eCH-0107 Principes de conception pour la gestion de l’identité et de l’accès (IAM)

Titre	Principes de conception pour la gestion de l’identité et de l’accès (IAM)
Code	eCH-0107
Type	Norme (nouveau)
Stade	définie; expérimentale; appliquée; diffusée
Version	2.0
Statut	Annulé
Validation	2018-11-28
Date de publication	2013-12-04
Remplace	1.00 (Best Practice)
Langues	Allemand (original), français (traduction)
Annexes	--
Auteurs	Ronny Bernold, BFH FBW, ronny.bernold@bfh.ch Gerhard Hassenstein, BFH TI, gerhard.hassenstein@bfh.ch Annett Laube-Rosenpflanzer, BFH TI, annett.laube@bfh.ch Andreas Spichiger, BFH FBW, andreas.spichiger@bfh.ch Martin Topfel, BFH FBW, martin.topfel@bfh.ch eCH groupe spécialisé IAM V1.0: Willy Müller, UPIC, willy.mueller@isb.admin.ch Hans Häni, AFT TG Groupe de projet SEAC IAM
Editeur / distributeur	Association eCH, Mainaustrasse 30, Case postale, 8034 Zurich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Condensé

Le présent document définit les principes, les règles et les cadres réglementaires relatifs à la conception du système IAM, devant être pris en compte dans le cadre de la mise à disposition des solutions IAM fédératives dans la cyberadministration Suisse. Le principe de conception définit un paysage IAM modèle pour les scénarios d'application inter-organisationnels pour les applications existantes et nouvelles, en partant du principe que les services administratifs peuvent être fournis et utilisés par diverses parties prenantes. La norme définit les exigences, les parties prenantes, les processus, l'architecture de l'information, les services administratifs et les modèles d'Identity Federation. La norme peut être utilisée dans l'ensemble des secteurs de l'E-society.

Sommaire

Liste des illustrations

Liste des tableaux

1 Statut du document

Annulé: Le document a été retiré de eCH. Il ne doit plus être utilisé.

2 Introduction

2.1 Vue d‘ensemble

Au cours des dernières années, l’utilisation d’internet s’est accrue de manière constante. Internet est de plus en plus fréquemment utilisé, non seulement en tant que source d’information, mais également pour réaliser des affaires.

Les processus administratifs basés sur internet présupposent des agents dignes de confiance et donc une entente avec les partenaires administratifs. Le service de gestion de l’identité et de l’accès (Identity and Access Management, IAM) interne à l’organisation a jusqu’à présent garanti des services administratifs adaptés. Les scénarios d’utilisation interorganisationnels montrent les limites de l’IAM interne. En effet, des dépenses considérables sont nécessaires pour qu’il puisse être utilisé par plusieurs domaines. La présente norme définit les tâches et les principes de conception pour l’organisation de systèmes IAM fédérés, afin que la limite mentionnée ci-dessus puisse être surmontée. Ces principes doivent être pris en compte lors de la préparation de solutions destinées à l’E-Government suisse, afin que les applications et les services locaux puissent être utilisés par toutes les organisations. La norme sert de base pour toutes les personnes qui élaborent des solutions destinées à un environnement E-Government, potentiellement ou déjà préparé pour un accès externe (Internet-eServices).

Dans un environnement E-Government, il s’agit, comme dans le contexte global de l’E-Society (E-Government, E-Health, E-Economy), du principe que des sujets (administrations, citoyens, organisations, entreprises, applications spécifiques) veuillent utiliser des ressources (services des municipalités, des cantons, de la confédération ou d’un tiers). Le défi majeur réside dans le fait que les ressources et les sujets puissent se trouver dans des domaines différents.

2.1.1 Introduction IAM

Les éléments-clés d’un IAM sont essentiels pour comprendre la norme et sont donc brièvement expliqués dans ce paragraphe.

Les éléments-clés de l’IAM sont présentés ci-dessous par la Figure 1. Le centre de toutes les préoccupations IAM est l’accès contrôlé d’un sujet à une ressource.

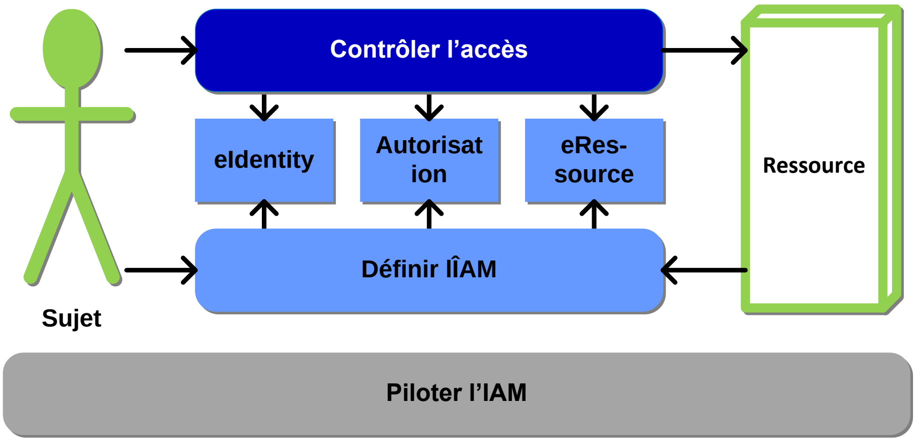

Figure 1 Vue d'ensemble de l'IAM

Les éléments *contrôler l'accès* et *définir l'IAM* constituent les processus centraux utilisés par le sujet et la ressource. Ces processus centraux sont utilisés à des moments différents, symbolisés par les couleurs bleu clair et bleu foncé.

gris	Dans ce document, les éléments en gris sont des éléments qui sont déjà actifs avant le temps de définition (p. ex. Governance).
bleu clair	Dans ce document, la couleur bleu clair est utilisée exclusivement pour le temps de définition, pendant lequel toutes les informations des éléments d'information sont classées (c.-à-d. définies).
bleu foncé	La couleur bleu foncé est systématiquement utilisée pour la durée d'exécution. L'accès basé sur les éléments d'information définis est contrôlé (octroyé ou refusé) pendant la durée d'exécution.
vert clair	Dans ce document, la couleur vert clair est exclusivement utilisée pour les objets du monde réel.

Tableau 1 Utilisation des couleurs dans le document

Le *sujet* et la *ressource* sont des agents (et des objets du monde réel) qui remplissent leurs objectifs à l'aide des processus IAM. L'objectif du *sujet* est l'accès à la *ressource* souhaitée. L'objectif de la *ressource* est de se protéger ses ressources contre des accès non-autorisés aux informations et aux services.

Des illustrations numériques, également appelés des éléments d'information, sont attribuées aux objets du monde réel (sujet, ressource), afin que les processus principaux puissent également fonctionner dans l'univers numérique. L'*eIdentity* (bleu clair) est attribuée au sujet (vert), et l'eRessource (bleu clair) est attribuée aux ressources (vert). Afin de réaliser ses objectifs, la ressource définit dans l'élément d'information Autorisation (règle d'accès/droit d'accès) quelle *eIdentity* peut avoir accès à quelle *ressource* et sous quelles conditions.

Le processus *Contrôler l'IAM* décrit les activités de définition des exigences et des conditions générales pour exploiter un environnement IAM.

2.1.2 IAM fédéré

Contrairement à l'IAM interne à l'organisation, l'IAM fédéré part d'*eIdentities* inter-organisationnelles. L'*eIdentity* d'un *sujet* est établie dans le *domaine* A, mais peut également comporter des informations dans le *domaine* B, qui sont attribuées à l'*eIdentity* du *domaine* A. De plus, il est possible que des sujets dont l'*eIdentity* provient du *domaine* A puissent accéder à des *ressources* du *domaine* B. Afin de pouvoir établir un IAM *fédéré*, les différents *domaines* doivent avoir confiance l'un dans l'autre. Cette confiance est fondée sur des accords implicites et explicites.

2.1.3 Domaine d'application

La vision de la gestion mise en réseau et des processus globaux en résultant dans l'E-Government suisse nécessite une *gestion de l'identité et des autorisations* inter-autorités. La présente norme eCH-0107 constitue la base de la standardisation IAM. Elle définit les principes, les règles et les cadres réglementaires pour la conception du système IAM devant être pris en compte lors de la mise en place de solutions IAM inter-organisationnelles, dans l'E-Government fédéral suisse.

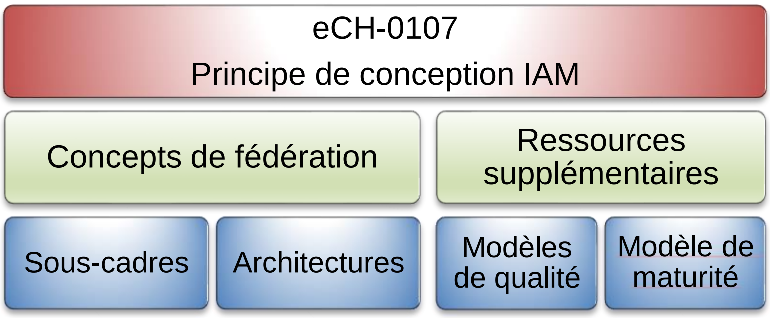

Figure 2 Classement de la norme eCH-0107

Les concepts pour les solutions IAM fédérées et les ressources supplémentaires se positionnent sous la norme eCH-0107. Les concepts sont des descriptions concrètes de la forme que doit avoir une proposition de solution IAM et contiennent des sous-cadres et architectures devant être pris en compte pour la mise en œuvre. Par ailleurs, des ressources sont proposées aux concepts, mettant des informations complémentaires à disposition et qui sont pertinentes pour plus d'un concept. Les modèles de qualité et de maturité représentés sont des exemples de ressources et ne sont pas définitifs.

Les exigences et les principes de conception doivent être pris en compte lors de la préparation dans les solutions *IAM* inter-organisationnelles de l'E-Government suisse afin de pouvoir utiliser des applications et services locaux de manière inter-organisationnelle.

2.1.4 Définition

Les principes de conception et les règles figurant dans cette norme constituent le cadre réglementaire des systèmes *IAM* fédéraux. Les éléments principaux et les parties prenantes les plus fréquentes seront expliqués. Les différentes typologies des systèmes IAM fédéraux seront également introduites dans cette norme. L'orchestration et la mise en œuvre concrète des propositions de solutions seront toutefois thématisées dans les concepts et ne seront pas prises en compte dans cette norme.

L'*IAM* est l'un des moyens permettant de mettre en place des mesures importantes en termes de sécurité. En conséquence, les solutions IAM doivent naturellement satisfaire aux exigences de sécurité en vigueur, qui sont souvent élevées. Ces exigences sont décrites dans les normes de sécurité correspondantes et ne seront pas à nouveau mentionnées dans ce document.

2.1.5 Avantages

Des progrès considérables (désormais documentés et définis dans la deuxième version de la norme) ont été réalisés dans l'environnement *IAM* fédéré, depuis la version 1 de la norme eCH-0107. La présente norme présente les avantages suivants:

- La définition d'un cadre réglementaire et des exigences pour les systèmes *IAM*.
- Les éléments principaux d'un *IAM* fédéré sont connus et constituent la base pour le remaniement d'idées et de propositions de solutions.
- La définition d'un paysage *IAM* modèle (parties prenantes, processus, modèle d'information, services administratifs) dans des scénarios d'application inter-organisationnels.
- Les concepts d'Identity Federations possibles sont représentés.
- La terminologie utilisée dans le contexte de l'*IAM* fédéré est expliquée dans un glossaire circonstancié relatif à l'environnement *IAM*, et permet de discuter de ce thème à l'aide d'un vocabulaire commun.

2.2 Axes principaux

La présente norme eCH-0107 se divise en six chapitres (en plus de l'introduction), brièvement décrits ci-dessous.

Le chapitre 3 identifie les parties prenantes majeures d'un *IAM* fédéré.

Le chapitre 4 dresse la liste des visions architecturales et des exigences générales, du point de vue des agents *Sujet* et *Ressource*.

Le chapitre 5 présente les informations architecturales et explique les différents éléments. À l'aide de la sémantique, les objets du monde réel sont attribués objets des interfaces au moyen de l'architecture d'information.

Le chapitre 6 définit les processus importants pour toutes les parties prenantes, ce qui signifie que ce ne sont pas uniquement les processus du prestataire *IAM* qui sont pris en compte, mais également ceux des utilisateurs *IAM*.

Le chapitre 7 présente les services dans un *IAM* fédéré, du point de vue administratif. Les fonctions et interfaces des services sont également définies.

Le chapitre 8 présente les différentes variantes pour le développement d'un *IAM* fédéré.

Afin que les mêmes termes soient systématiquement utilisés dans le contexte d'un *IAM* fédéré, l'annexe D comporte un glossaire circonstancié qui explique les termes-clés de l'environnement *IAM*.

2.3 Caractère normatif des chapitres

Les chapitres de la présente norme sont soit de caractère normatif, soit descriptif. Le tableau ci-dessous illustre ce classement:

Chapitre	Description
2 Introduction	Descriptif
3 Parties prenantes	Normatif
4.1 Vision architecturale 4.4 Les principes de design mentionnés ci-après soutiennent la mise en œuvre des visions et des exigences mentionnées ci-dessus.	Normatif
4.2 Exigences relatives aux ressources & 4.3 Exigences relatives au sujet	Descriptif
5 Architecture de l'information	Normatif
6 Processus	Les désignations et leurs définitions sont normatives. Les activités et remarques sont descriptives.
7 Services administratifs	Les désignations et leurs définitions sont normatives. Les tâches et remarques sont descriptives.
7.6 Attribution des services aux éléments d'information	Normatif
7.7 Compétences pour les services administratifs	Descriptif
8 Concepts de l'Identity Federation	Ce chapitre est descriptif, mais doit cependant aider à établir un classement.
Annexe A – Références & bibliographie	Descriptif
Annexe B – Collaborateurs & vérification	Descriptif
Annexe C – Abréviations	Normatif
Annexe D – Glossaire	Normatif

Tableau 2 Aperçu du caractère normatif des chapitres

3 Parties prenantes

L'Identity et Access Management a quatre parties prenantes essentielles qui occupent différents rôles en fonction de la combinaison et de l'organisation. Les quatre parties prenantes et les éléments fondamentaux de leur collaboration sont présentés dans la Figure 3 et ensuite brièvement détaillés. Les relations entre les parties prenantes indiquent qui est en relation avec qui et qui est à l'origine de la première prise de contact.

