

## eCH-0219 – Glossaire IAM

<b>Nom</b>	Glossaire IAM
<b>eCH-nombre</b>	eCH-0219
<b>Catégorie</b>	Norme
<b>Stade</b>	Défini
<b>Version</b>	2.0.0
<b>Statut</b>	Approuvé
<b>Date de décision</b>	2025-12-11
<b>Date de publication</b>	2025-10-16
<b>Remplace la version</b>	1.0 – Major Change
<b>Conditions préalables</b>	---
<b>Annexes</b>	---
<b>Langues</b>	Allemand (original), français (traduction)
<b>Groupe spécialisé</b>	IAM
<b>Éditeur / distribution</b>	Association eCH, Affolternstrasse 52, 8050 Zurich T 44 388 74 64 / <a href="mailto:info@ech.ch">info@ech.ch</a> / <a href="http://www.ech.ch">www.ech.ch</a>

### Condensé

La présente norme définit les termes les plus importants pour les solutions IAM dans la cyberadministration fédérale suisse. L'ensemble des normes eCH relatives aux domaines IAM s'appuient sur cette norme.

Les termes intégrés incluent les Stakeholders, les processus, les services jusqu'aux détails d'implémentation dans les solutions IAM fédérées et non fédérées. Les termes tirés de normes internationales actuelles sont mis en relation avec la terminologie définie dans un souci d'intelligibilité.

La version 2.0.0 contient aussi des termes relatifs aux identités décentralisées et aux Self-Sovereign Identities (SSI).

## Table des matières

<b>1</b>	<b>Introduction .....</b>	<b>8</b>
<b>1.1</b>	<b>Statut .....</b>	<b>8</b>
<b>1.2</b>	<b>Champ d'application.....</b>	<b>8</b>
<b>1.3</b>	<b>Délimitation .....</b>	<b>8</b>
<b>1.4</b>	<b>Caractère normatif des chapitres .....</b>	<b>8</b>
<b>2</b>	<b>Terminologie.....</b>	<b>9</b>
<b>2.1</b>	<b>Abonné/e .....</b>	<b>9</b>
<b>2.2</b>	<b>Acteur .....</b>	<b>9</b>
<b>2.3</b>	<b>Requérant/e.....</b>	<b>9</b>
<b>2.4</b>	<b>Attribut.....</b>	<b>9</b>
<b>2.5</b>	<b>Contrôle des accès basés sur les attributs (ABAC).....</b>	<b>10</b>
<b>2.6</b>	<b>Confirmation d'attributs .....</b>	<b>10</b>
<b>2.7</b>	<b>Attribute Assertion Service.....</b>	<b>11</b>
<b>2.8</b>	<b>Attribute Provider (AP).....</b>	<b>11</b>
<b>2.9</b>	<b>Attribute Service .....</b>	<b>11</b>
<b>2.10</b>	<b>Auditing.....</b>	<b>11</b>
<b>2.11</b>	<b>Authentication Proxy.....</b>	<b>11</b>
<b>2.12</b>	<b>Authentication Service .....</b>	<b>11</b>
<b>2.13</b>	<b>Authentification .....</b>	<b>12</b>
<b>2.14</b>	<b>Confirmation d'authentification.....</b>	<b>12</b>
<b>2.15</b>	<b>Moyen d'authentification.....</b>	<b>12</b>
<b>2.16</b>	<b>Authorization Service .....</b>	<b>14</b>
<b>2.17</b>	<b>Autorisation.....</b>	<b>14</b>
<b>2.18</b>	<b>Autorité.....</b>	<b>14</b>
<b>2.19</b>	<b>Utilisateur/trice.....</b>	<b>15</b>
<b>2.20</b>	<b>User Account .....</b>	<b>15</b>
<b>2.21</b>	<b>Autorisation.....</b>	<b>15</b>
<b>2.22</b>	<b>Moyen de preuve .....</b>	<b>15</b>
<b>2.23</b>	<b>Caractéristique biométrique .....</b>	<b>15</b>

<b>2.24 Broker Service</b> .....	<b>16</b>
<b>2.25 Certificate Policy (CP)</b> .....	<b>16</b>
<b>2.26 Certificate Revocation List (CRL)</b> .....	<b>17</b>
<b>2.27 Certification Authority (CA)</b> .....	<b>17</b>
<b>2.28 Certification Practice Statement</b> .....	<b>17</b>
<b>2.29 Challenge Response</b> .....	<b>17</b>
<b>2.30 Claim</b> .....	<b>17</b>
<b>2.31 Client Platform</b> .....	<b>18</b>
<b>2.32 Credential</b> .....	<b>18</b>
<b>2.33 Credential Service</b> .....	<b>19</b>
<b>2.34 Période de définition</b> .....	<b>19</b>
<b>2.35 Identité décentralisée</b> .....	<b>19</b>
<b>2.36 Prestataire de services</b> .....	<b>19</b>
<b>2.37 Identité numérique</b> .....	<b>19</b>
<b>2.38 Processus numérique</b> .....	<b>20</b>
<b>2.39 Digitale Ressource</b> .....	<b>20</b>
<b>2.40 Digital Resource Service</b> .....	<b>20</b>
<b>2.41 Signature numérique</b> .....	<b>20</b>
<b>2.42 Certificat numérique</b> .....	<b>21</b>
<b>2.43 Digital Identity Service</b> .....	<b>21</b>
<b>2.44 Chose</b> .....	<b>21</b>
<b>2.45 Discovery Service</b> .....	<b>21</b>
<b>2.46 Domaine</b> .....	<b>21</b>
<b>2.47 Propriété</b> .....	<b>21</b>
<b>2.48 Mot de passe à usage unique</b> .....	<b>22</b>
<b>2.49 Signature électronique</b> .....	<b>22</b>
<b>2.50 Moyen d'identification électronique</b> .....	<b>22</b>
<b>2.51 Système d'identification électronique</b> .....	<b>22</b>
<b>2.52 Cachet électronique</b> .....	<b>22</b>
<b>2.53 Entité</b> .....	<b>23</b>
<b>2.54 Management</b> .....	<b>23</b>
<b>2.55 Lien avec le dispositif</b> .....	<b>23</b>

2.56	Certificat règlementé .....	23
2.57	Holder .....	24
2.58	Holder of Key (HoK).....	24
2.59	Architecture IAM .....	24
2.60	Prestataire de services IAM .....	24
2.61	IAM Management .....	25
2.62	IAM Policy .....	25
2.63	IAM Regulator .....	25
2.64	Service IAM .....	25
2.65	IAM Support .....	26
2.66	Système IAM .....	26
2.67	Identificateur .....	26
2.68	Identification .....	26
2.69	Identité.....	26
2.70	Document d'identité .....	27
2.71	Fédération d'identité.....	28
2.72	Identity and Access Management (IAM).....	29
2.73	Identity Linking .....	29
2.74	Identity Mapping .....	29
2.75	Identity Provider (IdP).....	29
2.76	Lien avec le détenteur .....	30
2.77	Institution .....	30
2.78	Issuer.....	30
2.79	Personne morale.....	30
2.80	Kerberos.....	30
2.81	Caractéristique physique .....	31
2.82	Token cryptographique .....	31
2.83	Période d'exécution.....	31
2.84	Linking Protocole.....	31
2.85	Bénéficiaire de prestations (BP) .....	31
2.86	Fournisseur de prestations (FP) .....	31
2.87	Logging Service.....	32

<b>2.88 Look-Up Secret .....</b>	<b>32</b>
<b>2.89 Magic Link .....</b>	<b>32</b>
<b>2.90 Memorized Secret .....</b>	<b>32</b>
<b>2.91 Méta-attribut .....</b>	<b>33</b>
<b>2.92 Métadonnées .....</b>	<b>33</b>
<b>2.93 Espace de nom .....</b>	<b>33</b>
<b>2.94 Personnes physiques .....</b>	<b>33</b>
<b>2.95 Réseau .....</b>	<b>34</b>
<b>2.96 Non-réputabilité .....</b>	<b>34</b>
<b>2.97 OAuth 2.0 .....</b>	<b>34</b>
<b>2.98 Objet .....</b>	<b>34</b>
<b>2.99 Online Certificate Status Protocol (OCSP) .....</b>	<b>34</b>
<b>2.100 OpenID Connect (OIDC) .....</b>	<b>34</b>
<b>2.101 Organisation .....</b>	<b>35</b>
<b>2.102 OTP-Device .....</b>	<b>35</b>
<b>2.103 Out-of-Band Authenticator .....</b>	<b>35</b>
<b>2.104 Passkey .....</b>	<b>36</b>
<b>2.105 Mot de passe .....</b>	<b>36</b>
<b>2.106 Authentification sans mot de passe .....</b>	<b>36</b>
<b>2.107 Pièce d'identité physique .....</b>	<b>37</b>
<b>2.108 Policy .....</b>	<b>37</b>
<b>2.109 Provisionnement .....</b>	<b>37</b>
<b>2.110 Processus .....</b>	<b>37</b>
<b>2.111 Messages push .....</b>	<b>37</b>
<b>2.112 Signature électronique qualifiée (QES) .....</b>	<b>38</b>
<b>2.113 Certificat qualifié .....</b>	<b>38</b>
<b>2.114 Droits .....</b>	<b>38</b>
<b>2.115 Registre .....</b>	<b>38</b>
<b>2.116 Enregistrement .....</b>	<b>38</b>
<b>2.117 Service d'enregistrement / Registration Authority (RA) .....</b>	<b>38</b>
<b>2.118 Regulator .....</b>	<b>39</b>
<b>2.119 Relying Party (RP) .....</b>	<b>39</b>

<b>2.120 Ressource</b> .....	<b>39</b>
<b>2.121 Responsable des ressources</b> .....	<b>39</b>
<b>2.122 Rôle</b> .....	<b>39</b>
<b>2.123 Contrôle des accès basé sur les rôles (RBAC)</b> .....	<b>40</b>
<b>2.124 Security Assertion Markup Language (SAML)</b> .....	<b>40</b>
<b>2.125 Security Token</b> .....	<b>40</b>
<b>2.126 Security Token Service</b> .....	<b>40</b>
<b>2.127 Divulgence sélective</b> .....	<b>40</b>
<b>2.128 Self-Sovereign Identity (SSI)</b> .....	<b>41</b>
<b>2.129 Service</b> .....	<b>41</b>
<b>2.130 Service Level Agreement (SLA)</b> .....	<b>41</b>
<b>2.131 Single Sign-On (SSO)</b> .....	<b>41</b>
<b>2.132 Identité électronique reconnue par l'État (E-ID)</b> .....	<b>41</b>
<b>2.133 Stakeholder</b> .....	<b>42</b>
<b>2.134 Sujet</b> .....	<b>42</b>
<b>2.135 Topologie</b> .....	<b>43</b>
<b>2.136 Trust Service</b> .....	<b>44</b>
<b>2.137 Trusted Third Party</b> .....	<b>44</b>
<b>2.138 Unité IDE</b> .....	<b>44</b>
<b>2.139 Porteur/porteuse</b> .....	<b>44</b>
<b>2.140 Verifiable Credential (VC)</b> .....	<b>45</b>
<b>2.141 Verifiable Data Registry</b> .....	<b>45</b>
<b>2.142 Verifiable Presentation (VP)</b> .....	<b>45</b>
<b>2.143 Verifier</b> .....	<b>46</b>
<b>2.144 Source faisant autorité</b> .....	<b>46</b>
<b>2.145 Broker</b> .....	<b>46</b>
<b>2.146 Confiance</b> .....	<b>47</b>
<b>2.147 Niveau de confiance</b> .....	<b>47</b>
<b>2.148 Wallet</b> .....	<b>47</b>
<b>2.149 Révocation</b> .....	<b>47</b>
<b>2.150 Service droit d'accès</b> .....	<b>48</b>
<b>2.151 Contrôle d'accès</b> .....	<b>48</b>

<b>2.152Zero-Knowledge Proof (ZKP) .....</b>	<b>48</b>
<b>3 Exclusion de responsabilité – droits de tiers .....</b>	<b>49</b>
<b>4 Droits d’auteur.....</b>	<b>49</b>
<b>Annexe A – Références &amp; bibliographie .....</b>	<b>50</b>
<b>Annexe B – Collaboration &amp; vérification.....</b>	<b>52</b>
<b>Annexe C – Abréviations et glossaire.....</b>	<b>52</b>
<b>Annexe D – Modifications par rapport à la version précédente .....</b>	<b>54</b>
<b>Annexe E – Liste des illustrations.....</b>	<b>56</b>
<b>Annexe F – Liste des tableaux.....</b>	<b>56</b>

## Remarque

La formulation employée dans le présent document pour désigner les personnes est neutre en termes de genre. Elle repose sur le [guide](#) de la Chancellerie fédérale. On recourt, selon la situation, à des doublets intégraux (citoyens et citoyennes), à des formes abstraites en termes de genre (personne assurée), à des formes neutres du point de vue du genre (les assurés) ou à des périphrases dépourvues de référence à la personne. L’utilisation du masculin générique (citoyens) n’est plus admise. Les formes intégrales sont employées dans les textes continus, autrement dit les textes constitués de phrases rédigées. Les formes abrégées sont acceptées dans les passages de texte concis, les tableaux par exemple. On utilise alors la forme courte avec barre oblique, toutefois sans tiret (référent/e). Les points médians et autres caractères similaires sont proscrits.

# 1 Introduction

L'Identity and Access Management (IAM) est un élément central de la sécurité informatique et régit l'accès aux ressources dans les processus électroniques. Un système IAM performant garantit que seules les personnes ou services authentifiés et/ou autorisés sont en mesure d'accéder aux ressources sensibles. Il faut pour ce faire gérer les identités et les autorisations.

Cette norme définit les termes et notions fondamentales dans le domaine de l'IAM, servant ainsi de base à tous ceux qui élaborent des solutions dans le domaine de la cyberadministration.

## 1.1 Statut

Approuvé: le document a été approuvé par le Comité des experts. Il a pouvoir normatif pour le domaine d'utilisation défini dans le domaine de validité donné.

## 1.2 Champ d'application

Les concepts et termes définis dans la présente norme offrent une synthèse terminologique des normes eCH existantes dans le domaine de l'IAM, qu'ils viennent consolider. Les termes intégrés incluent les Stakeholders, processus, services jusqu'aux détails de mise en œuvre dans les solutions IAM fédérées, non fédérées et décentralisées.

