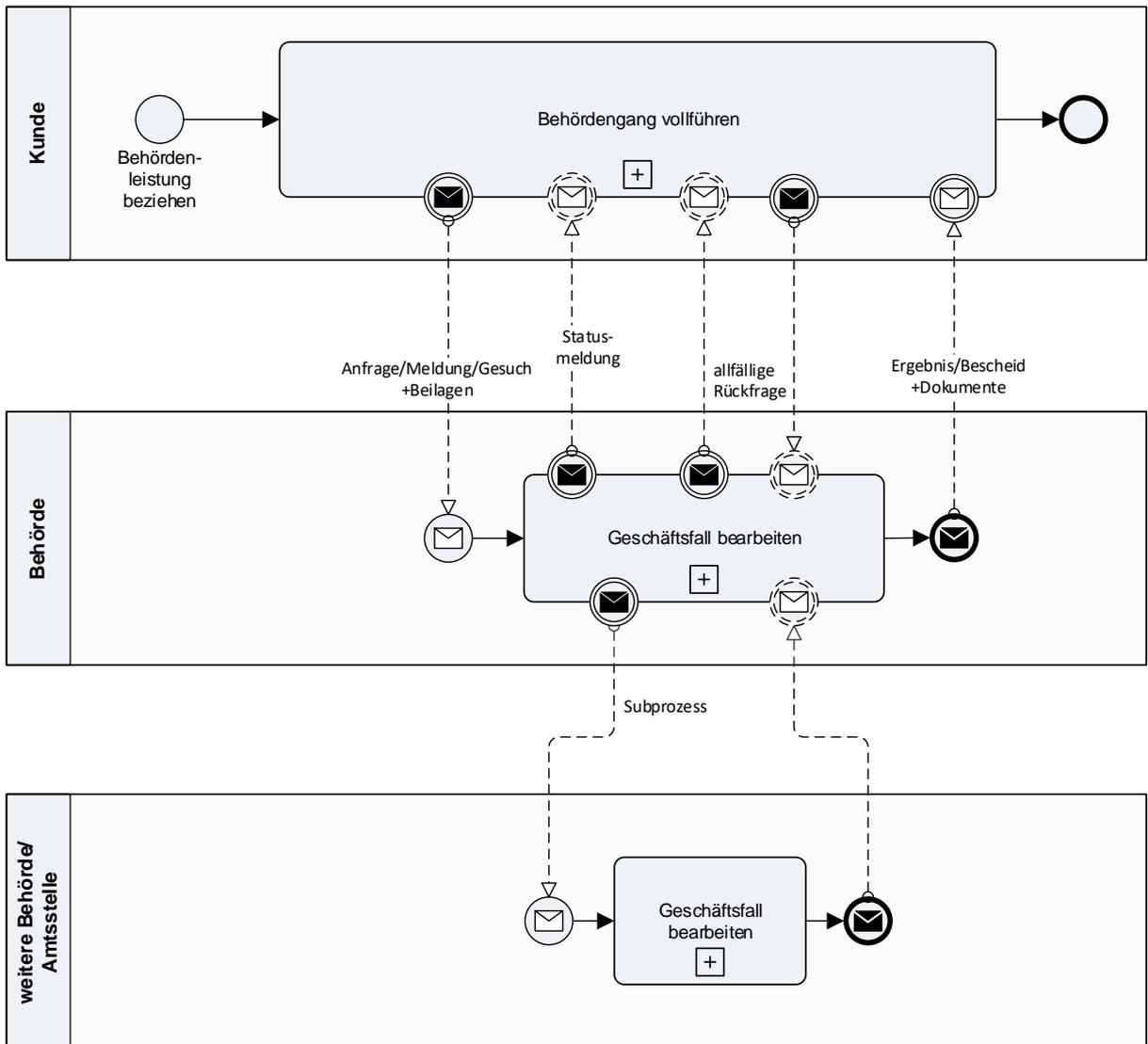


Abbildung 5: Involvierung einer weiteren Behörde/Amtsstelle in die Geschäftsbearbeitung nach dem Muster Subprozess

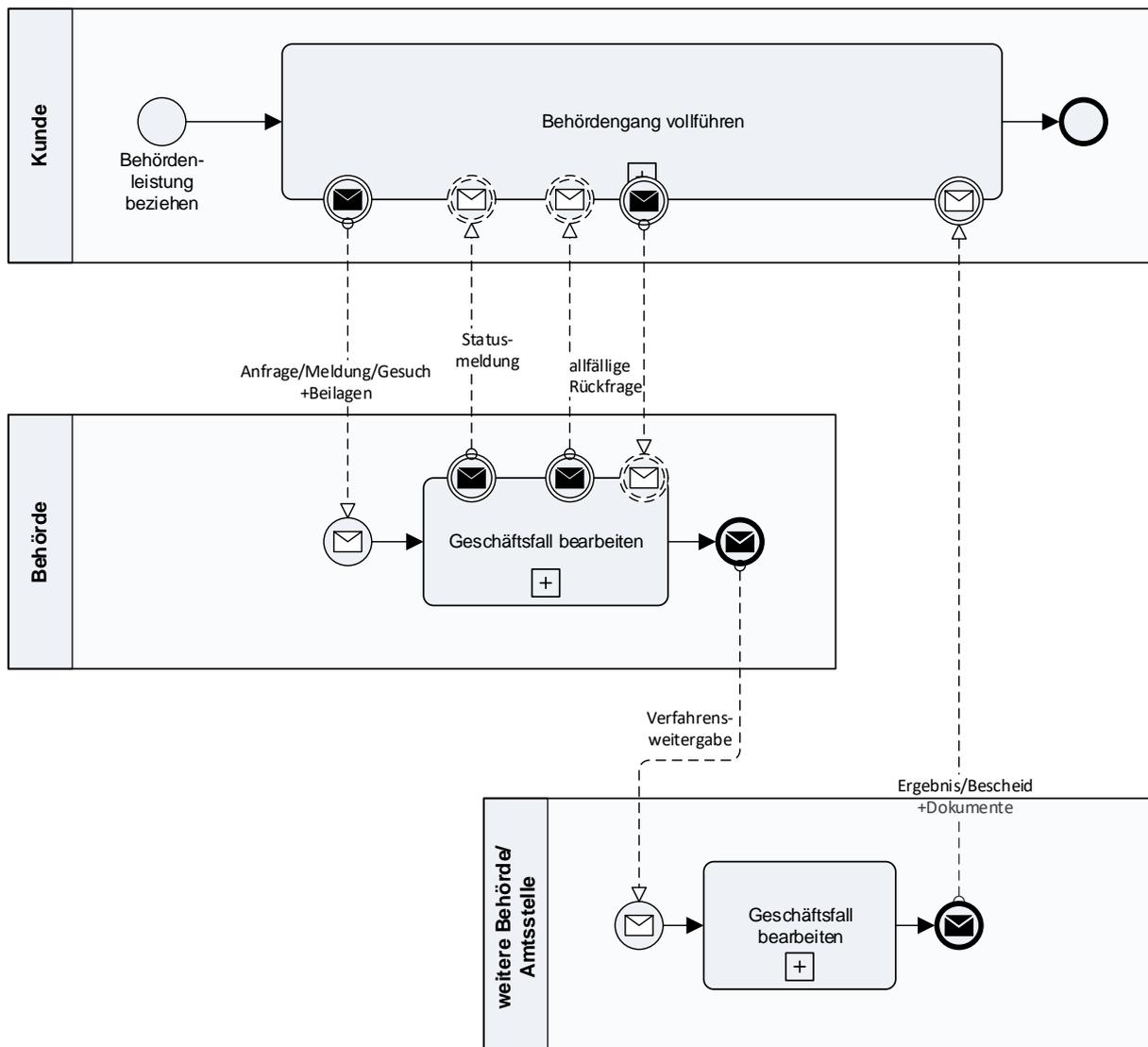


Abbildung 6: Involvierbarkeit einer weiteren Behörde/Amtsstelle in die Geschäftsfallbearbeitung nach dem Muster **Verfahrensweitergabe**

Während beim ersten Muster Subprozess weitere involvierte Amtsstellen auf der Kundenseite nicht direkt in Erscheinung treten, ist der Kunde beim zweiten Muster Verfahrensweitergabe mit wechselnden Zuständigkeiten konfrontiert.

Hinweis: Im Rahmen dieser Studie stehen Behördenleistungen im Fokus, die nicht anonym beziehbar und mit einem Geschäftsfall verbunden sind. So fallen Informationsleistungen, die anonym in Selbstbedienung nutzbar sind (wie z.B. ein Steuerrechner) nicht darunter, ebenso wie Self Services, die keinen Geschäftsfall in der Behörde auslösen (wie z.B. das Verwaltungstool von Kontingentanteilen bezüglich einer erteilten Generaleinfuhrbewilligung des BLW¹¹). Der erste Fall ist dem in Kapitel 2.1.3 eingeführten Informationslayer zuzuordnen, der zweite kann trotz des oben genannten Ausschlusses durch das in Kapitel 2.1.6 eingeführte Integrationsmuster 2 (Einbindung) unterstützt werden.

¹¹ siehe <https://www.ekontingente.admin.ch/>

2.1.2 Behördenleistungsportal als digitaler Zugangskanal

Mit Hilfe eines Behördenleistungsportals¹² bietet ein Portalbetreiber Behördenleistungen dem Kunden auf digitaler Ebene an (siehe Abbildung 7¹³). Es stellt einen Zugangskanal für den Kunden auf ein oder mehrere Behördengänge dar. Die Behörde kann dabei auch selbst als Portalbetreiber fungieren (siehe Abbildung 8). Ebenso gut kann ein Portalbetreiber oder die Behörde selbst Kunde einer anderen Behördenleistung auf einem weiteren Portal sein.

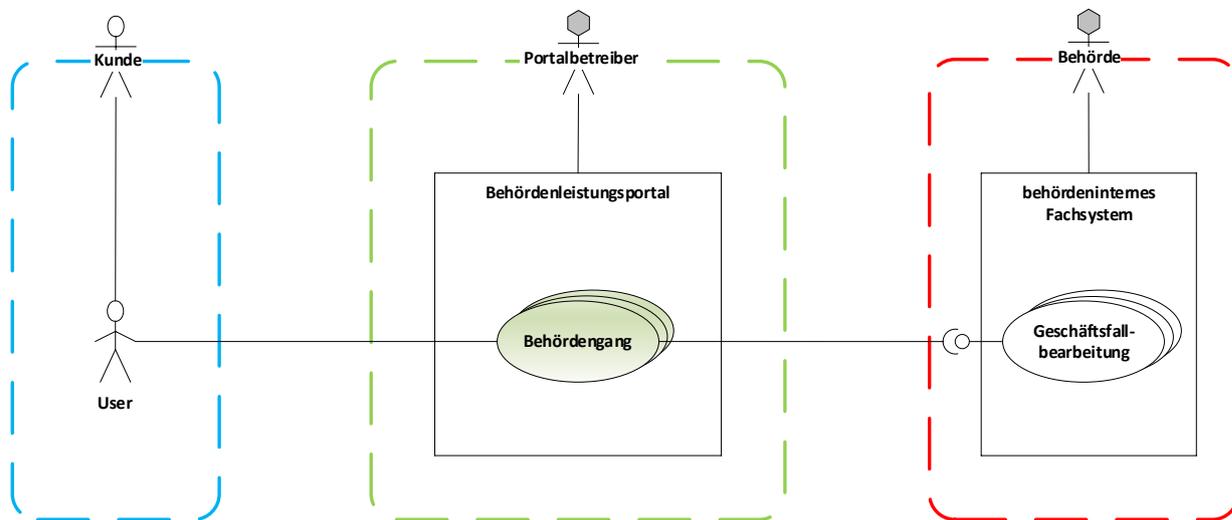


Abbildung 7: Behördenleistungsportal als digitaler Zugangskanal für ein oder mehrere Behördenleistungen für den Kunden (UML-Use Case Diagramm)

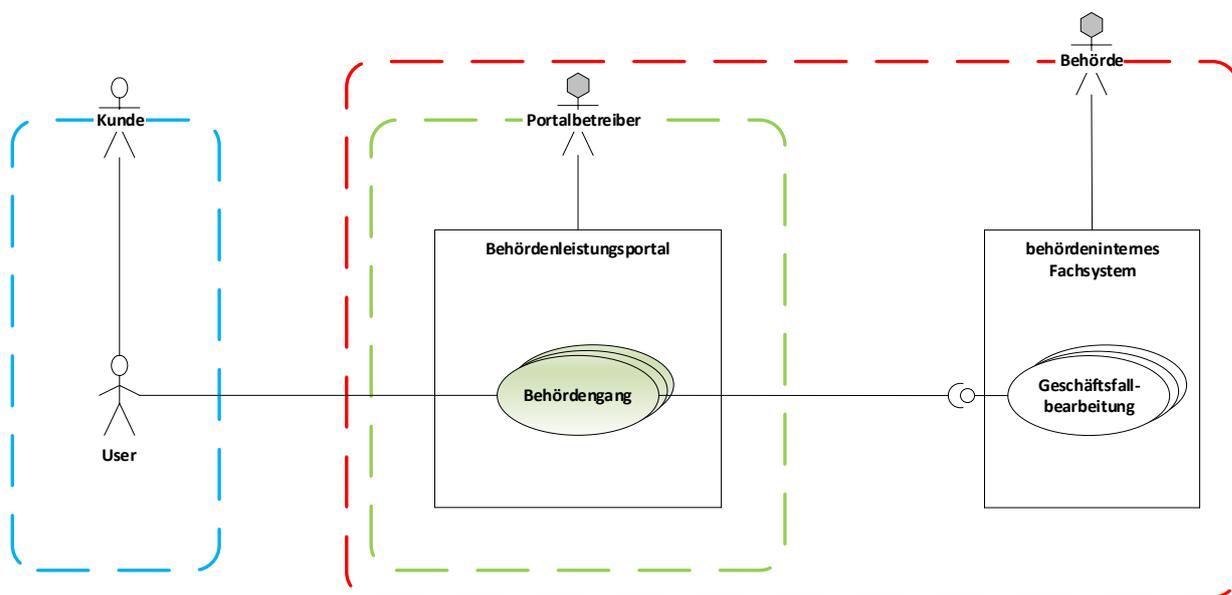


Abbildung 8: Portalbetreiber kann auch die Behörde selbst sein

¹² Mitunter auch als Plattform bezeichnet. Siehe Begriffserläuterung in Tabelle 1, Kapitel 2.1.5

¹³ In diesen und allen in dieser Studie nachfolgenden Abbildungen der Beziehungen zwischen Kunde, Portalbetreiber und Behörde gelten folgende Farbkodierungen für die Akteure: Kunde = Blau, Portalbetreiber = Grün, Behörde = Rot. Alle Elemente innerhalb einer Farbbox sind im Verantwortungsbereich des entsprechenden Akteurs.

Aus User-Sicht bildet ein Behördenleistungsportal per se nur die Belange des Kunden nebst allfälliger Kommunikation zwischen ihm und der jeweiligen Behörde ab und greift nicht in die behördeninternen Prozesse ein. Das entspricht gemäss Abbildung 4 dem kundenseitigen Behördengang. In diesem Rahmen kommuniziert das Behördenleistungsportal mit dem internen Fachsystem der zuständigen Behörde, welches deren Geschäftsfallbearbeitung unterstützt. Die folgende Abbildung 9 verdeutlicht diese Abgrenzung:

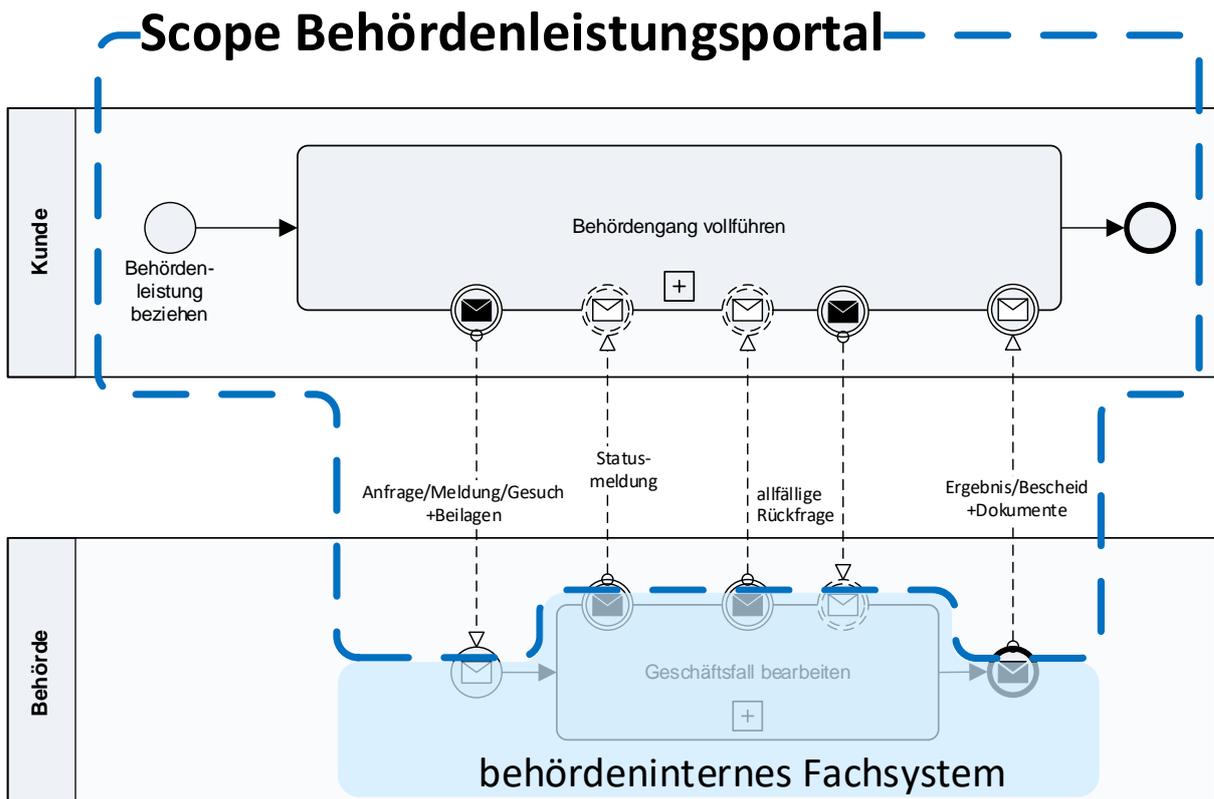


Abbildung 9: Abgrenzung des Scopes eines Behördenleistungsportals auf den kundenseitigen Prozess. Behördeninterne Prozesse werden dagegen vom behördeninternen Fachsystem unterstützt.

Ein Behördenleistungsportal kann als Kunden-Front-End¹⁴ verstanden werden, welches - im Sinne von Abbildung 9 – die Schnittstelle zwischen Kunde und Behörde unterstützt. "Kunde" ist dabei als abstrakter Begriff im Sinne eines Rechtssubjekts zu sehen, was für eine juristische oder natürliche Person stehen kann. In jedem Fall gilt: Der digitale Behördengang wird durch einen User des Behördenleistungsportals vorgenommen, der in Vollmacht des Kunden handelt. Im Falle "Kunde = natürliche Person" werden die Rollen Kunde und User meist von derselben physischen Person wahrgenommen (mitunter aber auch nicht, z.B. wenn der Steuerberater die Steuerdeklaration für seinen Kunden vornimmt).

¹⁴ Siehe auch Begriffsbestimmung Front-End/Back-End im Glossar im Anhang A. Aus Kundensicht ist das Behördenleistungsportal das Front-End und das behördeninterne IT-System das Back-End.

2.1.3 Funktionelle Struktur eines Behördenleistungsportals

Neben der reinen Abbildung des Behördengangs kann ein Behördenleistungsportal dem Kunden darüber hinaus Hilfestellungen geben, insbesondere bei der Frage: "Ich habe XX vor, welche Behördenleistungen sind dafür relevant? Welche Behörde ist dafür zuständig?". Zur Differenzierung dieser Ebene von der eigentlichen Behördenleistung sei die in [18] verwendete Begrifflichkeit übernommen, welche zwischen Informations- und Transaktionslayer unterscheidet. Im Informationslayer wird das Angebot der Behördenleistungen – in welcher Form auch immer – präsentiert, wogegen im Transaktionslayer die Abwicklung einer Behördenleistung, d.h. des diesbezüglichen Behördengangs abgebildet wird. In Anlehnung an die vorausgegangene Abbildung 9 verortet die folgende Abbildung 10 die beiden Ebenen aus Prozesssicht:

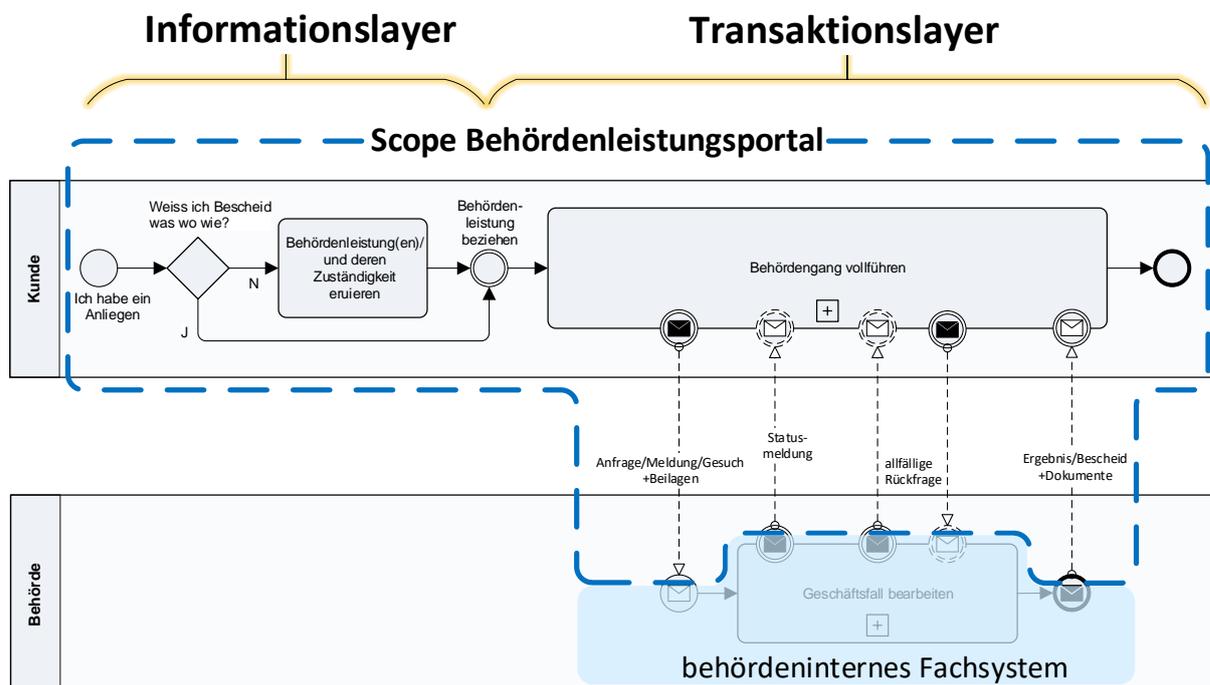


Abbildung 10: Verortung von Informations- und Transaktionslayer in der Prozesssicht

Letztlich dient der Informationslayer dazu, den User zu einer bestimmten Behördenleistung zu führen, zu der er schliesslich im Transaktionslayer einen Behördengang anstossen kann. Verwaltungskunden beanspruchen und beziehen öffentliche Leistungen aufgrund von Anliegen, die bestimmte Lebenslagen (z.B. Heirat, Umzug) oder Geschäftssituationen (z.B. Unternehmensgründung) widerspiegeln¹⁵. Wie Abbildung 11 illustriert, kann für diesen Zweck eine Orchestrierung von Leistungen angeboten werden, welche den User für ein solches Kundenanliegen mittels eines Wizards über alle dafür relevanten Muss- und Kann-Behördenleistungen - quasi an einem "Faden" - führt. Ein Beispiel dafür ist die Abbildung der Unternehmensgründung in EasyGov, welche schrittweise über die nötigen Formalitäten und Anmeldungen (Handelsregister, AHV, Mehrwertsteuer etc.) lotst.

¹⁵ Eine Übersicht typischer Lebenslagen oder Geschäftssituation gibt [38] bzw. [39].

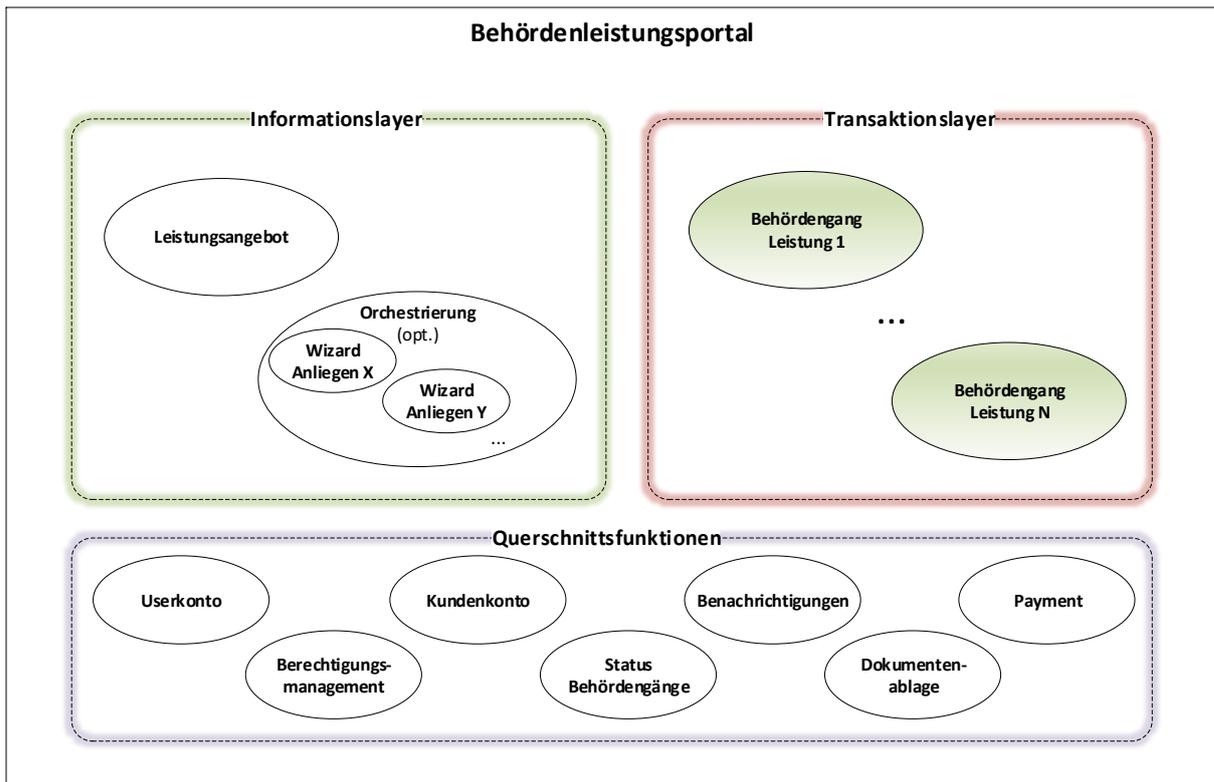


Abbildung 11: Prinzipielle funktionelle Struktur eines Behördenleistungsportals

Weiterhin zeigt Abbildung 11 die Tatsache auf, dass ein Behördenleistungsportal eine Reihe von Querschnittsfunktionen enthalten kann, die in beiden Layern zur Anwendung kommen. Typische Querschnittsfunktionen sind zum Beispiel:

- Userkonto
- Berechtigungsmanagement
- Kundenkonto¹⁶
- Status der Behördengänge
- Benachrichtigungen von Behörden
- Dokumentenablage

Der Umfang der Querschnittsfunktionen variiert im Spektrum der existierenden Behördenleistungsportale. So finden sich Portale, bei denen der Informationslayer zum grossen Teil nicht im Portal selbst, sondern im Webauftritt der jeweiligen Behörde realisiert ist. In diesem Fall weist der Informationslayer keine Querschnittsfunktionen im obigen Sinne auf. Ähnlich sind als

¹⁶ mitunter auch als (Kunden-)Stammdatenverwaltung oder Geschäftspartnerverwaltung bezeichnet. Zur Klärung der Synonyme siehe Glossar im 4

zustandslose¹⁷ eFormulare realisierte Transaktionslayer zu deuten, welche ebenfalls keine Querschnittsfunktionen aufweisen.

Letztlich ist festzustellen, dass bei existierenden Behördenleistungsportalen die Umfänge der drei logischen Ebenen Informationslayer, Transaktionslayer und Querschnittsfunktionen entsprechend ihrer spezifischen Ausrichtungen unterschiedlich ausgeprägt sind. Die folgende Grafik illustriert anhand von Beispielen diese Vielfalt.

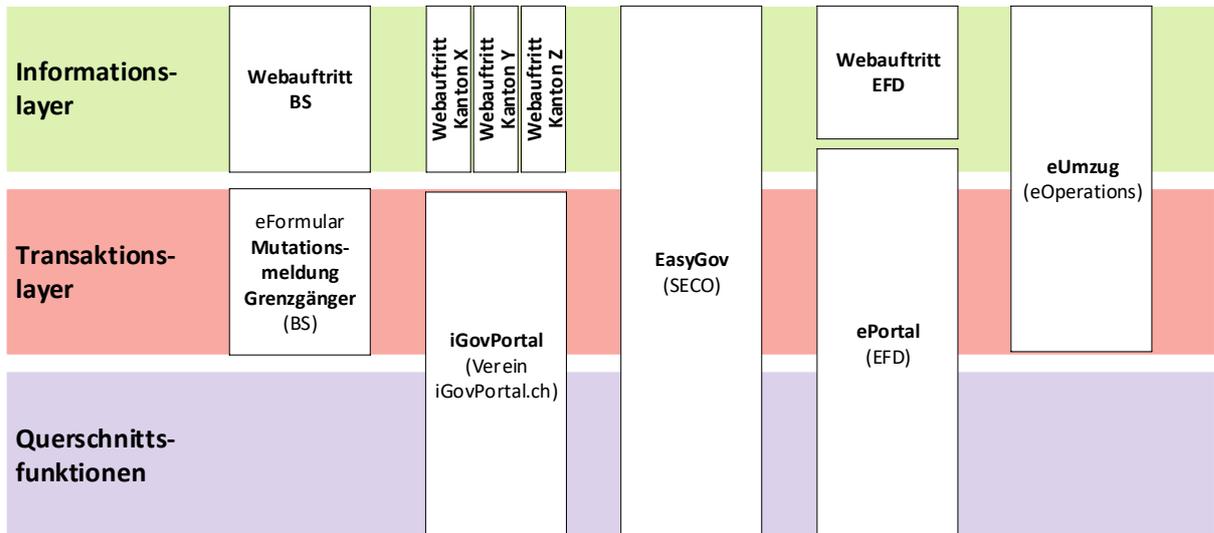


Abbildung 12: Vielfältige Layer-Ausprägungen in existierenden Behördenleistungsportalen

Darüber hinaus zeigt das in Abbildung 12 gezeigte Beispiel des vom BIT betriebenen ePortal Bund¹⁸, dass die einzelnen Layer auch auf mehrere Subsysteme verteilt sein können. Das ermöglicht die Trennung von Verantwortlichkeiten: Während das ePortal vom BIT entwickelt und verantwortet wird, werden die Behördengänge von den jeweils zuständigen Ämtern realisiert, wie beispielsweise die Portal-Fachanwendung "Mehrwertsteuer Abrechnung easy" Sache der ESTV ist. Die beteiligten Institutionen wirken als Portalbetreiber-Gemeinschaft zusammen.

¹⁷ Siehe Glossar im Anhang A

¹⁸ Siehe <https://eportal.admin.ch/>

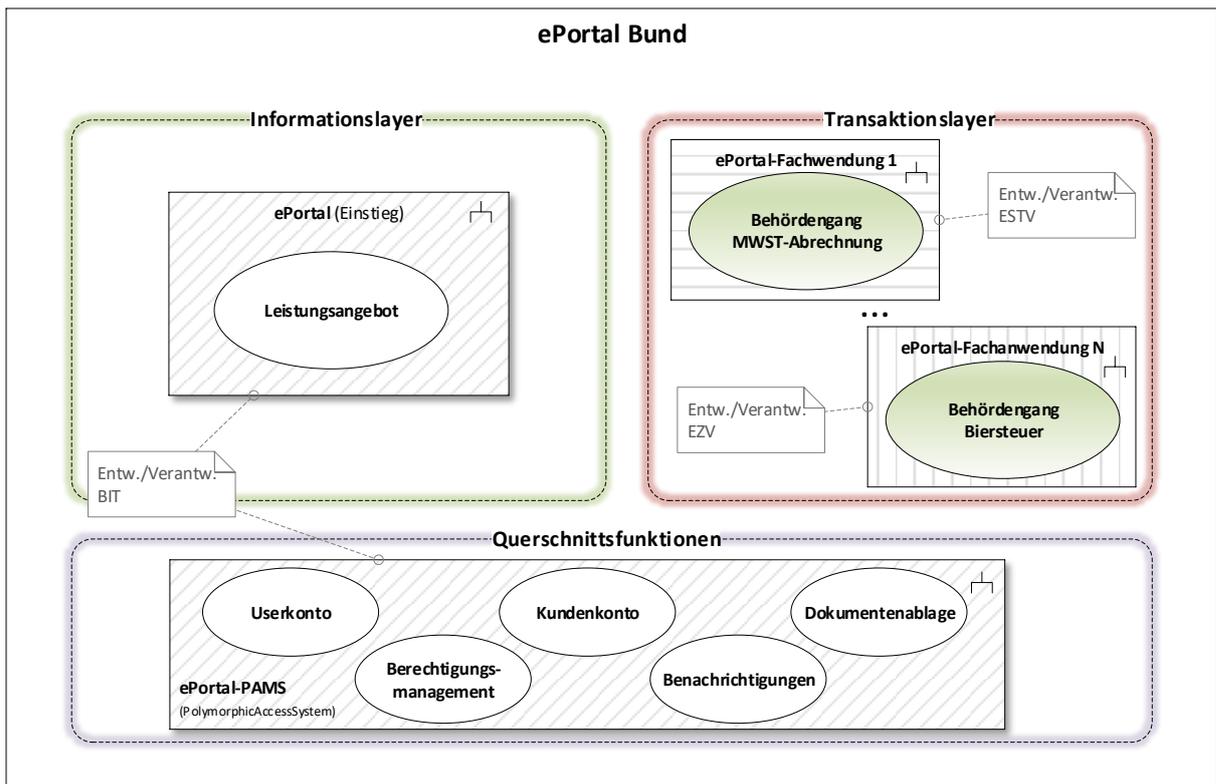


Abbildung 13: ePortal-Aufbau mit verteilten Subsystemen unter verschiedenen Verantwortlichkeiten

2.1.4 Portallandschaft der Behördenleistungsportale

Die in der Schweiz bestehenden oder gerade im Aufbau befindlichen Behördenleistungsportale sind in der Regel unabhängig voneinander entstanden und bilden jeweils ein bestimmtes Set an Behördenleistungen ab. Dieses Set ist durch die inhaltliche Ausrichtung der Portale begründet, diese kann entweder

- (A) auf das Portfolio einer Behörde (siehe Abbildung 14, z.B. Online-Schalter des Kantons SG, Virtueller Schalter des Kantons FR, ePortal Bund)
- oder (B) auf den Bedarf einer bestimmten Kundenzielgruppe (siehe Abbildung 15, z.B. EasyGov für Unternehmen)
- oder (C) auf eine Mischform von beidem fokussieren.

In jedem Fall spiegelt sich die Ausrichtung des jeweiligen Behördenleistungsportals in seinem Informationslayer nieder.

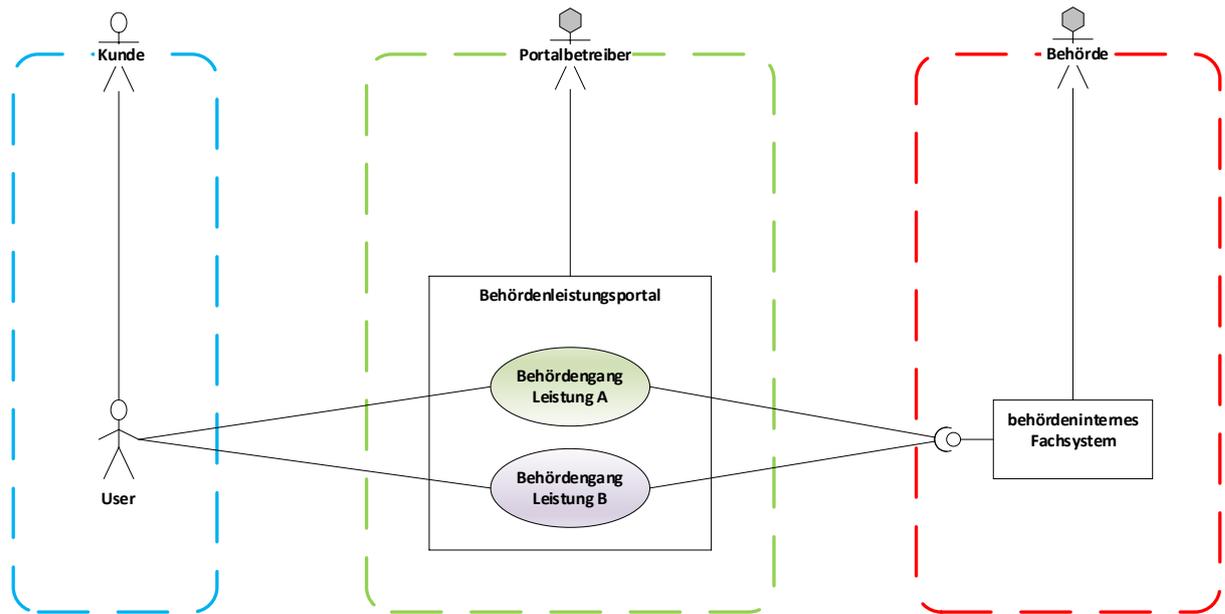


Abbildung 14: Auf das Portfolio einer Behörde ausgerichtetes Behördenleistungsportal (A): Das Portal bildet das Leistungsangebot einer bestimmten Behörde ab

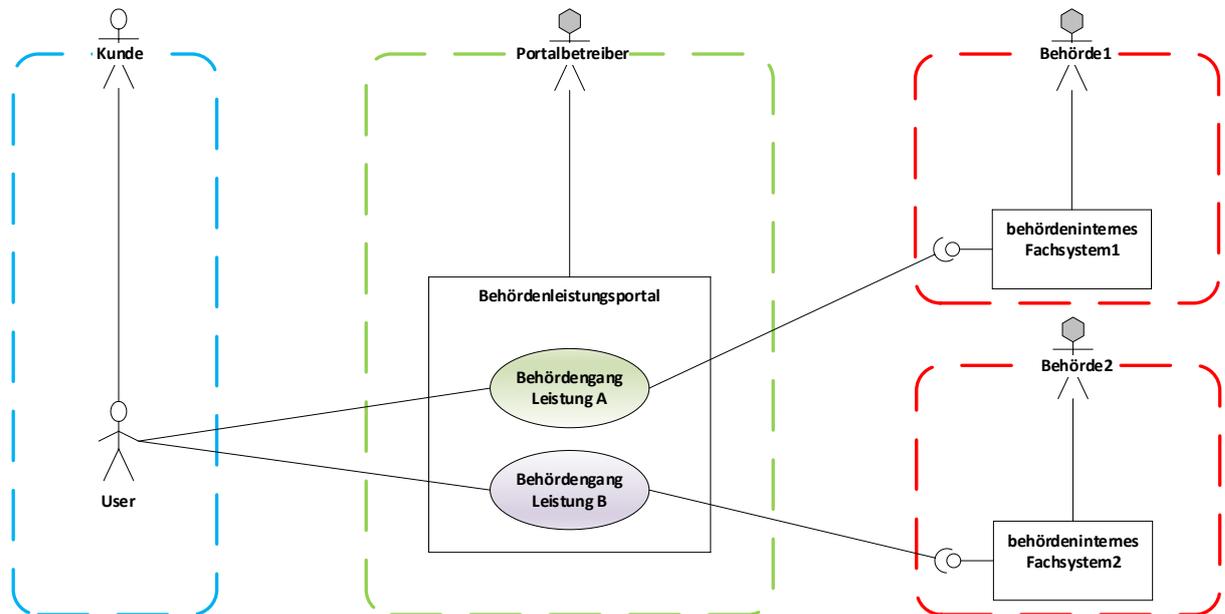


Abbildung 15: Auf den Bedarf einer bestimmten Kundenzielgruppe ausgerichtetes Behördenleistungsportal (B): Das Portal bildet das für die Kundenzielgruppe relevante Set an Behördenleistungsangeboten ab, die von verschiedenen Behörden stammen können

Die nach Kundenbedarf orientierte Ausrichtung (B) kann sich auch darin manifestieren, dass eine kantonale oder kommunale Behördenleistung unabhängig der konkreten Zuständigkeit angeboten wird (z.B. Handelsregistereintragungen für Unternehmen in EasyGov), damit aus Sicht des Users die Behördenleistung ungeachtet der tatsächlichen Zuständigkeit gleich

erscheint (B'). Das Wissen über die jeweilige Zuständigkeit ist in diesem Fall im Portal implementiert, aufgrund dessen es die Kommunikation auf das Fachsystem der tatsächlich zuständigen kantonalen oder kommunalen Behörde richtet.

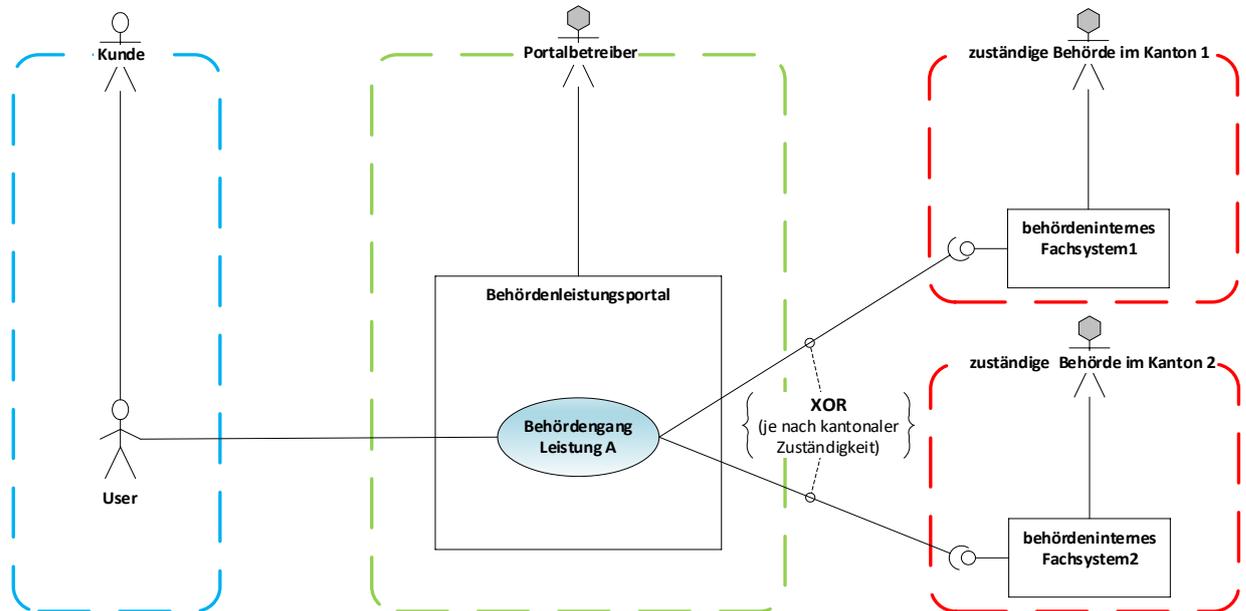


Abbildung 16: Kapselung der konkreten Zuständigkeit einer kantonalen/kommunalen Behördenleistung durch ein übergreifendes Angebot (B')

Eine Umsetzungsvariante der Mischform (C) ist ein Portal, welches mit allen notwendigen Portal-Basisfunktionalitäten (Informationslayer und Querschnittsfunktionen) ausgerüstet ist. Diese Basisfunktionalitäten können durch eine Stelle entwickelt und betrieben werden. Basierend auf den verfügbaren Basisfunktionalitäten können anschliessend interessierte Behörden ihr eigenes Angebot entwickeln und auf dem Portal anbieten, ohne die Basisfunktionalitäten jeweils neu zu entwickeln. Dadurch entsteht ein Portal mit Angeboten mehrerer Behörden.

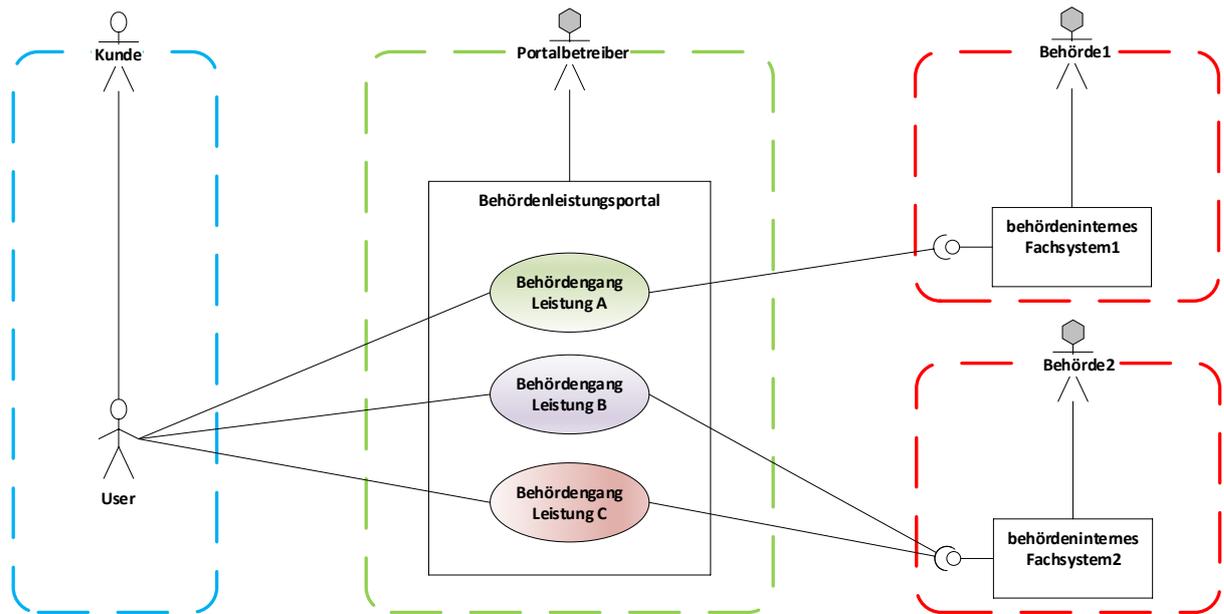


Abbildung 17: Mischform (C) aus (A) und (B)

Aufgrund der vielfältigen Ausrichtungen der Behördenleistungsportale – insbesondere der bedarfsorientierten (B) – sind die jeweiligen Sets zum Teil überlappend, d.h. einige Behördenleistungen sind nicht exklusiv auf einem, sondern auf verschiedenen Portalen individuell abgebildet. Diesen Fall illustriert die folgende Abbildung 18.

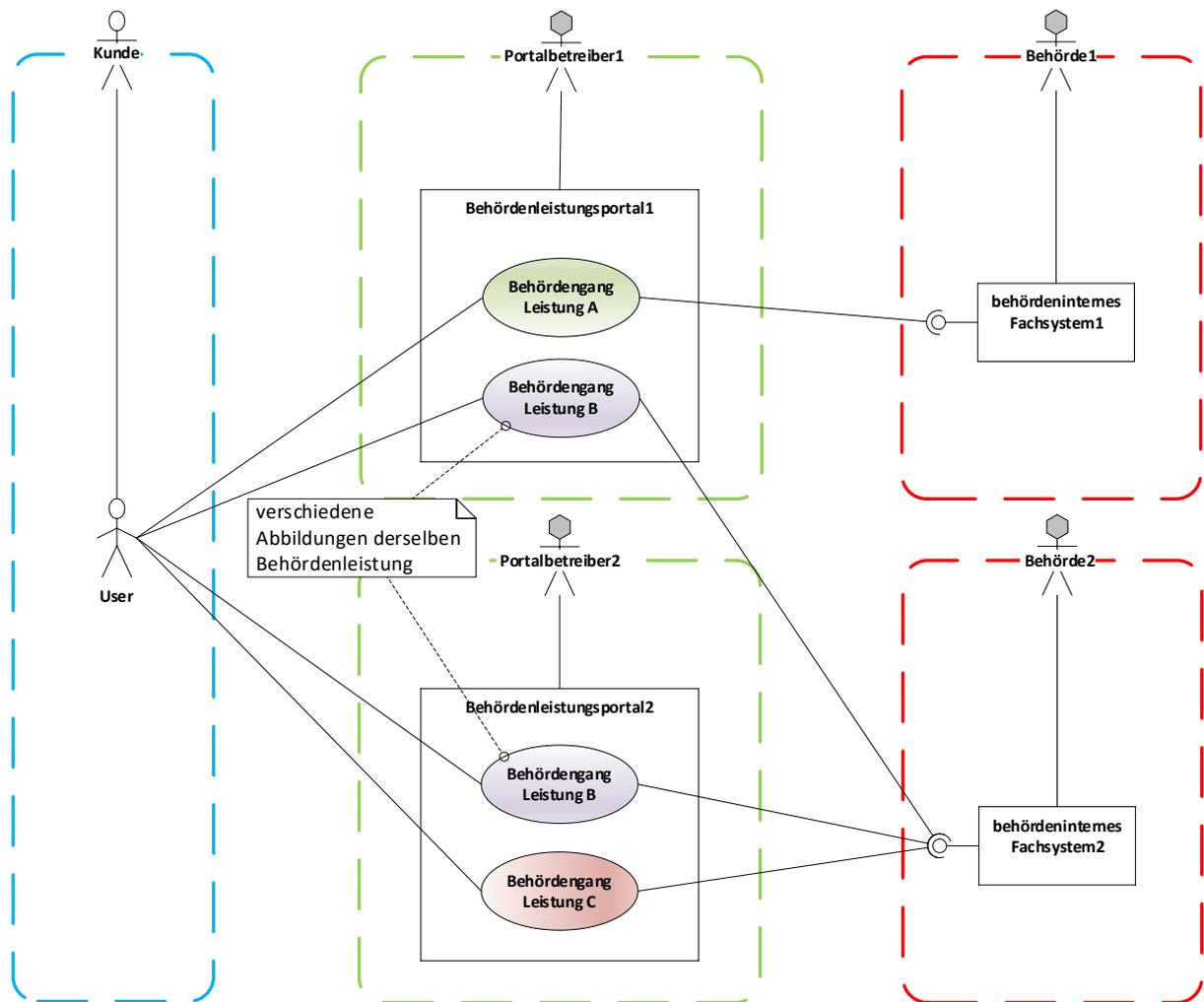


Abbildung 18: Individuelle Abbildung einer Behördenleistung auf verschiedenen Portalen

Das vom Kundenbedürfnis getriebene Muster der individuellen Abbildungen einer Behördenleistung auf verschiedenen Portalen hat sowohl Vor- als auch Nachteile.

