eCH-0169 SuisseTrustIAM-Geschäftsarchitektur

Name	SuisseTrustIAM-Geschäftsarchitektur
Standard-Nummer	eCH-0169
Kategorie	Standard
Reifegrad	Definiert
Version	1.0
Status	Genehmigt
Genehmigt am	2014-09-03
Ausgabedatum	2014-09-04
Ersetzt Standard	
Sprachen	Deutsch und Französisch
Autoren	Fachgruppe IAM Konrad Walser, E-Government-Institut, Berner Fachhochschule, konrad.walser@bfh.ch Roman Hosang, E-Government-Institut, Berner Fachhochschule, roman.hosang@bfh.ch
Herausgeber / Vertrieb	Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Zusammenfassung

Dieser Standard beschreibt die Geschäftsarchitektur für SuisseTrustIAM (STIAM), einer föderierten Identity- und Access-Management-Lösung basierend auf dem Hub-'n'-Spoke-Modell. Er beschreibt aus Geschäftssicht, welche Stakeholder in welcher Form im STIAM-Kontext zusammenarbeiten, welche Rollen in welchen Prozessen mit welchen Aufgaben, Kompetenzen und Verantwortungen zum Einsatz gelangen und wie die Governance und das Management einer STIAM-Domäne aussehen.

Die Governance und das Management der Domäne werden aus Sicht dieses Standards als bewusst zu trennende Aufgaben verstanden, für die je separate Gremien zu schaffen sind. Das Governance-Gremium gibt Policies vor und überwacht deren Einhaltung. Das Management-Gremium setzt die Policies in und zwischen den Stakeholdern um und überwacht deren Umsetzung. Damit wird sichergestellt, dass sich die unter Umständen sehr vielen Stakeholder der Domäne bezüglich der Definition ihres Vertrauensraums koordinieren.

Ein föderiertes Identity- und Access Management stellt eine wesentliche mögliche Komponente für integriertes, durchgängiges und elektronisches E-Government, E-Health, E-Education und eine ebensolche E-Economy dar.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Status des Dokuments

Das vorliegende Dokument wurde vom Expertenausschuss **genehmigt.** Es hat für das definierte Einsatzgebiet im festgelegten Gültigkeitsbereich normative Kraft.

2 Einleitung

2.1 Überblick und Einführung

SuisseTrustIAM (STIAM) basiert auf eCH-0107 IAM-Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM) [eCH-0107] und stellt eine Ausprägungsmöglichkeit des Hub-'n'-Spoke-Modells dar, das in [eCH-0107] als Identity Federation Konzept präsentiert wird. Die Beschreibung der Geschäftsarchitektur erfolgt nicht aus der Broker-, sondern aus der Domänensicht[1], in welcher der Broker eine zentrale Vermittlertätigkeit einnimmt. Die Begrifflichkeiten folgen denen aus [eCH-0107], sofern diese nicht im vorliegenden Dokument definiert werden.

Die Vorteile des Hub-'n'-Spoke-Modells liegen darin, dass die Relying Party die Identitäts- und Attributbestätigungen auslagert. Dadurch muss sie nicht mit diversen Attribute- und Authentifikations-Autoritäten je separate Beziehungen und Schnittstellen pflegen. STIAM strebt als erwünschten Zielzustand an, dass alle Stakeholder nur noch je eine Schnittstelle zum STIAM-Broker haben.

Für STIAM sind die nachfolgenden Stakeholder relevant:

- Das **Subjekt** will elektronisch auf Ressourcen von Relying Parties zugreifen.
- Die **Ressource** ist ein Service oder stellt Daten bereit, auf welche ein Subjekt zugreifen kann, wenn es sich authentisiert hat und es basierend auf den benötigen Attributen autorisiert wurde.
- Die **Relying Party (RP)** vertritt die Interessen der Ressource und stellt die Zugriffskontrolle sicher.
- Die **Authentifikations-Autorität (AuthnA)** bestätigt die behauptete eIdentity eines Subjekts.
- Die **Attribut-Autorität (AA)** liefert die erforderlichen Bestätigungsinformationen bezüglich der Attribute. Dies sind Eigenschaften des entsprechenden Subjekts, wodurch dieses auf die Ressource der Relying Party zugreifen kann.
- Der **STIAM-Broker** vermittelt zwischen Subjekt und Ressourcen, um der Relying Party unter Einhaltung der Domänenregeln im Vertrauensraum die notwendigen Bestätigungen für die Zugriffskontrolle zuzuführen.
- Das **Governance-Gremium** ist ein übergreifendes Gremium und führt, steuert, überwacht und evaluiert anhand von Policies die vertrauensvolle Vermittlung von Bestätigungen in einer Domäne. Das Governance-Gremium ist verantwortlich für die korrekte Umsetzung von Policies im Zusammenspiel der Stakeholder.
- Das **Management-Gremium** ist ein übergreifendes Gremium und sorgt für die Umsetzung der Governance-Vorgaben innerhalb der Domäne. Es wirkt koordinierend über die verschiedenen Stakeholder hinweg.

[1] Laut eCH-0107 ist eine Domäne eine „Administrative / technische Gemeinschaft oder Organisation mit einer gemeinsamen Policy“ [eCH-0107].

Um STIAM im Überblick zu beschreiben, werden die aus [eCH-0107] definierten Prozesse (Zugriff kontrollieren, IAM definieren und IAM steuern) den Stakeholdern anhand einer einheitlichen Farbverwendung zugeordnet. Die Elemente *Zugriff kontrollieren* (zur Laufzeit) und *IAM definieren* (zur Definitionszeit) stellen die Kernprozesse dar, welche vom Subjekt und der Ressource genutzt werden. Diese Kernprozesse gelangen zu unterschiedlichen Zeitpunkten zur Anwendung, welche durch die hellblaue und dunkelblaue Farbe repräsentiert werden (vgl. Tabelle 1).

grau	Die Farbe Grau visualisiert Gremien, die **vor und während der Definitionszeit** aktiv sind. Vor der Definitionszeit wird die Domäne mit ihren Governance- und Management-Gremien aufgebaut und organisiert. Dieser Aufbau ist zwingend notwendig, damit die Prozesse der Definitions- und Laufzeit im gebildeten Vertrauensraum der Domäne für alle Beteiligten verlässlich und sicher ausgeführt werden können.
hellblau	Die hellblaue Farbe wird für die **Definitionszeit** verwendet, während der alle Informationen den Informationselementen zugeordnet (also definiert) werden.
dunkelblau	Die dunkelblaue Farbe wird für die **Laufzeit** verwendet. Zur Laufzeit wird der Zugriff basierend auf den definierten Informationselementen kontrolliert, gewährt oder abgelehnt.
hellgrün	Die hellgrüne Farbe wird konsequent für Realweltobjekte verwendet.

Tabelle 1: Farbverwendung in Abbildung 1

In Abbildung 1 und Abbildung 2 wird ausgehend von den oben geschilderten Stakeholdern die Geschäftsarchitektur von STIAM dargestellt.

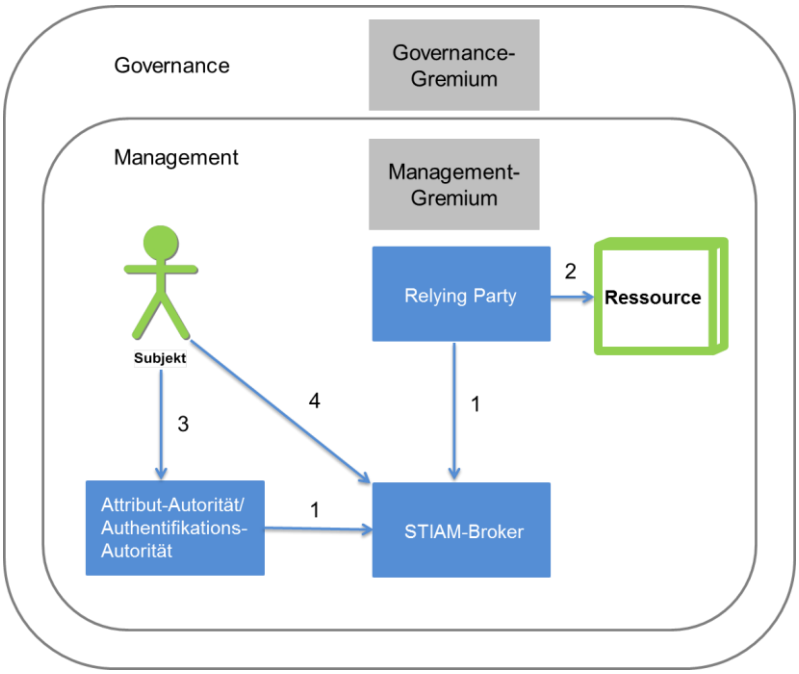

Abbildung 1: STIAM-Geschäftsarchitektur (Definitionszeit)

Während der **Definitionszeit** werden alle notwendigen Bedingungen geschaffen, damit zur Laufzeit geprüft werden kann, ob ein Subjekt auf eine Ressource zugreifen darf. In der nachfolgenden Aufzählung werden die nummerierten Pfeile in der Abbildung 1 beschrieben.

1. Die Relying Party (inklusive Ressource), die Attribut-Autorität und die Authentifikations-Autorität registrieren sich beim STIAM-Broker.
2. Die Relying Party definiert die Zugriffsrechte auf die Ressource.
3. Das Subjekt registriert sich bei der Authentifikations-Autorität und liefert der Attribut-Autorität die nötigen Daten.
4. Das Subjekt erstellt ein neues Konto beim STIAM-Broker und verlinkt seine Identitäten.

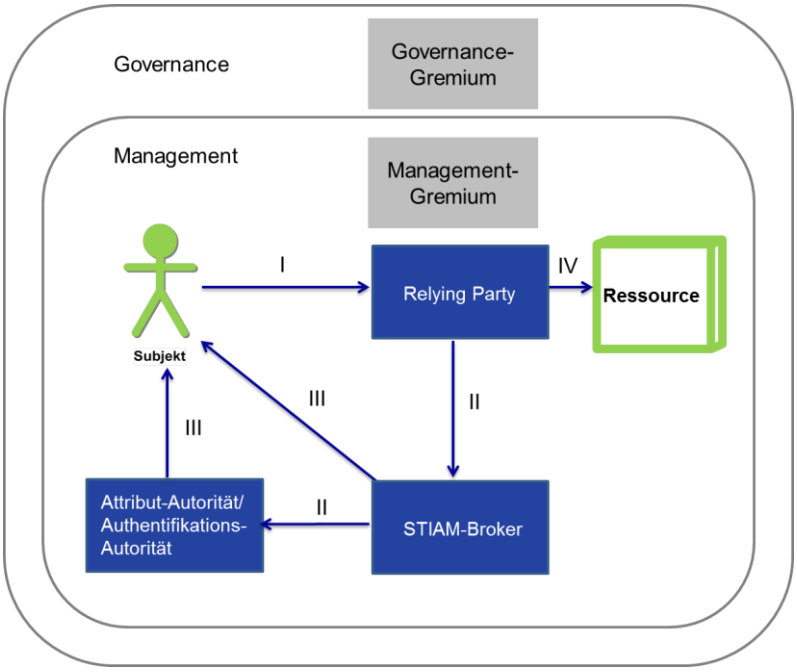

Abbildung 2: STIAM-Geschäftsarchitektur (Laufzeit)

Das Ziel der **Laufzeit** ist die kontrollierte und garantierte Einhaltung der Regeln für den Zugriff eines Subjekts auf eine Ressource im Vertrauensraum der Domäne. Das Zusammenspiel der Stakeholder zur Laufzeit läuft vereinfacht dargestellt wie folgt ab (vgl. dazu nummerierte Pfeile in Abbildung 2):

I. Das Subjekt will auf eine Ressource der Relying Party zugreifen.
II. Die Relying Party lässt sich die Identität des Subjektes durch die Authentifikations-Autorität und die entsprechenden Attribute zur weiteren Charakterisierung des Subjektes durch die Attribut-Autorität über den STIAM-Broker bestätigen.
III. Das Subjekt wird authentifiziert und erhält eine Anfrage zur Bestätigung der Übermittlung der Daten an die Relying Party.
IV. Die Relying Party lässt das Subjekt auf seine Ressource zugreifen.