La norme s'adresse à tous ceux et celles qui sont en contact avec l'IAM, du développeur à l'architecte en passant par la direction.

## 1.3 Délimitation

Les termes du présent glossaire sont définis dans le contexte de la gestion des identités et des accès (Identity and Access Management, IAM). Les modes de lecture de termes sortant du cadre de l'IAM ne sont pas pris en compte.

## 1.4 Caractère normatif des chapitres

Les chapitres dans la présente norme sont de nature normative ou descriptive. Le tableau suivant en définit la classification.

Chapitre	Description
<b>1 Introduction</b>	<b>Descriptif</b>
<b>2 Terminologie</b>	<b>Normatif</b>

L'annexe A et l'annexe C sont elles aussi de nature normative. Toutes les autres annexes de cette norme sont descriptives

## 2 Terminologie

### 2.1 Abonné/e

Un **abonné** ou une **abonnée** [1] est un *sujet*, qui au terme d'un processus *d'enregistrement* mené avec succès devient un *acteur* dans le *système IAM*.

Synonyme: Subscriber (angl.)

### 2.2 Acteur

Un **acteur** [2] est une *entité* ou un *sujet* dans un *système IAM*, qui exécute des *processus*. Un acteur est motivé par un ou plusieurs *stakeholders*.

Les acteurs sont notamment:

- *Sujet*,
- *Relying Party*,
- *Prestataire de services IAM*,
- *IAM Management*
- *IAM Support*,
- *IAM Regulator*.

### 2.3 Requérant/e

Un **requérant** ou un **requérante** [1] est un *objet*, qui souhaite être intégré à un *système IAM* et passe à cet effet par la procédure *d'enregistrement*. Si cette dernière est acceptée, le requérant ou la requérante devient *abonné* respectivement *abonnée*.

Synonyme: Applicant (angl.)

### 2.4 Attribut

Un **attribut** est une représentation numérique d'une *propriété* prêtée à un *sujet*, qui décrit le sujet plus en détail.

Un attribut se compose des *méta-attributs suivants*: nom de l'attribut (par ex. «pointure»), type de données d'attribut (par ex. «nombre entier») et valeur d'attribut (par ex. «39»).

Un *identificateur* est un attribut utilisé de manière spécifique.

Les attributs peuvent être déclinés en différents groupes, qui peuvent parfois se recouper:

- **Attributs d'identification et de description du sujet:**
  - Identificateur et clé étrangère,
  - Attributs d'identification du sujet, par ex. nom, sexe, date de naissance, ...
  - Attributs de communication, tels qu'adresse e-mail, numéro de téléphone, adresse postale, ...
  - Attributs biométriques, tels que photographies, ...
  - ...
- **Attributs d'authentification:** Il s'agit notamment des *Credentials* ou des références aux *Credentials*.
- **Attributs pertinents pour l'autorisation:** il s'agit de tous les attributs utiles pour une décision d'autorisation, dont:
  - Attributs contextuels décrivant la classification dans une organisation,
  - Attributs de rôle qui décrivent la fonction dans une organisation (contexte),
  - ...
- **Attributs de métadonnées:** Informations concernant la saisie de données, le statut et la validité.

Les attributs peuvent être définis et gérés dans le système IAM lui-même ou dans des systèmes associés, par ex. dans un système HR ou CRM.

Synonyme: *Claim*

## 2.5 Contrôle des accès basés sur les attributs (ABAC)

Le **contrôle des accès basés sur les attributs (ABAC)** [3] désigne un type de *contrôle d'accès*, au moyen duquel un *Relying Party* autorise l'accès à une *Ressource* sur la base d'un ou de plusieurs *Attributes* du *sujet*.

Synonyme: Attribute based Access Control (angl.)

## 2.6 Confirmation d'attributs

Une **confirmation d'attribut** est une confirmation de la valeur d'un *attribut* pour un *sujet* par un *Attribute Provider (AP)*, un *IdP* ou un *Issuer*.

Les confirmations d'attributs sont fréquemment délivrées en même temps que les *confirmations d'authentification*, une fois l'*authentification* du sujet réussie.

Exemples:

- *SAML*: SAML 2.0 Attribute Assertion [4]
- *OIDC*: *Claims* dans l'*ID-Token*,
- *SSI*: *Claims* dans *Verifiable Credentials*

Synonyme: Attribute Assertion (angl.), confirmation des valeurs d'attribut

## 2.7 Attribute Assertion Service

Un **Attribute Assertion Service** [2] est un *service IAM*, qui émet des *confirmations d'attributs* via une interface définie.

Synonyme: Service de confirmation des attributs

## 2.8 Attribute Provider (AP)

Un **Attribute Provider** est une *entité*, la plupart du temps un *registre* ou un autre répertoire, avec un *Attribute Service* pour gérer les *attributs* et un *Attribute Assertion Service* pour la délivrance de *confirmations d'attributs*.

Synonymes: Attribute Authority (AA), fournisseur de données, fournisseur d'informations, OIDC Claims Provider

## 2.9 Attribute Service

L'**Attribute Service** [2] est un *service IAM*, compétent pour la mise à jour en temps réel des *attributs* pour des *sujets* définis.

## 2.10 Auditing

L'**auditing** désigne le processus continu ou périodique de vérification systématique des *processus* ou systèmes visant à s'assurer de leur conformité avec les directives, des normes ou exigences légales.

Dans le contexte de l'IAM, l'auditing couvre par exemple la consignation et l'analyse des activités des utilisateurs, des accès au système ou encore des événements affectant la sécurité, en vue de détecter les activités douteuses, de veiller au respect des directives de sécurité ou de satisfaire à des exigences légales.

## 2.11 Authentication Proxy

Un **Authentication Proxy** associe deux sections de protocole, constituant ainsi un point final de protocole. Il peut transformer et transférer les demandes et réponses d'authentification. L'Authentication Proxy peut être une partie d'un *Broker*.

## 2.12 Authentication Service

L'**Authentication Service** [2] est un *service IAM* et une partie intégrante du *Verifier*. Il se charge de comparer les moyens *d'authentification* présentés aux *Credentials* enregistrés et est ainsi en mesure de déterminer si le ou les accédants (*sujet*) possède bien *l'identité numérique* prétendue.

## 2.13 Authentification

L'**authentification** est le processus de vérification d'une *identité numérique* prétendue d'un *sujet* en suivant des règles précises. Le *niveau de confiance* visé de l'authentification détermine les règles en question.

Ce faisant, un ou plusieurs *moyens d'authentification* utilisés concernant l'identité numérique prétendue font l'objet d'une vérification de validité. Il est alors déterminé si le *sujet* qui tente d'accéder à un *Relying Party* contrôle bien les secrets utilisés à des fins d'authentification.

À l'heure actuelle, *l'authentification sans mot de passe* a le vent en poupe dans l'optique d'améliorer la convivialité.

Synonymes: Authentification<sup>1</sup>

## 2.14 Confirmation d'authentification

Une **confirmation d'authentification** est un justificatif numérique délivrée par un *Identity Provider* (IdP) suite au succès d'une *authentification* du *sujet*. La confirmation d'authentification a une validité courant sur une période déterminée et peut spécifier le contexte d'authentification ou un *niveau de confiance*.

Exemples:

- Dans le cas du *SAML*, la confirmation d'authentification correspond à «l'Authentication Assertion», elle est délivrée par l'Identity Provider (SAML).
- Dans la cas de *l'OIDC*, la confirmation d'authentification est «l'ID Token», elle est délivrée par «l'Authorization Server».
- Dans le cas de *Kerberos*, la confirmation d'authentification est un «Ticket Granting Ticket» (TGT), elle est délivrée par le *Kerberos Distribution Center* (KDC).

## 2.15 Moyen d'authentification

Les **moyens d'authentification** sont des informations et/ou des *processus* pouvant être utilisés à des fins d'*authentification* d'un *sujet*. Les moyens d'authentification peuvent être fondés sur différents caractères:

- Basé sur la connaissance: repose sur la connaissance (par ex. quelque chose que le sujet sait/connait, *mot de passe*, PIN)
- Basé sur la possession: repose sur la possession (par ex. quelque chose que possède le sujet, Soft Token/Hardware Token avec clé privée, passeport ou carte d'identité électronique)
- *Caractéristique* du sujet: repose sur une *caractéristique biométrique*,
- Basé sur le comportement (rarement employé): repose sur le comportement (quelque chose qui singularise le sujet, une façon de signer dynamique par exemple).

---

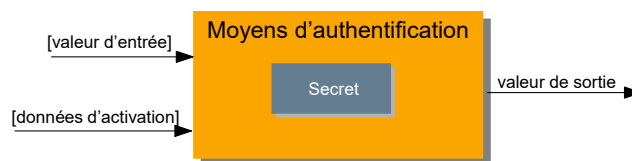
<sup>1</sup> Un sujet s'authentifie auprès d'un système. Un système authentifie un sujet.

Un moyen d'authentification peut être fondé sur un facteur unique (authentification à facteur unique, SFA) ou en combiner plusieurs (authentification à facteurs multiples, MFA) en vue d'améliorer la sécurité.

La combinaison d'un mot de passe et d'un *mot de passe à usage unique*, envoyé sur un téléphone portable, constitue un exemple classique de MFA.

La valeur de sortie générée par le moyen d'authentification l'est par une fonction mathématique à partir d'une valeur secrète (par ex. une clé privée), d'une ou plusieurs données d'activation facultatives (par ex. code PIN ou *caractère biométrique*) et d'une ou plusieurs valeurs d'entrée facultatives (par ex. valeurs aléatoires ou challenges). Dans un cas banal, le moyen d'authentification peut être la valeur secrète elle-même (par ex. dans le cas d'un mot de passe).

Les moyens d'authentification sont émis par le *Credential Service*.



$$\text{Valeur de sortie} = \text{fonction}(\text{secret}, [\text{valeur d'entrée}], [\text{données d'activation}])$$

Figure 1 - Fonctionnement schématique d'un moyen d'authentification

	Mot de passe	SMS	OTP	Mobile-ID	FIDO-Token	Smartcard
<b>Type d'authentification</b>	SFA	MFA - 1. facteur est généralement un mot de passe	MFA - 1. facteur est généralement un mot de passe	MFA - 1. facteur est généralement un mot de passe	SFA/MFA	MFA
<b>Token-Type</b>	SW	SW/HW Smartphone	SW-HW	HW (e)SIM	HW	HW
<b>Valeur d'entrée</b>	-	Code reçu	Seed of Devices	Code reçu	Nonce auto-généré	Nonce auto-généré
<b>Secret</b>	Mot de passe	Code reçu	Device Key	Private Key	Private Key	Private Key
<b>Données d'activation</b>	-	-	Heure actuelle ou compteur	PIN	Présence, code PIN ou caractéristique biométrique	PIN
<b>Fonction d'authentification</b>	Aucune ou fonction hash	Lecture et écriture du code reçu	HMAC	Signature	Signature	Signature

	Mot de passe	SMS	OTP	Mobile-ID	FIDO-Token	Smartcard
<b>Valeur de sortie</b>	Mot de passe, hash du mot de passe	Code reçu	Code reçu	Signe (code reçu)	Sign (Nonce)	Sign (Nonce)
<b>Credential<sup>2</sup></b>	Mot de passe enregistré auprès du Verifier	Le Vérifier connaît le numéro de portable du sujet	Seed synchrone pour le Verifier	N° de portable et clé publique enregistrés par le Verifier	Certificat enregistré auprès du Verifier	Certificat enregistré auprès du Verifier

Tableau 1: Exemples de moyens d'authentification

Synonymes: Facteur d'authentification, caractéristique d'authentification

## 2.16 Authorization Service

L'**Authorization Service** [2] est un *service IAM*. Il vérifie pour la période d'exécution que les droits d'utilisation de la *ressource numérique* sont bien respectés et autorise le *sujet* à utiliser la ressource dès lors qu'il en possède les droits.

Synonyme: Service d'accès, Access Service (angl.)

## 2.17 Autorisation

L'**autorisation** est un processus rapide consistant à accorder ou à refuser l'utilisation d'une *ressource* par un *sujet* authentifié sur la base de règles préalablement établies.

Synonyme: *Autorisation* (au sens de la procédure), Authorization (angl.)

## 2.18 Autorité

Une autorité est une *organisation*, un organe de l'État (Confédération, canton) ou d'une entité administrative indépendante (district, commune) qui assume des tâches de l'administration publique de l'État ou de l'entité administrative et qui représente celle-ci auprès de l'extérieur dans le domaine de compétence affecté. Des autorités peuvent exister aux niveaux administratifs de la commune, du canton ou de la Confédération et relever du pouvoir législatif, exécutif ou judiciaire (voir aussi eCH-0177 [5] – Annexe 1)

<sup>2</sup> L'Identifiant, par exemple le nom de l'utilisateur ou de l'utilisatrice, fait toujours partie du credential.

## 2.19 Utilisateur/trice

L'**utilisateur** ou l'utilisatrice est une *personne physique (sujet)* disposant d'un *User Account* chez un *RP*. À l'aide de son *User Account*, l'utilisateur ou l'utilisatrice est en mesure de prendre une part active aux processus électroniques numériques du *RP*.

Synonyme: User (angl.)

## 2.20 User Account

Un **User Account** comporte les *attributs* et données d'un *utilisateur* ou d'une utilisatrice dans le *RP*. Il est rattaché à une ou plusieurs *identités numériques* d'un utilisateur ou d'une utilisatrice, qui peuvent être utilisées à des fins *d'authentification* auprès du *RP*. L'*User Account* est créé lors de *l'enregistrement* du *sujet* auprès du *RP*.

Synonyme: Objet utilisateur, compte utilisateur

## 2.21 Autorisation

Le terme **Autorisation** prend deux sens:

1. Le processus d'autorisation comme synonyme d'*autorisation*.
2. Les autorisations d'un *sujet* correspondent à toutes les règles qui définissent quand le sujet peut accéder aux *ressources* d'un *Relying Party* et à quelles conditions.

## 2.22 Moyen de preuve

Un **moyen de preuve** (dans le contexte *IAM*) est un document émanant d'une source fiable et contenant des renseignements concernant le *requérant*. Il peut être utilisé à des fins de vérification d'une *identité*.