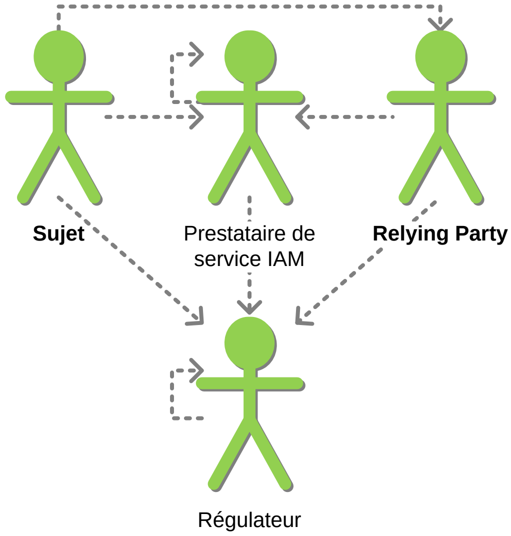

Figure 3 Les parties prenantes et leur collaboration

Relying Party	Le *Relying Party* représente les intérêts de la *ressource*. Il utilise les services administratifs *IAM* et traite les informations des *prestataires de services* pour protéger ses *ressources.* Il a besoin d'informations plus approfondies concernant le *sujet* afin de pouvoir juger et *autoriser* l'accès à une *ressource*.
Prestataire de services IAM	Le *prestataire de services IAM* gère un ou plusieurs services administratifs *IAM*, conformément au chapitre 7.
Regulator	Le *Regulator* définit les conditions générales juridiques, procédurales, organisationnelles, sémantiques et techniques dans le cadre desquelles l'*IAM* peut être développé. Il veille à ce que toutes les autres parties prenantes soient impliquées dans la définition de manière adaptée.
Sujet	Une personne physique, une organisation ou un service qui souhaite avoir accès à une *ressource* d'un *Relying Party*. Un sujet est défini par une *eIdentity*.

Les parties prenantes sont donc responsables de différentes parties du processus *IAM*. Leurs responsabilités sont décrites dans la

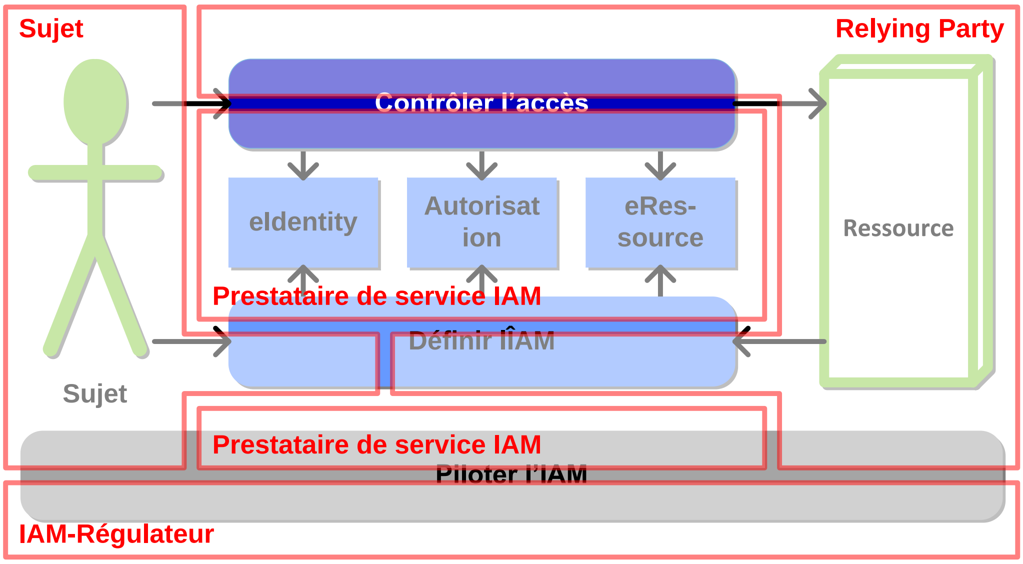

Figure 4. Par conséquent, dans le cadre du recouvrement d'un processus par plusieurs parties prenantes, on déduit que les parties prenantes doivent collaborer pour atteindre les objectifs du processus.

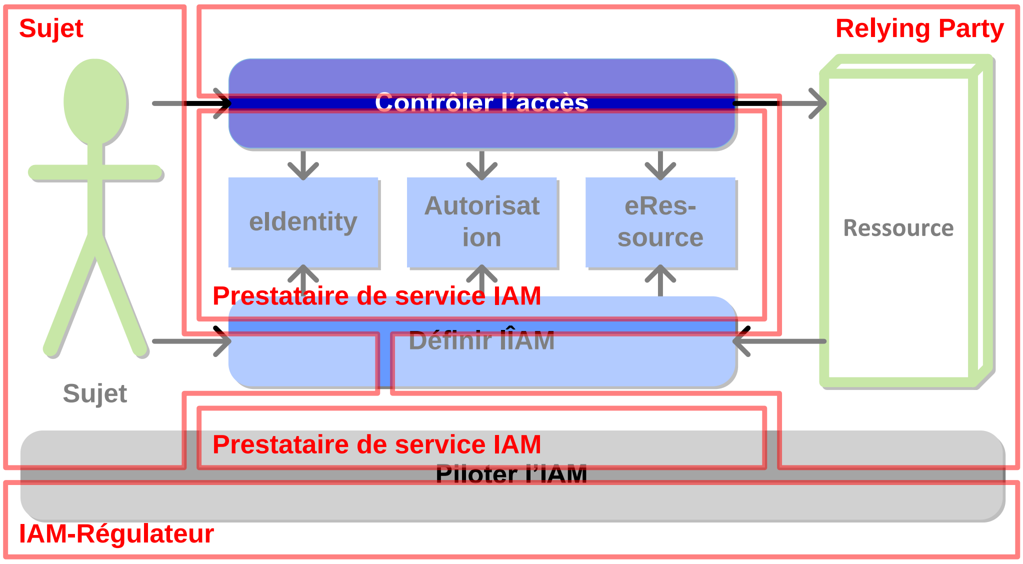

Figure 4 Compétences des parties prenantes

4 Exigences

Les principes et exigences décrits et définis dans ce chapitre doivent être appliqués ou remplis afin de pouvoir instaurer un *IAM* fédéré efficace et efficient.

4.1 Vision architecturale

La vision architecturale définit les principes généraux de l'organisation d'un *IAM* fédéré.

- L'*Identity Management* repose sur une infrastructure fédérée et interopérable à l'échelle internationale. [SOWISCH] Vision-1
    - L'*IAM* peut facilement être intégré à d'autres *IAM* (également à l'échelle internationale). Vision-1.1
    - L'*IAM* peut facilement intégrer des solutions *IAM* existantes Vision-1.2

- Les informations et les données sont fédérées au lieu d'être dupliquées. Vision-2
- Au lieu de maintenir les caractéristiques d'autorisation, ce sont les caractéristiques des personnes qui sont utilisées pour l'*autorisation*. Vision-3

- Les infrastructures *IAM* sont modulables et évolutives. Vision-4
- Les services administratifs travaillent ensemble sur des interfaces standardisées qui utilisent des standards ouverts (p. ex. «Security Assertion Markup Language» (SAML)). Vision-5
- Les processus d'authentification plus ou moins approfondis, nécessaires en fonction des besoins de protection, peuvent être réalisés sur la même infrastructure *IAM*. Vision-6
- La quantité des *Credentials* et *Attributs* doit être aussi faible que possible et doit éventuellement être consolidée. Vision-7
- L'efficacité et l'efficience de l'*IAM* inter-organisationnelle nécessite d'avoir confiance en son partenaire. Vision-8
- Les concepts *fédérés* sont utilisés pour établir des relations de confiance (Trusts) avec d'autres *domaines* et pour l'utilisation de *Credentials* et d'*Attributs* définis ailleurs. Vision-9
- Dans la mesure où le Trust Level le permet, les identités, *Credentials* et *attributs* existants peuvent être repris par d'autres instances (fédération). Vision-10

4.2 Exigences relatives aux ressources

Cette partie décrit les exigences générales relatives aux ressources.

- L'utilisation abusive des *ressources* n'est pas possible. Res-1
- L'*accès* aux *ressources* n'est autorisé qu'aux *sujets* autorisés. Si le *sujet* ne dispose pas des droits nécessaires pour la *ressource* demandée, la demande ne sera pas transmise à l'*eRessource*. Res-2
- L'investissement lié à la gestion des *eRessources* est minimal. Res-3
- L'investissement lié à la gestion des *autorisations* (*règles d'accès* et *droits d'accès*) est minimal. Res-4
- L'investissement pour l'administration des *eIdentities* (*Credentials* et *Attributs*) est minimal. Res-5
- Les confirmations de différentes qualités sont délivrées par les *Claim Assertion Services*. [SOWISCH] Res-6

- Les personnes physiques et les organisations ont un *identifiant* public biunivoque. [SOWISCH] Res-7
- Le respect des prescriptions juridiques, organisationnelles et techniques (notamment la protection des données, ainsi que toutes les normes de sécurité spécifiques à l'organisation) doivent être garanties à tout moment. Res-8
  - La garantie de la traçabilité et la non-répudiation indiquant quel *sujet* a accédé à quelle *ressource* et à quel moment. Res-8.1
  - Le rapport entre l'*eIdentity* et les *Credentials* s'y rapportant doit systématiquement être garanti. Res-8.2
- Le *sujet* est tenu de signaler tout soupçon de l'utilisation abusive de son *eIdentity*. [SOWISCH] Res-9

4.3 Exigences relatives au sujet

Les exigences relatives au sujet sont établies par des personnes physiques, organisations ou services qui souhaitent avoir accès aux informations et aux services des *ressources*.

- Le *sujet* peut avoir accès aux *ressources* dans le monde entier, indépendamment de sa localisation. Sub-1
- Le *sujet* ne doit indiquer son identité que lorsque cela est nécessaire. Sub-2
- Si la *ressource* n'a pas besoin de savoir qui y a accès, un *identifiant* pseudonymisé est transmis. Sub-3
- La quantité *d'attributs* nécessaire à l'*autorisation* du *sujet* est minimale. Sub-4
- Les *attributs* de différents *Attribute Services* sont acceptés. Sub-5
- Le *sujet* n'a besoin que d'un faible nombre d'*eIdentities*. Sub-6
- Le *sujet* peut choisir combien de *Credentials* il souhaite avoir, et de quelle qualité. Sub-7
- Le *sujet* peut choisir, lors de l'*authentification*, quel *Credential* de la qualité minimale requise de l'*authentification il utilise*. Sub-8
- L'approvisionnement d'*eIdentities* et de *Credentials* est simple et peu coûteux. Sub-9
- L'utilisation d'*eIdentities* et de *Credentials* est simple et pratique. Sub-10
- Un autre *sujet* peut agir en tant que représentant d'un *sujet*. Sub-11
- Personne ne peut accéder aux *attributs* d'une *eIdentity*, sauf si le *sujet* en donne explicitement son autorisation ou que le droit est inscrit dans la loi. Sub-12
- Le *sujet* obtient de l'aide pour la prévention et la Recovery d'une utilisation abusive de son *eIdentity*. [SOWISCH] Sub-13
- Les *prestataires de services IAM* font tout ce qui est en leur pouvoir pour empêcher l'utilisation abusive de l'identité d'un *sujet*. [SOWISCH] Sub-14

4.4 Principes généraux de design

Les principes de design mentionnés ci-après soutiennent la mise en œuvre des visions et des exigences mentionnées ci-dessus.

- Pour *l'authentification* et l'*accès*, les *ressources* utilisent des services découplés. Design-1
- L'*authentification* et *l'autorisation* pour l'*accès* sont basées sur les *Credentials* et les *attributs* standardisés. Design-2
- L'*authentification* du *sujet* accédant doit avoir lieu avant l'*autorisation* d'un *accès* à une *ressource* (dans la mesure où cela est techniquement nécessaire). Design-3
- Aucune information n'est transmise à la *ressource* concernant le *sujet* accédant lorsque cela n'est pas techniquement nécessaire. Design-4
- L'*accès* est accordé sur la base des *attributs* indiqués. Design-5

5 Architecture de l'information

Le modèle ci-dessous présente les termes-clés de l'*IAM*, ainsi que leurs relations dans une vue d'ensemble représentée sous forme de diagramme de classes UML. Du fait que les éléments du modèle d'information *IAM* soient utilisés dans de nombreux endroits (pas uniquement dans l'*IAM*), il est capital d'utiliser des termes nuancés, afin que la syntaxe et la sémantique puissent être définies de manière précise et claire pour tous les intéressés. La Figure 5 présente le modèle d'information relative à l'IAM inter-organisations.

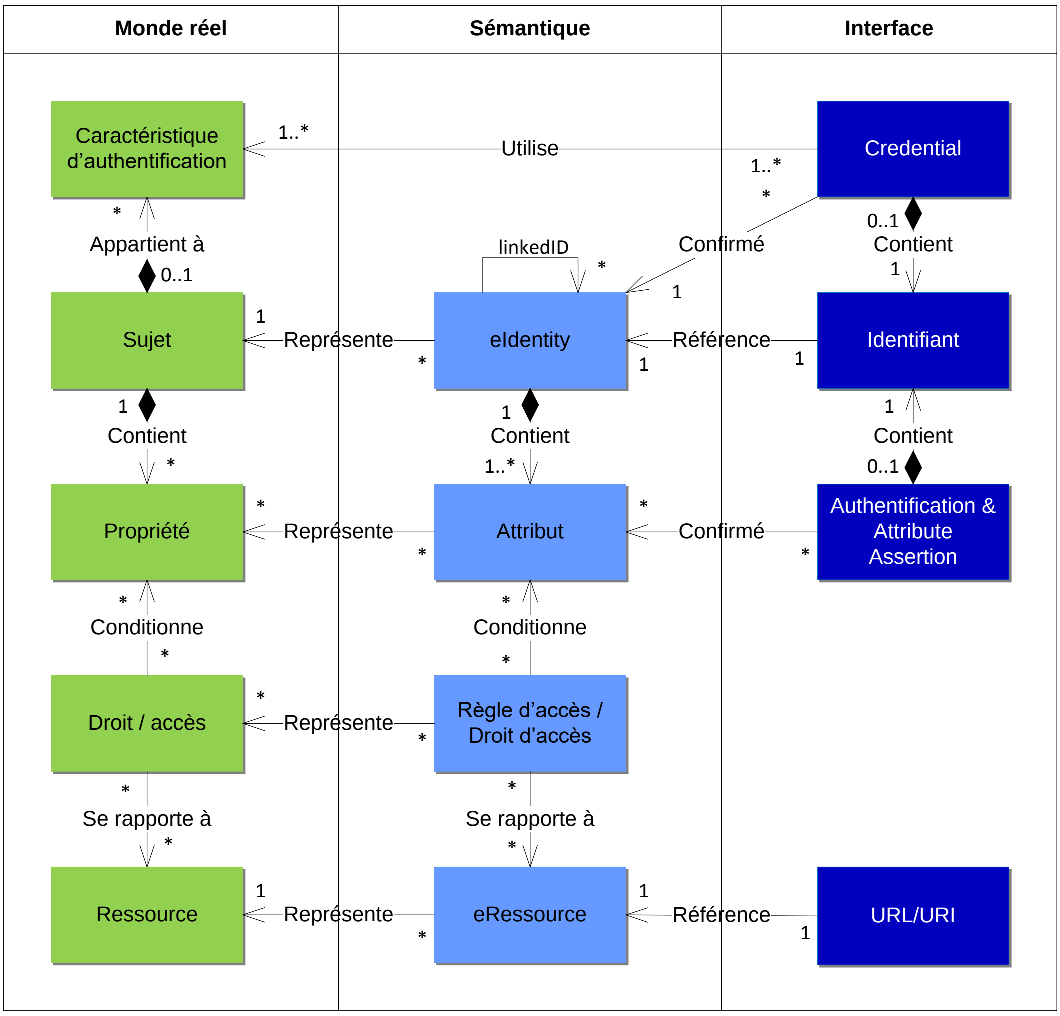

Figure 5 Modèle d'information

Il est courant d'utiliser les mêmes marqueurs entre le domaine spécialisé et les systèmes d'information pour les éléments du monde réel. Puisque les différences entre l'aspect sémantique (les systèmes d'information concernés) et le monde réel sont fondamentales, on utilisera ici différents marqueurs pour les différents éléments. Le modèle d'information de la Figure 5 indique à gauche (en vert) les éléments du monde réel, au centre (en bleu clair) le modèle sémantique (des systèmes d'information), et à droite (en bleu foncé), les objets de l'interface utilisés pour l'échange d'informations entre les différents systèmes d'informations.

