# eCH-0169 Architecture administrative de SuisseTrustIAM

| | |
|---|---|
| **Titre** | Architecture administrative de SuisseTrustIAM |
| **Code** | eCH-0169 |
| **Type** | Norme |
| **Stade** | Définie |
| **Version** | 1.0 |
| **Statut** | Approuvée |
| **Validation** | 2014-09-03 |
| **Date de publication** | 2014-10-01 |
| **Remplace** | |
| **Langues** | Allemand et français |
| **Auteurs** | Konrad Walser, Institut eGovernment, Haute école spécialisée bernoise, konrad.walser@bfh.ch<br>Roman Hosang, Institut eGovernment, Haute école spécialisée bernoise, roman.hosang@bfh.ch |
| **Editeur / distributeur** | Association eCH, Mainaustrasse 30, case postale, 8034 Zurich<br>T 044 388 74 64, F 044 388 71 80<br>www.ech.ch / info@ech.ch |
| | |

# Condensé

Cette norme décrit l'architecture administrative SuisseTrustIAM (STIAM), une solution d'Identity & Access Management fédérée, basée sur le modèle Hub-'n'-Spoke. Elle décrit du point de vue administratif, quelles parties prenantes collaborent sous quelle forme dans le contexte STIAM, quels rôles interviennent dans quels processus avec quelles tâches, compétences et responsabilités et à quoi ressemblent la gouvernance et la gestion d'un domaine STIAM.

Du point de vue de cette norme, la gouvernance et la gestion du domaine sont comprises comme des tâches à distinguer de manière consciente, pour lesquelles il faut créer des organes séparés. L'organe de gouvernance prescrit des Policies et veille à leur respect. L'organe de gestion met en œuvre les Policies dans et entre les parties prenantes et veille à leur application. Cela permet de s'assurer que les participants des domaines, qui peuvent être très nombreux selon les circonstances, coordonnent leurs efforts relatifs à la définition de leur zone de confiance.

Un Identity & Access Management fédéré représente un composant essentiel possible pour une cyberadministration, cybersanté, cyberéducation et cyberéconomie électroniques intégrées et continues.

**Sommaire**

**1 Statut du document ..... 6**
**2 Introduction ..... 7**
2.1 Vue d'ensemble et introduction ..... 7
2.2 Domaine d'application et délimitation ..... 10
2.3 Avantages ..... 10
2.4 Priorités ..... 11
2.5 Caractère normatif des chapitres ..... 11
**3 Parties prenantes ..... 13**
3.1 Sujet ..... 14
3.1.1 Personnes physiques ..... 15
3.1.2 Service ..... 15
3.1.3 Organisation ..... 15
3.2 Relying Party ..... 16
3.3 Broker STIAM ..... 16
3.4 Autorité d'authentification ..... 17
3.5 Autorité d'attributs ..... 18
3.6 Organe de gouvernance ..... 18
3.7 Organe de gestion ..... 19
**4 Organisation ..... 21**
4.1 Vue d'ensemble ..... 21
4.2 Principes d'organisation de STIAM ..... 22
**5 Rôles ..... 25**
5.1 Vue d'ensemble ..... 25
5.2 Description des rôles ..... 26
5.2.1 Président de l'organe de gouvernance ..... 26
5.2.2 Membres de l'organe de gouvernance ..... 26
5.2.3 Président de l'organe de gestion ..... 27
5.2.4 Membres de l'organe de gestion ..... 27
5.2.5 Délégué de l'organisation ..... 28
5.2.6 Responsable de l'organisation ..... 28
5.2.7 Organisation-SysAdmin ..... 29

5.2.8 STIAM-SysAdmin ..... 29
**6 Processus ..... 30**
6.1 Processus de gouvernance ..... 31
6.2 Processus de gestion ..... 32
6.3 Processus principaux ..... 33
6.4 Processus de soutien ..... 34
**7 Exclusion de responsabilité – droits de tiers ..... 36**
**8 Droits d'auteur ..... 36**
**Annexe A – Références & bibliographie ..... 37**
**Annexe B – Collaboration & vérification ..... 37**
**Annexe C – Abréviations ..... 38**
**Annexes techniques ..... 39**
Annexe technique A – Architecture de contrats et accords ..... 39
Annexe technique B – Structure possible d'un Service Level Agreement spécifique STIAM (SLA) ..... 40
Annexe technique C – Eléments possibles d'une Policy STIAM ..... 41
Annexe technique D – Mapping des processus COBIT avec les organes STIAM ..... 42
Annexe technique E – Mapping des processus ITIL avec les parties prenantes STIAM 44
Annexe technique F - Mapping entre COBIT et ITIL ..... 46

# Liste des illustrations

Figure 1: architecture administrative de STIAM (période de définition) ..... 8

Figure 2: architecture administrative de STIAM (période d'exécution) ..... 9

Figure 3: Positionierung des Standards eCH-0169 architecture administrative de STIAM .... 10

Figure 4: Übersichtsgrafik parties prenantes ..... 14

Figure 5: Relationen zwischen Governance- et Management-Ebene von STIAM basierend auf COBIT 5/ISO IEC 38500 ([ISACA 2012a], [ISACA 2012b], [ISO/IEC 38500]) ..... 21

Figure 6: Relations de représentation et -Hierarchie in Gremien im STIAM-Kontext ..... 22

Figure 7: STIAM-Prozesslandkarte ..... 31

Figure 8: Vertragsarchitektur im SLA-Kontext (nach [Prengemann 2006]) ..... 39

# Liste des tableaux

Tableau 1: Farbverwendung in Figure 1 ..... 8

Tableau 2: Übersicht über normativen et descriptifen Charakter der Kapitel des vorliegenden Standards ..... 12

Tableau 3: Mapping des parties prenantes ..... 13

Tableau 4: Rôles aus STIAM-Sicht ..... 25

Tableau 5: matrice RACI EDM ..... 32

Tableau 6: matrice RACI APO ..... 32

Tableau 7: matrice RACI BAI ..... 33

Tableau 8: matrice RACI DSS ..... 33

Tableau 9: matrice RACI MEA ..... 33

Tableau 10: COBIT-Processus sowie deren Zuordnung et Bedeutung in Relation zum Governance- et Organe de gestion ..... 43

Tableau 11: ITIL-Processus et deren Relevanz für die STIAM-parties prenantes ..... 45

Tableau 12: Mapping zwischen COBIT et ITIL ..... 47

# 1 Statut du document

Le Comité d'experts a ***approuvé*** le présent document, lui conférant force normative pour le domaine d'application défini et dans les limites de validité fixées.

# 2 Introduction

## 2.1 Vue d'ensemble et introduction

SuisseTrustIAM (STIAM) repose sur la norme eCH-0107 Principes de conception IAM pour la gestion de l'identité et de l'accès (IAM) [eCH-0107] et représente une possibilité de modalité du modèle Hub-'n'-Spoke, qui est présenté comme concept d'Identity Federation dans [eCH-0107]. L'architecture administrative est décrite du point de vue non pas du Broker, mais du domaine[1], dans lequel le Broker remplit une activité de médiateur central. La terminologie suit celle de la norme [eCH-0107], dans la mesure où les termes ne sont pas définis dans le présent document.

Le modèle Hub-'n'-Spoke a pour avantage de délocaliser les confirmations d'identité et d'attributs pour le Relying Party. Ce dernier ne doit ainsi pas composer avec diverses autorités d'attributs et d'authentification pour chaque relation séparée et interface. Le but de STIAM est que toutes les parties prenantes ne disposent plus que d'une seule interface avec le Broker STIAM.

Les parties prenantes suivantes sont pertinentes pour STIAM:

- Le **sujet** veut accéder aux ressources des Relying Parties par voie électronique.
- La **ressource** est un service ou met à disposition des données, auxquelles un sujet peut accéder, lorsqu'il s'est authentifié et a été autorisé sur la base des attributs requis.
- Le **Relying Party (RP)** défend les intérêts de la ressource et sécurise le contrôle des accès.
- L'**autorité d'authentification (AuthnA)** confirme la prétendue eIdentity d'un sujet.
- L'**autorité d'attributs (AA)** fournit les informations de confirmation nécessaires concernant les attributs. Il s'agit de propriétés du sujet correspondant, grâce auxquelles celui-ci peut accéder à la ressource du Relying Party.
- Le **Broker STIAM** assure la médiation entre le sujet et les ressources en vue de faire parvenir au Relying Party les confirmations nécessaires pour le contrôle d'accès, en respectant les règles du domaine dans la zone de confiance.
- L'**organe de gouvernance** est un organe global et dirige, contrôle, surveille et évalue, au moyen de Policies, la transmission, en toute confiance, de confirmations dans un domaine. L'organe de gouvernance est responsable de la mise en œuvre concrète des Policies en collaboration avec les parties prenantes.
- L'**organe de gestion** est un organe global et veille à la mise en œuvre des directives de gouvernance à l'intérieur du domaine. Il fait office de coordinateur entre les différentes parties prenantes.

Afin de fournir une vue d'ensemble descriptive de STIAM, les processus définis dans [eCH-0107] (contrôler l'accès, définir l'IAM et contrôler l'IAM) sont affectés aux parties prenantes en utilisant des couleurs de façon homogène. Les éléments *Contrôler l'accès* (pour la pé-

[1] Selon la norme eCH-0107, un domaine est une «communauté administrative / technique ou organisation avec une Policy commune» [eCH-0107].

riode d'exécution) et *Définir l'IAM* (pour la période de définition) représentent les processus principaux, qui sont utilisés par le sujet et la ressource. Ces processus principaux sont utilisés à des moments distincts, qui sont représentés par la couleur bleu clair et bleu foncé (cf. Tableau 1).

| | |
|---|---|
| gris | La couleur grise permet de visualiser les organes, qui sont actifs **avant et pendant la période de définition**. Avant la période de définition, le domaine est structuré et organisé avec ses organes de gouvernance et de gestion. Cette structure est impérative pour que les processus de la période de définition et d'exécution puissent être exécutés, de manière fiable et sûre, dans la zone de confiance constituée des domaines pour tous les participants. |
| bleu clair | La couleur bleu clair est utilisée pour la **période de définition**, au cours de laquelle toutes les informations sont affectées aux éléments d'information (c'est-à-dire définis). |
| bleu foncé | La couleur bleu foncé est utilisée pour la **période d'exécution**. Pour la période d'exécution, l'accès est contrôlé, accordé ou refusé sur la base des éléments d'information définis. |
| vert clair | La couleur vert clair est utilisée exclusivement pour les objets de la vie réelle. |

**Tableau 1: utilisation des couleurs dans la figure 1**

L'architecture administrative de STIAM est représentée par la Figure 1 et la Figure 2 à partir des parties prenantes décrites ci-dessus.

