

eCH-0170 – Modèle de qualité pour l’authentification des sujets

Nom	Modèle de qualité pour l’authentification des sujets
eCH-nombre	eCH-0170
Catégorie	Norme
Stade	Implémenté
Version	2.0.1
Statut	Approuvé
Date de décision	2025-09-03
Date de publication	2018-01-10
Remplace la version	2.0.0 – Minor Change
Conditions préalables	Aucune
Annexes	BEIL1_d_2017-06-02_eCH-0170_V2.0_Hilfsmittel_Vergleich-v1.0-und-v2.0.xlsx BEIL2_d_2017-06-02_eCH-0170_V2.0_Hilfsmittel_Vertrauensstufen-Rechner.xlsx
Langues	Allemand (original), français (traduction)
Groupe spécialisé	IAM
Éditeur / distribution	Association eCH, Räflestrasse 20, 8045 Zurich T 044 388 74 64 / info@ech.ch / www.ech.ch

Condensé

La norme *eCH-0170 Modèle de qualité pour l'authentification des sujets* a pour vocation de classer par qualité et de comparer l'authentification des personnes physiques et morales. A ce titre, la norme revêt une importance majeure, eu égard à l'élaboration d'une base de confiance commune dans les systèmes IAM fédérés et interorganisations, et peut être servir de point de départ pour la certification des prestataires IAM.

Le modèle de qualité décrit dans la présente norme définit **4 niveaux de confiance**. Ces 4 niveaux de confiance se composent des quatre modèles partiels suivants:

- *Modèle de qualité de l'authentification*: définit les niveaux de confiance de l'authentification (NDCA) sur la base de la force et des certifications possibles d'un moyen d'authentification.
- *Modèle de qualité de l'enregistrement*: définit les niveaux de confiance de l'enregistrement (NDCE), une distinction étant alors établie entre les personnes physiques et morales. La qualité de l'enregistrement des personnes physiques est déterminée par la force de l'identification de la personne ainsi que la transmission et la prolongation du moyen d'authentification. L'enregistrement des personnes morales est déterminé par la force de l'enregistrement de la personne physique correspondante, de l'identification de la personne morale ainsi que le lien entre les deux personnes.
- *Modèle de qualité du pilotage*: définit les niveaux de confiance du pilotage (NDCP) sur la base des critères surveillance, responsabilité et maturité.
- *Modèle de qualité de la fédération*: définit les niveaux de confiance de la fédération (NDCF) sur la base de l'authenticité, de la protection de la confidentialité, de la forme de transmission et du justificatif de détention de la confirmation d'authentification.

Pour satisfaire à un niveau de confiance du modèle complet, tous les modèles partiels doivent correspondre aux niveaux répertoriés. Le niveau le plus bas d'un modèle partiel détermine ainsi le niveau du modèle global.

Des critères de qualité, décrits en détail avec des exemples, sont attribués à chaque modèle partiel. Les critères de qualité contiennent des modalités devant être satisfaites. C'est ainsi que l'on obtient un niveau d'évaluation. Le niveau le plus bas des critères détermine ainsi le niveau de confiance du modèle partiel.

Le tableau suivant présente une vue d'ensemble des principales modalités pour chaque modèle partiel et leur composition par rapport aux quatre niveaux de confiance. Ces propriétés sont décrites et évaluées de manière détaillée et exhaustive aux chapitres 4 à 8.

Niveau de confiance	Désignation	NDCA	NDCE	NDCP	NDCF
1	Confiance nulle ou minime	Single Factor Authentication (SFA)	Renseignements déclaratifs	Aucune vérification, aucune responsabilité du CSP	Confirmation authentifiée
2	Peu de confiance	Multi Factor Authentication (MFA)	Vérification des justificatifs, présence en ligne, sécurité de transmission du moyen d'auth.	Règles internes et normes, responsabilité limitée	+ confirmation cryptée
3	Confiance considérable	HW-MFA	Validation des justificatifs reconnus, présence en ligne, transmission personnelle du moyen d'auth.	Vérification externe des règles et normes, responsabilité selon la loi	
4	Confiance élevée	HW-MFA certifié	Justificatifs officiellement reconnus, documentation de la présence (physique ou Virtual-in-Person), transmission autonome du moyen d'auth.	Normes vérifiées par l'instance officiellement accréditée, processus automatisés, responsabilité accrue et peine conventionnelle	+ authentification du porteur (HoK)

En conclusion, le modèle de qualité est mis en regard des normes internationales de l'ordonnance eIDAS 910/2014 [1], ISO/IEC 29115 [2], NIST SP 800-63-3 [3] (voir chapitre 8).

Table des matières

1	Introduction	9
1.1	Statut	9
1.2	Vue d'ensemble	9
1.3	Objectif du document	9
1.4	Utilisateurs de la norme	12
1.5	Délimitation	12
1.6	Architecture de l'information	13
1.7	Fondements	14
1.7.1	STORK.....	14
1.7.2	eIDAS.....	14
1.7.3	ISO.....	15
1.7.4	NIST.....	15
1.7.5	SCSE/OSCSE.....	15
1.8	Avantages	15
1.9	Priorités	15
1.10	Caractère normatif des chapitres	16
2	Terminologie	16
2.1	Authenticateur	16
2.2	Authentification	17
2.3	Confirmation d'authentification	17
2.4	Facteur d'authentification	17
2.5	Moyen d'authentification.....	18
2.6	Justificatif.....	20
2.7	Caractéristique biométrique	20
2.8	Certificate Authority/Certification Authority (CA).....	21
2.9	Client Platform	21
2.10	Credential	21
2.11	Credential Service Provider (CSP).....	22
2.12	E-Identity	22
2.13	Moyen d'identification électronique	22

2.14	Système d'identification électronique	22
2.15	Période de définition	23
2.16	Fédération / Federation	23
2.17	Identification	24
2.18	Document d'identité	24
2.19	Identity Provider (IdP)	24
2.20	Personne morale	24
2.21	Caractéristique physique	24
2.22	Période d'exécution	24
2.23	Autorité d'enregistrement/Registration Authority (RA)	25
2.24	Sujet	25
2.25	Unité IDE	26
2.26	Source fiable	26
2.27	Administration	26
3	Modèle de qualité	27
3.1	Niveaux de confiance	28
3.2	Composition des niveaux de confiance	30
3.3	Utilisation pour classer les prestataires IAM	31
3.3.1	Classer les RA	31
3.3.2	Classer un IdP	31
3.3.3	Classer un CSP	31
3.4	Critères de qualité	32
3.5	Conditions préalables	32
4	Modèle de qualité de l'authentification	35
4.1	Niveaux de confiance de l'authentification (NDCA)	35
4.2	Critères d'authentification	36
4.2.1	Moyen d'authentification	36
4.2.2	Certification du moyen d'authentification	37
4.2.3	Réauthentification	38
5	Modèle de qualité de l'enregistrement	39
5.1	Niveaux de confiance de l'enregistrement (NDCE)	39

5.1.1	Pour les personnes physiques	39
5.1.2	Pour les personnes morales	40
5.2	Critères de l'enregistrement	41
5.2.1	Facteurs d'identification.....	41
5.2.1.1	Facteur Présence.....	41
5.2.1.2	Facteur Justificatif	42
5.2.1.3	Facteur Validation des renseignements	44
5.2.1.4	Facteur Non-répudiabilité	45
5.2.1.5	Facteur Procuration.....	46
5.2.2	Identification des personnes physiques	47
5.2.3	Identification des personnes morales	49
5.2.4	Lien entre personne physique et morale.....	50
5.2.5	Transmission du moyen d'authentification	51
5.2.6	Prolongation/remplacement du moyen d'authentification.....	54
6	Modèle de qualité du pilotage	56
6.1	Niveaux de confiance du pilotage (NDCP)	56
6.2	Critères du pilotage	57
6.2.1	Surveillance.....	57
6.2.2	Responsabilité.....	58
6.2.3	Maturité	59
7	Modèle de qualité de la fédération	61
7.1	Niveaux de confiance de la fédération (NDCF)	61
7.2	Critères de la fédération	62
7.2.1	Justificatif de détention de la confirmation d'authentification.....	62
7.2.2	Authenticité de la confirmation d'authentification	63
7.2.3	Protection de la confidentialité de la confirmation d'authentification	63
7.2.4	Forme de transmission de la confirmation d'authentification.....	64
8	Comparaison avec les normes internationales	65
8.1	Modèle de qualité de l'authentification	66
8.2	Modèle de qualité de l'enregistrement	67
8.2.1	Enregistrement pour les personnes physiques	67

8.2.2	Enregistrement des personnes morales	67
8.3	Modèle de qualité du pilotage	68
8.4	Modèle de qualité de la fédération.....	68
9	Exclusion de responsabilité - droits de tiers	69
10	Droits d'auteur	69
Annexe A - Références & bibliographie		70
Annexe B - Collaboration & vérification.....		72
Annexe C - Abréviations et glossaire		72
C.1	Abréviations.....	72
C.2	Glossaire	73
Annexe D - Modifications par rapport à la version précédente.....		76
Annexe E - Liste des illustrations.....		78
Annexe F - Liste des tableaux		79
Annexe G - Processus		81
G.1	Authentifier le sujet et fédérer l'identité.....	81
G.1.1	Authentifier le sujet.....	81
G.1.2	Fédérer l'identité	82
G.2	Enregistrer un sujet.....	84
G.2.1	Vérifier l'identité de la personne physique	85
G.2.2	Vérifier l'identité d'une personne morale.....	85
G.2.3	Stipuler le moyen d'authentification	86
G.3	Piloter l'IAM.....	87
G.3.1	Stipuler les niveaux de confiance	87
G.3.2	Stipuler les prestataires de service.....	88
G.3.3	Stipuler les processus de pilotage	88
G.3.4	Evaluer et gérer les risques.....	89
Annexe H - Exigences relatives aux moyens d'authentification.....		90
H.1	Memorized Secrets	90
H.2	Look-Up Secrets	90
H.3	Out of Band Authenticators	91
H.4	OTP Devices.....	91

H.5 Single Factor Cryptographic Devices.....	92
H.6 Multi-Factor Cryptographic Software	92
H.7 Multi-Factor Cryptographic Devices.....	92
Annexe I - Exigences relatives au facteur Validation des renseignements....	93

Remarque

La forme épiciène sera évitée lorsque cela est possible dans un souci de lisibilité et d'intelligibilité. Le nom commun sera utilisé si besoin afin de simplifier la forme, ce qui implicitement couvre l'autre genre.

1 Introduction

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 Vue d'ensemble

La norme eCH-0107 [4] regroupe les concepts et documents auxiliaires complémentaires relatifs aux solutions IAM fédérées.