Le modèle sémantique au centre ne fait aucun commentaire concernant la répartition de l'information dans les systèmes d'information.

Les objets du monde réel ainsi que leurs caractéristiques et relations dans les systèmes d'information (sémantique) sont représentés dans le temps de définition (voir les processus dans la partie 6.2 et les services administratifs dans la partie 7.2).

Les objets des interfaces sont établis sur la base du contenu du modèle sémantique et échangés entre les systèmes d'information pendant le temps d'exécution (voir les processus de la partie 6.1 et les services administratifs de la partie 7.3).

Le tableau suivant définit les éléments figurant dans la Figure 5.

Monde réel	
Ressource	Service ou données auxquels un *sujet* peut accéder lorsqu'il s'est *authentifié* et que l'accès a été *autorisé*, sur la base des *attributs* requis. Ceci inclut les ressources physiques telles que bâtiments et installations, dont l'utilisation est gérée par des systèmes IT.
Droit/accès	Les *droits* ou *accès* dont le *sujet* a besoin pour accéder aux *ressources*. Celles-ci peuvent par exemple être stipulées dans la loi ou un contrat.
Propriétés	Les *propriétés* sont des caractéristiques, critères ou actions d'un *sujet*.
Sujet	Une personne physique, une organisation ou un service qui a accès ou souhaite avoir accès à une *ressource.* Un *sujet* est défini par des *eIdenties*.
Critère d'authentification	Le *critère d'authentification* peut s'appuyer sur une connaissance (mot de passe, PIN), une possession (certificat, clé privée) ou sur une propriété (critère biométrique, p. ex. voix, lecture de l'iris, empreinte digitale), ou sur une combinaison de ces critères.
Sémantique	
eRessource	Représentation numérique d'une *ressource*. Une *eRessource* a un *Identifiant* (nom unique, souvent une URL/URI), pouvant être attribuée à une *ressource* de manière explicite dans le cadre d'un *espace de noms*.
Règles d'accès / droit d'accès	Les responsables des *ressources* définissent les *règles d'accès* et les *droits d'accès* à leurs *eRessources*. Les *règles d'accès* et les *droits d'accès* définissent les conditions auxquelles le *sujet* a le droit d'accéder à une *ressource* (*autorisation grossière*) et peut l'utiliser (*autorisation précise*), par exemple lorsque *l'authentification* a été effectuée et que les *attributs* définis ont été validés.
Attribut	La représentation sémantique d'une *propriété* attribuée à un *sujet*, qui décrit le *sujet* de manière plus approfondie. L'*identifiant* et les *Credentials* sont également des *attributs*.

eIdentity	Représentation d'un *sujet*. Une *eIdentity* (identité numérique) comprend un *identifiant* (nom explicite), généralement accompagné d'une quantité d'*attributs* supplémentaires pouvant être attribués à un *sujet* de manière explicite dans le cadre d'un *espace de noms* (et donc d'un *domaine*). Un *sujet* peut posséder plusieurs *eIdentities*.[1]
linkedID	Dans le contexte inter-organisations, *linkedID* permet de mettre en relation les eIdentities de différents domaines. Les eIdentities peuvent être associées à n'importe quel graphique avec *linkedID*. La mise en œuvre concrète d'eCH-0107 peut restreindre encore la forme (ex. arborescence au lieu du graphique) et règle l'interprétation (sémantique) du graphique en fonction de leurs compétences (cf. 7.3.3 *Broker Service*).
Interface	
Authentication & Attribut Assertion	La confirmation de *l'authentification* d'un *sujet* (*Authentication Assertion*), ou la confirmation d'un *attribut* (*Attribute Assertion*). Contient l'*identifiant*.
Identifiant	Une chaîne de caractères qui définit explicitement une *eIdentity* ou une *eRessource*, dans le cadre d'un *espace de noms*.[2]
Credential	Justificatif pour la confirmation de *l'eIdentity* d'un *sujet*. On utilise un ID utilisateur (*identifiant*), avec un (ou plusieurs) *critère(s) d'authentification* dans le contexte *IAM* pour confirmer *l'eIdentity*.

Tableau 3 Description des éléments du modèle d'information

[1] Cette déclaration (dans le cadre de eCH-0107) vaut pour les systèmes inter-organisations. Il est toutefois recommandé de n'imposer aucune restriction même en interne dans l'organisation concernant l'unicité.

[2] L'*identifiant* d'une ressource est souvent une URL/URI.

6 Processus

La Figure 6 représente une vue d'ensemble des processus administratifs. Elle sert à illustrer les activités top down, nécessaires pour une bonne coopération entre les différentes parties prenantes. La Figure 6 reprend les processus de la Figure 1 et complète leurs sous-processus.

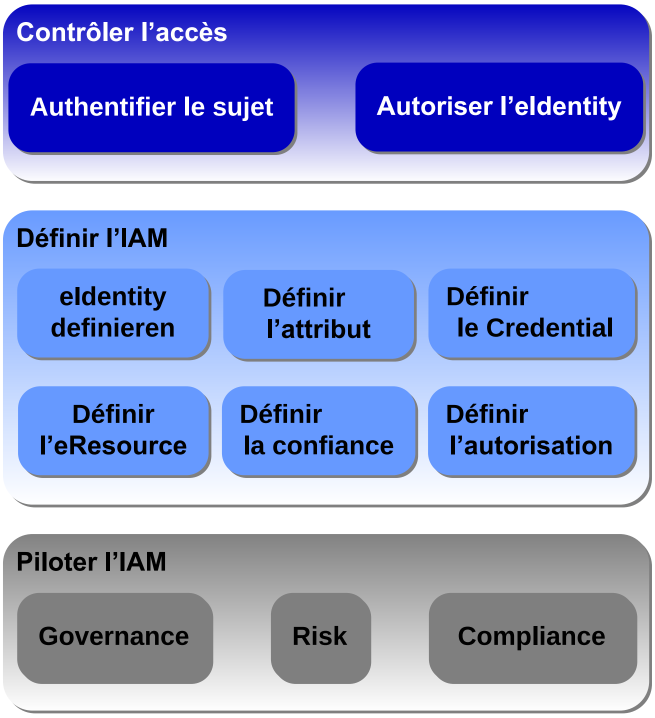

Figure 6 Diagramme de processus IAM

Les différentes parties prenantes participent à ces processus, conformément au chapitre 3. Les paragraphes suivants décrivent les processus administratifs, ainsi que leurs sous-processus.

6.1 Contrôler l'accès

Le *contrôle de l'accès* comprend les processus du temps d'exécution. L'objectif du *contrôle de l'accès* est l'observation contrôlée et garantie des règles d'*accès* d'un *sujet* à une *ressource*. Lors de l'*accès* du *sujet*, celui-ci est *authentifié* puis, dans la mesure où cela est *autorisé*, l'*accès* aux *ressources* est débloqué. Dans l'intérêt d'une mise à disposition fiable d'informations, le *contrôle de l'accès* garantit que seuls les sujets ayant le droit d'accéder aux *ressources* aient effectivement *accès* à celles-ci. Toute autre personne se verra refuser l'*accès* aux fonctionnalités de la *ressource* ou même à la *ressource* elle-même.

En cas d'erreur, le déroulement du processus est interrompu lors des étapes de contrôle correspondantes et tous les *accès* sont enregistrés (même ceux qui sont sans erreurs).

Les services administratifs, qui soutiennent les processus pendant la durée d'exploitation sont décrits dans la partie 7.3.

6.1.1 Authentifier le sujet

Authentifier le sujet	Processus de contrôle de l'*eIdentity* supposée d'un *sujet.*

Activités:

- Le *sujet* est authentifié à l'aide des *Credentials*.

6.1.2 Autoriser l'eIdentity

Autorisé l'eIdentity	Contrôler *l'autorisation* d'*accès* d'une *eIdentity authentifiée* à une *eRessource* et délivrer l'*accès* à une *ressource* pendant le temps d'exécution. Il convient de distinguer *l'autorisation grossière* de *l'autorisation précise*.

Activités:

- La condition préalable à toute *autorisation* est *l'authentification* réussie d'un *sujet*.
- Les *règles d'accès* et les *droits d'accès* sont définis pour l'*accès* à l'*eRessource*, et les *attributs* nécessaires à l'*eIdentity* en sont déduits.
- Les *attributs* sont confirmés (habituellement centrés sur l'utilisateur).
- L*'entrée* et l'*accès* sont autorisés.
- L'*accès* est réalisé.

6.2 Définir l'IAM

Pendant le temps de définition, toutes les conditions nécessaires sont réunies pour pouvoir déterminer si un *sujet* peut avoir *accès* à une *ressource* pendant le temps d'exécution. Le temps de définition doit se dérouler avant la première utilisation de la *ressource* par le *sujet*. La mise en œuvre de *définir l'IAM* impacte directement sur la qualité du *contrôle de l'accès*.

Les services administratifs qui soutiennent les processus pendant la durée de définition, sont décrits de manière plus détaillée dans la partie 7.2.

6.2.1 Définir l'eIdentity

Définir l'eIdentity	Regroupe les processus d'enregistrement, de maintien et de suppression des *eIdentities*

Activités:

- Identifier le *sujet* et enregistrer l'*eIdentity* correspondante.
- Relier les *eIdentities* entre-elles.
- Supprimer l'*eIdentity*.

Remarques:

L'*eIdentity* constitue l'élément central de tout environnement *IAM*. Un *sujet* enregistré possède systématiquement au moins une *eIdentity* dans un *espace de noms*.

6.2.2 Définir l'attribut

Définir l'attribut	Définition, maintien et utilisation d'*attributs*.

Activités:

- Envoyer la demande d'attribution d'un *attribut* à un organisme agréé.
- Après *l'authentification* d'un *sujet*, attribuer les *attributs* correspondants.
- Enregistrer les *attributs* fournis/existants pour l'*eIdentity*.
- Supprimer l'*attribut*.

Remarques:

Un *attribut* représente une *propriété* attribuée à un *sujet* qui décrit le *sujet* de manière plus détaillée. Le processus d'établissement ou de contrôle de ces *propriétés* doit être documenté, conformément à la qualité demandée.

6.2.3 Définir Credential

Définir l'eIdentity	Regroupe les processus d'enregistrement, de maintien et de suppression des *eIdentities*

Activités:

- Etablir, relever et attribuer les *critères d'authentification* (p. ex. le certificat d'authentification des *Credentials*).
- Sauvegarde des éléments publics des *critères d'authentification* (p. ex. clé publique) pour l'*eIdentity* dans le Directory de l'*Identity Provider.*
- Délivrance du *critère d'authentification* (éventuellement plusieurs) au *sujet*.
- Révocation des *Credentials*.

6.2.4 Définir l'eRessource

Définir l'eRessource	Définition, maintien et utilisation des *eRessources*.

Activités:

- Identifier la *ressource* et enregistrer l'*eRessource correspondante* (avec *identifiant*)
- Supprimer l'*eRessource*

Remarques:

- Une *ressource* enregistrée a toujours au minimum une *eRessource* dans un *domaine*.

6.2.5 Définir la confiance

Définir la confiance	Etablir, maintenir et supprimer les *prestataires de services IAM* dignes de confiance

Activités:

- Le maintien des *métadonnées* des *prestataires de services IAM*.
- La définition et l'annulation des relations de confiance (*Trust*) entre les parties prenantes qui effectuent les tâches dans le système fédéré, comme par exemple *Authentication*, *Attribute Assertion* ou les *services d'accès*.

6.2.6 Définir l'autorisation

Définir l'autorisation	Attribution et suppression des *règles d'accès* pour l'*autorisation grossière* et des *droits d'accès* pour l'*autorisation précise*. Définition des relations de confiance.

Activités:

- La définition des *règles d'accès* et des *droits d'accès* au moyen des *attributs* des *eIdentities* disponibles (conformément aux métadonnées et aux relations de confiance de *Définir confiance*).
- L'attribution des *règles d'accès* et des *droits d'accès* à une ou plusieurs *eRessources*.
- Suppression des *règles d'accès/droits d'accès*

6.3 Contrôler l'IAM

Les processus Governance, Risk et Compliance (GRC) font partie du processus administratif *Contrôler l'IAM*, qui sert à contrôler l'*IAM* dans l'E-Government.

Ces processus définissent le déroulement de la définition des prescriptions requises et des conditions générales d'exploitation de l'environnement *IAM*, telles que la définition de l'offre, la définition des règles et des déroulements, la définition de la révision, etc.

6.3.1 Governance

Governance définit l'infrastructure *IAM*, ainsi que l'organisation *IAM*. Governance regroupe:

- Etablissement de l'*IAM* policy: l'*IAM policy* (avec stratégie *IAM*, architecture *IAM* et processus de commande *IAM*) définit les contraintes et la portée de la solution *IAM* recherchée. La définition de la traçabilité de l'ensemble du déroulement du processus (p. ex. le classement des documents pertinents) et son audit sont particulièrement importants.
- Etablissement de l'organisation (parties prenantes), ainsi que leur relation les uns par rapport aux autres (collaboration). L'organisation *IAM* définit de quelle manière les parties prenantes sont impliquées les unes par rapport aux autres: qui prend les décisions, comment les responsabilités sont régies, comment les *ressources* sont utilisées, etc. Les rôles sont attribués aux parties prenantes appropriées en question.