2.2 Anwendungsgebiet und Abgrenzung

Anhand der Abbildung 3 kann der vorliegende Standard eCH-0169 STIAM-Geschäftsarchitektur positioniert werden (roter Rahmen). [eCH-0107] definiert generische Gestaltungsprinzipien, welche in verschiedenen Federation Konzepten und ergänzenden Hilfsmitteln konkretisiert werden. SuisseTrustIAM stellt eine Ausprägungsmöglichkeit des Hub-'n'-Spoke-Modells dar, das in [eCH-0107] unter den entsprechenden Identity Federation Konzepten präsentiert wird.

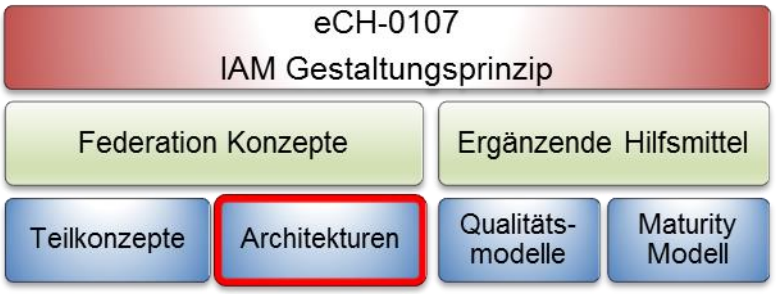

Abbildung 3: Positionierung des Standards eCH-0169 STIAM-Geschäftsarchitektur

2.3 Vorteile

Dieser Standard erzielt folgende Vorteile:

- Ermöglichen einer geschäftsorientierten Präsentation von STIAM.
- Konkretisieren von Abhängigkeiten sowie Governance- und Umsetzungsprinzipien für Domänen, die über STIAM föderiert werden.
- Präsentieren der Zusammenarbeit und Koordination der Stakeholder im STIAM-Umfeld zur Bildung eines einheitlichen Vertrauensraums einer Domäne.
- Darstellen der Form des Zusammenspiels der Rollen in Prozessen sowie Aufgaben und Beziehungsverhältnissen.
- Konkretisieren der Governance zur Sicherstellung eines Vertrauensraums in der Domäne.
- Aufzeigen der relevanten Prozesse in der STIAM-Geschäftsarchitektur.

2.4 Schwerpunkte

Der vorliegende Standard ist wie folgt aufgebaut:

- Das Kapitel 1 präsentiert den Status des Dokuments.
- Das Kapitel 2 präsentiert die Einleitung zur STIAM-Geschäftsarchitektur.
- Das Kapitel 3 präsentiert die im STIAM-Kontext auftretenden möglichen Stakeholder.
- Das Kapitel 4 beschreibt organisatorische Aspekte rund um die Governance im STIAM-Vertrauensraum ausgehend von einer Domäne.
- Das Kapitel 5 präsentiert Rollen sowie deren Aufgaben, die bei den verschiedenen STIAM-Stakeholdern vorkommen.
- Das Kapitel 6 widmet sich der Darstellung von Geschäftsprozessen, die bei STIAM-Stakeholdern zu integrieren sind, um das Zusammenspiel der Stakeholder im Vertrauensraum einer Domäne zu ermöglichen.

2.5 Normativer Charakter der Kapitel

Die Kapitel des vorliegenden Standards sind von normativem oder deskriptivem Cha-rakter. Die Tabelle 2 veranschaulicht die entsprechende Zuordnung.

Kapitel	Beschreibung
2 Einleitung	Deskriptiv
3 Stakeholder	Normativ
4 Organisation	Deskriptiv
5 Rollen	Normativ
5.2 Beschreibung der Rollen	Deskriptiv
6.1 Governance-Prozesse	Deskriptiv
6.2 Management-Prozesse	Deskriptiv
6.3 Kernprozesse	Normativ
6.4 Supportprozesse	Deskriptiv
Anhang A – Referenzen & Bibliografie	Deskriptiv
Anhang B – Mitarbeit & Überprüfung	Deskriptiv
Anhang C – Abkürzungen	Normativ
Fachlicher Anhang A – Vertrags- und Vereinbarungsarchitektur	Deskriptiv
Fachlicher Anhang B – Mögliche Struktur eines	Deskriptiv

STIAM-spezifischen Service Level Agreements	
Fachlicher Anhang C – Mögliche Policy-Elemente einer STIAM-Policy	Deskriptiv
Fachlicher Anhang D – COBIT-Prozess-Mapping mit STIAM-Gremien	Deskriptiv
Fachlicher Anhang E – ITIL-Prozess-Mapping mit STIAM-Stakeholder	Deskriptiv
Fachlicher Anhang F - Mapping zwischen COBIT und ITIL	Deskriptiv

Tabelle 2: Übersicht über normativen und deskriptiven Charakter der Kapitel des vorliegenden Standards

3 Stakeholder

Die Stakeholder und deren Aufgaben werden teilweise aus [eCH-0107] übernommen und wo nötig ergänzt und konkretisiert. Die Tabelle 3 präsentiert das Mapping der Stakeholder dieses Standards mit [eCH-0107].

Stakeholder eCH-0169 STIAM-Geschäftsarchitektur	Stakeholder [eCH-0107]
Attribut-Autorität, Authentifikations-Autorität, STIAM-Broker, andere STIAM-Broker	IAM-Dienstanbieter
Governance-Gremium, Management-Gremium	Regulator

Tabelle 3: Stakeholder-Mapping

Wie aus Tabelle 3 ersichtlich, werden die beiden [eCH-0107]-Stakeholder „IAM-Dienstanbieter“ und „Regulator“ im vorliegenden Standard konkretisiert.

In Abbildung 4 wird die für STIAM relevante Stakeholder-Struktur dargestellt.

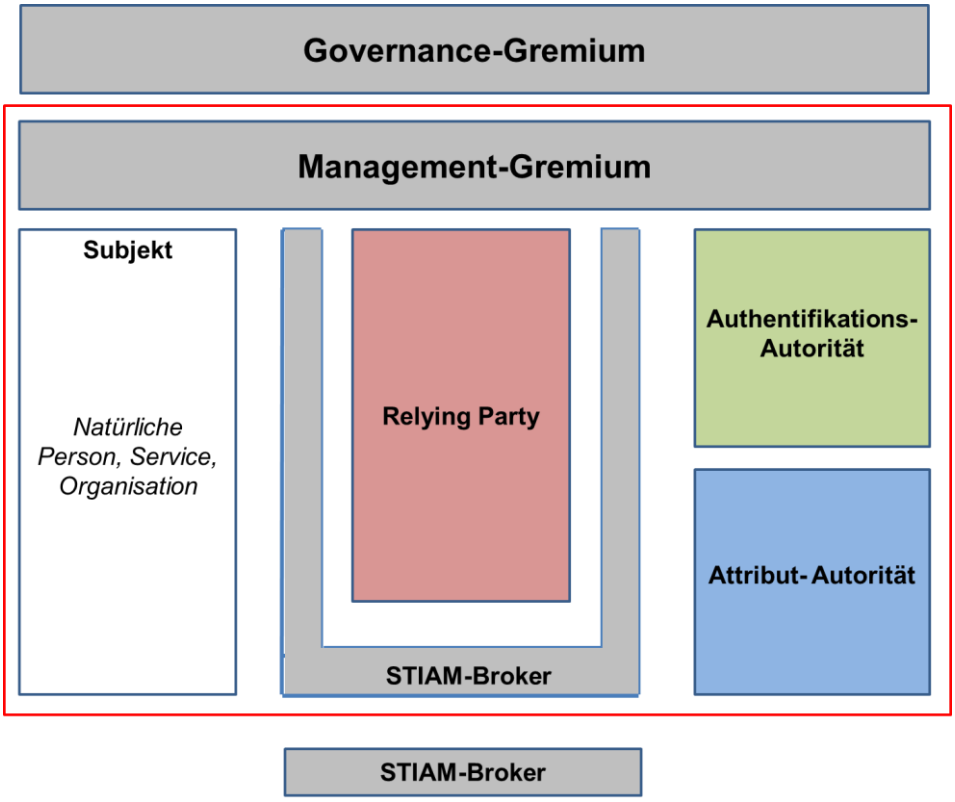

Abbildung 4: Übersichtsgrafik Stakeholder

Pro Domäne können mehrere STIAM-Broker, Subjekte, Relying Parties, Authentifikations- und Attribut-Autoritäten vorkommen. Entsprechende Stakeholder können als Stakeholder in mehreren Domänen vorkommen. Zudem kann ein Stakeholder gleichzeitig in mehreren Domänen involviert sein. Weiter wird über die Kommunikation zwischen Brokern die Zusammenarbeit zwischen verschiedenen Domänen sichergestellt.

Nachfolgend werden die in der Abbildung 4 differenzierten Stakeholder kurz beschrieben. Zusätzlich werden Aufgaben, Kompetenzen und Verantwortungen, welche teilweise aus [eCH-0107] abgeleitet wurden, näher definiert und den jeweiligen Stakeholdern zugeordnet. Die Aufgaben des Prozesses IAM steuern (Governance, Risk und Compliance) aus [eCH-0107] werden in diesem Kapitel vorausgesetzt und wo nötig ergänzt. Ausserdem wird in einem letzten Teil dargestellt, wie die neu definierten Gremien gebildet werden.

3.1 Subjekt

Subjekt	Dies ist eine natürliche Person, Organisation oder ein Service, der auf eine Ressource zugreift oder zugreifen möchte. Ein Subjekt wird durch digitale Identitäten beschrieben ([eCH-0107], Abbildung 19).

Aufgaben:

- Beschaffen einer Elektronischen Identität
- Entgegennehmen von Authentifizierungsmerkmalen
- Auswählen und nutzen von Ressourcen

Kompetenzen:

- Zustimmen zur Übermittlung von Authentication und Attribute Assertions

Verantwortung:

- Beweisen von Eigenschaften gegenüber Attribute Services
- Anwenden von Authentifizierungsmerkmalen

3.1.1 Natürliche Personen

Natürliche Person	Dies ist der Mensch in seiner Rolle als Rechtssubjekt, der auf Ressourcen einer Relying Party zugreifen will.

Hier werden keine Aufgaben erwähnt, da diese schon für das Subjekt konkretisiert wurden.

3.1.2 Service

Service	Ein Service ist eine Applikation, ein System, ein Gebäude, …, der auf Ressourcen von Relying Parties zugreift.