Vorteile:

- Ein Portal kann sich exklusiv auf die Bedürfnisse einer Kundenzielgruppe fokussieren – aus Kundensicht ist somit die Ausprägung (B) die bevorzugte Variante
- Indem die Kundengruppe im Fokus des Portals möglichst alle notwendigen Behördenleistungen an einem Ort beziehen kann, eröffnet sich folgender Nutzen:
 - Unterstützung des Once-Only-Prinzips über alle im Portal abgebildeten Behördengänge
 - Registrierung an nur einem Portal
 - Orchestrierung von Leistungen bezüglich einer Lebenslage/Geschäftssituation
 - Die Kundengruppe kennt das Portal und dessen Anwendungscharakteristik, kann daher das Portal einfacher und schneller bedienen

- Die Kundengruppe muss nicht aufwendig je nach Bedürfnis und Zuständigkeit das jeweilig relevante Portal aufsuchen, sondern hat alle Bedürfnisse an einem Ort abgedeckt und muss sich nicht um Zuständigkeiten kümmern
- Bei Behördengängen mit kantonalem Vollzug kann die Frage der kantonalen Zuständigkeit bereits innerhalb des Portals geklärt und anschliessend der korrekte Prozess angeboten werden.

Nachteile:

- Jede Implementation des betreffenden Behördengangs muss ändernden Anforderungen der zuständigen Behörde separat nachgeführt werden
- Das für die Abbildung eines Behördengangs nötige Fachwissen ist meist umfassend und vom Portalbetreiber nur aus zweiter Hand verfügbar. (Es sei denn, der Portalbetreiber ist Teil der Behörde, wie in Abbildung 8 illustriert)
- Separate individuelle Abbildungen von bestehenden, digitalen Behördengängen widersprechen dem wirtschaftlichen Prinzip der Wiederverwendung (ausser bei bestehenden, kantonalen Behördengängen ohne Zuständigkeitszuordnung und durchgängige Transaktion)

Um die Vorteile nutzen zu können und gleichzeitig die Nachteile zu umgehen, gibt es auch die Möglichkeit, dass Portale Behördengänge, die bereits auf einem anderen Portal implementiert wurden, nachnutzen. Das heisst, ein Portal bindet einen Behördengang ein, der auf einem anderswo bestehenden Transaktionslayer implementiert ist (siehe das in Abbildung 19 dargestellte exemplarische Konstrukt, bei dem Behördenleistungsportal A den Behördengang "Leistung 3" nicht selbst implementiert, sondern von Behördenleistungsportal B einbindet). Auf diese Weise ist zum Beispiel in EasyGov die Mehrwertsteueranmeldung realisiert: Statt einer Eigenentwicklung wurde die bestehende Implementation der ESTV eingebunden.

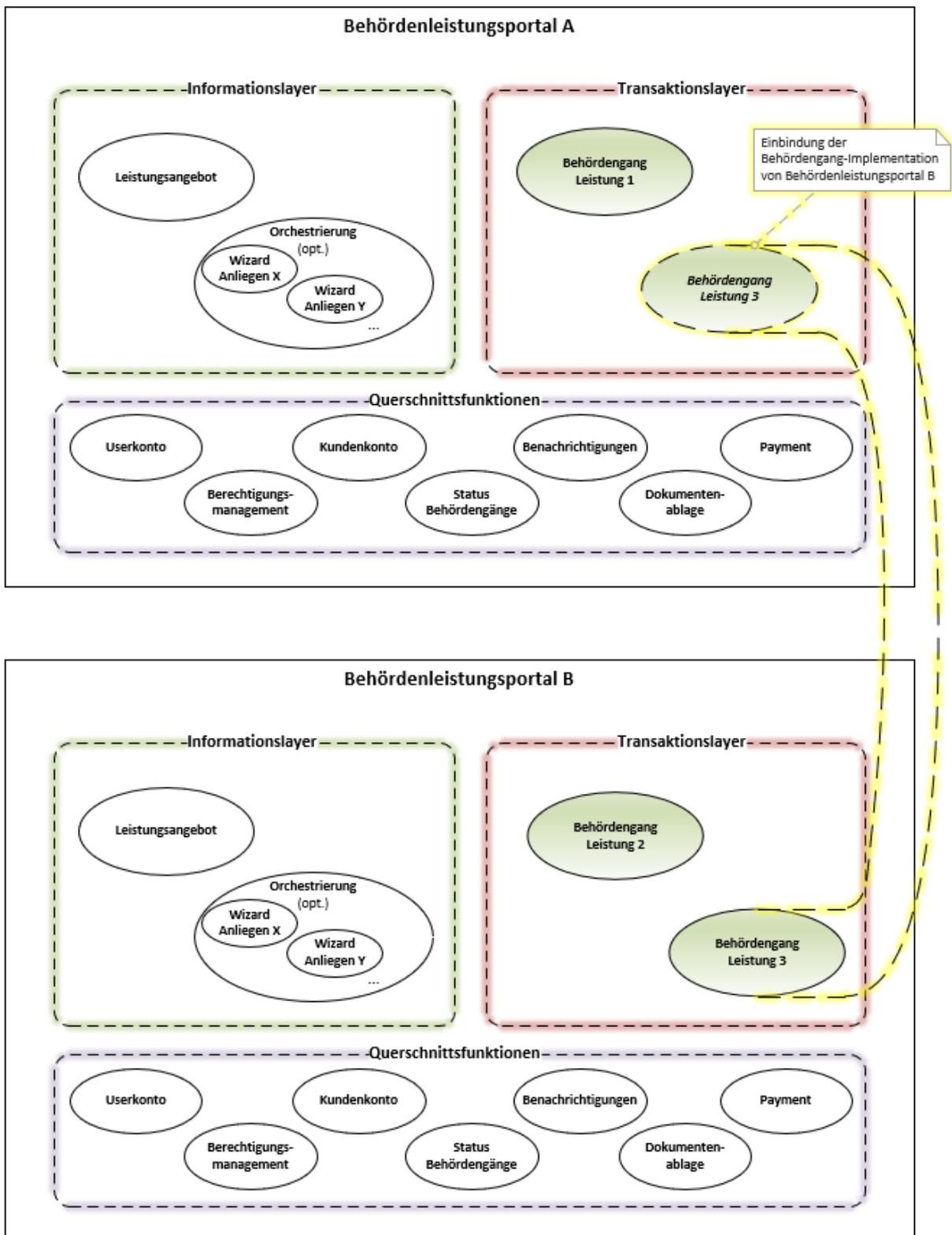


Abbildung 19: Einbindung einer bestehenden Implementation eines Behördengangs in einem anderen Portal

Die möglichen technischen Einbindungsmuster seien an dieser Stelle vorerst nicht betrachtet (dies erfolgt im Kapitel 2.1.6); es sei lediglich festgestellt, dass die Integration derzeit durch individuelle Schnittstellen erfolgt und folglich entsprechend aufwändig ist. Dies wird insbesondere durch konzeptuelle Unterschiede der Portalsysteme erschwert. Letztlich ist dieser Umstand ein wesentlicher Treiber für die vorliegende Studie. Die entsprechend grosse Komplexität gilt es zu beherrschen und nach Möglichkeit schrittweise zu reduzieren.

2.1.5 Informationsmodell der wichtigsten Begriffe

Die in den vorangegangenen Abschnitten herausgearbeiteten Begriffe seien nun in einem Informationsmodell in Beziehung gebracht.

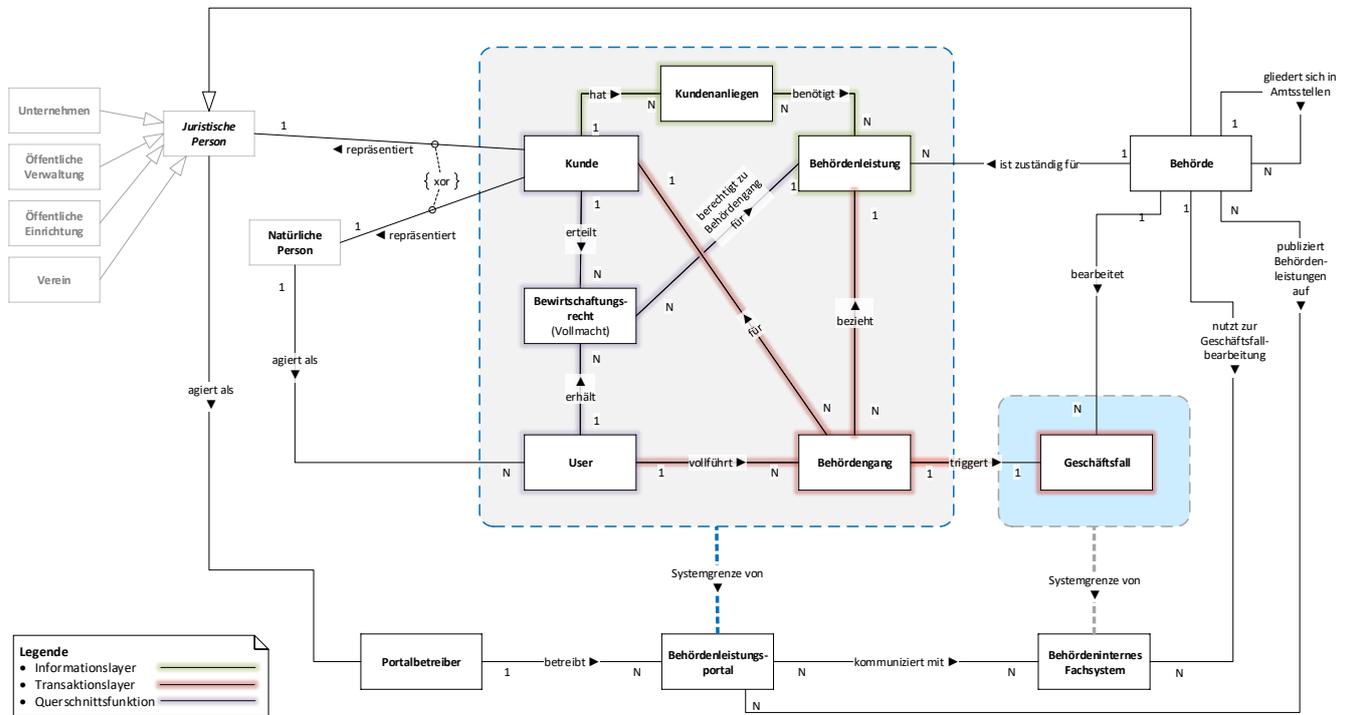


Abbildung 20: Informationsmodell für Behördenleistungsportale (UML-Klassendiagramm, vergrößerte Darstellung siehe Anhang B)

Hinweise:

- Die beiden farbig hinterlegten Flächen umreissen jeweils den inhaltlichen Scope von Behördenleistungsportal bzw. behördeninternem Fachsystem
- Die in der Abbildung grau umrandeten Entitäten dienen der Illustration. So wird z.B. aufgezeigt, dass als Kunde entweder eine juristische Person (z.B. in Form eines Unternehmens) oder eine natürliche Person auftritt. Letztere kann zusätzlich auch als User mit dem Behördenleistungsportal interagieren. Die grau umrandeten Illustrierungen werden nachfolgend nicht weiter erläutert.
- Das Informationsmodell weicht in einigen Punkten von dem im eCH-0177 [16] formulierten Modell ab. Letzteres weist bekanntermassen Schwächen auf, der Standard ist zur Überarbeitung vorgesehen.

Tabelle 1: Erläuterung der im Informationsmodell dargestellten Entitäten

Entität bzw. Begriff	Beschreibung
Behörde	Eine öffentlich-rechtlich begründete Organisation, welche hoheitliche Staatsaufgaben der Schweiz wahrnimmt. Behörden können auf Ebene von

Entität bzw. Begriff	Beschreibung
	<p>Gemeinde, Kanton oder Bund existieren und zur Legislative, Exekutive oder Judikative gehören.</p> <p>Hinweise:</p> <ul style="list-style-type: none"> • Die Staatsaufgaben können sowohl einer öffentlichen Stelle auch als auch einer privaten Organisation übertragen werden. • Die hierarchische Gliederung in Organisationseinheiten (auch Stellen genannt) wird mit dem Begriff Behörde nicht weiter differenziert. Der Begriff adressiert eine Organisationseinheit, gleich auf welcher Hierarchiestufe sie angesiedelt ist und ob bzw. wieviel unter- oder übergeordnete Einheiten sie hat.
Behörden-gang	<p>Der Behördengang ist ein Prozess, der aus der Kundensicht alle Aktivitäten und Verfahrensschritte umfasst, die zum Bezug einer Behördenleistung erforderlich sind. Er widerspiegelt die Sicht des Leistungsbezügers auf das behördliche Verwaltungsverfahren. Die Prozessschritte verhalten sich komplementär zu denen der Geschäftsfallbearbeitung auf Behördenseite.</p> <p>Dabei können folgende Prozessschritte unterschieden werden:</p> <ul style="list-style-type: none"> • Anstoss des Verfahrens durch den Kunden (z.B. Gesuchstellung) • Im Rahmen der Bearbeitungsphase: <ul style="list-style-type: none"> - Der Kunde wird möglicherweise mehrmals von den Behörden kontaktiert, z.B. um Auskunft zu geben oder Dokumente nachzuliefern. - Leistungsentgegennahme beim Kunden in Zusammenhang mit der Eröffnung (Übergabe) eines behördlichen Entscheides (z.B. Erteilung einer Baubewilligung). • Verfahrensabschluss. Mit der Leistungsübergabe ist für den Kunden das Verfahren entweder abgeschlossen oder aber er kann gegen einen missliebigen Behördenentscheid rekurrieren (mit der Eingabe des Rekurses wird ein neuer Durchgang ab der Phase „Anstoss“ eingeleitet)
Behördenin-ternes Fach-system	<p>Eine oder mehrere Fachanwendungen, welche die Geschäftsfallbearbeitung von einer oder mehreren Behördenleistungen innerhalb einer Behörde unterstützen. Benutzer sind ausschliesslich Mitarbeitende der jeweiligen Behörde.</p> <p>Aus Sicht eines Behördenleistungsportals kann man das behördeninterne Fachsystem als Back-End assoziieren.</p>
Behörden-leistung	<p>Öffentliche Leistung (A2A, A2B oder A2C-Tätigkeit), die eine Behörde im Rahmen ihrer Zuständigkeit gemäss staatlichem Auftrag für den Kunden (NP oder JP) anbietet. Die Inanspruchnahme erfolgt durch einen kundenseitigen Behördengang, die Leistungserbringung durch die behördenseitige Geschäftsfallbearbeitung.</p>
Behörden-leistungsportal	<p>Öffentlich zugängliche Applikation (z.B. Single Page Application, mobile App, etc.), mit der der Portalbetreiber im Rahmen des E-Governments dem Kunden einen digitalen Zugangskanal für eine oder mehrere</p>

Entität bzw. Begriff	Beschreibung
	<p>Behördenleistungen bietet. Es stellt das Kunden-Front-End¹⁴ für digitale Behördenleistungen dar, welches von entsprechend bevollmächtigten Usern bedient wird. Die Funktionen eines Behördenleistungsportals lassen sich in Informationslayer, Querschnittsfunktionen und Transaktionslayer logisch gliedern. Im Transaktionslayer des Portals wird der kundenseitige Behördengang abgebildet, jedoch keine behördeninternen Prozesse (siehe Abbildung 10).</p> <p>Hinweise:</p> <ul style="list-style-type: none">• Als Synonym für Behördenleistungsportal ist auch der Begriff Plattform gebräuchlich. Dieser Begriff findet jedoch auch in anderen Zusammenhängen Verwendung (z.B. Betriebssystem, Cloud, Softwareentwicklung, siehe Wikipedia) und wird deshalb im Rahmen der Studie nicht weiter verwendet.• Bei einigen Portalen (z.B. ePortal Bund) wird der Transaktionslayer modular in separaten Portal-Fachanwendungen realisiert (siehe Kapitel 2.1.6).• Der inhaltliche Umfang des Informationslayers variiert von Portal zu Portal je nach dessen Ausrichtung. Die Bandbreite erstreckt sich von der puren Leistung der angebotenen Behördenleistungen bis hin zu umfangreichen Orchestrierungen.
Bewirtschaftungsrecht (Vollmacht)	<p>Das Bewirtschaftungsrecht bildet eine Vollmacht ab, die im juristischen Sinne einen Vertreter zu Handlungen im Namen des Rechtssubjekts - d.h. dem Kunden - legitimiert. Auf dem Behördenleistungsportal ermächtigt diese Vollmacht einen User das betreffende Kundenkonto zu bewirtschaften und dabei Behördengänge für eine bestimmte Behördenleistung zu vollführen, wobei die Berechtigung abgestuft erfolgen kann (z.B. Einsicht, Bearbeiten, Einreichen, Superuser).</p> <p>Die Erteilung und Verwaltung der Bewirtschaftungsrechte obliegen der Verantwortung des Kunden bzw. dem von ihm dazu ermächtigten Vertreter. Praktischerweise wird dem Initialuser eines Kunden nach einem vorausgehenden Vollmachtenprozess¹⁹ ein pauschales "Darf alles"-Superuser-Bewirtschaftungsrecht erteilt (quasi eine Sammelvollmacht), das bezüglich dieses Kunden für alle Behördenleistungen sowie der Berechtigungsverwaltung berechtigt (siehe Bedürfnis [B-10]).</p>

¹⁹ Im Vollmachtenprozess wird eine schriftliche Kundenbestätigung eingeholt, dass der betreffende User für den Kunden Behördengeschäfte ausführen darf.

Entität bzw. Begriff	Beschreibung
Geschäftsfall/ Geschäftsfallbearbeitung	<p>Prozess, der infolge eines Behördengangs (d.h. bei Bezug einer Behördenleistung durch den Kunden) in der zuständigen Behörde ausgelöst wird. Die Geschäftsbearbeitung umfasst alle Aktivitäten und Verfahrensschritte, die aus behördlicher Sicht zur Erbringung einer Behördenleistung erforderlich sind. Sie widerspiegelt die Sicht des Leistungserbringers auf das Verwaltungsverfahren. Die Prozessschritte verhalten sich komplementär zu denen des Behördengangs auf Kundenseite. Die Geschäftsbearbeitung kann als Ganzes von einer oder mehreren Amtsstellen erbracht werden.</p> <p>In der Regel unterstützt ein behördeninternes Fachsystem die Geschäftsbearbeitung.</p>
Informationslayer	<p>Funktionsbereich eines Behördenleistungsportals, der dem User einen Überblick über die verfügbaren Behördenleistungen (Leistungsangebot) gibt und zur benötigten Leistung führt. Wie Abbildung 11 illustriert, kann dabei auch eine Orchestrierung von Leistungen angeboten werden, welche den User für ein bestimmtes Kunden-Anliegen mittels eines Wizards über alle dafür relevanten Muss- und Kann-Behördenleistungen führt. Das ist z.B. bei einer Unternehmensgründung in EasyGov der Fall, welche schrittweise über die nötigen Formalitäten und Anmeldungen führt (Handelsregister, AHV, Mehrwertsteuer etc.). Der Informationslayer kann sich zum Teil auch über das Behördenleistungsportal hinaus auf die Webpräsenz der jeweiligen Behörde erstrecken.</p>
Kunde	<p>Rechtssubjekt, für die eine Behördenleistung in Anspruch genommen wird. Dies ist entweder eine juristische oder eine natürliche Person (oder eine Gruppe dessen), welche gemäss gesetzlicher Grundlage Verpflichtung oder Anspruch auf eine Behördenleistung hat. Der Kunde wird im Portal durch ein Kundenkonto abgebildet. Zur Vereinfachung von A2B- und A2C-Geschäften wurden in der Schweiz gesetzliche Regelungen für eindeutige Kunden-Identifikatoren getroffen. Für juristische Personen gibt es die UID²⁰, für natürliche Personen die Versichertennummer (AHVN13)²¹.</p> <p>Hinweis: Als Synonym für Kunde ist auch der Begriff Geschäftspartner gebräuchlich, welcher aus dem SAP-Umfeld kommt. Ebenso sei auch der Begriff Stammdaten erwähnt, der mitunter als Synonym für Kundendaten gebraucht wird. Diese und weitere Synonyme sind im Glossar (siehe Anhang A) zugeordnet.</p>
Kundenanliegen	<p>Ein Kundenanliegen bezeichnet den Grund bzw. den Auslöser, weshalb eine Behördenleistung bezogen wird. Im Falle von NP-Kunden spricht man</p>

²⁰ Die UID wird für Unternehmen vom UID-Register des BFS herausgegeben, wobei der Unternehmensbegriff als in der Schweizer Wirtschaft aktive Einheiten weit gefasst ist. Siehe <https://www.bfs.admin.ch/bfs/de/home/register/unternehmensregister/unternehmens-identifikationsnummer.html>

²¹ Siehe <https://www.bfs.admin.ch/bfs/de/home/register/nationaler-adressdienst.html> und <https://www.egov.ch/de/umsetzung/umsetzungsziele/nationaler-adressdienst/>

Entität bzw. Begriff	Beschreibung
	<p>hierbei auch von «Lebenslage», im Falle von JP-Kunden auch von «Geschäftssituation» (siehe eCH-0126 [14] und eCH-0138 [15])²².</p> <p>Beispiel: Ein Landwirt will temporär eine ausländische Person (z.B. aus der EU) als Erntehelfer anstellen und sich dabei legal verhalten. Als Folge davon muss dieser Landwirt mehrere Behördenleistungen beziehen (Anmeldung der Anstellung aufgrund der Freizügigkeitskontingente, Anmeldung Sozialversicherungen, Anmeldung Unfallversicherung, Anmeldung Quellensteuer, evtl. weitere).</p> <p>Eine systematische Zusammenstellung von Kundenanliegen findet man für NP in [38] und für JP in [39].</p>
Portalbetreiber	<p>Unternehmen oder Organisation, welche/s als Leistungserbringer/Service Provider der Behörde als Leistungsbezüger ein Behördenleistungsportal zur Verfügung stellt. Dies kann auch eine Amtsstelle der Behörde selbst oder ein privater Anbieter sein.</p>
Querschnittsfunktion	<p>Sammelbegriff für allgemeine Portalfunktionen die sowohl im Informations- als auch im Transaktionslayer zur Anwendung kommen: z.B. Userkonto, Berechtigungsmanagement, Kundenkonto, Status der Behördengänge, behördliche Benachrichtigungen, Dokumentenablage, Payment, etc.</p>
Transaktionslayer	<p>Funktionsbereich zur Abwicklung einer Behördenleistung. Das umfasst sowohl den kundenseitigen Behördengang im Portal als auch die behördenseitige Geschäftsfallbearbeitung im behördeninternen Fachsystem (vergleiche Abbildung 10).</p>
User	<p>Natürliche Person, welche das Behördenleistungsportal über eine Benutzeroberfläche (UI) aktiv benutzt^{23, 24} und dabei Behördengänge für einen bestimmten Kunden vollführt. Der User wird im Portal durch ein Userkonto repräsentiert, welches mit Sicherheitsfunktionen zur Authentisierung / Autorisierung verbunden ist. Die Authentisierung bezieht sich auf den Systemzugang, die Autorisierung auf die kundenspezifischen Bewirtschaftungsrechte.</p>

Für weitere Begriffe, die im Verlauf dieser Studie Verwendung finden, sei auf das Glossar im Anhang A verwiesen.

²² Die Definition folgt dem Vorschlag von Alexander Kämpfer (BK).

²³ Eine natürliche Person kann mehrere User bzw. Benutzerkonten unterhalten. Umgekehrt sei davon ausgegangen, dass hinter einem User genau eine Person steht, da die Weitergabe von Credentials in der Regel nicht legal ist.

²⁴ Prinzipiell kann hinter einem User auch eine Maschine stehen. Dies sei jedoch hier ausgeschlossen, da sich der Kontext bewusst auf das User Interface beschränkt, denn Behördenleistungsportale werden für Mensch-User gebaut. Maschinenschnittstellen werden an anderer Stelle behandelt, siehe Abbildung 29 und Abbildung 30.

2.1.6 Integrationsmuster für die Abbildung von Behördengängen

Abschliessend sei für die Abbildung von Behördengängen aufgezeigt, welche Integrationsmuster aus der Praxis zu abstrahieren sind.

- Integrationsmuster 1: **Implementation** des Behördengangs direkt im Portal²⁵
- Integrationsmuster 2: **Einbindung** eines extern implementierten Behördengangs²⁶

Das erste Muster entspricht einer Implementation (in der Regel eine Individualentwicklung) des kundenseitigen Behördengangs direkt im Portal. Dabei wird der Behördengang für eine bestimmte Leistung vollständig im Portal abgebildet, die Umsetzung unterliegt somit der Verantwortung des Portalbetreibers²⁷. Die gemäss Abbildung 9 (Kapitel 2.1.2) nötige Kommunikation zwischen dem Behördengang und der Geschäftsfallbearbeitung wird über eine Schnittstelle vom Portal zum behördeninternen Fachsystem abgewickelt, welche als Schnittstelle "Behördengang↔Geschäftsfallbearbeitung" bezeichnet sei. Wie die folgende Abbildung 21 illustriert, fungiert das behördeninterne Fachsystem hierbei als Provider (des Services Geschäftsfallbearbeitung), das Portal hingegen als Consumer, da die Behördengang-Implementation den Service der Geschäftsfallbearbeitung nutzt.

Die Provider-Rolle der Geschäftsfallbearbeitung ist dabei nicht so zu verstehen, dass sie nur einem Consumer-Portal dient. Vielmehr können durchaus mehrere Consumer-Portale bedient werden, welche den Behördengang für die betreffende Leistung implementieren. Die nächstfolgende Abbildung 22 illustriert diesen Fall: Der User kann den Behördengang für die Leistung X sowohl auf Portal 1 als auch auf Portal 2 vollführen. Portal 1 könnte z.B. der Online-Schalter der betreffenden Behörde sein bzw. Portal 2 ein kundenspezifisches wie EasyGov.

²⁵ Im EasyGov-Umfeld ist dafür auch der Begriff "Vollintegration" üblich

²⁶ Im EasyGov-Umfeld ist dafür auch der Begriff "Teilintegration" üblich

²⁷ dies kann auch die Behörde selbst sein, siehe Abbildung 8

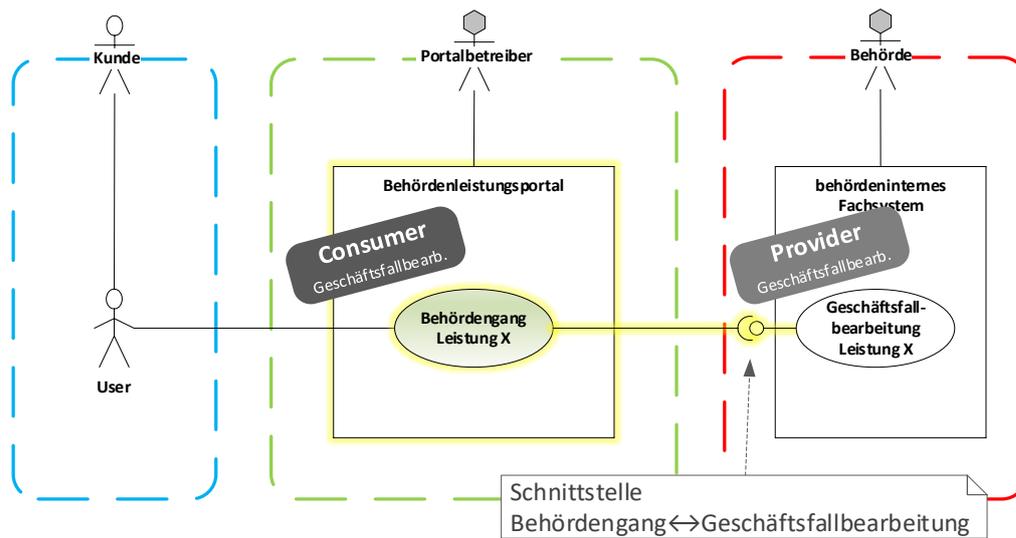


Abbildung 21: Integrationsmuster 1 - Implementation des Behördengangs direkt im Portal

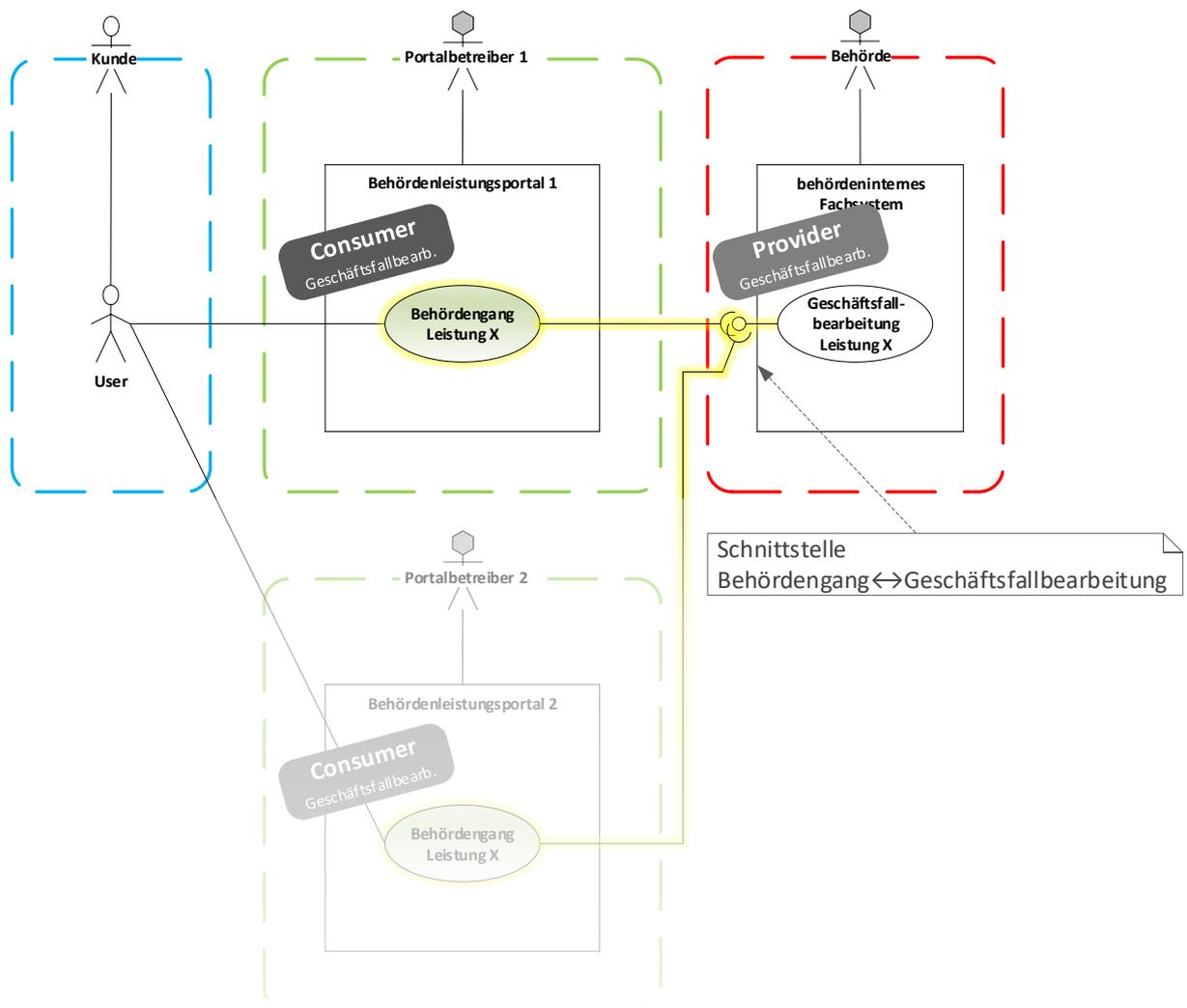


Abbildung 22: Integrationsmuster 2 erlaubt auch mehrere Consumer-Portale

Als Spezialfall von Integrationsmuster 1 ist es zu werten, wenn ein Behördenleistungsportal als Ausführungsumgebung oder wiederverwendbare/s Framework/Plattform (z.B. iGovPortal, e-Portal Bund²⁸) für digitale Behördenleistungen fungiert. Das heisst, es bietet die nötige Querschnittsfunktionalität, auf deren Basis konkrete Behördengänge als Portal-Fachanwendung (quasi als AddIn) implementiert bzw. in vorgefertigten Komponenten konfiguriert werden können. Dieser Ansatz ermöglicht, dass eine Behörde ihre Leistungen unter eigener Verantwortung digital anbieten kann, ohne dass sie selbst ein eigenes Portal betreiben bzw. entwickeln muss. Letztlich bleibt es aber beim Prinzip von Integrationsmuster 1, weshalb die Spezialfälle aus Sicht der Integrations-Sollarchitektur keine differenzierte Betrachtung verlangen.

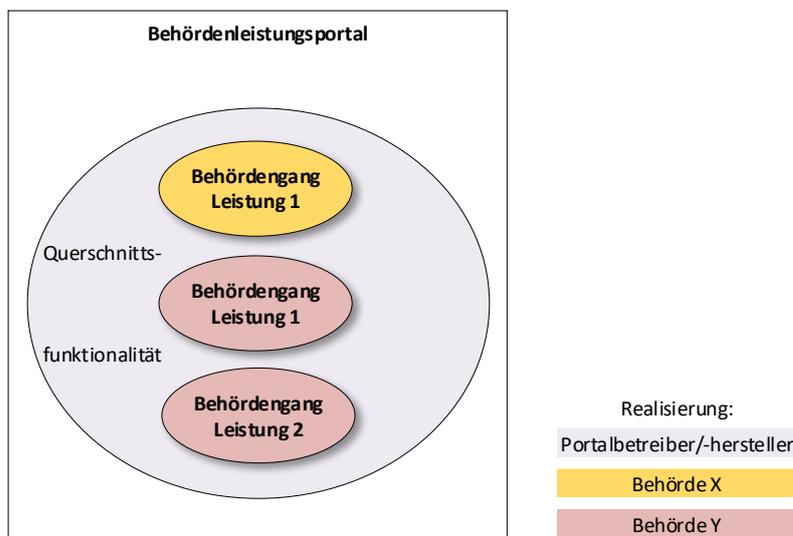


Abbildung 23: Spezialfall Integrationsmuster 1: Ein Behördenleistungsportal bietet eine Ausführungsumgebung/Framework für Behördenleistungen, auf der Behörden ihre Behördenleistungen als Portal-Fachanwendung implementieren bzw. in vorgefertigten Komponenten konfigurieren

Im Unterschied zur direkten Implementation im Portal kann auch eine bestehende Implementation von einem externen System eingebunden werden. Diese Konstellation wird durch das zweite Integrationsmuster unterstützt. Es erlaubt die in Kapitel 2.1.4 / Abbildung 19 aufgezeigte Nachnutzung eines in einem anderen Portal direkt implementierten Behördengangs, was insbesondere für die Umsetzung eines orchestrierten Leistungsangebots hilfreich ist. Wie die folgende Abbildung 24 illustriert, fungiert dieses andere Portal (rechts) als Provider, denn es stellt im Service-Sinne den Behördengang komplett samt UI, Geschäftslogik und Datenhaltung zur Verfügung. Das einbindende Portal (links) ist der Consumer der Behördengang-Implementation, indem es diese bei sich an geeigneter Stelle "reinhängt"²⁹. Der User vollführt einen «Absprung» vom Consumer- zum Provider-Portal, wobei im Hintergrund auch der Session-Kontext

²⁸ Das ePortal mit den darin enthaltenen Portal-Fachanwendungen ist aus äusserer Sicht ein Portal-System im Sinne von Abbildung 23. Intern steckt dahinter ein Ökosystem von zentralen Komponenten (z.B. PAMS, Notification-Service, etc. sowie das ePortal selbst) und Portal-Fachanwendungen, die in einer Microservice-Architektur zusammenwirken.

²⁹ Diese Aussage ist technologieunabhängig zu verstehen. Ob die technische Einbindung via Weiterleitung, Web Components, iFrame o.ä. erfolgt, berührt das Prinzip nicht.

übertragen wird, so dass der User auf dem Provider-Portal nahtlos weiterarbeiten kann (wie in der später folgenden Abbildung 34 veranschaulicht). Das bedeutet insbesondere, dass der Übergang mit Single Sign On (SSO) und einer Kontextsynchronisation (Leistungs- und Kunden- selektion, Bewirtschaftungsrechte) einhergeht. Für das Behördengang-Consumer-Portal bleibt die Schnittstelle Behördengang↔Geschäftsfallbearbeitung (siehe Integrationsmuster 1 oben) verborgen, sie spielt beim Integrationsmuster 2 keine Rolle.

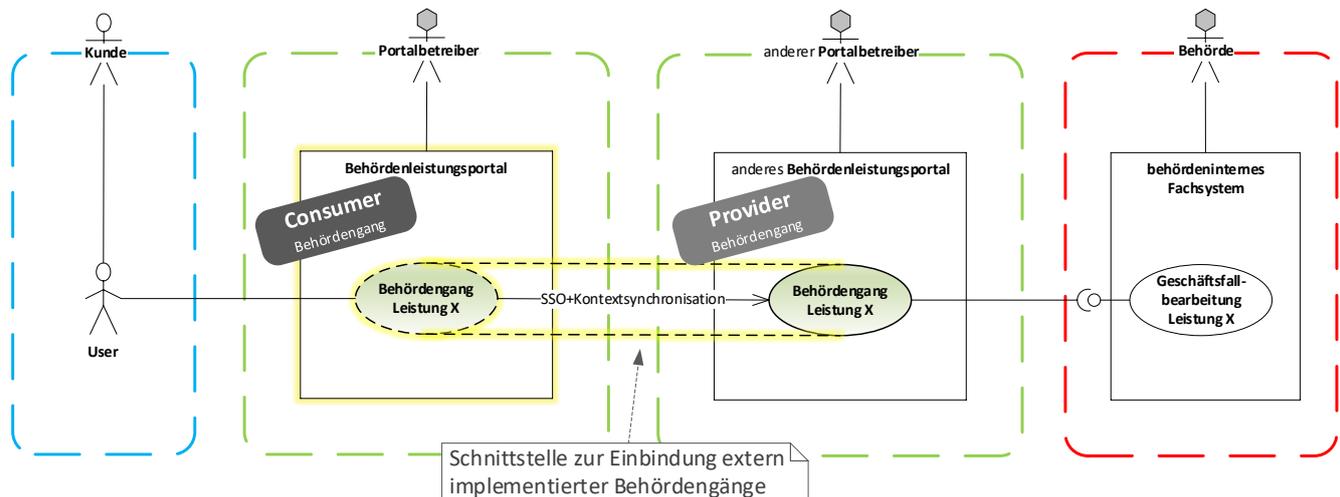


Abbildung 24: Integrationsmuster 2 - Einbindung eines extern implementierten Behördengangs

Die genannten Integrationsmuster treten in der Praxis oft in Kombination auf. Ein Portal kann den einen Behördengang direkt implementieren (nach Integrationsmuster 1) und einen anderen von extern einbinden (Integrationsmuster 2). Ein Beispiel für eine solche Mischform ist EasyGov, das anfänglich nur direkt implementierte Behördengänge enthielt, aber im weiteren Ausbau zunehmend die Möglichkeit der Einbindung nutzt.

Die folgende Abbildung 25 zur Mischform illustriert am Beispiel eines fiktiven Behördenleistungsportals 1, dass

- der direkt implementierte Behördengang Leistung X die Schnittstelle "Behördengang↔Geschäftsfallbearbeitung" des behördeninternen Fachsystems 2 der für die Leistung zuständigen Behörde nutzt,
- es den Behördengang Leistung Y des anderen Portals 3 einbindet,
- der User den Behördengang Leistung Y sowohl auf dem Portal 1 als auch auf dem anderen Portal 3 durchführen kann, welches den hinter der Einbindung stehenden Behördengang implementiert.

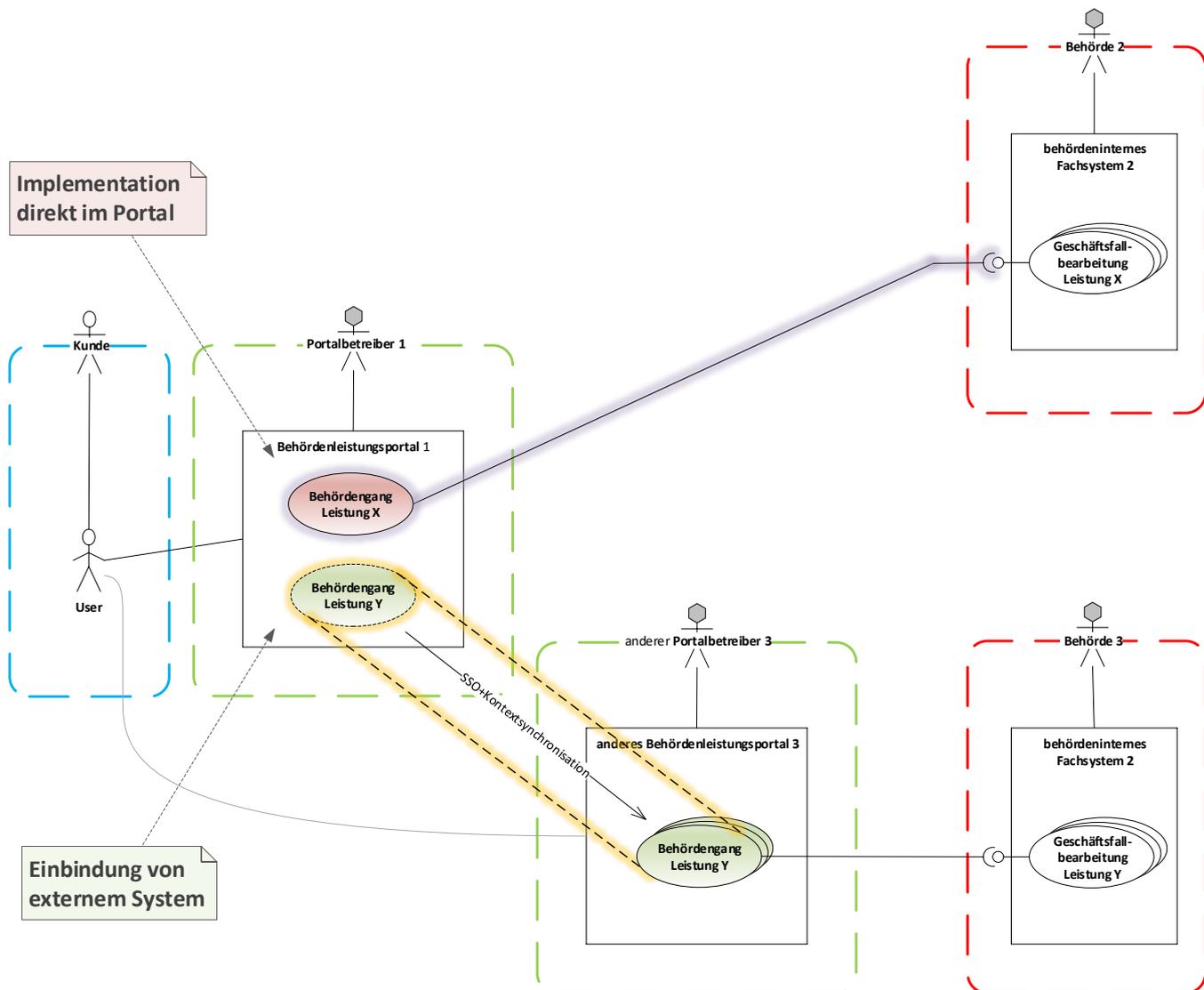


Abbildung 25: Mischform – Portal bildet Behördengänge sowohl nach Integrationsmuster 1 und 2 ab

2.2 Bedürfnisse an die Domäne Behördenleistungsportale aus Business-Sicht

2.2.1 Rahmenbedingungen

Sowohl aus dem Projektinitialisierungsauftrag als auch aus der Bedürfnisabklärung (siehe 2.2.2) lassen sich folgende Rahmenbedingungen für die Erarbeitung der Sollarchitektur ableiten:

Tabelle 2: Rahmenbedingungen für die Entwicklung der Sollarchitektur

Nr.	Titel	Rahmenbedingung
[F-1]	eCH-Standards	Die Sollarchitektur wird unter Berücksichtigung von eCH-0123 [12], eCH-0124 [13] und eCH-0177 [16] erarbeitet. Bei Abweichungen werden RFCs (Request for Changes) zuhanden von eCH erstellt. Die Modellierung von Geschäftsprozessen und -regeln muss konform zu diesen Standards erfolgen:

		<ul style="list-style-type: none"> • eCH-0074 Grundsätze zur grafischen Modellierung von Geschäftsprozessen, Version 2.2 (2020) [24] • eCH-0158 BPMN-Modellierungskonventionen für die öffentliche Verwaltung, Version 1.2 (2020) [11] • eCH-0242 Modellierung von Geschäftsregeln, Version 1.0 (2020) [25]
[F-2]	ISA ² -Lösungen	Es werden die folgenden ISA ² -Lösungen ³⁰ berücksichtigt: Core Public Service Vocabulary Application Profile ³¹ (CPSV-AP) und The New European Interoperability Framework (EIF) [17].
[F-3]	Natürliche und juristische Personen	Der Architekturvorschlag soll sowohl für Leistungen für juristische als auch für natürliche Personen Gültigkeit haben.
[F-4]	Fokus A2C	Der Fokus liegt auf der Schnittstelle Kunde-Behörde (A2B, A2C). Für interne Behördenprozesse sind die jeweiligen Fachsysteme zuständig.
[F-5]	UX-Architektur-anforderungen	Aus UX-bezogenen Bedürfnissen resultierende Architektur-anforderungen sind zu berücksichtigen, die UX-Bedürfnisse selbst sind jedoch nicht relevant.
[F-6]	Barrierefreiheit	Gemäss gesetzlicher Vorgabe ist die Barrierefreiheit zu gewährleisten.

2.2.2 Bedürfnisse

In den nachfolgenden Kapiteln 2.2.2.3 bis 2.2.2.9 sind Bedürfnisse zusammengetragen, die für die Domäne Behördenleistungsportale – sprich der Digitalisierung von Behördenleistungen in der Gesamtsicht – ermittelt wurden. Diese wurden mittels einer Umfrage bei den im Projektausschuss angesiedelten Stakeholdern initial erarbeitet und um Wünsche von weiteren Stakeholdern des Architekturboards E-Government Schweiz ergänzt, welche im Rahmen der Sitzung vom 11. August 2020 genannt wurden. Schlussendlich wurden die Bedürfnisse in mehreren Iterationen mit dem Projektausschuss und dem Fachausschuss Architekturreview EasyGov verifiziert und finalisiert.

Um eine bessere Übersicht über die Bedürfnisse zu erhalten, wurden sie gemäss Tallinn-Deklaration zum E-Government kategorisiert und verschiedenen Themen zugewiesen. Zudem wird pro Bedürfnis angegeben, für welche Akteure dieses relevant ist. Am Ende dieses Kapitels (Kap. 2.2.2.10) wird die Kategorisierung visualisiert.

Hinweis: Es ist bewusst von Bedürfnissen und nicht von Anforderungen die Rede, da deren Stakeholder-nahe Formulierungen nicht dem Qualitätsanspruch von detaillierten Anforderungen entspricht, aus

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

denen man z.B. Testfälle ableiten kann. Der Bedürfniskatalog dient vielmehr als Grundlage und Anregung für die Formulierung des Zielbilds. In diesem Sinne wird auch im Kapitel 2.6 letztlich bilanziert, inwiefern die Stakeholder-Bedürfnisse vom Zielbild abgedeckt werden.

2.2.2.1 Kategorisierung gemäss Tallinn-Deklaration zum E-Government

Bundesrat Ueli Maurer hat 2017 zusammen mit den Regierungen der EU und der EFTA die Tallinn Declaration on eGovernment³² unterzeichnet. Die Ziele der Deklaration stehen im Einklang mit der von Bund, Kantone und Gemeinden verabschiedeten E-Government-Strategie Schweiz. Die Prinzipien von Tallinn sind nachfolgend aufgeführt. Eine konsequente Umsetzung dieser Prinzipien bietet Bevölkerung und Wirtschaft eine zukunftsfähige, digitale öffentliche Infrastruktur.³³

Tabelle 3: Prinzipien der Tallin Deklaration zum E-Government

T1	Digital by default, inclusiveness and accessibility	Standardmässig digital, inklusive und zugänglich
T2	Once-only	Einmalige Eingabe von Daten durch den User (und nicht wiederkehrend bei jedem Behördengang)
T3	Trustworthiness and security	Vertrauenswürdigkeit und Sicherheit
T4	Openness and transparency	Offenheit und Transparenz
T5	Interoperability by default	Standardmässige Interoperabilität

2.2.2.2 Strukturierung der Bedürfniserhebung

Bei der in Kapitel 2.2.2 erwähnten Umfrage wurden die Stakeholder gebeten, die Bedürfnisse aus unterschiedlichen Perspektiven zu identifizieren.

Die Perspektiven leiteten sich dabei aus den vorangegangenen Betrachtungen – insbesondere Kapitel 2.1.4 und 2.1.5 – identifizierten Akteure ab:

- User
- Kunde (natürliche wie auch juristische Personen)
- Behörde
- Portalbetreiber

Nach Abschluss der Bedürfniserhebung wurden die mannigfaltigen Inputs verdichtet und kategorisiert. Das Ergebnis ist in den folgenden Kapiteln 2.2.2.3 bis 2.2.2.9 dokumentiert. Dabei wird pro Bedürfnis angegeben, aus welcher Akteursperspektive dieses relevant ist bzw. von welchem Akteur es rührt. Die originalen Rückmeldungen sind im Anhang G.F einsehbar.