La présente norme eCH-0170 consiste en un modèle de qualité et fait partie du groupe des documents auxiliaires complémentaires (voir également Figure 1), au même titre que la norme eCH-0171 [5].

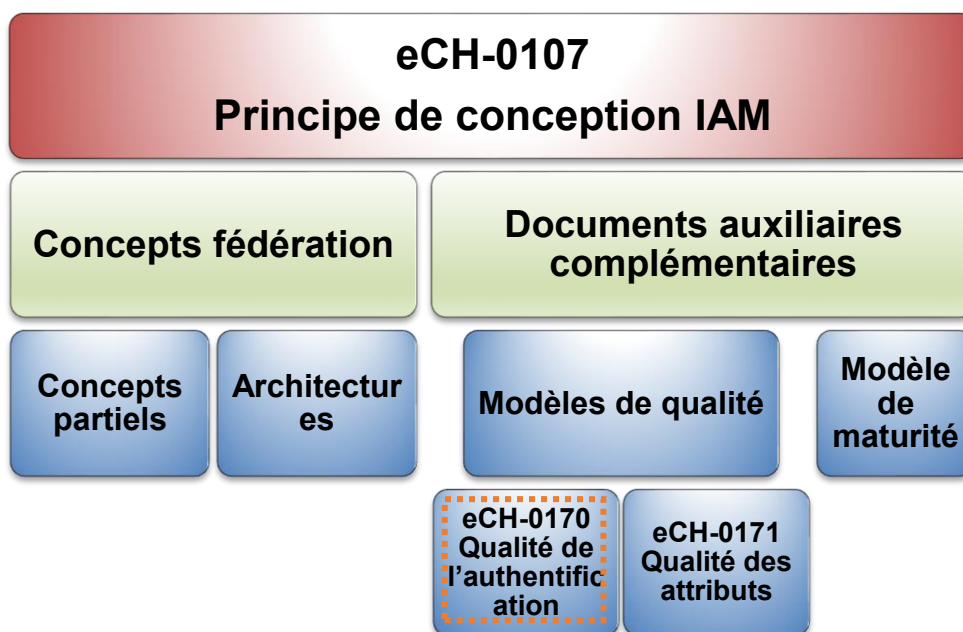


Figure 1: Classification de la norme de la norme eCH-0170

1.3 Objectif du document

Cette norme a pour vocation de fournir aux Stakeholders dans le domaine de l'IAM (selon la définition des Stakeholders dans eCH-0107 [4]), un règlement relatif à la classification qualitative et à la comparaison de l'authentification des sujets. Les Stakeholders peuvent ainsi mieux apprécier dans quelle mesure un sujet, qui s'est authentifié dans un système IAM donné, est réellement la personne qu'il déclare être.

Comme le montre la Figure 2, cette norme traite en premier lieu des systèmes IAM interorganisations fédérés. Cela signifie que dans un système IAM fédéré typique, l'Identity Provider (IdP) et le Relying Party (RP) font partie d'organisations différentes. Ainsi, les sujets et les ressources se trouvent-ils dans des domaines distincts. Dans un système IAM fédéré, il existe une séparation logique et physique entre l'IdP et le RP et les informations relatives à l'authentification et au sujet sont transmises via un réseau.

Toutefois, il est aisément possible d'appliquer le modèle de qualité pour les systèmes IAM non fédérés ou internes à une organisation. En particulier, les Stakeholders, qui doivent, le cas échéant, être intégrés ultérieurement à un système d'identité fédéré, devraient commencer suffisamment tôt à mettre en œuvre les exigences auxquelles ils sont confrontés dans ce contexte. L'UE elle-même cherche à mettre en place un marché numérique unique. La norme eCH-0170 tient compte des exigences internationales et de l'UE afin de contribuer à l'interopérabilité au niveau international et européen des solutions suisses, qui sont conformes à cette norme.

Cette norme se veut non seulement une règle d'évaluation des prestataires IAM, mais peut aussi être mise à contribution en tant que point de départ pour la certification des prestataires IAM.

La Figure 2 présente les principaux éléments nécessaires à la détermination de la qualité de l'authentification d'un sujet. Le code couleur utilisé dans cette figure comme dans les autres modèles du document est le même que celui du .

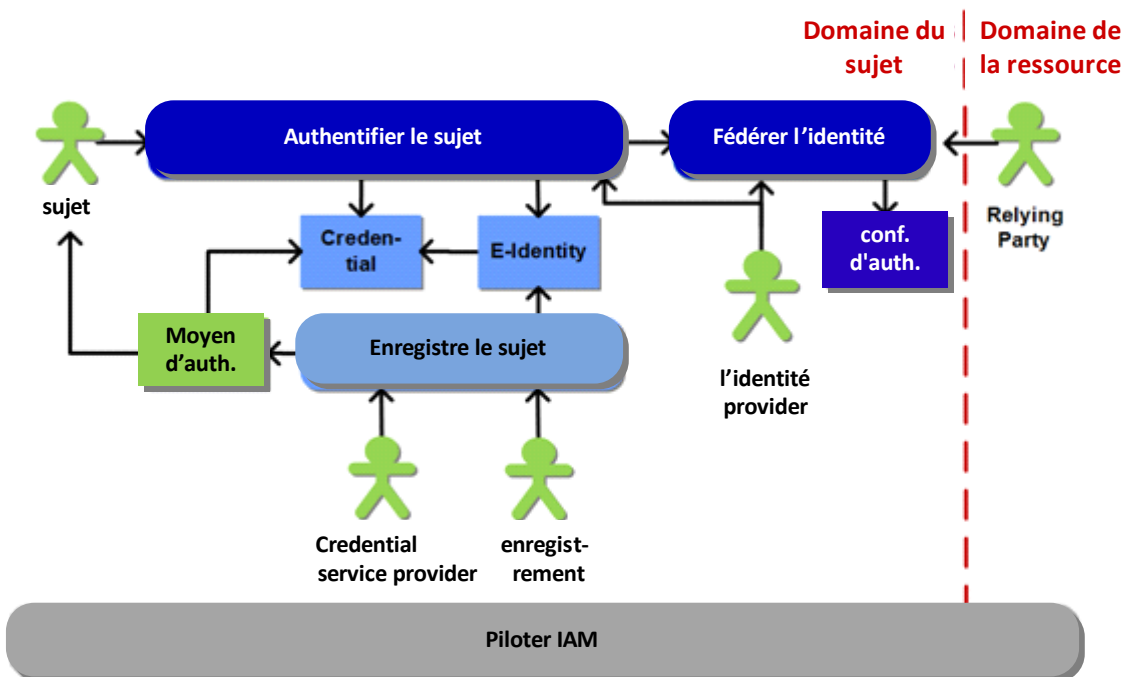


Figure 2: Modèle de processus Authentification d'un sujet

Le modèle s'articule autour de l'authentification du sujet pour la période d'exécution (processus *Authentifier le sujet*). Outre l'authentification du sujet, cette opération a pour objectif de permettre de contrôler les accès à une ressource par un Relying Party (RP). La présente norme ne traite pas du contrôle des accès.

Lors de l'authentification, le sujet utilise un moyen d'authentification, qui prend en charge un ou plusieurs facteurs d'authentification. Au cours de l'authentification, un authentificateur convertit au moyen d'un secret – accessible à lui seul – les possibles facteurs d'authentification en une valeur de sortie.

Le service authentifiant (IdP) contrôle la valeur de sortie de l'authentificateur au moyen du Credential, qui forme le lien entre l'authentificateur et l'E-Identity (voir également chapitre 3.5). Si la vérification est positive, l'authentification est réussie et l'E-Identity déclarée est confirmée.

Si l'authentification du sujet a lieu dans un système IAM fédéré, le résultat de cette opération est transmis, une fois le sujet authentifié auprès de l'IdP, par ce dernier au RP sous la forme d'une confirmation d'authentification (processus *Fédérer l'identité*).

Avant de pouvoir s'identifier pour la période d'exécution, un sujet doit s'enregistrer auprès d'une autorité d'enregistrement (RA). La RA vérifie l'identité du sujet et crée une E-Identity avec un identificateur unique pour le sujet. Le Credential Service Provider (CSP) délivre pour cette E-Identity un nouveau moyen d'authentification ou en associe un existant à cette E-Identity. Le lien entre l'E-Identity et le moyen d'authentification apparaît dans le Credential. Le moyen d'authentification peut prendre en charge un ou plusieurs facteurs d'authentification.

La RA et l'IdP peuvent faire partie intégrante du CSP ou être mandatés par ce dernier.

Tous les Stakeholders impliqués doivent au préalable s'être mis d'accord conjointement sur les règles et conditions cadres nécessaires au fonctionnement du système IAM (processus *Piloter l'IAM*).

gris	La couleur grise dans ce document représente les éléments, qui sont déjà actifs avant le moment de la définition (ex. Governance).
bleu clair	La couleur bleu clair est utilisée, de manière cohérente, dans ce document pour la période de définition, au cours de laquelle toutes les informations sont affectées aux éléments d'information (c'est à dire définis).
bleu foncé	La couleur bleu foncé est utilisée, de manière continue, dans ce document pour la période d'exécution. Une propriété est confirmée pour la période d'exécution sur la base des éléments d'information.
vert clair	La couleur vert clair est utilisée, de manière cohérente dans le présent document, pour les objets du monde réel.

Tableau 1: Code de couleur dans le document

1.4 Utilisateurs de la norme

Cette norme peut être utilisée de différentes façons par les Stakeholders fondamentaux au sein d'une fédération d'identité (voir également eCH-0107 [4]):

- Le modèle de qualité décrit aide les **sujets** à mieux comprendre les exigences relatives aux différents moyens d'authentification ainsi qu'aux processus d'enregistrement.
- Les **Relying Parties** peuvent évaluer et comparer les prestations des prestataires IAM au moyen de la présente norme.
- Les **prestataires IAM** peuvent utiliser cette norme à des fins de spécification et d'évaluation de leurs propres prestations.
- Les **régulateurs** bénéficient ainsi d'une compréhension conceptuelle des points de rattachement pour la fixation des règles.

1.5 Délimitation

Ce chapitre montre quelles sont les parties qui sont intégrées ou traitées dans la détermination du modèle de qualité, et quelles sont celles qui ne le sont pas.