- Identification/établissement de la collaboration de plusieurs *domaines*. Dans l'environnement de l'E-Government, l'*IAM* est généralement effectuée par plusieurs *domaines*. L'organisation et le déroulement entre les *domaines* doivent être clairement organisés.
- Définition des *rôles* avec des tâches, compétences et responsabilités. Les processus sont exécutés par les parties prenantes. Ces dernières ont un (ou éventuellement plusieurs) *rôles*.

6.3.2 Risk

Le risk définit le déroulement de la gestion du risque (évaluation et adressage des risques) pour les processus *IAM*. Le risk comprend:

- L'analyse des besoins de protection. L'analyse des besoins de protection garantit des exigences de sécurité adaptées (autant de sécurité que nécessaire, par opposition à autant de sécurité que possible).
- Exécution et application d'une analyse des risques.
- Réalisation d'un concept de protection des informations et des données.
- Amélioration continue du concept de sécurité défini dans ISO 27001. En raison de la situation actuelle, des mesures périodiques sont planifiées, appliquées, contrôlées et optimisées. Ce processus d'amélioration est un procédé éprouvé et efficient, et constitue aujourd'hui un élément central de Best Practice.
- [FACULTATIF] Renforcement de la gestion des risques par un système de gestion de la sécurité de l'information (ISMS), selon ISO 27001.
- [FACULTATIF] Renforcement de la gestion des risques dans un outil, tel que COBIT par exemple.

6.3.3 Compliance

La Compliance assure l'observation des règlementations juridiques, internes à l'entreprise et contractuelles. La Compliance est obtenue avec:

- L'élaboration et l'actualisation des prescriptions pertinentes: l'identification des directives/règlementations en vigueur. Les modifications sont également reprises dans les prescriptions, et les éventuelles mesures en résultant sont identifiées.
- Reporting de toutes les activités pertinentes.
- Auditer et contrôler l'application des prescriptions. Conformément aux exigences de qualité, le paysage *IAM* est contrôlé au moyen d'audits réguliers. L'objectif des audits est de garantir l'application des prescriptions.

7 Services administratifs

L'ensemble des services *IAM* proposés par les différentes parties prenantes (voir chapitre 7) sont décrits ci-dessous. Il s'agit de services administratifs et non de composants de services techniques, c.-à-d. que lors de la mise en œuvre, un ou plusieurs services administratifs peuvent être implémentés par un composant de service technique, ou qu'un service administratif peut être distribué par plusieurs composants de service technique.

Les modèles de ce chapitre définissent aussi bien le temps d'exécution (lorsqu'un *sujet* tente d'accéder à une *ressource*) que le temps de définition pendant lequel les différentes (méta)données sont saisies et maintenues. Les services administratifs qui soutiennent le processus *Contrôler l'IAM* (cf. partie 6.3) ne sont pas présentés dans cette norme.

Les services du temps de définition (en bleu clair) et les services du temps d'exécution (en bleu foncé) sont visuellement séparés des objets du monde réel (en vert) dans les figures.

La *gestion de l'identité et des autorisations* des services IAM administratifs présentés ici ne fait pas partie de cette norme. En principe, toute utilisation d'un service peut être différenciée par rapport aux agents *sujet* et *ressource*, et la présente norme peut être appliquée de manière récursive. Il convient de déterminer au cas par cas si cela est judicieux dans la pratique.

7.1 Objets du monde réel

Les objets du monde réel (agents) et leurs tâches sont décrits de manière plus approfondie ci-dessous. Ils sont systématiquement affichés en vert clair dans les modèles.

7.1.1 Sujet

Sujet	Une personne physique, une organisation ou un service, qui a accès ou souhaite avoir accès à une *ressource*. Un *sujet* est défini par des *eIdentities*.

Tâches (pour le temps d'exécution):

- *S'authentifie*.
- Débloque l'envoi des *attributs*.
- Accède aux *ressources*.

7.1.2 Ressource

Ressource	Service ou données auxquelles un *sujet* peut avoir *accès* lorsqu'il s'est *authentifié* et que cela a été *autorisé* sur la base des *attributs* nécessaires.

Tâches (pour le temps d'exécution):

- Met ses fonctionnalités à la disposition du *sujet* (les informations et services correspondant à l'*identifiant*)

7.2 Services pour le temps de définition

La Figure 7 représente les services du temps de définition (dans les modèles en bleu clair) devant être utilisés pour la gestion des différents objets. Le premier groupe se réfère au *sujet*. Le deuxième groupe définit les objets en relation avec la *ressource*.

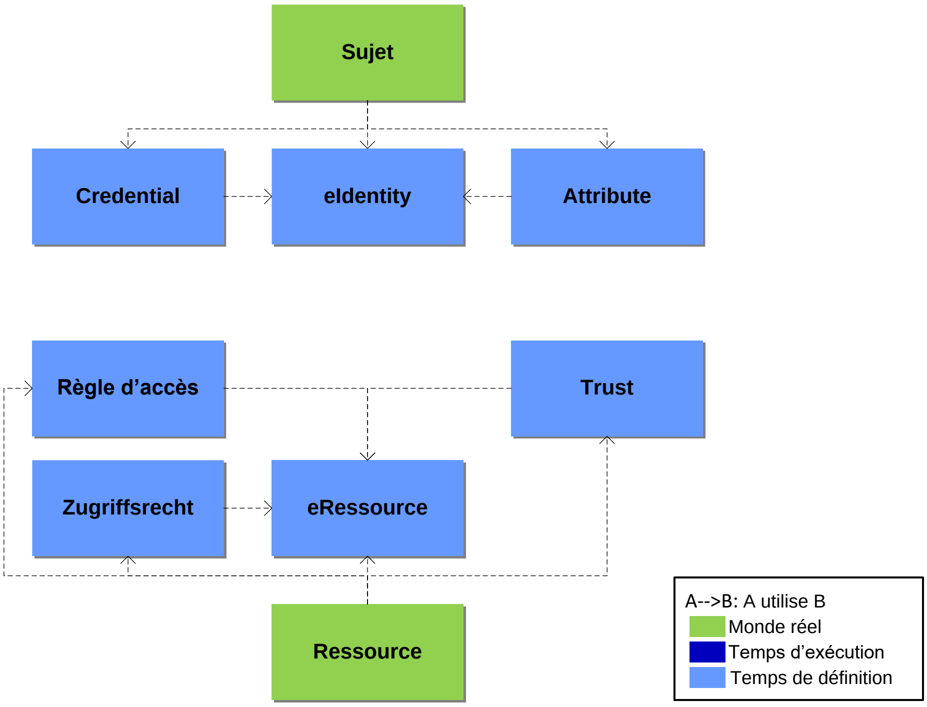

Figure 7 Services administratifs – temps de définition

7.2.1 eIdentity Service

eIdentity Service	L'*eIdentity Service* délivre des *eIdentities* au *sujet* et les gère.

Tâches:

- Permet l'enregistrement de *sujets*.
- Met à disposition les fonctions pour la délivrance, le maintien et la gestion des *eIdentities*.
- Assure l'*identification* physique du *sujet*, à l'aide des règles définies, relatives à la qualité recherchée (chaîne de confiance entre *l'eIdentity* et le *sujet*).
- Connaît d'autres *eIdentity Services* et permet de maintenir le *linkedID* avec les autres *eIdentities* d'un *sujet*.
- Assure la qualité et l'actualité de l'*eIdentity* de façon appropriée.
- Limite la durée de vie des *eIdentities* et aide les *sujets* à renouveler leurs *eIdentities*.
- Peut annuler des *eIdentities*.
- Garantit l'*accès* aux *eIdentities* des *Credentials* et des *Attribute* Services électroniques dignes de confiance.

- Garantit l'*accès* électronique aux informations d'identité des *Authentication Services* dignes de confiance.

7.2.2 Credential Service

Credential Service	Le *Credential Service* délivre et gère les *Credentials*. Il existe différents types de *Credentials*. Un Credential se réfère à une *eIdentity* et est délivré pour un *sujet* précis.

Tâches:

- Enregistre les *Credentials* dans le cadre d'une utilisation éventuelle des *critères d'authentification* du *sujet*.
- Met les fonctions de délivrance et de gestion des *Credentials* à disposition.
- Utilise une gestion des clés pour les clés cryptographiques (ne fait pas partie des services administratifs IAM).
- Permet le contrôle de la validité des *Credentials* gérés et de l'appartenance à une *eIdentity* ou au *sujet* correspondant.
- Limite la durée de vie des *Credentials* délivrés et soutient les *sujets* dans le renouvellement de leurs *Credentials*.
- Peut annuler les *Credentials*.

7.2.3 Attribute Service

Attribute Service	L'*Attribute Service* maintient un ou plusieurs *attributs* actuels pour des *sujets* définis.

Tâches:

- Met des fonctions à disposition pour le maintien et la gestion des informations nécessaires pour pouvoir déterminer si un *sujet* remplit une *caractéristique* définie ou non (p. ex. «Hans Meier est le géomètre du canton de Berne»).
- Représente les *caractéristiques* en tant qu'*attributs* et relie les *attributs* à l'*eIdentity* du sujet.
- Permet les mutations des *attributs*, ainsi que leur annulation.
- Assure la qualité et l'actualité des *attributs*, de manière adéquate (peut par exemple limiter leur durée de vie).
- Doit éventuellement également être en mesure d'interroger les informations d'identité de l'*eIdentity Service* (p. ex. la vérification de l'*eIdentity*).

Remarques:

- Les *attributs* définissent systématiquement l'*eIdentity* correspondante, mais peuvent également être indiqués par le contexte commun des *sujets* (p. ex. employeur commun). Le maintien de ces *attributs* est indépendant du Lifecycle de l'*eIdentity*. Seule la relation de *l'eIdentity* avec ces *attributs* dépend du Lifecycle de *l'eIdentity*.

7.2.4 Trust Service

Trust Service	Le *Trust* Service maintient les *prestataires de services IAM* acceptés et dignes de confiance.

Tâches:

- Enregistre, maintient et gère les relations de confiance (cycle de vie inclus) des ressources (*Relying Party*) par rapport aux *prestataires de services IAM* et entre les *prestataires de services* IAM.
- Effectue des définitions de contrat.
- Définit le Trust-Anchor concernant le choix du Certification Service Provider (CSP).
- Enregistre les services du *prestataire de services IAM* et leur qualité (p. ex. les sources de données autoritatives).
- Définit les métadonnées et la sémantique des *attributs* des *eIdentities* et des *eRessources* pour le *Broker Service,* ainsi que les autres services administratifs dépendant des métadonnées.
- Connaît les autres *Trust Services* et peut utiliser leurs informations

7.2.5 eRessource Service

eRessource Service	L'eRessource Service délivre des *eRessources* aux *ressources* et les gère.

Tâches:

- Met des fonctions à disposition pour la définition et la gestion des *eRessources*.
- Une *ressource* peut être représentée par plusieurs *eRessources.*
- Attribue à chaque *eRessource* précisément un *identifiant* unique.

7.2.6 Service règle d'*accès*

Service règle d'accès	Le *Service règle d'accès* gère les *règles d'accès* à une *eRessource*. Les règles sont définies sur la base de *l'authentification* ou des *attributs*.

Tâches:

- Met des fonctions à disposition pour la gestion des *règles d'accès*, qui régissent l'*accès* aux *eRessources* (*autorisation grossière*). Les *règles d'accès* contiennent des instructions relatives à *l'authentification* et aux *attributs* (qualité incluse), dont un *sujet* doit s'acquitter, conformément au besoin de protection.

7.2.7 Service droit d'accès

Service droit d'accès	Le *Service droit d'accès* gère les droits d'utilisation d'une *eRessource*. Les droits sont définis sur la base de *l'authentification*, des *attributs* ou des modèles (groupes, rôles, autorisations individuelles).

Tâches:

- Met des fonctions à disposition pour la gestion des informations: les conditions (autorisation et/ou attributs ou informations provenant de modèles personnels) qu'un *sujet* doit remplir et leur qualité (conformément au besoin de protection), pour pouvoir accéder aux fonctions de la *ressource* (*autorisation précise*).

7.3 Services pour le temps d'exécution

Les services administratifs de la durée d'exploitation (en bleu foncé dans les modèles) sont présentés dans la Figure 8. La figure comprend tous les services utilisés pendant le temps d'exécution pour le développement des processus *Authentifier le sujet* et *Autoriser l'eIdentity*.

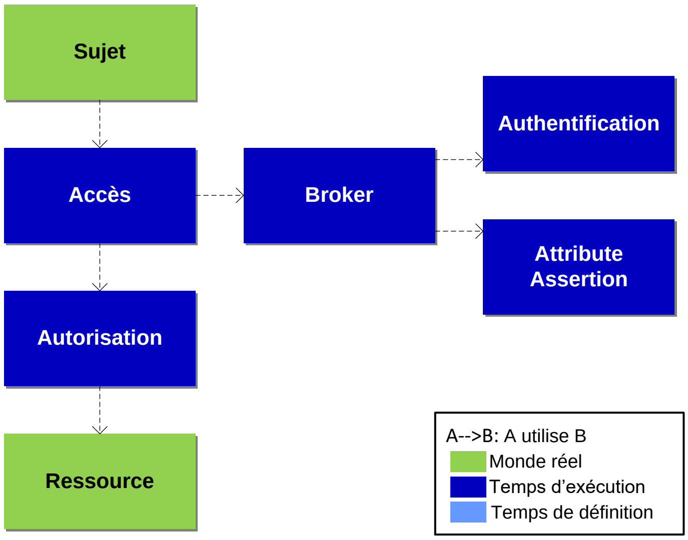

Figure 8 Services administratifs – Temps d'exécution

7.3.1 Authentication Service

Authentication Service	À l'aide des *Credentials*, l'*Authentication Service* contrôle si celui qui accède (*sujet*) est celui qu'il prétend être.

Interface:

In: *Identifiant, critères d'authentification*

Out: *Confirmation de l'authentification* (indique si le contrôle du *sujet* s'est révélé positif ou non)

Tâches:

- Contrôle si les *caractéristiques d'authentification* livrées appartiennent aux *Credentials* de l'*eIdentity* de l'*identifiant* indiqué.
- En cas d'acceptation, confirme l'authenticité du *sujet* appelé via une *confirmation d'authentification* d'une qualité adéquate.
- Demande l'accord du *sujet* pour transmettre la *confirmation d'authentification* au service appelé (accord; s'effectue éventuellement avec l'accord de transmission des *confirmations d'attributs)*.

7.3.2 Attribute Assertion Service

Attribute Assertion Service	Une *entité* qui délivre des *Attribute Assertions* à partir d'une interface définie.

Interface:

In: Attribute Request, *identifiant*

Out: *Confirmation d'attribut* (indique si le contrôle de la relation entre un *attribut* et le *sujet* s'est révélé positif ou non).