Hier werden keine Aufgaben erwähnt, da diese schon für das Subjekt konkretisiert wurden.

3.1.3 Organisation

Organisation	Organisatorische Einheit bestehend aus mehreren Subjekten (Juristische Person, Unternehmen, Verein, Amtsstelle, Gruppe von Subjekten, …) [eCH-0107].

Aufgaben:

- Definieren von Berechtigungen von Subjekten im STIAM-Kontext

Kompetenzen:

- Zuordnen von AKV's zu Rollen

Verantwortung:

- Klären der Rollen des Subjekts innerhalb der Organisation
- Regeln der Verwendung der Authentifizierungsmittel der Organisation

3.2 Relying Party

Relying Party	Diese stellt Services oder Informationen mittels Ressourcen zur Verfügung, auf welche das Subjekt zugreifen kann, falls es sich korrekt identifiziert und authentisiert hat und es auf Basis der benötigten Attribute ausgehend von einem Berechtigungskonzept autorisiert wurde [eCH-0107].

Aufgaben:

- Realisieren der nachstehenden Geschäftsservices gemäss [eCH-0107]
    - Zugang
    - Zugangsregel
    - Autorisation
    - Zugriffsrecht
    - eRessource
- [Optional] Erwerben und aufrechterhalten von ISO-Zertifizierungen (ISO/IEC 20000, ISO/IEC 27000, ISO/IEC 31000, ISO/IEC 38500)

Kompetenzen:

- Abschliessen von
    - Rahmenverträgen
    - Leistungsvereinbarungen und
    - Service Level Agreements mit STIAM-Broker

Verantwortung:

- Sicherstellen
    - interner Rollenzuordnungen
    - des Zugriffs auf die Ressource
    - der Policy-Implementierung
    - einer Vertretung im Governance-Gremium
    - einer Vertretung im Management-Gremium

3.3 STIAM-Broker

STIAM-Broker	Dieser stellt den eigentlichen Intermediärsdienst bereit, über den die Bestätigungen von erforderlichen Identitäten und Attributen zuhanden der Relying Party vermittelt werden.

Aufgaben:

- Realisieren von folgenden Geschäftsservices gemäss [eCH-0107]:
    - Trust
    - Broker
- [Optional] Erwerben und aufrechterhalten von ISO-Zertifizierungen (ISO/IEC 20000, ISO/IEC 27000, ISO/IEC 31000, ISO/IEC 38500)

Kompetenzen:

- Abschliessen von
  - Rahmenverträgen
  - Leistungsvereinbarungen
  - Service Level Agreements mit anderen Stakeholdern

Verantwortung:

- Sicherstellen
  - interner Rollenzuordnungen
  - von Policies
  - der Vertretung im Governance-Gremium
  - der Vertretung im Management-Gremium

3.4 Authentifikations-Autorität

Authentifikations-Autorität	Diese stellt einen Authentication Service zur Verfügung, gegen den sich das Subjekt authentifizieren kann. Der Authentication Service benutzt Credentials, die von einem Credential Service ausgestellt werden. Der Credential Service kann ein Bestandteil der AuthnA sein [eCH-0107].

Aufgaben:

- Realisieren nachfolgender Geschäftsservices gemäss [eCH-0107]:
  - eIdentity
  - Credential
  - Authentication
- [Optional] Erwerben und aufrechterhalten von ISO-Zertifizierungen (ISO/IEC 20000, ISO/IEC 27000, ISO/IEC 31000, ISO/IEC 38500).

Kompetenzen:

- Abschliessen von
  - Rahmenverträgen
  - Leistungsvereinbarungen
  - Underpinning Contracts[2]

Verantwortung:

- Sicherstellen
  - interner Rollenzuordnung
  - von Policies
  - der Vertretung im Governance-Gremium
  - der Vertretung im Management-Gremium

[2] Ein Underpinning Contract (Vertrag mit Drittparteien, UC) ist ein Vertrag zwischen einem STIAM-Broker und einer Attribut-Autorität oder Authentifikations-Autorität.

3.5 Attribut-Autorität

Attribut-Autorität	Dabei handelt es sich um ein Register oder ein sonstiges Verzeichnis mit einem Attribute Service zur Pflege von Attributen und einem Attribute Assertion Service zur Ausstellung von Attribute Assertions [eCH-0107].

Aufgaben:

- Realisieren von nachfolgender Geschäftsservices gemäss [eCH-0107]:
  - Attribute
  - Attribute Assertion
- [Optional] Erwerben und aufrechterhalten von ISO-Zertifizierungen (ISO/IEC 20000, ISO/IEC 27000, ISO/IEC 31000, ISO/IEC 38500).

Kompetenzen:

- Abschliessen von
  - Rahmenverträgen
  - Leistungsvereinbarungen
  - Underpinning Contracts

Verantwortung:

- Sicherstellen
  - interner Rollenzuordnungen
  - von Policies
  - der Vertretung im Governance-Gremium
  - der Vertretung im Management-Gremium

3.6 Governance-Gremium

Governance-Gremium	Dieses definiert die rechtlichen, prozessualen, organisatorischen, semantischen und technischen Rahmenbedingungen, innerhalb derer das föderierte IAM in einer Domäne abgewickelt wird.

Aufgaben:

- Ausüben von Steuerungskompetenzen über alle Stakeholder der Domäne
- Steuern des föderierten IAM in der Domäne
- Führen der Domäne ausgehend von Policies
- Evaluieren der Umsetzung der Governance
- Überwachen von Performance und Conformance der Domäne

Kompetenzen:

- Abschliessen von
  - Rahmenverträgen
  - Leistungsvereinbarungen
  - Underpinning Contracts
- Entscheiden
  - über Ein- und Ausschluss von Stakeholdern in der Domäne

  - bezüglich Beteiligung an und Zulassung der Zusammenarbeit mit anderen Domänen

Verantwortung:

- Sicherstellen, dass
  - ein Governance-Framework implementiert wird
  - auf Basis des STIAM-Service Wertbeiträge geliefert werden
  - das Risiko minimiert wird
  - die Ressourcen optimiert werden
  - Transparenz gegenüber Stakeholdern gegeben ist
  - Policies definiert und eingehalten werden
  - die Übertragung der Letzt-Verantwortlichkeit an einen Vertreter im Governance-Gremium erfolgt
  - erforderliche Betriebsmittel vorhanden sind

Zusammensetzung:

- Vertreter der Subjekte (im Falle von Unternehmen und sonstigen Institutionen Vertretung durch Delegierten der Organisation)
- Delegierter der Organisation der Relying Parties (bzw. deren Vertreter)
- Delegierter der Organisation der Attribut-Autoritäten (bzw. deren Vertreter)
- Delegierter der Organisation der Authentifikations-Autoritäten (bzw. deren Vertreter)
- Delegierter der Organisation des STIAM-Brokers (bzw. deren Vertreter)

3.7 Management-Gremium

Management-Gremium	Das Management-Gremium ist für die Umsetzung der durch das Governance-Gremium festgelegten Rahmenbedingungen in einer Domäne und für die entsprechende Domänenkoordination zuständig.

Aufgaben:

- Umsetzen der Vorgaben des Governance-Gremiums der Domäne
- Verwalten der Strategie und der Unternehmensarchitektur der Domäne
- Verwalten des STIAM-Service-Portfolios
- Verwalten von Budget und Kosten
- Koordinieren der Zusammenarbeit der Stakeholder
- Verwalten von organisatorischen Veränderungen (z.B. Einbinden von neuen Stakeholdern)

Kompetenzen:

- Gewährleisten von Qualität, Risikomanagement und Sicherheit

Verantwortung:

- Sicherstellen der Durchsetzung der Policy

Zusammensetzung:

- Vertreter der Subjekte (im Falle von Unternehmen und sonstigen Institutionen Vertretung durch Organisationsverantwortlichen für STIAM)
- Organisationsverantwortliche der Relying Parties (bzw. deren Vertreter)

- Organisationsverantwortliche der Attribut-Autoritäten (bzw. deren Vertreter)
- Organisationsverantwortliche der Authentifikations-Autoritäten (bzw. deren Vertreter)
- Organisationsverantwortliche der STIAM-Broker (bzw. deren Vertreter)
- Allenfalls weitere externe Vertreter, etwa zur STIAM-Umsetzung in der Domäne

4 Organisation

4.1 Übersicht

In Kapitel 4 werden wesentliche Organisationsprinzipien aus einer Domänen-Sicht formuliert, die für das Funktionieren des Vertrauensraums erforderlich sind. Die im Folgenden präsentierten Prinzipien beziehen sich auf die Abbildung 5 und die Abbildung 6.

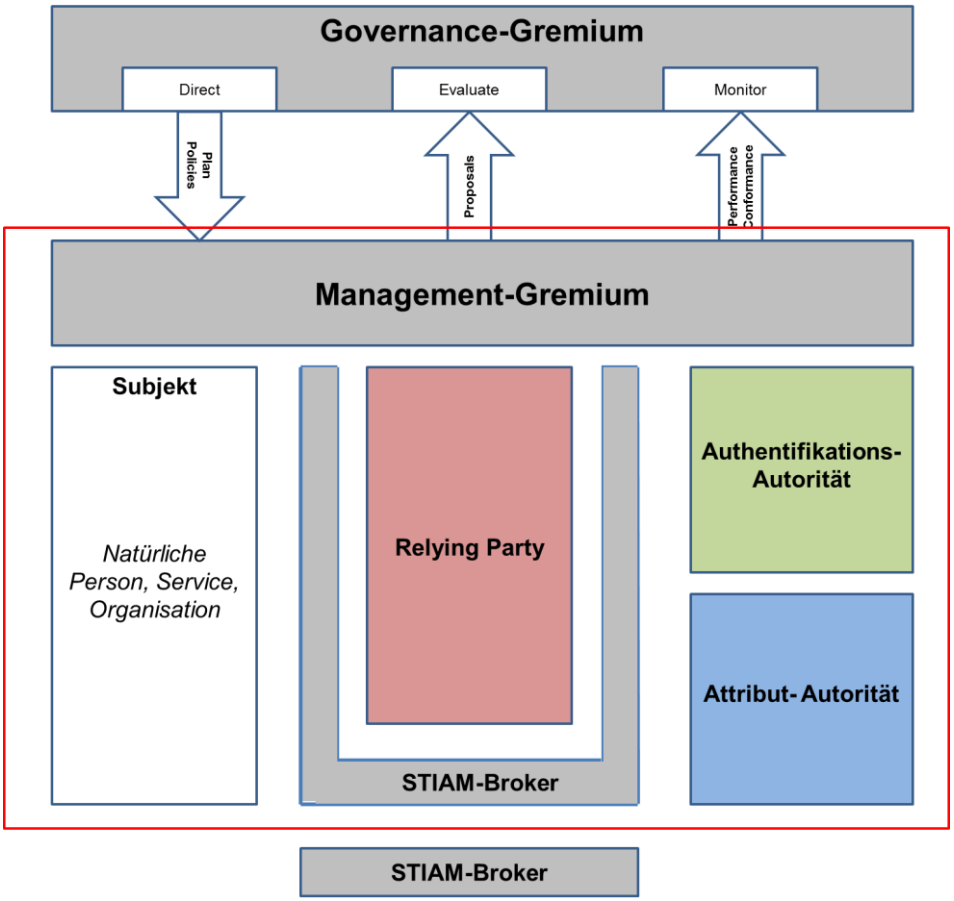

Abbildung 5: Relationen zwischen Governance- und Management-Ebene von STIAM basierend auf COBIT 5/ISO IEC 38500 ([ISACA 2012a], [ISACA 2012b], [ISO/IEC 38500])