- Cette norme se contente de traiter de l'authentification des personnes physiques et des personnes morales selon l'art. 52 et suivants du CC ainsi que selon les dispositions applicables du droit des sociétés du CO.
- Les personnes physiques, qui agissent pour le compte d'une organisation (ex. dans l'administration), d'une entreprise ou d'une unité IDE, ne sont pas différenciées lors de l'authentification de personnes physiques, qui agissent en leur nom propre, et devraient être traitées en conséquence lors de la définition des droits d'accès (ex. par l'attribution de rôles ou l'affectation d'attributs).
- L'authentification des services et des objets (ex. nœuds de capteurs dans l'Internet des choses ou communication machine-machine entre serveurs) n'est pas prise en compte dans cette version en raison de l'absence de normes internationales¹.
- Cette norme définit les critères de qualité pour l'authentification de personnes physiques et morales dans les systèmes IAM fédérés et non-fédérés. Les exigences propres aux systèmes IAM dotées d'une infrastructure centrale de transmission ou une interfédération ne sont pas prises en compte et doivent être complétées le cas échéant.

¹A titre d'exemple, les premières tentatives de normalisation sont disponibles sur: <https://kantarainitiative.org/confluence/display/IDoT/Home>

1.6 Architecture de l'information

L'architecture de l'information de la Figure 3 vient compléter l'architecture de l'information de eCH-0107 [4].

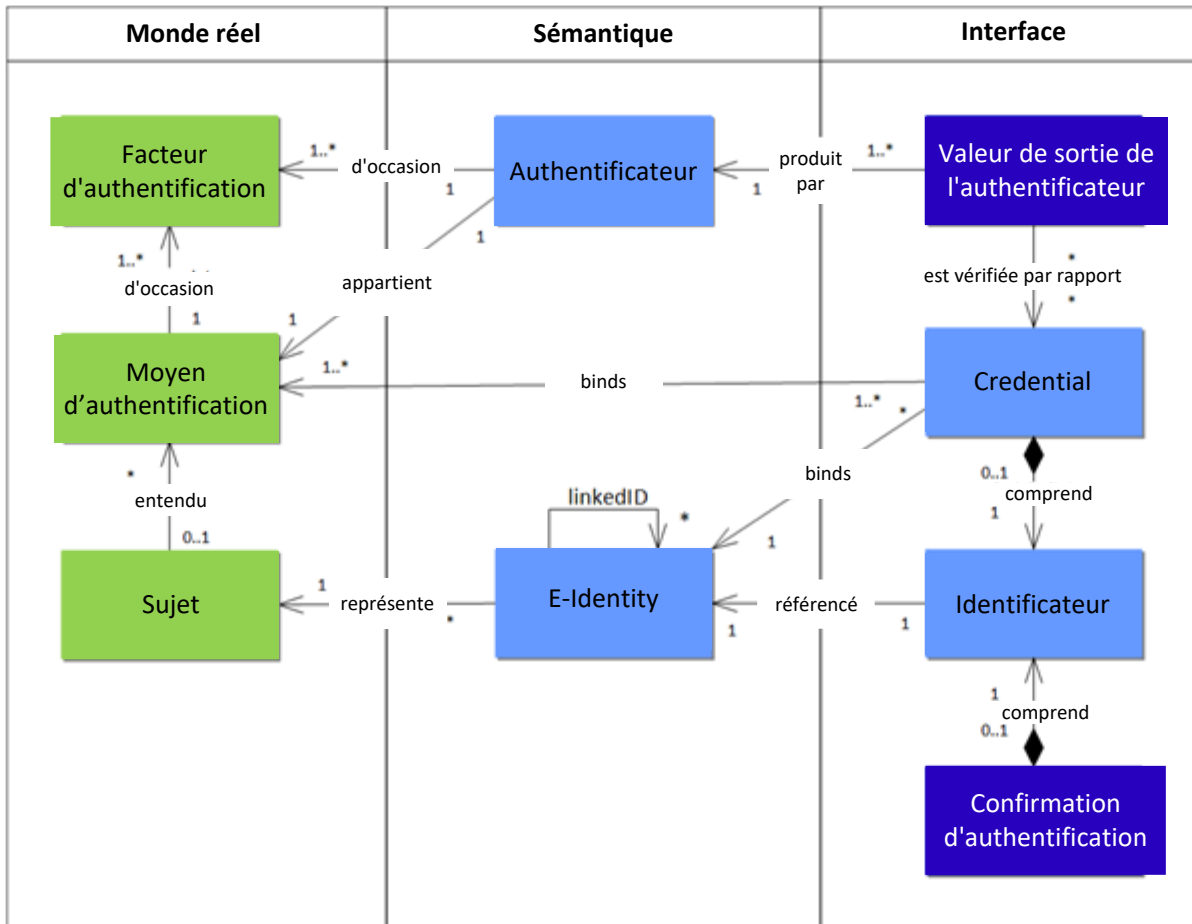


Figure 3: Architecture de l'information

L'architecture de l'information (voir Figure 3) établit une distinction claire entre facteur d'authentification (voir chapitre 2.4), moyen d'authentification (voir chapitre 2.5), authentificateur (voir chapitre 2.1) et Credential (voir chapitre 2.9). Le moyen d'authentification et les facteurs d'authentification utilisés par ce dernier sont les objets du monde réel. L'authentificateur est utilisé dans le processus d'authentification afin de convertir les facteurs d'authentification en une valeur de sortie.

Dans le Credential, le lien entre un moyen d'authentification et l'E-Identity est constitué et enregistré au moyen de l'identificateur pour la période de définition. Au cours de la période d'exécution, la valeur de sortie de l'authentificateur est vérifiée à l'aide du Credential. Si la vérification est positive, l'authentification est considérée comme réussie et l'E-Identity déclarée est confirmée.

Exemple

Dans le cas d'une SuisseID, le moyen d'authentification est le Crypto Device (Smartcard) avec Driver et Middleware. Ce moyen d'authentification contient deux facteurs d'authentification: les Hardware-Token avec clé privée (détention) et le PIN (connaissances). La saisie du PIN, le deuxième facteur d'authentification (clé privée) activé sur SuisseID, afin de calculer avec la fonction d'authentification (Signature), une valeur de sortie, qui sera transmise au service authentifiant (IdP). Grâce au Credential fourni (certificat), qui contient l'identificateur (numéro SuisseID), l'authenticité et la validité de la valeur de sortie sont contrôlées par l'IdP SuisseID (ou directement par une application Web). Le résultat de ce contrôle est transmis au Relying Party (ou en interne dans une application) en tant que confirmation d'authentification.

1.7 Fondements

La version 1.0 de la norme eCH-0170 reposait principalement sur le Quality Authentication Assurance Framework STORK [6]. La présente version s'appuie sur d'autres modèles de qualité européens et internationaux, présentés de façon succincte dans la suite du document.

1.7.1 STORK

STORK était un projet de l'Union européenne mené en deux phases, qui s'est achevé fin 2015. Ce projet avait pour objectif de créer une plateforme d'interopérabilité européenne pour les solutions d'identité électronique, devant permettre à un ressortissant de l'UE d'utiliser son identité électronique nationale (eID) dans les autres pays membres. Dans le cadre du projet STORK, un modèle de qualité, le Quality Authentication Assurance Framework [6] a été défini à des fins d'évaluation et de comparaison des identités électroniques. Ce modèle de qualité a servi de base à l'élaboration de la version 1.0 de eCH-0170.

Par la suite, ce modèle de qualité a été pris en compte lors de l'élaboration de l'ordonnance eIDAS 910/2014 [1].

1.7.2 eIDAS

eIDAS repose sur le règlement de l'UE n° 910/2014 relatif à l'identification électronique et les services de confiance pour les transactions électroniques sur le marché intérieur [4] et le règlement d'exécution de l'UE 2015/1502 [7]. Il a pour but d'établir un système d'identité fédéré et transfrontalier entre les Etats-membres. Les exigences de ce règlement de l'UE s'appliquent aux moyens d'identification électronique *notifiés*, qui ont été délivrés selon un système d'identification électronique notifié. Les concepts et méthodes du projet STORK ont été repris et en partie adaptés.

Le modèle de qualité pour les systèmes d'identification électroniques d'eIDAS est divisé en *niveaux de sécurité*, les différents niveaux étant «faible», «significatif» et «élevé». eIDAS limite l'application de ces niveaux de sécurité aux systèmes d'identification électroniques *notifiés*. On établit une distinction entre personnes physiques et morales.

Si les règlements eIDAS ne revêtent pas de caractère obligatoire en Suisse, ils n'en sont vraisemblablement pas moins fondamentaux pour l'acceptation des identités électroniques suisses en cas d'éventuelle coopération. Ceci explique que le modèle de qualité eIDAS serve notamment de base à l'élaboration de cette norme.

1.7.3 ISO

L'International Organization for Standardization (ISO) a élaboré la norme ISO/IEC 29115 [2]. La norme décrit 4 «levels of entity authentication assurance», ou LoA en abrégé. Ces 4 niveaux ont été pris en compte lors de l'élaboration du règlement eIDAS 910/2014 [1].

1.7.4 NIST

Le NIST (National Institute of Standards and Technology) a élaboré, avec la Special Publication «Digital Authentication Guideline» NIST SP 800-63-3 [3] disponible en plusieurs versions, une norme globale servant de directive de mise en œuvre des systèmes d'authentification numériques par les autorités nationales des Etats-Unis. Dans la mesure où cela est judicieux, le présent document se réfère à NIST SP 800-63-3 [3] pour définir la terminologie. En particulier, le glossaire [8] figurant dans le document NISTIR 7298 révision 2 a été utilisé pour cette norme.

1.7.5 SCSE/OSCSE

SCSE est la loi fédérale sur les services de certification dans le domaine de la signature électronique (RS 943.03) en Suisse. OSCSE [10] est l'ordonnance associée à la SCSE relative aux services de certification dans le domaine de la signature électronique (RS 943.032).

1.8 Avantages

Le modèle de qualité défini dans cette norme permet d'évaluer et de comparer les systèmes IAM fédérés et non fédérés. La norme propose une directive relative aux exigences devant être remplies afin d'obtenir une qualité correspondante.

Le modèle de qualité étant également axé sur l'eIDAS, il peut être comparé aux solutions européennes en matière d'identité et constitue ainsi une base pour l'interopérabilité à venir avec les solutions européennes et internationales.

1.9 Priorités

Le chapitre 2 définit la terminologie utilisée dans le document.

Le chapitre 3 décrit le modèle de qualité avec ses quatre niveaux de confiance et la composition avec quatre modèles partiels. En outre, l'utilisation du modèle de qualité est prise en compte pour la classification qualitative des différents prestataires IAM. Ce chapitre fournit une vue d'ensemble de tous les critères de qualité fondamentaux et répertorie les conditions préalables pour leur utilisation.