Un moyen de preuve doit contenir le nom du requérant ou de la requérante. Il peut en outre contenir un *identificateur* sans ambiguïté, une caractéristique physique et biométrique, mais également n'importe quel autre renseignement concernant le requérant ou la requérante. Il devrait contenir des caractères de sécurité rendant toute reproduction difficile.

Exemples de moyens de preuve:

- Acte certifié, par ex. acte de naissance
- Permis de conduire
- *Documents d'identité*

## 2.23 Caractéristique biométrique

Une **caractéristique biométrique** correspond à une caractéristique physique unique et mesurable d'une personne qui permet une *identification* sans ambiguïté de cette personne. Contrairement aux caractéristiques physiques générales telles que la taille ou la couleur des cheveux, les caractéristiques biométriques sont bien souvent immuables et offrent une grande sécurité pour les procédures d'authentification.

L'*authentification* biométrique a pour principal inconvénient de ne pas permettre d'invalider ou de recréer des caractéristiques biométriques compromises.

Exemples de caractéristiques biométriques:

- Caractéristiques physiologiques:
  - empreintes digitales
  - Caractères du visage (par ex. écartement des yeux, forme du visage)
  - Motifs de l'iris et de la rétine
  - Géométrie de la main et des doigts
  - Cartographie veineuse
  - ADN
- Caractéristiques comportementales:
  - signature
  - Vitesse de frappe
  - Démarche
  - Voix

Les caractéristiques biométriques peuvent être classées en fonction de leur fonction, de leur sécurité, de leur falsifiabilité et de leur facilité d'utilisation, voir [6].

## 2.24 Broker Service

Le **Broker Service** [2] est un *service IAM*, qui intervient en tant qu'intermédiaire entre le *sujet*, les *ressources* et les *services IAM de la période d'exécution* et fédère les *confirmations d'authentification et d'attributs*.

## 2.25 Certificate Policy (CP)

Une **Certificate Policy** est un document (*Policy*) qui définit les règles, exigences et procédures relatives aux contenus, à la délivrance, à la gestion et à l'utilisation des *certificats numériques*, le plus souvent au sein d'une Public Key Infrastructure (PKI).

Toutefois, les applications des CP concernent également d'autres domaines où l'on a recours à des certificats numériques ou des identités cryptographiques par exemple:

- *SSI*: Les CP peuvent définir des directives concernant la délivrance et la gestion des *Verifiable Credentials* (VC).
- *IoT*: Les CP peuvent définir des règles concernant les certificats dans les dispositifs et machines en réseau.
- *Signatures électroniques*: Les CP peuvent définir des exigences concernant les certificats de signatures électroniques qualifiées, par exemple dans la SCSE [7] ou l'eIDAS [8].

## 2.26 Certificate Revocation List (CRL)

Une **CRL** correspond à une liste publiée par une ou plusieurs *autorités de certification (CA)* et recensant tous les *certificats numériques* révoqués avant leur date d'expiration ordinaire (voir *Révocation*). Chaque élément de la liste inclut au moins le numéro de série du certificat révoqué et le moment de la révocation.

## 2.27 Certification Authority (CA)

Une *Certification Authority* est une *entité digne de confiance* qui délivre, renouvelle et révisé des *certificats numériques*, par ex. X.509.

Selon la SCSE [7] fournisseur de services de certification: «organisme qui certifie des données dans un environnement électronique et qui délivre à cette fin des *certificats numériques*»

Synonymes: Fournisseur de services de certification [7], prestataire de service de certification, autorité de certification pour certificats numériques, Certification Service Provider (angl.)

Termes génériques: autorité de certification, Trust Service Provider (TSP), fournisseur de services de confiance (FSC)

## 2.28 Certification Practice Statement

Une **Certification Practice Statement** est un document détaillé (*Policy*) d'une *Certification Authority (CA)* qui décrit les procédures concrètes, les mesures de sécurité et les pratiques opérationnelles lui servant à la mise en œuvre des exigences définies dans la *Certificate Policy (CP)*.

## 2.29 Challenge Response

Le Challenge Response est une méthode interactive permettant de prouver une connaissance (Proof of Knowledge) sans révéler cette connaissance.

Sans divulguer l'information, la personne qui connaît (le prouveur) démontre son savoir à l'examineur (le vérificateur) en résolvant une ou plusieurs tâches (challenges) proposées par ce dernier. La réponse correcte (response) à l'ensemble des tâches ne peut être fournie que par la personne connaissant l'information, avec une très grande probabilité.

## 2.30 Claim

1. Une **Claim** est une affirmation concernant une *propriété* d'un *sujet*. Les Claims peuvent être confirmées par un *IdP* ou un *Issuer*, elles peuvent alors faire office de confirmation d'attributs.
2. Dans le contexte *SSI*, les Claims sont représentées en tant que relation sujet-attribut-valeur. Les différentes Claims peuvent être associées, constituant ainsi un graphique avec des affirmations relatives à un ou plusieurs *sujets* (voir Figure 2).

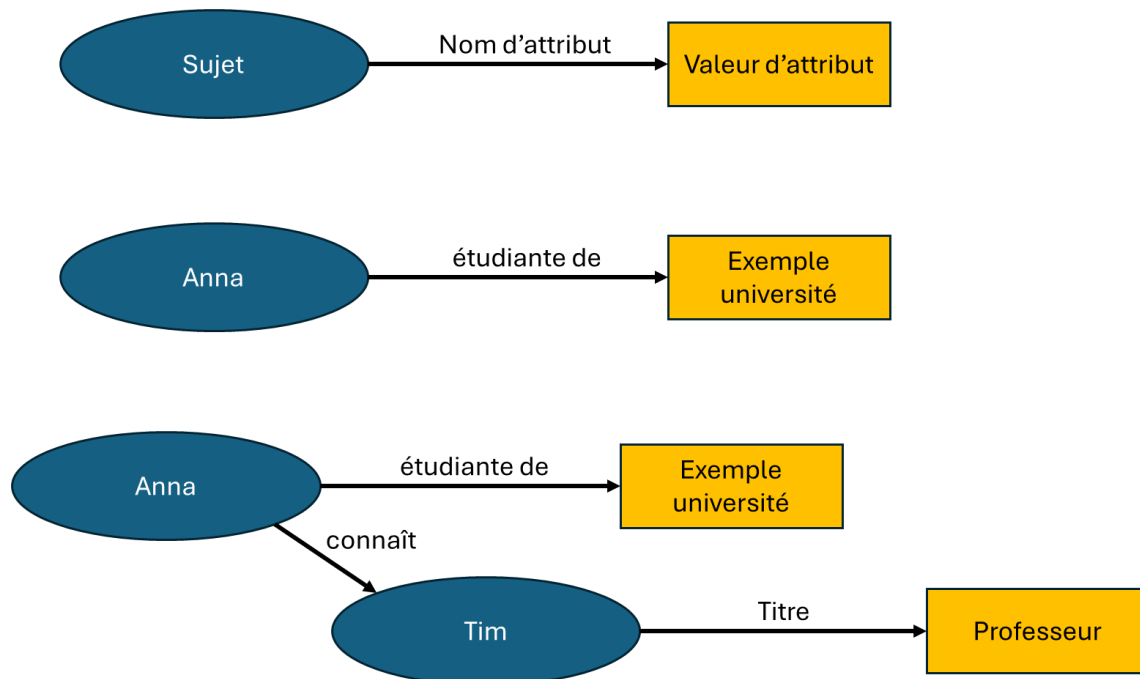


Figure 2 - Claims individuelles et associées dans le contexte SSI

Synonyme: déclaration, affirmation

### 2.31 Client Platform

La **Client Platform** ou plateforme client représente le système ou dispositif depuis lequel le *sujet* déclenche un processus d'authentification. Il peut s'agir par exemple d'un navigateur sur un PC/ordinateur portable ou d'une application sur un appareil mobile.

Synonyme: Client, user agent (angl.)

### 2.32 Credential

Un Credential représente une quantité de données (ni matériel, ni autre conteneur physique) servant à associer une *identité électronique* à un *moyen d'authentification*, que le *sujet* contrôle. Le lien est établi par l'identificateur de l'identité numérique.

Le Credential est utilisé par le *Verifier* avec la valeur de sortie du moyen d'authentification en tant que justificatif de l'identité numérique.

Par exemple, le hash d'un *mot de passe*, une représentation d'une *caractéristique biométrique* ou un *certificat numérique* (voir Tableau 1).

L'authenticité et la crédibilité d'un Credential doivent toujours être vérifiées avant son utilisation (voir aussi ISO 29115 [9], annexe B et NIST SP 800-63B [1], chap. 3).

Synonyme: preuve d'identité, courant identifiants de de connexion

### 2.33 Credential Service

Le **Credential Service** [2] est un *service IAM* responsable de la délivrance et de la gestion des *moyens d'authentification* pour les *sujets*. Il permet également le renouvellement ou le remplacement convivial des moyens d'authentification.

### 2.34 Période de définition

Au cours de la **période de définition** le *système IAM* est mis en place et configuré. Des *identités numériques* sont en outre établies. La période de définition comprend ainsi les processus de mise à disposition de toutes les informations nécessaires pour tous les composants impliqués, ainsi que pour les composants eux-mêmes.

Voir également *période d'exécution*

### 2.35 Identité décentralisée

L'**identité décentralisée** est un concept d'identité numérique selon lequel *les identités numériques* sont conservées dans un endroit décentralisé, le plus souvent dans un *Wallet*. On peut ainsi dissocier la délivrance de l'utilisation de l'identité.

Exemples d'identités décentralisées:

- *Verifiable Credentials (VC) avec lien avec le détenteur*
- *Certificats X.509*
- *nPA [10]*

Synonyme: Identité centrée sur l'utilisateur

### 2.36 Prestataire de services

Le **prestataire de services (IAM)** [2] est un *Stakeholder* dans un *système IAM* et entend fournir des prestations IAM.

Synonyme: *Prestataire de services IAM*

### 2.37 Identité numérique

Une **identité numérique** correspond à une représentation numérique des *propriétés* d'un *sujet* (voir *identité*). Une *identité numérique* permet à un *sujet* d'intervenir dans un *processus numérique*.

Une identité numérique est liée via un *Credential* à un *moyen d'authentification* de sorte qu'un sujet peut s'en servir pour s'authentifier (voir *Authentification*).

Un *sujet* peut avoir plusieurs identités, qui peuvent à leur tour comporter plusieurs identités numériques (voir Figure 4 - Identité). En règle générale, un sujet a une identité par domaine.

Exemples:

- Un *User Account* sur une boutique en ligne est lié à une identité numérique, qui se compose d'un *identificateur* (par ex. adresse e-mail), de renseignements concernant la personne (nom, date de naissance, ...) ainsi qu'un mot de passe comme *moyen d'authentification*.
- Un collaborateur ou une collaboratrice a une identité gérée dans une application de RH. Il en résulte des identités numériques, par ex. dans un AD ou un système SAP.

Synonymes: Identité électronique, angl. Digital Identity, Electronic Identity

### 2.38 Processus numérique

Un processus numérique désigne une séquence définie d'activités ou d'étapes de travail exécutées pour atteindre un objectif spécifique. Dans le contexte de la gestion des *identités et des accès (IAM)*, ces processus servent à la gestion et au contrôle de l'accès des *sujets* aux *ressources* protégées.

Un tel processus implique :

- Directement et activement : *sujets*
- Indirectement ou passivement : *objet, ressources*
- Données sous forme électronique, jointes à d'autres données électroniques ou logiquement liées à celles-ci, et servant à leur *authentification*

Synonyme : processus électronique

### 2.39 Digitale Ressource

Une **Digitale Ressource** correspond à l'*identité* d'une *Ressource*. Une ressource numérique possède un identificateur (nom sans ambiguïté, souvent URL/URI) qui peut être attribué sans ambiguïté à une ressource dans un espace de noms. Une ressource peut avoir plusieurs ressources numériques.

### 2.40 Digital Resource Service

Le **Digital Resource Service** [2] est un *service IAM* qui délivre des *ressources numériques* concernant les *ressources* et se charge de les gérer.

### 2.41 Signature numérique

Une **signature numérique** est une forme particulière de *signature électronique*. Elle repose sur une procédure technique utilisant des méthodes cryptographiques pour vérifier l'intégrité d'un message ou d'un document et garantir l'authenticité du signataire. Des certificats numériques sont souvent utilisés pour créer des *signatures numériques*.

## 2.42 Certificat numérique

Un **certificat numérique** est un fichier électronique signé par une *Certification Authority* qui vient confirmer l'identité d'une personne, d'une entreprise ou d'un site web.

Les certificats numériques peuvent être utilisés à plusieurs fins telles que le chiffrement, l'*authentification* et la *signature électronique*. Ces certificats numériques sont émis par des entreprises ou des autorités de certification dédiées (voir *Certification Authority*). Ces dernières peuvent être reconnues par l'État et sont l'objet de contrôles réguliers. [7]

Synonymes: Certificat d'identité, Public Key Certificate

## 2.43 Digital Identity Service

Le **Digital Identity Service** [2] est un *service IAM*, qui délivre des *identités numériques* concernant les *sujets* et se charge de les gérer.

## 2.44 Chose

Dans le contexte de l'IAM, une **chose** est un objet physique pouvant être rendu accessible via un *réseau*. Au sein du réseau, la chose est identifiable sans ambiguïté au moyen d'un *identificateur*. Plusieurs choses reliées entre elles via un réseau forment un Internet des objets (Internet of Things, IoT). Des choses peuvent en contenir d'autres. Une chose appartient toujours à une *organisation* ou à une *personne physique*.

Synonymes: Objet, angl. Thing (IoT)

## 2.45 Discovery Service

Le **Discovery Service** [2] est un *service IAM* chargé d'orienter le *sujet* vers un *IdP* de son choix et ce, à des fins *d'authentification*.

Synonyme: WAYF (Where Are You From) Service

## 2.46 Domaine

Dans le contexte de l'IAM, un **domaine** désigne un secteur délimité de *ressources*, d'*identités* et de règles, organisée sous une structure administrative et une autorité communes.

Synonyme: écosystème

## 2.47 Propriété

Les **propriétés** sont des caractéristiques ou signes distinctifs d'un *sujet* ou d'un *objet* (voir Figure 4) qui dans leur ensemble sont spécifiques.