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

³³ Aus <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaefft?AffairId=20193686>

2.2.2.3 Bedürfnisse bezüglich der Integration von Behördenleistungen

Tabelle 4: Bedürfnisse bezüglich der Integration von Behördenleistungen

Nr.	Titel	Bedürfnis	Tallinn	Bedürfnis von...
[B-1]	Systeminteroperabilität	Die Behördenleistungen lassen sich in verschiedenen Portalplattformen einbinden (übergreifendes Portal, Gemeinde, Kanton, Bund) / Unterstützung verschiedener Integrationspattern (eCH). Mit anderen Worten gemäss [EIF-6]: Behördenleistungen sollen über verschiedene Kanäle bzw. Portale zugänglich sein, damit der User den Kanal auswählen kann, der seinen Bedürfnissen am besten gerecht wird.	T2, T5	Alle
[B-2]	Dateninteroperabilität	Verschiedene Behördenleistungsportale und relevante Quellsysteme müssen die Möglichkeit zum elektronischen Datenaustausch haben. Der Datenaustausch muss daher standardisiert (eCH-Standard) und nachvollziehbar erfolgen – sowohl A2C als auch A2B.	T5	Behörde, Portalbetreiber
[B-3]	Angebot Basisdienste	Bestehende Basisdienste und Portalinfrastrukturen können genutzt werden, um Behörden den Aufbau von neuen E-Government Angeboten zu vereinfachen.	T2	Behörde, Portalbetreiber
[B-4]	Metadaten-Verzeichnis	Ein zentrales Verzeichnis über alle digitalen Behördenleistungen samt den für die Integration notwendigen Spezifikationen soll vorhanden sein.	T4, T5	Behörde, Portalbetreiber
[B-5]	Integration bestehender Systeme ohne Impact auf andere Systeme	Die Integration bestehender Lösungen der verschiedenen Verwaltungsebenen Bund, Kanton und Gemeinden, sowie der verschiedenen Hersteller der Lösungen, soll zur Laufzeit, also ohne Herunterfahren und Hochfahren des Gesamtsystems, erfolgen können, soweit diese Lösungen die vereinbarten Schnittstellenstandards berücksichtigen.	T5	Behörde, Portalbetreiber

2.2.2.4 Bedürfnisse bezüglich Authentisierung und Autorisierung

Tabelle 5: Bedürfnisse bezüglich Authentisierung und Autorisierung

Nr.	Titel	Bedürfnis	Tallinn	Bedürfnis von...
[B-6]	Single sign on	Der User soll sich für die Nutzung der Behördenleistungen (auch für mehrere Kunden) nur einmal einloggen. Falls er mehrere Benutzernamen (logische Identitäten, z.B. eine für seine Behördengänge als natürliche Person und eine für Behördengänge, welche er als natürliche Person handelnd für eine juristische Person tätig) hat, können diese im Single Sign on zusammengeführt und verknüpft werden. Der dabei verwendete Level of Assurance (LoA, z.B. 2FA) oder die initialen Sicherheitsprüfungen (z.B. Email-Verifikation) soll von allen Behördenleistungen akzeptiert werden, unabhängig davon, auf welchem System diese ausgeführt wird.	T2	User
[B-7]	Mehrere Identitäten verwendbar	Für das Login sollen verschiedene bestehende elektronische Identitäten verwendet werden können (z.B. eID, SwissID, TrustID oder andere Identitäten wie Facebook, Google bei reduziertem Leistungsumfang).	T3	User
[B-8]	LoA differenziert	Eine Behördenleistung soll vom User keinen höheren LoA als notwendig verlangen (Z.B. ist das Informationsangebot ohne Authentifizierung einsehbar).	T3	User, Behörde
[B-9]	Elektronische Signatur	Notwendige Unterschriften sollen soweit möglich über den Authentisierungslevel (LoA) abgedeckt werden und somit entfallen. Dies unter der Voraussetzung der nachweislichen Prüfung der authentisierten Identität, dass die dahinterstehende Person auch wirklich die ist, die sie vorgibt zu sein. Dazu sind nicht nur die technischen, sondern auch die rechtlichen Grundlagen massgebend. Für Fälle, bei denen dies nicht möglich ist, soll eine elektronische Signatur verwendet werden können.	T3	User, Behörde
[B-10]	Berechtigungen selbst verwalten	Der Kunde (bzw. der ihn vertretende User) soll die Bewirtschaftungsrechte der Unternehmensmitarbeitenden und der natürlichen Personen im Self-Service Modus bewirtschaften können. Dazu soll eine Übersicht über die erteilten Berechtigungen bereitgestellt werden.	T3	Kunde

[B-11]	Standardisierte Vollmacht	Im Rahmen der Interoperabilität von Behördenleistungsportalen muss es das Ziel sein, eine standardisierte juristische Vollmacht zu erarbeiten und anzubieten, welche durch den Kunden nur einmal für einen bestimmten User erteilt werden muss. Der User soll dann in der Lage sein, alle interoperablen Behördengänge auf allen föderalen Ebenen für den Kunden zu vollführen.	T2, T5	User, Kunde
--------	---------------------------	---	--------	-------------

2.2.2.5 Bedürfnisse bezüglich Kommunikation Kunde – Behörde

Tabelle 6: Bedürfnisse bezüglich Kommunikation Kunde – Behörde

Nr.	Titel	Bedürfnis	Tallinn	Bedürfnis von...
[B-12]	Einfache Kontaktaufnahme mit Behörde	Der Kunde (bzw. der ihn vertretende User) kann im Falle von Fragen aus seiner Kundensicht einfach, daher spontan, sowie digital wie auch analog, mit der zuständigen Behörde Kontakt aufnehmen und Rückmeldungen an die zuständige Behörde geben. Es besteht ein klar definierter Supportprozess.	T4	Alle
[B-13]	Sichere und rechtsverbindliche Kommunikation Behörde – Kunde	Die Behörde soll mit einzelnen Kunden (z.B. Unterlagen nachzufordern, Fragen zu stellen) und mit ganzen Kundengruppen (z.B. für die Kommunikation von generellen Informationen) rechtsverbindlich und sicher ³⁴ kommunizieren können.	T3	Behörde

³⁴ Sicher bedeutet hier: Dem Use Case angemessen und dem heutigen Standard mittels Papier auf dem Postweg entsprechend.

2.2.2.6 Bedürfnisse bezüglich Präsentation (UI)

Tabelle 7: Bedürfnisse bezüglich Präsentation (UI)

Nr.	Titel	Bedürfnis	Tallinn	Bedürfnis von...
[B-14]	Sicht auf Behördenleistungen personalisieren	Der User soll seine Sicht auf die verfügbaren Behördenleistungen personalisieren können (z.B. Sprache, Bookmarks/Shortcuts für häufig verwendete Leistungen).	T1	User
[B-15]	Hilfe in der Vielfalt von Behördenleistungen	Dem User soll eine behördenübergreifende thematische Sicht geboten werden, um die Behördenleistungen einfach zu finden. Dabei soll ein leistungsübergreifend einheitliches Vokabular zur Verfügung stehen, z.B. für die Beschreibung von Dienstleistungen. Allenfalls kann für die Ordnung der Themen respektive der Geschäftsfälle ein Standard aus Sicht User angewendet werden.	T4	User
[B-16]	Behördenleistungen von einem Einstiegspunkt zugänglich	Der Kunde kann die für ihn relevanten Behördenleistungen möglichst von einem Einstiegspunkt (Portal) abwickeln. (Hinweis: Das heisst nicht, dass es nur ein Behördenleistungsportal geben darf).	T1	User

2.2.2.7 Bedürfnisse bezüglich Geschäftsabwicklung von Behördenleistungen

Tabelle 8: Bedürfnisse bezüglich Geschäftsabwicklung

Nr.	Titel	Bedürfnis	Tallinn	Bedürfnis von...
[B-17]	Once-Only	Der Kunde (bzw. der ihn vertretende User) will Daten behördenübergreifend nur einmal erfassen müssen (behördenübergreifendes Once-Only-Prinzip) ³⁵ . Wo verfügbar, werden die Daten aus einem Register oder Basisdienst bezogen. Falls spezifische Daten noch nicht behördenübergreifend verfügbar sind, müssen diese einmalig erfasst werden.	T2, T5	User, Kunde
[B-18]	Transparenz der Geschäftsfallbearbeitung	Der Kunde (bzw. der ihn vertretende User) muss sich über den Status der Geschäftsfallbearbeitung seiner laufenden und abgeschlossenen Behördengänge informieren können: Status der Bearbeitung, Zuständigkeit, allfällige Mitteilungen / Rückfragen, Ergebnis. Daraus folgt, dass die behördenseitige Geschäftsfallbearbeitung nachverfolgbar und transparent sein müssen.	T1, T3, T4	User, Kunde
[B-19]	Auch klassisch angestossene Geschäftsfälle verfolgbar	[B-18] gilt unabhängig davon, ob der jeweilige Geschäftsfall digital oder per klassischem analogem Behördengang initiiert wurde. (D.h. in letzterem Fall müsste die Behörde den Behördengang zusätzlich auf digitaler Ebene einstellen).	T1	Kunde, Behörde
[B-20]	Medienbruchfreie Geschäftsabwicklung	Der Kunde kann seine Behördengänge vollständig elektronisch (medienbruchfrei) abwickeln. Das gilt insbesondere für die Schnittstelle zur Geschäftsfallbearbeitung der jeweiligen Behörde.	T1	Alle

³⁵ Analog haben Behörden bei der Geschäftsfallbearbeitung auch ein Bedürfnis nach Once-Only. Dieses Bedürfnis wird bereits vom eGovernment.ch-Projekt UZ9 "Behördenübergreifende Stammdatenverwaltung aufbauen" angegangen und wird in dieser Studie nicht weiter behandelt.

[B-21]	Geführter Prozess	Die Behördengänge sollen soweit möglich schweizweit einheitlich und mit möglichst wenigen Interaktionen abgewickelt werden können und selbsterklärend sein (geführter Prozess).	T1	User, Kunde
[B-22]	Angebot für Unternehmen ohne UID	Behördengänge müssen auch für Unternehmen ohne UID (d.h. Unternehmen in Gründungsphase oder aus dem Ausland) – soweit sinnvoll – angeboten werden.	T1	Kunde, Behörde
[B-23]	Behörde behält Kontrolle über Behördenleistung	Die Behörde muss die Kontrolle über ihre Behördenleistung behalten (Inhalt, Prozess und Darstellung).	T1	Behörde
[B-24]	Proaktive Erkennung des Kundenbedarfs durch das Behördenleistungsportal	Proaktive Erkennung des Kundenbedarfs durch das Behördenleistungsportal soll integraler Bestandteil von Behördenleistungsportalen sein. Der Kunde soll da abgeholt werden, wo und wann er eine Leistung benötigt. Beispielsweise sollen Prozesse wie Aboerneuerungen oder Erneuerung des Passes bei Ablauf der Gültigkeit automatisch durch die Behörden angestossen werden, es kann sich jedoch auch um komplexere Bedürfniserkennung handeln. Weiter soll der Kunde, über weitere für ihn relevante Behördenfunktionalitäten informiert werden.	T1	Kunde, Behörde

2.2.2.8 Bedürfnisse bezüglich ISDS

Tabelle 9: Bedürfnisse bezüglich ISDS

Nr.	Titel	Bedürfnis	Tallinn	Bedürfnis von...
[B-25]	Gewährleistung ISDS	Informationssicherheit und Datenschutz müssen gewährleistet werden.	T3	alle
[B-26]	Transparenz bezüglich Verwendung der Daten	Der Kunde soll sich informieren können, wo seine Daten liegen und welche Behörden für welchen Zweck darauf zugreifen.	T3	User, Kunde
[B-27]	Verfügbarkeit des Gesamtsystems	Die Verfügbarkeit der Gesamtheit der beteiligten Systeme soll durch die Behörde, unter Berücksichtigung des Kundenwunsches, bestimmt und gewährleistet werden. Der Kunde soll sich über aktuelle Ausfälle, wie auch geplante Wartungsarbeiten informieren können.	T1	alle

2.2.2.9 Bedürfnisse bezüglich der Umsetzung und des Betriebes

Tabelle 10: Bedürfnisse bezüglich der Rahmenbedingungen für die Umsetzung

Nr.	Titel	Bedürfnis	Tallinn	Bedürfnis von...
[B-28]	Wirtschaftlichkeit	Die SOLL-Architektur muss Wirtschaftlichkeitsaspekte aller beteiligten Partner berücksichtigen.	T5	Kunde, Behörde, Portalbetreiber
[B-29]	Weiterentwicklungsqualität	... wie Reliability, Maintainability und Portability	-	Portalbetreiber

2.2.2.10 Verteilung der Bedürfnisse nach Kategorien

In der nachfolgenden Abbildung 26 sind die unverdichteten Originalinputs der Bedürfnisumfrage (siehe Anhang G.F) gemäss der in Kapitel 2.2.2.2 beschriebenen Strukturierung visualisiert. Es zeigt sich folgendes:

- Alle Prinzipien der Tallin Deklaration zum E-Government scheinen von den Bedürfnissen ausreichend abgedeckt zu sein.
- Die Schwerpunkte liegen in den Kategorien der Integration von Behördenleistungen, der Geschäftsabwicklung, sowie ISDS.
- Die Kategorie der Präsentation (UI) wird nur durch drei Bedürfnisse abgedeckt. Dies wird jedoch für die architekturbezogene Ausrichtung der Studie als genügend erachtet.
- Die Akteurs-Perspektiven sind einigermassen gleichmässig verteilt.

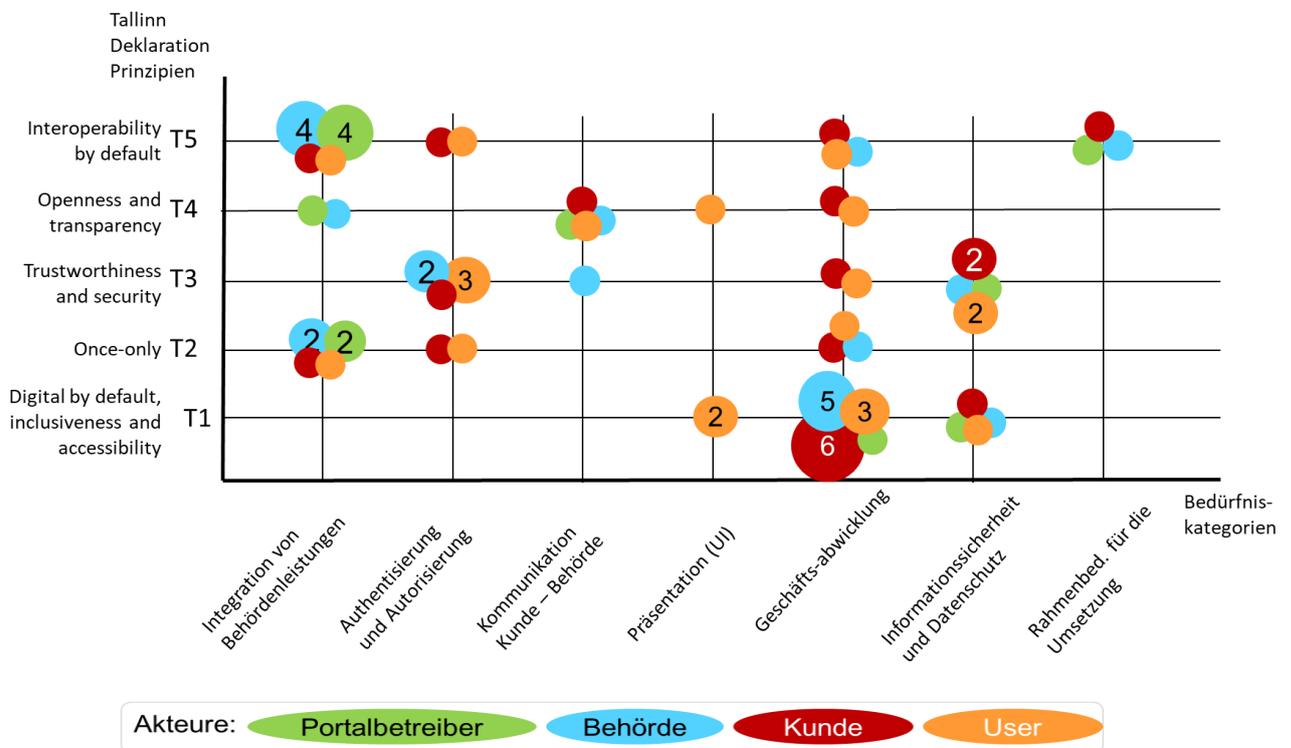


Abbildung 26: Kategorisierung der Bedürfnisse nach Tallinn, Themen und Akteuren (Grösse der Bubbles steht für die Anzahl der Nennungen)

2.2.3 Abgrenzungen

Die folgenden Bedürfnisse liegen ausserhalb des Scopes der vorliegenden Studie und wurden explizit abgegrenzt:

Tabelle 11: Abgrenzungen zum Scope der Sollarchitektur

Nr.	Titel	Abgrenzung
[A-1]	UX	Es werden nur architekturelevante UX-Themen betrachtet. Darüberhinausgehende Bedürfnisse im Bereich von UX sind explizit abgegrenzt.
[A-2]	Behörden-interne Prozesse	Der Fokus der Sollarchitektur liegt in der Abdeckung der Behördenleistungen für die Kunden bzw. User. Die Behörden-internen Prozesse und Fachsysteme sind ausserhalb des Scopes, ebenso die Kommunikation und die Schnittstellen zwischen verschiedenen Amtsstellen. (Siehe auch Abbildung 9)
[A-3]	Fokus	Die in der Massnahme M1 (siehe Kap. 1) geforderte grobe Integrations-Sollarchitektur für Behördenleistungsportale wird unabhängig von EasyGov erarbeitet. Erst die für den Schritt M2 geplante Gap-Analyse fokussiert auf EasyGov.
[A-4]	Finanzierung	Fragen bezüglich der Finanzierung (z.B. zur Realisierung eines Behördenportals) sind ausserhalb des Scopes dieser Studie.
[A-5]	AKV	Strukturelle Verantwortlichkeiten werden in der vorliegenden Studie grob definiert, siehe dazu Kapitel 2.5. Wie diese Verantwortlichkeiten in der Praxis umgesetzt und gelebt werden, ist jedoch ausserhalb des Scopes dieser Studie.
[A-6]	Schnittstellen	Nur externe Schnittstellen zwischen verschiedenen Verantwortlichkeiten sind hinsichtlich der Interoperabilität relevant. Interne Schnittstellen interessieren nicht und werden in dieser Studie nicht weiterverfolgt.

Hinweis: Die Abgrenzungen beziehen sich wohlgerneht auf die vorliegende Studie. Sie können in nachgelagerten Aktivitäten durchaus obsolet werden (siehe Kapitel 2.7).

2.2.4 Qualitätserwartungen an die Sollarchitektur

Bei der Bedürfniserhebung (siehe Kapitel 2.2.2) wurden neben den eigentlichen Bedürfnissen auch qualitative Erwartungen an die angestrebte Integrations-Sollarchitektur für Behördenleistungsportale geäussert. Diese sind nachfolgend aufgeführt. In Anlehnung an den am Schluss von 2.2.2 platzierten Hinweis sei auch an dieser Stelle vermerkt: Es handelt sich um Erwartungen, nicht um präzise Anforderungen. Diese Erwartungen vermitteln einen Eindruck, welche "weichen" Faktoren die Akzeptanz bei den Stakeholdern für die Sollarchitektur in erster Linie bestimmen.

Tabelle 12: Qualitätserwartungen an die Sollarchitektur

Nr.	Bedürfnis	Bedürfnis von...
[Q-1]	Offenes, einfach erweiterbares Konzept.	Portalbetreiber, Behörde
[Q-2]	Technische Einfachheit der Integration / Bring your own Service muss sehr einfach umsetzbar sein / Adäquate Integrationspattern (Kosten / Nutzen) / Flexibilität.	Behörde
[Q-3]	Unterstützung unterschiedlicher Umsetzungsreife von Gemeinden für Digitalisierungsgrundsätze (Bsp: Wenn Once-Only kommt, dann wird die Umsetzung einige Zeit in Anspruch nehmen).	Behörde
[Q-4]	Einbezug aller Stakeholder / Commitment aller Beteiligten für die Lösung.	Portalbetreiber, Behörde
[Q-5]	Keine politischen Kompromisse, rein sachliche Lösungen.	Portalbetreiber, Behörde
[Q-6]	Unterstützung durch entsprechende Institutionen (eCH).	Portalbetreiber, Behörde
[Q-7]	Wenn Standards definiert werden, muss sichergestellt werden, dass sie eingehalten und umgesetzt werden.	Portalbetreiber

2.3 Architekturprinzipien

2.3.1 Vorbetrachtung: Interoperability Principles des EIF

In Konsequenz der vom Projektinitialisierungsauftrag [1] eingeflossenen Rahmenbedingung ([F-2], siehe Kapitel 2.2.1) wurden die im Dokument "The New European Interoperability Framework" (EIF) [17] unter Kapitel 2 aufgeführten "interoperability principles" analysiert. Die folgende Tabelle 13 dokumentiert, wie diese Prinzipien in der Studie zur Anwendung kommen. Das EIF wird von der Tallinn-Deklaration (siehe 2.2.2.1) referenziert.

Tabelle 13: Verarbeitung der Interoperability Principles des EIF in der Studie

Nr.	Titel	Empfehlungen	Konsequenzen für die Entwicklung der Sollarchitektur
		relevant teilw. relevant nicht relevant	
[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.	Dieser Grundsatz ist der Anstoss für das Architekturprinzip [P-1]. Darüber hinaus verfolgt die Rahmenbedingung [F-2] einen analogen Gedanken.
[EIF-2]	Openess	Publish the data you own as open data unless certain restrictions apply.	Nicht relevant für die vorliegende Sollarchitektur.
		Ensure a level playing field for open source software and demonstrate active and fair consideration of using open source software, taking	Ausserhalb des Scopes der Studie (siehe Abgrenzungen [A-3] und [A-4]). Die Sollarchitektur schafft <i>konzeptuelle</i> Rahmenbedingungen für die

Nr.	Titel	Empfehlungen	Konsequenzen für die Entwicklung der Sollarchitektur
		relevant teilw. relevant nicht relevant	
		<p>into account the total cost of ownership of the solution.</p> <p>Give preference to open specifications, taking due account of the coverage of functional needs, maturity and market support and innovation.</p>	<p>Entwicklung von Behördenleistungsportalen.</p> <p>Deckt sich mit Rahmenbedingung [F-1].</p>
[EIF-3]	Transparency	Ensure internal visibility and provide external interfaces for European public services.	Die Entwicklung der Sollarchitektur ist eine Massnahme im Sinne der Empfehlung. Zusätzlich werden im Rahmen der Sollarchitektur mögliche bestehende Standards und Basisleistungen identifiziert und auf mögliche Verwendung geprüft.
[EIF-4]	Reusability	<p>Reuse and share solutions and cooperate in the development of joint solutions when implementing European public services.</p> <p>Reuse and share information and data when implementing European public services, unless certain privacy or confidentiality restrictions apply.</p>	<p>Der Aufbau des für diese Sollarchitektur zuständigen Fachgremiums mit Ausrichtung auf alle föderalen Ebenen ist eine Massnahme im Sinne der Empfehlung.</p> <p>Das Einbringen der Sollarchitektur in den öffentlichen eCH-Standard (siehe Rahmenbedingung [F-1]) ist eine Massnahme im Sinne der Empfehlung.</p>
[EIF-5]	Technological neutrality and data portability	<p>Do not impose any technological solutions on citizens, businesses and other administrations that are technology-specific or disproportionate to their real needs.</p> <p>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.</p>	<p>Dieser Grundsatz ist der Anstoss für das Architekturprinzip [P-2].</p> <p>Deckt sich mit Bedürfnis [B-2].</p>
[EIF-6]	User-centricity	<p>Use multiple channels to provide the European public service, to ensure that users can select the channel that best suits their needs.</p> <p>Provide a single point of contact in order to hide internal administrative complexity and facilitate users' access to European public services.</p> <p>Put in place mechanisms to involve users in analysis, design, assessment and further development of European public services.</p>	<p>Deckt sich mit Bedürfnis [B-1].</p> <p>Deckt sich mit Bedürfnis [B-16].</p> <p>Der im Rahmen der Studie erhobene Bedürfniskatalog (siehe 2.2.2) involviert die Perspektive des Kunden und des Users. Dies ist eine Momentaufnahme. Eine kontinuierliche Kundeneinbindung – wie vom EIF empfohlen – liegt jedoch ausserhalb des Scopes der Studie (siehe Abgrenzung [A-1]).</p>

Nr.	Titel	Empfehlungen	Konsequenzen für die Entwicklung der Sollarchitektur
		relevant teilw. relevant nicht relevant	
		As far as possible under the legislation in force, ask users of European public services once-only and relevant-only information.	Der erste Teil (once-only) deckt sich mit Bedürfnis [B-17]. Der zweite Teil liegt in der Verantwortung der jeweiligen Behörde.
[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.	Deckt sich mit Rahmenbedingung [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.	Deckt sich mit Bedürfnis [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.	Deckt sich mit Rahmenbedingung [F-6] und Bedürfnis [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.	Die Entwicklung der Sollarchitektur ist eine Massnahme im Sinne der Empfehlung.
[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.	Bezieht sich auf die Zugänglichkeit und Aufbewahrung von Akten. Dies fällt in die Verantwortung der Behörde. Behördeninterne Prozesse sind ausserhalb des Scopes der Studie, siehe Abgrenzung [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.	Die im Rahmen der Studie erarbeiteten Zielbilder und Lösungsvarianten werden gegen den Bedürfniskatalog evaluiert (Standardvorgehen HERMES). Der Evaluationsprozess ist damit nicht abgeschlossen, sondern ist ein ständiger Begleiter der über die Studie hinausgehenden Massnahmen.

2.3.2 Architekturprinzipien zur Sollarchitektur

Die hier formulierten Architekturprinzipien geben eine Richtung für die Erarbeitung der Sollarchitektur vor. Es handelt sich dabei wohlgerne nicht um Rahmenbedingungen (diese wurden bereits im Kapitel 2.2.1 zusammengetragen). Die Architekturprinzipien dienen vielmehr der Orientierung im Entwicklungsprozess, insbesondere bei der Entscheidung zwischen gleich schlechten Alternativen³⁶. Im Gegensatz zu den Rahmenbedingungen gilt deshalb für die Architekturprinzipien:

- "Weniger ist mehr"
- Die Formulierung darf auch Raum für Interpretationen lassen

Tabelle 14: Architekturprinzipien zur Sollarchitektur

Nr.	Titel	Beschreibung	Konsequenzen für die Entwicklung der Sollarchitektur
[P-1]	Nachnutzung vor Eigenkreation	Bewährte Lösungsansätze nach Möglichkeit der Erschaffung eigener Lösungen Vorrang geben. Dies bedeutet auch, Standards soweit als möglich zu nutzen.	Für ein bestimmtes Problem zunächst nach bestehenden Lösungen Ausschau halten und diese auf Nachnutzungspotential analysieren.
[P-2]	Konzept vor Technologie	Probleme primär auf konzeptueller Ebene behandeln. Die technologische Ebene steht nicht im Vordergrund, die Machbarkeit ist jedoch zu gewährleisten.	Beschränkung – soweit möglich und sinnvoll – auf konzeptuelle Vorgaben, Vermeidung von Abhängigkeiten zu konkreten Technologien oder Herstellern. Technische Empfehlungen sind jedoch gewünscht.
[P-3]	Integrationsarchitektur vor Systemarchitektur	Die angestrebte o.a. Integrations-Sollarchitektur für Behördenleistungsportale fokussiert nicht auf die Systemarchitekturen einzelner Portale, sondern vielmehr auf ein portalübergreifendes "Ökosystem", welches das Zusammenspiel regelt und die Interoperabilität verbessert, siehe Abbildung 1.	Orientierung auf Schnittstellen, so wenig wie möglich Vorgaben für einzelne Systemarchitekturen, diese sollen nach wie vor frei sein.
[P-4]	Dezentralisierung vor Zentralisierung	... um die agile Entwicklung der Portallandschaft nicht zu behindern. Aufgrund der Komplexität der Behördenleistungen über alle föderalen Ebenen ist eine zentrale Lösung auch de facto nicht möglich.	Ohne zentrale Vorgaben wird es nicht gehen, aber sie sollen nur so weit gehen wie für die Interoperabilität notwendig.

³⁶ Sprichwörtlich: "Die Wahl zwischen Pest und Cholera"

[P-5]	Bedürfnisse der User-/Kunden ³⁷ vor denen von Behörden und Portalbetreibern	Bei der Evaluation von Lösungsvarianten Bedürfnisse von User /Kunden höher gewichten als von Behörden und Portalbetreibern. Dieses Prinzip ist infolge der Anwendung der Tallinn-Deklaration ³⁸ , siehe Kapitel 2.2.2.1, klar bedingt.	Es kann sein, dass die Erfüllung von User-Erwartungen mit lokalen Gesetzen, Verordnungen, etc. kollidiert (z.B. Datenschutz oder IT-Verordnungen). Derlei Konflikte sind im Rahmen der Studie zeitnah soweit als möglich zu klären.
[P-6]	Fokussierung auf Behörden-unabhängige Aspekte	Abhängigkeiten der Sollarchitektur von Behördenleistungs-spezifischen Aspekten vermeiden, um übergreifende Regeln zu ermöglichen	Die Sollarchitektur abstrahiert allgemeine von leistungsspezifischen Aspekten und regelt nur erstere.
[P-7]	Lose Koppelung	Bezeichnet einen geringen Grad der Abhängigkeit mehrerer Komponenten oder Systemen untereinander.	Systeme, die unter verschiedenen Verantwortungen stehen, sollen nach Möglichkeiten lose gekoppelt werden.

³⁷ Siehe auch nationale E-Government-Studie <https://www.egovernment.ch/de/dokumentation/nationale-e-government-studie-2019/>

³⁸ Siehe Vision der Tallinn Declaration on eGovernment, Seite 3 der Deklaration, http://ec.europa.eu/news-room/document.cfm?doc_id=47559

<p>[P-8]</p>	<p>Nutzung relevanter Bundesinitiativen</p>	<p>Die erfolgreiche Umsetzung von Vorhaben des Bundes darf antizipiert werden. Unter Vorhaben des Bundes wird folgendes verstanden:</p> <ul style="list-style-type: none"> • Bundesgesetze und -entwürfe, die sich zum Zeitpunkt der Erarbeitung dieser Studie im Gesetzgebungsverfahren befinden und entsprechend noch nicht in Kraft getreten sind. Relevant sind unter anderem die Änderung des AHV Gesetzes zur breiteren Verwendung der AHV-Nummer durch Behörden³⁹ wie auch das EmbaG⁴⁰ und das UEG⁴¹. • Auf Bundesebene angestossene Projekte, die zum Zeitpunkt der Erarbeitung dieser Studie noch nicht umgesetzt sind. Zu erwähnen sind hier beispielsweise die Umsetzungsziele gemäss dem Umsetzungsplan 2021 – 2023 von E-Government Schweiz [19] und das Diskussionspapier zum «Zielbild E-ID» [36]. <p>Damit soll folgendes erreicht werden:</p> <ul style="list-style-type: none"> • Die Sollarchitektur soll möglichst lange aktuell bleiben und nicht durch in absehbarer Zukunft umgesetzten Vorhaben des Bundes veraltet und nutzlos werden • Umgesetzte Vorhaben des Bundes sollen durch die Verarbeitung dieser in der Sollarchitektur und einer verbreiteten Nutzung der Architektur zusätzlich gestärkt werden. 	<p>Die Sollarchitektur darf (muss aber nicht) das Inkrafttreten von geplanten und relevanten Bundesgesetzen und die erfolgreiche Umsetzung von relevanten Projekten auf Bundesebene antizipieren und entsprechend wo sinnvoll für die Zwecke der Architektur nutzen.</p>
--------------	---	---	--

2.4 Zielbild

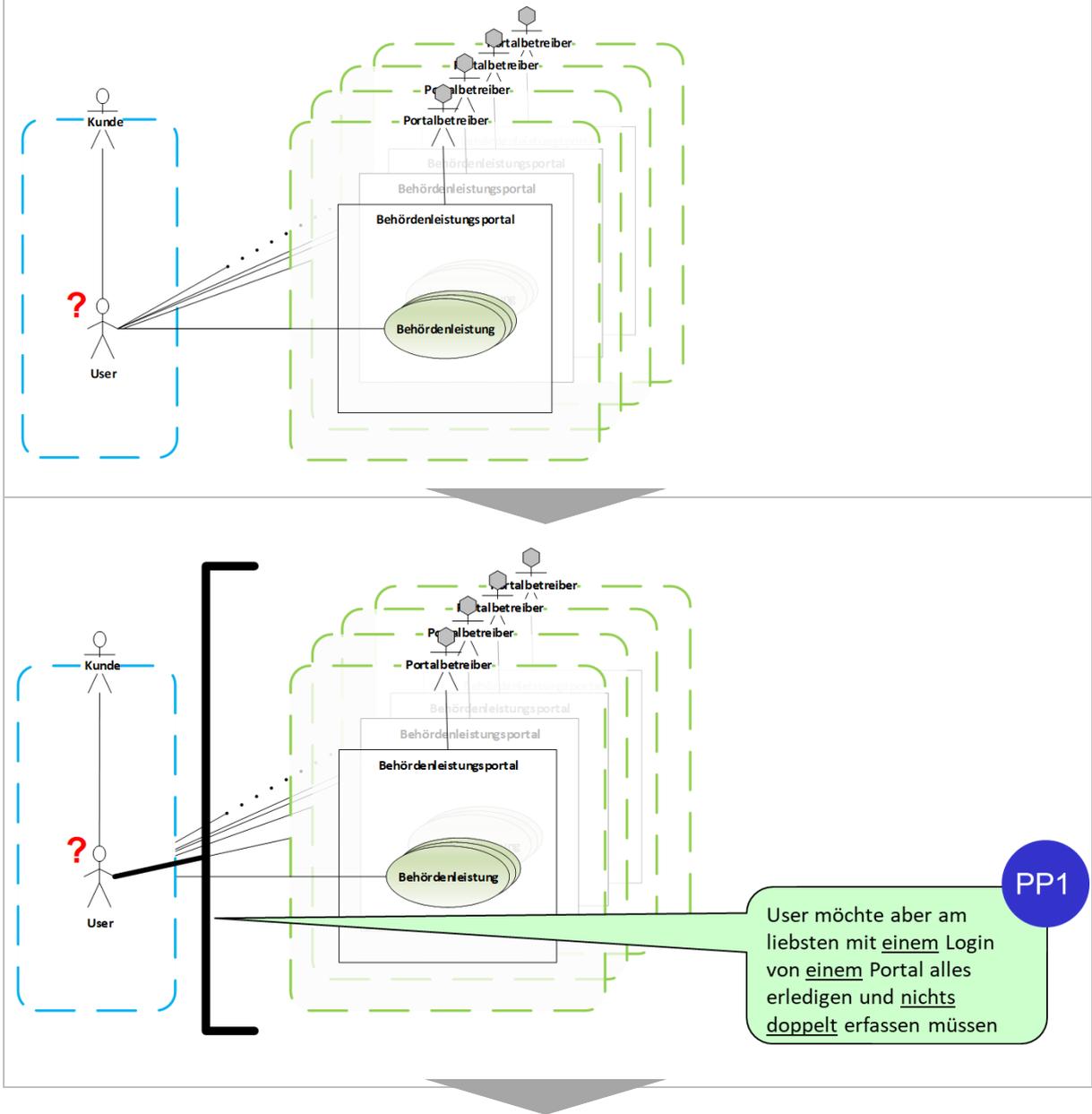
Das Zielbild folgt aus den im Kapitel 2.2.2 aufgezeigten Bedürfnissen. Deren Schwerpunkte lassen sich – wie von den nachfolgenden Bildfolgen veranschaulicht - zu Pain Points (PP) zusammenfassen. Unter Beachtung von Architekturprinzip [P-5] werden die Bedürfnisse von User/Kunde dabei vorangestellt.

³⁹ Siehe: <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaefft?AffairId=20190057>

⁴⁰ Siehe: <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-81580.html>

⁴¹ Siehe: <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-83285.html>

User sind mit einer Vielzahl von Portalen und Behördenleistungen konfrontiert:



PP1

User möchte aber am liebsten mit einem Login von einem Portal alles erledigen und nichts doppelt erfassen müssen

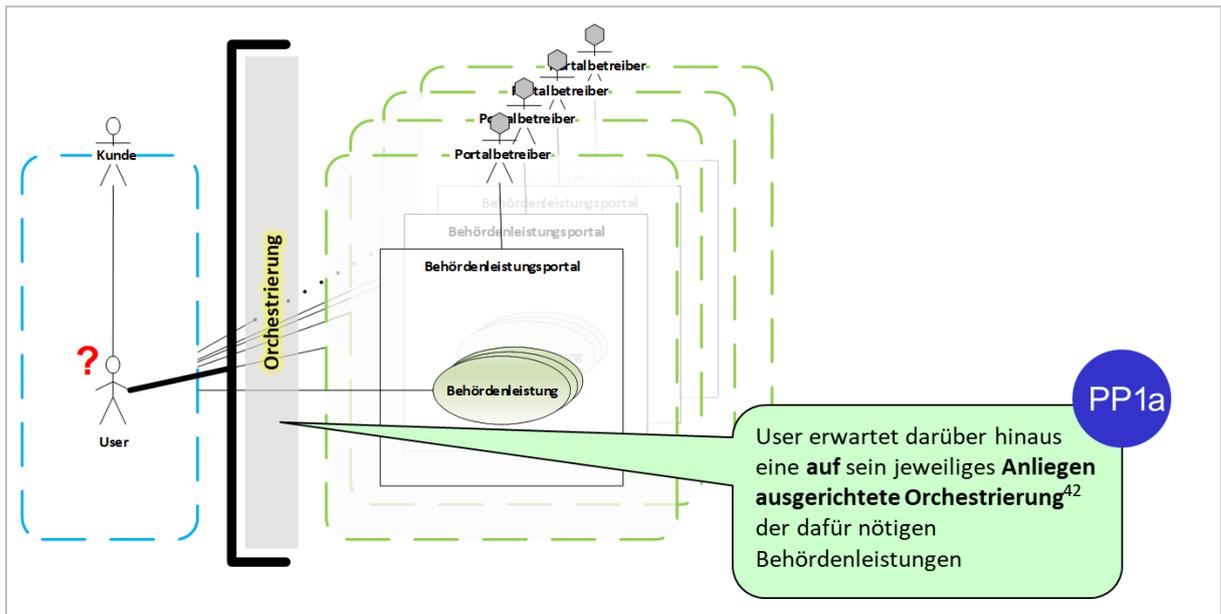
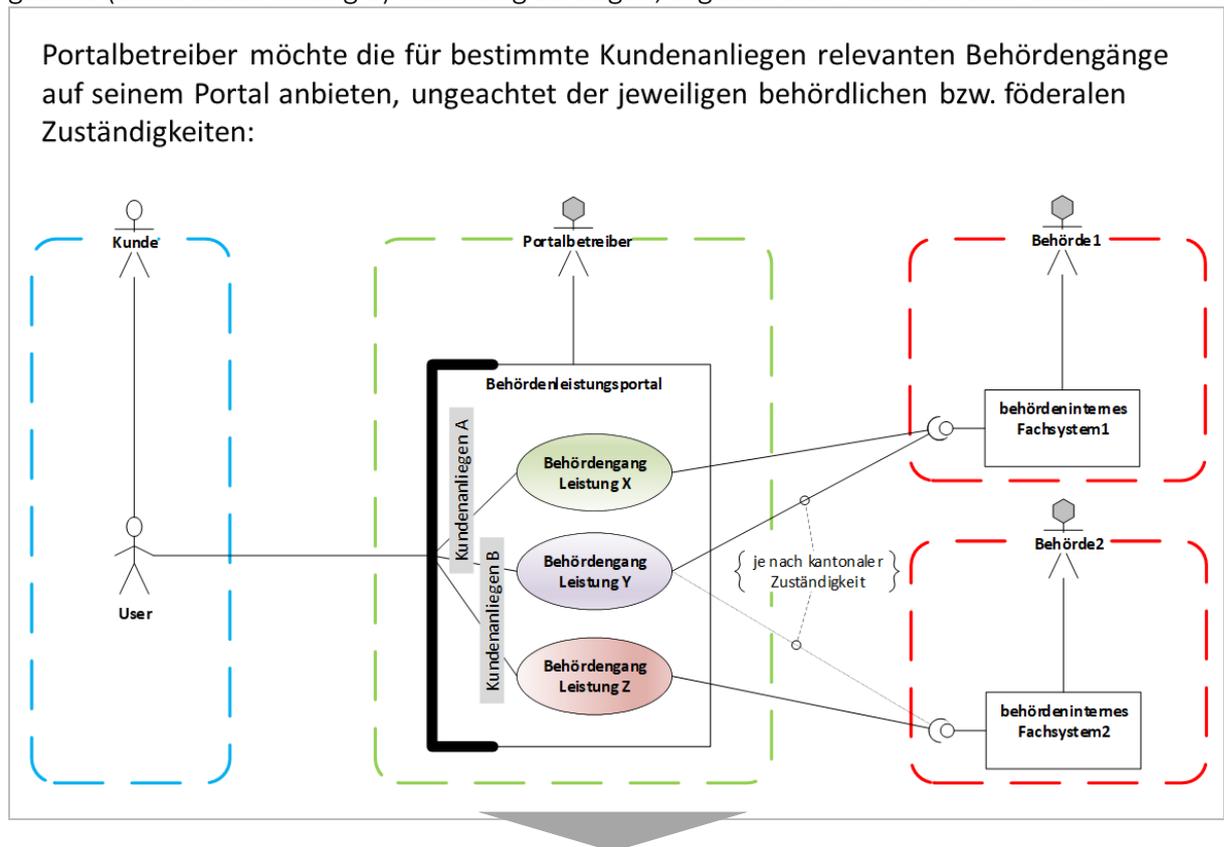
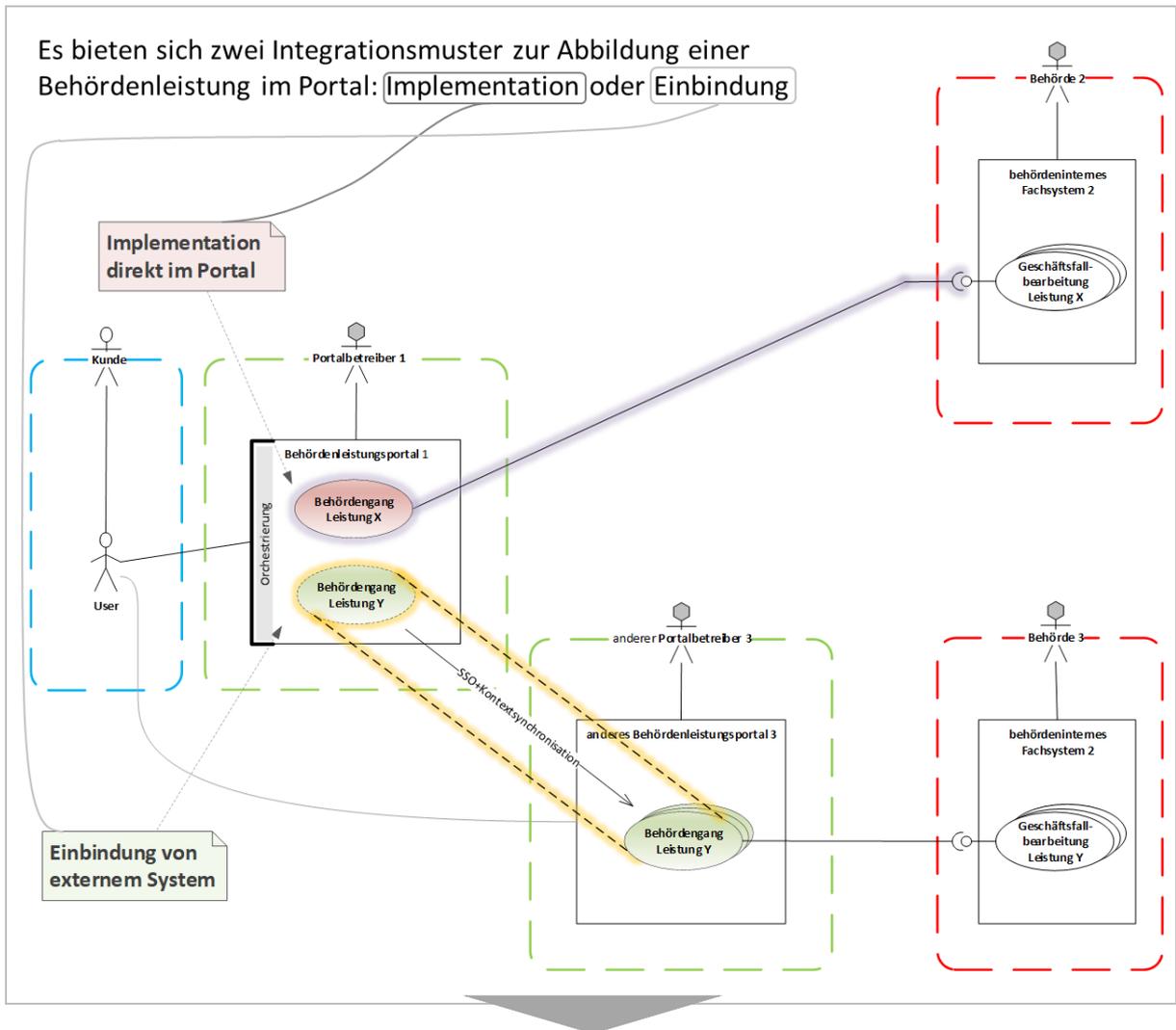


Abbildung 27: Bildfolge zu Pain Point 1

In dem Bemühen der Portalbetreiber, diesem Pain Point PP1 bzw. PP1a durch integrative Angebote (siehe dazu Anhang E) Rechnung zu tragen, ergeben sich weitere Pain Points:





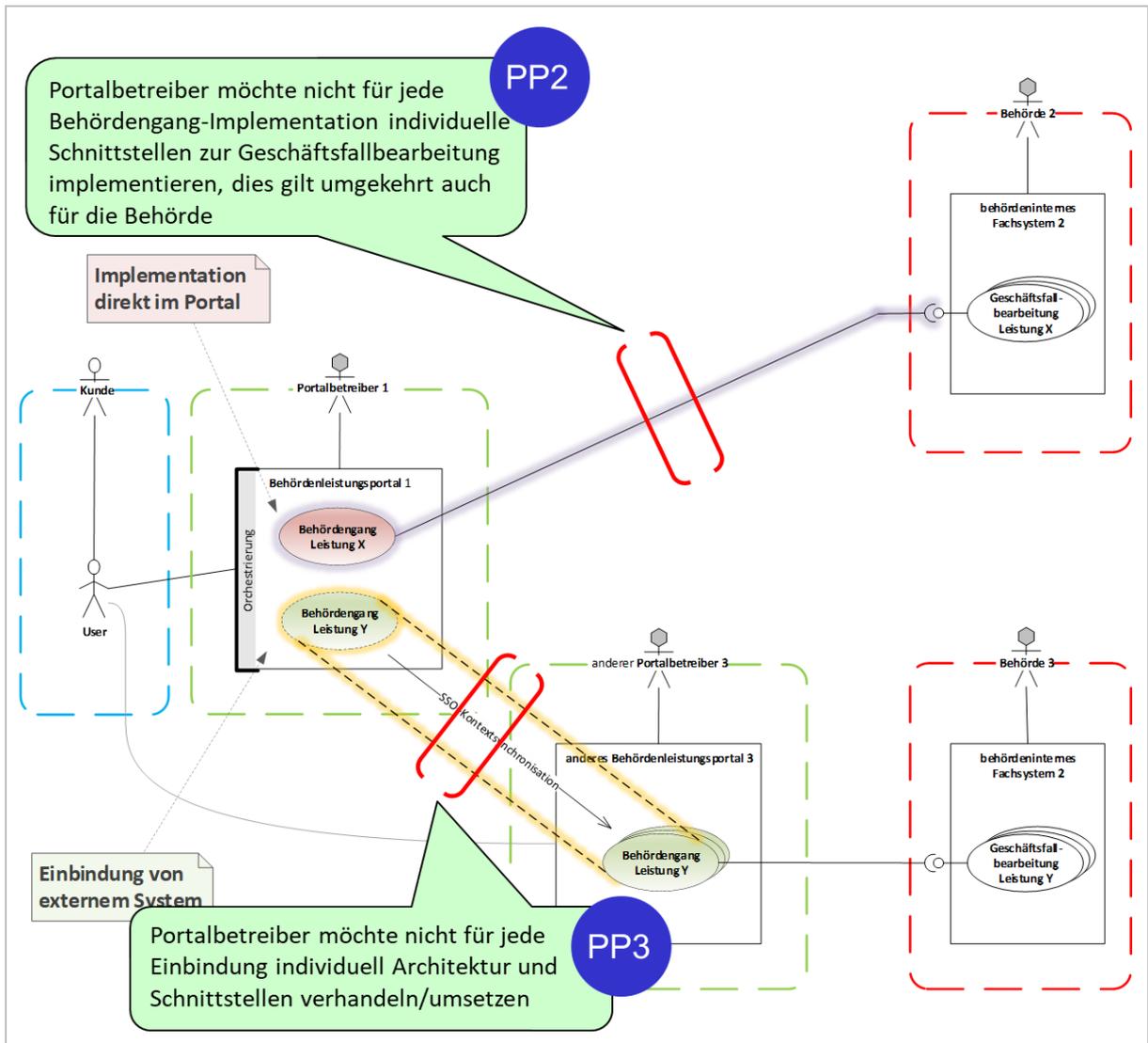


Abbildung 28: Bildfolge zu Pain Point 2 und 3

Um diesen Pain Points zu begegnen, braucht es vor allem ein ausreichendes Mass an Dateninteroperabilität auf Ebene der Schnittstellen, was wiederum ein übergreifendes konzeptuelles Fundament voraussetzt. Aus dieser Überlegung führen die Pain Points zum Zielbild der **Standardisierungsthemen**:

⁴² Orchestrierung bedeutet, dass das Portal den User über die relevanten Behördenleistungen führt, indem es z.B. die nötigen Behördengänge in einem Wizard (siehe Abbildung 11) aneinanderreicht.



- Definition eines Interoperabilitätsrahmens (siehe Anforderungen gemäss Kapitel 2.5.1.1)
 - Übergreifendes Informationsmodell
 - Festlegung von Identifikationssystemen und kontrolliertem Vokabular
 - Festlegung und Abgrenzung der interoperablen Kerndaten



- Standardisierung der Schnittstelle Behördengang↔Geschäftsfallbearbeitung (Integrationsmuster 1 gemäss Kapitel 2.1.6 und Anforderungen gemäss Kapitel 2.5.1.2)
 - Gerüst aus allgemeinen (nicht-leistungsspezifischen) Kommunikationsprozessen
 - Übermittlung Bearbeitungsstatus, Benachrichtigungen, Dokumente



- Standardisierung der Schnittstelle zur Einbindung extern implementierter Behördengänge (Integrationsmuster 2 gemäss Kapitel 2.1.6 und Anforderungen gemäss 2.5.1.3)
 - Laufzeit-Prozesse beim Aufruf eines eingebunden Behördengangs
 - Spezifikation der nötigen Vertrauensstellungen

Zusammengefasst lautet das Zielbild:

Die angestrebte Standardisierung soll die für das Zusammenwirken der Behördenleistungsportale nötige Daten- und Prozessinteroperabilität ermöglichen.

2.5 Entwicklung der Integrations-Sollarchitektur

In diesem Kapitel wird im Sinne des oben in Kapitel 2.4 beschriebenen Zielbildes (und den entsprechenden Pain Points PP1 bis PP3) die Integrations-Sollarchitektur grob entwickelt. "Grob" bedeutet dabei, es werden die zu regelnden Themenbereiche abgesteckt und darin fundamentale Festlegungen getroffen, aber es erfolgt keine detaillierte Spezifikation. Es werden Anforderungen formuliert, was die angestrebte Standardisierung konkret leisten soll und wie das logische Gerüst dazu aussieht.

Hinweise:

- Gemäss des im Kapitel 1 aufgeführten Ziels geht die Detailtiefe der folgenden Betrachtungen nur soweit, dass der Boden für den Entwurf eines eCH-Standards bereitet wird.
- Die Integrations-Sollarchitektur wurde zusammen mit dem Projekt-Fachausschuss aus Vertretern aller föderalen Ebenen im Rahmen von zehn halbtägigen Workshops entwickelt (siehe Anhang G.A und Anhang G.B). Dabei wurden die zu lösenden Herausforderungen identifiziert und schrittweise in Form von Variantenentscheiden abgearbeitet. Der argumentative Hergang und die Begründung der einzelnen Entscheide sind in Anhang G.D dokumentiert.
- Die Frage, inwieweit die entwickelte Integrations-Sollarchitektur die erhobenen Bedürfnisse abdeckt, wird in Kapitel 2.6 bilanziert.

2.5.1 Standardisierungsthemen

Die einzelnen Themen werden in Form von Anforderungen [REQ-n] spezifiziert, die im Interesse der Zukunftsfähigkeit im Einklang mit Architekturprinzip [P-2] soweit wie möglich Technologie-neutral gehalten sind. Deshalb stehen vor allem allgemeine fachliche Aspekte im Fokus, die für alle möglichen Behördenleistungen gleichermaßen von Belang sind.

- In-Scope:
 - interoperable Datenbereiche (z.B. Identifikatoren)
 - Verantwortlichkeiten (Definitionshoheit, Datenhoheit)
 - Schnittstellen-Prozesse
- Out-of-Scope:
 - Festlegung der Technologie (z.B. Protokoll, allfälliges Bus-System)
 - leistungsspezifische Datenbereiche

Die In-Scope/Out-of-Scope Betrachtung berücksichtigt das in Kapitel 2.4 beschriebene Zielbild insofern, dass der Fokus der Standardisierung auf den interoperablen - sprich nicht leistungsspezifischen - Schnittstellendaten und -prozessen liegt.