Les chapitres suivants proposent une description des critères et de leur composition pour la détermination des niveaux de confiance pour les 4 modèles partiels :

Chapitre 4: Modèle de qualité de l'authentification,

Chapitre 5: Modèle de qualité de l'enregistrement,

Chapitre 6: Modèle de qualité du pilotage

Chapitre 7: Modèle de qualité de la fédération

Le chapitre 8 propose une comparaison des niveaux de confiance définis avec les principaux modèles de qualité internationaux.

1.10 Caractère normatif des chapitres

Les chapitres de la présente norme sont de nature normative ou également descriptive. Tableau 2 définit la classification des chapitres.

Chapitre	Description
1 Introduction	Descriptif
2 Terminologie	Normatif
3 Modèle de qualité	Normatif, hormis 4.5
4 Modèle de qualité de l'authentification	Normatif
5 Modèle de qualité de l'enregistrement	Normatif
6 Modèle de qualité du pilotage	Normatif
7 Modèle de qualité de la fédération	Normatif
8 Comparaison avec les normes internationales	Descriptif

Tableau 2: Vue d'ensemble du caractère normatif des chapitres

Les annexes A, C et H ont également caractère normatif. Toutes les autres annexes de cette norme sont descriptives.

2 Terminologie

La présente norme eCH-0170 utilise par principe la terminologie de la norme eCH-0107 [4]. De plus, d'autres notions, qui sont nécessaires à la compréhension du présent document, sont utilisées selon un degré d'importance variable ou été complétées, sont répertoriées par ordre alphabétique ci-dessous.

2.1 Authentificateur

L'**authentificateur** est la représentation fonctionnelle du *moyen d'authentification du monde réel*. La fonction d'un authentificateur permet en général de créer une valeur de sortie à partir d'une valeur de saisie (Challenge) et d'une valeur secrète. En fonction de la modalité, la valeur secrète doit être activée par un deuxième facteur (PIN).

Synonyme: fonction d'authentification, authenticator en anglais

2.2 Authentification

L'**authentification** est l'opération qui consiste à vérifier l'*E-Identity* déclarée d'un sujet selon des règles précises. Ce sont ces règles qui fixent le niveau de sécurité recherchée par l'authentification.

Synonyme: authentification.

Cas spécial eIDAS: authentification dynamique (pas de SSO)

2.3 Confirmation d'authentification

La **confirmation d'authentification** est le justificatif, qui est délivré par l'*Identity Provider* une fois le sujet authentifié avec succès. La confirmation d'authentification est valable pour une période définie et a l'un des niveaux de confiance décrits dans le présent document.

Exemples

Dans la Security Assertion Markup Language (SAML) [11], la confirmation d'authentification est l'«Authentication Assertion» et est délivrée par le (SAML) Identity Provider.

Dans l'OIDC [Ref], la confirmation d'authentification est appelée «ID Token» et délivrée par l'«Authorization Server».

Dans Kerberos, la confirmation d'authentification est un «Ticket Granting Ticket» (TGT) et délivrée par le Kerberos Distribution Center (KDC).

2.4 Facteur d'authentification

Les facteurs d'authentification sont les informations et/ou les processus, qui peuvent être utilisés afin d'authentifier un sujet. Les facteurs d'authentification peuvent reposer sur quatre caractéristiques distinctes voire des combinaisons:

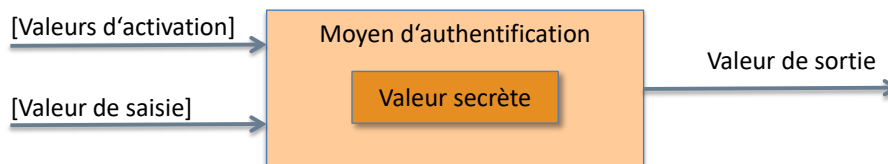
- Facteur d'authentification en fonction de la détention: repose sur la détention (c'est-à-dire ce que le sujet détient, ex. certificat, Hardware-Token avec clé privée, carte d'identité ou passeport électronique),
- Facteur d'authentification en fonction des connaissances: repose sur les connaissances (c'est-à-dire ce que le sujet sait, ex. mot de passe, PIN),
- Facteur d'authentification inhérent: repose sur une *caractéristique biométrique* (c'est-à-dire ce que le sujet est, comme l'iris, la rétine, les empreintes digitales),
- Facteur d'authentification basé sur le comportement: repose sur le comportement (ce que le sujet a l'habitude de faire, ex. façon de signer dynamique).

Synonyme: caractéristique d'authentification

2.5 Moyen d'authentification

Un **moyen d'authentification** est ce qu'un sujet a en sa détention et sous son contrôle (généralement une clé cryptographique, un secret ou une caractéristique biométrique). Un moyen d'authentification n'a pas forcément de forme matérielle, il peut aussi être un Soft-Token ou un composant de logiciels. Un moyen d'authentification peut utiliser un (*single-factor authenticator*) ou plusieurs facteurs d'authentification (*multi-factor authenticator*) indépendants (voir également Annexe H -Exigences relatives aux moyens d'authentification).

La valeur de sortie générée par le moyen d'authentification (*Authenticator output* ou *authenticator response* en anglais) est produite par une fonction mathématique (*authentificateur* ou fonction d'authentification) à partir d'une valeur secrète (ex. clé privée), d'une ou de plusieurs valeurs d'activation facultatives (ex. PIN ou informations biométriques), et d'une ou de plusieurs valeurs de saisie facultatives (ex. valeurs aléatoires ou Challenges). Dans un cas anodin, le moyen d'authentification peut être la valeur secrète elle-même (ex. dans le cas d'un mot de passes). Voir Tableau 3 pour plus d'exemples.



Valeurs de sortie=
 fonction d'authentification(valeur secrète,
 [valeurs d'activation],
 [valeurs de saisie])

Figure 4: Schéma de fonctionnement d'un moyen d'authentification

	Mot de passe	Liste de dé-compte	SMS	OTP	Mobile-ID	SuisseID
Type	SFA	SFA	SFA	(HW-)MFA	HW-MFA	HW-MFA
Valeur de saisie	-	Index	Code envoyé	Seed	Code envoyé	Nonce
Valeur secrète	Mot de passe	Valeur (alpha)numérique	-	Device Key	Private Key	Private Key
Valeur d'activation	-	-	-	-	PIN	PIN

		Mot de passe	Liste de dé-compte	SMS	OTP	Mobile-ID	SuisseID
Authenti-ficateur		-	Liste des valeurs (alpha) numériques	Por-table	Device	Carte SIM	Crypto-De-vice
Fonction d'authentifi-cation		Aucune ou fct. hash.	Sélection	Lecture et écriture du code envoyé	HMAC	Signature	Signature
Valeur de sortie		Mot de passe, hash du mot de passe	Valeur (alpha)numérique	Code envoyé	Code	Sign (code envoyé)	Sign (Nonce)
Credential²		Mot de passe, Hash du mot de passe	Liste des valeurs (alpha)numériques	n° mo-bile	n° de-vice/Seed	Carte SIM avec n° de mobile/Public Key	Certificate

Tableau 3: Exemples de moyen d'authentification et de Credential associé

Synonyme:

- Authenticator (voir NIST 800-63-3 [3]), auparavant désigné comme **Token** dans NIST 800-63-2 [13].
- Désigné comme identity token ou authentication token dans STORK

² L'Identifiant, comme le nom de l'utilisateur par exemple, fait toujours partie du Credential.

2.6 Justificatif

Un **justificatif** pour la vérification de l'identité est un document ou objet émanant d'une source fiable, qui contient des renseignements concernant le requérant.

Un justificatif doit contenir le nom du requérant. Il peut en outre inclure un identificateur sans ambiguïté, une caractéristique physique et biométrique, mais aussi d'autres renseignements sur le requérant. Il devrait comprendre des caractéristiques de sécurité, qui rendent toute reproduction difficile.

Exemples:

- Acte certifié,
- Cartes de crédit,
- Permis de conduire,
- Pièces d'identité.

2.7 Caractéristique biométrique

Une **caractéristique biométrique** est une *caractéristique physique* d'une personne, qui permet de la distinguer suffisamment des autres et peut donc être utilisée à des fins d'identification. Une caractéristique biométrique devrait peu changer au fil du temps. Des combinaisons de plusieurs caractéristiques sont possibles, ex. forme du visage combinée à la reconnaissance vocale. L'utilisation des caractéristiques biométriques à des fins d'authentification présente l'inconvénient majeur de ne pouvoir les déclarer non valides ni les régénérer à nouveau lorsqu'elles sont compromises

Les principales caractéristiques biométriques sont:

- Empreintes digitales,
- Signature (dynamique),
- Géométrie du visage,
- Portrait (photo),
- Motifs de l'iris,
- Rétine,
- Géométrie de la main,
- Géométrie des doigts,
- Forme des oreilles,
- Voix (timbre),
- ADN,
- Odeur,
- Frappe au clavier.

A l'heure actuelle, les seules caractéristiques utilisées dans la plupart des cas afin d'identifier les personnes physiques sont les suivantes:

- Empreintes digitales,
- Iris,
- Rétine,
- Géométrie du visage,
- Portrait (photo).

Les caractéristiques biométriques peuvent également être classées selon la fonction, la sécurité, la falsifiabilité et la convivialité d'utilisation. NIST a apporté une première contribution dans ce sens avec sa publication en ligne «Strength of Function for Authenticators – Biometrics» [14] ou SOFA-B en abrégé.

2.8 Certificate Authority/Certification Authority (CA)

Une **Certificate Authority** est un Credential Service Provider spécial (CSP), qui délivre, renouvelle et révoque des certificats numériques (Public Key certificate, e.g. X.509) en tant que moyen d'authentification.

Synonyme: Certification Service Provider, Trust Service Provider (TSP)

Synonyme français: service de certification pour les certificats numériques, fournisseur de services de confiance

2.9 Client Platform

La **Client Platform** est le système ou l'appareil, depuis lequel le sujet initie un processus d'authentification. Il peut s'agir par exemple d'un navigateur sur un PC ou d'une application sur un appareil mobile.

2.10 Credential

Un **Credential** représente une quantité de données (non matériel ou autre Container physique), par lequel une identité électronique (*E-Identity*) est associée à un moyen d'authentification détenu et contrôlé par le sujet.

Le Credential est utilisé avec la valeur d'émission du moyen d'identification afin de justifier l'E-Identity déclarée. En fonction des facteurs d'authentification utilisés, il peut s'agir par exemple du hash d'un mot de passe, d'une représentation d'une caractéristique biométrique ou d'un certificat (voir Tableau 3) qui, au moment de la définition, a été associé par un CSP à une E-Identity.