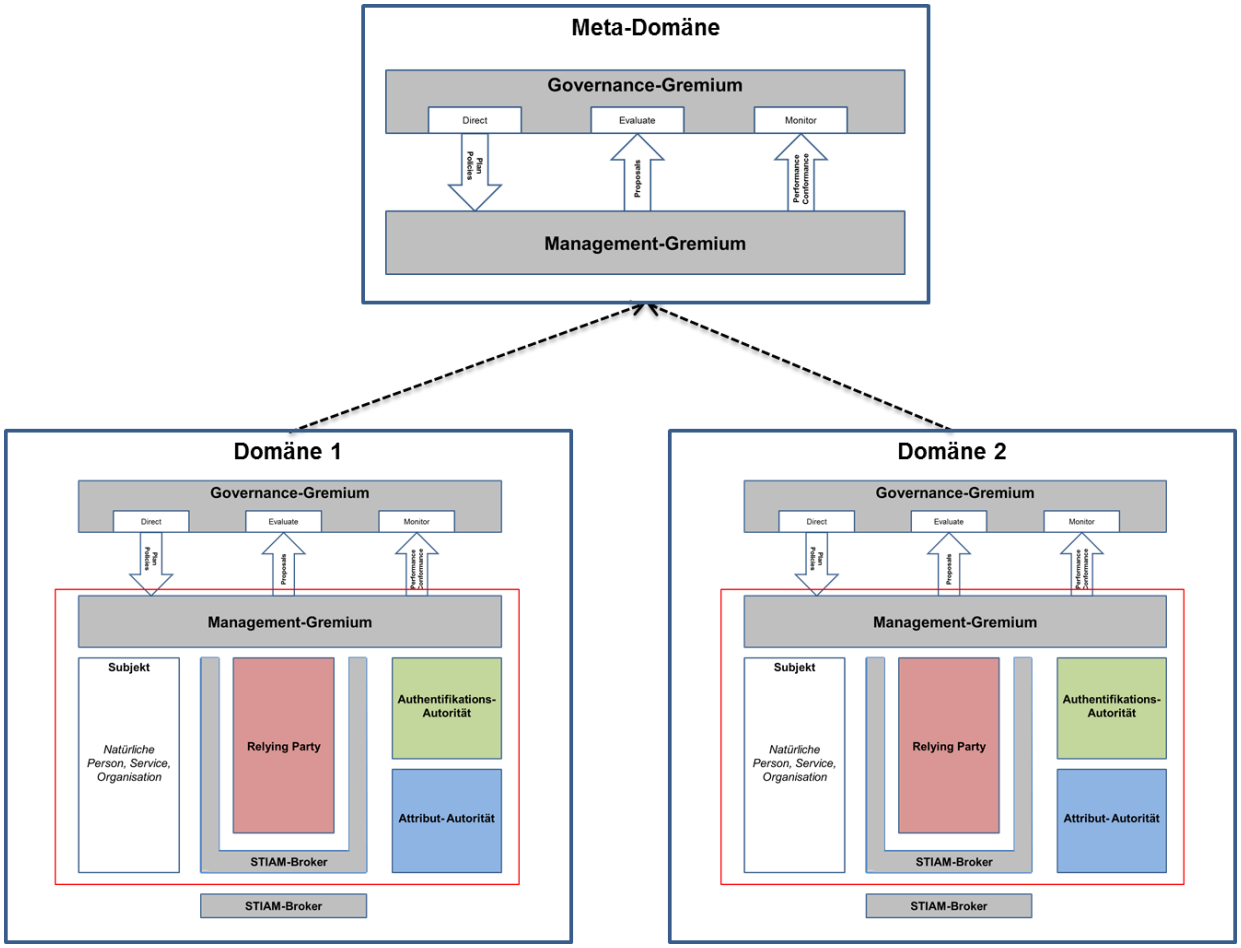

Abbildung 6: Vertretungsbeziehungen und -Hierarchie in Gremien im STIAM-Kontext

Minimal enthält die Meta-Domäne das Governance- und das Management-Gremium um sicherzustellen, dass die Steuerung, Harmonisierung sowie Umsetzung der Policies aus Sicht der Meta-Domäne über die eingeschlossenen Domänen gewährleistet ist.

4.2 Prinzipien zur Organisation von STIAM

Prinzip 1: Die STIAM-Leitung innerhalb einer Domäne ist aus Gründen der Gewaltenteilung in ein Governance- und ein Management-Gremium zu trennen.

STIAM erfordert ein Zusammenspiel der verschiedenen charakterisierten STIAM-Stakeholder. Dieses Zusammenspiel wird durch das Management-Gremium koordiniert. Das Management-Gremium wird durch das Governance-Gremium gemäss Kapitel 3.6 gesteuert und überwacht.

Prinzip 2: Die Bildung einer Domäne stellt die Voraussetzung für die Bildung von Meta-Domänen dar. Eine Meta-Domäne koordiniert eine oder mehrere Domänen.

In einem ersten Schritt geht es darum, verschiedene Domänen aufzubauen, welche zu einem späteren Zeitpunkt zu einer Meta-Domäne zusammengeschlossen werden können (siehe Abbildung 6). Die Governance der Meta-Domäne erfolgt nach den gleichen Prinzipien wie die Governance der Domäne.

Prinzip 3: Die Bildung der Domäne und des damit verbundenen Vertrauensraums wird aus Governance-Sicht durch Gesetzgebung, Regelungen und Policies sowie vertragliche Regelungen auf unterschiedlichen Ebenen und in verschiedenen Richtungen unterstützt.

Dies umfasst im Wesentlichen gesetzliche Regelungen, zu definierende Policies[3], vertragliche Regelungen (Rahmenverträge), Leistungsvereinbarungen, Service Level Agreements, Operational Level Agreements sowie Underpinning Contracts ausgehend vom IT-Serviceprovider oder Betreiber des STIAM-Brokers.[4]

Prinzip 4: Vertretungen in den Gremien können grundsätzlich von den Stakeholdern frei definiert werden.

Ein Vorschlag für die Vertretung der IAM-Dienstanbieter in den Gremien bieten die Kapitel 3.6 und 3.7.

- Das Governance-Gremium wird durch die Delegierten der Organisation repräsentiert, jedoch kann jeder Stakeholder frei wählen, welcher Delegierte im Governance-Gremium Einsitz nimmt.
- Das Management-Gremium wird durch die Organisationsverantwortlichen repräsentiert, jedoch kann jeder Stakeholder frei wählen, welcher Organisationsverantwortliche im Management-Gremium Einsitz nimmt.

Prinzip 5: Die Interaktion zwischen Governance- und Management-Gremium sowie den Stakeholdern ist als bidirektional (Top-Down sowie Bottom-Up gerichtet) zu verstehen.

Um die bestmögliche Governance der Domäne zu ermöglichen, braucht es (analog zu ISO/IEC 38500) sowohl Bottom-Up- als auch Top-Down-Kommunikation, Governance-Instrumente sowie Informationsflüsse (vgl. Abbildung 5). Top-Down- und Bottom-Up-Steuerungsinstrumente werden in Abbildung 5 durch die Bezeichnungen „Proposals, Reports zu Performance und Conformance“ sowie „Plan, Policies“ dargestellt.

Prinzip 6: Die Domäne einigt sich auf ein Governance-Rahmenwerk, das in der Domäne entsprechend durch- und umgesetzt wird.

Aus Domänen-Sicht erstellt das Governance-Gremium Policies und Pläne und überprüft die Umsetzung derselben durch das Management-Gremium. Dies erfordert u.a. auch die Prüfung dafür relevanter Prozesse. Als ein mögliches zu implementierendes Rahmenwerk zur Überprüfung von IT-Controls und IT-Prozessen bietet sich das Rahmenwerk COBIT (Control Objectives of Information and related Technology) an.[5]

Setzt die Domäne ein anderes und nicht das erwähnte Rahmenwerk ein, muss sie über ein Mapping Compliance zu COBIT nachweisen.

---

[3] Vgl. zum möglichen Inhalt einer Policy den Fachlichen Anhang C.

[4] Vgl. dazu den fachlichen Anhang A.

[5] Vgl. zu COBIT den fachlichen Anhang D.

Prinzip 7: Die STIAM-Laufzeitprozesse bauen auf einem Servicemanagement-Framework auf.

Im Gegensatz zur Ebene der Governance- und Management-Gremien haben die Kern- und Supportprozesse im STIAM-Umfeld (vgl. Kapitel 6) die effektive Bildung und Umsetzung von STIAM-Prozessen innerhalb von IAM-Dienstanbietern sowie über mehrere IAM-Dienstanbieter hinweg im Auge.

Hier bietet sich zur Unterstützung der organisationsübergreifenden Supportprozesse die Information Technology Infrastructure Library (ITIL) als mögliches Rahmenwerk an.[6]

Setzt die Domäne ein anderes und nicht das erwähnte Rahmenwerk ein, muss sie über ein Mapping Compliance zu ITIL nachweisen.

Prinzip 8: Das Management-Gremium setzt die vom Governance-Gremium definierten Massnahmen zur Schaffung eines „Vertrauensraums“ im Zusammenspiel der Stakeholder um.

Zu den Aufgaben des Management-Gremiums gehört die Umsetzung der Führungsentscheide in der Domäne und damit die Sicherstellung, dass der „Vertrauensraum“ geschaffen ist.

Prinzip 9: Die Domäne stellt zwischen unterschiedlichen Domänen und Föderierungskonzepten Interoperabilität sicher.

In der realen Welt ist von verschiedenen STIAM-Brokern und Föderierungskonzepten auszugehen [eCH-0107]. Die Domäne stellt sowohl zwischen STIAM(-ähnlichen)-Brokern und weiteren IAM-Föderierungskonzepten die Interoperabilität sicher.

[6] Vgl. zu ITIL den fachlichen Anhang E.

5 Rollen

Das Kapitel 5 befasst sich mit den Rollen, welche im STIAM-Kontext und bei dessen Stakeholdern auftreten. Dabei werden einerseits Rollen definiert, andererseits werden für die entsprechenden Rollen Aufgaben, Kompetenzen und Verantwortungen definiert.

5.1 Übersicht

Die verschiedenen Rollen werden in Tabelle 4 dargestellt, um die unterschiedlichen Entscheidungsbefugnisse und Entscheidungsbereiche zu charakterisieren.

Rolle	**Stakeholder**				
	Governance-Gremium	Management-Gremium	RP	STIAM-Broker	AA/AuthnA
Vorsitzender des Governance-Gremiums (strategische Rolle)	X				
Mitglieder des Governance-Gremiums (strategische Rolle)	X				
Vorsitzender des Management-Gremiums (strategische Rolle)		X			
Mitglieder des Management-Gremiums (strategische Rolle)		X			
Delegierter der Organisation (strategische Rolle)			X	X	X
Organisationsverantwortlicher (taktische Rolle)			X	X	X
OrgSysAdmin (operative Rolle)			X		X
STIAM-SysAdmin (operative Rolle)				X	

Tabelle 4: Rollen aus STIAM-Sicht

Das Subjekt wird nicht weiter berücksichtigt, da es im weiteren Verlauf dieses Kapitels nicht relevant ist. Ausgehend von den unterschiedlichen Aufgaben wird zwischen einem STIAM- und einem OrgSysAdmin unterschieden.