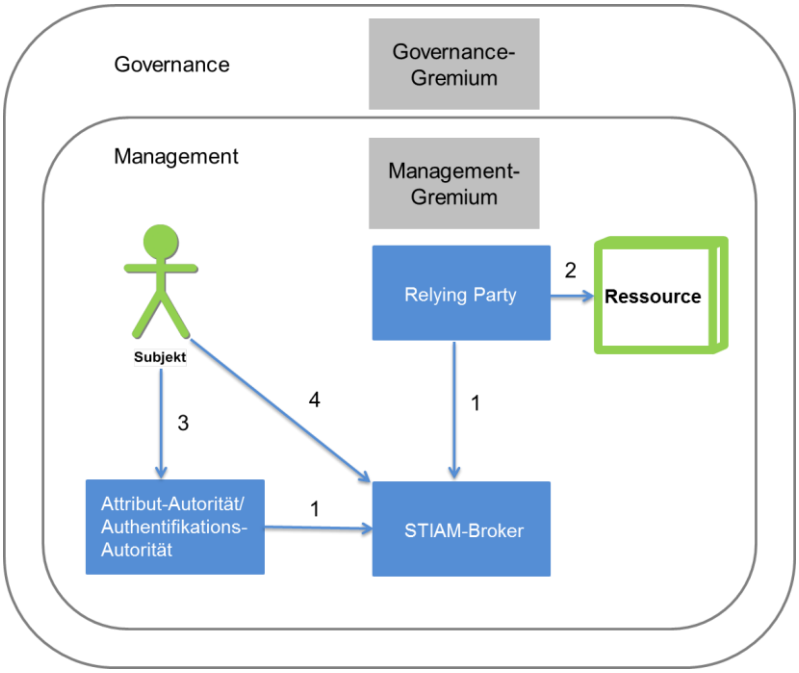


**Figure 1: architecture administrative de STIAM (période de définition)**

Au cours de la **période de définition**, toutes les conditions nécessaires sont réunies afin qu'il soit possible de vérifier, pour la période d'exécution, si un sujet est autorisé à accéder à une ressource. La liste suivante décrit les flèches numérotées dans la Figure 1.

1. Le Relying Party (y compris la ressource), l'autorité d'attributs et l'autorité d'authentification s'inscrivent auprès du Broker STIAM.
2. Le Relying Party définit les droits d'accès à la ressource.
3. Le sujet s'inscrit auprès de l'autorité d'authentification et fournit les données nécessaires à l'autorité d'attributs.
4. Le sujet crée un nouveau compte auprès du broker STIAM et établit un lien vers ses identités.

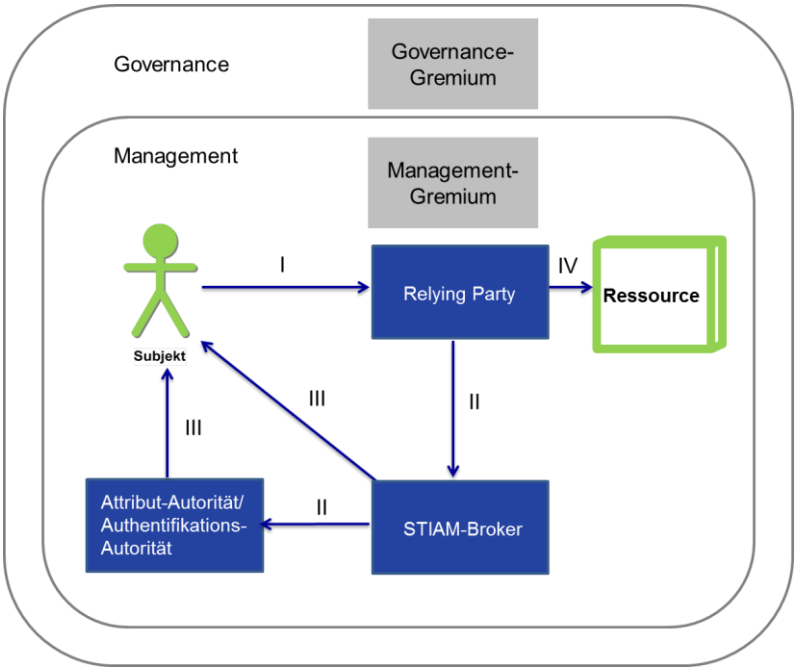


**Figure 2: architecture administrative de STIAM (période d'exécution)**

La **période d'exécution** a pour objet le respect contrôlé et garanti des règles établies concernant l'accès par un sujet à une ressource dans la zone de confiance des domaines. L'interaction entre les parties prenantes pour la période d'exécution se déroule de la manière suivante, représentée de manière simplifiée (cf. à ce sujet les flèches numérotées dans la Figure 2):

I. Le sujet veut accéder à une ressource du Relying Party.
II. Le Relying Party obtient la confirmation de l'identité du sujet par l'autorité d'authentification et la confirmation des attributs correspondants pour la suite de la caractérisation du sujet par l'autorité d'attributs via le Broker STIAM.
III. Le sujet est authentifié et reçoit une demande de confirmation de transmission des données au Relying Party.
IV. Le Relying Party laisse ensuite le sujet accéder à sa ressource.

## 2.2 Domaine d'application et délimitation

La Figure 3 permet de situer la présente norme eCH-0169 Architecture administrative de STIAM (cadre rouge). [eCH-0107] définit les principes de conception génériques, qui sont explicités dans les différents concepts de fédération et les documents auxiliaires complémentaires. SuisseTrustIAM constitue une possibilité de modalité du modèle Hub-'n'-Spoke, qui est présenté dans [eCH-0107] sous le concept d'Identity Federations correspondant.

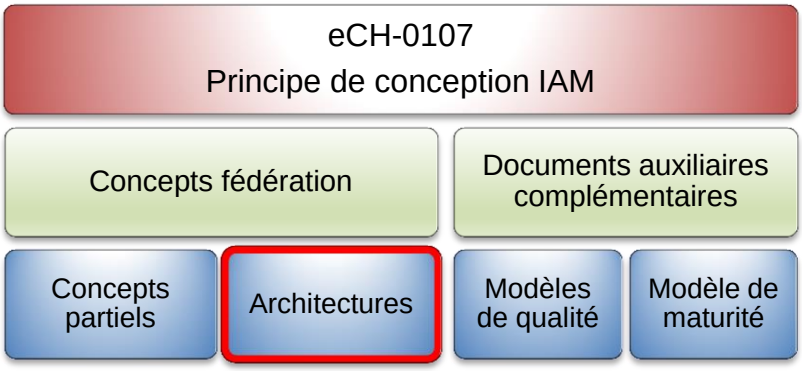


**Figure 3: Positionnement de la norme eCH-0169 Architecture administrative de STIAM**

## 2.3 Avantages

Les avantages visés par la présente norme sont les suivants:

- Permettre une présentation orientée sur les activités de STIAM
- Concrétiser des dépendances et des principes de gouvernance et de mise en œuvre pour les domaines, qui sont fédérés via STIAM
- Présenter la coopération et la coordination des parties prenantes dans l'environnement STIAM en vue de la constitution d'une zone de confiance homogène d'un domaine
- Représenter la forme de collaboration des rôles dans les processus ainsi que les tâches et les relations
- Concrétiser la gouvernance afin de garantir une zone de confiance dans le domaine
- Mettre en évidence les processus pertinents dans l'architecture administrative STIAM.

## 2.4 Priorités

Cette norme est structurée comme suit:

- Le chapitre 1 présente le statut du document
- Le chapitre 2 présente l'introduction à l'architecture administrative STIAM
- Le chapitre 3 présente les parties prenantes pouvant intervenir dans le contexte STIAM
- Le chapitre 4 décrit les aspects d'organisation liés à la gouvernance dans la zone de confiance STIAM partant d'un domaine
- Le chapitre 5 présente les rôles ainsi que leurs tâches, qui interviennent dans les différentes parties prenantes STIAM.
- Le chapitre 6 est consacré à la représentation des processus administratifs, qui doivent être intégrés pour les parties prenantes STIAM, afin de permettre la collaboration des parties prenantes dans la zone de confiance d'un domaine.

## 2.5 Caractère normatif des chapitres

Les chapitres de la présente norme revêtent un caractère normatif ou descriptif. le Tableau 2 illustre la classification correspondante.

| Chapitre | Description |
|---|---|
| 2 Introduction | Descriptif |
| 3 Parties prenantes | Normatif |
| 4 Organisation | Descriptif |
| 5 Rôles | Normatif |
| 5.2 Description des rôles | Descriptif |
| 6.1 Processus de gouvernance | Descriptif |
| 6.2 Processus de gestion | Descriptif |
| 6.3 Processus principaux | Normatif |
| 6.4 Processus de soutien | Descriptif |
| Annexe A – Références & bibliographie | Descriptif |
| Annexe B – Collaboration & vérification | Descriptif |
| Annexe C – Abréviations | Normatif |
| Annexe technique A – Architecture de contrats et accords | Descriptif |

| | |
|---|---|
| Annexe technique B – Structure possible d'un Service Level Agreement spécifique à STIAM | Descriptif |
| Annexe technique C – Eléments possibles de Policy d'une Policy STIAM | Descriptif |
| Annexe technique D – Mapping des processus COBIT avec les organes STIAM | Descriptif |
| Annexe technique E – Mapping des processus ITIL avec les parties prenantes STIAM | Descriptif |
| Annexe technique F - Mapping entre COBIT et ITIL | Descriptif |

**Tableau 2: Vue d'ensemble du caractère normatif et descriptif des chapitres de la présente norme**

# 3 Parties prenantes

Les parties prenantes et leurs tâches sont partiellement reprises de [eCH-0107] et, là où cela est nécessaire, complétées et explicitées. Le **Fehler! Ungültiger Eigenverweis auf Textmarke.** présente le mapping des parties prenantes de cette norme avec [eCH-0107].

| **Parties prenantes eCH-0169 Architecture administrative STIAM** | **Parties prenantes [eCH-0107]** |
|---|---|
| Autorité d'attributs, autorité d'authentification, Broker STIAM, autres Brokers STIAM | Prestataires de service IAM |
| Organe de gouvernance, organe de gestion | Régulateur |

**Tableau 3: Mapping des parties prenantes**

Comme le montre le Les parties prenantes et leurs tâches sont partiellement reprises de [eCH-0107] et, là où cela est nécessaire, complétées et explicitées. Le **Fehler! Ungültiger Eigenverweis auf Textmarke. présente le** mapping des parties prenantes de cette norme avec [eCH-0107].

| **Parties prenantes eCH-0169 Architecture administrative STIAM** | **Parties prenantes [eCH-0107]** |
|---|---|
| Autorité d'attributs, autorité d'authentification, Broker STIAM, autres Brokers STIAM | Prestataires de service IAM |
| Organe de gouvernance, organe de gestion | Régulateur |

**Tableau 3** les deux parties prenantes [eCH-0107] «Prestataires de service IAM» et «Régulateur» sont explicitées dans la présente norme.