Avant d'utiliser un Credential, il faut toujours s'assurer qu'il est bien authentique et digne de confiance.

(voir également ISO 29115 [2], annexe B et NIST SP 800-63B [15], chap 3).

Synonyme: justificatif d'identité

2.11 Credential Service Provider (CSP)

Un **Credential Service Provider** est une entité, qui agit en tant qu'éditeur digne de confiance de certificats numériques et d'autres tokens de sécurité (moyens d'authentification).

Le CSP peut contenir sa propre Registration Authority (RA) et comprendre des services d'identification (Identity Provider, voir chapitre 2.20). Un CSP peut se présenter en tant qu'instance publique ou être intégré comme service dans un domaine fermé.

Synonyme: est désigné comme Identity Provider (IdP) dans NIST 800-63-3 [3].

2.12 E-Identity

Une **E-Identity** est la représentation d'un sujet. Une *E-Identity (identité numérique)* a un *identificateur* (nom sans ambiguïté), dans la plupart des cas avec une quantité d'*attributs supplémentaires*, qui peuvent être affectés à un *sujet* sans ambiguïté à l'intérieur d'un espace de noms. Un *sujet* peut avoir plusieurs *E-Identities*.

Une **E-Identity notifiée** est une E-Identity, qui doit remplir toutes les conditions stipulées par eIDAS 910/2014 [1] article 7.

2.13 Moyen d'identification électronique

Terme tiré d'eIDAS 910/2014 [1]: un «*moyen d'identification électronique*» est une *unité matérielle et/ou immatérielle, qui contient les données d'identification des personnes et est utilisée à des fins d'authentification dans les services en ligne.*

Un **moyen d'identification électronique** contient des facteurs d'authentification, les attributs pour les personnes, et a une validité. Dans le cas d'une authentification (dynamique), le processus global *Authentifier le sujet* est géré par le moyen d'identification électronique. Il englobe donc aussi bien le moyen d'authentification et le Credential que l'IdP. Le résultat d'une authentification avec un moyen d'identification électronique est une confirmation d'authentification permettant de confirmer l'identité du sujet et la réussite de l'authentification.

Les exemples pour les moyens d'identification électroniques sont la nouvelle carte d'identité allemande (nPA), Middleware (AusweisApp) incl., ou l'infrastructure SuisseID globale composé de SuisseID Token, Middleware (pilote du périphérique) et SuisseID Id.

2.14 Système d'identification électronique

Terme tiré d'eIDAS 910/2014 [4]: un «*système d'identification électronique*» est un système pour l'identification électronique, dans le cadre duquel des moyens d'identification électroniques sont délivrés pour les personnes physiques ou morales ou les personnes morales, qui représentent des personnes juridiques.

Un système d'identification électronique notifié doit remplir toutes les conditions prérequis répertoriées dans eIDAS 910/2014 [1] Article 7.

2.15 Période de définition

Le système IAM est conçu et configuré lors de la **période de définition**. De plus, les identités électroniques sont établies. La période de définition comprend ainsi les processus pour la préparation de toutes les informations nécessaires pour tous les composants impliqués ainsi que les composants elles-mêmes.

2.16 Fédération / Federation

Une **fédération** d'identité est une coopération entre différentes entités d'un système IAM par delà les limites des organisations et des systèmes, sans dupliquer, ni répliquer les données d'utilisateur nécessaires à cela (*E-Identities*).

Une fédération d'identités permet de transmettre des informations concernant une authentification de sujet et, à titre facultatif, des informations d'identité relatives à ce sujet via un réseau.

Comme cela est représenté à la Figure 5, un système d'identité fédéré se compose des trois entités Sujet, Relying Party (RP) et Identity Provider (IdP). La séquence des informations varie fonction de la modalité du protocole utilisé. Toutefois, le sujet communique toujours avec l'IdP, comme avec le RP. Le sujet s'authentifie par rapport à l'IdP dans le cadre d'une procédure d'authentification principale avec un moyen d'authentification précis (Authenticator). Cet événement est ensuite transmis au RP via le réseau, sous la forme d'une confirmation d'authentification. L'IdP peut joindre à cette confirmation d'authentification d'autres attributs (de personnes) concernant le sujet à authentifier.

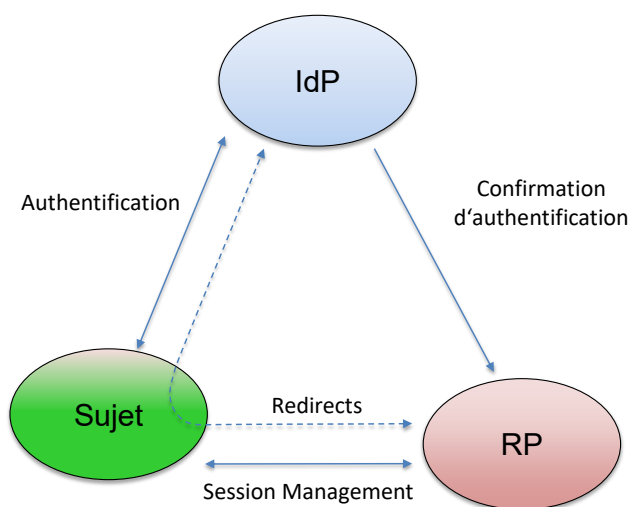


Figure 5: Modèle d'une Identity Federation

Synonyme: système d'identité fédéré, système IAM fédéré

2.17 Identification

L'**identification** est une opération qui a lieu lors de la période de définition, par laquelle l'identité du sujet est le plus souvent vérifiée à l'aide de justificatifs. L'identification est le plus souvent effectuée par une Registration Authority (RA).

Synonyme: détermination de l'identité

2.18 Document d'identité

En Suisse, les **pièces d'identité** valables sont les documents suivants:

- Passeport,
- Carte d'identité suisse,
- Une carte d'identité reconnue pour l'entrée sur le territoire suisse.

2.19 Identity Provider (IdP)

Entité, qui vérifie l'E-Identity du sujet pour la période d'exécution. Il pour cela vérifier la possession ou le contrôle du sujet au moyen du moyen d'authentification et la relation du sujet avec les moyens d'identification utilisés à l'aide des Credentials.

Un IdP met à disposition un Authentication Service et, le plus souvent, également un Attribute Assertion Service.

Synonyme: Authorization Provider (pour OIDC [12]), Verifier (dans NIST 800-63-3 [3])

2.20 Personne morale

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

Les personnes morales peuvent agir **uniquement** via des personnes physiques et sont donc toujours liées à une personne physique (voir Figure 6).

2.21 Caractéristique physique

Une **caractéristique physique** est une caractéristique d'une personne, comme la taille du corps ou la couleur des yeux. Les *caractéristiques biométriques* (voir chap. 2.7) sont des caractéristiques physiques spéciales.

2.22 Période d'exécution

Les processus électroniques, par lesquels un sujet – en cas de succès – se voit accorder l'accès aux ressources d'un Relying Party, ont lieu pour la période d'exécution.

2.23 Autorité d'enregistrement/Registration Authority (RA)

Une **autorité d'enregistrement** est une entité, qui enregistre et vérifie suffisamment d'informations concernant un sujet, afin de pouvoir s'assurer de son identité.

La RA peut agir comme partie intégrante d'un CSP ou en tant que service propre pour le compte du CSP.

2.24 Sujet

Un **sujet** est une personne physique, une *personne morale*, un service ou un objet, qui accède ou souhaite accéder à une *ressource*. Un **sujet** est représenté par des *E-Identities*.

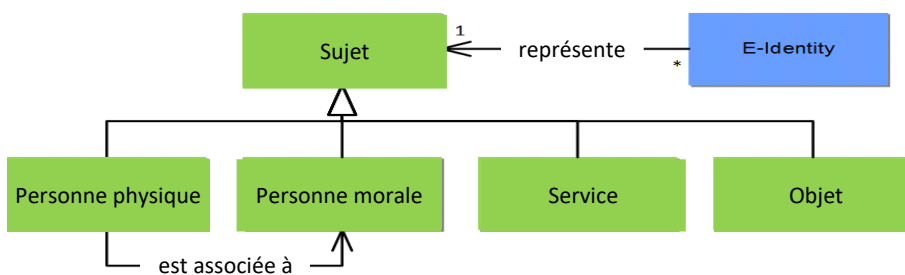


Figure 6: Définition du *sujet*

Un **abonné** (*Subscriber* en anglais, voir NIST 800-63-3A [16]) est un *sujet* qui, suite à un processus d'enregistrement achevé avec succès (processus *Enregistrer un sujet*), a obtenu un moyen d'authentification de la part d'un CSP. Le sujet devient alors un participant autorisé à l'Identity Federation Community.

Un **requérant** (*Applicant* en anglais, voir NIST 800-63-3A [16]) est un *sujet*, qui souhaite être intégré à l'Identity Federation Community et, pour y parvenir, passe par le processus *Enregistrer un sujet*. Une fois ce processus achevé avec succès, le *requérant* devient un *abonné*.

Un **porteur** (*Bearer* en anglais) est un *sujet*, qui transmet au RP une confirmation d'authentification délivrée par l'IdP.

2.25 Unité IDE

Les entités IDE sont établies selon l'article 3.c de la loi fédérale sur le numéro d'identification des entreprises [17].

Les **entités IDE** sont toutes les entreprises et institutions identifiées par une IDE. Dans le système IDE, la notion d'entreprise s'entend au sens large. Les entités IDE ne comprennent pas seulement toutes les entreprises actives en Suisse au sens strict du terme, mais aussi tous les «clients de l'administration publique» qui possèdent les caractéristiques d'une entreprise ou qui doivent être identifiées à des fins juridiques, administratives ou statistiques.³

Synonyme: entreprise

2.26 Source fiable

Une **source fiable** est n'importe quelle source d'information considérée comme digne de confiance pour une situation concrète.

eIDAS 2015/1502 [7]: *une «source fiable» est n'importe quelle source d'information, qui met à disposition, de manière fiable, des données, informations et/ou justificatifs précis, pouvant être utilisés comme justificatif d'identité.*

Les sources fiables peuvent prendre de nombreuses formes différentes, ex. registre, certificats, services etc.

2.27 Administration

L'**administration** désigne une collectivité publique (offices et autorités, le cas échéant organismes privés mandatés pour de telles tâches), qui s'acquittent de tâches de l'Etat qui lui sont confiées par la loi.

Le terme Administration est un terme d'organisation qui n'est pas couvert par la définition juridique d'une personne physique et morale.