Tâches:

- Génère des valeurs d'*attributs* calculées et déduites à partir des *attributs* (p. ex. over18).
- Confirme électroniquement si un *attribut* précis est attribué à un *sujet* ou non, avec la qualité adéquate.
- Demande l'accord du *sujet*, transmet les *confirmations des attributs* au service appelant (accord).

7.3.3 Broker Service

Broker Service	Ce service est l'intermédiaire entre le *sujet*, les *ressources* et les services de la durée d'exécution.

Interface:

In: *Identifiant*, [*Credentials*], type et qualité de *l'authentification*, type et qualité des *attributs*

Out: *Confirmations d'authentification, confirmations d'attributs*

Tâches:

- *Trusted Third Party*, qui transmet des services et métadonnées (Discovery)
- Contacte les *Authentication Services* dignes de confiance, conformément au Trust, en vue de *l'authentification* du *sujet*.
- [FACULTATIF] Contacte à partir de l'eIdentity référencée par l'*Identifiant* de manière récurrente le long des relations *linkedID* d'autres *Authentication Services* pour l'*Authentification* du *sujet*, dignes de confiance, conformément au *Trust*.
- [FACULTATIF] Contacte les *Attribut*e Assertion Services dignes de confiance, conformément au *Trust*, et exige une confirmation des *attributs* souhaités dans la qualité souhaitée.
- [FACULTATIF] Contacte à partir de l'eIdentity référencée par l'*Identifiant* de manière récurrente le long des relations *linkedID* d'autres *Attribute Assertion* Services dignes de confiance, conformément au *Trust* et demande une confirmation des attributs souhaités dans la qualité souhaitée.
- [FACULTATIF] Combine les *Authentication* et *Attribut*e Assertions souhaités, ce qui permet différents niveaux de configuration, d'un simple intermédiaire (proxy) à un service *broker* complexe.
- [FACULTATIF] Peut assumer la responsabilité du *Attribute Assertion Service* de demander l'accord au *sujet* et de transmettre les *Authentication & Attribute Assertions* au service appelant (accord).
- Sélection des partenaires d'authentification (*Authentication Services*) et d'*attribut* (*Attribut*e Assertion Services) nécessaires dans le Metadirectory.
- Connaît d'autres Broker Services et les utilise en adéquation avec les relations de confiance définies dans Trust.

7.3.4 Service accès

Service accès	Le service contrôle le respect des *règles d'accès* et autorise l'*accès* à un *sujet*, lorsque les règles correspondantes sont respectées.

Interface:

In: *Sujet (identifiant, Credential), identifiant d'une ressource*

Out: *Confirmations d'authentifications, confirmations d'attributs*

Tâches:

- Appelle un *Broker* Service et demande une *confirmation d'authentification* et une *confirmation d'attribut,* conformément à la *règle d'accès* pour l'*eRessource*.
- Autorise l'*accès* à la *ressource* lorsque *l'authentification* demandée est réussie et que les *attributs* demandés ont été fournis dans la qualité souhaitée. Cette fonctionnalité est également définie en tant qu'*autorisation grossière*.

- Transmet les *Authentication Assertions* et les *Attribute Assertions* à l'*Autorisation Service*.
- Informe le *sujet* à propos des informations de sécurité nécessaires (p. ex. les *attributs* nécessaires et le niveau de qualité demandé) en termes d'*accès*.
- FACULTATIF] Génère et gère des informations d'*accès*, lorsque demandé. Celles-ci contiennent toutes les données nécessaires à une traçabilité exhaustive.
- [FACULTATIF] Propose des fonctions d'audit et de monitoring vérifiées et vérifiables, pour une traçabilité exhaustive.

7.3.5 Autorisation Service

Autorisation Service	Le service contrôle pour la durée d'exécution le respect des droits pour l'utilisation de l'*eRessource* et autorise l'utilisation de la *ressource* au *sujet*, lorsqu'il possède les droits correspondants.

Interface:

In: *Confirmations d'authentifications, confirmations d'attributs, identifiant d'une eRessource*

Out: Security Token (avec toutes les informations pertinentes pour l'*accès* à la *ressource*, notamment les confirmations d'attributs)

Tâches:

- Contrôle si les confirmations transmises (*Assertions*), ainsi que leur qualité exigée correspondent aux *droits d'accès* et permet, le cas échéant, l'utilisation des fonctions correspondantes de la *ressource* (*autorisation précise*).
- Génère un Security Token pour le *sujet* autorisé, avec les *attributs* pertinents et confirmés par le contexte d'*accès*.
- Limite la durée de vie du Security Token.
- [FACULTATIF] Génère et gère, si nécessaire, les informations d'*accès*. Ces informations contiennent toutes les données nécessaires pour une traçabilité exhaustive.
- [FACULTATIF] Propose des fonctions d'audit et de surveillance légalement vérifiées et vérifiables qui permettent une traçabilité exhaustive.
- [FACULTATIF] Travaille de concert avec la gestion des licences, par exemple pour refuser l'*accès* lorsque le nombre maximal d'utilisateurs simultanés a été atteint.

7.4 Modèle global

Tous les services administratifs *IAM* sont présentés simultanément dans la Figure 9. On s'aperçoit que les services de durée d'exécution accèdent aux données des services du temps de définition pour remplir leurs fonctionnalités.

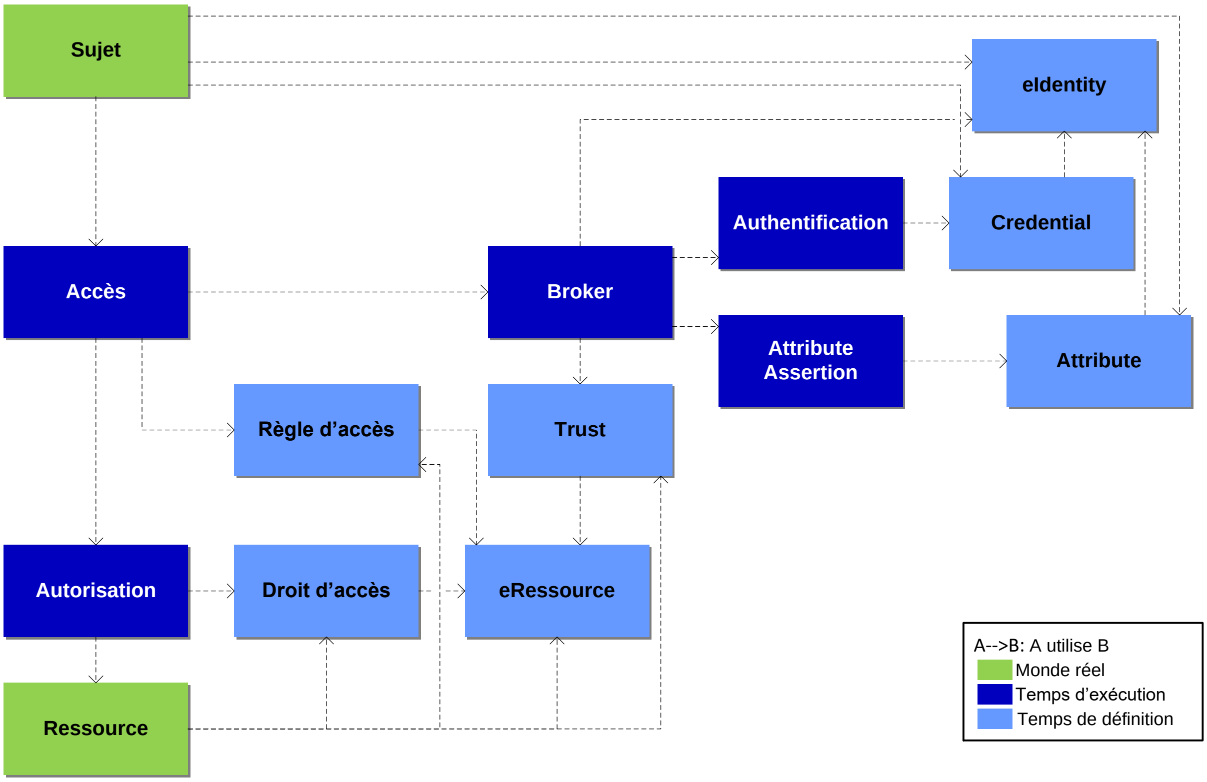

Figure 9 Services administratifs – vue d'ensemble

7.5 Support de processus par les services administratifs

Cette partie présente comment les services travaillent ensemble pendant la durée d'exécution. La collaboration des services pour réaliser les processus de définition est simple et directement abordée par les services. Ces processus ne sont donc pas présentés ici.

7.5.1 Authentifier le sujet

La Figure 10 indique les applications des services administratifs, dans le cadre du processus *1.1. Authentifier le sujet*.

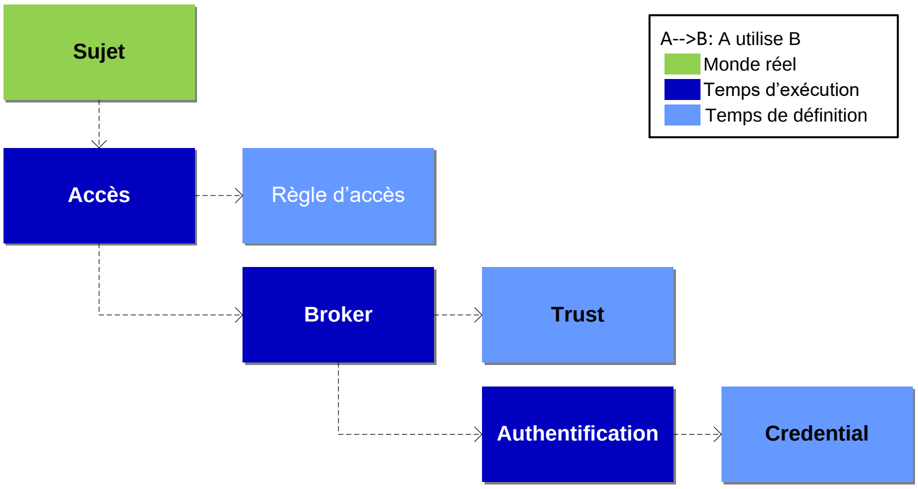

Figure 10 Support de processus *Authentifier le sujet*

Authentifier le sujet suit le déroulement suivant:

- Le *sujet* souhaite accéder à la *ressource* en indiquant l'*identifiant* d'une *ressource*.
- Le service *accès* contrôle les *règles d'accès* pour l'*eRessource* référencée par l'identifiant et exige du *Broker Service* qu'il authentifie le *sujet*, conformément aux exigences.
- Le *Broker Service* contrôle quels *Authentication Services* satisfont aux exigences du *service accès*, conformément au *Trust Service*. Il propose le choix correspondant au *sujet*.
- Le *sujet* s'authentifie auprès d'un de ces *Authentication Services*, qui contrôle le *Credential* du *sujet*.

7.5.2 Autoriser l'eIdentity

La Figure 11 indique les applications des services administratifs dans le cadre du processus *Autoriser l'eIdentity.*

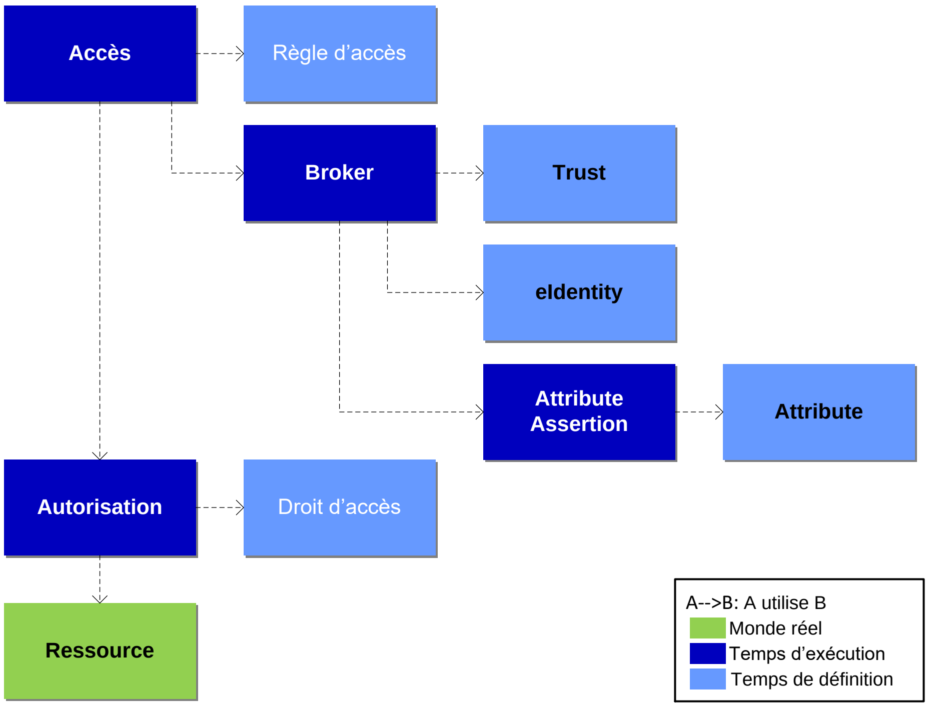

Figure 11 Support de processus *Autoriser l'eIdentity*

Autoriser l'eIdentity suit le déroulement suivant:

- La condition préalable à une *autorisation* est l'*authentification* réussie du *sujet* (cf. partie 7.5.1).
- Le service *accès* contrôle les règles d'accès pour cette eRessource et demande au Broker qu'il confirme les attributs de l'*eIdentity*, conformément aux exigences.
- Le *Broker* Service contrôle quels *Attribute Assertion Services* satisfont aux exigences du Service *accès*, conformément au *Trust Service*. Ce choix d'*Attribute Assertion Services* est alors réduit à ceux qui conduisent aux informations de l'*eIdentity Service*, conformément aux *eIdentities* (linkedID) reliées.
- Le *Broker Service* demande à l'*Attribute Assertion Service* correspondant la confirmation des *attributs* correspondants.
- L'*Autorisation Service* contrôle le droit d'*accès* sur la base des Authentication & *Attribute* Assertions.
- L'*Autorisation Service* accorde l'*accès* à la *ressource*.

Remarque: dans les parties 7.5.1 et 7.5.2 respectivement, l'*accès* s'adresse une fois au Broker. Ces demandes peuvent également être combinées en une seule demande.

7.6 Attribution des services aux éléments d'information

Le tableau suivant présente la relation entre les services d'administration et les éléments de l'architecture d'information (sémantique et interface). Les services du temps de définition traitent (B) les objets et leurs relations réciproques. Les services du temps d'exécution lisent (L) les objets et leurs relations réciproques. Certains services n'utilisent cependant que les métadonnées (M) d'autres services.

