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

Titre	Principes de conception de l'IAM
Code	eCH-0107
Type	Best Practice
Stade	Définie
Version	1.00
Statut	Annulé
Validation	2011-03-11
Date de publication	2014-09-03
Remplace	
Langues	Français, Allemand
Auteur(s)	Willy Müller, ISB, willy.mueller@isb.admin.ch Hans Häni, AFT TG, hans.haeni@tg.ch Groupe de projet -SEAC IAM
Éditeur / Distributeur	Association eCH, Mainaustrasse 30, Case postale, 8034 Zürich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Condensé

Le présent document définit les exigences, les principes et les règles relatifs à la conception du système IAM, qui doivent être considérés dans le cadre de la mise à disposition des solutions IAM fédératives dans la cyberadministration Suisse, pour que les applications et les services locaux dans les infrastructures nouvelles et existantes puissent utiliser ces offres. Ces bonnes pratiques doivent aussi être utilisées dans le service de la cybersanté Suisse.

Table des matières

Statut du document

Le présent document a été **annulé** par le Comité d'experts. Par conséquent, il a force normative pour le champ d'application défini dans le domaine de validité déterminé.

1 Introduction

1.1 Domaine d'application

Le présent document définit les exigences et les principes de conception du système de gestion des identité et des accès (IAM). Ces principes doivent être considérés dans le cadre de la mise à disposition des solutions IAM fédératives dans la cyberadministration suisse, pour que les applications et les services locaux puissent utiliser ces offres de façon intra-organisationnelle.

Ce document sert de guide pour tous ceux qui créent des solutions IAM dans le domaine de la cyber-administration. Le document décrit une architecture conceptionnelle qui doit constituer la base du projet en vue de la création de nouvelles solutions IAM et de l'évaluation des solutions IAM existantes.

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.

La structure du document est basée sur le cadre d'architecture [TOGAF].
Elle contient des principes de projet qui seront appliqués[1] dans les phases « B. Structure organisationnelle» et « C. Architecture du système d'information ».

1.2 Définitions IAM

Définition des termes souvent utilisés dans ce document :

IAM	Gestion des identités et des accès (Identity and Access Management)
Sujet	Entité qui a accès ou voudrait avoir accès à une *ressource* électronique. Il peut s'agir d'une personne physique ou morale, mais aussi d'une machine.
Ressource	Application, service, fonction, processus ou données, auquel un *sujet* voudrait avoir accès.
Client	Système technique (application, navigateur Internet etc.), au moyen duquel le sujet accède à la ressource.

[1] eCH-0107 peut être considéré comme « Foundation Architecture » dans le sens du continuum d'architecture selon TOGAF, voir The Open Group. TOGAF Version 9. The Open Group Architecture Framework (TOGAF), p 543 et suivantes.

Identité	*Identifiant*, souvent associé à une quantité de caractéristiques supplémentaires, qui peuvent être attribuées clairement à un *Sujet* dans un *espace de noms*. Un sujet peut posséder plusieurs identités.
Identité numérique	*Identité*, au format codé, qui peut être traitée en format électronique.
Identifiant	Chaîne de caractères qui définit clairement un s*ujet* dans un *espace de noms*.
Espace de noms	Domaine d'application, pour lequel une chaîne de caractères est définie (p. ex. une entreprise, un Etat, une communauté spécialisée, une communauté linguistique).
Credential	Habilitation et information d'identification, grâce auxquelles l'*identité* d'un *sujet* demandant l'accès peut être vérifiée.
Security Token	Jeton de sécurité (token de sécurité) qui peut être utilisé pour autoriser l'accès à une *ressource.*
Claim	Affirmation sur un *sujet*, certifiée conforme par un organisme officiel, p. ex. "a 18 ans", "est médecin". (Dans les ouvrages IAM, on trouve également les termes 'rôle', 'attribut' ou 'groupe' selon le contexte).
Inscription	Processus visant à obtenir une *identité* ou un *credential* délivré par un service d'inscription.
Administration	Dans notre contexte, obtention de toutes les conditions nécessaire afin de pouvoir définir, au moment de l'accès, si un sujet est autorisé à accéder à une ressource.
Authentification	Justification de l'identité d'un sujet.
Authentification	Processus de vérification d'une *identité.*
Autorisation	Délivrance d'un droit d'accès pour une *identité* vérifiée.
Identity Provider (IdP)	Fournisseur d'*identités numériques.*
Credential Provider	Fournisseur de *Credentials*, p. ex. fournisseur de certificats électroniques.

Claim Provider (CP)	Organisme qui enregistre les *Claims* et certifie qu'un *sujet* correspond à un *Claim* défini (p. ex. occupe un certain rôle).
Responsable de ressource	Organisme responsable de l'attribution de droits de *Claims* pour l'accès aux *ressources* qu'il gère (p. ex. : responsable d'application, responsable de service, propriétaire de données).
Access Provider	Organisme qui réalise de façon centralisée l'ensemble du protocole d'authentification et d'autorisation et prend la décision définitive d'autoriser l'accès en se basant sur les Credentials mis à disposition etc. L'Access Provider met également à disposition les données nécessaires aux services de comptabilité, de facturation et de délivrance de licences d'utilisation.
Authentication Provider	Organisme qui fournit une prestation d'*authentification*.
Authorization Provider	Organisme qui fournit une prestation d'*autorisation*.
Policy	Dans notre contexte : IAM-Policy. Réglementations et prescriptions consignées par écrit et devant être observées pour respecter les objectifs des *domaines* concernés.
Policy Enforcement Point	(PEP) – Lieu où la *policy* est appliquée.
User	Personne qui souhaite accéder à une *ressource*.
Trust-Level	Niveau de confiance conclu entre les participants, qui définit les exigences en terme de sécurité des processus et des composants technologiques.
Autorisation grossière	Autorisation ou refus de l'accès à une ressource.
Autorisation précise	Autorisation ou refus de l'accès à certaines fonctions ou données mises à disposition par une ressource.
Accès	Activation d'une ressource, dans le but d'exécuter une fonction ou d'extraire des données. Pour garantir la clarté et la vérifiabilité, les accès sont enregistrés.
Auditing	a) Vérification de la conformité à la Policy. b) Liste de toutes les actions et décisions pour garantir la traçabilité.
Domaine	Communauté ou organisation avec une *policy* commune.
Domaine de base	Domaine qui gère des *ressources* et qui impose le respect de la *Policy* pour les *Policy Enforcement Points*.