³ Voir également: <https://www.bfs.admin.ch/bfs/fr/home/registres/registre-entreprises/numero-identification-entreprises/entites-ide-entreprises.html>

3 Modèle de qualité

Le modèle de qualité pour l'authentification des sujets est divisé en étapes et niveaux. On parle dans cette norme de **niveaux de confiance (NDC)**.

Le modèle de qualité pour l'authentification des sujets se compose de quatre parties (voir Tableau 4). A chacun de ces modèles partiels est affecté un processus. Les processus sont décrits à la Figure 2 et dans l'annexe G.

Modèle de qualité	Processus	Niveaux de confiance (NDC)
Modèle de qualité de l'authentification	Authentifier le sujet	Niveaux de confiance de l'authentification (NDCA)
Modèle de qualité de l'enregistrement	Enregistrer un sujet	Niveaux de confiance de l'enregistrement (NDCE)
Modèle de qualité du pilotage	Piloter l'IAM	Niveaux de confiance du pilotage (NDCP)
Modèle de qualité de la fédération	Fédérer l'identité	Niveaux de confiance de la fédération (NDCF)

Tableau 4: Parties du modèle de qualité et niveaux de confiance correspondants

Les modèles partiels sont constitués en fonction du type de système IAM (voir chapitre 3.2) ou peuvent également être utilisés individuellement pour classer les prestataires IAM (voir chapitre 3.3). Ainsi le modèle de qualité de l'enregistrement peut par exemple être utilisé à des fins d'évaluation de la qualité d'une RA.

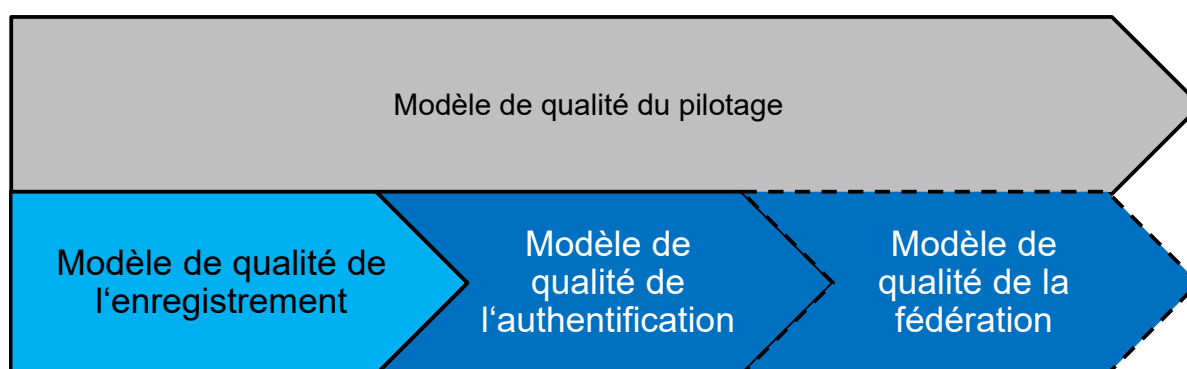


Figure 7: Composition du modèle de qualité

A chaque modèle partiel ou chaque processus correspondent des critères de qualité. Les critères de qualité comprennent des modalités, qui doivent être remplies. On obtient ainsi un niveau d'évaluation. Ces niveaux d'évaluation sont regroupés au niveau des processus et aboutissent au niveau d'évaluation de processus. Les niveaux d'évaluation de processus sont regroupés au niveau de l'évaluation globale et donnent la qualité globale de l'authentification des sujets.

3.1 Niveaux de confiance

Quatre niveaux de confiance ont été définis dans le modèle de qualité pour l'authentification des sujets physiques et moraux. Le niveau de confiance 1 est le plus faible et signifie qu'il est le moins digne de confiance pour le Relying Party. Le niveau de confiance 4 est le niveau le plus élevé et jouit, de la part du Relying Party, du degré de confiance le plus élevé. Le Tableau 5 décrit les 4 niveaux de confiance avec leurs caractéristiques. La couleur du rouge (confiance faible) au vert (confiance élevée) souligne la qualité.

Niveaux de confiance	Désignation	Description
1	Confiance nulle ou minimale	Le niveau de confiance 1 est le niveau le plus faible.
		NDCA: l'authentification ne nécessite qu'un seul facteur d'authentification, au moyen duquel l'on peut assurer avec une certitude moindre qu'une même E-Identity correspond à un même sujet en cas d'accès répété à un RP.
		NDCE: toutes les informations à disposition concernant l'E-Identity du sujet ont été déclarées par ce dernier et n'ont fait l'objet d'aucune vérification. [Uniquement pour les personnes morales: le lien entre personne physique et personne morale est lui-même déclaré.]
		NDCP: les prestataires IAM impliqués utilisent des processus, mais ne sont soumis à aucune forme de surveillance et excluent toute responsabilité, dans la mesure où cela est autorisé.
		NDCF: l'origine et l'intégrité des données d'une confirmation d'authentification doivent pouvoir être constatées sans difficultés.

Niveaux de confiance	Désignation	Description
2	Confiance faible	NDCA: dans le cas du niveau de confiance 2, le sujet doit se connecter avec au moins 2 Single-Factor Authenticators différents ou avec un Multi-Factor Authenticator, afin d'accroître la certitude qu'une même E-Identity puisse être affectée à un même sujet en cas d'accès réitéré à un RP.
		NDCE: lors de l'enregistrement, les renseignements du requérant ont été contrôlés au moyen de justificatifs. Pour ce faire, le sujet doit être au moins présent en ligne. [personnes morales uniquement: le lien entre la personne physique et morale a été établi.] Le moyen d'authentification a été transmis de manière sûre.
		NDCP: les prestataires IAM impliqués utilisent des normes et règles internes afin de sécuriser la qualité de leur processus. Les processus sont définis et communiqués. La responsabilité existante est limitée.
		NDCF: une confirmation d'authentification doit être suffisamment protégée concernant la confidentialité.
3	Confiance significative	NDCA: avec le niveau de confiance 3, le sujet doit se connecter avec un hardware-based Multi-Factor Authenticator
		NDCE: lors de l'enregistrement, les renseignements des requérants ont été validés de manière forte à l'aide de justificatifs et le justificatif avec les caractéristiques physiques a été copié. Le sujet doit pour cela être présent au moins en ligne. [personnes morales uniquement: le lien entre la personne physique et morale a été vérifié.] Le moyen d'authentification a été transmis ou livré personnellement.
		NDCP: les prestataires IAM impliqués utilisent des normes afin de sécuriser la qualité de leur processus. Les processus sont surveillés et mesurés. Le respect des normes est contrôlé par une instance externe. Les prestataires de service impliqués assument une responsabilité conformément à la législation.
		NDCF: une confirmation d'authentification doit être suffisamment protégée concernant la confidentialité.

Niveaux de confiance	Désignation	Description
4	Confiance élevée	Le niveau de confiance 4 est le niveau le plus élevé. Il offre un très grand degré de confiance concernant l'E-Identity déclarée par le sujet.
		NDCA: lors de l'authentification, le sujet doit se connecter avec un avec un hardware-based Multi-Factor Authenticator, qui doit être certifié.
		NDCE: lors de l'enregistrement, le sujet doit être présent physiquement ou Virtual-in-Person. Cette présence sera documentée. Les justificatifs doivent être reconnus par l'Etat et inclure les caractéristiques biométriques, qui – dans la mesure du possible – doivent être vérifiées. [personnes morales uniquement: le lien entre la personne physique et morale a été vérifié au moyen d'un extrait de registre du commerce et il existe une déclaration de consentement.]
		Le moyen d'authentification doit être remis en main propre. En cas de prolongement du moyen d'authentification, il faut à nouveau présenter un justificatif reconnu par l'Etat et validé.
		NDCP: les prestataires IAM impliqués utilisent les normes afin de sécuriser la qualité de leurs processus. Les processus sont optimisés et automatisés. Le respect est contrôlé par une instance titulaire d'une habilitation officielle. Les prestataires impliqués sont tenus responsables conformément à la loi. La responsabilité relative à l'exécution des demandes d'indemnisation est allégée par des peines conventionnelles.
		NDCF: le porteur d'une confirmation d'authentification doit pouvoir en outre s'authentifier en tant que détenteur.

Tableau5: Niveaux de confiance du modèle de qualité pour l'authentification des sujets

3.2 Composition des niveaux de confiance

Les niveaux de confiance du modèle de qualité pour l'authentification des sujets se composent de 4 modèles partiels. Cette composition est décrite dans le Tableau 6.

Pour satisfaire à un niveau de confiance, tous les modèles partiels doivent correspondre aux niveaux répertoriés. Le niveau le plus faible pour les modèles partiels NDCA, NDCE et NDCP détermine ainsi le niveau du modèle global.

Concernant le modèle partiel avec les niveaux de confiance de l'enregistrement (NDCE), l'on a recours, en fonction du type de sujet, au modèle pour les personnes physiques (NDCPP) ou au modèle pour les personnes morales (NDCPM).

Le modèle partiel avec les niveaux de confiance de la fédération (NDCF) intervient uniquement pour les systèmes IAM fédérés et est omis lors de la composition pour les systèmes non fédérés.

Niveau de confiance	Désignation	NDCA	NDCE NDCPP/NDC PM	NDCP	NDCF
1	Confiance nulle ou minimale	1	1	1	1
2	Confiance faible	2	2	2	2
3	Confiance significative	3	3	3	2
4	Confiance élevée	4	4	4	3

Tableau 6: Composition des niveaux de confiance aux niveaux des modèles partiels

3.3 Utilisation pour classer les prestataires IAM

Les modèles de qualité partiels proposés dans la présente norme peuvent également être utilisés afin de classer qualitativement les différents prestataires IAM.

3.3.1 Classer les RA

Le modèle de qualité de l'enregistrement (NDCE) et celui du pilotage (NDCP) sont employés afin de classer les RA. Concernant le modèle de qualité du pilotage, seuls les critères rapportés aux prestataires de service considérés sont utilisés.

3.3.2 Classer un IdP

Le modèle de qualité de l'authentification (NDCA) et celui du pilotage (NDCP) sont employés afin de classer les IdP. A ce titre, les critères ne sont appliqués qu'aux prestataires de service considérés concernant le modèle de qualité du pilotage. Si l'IdP doit être utilisé par ailleurs pour la fédération des identités, il faut encore prendre en compte le modèle de qualité de la fédération (NDCF) dans l'évaluation.

3.3.3 Classer un CSP

Le modèle de qualité de l'authentification (NDCA), celui de l'enregistrement (NDCE) et celui du pilotage (NDCP) sont employés afin de classer les CSP, IdP inclus. Le modèle de qualité de la fédération est facultatif. Les niveaux correspondent aux niveaux de confiance du modèle global (voir Tableau 5 et Tableau 6).