2.5.1.1 Interoperabilitätsrahmen

In diesem Bereich wird von folgenden beiden Punkten ausgegangen:

- Den zentralen Bedürfnissen [B-6] und [B-7], sowie
- der IAM-Anforderung, dass digitale Identität und Kunden-Identifikator zwei unterschiedliche Dinge sind. Ersteres dient der Authentifizierung⁴³ von Usern, letzteres der Kunden-Identifikation⁴⁴.

Basierend auf diesen beiden Punkten ergibt sich folgende Forderung:

[REQ-1] Ein User kann mit gleichem Login (sprich: digitale Identität) für mehrere Kunden (NP und/oder JP) Behördenleistungen erledigen. Gleichzeitig kann ein User für die Anmeldung verschiedene digitale Identitäten verwenden.

Abbildung 29 illustriert den aus [REQ-1] folgenden Zusammenhang zwischen User und Kunde. Eine unter einer digitalen Identität auftretende natürliche Person wird in einem Behördenleistungsportal als User repräsentiert. Analog bildet ein in einem Behördenleistungsportal geführter (Behörden-)Kunde eine juristische oder natürliche Person ab, die durch einen extern definierten Identifikator eindeutig bezeichnet wird.

⁴³ Siehe: <https://de.wikipedia.org/wiki/Authentifizierung>

⁴⁴ Siehe: <https://de.wikipedia.org/wiki/Identifikator>

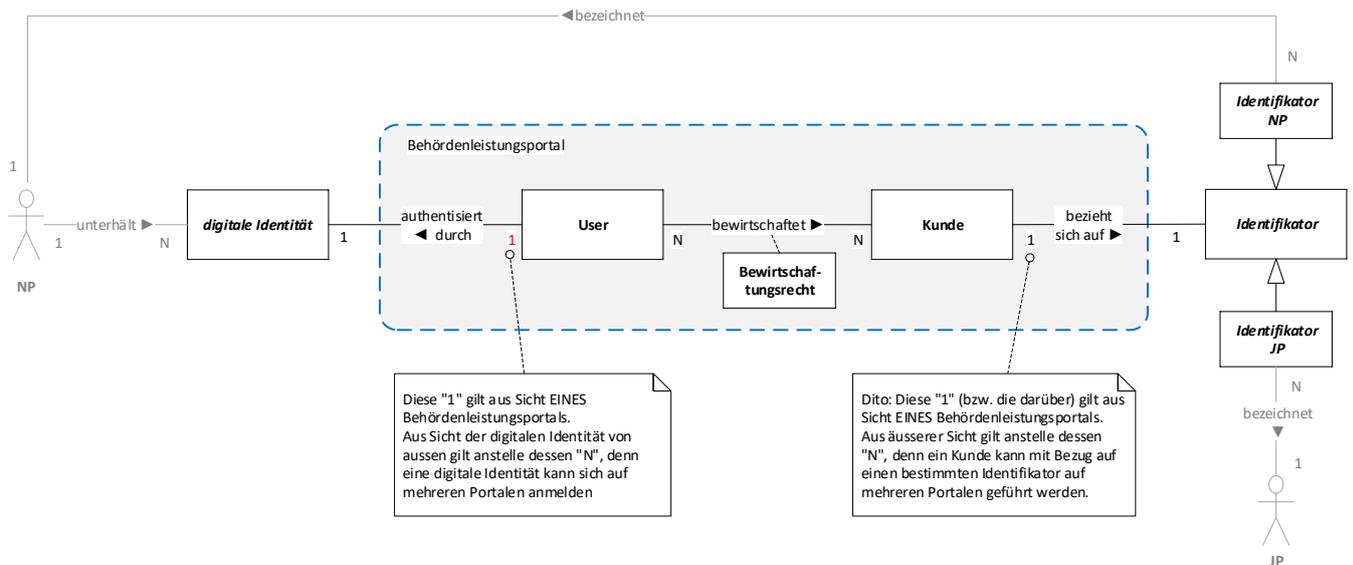


Abbildung 29: Ein Behördenleistungsportal nutzt zur User-Authentifizierung eine extern definierte digitale Identität⁴⁵, wogegen es Kunden mit Hilfe eines extern definierten Identifikators⁴⁶ identifiziert

Anhand der folgenden Grafik Abbildung 30 sei illustriert, welche Konstellationen auftreten können und wie diese gemäss [REQ-1] abzubilden sind.

- Die Person "Rainer Zufall" verwendet auf Behördenleistungsportal X zwei von jeweils verschiedenen Identitätsprovidern (IdP1 und IdP2) getragenen digitale Identitäten⁴⁷, und hat entsprechend zwei User-Accounts (xu1 und xu2). Beide sind für seinen gleichnamigen NP-Kunden berechtigt, welcher durch die betreffende Versichertennummer⁴⁶ identifiziert ist. Er kann also mit beiden digitalen Identitäten ein und dasselbe Kundenkonto bewirtschaften.
- Sowohl "Rainer Zufall" als auch "Inge Borg" verwenden eine ihrer digitalen Identitäten zur Anmeldung auf verschiedenen Portalen
- Mit Hilfe seiner digitalen Identität bei IdP1 bewirtschaftet User "Rainer Zufall" auf Behördenleistungsportal X nicht nur den ihn repräsentierenden NP-Kunden, sondern erledigt damit auch Behördengeschäfte für seine Firma "Keis-Problem AG", die durch ihre UID identifiziert ist.
- Der NP-Kunde "Rainer Zufall" kann auf beiden Portalen unabhängig voneinander bewirtschaftet werden. Die Person "Rainer Zufall" kann dies auf Behördenleistungsportal X und Y tun, die Person "Inge Borg" nur auf X. Der bewirtschaftete NP-Kunde ist in jedem Fall durch den gleichen eindeutigen Identifikator (im Beispiel sei die Versichertennummer angenommen) identifiziert.

⁴⁵ Der Fall, dass verschiedene digitale Identitäten durch einen zwischen Identitätsprovider und Portal zwischengeschalteten Vermittlerdienst gekapselt werden können, wird im Zielbild zunächst nicht thematisiert. Diesbezüglich sei auf [Herausforderung-1] im Anhang G.D verwiesen.

⁴⁶ Zur Frage, welche konkreten Identifikatoren von welchen Herausgebern zum Einsatz kommen sollen, sei auf [Herausforderung-2] im Anhang G.D verwiesen.

⁴⁷ Unter der Annahme, dass Portal X mehrere Identitätsprovider verwendet.

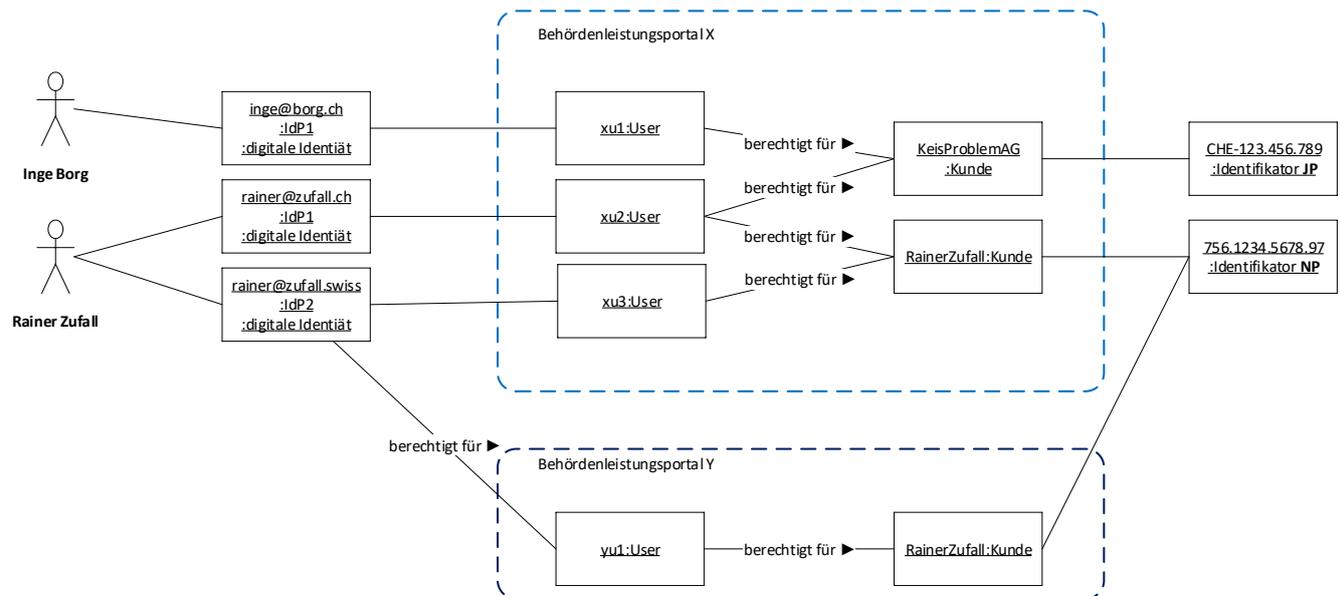


Abbildung 30: Illustration [REQ-1] anhand eines exemplarischen Kontexts (UML-Objektdiagramm)

2.5.1.1.1 Informationsmodell

Das in Kapitel 2.1.5 aufgestellte Informationsmodell trägt Forderung [REQ-1] bereits Rechnung, deshalb kann es als Fundament für den Interoperabilitätsrahmen zur Anwendung kommen.

[REQ-2] Die konzeptuelle Basis für den Interoperabilitätsrahmen bildet das in Kapitel 2.1.5 beschriebene Informationsmodell.

Anhand des Informationsmodells lässt sich differenziert aufzeigen, für welche Information die beiden thematisierten Schnittstellen jeweils Interoperabilität benötigen (siehe Abbildung 31). So spielt beispielsweise bei der Schnittstelle zur Einbindung extern implementierter Behörden-gänge (siehe Integrationsmuster 2 in Kapitel 2.1.6) die Behördenleistung keine Rolle, da die Auswahl im Consumer-Portal erfolgt und der betreffende Behördengang im externen Provider-Portal direkt adressiert wird (siehe Kapitel 2.5.1.2). Für die Schnittstelle "Behördengang ↔ Geschäftsfallbearbeitung" ist hingegen nicht von Belang, welcher User mit welchem Recht den Behördengang ausgeführt hat, da dies für die Geschäftsfallbearbeitung unerheblich ist. Letztere verlangt vielmehr die Kundendaten.

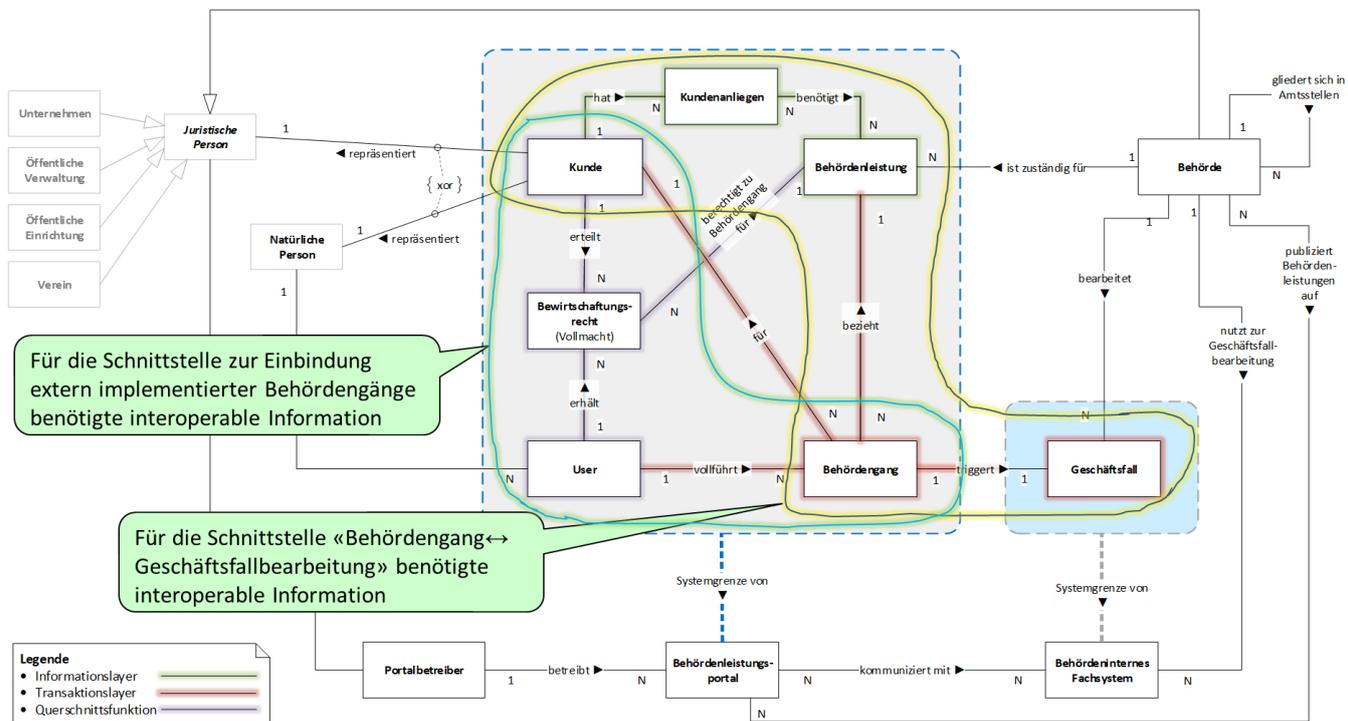


Abbildung 31: Verortung der Interoperabilitätsanforderungen im Informationsmodell

[REQ-3] Für die Entitäten des Informationsmodells ist ein interoperabler Kern definiert.

Dieser interoperable Kern beschränkt sich auf den Datenteil, der aufgrund der in den folgenden Kapiteln 2.5.1.2 und 2.5.1.3 spezifizierten Schnittstellenanforderungen von den beteiligten Systemen (Portale und behördeninterne Fachsysteme) auf beiden Seiten semantisch gleichermaßen verstanden werden müssen. Das betrifft vor allem Identifikatoren (z.B. Kunde.ID) und kontrolliertes Vokabular (z.B. Geschäftsfall.Bearbeitungsstatus). Demgegenüber fallen darüber hinaus gehende Inhalte in den nicht-interoperablen Teil. Für eine allfällige Schnittstellenübertragung wäre dieser nicht-standardisierte Teil individuell zwischen den beteiligten Partnern abzustimmen. Das betrifft z.B. leistungsspezifische Daten.

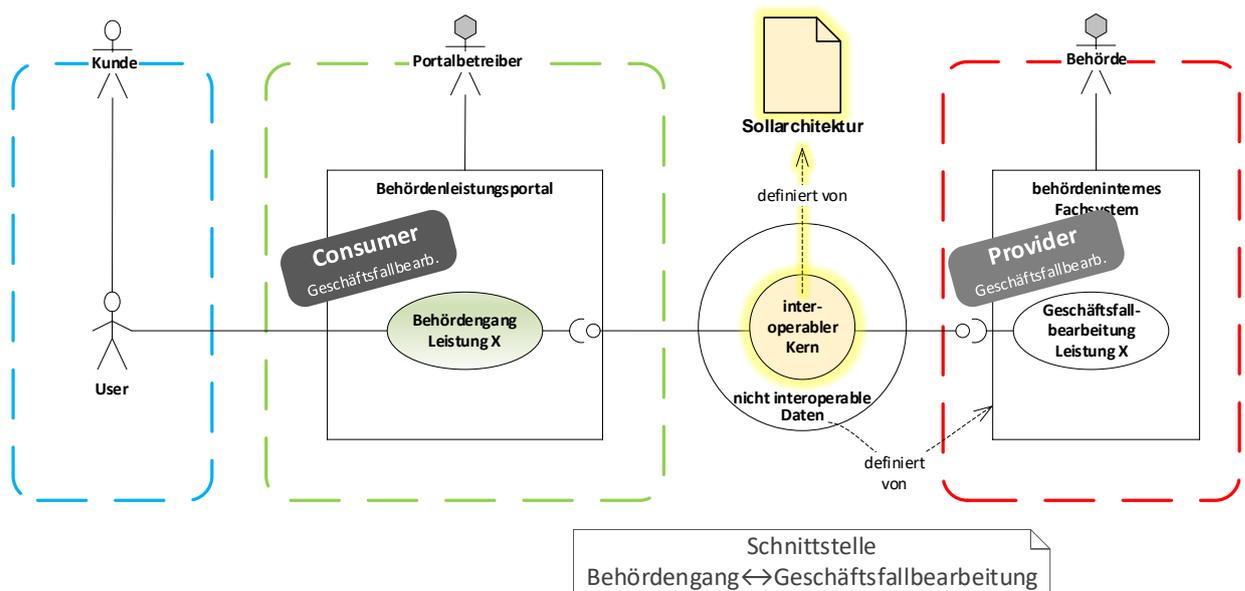


Abbildung 32: Illustration des interoperablen Kerns am Beispiel der Schnittstelle Behördengang ↔ Geschäftsbearbeitung (Integrationsmuster 1)

2.5.1.1.2 Identifikation Behördenleistung

[REQ-4] Zur Identifikation oder Referenzierung einer Behördenleistung ist das Inventar der Leistungen der öffentlichen Verwaltung der Schweiz eCH-0070 [27] verbindlich.

Leistungsreferenzen sind gemäss der Vorgabe von eCH-0070 zu kodieren. Das ist gemäss Abbildung 35 bei folgenden Entitäten der Fall:

- Behördengang: Referenz auf die bezogene Leistung
- Bewirtschaftungsrecht: Referenz auf die Leistung, für die der betreffende User für den jeweiligen Kunden einen Behördengang bewirtschaften darf.

Der Leistungskatalog stellt ein kontrolliertes Vokabular dar, dessen Definitionshoheit beim Verein eCH liegt.

Hinweis: Die im derzeit im eCH-0070 praktizierte Leistungsdifferenzierung erscheint stark heterogen. So wird zum Beispiel bei Handelsregistereintragungen neben der Art der Eintragung (Rechtsformen, Zeichnungsberechtigten, ...) zwischen Neueintrag, Mutation, Löschung differenziert, bei für die Leistungen im Bereich Arbeitsbewilligungen ist dies hingegen nicht der Fall. Zum Beispiel erscheint die Angabe ID=1128 ("Grenzgänerbewilligung für EU/EFTA-Angehörige (Ausweis G EG/EFTA) ") nicht präzise genug, da in der Praxis Neuausstellung, Verlängerung, Wiedererteilung, Umwandlung, Namensänderung, Stellenwechsel, etc. unterschieden wird.

2.5.1.1.3 Identifikation Kundenanliegen

[REQ-5] Derzeit gibt es noch kein kontrolliertes Vokabular für Kundenanliegen. Sollte sich das zukünftig ändern, ist das im Interoperabilitätsrahmen zu berücksichtigen.

2.5.1.1.4 Identifikation Kunde und Stammdatenmanagement

Für eine interoperable Kundenidentifikation braucht es einen unabhängig vom Portal existierendes Identifikationssystem. Hierzu bieten sich staatliche Register (wie z.B. das [UID-Register](#))

oder Basisdienste⁴⁸ an, die von Behördenleistungsportalen referenziert werden können. Darüber einhergehend gelten die mit dem jeweiligen Identifikator verbundenen Stammdaten, die die Register ebenfalls vorhalten, portalübergreifend.

Aufgrund verschiedener verwaltungsrechtlicher Behandlung zwischen juristischen Personen (JP) und natürlichen Personen (NP) werden JP- und NP-Kunden differenziert betrachtet.

2.5.1.1.4.1 JP-Kunde

[REQ-6] Zur Identifikation oder Referenzierung eines JP-Kunden ist die Unternehmensidentifikationsnummer UID zu verwenden.

Der UID-Aufbau ist durch den Standard eCH-0097 [28] definiert. Zur korrekten Zuteilung, Verwaltung und Verwendung der UID führt das BFS das UID-Register⁴⁹. Gemäss Auskunft vom BFS können ausländische, d.h. nicht in der Schweiz ansässige Unternehmen zukünftig auch eine UID bekommen⁵⁰.

[REQ-7] Behördenleistungsportale nutzen das UID-Register als führendes System für den interoperablen Kern der Stammdaten von JP-Kunden.

Das bedeutet nicht, dass Behördenleistungsportale keine Kundenstammdaten vorhalten sollen. Die Anforderung sagt lediglich aus, dass die Datenhoheit (im Sinne der amtlichen Wahrheit) beim Register liegt.

Behördenleistungsportale können für den elektronischen Datenabruf aus dem UID-Register einen Webservice⁵¹ nutzen. Die Datenstruktur basiert auf eCH-0108 [30], der sich wiederum auf eCH-0097 [28] und eCH-0098 [29] stützt.

[REQ-8] Der interoperable Kern der JP-Kundenstammdaten entspricht dem in eCH-0108 [30] unter Kapitel 3.2 definierten Datensatz "organisationType".

Dieser Datensatz umfasst die im UID-Register öffentlich einsehbaren Daten.

Der Abgleichprozess der Kerndaten zwischen dem führenden UID-Register und den Behördenleistungsportalen wird im Kapitel 2.5.1.1.4.3 betrachtet.

2.5.1.1.4.2 NP-Kunde

[REQ-9] Zur Identifikation oder Referenzierung eines NP-Kunden ist die Versichertennummer AHVN13 zu verwenden.

⁴⁸ Im Rahmen dieser Studie wird nachfolgend nur noch der Begriff «Register» benutzt. Dieser beinhaltet grundsätzlich auch Basisdienste.

⁴⁹ Rechtsgrundlage: Bundesgesetz über Unternehmens-Identifikationsnummer ([UIDG](#)), Verordnung über die Unternehmens-Identifikationsnummer ([UIDV](#))

⁵⁰ Dies ist in den neuesten Versionen der relevanten Standards eCH-0097 [28], eCH-0098 [29] und eCH-0108 [30] bereits berücksichtigt. Die Umsetzung im UID-Register selbst soll laut [33] im Zeithorizont bis Ende 2022 erfolgen.

⁵¹ siehe <https://www.bfs.admin.ch/bfs/de/home/register/unternehmensregister/unternehmens-identifikationsnummer/uid-register/uid-schnittstellen.assetdetail.11007268.html>

Die Rechtsgrundlage ist durch das angepasste AHV-Gesetz⁵² gegeben. Der argumentative Her- gang zum Fachausschussentscheid für die AHN13 als NP-Identifikator gegenüber anderen Al- ternativen kann im Anhang G.D ([Herausforderung-2]) nachvollzogen werden. Dort wird auch die Frage behandelt, welche Möglichkeiten sich für die Identifikation ausländischer NPs erge- ben.

Die Verwaltung des Identifikators AHV-Nummer im zentralen Versichertenregister der Sozial- versicherungen des Bundes und die Kommunikation der AHV-Nummer ausserhalb des AHV- Bereichs erfolgt durch die UPI-Datenbank des ZAS⁵³. Für die maschinelle Abfrage der UPI-Da- tenbank stehen die UPI-Services zur Verfügung. Deren externe Schnittstelle ist durch die Stan- dards eCH-0084 [5], eCH-0085 [6] und eCH-0086 [7] spezifiziert. Der Zugang ist auf systemati- sche Benutzer der AHV-Nummer beschränkt. Diese Voraussetzung wird jedoch von Behörden- leistungsportalen per se erfüllt.

Allerdings kann die UPI-Datenbank keine Adressdaten liefern. Das ist vielmehr Aufgabe des zu- künftigen zentralen Referenzdatensystems⁵⁴ Nationaler Adressdienst (NAD)⁵⁵ bzw. Gegenstand des Projekts UZ10⁵⁶ im Umsetzungsplan 2021-2023 von E-Government Schweiz [19]. Der NAD bezieht die Adressdaten von den Meldeämtern und Einwohnerregistern und basiert ebenfalls auf der Versichertennummer. Er kann somit aus Sicht der NP-Stammdaten als Ergänzung zur UPI-Datenbank angesehen werden (siehe [Herausforderung-2]).

[REQ-10] Behördenleistungsportale nutzen die UPI-Datenbank zusammen mit dem NAD⁵⁷ als führendes System für den interoperablen Kern der Stammdaten von NP-Kunden.

Der Abgleichprozess der Kerndaten zwischen den führenden Systemen und den Behördenlei- stungsportalen wird im Kapitel 2.5.1.1.4.3 betrachtet.

[REQ-11] Der interoperable Kern der NP-Kundenstammdaten entspricht den gemäss eCH-0084 [5] aus der UPI-Datenbank abfragbaren Identitätsmerkmalen (Name, Vorname, Ge- burtsdatum, Geburtsort, Geschlecht, Nationalität, etc.) sowie den aus dem NAD ab- fragbaren Adressdaten (Wohnadresse, Zustelladresse, Niederlassungs- oder Aufent- haltsgemeinde)^{55, 58, 59}.

Angaben über Zivilstand und Beziehungen zu anderen NP's (Ehepartner etc.), welche im Perso- nenstandsregister Infostar⁶⁰ verwaltet werden, können nicht in den interoperablen Kern der

⁵² Rechtsgrundlage: Angepasstes AHV-Gesetz <https://www.fedlex.admin.ch/eli/fga/2020/2693/de>

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

⁵⁴ Im Unterschied zum UID-Register ist der NAD nicht rechtlich massgebend, deshalb wird von einem Referenz- datensystem und nicht von einem Register gesprochen.

⁵⁵ Siehe <https://www.bfs.admin.ch/bfs/de/home/register/nationaler-adressdienst.html>

⁵⁶ Siehe <https://www.egovernment.ch/de/umsetzung/umsetzungsziele/nationaler-adressdienst/>

⁵⁷ Die rechtlichen Voraussetzungen für den Zugang zum NAD durch Behördenleistungsportale müssen noch im Rahmen des NAD-Projekts geklärt werden

⁵⁸ Stand Vorentwurf ADG: https://fedlex.data.admin.ch/eli/dl/proj/6019/57/cons_1

⁵⁹ Für die amtlichen Personenregister gelten die Nomenklaturen (bzw. kontrollierte Vokabular) des BFS, siehe <https://www.bfs.admin.ch/bfs/de/home/register/personenregister/registerharmonisierung/nomenklatu- ren.html>

⁶⁰ Siehe <https://www.bj.admin.ch/bj/de/home/gesellschaft/zivilstand.html> und <https://de.wikipe- dia.org/wiki/Infostar>

NP-Stammdaten eingehen, solange es keine für Behördenleistungsportale nutzbare Abfragemöglichkeit gibt.

Portale können für bestimmte Fälle auch weitere NP-Identifikatoren erheben. Dies ist z.B. zwingend notwendig, wenn bei einer ausländischen Person noch keine AHV-Nummer verfügbar ist (siehe Anhang G.D, [Herausforderung-2]. Aus diesem Grund können gemäss eCH-0044 [3] auch mehrere Identifikatoren vorgehalten und übermittelt werden.

2.5.1.1.4.3 Abgleich des interoperablen Kerns der Kundenstammdaten zwischen Portal und führendem Register

Gemäss der o.a. Anforderungen [REQ-7] und [REQ-10] soll der interoperable Kern der in einem Behördenleistungsportal vorgehaltenen JP- bzw. NP-Kundenstammdaten dem Datenstand der festgelegten Register folgen. Um dabei Konfliktpotenzial für allfällige Konsistenzprobleme zu vermeiden, soll folgende Regel gelten:

[REQ-12] Behördenleistungsportale sind für den Abgleich des Datenstands zum betreffenden Register selbst verantwortlich.

Das bedeutet, es braucht seitens der betreffenden Register im Falle einer Mutation weder einen automatischen Replikationsprozess noch einen Anstoss zu einer Datenpropagation. Vielmehr sollen Portale allfällige Differenzen zwischen ihrem Datenstand und dem im Register selbst erkennen. Dazu stellen die UPI-Services die in eCH-0086 [7] spezifizierte Vergleichsfunktion zur Verfügung. Dieser Check muss nicht proaktiv erfolgen. Es reicht meist aus, wenn der Aktualitätscheck der Stammdaten eines Kunden lediglich dann ausgeführt wird, wenn ein berechtigter User auf das betreffende Kundenkonto zugreift (z.B. um einen Behördengang auszuführen). Das Portal kann dem User allfällige Abweichungen visualisieren und ihm manuelle Abgleichfunktionen Register→Portal anbieten⁶¹.

⁶¹ Beispiel EasyGov: Beim Zugriff auf ein Kundenkonto wird im Falle einer Diskrepanz zwischen den Unternehmensstammdaten im Portal und dem UID-Register ein Hinweis angezeigt, dass diese nicht dem aktuellen Stand im UID-Register entsprechen und der User eine Aktualisierung starten kann.

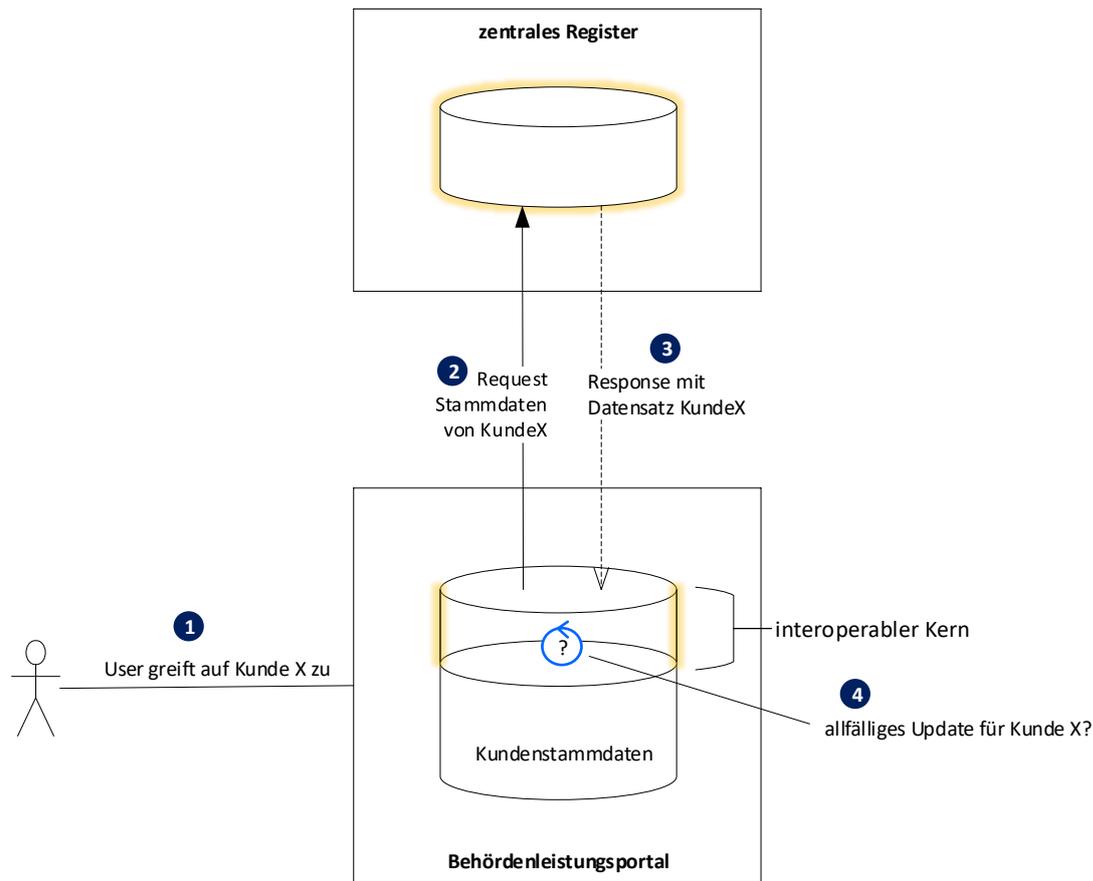


Abbildung 33: Abgleich des interoperablen Kerns eines Kunden-Stammsatzes in einem Behördenleistungsportal

Ungeachtet dessen gilt speziell im Falle NP: Der eCH-Standard eCH-0212 (Mutationsmeldungen UPI an Dritte) beschreibt den Broadcast der AHVN13-Mutationen im UPI-Register an Dritte, den die ZAS an alle Kunden sendet, die sich abonniert haben. Die behandelten Mutationen sind diejenigen, die den Status der Versichertennummer oder die demographischen Attribute einer Person in UPI ändern.

2.5.1.1.5 Prozessmetadaten von Behördengang und Geschäftsfall

Wie schon Abbildung 32 illustriert, ist für den Datenaustausch über die Schnittstelle Behördengang↔Geschäftsfallbearbeitung - welche im noch folgenden Kapitel 2.5.1.2 beschrieben wird – ein interoperabler Kern festzulegen. Dieser sei hier vorab auf die Metadaten der allgemeinen (nicht-leistungsspezifischen) Kommunikationsprozesse (siehe Abbildung 36 in Kapitel 2.5.1.2) umrissen.

[REQ-13] Die Metadaten der allgemeinen (nicht-leistungsspezifischen) Kommunikationsprozesse bilden den interoperablen Kern und geben den im eCH-0039 [2], eCH-0058 [4] und eCH-0147 [35] definierten Schemen Struktur und kontrolliertes Vokabular (z.B. Bearbeitungsstatus) vor.

[REQ-14] Zur Identifikation eines Behördengangs über die Systemgrenze des jeweiligen Behördenleistungsportals hinaus muss dieses einen permanenten global eindeutigen Schlüsselwert⁶² zur Verfügung stellen.

[REQ-15] Zur Identifikation eines Geschäftsfalls über die Systemgrenze des jeweiligen Behördenleistungsportals hinaus muss dieses einen permanenten global eindeutigen Schlüsselwert⁶² zur Verfügung stellen.

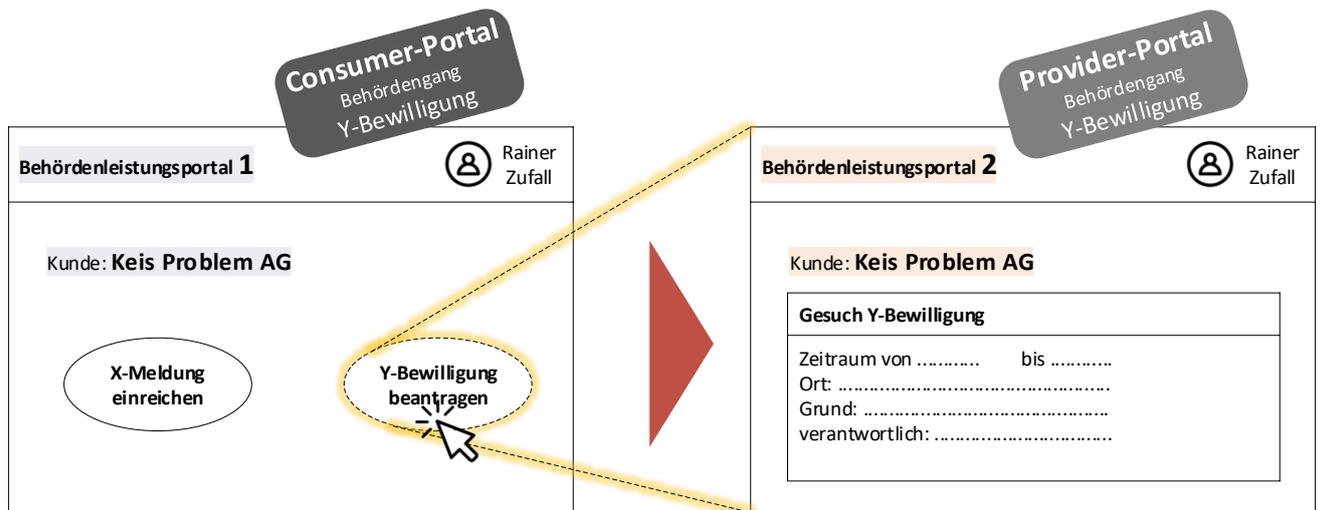
Für die Referenzierung der bezogenen Leistung kommen die Festlegungen in Kapitel 2.5.1.1.2 zur Anwendung.

Leistungsspezifische Inhalte setzen auf das beschriebene Fundament auf. Zu einzelnen Themenfeldern definieren bereits diverse eCH-Standards entsprechende Datenschemen und kontrollierte Vokabularien (eCH-0006 (Ausländerkategorien), eCH-0007 (Gemeinden), eCH-0008 (Staaten und Gebiete), eCH-0010 (Postadresse), eCH-0011 (Personendaten), eCH-0021 (Personenzusatzdaten), eCH-0046 (Kontakte), eCH-0119 (E-Tax Filing), eCH-0129 (Objektwesen), eCH-0229 (Steuerdeklarationsdaten juristische Personen)). Letztlich bleiben jedoch leistungsspezifische Vorgaben den jeweiligen Fachbereichen vorbehalten.

2.5.1.1.6 Userkonto

Wesentliches Element der Einbindung eines extern implementierten Behördengangs (Integrationsmuster 2, siehe Kapitel 2.1.6) ist die Weiterleitung, d.h. die Übertragung der Usersession vom Portal auf das externe System bzw. Provider-Portal zur Laufzeit. Damit der User beim Sprung in den eingebetteten – auf einem anderen Portal implementierten – Behördengang im Sinne von [REQ-1] und des letzten Teils von Bedürfnis [B-6] nahtlos weiterarbeiten kann, muss die Übertragung bzw. Weiterleitung mit Single Sign On (SSO) und Kontextsynchronisation einhergehen. Das bedeutet, es muss neben der Behördengang-Adressierung und User-Login auch der Kontext des Behördengangs, bestehend aus Kundenselektion und dazugehörigem Bewirtschaftungsrecht, vom Consumer-Portal auf dem Provider-Portal analog hergestellt werden (siehe Illustration in Abbildung 34).

⁶² Ein globaler Schlüsselwert kann z.B. nach dem Muster <Lokaler Schlüssel>@<URL des Herausgebersystems> oder durch eine GUID gebildet werden.



SSO + Kontextsynchronisation →

Abbildung 34: Herstellung des Session-Kontextes beim Aufruf des Behördengangs "Y-Bewilligung beantragen" im Provider-Portal konform zum Absprung-Kontext vom Consumer-Portal mittels SSO + Kontextsynchronisation

Für eine solche Kontextsynchronisation braucht es über die bereits behandelte interoperable Kundenidentifikation (siehe 2.5.1.1.4) hinaus eine Interoperabilität von User-Identifikation, -Einstellungen, LoA des Logins sowie des Bewirtschaftungsrechts. Dies wird in den folgenden Abschnitten 2.5.1.1.6.1 und 2.5.1.1.6.4 behandelt, die nötigen Vertrauensstellungen in Kapitel 2.5.1.3.

2.5.1.1.6.1 Identifikation

Beim Übergang muss zunächst das Provider-Portal für das korrespondierende Userkonto eine Session eröffnen (siehe Prozessbeschreibung in Kapitel 2.5.1.3). Die damit einhergehende User-Zuordnung vom Consumer- auf das Provider-Portal muss sich dabei nach einem eindeutigen Identitätsmerkmal, d.h. nach einem Identifikator richten, der vom Consumer-Portal herausgegeben wird. Ob der User-Identifikator dabei vom Consumer-Portal selbst oder ursprünglich von dessen Identitätsprovider stammt, ist dabei unerheblich. Wichtig ist, dass der herausgegebene Identifikator global eindeutig unterscheidbar ist.

[REQ-16] Zur Identifikation eines Users über die Systemgrenze des betreffenden Behördenleistungsportals hinaus muss dieses einen permanenten global eindeutigen Schlüsselwert⁶² zur Verfügung stellen.

2.5.1.1.6.2 Einstellungen (Benutzerprofil)

Ein nahtloser Übergang bei der in Abbildung 34 skizzierten Einbindung erfordert im Sinne von Bedürfnis [B-14], dass das Benutzerprofil im Provider-Portal analog fortgesetzt wird⁶³. Wenn

⁶³ Die nötigen Vertrauensstellungen werden in Kapitel 2.5.1.3 behandelt.

der User beispielsweise im Consumer-Portal italienisch als Sprache eingestellt hat, dann muss die adressierte Landingpage im Provider-Portal auch auf Italienisch erscheinen.

[REQ-17] Der interoperable Kern der Einstellungen im Benutzerprofil umfasst mindestens Name, Vorname und die Spracheinstellung des Users.

[REQ-18] Für die Spracheinstellung wird das kontrollierte Vokabular gemäss ISO 639-1⁶⁴ verwendet.

2.5.1.1.6.3 LoA des Logins

Ebenso darf im Provider-Portal kein anderer LoA gelten als im Consumer-Portal. Der LoA des Logins dokumentiert, inwieweit man der hinter dem authentifizierten User tatsächlich stehenden realen Person trauen kann, dass sie wirklich die Person ist, für die sie sich ausgibt. Je gründlicher der Registrierungsprozess (z.B. mit zusätzlicher Identitätsprüfung) und je stärker die Authentifizierung (z.B. 2FA statt 1FA) desto höher ist der Grad dieses Vertrauens.

[REQ-19] Für den LoA des Logins kommen als kontrolliertes Vokabular die in eCH-0170 [21] definierten Vertrauensstufen zur Anwendung.

Tabelle 15: LoA-Vertrauensstufenmodell gemäss eCH-0170 [21]

LoA-Stufe	Beschreibung
LoA 1	Kein oder minimales Vertrauen
LoA 2	Geringes Vertrauen
LoA 3	Beträchtliches Vertrauen
LoA 4	Hohes Vertrauen

Die einzelnen Vertrauensstufen des Modells von eCH-0170 [21] beziehen sich auf Kombinationen von skaliertem Authentifizierungsstärke und Qualität des Registrierungsprozesses.

2.5.1.1.6.4 Bewirtschaftungsrecht

Weiterhin erfordert ein nahtloser Übergang bei der in Abbildung 34 skizzierten Einbindung, dass das für den ausgewählten Behördengang des betreffenden Kunden nötige Bewirtschaftungsrecht im Provider-Portal ebenfalls gewährt wird^{63,65}. Wenn der User beispielsweise im Consumer-Portal den eingebundenen Behördengang Y-Bewilligung aufgrund seines Bewirtschaftungsrechts mit Berechtigungsstufe "Einreicher" aufgerufen hat, dann muss er auch im Provider-Portal genau dieses Recht haben, nicht mehr und nicht weniger.

Der Aufruf eines eingebundenen Behördengangs setzt das Bewirtschaftungsrecht des Users für den betreffenden Kunden für diesen Behördengang voraus

⁶⁴ siehe https://de.wikipedia.org/wiki/Liste_der_ISO-639-1-Codes

⁶⁵ Das nötige Bewirtschaftungsrecht muss per se im Consumer-Portal vorgelegen haben, sonst hätte der User den eingebundenen Behördengang nicht anwählen können.

[REQ-20] Der interoperable Kern des Bewirtschaftungsrechts umfasst mindestens die Berechtigungsstufe.

[REQ-21] Für die Berechtigungsstufe wird ein - noch per eCH-Standard zu definierendes - kontrolliertes Vokabular verwendet.

An dieser Stelle sei mit Tabelle 16 exemplarisch ein solches Berechtigungsstufenmodell illustriert, welches sich an den in gegenwärtigen Behördenleistungsportalen praktizierten Modellen orientiert, die sich interessanterweise weitgehend ähneln.

Tabelle 16: Exemplarisches Berechtigungsstufenmodell⁶⁶

Berechtigungsstufe	Beschreibung
Bearbeiten	Erlaubt die Bearbeitung von Behördengängen für einen bestimmten Kunden
Einreichen	Erlaubt das Einreichen von Gesuchen/Anträgen/Meldungen einer bestimmten Behördenleistung für einen bestimmten Kunden
Superuser	Erlaubt die Verwaltung der Bewirtschaftungsrechte für die Abwicklung von Geschäftsfällen für einen bestimmten Kunden. Die Gewährung dieser Berechtigungsstufe an einen User erfordert eine schriftliche Vollmacht des Kunden, dass die hinter dem User stehende Person das Kundenkonto ohne Einschränkungen bewirtschaften darf. Hiervon ausgenommen ist der Fall "NP-Kunde und User repräsentieren dieselbe Person".

Mit der Frage, inwieweit ein solches portalübergreifendes kontrolliertes Vokabular bzw. Berechtigungsstufenmodell eindeutig auf portalindividuelle Berechtigungsfunktionalitäten⁶⁷ abbildbar ist, beschäftigt sich [Herausforderung-4] im Anhang G.D.

Ähnlich dem im vorangegangenen Kapitel 2.5.1.1.6.3 behandelten LoA des Logins braucht das Provider-Portal vom Consumer-Portal die Angabe des Vertrauensgrads (LoA) der übermittelten Berechtigungsstufe, welche die Prozessqualität der Rechtevergabe dokumentiert.

[REQ-22] Für die Angabe des LoA eines Bewirtschaftungsrechts kommen als kontrolliertes Vokabular die in eCH-0171 [22] definierten Qualitätsstufen für Attributwertbestätigungen zur Anwendung.

Die einzelnen von eCH-0171 [22] spezifizierten Qualitätsstufen (siehe Tabelle 17) beziehen sich auf Attributwerte von digitalen Identitäten (wie z.B. Geburtsdatum) und quantifizieren die Prozessqualität der Erhebung. Das Stufenmodell ist auch für die Angabe des LoA der Berechtigungsstufe anwendbar, zumal jene im weiteren Sinne auch als Attributwert aufgefasst werden kann.

⁶⁶ Achtung: Das Beispiel ist nicht als Entwurf eines Standards für die Berechtigungsmodell zu verstehen.

⁶⁷ z.B. "kann Termine im Zusammenhang mit Behördengang X einsehen, aber nicht verschieben"

Tabelle 17: Qualitätsstufen gemäss eCH-0171 [22]

Qualitätsstufe	Beschreibung
1 – tief	Auf Stufe 1 besteht ein minimales Vertrauen in den behaupteten oder bestätigten Attributwert. Diese Vertrauensstufe wird genutzt, wenn ein minimales Risiko mit dem verwendeten Attributwert verbunden wird. Eine Vielzahl von Attribut-Autoritäten liefern Attributwertbestätigungen dieser Stufe und es werden keine bis sehr wenige Anforderungen an sie gestellt.
2 – mittel	Auf Stufe 2 besteht einiges Vertrauen in den behaupteten oder bestätigten Attributwert. Diese Vertrauensstufe wird genutzt, wenn ein mässiges Risiko mit dem verwendeten Attributwert verbunden wird. Es werden grundlegende Kontrollen und Prozesse eingehalten, jedoch findet keine generelle externe Überwachung der Attribut-Autorität statt. Attributwertbestätigungen dieser Stufe genügen, um einfache Geschäfte abzuwickeln.
3 – hoch	Auf Stufe 3 besteht ein hohes Vertrauen in den behaupteten oder bestätigten Attributwert. Diese Vertrauensstufe wird genutzt, wenn ein erhebliches Risiko mit dem verwendeten Attributwert verbunden wird. Es werden Kontrollen und Prozesse eingehalten, die von einer externen Stelle überwacht und überprüft werden. Attribute dieser Stufe genügen, um mittel-kritische Geschäfte abzuwickeln.
4 – sehr hoch	Auf Stufe 4 besteht ein sehr hohes Vertrauen in den behaupteten oder bestätigten Attributwert. Diese Vertrauensstufe wird genutzt, wenn ein hohes Risiko mit dem verwendeten Attributwert verbunden wird. Es werden Kontrollen und Prozesse eingehalten, die gesetzlich vorgeschrieben werden. Attributwertbestätigungen dieser Stufe genügen, um alle möglichen Geschäfte abzuwickeln.

Ergänzend sei darauf hingewiesen, dass der eCH-0107 [10] die grundsätzlichen Prozesse zur Verwaltung und Gewährung von Zugriffsrechten definiert.

Dem Bedürfnis [B-11] Rechnung tragend, sei weiterhin festgehalten:

[REQ-23] Für Berechtigungsstufen, die einer Vollmacht bedürfen (siehe Beispiel "Superuser" in Tabelle 16 oben), wird eine - noch zu definierende – juristisch belastbare Standardvollmacht verwendet, die portalübergreifend anerkannt wird.

2.5.1.1.7 Zusammenfassende Übersicht Interoperabilitätsrahmen

Die folgende Tabelle 18 fasst die einzelnen Elemente des Interoperabilitätsrahmens zusammen:

Tabelle 18: Zusammenstellung des Interoperabilitätsrahmens

Entität	Führendes System	Identifikation	Interoperabler Kern
Behörden-gang	Portal, auf dem der Behördengang ausgeführt wird ⁶⁸	Globaler Schlüsselwert ⁶⁹	Prozessmetadaten gemäss eCH-0039 [2] und eCH-0058 [4] Messagetypen für die Kommunikation zum komplementären Geschäftsfall (siehe [REQ-33]) gemäss einem noch zu schaffenden Standard
Behörden-leistung	eCH-0070	kontrolliertes Vokabular	
Bewirt-schaf-tungs-recht	(physischer) Kunde, vertreten durch bevollmächtigten Superuser ⁷⁰		Berechtigungsstufe (gemäss einem noch zu schaffenden Standard) sowie deren LoA (kontrolliertes Vokabular gemäss eCH-0171 [22])
Geschäfts-fall	behördeninternes Fachsystem, auf dem der Geschäftsfall bearbeitet wird	Globaler Schlüsselwert ⁶⁹	Prozessmetadaten gemäss eCH-0039 [2] und eCH-0058 [4] Messagetypen für die Kommunikation zum komplementären Geschäftsfall (siehe [REQ-33]) gemäss einem noch zu schaffenden Standard
JP-Kunde(-konto)	UID-Register	UID	Dem öffentlich zugänglichen Inhalt des UID-Registers entsprechend (Grundlage eCH-0097 [28], eCH-0098 [29], eCH-0108 [30])
Kunden-anliegen	zukünftiger eCH-Standard	kontrolliertes Vokabular	
NP-Kunde(-konto)	UPI-Register/NAD	AHVN13	Dem Inhalt dem für Behördenleistungsportale zugänglichen Inhalt des UPI-Registers (gemäss eCH-0084 [5], eCH-0085 [6], eCH0086 [7]) und des NAD (gemäss ADG) entsprechend

⁶⁸ Im Falle von Integrationsmuster 1 (Implementation, siehe Abbildung 21) ist es das Consumer-Portal, hingegen bei Integrationsmuster 2 (Einbindung, siehe Abbildung 24) ist es das Provider-Portal.