Meta-domaines	*Domaines* que le travail en collaboration régit entre deux ou plusieurs domaines.
Auditing	a) Vérification de la conformité à la Policy. b) Liste de toutes les actions et décisions pour garantir la traçabilité.

Remarque : certains termes sont souvent utilisés en anglais dans les ouvrages de référence. Nous avons évité d'utiliser des termes français de façon conséquente.

2 Exigences

Exigences IAM à l'égard des utilisateurs

- Je dois indiquer mon identité uniquement lorsque cela est nécessaire.
- Je dois indiquer mes Credentials uniquement lorsque cela est nécessaire.
- Je peux accéder aux ressources sécurisées dans le monde entier, indépendamment du lieu où je me trouve.
- Je n'ai besoin que de peu d'identités électroniques.
- Je ne dois gérer qu'un faible nombre de Credentials.
- Il est bon marché de se procurer des identités électroniques et des Credentials.
- Il est facile de se procurer des identités électroniques et des Credentials.
- Les identités électroniques et les Credentials sont faciles à utiliser.
- Un éventuel représentant peut agir à ma place. Dans le cas où il me représente (confirmé par les Claims correspondants), son identité électronique recevra les droits nécessaires pour les ressources requises.
- Personne ne peut avoir accès à mes données personnelles, sauf si je l'autorise expressément.
- La solution est fiable.
- Je peux définir un représentant qui peut agir à ma place. Le représentant peut être une autre personne ou une machine.

Exigences IAM à l'égard des responsables de ressources

- Il est impossible d'abuser des ressources.
- L'accès aux ressources est accordé uniquement aux personnes ou aux systèmes autorisés.
- Les dépenses liées à la gestion des identités électroniques sont minimales.
- Les dépenses liées à la gestion des Credentials sont minimales.

- Les dépenses liées à la gestion des Claims sont minimales.
- Les dépenses liées à la gestion des autorisations sont minimales.
- Les objectifs juridiques, notamment la protection des données ainsi que tous les autres objectifs de sécurité spécifiques à l'organisation doivent être garantis à tout moment.
- La clarté et la vérifiabilité de l'accès d'un certain sujet à une ressource définie à un moment donné sont garanties. Le rapport entre une identité électronique et ses Credentials doit être garanti à tout moment.
- Les normes et standards techniques et organisationnels en vigueur doivent être respectés.

3 Structure organisationnelle

3.1 Aperçu

Le graphique suivant représente la structure organisationnelle de l'IAM de façon schématique. La distinction entre le temps de définition et le temps d'exécution est essentielle, puisque les Provider responsables ont des rôles différents.