Les critères sont appliqués uniquement aux prestataires de service considérés pour classer la qualité du pilotage. Si le CSP a externalisé les processus d'enregistrement à une RA, celle-ci doit également être prise en compte dans l'évaluation (NDCE et NDCP).

3.4 Critères de qualité

Les trois niveaux de définition de la qualité de l'authentification d'un sujet sont représentés par la Figure 8. La désignation dans le graphique se rapporte toujours à la qualité de l'élément correspondant.

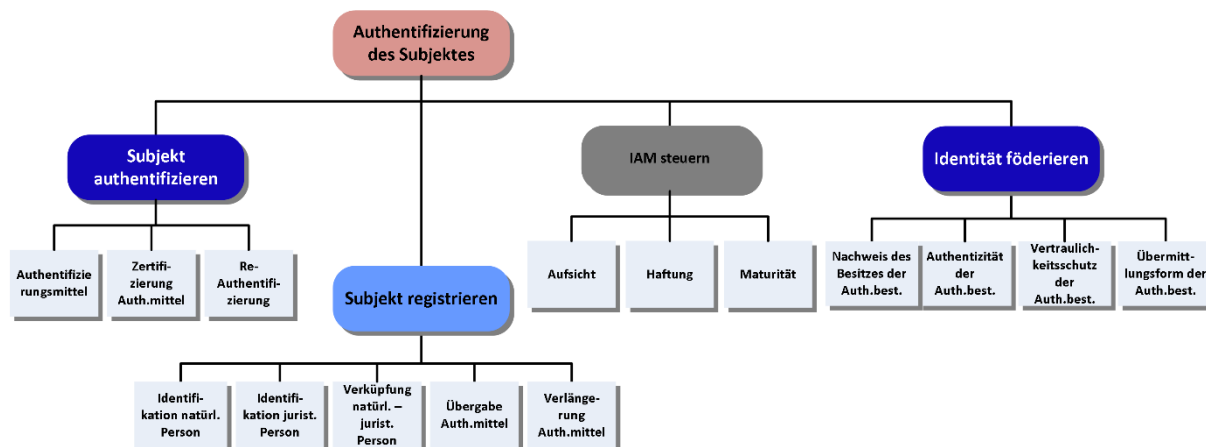


Figure 8: Vue d'ensemble de tous les critères

Les critères de qualité et leurs modalités sont décrits aux chapitres 4 à 10 avec également les modèles de qualité, dans lesquels ils sont utilisés.

3.5 Conditions préalables

Les conditions préalables suivantes (Tableau 7) sont considérées comme réunies par les systèmes d'Identity Federation pour les critères de qualité traités ici. Le non-respect de ces conditions préalables peut avoir un impact négatif sur l'ensemble du système IAM et ainsi nuire également à la qualité de l'authentification.

N°	Conditions préalables	Description
A1	Vérification du niveau d'authentification	Le RP doit vérifier le niveau d'authentification du sujet dans la confirmation d'authentification dont il dispose. (NIST 800-63-3 [3] chap. 4.4.2)
A2	Autorisation du RP	Un IdP doit, si nécessaire, vérifier en amont de la délivrance d'une confirmation d'authentification, si le destinataire (RP) est bien habilité à en demander une. (NIST 800-63-3 [3] chap. 4.1)

N°	Conditions préalables	Description
A3	Consentement du sujet (User consent)	Concernant les informations d'identité personnelles, l'IdP doit soumettre au sujet pour approbation, les informations d'identité à transmettre, en amont de la délivrance d'une confirmation d'authentification à un RP précis. ⁴ (NIST 800-63-3 [3] chap. 4.1)
A4	Base temporelle	L'IdP doit utiliser une base temporelle fiable pour délivrer la confirmation d'authentification (ex. service temporel public ou estampille temporelle reconnue par l'Etat). Il est en outre important que le temps du RP et de l'IdP soient aussi synchrones que possible. (NIST 800-63-3 [3] chap. 4.4.1)
A5	Canal de communication sûr	La communication entre l'IdP, la Client Platform et le RP doit être sécurisée (ex. avec TLS). ⁵ (NIST 800-63-3 [3] chap. 7.1)
A6	Points de communication terminaux dignes de confiance	Les points de communication terminaux doivent être dignes de confiance (ex. au moyen de certificats et d'un Trust Anchor) et que cela peut être vérifié pour la période d'exécution. (NIST 800-63-3 [3] chap. 4.4.1)
A7	Client Platform sûre	Il peut être supposé que l'environnement de l'application Client est aussi protégé que possible contre les logiciels malveillants, présente un statut de système et de sécurité aussi à jour que possible et n'est pas exploité en mode administrateur. ^{6 7}

⁴ Un User Consent n'est par exemple pas nécessaire, lorsqu'il s'agit d'une entreprise IAM (Voir également eCH-0168 [25], chap. 3.11).

⁵ Voir également eIDAS 2015/1502 [7] chap. 2.4.6. Contrôles techniques: «*Les modes de communication électronique, qui sont utilisés pour la transmission d'informations personnelles ou sensibles, doivent être protéger contre l'écoute, la manipulation et le replay.*»

Correspond à la Special Publication (SP) 800-52 [26], publiée par NIST.

⁶ L'exigence A7 ne peut être pleinement remplie que si la Client-Platform se trouve sous le contrôle de l'ensemble du système IAM, par exemple dans un environnement d'administration ou d'entreprise. Mais dans un environnement ouvert en particulier, par exemple avec des citoyens comme utilisateurs finaux, il faut, lors de la conception du système global, tenir compte des dommages qu'un terminal infecté par exemple peut causer et comment l'on peut réduire le potentiel de nuisance en choisissant des moyens d'authentification appropriés en même temps que l'explication/la formation correspondante.

⁷ Les composants de logiciel des moyens d'authentification matériels devraient toujours être à jour. Il faut à cet égard signaler à l'utilisateur final que des mises à jour sont disponibles.

N°	Conditions préalables	Description
A8	Environnement de serveur sûr	Les environnements de serveur dans le système d'identité fédéré peuvent être protégés aussi vite que possible contre les vulnérabilités connues. (NIST 800-63-3 [3] chap. 2.2)
A9	Cryptoparamètres	Les algorithmes cryptographiques et les longueurs de clé aujourd'hui recommandés sont utilisés dans tous les systèmes impliqués. Nous vous renvoyons vers ces sources ⁸ concernant l'utilisation des paramètres adéquats. (NIST 800-63B [15] chap. A2)
A10	Validité adéquate de la confirmation d'authentification	Les confirmations d'authentification ne doivent être valables que pour une durée limitée de façon judicieuse, afin de réduire la réutilisation (assertion reuse). (NIST 800-63C [18] chap. 8.1)
A11	Révocation	Le sujet et le CSP doivent avoir à tout moment la possibilité de révoquer une E-Identity ou de déclarer l'E-Identity invalide. (NIST 800-63B [15] chap. 6.4)
A12	Prise en compte des dangers et des aspects de sécurité	Les éventuels dangers et mesures contre les attaques envers le moyen d'authentification doivent être prise en compte. (NIST 800-63B [15] chap. 8.1, NIST 800-63B [15] chap. 8.2)

Tableau 7: Conditions préalables pour les Identity Federation Systems

En outre, les technologies les plus fréquemment utilisées sont souvent soumises à des exigences fondamentales techniques supplémentaires, voir par exemple pour SAML: https://www.owasp.org/index.php/SAML_Security_Cheat_Sheet.

⁸ BlueKrypt: www.keylength.org

ETSI: http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts_119312v01010101p.pdf

Office fédéral allemand de la sécurité dans l'informatique: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile

4 Modèle de qualité de l'authentification

Le modèle de qualité de l'authentification est déterminé par l'évaluation des critères du processus *Authentifier le sujet* (voir Annexe G.1.1 pour une description du processus).

4.1 Niveaux de confiance de l'authentification (NDCA)

Les niveaux de confiance de l'authentification (NDCA) sont déduits des deux critères suivants (voir Figure 9):

- Moyen d'authentification (chapitre 4.2),
- Certification du moyen d'authentification (chapitre 4.2.2).
- Réauthentification (chapitre 5.2.3)

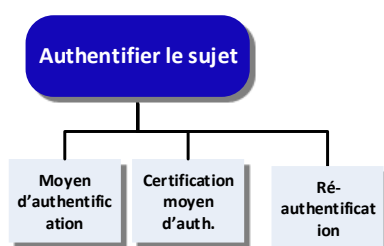


Figure 9: Critères pour le modèle de qualité de l'authentification

Le niveau de confiance de l'authentification (NDCA) est déterminé par la modalité la plus basse des critères. La couleur du rouge (confiance faible) au vert (confiance élevée) souligne la qualité.

Concernant le critère Moyen d'authentification, on établit une distinction entre l'authentification régulière et une authentification unique après une identification en ligne réussie de niveau correspondant. L'authentification unique après identification en ligne est utilisée principalement lors d'un premier contact du requérant avec la ressource.

Niveau de confiance de l'authentification (NDCA)	Moyen d'authentification		Certification moyen. auth.	Re-authentification
	Authentification régulière	Authentification unique après identification en ligne		
1	SFA	IDN1	aucun	ReAuth1
2	MFA	IDN2	aucun	ReAuth2
3	HW-MFA	IDN3	aucun	ReAuth3
4	HW-MFA	IDN4	Certification	ReAuth4

Tableau 8: Niveaux de confiance de l'authentification (NDCA)

4.2 Critères d'authentification

4.2.1 Moyen d'authentification

Questions:	<p>Le moyen d'authentification ne peut-il être utilisé que si le sujet auquel il appartient le détient ou le contrôle?</p> <p>Le moyen d'authentification offre-t-il une protection contre la duplication et la falsification par des tiers?</p> <p>Le moyen d'authentification est-il conçu de manière à pouvoir être protégé de manière fiable contre une utilisation par autrui?</p>
------------	---

Remarques:

- Les modalités SFA,
- MFA et HW-MFA correspondent à la liste des *permitted authenticator types* pour les 3 Authenticator Assurance Level (AAL) de NIST SP 800-63B [15]
- Les modalités SFA, MFA et HW-MFA correspondent aux 3 niveaux des «caractéristiques et conception des moyens d'identification électroniques» d'eIDAS 2015/1502 [5]
- Les exigences relatives aux différents moyens d'authentification évoqués (SFA, MFA et HW-MFA) sont mentionnées avec des exemples dans l'annexe H.