La structure des parties prenantes pertinentes pour STIAM est représentée par la fFigure 4.

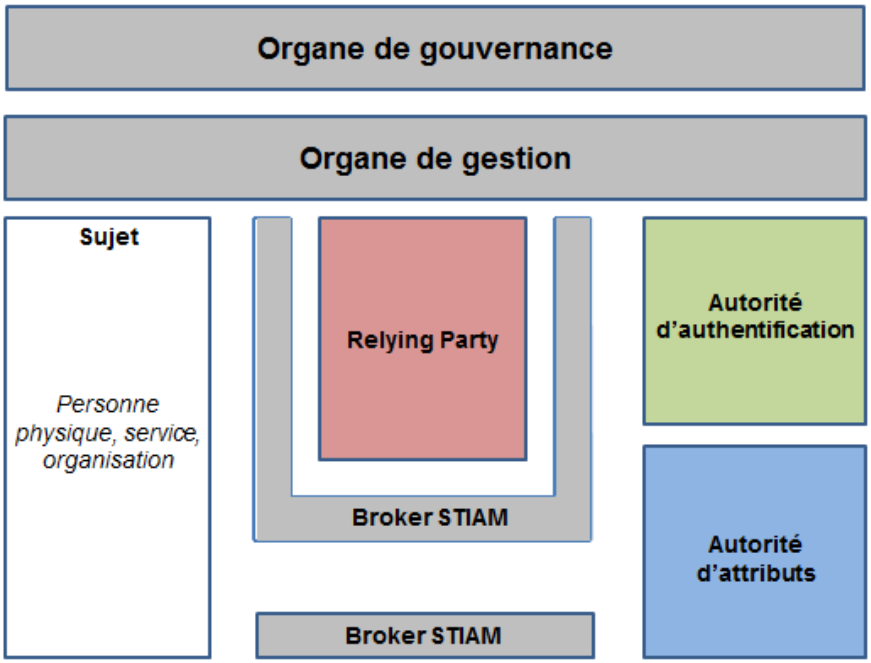


**Figure 4: Graphique de vue d'ensemble des parties prenantes**

Plusieurs brokers STIAM, sujets, Relying Parties, autorités d'authentification et d'attributs peuvent apparaître pour chaque domaine. Les parties prenantes correspondantes peuvent apparaître en tant que parties prenantes dans plusieurs domaines. Une partie prenante peut en outre être impliquée dans plusieurs domaines à la fois. De plus, la coopération entre les différents domaines est assurée via la communication entre les brokers.

Les parties prenantes différenciées dans la Figure 4 sont brièvement décrites ci-après. En outre, des tâches, compétences et responsabilités qui découlent en partie de [eCH-0107], sont définies plus en détail et affectées aux parties prenantes concernées. Les tâches des processus Contrôler l'IAM (Governance, Risk & Compliance) de [eCH-0107] sont présupposées dans ce chapitre et complétées lorsque cela est nécessaire. En outre, une dernière partie illustre comme les organes nouvellement définis sont constitués.

## 3.1 Sujet

| | |
|---|---|
| Sujet | Il s'agit d'une personne physique, d'une organisation ou d'un service, qui accède ou souhaite accéder à une ressource. Un sujet est décrit par des identités numériques [eCH-0107], figure 19). |

**Tâches:**

- Se procurer une identité électronique
- Recevoir les caractéristiques d'authentification
- Sélectionner et utiliser des ressources

**Compétences:**

- Approuver la transmission d'Authentication et Attribute Assertions

**Responsabilité**

- Attester de propriétés par rapport à l'Attribute Service

- Utiliser des caractéristiques d'authentification

### 3.1.1 Personnes physiques

| | |
|---|---|
| Personne physique | Il s'agit de la personne dans son rôle en tant que sujet de droit, qui veut accéder aux ressources d'une Relying Party. |

Aucune tâche n'est mentionnée sous cette rubrique, car elles ont déjà été explicitées pour le sujet.

### 3.1.2 Service

| | |
|---|---|
| Service | Un service est une application, un système, un bâtiment…, qui accède aux ressources des Relying Parties. |

Aucune tâche n'est mentionnée sous cette rubrique, car elles ont déjà été explicitées pour le sujet.

### 3.1.3 Organisation

| | |
|---|---|
| Organisation | Unité organisationnelle composée de plusieurs sujets (personne morale, entreprise, association, service officiel, groupe de sujets…) [eCH-0107]. |

**Tâches:**

- Définir les autorisations des sujets dans le contexte STIAM

**Compétences:**

- Affecter les TCR aux rôles

**Responsabilité**

- Clarifier les rôles du sujet au sein de l'organisation
- Réglementer l'utilisation des moyens d'authentification de l'organisation

## 3.2 Relying Party

| | |
|---|---|
| Relying Party | Celle-ci met à disposition des services ou des informations au moyen de ressources, auxquelles le sujet peut accéder, à condition qu'il se soit correctement identifié et authentifié et qu'il y ait été autorisé sur la base des attributs requis en partant d'un concept d'autorisation [eCH-0107]. |

**Tâches:**

- Réaliser les services administratifs suivants selon [eCH-0107]
  - Accès
  - Règles d'accès
  - Autorisation
  - Droit d'accès
  - eRessource
- [Facultatif] Obtenir et tenir à jour les certifications ISO (ISO/IEC 20000, ISO/IEC 27000, ISO/IEC 31000, ISO/IEC 38500)

**Compétences:**

- Conclure des
  - Contrats cadre
  - Accords de prestations
  - Service Level Agreements avec le broker STIAM

**Responsabilité**

- Garantir
  - l'affectation de rôles internes
  - l'accès à la ressource
  - l'implémentation de la Policy
  - une représentation au sein de l'organe de gouvernance
  - une représentation au sein de l'organe de gestion

## 3.3 Broker STIAM

| | |
|---|---|
| Broker STIAM | Celui-ci met à disposition le service intermédiaire effectif, par lequel les confirmations d'identités et d'attributs nécessaires sont fournies à l'attention du Relying Party. |

**Tâches:**

- Réaliser les services administratifs suivants selon [eCH-0107]:
  - Trust
  - Broker
- [Facultatif] Obtenir et tenir à jour les certifications ISO (ISO/IEC 20000, ISO/IEC 27000, ISO/IEC 31000, ISO/IEC 38500)

**Compétences:**

- Conclure des
  - Contrats cadre
  - Accords de prestations
  - Service Level Agreements avec d'autres parties prenantes

**Responsabilité**

- Garantir
  - l'affectation de rôles internes
  - de Policies
  - la représentation au sein de l'organe de gouvernance
  - la représentation au sein de l'organe de gestion

## 3.4 Autorité d'authentification

| | |
|---|---|
| Autorité d'authentification | Celle-ci met à disposition un Authentication Service vis-à-vis duquel le sujet peut s'authentifier. L'Authentication Service utilise des Credentials, qui sont délivrés par un Credential Service. Le Credential Service peut être un composant de l'AuthnA [eCH-0107]. |

**Tâches:**

- Réaliser les services administratifs suivants selon [eCH-0107]:
  - eIdentity
  - Credential
  - Authentication
- [Facultatif] Obtenir et tenir à jour les certifications ISO (ISO/IEC 20000, ISO/IEC 27000, ISO/IEC 31000, ISO/IEC 38500).

**Compétences:**

- Conclure des
  - Contrats cadre
  - Accords de prestations
  - Underpinning Contracts[2]

**Responsabilité**

- Garantir
  - l'affectation de rôles internes
  - de Policies
  - la représentation au sein de l'organe de gouvernance
  - la représentation au sein de l'organe de gestion

[2] Un Underpinning Contract (contrat avec des tierce-parties, UC) est un contrat conclu entre un broker STIAM et une autorité d'attributs ou une autorité d'authentification.

## 3.5 Autorité d'attributs

| | |
|---|---|
| Autorité d'attributs | Il s'agit là d'un registre ou d'un autre répertoire avec un Attribute Service pour tenir à jour les attributs et un Attribute Assertion Service qui délivre des Attribute Assertions [eCH-0107]. |

**Tâches:**

- Réaliser les services administratifs suivants selon [eCH-0107]:
  - Attributs
  - Attribute Assertion
- [Facultatif] Obtenir et tenir à jour les certifications ISO (ISO/IEC 20000, ISO/IEC 27000, ISO/IEC 31000, ISO/IEC 38500).

**Compétences:**

- Conclure des
  - Contrats cadre
  - Accords de prestations
  - Underpinning Contracts

**Responsabilité**

- Garantir
  - l'affectation de rôles internes
  - les Policies
  - la représentation au sein de l'organe de gouvernance
  - la représentation au sein de l'organe de gestion

## 3.6 Organe de gouvernance

| | |
|---|---|
| Organe de gouvernance | Celui-ci définit les conditions cadre légales, procédurales, organisationnelles, sémantiques et techniques, à l'intérieur desquelles l'IAM fédéré est réalisé dans un domaine. |

**Tâches:**

- Exercer les compétences de commande sur toutes les parties prenantes du domaine
- Commander l'IAM fédéré dans le domaine
- Diriger les domaines à partir des Policies
- Evaluer la mise en œuvre de la gouvernance
- Surveillance des performances et conformité du domaine

**Compétences:**

- Conclure des
  - Contrats cadre
  - Accords de prestations
  - Underpinning Contracts
- Décider
  - de l'inclusion et de l'exclusion de parties prenantes dans le domaine
  - concernant la participation à et l'approbation de la collaboration avec d'autres domaines

**Responsabilité**

- Garantir
  - La mise en œuvre du cadre de gouvernance (Governance Framework)
  - La fourniture de contributions de valeur sur la base du service STIAM
  - La minimisation du risque
  - L'optimisation des ressources
  - La transparence vis-à-vis des parties prenantes
  - La définition et le respect des Policies
  - Le transfert der responsabilité finale à un représentant au sein de l'organe de gouvernance
  - La disponibilité des outils requis

**Composition:**

- Représentant des sujets (dans le cas d'entreprises et d'autres institutions, représentation par des délégués de l'organisation)
- Délégué de l'organisation des Relying Parties (resp. son représentant)
- Délégué de l'organisation des autorités d'attributs (resp. son représentant)
- Délégué de l'organisation des autorités d'authentification (resp. son représentant)
- Délégué de l'organisation du Broker STIAM (resp. son représentant)