## 2.48 Mot de passe à usage unique

Un **mot de passe à usage unique** est un mot de passe qui ne peut être utilisé qu'une seule fois et dont la validité est limitée à une courte période. On distingue les mots de passe à usage unique limités dans le temps des mots de passe à usage unique générés de manière aléatoire. Bien souvent, les mots de passe à usage unique sont utilisés dans l'authentification à deux-facteurs (2FA) en combinaison avec un mot de passe (voir chap. 2.15 Moyen d'authentification).

Synonyme: code à usage unique, angl. One-Time Password (OTP)

## 2.49 Signature électronique

**Signatures électroniques** sont « des données sous forme électronique qui sont jointes ou liées de façon logique à d'autres données électroniques et servent à leur *authentification*. » [7]

Les signatures électroniques peuvent aussi être utilisées afin de vérifier l'*identité* du ou des signataires.

Le terme « signature électronique » est de nature juridique et constitue un terme générique englobant toutes les formes de signatures sous forme numérique. Les signatures électroniques incluent donc également les procédés non cryptographiques (p. ex. signature manuscrite scannée – fac-similé). Avec les *signatures numériques*, il est possible de créer des signatures électroniques sécurisées.

## 2.50 Moyen d'identification électronique

Terme tiré d'eIDAS 2024/1183 [8]: un «**moyen d'identification électronique**» est un élément matériel et/ou immatériel qui contient des données d'identification personnelle et est utilisé pour l'authentification pour un service en ligne ou, le cas échéant, pour un service hors ligne.»

## 2.51 Système d'identification électronique

Terme tiré d'eIDAS 2024/1183 [8]: un «**schéma d'identification électronique**» est un système pour l'identification électronique en vertu duquel des moyens d'identification électronique sont délivrés à des personnes physiques ou morales ou à des personnes physiques représentant d'autres personnes physiques ou des personnes morales.»

## 2.52 Cachet électronique

Un **cachet électronique** est une *signature électronique* conçue tout spécialement pour les *organisations*, les entreprises ou les *autorités*. En Suisse, le cachet électronique est lié à un *certificat réglementé*. Au sein de l'UE, il est possible – pour des raisons de compatibilité entre États membres – d'utiliser des cachets assortis de certificats qualifiés.

### 2.53 Entité

Une entité <sup>3</sup>est un élément d'un système informatique, par ex. un composant ou un sous-système qui opère en tant *qu'identité numérique* dans un *processus numérique* (voir Figure 7 - Objet et sujet).

Les exemples pour les entités sont:

- *Identity Provider*,
- *RP*,
- *Services*,
- applications.
- Bots autonomes.

Synonyme: Entity

### 2.54 Management

Le **Management** [2] est un *Stakeholder* dans un *système IAM*. Il aspire à un système IAM fonctionnel et stable, qui réponde aux besoins de tous les Stakeholders. Pour ce faire, il oriente les *acteurs* impliqués.

### 2.55 Lien avec le dispositif

Le **lien avec le dispositif** assure qu'une *identité décentralisée* ou un VC est lié sans ambiguïté à un dispositif particulier (*entité*) et ne peut être transféré vers un autre dispositif.

Contrairement au *lien avec le détenteur*, le lien avec le dispositif n'offre aucune garantie que le *sujet* soit aussi le détenteur ou la détentrice (Holder) de l'*identité décentralisée* ou du VC.

Synonyme: Device Binding (angl.)

### 2.56 Certificat réglementé

Un **certificat réglementé** est un *certificat numérique* délivré pour une *personne physique* ou une *entité IDE* qui satisfait aux prescriptions correspondantes de la SCSE [7]. Les certificats réglementés peuvent être utilisés pour des *cachets électroniques* ou pour l'authentification de sites web par exemple.

---

<sup>3</sup> Le terme «entité» n'est pas employé de la même manière dans le contexte IAM que dans la modélisation des données en général. Dans la modélisation des données, le terme «entité» renvoie à un objet ou une unité d'information identifiable sans ambiguïté. Une entité représente une chose physique ou abstraite, telle qu'une personne, un produit, une commande ou un livre.

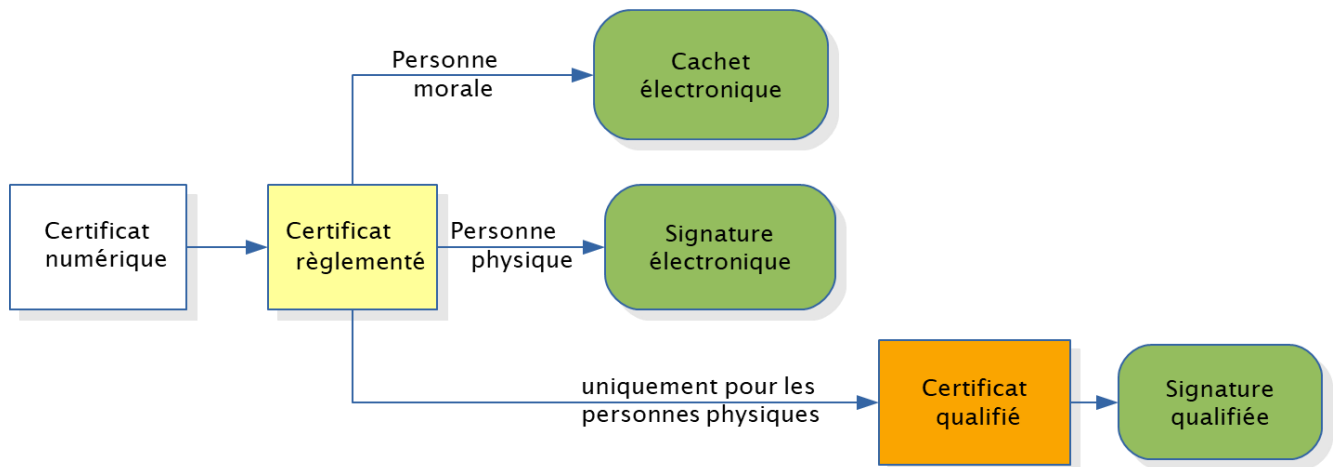


Figure 3 - Vue d'ensemble des différents certificats numériques

## 2.57 Holder

Un **holder** est un *rôle* qu'un *sujet* endosse dans le contexte *SSI*. Le détenteur conserve les *Verifiable Credentials (VCs)* en un emplacement décentralisé (*Wallet*) qu'il contrôle. Le Holder est ainsi en mesure de contrôler ses VC et de les présenter, dans leur intégralité ou en partie, à un *Verifier* au moyen de son *Wallet*.

Synonyme: Détenteur/trice, titulaire

## 2.58 Holder of Key (HoK)

Un **Holder of Key (HoK)** est un *sujet* qui remet au RP une *confirmation d'authentification* délivrée par l'*IdP* et qui atteste ainsi, sous une forme cryptographique, qu'il est bien en possession d'une clé privée correspondante, par opposition à un *porteur* ou une *porteuse (Bearer)* qui n'apporte pas une telle preuve.

## 2.59 Architecture IAM

L'**architecture IAM** se compose de concepts, de *processus* et de *topologies*, ainsi que de leurs relations au sein du *système IAM*.

## 2.60 Prestataire de services IAM

Un **prestataire de services IAM** [2] est un *acteur* dans un *système IAM* et est responsable de l'exploitation d'un ou de plusieurs *services IAM*.

Les prestataires de services IAM sont notamment:

- *IdP*
- *Broker*
- *Attribute Provider*
- *Service d'enregistrement.*

## 2.61 IAM Management

L'**IAM Management** [2] est un *acteur* dans un *système IAM*. Il recense les *fournisseurs de services IAM* et les *Relying Parties* participants.

## 2.62 IAM Policy

L'**IAM Policy** définit les objectifs, principes et limites d'un *système IAM*.

## 2.63 IAM Regulator

L'**IAM Regulator** [2] est un *acteur* dans un *système IAM*. Il définit les conditions-cadres juridiques, procédurales, organisationnelles/architectoniques et techniques selon lesquelles doit être mis en œuvre l'IAM. Il tient compte des intérêts de l'ensemble des *Stakeholders* et implique tous les autres dans la définition de manière appropriée.

Les régulateurs IAM peuvent prendre différentes formes et opérer au sein d'une seule et même organisation, mais peuvent également agir de manière transversale.

- Le pilotage IAM définit l'*IAM Policy* régissant un système IAM interne ou externe à l'organisation ou des services IAM.
- Le législateur pose les conditions juridiques devant encadrer l'évolution et le développement du système global.
- L'organisme de normalisation élabore des normes et directives relatives aux conditions-cadres procédurales, organisationnelles/ architecturales et techniques.

## 2.64 Service IAM

Un **service IAM** [2] est un *service* fourni par un *prestataire de services IAM*. Les services IAM ne sont pas des composants techniques, autrement dit lors d'une réalisation, un ou plusieurs services IAM peuvent être mise en œuvre par un composant technique. De même, un service IAM peut être réparti sur plusieurs composants techniques.

Les services IAM sont notamment:

- *Attribute Assertion Service*
- *Attribute Service*
- *Authentication Service*
- *Authorization Service*
- *Broker Service*
- *Credential Service*
- *Digital Identity Service*
- *Digital Resource Service*
- *Discovery Service*
- *Logging Service*
- *Trust Service*
- *Service droit d'accès*

Synonyme: service IAM

## 2.65 IAM Support

L'**IAM Support** [2] est un *acteur* dans un *système IAM*. Il assume la responsabilité de l'ensemble des activités visant à trouver et à résoudre les problèmes dans le système IAM.

## 2.66 Système IAM

Un **système IAM** correspond à une mise en œuvre d'un *IAM* dans un domaine d'application défini, par une *organisation*.

Un système IAM comprend des *entités* techniques telles que l'*Identity Provider* (IdP) et les *Relying Parties* (RP), les personnes de l'organisation impliquées, telles que les *sujets* et responsables IAM, ainsi que les *processus* sur lesquels ils reposent, par ex. *l'enregistrement* et la gestion des utilisateurs.

Synonyme: Système d'identité

## 2.67 Identificateur

Un **identificateur** est une identification (chaîne de caractères par exemple) qui désigne sans ambiguïté une *identité numérique* ou une *ressource numérique* au sein d'un *espace de noms (domaine)*. L'identificateur d'une *ressource* est souvent une URL/URI.

Synonyme: angl. Identifier

## 2.68 Identification

Une **identification** est le processus qui permet de reconnaître un *sujet* et, par conséquent, de vérifier *l'identité* du sujet ou certaines de ses *propriétés*. Des moyens de preuve sont utilisés à des fins d'identification. L'identification est le plus souvent du ressort d'un service d'enregistrement dans le cadre de *l'enregistrement*.

Synonyme: vérification de l'identité, identification, processus d'établissement d'identité

## 2.69 Identité

L'**identité** englobe les propriétés d'un *sujet* ou d'un *objet*. L'identité correspond à un jeu de données qui représente le *sujet* ou *l'objet* sans ambiguïté dans un *espace de noms*.

Une identité possède un *identificateur* (identification unique), généralement assorti d'un ensemble d'*attributs* supplémentaires, qui peut être attribué sans ambiguïté à un *objet* ou un *sujet* au sein d'un *espace de noms* (et donc d'un *domaine*).

L'identité d'un *sujet* est établie lors de *l'enregistrement*, qui peut inclure une *identification*.

Synonyme: Identity (angl.)

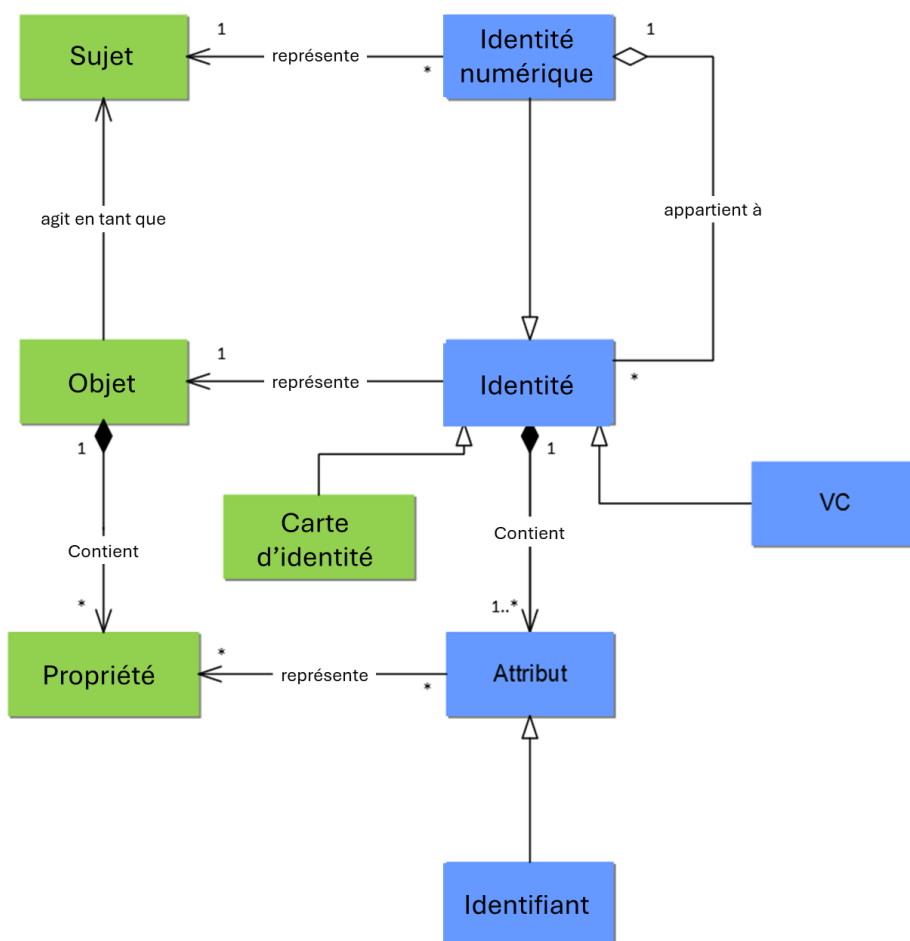


Figure 4 - Identité

Exemples:

- Un exemple d'identité est une entrée dans une feuille de calcul Excel ou une base de données.

## 2.70 Document d'identité

En Suisse, les documents considérés comme des documents d'identité sont les suivants:

- passeport,
- carte d'identité suisse,
- document d'identité reconnu pour l'entrée en Suisse.