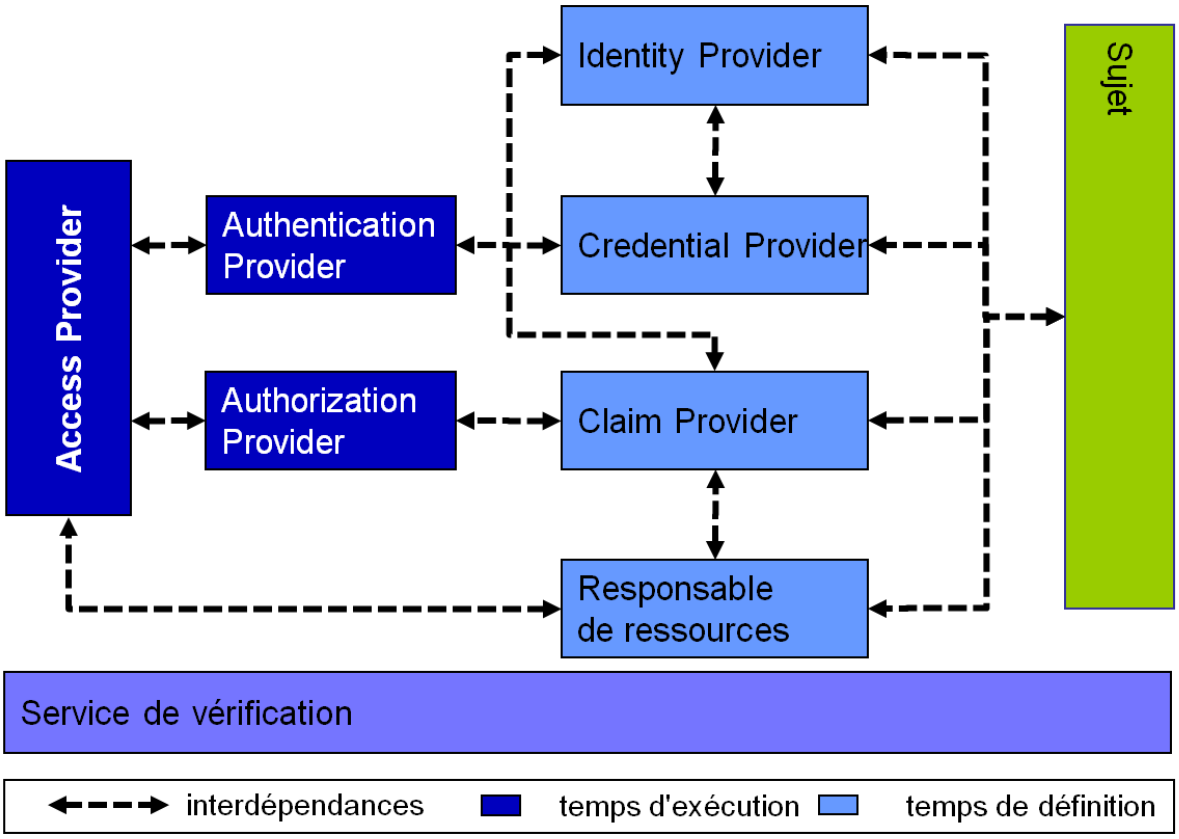

Illustration 1 : Structure organisationnelle

Processus du temps de définition
Pendant le temps de définition, toutes les conditions requises sont créées pour pouvoir définir au moment de l'accès si un sujet a le droit d'accès à une ressource. Le déroulement du "temps de définition" doit avoir lieu avant la première utilisation de la ressource par le sujet.

- L'Identity Provider garantit l'identification physique du sujet à l'aide des règles définies.
- En se basant sur l'identité, le Credential Provider met à disposition des Credentials.

- Le Claim Provider enregistre les informations dont il a besoin pour apporter la preuve qu'un sujet correspond bien aux Claims demandés en vue du temps d'exécution.

Processus du temps d'exécution
L'organisme responsable de l'accès au moment de l'exécution est l'Access Provider. Il contrôle l'accès à la ressource de façon centralisée. Pour cela, il a recours aux services mis à disposition par l'Authentication Provider et l'Authorization Provider.

Le graphique représente clairement l'interdépendance des Providers (lignes discontinues). Elles indiquent que les Providers du temps de définition mettent les données appropriées (certificats, Claims etc.) à la disposition des Providers du temps d'exécution.

Chacun des processus effectués peut être assuré par différents rôles, unités d'organisation, souvent même par des organisations (voir **Tableau 1**). Les chapitres suivants décrivent brièvement les tâches des différents rôles (et implicitement les processus).

Processus	**Rôles**
Temps de définition :	
Identity Management	Identity Provider
Credential Management	Credential Provider
Claim Management	Claim Provider
Gestion des droits	Responsable des ressources
Vérification de l'attribution des droits	Service de vérification de l'attribution des droits
Temps d'exécution :	
Utilisation des ressources	Sujet
Vérification de l'accès	Access Provider
Authentification	Authentication Provider
Autorisation	Authorization Provider

Tableau 1 : Processus IAM et rôles ou organismes correspondants

Relations de confiance (Trust-Relationships)

Comme les services de gestion sont fournis en règle générale par des organisations ou des unités d'organisation extérieures, les relations de confiance doivent être établies entre les différents Providers. L'établissement de ces relations de confiance est assuré habituellement

dans le cadre de la négociation des contrats correspondants. Ceux-ci dépassent souvent les limites du réseau. L'ensemble des protocoles d'authentification et d'autorisation intègre uniquement les services des Providers liés par une relation de confiance. Les indications des autres Providers ne sont pas acceptées.

3.2 Principes généraux de projet

Les processus et les fonctions liés à l'attribution d'identifiants, de Credentials, de Claims et de droits relatifs aux Claims peuvent être gérés indépendamment les uns des autres par différentes organisations et les ressources correspondantes peuvent être intégrées et administrées indépendamment les unes des autres sur le plan technique.

3.3 Identity Provider (IdP)

L'Identity Provider attribue des identités numériques.

Tâches :

- Gestion des identités avec des mesures appropriées pour éviter les doublons
- Mise à disposition d'un service d'information
- L'Identity Provider définit et publie:
    - les règles d'attribution, d'utilisation et de gestion des identités
    - la qualité de l'identification
    - le domaine de validité des identités attribuées
    - le processus d'identification
    - les conditions d'utilisation par les partenaires

Principes de conception :

- Il peut y avoir différents ID Managment Providers.
- L'ID-Provider peut choisir le type d'identifiant.
- Le service doit pouvoir être contrôlé et vérifié en permanence.

3.4 Credential Provider

Le Credential Provider fournit des moyens de vérifier les identités numériques.

Tâches :

- Mise à disposition des Credentials appropriés pour une identité
- Gestion du lien entre l'identité et ses Credentials

Principes de conception :

- Il peut y avoir différents Credential Providers.

- Les Credentials peuvent se différencier au regard de la conception technologique et du niveau de sécurité ainsi atteint. Le niveau de confiance et de sécurité des Credentials est défini et publié.
- Les processus d'attribution, après l'expiration et l'abus de Credentials, sont définis.

3.5 Claim Provider (CP)

Le Claim Provider gère les informations requises pour vérifier si un sujet correspond à un Claim à un moment donné.

Tâches :

- Gestion de la banque de données de Claims
- Vérification, enregistrement ou suppression de Claims, c.à.d. annonce qu'une certaine identité remplit un Claim défini.
- Certification des Claims gérée auprès des demandeurs autorisés
- Définition des processus d'attribution, après l'expiration et l'abus de Claims

Principes de conception :

- Le Trust Level attribué pour la certification des Claims est défini.

3.6 Authentication Provider

L'Authentication Provider met à disposition un service qui vérifie l'identité numérique à l'aide d'un Credential.

Tâches :

- Met à disposition un service électronique d'authentification (Authentication Service).
- Gère et documente les relations de confiance, auprès des Identity Providers et Credential Providers qu'il assiste
- Documente les Trust Levels qu'il a attribués et les technologies de sécurité.