## 3.7 Organe de gestion

| | |
|---|---|
| Organe de gestion | L'organe de gestion est compétent pour la mise en œuvre des conditions cadre définies par l'organe de gouvernance dans un domaine et pour la coordination correspondante du domaine. |

**Tâches:**

- Mettre en œuvre les directives de l'organe de gouvernance du domaine
- Gérer la stratégie et l'architecture de l'entreprise du domaine
- Gérer le portefeuille de services STIAM
- Gérer le budget et les coûts
- Coordonner la coopération des parties prenantes
- Gérer les changements organisationnels (ex. intégrer les nouvelles parties prenantes)

**Compétences:**

- Garantir la qualité, la gestion des risques et la sécurité

**Responsabilité**

- Garantir la mis en œuvre de la Policy

**Composition:**

- Représentant du sujet (dans le cas d'entreprises et d'autres institutions, représentation par des responsables de l'organisation pour STIAM)
- Responsable de l'organisation des Relying Parties (resp. son représentant)
- Responsable de l'organisation des autorités d'attributs (resp. son représentant)
- Responsable de l'organisation des autorités d'authentification (resp. son représentant)
- Responsable de l'organisation du Broker STIAM (resp. son représentant)

- Le cas échéant, d'autres représentants externes, notamment pour la mise en œuvre de STIAM dans le domaine

# 4 Organisation

## 4.1 Vue d'ensemble

Le chapitre 4 répertorie les principes d'organisation essentiels formulés du point de vue du domaine, qui sont nécessaires au fonctionnement de la zone de confiance. Les principes présentés ci-après se rapportent à la Figure 5 et la Figure 6.

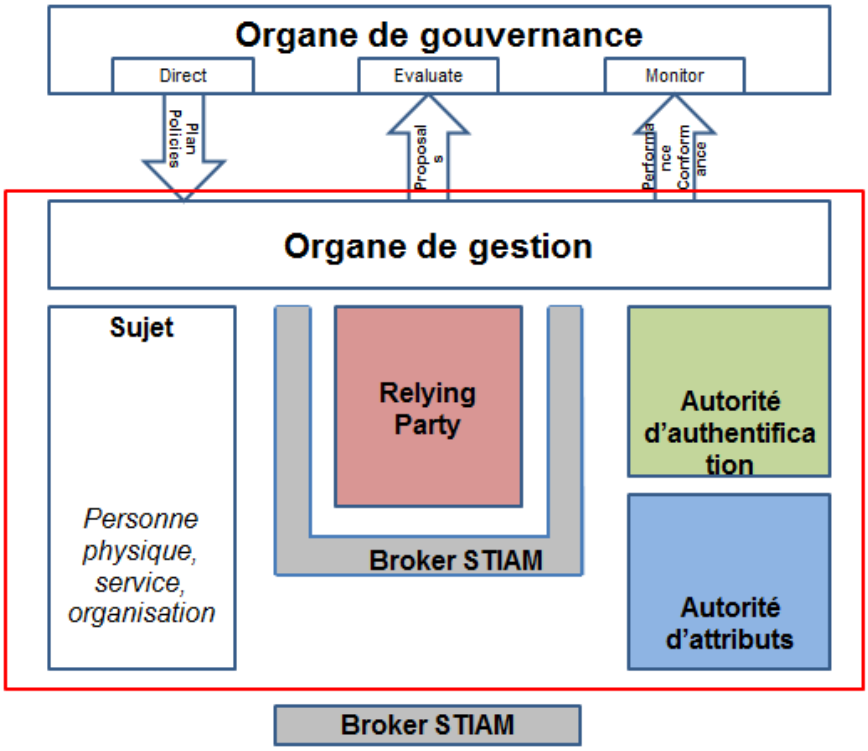


**Figure 5: Relations entre niveaux gouvernance et gestion de STIAM basées sur COBIT 5/ISO IEC 38500 ([ISACA 2012a], [ISACA 2012b], [ISO/IEC 38500])**

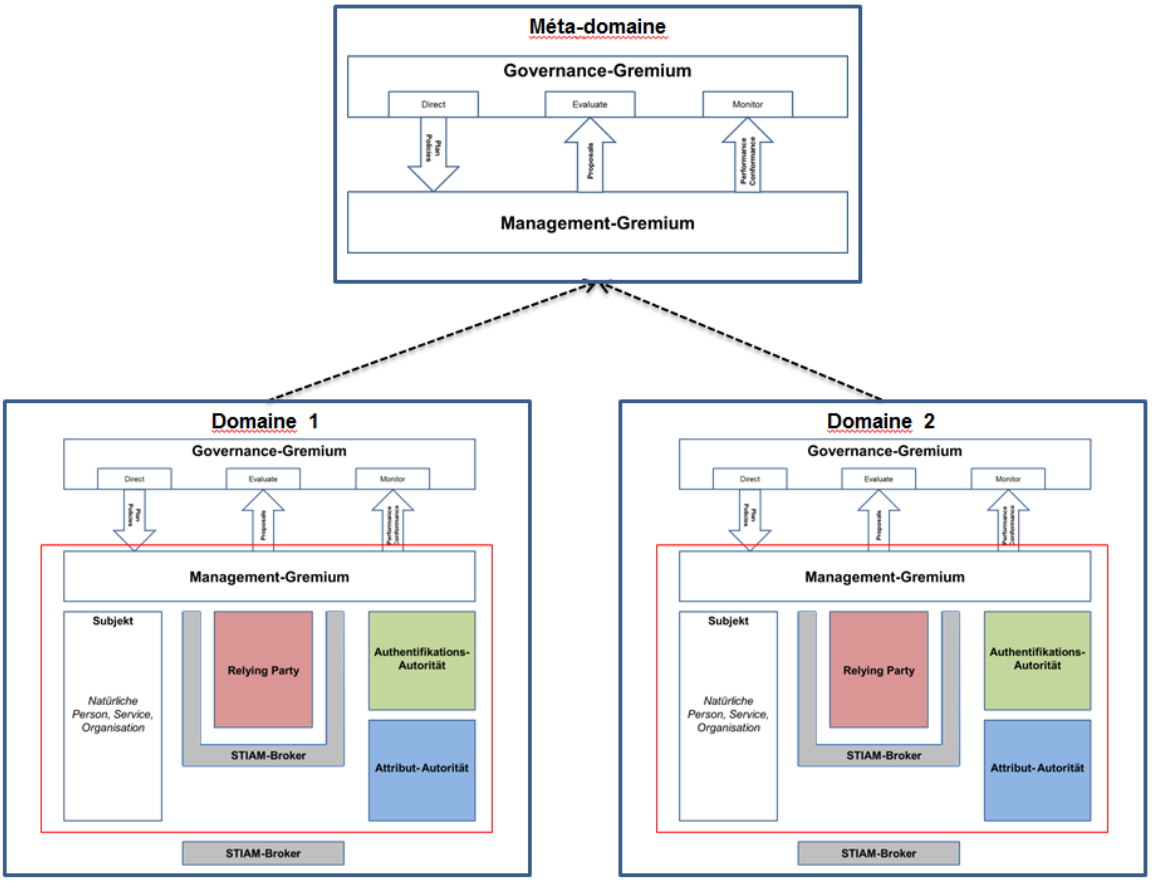


**Figure 6: Relations et hiérarchie de représentation au sein des organes dans le contexte STIAM**

Le méta-domaine contient au minimum l'organe de gouvernance et l'organe de gestion afin de garantir que la commande, l'harmonisation ainsi que la mise en œuvre des Policies est garantie par delà les domaines inclus, du point de vue du méta-domaine.

## 4.2 Principes d'organisation de STIAM

**Principe 1:** la direction STIAM à l'intérieur d'un domaine doit être divisée entre un organe de gouvernance et un organe de gestion à des fins de partage des pouvoirs.

STIAM requiert une collaboration entre les différentes parties prenantes STIAM caractérisées. Cette collaboration est coordonnée par l'organe de gestion. L'organe de gestion est commandé et surveillé par l'organe de gouvernance selon le chapitre **Fehler! Verweisquelle konnte nicht gefunden werden.**.

**Principe 2:** la constitution d'un domaine représente la condition préalable requise pour la formation de méta-domaines. Un méta-domaine coordonne un ou plusieurs domaines.

Il s'agit, dans une première étape, de mettre en place les différents domaines, qui pourront être par la suite rattachés à un méta-domaine (voir Figure 6). La gouvernance du méta-domaine suit les mêmes principes que la gouvernance du domaine.

**Principe 3:** du point de vue de la gouvernance, la constitution du domaine et de la zone de confiance associée est soutenue par la législation, les règlementations et les Policies ainsi que les règlementations contractuelles à différents niveaux et dans différentes directions.

Ceci comprend pour l'essentiel les règlementations légales, les Policies à définir, les règlementations contractuelles (contrats cadre), les accords de prestations, les Service Level Agreements, les Operational Level Agreements ainsi que les Underpinning Contracts partant de l'IT Service Provider ou de l'exploitant du Broker STIAM.[3]

**Principe 4:** les représentations dans les organes peuvent être par principe définies librement par les parties prenantes.

Les chapitres **Fehler! Verweisquelle konnte nicht gefunden werden.** et **Fehler! Verweisquelle konnte nicht gefunden werden.** contiennent une proposition de représentation des prestataires de service IAM dans les organes.

- L'organe de gouvernance est représenté par les délégués de l'organisation, chaque partie prenante est cependant libre de choisir quels délégués prennent place au sein de l'organe de gouvernance.
- L'organe de gestion est représenté par les responsables de l'organisation, chaque partie prenante est cependant libre de choisir quels responsables d'organisation prennent place au sein de l'organe de gestion.

**Principe 5:** l'interaction entre l'organe de gouvernance et de gestion ainsi que les parties prenantes doivent être comprises comme bidirectionnelle (orientée Top-Down et Bottom-Up).

Afin de permettre la meilleure gouvernance possible du domaine, il faut (comme pour ISO/IEC 38500) une communication à la fois Bottom-Up et Top-Down, des instruments de gouvernance ainsi que des flux d'informations (cf. Figure 5). Les instruments de commande Top-Down et Bottom-Up sont représentés dans la Figure 5 par les désignations «Proposals, Reports zu Performance et Conformance » ainsi que «Plan, Policies».

**Principe 6:** le domaine s'accorde sur un cadre de gouvernance, qui est imposé et mis en œuvre en conséquence dans le domaine.