		Elément d'information									
		eIdentity[3]	Attribut[4]	Règle d'accès	Droit d'accès	eRessource	Credential	Identifiant d'une eIdentity	Authentication Statem.	Attribute Statement	Identifiant d'une ressource
Services administratifs	eIdentity	B	B[5]					B			
	Credential	L	B[6]				B	L			
	Attribut	L	B					L			
	Trust	M	M			M					
	eRessource					B					B
	Règle d'accès	M	M	B		L					
	Droit d'accès	M	M	L	B	L					
	Authentication	L					L	L	B		
	Attribut Assertion		L					L		B	
	Broker	L						L	LB7	LB[7]	L
	Accès			L		L		L	L	L	L
	Autorisation				L	L		L	L	L	L

B = Traiter (Create/Read/Update/Delete), L = Lire (Read), M = ne lit que les métadonnées

Tableau 4 Relation entre les services et la sémantique du modèle d'information

[3] Relation linkedID incluse
[4] Relation à eIdentity incluse
[5] B pour l'identifiant (est également un attribut)
[6] B pour les Credentials (sont également des attributs)
[7] B, lorsque le Broker délivre lui-même des *Authentication and Attribute Assertions* combinées

7.7 Compétences pour les services administratifs

Le Tableau 5 démontre quelles parties prenantes proposent idéalement quel type de service. Les services administratifs sont décrits de manière plus approfondie dans le chapitre 7. La répartition proposée ici optimise la réutilisation des services. C'est pourquoi le *Relying Party* donne autant de responsabilité organisationnelle que possible aux prestataires de services *IAM*.

		Parties prenantes			
		Sujet	Prestataire de services IAM	Relying Party	Regulator
Services administratifs	eIdentity		X		
	Credential		X		
	Attributs		X		
	Trust		X		
	eRessource			X	
	Règle d'accès		X		
	Droit d'accès			X	
	Authentication		X		
	Attribute Assertion		X		
	Broker		X		
	Accès		X		
	Autorisation			X	

Tableau 5 Relation entre les services administratifs et les parties prenantes

8 Concepts de l'Identity Federation

E-Government demande une collaboration électronique au travers des limites organisationnelles. Le problème qui se pose est que aussi bien les *ressources* que les *sujets*, comme représenté sur la Figure 12, se trouvent dans différents *domaines* administratifs.[8]

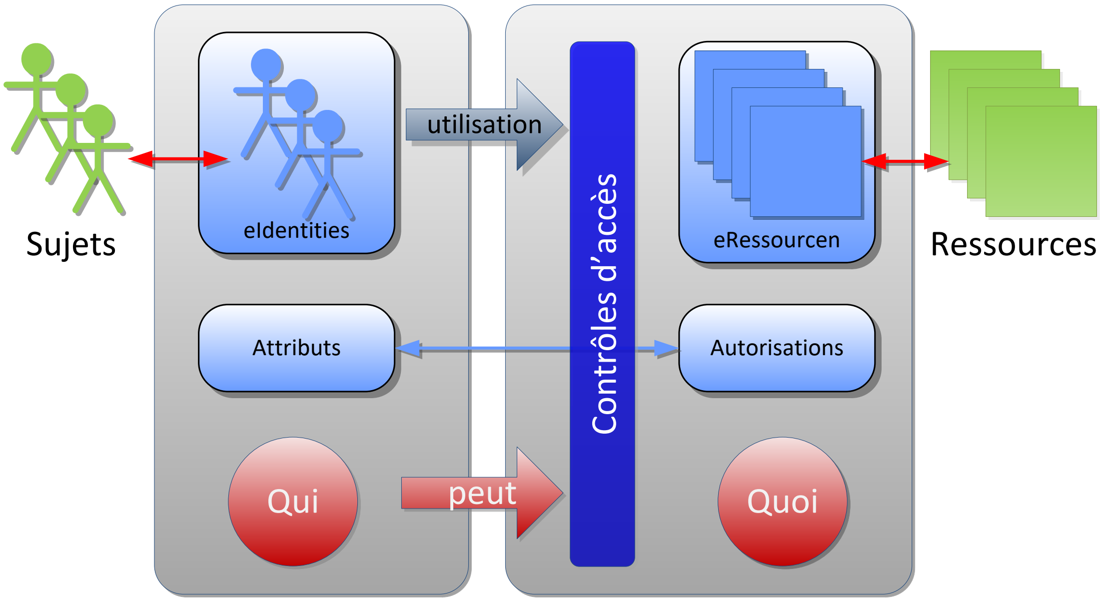

Figure 12 Qui peut quoi?

Par conséquent, E-Government représente un domaine de légitimité quant à l'ensemble de ses domaines et organisations. L'*accès* de l'«extérieur» à une *ressource* protégée d'un *domaine* est rendu possible par des moyens appropriés. Pour ce faire, le *sujet* est authentifié et autorisé, sur la base des autorisations à avoir *accès* aux *ressources*. Il existe quelques approches de résolution tel ce problème peut être rencontré.

1. Les *domaines* concernés échangent les informations de leurs *eIdentities* de manière à ce qu'elles soient connues dans les autres *domaines* respectifs.
2. Les *domaines* établissent entre eux ou par rapport à un tiers une relation de confiance.

Notamment, si un nombre plus important de *domaines* est concerné, la première solution est mal adaptée. De plus, les *eIdentities* doivent être comparées en permanence, ce qui peut devenir onéreux. La seconde approche est nettement plus flexible. Il en existe quelques modèles décrivant comment de telles relations de confiance entre des *domaines* administratifs peuvent être établies (bilatérales, à hiérarchie indirecte ou fédérées). Dans ce cas de figure, l'accent est mis sur l'*Identity Federation*.

[8] Les figures contenues dans ce chapitre utilisent des couleurs pour les objets qui ne font pas référence à la signification des couleurs utilisée jusqu'ici dans ce document.

8.1 Confiance et fédération

Une *fédération* consiste en une délégation de personnes compétentes et la responsabilité entre les différentes parties. Cela implique un travail basé sur la confiance. Dans le cas d'une *fédération d'eIdentities* entre plusieurs *domaines*, la méthode Single-Sign-On est communément appliquée. Cette simplification de *l'authentification* d'un *sujet* n'est pas le seul objet qui peut être délégué dans une *Identity Federation*. Selon le degré, des autorisations et même l'ensemble de l'*Identity Management* peuvent être transférés.

Une *Identity Federation* avec une fonction d'ouverture de session unique doit donc disposer d'une procédure standardisée, comme les parties échangent des informations entre elles de manière à ce qu'elles puissent être comprises mutuellement et être vérifiées quant à leur authenticité et intégrité.

8.2 Eléments de base de l'Identity Federation

Une *Identity Federation* établit de nouveaux concepts et composants qui constituent des éléments constitutifs. Le terme IdP/AA est utilisé dans les paragraphes suivants correspondant au service administratifs *Authentication Service*, *Attribute Assertion Service*, *Credential Service*, *eIdentity Service* et *Attribute Service* du chapitre 7.

Lorsqu'un *sujet* souhaite avoir *accès* à une *ressource* précise d'une *Relying Party* (RP) (cf. (1) dans la Figure 13), le *sujet* sélectionne son *service d'authentification* d'origine (*Identity Provider*). La *Relying Party* transmet le *sujet* à celui-ci (2). L'*Identity Provider* (IdP) entretient des *eIdentities* locales comme sous la forme d'une liste de *sujets*, par exemple. L'*Identity Provider* authentifie le *sujet* et peut certifier le résultat sous forme standardisée auprès de l'entité demandeuse (*Relying Party*). L'*Identity Provider* peut également agir comme *Attribute Authority* (AA) en fournissant d'autres informations du *sujet* sous forme de confirmations d'*attribut* destinées à la confirmation d'authentification. Le *sujet* donne son accord (3) avant que ces confirmations d'*attribut* peuvent être données.

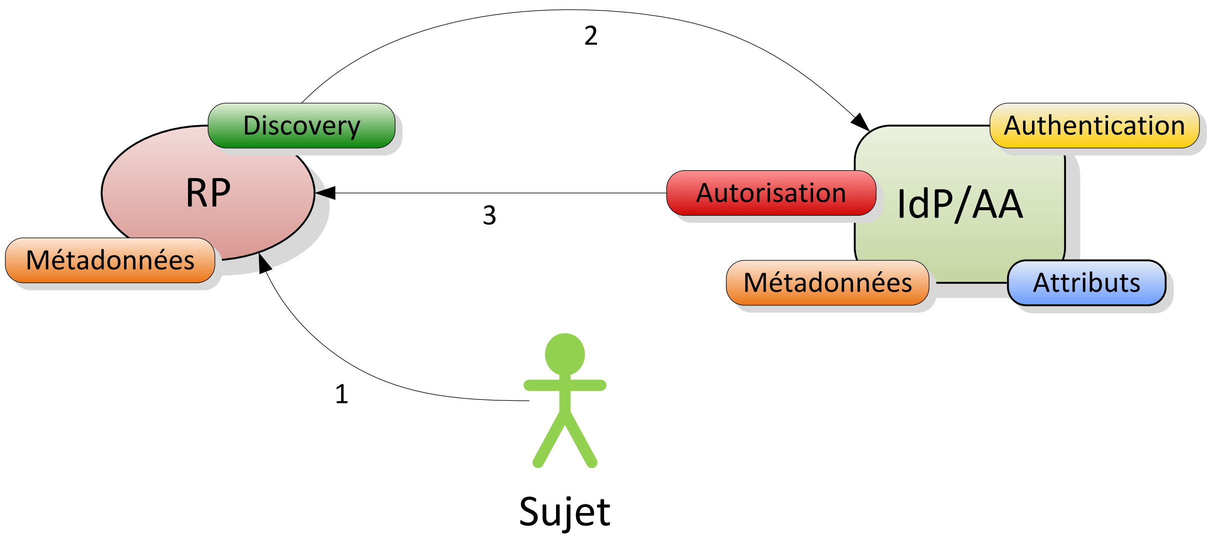

Figure 13 Eléments de base d'une Identity Federation

La *Relying Party* vérifie la réponse et accorde au *sujet* l'*accès* ou le refuse à la *ressource* en raison du résultat. La *Relying Party* donne son autorisation localement. Pour que les services respectifs connaissent les caractéristiques respectives et peuvent se faire confiance entre eux, le système a besoin d'informations précises sur tous les composants concernées. Ces informations sont transmises sous forme de *métadonnées*.

8.3 Modèles Identity Federation

Dès que plusieurs RP et IdP/AA rentrent en jeu, on parle de modèles complexes d'*Identity Federation*. À ce niveau, plusieurs scénarios sont possibles qui s'adaptent plus ou moins bien selon l'objectif et les conditions marginales.
Les cinq variantes d'application suivantes sont optimales pour des situations spécifiques. Pour l'application d'une solution *IAM fédérée*, il convient d'implémenter une de ces variantes ou leur forme mixte.

8.3.1 Modèle centré RP

Le *modèle centré RP* (cf. Figure 14) convient à une *Relying Party* laquelle met à disposition une *ressource* à un plus grand nombre d'organisations partenaires. Les sujets de ces organisations peuvent s'authentifier à leur IdP/AA d'origine de leur *domaine* et avoir accès à la *ressource* avec leurs *attributs*. L'avantage principal de la *Relying Party* se trouve dans le fait qu'elle ne doit pas gérer elle-même les *eIdentities*. Une *confirmation d'attribut et d'authentification* lui suffit pour autoriser l'*accès* à la *ressource* au *sujet*.

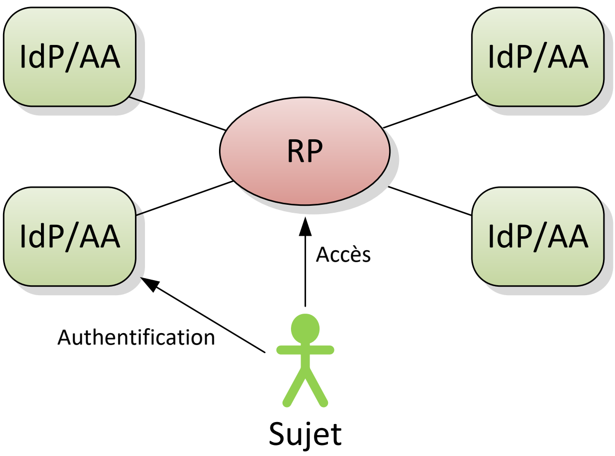

Figure 14 Modèle centré RP

8.3.2 Modèle centré IdP/AA

Le modèle centré IdP/AA (cf. Figure 15) est appliqué lorsque plusieurs systèmes *IAM* sont consolidés sur un seul IdP/AA, qui est ensuite utilisé par le plus de *Relying Parties* possible en vue d'authentifier et d'autoriser les *sujets*. Il est la plupart du temps facile à appliquer au sein d'une organisation. En revanche, au-delà des limites organisationnelles, il existe une multitude d'obstacles juridiques conséquents pour pouvoir mettre en œuvre ce scénario.

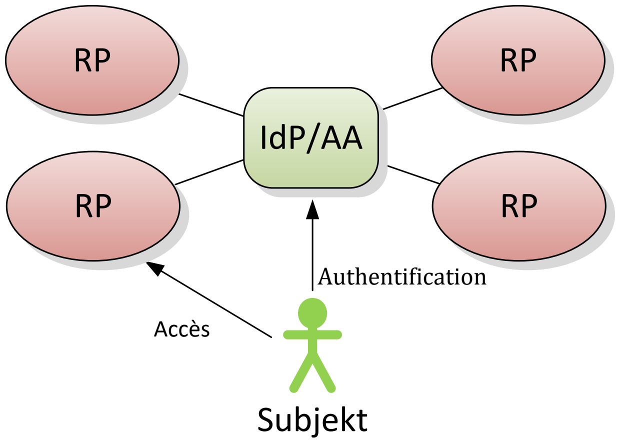

Figure 15 Modèle centré IdP/AA

8.3.3 Modèle Cross Domain

Dans un *modèle Cross Domain,* chaque organisation peut être aussi bien un *Identity Provider* qu'une *Relying Party*. C'est un scénario fréquent quand un *modèle centré IdP/AA* ne peut être mis en œuvre. Toutes les organisations tiennent à la disposition les *eIdentities* de leurs *sujets* en extérieur et en même temps exploitent elles-mêmes des *ressources* qui peuvent être utilisées via l'infrastructure *Cross Domain* non seulement par des *sujets* internes (par l'IdP/AA propre) mais également par des *sujets* externes.