5.2 Beschreibung der Rollen

Im Folgenden werden die Rollen, welche in Tabelle 4 dargestellt sind mit ihren Aufgaben, Kompetenzen und Verantwortungen beschrieben.

5.2.1 Vorsitzender des Governance-Gremiums

Vorsitzender des Governance-Gremiums (VGG)	Der Vorsitzende des Governance-Gremiums wird vom Governance-Gremium gewählt und ist für dessen Führung zuständig.

Aufgaben:

- Führen und koordinieren des Governance-Gremiums
- Verantworten der Entscheide des Governance-Gremiums
- Kommuniziert gegenüber dem Vorsitzenden des Management-Gremiums bezüglich Policy-Anforderungen

Kompetenzen:

- Kommunizieren der Entscheide des Governance-Gremiums

Verantwortung:

- Übernehmen von Stichentscheiden bei Patt-Situationen
- Sicherstellen der Kommunikation mit dem Vorsitzenden des Management-Gremiums

5.2.2 Mitglieder des Governance-Gremiums

Mitglieder des Governance-Gremiums (MGG)	Die Mitglieder des Governance-Gremiums vertreten die entsprechenden Stakeholder im Governance-Gremium.

Aufgaben:

- Ausüben von Steuerungskompetenzen über alle Stakeholder der Domäne hinweg
- Steuern des föderierten IAM in der Domäne
- Führen der Domäne ausgehend von relevanten Policies
- Evaluieren der Umsetzung der Governance
- Überwachen von Performance und Conformance der Domäne

Kompetenzen:

- Abschliessen von
  - Rahmenverträgen
  - Leistungsvereinbarungen
  - Underpinning Contracts
- Entscheiden über Ein- und Ausschluss von Stakeholdern in der Domäne
- Entscheiden bezüglich Beteiligung an und Zulassung der Zusammenarbeit mit anderen Domänen

Verantwortung:

- Sicherstellen, dass
  - ein Governance-Framework implementiert wird
  - Wertbeiträge geliefert werden

- das Risiko minimiert wird
- die Ressourcen optimiert werden
- Transparenz gegenüber Stakeholdern gegeben ist
- Policies definiert und eingehalten werden
- die Übertragung der Letzt-Verantwortlichkeit an einen Vertreter im Governance-Gremium erfolgt
- erforderliche Betriebsmittel vorhanden sind

5.2.3 Vorsitzender des Management-Gremiums

Vorsitzender des Management-Gremiums (VMG)	Der Vorsitzende des Management-Gremiums trägt die Verantwortung für die Entscheide des Management-Gremiums.

Aufgaben:

- Führen und koordinieren des Management-Gremiums
- Verantworten der Entscheide des Management-Gremiums
- Kommuniziert gegenüber dem Vorsitzenden des Governance-Gremiums bezüglich Umsetzung

Kompetenzen:

- Kommunizieren der Entscheide des Management-Gremiums

Verantwortung:

- Übernehmen von Stichentscheiden bei Patt-Situationen
- Sicherstellen der Kommunikation mit dem Vorsitzenden des Governance-Gremiums

5.2.4 Mitglieder des Management-Gremiums

Mitglieder des Management-Gremiums (MMG)	Die Mitglieder des Management-Gremiums vertreten die entsprechenden Stakeholder im Management-Gremium.

Aufgaben:

- Umsetzen der Vorgaben des Governance-Gremiums der Domäne
- Verwalten der Strategie und der Unternehmensarchitektur der Domäne
- Verwalten des STIAM-Service-Portfolios
- Verwalten von Budget und Kosten
- Koordinieren der Zusammenarbeit der Stakeholder
- Verwalten von organisatorischen Veränderungen (z.B. Einbinden von neuen Stakeholdern)

Kompetenzen:

- Gewährleisten von Qualität, Risikomanagement und Sicherheit

Verantwortung:

- Sicherstellen der Durchsetzung der Policy

5.2.5 Delegierter der Organisation

Delegierter der Organisation (Del.)	Der Delegierte der Organisation ist ein Vertreter der Geschäftsleitung und kann ins Governance-Gremium delegiert werden.

Aufgaben:

- Kommunizieren und sicherstellen der Einhaltung von Policies
- Repräsentieren der Domäne nach aussen zusammen mit anderen Delegierten der Organisation

Kompetenzen:

- Aushandeln und überwachen der Verträge und Vereinbarungen (Rahmenvertrag; Mitarbeiten bei der Aushandlung und Umsetzung der Leistungsvereinbarung[7])
- Führen der STIAM-Umsetzung in der Organisation
- Führen und beaufsichtigen des Organisationsverantwortlichen
- Vertreten der Geschäftsleitung und deren Interessen im Governance-Gremium

Verantwortung:

- Sicherstellen der Eskalationsinstanz in Vertragsfragen
- Sicherstellen der Korrektheit der Informationen in der Domäne und im STIAM-Kontext
- Wahrnehmen der letztlichen Verantwortung für die STIAM- und IAM-Implementierung

5.2.6 Organisationsverantwortlicher

Organisationsverantwortlicher (OV)	Der Organisationverantwortliche kann ins Management-Gremium delegiert werden.

Aufgaben:

- Unterstützen des Delegierten der Organisation beim Abschluss der Rahmenverträge im STIAM-Kontext
- Ausgestalten und Umsetzen von Policies

Kompetenzen:

- Abschliessen und sicherstellen von Leistungsvereinbarungen und Service Level Agreements
- Vertreten der Organisation im Management-Gremium
- Führen und beaufsichtigen des OrgSysAdmin/STIAM-SysAdmin
- Einbringen der Organisationsrichtlinien in das Management-Gremium

Verantwortung:

- Pflegen organisationsrelevanter Daten
- Sicherstellen der Eskalationsinstanz bei Streitfragen im Rahmen von Service Level Agreements und Leistungsvereinbarungen

[7] Vgl. dazu fachliche Anhänge A und B.

5.2.7 Organisations-SysAdmin

Organisations-SysAdmin (OSA)	Der OrgSysAdmin ist verantwortlich für die Systemadministration der Fachanwendungen (Ressourcen), auf die Subjekte zugreifen.

Aufgaben:

- Operationalisieren, implementieren sowie sicherstellen der STIAM-Policies sowie deren Umsetzung
- Pflegen von Verzeichnissen mit STIAM-relevanten Daten zur Organisation
- Verwalten
    - von Attributen sowie deren Qualität
    - der Identität sowie deren Qualität
    - der Organisationen
    - von Ressourcen
- Unterstützen des Organisationsverantwortlichen beim Monitoring durch Reporting

Verantwortung:

- Sicherstellen eines proaktiven, reaktiven und nachvollziehbaren Handelns in Bezug auf die Datenqualität gemäss Anforderungen

5.2.8 STIAM-SysAdmin

STIAM-SysAdmin (SSA)	Der STIAM-SysAdmin ist verantwortlich für die Systemadministration des STIAM-Brokers.

Aufgaben:

- Operationalisieren, implementieren und weiterentwickeln des STIAM-Services sowie der STIAM-Policies aus Sicht des STIAM-Brokers
- Unterstützen des Organisationsverantwortlichen beim Monitoring durch Reporting
- Administrieren von Daten zu Delegierten der Organisation
- Administrieren von Daten zu Organisationsverantwortlichen

Verantwortung:

- Sicherstellen eines proaktiven, reaktiven und nachvollziehbaren Handelns in Bezug auf den STIAM-Service und dessen Qualität gemäss Anforderungen
- Sicherstellen eines sicheren Betriebs zur Gewährleistung des Vertrauensraums

6 Prozesse

Wie in Kapitel 2.1 erwähnt wird, basiert die Interaktion zwischen den STIAM-Stakeholdern im Wesentlichen auf den grundlegenden Prozessen, wie sie in Abbildung 7 dargestellt werden. Diese Prozesse laufen zwischen mehreren IAM-Dienstanbietern ab. Dies erfordert eine Erweiterung des Prozess-Rahmenwerks aus Geschäftsarchitektursicht um Governance-, Management- sowie Supportprozesse. Die Kernprozesse zur Definitions- und zur Laufzeit entsprechen [eCH-0107].

Als Grundlage für die Definition der generischen STIAM-Governance und STIAM-Management-Prozesse wird auf die IT-Governance verwiesen. Ein hierfür breit abgestütztes und branchenübergreifend eingesetztes Rahmenwerk ist COBIT 5, in das neuerdings der bereits erwähnte ISO/IEC-Standard 38500 integriert ist. Dabei werden die Prozesse nicht als auszuführende, sondern als zu steuernde oder zu überwachende Prozesse verstanden.

Der STIAM-Service stellt ein Service wie jeder andere IT-Service dar. Für das IT-Servicemanagement gelangt in der Industrie der ITIL-Standard als weiteres Best-Practice-Framework zum Einsatz. Daher wird bezüglich der STIAM-Supportprozesse in diesem Kapitel auf der ITIL 2011 edition aufgesetzt. Dieses Best-Practice-Framework ist teilweise mit dem in diesem Standard ebenfalls erwähnten ISO/IEC 20000 Standard abgeglichen. Dabei werden Servicemanagement-Prozesse als auszuführende Prozesse verstanden, die sicherstellen, dass den Kunden durch die Serviceerbringung ein Nutzen entsteht.

Das Mapping zwischen den steuernden Prozessen (COBIT/Governance und Management) und den zu implementierenden Prozessen (ITIL/IT-Servicemanagement) wird im Anhang F grob tabellarisch dargestellt.

Die Abbildung 7 stellt die STIAM-Prozesslandkarte dar. Die entsprechenden Governance-, Management-, sowie Supportprozesse werden im folgenden Kapitel detaillierter beschrieben. Sie werden in dieser Form in [eCH-0107] nicht erwähnt.