Du point de vue du domaine, l'organe de gouvernance élabore les Policies et les plans et vérifie leur mise en œuvre par l'organe de gestion. Ceci implique notamment aussi le contrôle des processus pertinents à cet égard. Le cadre COBIT (Control Objectives of Information and related Technology) est une possibilité de cadre à implémenter pour la vérification des IT Controls et des processus IT. Mais le domaine est par principe libre de créer ou de sélectionner un cadre lui convenant pour la vérification des IT-Controls et des processus IT.[4]

[3] Cf. à ce sujet l'annexe technique A.

[4] Cf. au sujet de COBIT l'annexe technique D.

Si le domaine a recours à un cadre autre que celui qui a été mentionné, il doit justifier de la Mapping Compliance avec COBIT.

**Principe 7:** les processus de la période d'exécution STIAM reposent sur un Service Management Framework.

Contrairement au niveau des organes de gouvernance et de gestion, les processus principaux et de soutien dans l'environnement STIAM (cf. chapitre 6) visent la constitution et la mise en œuvre effectives des processus STIAM à l'intérieur des prestataires de service IAM ainsi que par delà plusieurs prestataires de service IAM.

L'Information Technology Infrastructure Library (ITIL) constitue un cadre possible pour assister les processus de soutien inter-organisations.[5]

Si le domaine a recours à un cadre autre que celui qui a été mentionné, il doit justifier de la Mapping Compliance avec ITIL.

**Principe 8:** l'organe de gestion met en œuvre les mesures définies par l'organe de gouvernance pour la création d'une «zone de confiance» en collaboration avec les parties prenantes.

La mise en œuvre des décisions de direction dans le domaine et ainsi la garantie que la «zone de confiance» est bien créée fait partie des tâches de l'organe de gestion.

**Principe 9:** le domaine garantit l'interopérabilité entre les différents domaines et concepts de fédération.

Dans le monde réel, il faut partir du principe qu'il y a différents Brokers STIAM et concepts de fédération [eCH-0107]. Le domaine garantit l'interopérabilité tant entre les Brokers STIAM (semblables) et les autres concepts de fédération IAM.

[5] Cf. au sujet d'ITIL l'annexe technique E.

# 5 Rôles

Le chapitre 5 traite des rôles, qui interviennent dans le contexte STIAM et de ses parties prenantes. A cet égard, les rôles d'une part, les tâches, compétences et responsabilités pour les rôles correspondants d'autre part sont définis.

## 5.1 Vue d'ensemble

Les divers rôles sont représentés dans le Tableau 4 afin de caractériser les différents pouvoirs de décision et domaines de décision.

| **Rôle** | **Parties prenantes** | | | | |
|---|---|---|---|---|---|
| | Organe de gouvernance | Organe de gestion | RP | Broker STIAM | AA/AuthnA |
| Président de l'organe de gouvernance (rôle stratégique) | X | | | | |
| Membres de l'organe de gestion (rôle stratégique) | X | | | | |
| Président de l'organe de gestion (rôle stratégique) | | X | | | |
| Membres de l'organe de gestion (rôle stratégique) | | X | | | |
| Délégué de l'organisation (rôle stratégique) | | | X | X | X |
| Responsable d'organisation (rôle tactique) | | | X | X | X |
| OrgSysAdmin (rôle opérationnel) | | | X | | X |
| STIAM-SysAdmin (rôle opérationnel) | | | | X | |

**Tableau 4: rôles du point de vue de STIAM**

Le sujet n'est plus pris en compte, car cela n'est plus pertinent dans la suite de ce chapitre. Partant des tâches différentes, une distinction est établie entre un STIAMSysAdmin. et un OrgSysAdmin.

## 5.2 Description des rôles

Les rôles, qui sont représentés dans le Tableau 4 sont décrits avec leurs tâches, compétences et responsabilités dans la suite du document.

### 5.2.1 Président de l'organe de gouvernance

| | |
|---|---|
| Président de l'organe de gouvernance (POG) | Le président de l'organe de gouvernance est élu par l'organe de gouvernance et est compétent pour sa direction. |

**Tâches:**

- Diriger et coordonner l'organe de gouvernance
- Assumer la responsabilité des décisions de l'organe de gouvernance
- Communiquer auprès du président de l'organe de gestion concernant les exigences en matière de Policy

**Compétences:**

- Communique les décisions de l'organe de gouvernance

**Responsabilité**

- Disposer des voix prépondérantes en cas d'impasses
- Garantir la communication avec le président de l'organe de gestion

### 5.2.2 Membres de l'organe de gouvernance

| | |
|---|---|
| Membres de l'organe de gouvernance (MOGo) | Les membres de l'organe de gestion représentent les parties prenantes correspondantes au sein de l'organe de gouvernance. |

**Tâches:**

- Exercer les compétences de commande sur toutes les parties prenantes des domaines
- Commander l'IAM fédéré dans le domaine
- Diriger les domaines à partir des Policies pertinentes
- Evaluer la mise en œuvre de la gouvernance
- Surveillance des performances et conformité du domaine

**Compétences:**

- Conclure des
  - Contrats cadre
  - Accords de prestations
  - Underpinning Contracts
- Décider de l'inclusion et de l'exclusion de parties prenantes dans le domaine
- Décider concernant la participation à et l'approbation de la collaboration avec d'autres domaines

**Responsabilité**

- Garantir

- La mise en œuvre du cadre de gouvernance (Governance Framework)
- La fourniture de contributions de valeur
- La minimisation du risque
- L'optimisation des ressources
- La transparence vis-à-vis des parties prenantes
- La définition et le respect des Policies
- Le transfert de la responsabilité finale à un représentant au sein de l'organe de gouvernance
- La disponibilité des outils requis

### 5.2.3 Président de l'organe de gestion

| | |
|---|---|
| Président de l'organe de gestion (POG) | Le président de l'organe de gestion assume la responsabilité pour les décisions de l'organe de gestion. |

**Tâches:**

- Diriger et coordonner l'organe de gestion
- Assumer la responsabilité des décisions de l'organe de gestion
- Communiquer auprès du président de l'organe de gouvernance concernant la mise en œuvre

**Compétences:**

- Communiquer les décisions de l'organe de gestion

**Responsabilité**

- Disposer des voix prépondérantes en cas d'impasses
- Garantir la communication avec le président de l'organe de gouvernance

### 5.2.4 Membres de l'organe de gestion

| | |
|---|---|
| Membres de l'organe de gestion (MOGe) | Les membres de l'organe de gestion représentent les parties prenantes correspondantes au sein de l'organe de gestion. |

**Tâches:**

- Mettre en pratique les directives de l'organe de gouvernance du domaine
- Gérer la stratégie et l'architecture d'entreprise du domaine
- Gérer le portefeuille de services STIAM
- Gérer le budget et les coûts
- Coordonner la collaboration des parties prenantes
- Gérer les modifications de l'organisation (ex. intégration de nouvelles parties prenantes)

**Compétences:**

- Garantir la qualité, la gestion du risque et la sécurité

**Responsabilité**

- Garantir l'exécution de la Policy

### 5.2.5 Délégué de l'organisation

| | |
|---|---|
| Délégué de l'organisation (Dél.) | Le délégué de l'organisation est un représentant de la direction et peut être délégué dans l'organe de gouvernance. |

**Tâches:**

- Communiquer et garantir le respect des Policies
- Représenter le domaine à l'extérieur avec les autres délégués de l'organisation

**Compétences:**

- Négocier et surveiller les contrats et accords (contrat cadre; collaboration lors de la négociation et de la mise en œuvre de l'accord de prestations[6])
- Diriger la mise en œuvre STIAM dans l'organisation
- Diriger et superviser le responsable de l'organisation
- Représenter la direction et ses intérêts au sein de l'organe de gouvernance

**Responsabilité**

- Garantir l'instance d'escalade dans les questions contractuelles
- Garantir l'exactitude des informations dans le domaine et dans le contexte STIAM
- Assumer la responsabilité finale pour l'implémentation STIAM et IAM.

### 5.2.6 Responsable de l'organisation

| | |
|---|---|
| Responsables de l'organisation (RO) | Le responsable de l'organisation peut être délégué dans l'organe de gestion. |

**Tâches:**

- Soutenir les délégués de l'organisation lors de la conclusion de contrats cadre dans le contexte STIAM
- Concevoir et mettre en œuvre des Policies

**Compétences:**

- Conclure et garantir des accords de prestations et des Service Level Agreements
- Représenter l'organisation au sein de l'organe de gestion
- Diriger et superviser l'OrgSysAdmin/STIAM-SysAdmin
- Intégrer les directives de l'organisation dans l'organe de gestion

**Responsabilité**

- Se charger de la maintenance des données pertinentes pour l'organisation
- Garantir l'instance d'escalade concernant les questions litigieuses dans le cadre des Service Level Agreements et des accords de prestations.

[6] Cf. à ce sujet les annexes techniques A et B.

### 5.2.7 Organisation-SysAdmin

| | |
|---|---|
| Organisation SysAdmin (OSA) | L'administration système des applications techniques (ressources), auxquelles accèdent les sujets relève de la compétence de l'OrgSysAdmin. |

**Tâches:**

- Opérationnaliser, implémenter et garantir les Policies STIAM ainsi que leur mise en œuvre
- Se charger de la maintenance des répertoires avec des données pertinentes pour STIAM concernant l'organisation
- Gérer
  - Les attributs ainsi que leur qualité
  - L'identité ainsi que sa qualité
  - Les organisations
  - Les ressources
- Soutenir le responsable de l'organisation dans le monitoring par du reporting

**Responsabilité**

- Garantir une action proactive, réactive et compréhensible concernant le service STIAM et sa qualité selon les exigences

### 5.2.8 STIAM-SysAdmin

| | |
|---|---|
| STIAM-SysAdmin (SSA) | L'administration système du Broker STIAM relève de la responsabilité du STIAM-SysAdmin. |

**Tâches:**

- Opérationnaliser, implémenter et perfectionner le service STIAM ainsi que les Policies STIAM du point de vue du Broker STIAM
- Soutenir le responsable de l'organisation dans le monitoring par du reporting
- Administrer les données concernant les délégués de l'organisation
- Administrer les données concernant les responsables de l'organisation

**Responsabilité**

- Garantir une action proactive, réactive et compréhensible concernant le service STIAM et sa qualité selon les exigences
- Garantir une exploitation sûre afin de préserver la zone de confiance

# 6 Processus

Comme cela est évoqué au chapitre 2.1, la collaboration entre les parties prenantes STIAM repose pour l'essentiel sur les processus fondamentaux, tels que représentés à la Figure 7. Ces processus impliquent plusieurs prestataires de service IAM. Ceci requiert une extension du cadre des processus aux processus de gouvernance, de gestion et de soutien du point de vue de l'architecture administrative. Les processus principaux pour la période de définition et d'exécution correspondent à ceux de la norme [eCH-0107].