Principes de conception :

- Pour fournir sa prestation, l'Authentication Provider collabore avec les Identity Providers et Credential Providers concernés.

3.7 Authorization Provider

L'Authorization Provider met à disposition un service qui vérifie si un sujet a le droit d'accéder à une ressource et dans quelles conditions.

Tâches :

- Met à disposition un service électronique en vue de l'autorisation.
- Gère les relations de confiance des Access Providers et des Claim Providers qu'il assiste
- Documente les Claims qu'il attribue
- Gère les exigences en termes d'autorisation en vue de l'accès aux ressources qu'il administre et qui lui sont signalées par les responsables des ressources.

Principes de conception :

- Attribution de Claims gérés par divers Claim Providers indépendants.
- Les règles d'autorisation sont définies exclusivement pour les Claims, jamais pour des sujets précis.

3.8 Access Provider

L'Access Provider met à disposition un service qui vérifie l'identité d'un demandeur pour le rediriger vers une ressource uniquement si ce demandeur a le droit d'y avoir accès.

Tâches :

- Met à disposition un service électronique - l'Access Service - qui garantit le respect des directives relatives à la sécurité de l'accès aux ressources utilisées.
- Gère les relations de confiance des Authentication Providers et des Authorization Providers qu'il assiste.
- Garantit, si nécessaire, le caractère complet des documentations de tous les accès (Auditing), ainsi que la qualité des Credential utilisés.

Principes de conception :

- L'Access Provider assiste les différents Identity Providers, Credential Providers et Claim Providers - au mieux, tous les Providers concernés.
- L'Access Provider attribue tous les Trust Levels courants.
- L'Access Provider attribue de façon idéale toutes les technologies de sécurité appropriées (p. ex. mots de passe, certificats électroniques, mots de passe uniques pour l'authentification).
- L'Access Provider peut occuper le rôle d'un Authentication Provider et d'un Authorization Provider.

3.9 Responsable des ressources

Le responsable des ressources définit qui a le droit d'avoir accès aux ressources.

Tâches :

- Le responsable des ressources est l'organisme responsable de l'attribution des droits aux Claims donnant accès aux ressources qu'il gère.

- Le responsable des ressources définit les exigences en termes de sécurité relative aux ressources qu'il gère et les signale à l'Authorization Provider.
  Il définit en particulier :
  - le Trust/Security Level requis pour une ressource,
  - à quel Identity Provider, Credential Provider et Claim Provider la ressource est confiée (c.-à-d. par quel organisme d'attribution les identités, les Credentials et les certifications de Claim seront acceptés),
  - à quel Claims un sujet doit correspondre, pour avoir le droit d'avoir accès à une ressource,
  - quels droits sont accordés en fonction des Claims, lors de l'accès à la ressource,
- Le responsable des ressources assure la convivialité de la présentation des conditions d'utilisation et de responsabilité, valables dans le cadre de l'utilisation de la ressource.

Principes de conception :

- Les droits sont toujours accordés exclusivement selon les Claims (ou une combinaison de ceux-ci), jamais directement à l'utilisateur.
- Les administrateurs sont soumis aux mêmes exigences en termes de sécurité (accès et autorisation) que les autres sujets. Des Claims spécifiques sont définis même pour les tâches de gestion. Ce principe est valable pour tous les sujets et les ressources, p. ex. pour les gestionnaires d'identités, de Credentials et de Claims.

3.10 Service de vérification de l'attribution des droits

Le service de vérification assure que les droits sont accordés de façon conforme aux directives relatives à la sécurité de l'accès, au-delà du système.

4 Architecture du système d'information

4.1 Architecture des données

Conformément à la notation UML [UML], le graphique suivant représente les principaux objets de données dans le domaine de l'IAM et autres domaines connexes :

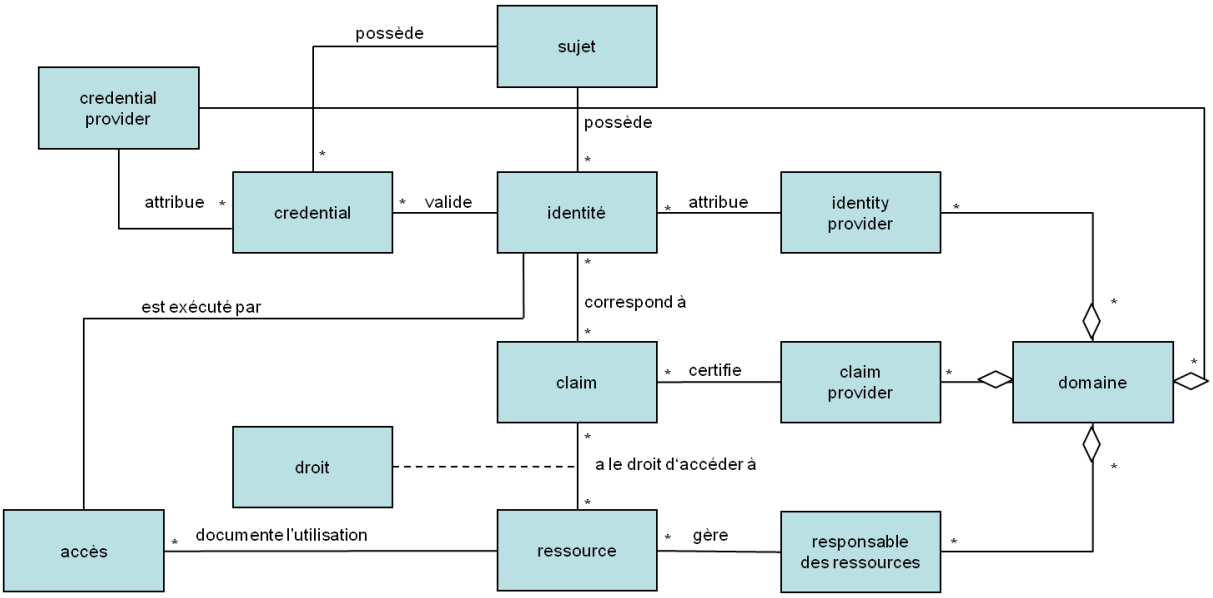

Illustration 2 : Architecture des données. *Une étoile signifie « 0 à plusieurs ». Une fin de ligne sans étoile signifie « exactement 1 ».*

Un sujet peut avoir plusieurs identités avec chacune un identifiant respectif. Chaque identifiant est attribué habituellement par un Identity Provider différent.