## 2.71 Fédération d'identité

Une **fédération d'identités** désigne la mise en relation de systèmes d'identité d'*organisations* ou *domains* distincts en vue de permettre aux sujets une *authentification* et une *autorisation* par-delà les limites du système ou de l'organisation.

Afin qu'une fédération d'identités puisse être établie, les différents domaines doivent avoir confiance les uns dans les autres quant à certains aspects. Cette confiance se fonde sur différents accords explicites et implicites (*SLA*).

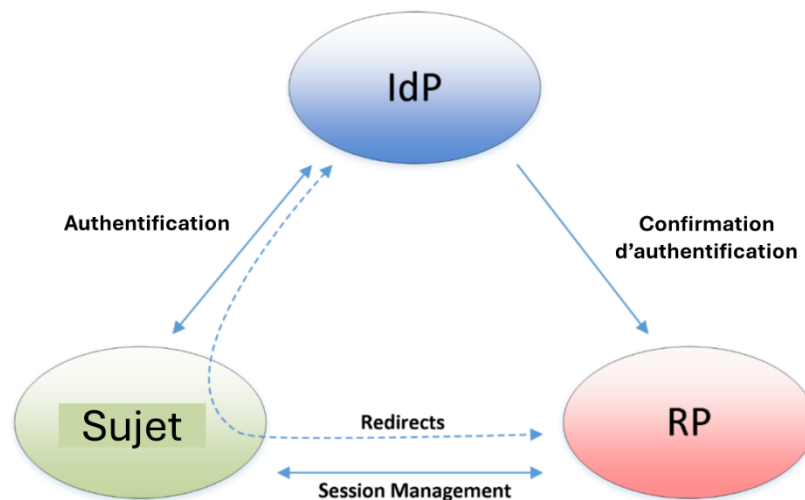


Figure 5 - Modèle d'une fédération d'identité

Comme cela est représenté dans Figure 5 une fédération d'identités est constituée de trois *entités*: *sujet*, *Relying Party* (RP) et un *Identity Provider* (IdP). La séquence d'informations varie en fonction des spécificités du protocole employé. Toutefois, la communication du sujet avec l'IdP, tout comme avec le RP, est une constante. Le sujet s'authentifie auprès de l'IdP. Cet événement est ensuite transmis au RP sous la forme d'une *confirmation d'authentification*.

Dans une fédération d'identités, l'on a recours à des protocoles fédérés tels que *SAML*, *OAuth 2.0* ou encore *OpenID Connect*.

### Système IAM fédéré dans la cyberadministration:

Dans la cyberadministration, la fédération d'identités permet aux *autorités* de fournir des *ressources* aux partenaires aussi bien internes (par ex. autres autorités suisses) et externes (par ex. *personnes*, *entreprises*, *organisations* ou autorités étrangères). Ces ressources sont utilisées afin de rendre disponibles en ligne des prestations définies relevant du domaine de compétence de l'autorité. Les sujets du *domaine* propre et ceux ayant des *identités numériques* issues d'autres domaines doivent pouvoir accéder à ces ressources de la même manière. Une autorité peut agir à la fois en tant que *Relying Party* et, le cas échéant, en tant que *prestataire de services IAM*.

Synonyme: système d'identité fédéré, IAM fédéré, Identity Federation System (angl.) Identity Federation (angl.)

## 2.72 Identity and Access Management (IAM)

L'IAM englobe tout ce qui répond aux questions suivantes relatives à tous les participants et participantes d'un système:

- Qui es-tu?
- A quoi te reconnaît-on?
- Qu'as-tu le droit de faire et qu'es-tu autorisé à faire?
- Comment les limites de ton autorisation sont-elles appliquées?

«*Identity and Access Management (IAM) is a security and business discipline that includes multiple technologies and business processes to help the right people or machines to access the right assets at the right time for the right reasons, while keeping unauthorized access and fraud at bay.*»<sup>4</sup>

Synonyme: (fr.) Gestion des identités et des accès

## 2.73 Identity Linking

L'**Identity Linking** permet, dans un contexte inter-organisations de mettre en relation et d'enchaîner des *identités numériques* issues de différents domaines.

L'Identity Linking est l'opération pour la *période de définition* par laquelle deux identités numériques sont reliées entre elles et ces informations de liaison sont archivées.

## 2.74 Identity Mapping

L'**Identity Mapping** est l'opération pour la *période d'exécution*, par laquelle sont rompus des liens entre identités numériques. Une identité numérique locale peut ainsi être associée à l'identité numérique fédérée.

## 2.75 Identity Provider (IdP)

Un **Identity Provider (IdP)** est une *entité* qui émet et gère *des identités numériques*. Un IdP met à disposition un *Authentication Service* et, à titre facultatif, un *Attribute Assertion Service* concernant la délivrance de *confirmations d'attributs*. De façon caractéristique, un IdP compte un *service d'enregistrement*.

Synonyme: Authorization Provider, fournisseur de données, fournisseur d'identité, fournisseur d'informations, autorité d'authentification (AuthnA), Authentication Authority (angl.)

---

<sup>4</sup> Gartner Glossary, <https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam>, consulté le: 16.11.2023 )

## 2.76 Lien avec le détenteur

Le **lien avec le détenteur** est un concept d'*identités décentralisées*, qui assure qu'une *identité numérique* peut être attribuée sans ambiguïté à un *sujet* particulier.

L'*Issuer* (émetteur) de l'*identité numérique* n'étant pas impliqué dans le processus de son utilisation et aucune *authentification* directe du sujet n'étant effectuée, il faut recourir à un autre moyen pour s'assurer que l'identité numérique présentée a bien été délivrée pour le sujet qui l'utilise.

D'ordinaire, ceci est réalisé en y associant une clé cryptographique ou à un secret du sujet légitime.

Dans la pratique, le lien avec le détenteur est souvent associée à un *lien avec le détenteur*.

Synonymes: Holder Binding (angl.), User Binding (angl.)

## 2.77 Institution

Une institution est une organisation structurée, dotée de responsabilités clairement définies, de structures organisationnelles établies et de missions précises.

Cela inclut :

- autorités publiques
- entreprises

## 2.78 Issuer

Un **Issuer** est une *entité* qui endosse un *rôle* dans le contexte SSI. L'*Issuer* vérifie les *Claims* concernant un ou plusieurs *sujets* et/ou *objets* et émet à cet effet des *Verifiable Credentials* pouvant être repris par le *Wallet* du *Holder* (caractère volontaire du Holder).

Synonyme: émetteur

## 2.79 Personne morale

Les **personnes morales** sont des organisations définies par l'art. 52 et suivants du CC et par les dispositions applicables du droit des sociétés du CO.

Les personnes morales ne peuvent agir que par le biais de *personnes physiques* et sont donc toujours associées au minimum à une *personne physique*.

## 2.80 Kerberos

**Kerberos** [11] est un protocole d'authentification basé sur le réseau qui permet une *authentification* mutuelle entre clients et services (*RP*). Il recourt à un système basé sur les tickets et s'appuie sur une instance centrale digne de confiance, le Key Distribution Center (KDC). Le KDC se charge de l'attribution des tickets, ce qui permet le *Single Sign-On* (SSO).

## 2.81 Caractéristique physique

Une **caractéristique physique** est une *propriété* d'une personne, comme la taille et la couleur des yeux. Les *caractéristiques biométriques* sont des caractéristiques physiques spéciales.

## 2.82 Token cryptographique

Un **token cryptographique** est un dispositif de sécurité physique ou virtuel (support matériel ou logiciel) qui enregistre la clé cryptographique et exécute les opérations cryptographiques, telles que l'authentification, les signatures numériques ou le chiffrement, sans que les clés puissent être directement lues.

Exemples:

- Software: Microsoft Certificate Manager dans Windows OS
- Hardware: SmartCard, USB-Token, Hardware Security Module (HSM)

Synonymes: jeton de certificat, Cryptographic Token, jeton cryptographique

## 2.83 Période d'exécution

Les *processus numériques* par lesquels un *sujet* – en cas de succès – obtient l'accès aux ressources d'un RP ont lieu pour la **période d'exécution**.

Synonyme: Période de réalisation

Voir également: *période de définition*

## 2.84 Linking Protocole

Un **Linking Protocole** est mis à contribution afin de relier deux identités numériques (voir *Identity Linking*)

## 2.85 Bénéficiaire de prestations (BP)

Le **bénéficiaire de prestations** [2] est un *Stakeholder* dans un *système IAM* souhaitant se procurer en ligne une prestation technique auprès d'un Relying Party (par ex. commande d'un macaron de stationnement).

## 2.86 Fournisseur de prestations (FP)

Le **fournisseur de prestations** [2] est un *Stakeholder* dans un *système IAM* souhaitant offrir des prestations techniques en ligne. Il souhaite transmettre l'accès et la protection des ressources au *prestataire de services IAM* en fonction de ses besoins (par ex. propension au risque, rentabilité).

## 2.87 Logging Service

Le **Logging Service** [2] est un *service IAM*, qui documente l'utilisation d'un *service IAM* pour la période d'exécution. Il fournit à la Support Organisation les informations nécessaires afin de clarifier les problèmes d'utilisation ou les erreurs.

## 2.88 Look-Up Secret

Les **Look-Up Secrets** contiennent une liste de valeurs (alpha) numériques qui ont été préalablement échangées entre *le sujet* et *l'IdP*. Les valeurs échangées doivent être générées de façon aléatoire. Elles ne peuvent être utilisées qu'une seule fois et posséder une entropie suffisamment élevée. Les Look-Up Secrets doivent être conservés de manière sûre afin d'éviter qu'ils ne parviennent entre de mauvaises mains.

Les **Look-Up Secrets** peuvent être utilisés comme 2<sup>e</sup> facteur en cas de MFA ou comme code d'urgence ou de secours.

Exemples: listes de décompte (angl. tally sheet), blocs TAN, Recovery Codes

Synonyme: secrets consultables

## 2.89 Magic Link

Dans le cas de **Magic Links**, le *sujet* reçoit un lien original, à usage unique, par e-mail ou SMS. En cliquant sur ce lien, le sujet s'authentifie directement. La période de validité du lien est souvent courte. Les Magic Links compte parmi les procédures *d'authentification sans mot de passe*.

## 2.90 Memorized Secret

Les **Memorized Secrets** sont des *moyens d'authentification* basés sur la connaissance, par lesquels le sujet est authentifié en saisissant un secret connu de lui seul. Les mots de passe, les codes PIN (numéros d'identification personnels) mais aussi les questions de sécurité en sont des exemples caractéristiques.

Les Memorized Secrets doivent être suffisamment complexes et aléatoires pour ne pas être devinés ou calculés de quelque manière que ce soit par un cyberpirate. Les mots de passe ou codes PIN simples sont potentiellement vulnérables aux attaques par hameçonnage ou de type Brute force. Les règles en matière de mot de passe, par exemple, posent des exigences en matière de longueur, de complexité, de variété de caractères, de durée d'expiration et de réutilisation, et déterminent ainsi la robustesse du Memorized Secret.

Synonyme: secret mémorisé

### 2.91 Méta-attribut

Un **méta-attribut** est utilisé afin de décrire et de spécifier des *attributs* en vue de définir ou de normaliser la structure, la signification ou l'objectif des attributs dans le cadre d'un schéma d'attributs. Il fournit donc des «données sur les données» et favorise la cohérence et la gestion des informations à travers différents systèmes.

Quelques exemples de méta-attributs:

- Nom d'attribut (par ex. «pointure»),
- Type de données d'attribut (par ex. «nombre entier») et
- Valeur d'attribut (par ex. «39»).

### 2.92 Métadonnées

Les **métadonnées** sont des informations structurées complémentaires. Elles sont nécessaires à l'exécution de *processus (IAM)* et décrivent notamment les données, les structures de données, les protocoles employés ou les informations d'audit (horodatage).

Synonyme: Metadata (angl.)

### 2.93 Espace de nom

Champ d'application (une entreprise, un État, une communauté professionnelle, une communauté linguistique par exemple) pour lequel est définie la signification d'une identification ou d'une chaîne de caractères (par ex. un identificateur).

Dans un espace de noms, les *sujets* et les *ressources* sont désignés sans ambiguïté, ce qui signifie qu'au moins un *identificateur unique* leur est attribué (en tant que partie de leur représentation numérique, autrement dit de l'*identité numérique* ou de la *ressource numérique*).

Synonyme: Namespace (angl.)

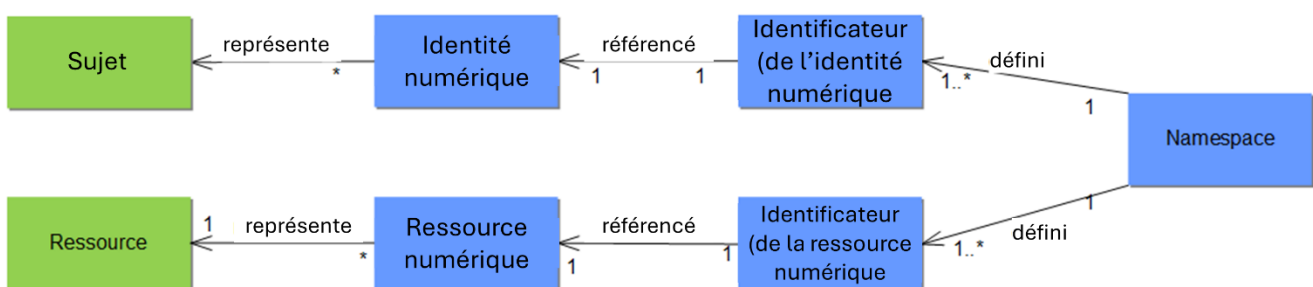


Figure 6 - Namespaces & identificateurs

### 2.94 Personnes physiques

Une **personne physique** est un être humain en tant que sujet de droit. Les personnes physiques peuvent appartenir à une ou plusieurs *organisations*.

## 2.95 Réseau

Un **réseau** correspond à un groupe de dispositifs ou de systèmes reliés entre eux, qui peuvent communiquer et échanger des données les uns avec les autres.

## 2.96 Non-répudiabilité

La **non-répudiabilité** garantit que les données ou messages peuvent être attribués sans ambiguïté à un *sujet* précis qui ne peut donc pas en contester la paternité.

Dans la pratique, la non-répudiabilité est obtenue par des *signatures numériques*. On part du principe que si une signature a été vérifiée avec une clé publique, cela prouve également que la signature a été créée avec la clé privée correspondante.