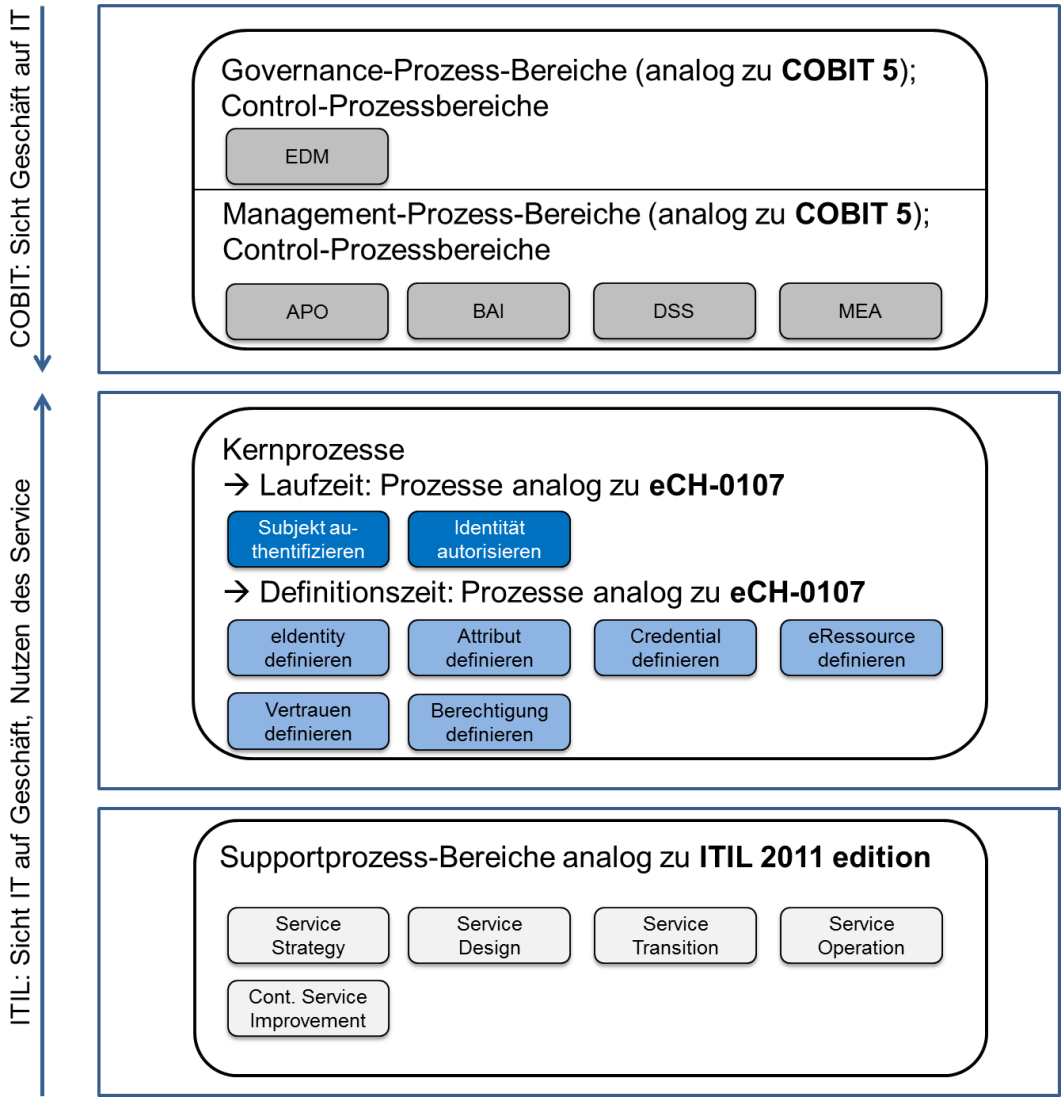

Abbildung 7: STIAM-Prozesslandkarte

6.1 Governance-Prozesse

In den Kapiteln 6.1 und 6.2 wird definiert, welche COBIT-Governance- und COBIT-Management-Prozesse für STIAM notwendig sind. Ausserdem wird anhand von RACI-Charts[8] bestimmt, welche STIAM-Rolle für welchen Prozess zuständig ist. Die vollständige Liste der COBIT-Prozesse mit der Kategorisierung empfehlenswert, vernachlässigbar und nicht relevant befindet sich im Anhang D.

[8] In der RACI-Chart-Methodik stehen die Buchstaben R für Responsible (Durchführungszuständigkeit), A für Accountable (Letztverantwortung), C für Consulted (zu konsultieren), I für Informed (zu Informieren).

Governance-Prozesse	Über die Governance-Prozesse wird sichergestellt, dass in einer STIAM-Domäne die Implementierung eines Governance-Rahmenwerks, der Mehrwert, die Risikominimierung sowie die Transparenz über alle IAM-Dienstanbieter erreicht werden.

Evaluate, Direct and Monitor (EDM)

Prozesse	**Rollen**					
	MGG	MMG	Del.	OV	OSA	SSA
Sicherstellen und beauftragen der Einrichtung und Pflege des (STIAM-)Governance-Rahmenwerks.	A	C	R	C	I	I
Sicherstellen und beauftragen der Bereitstellung von Mehrwert (durch den STIAM-Service).	A	C	R	C	I	I
Sicherstellen und beauftragen der Risikominimierung bezüglich STIAM.	A	C	R	C	I	I
Sicherstellen und beauftragen der Ressourcenoptimierung bezüglich des STIAM-Services	A	C	R	C	I	I
Sicherstellen der Transparenz gegenüber allen Stakeholdern in der STIAM-Domäne und darüber hinaus.	A	C	R	C	I	I

Tabelle 5: RACI-Chart EDM

6.2 Management-Prozesse

Management-Prozesse	Über die Management-Prozesse wird sichergestellt, dass die STIAM-Domäne operativ lauffähig wird und die entsprechenden Vorgaben aus den Governance-Prozessen umgesetzt werden.

Align, Plan and Organize (APO)

Prozesse	**Rollen**					
	MGG	MMG	Del.	OV	OSA	SSA
Sicherstellen, dass für STIAM ein entsprechendes Governance-Rahmenwerk implementiert ist.	C	A	I	R		
Sicherstellen, dass eine Domänen-weite STIAM-Strategie definiert und verabschiedet ist.	C	A	I	R		
Sicherstellen, dass eine STIAM-Architektur entwickelt, implementiert und weiterentwickelt wird.	C	A	I	R		
Sicherstellen, dass ein STIAM-Serviceportfolio aufgebaut und eingebunden wird.	C	A	I	R		
Sicherstellen, dass kontinuierlich die für STIAM relevanten finanziellen und personellen Ressourcen bereitgestellt werden.	C	A	I	R		
Sicherstellen der Beziehungen zwischen den Stakeholdern.	C	A	I	R		
Sicherstellen der Service-Level-Vereinbarungen	C	A	I	R		
Sicherstellen, dass die Qualität von STIAM gewährleistet ist.	C	A	I	R		
Sicherstellen eines angemessenen Risikomanagements.	C	A	I	R		
Sicherstellung der Sicherheit von STIAM.	C	A	I	R		

Tabelle 6: RACI-Chart APO

Build, Acquire and Implement (BAI)

Prozesse	Rollen					
	MGG	MMG	Del.	OV	OSA	SSA
Sicherstellen, dass über alle Beteiligten hinweg für STIAM adäquate Kapazitäten und Verfügbarkeiten vorhanden sind.	C	A	I	R		
Sicherstellen, dass, rund um STIAM adäquate organisatorische Änderungen vorgenommen werden, sodass die Nutzung des STIAM-Services möglichst effizient und effektiv erfolgt und die Schaffung des Vertrauensraums den Stakeholdern in der Domäne den grösstmöglichen Nutzen stiftet.	C	A	I	R		
Sicherstellen, dass für STIAM ein effizient und effektiv organisiertes Change Management betrieben wird und Änderungen systematisch dokumentiert und abgenommen werden.	C	A	I	R	I	I
Sicherstellen, dass die Betriebsmittel verwaltet werden.	C	A	I	R		

Tabelle 7: RACI-Chart BAI

Deliver, Service and Support (DSS)

Prozesse	Rollen					
	MGG	MMG	Del.	OV	OSA	SSA
Sicherstellen des Betriebs des STIAM-Service.	C	A	I	R		
Sicherstellen eines für die STIAM-Mitinvolvierten adäquaten Managements von Service Requests und Incidents.	C	A	I	R		
Sicherstellen einer STIAM-adäquaten Form des Continuity Managements hinsichtlich Katastrophen ausgehend von Business-Continuity-Anforderungen.	C	A	I	R		
Sicherstellen eines für STIAM-Zwecke adäquaten Managements der Informationssicherheit und eines entsprechenden Sicherheitssystems.	C	A	I	R	I	I
Sicherstellen der Geschäftsprozesskontrollen	C	A	I	R		

Tabelle 8: RACI-Chart DSS

Monitor, Evaluate and Assess (MEA)

Prozesse	Rollen					
	MGG	MMG	Del.	OV	OSA	SSA
Überwachen, Evaluieren und Beurteilen von Leistung und Konformität des STIAM-Services.	C	A	I	R	C	C
Überwachen, Evaluieren und Beurteilen des internen Kontrollsystems in Relation zum STIAM-Service.	C	A	I	R	I	I
Überwachen, Evaluieren und Beurteilen der Compliance mit externen Anforderungen bezüglich STIAM-Service.	C	A	I	R	I	I

Tabelle 9: RACI-Chart MEA

6.3 Kernprozesse

Kernprozesse	Die Kernprozesse umfassen alle Prozesse der Definitions- und Laufzeit gemäss [eCH-0107].

Auf eine detaillierte Beschreibung wird verzichtet und dazu auf [eCH-0107] verwiesen.

6.4 Supportprozesse

Im Folgenden werden die STIAM-Supportprozesse konkretisiert.

Wie erwähnt stellt das auf diesen Bereich zugeschnittene Rahmenwerk ITIL 2011 edition dar. Im Folgenden wird auf die darin thematisierten notwendigen Prozesse/-gruppen eingegangen und es wird zusätzlich spezifiziert, wie diese im STIAM-Kontext zur Anwendung gelangen können. Die vollständige Liste der ITIL-Prozesse mit der Kategorisierung empfehlenswert, vernachlässigbar und nicht relevant befindet sich im Anhang E.

Supportprozesse	Die Supportprozesse umfassen das IT-Servicemanagement und beschreiben Anforderungen an die Einrichtung und den Betrieb der STIAM-IT-Services durch IT-Serviceprovider.

Service Strategy

- Strategy Management for IT-Services: Umsetzen einer adäquaten Strategie für STIAM aus IT-Service-Sicht.
- Service Portfolio Management: Führen einer Entwicklungs-Pipeline zu STIAM-Services, Führen des STIAM-Services im Servicekatalog (des STIAM Service Providers), Führen von Retired Services im STIAM-Kontext.
- Financial Management: Umsetzen des Managements von Budgetierung rund um den STIAM-Service seitens STIAM-Broker, Kostenrechnung zum STIAM-Service sowie Verrechnung des STIAM-Services, sofern laut Geschäftsmodell eine Verrechnung angedacht ist.
- Business Relationship Management: Dies umfasst das strategische Beziehungsmanagement zwischen den beteiligten Stakeholdern, was den STIAM Broker Service betrifft.
- Demand Management: Strategisches Management der Nachfrage nach STIAM-Services und deren Abstimmung mit der bereitzustellenden Kapazität des STIAM Services.

Service Design

- Service Catalogue Management: Dokumentation und laufende Pflege des STIAM-Services im Kunden- und im Technischen Servicekatalog
- Service Level Management: Entgegennehmen und Aufnehmen von Service Level Requests, Umsetzen von Service Levels sowie Management der Service- und Opera-

tional Level Agreements sowie Underpinning Contracts in Relation zu STIAM-SLA's.[9] Dies stellt eine zentrale Voraussetzung für die Bildung eines Vertrauensraums dar.

- Capacity Management: Umsetzen der Planung und Qualität der STIAM-Service-Kapazität zu adäquaten Kosten ausgehend von den Anforderungen des Geschäfts an die Kapazität.
- Availability Management: Prüfen der adäquaten Umsetzung der erforderlichen Verfügbarkeit des STIAM-Service analog dem Service Level Agreement sowie deren Absicherung durch Operational Level Agreements (innerhalb des Service Providers) und Underpinning Contracts (zu Lieferanten).
- IT Service Continuity Management: Planen und Umsetzen einer adäquaten Kontinuität des STIAM-Services im Katastrophenfall ausgehend von Geschäftsanforderungen.
- Information Security Management: Umsetzen einer adäquaten Informationssicherheit bezüglich STIAM-Service und Etablierung eines STIAM-Sicherheitssystems.