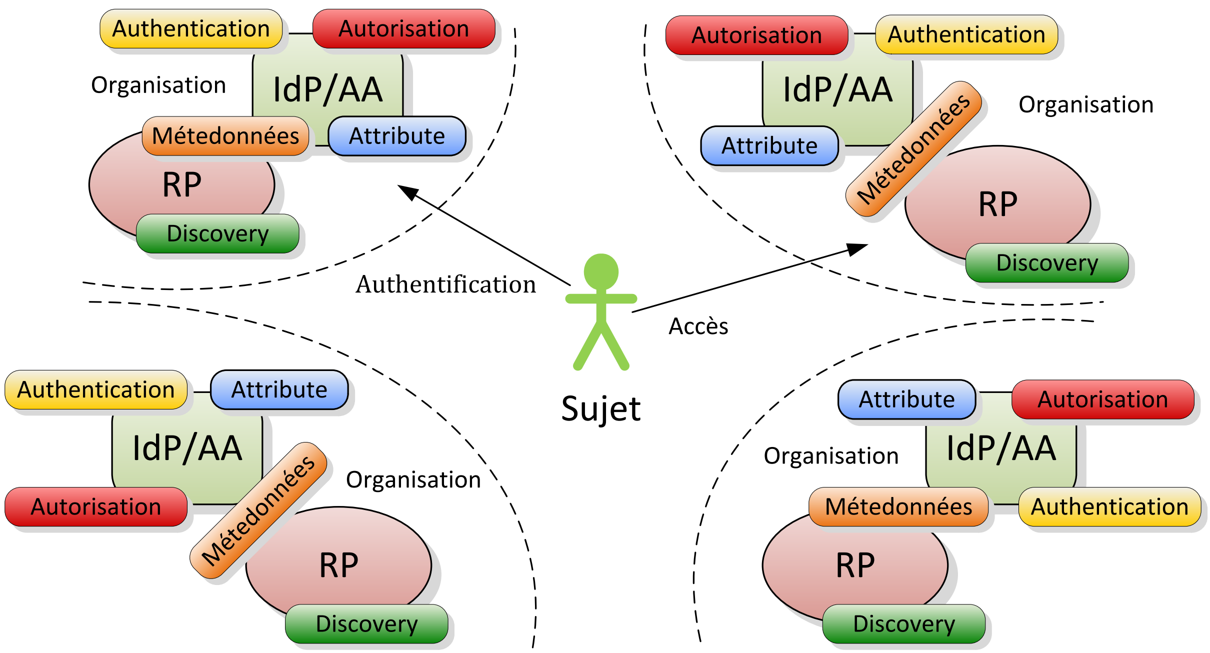

Figure 16 Modèle Cross Domain

Chaque organisation échange dans le *modèle Cross Domain* Peer-to-Peer leurs *métadonnées* et informations *Identity Provider* Discovery. Lorsque le groupement des organisations est trop important cela s'adapte mal. C'est pourquoi, ces services sont souvent centralisés et entretenus par un seul exploitant digne de confiance (cf. partie 8.3.4).

8.3.4 Métadonnées centralisées et Discovery

Le transfert des deux services Métadonnées et Discovery, comme représenté sur la Figure 17, constitue un scénario typique. Un Prestataire central de services *IAM* gère et publie les métadonnées de tous les composants impliqués avec un service Metadata Aggregator (MDA) et entretient en outre un Discovery Service (DS) centra.

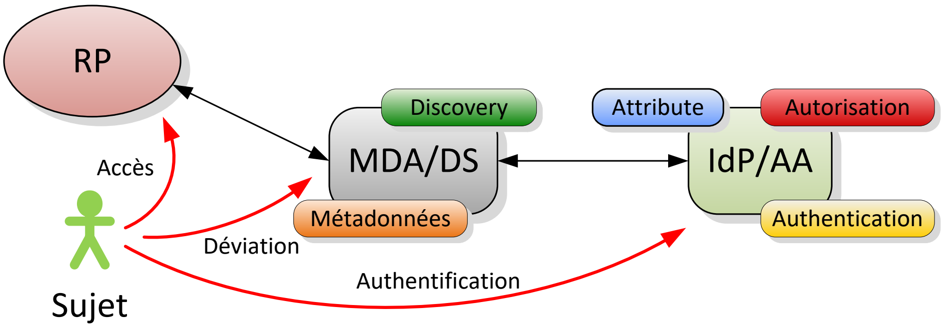

Figure 17 Métadonnées centralisées et Discovery Service

Mais bien d'autres services peuvent être centralisés tels que le montre le *modèle Hub-'n'-Spoke* à la partie 8.3.5.

8.3.5 Modèle Hub-'n'-Spoke

Le modèle Hub-'n'-Spoke[9] se base sur une *Identity Hub* centrale, à laquelle toutes les parties concernées avec leurs services font confiance. Comme indiqué sur la Figure 18, cette *Identity Hub* peut se charger d'autres services des parties et les mettre en pratique de manière centrale. Le déroulement du protocole quant au temps d'exploitation est modifié dans ce modèle et par là même est plus direct. Les RP communiquent seulement avec l'*Identity Hub* centrale. Cette dernière entretient un tableau central avec les *eIdentities* des *sujets* (Identity Linking). De cette manière, elle peut faire authentifier un *sujet* par un des *Identity Provider* indiqués, recueillir des informations d'*attribut* d'autres sources IdP/AA et les rassembler pour une réponse agrégée à la *Relying Party*.

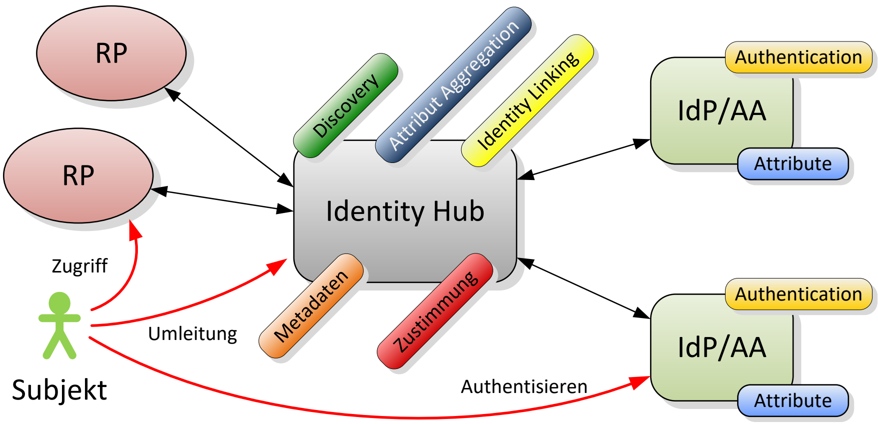

Figure 18 Modèle Hub-'n'-Spoke

---

[9] Structure en étoile

Le *modèle Hub-'n'-Spoke* représenté sur la Figure 18 indique une possibilité de centralisation de services. Des niveaux de centralisation bien différents sont possibles ici comme il existe aussi des formes mixtes des modèles d'*Identity Federation* présentés ici.

Indépendamment du type de modèle d'*Identity Federatio*n utilisé, la collaboration (électronique) au-delà des limites organisationnelles représente dans tous les cas un défi quant à la planification, l'uniformisation des processus et la sémantique ainsi qu'à l'infrastructure. Plus le groupement d'organisations est important dans une Identity Federation, plus un règlement contractuel doit fixer les directives relatives aux relations entre chacune des parties.

9 Exclusion de responsabilité – Droit 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.

10 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 toutes restrictions 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

[CAS]	SECO. Claim Assertion Service Technical Specification. Version 0.98.05, 19.1.2011. http://www.suissecas.org/media/CAS_Specification_0.98.05.pdf
[ISBRefM]	eCH groupe spécialisé *IAM*. Identity & Access Management *IAM* – Modèle de référence *IAM*. White Paper. Version 1.1d, 16.3.2011. http://www.isb.admin.ch/themen/architektur/00183/01368/01371/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCEeHt5g2ym162epYbg2c_JjKbNoKSn6A--&t=.pdf
[OASIS]	http://docs.oasis-open.org
[SAML 2.0 TechOverview]	OASIS. Security Assertion Markup Language (SAML) V2.0 Technical Overview. Committee Draft 02, 25.3.2008. http://www.oasis-open.org/committees/download.php/27819/sstcsaml-tech-overview-2.0-cd-02.pdf
[SAML Glossaire]	OASIS. Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0. 15.3.2005. https://www.oasis-open.org/committees/download.php/21111/saml-glossary-2.0-os.html
[SOWISCH]	Rapport de l'atelier d'experts «Les opportunités de sécurité pour la place économique Suisse» en date du 8.11.2012 (cf. stratégie de la société de l'information)
[Stabi3]	eCH groupe spécialisé *IAM*, Projet E-Government B2.06. Stabi3eGov B2.06 Architecture de solution *IAM*. Rapport. 4.1.2011. http://www.ech.ch/alfresco/guestDownload/attach/workspace/SpacesStore/f91f7628-2050-4889-bd69-f2b27b580e67/E-Gov%20B2.06_*IAM*-Loesungsarchitektur_V120_04.01.2011_d.pdf
[TOGAF]	http://www.opengroup.org/togaf/
[UML]	http://www.uml.org/

Annexe B – Collaboration & contrôle

Bernold Ronny	Haute école spécialisée bernoise
Besiryan René	accessec
Buff Raffael	Abraxas
Burger Hans	Adnovum
Eberle Marcel	Canton SG
Fischer Markus	
Häni Hans	Haute école spécialisée bernoise
Hassenstein Gerhard	Haute école spécialisée bernoise
Hempel Torsten	IC Consult
Kuhn Fabienne	Haute école spécialisée bernoise
Laube-Rosenpflanzer Annett	Haute école spécialisée bernoise
Leiser Daniel	ATOS AG
Minth Lars	UPIC
Muhm Christofer	IC Consult
Müller Willy	UPIC
Rohr Sebastian	Accessec
Spichiger Andreas	Haute école spécialisée bernoise
Topfel Martin	Haute école spécialisée bernoise
	eCH groupe spécialisé IAM

Annexe C – Abréviations

AA	Attribute Authority
CAS	Attribute Assertion Service
CP	Credential Provider
IAM	Identity and Access Management
IdP	Identity Provider
OASIS	Advancing open standards for the information society
RP	Relying Party
SAML	Security Assertion Markup Language
SLA	Service Level Agreement
SSO	Single Sign-On
Stabi3	Stabilisation conjoncturelle
TOGAF	The Open Group Architecture Framework
UML	Unified Modelling Language [UML]
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

Annexe D – Glossaire

Dans le contexte du présent document, les mots suivants signifient:

ABAC	Attribute Based Access Control Lors du *contrôle d'accès* sur la base des attributs, les utilisateurs se voient accorder de façon dynamique *l'entrée/l'accès* aux *ressources* sur la base de leur attribut. cf. *RBAC*
Accès	Interaction avec une *entité* pour manipuler ou utiliser une ou plusieurs de ses *ressources*. [glossaire SAML] Les *accès* sont enregistrés pour garantir la traçabilité et la non-répudiation.
Access	Voir *accès*
Access Control	voir *contrôle d'accès*
Access Service	voir Service *Accès*
Access Service Provider	*Entité* en charge de l'ensemble du processus d'*authentification* et d'*autorisation*, qui décide de donner ou non l'*accès* définitif sur la base des *Credentials* disponibles. L'Access Service Provider met également à disposition les données requises pour la comptabilité, la facturation et l'octroi des licences, en fonction du type d'utilisation.
Agent	Un *agent* abstrait un système d'information à partir d'un utilisateur réel. Il joue le rôle qu'occupe un utilisateur réel dans le cadre d'une transaction par rapport au système d'information.
Assertion	Voir *Authentication Assertion* ou *Attribute Assertion*
Assertion de validation	Voir *Authentication Assertion.*
Attribut / Attribute	Représentation sémantique d'une *propriété* qui caractérise un *sujet* qui le décrit au mieux. L'*identifiant* et les *Credentials* sont également des *attributs*. Un attribut se compose des méta-attributs suivants: nom d'attribut (p. ex. «pointure»), type d'attribut (p. ex. «intègre») et valeur d'attribut (p. ex. «39»). En cas de suppléance, l'*eIdentity* du supplément possède pour un certain temps une quantité d'*attributs* de l'*eIdentity* du *sujet* représenté.
Attribute Management	Processus de définition, de gestion et d'utilisation d'*attributs*.

Attribute Assertion	Confirmation d'un *attribut* par une *Attribute Authority*. Correspond à une SAML 2.0 *Attribute* Assertion [SAML 2.0 TechOverview].
Attribute Assertion Service	Voir *Attribute Authority*.
Attribute Authority	Une *entité* (service) technique, qui délivre des *Attribute Assertions* à partir d'une interface définie. [glossaire SAML]. Synonyme: *Attribute* Assertion Service
Attribute Service	L'*Attribute* Service maintient un ou plusieurs *attributs* actuels pour des *sujets* définis. Voir également *Attribute Management*.
Auditing	a) Contrôle de la conformité de la *Policy* b) Enregistrement de toutes les actions et décisions, pour garantir la traçabilité.
Authentication Assertion	Confirmation de *l'authentification* réussie d'un *sujet*. [glossaire SAML]
Authentication Authority	*Entité* (service) technique, qui propose *l'authentification* en tant que service et délivre des *Authentication Assertions* pour les *sujets*. [glossaire SAML]
Authentication Service	À l'aide des *Credentials*, l'*Authentication* Service contrôle si celui qui accède (*sujet*) est celui qu'il prétend être. Voir également *Authentication Authority*.
Authentification	Processus de contrôle d'une *eIdentity* supposée. Synonyme: validation.
Authentification	Voir *Authentification.*
Authentification	Justification de l'*eIdentity* d'un sujet.[10]
Authorization Provider	*Entité* qui fournit l'*autorisation* en tant que service.
Authorization Service	Pendant la durée d'exécution, le service contrôle le respect des droits d'utilisation des e*Ressources*, et autorise l'utilisation au *sujet*, lorsque celui-ci possède les droits nécessaires.
Autorisation	a) Administration: définition des *règles* et *droits d'accès* à une *eRessource*. b) Pour la durée de validité: vérification du droit d'*accès* d'un *sujet* authentifié à une *ressource* et délivrance de l'*accès* pour la durée de validité. On différencie *l'autorisation grossière* de *l'autorisation précise.*

[10] En allemand, les termes *Authentisierung* et *Authentifikation* sont fréquemment utilisés en tant que synonymes.