L'on a recours à la gouvernance IT comme base de définition des processus génériques de gouvernance STIAM et de gestion STIAM. COBIT 5, dans laquelle a été récemment intégrée la norme ISO/IEC 38500 déjà évoquée, constitue à cet égard un vaste cadre, utilisé dans plusieurs branches. A cet égard, les processus sont compris comme des processus non pas à exécuter, mais à contrôler et à surveiller.

Le service STIAM constitue un service comme tous les autres services IT. Concernant la gestion de services IT, l'on a recours dans l'industrie à la norme ITIL en tant que Best-Practice-Framework supplémentaire. C'est la raison pour laquelle l'édition 2011 ITIL est utilisée dans ce chapitre concernant les processus de soutien STIAM. Ce Best-Practice-Framework est en partie comparable avec la norme ISO/IEC 20000 déjà évoquée dans la présente norme. Ce faisant, les processus de gestion de service s'entendent comme processus à exécuter, qui garantissent que les services fournis apportent de la valeur ajoutée pour le client.

Le mapping entre les processus à contrôler (COBIT/Governance et Management) et les processus à mettre en œuvre (ITIL/gestion de services IT) est expliqué plus en détail en annexe F par un tableau sommaire.

La Figure 7 représente la carte nationale des processus STIAM. Les processus correspondants de gouvernance, de gestion et de soutien sont décrits plus en détail au chapitre suivant. Ils ne sont pas mentionnés sous cette forme dans [eCH-0107].

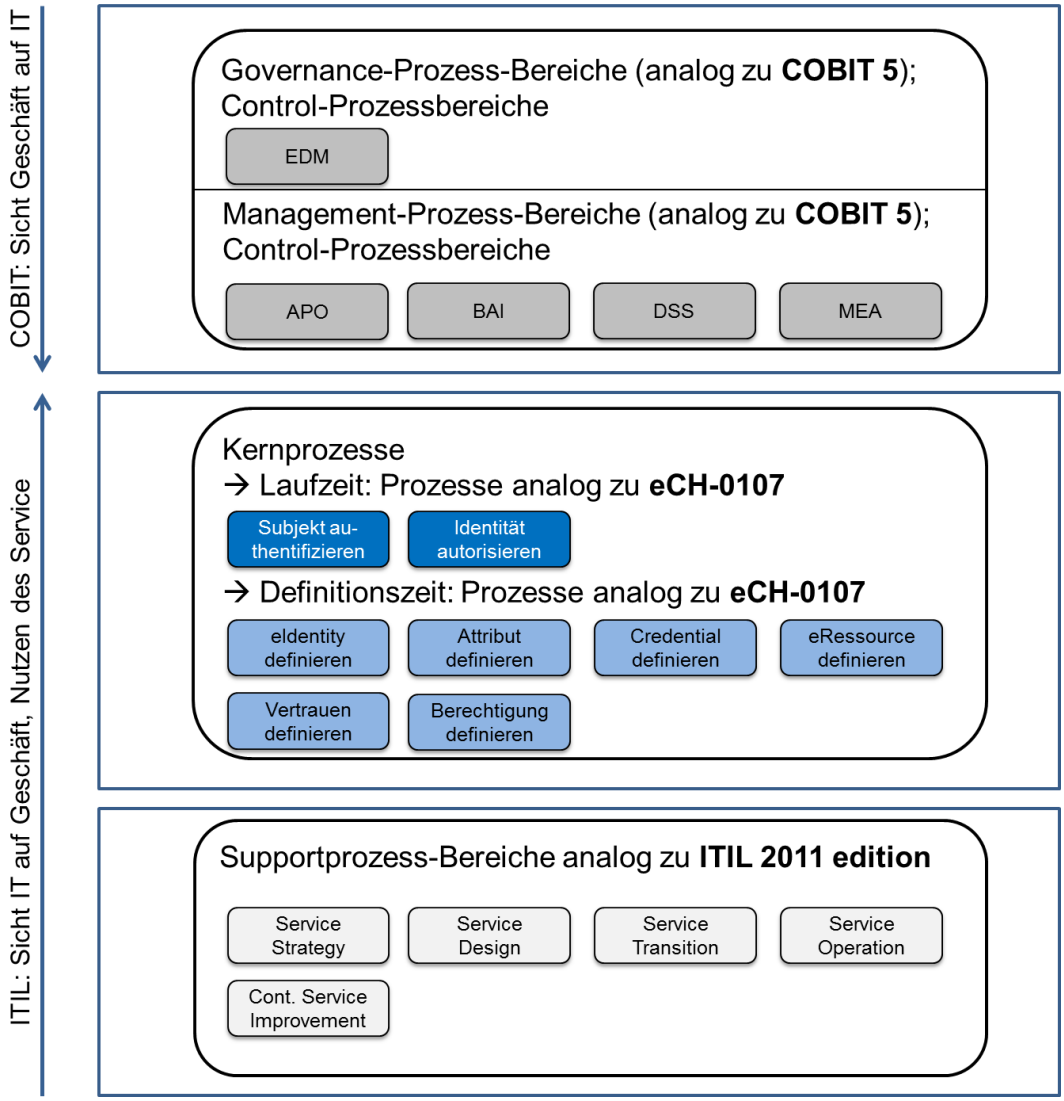


**Figure 7: Carte nationale des processus STIAM**

## 6.1 Processus de gouvernance

Les chapitres 6.1 et 6.2 définissent quels processus de gouvernance COBIT et de gestion COBIT sont nécessaires pour STIAM. En outre, des matrices RACI[7] servent à déterminer quel rôle STIAM est compétent pour quel processus. La liste complète des processus COBIT, avec la catégorisation recommandé, négligeable et non pertinent, se trouve en annexe D.

[7] Dans le cadre de la méthode de matrice RACI, les lettres ont les significations suivantes: R = Responsible (compétence d'exécution), A = Accountable (responsabilité finale), C = Consulted (pour consulter), I = Informed (pour informer).

| | |
|---|---|
| Processus de gouvernance | Les processus de gouvernance permettent de garantir que, dans un domaine STIAM, l'implémentation d'un cadre de gouvernance, la valeur ajoutée, la minimisation des risques ainsi que la transparence au-delà de toutes les barrières de prestataires de service IAM, soient atteintes. |

**Evaluate, Direct and Monitor (EDM)**

| Processus | Rôles | | | | | |
|---|---|---|---|---|---|---|
| | MOGo | MMGe | Dél. | RO | OSA | SSA |
| Garantir et commissionner la mise en place et la maintenance du cadre de gouvernance (STIAM). | A | C | R | C | I | I |
| Garantir et commissionner la mise à disposition de la valeur ajoutée (par le service STIAM). | A | C | R | C | I | I |
| Garantir et commissionner la minimisation des risques concernant STIAM. | A | C | R | C | I | I |
| Garantir et commissionner l'optimisation des ressources concernant le service STIAM | A | C | R | C | I | I |
| Garantir la transparence vis-à-vis de toutes les parties prenantes dans le domaine STIAM et au-delà. | A | C | R | C | I | I |

**Tableau 5: matrice RACI EDM**

## 6.2 Processus de gestion

| | |
|---|---|
| Processus de gestion | Les processus de gestion permettent de s'assurer que le domaine STIAM est opérationnellement fonctionnel et que les directives correspondantes dans les processus de gouvernance sont bien mises en œuvre. |

**Align, Plan and Organize (APO)**

| Processus | Rôles | | | | | |
|---|---|---|---|---|---|---|
| | MOGo | MMGe | Dél. | RO | OSA | SSA |
| Garantir qu'un cadre de gouvernance correspondant est bien implémenté pour STIAM. | C | A | I | R | | |
| Garantir qu'une stratégie STIAM a bien été définie et adoptée à l'échelle du domaine. | C | A | I | R | | |
| Garantir qu'une architecture STIAM est développée, implémentée et perfectionnée. | C | A | I | R | | |
| Garantir qu'un portefeuille de services STIAM est élaboré et intégré. | C | A | I | R | | |
| Garantir que les ressources financières et personnelles pertinentes pour STIAM sont constamment à disposition. | C | A | I | R | | |
| Garantir les relations entre les parties prenantes. | C | A | I | R | | |
| Garantir les accords de Service Level | C | A | I | R | | |
| Garantir que la qualité de STIAM est garantie. | C | A | I | R | | |
| Garantir une gestion des risques raisonnable. | C | A | I | R | | |
| Garantir la sécurité de STIAM. | C | A | I | R | | |

**Tableau 6: matrice RACI APO**

**Build, Acquire and Implement (BAI)**

| Processus | Rôles | | | | | |
|---|---|---|---|---|---|---|
| | MOGo | MMGe | Dél. | RO | OSA | SSA |
| Garantir que toutes les capacités et disponibilités adéquates pour STIAM sont bien réunies, au-delà de toutes les barrières des participants. | C | A | I | R | | |
| Garantir que les changements organisationnels autour du STIAM sont bien entrepris, que l'utilisation du service STIAM est aussi efficace et effective que possible et que la création de la zone de confiance dans le domaine apporte la plus grande utilité possible pour les parties prenantes. | C | A | I | R | | |
| Garantir que la gestion des changements pour STIAM est efficace et effective et que les changements sont documentés et repris de manière systématique. | C | A | I | R | I | I |
| Garantir que les outils sont bien gérés. | C | A | I | R | | |

**Tableau 7: matrice RACI BAI**

**Deliver, Service and Support (DSS)**

| Processus | Rôles | | | | | |
|---|---|---|---|---|---|---|
| | MOGo | MMGe | Dél. | RO | OSA | SSA |
| Garantir l'exploitation du service STIAM. | C | A | I | R | | |
| Garantir une gestion adéquate pour les co-participants à STIAM, les Service Requests et Incidents. | C | A | I | R | | |
| Garantir une gestion adéquate, du point de vue STIAM, pour tous les participants, des problèmes de service STIAM. | C | A | I | R | | |
| Garantir une forme, adéquate pour le STIAM, de la Continuity Management, concernant les catastrophes en partant des exigences de Business-Continuity. | C | A | I | R | I | I |
| Garantir les contrôles des processus administratifs | C | A | I | R | | |

**Tableau 8: matrice RACI DSS**

**Monitor, Evaluate and Assess (MEA)**

| Processus | Rôles | | | | | |
|---|---|---|---|---|---|---|
| | MOGo | MMGe | Dél. | RO | OSA | SSA |
| Surveiller, évaluer et juger la performance et la conformité du service STIAM. | C | A | I | R | C | C |
| Surveiller, évaluer et juger le système de contrôles interne en relation avec le service STIAM. | C | A | I | R | I | I |
| Surveiller, évaluer et juger de la conformité avec les exigences externes concernant le service STIAM. | C | A | I | R | I | I |

**Tableau 9: matrice RACI MEA**

## 6.3 Processus principaux

| | |
|---|---|
| Processus principaux | Les processus principaux comprennent tous les processus de la période de définition et d'exécution selon [eCH-0107]. |

Pas de description détaillée à ce stade, renvoi est fait à la norme [eCH-0107].