Service Transition

- Change Management: Umsetzen eines systematischen und dokumentierten Änderungsmanagements bezüglich STIAM-Services.
- Service Asset and Configuration Management: Umsetzen einer korrekten Dokumentierung von STIAM-Services über alle beteiligten Stakeholder hinweg.

Service Operation

- Incident Management: Umsetzen eines Incident Managements über alle beteiligten Stakeholder im STIAM-Kontext hinweg.
- Request Fulfillment: Umsetzen eines adäquaten Request Fulfillments über alle beteiligten STIAM-Partner hinweg hinsichtlich primären und sekundären STIAM-Services.
- Access Management: Sicherstellung eines adäquaten Zugangsmanagements zum STIAM-Service.
- Problem Management: Sicherstellung eines adäquaten Problem Managements hinsichtlich STIAM Service über alle beteiligten STIAM-Stakeholder hinweg.

Continual Service Improvement

- Seven-step Improvement Process: Umsetzen eines adäquaten Verbesserungsprozesses bezüglich STIAM-Service über alle beteiligten Stakeholder hinweg.

[9] Vgl. hierzu die fachlichen Anhänge A und B.

7 Haftungsausschluss/Hinweise auf Rechte Dritter

eCH-Standards, welche der Verein **eCH** dem Benutzer zur unentgeltlichen Nutzung zur Verfügung stellt, oder welche **eCH** referenziert, haben nur den Status von Empfehlungen. Der Verein **eCH** haftet in keinem Fall für Entscheidungen oder Massnahmen, welche der Benutzer auf Grund dieser Dokumente trifft und / oder ergreift. Der Benutzer ist verpflichtet, die Dokumente vor deren Nutzung selbst zu überprüfen und sich gegebenenfalls beraten zu lassen. **eCH**-Standards können und sollen die technische, organisatorische oder juristische Beratung im konkreten Einzelfall nicht ersetzen.

In **eCH**-Standards referenzierte Dokumente, Verfahren, Methoden, Produkte und Standards sind unter Umständen markenrechtlich, urheberrechtlich oder patentrechtlich geschützt. Es liegt in der ausschliesslichen Verantwortlichkeit des Benutzers, sich die allenfalls erforderlichen Rechte bei den jeweils berechtigten Personen und/oder Organisationen zu beschaffen.

Obwohl der Verein **eCH** all seine Sorgfalt darauf verwendet, die **eCH**-Standards sorgfältig auszuarbeiten, kann keine Zusicherung oder Garantie auf Aktualität, Vollständigkeit, Richtigkeit bzw. Fehlerfreiheit der zur Verfügung gestellten Informationen und Dokumente gegeben werden. Der Inhalt von **eCH**-Standards kann jederzeit und ohne Ankündigung geändert werden.

Jede Haftung für Schäden, welche dem Benutzer aus dem Gebrauch der **eCH**-Standards entstehen ist, soweit gesetzlich zulässig, wegbedungen.

8 Urheberrechte

Wer **eCH**-Standards erarbeitet, behält das geistige Eigentum an diesen. Allerdings verpflichtet sich der Erarbeitende sein betreffendes geistiges Eigentum oder seine Rechte an geistigem Eigentum anderer, sofern möglich, den jeweiligen Fachgruppen und dem Verein **eCH** kostenlos zur uneingeschränkten Nutzung und Weiterentwicklung im Rahmen des Vereinszweckes zur Verfügung zu stellen.

Die von den Fachgruppen erarbeiteten Standards können unter Nennung der jeweiligen Urheber von **eCH** unentgeltlich und uneingeschränkt genutzt, weiterverbreitet und weiterentwickelt werden.

eCH-Standards sind vollständig dokumentiert und frei von lizenz- und/oder patentrechtlichen Einschränkungen. Die dazugehörige Dokumentation kann unentgeltlich bezogen werden.

Diese Bestimmungen gelten ausschliesslich für die von **eCH** erarbeiteten Standards, nicht jedoch für Standards oder Produkte Dritter, auf welche in den **eCH**-Standards Bezug genommen wird. Die Standards enthalten die entsprechenden Hinweise auf die Rechte Dritter.

Anhang A – Referenzen & Bibliographie

[Cannon 2011] Cannon, D. (2011): ITIL Service Strategy 2011 edition, TSO, Norwich.

[eCH-0107] eCH-0107 (2013): Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM). eCH. Zürich.

[Hunnebeck 2011] Hunnebeck, L. (2011): ITIL Service Design 2011 edition, TSO, Norwich.

[ISACA 2012a] ISACA (2012a): COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT, Rolling Meadows.

[ISACA 2012b] ISACA (2012b): COBIT 5 – Enabling Processes, Rolling Meadows.

[Lloyd 2011] Lloyd, V. (2011): ITIL Continual Service Improvement 2011 dition, TSO, Norwich.

[Prengemann 2006] Prengemann, U. (2006): SLAs und Leistungsvereinbarungen: Potentiale für Anwender und Dienstleister in der ÖV. http://www.gartner.de/events/0609gt/prengemann.pdf ((Aufruf per 2013-11-26).

[Rance 2011] Rance, S. (2011): ITIL Service Transition 2011 edition, TSO, Norwich.

[Steinberg 2011] Steinberg, R. (2011): ITIL Service Operation 2011 edition, TSO, Norwich.

Anhang B – Mitarbeit & Überprüfung

- Stefan Agosti, BFH
- Ronny Bernold, BFH
- Olivier Brian, BFH
- Jerome Brugger, BFH
- Marcel Eberle, Kanton St. Gallen
- Hans Häni, BFH
- Gerhard Hassenstein, BFH
- Thomas Selzam, BFH
- Andreas Spichiger, BFH
- Martin Topfel, BFH

Anhang C – Abkürzungen

AKV	Aufgaben, Kompetenzen und Verantwortung
APO	COBIT-Domäne Align, Plan, Organize
BAI	COBIT-Domäne Build, Acquire, Implement
COBIT	Control Objectives for Information and Related Technology
DSS	COBIT-Domäne Deliver, Service, Support,
EDM	COBIT-Domäne Evaluate, Direct, Monitor
E-Economy	Electronic Economy
E-Education	Electronic Education
E-Government	Electronic Government
E-Health	Electronic Health
IAM	Identity and Access Management
ISO/IEC	International Standardization Organisation / International Electrotechnical Commission
ITIL	Information Technology Infrastructure Library
MEA	COBIT-Domäne Monitor, Evaluate, Assess

Fachliche Anhänge

Fachlicher Anhang A – Vertrags- und Vereinbarungsarchitektur

Im Rahmen der STIAM-Serviceerbringung können verschiedene Arten von Verträgen unterschieden werden, welche typischerweise als Ganzes in einer Vertragsarchitektur (Abbildung 8) zusammengeführt werden. Die Idee hinter der Trennung der entsprechenden Vertrags- und Vereinbarungsarten ist, dass die generellen Vertragsaspekte nicht in jedem SLA einzeln, sondern auf der Vertragsebene der Rahmenverträge und Leistungsvereinbarungen geregelt werden. Weitere Details zur Charakterisierung der verschiedenen vertraglichen Dokumentenarten sind in Abbildung 8 aufgeführt.

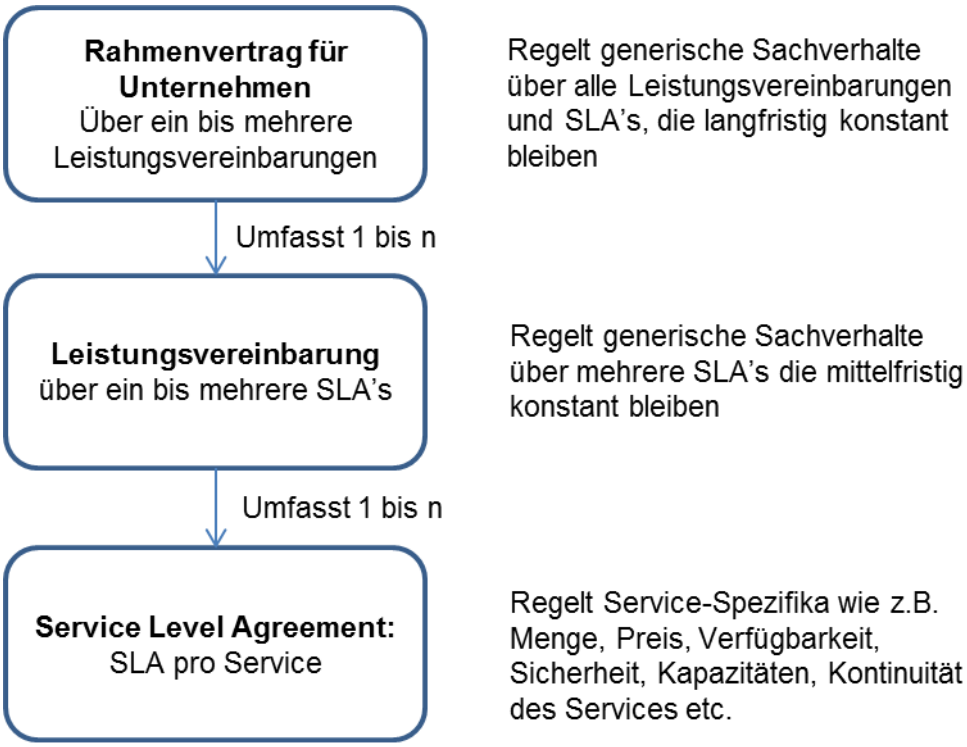

Abbildung 8: Vertragsarchitektur im SLA-Kontext (nach [Prengemann 2006])

Fachlicher Anhang B – Mögliche Struktur eines STIAM-spezifischen Service Level Agreements (SLA)

Im Folgenden wird der mögliche Inhalt eines SLA's für den STIAM-Service konkretisiert ([Hunnbeck 2011], [Steinbeck 2011]). Mit Ausnahme der STIAM-spezifischen Elemente (kursiv), entstammen die SLA-Elemente [Hunnebeck 2011] und [Steinberg 2011] (ITIL 2011 edition/Best Practice).