Synonyme: nature contraignante, (angl.) Non-repudiation

## 2.97 OAuth 2.0

**OAuth 2.0** [12] est un protocole d'autorisation ouvert qui permet à des applications tierces d'accéder, au nom d'un *utilisateur* ou une utilisatrice, à des *ressources* sans devoir divulguer ses données d'authentification. Il repose au contraire sur des Access Tokens délivrés par l'Authorization Server.

## 2.98 Objet

Un **objet** est une *personne physique*, une *organisation* agissante ou une *entité* qui participe à un *processus numérique* ou qui y est référencée. Un objet devient *sujet* dès lors qu'il *s'authentifie* dans ce *processus numérique*.

Une vue d'ensemble est proposée dans Figure 7.

## 2.99 Online Certificate Status Protocol (OCSP)

**OCSP** [13] constitue un protocole servant à interroger le statut de validité d'un *certificat numérique*. Voir également *Révocation* et *Certificate Revocation List (CRL)*.

## 2.100 OpenID Connect (OIDC)

**OpenID Connect (OIDC)** [14] est une norme ouverte portant sur l'*authentification* qui s'appuie sur *OAuth 2.0*.

## 2.101 Organisation

Une organisation (entreprise, association, service, groupe de personnes) est un groupe constitué de plusieurs *personnes physiques ou de choses*. Une organisation peut contenir des (sous-)organisations. Voir aussi Figure 7.

Concernant les organisations, on distingue entre organisations agissantes et non agissantes. Les **organisations agissantes** (par ex. identités de groupe) peuvent s'authentifier et se voir accorder l'accès aux ressources. Les **organisations non agissantes** (par ex. *personnes morales*) ne peuvent s'authentifier par elles-mêmes, mais uniquement par le biais du *sujet* correspondant (une *personne physique* la plupart du temps) auquel elle délègue ses droits.

## 2.102 OTP-Device

Un OTP-Device est un logiciel ou un dispositif physique qui génère un *mot de passe à usage unique* selon un algorithme spécifique (basé sur les événements ou sur le temps). Un secret caché intégré (clé) est enregistré dans l'OTP-Device. Il sert à générer le mot de passe à usage unique avec une valeur d'entrée (par ex. l'heure actuelle ou un compteur incrémentiel).

Un **Single-Factor OTP Device** n'a besoin d'aucun facteur d'authentification supplémentaire. Le SafeNet MobilePass ou un SecureID Token en sont des exemples caractéristiques.

Un **Multi-Factor OTP Device** a besoin d'un second facteur d'authentification, sous la forme par exemple d'un facteur de connaissance (par ex. code PIN) ou d'un *facteur biométrique* (par ex. empreinte digitale). De tels dispositifs sont bien souvent équipés d'un pavé numérique intégré, de capteurs biométriques ou d'une interface (USB par exemple). Le SecureID Token avec pavé numérique ou le HID ActivID Token en sont de bons exemples.

Synonyme: Générateur de mots de passe à usage unique

## 2.103 Out-of-Band Authenticator

Un **Out-ofBand Authenticator** est un *moyen d'authentification* dans lequel un canal de communication séparé sert de canal indépendant supplémentaire à la demande d'authentification primaire.

Un Out of Band Authenticator est un dispositif physique qui détient le *sujet*, dont l'adresse doit être sans ambiguïté et qui peut recevoir des secrets prévus pour un usage unique.

Les Out of Band Authenticators peuvent fonctionner selon deux modes distincts:

1. Le sujet présente le secret, qu'il a reçu via le second canal, au service authentifiant via le canal de communication primaire.

2. Le sujet renvoie au service authentifiant une réponse directement via le second canal de communication.

Les exemples d'Out-of-Band Authentication sont:

- Un smartphone avec numéro de mobile et code SMS
- Un *message push* envoyé sur le téléphone portable de *l'utilisateur* ou de l'utilisatrice lorsque celui-ci ou celle-ci tente de s'authentifier.
- Un appel vers un numéro de téléphone préalablement enregistré pour vérification.

Synonyme: Canal externe

## 2.104 Passkey

Une **Passkey** représente une *méthode d'authentification sans mot de passe* développée par FIDO (Fast Identity Online) et Google. Elle permet de se connecter à des sites web ou à des services de manière simple et sûre, sans devoir utiliser de mot de passe conventionnel. Au lieu de cela, une Passkey utilise des données biométriques, des clés de sécurité ou des dispositifs comme des smartphones.

Lorsqu'un sujet se connecte à un service, la clé publique enregistrée sur le serveur est comparée à la clé privée se trouvant sur l'appareil du sujet. Le sujet confirme alors son identité soit par des caractéristiques biométriques, un mot de passe ou un code PIN, soit en utilisant un dispositif physique.

## 2.105 Mot de passe

Un **mot de passe** correspond à une séquence de caractères confidentielle qu'un *sujet* et un *Verifier* définissent lors de *l'enregistrement*. Le sujet peut ensuite se servir du mot de passe afin de *s'authentifier* auprès du *Verifier*.

## 2.106 Authentification sans mot de passe

L'**authentification sans mot de passe** est une méthode moderne d'authentification qui ne nécessite pas de recourir à des mots de passe.

Les méthodes courantes d'authentification sans mot de passe sont les suivantes:

- *Caractéristiques biométriques* (par ex. empreintes digitales ou reconnaissance des visages),
- *Mots de passe à usage unique* (par ex. Google Authenticator),
- *Magic Links* (par ex. Slack),
- Hardware Token (par ex. Yubikey ou Smartcards),
- *Messages push*

Il ne faut pas confondre une authentification sans mot de passe avec une authentification à facteurs multiples (MFA), dans laquelle un mot de passe peut tout à fait être utilisé en tant que facteur comme moyen d'authentification.

### 2.107 Pièce d'identité physique

Une **pièce d'identité** est un document physique qui contient les *attributs* d'une *personne physique* et a été délivré comme confirmation ou légitimation de quelque chose (voir Figure 4).

Exemples: passeport, carte de crédit, permis de conduire

### 2.108 Policy

Une **Policy** comprend des règles et prescriptions rédigée, qui définissent et guident le comportement souhaitable ou les actions autorisées dans le cadre d'un système, d'une *organisation* ou d'un *processus*.

Exemple: Une Policy pour un *système IAM* est une *IAM Policy*.

### 2.109 Provisionnement

Le **provisionnement** est le processus par lequel des *identités numériques* ou des *User Accounts* sont configurés, gérés et supprimés auprès d'*entités* dans le *système IAM* (par ex. IdP, RP). La plupart du temps, les données d'identité sont transférées d'un système source central vers un ou plusieurs systèmes cibles. Le provisionnement peut être manuel, automatisé (unique ou périodique) ou prendre une forme hybride et comprend habituellement l'initialisation, la mise à jour, la désactivation et la suppression des identités numériques ou des *User Accounts*.

Voir aussi *Fédération d'identités*

Synonyme: Provisioning (angl.)

### 2.110 Processus

Un **processus** est une série structurée d'activités qui, guidées par des saisies spécifiques, aboutissent à un résultat défini.

### 2.111 Messages push

Un **message push** est un message court envoyé directement par une application ou un service à l'appareil mobile du *sujet*. Les messages push sont envoyés via des services spéciaux tels qu'Apple Push Notification Service (APNs) pour iOS ou Firebase Cloud Messaging (FCM) pour Android.

Un message push peut être utilisé à des fins d'*authentification* (authentification push). Le sujet peut, sans devoir saisir de code, confirmer la demande d'authentification en tapant ou en faisant glisser.

Un message push peut également être utilisé comme *Out-of-Band Authenticator* en tant que deuxième facteur dans le cas d'une MFA.

### 2.112 Signature électronique qualifiée (QES)

Selon l'art. 14, al. 2bis du CO, une signature électronique qualifiée peut être assimilée juridiquement à une signature manuscrite. Par principe, l'Office fédéral de la communication (OFCOM) réglemente dans la Loi fédérale sur la signature électronique SCSE les signatures et cachets reconnus [7].

La signature électronique qualifiée (QES) est une solution indispensable à une communication électronique et à un traitement des contrats conformes à la loi et sécurisés.

### 2.113 Certificat qualifié.

Un **certificat qualifié** est un *certificat numérique* délivré pour une *personne physique* qui satisfait aux prescriptions correspondantes de la SCSE [7]. Une signature électronique qualifiée doit reposer sur un certificat qualifié.

(remarque: le règlement européen eIDAS 2014/1183 [8] propose une définition plus large du certificat qualifié. En effet, le terme y englobe, outre le certificat de signature électronique qualifiée, les certificats pour les *cachets électroniques* et pour l'authentification de site web).

### 2.114 Droits

Les **droits** sont des *propriétés* spécifiques abstraites que doit posséder le *sujet* pour pouvoir accéder à une *ressource*. Ceux peuvent être fixés par des lois ou stipulés par des contrats par exemple.

### 2.115 Registre

Un **registre** est un corpus de données géré par des instances officielles (autorités) et dont la gestion fait l'objet est régie par une prescription légale explicite (voir aussi eCH-0177 [5] – Annexe 1)

Les registre des habitants, registre des avocats, registre d'état civil, registre du commerce, en sont de bons exemples.

### 2.116 Enregistrement

Un **enregistrement** est un *processus*, dans le cadre duquel une *identité numérique* est créée pour un *sujet* ou est reliée à un *User Account*. La plupart du temps, l'enregistrement comporte une *identification*.

Synonyme: Registration (angl.), Onboarding (angl.)

### 2.117 Service d'enregistrement / Registration Authority (RA)

Un **service d'enregistrement** est une *entité* qui autorise la délivrance d'une *identité numérique* à un *sujet* qui a été vérifié au préalable. Le service d'enregistrement vérifie à cette fin les moyens de preuve présentés par le sujet ou recueillis par d'autres méthodes.

Le RA peut être partie intégrante d'un IdP ou opérer en tant que service indépendant pour le compte de l'IdP.

## 2.118 Regulator

Le **Regulator** [2] est un *Stakeholder* dans un *système IAM* et souhaite garantir l'interopérabilité (dans le cas de sous-systèmes dirigés de manière autonome en particulier), la solidité et la sécurité du système IAM global.

## 2.119 Relying Party (RP)

Le **Relying Party** [2] est un *acteur* dans un *système IAM*. Il est responsable du contrôle d'accès à ses *ressources*. Il utilise des services d'affaires IAM [2] et traite des informations émanant de *prestataires de services IAM* en vue de les protéger. Pour pouvoir évaluer l'autorisation d'accès à une ressource, elle doit disposer d'informations concernant un sujet, autrement dit son identité numérique avec les attributs pertinents pour l'autorisation, ainsi que le contexte de l'accès (lieu, heure, niveau de sécurité, etc.).

Synonymes: bénéficiaires d'informations, consommateur d'informations, consommateur d'identité, fournisseur de solutions, SAML Service Provider, Verifier

## 2.120 Ressource

Les **ressources** sont des services ou des données auxquels un sujet peut accéder. Cette notion englobe les ressources physiques comme les bâtiments et installations, dont l'utilisation est pilotée par des systèmes informatiques.

On distingue trois types de ressources:

- ressources **publiques** (pas dignes d'être protégées): ces ressources sont en libre accès et aucune authentification ni autorisation n'est nécessaire pour y accéder. Les sites Web d'information (accès en lecture) et les données publiques en sont de bons exemples.
- ressources **cachées**: ces ressources ne nécessitent pas non plus d'authentification/autorisation avant l'accès, toutefois la ressource n'est pas disponible de manière générale, mais connue uniquement d'un certain nombre d'utilisateurs. Quiconque connaît l'URL correspondante peut également accéder à la ressource. Les accès aux Google-Docs ou Doodle-Links en sont de bons exemples.
- ressources **dignes d'être protégées** (non publiques): ces ressources exigent une authentification et autorisation réussies pour le sujet.

## 2.121 Responsable des ressources

Le responsable des ressources est l'entité responsable des *ressources* gérées par le *Relying Party* (par ex.: responsable d'applications, responsable de service, détenteur de données).

## 2.122 Rôle

Un rôle est un ensemble d'*autorisations* pour les groupes de sujets qui sont associés à une fonction ou à une tâche spécifique au sein de l'organisation

Synonyme: Role (angl.)

### 2.123 Contrôle des accès basé sur les rôles (RBAC)

Le **contrôle des accès basé sur les rôles (RBAC)** [15] désigne un type de *contrôle d'accès* par lequel un *Relying Party* autorise l'accès à une *ressource* en fonction des *rôles* d'un *sujet* dans une *organisation*.

Synonyme: Role based Access Control (angl.)

### 2.124 Security Assertion Markup Language (SAML)

**SAML** [16] est une norme qui permet l'échange sécurisé et standardisé d'informations d'authentification et d'attributs. Il définit aussi bien la structure des SAML Assertions que les protocoles et Bindings correspondants pour la transmission des assertions [17]. SAML est souvent employé dans les scénarios Single Sign-On (SSO) (voir SAML 2.0 Web Browser SSO Profil [18])

SAML constitue la base d'autres protocoles de sécurité, tels que WS-Federation [19], WS-Trust [20] et WS-Security [21].

### 2.125 Security Token

Un **Security Token**<sup>5</sup> [21] est un paquet de données qui contient des Claims sur un sujet et peut être utilisé afin d'autoriser l'accès à une ressource.

Synonyme: Jeton de sécurité

### 2.126 Security Token Service

Un **Security Token Service** (STS) est un service qui délivre des Security Tokens selon à la spécification [21] de WS-Security afin d'authentifier des sujets et de leur permettre d'accéder à des ressources protégées.

### 2.127 Divulgence sélective

La **divulgence sélective** désigne la transmission ciblée et contrôlée d'informations spécifiques depuis un plus large ensemble de données signées. Cela permet de ne partager que les données nécessaires à une finalité précise, sans devoir divulguer par ailleurs des données inutiles, tout en garantissant l'intégrité et l'authenticité des données.

Synonyme: Selective Disclosure (angl.)

---

<sup>5</sup> Le terme est également employé, avec une signification différente, dans le contexte des crypto-monnaies et de la technologie blockchain.

### 2.128 Self-Sovereign Identity (SSI)

**Self-Sovereign Identity (SSI)** désigne un concept de gestion décentralisée et sécurisée de *Verifiable Credentials*. Les *Issuers* émettent des *Verifiable Credentials (VCs)* assortis de *Claims* sur des *objets* ou des *objets*. Les *Holder*s stockent ces *Credentials* de façon décentralisée (par ex. sur un téléphone portable) et peuvent les présenter à un *Verifier*.