Pour chaque identité, un sujet peut avoir plusieurs Credentials, qui peuvent avoir différentes qualités (p. ex. mots de passe, certificats électroniques) et être attribués par des Providers ayant différentes règles de sécurité. Il faut observer que les Credentials peuvent aussi correspondre à des identités existantes, c.-à-d. que l'identification n'est nécessaire qu'une seule fois, toutefois, on peut utiliser un nombre quelconque de Credentials.

Un sujet correspond habituellement à plusieurs Claims, p. ex. il peut occuper différents rôles, qui, en règle générale, ne sont pas tous attribués (certifiés) par le même Claim Provider.

Les droits sont gérés par le responsable des ressources. Les droits définissent quel Claim (ou quelle combinaison de Claims) a le droit d'accéder à une ressource et dans quelles conditions.

Chaque accès d'un sujet à une ressource - dans la mesure où il y a une demande - est documenté. La somme des informations relatives à l'accès permet la vérification contrôlable et

exigée d'un point de vue légal. L'information relative à l'accès peut aussi être consultée à d'autres fins, p. ex. pour facturer les prestations et réaliser des statistiques.

Ces objets sont décrits de façon détaillée dans le chapitre 1.2.

4.2 Architecture des applications

4.2.1 Aperçu

L'architecture du système d'information est définie par les composants représentés sur l'illustration suivante. Il y a une claire distinction entre les services de gestion (représentés en bleu clair) et les services d'opération. Les services d'opération sont concernés en premier lieu pour autoriser l'accès à une ressource.

Dans certains cas, le sujet utilise un composant hardware (p. ex. Smartcard, Carte mémoire Memory Stick) pour enregistrer ses Credentials, impliquant la collaboration avec le Client pour l'utilisation d'un composant hardware.

Selon les fournisseurs, les services d'authentification et d'autorisation peuvent accéder directement (service synchrone) ou indirectement (le service de gestion fournit les données dans le cadre d'une réplication) aux services de gestion correspondants.

Dans ce cas, l'Access Service correspond au terme Policy Enforcement Point (PEP), souvent employé dans les ouvrages de références. Le PEP est chargé de garantir le respect de la Policy définie également par des moyens techniques (p. ex. par des protocoles sécurisés semblables à ceux utilisés dans le cadre de transactions etc.)

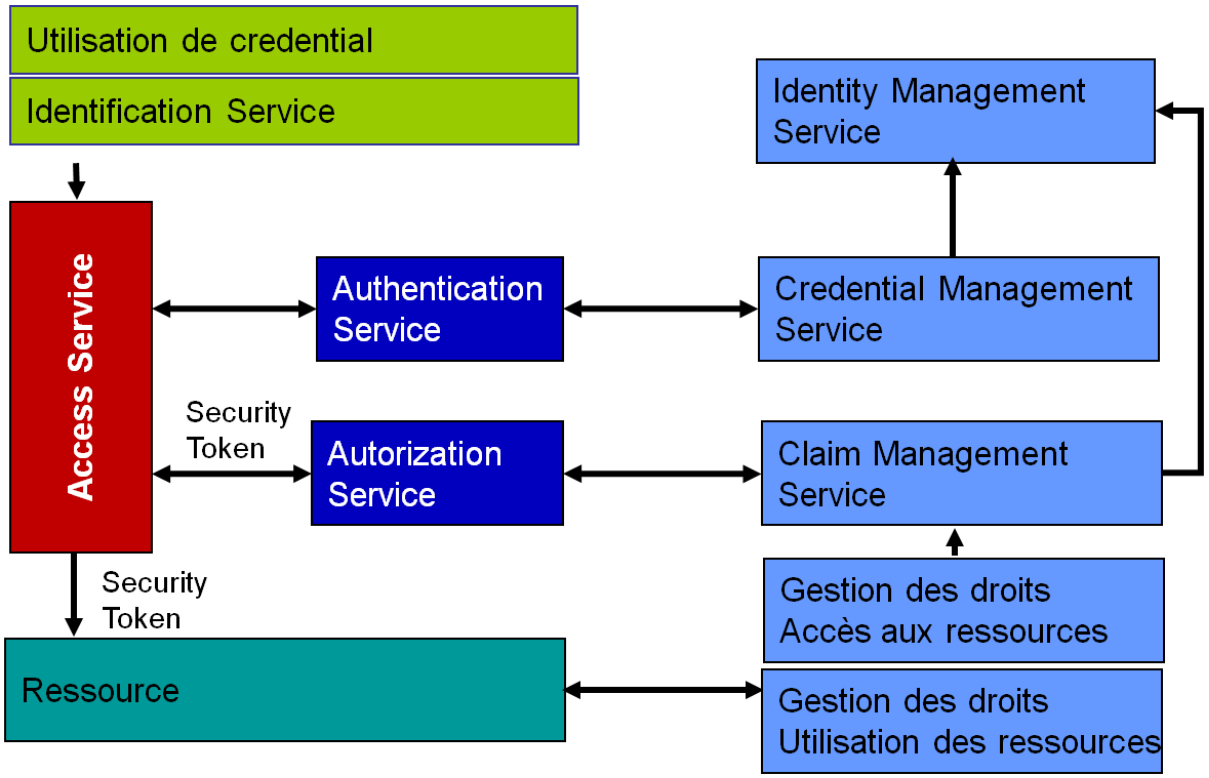

Illustration 3 : Architecture des applications

La gestion des droits contrôle, d'une part, l'accès à la ressource, et d'autre part, la granularité fine de l'accès aux fonctions mises à disposition par la ressource.