Autorisation grossière	Octroi ou refus de l'*accès* à une *ressource*.
Autorisation précise	Octroi ou refus de l'*accès* à l'une des fonctions ou données mises à disposition par une *ressource*.
Autorité d'*attributs* (AA)	Une *autorité d'attributs* est un *registre* ou une *liste* constituée d'un *Attribute Service* destiné à l'entretien des *attributs*, et d'un *Attribute Assertion Service* pour l'émission d'*Attribute Assertions*.
Autorité d'authentification (AuthnA)	Une *AuthnA* met un *Authentication Service* à disposition, auprès duquel le *sujet* peut s'authentifier. L'*Authentication Service* utilise les *Credentials* délivrés par un *Credential Service*. Le *Credential* Service peut faire partie de l'*AuthnA*. Quelques exemples *d'autorités d'authentification*: IdPs (d'après SAML), OpenID Provider et MobilID Provider.
Broker Service	Ce service transmet la durée d'exécution entre le *sujet*, les *ressources* et les services.
Caractéristique d'identification	La *caractéristique d'identification* peut être basée sur une connaissance (mot de passe, PIN), sur une propriété (certificat, clé personnelle) ou sur une *caractéristique* (caractéristique biométrique, p. ex. voix, lecture de l'iris, empreinte digitale), ou sur une combinaison de ces caractéristiques.
Certificat numérique / Digital Certificate	Données structurées qui authentifient le propriétaire, ainsi que d'autres caractéristiques d'une clé publique (également certificat ou certificat de clé publique).
Certification Authority (CA)	Instance qui authentifie les données et délivre les certificats numériques à cet effet, dans le cadre d'un environnement électronique. Synonyme: Certification Service Providers (CSP)
Certification Service Providers (CSP)	Instance qui authentifie les données et délivre les certificats numériques à cet effet, dans le cadre d'un environnement électronique. Synonyme: *Certification Authority* (CA)
Claim	Le terme *Claim* n'est pas explicitement utilisé dans ce document, puisqu'il existe différentes significations, dont certaines se contredisent en partie. Par conséquent, l'utilisation de ce terme n'est pas conseillée. voir *Attribute Assertion*
Claim Assertion Service (CAS)	Le *Claim Assertion Service* est un type particulier d'*Attribute Authority*. Sa fonction est d'autoriser l'utilisateur à authentifier des caractéristiques qui lui sont attribuées par une organisation ou un registre. [CAS]
Confiance	Relation de confiance le plus souvent définie dans le *SLA* entre les instances responsables. ex. la description formelle des critères devant être remplis, afin que deux *organisations*, *entités*, *domaines* etc. se fassent mutuellement confiance (engl. Trust).

Confirmation d'*attributs*	Voir *Attribute Assertion.*
Contrôle d'accès	Surveillance et contrôle de l'*accès* aux *ressources*. L'objectif est de garantir l'intégrité, la confidentialité et l'accessibilité des informations.
Credential	Justificatif de confirmation de l'*eIdentity* d'un *sujet*. Dans un contexte *IAM*, utilisé pour vérifier l'*eIdentity* d'identification d'un utilisateur (*identifiant*), en relation avec une (ou plusieurs) *caractéristique(s) d'authentification*. Synonyme: preuve d'identité
Credential Management	Processus d'établissement et d'attribution de *Credentials.*
Credential Service	Le *Credential* Service délivre et gère les *Credentials*. Il existe différents types de *Credentials*. Un Credential se réfère à une *eIdentity* et est délivré pour un *sujet* précis.
Credential Service Provider	*Entité* qui agit en tant que fournisseur fiable de certificats électroniques ou d'autres tokens de sécurité (*Credentials*).
Domaine	Communauté administrative / technique ou organisation avec une *policy* commune*.*
Droit d'accès	Les *responsables des ressources* définissent les *droits d'accès* à leurs *eRessources*. Les *droits d'accès* définissent les conditions auxquelles le *sujet* a le droit d'utiliser les différentes fonctionnalités d'une *ressource* (*autorisation précise*), par exemple lorsque *l'authentification* a été effectuée et que les *attributs* définis ont été validés.
eIdentity	Représentation d'un sujet. Une *eIdentity* (*identité numérique*) a un *identifiant* (nom unique), le plus souvent avec une quantité d'*attributs supplémentaires*, qui peuvent être attribués de manière claire à un *sujet* dans un *espace de noms*. Un *sujet* peut avoir plusieurs *eIdentities*.
eIdentity Service	L'eIdentity Service délivre des *eIdentities* aux *sujets* et les gère.
Enregistrement / Registration	Processus d'une instance d'enregistrement qui délivre une *eIdentity* avec le *Credential* correspondant à un *sujet*..
Entité / Entity	Elément actif d'un système informatique, p.ex. un processus automatisé ou un grand nombre de processus, un système partiel, une personne ou un groupe de personnes ayant des fonctionnalités définies. [glossaire SAML]
Entreprise	Voir *organisation*
eRessource	Représentation numérique d'une *ressource*. Une *eRessource* possède un identifiant (nom explicite, souvent une URL/URI), qui peut être explicitement attribuée à une *ressource*, dans un espace de noms. Une *ressource* peut avoir plusieurs *eRessources*.

eRessource Service	L'*eRessource* Service délivre des *eRessources* aux *ressources* et les gère.
Espace de noms	Domaine d'utilisation (p.ex. une entreprise, un Etat, une communauté spécialisée, une communauté linguistique) pour lequel la signification de la chaîne de caractères est définie (p. ex. l'identifiant).
Fédération / Federation	Collaboration par delà les limites des organisations et systèmes, sans duplication ou réplication des données d'utilisateur nécessaires à cela (*eIdentities*).
Fonction	Caractéristique qui attribue des tâches, compétences et responsabilités précises à un *sujet* dans le cadre d'une organisation. Un *sujet* peut avoir plusieurs fonctions (cf. rôle).
Gestion de l'identité et de l'accès / Identity and Access Management (*IAM*)	Tous les processus et systèmes qui permettent l'*accès* des *sujets* aux *ressources* dont ils ont besoin, en raison de leur fonction au sein de l'organisation.
Gestion fédérée des identités / Federated Identity Management (FIdM)	La gestion fédérée des identités permet l'utilisation transversale d'*eIdentities* dans des domaines normalement fermés. FIdM permet aux utilisateurs d'un *domaine* d'accéder de manière simple et sûre aux systèmes d'un autre *domaine*, sans bâtir de gestion redondante des utilisateurs.
Habilitation	Droit d'un *sujet* d'utiliser certaines *ressources*.
I*dentifiant*	Une chaîne de caractères qui définit clairement une *eIdentity* ou une *eRessource* dans un *espace de noms*. L'*identifiant* d'une ressource est souvent une URL/URI.
Identité / Identity	L'identité correspond à la totalité des caractéristiques qui caractérisent un *sujet* et le distinguent de tous les autres en tant qu'individu. Dans le contexte *IAM*, on utilise principalement l'*eIdentity* d'un *sujet* (cf. *eIdentity*).
Identité électronique / Electronic Identity	Voir *eIdentity*
Identité numérique / Digital Identity	voir *eIdentity*.
Identity Provider (IdP)	*Entité* qui gère et publie l'*eIdentity*. Un IdP met un *Authentication Service,* et souvent également un *Attribute Assertion Service,* à disposition.
Infrastructure d'intermédiaire	voir *Broker* Service

linkedID	Dans le contexte inter-organisations, *linkedID* permet de mettre en relation les eIdentities de différents domaines. Les eIdentities peuvent être associées à n'importe quel graphique avec *linkedID*. La mise en œuvre concrète d'eCH-0107 peut restreindre encore la forme (ex. arborescence au lieu du graphique) et règle l'interprétation (sémantique) du graphique en fonction de leurs compétences (cf. 7.3.3 *Broker Service*).
Liste	Collecte systématique d'informations possédant des caractéristiques communes.
Méta-domaine	*Domaine* qui régule la collaboration entre deux ou plusieurs *domaines*.
Métadonnées	Moyen qui permet la confiance et l'interopérabilité technique entre les composants *SAML* (*entités*). Les métadonnées peuvent également être utilisées pour échanger les informations d'*attributs*.
Organisation	Unité organisationnelle composée de plusieurs *sujets* (personne morale, entreprise, association, service administratif, groupe de sujets etc.). cf. *sujet* et Figure 19.
Personne morale	voir Organisation
Policy	Réglementations et directives consignées par écrit et devant être observées.
Prestataire de services IAM	Le *prestataire de services IAM* est l'exploitant d'un ou de plusieurs services administratifs IAM selon le chapitre 7.
RBAC	Role Based Access Control Lors du contrôle d'accès basé sur les rôles, un ou plusieurs *rôles* peuvent être attribués à des utilisateurs ou groupes d'utilisateurs. Un *rôle* contient une quantité d'autorisations (Permissions), qui décrivent les opérations autorisées sur une r*essource*. cf. ABAC
Registre	Listes dans le langage administratif, p.ex. le registre des habitants, le registre des avocats, le registre de l'état civil, le registre du commerce, etc. En règle générale, ces registres sont tenus par des instances (autorités) officielles
Règle d'*accès*	Les *responsables des ressources* définissent les *règles d'accès* à leurs *eRessources.* Les *règles d'accès* définissent les conditions auxquelles un *sujet* obtient l'*accès* à une *ressource* (*autorisation grossière*), par exemple lorsque *l'authentification* a été effectuée et que les *attributs* définis ont été validés.
Relying Party (RP)	Le *Relying Party* représente les intérêts de la *ressource.* Il utilise les services administratifs *IAM* et traite les informations des *prestataires de services IAM*, pour protéger ses *ressources*. En vue de l'évaluation et de l'autorisation d'un *accès* aux *ressources*, il a besoin d'informations plus approfondies concernant un *sujet*.

Responsable des ressources	Autorité responsable des *ressources* gérées par le *Relying Party* (p. ex: responsable des applications, responsable de service, détenteur des données).
Ressource	Service ou données auxquels un *sujet* peut avoir *accès* s'il s'est authentifié et que cela a été autorisé sur la base des *attributs* nécessaires. Ceci inclut les ressources physiques comme les bâtiments et installations, dont l'utilisation est commandée par des système IT.
Rôle / Role	a) *Sujet*: nombre précis de fonctions exécutées par un *sujet*. Un ou plusieurs *rôles* peuvent être attribués à un *sujet*. b) *eIdentity*: *attributs*, qui représentent les rôles/fonctions du sujet c) *Entité*: rôle et objectif d'une *entité* au sein d'une *fédération*. Un ou plusieurs rôles de partie prenantes peuvent être attribués à une *entité* (voir chapitre 3).
Security Assertion Markup Language (SAML)	Le SAML (Security Assertion Markup Language) est spécifié pour permettre le Sign-On, indépendamment du fabricant. Le SAML est un outil XML qui permet d'échanger les informations d'*authentification* et d'*autorisation*. Le SAML a été standardisé par un consortium international, dans le cadre de l'OASIS. [OASIS]
Security Token	Un paquet de données qui peut être utilisé pour autoriser l'*accès* à une *ressource*.
Service d'accès	Le service contrôle le respect des règles d'accès et permet au sujet l'accès, lorsque les règles correspondantes sont remplies. Synonyme: *Access* Service.
Service droit d'accès	Ce service gère les droits d'utilisation d'une *eRessource*. Les droits sont définis sur la base de *l'authentification*, des *attributs* ou des modèles (groupes, rôles, autorisations individuelles).
Service Level Agreement (SLA)	Définit un contrat entre le donneur d'ordres et le prestataire de services, pour des prestations répétitives.
Service *règles d'accès*	Ce service gère les *règles d'accès* à une *ressource*. Les règles sont définies sur la base de *l'authentification* ou des *attributs*.

Sujet	Personne physique, *organisation* ou service qui a *accès* ou voudrait avoir accès à une *ressource*. Un *sujet* est représenté par des *eIdentities*.

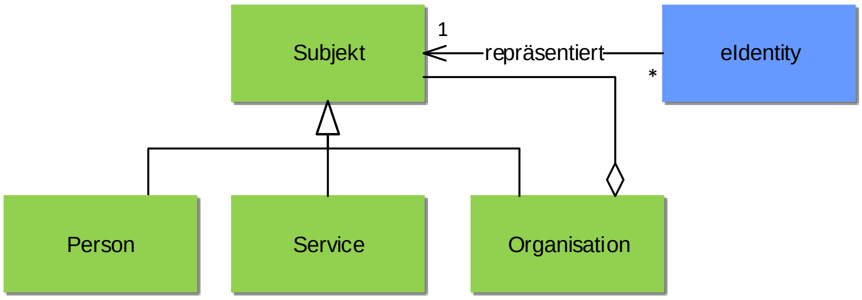

Figure 19 Définition du sujet

Trust Service	Le *Trust* Service maintient et accepte les prestataires de services *IAM* dignes de confiance.
Trust-Level	Niveau de confiance convenu entre les parties concernées, qui définit l'obligation de sécurité pour les processus et les composants technologiques.
Trusted Third Party	Instance digne de confiance, p.ex. pour la gestion de clés publiques ou de certificats.
User	Voir *utilisateur*
Utilisateur	*Sujet* moral.

Annexe E – Modifications par rapport à la version 1.00

La présente norme est basée sur les principes opérationnels de l'eCH-0107 v1.00. La version remaniée comporte cependant de nouveaux concepts et connaissances fondamentaux. La version 2.0 de l'eCH-0107 a été en grande partie remaniée. Les modifications générales sont énumérées ci-dessous et renvoient au contenu de la version 1.00 de l'eCH-0107.

Modifications principales:

- *V1.00 est un Best Practice, la V2.0 est une nouvelle norme.*
- *La structure des chapitres a été complètement modifiée et doit garantir une entrée en matière plus simple dans l'IAM inter-organisationnelle.*
- *Les travaux relatifs au projet Stabi 3 eGov, ainsi que leur architecture de solutions, ont été intégrés et appliqués.*
- *V2.0 se limite en conséquence à l'IAM inter-autorités.*

Chapitre 2 Introduction **[eCH-0107 v1.00 Chapitre 1]**

- *Le glossaire a été nettement enrichi, remanié et se trouve à présent à l'annexe D.*
- *L'introduction a été entièrement remaniée et se focalise sur l'IAM fédéré.*

Chapitre 3 Parties prenantes **[nouveau]**

- *Les catégories de base des parties prenantes et leur mapping par rapport aux services administratifs ont été remaniés.*

Chapitre 4 Exigences **[eCH-0107 v1.00 Chapitre 2]**

- *Les visions architecturales et les principes généraux du design ont été introduits.*
- *Les exigences ont été retravaillées et complétées par de nouvelles connaissances.*

Chapitre 5 Architecture de l'information **[eCH-0107 v1.00 partiellement Chapitre 4]**

- *Le modèle d'information a été entièrement remanié.*
- Le modèle d'information distingue les éléments du monde réel, le modèle sémantique et les objets de l'interface.

Chapitre 6 Processus **[nouveau]**

- *Les processus ont été désormais été insérés (Basis Stabi 3 eGov).*

Chapitre 7

Services administratifs **[eCH-0107 v1.00 partiellement Chapitre 4]**

- *Les services administratifs ont été considérablement retravaillés et conçus pour l'IAM fédéré.*

Chapitre 8 Concepts de l'Identity Federation **[nouveau]**

- *Les concepts de l'Identity Federation ont été inclus et documentés.*