SSI permet d'espacer géographiquement et dans le temps l'émission d'un *Verifiable Credential* de sa présentation. Un *Holder* est ainsi en mesure de présenter un *Credential* sans que l'Issuer ne soit impliqué (contrairement aux *Attribute Providers* ou aux *Identity Providers*). La confidentialité des *Holder*s s'en trouve ainsi renforcée.

Qui plus est, les *Holder*s peuvent décider des *Verifiable Credentials* ou parties de ceux-ci qu'ils présenteront, à titre facultatif sous la forme d'une *Verifiable Presentation*.

### 2.129 Service

Un **service** est un service numérique mis à disposition par l'intermédiaire d'un *réseau*. Les services peuvent inclure des applications, des bases de données, des API, des serveurs etc., qui fournissent des fonctions ou des informations spécifiques.

Synonyme: Service

### 2.130 Service Level Agreement (SLA)

Un **Service Level Agreement (SLA)** désigne un accord contractuel entre donneurs d'ordre et mandataires, qui définit, de manière claire et mesurable, les prestations de service, normes de qualité et responsabilités attendues pour un service.

### 2.131 Single Sign-On (SSO)

Un Single Sign-On (SSO) est une procédure d'authentification par laquelle un *objet* s'authentifie une seule fois afin d'accéder à plusieurs ressources sans avoir à *s'authentifier* à chaque fois.

Le SSO est souvent rendu possible par des services d'authentification centralisés tels qu'*Identity Provider (IdP)* et des protocoles comme *Kerberos*, *SAML* ou *OIDC*.

### 2.132 Identité électronique reconnue par l'État (E-ID)

Une **identité électronique reconnue par l'État (E-ID)** est une *identité numérique* délivrée par un organisme public ou reconnu par l'État, qui peut être utilisée pour *l'identification sûre et juridiquement contraignante de personnes* dans des *services en ligne*.

### 2.133 Stakeholder

Les **Stakeholders** [2] dans le contexte de l'IAM sont des objets du monde réel, autrement dit des *personnes*, des groupes de personnes ou d'*organisations* ayant des intérêts communs dans l'IAM. Les Stakeholders ont des exigences à l'égard des différents *acteurs* dans un *système IAM*.

Les Stakeholders que l'on trouve dans un système IAM sont les suivants:

- *Bénéficiaire de prestations,*
- *Fournisseur de prestations,*
- *Prestataire de services,*
- *Management,*
- *Regulator.*

### 2.134 Sujet

Un **sujet** [2] est un *acteur* dans un *système IAM* et souhaite accéder à une *ressources* dans un *processus* numérique.

Un sujet peut avoir plusieurs représentations numériques, appelées *identités numériques*, dans un *domaine*.

Un sujet peut déléguer à un autre sujet les droits qui lui reviennent.

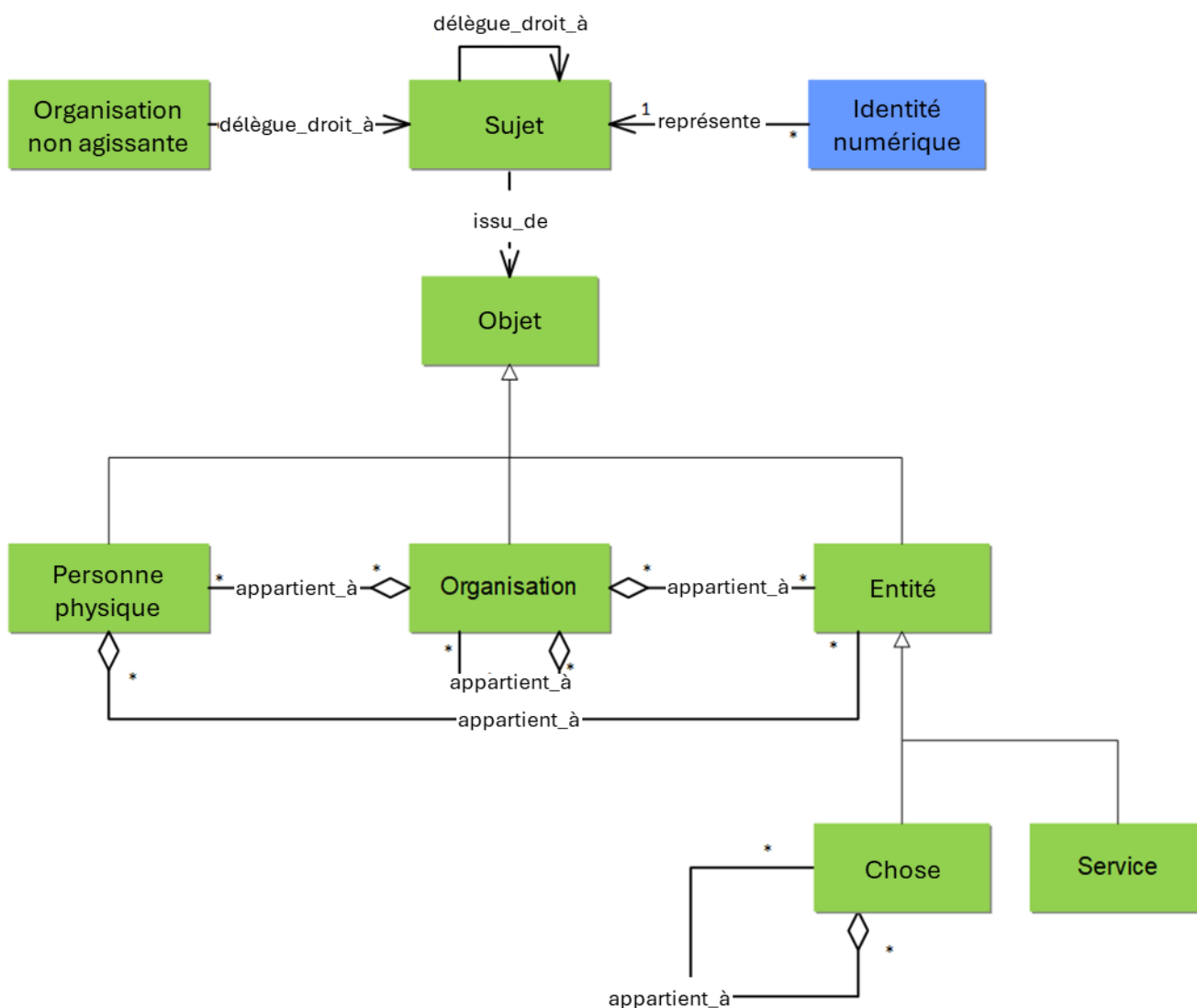


Figure 7 - Objet et sujet

Figure 7 indique quels objets peuvent être contenus dans quoi (par exemple, les organisations peuvent contenir plusieurs (sous-)organisations).

Synonymes:

- Une *personne physique* agissant en tant que *sujet* est souvent appelée *utilisateur/utilisatrice*.
- La plupart du temps, le sujet est généralement désigné en tant que *Holder* dans le contexte SSI.
- *Abonné/e*
- *Porteur/porteuse*

## 2.135 Topologie

La **topologie** d'un système IAM décrit l'agencement des différentes entités, telles que les IdP ou les RP, et leurs liens logiques.

### 2.136 Trust Service

Le **Trust Service** [2] est un service *IAM*, qui gère les prestataires de services *IAM* et *Relying Parties* dignes de confiance acceptés dans un système *IAM*.

### 2.137 Trusted Third Party

Un **Trusted Third Party** est une *entité* indépendante et digne de confiance qui assure l'authenticité, l'intégrité ou la confidentialité des informations et transactions dans les systèmes de gestion de la sécurité et de l'identité.

Quelques exemples:

- *Certification Authority (CA)* dans une *Public Key Infrastructure (PKI)*
- *Identity Provider (IdP)* dans les fédérations d'identité.

### 2.138 Unité IDE

Les **unités IDE** sont définies selon l'article 3.c de la Loi fédérale sur le numéro d'identification des entreprises (LIDE) [22].

Les unités IDE correspondent à toutes les entreprises et institutions qui se voient attribuer une IDE. Dans le système IDE, la notion d'entreprise est plutôt large. Par unité IDE, on entend donc non seulement toutes les sociétés actives en Suisse au sens propre du terme, mais également l'ensemble des «clients et clientes de l'administration publique» qui présentent les caractéristiques d'une entreprise ou qui sont identifiés à des fins juridiques, administratives ou statistiques.

### 2.139 Porteur/porteuse

Un **porteur** ou une porteuse est un *sujet* qui transmet au RP une confirmation d'authentification émise par l'*IdP* (voir *Holder of Key (HoK)*)

Synonyme: Bearer (angl.)

### 2.140 Verifiable Credential (VC)

Un **Verifiable Credential** correspond à un paquet de données signé qui contient des *Claims* portant sur un ou plusieurs *sujets* et/ou *objets* et délivré par un *Issuer*. Un *Verifiable Credential* est un justificatif à l'intégrité protégée, dont il serait idéale de prouver la paternité. Un *Verifiable Credential* peut être présenté directement ou sous la forme d'une *Verifiable Presentation* à un *Verifier*.

Les Verifiable Credentials peuvent contenir des métadonnées décrivant les VC, par ex. *Issuer* ou date d'expiration.

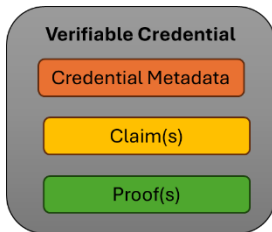


Figure 8 - Structure schématique d'un Verifiable Credential

Synonyme: justificatif numérique vérifiable

### 2.141 Verifiable Data Registry

Un **Verifiable Data Registry (VDR)** est un service dans le contexte *SSI*, qui sert de source de données transparente et digne de confiance pour la vérification décentralisée de l'authenticité et de la validité des *Verifiable Credentials (VC)*. Le VDR enregistre et gère à cet effet les schémas, identifiants, listes de révocation, ainsi que les clés publiques des *Issuers* et des *Verifiers*.

### 2.142 Verifiable Presentation (VP)

Une **Verifiable Presentation** est un paquet de données signé, qui contient des *Verifiable Credentials* émanant de différents *Issuers* ou des parties de ceux-ci, créés par le *Wallet* du *Holder*. Les Verifiable Presentations autorisent la divulgation sélective de *Claims* à partir de *Verifiable Credentials*. Le *Holder* transmet au *Verifier* la Verifiable Presentation créée à l'aide de son *Wallet*.

Une Verifiable Presentation contient des métadonnées, des *Verifiable Credentials* ou des parties de ceux-ci, ainsi que des justificatifs cryptographiques (voir Figure 9). Les métadonnées décrivent la VP, comme la date d'expiration par exemple. Les Proofs peuvent avoir différentes finalités, par ex. le *lien avec le détenteur ou le dispositif* ainsi que la protection de l'intégrité.

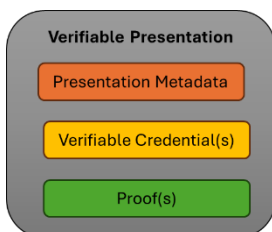


Figure 9 - Structure schématique d'une Verifiable Presentation

### 2.143 Verifier

Le terme **Verifier** est utilisé différemment selon le contexte . Selon le contexte, on distingue ce qui est vérifié, comme des identités, des données ou des processus dans un cadre informatique.

1. *Système IAM classique*: Le **Verifier** est une partie d'un *Identity Provider* (IdP) ou d'un *Relying Party* (RP). Il authentifie le *sujet* à l'aide de son *Authentication Service*, en comparant pour cela la valeur de sortie fournie par l'authentificateur avec les *Credentials* qu'il stocke. Ce faisant, il vient confirmer la prétendue *identité numérique* du sujet.
2. *SSI*: Un **Verifier** est un rôle qu'une *entité endosse* dans le contexte SSI. Un Verifier contrôle l'intégrité, la validité et, dans l'idéal, la paternité des *Verifiable Credentials* ou des *Verifiable Presentations* qu'il reçoit du Wallet d'un *Holder*.

### 2.144 Source faisant autorité

Une **source faisant autorité** est une source d'information, quelle qu'elle soit, à laquelle on peut se fier dans une situation concrète.

eIDAS 2015/1502 [23]: Une «„**source faisant autorité**“ désigne toute source d'information qui fournit de manière fiable des données, informations et/ou moyens de preuve précis pouvant être utilisés pour prouver l'identité.»

Les sources faisant autorité peuvent prendre de nombreuses formes différentes, par ex. registres, actes, etc.

L'eIDAS 2024/1183 [8] définit en outre: Une «„**source authentique**“ est un répertoire ou un système, administré sous la responsabilité d'un organisme du secteur public ou d'une entité privée, qui contient et fournit les attributs concernant une personne physique ou morale ou un objet et qui est considéré comme étant une source première de ces informations ou est reconnu comme authentique conformément au droit de l'Union ou au droit national, y compris les pratiques administratives.»

### 2.145 Broker

Un Broker propose des services communs, tels qu'administration des métadonnées, IdP-Discovery (*Discovery Service*), *Identity Linking* ou transformation de la *confirmation d'authentification et d'attributs* (*Broker Service*), pour tous les autres *prestataires de services IAM* et *Relying Parties* dans une *fédération d'identités* selon le modèle Hub-'n'-Spoke. Une *Authentication Proxy* est toujours une partie intégrante d'un Broker.

Synonyme: Hub

## 2.146 Confiance

La **confiance** dans le contexte IAM se réfère à la décision consciente d'accepter l'authenticité et l'intégrité d'un participant à un *processus*, même s'il existe un risque que ces attentes ne soient pas satisfaites.

La confiance est primordiale dans les *systèmes IAM*, car elle permet d'interagir en dépit d'inéluctables incertitudes. Les systèmes IAM sont conçus pour garantir un degré défini de sécurité et de fiabilité et rendre le risque maîtrisable. Ils instaurent ainsi la confiance nécessaire.

De manière formelle, la confiance entre deux *organisations, entités, domaines* est généralement définie dans *SLA*.

Synonyme: Trust (angl.)