Les principes généraux de conception et les différents composants sont décrits en détail ci-dessous.

4.2.2 Principes généraux de conception

- Les infrastructures de l'IAM sont modulaires et scalables.
- Les services collaborent par l'intermédiaire d'interfaces standardisées qui utilisent des standards ouverts (p. ex. Security Assertion Markup Language' (SAML)).
- Pour l'authentification et l'autorisation sommaire, les ressources utilisent des services délocalisés.
- Les protocoles d'authentification nécessaires selon les exigences de l'utilisateur peuvent être effectués sur la même infrastructure de l'IAM.
- Les infrastructures existantes peuvent être intégrées.
- L'authentification et l'autorisation en vue de l'accès aux ressources reposent sur les identifiants, Credentials et Claims standardisés et certifiés selon le type d'application.
- Le nombre d'identifiants, de Credentials et de Claims utilisés doit être réduit au minimum et si possible consolidé :
    - Quand cela est possible, il faut utiliser en règle générale des identifiants, Credentials et Claims valables pour contrôler les droits d'accès.
    - Des concepts fédératifs permettent de construire les relations de confiance (Trusts) avec d'autres domaines et d'utiliser des identifiants, Credentials et Claims définis ailleurs.
- L'autorisation de l'accès à une ressource (dans la mesure où elle est nécessaire sur le plan technique) nécessite préalablement l'authentification du sujet demandant l'accès.
- Aucune information sur le sujet demandant l'accès n'est transmise à la ressource si cela n'est pas nécessaire techniquement. (Dans tous les cas, l'autorisation a lieu uniquement sur la base des Claims indiqués.)
- Afin d'encourager la réutilisation, l'accès aux données de type Claim doit s'effectuer par le biais d'interfaces et de protocoles standardisés.

4.2.3 Services de gestion

4.2.3.1 Identity Management Service

L'Identity Management Service délivre et gère des identités électroniques.

Tâches :

- Fournit des fonctions d'attribution et de gestion d'identités électroniques.
- Limite la durée de vie des identités électroniques.
- Donne aux Authentication Service Providers dignes de confiance au moins l'accès électronique aux informations relatives aux identités.

4.2.3.2 Credential Management Service

Le Credential Management Service délivre et gère des Credentials. Les Credentials peuvent être de différents types et sont attribués à un sujet défini.

Tâches :

- Fournit des fonctions d'attribution et de gestion des Credentials.
- Permet de vérifier la validité des Credentials gérés et l'appartenance à un identifiant.
- Limite la durée de vie des Credentials attribués.
- Donne aux Authentication Service Providers dignes de confiance au moins l'accès électronique aux informations relatives aux Credentials.

4.2.3.3 Claim Management Service

Le Claim Management Service documente un ou plusieurs Claims pour des sujets définis.

Tâches :

- Fournit des fonctions de gestion des informations nécessaires pour pouvoir définir de manière incontestable si un sujet (précisément : l'identifiant d'un sujet) correspond à un Claim défini (p. ex. "Hans Meier est géomètre pour le canton de Berne").
- Certifie par voie électronique l'attribution ou la non-attribution d'un Claim défini à un sujet (précisément : l'identifiant d'un sujet).
- Donne aux Authorization Providers dignes de confiance au moins l'accès électronique aux informations relatives aux Claims gérés.

4.2.3.4 Gestion des droits pour l’accès aux ressources

La gestion des droits pour l’accès aux ressources administre les droits d'accès à une ressource, c.-à-d. les indications qui doivent être remplies par les Claims pour qu’un sujet puisse accéder à une ressource (autorisation sommaire).

Tâches :

- Fournit des fonctions de gestion des informations sur les Claims qui sont autorisé à accéder aux ressources définies.
- Donne aux Authorization Services dignes de confiance l'accès électronique aux informations relatives aux autorisations gérées.

4.2.3.5 Gestion des droits, utilisation des ressources

La gestion des droits pour l'utilisation des ressources définit quels Claims/rôles peuvent appeler quelles fonctions des ressources (autorisation fine).

Tâches :

- Met à disposition les fonctions pour la gestion des informations sur les Claims qui doivent être remplis par un sujet pour pouvoir accéder à la fonction de la ressource correspondante.
- Garantit l'accès électronique à la ressource pour les informations d'autorisation concernées.

4.2.4 Access Services

4.2.4.1 Client

Le Client accède à une ressource et vérifie l'identité du sujet demandant l'accès, dans la mesure où cela est nécessaire. Il délègue l'authentification à un service d'identification ou assure lui-même ces tâches.

Interface :

Out : Identifiant, Credential, [Claims]

Tâches :

- En option : appelle le service d'identification en vue de l'authentification.
- Appelle la ressource et lui transmet l'identifiant et le Credential, éventuellement les Claims certifiés du sujet demandant l'accès.
- Si le Client est une interface utilisateur :
  publie les conditions de responsabilité lors du Login, si exigé.

4.2.4.2 Service d'identification

Le service d'identification permet au sujet de s'authentifier, par exemple en demandant son identifiant d'utilisateur et son mot de passe ou un mot de passe unique, ou en lisant les informations nécessaires à partir d'un Smartcard.