## 6.4 Processus de soutien

Les processus de soutien STIAM sont explicités dans la suite du document.

Comme cela a été évoqué, le ITIL édition 2011 représente un cadre taillé sur mesure pour ce secteur. Les processus/groupes de processus nécessaires qui y sont abordés sont traités ci-après, en spécifiant en outre comment ceux-ci peuvent être utilisés dans le contexte STIAM. L'annexe F fournit une liste complète des processus ITIL avec la catégorisation E avec la catégorisation recommandé, négligeable et non pertinent.

| | |
|---|---|
| Processus de soutien | Les processus de soutien incluent la gestion des services IT et décrivent les exigences imposées à la mise en place et à l'exploitation des services IT STIAM par l'IT Service Provider IT. |

**Service Strategy**

- Strategy Management for IT-Services: mise en œuvre d'une stratégie adéquate pour STIAM du point de vue du service IT.
- Service Portfolio Management: gérer un «pipeline» de développement pour les services STIAM, gérer le service STIAM dans le catalogue des services (du Service Provider STIAM), gérer les Retired Services dans le contexte STIAM.
- Financial Management: mise en œuvre de la gestion de l'établissement de budgets autour du service STIAM côté Broker STIAM, calcul des coûts pour le service STIAM ainsi que décompte du service STIAM, dans la mesure où le décompte est envisagé selon le modèle commercial.
- Business Relationship Management: ceci comprend la gestion stratégique des relations entre les parties prenantes impliquées, en ce qui concerne le STIAM Broker Service.
- Demand Management: gestion stratégique de la demande de services STIAM et de son adéquation avec la capacité à fournir du service STIAM.

**Service Design**

- Service Catalogue Management: documentation et maintenance en continu du service STIAM dans le catalogue de services client et technique
- Service Level Management: réception et intégration de Service Level Requests, mise en œuvre des Service Levels ainsi que gestion des Service & Operational Level Agreements et Underpinning Contracts en lien avec les STIAM-SLA.[8] Ceci représente une condition nécessaire centrale pour la constitution d'une zone de confiance.

[8] Cf. à ce sujet les annexes techniques A et B.

- Capacity Management: mise en œuvre de la planification et qualité de la capacité du service STIAM à des coûts adéquats en partant des exigences administratives en matière de capacité.
- Availability Management: contrôle de la mise en œuvre adéquate de la disponibilité requise du service STIAM, comme pour le Service Level Agreement ainsi que sa sécurisation par des Operational Level Agreements (à l'intérieur du Service Provider) et Underpinning Contracts (fournisseurs).
- IT Service Continuity Management: planification et mise en œuvre d'une continuité adéquate du service STIAM en cas de catastrophe en partant des exigences administratives.
- Information Security Management: mise en œuvre d'une sécurité adéquate des informations concernant le service STIAM et mise en place d'un système de sécurité STIAM.

**Service Transition**

- Change Management: mise en œuvre d'une gestion systématique et documentée des modifications concernant les services STIAM.
- Service Asset and Configuration Management: mise en œuvre d'une documentation correcte des services STIAM au-delà des barrières des parties prenantes impliquées.

**Service Operation**

- Incident Management: mise en œuvre d'un Incident Management au-delà des barrières des parties prenantes impliquées dans le contexte STIAM.
- Request Fulfillment: mise en œuvre d'un Request Fulfillment adéquat au-delà des barrières des partenaires STIAM impliqués, concernant les services STIAM primaires et secondaires.
- Access Management: garantie d'une gestion adéquate des accès concernant le service STIAM.
- Problem Management: garantie d'une gestion adéquate des problèmes de service STIAM au-delà des barrières des parties prenantes impliquées dans le STIAM.

**Continual Service Improvement**

- Seven-step Improvement Process: mise en œuvre d'un processus d'amélioration adéquat au-delà des barrières des parties prenantes impliquées concernant le service STIAM.

# 7 Exclusion de responsabilité – droits de tiers

Les normes élaborées par l'Association **eCH** et mises gratuitement à la disposition des utilisateurs, ainsi que les normes de tiers adoptées, ont seulement valeur de recommandations. L'Association **eCH** ne peut en aucun cas être tenue pour responsable des décisions ou mesures prises par un utilisateur sur la base des documents qu'elle met à disposition. L'utilisateur est tenu d'étudier attentivement les documents avant de les mettre en application et au besoin de procéder aux consultations appropriées. Les normes **eCH** ne remplacent en aucun cas les consultations techniques, organisationnelles ou juridiques appropriées dans un cas concret.

Les documents, méthodes, normes, procédés ou produits référencés dans les normes **eCH** peuvent le cas échéant être protégés par des dispositions légales sur les marques, les droits d'auteur ou les brevets. L'obtention des autorisations nécessaires auprès des personnes ou organisations détentrices des droits relève de la seule responsabilité de l'utilisateur.

Bien que l'Association **eCH** mette tout en œuvre pour assurer la qualité des normes qu'elle publie, elle ne peut fournir aucune assurance ou garantie quant à l'absence d'erreur, l'actualité, l'exhaustivité et l'exactitude des documents et informations mis à disposition. La teneur des normes **eCH** peut être modifiée à tout moment sans préavis.

Toute responsabilité relative à des dommages que l'utilisateur pourrait subir par suite de l'utilisation des normes **eCH** est exclue dans les limites des réglementations applicables.

# 8 Droits d’auteur

Tout auteur de normes **eCH** en conserve la propriété intellectuelle. Il s’engage toutefois à mettre gratuitement, et pour autant que ce soit possible, la propriété intellectuelle en question ou ses droits à une propriété intellectuelle de tiers à la disposition des groupes de spécialistes respectifs ainsi qu’à l’association **eCH**, pour une utilisation et un développement sans restriction dans le cadre des buts de l’association.

Les normes élaborées par les groupes de spécialistes peuvent, moyennant mention des auteurs **eCH** respectifs, être utilisées, développées et déployées gratuitement et sans restriction.

Les normes **eCH** sont complètement documentées et libres de toute restriction relevant du droit des brevets ou de droits de licence. La documentation correspondante peut être obtenue gratuitement.

Les présentes dispositions s’appliquent exclusivement aux normes élaborées par **eCH**, non aux normes ou produits de tiers auxquels il est fait référence dans les normes **eCH**. Les normes incluront les références appropriées aux droits de tiers.

# Annexe A – Références & bibliographie


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

[eCH-0107] eCH-0107 (2013): Principes de conception pour la gestion de l'identité de l'accès (IAM). eCH. Zurich.

[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 edition, 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 (consulté le 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.


# Annexe B – Collaboration & vérification

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

# Annexe C – Abréviations

| | |
|---|---|
| TCR | Tâches, compétences et responsabilité |
| APO | Domaine COBIT Align, Plan, Organize |
| BAI | Domaine COBIT Build, Acquire, Implement |
| COBIT | Control Objectives for Information and related Technology |
| DSS | Domaine COBIT Deliver, Service, Support, |
| EDM | Domaine COBIT 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 | Domaine COBIT Monitor, Evaluate, Assess |

# Annexes techniques

## Annexe technique A – Architecture de contrats et accords

Dans le cadre de la fourniture de prestations de services STIAM, on peut établir une distinction entre différents types de contrats qui, de manière typique, sont regroupés en un tout dans une architecture contractuelle (Figure 8). L'idée de la séparation des différents types de contrats et accords est que les aspects généraux des contrats soient réglés non pas individuellement dans chaque SLA, mais au contraire au niveau des contrats cadres et accords de prestations. Pour plus de détails concernant la caractérisation des différents types de documents contractuels, se reporter à la Figure 8.

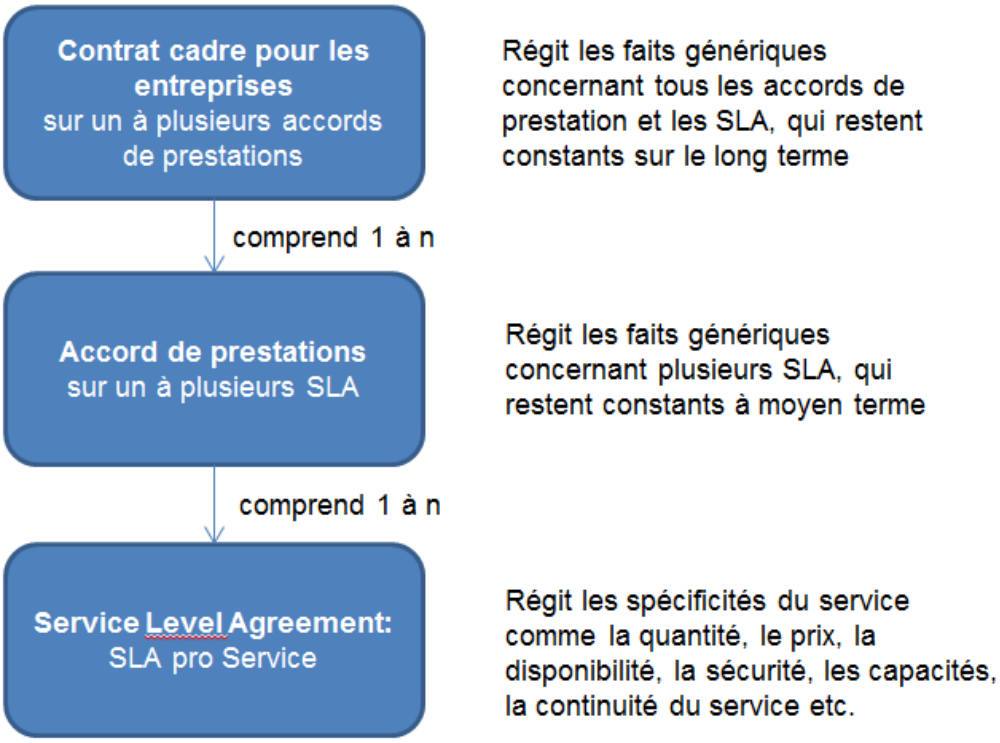


**Figure 8: Architecture contractuelle dans le contexte des SLA (d'après [Prengemann 2006])**

## Annexe technique B – Structure possible d'un Service Level Agreement spécifique STIAM (SLA)

Le contenu possible d'un SLA est explicité dans la suite du document pour le service STIAM ([Hunnbeck 2011], [Steinbeck 2011]). A l'exception des éléments spécifiques STIAM (italique), les éléments SLA proviennent de [Hunnebeck 2011] et [Steinberg 2011] (ITIL 2011 edition/Best Practice).