## 2.147 Niveau de confiance

Le **niveau de confiance** précise la qualité d'authentification d'un *sujet*, en établissent une distinction entre personnes physiques et morales. Le modèle tiré d'eCH-0170 permet ainsi de déterminer le niveau de confiance global à partir de 4 sous-modèles (niveau de confiance de l'authentification, niveaux de confiance de l'enregistrement, niveaux de confiance du pilotage et niveaux de confiance de la fédération). [24]

Synonyme: Niveau de confiance

## 2.148 Wallet

Un **Wallet** est une application numérique qui permet aux *sujets* de stocker, de gérer et d'utiliser leurs clés cryptographiques, des *Verifiable Credentials* ou autres de manière décentralisée.

Synonyme: Identity Wallet (angl.)

## 2.149 Révocation

La **révocation** désigne le *processus* de déclaration de l'invalidité des *autorisations, moyens d'authentification, certificats numériques certificats, Verifiable Credentials* ou autres. La révocation permet de s'assurer qu'un élément donné n'est plus digne de confiance et ne peut plus être utilisé.

Exemples:

- Un Issuer peut révoquer les certificats numériques ou les *Verifiable Credentials* qu'il a lui-même émis. voir aussi *OCSP* et *CRL*.
- Un *Relying Party* retire à un *sujet* son *autorisation* d'accéder à une *ressource*.
- *API Tokens*: Invalidation des Tokens compromis ou obsolètes.
- *OTP Devices*: Les générateurs de mots de passe à usage unique peuvent être révoqués.
- Les *Active Session Tokens* sont révoqués en cas d'incident affectant la sécurité par exemple.

Synonymes: Révocation, Revocation (angl.), blocage

### 2.150 Service droit d'accès

Le **service de droits d'accès** [2] est un *service IAM* qui gère les règles d'utilisation d'une *ressource numérique*. Les règles sont définies sur la base de l'*authentification*, des *attributs*, du contexte de l'accès (localisation, heure, niveau de confiance, etc.) ou de modèles propres (groupes, *rôles*, autorisations individuelles).

Synonyme: Règle d'accès service

### 2.151 Contrôle d'accès

Le **contrôle d'accès** est un processus de surveillance et de pilotage de l'utilisation des *ressources*. Il a pour objectif de garantir l'intégrité, la confidentialité et la disponibilité des informations. L'*authentification* et l'*autorisation* des sujets accédant au système constituent une partie intégrante du contrôle d'accès.

Les décisions concernant l'accès sont généralement consignées par écrit dans un souci de garantir la traçabilité et la détectabilité.

En règle générale, les décisions concernant l'accès sont prises automatiquement sur la base des attributs ou des rôles d'un *sujet* authentifié (*ABAC* ou *RBAC*) et, le cas échéant, d'autres informations (par ex. contexte de l'accès, tel que le lieu, l'heure, le niveau de sécurité, etc.)

Synonyme: Access Control (angl.)

### 2.152 Zero-Knowledge Proof (ZKP)

Dans les **Zero-Knowledge Proofs (ZKP)**, on distingue entre protocoles interactifs et non interactifs.

Le protocole interactif est un type particulier de *Challenge-Response* protocol. Le vérificateur (Verifier) d'une preuve ne peut, en ZKP, démontrer à un tiers que le prouveur (Prover) a fourni cette preuve. Le prouveur peut ainsi nier auprès d'un tiers avoir fourni la preuve.

Le protocole non interactif est dérivé du protocole interactif. Dans le protocole non interactif, on distingue si le prouveur peut ou non désavouer la preuve qu'il a produite. La preuve d'un protocole non interactif est souvent désignée comme signature.

### 3 Exclusion de responsabilité – droits de tiers

Les normes élaborées par l'Association **eCH** et mises gratuitement à la disposition des utilisatrices et 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 une utilisatrice ou un utilisateur sur la base des documents qu'elle met à disposition. L'utilisatrice ou 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'utilisatrice ou 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'utilisatrice ou l'utilisateur pourrait subir par suite de l'utilisation des normes **eCH** est exclue dans les limites des réglementations applicables.

### 4 Droits d'auteur

Quiconque élabore des normes **eCH** en conserve la propriété intellectuelle. Elle ou 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 du détenteur/de la détentrice des droits d'auteur **eCH** respectifs, être utilisées, développées et déployées gratuitement et sans restriction.

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

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

## Annexe A – Références & bibliographie

- [1] NIST, «NIST Special Publication 800-63B - Digital Identity Guidelines,» June 2017. [Online]. Available: <https://pages.nist.gov/800-63-3/sp800-63b.html>.
- [2] eCH, «eCH-0107 Principes de conception pour la gestion des identités et des accès (IAM), V3.0,» 14 01 2019. [Online]. Available: <https://ech.ch/de/ech/ech-0107/3.0>.
- [3] NIST, «Attribute Based Access Control ABAC,» 24 Mai 2016. [Online]. Available: <https://csrc.nist.gov/Projects/Attribute-Based-Access-Control>.
- [4] OASIS, «Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0,» 15 March 2005. [Online]. Available: <https://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf>.
- [5] eCH, «eCH-0177 Modèle d'information pour le déroulement d'une affaire dans une «administration interconnectée Suisse», 24 février 2016. [Online]. Available: <https://ech.ch/de/ech/ech-0177/1.0>.
- [6] NIST, «Strength of Function for Authenticators - Biometrics (SOFA-B),» 16 October 2023. [Online]. Available: <https://pages.nist.gov/SOFA/>. [consulté en 2024].
- [7] Confédération suisse, «Loi fédérale sur la signature électronique, SCSE» 01 01 2020. [Online]. Available: <https://www.fedlex.admin.ch/eli/cc/2016/752/de>.
- [8] LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE, «Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen pour une identité numérique,» 11 4 2024. [Online]. Available: <http://data.europa.eu/eli/reg/2024/1183/oj>.
- [9] ISO/IEC JTC 1, «ISO/IEC 29115:2013,» ISO/IEC, 2013.
- [10] Wikipedia, 29 décembre 2024. [Online]. Available: [https://de.wikipedia.org/wiki/Personalausweis\\_\(Deutschland\)#Der\\_elektronische\\_Personalausweis\\_\(nPA\)](https://de.wikipedia.org/wiki/Personalausweis_(Deutschland)#Der_elektronische_Personalausweis_(nPA)). [consulté le 17 janvier 2025].
- [11] C. Neumann, T. Yu, S. Hartman und K. Raeburn, «RFC 4120: The Kerberos Network Authentication Service (V5),» juillet 2005. [Online]. Available: <https://www.rfc-editor.org/rfc/rfc4120.html>. [consulté le 24 janvier 2025].
- [12] T. Hardt, «RFC 6749: The OAuth 2.0 Authorization Framework,» octobre 2012. [Online]. Available: <https://www.rfc-editor.org/rfc/rfc6749.html>. [consulté le 24 janvier 2025].
- [13] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin und C. Adams, «X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP,» [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc6960>.

- [14] N. Sakimura, NAT.Consulting, J. Bradley, Yubico, M. Jones, Self-Issued Consulting, B. de Medeiros, Google, C. Mortimore und Disney, «OpenID Connect Core 1.0 incorporating errata set 2,» 15 déc. 2023. [Online]. Available: [https://openid.net/specs/openid-connect-core-1\\_0.html](https://openid.net/specs/openid-connect-core-1_0.html).
- [15] NIST, «Role Based Access Control RBAC,» 21 novembre 2016. [Online]. Available: <https://csrc.nist.gov/projects/role-based-access-control>.
- [16] OASIS, «Security Assertion Markup Language (SAML) V2.0 Technical Overview,» 25 March 2008. [Online]. Available: <http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html>.
- [17] OASIS, «Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard,» 15 March 2005. [Online]. Available: <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>.
- [18] OASIS, «Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0,» mars 2005. [Online]. Available: <https://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>.
- [19] OASIS, «Web Services Federation Language (WS-Federation) Version 1.2,» May 2009. [Online]. Available: <https://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.htm>.
- [20] OASIS, «WS-Trust 1.4,» April 2012. [Online]. Available: <https://docs.oasis-open.org/ws-sx/ws-trust/v1.4/errata01/ws-trust-1.4-errata01-complete.html>.
- [21] OASIS, «Web Services Security: SOAP Message Security Version 1.1.1,» May 2012. [Online]. Available: <https://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-SOAPMessageSecurity-v1.1.1.html>.
- [22] Assemblée fédérale de la Confédération suisse, «Loi fédérale sur le numéro d'identification des entreprises (LIDE) 18 juin 2010 (état au 1<sup>er</sup> septembre 2023),» [Online]. Available: [https://lex.weblaw.ch/lex.php?norm\\_id=431.03&source=SR&lex\\_id=83199&file=de-pdf\\_file\\_a.pdf](https://lex.weblaw.ch/lex.php?norm_id=431.03&source=SR&lex_id=83199&file=de-pdf_file_a.pdf).
- [23] LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE, «RÈGLEMENT (UE) No 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL,» 28 8 2014. [Online]. Available: <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32014R0910>.
- [24] eCH, «eCH-0170 Modèle de qualité pour l'authentification des sujets, V2.0,» 9 octobre 2017. [Online]. Available: <https://ech.ch/de/ech/ech-0170/2.0>.
- [25] eCH, «eCH-0219 – Glossaire IAM V2.0.0,» 2025. [Online]. Available: <https://ech.ch/fr/ech/ech-0219/2.0.0>.

## Annexe B – Collaboration & vérification

Dominic Baumann	BFH
Gerhard Hassenstein	BFH
Annett Laube	BFH
Daniel Muster	it-rm IT-Riskmanagement GmbH

## Annexe C – Abréviations et glossaire

2FA	Authentification à deux facteurs
ABAC	Attribute Based Access Control (contrôle des accès basé sur les attributs)
AD	Active Directory
AP	Attribute Provider
CA	Certification Authority
CRL	Certificate Revocation List
CP	Certificate Policy
EIDAS	Electronic Identification and Trust Services Regulation
FIDO	Fast IDentity Online
HoK	Holder of Key
IAM	Identity and Access Management
IdP	Identity Provider
IoT	Internet of Things
JWT	JSON Web Token
LB	Bénéficiaire de prestations
FP	Fournisseur de prestations
MFA	Multi-Factor-Authenticator / Authentification multi-facteurs
NIST	National Institute of Standards and Technology
nPA	Nouvelle pièce d'identité
OCSP	Online Certificate Status Protocol
OIDC	OpenID Connect
OTP	One-Time Password / mot de passe à usage unique
PIN	Numéro d'identification personnel
PKI	Public Key Infrastructure
RA	Registration Authority
RP	Relying Party

---

QES	Signature électronique qualifiée
RBAC	Role based Access Control (contrôle des accès basé sur les rôles)
RP	Relying Party
SAML	Security Assertion Markup Language
SFA	Single-Factor-Authenticator / Authentification à facteurs uniques
SLA	Service Level Agreement
SSL	Self-Sovereign Identity
SSO	Single Sign On
STS	Security Token Service
TSP	Trust Service Provider
IDE	Identifiant unique
VC	Verifiable Credential
FSC	Fournisseur de service de confiance
VDR	Verifiable Data Registry
VP	Verifiable Presentation
WAYF	Where Are You From (Discovery Service)
ZKP	Zero Knowledge Proof

## Annexe D – Modifications par rapport à la version précédente

Tous les termes de la norme version 1.0 ont été revus et adaptés. Les termes nouveaux, renommés et supprimés sont répertoriés ci-dessous.

- Abonné(e)
- Acteur
- Requérant/e
- Auth 2.0
- Compte d'utilisateur
- Challenge Response
- Claim
- Identité décentralisée
- Identité numérique
- Processus numérique
- Signature numérique
- Moyen d'identification électronique
- Système d'identification électronique
- Lien avec le dispositif
- Holder
- Holder of Key (HoK)
- IAM
- Lien avec le détenteur
- Institution
- Issuer
- Kerberos
- Magic Link
- Objet
- Passkey
- Mot de passe
- Authentification sans mot de passe
- Pièce d'identité physique
- Processus
- Provisionnement
- Message push
- Divulgateion sélective
- Self Sovereign Identity (SSI)
- SSO
- Stakeholder
- Verifiable Credential (VC)
- Verifiable Data Registry
- Verifiable Presentation (VP)
- Verifier (2<sup>e</sup> signification)

- Wallet
- ZKP

**Termes renommés:**

- E-Ressource -> Ressource numérique
- Service de ressources électroniques -> Service de ressources numériques

**Termes supprimés et fusionnés:**

- Fournisseur de services de certification
- Artefact
- Autorité d'attribut (AA)
- Agrégation d'attributs
- Demande d'attribut
- Autorité d'authentification (AuthnA)
- Demande d'authentification
- Facteur d'authentification
- Authentificateur
- Valeur de sortie d'un authentificateur
- Backend Attribute Exchange (BAE)
- Gestion des identités centrée sur l'utilisateur
- Métadonnées Community
- Composant destinataire
- Métadonnées d'entités
- Système IAM fédéré
- Fonction
- Globally Unique Identifier (GUID)
- Identity and Attribute Provider (IdP/AP)
- LinkedID
- Méta-domaine
- Quality Authentication Assurance (QAA)
- Système IAM répliquant
- Service Provider (SP)
- STIAM - SuisseTrust Identity and Access Management
- STIAM Certificate Authority (STIAM-CA)
- STIAM Identity and Attribute Bus
- STIAM Community
- Destinataire STIAM
- STIAM Hub
- STIAM IdP
- Composant STIAM
- STIAM Metadata Repository (STIAM-MDR)

- Plateforme STIAM
- STIAM RLM (Reporting-Logging-Monitoring)
- STIAM Sender
- Répertoire
- Administration
- WS-Federation
- WS-Trust

## **Annexe E – Liste des illustrations**

Figure 1 - Fonctionnement schématique d'un moyen d'authentification .....	13
Figure 2 - Claims individuelles et associées dans le contexte SSI .....	18
Figure 3 - Vue d'ensemble des différents certificats numériques.....	24
Figure 4 - Identité.....	27
Figure 5 - Modèle d'une fédération d'identité .....	28
Figure 6 - Namespaces & identificateurs.....	33
Figure 7 - Objet et sujet.....	43
Figure 8 - Structure schématique d'un Verifiable Credential.....	45
Figure 9 - Structure schématique d'une Verifiable Presentation .....	45

## **Annexe F – Liste des tableaux**

Tableau 1: Exemples de moyens d'authentification.....	14
---	----