Interface :

Out : identificateur, Credential, [Claims]

Tâches :

- En option : demande la ressource à appeler, pour laquelle les Claims et les Trust / Security –levels sont nécessaires pour l'accès.
- Authentifie le sujet conformément au Trust / Security –level (par ex. grâce au log-in).

- Dans le cas où il s'agit d'une interface-utilisateur chez le Client :
  Publie les dispositions de responsabilité lors du Login, si exigé.

4.2.4.3 Access Service

L'Access Service vérifie l'identité du sujet demandant l'accès et refuse l'accès si le sujet n'y a pas droit.

Interface :

In : Identifiant, Credential, [Claims], Ressource

Out : Security Token

Tâches :

- Fournit au Client sur demande les informations nécessaires relatives à la sécurité de l'accès (p. ex. les Claims nécessaires, le Trust Level exigé).
- Appelle un service d'authentification et annule l'opération si l'authentification a échouée.
- Appelle un service d'autorisation pour vérifier l'autorisation et annule l'opération si aucun Claim avec droit d'accès à la ressource n'a été trouvé pour le sujet demandant l'accès (l'identifiant représenté par le sujet).
- Transmet à la ressource à appeler, dans le Security Token, les informations relatives à l'authentification et à l'autorisation vérifiées.
- Crée et gère les informations relatives à l'accès en vue d'un contrôle, si exigé. Ces informations contiennent toutes les données requises pour une clarté entière. Ces informations peuvent être consultées en cas de besoin à des fins de facturation.
- Fournit des fonctions d'Audit et de Monitoring vérifiées et vérifiables.
- Collabore éventuellement avec le service de gestion des licences, p. ex. pour refuser l'accès, si le nombre maximum de Concurrent User est atteint.

Principes de conception

- Si le sujet ne dispose pas du droit d'utilisation de l'application à appeler, l'appel n'est pas transmis à la ressource.
- L'Access Service fonctionne au-delà des limites des réseaux et des domaines.
- Il peut être utilisé pour sécuriser l'accès aux ressources les plus différentes.
- En cas de besoin, il peut collaborer avec plusieurs services d'authentification et d'autorisation.
- Dans la mesure où cela est possible en considérant le Trust-Level, les identités, Credentials et Claims existants peuvent être gérés par d'autres organismes (fédération).

4.2.4.4 Service d'authentification

Le service d'authentification vérifie à l'aide des Credentials si le sujet demandant l'accès est bien celui qu'il prétend être.

Interface :

In : Identifiant, Credentials

Out : Identité vérifiée, indique si la vérification de l'identité est positive ou non.

Tâches :

- Vérifie si les Credentials fournis correspondent à l'identité de l'identifiant fourni.
- Certifie l'identité du sujet demandant l'accès en cas de réponse positive.

4.2.4.5 Service d'autorisation

Le service d'autorisation vérifie que le demandeur a le droit d'accéder à la ressource.

Interface :

In : Id vérifiée, Credentials, Ressource, [Claims]

Out : Security Token (avec toutes les informations nécessaires pour accéder à la ressource, en particulier les certifications de Claims)

Tâches :

- Cherche les Claims qui ont accès à la ressource (dans la mesure où ils ne sont pas transmis comme paramètres de saisie).
- Vérifie que l'Id vérifiée correspond à un ou plusieurs des Claims exigés par la ressource.
- Crée un Security Token pour le sujet avec l'Id vérifiée et les Claims certifiés nécessaires à l'accès.
- Limite la durée de vie du Security Token.

Principes de conception

- Des Claims (rôles ou attributs) sont acceptés par différents services de gestion des Claims.
- Si la ressource n'exige pas de connaître le sujet demandant l'accès, l'Id n'est pas enregistrée dans le Security Token.

4.2.4.6 Ressource

La ressource permet au sujet d'accéder à autant de fonctions qu'il peut utiliser selon les droits qui lui sont accordés.

Interface :

In : Security Token (avec toutes les informations nécessaires pour accéder à la ressource, en particulier les certifications de Claims)

Tâches :

- La ressource obtient un Security Token standardisé sur lequel elle se base pour procéder à l'accès précis. Elle empêche l'accès à un sujet lorsque celui-ci ne dispose pas du droit d'accès en raison des informations fournies dans le Security Token.

- Les fonctionnalités de l'authentification et de l'autorisation sont indépendantes de la ressource appelée.
- Les autorisations sont définies exclusivement par rapport aux Claims transmis à la ressource.
- La ressource fournit - si nécessaire - des fonctions d'Audit et de Monitoring vérifiées et vérifiables.

Remarques :

Comme la ressource est appelée par l'intermédiaire d'interfaces et de Security Token standard, elle peut être intégrée dans les portails, si nécessaire.

5 Domaines et leur interaction

La cyberadministration requiert la collaboration électronique au-delà des frontières organisationnelles. Il existe une possibilité de résoudre les problèmes IAM en distinguant séparément chaque sujet avec un identifiant dans chaque contexte d'application, en lui attribuant un propre Credential et en lui affectant les Claims/rôles pertinents.
Chaque contexte d'application est considéré en tant que *domaine* propre et isolé (un « silo »). L'étendue augmente ainsi pour tous les intéressés. Les sujets doivent contourner une multitude d'identités et de Credentials. L'envergure de la gestion pour les droits est alors énorme. En même temps, le risque d'erreurs et d'abus augmente.