⁶⁹ Ein globaler Schlüsselwert kann z.B. nach dem Muster <Lokaler Schlüssel>@<URL des Herausgebersystems> oder durch eine GUID gebildet werden

⁷⁰ Mitunter auch als Kundenadministrator bezeichnet

User(-konto)	IdP/Vermittler des Portals, auf dem sich der User eingeloggt hat ⁷¹	Globaler Schlüsselwert ⁶⁹	Spracheinstellung (kontrolliertes Vokabular gemäss ISO-639) und LoA des Logins (kontrolliertes Vokabular gemäss eCH-0170 [21])
--------------	--	--------------------------------------	--

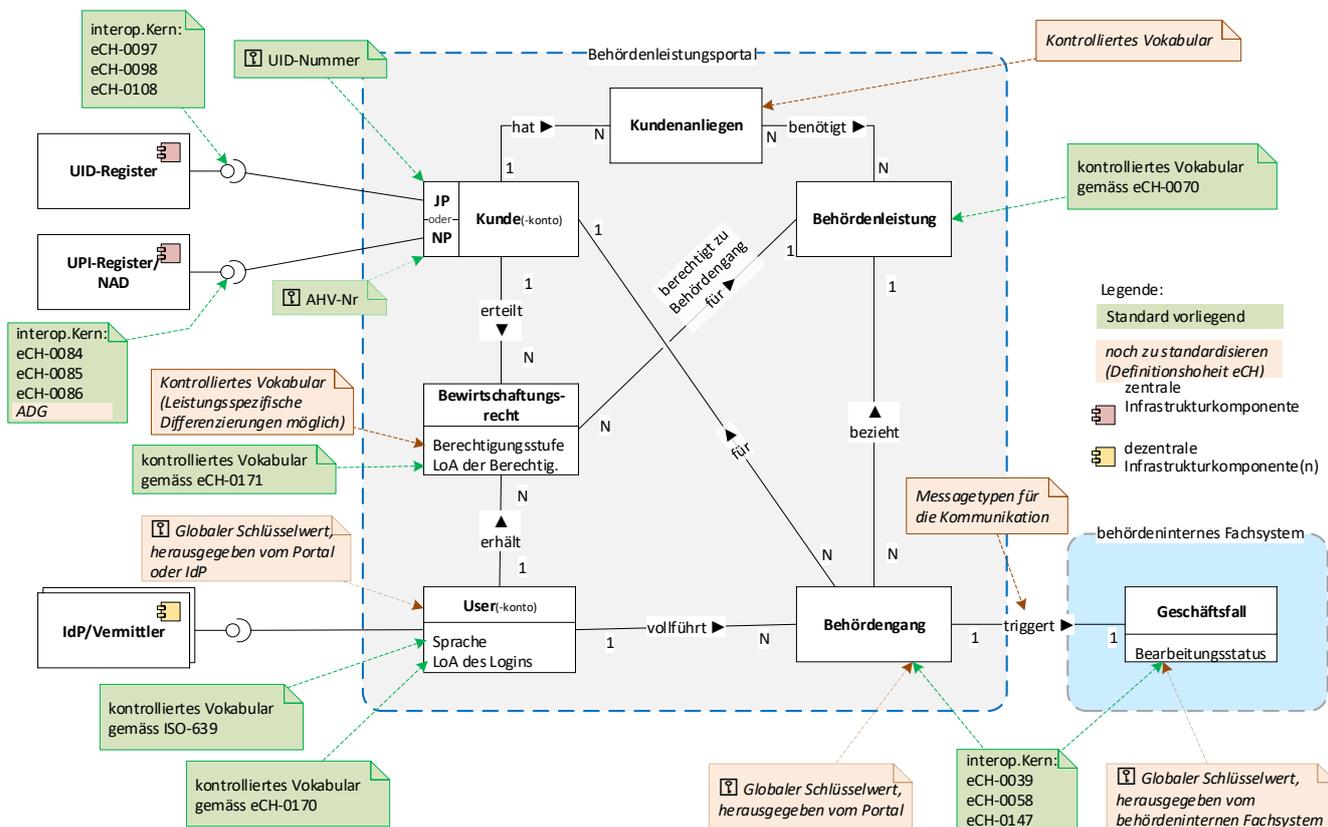


Abbildung 35: Verortung des Interoperabilitätsrahmens im Informationsmodell

2.5.1.2 Schnittstelle Behördengang ↔ Geschäftsfallbearbeitung

Grundsätzlich kann die Schnittstelle zwischen Behördengang und Geschäftsfallbearbeitung (siehe Integrationsmuster 1 in Kapitel 2.1.6) unter folgenden Prämissen portalübergreifend formuliert werden:

- Abstraktion vom leistungsspezifischen Inhalt der jeweiligen Behördenleistung
- Konzentration auf die allgemeinen Kommunikationsprozesse, die im Kapitel 2.1.1 herausgearbeitet wurden

⁷¹ Das ist sowohl bei Integrationsmuster 1 (Implementation, siehe Abbildung 21) als auch bei Integrationsmuster 2 (Einbindung, siehe Abbildung 24) das Consumer-Portal.

Motivation ist, die wechselseitigen Abhängigkeiten der Schnittstellen zwischen Behördenleistungsportal und behördeninternem Fachsystem aufzubrechen und weitgehend zu entkoppeln. Dies führt – dem Architekturprinzip [P-7] der losen Kopplung folgend – zu folgender Festlegung:

[REQ-24] Die Integrations-Sollarchitektur definiert die allgemeinen (nicht-leistungsspezifischen) Kommunikationsprozesse für den Datenaustausch zwischen Behördenleistungsportal und behördeninternem Fachsystem, auf deren Basis die jeweiligen leistungsspezifischen Inhalte übermittelt werden. Dies umfasst:

- Übermittlung Anfrage/Antrag/Gesuch/Beilagen von Kunde zu Behörde
- Statusmeldungen von Behörde zu Kunde
- Benachrichtigungen (Rückfrage/Information/Reminder) von Behörde zu Kunde und sowie umgekehrt allfällige Antwort von Kunde zu Behörde
- Übermittlung Verfahrensergebnis (Bescheid/Dokumente) von Behörde an Kunde

Allgemeine (nicht-leistungsspezifische) Kommunikationsprozesse stehen im Fokus der Standardisierung der Schnittstelle Behördengang ↔ Geschäftsfallbearbeitung

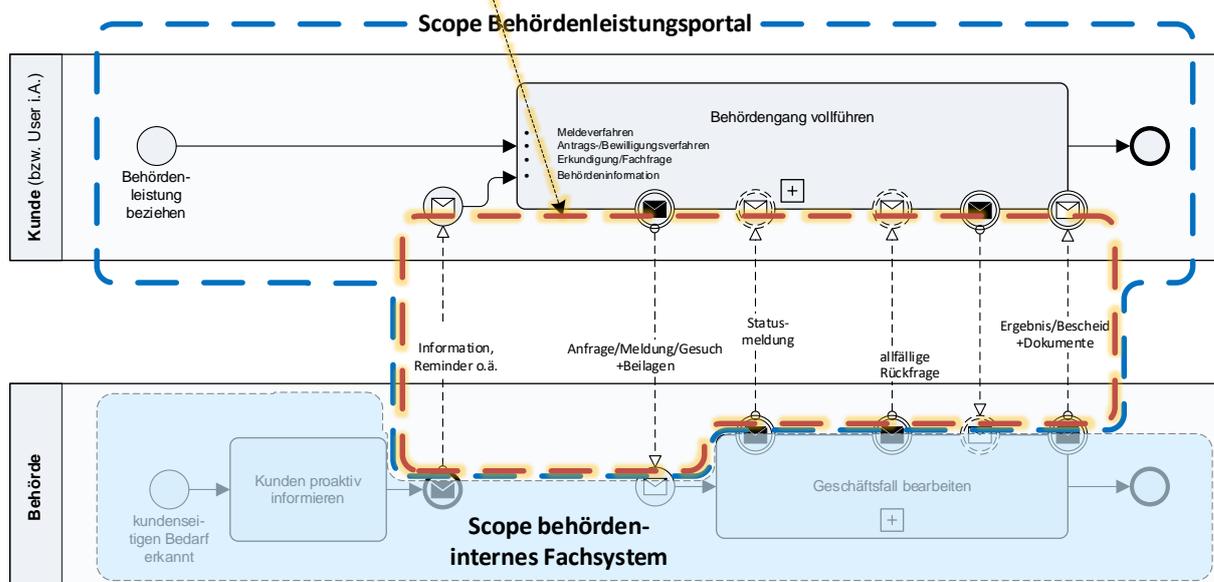


Abbildung 36: Die Integrations-Sollarchitektur spezifiziert die allgemeinen (nicht-leistungsspezifischen) Kommunikationsprozesse zwischen Behördenleistungsportal und behördeninternem Fachsystem

[REQ-25] Bei den Kommunikationsprozessen werden grundsätzlich die in Kapitel 2.5.1.1.5 spezifizierten Prozessmetadaten als Headerinformation mitgeliefert.

[REQ-26] Zusätzlich ist das Kundenanliegen zu übermitteln, sofern dieses bekannt ist⁷².

⁷² Derzeit ist diese Information mangels kontrollierten Vokabulars (siehe 2.5.1.1.3) allenfalls als Freitext im Kommentarfeld des Headers (siehe eCH-0058 [4]) übermittelbar.

Weiterhin gilt:

- [REQ-27]** Die Kommunikation muss zielgerichtet erfolgen, d.h. eine von einem bestimmten Kunden in einem Portal ausgehende Message muss vom internen Fachsystem der adressierten zuständigen Behörde nicht nur empfangen, sondern auch diesem Kunden zugeordnet werden.
- [REQ-28]** Analog gilt dies in der umgekehrten Richtung. Eine vom behördeninternen Fachsystem Behörde an jenen Kunden gerichtete Message muss im Portal, in dem der ursprüngliche Behördengang vollführt wurde, empfangen werden und dort im betreffenden Kundenkonto diesem Behördengang zugeordnet werden.

Hinweis: Die letzten beiden Anforderungen werden bereits von den in [REQ-13] festgelegten eCH-Standards unterstützt.

- [REQ-29]** Im Sinne des Prinzips der losen Kopplung sollten Dokumente komplett in Dateiform und nicht als Link übermittelt werden⁷³. Letzteres würde zu einer Abhängigkeit zum Link-Host führen.
- [REQ-30]** Im Falle von proaktiver behördlicher Benachrichtigung Behörde→Kunde (z.B. Remin-der an eine Meldungspflicht, nachträgliche Initiierung des digitalen Behördengangs nach klassisch physischem Kontakt im Sinne von [B-19]) muss es möglich sein, dass die Behörde beim Kunden einen Behördengang anstößt.
- [REQ-31]** Aufgrund der in Kapitel 2.1.1 erwähnten besonderen Verfahrenswege Subprozess und Verfahrensweitergabe (siehe Abbildung 5 bzw. Abbildung 6) muss die Schnittstellenkommunikation auch verschachtelte Prozesse abbilden können.
- [REQ-32]** In Konsequenz der beiden Anforderungen [REQ-28] und [REQ-31] findet das folgende für die Entitys Behördengang und Geschäftsfall verfeinerte Informationsmodell als Grundlage für die Schnittstellenprozesse Anwendung:

⁷³ Ungeachtet dessen kann eine Behörde– z.B. aus rechtlichen Gründen - Dokumente über anerkannte Zustellplattformen (wie IncaMail oder PrivaSphere) oder auf dem Postweg übermitteln. Dies liegt letztlich in Verantwortung der Behörde.

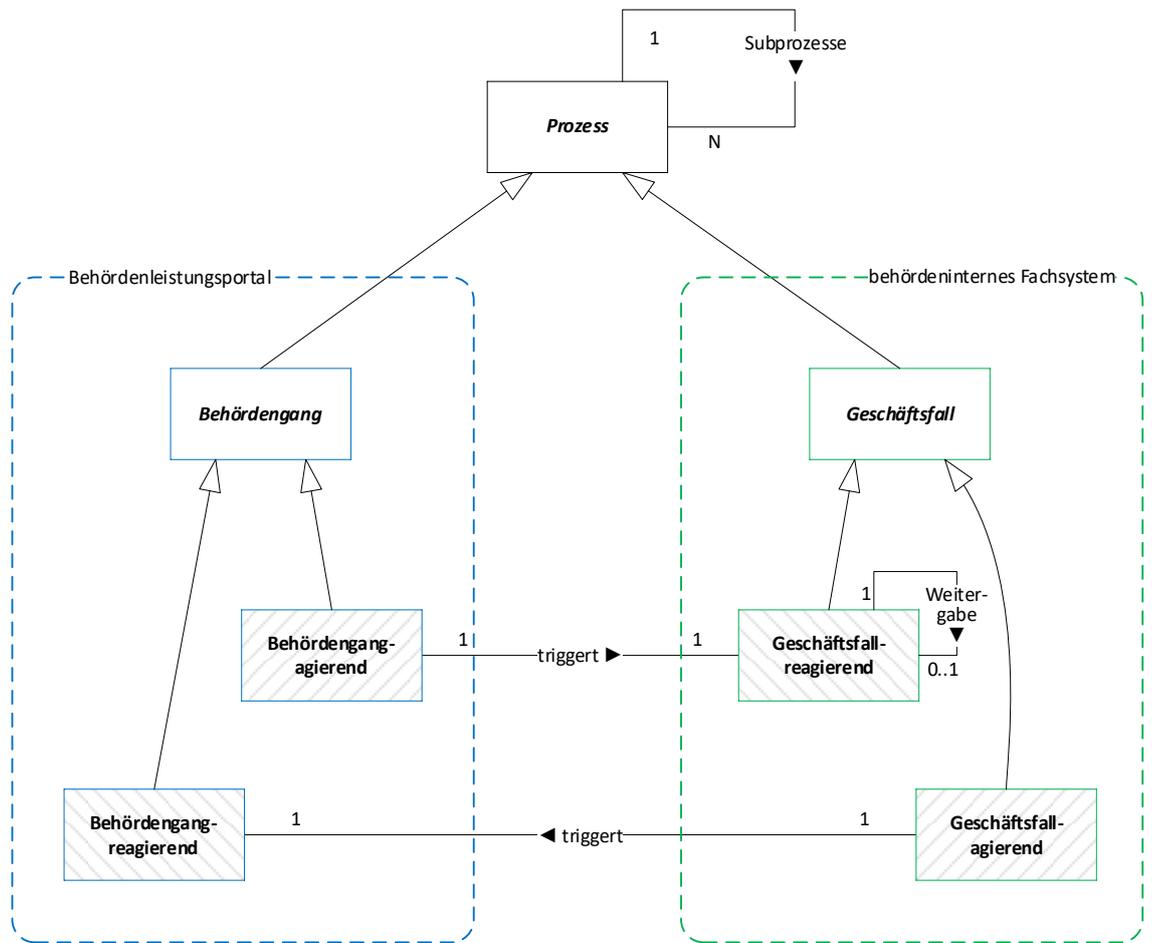


Abbildung 37: Informationsmodell der Schnittstellenprozesse Behördengang ↔ Geschäftsfallbearbeitung

- Sowohl Behördengang als auch Geschäftsfall können Subprozesse instanziiieren.
- Je nachdem, von welcher Seite der Anstoss initial erfolgt, wird - bezogen auf das Komplementärpaar Behördengang und Geschäftsfall - zwischen agierendem und reagierendem Prozess unterschieden.
- Der Spezialfall Verfahrensweitergabe (siehe Abbildung 6 in Kapitel 2.1.1) wird beim reagierenden Geschäftsfall durch die zusätzliche Referenzbeziehung "Weitergabe" unterstützt.

[REQ-33] Die Schnittstelle unterstützt für das Komplementärpaar Behördengang und Geschäftsfall ungeachtet der Seite des Anstosses zwei Messagetypen (siehe folgende Abbildung 38 bzw. korrespondierend dazu Abbildung 39):

- Initialmeldung
- Rückmeldung

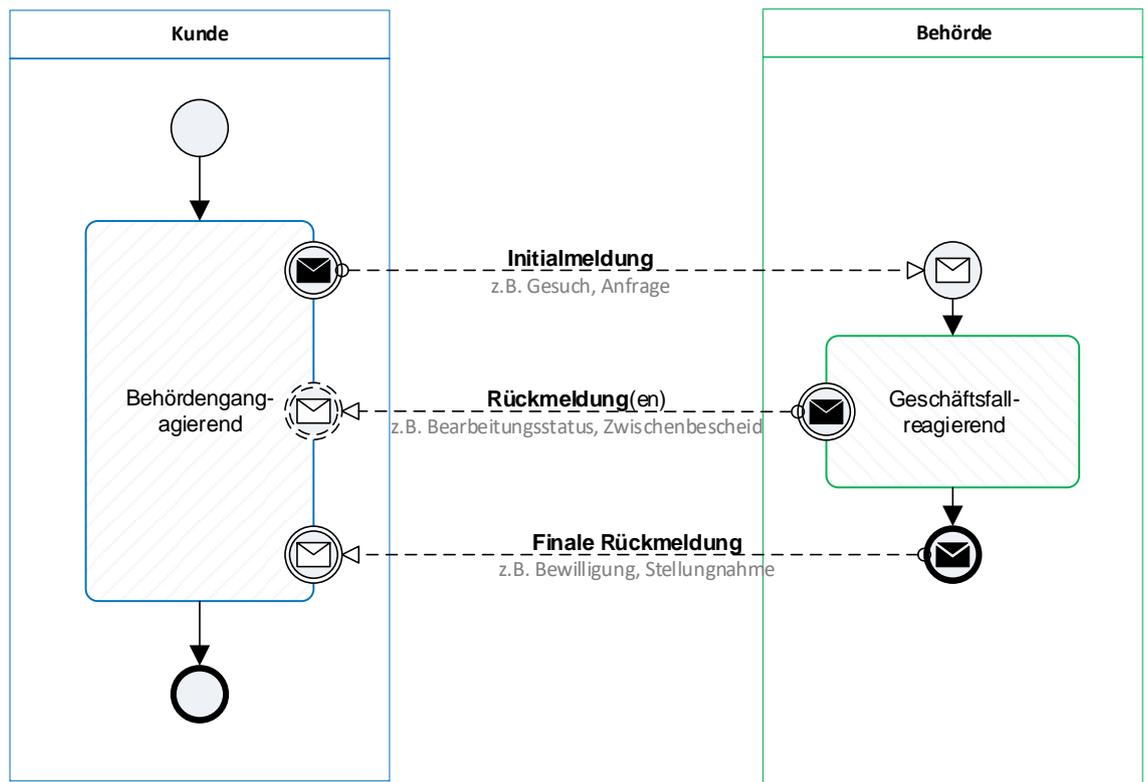


Abbildung 38: Prozessmodell Schnittstelle Behördengang ↔ Geschäftsbearbeitung im Fall "Anstoss durch Kunden"

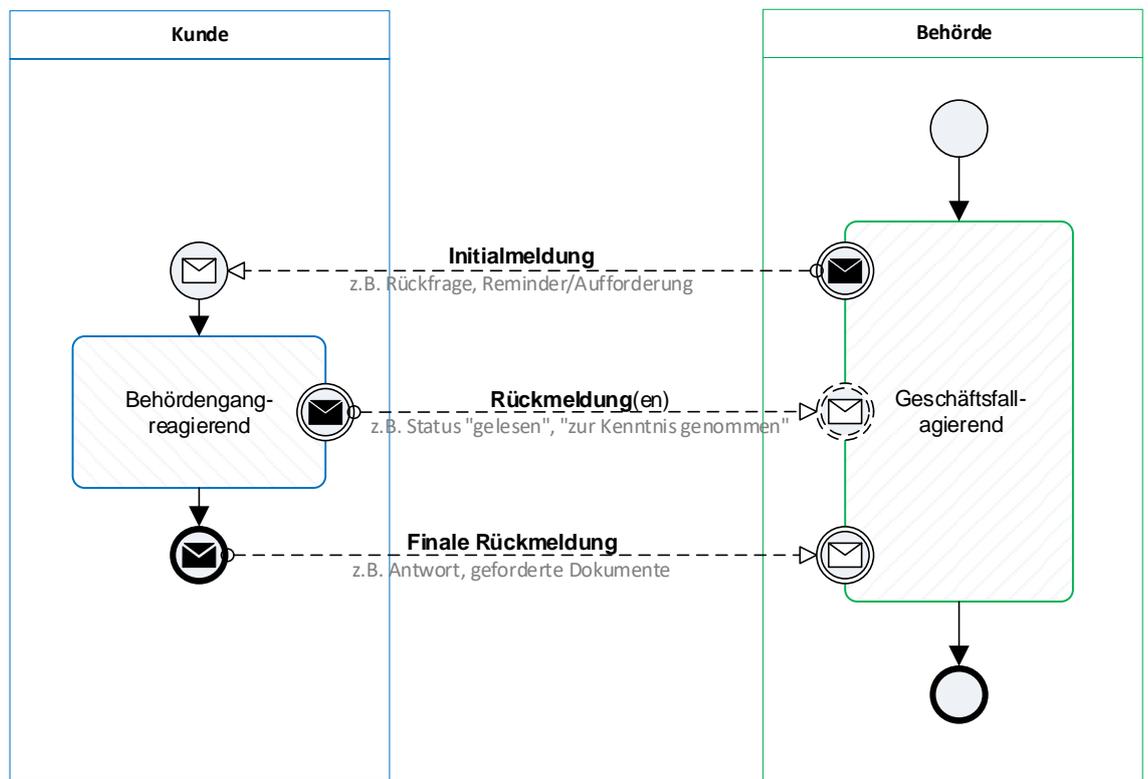


Abbildung 39: Prozessmodell Schnittstelle Behördengang ↔ Geschäftsbearbeitung im Fall "Anstoss durch Behörde"

Anhand des folgenden Szenarios sei das von den voran formulierten Anforderungen [REQ-24] bis [REQ-33] aufgespannte logische Gerüst veranschaulicht:

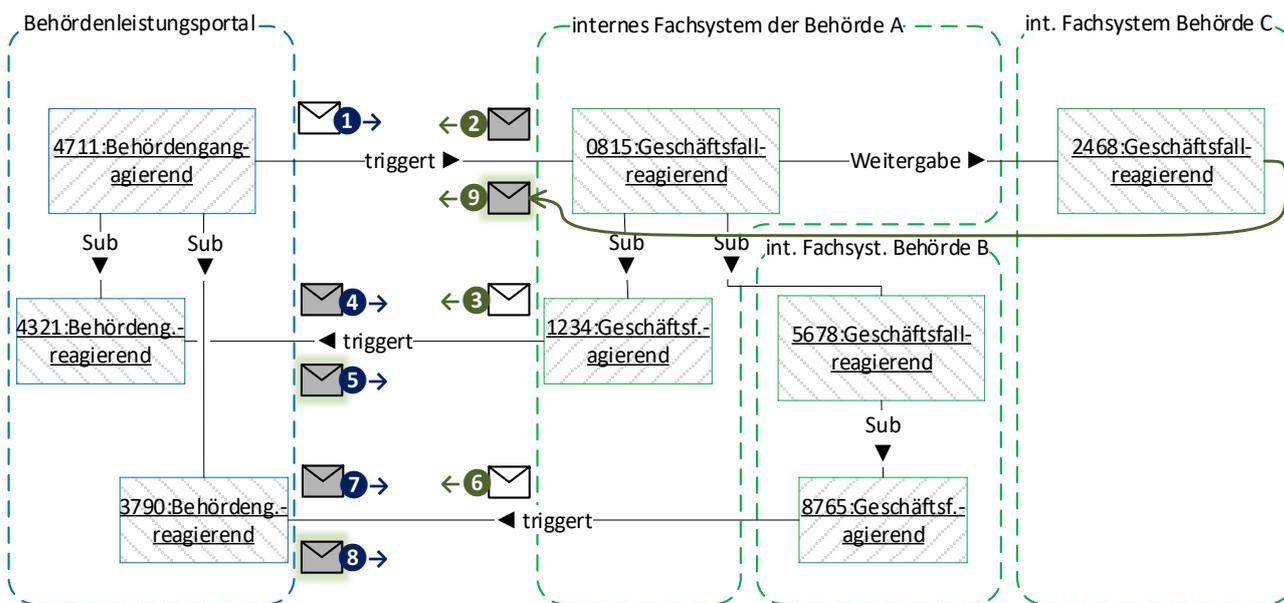


Abbildung 40: Szenario der Schnittstellenprozesse zwischen Behördengang und Geschäftsbearbeitung gemäss den diesbezüglichen Anforderungen

Im Behördenleistungportal wird ein Behördengang vollführt, in dessen Verlauf ein ausgefülltes Gesuch per Initialmeldung an das interne Fachsystem der Behörde A gesendet wird ①. Dabei wird auch die Behördengang-ID 4711 vom Portal übermittelt. In Reaktion auf den Empfang der Message legt das behördeninterne Fachsystem A einen komplementären Geschäftsfall an und gibt ihm die ID 0815. Bei jedem Wechsel des Bearbeitungsstatus sendet das Fachsystem der Behörde A eine Status-Rückmeldung an das Portal ②, das diese Information aufgrund der mitgelieferten Metadaten dem ursprünglichen Behördengang 4711 zuordnet und auch die ID des komplementären Geschäftsfalls notiert. Zwischenzeitlich taucht in der Behörde eine Frage auf, weshalb eine Rückfrage an den Kunden gestellt wird. Dabei wird ein Sub-Geschäftsfall mit der ID 1234 angestossen, in dem die Rückfrage an den Kunden zum Portal übermittelt wird ③. Das Portal bezieht die Message anhand der mitgelieferten Metadaten auf den ursprünglichen Behördengang und legt einen Sub-Behördengang 4321 an. Sobald ein vom Kunden bevollmächtigter User die Rückfrage im Portal zur Kenntnis nimmt, wird der Behörde A eine Status-Rückmeldung gesendet, die diese dem komplementären Geschäftsfall 1234 zuordnet ④. Schliesslich wird auf Kundenseite die Antwort auf die Rückfrage erfasst und mit einer finalen Rückmeldung (bezogen auf den Subprozess) versandt. Das empfangende Behördensystem A teilt diese wiederum dem Geschäftsfall 1234 zu ⑤. Nebenher findet ein Subprozess des Verfahrens bei der anderen Behörde B statt, zu dem eine Kundenkommunikation in gleicher Logik stattfindet ⑥ ⑦ ⑧. Letztlich sei angenommen, dass das Verfahren an Behörde C weitergegeben wird, dessen internes Fachsystem folglich einen Geschäftsfall mit ID 2468 angelegt und schliesslich am Ende des Verfahrens die finale Rückmeldung an das Portal sendet ⑨.

Für das beschriebene Szenario sind die in Abbildung 41 dargestellten API Endpoints nötig.

[REQ-34] Das Behördenleistungportal als Consumer der Geschäftsbearbeitung stellt einen API Endpoint für die Entgegennahme von behördenseitigen Messages zur Verfügung.

[REQ-35] Das behördeninterne Fachsystem stellt als Provider der Geschäftsbearbeitung einen API Endpoint für die Entgegennahme von kundenseitigen Messages zur Verfügung.

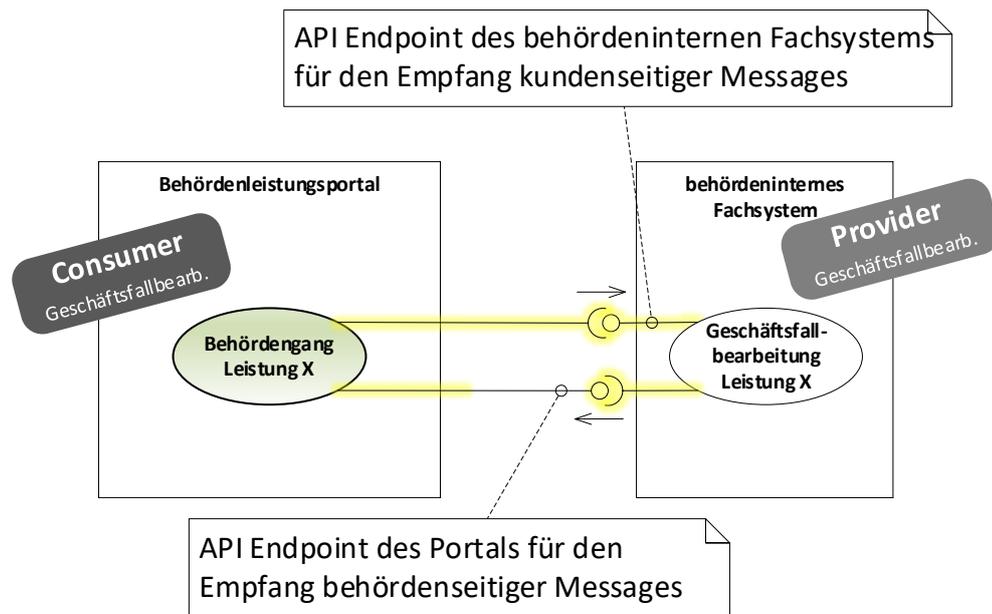


Abbildung 41: API Endpoints der Schnittstelle Behördengang↔Geschäftsbearbeitung

Generell gilt: In einem Kundenkonto eingehende Nachrichten sind für die entsprechend berechtigten User einsehbar. Ein Behördenleistungsportal kann darüber hinaus dem User eine Push-Benachrichtigungsfunktion anbieten (z.B. via E-Mail oder SMS-Dienst), die über neu für ihn einsehbare Nachrichten informiert. Solch eine Funktion muss jedoch nicht durch die Integrations-Sollarchitektur geregelt werden, sondern obliegt der Verantwortung des jeweiligen Portalbetreibers (Querschnittsfunktion).

Für die technische Umsetzung der Schnittstelle bieten sich zwei grundsätzliche Möglichkeiten:

- Bussystem: Ein zentraler Infrastrukturdienst wie z.B. Sedex stellt die Transportschicht zur Verfügung.
- API: Die Behörde stellt eine API für Portale zur Verfügung.

Vor- und Nachteile dieser beiden Varianten werden in [Herausforderung-5], Anhang G.D analysiert. Letztlich können die o.a. Schnittstellen-Anforderungen durch beide Möglichkeiten erfüllt werden. In jedem Fall müssen die Sicherheitsanforderungen (siehe Kapitel 2.5.2) erfüllt werden.

2.5.1.3 Schnittstelle zur Einbindung extern implementierter Behördengänge

Die Schnittstelle zur Einbindung extern implementierter Behördengänge ist das wesentliche Element des Integrationsmusters 2 (siehe Kapitel 2.1.6).

[REQ-36] Die Schnittstelle zur Einbindung extern implementierter Behördengänge umfasst - wie schon von Abbildung 34 in Kapitel 2.5.1.1.6 aufgezeigt - die Weiterleitung vom Consumer- auf das Provider-Portal. Dabei ist zunächst das SSO (siehe 2.5.1.3.1) zu bewerkstelligen und anschliessend der Kontext des Behördengangs auf dem Provider-Portal analog herzustellen (siehe 2.5.1.3.2).

[REQ-37] Bei der Hin- bzw. Rück-Weiterleitung soll der User im selben Browserfenster verbleiben, damit ihm der physische Systemwechsel nicht bewusst wird. Wahrnehmbare Änderungen im UI-Design können jedoch in Kauf genommen werden.

[REQ-38] Bei der Rückleitung vom Provider- auf das Consumer-Portal muss der User im selben Kontext wie vor dem Absprung ankommen.

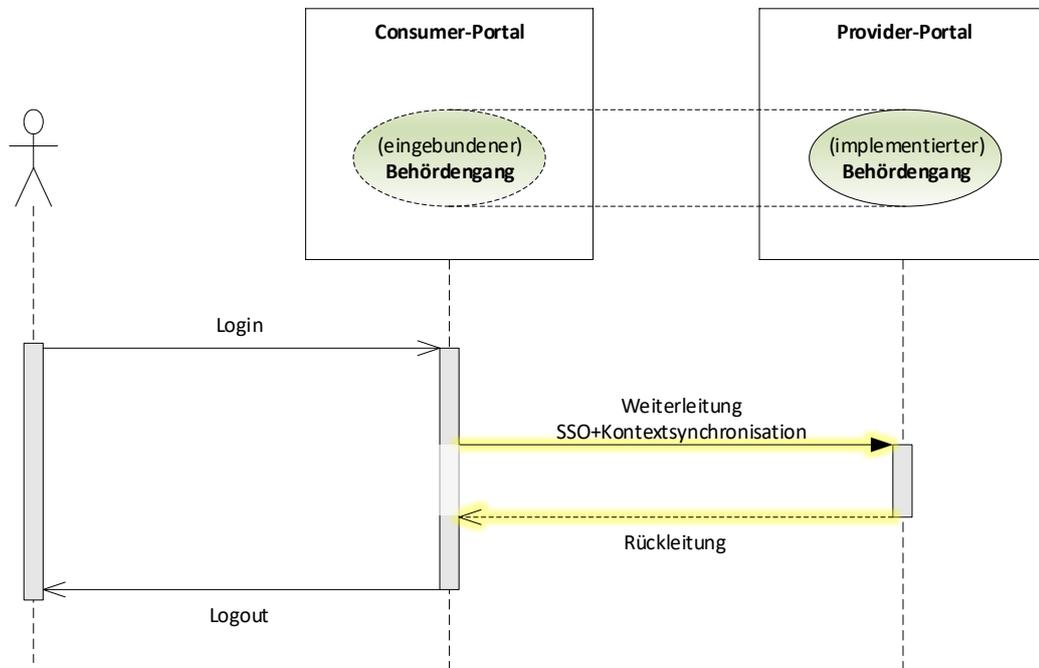


Abbildung 42: Die Einbindung eines extern implementierten Behördengangs umfasst Hin- und Rückleitung

2.5.1.3.1 Single Sign On (SSO)

Grundsätzlich sind zwei Konstellationen zu betrachten:

- A) Gemeinsamer Identitätsdienst: Consumer- und Provider-Portal verwenden denselben IdP/Vermittler⁷⁴
- B) Peer-to-Peer Trust (P2P-Trust): Consumer- und Provider-Portal verwenden unterschiedliche IdPs/Vermittler

Den ersten Fall A) veranschaulicht Abbildung 43 in folgendem Szenario.

Prolog: Der User meldet sich am Consumer-Portal an **1**, wobei das Portal die Authentisierung an seinen Identitätsprovider⁷⁵ (IdP) delegiert **2**. Unter der Annahme einer erfolgreichen Authentisierung stellt der IdP einen Identity Token⁷⁶ aus und übermittelt ihn an das Consumer-

⁷⁴ Ein Vermittler (wie z.B. eIAM Bund) kann mehrere IdPs anbieten, siehe auch Glossar im Anhang A

⁷⁵ Ob es sich hierbei um einen einzelnen Identitätsprovider oder um einen Vermittler von mehreren Identitätsprovidern handelt, spielt für das Szenario keine Rolle.

⁷⁶ Von technologischen Aspekten (Format und Medium des Identity Tokens, Verschlüsselungsart, etc.) wird in der Darstellung abstrahiert, da sie aus logischer Sicht nicht von Belang sind.

Portal ③. Dieses rückversichert sich zunächst beim IdP anhand der Signatur, dass der Token auch wirklich von ihm stammt ④. Erst danach stellt das Consumer-Portal eine angemeldete Session für das Userkonto mit der lokalen ID "4711"⁷⁷ her, welches der im Identity Token übermittelten ID "1234" zugeordnet ist ⑤. Sollte in der betreffenden Mappingtabelle für diese ID noch kein Userkonto vermerkt sein, wird es neu erstellt und im Mapping hinterlegt. In jedem Fall befindet sich der User nun in einer angemeldeten Session vom Consumer-Portal, in der er irgendwann den vom Provider-Portal eingebundenen Behördengang aufruft.

SSO: Bei der Weiterleitung wird auch der – vom IdP stammende – Identity Token an das Provider-Portal übermittelt ⑥⁷⁸. Das Provider-Portal stellt daraufhin nach dem gleichen Muster - wie im Consumer-Portal bei den Schritten ④ und ⑤ praktiziert - eine angemeldete Session für das (vorhandene oder neu in situ erstellte) Userkonto mit der lokalen ID 0815 her ⑦ ⑧. Der User arbeitet in seinem Browserfenster nahtlos auf dem Provider-Portal weiter und vollführt den beabsichtigten Behördengang ⑨.

⁷⁷ Die beispielhaften ID-Werte sind im Interesse der Lesbarkeit kurzgehalten.

⁷⁸ Das Protokoll der Übermittlung spielt hierbei keine Rolle. Es ist aus logischer Sicht unerheblich, ob sie z.B. via URL-Parameter oder Security Token erfolgt.

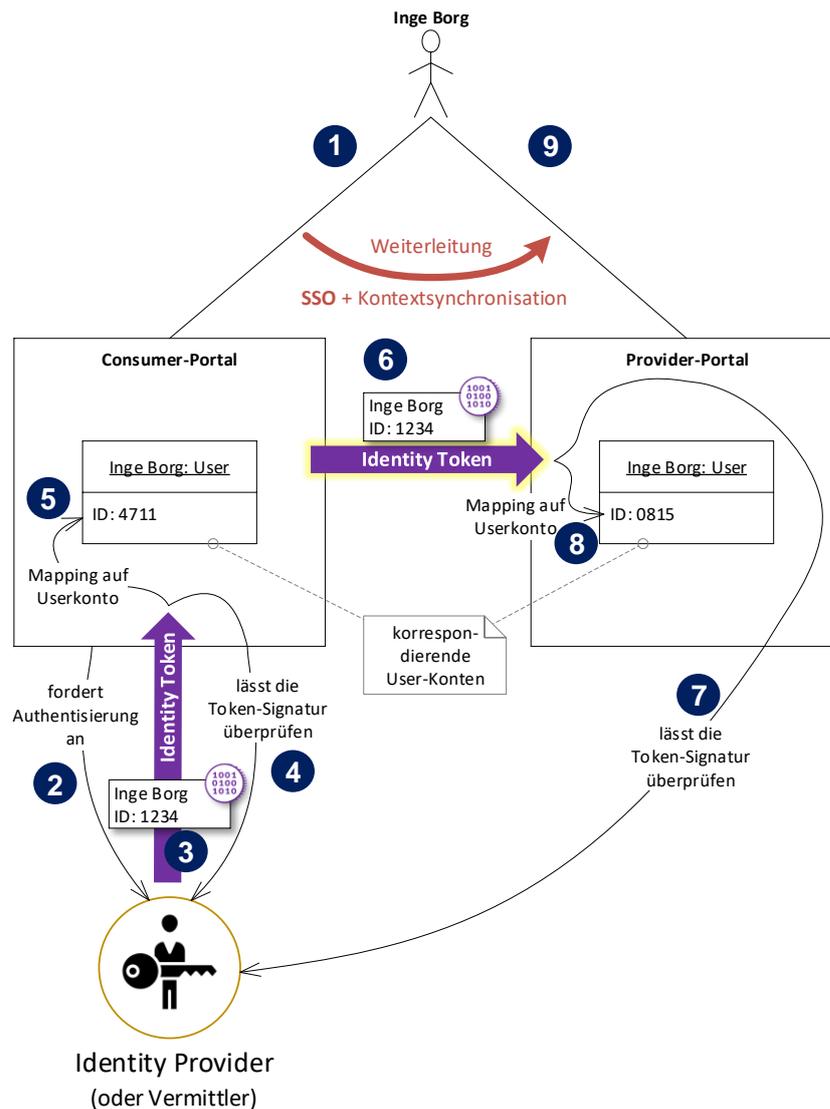


Abbildung 43: SSO-Szenario mit gemeinschaftlich verwendetem Identitätsprovider

Abbildung 44 zeigt den Rücksprung. Nach Beendigung des Behördengangs auf dem Provider-Portal navigiert der User zurück auf den letzten Screen des Consumer-Portals 10. Üblicherweise ist der Login-Zustand bzw. der Identity Token in einem Cookie erhalten geblieben. Andernfalls muss das Consumer-Portal die Session nach dem gleichen Muster - wie im Consumer-Portal bei den Schritten 4 und 5 praktiziert - für das vorhandene Userkonto mit der lokalen ID 0815 wiederherstellen. In jedem Fall stellt es den ursprünglichen Zustand zum Zeitpunkt des Absprungs her 11 12. Nun befindet sich der User wieder im Consumer-Portal, in dem er die Bewirtschaftung des betreffenden Kundenkontos fortsetzt oder anderweitige Tätigkeiten vornimmt 13.

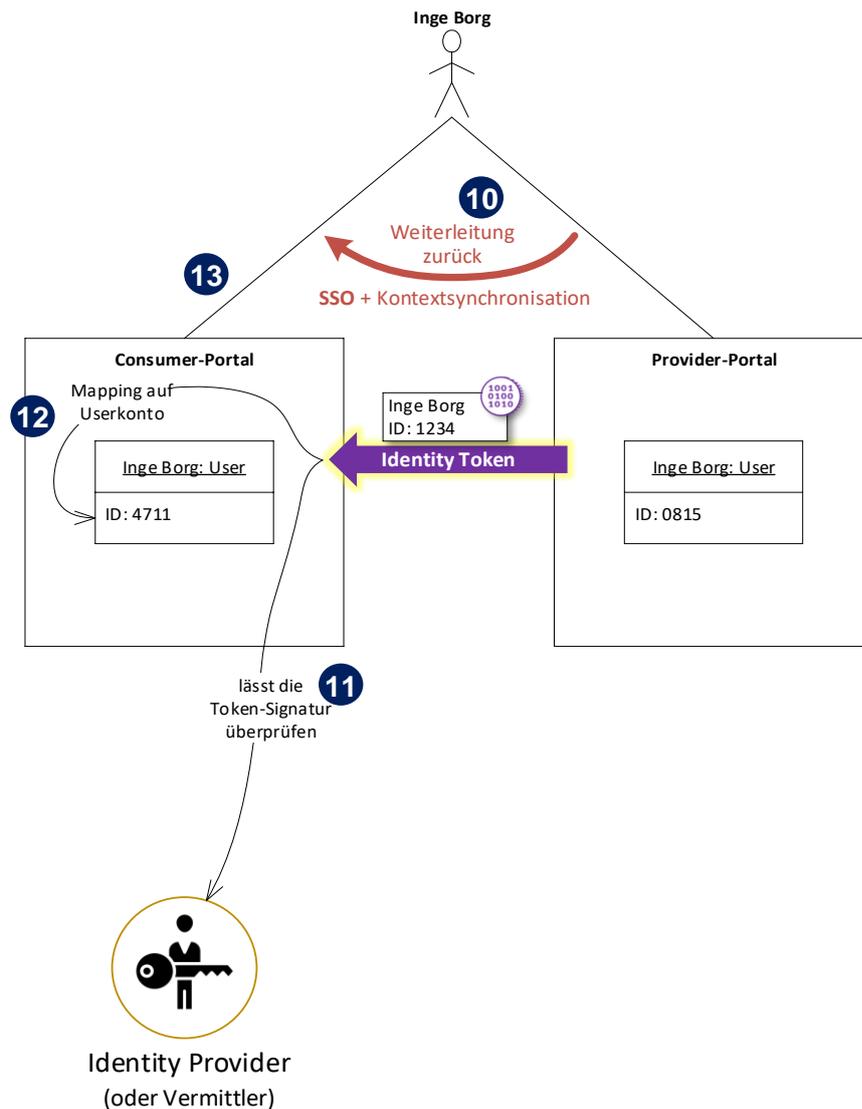


Abbildung 44: Rücksprung im SSO-Szenario mit gemeinschaftlich verwendetem IdP

Der zweite Fall B) verkörpert im Unterschied zum ersten Fall einen dezentralen Peer-To-Peer (P2P)-Trust Ansatz. Abbildung 45 zeigt dazu ein exemplarisches Szenario:

Zunächst befindet sich der User auf dem Consumer-Portal. Das Prozedere von der Anmeldung bis zum Aufruf des eingebundenen Behördengangs ①-⑤ ist genau dasselbe wie im Prolog oben beim ersten Fall A) geschildert. Dies bleibt jedoch für das Provider-Portal verborgen und es ist auch nicht von Bedeutung, mit welchem IdP das Consumer-Portal zusammenarbeitet. Bei der Weiterleitung wird lediglich ein Access Token⁷⁹ an das Provider-Portal übermittelt ⑥⁷⁸. Dieser Access Token berechtigt⁸⁰ das Provider-Portal, die Identity-Information vom Consumer-

⁷⁹ Der Begriff Access Token geht auf die Standards OAuth 2.0 bzw. OpenID connect (OIDC) zurück

⁸⁰ Die Berechtigung kann aus Sicherheitsgründen zeitlich befristet werden.

Portal zu erfragen ⑦. Letzteres stellt dazu einen entsprechenden Introspection⁸¹ API Endpoint zur Verfügung, welcher auf den Request des Provider-Portals die gewünschte Identity-Information in der Response zurückgibt. Ob in der Identity-Information die vom IdP stammende ID oder die des Userkontos enthalten ist, spielt keine Rolle. Wichtig ist nur, dass [REQ-16] erfüllt ist, also die ID das Userkonto global eindeutig identifiziert. Mit dieser Information kann das Provider-Portal nach dem gleichen Muster - wie im Consumer-Portal bei den Schritten ④ und ⑤ praktiziert - eine angemeldete Session für das (vorhandene oder neu in situ erstellte) Userkonto mit der lokalen ID 0815 herstellen ⑧. Der User arbeitet in seinem Browserfenster nahtlos auf dem Provider-Portal weiter und vollführt den beabsichtigten Behördengang ⑨.

Nach Beendigung des Behördengangs auf dem Provider-Portal navigiert der User zurück auf den letzten Screen des Consumer-Portals. Der Rücksprung erfolgt ähnlich dem oben für den Fall A) beschriebenen Szenario: Üblicherweise ist der Login-Zustand bzw. der Security Token in einem Cookie im Consumer-Portal erhalten geblieben. Andernfalls muss das Consumer-Portal die Session nach dem gleichen Muster - wie im Consumer-Portal bei den Schritten ④ und ⑤ auf Abbildung 45 praktiziert - für das vorhandene Userkonto mit der lokalen ID 0815 wiederherstellen. In jedem Fall stellt es den ursprünglichen Zustand zum Zeitpunkt des Absprungs her.

⁸¹ Der Begriff Introspection Endpoint geht auf den Standard OAuth 2.0 zurück. Der eCH-Standard eCH-0225 [32] zeigt darüber hinaus im Kapitel 10.3 auf, wie der Introspection Endpoint zu gestalten ist.

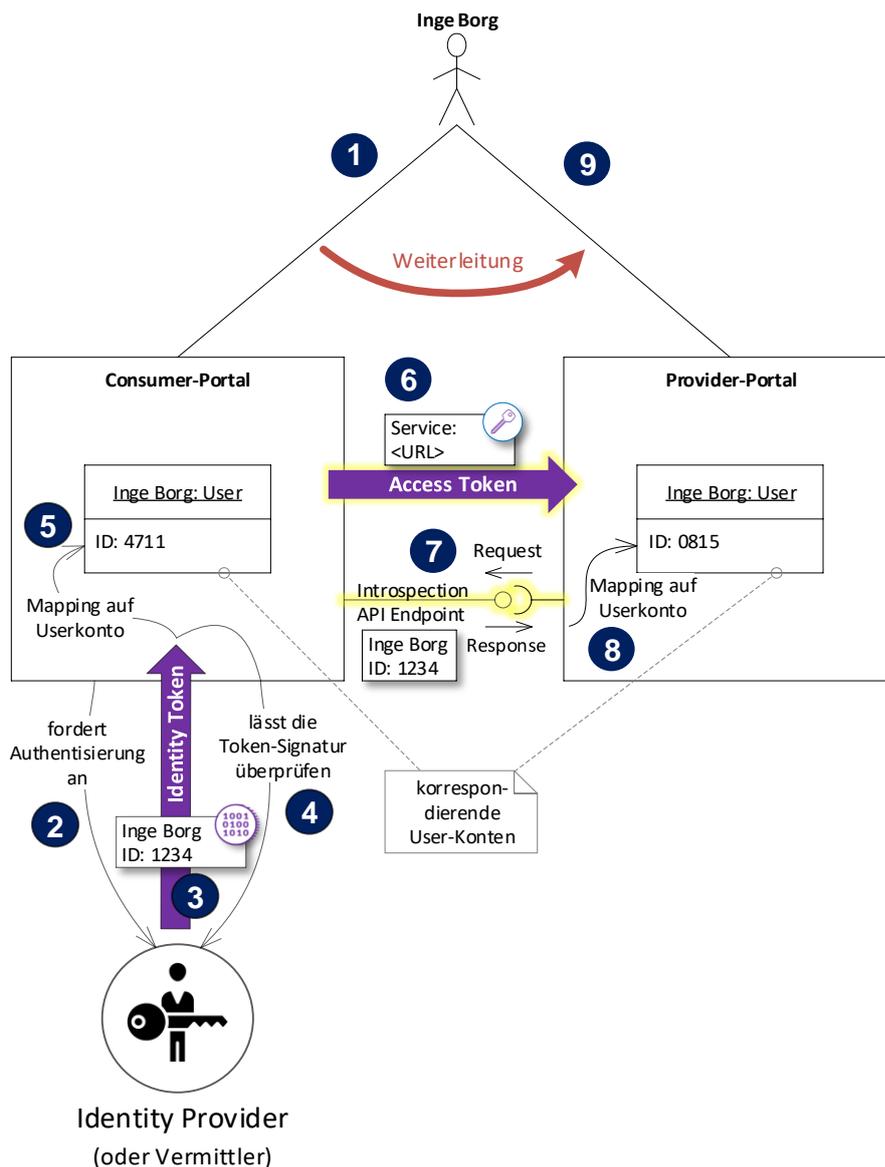


Abbildung 45: SSO-Szenario mit bilateralem Peer-to-Peer (P2P) Trust

Welche der beiden dargestellten Konstellationen A) oder B) zu präferieren ist, wurde in den Fachausschuss-Workshops intensiv diskutiert (siehe [Herausforderung-3] im Anhang G.D). Im Ergebnis wurde unter Beachtung der Architekturprinzipien [P-4] und [P-7] das dezentrale Muster B) P2P Trust empfohlen, da es die **IdP-Frage** von der Schnittstelle zur Einbindung extern implementierter Behördengänge **entkoppelt**. Aus Sicht des Provider-Portals interessiert es nicht, welche(n) IdP(s) oder Vermittler das Consumer-Portal hinter den Kulissen verwendet, da dies durch die Schnittstelle vollständig gekapselt ist. Auf diese Weise ermöglicht das P2P-Muster die für das Zusammenwirken über föderale Grenzen hinweg nötige Flexibilität sowie den Einbezug ausländischer Identitätsprovider. Der Ansatz B) P2P-Trust wird deshalb in der Umsetzungs-Roadmap (siehe 2.7.1) entsprechend aufgegriffen. Der Ansatz A) kann allenfalls in Ausnahmefällen zum Zuge kommen, wenn Consumer- und Provider-Portal ohnehin denselben Identitätsdienst verwenden (wie z.B. bei eIAM-basierten Portale/-Fachanwendungen im Bund).
Gemeinsam ist beiden Varianten:

[REQ-39] Anhand der vom Consumer-Portal für das Userkonto übermittelten ID wird im Provider-Portal das korrespondierende Konto selektiert (oder in situ erstellt, falls noch nicht vorhanden).

[REQ-40] Vom Consumer-Portal werden mindestens folgende Informationen an das Provider-Portal übermittelt: ID des Userkontos (siehe 2.5.1.1.6.1), Profileinstellungen (siehe 2.5.1.1.6.2), LoA des Logins (siehe 2.5.1.1.6.3)

[REQ-41] Beim Rücksprung vom Provider-Portal zum Consumer-Portal muss letzteres den ursprünglichen Zustand wiederherstellen, der unmittelbar vor der Weiterleitung zum Provider-Portal gegeben war. Dazu muss das Consumer-Portal die entsprechenden Kontextparameter (z.B. Absprung-Page, Kunden- und Leistungsselektion) zwischenzeitlich sichern.

Zwischen beiden Varianten gibt es bezüglich des im Provider-Portal angelegten korrespondierenden Userkontos einen Unterschied: Im Fall A) (gemeinsamer IdP) kann sich der User mit diesem korrespondierendem Konto im Provider-Portal direkt anmelden, im Fall B) (P2P-Trust) ist das hingegen nicht möglich, da dem korrespondierenden Userkonto kein Login zugeordnet ist.