- Amendment Sheet – Change History Document, etc.
- SLA entre partie 1 et partie 2 avec les adresses correspondantes
- SLA concernant le service X/Y/Z
- Durée de validité du SLA
- Signatures
- Description du service
- Portée du Service Level Agreement
- Temps (heures) de service
- Disponibilité du service
- Reliability – fiabilité du service
- Assistance client
- Points de contact et escalades
- Service Performance
- Fonctionnalité du service
- Change Management
- Service Continuity
- (Aspects) de sécurité
- Responsabilités
- Décompte, formules, prix, quantités, périodes de décompte, paiements de pénalités…
- Service Reporting et Reviews
- *Accord pour les niveaux de qualité et de confiance ex. sur la base de QAA*
- *Définition de la qualité des attributs*
- *Listes d'attributs, accords portant sur la sémantique et la syntaxe, etc., règles de remplissage pour les bases de données en lien avec le Broker STIAM*
- *Définition des limites de domaine*
- *Accords spéciaux concernant la fonction et la collaboration des organes de gouvernance et de gestion*
- *Accords des délégués de l'organisation, responsables de l'organisation et SysAdmin ainsi que leurs coordonnées*
    - *Règles concernant la nomination*
    - *Coordonnées*
    - *Tâches et obligations*
    - *Questions et clarifications relatives à la responsabilité*
- Glossaire sur les SLA

## Annexe technique C – Eléments possibles d'une Policy STIAM

Les Policies contiennent des éléments, qui régissent la collaboration dans le domaine et par delà les limites des domaines. Elles contiennent des règles génériques et spécifiques, qui sont pertinentes pour l'établissement de la confiance dans le domaine et dans la correspondance avec les autres domaines. Les Policies STIAM doivent traiter entre autres des points suivants:

- Définition des limites du (méta-)domaine
- Relations et tâches de et entre organe de gouvernance et de gestion
- Membres du (méta-)domaine pour chaque catégorie de parties prenantes
- Conditions (de confiance) de la coopération dans le (méta-)domaine
- Conditions (de confiance) de la coopération avec d'autres (méta-)domaines
- Directives portant sur l'IAM interne pour les parties prenantes impliquées
- Directives portant l'IAM fédéré «inter-parties prenantes»
- Directives portant sur la gestion des données pour l'intermédiaire STIAM en fonction des parties prenantes, qui assurent elles-mêmes la maintenance des données, par exemple sur l'intermédiaire STIAM
- Policies des contrats
- Policies concernant les rôles, leurs tâches, compétences, responsabilités ainsi que concernant les séparations des fonctions (Segregation of Duties)
- Policies concernant les aspects de qualité (notamment concernant la qualité des données) et de confiance (qu'ils soient institutionnels-organisationnels, contractuels, techniques)
- Policies technique par exemple au niveau du Decision & Enforcement Point

## Annexe technique D – Mapping des processus COBIT avec les organes STIAM

Le Tableau 10 présente, sur la base du cadre COBIT 5.0, une affectation de processus de contrôle COBIT aux deux organes, qui sont différents pour STIAM ([ISACA 2012a], [ISACA 2012b]). Les compétences correspondantes sont clairement stipulées et peuvent être comprises comme des définitions complémentaires de tâches, compétences et responsabilités pour STIAM.

De la même manière, les processus de contrôle COBIT peuvent être compris comme des différentiations complémentaires aux processus GRC traités sommairement dans [eCH-0107]. Pour de plus amples explications concernant les processus de contrôle, se reporter au cadre COBIT 5.0 ([ISACA 2012a], [ISACA 2012b]). Une matrice RACI détaillée y est présentée pour chacun des processus de contrôle répertoriés ci-après. Seuls les rôles STIAM pertinents sont abordés dans le processus correspondant.

Les abréviations utilisées sont expliquées après le Tableau 10.

Le nombre X indique la signification des contrôles de processus correspondants pour le contexte STIAM.

Légende du Tableau 10:

XXX Nécessaire

XX Recommandé

X Négligeable

--- non pertinent

| **Processus COBIT** | **Domaine COBIT** | **Compétence organe de gouvernance** | **Compétence organe de gestion** |
|---|---|---|---|
| Garantir la mise en place et la maintenance du cadre de gouvernance | EDM | XXX | --- |
| Garantir la livraison de contributions de valeur | EDM | XXX | --- |
| Garantir l'optimisation des risques | EDM | XXX | --- |
| Garantir l'optimisation des ressources | EDM | XXX | --- |
| Garantir la transparence à l'égard des parties prenantes | EDM | XXX | --- |
| Gérer le cadre IT-Management | APO | --- | XXX |
| Gérer la stratégie | APO | --- | XXX |
| Gérer l'architecture de l'entreprise | APO | --- | XXX |
| Gérer les innovations | APO | --- | X |
| Gérer le portefeuille | APO | --- | XXX |
| Gérer le budget et des coûts | APO | --- | XXX |

| | | | |
|---|---|---|---|
| Gérer le personnel | APO | --- | X |
| Gérer les relations | APO | --- | XXX |
| Gérer les accords de service | APO | --- | XXX |
| Gérer les fournisseurs | APO | --- | XX |
| Gérer la qualité | APO | --- | XXX |
| Gérer le risque | APO | --- | XXX |
| Gérer la sécurité | APO | --- | XXX |
| Gérer les programmes et les projets | BAI | --- | XX |
| Gérer la définition d'exigences | BAI | --- | XX |
| Gérer l'identification et la construction de solutions | BAI | --- | X |
| Gérer la disponibilité et de la capacité | BAI | --- | XXX |
| Gérer la facilitation des changements organisationnels | BAI | --- | XX |
| Gérer les changements | BAI | --- | XXX |
| Gérer la réception et de la transmission des modifications | BAI | --- | XX |
| Gérer les connaissances | BAI | --- | X |
| Gérer le matériel | BAI | --- | XXX |
| Gérer la configuration | BAI | --- | XX |
| Gérer l'exploitation | DSS | --- | XXX |
| Gérer les requêtes et dérangements de service | DSS | --- | XXX |
| Gérer les problèmes | DSS | --- | XX |
| Gérer la continuité | DSS | --- | XXX |
| Gérer les services de sécurité | DSS | --- | XXX |
| Gérer les contrôles des processus administratifs | DSS | --- | XXX |
| Surveiller, évaluer et juger la performance et la conformité | MEA | --- | XXX |
| Surveiller, évaluer et juger le système de contrôle interne | MEA | --- | XXX |
| Surveiller, évaluer et juger la conformité aux exigences externes | MEA | --- | XXX |

**Tableau 10: processus COBIT et leur affectation et signification en lien avec l'organe de gouvernance et de gestion**

## Annexe technique E – Mapping des processus ITIL avec les parties prenantes STIAM

A partir du cadre ITIL édition 2011, le Tableau 11 présente comment les processus ITIL sont affectés aux parties prenantes, qui sont différentes dans le contexte STIAM. Les compétences correspondantes sont clairement stipulées et peuvent être comprises comme des définitions complémentaires de tâches, de compétences et de responsabilité pour STIAM.

De la même manière, les processus ITIL peuvent être compris comme des différenciations complémentaires concernant les processus GRC traités sommairement dans [eCH-0107]. Pour de plus amples explications concernant les processus ITIL, se reporter au cadre ITIL 2011 edition ([Cannon 2011], [Hunnebeck 2011], [Rance 2011], [Steinberg 2011] et [Lloyd 2011]).[9]

**Légende du** Tableau 11**:**

XXX Nécessaire

XX Recommandé

X Négligeable

--- non pertinent

S Service Strategy

D Service Design

T Service Transition

O Service Operation

CSI Continual Service Improvement

| **Processus ITIL** | | **Broker STIAM** | **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 |

| Processus ITIL | | Broker STIAM | RP | AA | AuthnA |
|---|---|---|---|---|---|
| Availability Management | D | XXX | XXX | XXX | XXX |
| 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 |

**Tableau 11: processus ITIL et leur pertinence pour les parties prenantes STIAM**

## Annexe technique F - Mapping entre COBIT et ITIL

Le Tableau 12 met en évidence le mapping entre COBIT et ITIL édition 2011. Les processus COBIT doivent être compris comme des processus à contrôler (du point de vue de l'organe de gouvernance et de gestion). A l'inverse, les processus ITIL doivent être compris comme des processus à mettre en œuvre (du point de vue du fournisseur de service STIAM). Pour la plupart des processus COBIT, il existe des processus correspondants côté ITIL. Tous les processus COBIT et ITIL nécessaires pour le STIAM figurent dans le Tableau 12. Concernant l'architecture d'entreprise, il n'existe pas de mapping de COBIT vers ITIL pour les modifications de l'organisation et l'exploitation.

| | **Phases et processus ITIL** | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Service Strategy | | | | | Service Design | | | | | Service Transition | | Service Operation | | |
| | Strategie-Management for IT-Services | Service-Portfolio Management | Financial Management for 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 |
| **Processus COBIT** | | | | | | | | | | | | | | | |
| Gérer la stratégie | X | | | | | | | | | | | | | | |
| Gérer l'architecture de l'entreprise | | | | | | | | | | | | | | | |
| Gérer le portefeuille | | X | | | | | | | | | | | | | |
| Gérer le budget et des coûts | | | X | | | | | | | | | | | | |
| Gérer les relations | | | | X | X | | | | | | | | | | |
| Gérer les accords de service | | X | | | X | X | | | | | | | | | |
| Gérer la qualité | | | | | | | | | | X | | | | | |
| Gérer le risque | | | | | | | | | | X | | | | | |
| Gérer la sécurité | | | | | | | | | | X | | | | | |
| Gérer la disponibilité et des capacités | | | | | | | X | X | | | | | | | |
| Gérer les changements org. | | | | | | | | | | | | | | | |
| Gérer les outils | | | | | | | | | | | | X | | | |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Gérer les modifications | | | | | | | | | | | X | | | | |
| Gérer la configuration | | | | | | | | | | | | X | | | |
| Gérer l'exploitation | | | | | | | | | | | | | | | |
| Gérer les requêtes de service | | | | | | | | | | | | | X | X | |
| Gérer la continuité | | | | | | | | | X | | | | | | |
| Gérer les services de sécurité | | | | | | | | | | X | | | | | |
| Gérer les contrôles de processus administratifs | | | | | | | | | | | | | | | X |

**Tableau 12: Mapping entre COBIT et ITIL**