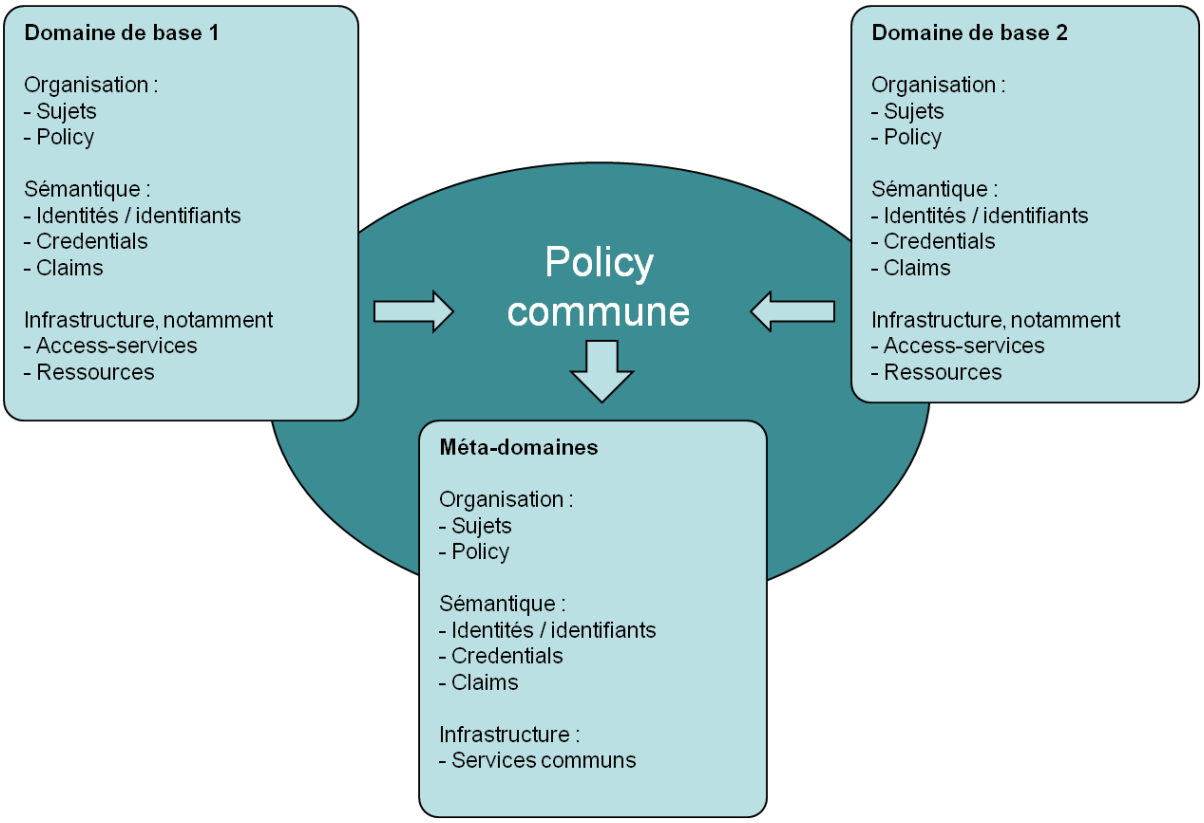

Illustration 4 : Domaines et leur interaction

Une autre approche de solution est privilégiée dans la plupart des cas (cf. illustration 1) : si différentes organisation souhaitent travailler ensemble, elles déterminent une Policy commune, selon les définitions existantes (notamment Identités, Credentials et Claims) qu'elles souhaitent utiliser ensemble. C'est-à-dire qu'elles forment un méta-domaine commun avec une Policy propre, qui a caractère obligatoire pour tous les intéressés. Le méta-domaine régit, entre autres, les points suivants :

- Quels sujets appartiennent au domaine ?
- Comment les sujets des domaines sont-ils identifiés de manière unique ?
- Quels Credentials de quelle qualité seront acceptés pour l'authentification des sujets ?
- Quels Claims de quelle qualité seront nécessaires pour les accès aux ressources ?
- À quelle identité, Credential et Claim Provider fera t-on confiance ?

5.1 Principes de conception

- La Policy d'un domaine doit être consignée par écrit et être publiée et accessible pour tous les participants du domaine.
- La quantité des domaines doit être maintenue au minium. Lorsque cela est possible, il faut se rattacher à un domaine supérieur déjà existant au lieu d'en créer un nouveau.

- Lorsque cela est possible, les identités, Credentials et Claims déjà existants doivent être réutilisés (par ex. fédération, méta-directory commun…)
- Lorsque cela est possible, les identités, Credentials et Claim-Provider déjà existants doivent être pris en compte.

6 Mise en œuvre

Les présents principes du projet décrivent, comme le titre l'indique, la façon dont une cyber-administration compatible avec un système IAM doit être administrée. Ces principes ne décrivent pas une solution concrète. Lors de la mise en œuvre, une série de résultats supplémentaires doit être établie, entre autres :

- Définitions des exigences mesurables
- Concept de protection et de sécurité des données
- Concepts des rôles
- Policies
- Structure des solutions.

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 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

[IAM Wiki] www.iam-wiki.org

[UML] http://www.uml.org/

[TOGAF] http://www.opengroup.org/togaf/

Annexe B – Collaboration & contrôle

Fischer Markus	
Gantenbein Reto	Sun Microsystems (Suisse) AG
Häni Hans	TG
Itin Markus	ZH
Jensen Rüdiger	Swisstopo
Lambelet Erich	BEDAG
Lippuner Mathias	SG
Mathys Wolfram	BEDAG
Meyer Elias	Abraxas
Müller Willy	ISB
Ottinger Vincent	Genève
Perroud Thierry	BIT
Petralia Andreas	Adnovum
Ueltschi Andreas	Sun/Oracle

Annexe C – Abréviations

IAM	Identity und Access Management
IdP	Identity Provider
CP	Credential Provider
UML	Unified Modelling Language
PEP	Policy Enforcement Point
SAML	Security Assertion Markup Language
TOGAF.	The Open Group Architecture Framework

Annexe D – Glossaire

Voir chap. 1.2