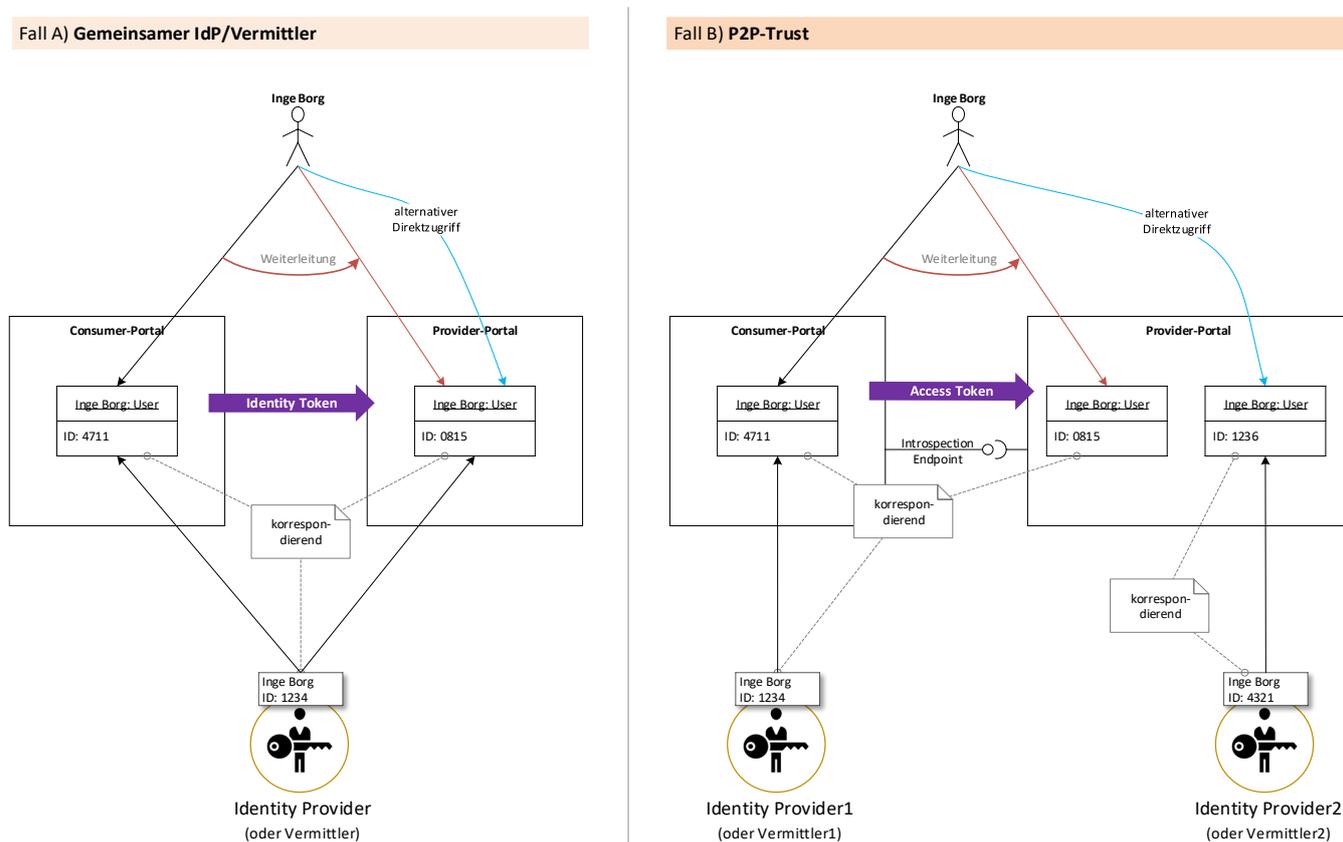


Abbildung 46: Unterschied zwischen Fall A) und B) bezüglich Weiterleitung und alternativem Direktzugriff

Eine besondere Bedeutung kommt dem LoA des Logins zu. Das Provider-Portal muss im Fall B) (P2P-Trust) dem Consumer-Portal vertrauen, dass der übermittelte Wert den Tatsachen entspricht. Diese Frage kann explizit in einer beiderseitigen Vertrauensvereinbarung geregelt und geprüft werden. Darüber hinaus ist es denkbar, dass eine staatliche Prüfstelle Herausgeber von LoA-Werten zertifiziert (Definitionszeit). Bei Vorlage eines solchen Zertifikates wäre die

bilaterale Vertrauensstellung nicht nötig. Diese Idee wird in der Umsetzungs-Roadmap (siehe 2.7.1) aufgegriffen.

Hinweis: Im Fall A) (gemeinsamer Identitätsdienst) ist die Vertrauensfrage gleichermassen für die Beziehung zwischen IdP/Vermittler und den angeschlossenen Portalen relevant. Dies liegt aber ausserhalb des Scopes der Integrations-Sollarchitektur.

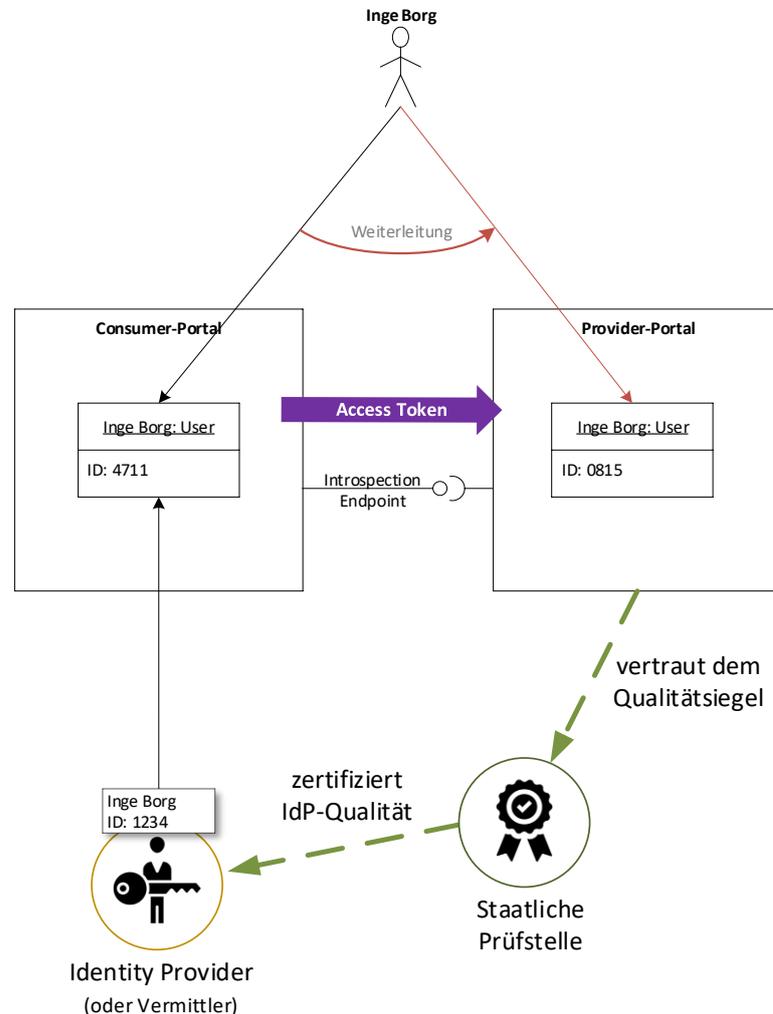


Abbildung 47: Eine staatliche Prüfstelle vereinfacht mittels einer Zertifizierung die Vertrauensstellung zum LoA des Logins

Welcher Login-LoA für einen Behördengang erforderlich ist⁸², definiert die für die jeweilige Leistung zuständige Behörde.

[REQ-42] Das Provider-Portal trägt die Verantwortung, dass der für den betreffenden Behördengang festgelegte Mindest-LoA des Logins eingehalten wird.

⁸² Achtung Verwechslungsgefahr: Login-LoA und Bewirtschaftungsrecht sind verschiedene Dinge. Ersteres beschreibt eine Vertrauensstufe, letztere ein explizit vom Kunden vergebenes Recht.

Um unnötige Konformitätskonflikte zu vermeiden, empfiehlt es sich aber, dass bereits das Consumer-Portal den Aufruf des eingebundenen Behördengang an den erforderlichen LoA knüpft.

2.5.1.3.2 Kontextsynchronisation

Wie bereits in Kapitel 2.5.1.1.6 vorab ausgeführt und in Abbildung 34 illustriert, muss neben dem SSO und User-Login auch der Kontext des Behördengangs, bestehend aus Kundenselektion und dazugehörigem Bewirtschaftungsrecht im Provider-Portal analog dem Kontext beim Abruf im Consumer-Portal synchronisiert werden. Dazu müssen zunächst die nötigen Informationen entsprechend des Interoperabilitätsrahmens über die Schnittstelle bei der Weiterleitung übermittelt werden:

[REQ-43] Vom Consumer-Portal werden mindestens folgende Informationen an das Provider-Portal übermittelt: Behördenleistung (kontrolliertes Vokabular gemäss Kapitel 2.5.1.1.2) auf die sich der adressierte Behördengang bezieht, ID des Kunden (siehe Kapitel 2.5.1.1.4) für den der Behördengang vollführt werden soll, Bewirtschaftungsrecht (kontrolliertes Vokabular gemäss Kapitel 2.5.1.1.6.4), LoA des Bewirtschaftungsrechts (siehe [REQ-22] in Kapitel 2.5.1.1.6.4). Sofern im Consumer-Portal ein bereits existierender Behördengang adressiert wurde, dann ist zusätzlich dessen ID (siehe [REQ-14] in Kapitel 2.5.1.1.5) zu übermitteln.

[REQ-44] Zusätzlich ist das Kundenanliegen zu übermitteln, sofern dieses bekannt ist⁷².

[REQ-45] Die Übermittlung erfolgt zusammen mit der in [REQ-40] beschriebenen SSO-Information.

Das bedeutet für den im vorangegangenen Kapitel 2.5.1.3.1 beschriebenen SSO-Fall A) (gemeinsamer IdP), dass das Consumer-Portal die in [REQ-43] genannte Information in einem Context Token anhängt. Im SSO Fall B) (P2P-Trust) liefert der Introspection API Endpoint den Kontextzusatz.

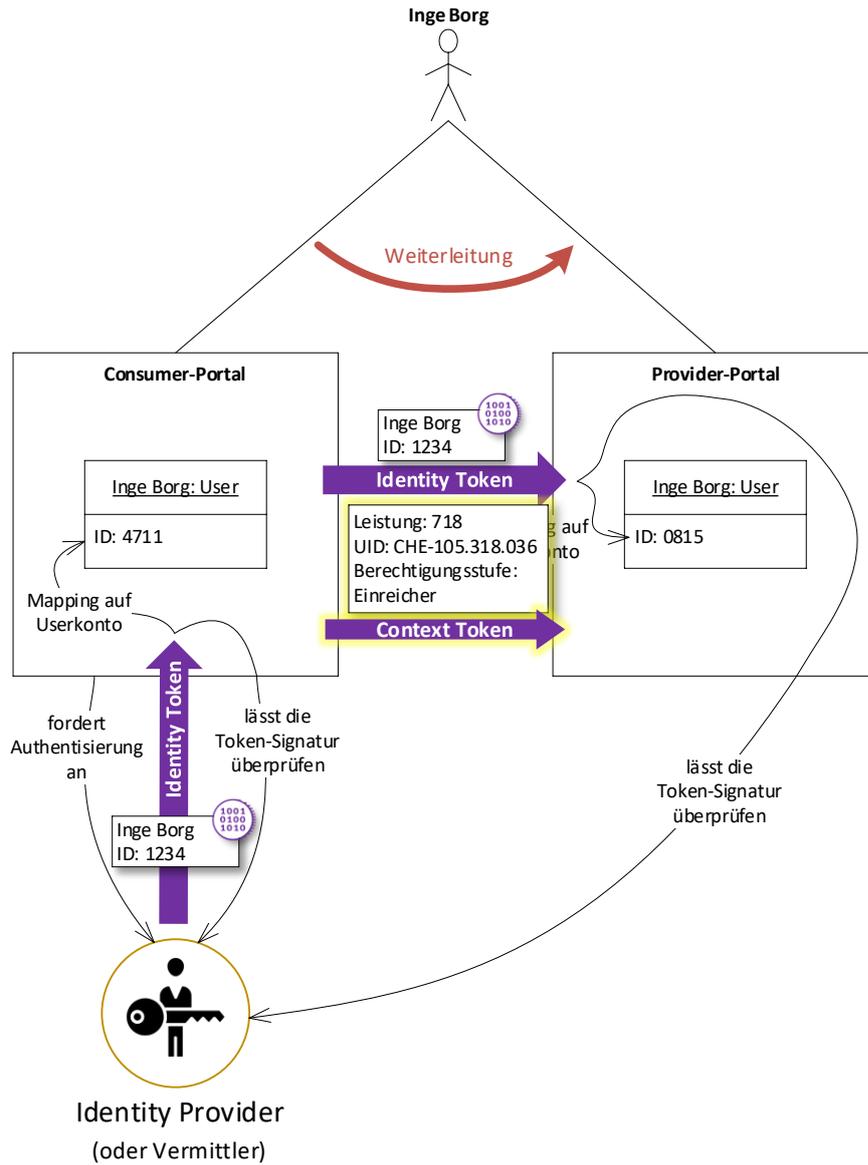


Abbildung 48: Übertragung der Kontextinformation im Fall A) per Context Token als Zusatz zum Identity Token (vergleiche Abbildung 43)

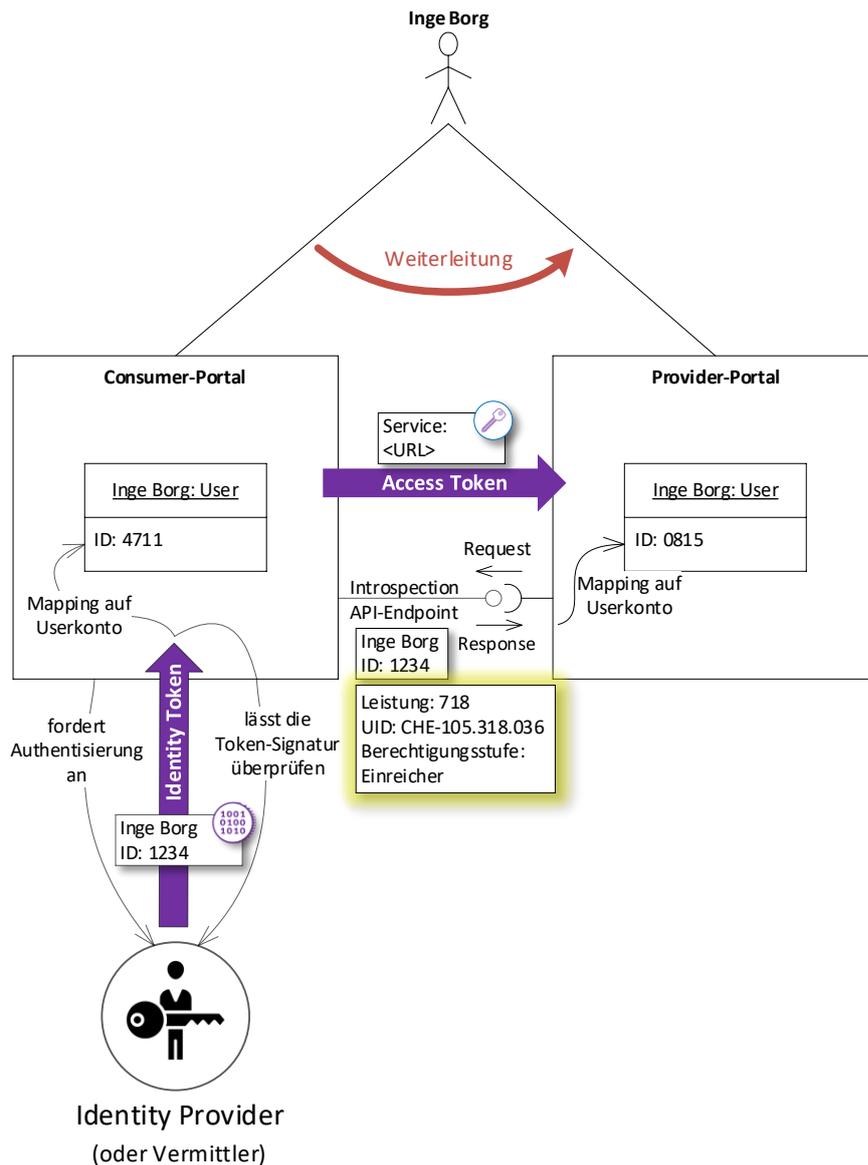


Abbildung 49: Übertragung der Kontextinformation im Fall B) als Zusatz der Response des Introspection API Endpoints (vergleiche Abbildung 45)

[REQ-46] Aufgrund der übermittelten Kontextinformation stellt das Provider-Portal seinen Kontext wie folgt her:

- Selektion des adressierten Kundenkontos. Falls dieses nicht vorhanden ist, wird es in situ angelegt. Die Stammdaten werden in dem Fall aus dem zuständigen Register bezogen (siehe 2.5.1.1.4.3)

- Temporäre Übernahme der übermittelten Berechtigungsstufe des betreffenden Users für die/den betreffende/n Leistung/Kunden in das Provider-Portal während der Lebensdauer der Session⁸³.
- Navigation zum Startscreen des adressierten Behördengangs mit Fokus auf das adressierte Kundenkonto sowie der Berechtigungsstufe entsprechenden Funktionalität

Voraussetzung ist, dass das Provider-Portal den im Consumer-Portal vergebenen Bewirtschaftungsrechten vertraut. Die Qualität des Vergabe- bzw. Vollmachtsprozesses im Consumer-Portal (wird durch den LoA des Bewirtschaftungsrechts dokumentiert) muss den Anforderungen des Provider-Portals genügen.

[REQ-47] Das Provider-Portal trägt die Verantwortung, dass es vom Consumer-Portal übermittelte Bewirtschaftungsrechte nur akzeptiert, wenn diese einen bestimmten Mindest-LoA aufweisen.

Um diesbezügliche Vertrauensvereinbarungen zu erleichtern, wäre wie beim LoA des Logins die Zertifizierung des LoA der Bewirtschaftungsrechte durch eine staatliche Prüfstelle denkbar (siehe Ausführungen im letzten Teil von Kapitel 2.5.1.3.1 sowie Abbildung 47).

2.5.1.3.3 Single Logout (SLO)

[REQ-48] Bei jeglichen SSO-Szenarien ist das SLO sicherzustellen.

Das bedeutet, die Abmeldung muss sowohl auf dem Consumer- als auch auf Provider-Portal erfolgen. Befindet sich beispielsweise der User auf dem Provider-Portal und meldet sich ab, so muss auch der Login-Zustand auf dem Consumer-Portal terminiert werden. Dies gilt ebenso umgekehrt: Wenn sich der User auf dem Consumer-Portal abmeldet, müssen auch eine allfällige per SSO initiierte Session auf dem Provider-Portal beendet werden. Sofern der User im Consumer-Portal mehrere eingebundene Behördengänge aufgerufen hat, müssen alle damit zusammenhängenden Sessions auf den jeweiligen Provider-Portalen terminiert werden.

2.5.1.3.4 Rückkanal für den Behördengang (Status, behördliche Benachrichtigungen, Ergebnisdokumente)

Im Sinne des Anspruchs von [REQ-37] (siehe Kapitel 2.5.1.3) sollten infolge der Bedürfnisse [B-18] und [B-24] Statusinformationen (sowohl zum Behördengang selbst als auch zur Geschäftsfallbearbeitung) und Ergebnisdokumente sowie allfällige behördliche Benachrichtigungen (z.B. Erneuerung eines Passes fällig) auch für eingebundene Behördengänge im Consumer-Portal ersichtlich sein. Dies ist zwar kein Muss (der User kann die Informationen im Provider-Portal einsehen, indem er den betreffenden Behördengang wieder aufruft), aber aus User-Sicht durchaus

⁸³ Das Bewirtschaftungsrecht darf im Provider-Portal über die Schnittstelle nicht dauerhaft persistiert werden, da es sonst zu Inkonsistenzen in der Weise kommen kann, dass nach Rechteentzug im Consumer-Portal das betreffende Recht im Provider-Portal weiterhin fortbesteht.

wünschenswert, da es sonst im Vergleich zu den implementierten Behördengängen einen geringeren Komfort hat.

[REQ-49] Das Consumer-Portal bietet einen API Endpoint, der dem Provider-Portal die Weiterleitung der zu einem Behördengang auftretenden Rückmeldungen zum Consumer-Portal erlaubt.

[REQ-50] Die Rückmeldungen umfassen sowohl Statusinformationen und Ergebnisdokumente des Behördengangs als auch proaktive Benachrichtigungen der Behörde an den Kunden (z.B. Erneuerung eines Passes fällig).

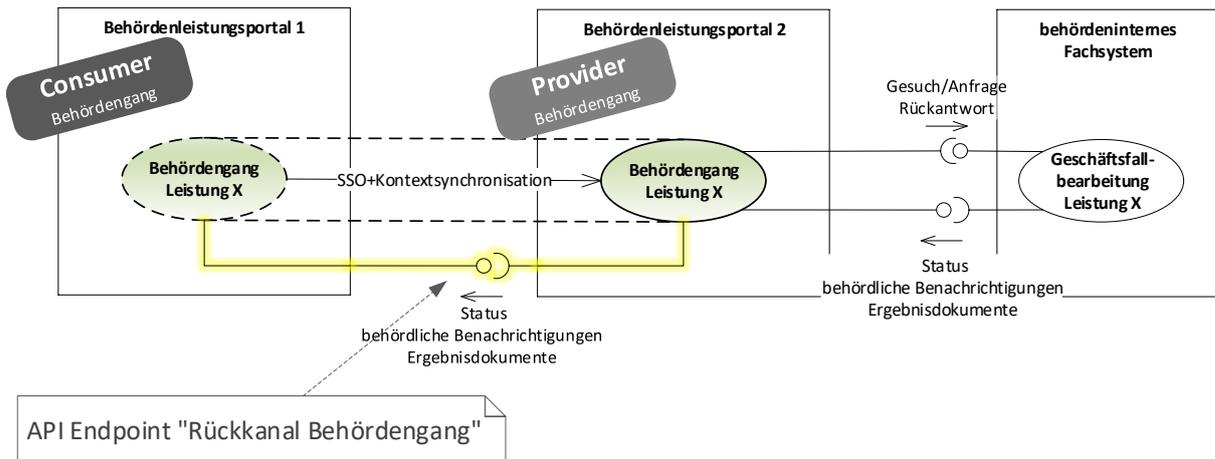


Abbildung 50: API Endpoint für die Behördengang-Rückmeldungen als Bestandteil der Schnittstelle zur Einbindung extern implementierter Behördengänge

2.5.1.4 Schnittstellen-Datenfluss im Überblick

Zusammenfassend sei der Datenfluss der beiden in den vorangegangenen Kapiteln 2.5.1.2 und 2.5.1.3 beschriebenen Schnittstellen anhand des in Abbildung 51 dargestellten exemplarischen Gesamtbilds verdeutlicht. Dieses beinhaltet das Behördenleistungsportal 1 mit einem vom Behördenleistungsportal 2 eingebundenen Behördengang, dessen Implementation im Behördenleistungsportal 2 über die Schnittstelle "Behördengang↔Geschäftsfallbearbeitung" mit dem dahinterstehenden Fachsystem der zuständigen Behörde kommuniziert.

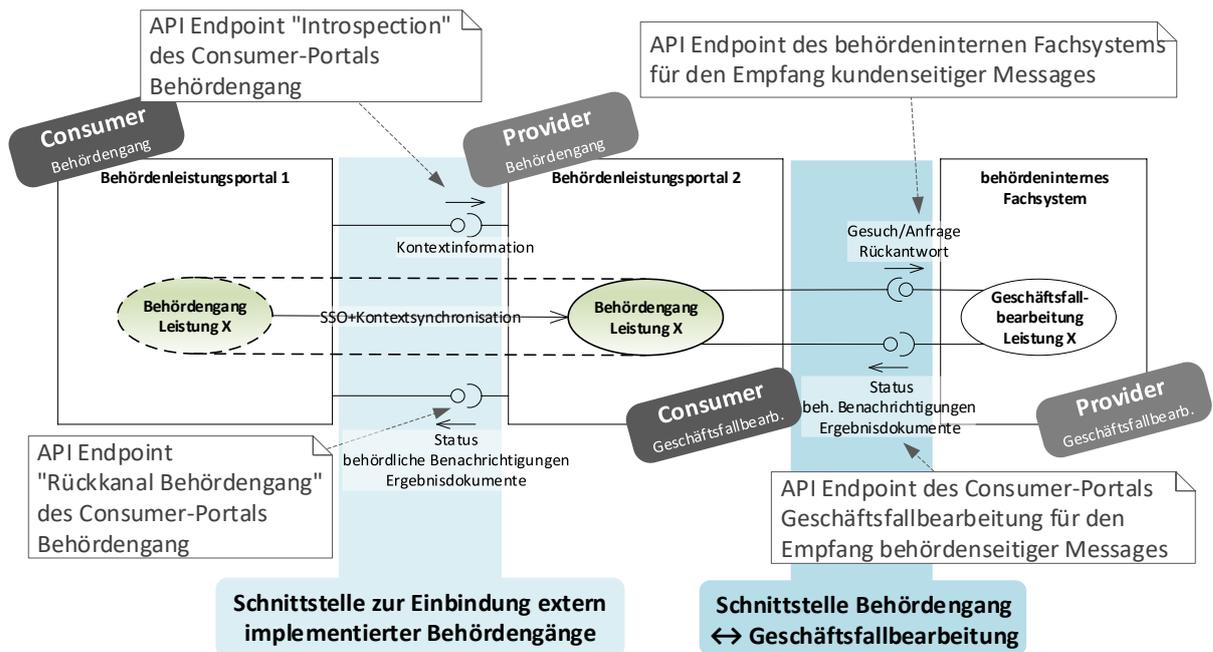


Abbildung 51: Gesamtbild eines eingebundenen Behördengangs mit der von dessen Provider-Portal gekapselten Schnittstelle zum dahinterstehenden behördeninternen Fachsystem

Abbildung 52 zeigt den Datenfluss differenziert für die einzelnen Bereiche des Interoperabilitätsrahmens, wobei der jeweilige interoperable Kern schematisch abgegrenzt ist. Die Darstellung verdeutlicht, welche Schnittstellen welche Bereiche übertragen. Ebenso illustriert die Grafik, dass der Ursprung des Flusses des interoperablen Kerns der Kundenstammdaten beim zuständigen Register liegt, wobei dieses sowohl vom Behördenleistungsportal 1 als auch vom Behördenleistungsportal 2 abgefragt wird (siehe Kapitel 2.5.1.1.4.3). Massgebend für beide Behördenleistungsportale sind also immer die Daten, welche von den Registern bezogen werden. Die Schnittstelle zwischen den beiden Portalen überträgt nur den Kundenidentifikator.

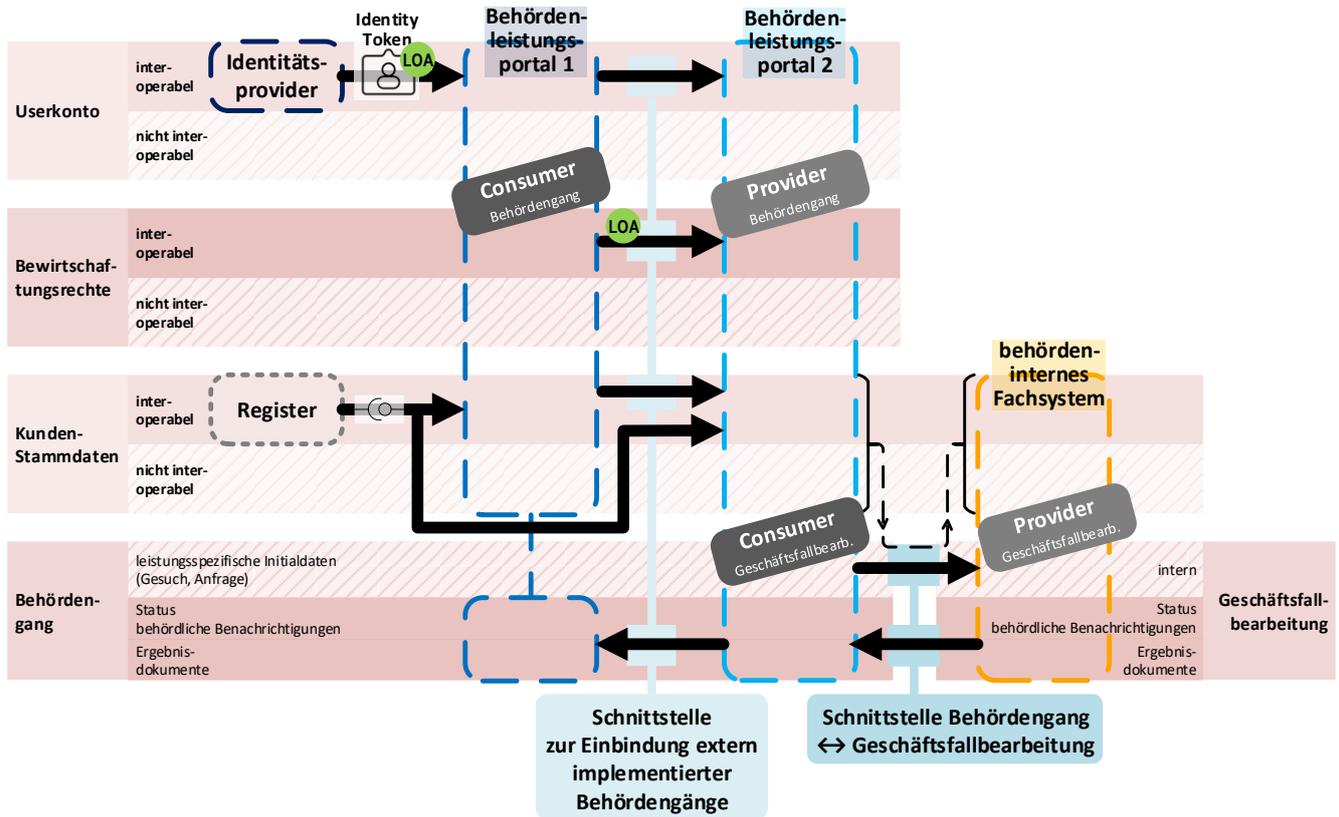


Abbildung 52: Schnittstellen-Datenfluss im Überblick

2.5.1.5 Schnittstellen-Verantwortung

Um zirkuläre Abhängigkeiten (wie in Abbildung 53 skizziert) zu vermeiden, muss die Verantwortung (d.h. die Definitionshoheit) über die Schnittstellen zwischen zwei Systemen in einer Hand liegen.

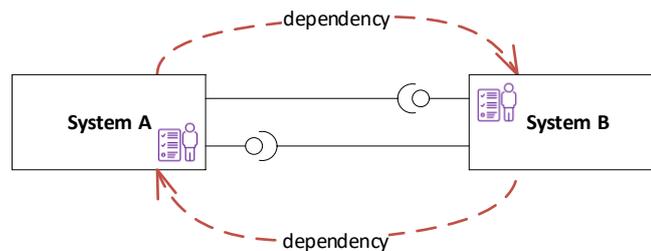


Abbildung 53: Zirkuläre Abhängigkeit infolge verteilter Schnittstellen-Verantwortung

In Bezug auf die verschiedenen API Endpoints der in den Kapiteln 2.5.1.2 und 2.5.1.3 behandelten Schnittstellen bedeutet das, die Verantwortung über die jeweiligen Endpoints muss komplett entweder dem Consumer oder dem Provider des Behördengangs bzw. der

Geschäftsfallbearbeitung zugeteilt sein⁸⁴. Im Ergebnis der Diskussion im Fachausschuss wurde diese Frage zugunsten des Providers entschieden. Folglich gilt:

[REQ-51] Die Verantwortung über die Schnittstelle "Behördengang↔Geschäftsfallbearbeitung" (siehe 2.5.1.2) liegt beim jeweilig zuständigen behördeninternen Fachsystem.

[REQ-52] Die Verantwortung über die Schnittstelle zur Einbindung extern implementierter Behördengänge (siehe 2.5.1.3) liegt beim jeweiligen Provider-Portal.

In Verbindung mit den relevanten Standards stellt sich die Abhängigkeitsbetrachtung wie folgt dar:

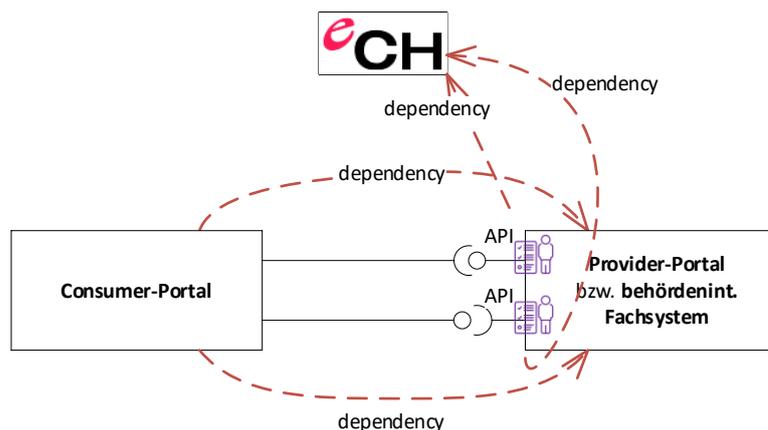


Abbildung 54: Eindeutige Abhängigkeiten zwischen den Systemen infolge Verantwortungsfestlegung und Standardisierung

Im Rahmen der Schnittstellenverantwortung sind u.a. folgende Dinge zu regeln:

[REQ-53] Bei der Umsetzung der Schnittstelle ist auf technischer Ebene ein Exception handling vorzusehen.⁸⁵

[REQ-54] Bei der Umsetzung der Schnittstelle zur Einbindung extern implementierter Behördengänge ist das "Right to forget" zu berücksichtigen. Das bedeutet z.B., dass eine Kontolöschung auf dem Consumer-Portal im Provider-Portal nachgeführt werden muss⁸⁶.

Abschliessend sei auf das Dokument API-Architektur Bund [34] verwiesen, welches u.a. die technischen und organisatorischen Gestaltungsoptionen für die Umsetzung einer API systematisiert. Die Schnittstelle "Behördengang↔Geschäftsfallbearbeitung" (siehe 2.5.1.2) stellt im Sinne der API-Architektur Bund einen klassischen Anwendungsfall für eine API dar.

⁸⁴ Schnittstellenrolle (agierend/reagierend) und Richtung Datenflusses spielen dabei keine Rolle.

⁸⁵ Beispielhaft sei auf Standard eCH-0090 2.0 [9] verwiesen, der dies für die Sedex-Kommunikation vorsieht.

⁸⁶ Dies gilt für jeden eingebundenen Behördengang. Wenn z.B. das Consumer-Portal einen Behördengang vom Provider-Portal A und einen Behördengang von einem anderen Provider-Portal B einbindet, dann ist eine Kontolöschung auf dem Consumer-Portal sowohl im Provider-Portal A als auch im Provider-Portal B nachgeführt werden.

2.5.2 ISDS-Themen

Bei der Integration einer Behördenleistung durch ein Behördenleistungsportal werden Informationen über die Grenzen der Behörde hinaus ausgetauscht und verarbeitet. Je nach Schutzbedarf der ausgetauschten Daten und der durch die Behörde zur Verfügung gestellten Behördenleistung müssen bestimmte Anforderungen an die Informationssicherheit und den Datenschutz erfüllt werden.

[REQ-55] Das Behördenleistungsportal muss sicherstellen, dass dem User und den Kunden, welche dieser vertritt, bei der Nutzung einer Behördenleistung ein angemessener IKT-Schutz gewährleistet wird.

2.5.2.1 Identifizierung des Schutzbedarfs

Der Schutzbedarf hängt im Wesentlichen von zwei Faktoren ab:

- Die vom Behördenleistungsportal integrierten Behördenleistungen und den entsprechenden Anforderungen an die Informationssicherheit und den Datenschutz der Behörde (Aussensicht) – siehe Exkurs hierzu in Kapitel 2.5.2.2
- Die vom Behördenleistungsportal selbst erhobenen, zu verarbeitenden und gespeicherten Daten des Users und die zur Verfügung gestellten Querschnittsfunktionen (Innensicht) – siehe Exkurs hierzu in Kapitel 2.5.2.3

[REQ-56] Bei der Integration einer neuen Behördenleistung (Aussensicht) und bei der Bereitstellung einer neuen Querschnittsfunktion (Innensicht) muss der Betreiber des Behördenleistungsportals beurteilen, ob es Veränderungen am Schutzbedarf gibt und die nötigen Massnahmen umsetzen.

Dies soll gemäss dem in der Schweiz üblichen Sicherheitsverfahren⁸⁷ erfolgen. Die Verantwortung für diesen Prozess wie auch für die Erstellung und Umsetzung eines allfälligen ISDS-Konzepts liegt beim Betreiber des Behördenleistungsportals.

[REQ-57] Der Betreiber muss zudem entscheiden, ob er individuelle ISDS-Anforderungen je Behördenleistung oder allgemeingültige ISDS-Anforderungen für alle integrierten Behördenleistungen umsetzen möchte.

2.5.2.2 Exkurs: ISDS-Anforderungen der Behörde

Es obliegt der Behörde, welche eine Behördenleistung zur Integration zur Verfügung stellt, die Bedingungen für die Integration seiner Behördenleistung in ein Portal zu definieren (vergleiche Anhang F, [Fokusbereich-2], Konzeption). Dazu zählen auch ISDS-Anforderungen an das Behördenleistungsportal (Aussensicht).

Die ISDS-Anforderungen hängen dabei u.a. von folgenden Faktoren ab:

- Art des Verfahrens: z.B. Meldung, Antrag, Anmeldung, Deklaration, Bewilligung

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

- Auszutauschende und zu verarbeitende Daten: z.B. Personendaten, öffentlich zugängliche Daten
- Kritikalität der Behördenleistung im Sinne der Verfügbarkeit

Die Behörde kann je Integrationsmuster unterschiedliche ISDS-Anforderungen stellen. Die folgende Tabelle gibt eine grobe Einschätzung darüber, ob erhöhte Anforderungen je nach Integrationsmuster benötigt werden.

Tabelle 19: Beurteilung ISDS-Risikofaktoren je nach Integrationsmuster

Risikofaktor	Bewertung und Anforderungen
Vertraulichkeit	<p>Aus Sicht der Vertraulichkeit ist die <i>Einbindung der Implementation</i> vorzuziehen.</p> <p>Im Fall der <i>Einbindung</i> werden durch das Consumer-Portal grundsätzlich nur die benötigten Benutzer- und Kundendaten dem Provider-Portal zur Verfügung gestellt, wo dann der Behördengang stattfindet. Umgekehrt kann das Provider-Portal lediglich Metadaten zum Behördengang zurückliefern, z.B. den Status des Behördengangs.</p> <p>Im Fall der <i>Implementation</i> müssen dem Consumer-Portal durch das behördeninterne Fachsystem alle relevanten Daten zur Verfügung gestellt werden, welche bei der Durchführung des Behördengangs anfallen (z.B. Ergebnisdokumente). Entsprechend müssen erhöhte Schutzanforderungen angewendet werden, sollten insbesondere besonders schützenswerte Personendaten übertragen werden. Mögliche Massnahmen sind die Verschlüsselung des Transportkanals oder der Daten, ein erhöhter LoA.</p> <p>Bei der Bestimmung der Anforderungen betreffend Vertraulichkeit sind ausserdem mögliche unterschiedliche Datenschutzbestimmungen zu berücksichtigen.</p>
Verfügbarkeit	<p>Aus Sicht der Verfügbarkeit ist die <i>Implementation der Einbindung</i> vorzuziehen.</p> <p>In beiden Fällen kann im Fall eines Ausfalls des durch den User genutzten Portals der Geschäftsfall trotzdem durch die Behörde, resp. durch das behördeninterne Fachsystem bearbeitet wird.</p> <p>Die Verfügbarkeit ist im Fall der Einbindung als geringer zu bewerten, weil sowohl das Consumer- wie auch das Provider Portal ausfallen können.</p>
Integrität	<p>In beiden Fällen (<i>Einbindung</i> und <i>Implementation</i>) muss die Echtheit, Korrektheit und Unversehrtheit der ausgetauschten Daten gewährleistet sein.</p> <p>Da im Fall der <i>Implementation</i> in der Regel auch Dokumente ausgetauscht werden, können die Auswirkungen bei nicht-Integrität der Daten als schwerwiegender beurteilt werden. Somit sollten erhöhte Massnahmen zum Schutz der Datenintegrität im Fall der Implementation vorgesehen werden.</p>

Nachvollziehbarkeit	In beiden Fällen müssen die Arbeitsvorgänge im Portal nachgewiesen werden können. Die Anforderungen an die Nachvollziehbarkeit unterscheiden sich je nach Integrationsmuster nicht.
---------------------	---

Welches Integrationsmuster aus ISDS-Sicht besser geeignet ist, hängt von der Gewichtung der Risikofaktoren ab. Eine allgemeine Empfehlung kann nicht ausgesprochen werden.

2.5.2.3 Exkurs: ISDS-Anforderungen an das Behördenleistungsportal

Unabhängig von den integrierten Behördenleistungen soll das Behördenleistungsportal gewisse allgemeingültige ISDS-Anforderungen erfüllen (Innensicht). Im Kapitel 2.2.2.8 wurden die im Rahmen dieser Studie erhobenen Bedürfnisse bezüglich ISDS beschrieben. Diese Bedürfnisse werden durch weitere Anforderungen ergänzt.

Tabelle 20: Anforderung an die ISDS

Anforderung	Beschreibung
Gewährleistung ISDS	Informationssicherheit und Datenschutz müssen gewährleistet werden.
Transparenz bezüglich Verwendung der Daten	Der Kunde soll sich informieren können, wo seine Daten liegen und welche Behördenstellen für welchen Zweck darauf zugreifen. Auch die Löschung der Daten muss gemäss den gesetzlichen Vorschriften gewährleistet sein.
Verfügbarkeit des Gesamtsystems	Das Behördenleistungsportal soll die Verfügbarkeitsziele erfüllen können (SLA). Im Falle von Integrationsmuster 2 (Einbindung) gilt das sowohl für das Provider als auch für das Consumer-Portal.
Sicherheit gesamtheitlich betrachten	Die Sicherheit soll nicht nur im Sinne der Technik / der Systeme betrachtet werden, sondern der Prozess selbst in seiner Abbildung über die Gesamtheit der Systeme (z.B. Was passiert nach einem Systemausfall?)
Datenschutzgesetzgebung (DSG) berücksichtigen	Der Austausch von Daten im Bereich des e-Government muss sich grundsätzlich an die geltende Datenschutzgesetzgebung halten. Auch die Pflicht zur Wahrung des Amtsgeheimnisses (Art. 320 StGB und Art. 22 Abs. 1 des Bundespersonalgesetzes) kann mit der Informationssicherheit verknüpft werden. Abhängig von den angebotenen Diensten können auch andere Geheimnisse betroffen sein. Die unterschiedlichen Datenschutzbestimmungen je nach Kanton sollen berücksichtigt werden (Compliance).
Nur benötigte Personendaten nutzen	Es sollen nur jene personenbezogenen Daten ausgetauscht und persistiert werden, welche für die Erfüllung des Behördengangs benötigt werden.
Keine Abschwächung LoA	Der vom integrierten Behördengang (bei Einbindung) oder Geschäftsfall (bei Implementation) geforderte Level of Assurance (LoA) darf durch das Consumer-Portal nicht abgeschwächt werden.

Nachvollziehbarkeit von Änderungen	Es sind Vorkehrungen zu treffen, dass die Daten vor, während und nach der Übertragung nur von dazu autorisierten Personen eingesehen und verändert werden können. Zur Nachvollziehbarkeit von Änderungen sind Werkzeuge, wie z.B. Audit-Trail einzusetzen.
Rechtssicherheit und Verbindlichkeit	Der Informationsaustausch zwischen Behörde und Kunde muss rechtssicher und verbindlich erfolgen. Dies erfolgt in der Regel über Verschlüsselung und Signierung.

Diese Anforderungen sollen bei der Standardisierung (siehe 2.5.1) berücksichtigt werden.

2.5.3 Rechtliche Fragen

Ein Behördenleistungsportal braucht keine fachspezifische Rechtsgrundlage, um eine Behördenleistung zu integrieren, da es nur ein Übermittlungssystem zur effektiv zuständigen Behörde ist. Durch das Portal wird weder die Geschäftsfallbearbeitung noch deren Zuständigkeiten verändert. Die fachspezifischen Rechtsgrundlagen kommen in der jeweils zuständigen Behörde zur Anwendung.

Allerdings muss das Behördenleistungsportal dem User transparent aufzeigen, dass aus technischen Gründen für den Leistungsbezug die Weitergabe gewisser Daten (insb. identifizierenden Nutzerdaten) an die verantwortliche Behörde notwendig ist. Dies muss in den Nutzungsbedingungen des Behördenleistungsportals explizit kommuniziert werden.

2.5.4 IT-Governance

Bisher haben wir in dieser Studie den Fokus auf die Entwicklung der Integrations-Sollarchitektur für Behördenleistungsportale gelegt. In diesem Kapitel widmen wir uns dem Management oder der Administration der Ressourcen, welche mit der Integrations-Sollarchitektur in Beziehung stehen: der IT-Governance.

2.5.4.1 IT-Governance im Kontext der Integrations-Sollarchitektur

Die IT-Governance im Kontext der Integrations-Sollarchitektur regelt den Umgang mit jenen Ressourcen (Personal, Prozesse, Infrastruktur, Information), welche einen Bezug zu systemübergreifenden Komponenten haben und für die Interoperabilität von Belang sind (gemäss Standardisierungsthemen 2.5.1.1 - 2.5.1.3). Dazu zählt ebenfalls die Integrations-Sollarchitektur, welche nach Bedarf weiterentwickelt werden soll.

[REQ-58] Die Digitale Verwaltung Schweiz (DVS) oder eine zu bestimmende Institution mit den nötigen Kompetenzen soll die Gesamtverantwortung für die IT-Governance und die Verantwortung für die strategische Ausrichtung (gemäss Anhang F, [Fokusbereich-1]) wahrnehmen. Die Verantwortung für andere Bereiche der IT-Governance und für die Erfüllung der entsprechenden Anforderungen kann die DVS an geeignete Partner oder Behörden delegieren.

[REQ-59] Im Rahmen der Standardisierungsarbeiten sollen die Anforderungen an die IT-Governance präzisiert und klare Verantwortlichkeiten für Teilbereiche definiert werden.

2.5.4.2 Anforderungen an die IT-Governance

Für die Herleitung der Anforderungen an die IT-Governance beziehen wir uns auf die 5 Fokusbereiche der IT-Governance:

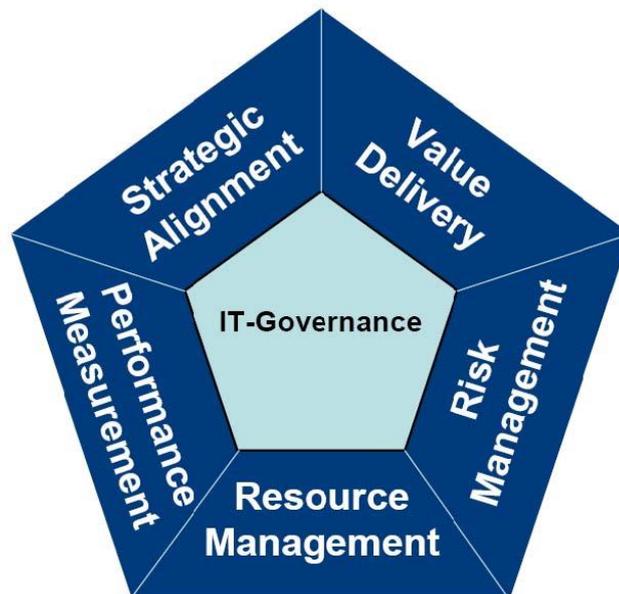


Abbildung 55: Fokusbereiche der IT-Governance

Im Rahmen von E-Government definieren wir die Fokusbereiche wie folgt:

- [Fokusbereich-1] *Strategic Alignment*: Sicherstellen, dass die E-Government Strategie berücksichtigt wird und E-Government Prinzipien, eCH-Standards und Rechtsgrundlagen angewendet werden
- [Fokusbereich-2] *Value Delivery*: Gewährleistung der Kontinuität der Leistungen mit einer hohen Wirtschaftlichkeit über den gesamten Life-Cycle, inklusive Weiterentwicklung der Integrations-Sollarchitektur.
- [Fokusbereich-3] *Risk Management*: Risikobewusstsein, -identifizierung, -messung, -bewertung, -überwachung und -minimierung sicherstellen, Fehlervermeidung fördern
- [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
- [Fokusbereich-5] *Performance Measurement*: Verfolgung und Überwachung der Leistungserbringung über den gesamten Life-Cycle

Im Anhang F werden Anforderungen zu den 5 Fokusbereichen ausformuliert.

2.6 Bedürfnisabdeckung

Die folgende Tabelle dient der Kontrolle und Nachvollziehbarkeit der Umsetzung der Bedürfnisse durch die Integrations-Sollarchitektur.