- Amendment Sheet – Change History Dokument, etc.
- SLA zwischen Partei 1 und Partei 2 mit den jeweiligen Adressen
- SLA betreffend Service X/Y/Z
- Dauer der Gültigkeit des SLA's
- Signaturen/Unterschriften
- Service Beschreibung
- Scope des Service Level Agreements
- Servicezeiten (-Stunden)
- Service Verfügbarkeit
- Reliability – Zuverlässigkeit des Services
- Kunden Support
- Kontaktpunkte und Eskalationen
- Service Performance
- Servicefunktionalität
- Change Management
- Service Continuity
- Sicherheit(saspekte)
- Verantwortlichkeiten
- Verrechnung, Formeln, Preise, Mengen, Verrechnungszeiträume, Strafzahlungen, …
- Service Reporting und Reviews
- *Vereinbarung für Qualitäts- und Vertrauenslevels z.B. auf Basis von QAA*
- *Attributqualitäts-Definition*
- *Attributlisten, Vereinbarungen zu Semantik und Syntax, etc., Befüllungs-Regeln zu Datenbanken auf dem STIAM-Broker*
- *Domänengrenzen-Definition*
- *Spezielle Vereinbarungen zur Funktion und zum Zusammenspiel von Governance- und Management-Gremien*
- *Vereinbarungen Delegierten der Organisation, Organisationsverantwortlichen und SysAdmin's sowie deren Kontaktdaten*
    - *Regeln zur Ernennung*
    - *Kontaktdaten*
    - *Aufgaben und Pflichten*
    - *Haftungsfragen und -klärungen*
- Glossar zum SLA

Fachlicher Anhang C – Mögliche Policy-Elemente einer STIAM-Policy

Policies enthalten Elemente, welche die Zusammenarbeit in der Domäne und über die Domänengrenzen hinaus regeln. Sie enthalten generische und spezifische Regelungen, welche für die Entwicklung des Vertrauens in der Domäne und im Verkehr mit anderen Domänen von Relevanz sind. Unter anderem sind folgende Punkte in STIAM-Policies abzuhandeln:

- Definition der Grenzen der (Meta-)Domäne
- Beziehungen und Aufgaben von und zwischen Governance- und Management-Gremium
- Mitglieder der (Meta-)Domäne je Stakeholder-Kategorie
- (Vertrauens-)Bedingungen der Zusammenarbeit in der (Meta-)Domäne
- (Vertrauens-)Bedingungen der Zusammenarbeit mit anderen (Meta-)Domänen
- Vorgaben zum internen IAM bei beteiligten Stakeholdern
- Vorgaben zum Stakeholder-übergreifenden föderierten IAM
- Vorgaben zum Datenmanagement beim STIAM-Intermediär in Abhängigkeit von den Stakeholdern, welche die Daten z.B. auf dem STIAM-Intermediär selber pflegen
- Vertrags-Policies
- Policies zu Rollen, deren Aufgaben, Kompetenzen, Verantwortlichkeiten sowie zu Funktionstrennungen (Segregation of Duties)
- Policies zu Qualitäts- (etwa Datenqualität betreffend) und Vertrauens-Aspekten (sei es institutionell-organisatorisch, vertraglich, technisch)
- Technische Policies z.B. auf Decision- und Enforcement-Point-Ebene

Fachlicher Anhang D – COBIT-Prozess-Mapping mit STIAM-Gremien

Die Tabelle 10 zeigt ausgehend vom Rahmenwerk COBIT 5 eine Zuordnung der COBIT-Control-Prozesse zu den zwei Gremien, welche für STIAM unterschieden werden ([ISACA 2012a], [ISACA 2012b]). Die entsprechenden Zuständigkeiten sind klar geregelt und können als ergänzende Aufgaben-, Kompetenz- und Verantwortungs-Definitionen für STIAM verstanden werden.

Ebenfalls können die COBIT-Control-Prozesse als ergänzende Differenzierungen zu den summarisch behandelten GRC-Prozessen in [eCH-0107] verstanden werden. Für weitergehende Ausführungen zu den Control-Prozessen ist auf das Rahmenwerk COBIT 5 zu verweisen ([ISACA 2012a], [ISACA 2012b]). Darin wird zu jedem der unten erwähnten Control-Prozesse ein umfassenderes RACI-Chart präsentiert. Im Folgenden werden nur die STIAM-relevanten Rollen je Prozess thematisiert.

Die verwendeten Abkürzungen werden nach der Tabelle 10 erklärt.

Die Anzahl X zeigt die Bedeutung der entsprechenden Prozess-Controls für den STIAM-Kontext.

Legende zur Tabelle 10:

XXX Notwendig

XX Empfehlenswert

X Vernachlässigbar

--- nicht relevant

COBIT-Prozess	**COBIT-Domäne**	**Zuständigkeit Governance-Gremium**	**Zuständigkeit Management-Gremium**
Sicherstellen der Einrichtung und Pflege des Governance-Rahmenwerks	EDM	XXX	---
Sicherstellen der Lieferung von Wertbeiträgen	EDM	XXX	---
Sicherstellen der Risiko-Optimierung	EDM	XXX	---
Sicherstellen der Ressourcenoptimierung	EDM	XXX	---
Sicherstellen der Transparenz gegenüber Anspruchsgruppen	EDM	XXX	---
Managen des IT-Management Rahmenwerks	APO	---	XXX
Managen der Strategie	APO	---	XXX
Managen der Unternehmensarchitektur	APO	---	XXX
Managen von Innovationen	APO	---	X
Managen des Portfolios	APO	---	XXX
Managen von Budget und Kosten	APO	---	XXX

Managen des Personals	APO	---	X
Managen von Beziehungen	APO	---	XXX
Managen von Servicevereinbarungen	APO	---	XXX
Managen von Lieferanten	APO	---	XX
Managen der Qualität	APO	---	XXX
Managen von Risiko	APO	---	XXX
Managen der Sicherheit	APO	---	XXX
Managen von Programmen und Projekten	BAI	---	XX
Managen der Definition von Anforderungen	BAI	---	XX
Managen von Lösungsidentifizierung und Lösungsbau	BAI	---	X
Managen von Verfügbarkeit und Kapazität	BAI	---	XXX
Managen der Ermöglichung organisatorischer Veränderungen	BAI	---	XX
Managen von Änderungen	BAI	---	XXX
Managen der Abnahme und Überführung von Änderungen	BAI	---	XX
Managen von Wissen	BAI	---	X
Managen von Betriebsmittel	BAI	---	XXX
Managen der Konfiguration	BAI	---	XX
Managen des Betriebs	DSS	---	XXX
Managen von Service-Anfragen und -Störungen	DSS	---	XXX
Managen von Problemen	DSS	---	XX
Managen der Kontinuität	DSS	---	XXX
Managen von Sicherheitsservices	DSS	---	XXX
Managen von Geschäftsprozesskontrollen	DSS	---	XXX
Überwachen, Evaluieren und Beurteilen von Leistung und Konformität	MEA	---	XXX
Überwachen, Evaluieren und Beurteilen des internen Kontrollsystems	MEA	---	XXX
Überwachen, Evaluieren und Beurteilen der Compliance mit externen Anforderungen	MEA	---	XXX

Tabelle 10: COBIT-Prozesse sowie deren Zuordnung und Bedeutung in Relation zum Governance- und Management-Gremium

Fachlicher Anhang E – ITIL-Prozess-Mapping mit STIAM-Stakeholdern

Die Tabelle 11 zeigt ausgehend vom Rahmenwerk ITIL 2011 edition eine Zuordnung der ITIL-Prozesse zu den Stakeholdern, welche im STIAM-Kontext unterschieden werden. Die entsprechenden Zuständigkeiten sind klar geregelt und können als ergänzende Aufgaben-, Kompetenz- und Verantwortungs-Definitionen für STIAM verstanden werden.

Ebenfalls können die ITIL-Prozesse als ergänzende Differenzierungen zu den summarisch behandelten GRC-Prozessen in [eCH-0107] verstanden werden. Für weitergehende Ausführungen zu den ITIL-Prozessen ist auf das Rahmenwerk ITIL 2011 edition zu verweisen ([Cannon 2011], [Hunnebeck 2011], [Rance 2011], [Steinberg 2011] sowie [Lloyd 2011]).[10]

Legende zur Tabelle 11**:**

XXX Notwendig

XX Empfehlenswert

X Vernachlässigbar

--- nicht relevant

S Service Strategy

D Service Design

T Service Transition

O Service Operation

CSI Continual Service Improvement

ITIL-Prozess		**STIAM-Broker**	**RP**	**AA**	**AuthnA**
Strategy Management for IT-Services	S	XXX	XX	XX	XX
Service Portfolio Management	S	XXX	XXX	XXX	XXX
Financial Management	S	XXX	X	X	X
Demand Management	S	XXX	XXX	XXX	XXX
Business Relationship Management	S	XXX	XXX	XXX	XXX
Design Coordination	D	X	X	X	X
Service Catalogue Management	D	XXX	X	X	X
Service Level Management	D	XXX	XXX	XXX	XXX
Capacity Management	D	XXX	XXX	XXX	XXX
Availability Management	D	XXX	XXX	XXX	XXX

ITIL-Prozess		STIAM-Broker	RP	AA	AuthnA
IT Service Continuity Management	D	XXX	XXX	XXX	XXX
Information Security Management	D	XXX	XXX	XXX	XXX
Supplier Management	D	XX	XX	XX	XX
Change Management	T	XXX	XXX	XXX	XXX
Change Evaluation	T	X	X	X	X
Release and Deployment Management	T	X	X	X	X
Service Validation and Testing	T	X	X	X	X
Service Asset and Configuration Management	T	XXX	XXX	XXX	XXX
Knowledge Management	T	X	X	X	X
Event Management	O	XX	X	X	X
Incident Management	O	XXX	XXX	XXX	XXX
Request Fulfillment	O	XXX	X	X	X
Access Management	O	XXX	XXX	XXX	XXX
Problem Management	O	XX	XX	XX	XX
Seven-step Improvement Process	CSI	XXX	XXX	XXX	XXX

Tabelle 11: ITIL-Prozesse und deren Relevanz für die STIAM-Stakeholder

Fachlicher Anhang F - Mapping zwischen COBIT und ITIL

In der Tabelle 12 wird das Mapping zwischen COBIT 5 und ITIL 2011 edition ersichtlich. Die COBIT-Prozesse sind als zu steuernde Prozesse (aus Governance- und Management-Gremiums-Sicht) zu verstehen. Die ITIL-Prozesse werden im Gegensatz dazu als zu implementierende Prozesse (aus STIAM-Serviceprovider-Sicht) verstanden. Für die meisten COBIT-Prozesse existieren auf der ITIL-Seite entsprechende Prozesse. Alle für STIAM notwendigen COBIT- und ITIL-Prozesse sind in Tabelle 12 aufgeführt. Für die Unternehmensarchitektur, die organisatorischen Veränderungen und für den Betrieb gibt es kein Mapping von COBIT zu ITIL.

	ITIL-Phasen und -Prozesse														
	Service Strategy					Service Design					Service Transition		Service Operation		
	Strategie-Management für IT-Services	Service-Portfolio Management	Financial Management für IT-Services	Business Relationship Management	Demand Management	Service Level Management	Capacity Management	Availability Management	IT Service Continuity Management	Information Security Management	Change Management	Service Asset Configuration	Incident Management	Request Fulfilment	Access Management
COBIT-Prozesse															
Managen der Strategie	X														
Managen der Unternehmensarchitektur															
Managen des Portfolios		X													
Managen von Budget und Kosten			X												
Managen von Beziehungen				X	X										
Managen von Servicevereinbarungen		X			X	X									
Managen der Qualität										X					
Managen von Risiko										X					
Managen der Sicherheit										X					
Managen von Verfügbarkeit und Kapazitäten							X	X							
Managen von org. Veränderungen															
Managen von Betriebsmittel												X			

Managen von Änderungen											X				
Managen der Konfiguration												X			
Managen des Betriebs															
Managen von Service-Anfragen													X	X	
Managen der Kontinuität									X						
Managen von Sicherheitsservices										X					
Managen von Geschäftsprozesskontrollen															X

Tabelle 12: Mapping zwischen COBIT und ITIL