Tabelle 21: Verarbeitung und Umsetzung der Bedürfnisse aus Kapitel 2.2.2 bei der Entwicklung des Zielbilds in Kapitel 2.4 und der Sollarchitektur in Kapitel 2.5

Nr	Titel	Verarbeitung/Umsetzung
[B-1]	Systeminteroperabilität	Die in Kapitel 2.1.6 beschriebenen Integrationsmuster 1 (Implementation) und 2 (Einbindung) ermöglichen die Integration von Behördenleistungen auf verschiedenen Portalplattformen.
[B-2]	Dateninteroperabilität (standardisierter Datenaustausch)	Der Interoperabilitätsrahmen (siehe 2.5.1.1, insbesondere 2.5.1.1.5) bildet die Grundlage für den standardisierten Datenaustausch zwischen Leistungsportalen und behördeninternen Fachsystemen (A2B und A2C).
[B-3]	Angebot Basisdienste (E-Gov Infrastruktur)	Die Sollarchitektur postuliert IdPs und öffentlich verwaltete Register (UID-Register, UPI-Register und NAD) als Basisdienste. Siehe insbesondere [REQ-6]-[REQ-12], [REQ-39]-[REQ-40]
[B-4]	Metadaten-Verzeichnis (zentrales Verzeichnis digitaler Behördenleistungen samt Spezifikationen für die Integration)	[REQ-4] stützt sich auf das Behördenleistungsinventar gemäss eCH-0070 [27] ab. Die in Kapitel 2.5.1.2 spezifizierte Schnittstelle Behördengang↔ Geschäftsfallbearbeitung bildet die Grundlage für das Angebot einer Behördenleistung in Form einer API. Ein zentrales API-Verzeichnis thematisiert die Sollarchitektur nicht, da das bereits Gegenstand von UZ14 ist.
[B-5]	Integration bestehender Systeme ohne Impact auf andere Systeme	Die in Kapitel 2.5.1.5 definierte Schnittstellenverantwortung auf Provider-Seite schafft eindeutig gerichtete Abhängigkeiten zwischen den beteiligten Systemen und beugt somit unkontrollierbare Seiteneffekten vor.
[B-6]	Single sign on (für mehrere Behördenleistungen, evtl. über verschiedene Systeme / mehrere Kunden NP/JP)	Der Interoperabilitätsrahmen (siehe 2.5.1.1) bildet insbesondere durch das Informationsmodell die Grundlage für das geforderte SSO in Bezug auf mehrere Kundenkonten. Dies ermöglicht das in Kapitel 2.5.1.3.1 spezifizierte SSO. Siehe auch [REQ-1], [REQ-2], [REQ-16], [REQ-39]
[B-7]	Mehrere Identitäten verwendbar	Ist gegeben, wenn das jeweilige Portal einen Vermittler verwendet (liegt in der Verantwortung des betreffenden Portalbetreibers). Für den Interoperabilitätsrahmen (siehe 2.5.1.1) ist es unerheblich, ob dies der Fall ist oder nicht.
[B-8]	LoA differenziert (nicht mehr als für die Behördenleistung nötig)	siehe [REQ-19], [REQ-42]
[B-9]	Elektronische Signatur (via LoA oder explizit)	Signatur mit (Mindest-) Login-LoA verknüpft: siehe [REQ-19], [REQ-42]

Nr	Titel	Verarbeitung/Umsetzung
		explizit ⁸⁸ : Signatur ist an das/den zu signierende/n elektronische Dokument oder Datensatz gebunden.
[B-10]	Bewirtschaftungsrechte selbst verwalten (Kunde)	Wird durch [REQ-20], [REQ-21], [REQ-22] unterstützt. Die Integrations-Sollarchitektur geht von einer dezentralen Verwaltung der Bewirtschaftungsrechte aus. D.h., deren Vergabe geschieht lokal im betreffenden Portal. Im Falle der Kontextsynchronisation (siehe Kapitel 2.5.1.3.2) wird das jeweilige Bewirtschaftungsrecht vom Consumer zum Provider temporär durchgereicht.
[B-11]	Standardisierte Vollmacht	siehe [REQ-23]
[B-12]	Einfache Kontaktaufnahme mit Behörde	Wird von der Definition der Schnittstelle "Behörden-gang↔Geschäftsfallbearbeitung" (siehe Kapitel 2.5.1.2) unterstützt, siehe insbesondere [REQ-24] und Abbildung 37
[B-13]	Sichere und rechtsverbindliche Kommunikation Behörde – Kunde	Der Aspekt ist im Kapitel 2.5.2.3 (ISDS) berücksichtigt. Betrifft vor allem den Datenverkehr über die Schnittstelle "Behörden-gang↔Geschäftsfallbearbeitung" (siehe Kapitel 2.5.1.2)
[B-14]	Sicht auf Behördenleistungen personalisieren	Die diesbezügliche Funktionalität ist Portal-spezifisch und liegt im Verantwortungsbereich des jeweiligen Portalbetreibers. Im Falle des Integrationsmusters 2 (Einbindung) wird die Übertragbarkeit der wichtigsten Benutzereinstellungen durch den Interoperabilitätsrahmen - insbesondere [REQ-17], [REQ-18] – unterstützt.
[B-15]	Hilfe in der Vielfalt von Behördenleistungen (+ leistungsübergreifend einheitliches Vokabular)	Dieser Aspekt wurde in [Herausforderung-6] analysiert. Die Umsetzung des Bedürfnisses fällt in die Zuständigkeit von UZ6/UZ7.
[B-16]	Behördenleistungen von einem Einstiegspunkt zugänglich	Die Integrationsmuster 1 und 2 bzw. die Standardisierungsthemen (siehe Kapitel 2.5.1) bilden die Grundlage für den Aufbau von behördenübergreifenden Portalen, die auf dedizierte Kundensegmente fokussieren.
[B-17]	Once-Only	Für den interoperablen Datenkern der leistungsübergreifenden Entitäten (siehe [REQ-3] und Abbildung 33) gewährleistet, darüber hinaus nicht.
[B-18]	Transparenz der Geschäftsfallbearbeitung	Wird durch den Interoperabilitätsrahmen bezüglich der Prozessmetadaten (siehe Kapitel 2.5.1.1.5) von

⁸⁸ Dieser Teil des Bedürfnisses zielt auf einen Aspekt ausserhalb des Scopes der Studie

Nr	Titel	Verarbeitung/Umsetzung
		den spezifizierten Schnittstellen (siehe Kapitel 2.5.1.2 und 2.5.1.3), speziell durch die übermittelten Statusinformationen unterstützt.
[B-19]	Auch klassisch angestossene Geschäftsfälle verfolgbar	Wird von der Schnittstelle "Behördengang↔Geschäftsfallbearbeitung" (siehe Kapitel 2.5.1.2), speziell [REQ-30] unterstützt.
[B-20]	Medienbruchfreie Geschäftsabwicklung	Wird von der Schnittstelle "Behördengang↔Geschäftsfallbearbeitung" (siehe Kapitel 2.5.1.2), insbesondere [REQ-24] unterstützt.
[B-21]	Geführter Prozess (Geschäftsfälle möglichst schweizweit einheitlich)	<p>Ausschluss: Fachaspekte wie der Wunsch nach schweizweit einheitlicher Prozessführung betrifft die Gestaltung eines Behördengangs. Dies fällt jedoch in den Verantwortungsbereich eines einzelnen Behördenportals, welcher ausserhalb des Scopes der Integrations-Sollarchitektur liegt.</p> <p>Ungeachtet dessen ermöglicht das Integrationsmuster 2 (Einbindung) (siehe Kapitel 2.1.6) die Nachnutzung einer bestehenden Behördengang-Implementation, was dem Bedürfnis nach Einheitlichkeit entgegenkommt.</p>
[B-22]	Angebot für Unternehmen ohne UID	Dieses Bedürfnis ist mit den bestehenden Möglichkeiten des UID-Registers bereits abgedeckt. Alle bestehenden Unternehmen erhalten entweder automatisch eine solche (Unternehmen, die im Handelsregister eingetragen sind) oder können eine solche beantragen (ausländische Unternehmen), siehe Kapitel 2.5.1.1.4.1.
[B-23]	Behörde behält Kontrolle über Behördenleistung	Dem Prinzip wird durch die Regelung der Schnittstellenverantwortlichkeit (siehe Kapitel 2.5.1.5) auf Ebene der Integrations-Sollarchitektur entsprochen.
[B-24]	Proaktive Erkennung des Kundenbedarfs durch das Behördenleistungsportal	<p>Hierbei ist zu unterscheiden:</p> <p>A) Externes Ereignis triggert ein Kundenanliegen, in deren Kontext der Kunde eine Behördenleistung in Anspruch nehmen möchte/muss.</p> <p>B) Externes Ereignis triggert proaktives Handeln der Behörde, das eine Information/Aufforderung/.. an bestimmte Kunden einschliesst.</p> <p>Fall A ist primär im Informationslayer abzuholen. Das betreffende Kundenanliegen wird im Interoperabilitätsrahmen berücksichtigt (siehe 2.5.1.1.3) und über die Schnittstellen kommuniziert (siehe [REQ-26] und [REQ-44]).</p> <p>Fall B wird von der Definition der Schnittstelle "Behördengang↔Geschäftsfallbearbeitung" (siehe</p>

Nr	Titel	Verarbeitung/Umsetzung
		Kapitel 2.5.1.2) unterstützt, siehe insbesondere Abbildung 37.
[B-25]	Gewährleistung ISDS	Wird im Kapitel 2.5.2 behandelt, welches die nötigen Requirements spezifiziert.
[B-26]	Transparenz bezüglich Verwendung der Daten	Dieses Thema fällt in den Zuständigkeitsbereich von UZ13 (siehe [19]) und ist deshalb in der Studie nicht weiter thematisiert.
[B-27]	Verfügbarkeit des Gesamtsystems	Wird im Kapitel 2.5.2.3 behandelt, welches die nötigen Requirements spezifiziert.
[B-28]	Wirtschaftlichkeit	Die spezifizierten Standardisierungsthemen (siehe 2.5.1) vereinfachen die Komplexität der Abbildung von Behördenleistungen auf Portalen und tragen somit zu einer höheren Wirtschaftlichkeit bei.
[B-29]	Weiterentwicklungsqualität	Die spezifizierten Standardisierungsthemen (siehe 2.5.1) vereinfachen die Komplexität der Abbildung von Behördenleistungen auf Portalen und tragen somit zu einer höheren Weiterentwicklungsqualität bei. Darüber hinaus ist in Kapitel 2.5.4 die nötige Governance auf.

2.7 Empfehlungen für das weitere Vorgehen

Die in dieser Studie entwickelte Integrations-Sollarchitektur für Behördenleistungsportale soll schrittweise umgesetzt werden. Die folgende Umsetzungs-Roadmap zeigt einen möglichen Weg hierfür auf.

2.7.1 Umsetzungs-Roadmap

Die Umsetzung der Standardisierung für die Interoperabilität von Behördenleistungsportalen soll etappiert erfolgen.

Prinzipien der Roadmap

- Die Etappen bauen aufeinander auf und sollen eine umsetzbare Grösse haben, damit erste Standards und darauf basierende Implementierung schnell verfügbar gemacht werden können.
- Die Standardisierung der Kontextsynchronisation beim Integrationsmuster 2 (Einbindung) soll in 4 Etappen gemäss folgender Priorisierung erfolgen:
 1. Userkonto (Identifikation des Users, Benutzerprofil, LoA) und Identifikation Kunde
 2. Bewirtschaftungsrecht
 3. Rückkanal für Status des Behördengangs und behördliche Benachrichtigungen
 4. Rückkanal für Dokumente

Die Standardisierung der Schnittstellen für das Integrationsmuster 1 (Implementierung) kann parallel zu den Etappen 1 und 2 erfolgen. Es soll in beiden Fällen wo immer möglich auf bestehende eCH-Standards aufgebaut werden.

- Der Zugang zu Register wird in der Roadmap nicht thematisiert, da die entsprechenden Schnittstellen bereits bestehen (z.B. UPI, UID) oder am Entstehen (z.B. NAD) sind.
- Das SECO war für die Erstellung der Integrations-Sollarchitektur und für diese Studie federführend. Für die Erarbeitung der benötigten Standards und die Umsetzung in Abstimmung mit Behörden und anderen Partnern soll die DVS federführend sein.

Peer-to-Peer Trust Schnittstellenarchitektur

In einem ersten Schritt soll ein Peer-to-Peer Trust Ansatz für die Kontextsynchronisation zwischen Consumer- und Provider-Portal berücksichtigt werden. Gleichzeitig soll ein bilaterales Vertrauensverhältnis zwischen den Integrationspartnern auf Basis einer schweizweit einheitlichen Vereinbarung geschaffen werden. Die Vorteile von diesem Vorgehen sind eine erleichterte Umsetzung mit relativ hohen Freiheitsgraden auf Seite der Portale und verhältnismässig geringen Risiken, da auf grösstenteils bestehenden Implementierungen aufgebaut werden kann.

Mögliche Ausbauschritte

Nach Umsetzung der erwähnten 4 Etappen zur Standardisierung und weiterer notwendiger, inhaltlicher Entscheide könnten z.B. weitere Ausbauschritte in Betracht gezogen werden. Das Ziel eines ersten Ausbauschritts kann die Eliminierung von bilateralen Vereinbarungen durch die Einführung einer staatlichen Prüfstelle für die Zertifizierung von Ausstellern digitaler Identitäten und Bewirtschaftungsrechten (siehe Ausführungen jeweils im letzten Teil von Kapitel 2.5.1.3.1 und 2.5.1.3.2 sowie Abbildung 47) und demzufolge ein vereinfachter Integrationsprozess sein. In einem weiteren möglichen Ausbauschritt können zentrale Infrastrukturkomponenten eingeführt werden (z.B. zentraler Vermittler von User-Identitäten, zentrale IAM-Komponente), um die Anzahl der Schnittstellen insgesamt zu verringern und die Wiederverwendbarkeit von Systemen zu erhöhen. Sobald eine staatlich regulierte E-ID zur Verfügung stehen wird, kann diese komplementär zu anderen digitalen Identitäten genutzt werden – dies im Sinne eines verbesserten Once-Only Prinzips.

Die Umsetzungs-Roadmap kann wie folgt zusammenfassend dargestellt werden (Vergrösserte Darstellung im Querformat in Anhang D):

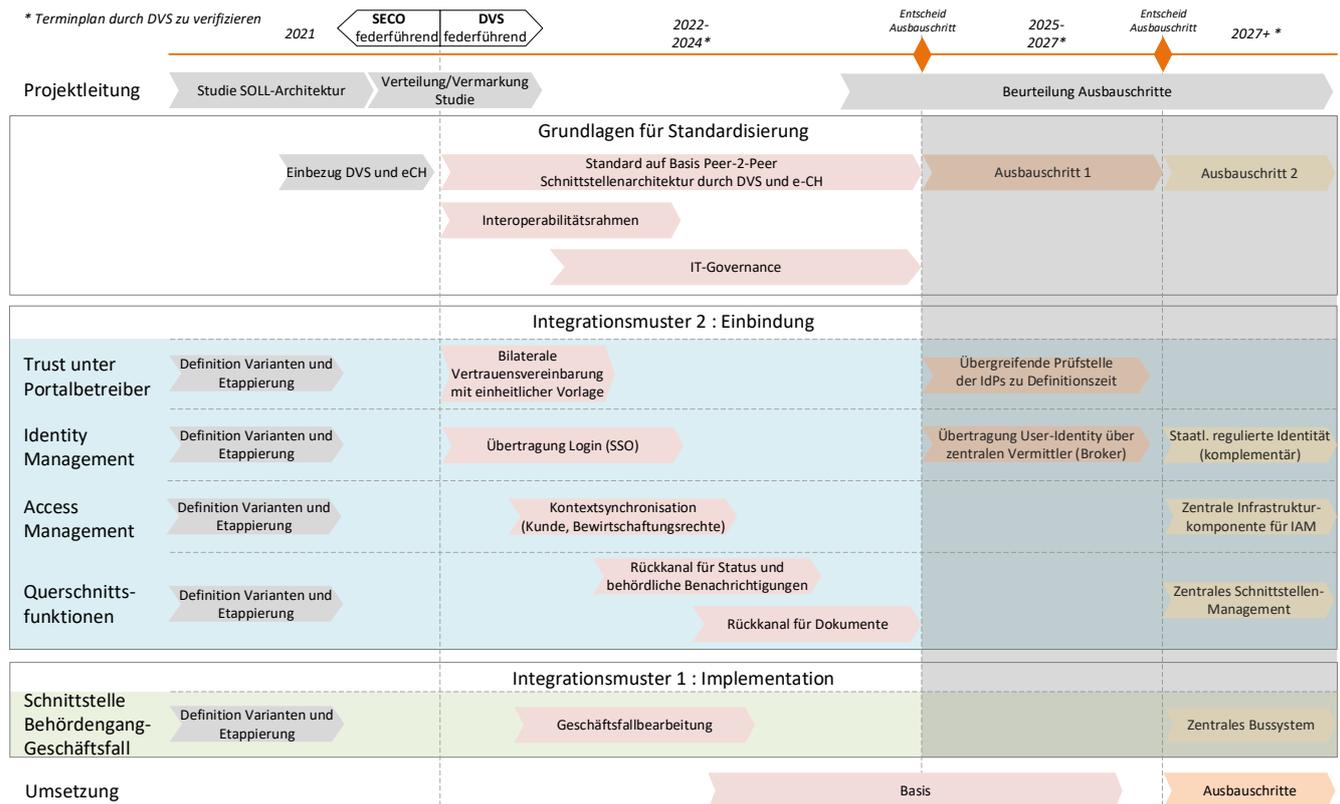


Abbildung 56: Roadmap zur Umsetzung der Standardisierung

Das SECO als Auftraggeber dieser Studie beteiligt sich an der DVS-Ambition «Behördenübergreifende digitale Identifikation ist etabliert» (siehe Grundlagenbericht [37]) und liefert mit der Studie einen wichtigen Input.

2.7.2 Handlungsempfehlungen

Für die Umsetzung der Integrations-Sollarchitektur in Form eines oder mehrerer Standards soll die Organisation «Digitale Verwaltung Schweiz» (DVS) federführend sein. Die DVS wird zur Steuerung der digitalen Transformation im föderalistischen System geschaffen. Sie fördert die digitale Transformation der Verwaltungen in der Schweiz und ist als politische Plattform mit Standardentwicklung konzipiert⁸⁹. Sie übernimmt die Aufgaben von E-Government Schweiz und der Schweizerischen Informatikkonferenz (SIK).

Handlungsempfehlungen zuhanden der DVS und anderen Akteuren:

Tabelle 22: Empfohlene Massnahmen unter Verantwortung SECO

Massnahme	Ergebnis
Distribution der Studie an interessierte Behörden	-

⁸⁹ «Politische Plattform mit Standardentwicklung» gemäss Schlussbericht vom Oktober 2019 (<https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-76798.html>) sowie den Beschlüssen der Plenarversammlung der KdK vom 27.03.2021 und des Bundesrates vom 03.04.2021.

Gap-Analyse Integrations-Sollarchitektur vs. easyGov Integrationen mit konkreten Use-Cases (z.B. ausländerrechtliche Arbeitsbewilligungen)	Studie Version 2.0
Lösungsvorschläge für die identifizierten Gaps erarbeiten	Studie Version 2.0

Tabelle 23: Empfohlene Massnahmen unter Verantwortung DVS

Massnahme	Ergebnis
Prüfung der Umsetzungs-Roadmap	Ergänzung der Roadmap und Einleitung erster Massnahmen.
Initialisierung Arbeitsgruppe 'Standardisierung'	Steuerung und Abstimmung mit Partnern hinsichtlich der Etablierung oder Ergänzung eines oder mehrerer Standards für interoperable Behördenleistungsportale.
Erarbeitung eines Standards oder mehrerer Standards für interoperable Behördenleistungsportale (Peer-to-Peer Trust)	eCH-Standards Berücksichtigung der Kundenzentrierung inkl. Aufbau eines Behördenleistungsverzeichnis auf allen föderalen Ebenen.
Initialisierung Arbeitsgruppe 'Recht'	Schaffung der Rechtsgrundlagen hinsichtlich einer Behördenübergreifenden Integration von Behördenleistungen über alle föderalen Ebenen hinweg. Fokus auf Datenschutzbestimmungen. Konkretisierung der rechtlichen Voraussetzungen für den Zugang zu Register und Basisdiensten (z.B. UPI, NAD) Klärung der Möglichkeiten zur Verbindlicherklärung eines Standards.
Erarbeitung standardisierte juristische Vollmacht	Standardisierte juristische Vollmacht, welche durch den Kunden nur einmal für einen bestimmten User für alle interoperablen Behördengänge erteilt werden muss.
Initialisierung Pilotprojekte mit Einbezug von Behörden auf allen föderalen Ebenen (z.B. iGovPortal, EasyGov, UVEK, ePortal)	Umsetzung der Standardisierungsarbeiten
Präzisierung der IT-Governance	Leitfaden für die IT-Governance Klärung der Verantwortlichkeiten (RACI) und Definitivonshoheit Präzisierung der Anforderungen
Regelmässige Evaluation des Standardisierungsbedarfs und allfällige	Empfehlung betr. Ausbausschritt

Umsetzung von Ausbausritten (gemäss Umsetzungs-Roadmap)	
---	--

3 Gapanalyse Ist-Architektur EasyGov bezüglich Integrations-Sollarchitektur

In einer zweiten Version dieser Studie wird beurteilt, welche Anpassungen an EasyGov notwendig sind, um der Integrations-Sollarchitektur gerecht zu werden (Gap-Analyse).

3.1 Identifizierte Gaps

Die Gaps werden in der 2. Version dieser Studie identifiziert.

3.2 Grobplanung zur Gap-Beseitigung

Die Grobplanung erfolgt im Rahmen der 2. Version.

4 Anhänge

Anhang A Glossar

Begriff	Definition / Erläuterung
Back-End und Front-End	<p>Die Begriffe <i>Front-End</i> und <i>Back-End</i> werden in der Informationstechnik in Verbindung mit einer Schichteneinteilung verwendet. Es gilt prinzipiell, dass das <i>Front-End</i> näher an der Eingabe durch den User (UI) und das <i>Back-End</i> näher an der Verarbeitung ist. Siehe auch https://de.wikipedia.org/wiki/Front-End_und_Back-End</p> <p>Hinweis: Die Unterscheidung zwischen den logischen Schichten Back- und Front-End ist nicht dasselbe wie die technische Differenzierung zwischen Client und Server. Sowohl Front- als auch Back-End können jeweils Client- und Serverkomponenten haben.</p>
Behörde	<p>Öffentlich-rechtlich begründete Organisation, welche hoheitliche Staatsaufgaben der Schweiz wahrnimmt. <i>Behörden</i> können auf Ebene von Gemeinde, Kanton oder Bund existieren und zur Legislative, Exekutive oder Judikative gehören.</p> <p>Siehe auch Tabelle 1 in Kapitel 2.1.5</p>
Behörden-gang	<p>Der <i>Behördengang</i> ist ein Prozess, der aus der <i>Kundensicht</i> alle Aktivitäten und Verfahrensschritte umfasst, die zum Bezug einer <i>Behördenleistung</i> erforderlich sind. Er widerspiegelt die Sicht des Leistungsbezügers auf das behördliche Verwaltungsverfahren. Die Prozessschritte verhalten sich komplementär zu denen der <i>Geschäftsfallbearbeitung</i> auf <i>Behördenseite</i>.</p> <p>Siehe auch Tabelle 1 in Kapitel 2.1.5</p>
Behördenin-ternes Fachsystem	<p>Eine oder mehrere <i>Fachanwendungen</i>, welche die <i>Geschäftsfallbearbeitung</i> von ein oder mehreren <i>Behördenleistungen</i> innerhalb einer <i>Behörde</i> unterstützen. Benutzer sind ausschliesslich Mitarbeitende der jeweiligen Behörde.</p> <p>Aus Sicht eines <i>Behördenleistungsportals</i> stellt das <i>behördeninterne Fachsystem</i> ein Umsystem dar.</p> <p>Siehe auch Tabelle 1 in Kapitel 2.1.5</p>
Behörden-leistung	<p>Öffentliche Verwaltungsleistung (A2A, A2B oder A2C-Tätigkeit), die eine Behörde im Rahmen ihrer Zuständigkeit gemäss staatlichem Auftrag für den <i>Kunden</i> (NP oder JP) anbietet. Die Inanspruchnahme erfolgt durch einen kundenseitigen <i>Behördengang</i>, die Leistungserbringung durch die behördenseitige <i>Geschäftsfallbearbeitung</i>.</p> <p>Siehe auch Tabelle 1 in Kapitel 2.1.5</p>
Behörden-leistungsportal	<p>Öffentlich zugängliche Applikation (z.B. Single Page Application, mobile App, etc.), mit der der <i>Portalbetreiber</i> im Rahmen des E-Governments dem <i>Kunden</i> einen digitalen Zugangskanal für ein oder mehrere <i>Behördenleistungen</i> bietet. Es stellt das <i>Kunden-Front-End</i> für digitale <i>Behördenleistungen</i> dar, welches von entsprechend bevollmächtigten <i>Usern</i> bedient wird.</p> <p>Siehe auch Tabelle 1 in Kapitel 2.1.5</p>

behördliche Benachrichtigung	<p>Mitteilung <i>Behörde</i> → <i>Kunde</i>, zum Beispiel:</p> <ul style="list-style-type: none"> • Bearbeitungsstatus eines <i>Geschäftsfalls</i> • Rückfrage nach weiteren Belegen • Reminder zur Wahrung einer Frist <p>Im Anhang C ist eine vom ePortal übernommene detaillierte Systematisierung von behördlichen Benachrichtigungen aufgeführt.</p>
Bewirtschaftungsrecht	<p>Das <i>Bewirtschaftungsrecht</i> bildet eine <i>Vollmacht</i> ab, die im juristischen Sinne einen Vertreter zu Handlungen im Namen des Rechtssubjekts – d.h. dem <i>Kunden</i> - legitimiert. Auf dem <i>Behördenleistungsportal</i> ermächtigt diese <i>Vollmacht</i> einen <i>User</i> das betreffende <i>Kundenkonto</i> zu bewirtschaften und dabei <i>Behördengänge</i> für eine bestimmte <i>Behördenleistung</i> zu vollführen, wobei die Berechtigung abgestuft erfolgen kann (z.B. Einsicht, Bearbeiten, Einreichen, Superuser).</p> <p>Die Erteilung und Verwaltung der <i>Bewirtschaftungsrechte</i> obliegen der Verantwortung des <i>Kunden</i> bzw. dem von ihm dazu ermächtigten Vertreter. Es muss das Ziel sein, eine standardisierte juristische Vollmacht zu erarbeiten und anzubieten, welche durch den Kunden nur einmal für einen bestimmten User für alle interoperablen Behördengänge erteilt werden muss.</p> <p>Siehe auch Tabelle 1 in Kapitel 2.1.5</p>
Datenhoheit	<p>Führende Rolle einer Institution im Datenmanagement. Das von dieser Institution dafür verwendete System ist das führende System (wie z.B. staatliche Register) für die betreffenden Daten. Nur im führenden System dürfen diese Daten verändert werden, alle anderen beteiligten Systeme übernehmen diese.</p>
Definitionshoheit	<p>Verantwortlichkeit über die Definition von Vorgaben, Regeln oder Schnittstellen o.ä., die zur <i>Laufzeit</i> zur Anwendung kommen. Die <i>Definitionshoheit</i> wird zur <i>Definitionszeit</i> ausgeübt.</p>
Definitionszeit	<p>Zeitspanne in der ein IT-System oder eine Vorgabe – wie z.B. ein kontrolliertes Vokabular - entwickelt, eingerichtet und konfiguriert wird und folglich noch nicht produktiv bzw. verbindlich ist.</p>
Digitale Identität	<p>Mit einem elektronischen Identitätsnachweis verbundene Repräsentation einer natürlichen Person in der digitalen Welt, welche von <i>Identitäts Providern</i> ausgestellt und verwaltet werden. Eine <i>digitale Identität</i> ermöglicht den Zugang zu <i>Portalen</i>. <i>Identitätsprovider</i> kann auch das <i>Portal</i> selbst sein.</p>
Elektronische Identität	<p>Synonym von <i>Digitale Identität</i></p>
Fachanwendung	<p>Eine <i>Fachanwendung</i> bildet Geschäftsprozesse ab und verwaltet typischerweise Daten oder Informationen, die einen geschäftlichen Wert darstellen.</p>
Front-End	<p>Siehe <i>Back-End</i></p>

Geschäftsfall (-bearbeitung)	<p>Prozess, der infolge eines <i>Behördengangs</i> (d.h. bei Bezug einer <i>Behördenleistung</i> durch den <i>Kunden</i>) in der zuständigen Behörde ausgelöst wird. Die <i>Geschäftsfallbearbeitung</i> umfasst alle Aktivitäten und Verfahrensschritte, die aus behördlicher Sicht zur Erbringung einer <i>Behördenleistung</i> erforderlich sind. Sie widerspiegelt die Sicht des Leistungserbringers auf das Verwaltungsverfahren. Die Prozessschritte verhalten sich komplementär zu denen des <i>Behördengangs</i> auf <i>Kundenseite</i>.</p> <p>Siehe auch Tabelle 1 in Kapitel 2.1.5</p>
Geschäftspartner	<p>Im SAP-Umfeld gebräuchlicher Begriff, welcher gemäss SAP Help Portals 'juristische oder natürliche Personen, mit denen Ihre Firma geschäftliche Beziehungen unterhält' umfasst. Im Falle von <i>Behördenleistungen</i> ist <i>Geschäftspartner</i> gleichbedeutend mit <i>Kunde</i> resp. als Synonym zu werten.</p>
Geschäftspartnerverwaltung	<p>Synonym von <i>Kundendatenverwaltung</i></p>
Identifikator	<p>Eine maschinell verarbeitbare Zeichenkette, welche ein Entitäts- bzw. Geschäftsobjekt innerhalb eines Namensraumes eindeutig bezeichnet. Beispiel Kundenidentifikator:</p> <ul style="list-style-type: none"> • JP-Kunde → UID • NP-Kunde → Versichertennummer (AHV-Nummer)
Identitätsprovider (IdP)	<p>Herausgeber und Verwalter von <i>digitalen Identitäten</i>. Ein <i>IdP</i> stellt einen Authentication Service zur Verfügung und fungiert für <i>Behördenleistungsportale</i> als Zugangssystem. Beispiele:</p> <ul style="list-style-type: none"> • CH-Login (eIAM-Bund) • FED-Login (eIAM-Bund) • BE-Login (Kanton Bern) • E-ID (zukünftige staatlich regulierte elektronische Identifizierungsmöglichkeit auf gesetzlicher Grundlage [23] und Diskussionspapier zum «Zielbild E-ID» [36])
Informationslayer	<p>Funktionsbereich eines <i>Behördenleistungsportals</i>, der dem <i>User</i> einen Überblick über die verfügbaren <i>Behördenleistungen</i> (Leistungsangebot) gibt und zur benötigten <i>Leistung</i> führt.</p> <p>Siehe auch Tabelle 1 in Kapitel 2.1.5</p>
Integrationsmuster	<p>Die Integrationsmuster «Implementation» und «Einbindung» sind Funktionsweisen, wie Behördenleistungsportale extern vorhandene Leistungen integrieren (siehe Kapitel 2.1.6).</p> <p>Bei der Implementation wird der Behördengang für eine bestimmte Leistung vollständig im Portal abgebildet. Es wird dazu auch der Begriff «Vollintegration» verwendet.</p>

	Bei der Einbindung wird eine bestehende Implementation von einem externen System durch Nachnutzung eingebunden. Es werden dazu auch die Begriffe «Teilintegration» oder «Absprung» verwendet.
Kunde	Rechtssubjekt, für die eine <i>Behördenleistung</i> in Anspruch genommen wird. Dies ist entweder eine juristische oder eine natürliche Person (oder eine Gruppe dessen), welche gemäss gesetzlicher Grundlage Verpflichtung oder Anspruch auf eine <i>Behördenleistung</i> hat. Siehe auch Tabelle 1 in Kapitel 2.1.5
Kundenanliegen	Ein Kundenanliegen bezeichnet den Grund bzw. den Auslöser, weshalb eine <i>Behördenleistung</i> bezogen wird. Im Falle von NP-Kunden spricht man hierbei auch von «Lebenslage», im Fall von JP-Kunden auch von «Geschäftssituation», siehe eCH-0126 [14] und eCH-0138 [15]. Siehe auch Tabelle 1 in Kapitel 2.1.5
Kundendatenverwaltung	Funktionsbereich zum Anlegen/Registrieren, Ändern oder Löschen eines <i>Kundenkontos</i>
Kundenkonto	Abbildung von <i>Kunde</i> im <i>Portal</i> . Neben dessen Stammdaten werden im Kontext des <i>Kundenkontos</i> behördliche <i>Benachrichtigungen</i> , <i>Behördengänge</i> und <i>Bewirtschaftungsrechte</i> geführt.
Kundenstammdatenverwaltung	Synonym von <i>Kundendatenverwaltung</i>
Laufzeit	Zeitspanne in denen die Systeme gemäss ihrer Bestimmung produktiv "leben".
Leistung	Kurzwort von <i>Behördenleistung</i>
LoA (Level of Assurance)	Dieser Begriff steht für die Sicherheitsstufen der Authentifizierung für E-Government-Transaktionen. Diese beschreiben den Grad der Gewissheit, ob der Benutzer tatsächlich die Person ist, für deren Identität er sich ausgibt. Der Standard eCH-00170 [21] definiert folgendes Stufenmodell für den LoA des Logins: <ul style="list-style-type: none"> • Stufe 1: Wenig oder kein Vertrauen in die Gültigkeit der behaupteten Identität. • Stufe 2: Ein gewisses Vertrauen in die Gültigkeit der behaupteten Identität. • Stufe 3: Hohes Vertrauen in die Gültigkeit der behaupteten Identität. • Stufe 4: Sehr hohes Vertrauen in die Gültigkeit der behaupteten Identität. Die Inanspruchnahme von <i>Behördenleistungen</i> ist in der Regel an ein bestimmtes <i>LoA</i> -Niveau gebunden.
Orchestrierung	Kombination von mehreren <i>Behördenleistungen</i> zu einem Gesamtpaket mit dem Ziel, bezüglich eines <i>Kundenanliegens</i> relevante <i>Leistungen</i> zu bündeln.

	<i>Orchestrierung</i> bedeutet insbesondere, dass das <i>Portal</i> den <i>User</i> über die betreffenden <i>Behördenleistungen</i> führt, indem es die nötigen <i>Behördengänge</i> aneinanderreicht (z.B. in einem Wizard) oder auf Querverbindungen anbietet (z.B. vorausgehende Stellenmeldepflicht bei Gesuch auf Arbeitsbewilligung Drittstaatsangehörige).
Plattform	Synonym von <i>Behördenleistungsportal</i>
Portal	Kurzwort von <i>Behördenleistungsportal</i>
Portal-Fachanwendung	Über ein <i>Behördenleistungsportal</i> zugängliche <i>Fachanwendung</i> , welche für ein- oder mehrere <i>Behördengänge</i> abbildet (siehe Abbildung 13 Kapitel 2.1.3).
Portalbetreiber	Unternehmen oder Organisation, welche/s als Leistungserbringer/Service Provider der <i>Behörde</i> als Leistungsbezüger ein <i>Behördenleistungsportal</i> zur Verfügung stellt. Siehe auch Tabelle 1 in Kapitel 2.1.5
Querschnittsfunktion	Sammelbegriff für allgemeine <i>Portalfunktionen</i> die sowohl im <i>Informations-</i> als auch im <i>Transaktionslayer</i> zur Anwendung kommen. Siehe auch Tabelle 1 in Kapitel 2.1.5
Register	Amtliches Verzeichnis, in dem eine systematische Sammlung und Identifikation über eine Gruppe von Objekten (z.B. Unternehmen) erfolgt.
Transaktionslayer	Das umfasst sowohl den kundenseitigen <i>Behördengang</i> im Portal als auch die behördenseitige <i>Geschäftsfallbearbeitung</i> im <i>behördeninternen Fachsystem</i> . Siehe auch Tabelle 1 in Kapitel 2.1.5
User	Natürliche Person, welche das <i>Behördenleistungsportal</i> über das UI aktiv benutzt und dabei <i>Behördengänge</i> für einen bestimmten <i>Kunden</i> vollführt. Siehe auch Tabelle 1 in Kapitel 2.1.5
Userkonto	Abbildung von <i>User</i> im <i>Portal</i> . Neben dessen Stammdaten werden im Kontext des <i>Userkontos</i> Credentials, Einstellungen (z.B. Sprache) verwaltet.
Vermittler	Infrastrukturdienst, der einem Behördenleistungsportal ermöglicht, digitale Identitäten verschiedener IdPs zu nutzen. Der Vermittler kapselt die verschiedenen IdPs und tritt selbst vor dem Portal als IdP auf. Gemäss eCH-0107 [10] bietet ein Vermittler gemeinsame Dienste, wie Metadatenverwaltung, IdP-Discovery, Identity Linking oder Transformation der Authentifizierungs- und Attributbestätigung, für alle anderen IAM-Dienstanbieter und Relying Parties in einer Identity Federation an. Ein Vermittler kann optional einen CSP enthalten. Weiterhin sei auf die eCH-Standards 0224 [31] und 0225 [32] verwiesen, welche eine vermittlerbasierte Identity Federation näher detaillieren.
Vollmacht	Juristische Grundlage für die Erteilung eines <i>Bewirtschaftungsrechts</i>
zustandslos	Eine zustandslose Komponente "vergisst" sämtliche Daten der Transaktion nach Eingabe/Verarbeitung/Ausgabe. Sie enthält nur die Geschäftslogik für

	die Transaktion und macht keine Datenhaltung. Siehe auch https://de.wikipedia.org/wiki/Zustandslosigkeit
--	---

Anhang C Systematisierung von behördlichen Benachrichtigungen



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	- 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

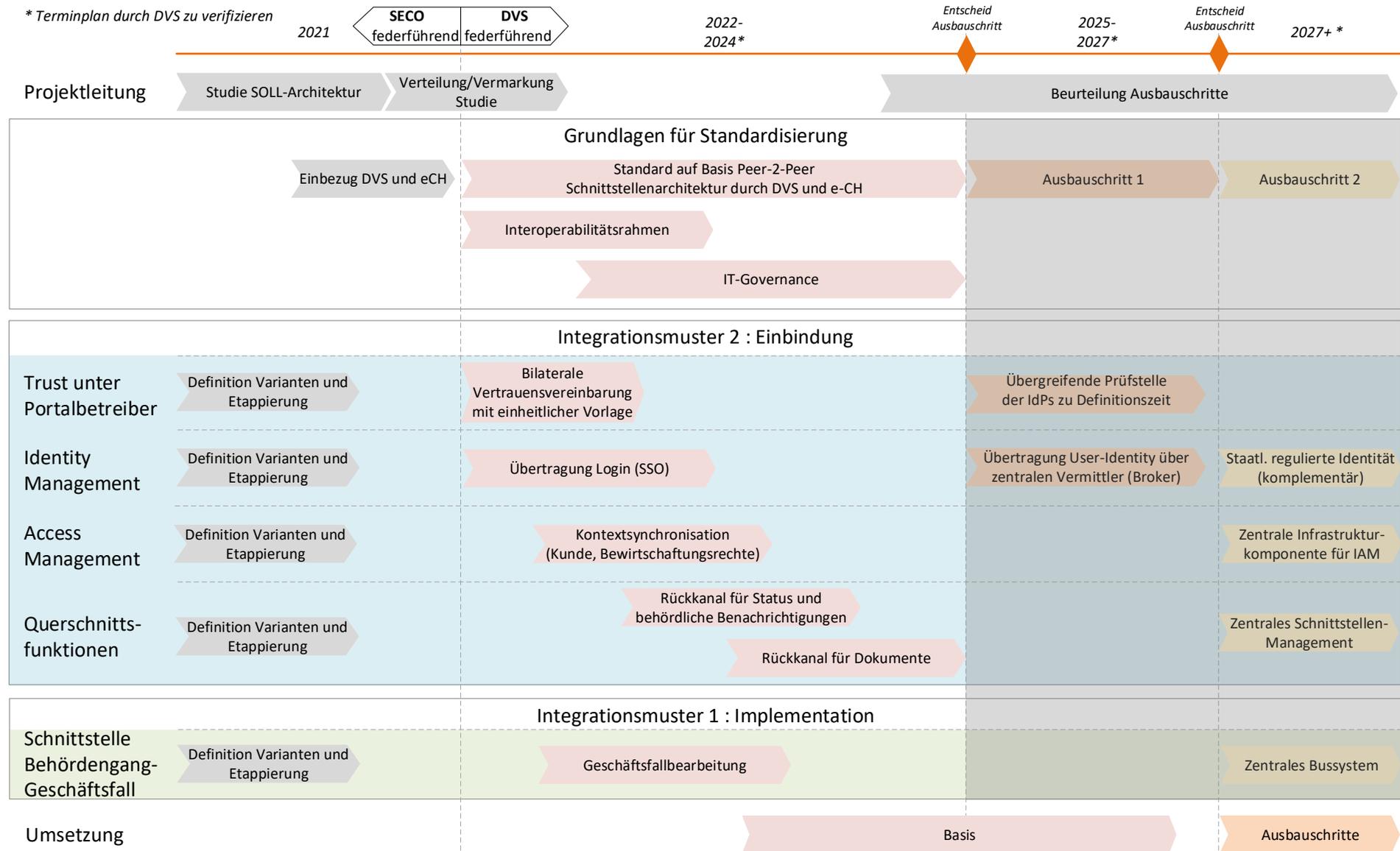
ABB Portal 31.03.2020 / ePortal / J. Umhang

19

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

Anhang D Umsetzungs-Roadmap in vergrößerter Darstellung im Querformat

* Terminplan durch DVS zu verifizieren



Anhang E Thesen zum Zielbild der integrativen Abbildung von Behördenleistungen auf Portalen

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.

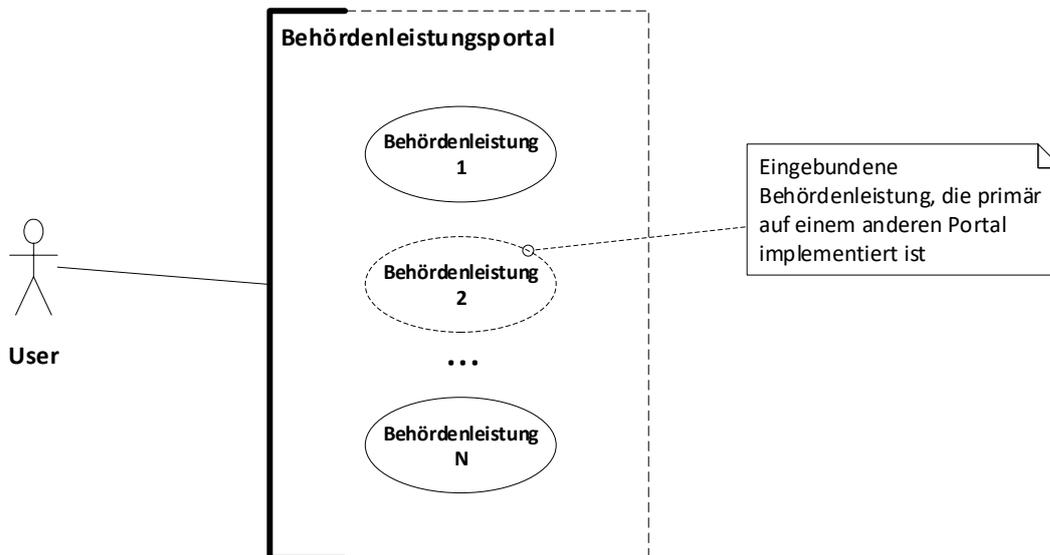


Abbildung 57: Ein Behördenleistungsportal bietet dem User die für ihn relevanten Behördenleistungen an, egal auf welchem System sie primär implementiert sind [These-1] (UML Use Case Diagramm)

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)

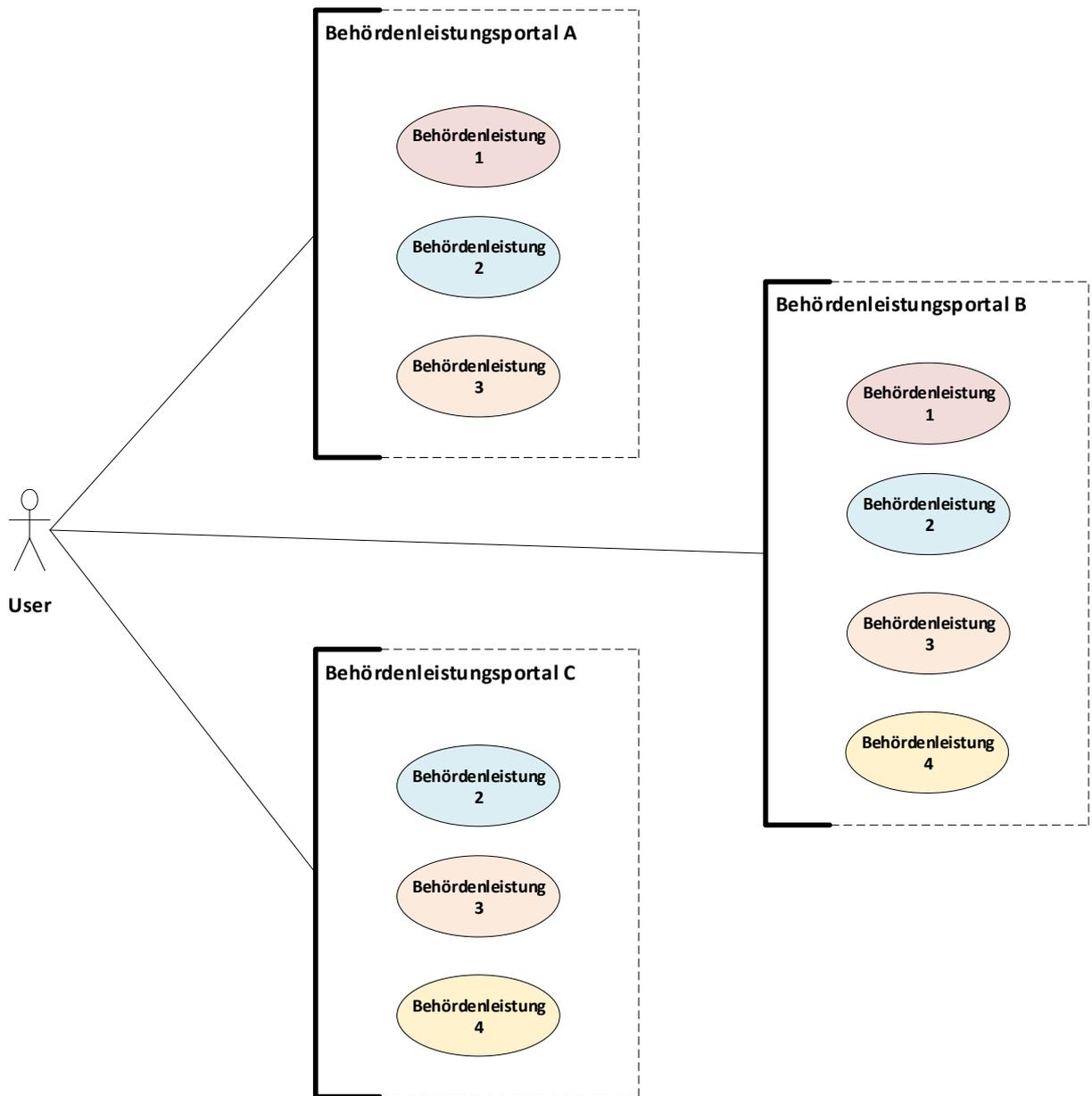


Abbildung 58: Behördenleistungsportale präsentieren überlappende Sets an Leistungen [These-2]

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 Abbildung 20) sei für das Zielbild ergänzt:

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

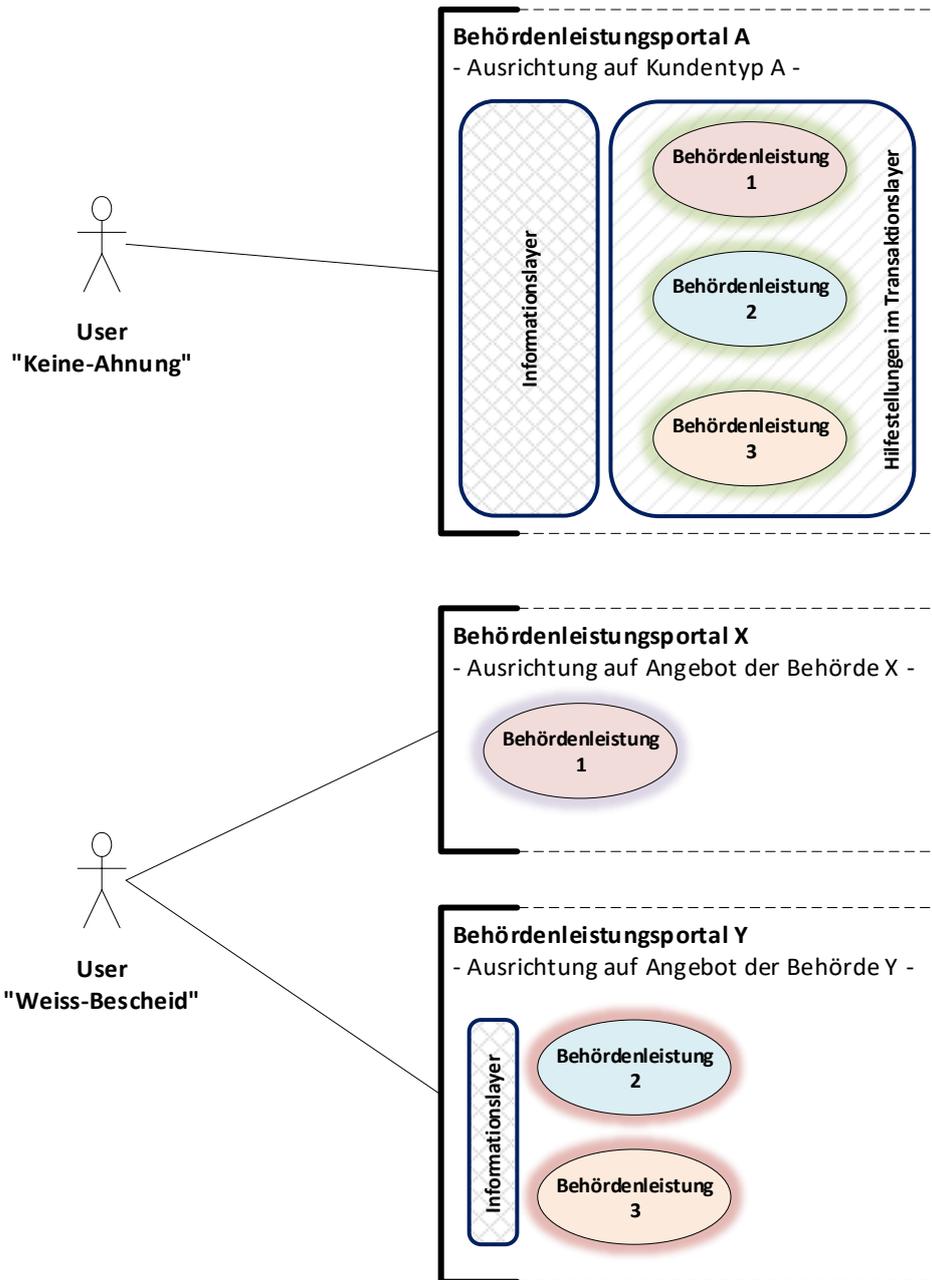


Abbildung 59: Abbildung von Behördenleistungen auf verschieden ausgerichteten Portalen in jeweils individuellem Design (verbildlicht durch die verschiedenen farblichen Umrandungen der Ovale) [These-3]

Anhang F Anforderungen an die IT-Governance

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.

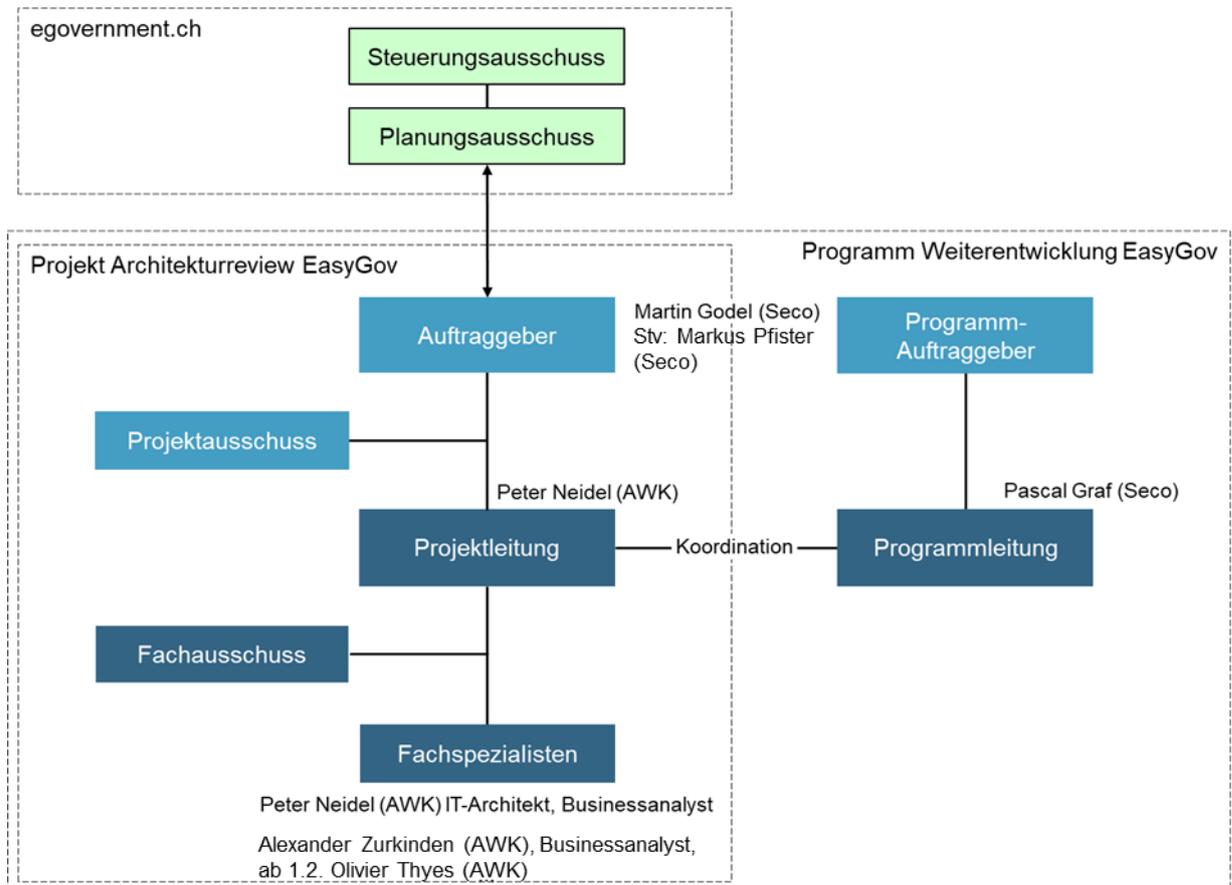
Anhang G Details zur Projektdurchführung

Anhang 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:

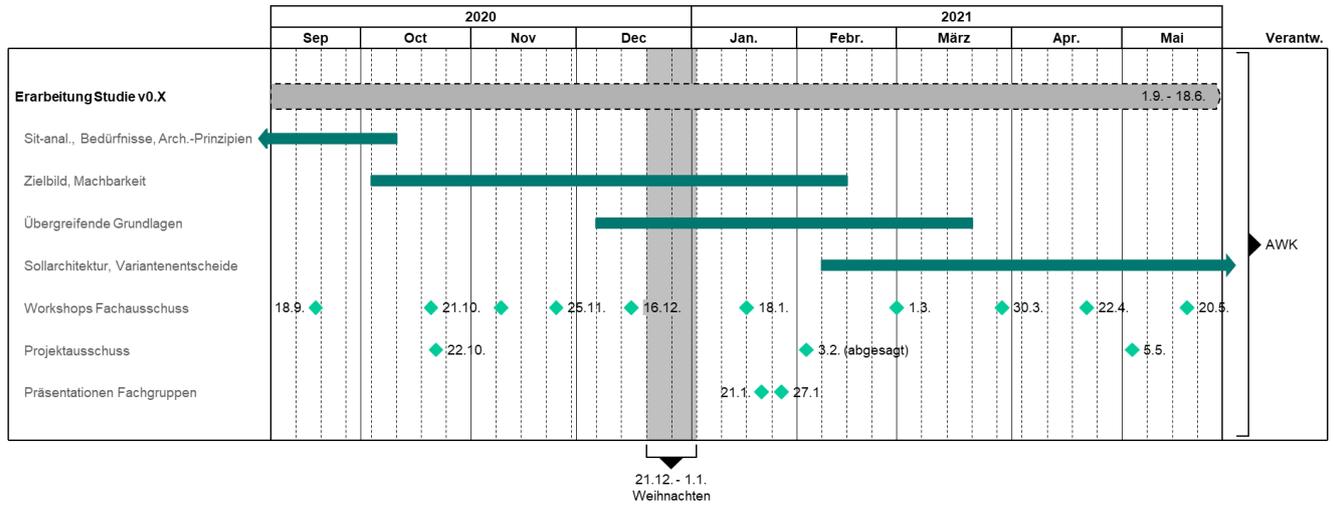
- Alexandra Collm, Leiterin Bereich Kunden, Direktion für Organisation und Informatik Stadt Zürich
- David De Groote, Mitglied Planungsausschuss eGov-CH, Kt. Jura
- Hansjörg Hänggi, Planungsausschuss eGov-CH, E-Government Verantwortlicher Kt. Baselstadt
- Marcel Kessler, Projektleiter Umsetzungsplan, 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

Anhang G.B Vorgehensweise und Termine

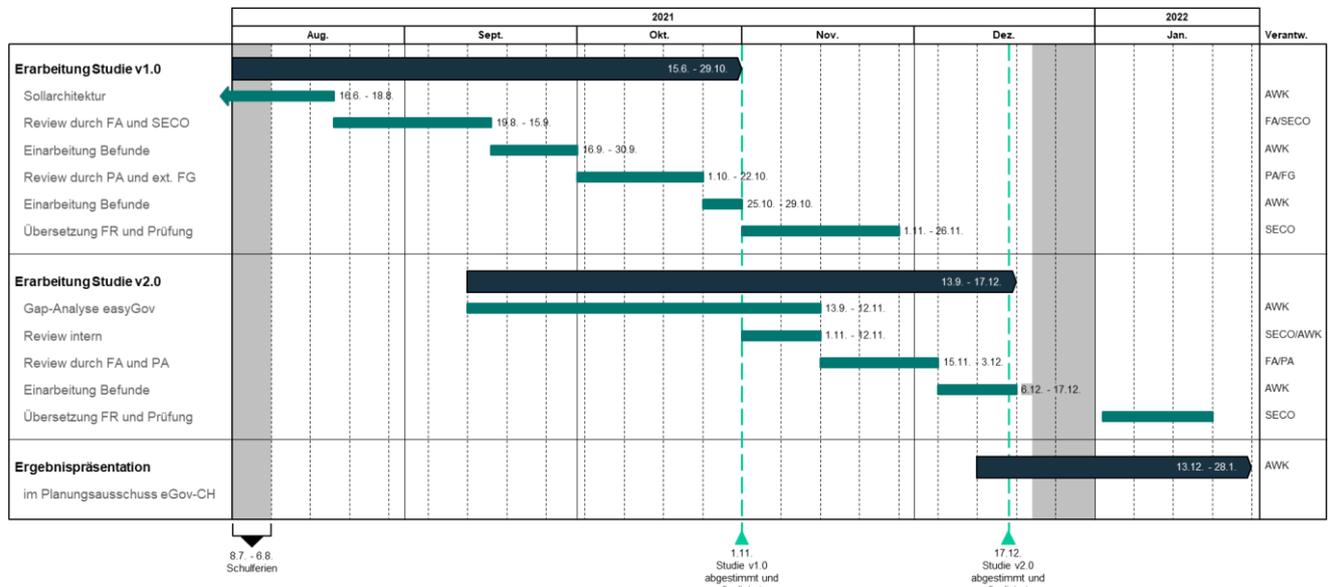
Die Integrations-Sollarchitektur wurde iterativ in einer Workshop-Reihe zusammen mit dem Fachausschuss gemäss folgendem Terminplan erarbeitet:



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>

Anhang 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.

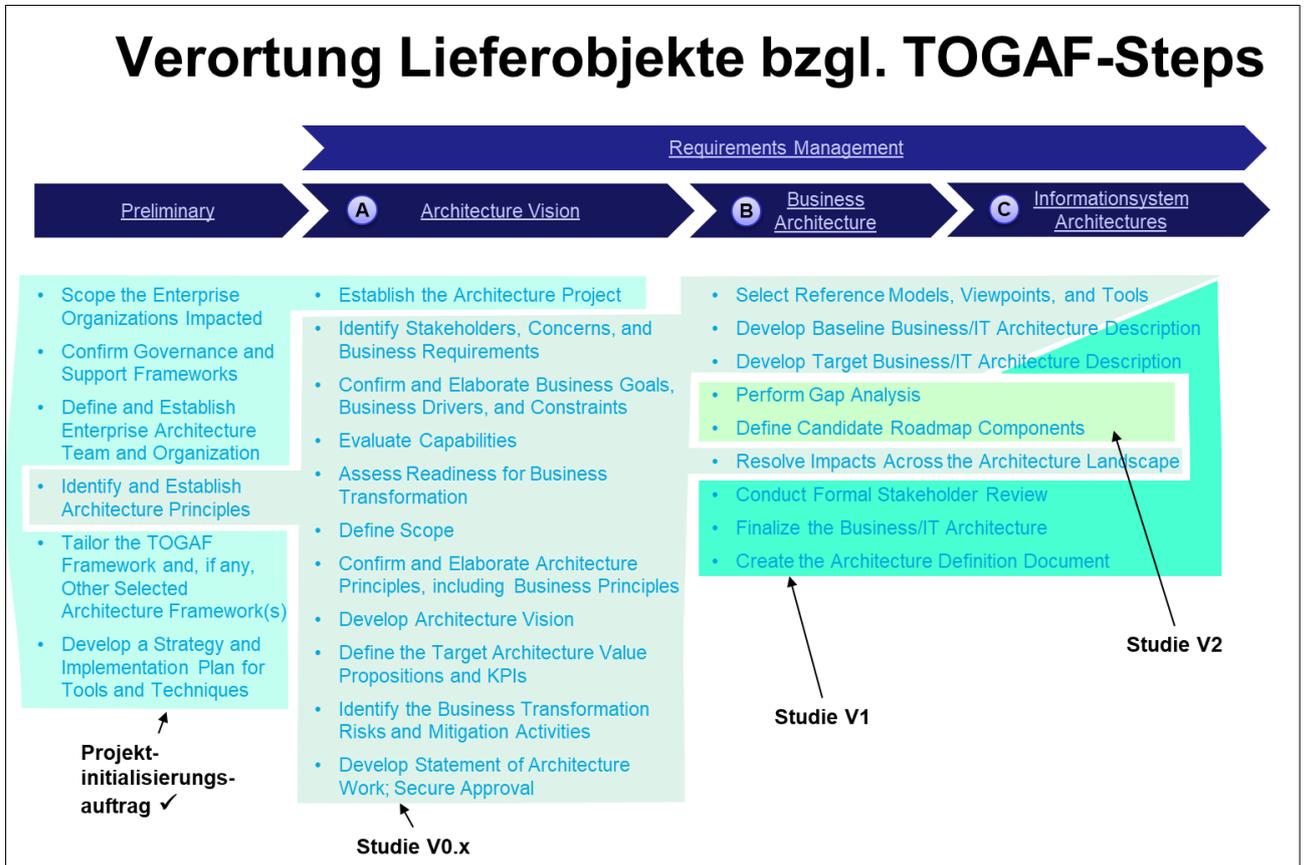


Abbildung 60: Verortung Lieferobjekte bezüglich TOGAF-Steps

Scope des Projekts bezüglich TOGAF

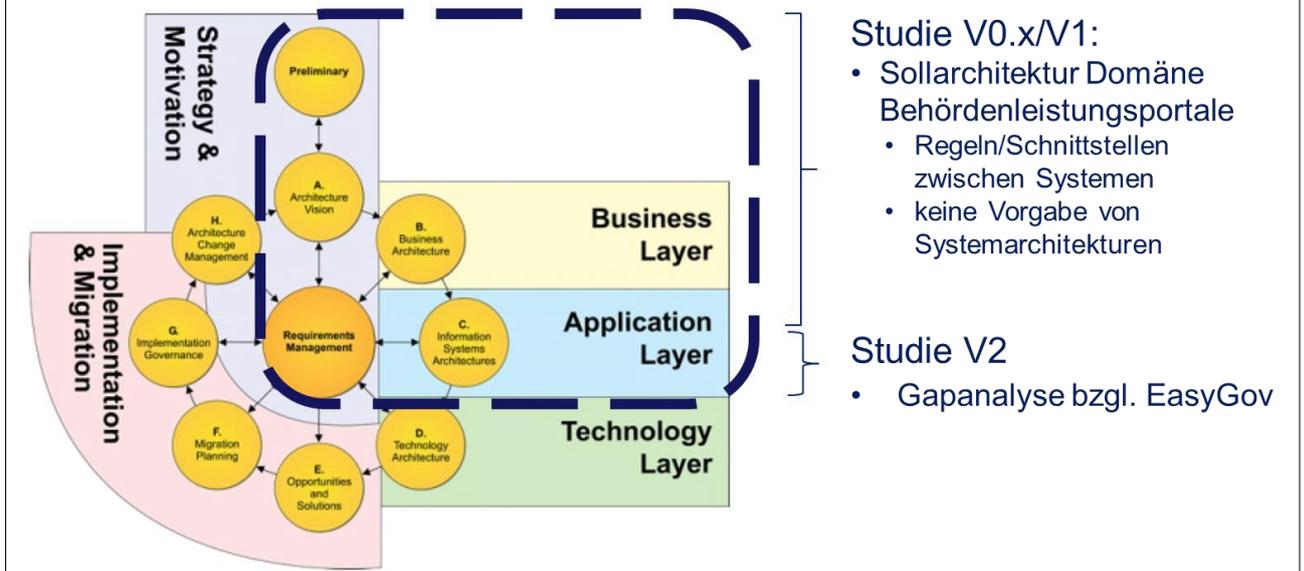


Abbildung 61: Scope des Projekts bezüglich TOGAF

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>

Anhang 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.

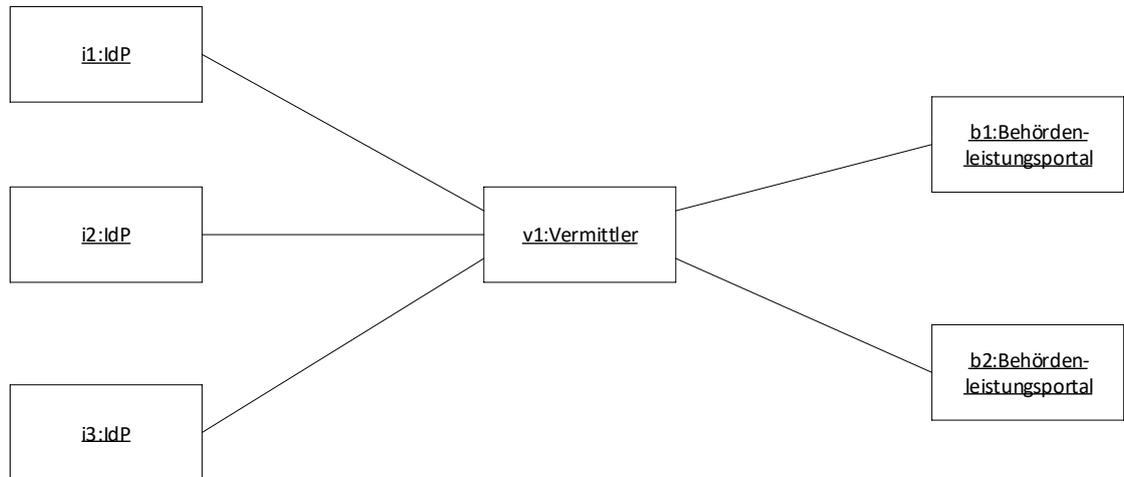


Abbildung 62: Vermittlerdienst zwischen IdPs und Behördenleistungsportalen

- (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.

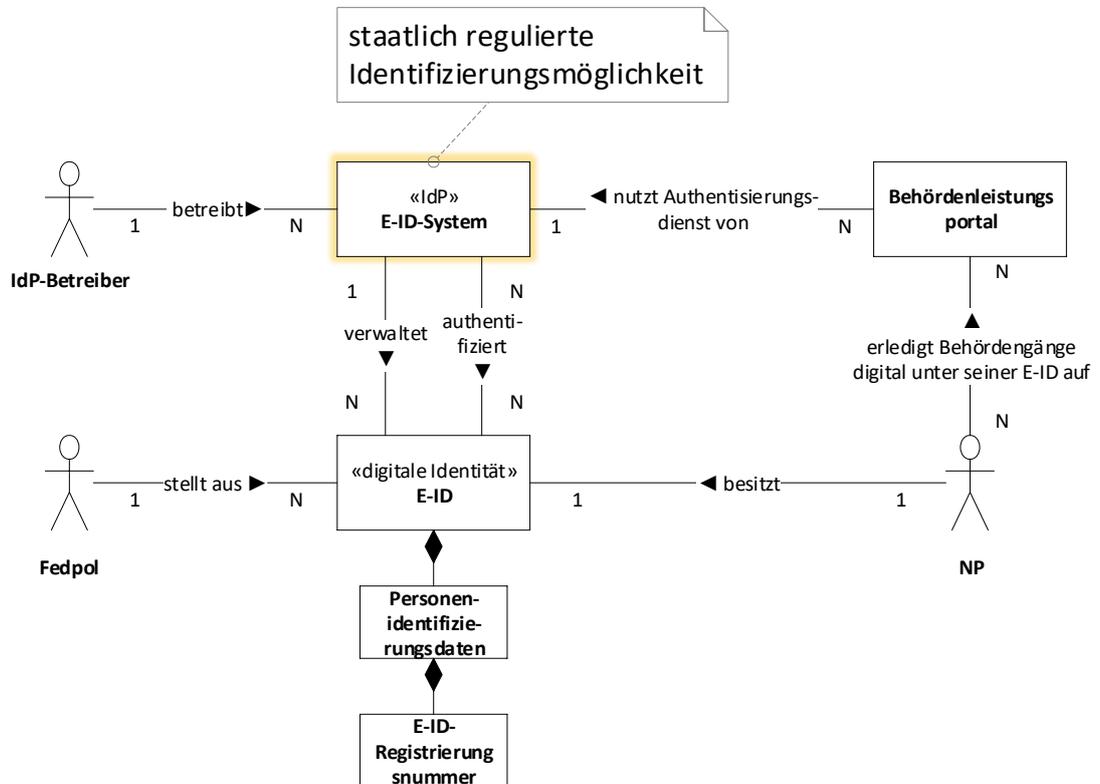


Abbildung 63: Aussagen des BGEID⁹⁸ [23] aus der Strukturperspektive

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.

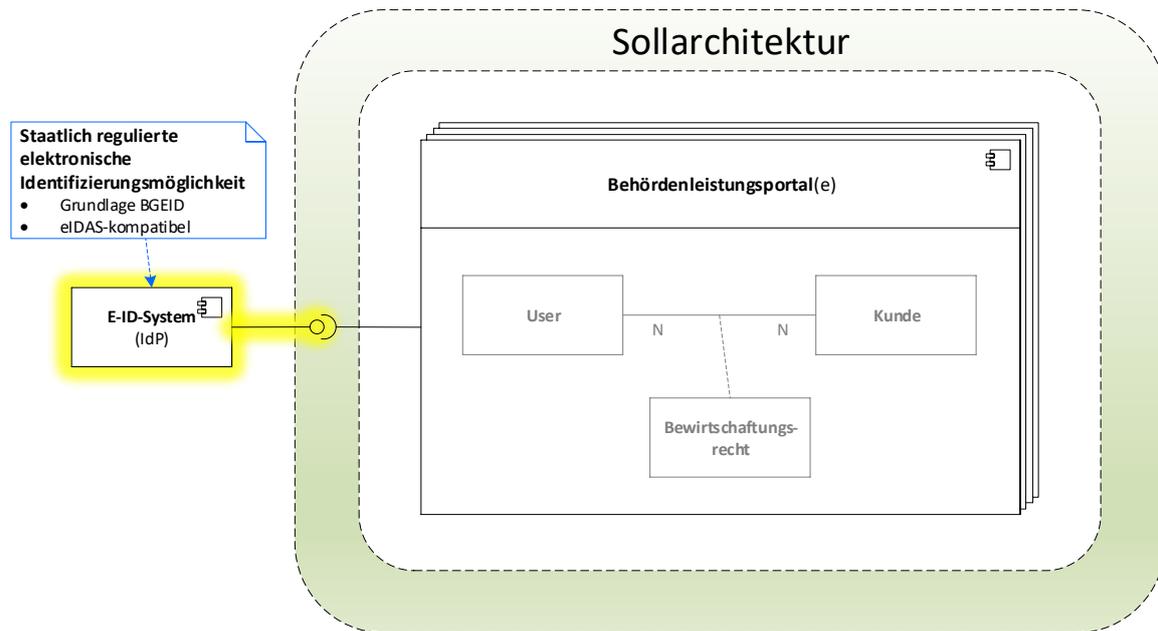


Abbildung 64: Die Nutzung eines E-ID-Systems als staatlich regulierte elektronische Identifizierungsmöglichkeit ist ein Schlüsselement der Sollarchitektur

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 Anhang 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 Vorhaben 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.

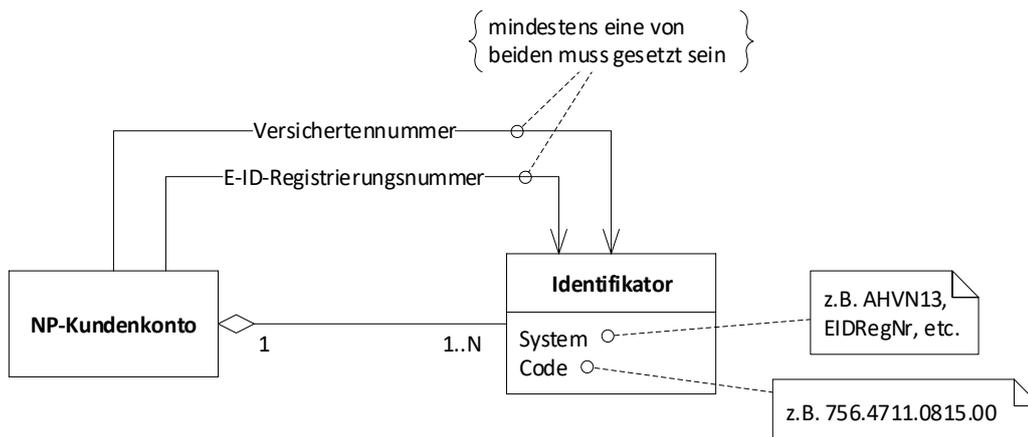


Abbildung 65: In einem NP-Kundenkonto können mehrere Identifikatoren hinterlegt werden, mindestens jedoch die Versichertennummer, optional die E-ID-Registrierungsnummer

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		Verfügbare Identifikator für Eröffnung NP-Kundenkonto		Kommentar
mit der hinter dem User stehenden Person identisch?	in der Schweiz gemeldet?	Versichertennummer	E-ID-Registrierungsnummer	
Ja (eigenhändige Eröffnung)	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.

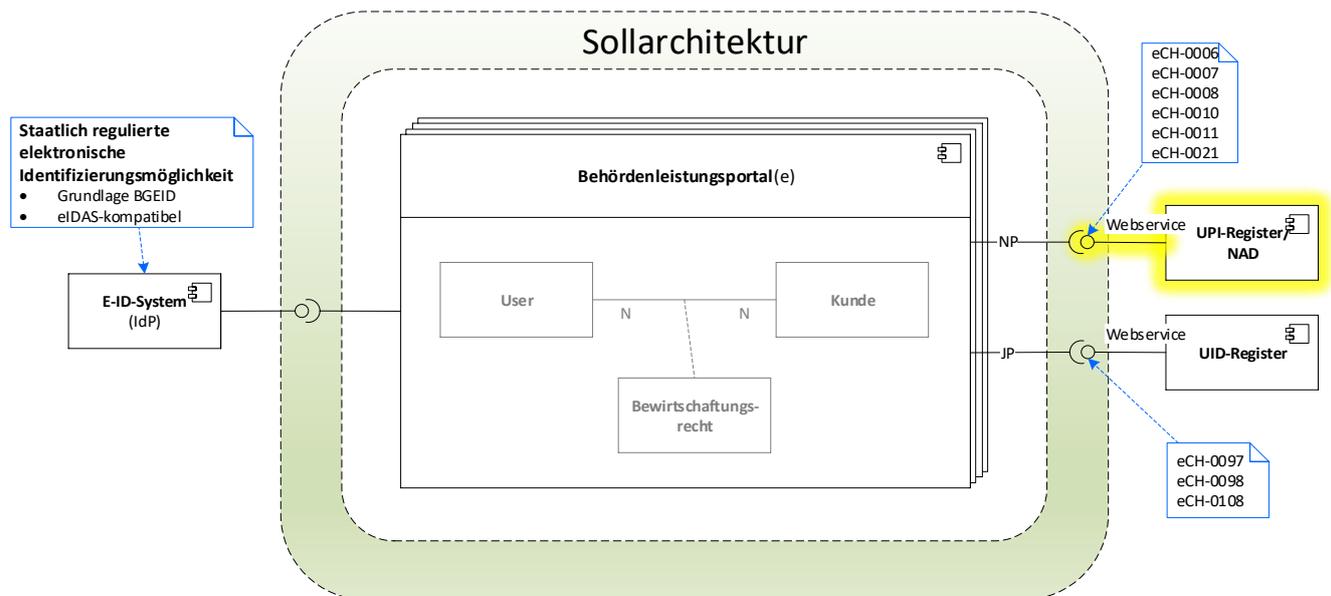


Abbildung 66: Die Nutzung des UPI-Registers und des entstehenden NAD für NP ist neben dem existierenden UID-Register für JP ein weiteres Schlüsselement der Sollarchitektur

[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.

Entscheidung¹⁰⁰: 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/>

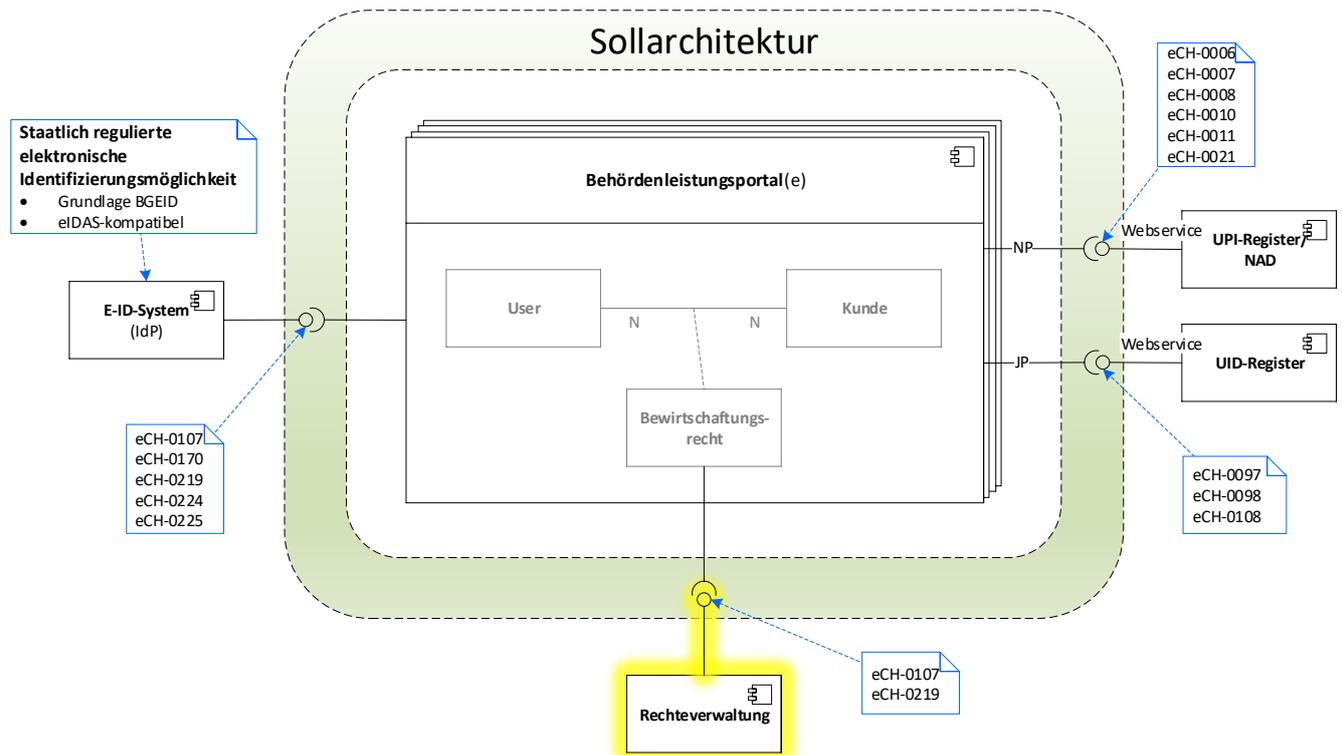


Abbildung 67: Die Nutzung eines zentralen Infrastrukturdienstes für die Verwaltung der Bewirtschaftungsrechte ist ein weiteres Schlüsselement der Sollarchitektur

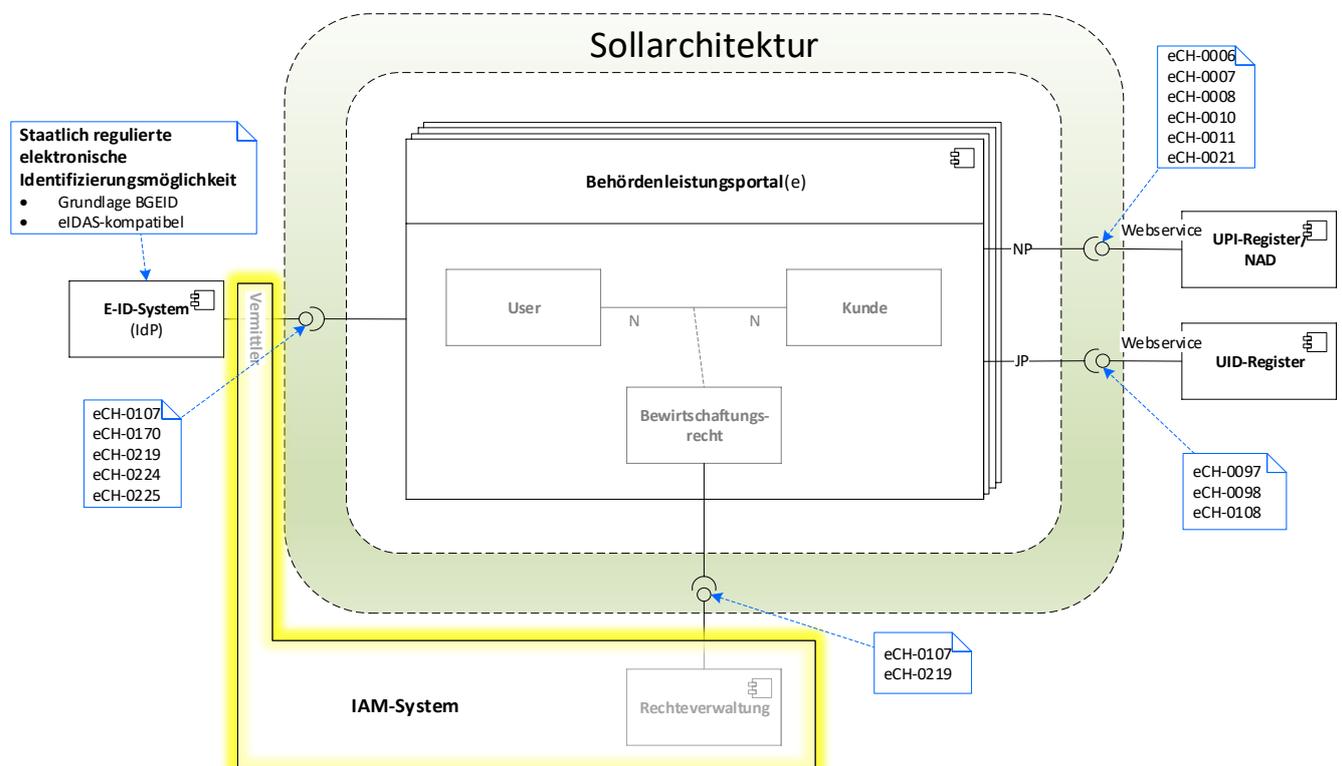


Abbildung 68: Ein geeignetes IAM-System kann die Aufgabe der zentralen Rechteverwaltung übernehmen und bringt darüber hinaus noch einen Vermittler ins Spiel

[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

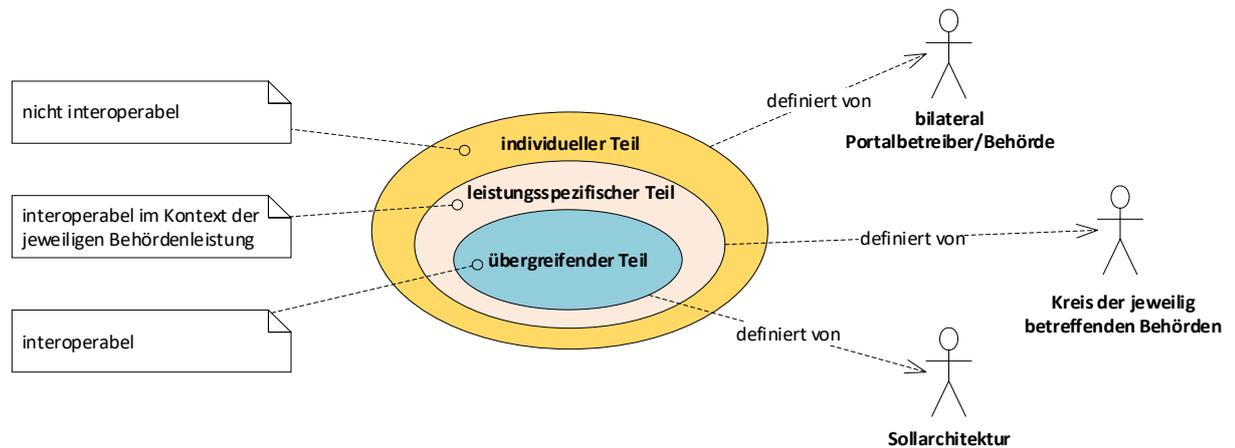


Abbildung 69: Muster eines Schalenmodells für ein Bewirtschaftungsrechtemodell

- (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.

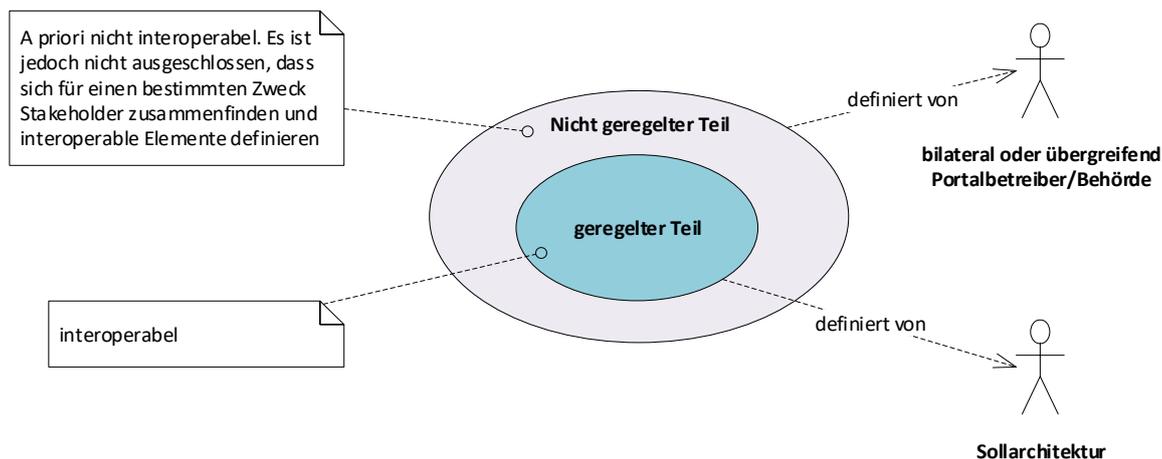


Abbildung 70: Muster eines Berechtigungsmodells mit einem geregelten und einem ungeregelten Teil

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 plattformspezifische 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>

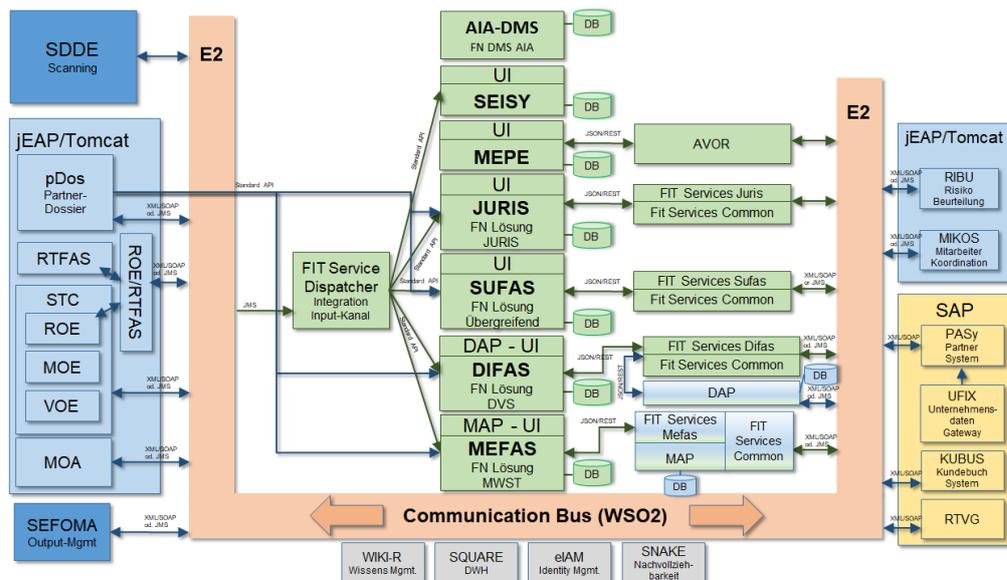


Abbildung 72: Beispiel einer Verwendung eines ESB auf Basis des WSO2 API Gateways bei FISCAL-IT

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 Abbildung 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.

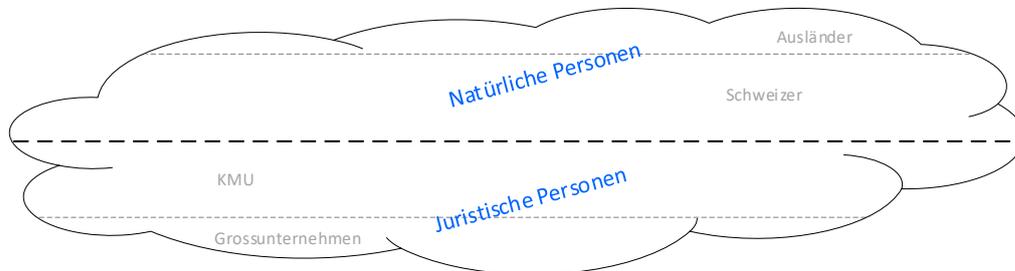


Abbildung 73: Kundensegmentierung Beispiel 1

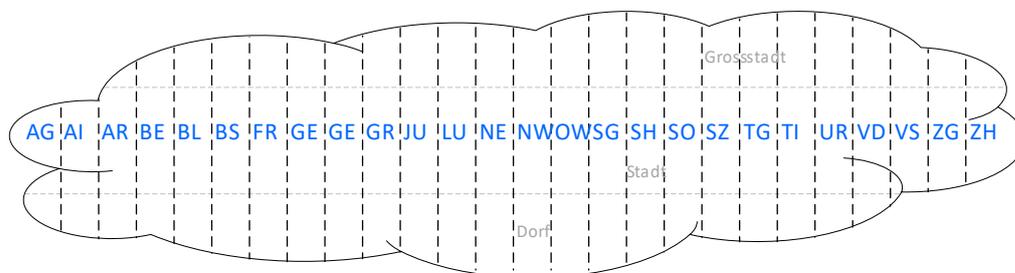


Abbildung 74: Kundensegmentierung Beispiel 2

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 Abbildung 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.

Anhang 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	Architurrelevante UX-Themen sollen als Bedürfnis aufgenommen werden. Wichtig ist, dass die Abgrenzung die Architurrelevanz 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

Anhang 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 électroniques

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 Groot

- Mise en place d'outils nationaux qui doivent permettre de mettre à disposition des prestations électroniques 100% digitales:
 - Services de base (service de paiement, éditeur de formulaires, scanner mobile, etc...)
 - Kit de développement national de prestations électroniques
 - Look & Feel national de prestations électroniques (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.

Abbildungsverzeichnis

Abbildung 1: Scope der angestrebten Integrations-Sollarchitektur (schematische Darstellung) .	25
Abbildung 2: Allgemeiner Ablauf eines Bewilligungsverfahrens (BPMN-Diagramm).....	26
Abbildung 3: Allgemeiner Ablauf eines Meldeverfahrens (BPMN-Diagramm)	27
Abbildung 4: Abstraktion der Abwicklung einer Behördenleistung als parallel auf Kunden- bzw. Behördenseite laufende Prozesse.....	28
Abbildung 5: Involvierung einer weiteren Behörde/Amtsstelle in die Geschäftsfallbearbeitung nach dem Muster Subprozess.....	29
Abbildung 6: Involvierung einer weiteren Behörde/Amtsstelle in die Geschäftsfallbearbeitung nach dem Muster Verfahrensweitergabe	30
Abbildung 7: Behördenleistungsportal als digitaler Zugangskanal für ein oder mehrere Behördenleistungen für den Kunden (UML-Use Case Diagramm).....	31
Abbildung 8: Portalbetreiber kann auch die Behörde selbst sein	31
Abbildung 9: Abgrenzung des Scopes eines Behördenleistungsportals auf den kundenseitigen Prozess. Behördeninterne Prozesse werden dagegen vom behördeninternen Fachsystem unterstützt.	32
Abbildung 10: Verortung von Informations- und Transaktionslayer in der Prozesssicht.....	33
Abbildung 11: Prinzipielle funktionelle Struktur eines Behördenleistungsportals	34
Abbildung 12: Vielfältige Layer-Ausprägungen in existierenden Behördenleistungsportalen ..	35
Abbildung 13: ePortal-Aufbau mit verteilten Subsystemen unter verschiedenen Verantwortlichkeiten	36
Abbildung 14: Auf das Portfolio einer Behörde ausgerichtetes Behördenleistungsportal (A): Das Portal bildet das Leistungsangebot einer bestimmten Behörde ab	37
Abbildung 15: Auf den Bedarf einer bestimmten Kundenzielgruppe ausgerichtetes Behördenleistungsportal (B): Das Portal bildet das für die Kundenzielgruppe relevante Set an Behördenleistungsangeboten ab, die von verschiedenen Behörden stammen können	37
Abbildung 16: Kapselung der konkreten Zuständigkeit einer kantonalen/kommunalen Behördenleistung durch ein übergreifendes Angebot (B´)	38
Abbildung 17: Mischform (C) aus (A) und (B).....	39
Abbildung 18: Individuelle Abbildung einer Behördenleistung auf verschiedenen Portalen....	40
Abbildung 19: Einbindung einer bestehenden Implementation eines Behördengangs in einem anderen Portal	42
Abbildung 20: Informationsmodell für Behördenleistungsportale (UML-Klassendiagramm, vergrösserte Darstellung siehe Anhang B)	43
Abbildung 21: Integrationsmuster 1 - Implementation des Behördengangs direkt im Portal ..	49
Abbildung 22: Integrationsmuster 2 erlaubt auch mehrere Consumer-Portale	49
Abbildung 23: Spezialfall Integrationsmuster 1: Ein Behördenleistungsportal bietet eine Ausführungsumgebung/Framework für Behördenleistungen, auf der Behörden ihre Behördenleistungen als Portal-Fachanwendung implementieren bzw. in vorgefertigten Komponenten konfigurieren.....	50
Abbildung 24: Integrationsmuster 2 - Einbindung eines extern implementierten Behördengangs	51
Abbildung 25: Mischform – Portal bildet Behördengänge sowohl nach Integrationsmuster 1 und 2 ab	52
Abbildung 26: Kategorisierung der Bedürfnisse nach Tallinn, Themen und Akteuren (Grösse der Bubbles steht für die Anzahl der Nennungen).....	62
Abbildung 27: Bildfolge zu Pain Point 1	71
Abbildung 28: Bildfolge zu Pain Point 2 und 3	73

Abbildung 29: Ein Behördenleistungsportal nutzt zur User-Authentifizierung eine extern definierte digitale Identität, wogegen es Kunden mit Hilfe eines extern definierten Identifikators identifiziert	76
Abbildung 30: Illustration [REQ-1] anhand eines exemplarischen Kontexts (UML-Objektdiagramm)	77
Abbildung 31: Verortung der Interoperabilitätsanforderungen im Informationsmodell.....	78
Abbildung 32: Illustration des interoperablen Kerns am Beispiel der Schnittstelle Behördengang↔Geschäftsfallbearbeitung (Integrationsmuster 1)	79
Abbildung 33: Abgleich des interoperablen Kerns eines Kunden-Stammsatzes in einem Behördenleistungsportal.....	83
Abbildung 34: Herstellung des Session-Kontextes beim Aufruf des Behördengangs "Y-Bewilligung beantragen" im Provider-Portal konform zum Absprung-Kontext vom Consumer-Portal mittels SSO + Kontextsynchronisation	85
Abbildung 35: Verortung des Interoperabilitätsrahmens im Informationsmodell.....	90
Abbildung 36: Die Integrations-Sollarchitektur spezifiziert die allgemeinen (nicht-leistungsspezifischen) Kommunikationsprozesse zwischen Behördenleistungsportal und behördeninternem Fachsystem	91
Abbildung 37: Informationsmodell der Schnittstellenprozesse Behördengang↔Geschäftsfallbearbeitung	93
Abbildung 38: Prozessmodell Schnittstelle Behördengang↔Geschäftsfallbearbeitung im Fall "Anstoss durch Kunden"	94
Abbildung 39: Prozessmodell Schnittstelle Behördengang↔Geschäftsfallbearbeitung im Fall "Anstoss durch Behörde"	94
Abbildung 40: Szenario der Schnittstellenprozesse zwischen Behördengang und Geschäftsfallbearbeitung gemäss den diesbezüglichen Anforderungen	95
Abbildung 41: API Endpoints der Schnittstelle Behördengang↔Geschäftsfallbearbeitung	96
Abbildung 42: Die Einbindung eines extern implementierten Behördengangs umfasst Hin- und Rückleitung.....	97
Abbildung 43: SSO-Szenario mit gemeinschaftlich verwendetem Identitätsprovider	99
Abbildung 44: Rücksprung im SSO-Szenario mit gemeinschaftlich verwendetem IdP.....	100
Abbildung 45: SSO-Szenario mit bilateralem Peer-to-Peer (P2P) Trust	102
Abbildung 46: Unterschied zwischen Fall A) und B) bezüglich Weiterleitung und alternativem Direktzugriff	103
Abbildung 47: Eine staatliche Prüfstelle vereinfacht mittels einer Zertifizierung die Vertrauensstellung zum LoA des Logins.....	104
Abbildung 48: Übertragung der Kontextinformation im Fall A) per Context Token als Zusatz zum Identity Token (vergleiche Abbildung 43)	106
Abbildung 49: Übertragung der Kontextinformation im Fall B) als Zusatz der Response des Introspection API Endpoints (vergleiche Abbildung 45).....	107
Abbildung 50: API Endpoint für die Behördengang-Rückmeldungen als Bestandteil der Schnittstelle zur Einbindung extern implementierter Behördengänge	109
Abbildung 51: Gesamtbild eines eingebundenen Behördengangs mit der von dessen Provider-Portal gekapselten Schnittstelle zum dahinterstehenden behördeninternen Fachsystem	110
Abbildung 52: Schnittstellen-Datenfluss im Überblick.....	111
Abbildung 53: Zirkuläre Abhängigkeit infolge verteilter Schnittstellen-Verantwortung	111
Abbildung 54: Eindeutige Abhängigkeiten zwischen den Systemen infolge Verantwortungsfestlegung und Standardisierung	112
Abbildung 55: Fokusbereiche der IT-Governance.....	117
Abbildung 56: Roadmap zur Umsetzung der Standardisierung	123

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)	135
Abbildung 58: Behördenleistungsportale präsentieren überlappende Sets an Leistungen [These-2]	137
Abbildung 59: Abbildung von Behördenleistungen auf verschiedenen ausgerichteten Portalen in jeweils individuellem Design (verbildlicht durch die verschiedenen farblichen Umrandungen der Ovale) [These-3]	139
Abbildung 60: Verortung Lieferobjekte bezüglich TOGAF-Steps	146
Abbildung 61: Scope des Projekts bezüglich TOGAF.....	147
Abbildung 62: Vermittlerdienst zwischen IdPs und Behördenleistungsportalen.....	149
Abbildung 63: Aussagen des BGEID [23] aus der Strukturperspektive	150
Abbildung 64: Die Nutzung eines E-ID-Systems als staatlich regulierte elektronische Identifizierungsmöglichkeit ist ein Schlüsselement der Sollarchitektur.....	153
Abbildung 65: In einem NP-Kundenkonto können mehrere Identifikatoren hinterlegt werden, mindestens jedoch die Versichertennummer, optional die E-ID-Registrierungsnummer	157
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 ...	158
Abbildung 67: Die Nutzung eines zentralen Infrastrukturdienstes für die Verwaltung der Bewirtschaftungsrechte ist ein weiteres Schlüsselement der Sollarchitektur	161
Abbildung 68: Ein geeignetes IAM-System kann die Aufgabe der zentralen Rechteverwaltung übernehmen und bringt darüber hinaus noch einen Vermittler ins Spiel	161
Abbildung 69: Muster eines Schalenmodells für ein Bewirtschaftungsrechtemodell	162
Abbildung 70: Muster eines Berechtigungsmodells mit einem geregelten und einem unregulierten Teil	163
Abbildung 71: Geschütztes Transportsystem für den zielgerichteten Datenaustausch bzw. die bidirektionale Kommunikation zwischen Behördenleistungsportalen und behördeninternem Fachsystemen	164
Abbildung 72: Beispiel einer Verwendung eines ESB auf Basis des WSO API Gateways bei FISCAL-IT	166
Abbildung 73: Kundensegmentierung Beispiel 1	168
Abbildung 74: Kundensegmentierung Beispiel 2	168

Tabellenverzeichnis

Tabelle 1: Erläuterung der im Informationsmodell dargestellten Entitäten	43
Tabelle 2: Rahmenbedingungen für die Entwicklung der Sollarchitektur	52
Tabelle 3: Prinzipien der Tallin Deklaration zum E-Government	54
Tabelle 4: Bedürfnisse bezüglich der Integration von Behördenleistungen	55
Tabelle 5: Bedürfnisse bezüglich Authentisierung und Autorisierung	56
Tabelle 6: Bedürfnisse bezüglich Kommunikation Kunde – Behörde.....	57
Tabelle 7: Bedürfnisse bezüglich Präsentation (UI).....	58
Tabelle 8: Bedürfnisse bezüglich Geschäftsabwicklung	59
Tabelle 9: Bedürfnisse bezüglich ISDS.....	61
Tabelle 10: Bedürfnisse bezüglich der Rahmenbedingungen für die Umsetzung.....	61
Tabelle 11: Abgrenzungen zum Scope der Sollarchitektur	63
Tabelle 12: Qualitätserwartungen an die Sollarchitektur	64
Tabelle 13: Verarbeitung der Interoperability Principles des EIF in der Studie.....	64

Tabelle 14: Architekturprinzipien zur Sollarchitektur	67
Tabelle 15: LoA-Vertrauensstufenmodell gemäss eCH-0170 [21]	86
Tabelle 16: Exemplarisches Berechtigungsstufenmodell	87
Tabelle 17: Qualitätsstufen gemäss eCH-0171 [22]	88
Tabelle 18: Zusammenstellung des Interoperabilitätsrahmens	89
Tabelle 19: Beurteilung ISDS-Risikofaktoren je nach Integrationsmuster	114
Tabelle 20: Anforderung an die ISDS	115
Tabelle 21: Verarbeitung und Umsetzung der Bedürfnisse aus Kapitel 2.2.2 bei der Entwicklung des Zielbilds in Kapitel 2.4 und der Sollarchitektur in Kapitel 2.5	118
Tabelle 22: Empfohlene Massnahmen unter Verantwortung SECO	123
Tabelle 23: Empfohlene Massnahmen unter Verantwortung DVS	124
Tabelle 24: Evaluation Lösungsvarianten [Herausforderung-1]	152
Tabelle 25: Evaluation Lösungsvarianten [Herausforderung-2]	155
Tabelle 26: Entscheidungsbaum bezüglich der Verfügbarkeit von Versichertennummer und/oder E-ID-Registrierungsnummer zur Verwendung als Identifikator bei der Eröffnung eines NP-Kundenkontos	157
Tabelle 27: Evaluation Lösungsvarianten [Herausforderung-3]	159
Tabelle 28: Evaluation Lösungsvarianten [Herausforderung-4]	163
Tabelle 29: Evaluation Lösungsvarianten [Herausforderung-5]	166
Tabelle 30: Evaluation Lösungsvarianten [Herausforderung-6]	170

Staatssekretariat für Wirtschaft SECO

Direktion für Standortförderung

KMU-Politik

Holzikofenweg 36, 3003 Bern

Tel. +41 58 462 28 71

www.seco.admin.ch, www.kmu.admin.ch