Modalités		Description
Authentification régulière	Single-Factor Authentication (SFA)	<p>Le moyen d'authentification dispose d'au moins un facteur d'authentification (Single-Factor Authenticator). Il est possible d'établir une distinction entre les types suivants:</p> <ul style="list-style-type: none"> • Memorized Secret (mot de passe, PIN par exemple) • Look-Up Secret (liste de décompte par exemple) • Out of Band Authenticator (confirmation par SMS par exemple), • Single Factor OTP Device (Google Authenticator par exemple).
	Multi-Factor Authentication (MFA)	<p>a) Le moyen d'authentification est un Multi-Factor Authenticator, comme par exemple.</p> <ul style="list-style-type: none"> • Multi-Factor Software Cryptographic Authenticator, • Multi-Factor OTP Software Authenticator, <p>ou</p> <p>b) L'authentification repose sur la combinaison de 2 Single-Factor Authenticators distincts en tant que moyen d'authentification devant reposer sur divers facteurs d'authentification.</p>
	Hardware based Multi-Factor Authentication (HW-MFA)	<p>Afin d'offrir la plus grande protection possible contre la duplication et la falsification, seuls les 3 Hardware-Devices suivants sont autorisés:</p> <ul style="list-style-type: none"> • Multi-Factor OTP Device • Multi-Factor Cryptographic Device • Single-Factor Cryptographic Device avec Memorized Secret.

Modalités		Description
	Authentification unique après identification en ligne	Juste après une identification en ligne réussie de la personne physique (voir chapitre 6.1.1), le sujet se voit accorder un accès unique à la ressource souhaitée. Le niveau de confiance de l'authentification (NDCA) varie selon la modalité de l'identification.

Tableau 9: Modalités du critère *Moyen d'authentification*

Exemple d'identification en ligne unique:

Suite à une identification vidéo audiovisuelle et à la vérification des justificatifs correspondants, le requérant est directement redirigé (données personnelles inclus) vers le système cible (RP). Parmi les exemples, on trouve les processus pour lesquels le requérant a déjà été préalablement en contact avec le système cible (ouverture d'un compte en ligne ou demande de crédit par exemple suivies de la signature de documents).

4.2.2 Certification du moyen d'authentification

Question:	Le moyen d'authentification est-il certifié? Le moyen d'authentification offre-t-il la meilleure protection possible contre les attaques?
-----------	--

Remarques:

- Correspond à *FIPS 140 verification* pour les 3 Authenticator Assurance Level (AAL) de NIST SP 800-63B [15]
- La certification couvre également les logiciels intégrés, les composants de logiciel (pilote, middleware), ainsi que le système d'exploitation selon FIPS 140-2 [19] chapitre 4.6.1.

Modalités	Description
Pas de certification	Le moyen d'authentification n'est pas certifié.
Certification	Le moyen d'authentification est certifié au moins Level 3 ou Common Criteria EAL 4+ selon FIPS 140-2.

Tableau 10: Modalités du critère *Certification du moyen d'authentification*

Exemples:

- Un moyen d'authentification hardware-based à plusieurs facteurs (HW-MFA) **sans** certification est la Mobile ID par exemple.
- Un moyen d'authentification hardware-based à plusieurs facteurs (HW-MFA) **avec** certification est la SuisseID par exemple.

4.2.3 Réauthentification

Question:	Au bout de combien de temps un RP – indépendamment de son propre Session Management – doit-il faire à nouveau identifier un sujet par l'IdP? Comment garantir, lors d'une session en cours que le sujet est bien toujours le même que lors de l'authentification initiale par l'IdP?
-----------	---

Remarques:

- Correspond au *reauthentication requirement* pour les 3 Authenticator Assurance Level (AAL) de NIST SP 800-63B [15]
- Contrairement aux événements déterminés par le RP, dans lesquels un sujet doit à nouveau s'authentifier:
 - après une période d'inactivité (5 minutes par exemple)
 - au bout d'une période maximale écoulée (30 minutes par exemple) par session
 - en amorçant une action spécifique (enregistrement de données par exemple)
 cette période de réauthentification représente le temps maximal autorisé au cours duquel un RP devrait toujours faire à nouveau authentifier un sujet actif par un l'IdP.

Concernant les modalités *ReAuth2* et *ReAuth3*, tous les facteurs d'authentification, qui ont été utilisés lors de l'authentification initiale, devraient être utilisés. La différence réside dans le fait que concernant *ReAuth3*, les facteurs d'authentification doivent être utilisés exactement de la même manière que lors de l'authentification initiale.

Modalités	Description
ReAuth1	Le sujet doit à nouveau être authentifié par l'IdP après une période adéquate (30 jours par exemple).
ReAuth2	Le sujet doit être à nouveau être authentifié par l'IdP au bout de 18 heures maximum, indépendamment de l'activité d'utilisation. Un facteur d'authentification suffit lors de la réauthentification.
ReAuth3	Le sujet doit être à nouveau être authentifié par l'IdP au bout de 12 heures maximum. La réauthentification doit tenir compte de tous les facteurs d'authentification, qui ont été utilisés lors de l'authentification initiale.
ReAuth4	Le sujet doit à nouveau être authentifié par l'IdP au bout de 30 minutes maximum. La réauthentification doit tenir compte de tous les facteurs d'authentification exactement de la même manière que lors de l'authentification initiale.

Tableau 11: Modalités du critère *réauthentification*

Exemple:

- Niveau ReAuth1
 - concernant OAuth [20], il est recommandé de réutiliser les Refresh Tokens non sans restriction et selon des critères définis (au bout d'une 50^e utilisation pour la création d'Access Token par exemple). Là encore, il faut exiger une réauthentification au niveau de l'OAuth Server ou définir des mesures pour contrer l'utilisation abusive de Refresh Tokens (nombre anormalement élevé de demandes d'Access Tokens par ex.).
- NiveauReAuth3
 - Dans le cas du *ReAuth3*, le caching d'un facteur basé sur les connaissances est possible, comme cela est déjà le cas concernant l'implémentation actuelle de SuisseID.
- NiveauReAuth4
 - Concernant SuisseID, l'utilisateur serait authentifié avec tous les facteurs d'authentification dans le même ordre (reconnaissance de l'appareil matériel et saisie du PIN). Le facteur basé sur la connaissance (PIN) ne doit pas faire l'objet de caching.

5 Modèle de qualité de l'enregistrement

Le modèle de qualité de l'enregistrement est déterminé par l'évaluation des critères du processus *Enregistrer un sujet* (voir Annexe G.2 pour une description du processus).

Le modèle de qualité de la fédération contient 5 critères (voir Figure 10).

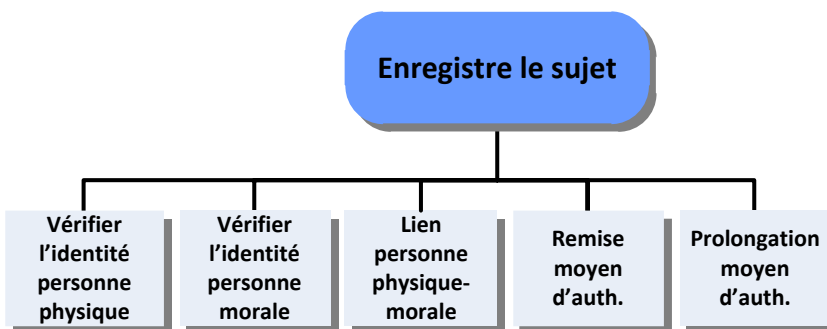


Figure 10: Critères pour le modèle de qualité de l'enregistrement

5.1 Niveaux de confiance de l'enregistrement (NDCE)

Les niveaux de confiance de l'enregistrement (NDCE) pour le processus *Enregistrer un sujet* sont déterminés différemment en fonction de la nature du sujet.

5.1.1 Pour les personnes physiques

Les niveaux de confiance de l'enregistrement (NDCPP) pour le processus *Enregistrer un sujet* pour les personnes physiques découlent des 3 critères suivants:

- Identification des personnes physiques (chapitre 5.2.2),
- Transmission du moyen d'authentification (chapitre 5.2.5),
- Prolongation/remplacement du moyen d'authentification (chapitre 5.2.6).

Le niveau de confiance de l'enregistrement (NDCPP) est déterminé par la modalité la plus faible des critères.

Niveaux de confiance de l'enregistrement (NDCPP) pour personnes phys.	Identification personnes phys.	Transmission moyen. auth. ⁹	Prolongation moyen. auth.
1	IDN1	1	CN1
2	IDN2	2	CN2
3	IDN3	3	CN3
4	IDN4	4a ou 4b	CN4

Tableau 12: Détermination du NDCE pour les personnes physiques

5.1.2 Pour les personnes morales

Les niveaux de confiance de l'enregistrement (NDCPM) pour le processus *Enregistrer un sujet* pour les personnes morales se composent des niveaux de confiance de l'enregistrement pour les personnes physiques et des deux critères supplémentaires suivants:

- Identification des personnes morales (chapitre 5.2.3),
- Lien entre personne physique et morale (chapitre 5.2.4)

Le niveau de confiance de l'enregistrement (NDCPM) est déterminé à ce égard par la modalité la plus faible du niveau de de confiance pour les personnes physiques (NDCPP) et des critères.

Dans le domaine des administrations publiques, les pouvoirs de représentations sont déterminés selon les bases légales en vigueur au niveau fédéral, cantonal et communal, ainsi que selon les règles internes des autorités correspondantes.

Exemple au niveau fédéral:

Le droit de signature est déterminé à l'échelon le plus élevé en vertu de la loi sur l'organisation du gouvernement et de l'administration (LOGA) [21] par le chef de département. Les directeurs des groupes et offices règlent au sein de leur service la question des autorisations de signature et délèguent, le cas échéant, les pouvoirs correspondants.

Niveaux de confiance de l'enregistrement (NDCPM) pour les personnes morales	NDCPP	Identification personnes mor.	Lien
1	1	IDJ1	L1
2	2	IDJ2	L2
3	3	IDJ3	L3
4	4	IDJ4	L4

Tableau 13: Détermination du NDCE pour les personnes morales

⁹ Le critère peut être omis lorsque le CSP associe un moyen d'authentification à l'E-Identity du sujet, qui est déjà détenue ou contrôlée par le sujet.

5.2 Critères de l'enregistrement

5.2.1 Facteurs d'identification

Tant le critère Identification des personnes physiques que le critère Identification de personnes morales sont constitués de plusieurs facteurs.

5.2.1.1 Facteur Présence

Le facteur *Présence (Physical Presence, PP)* définit si le requérant doit être ou non physiquement présent lors de l'enregistrement. Ce facteur ne peut s'appliquer qu'aux personnes physiques.

Questions:	Sous quelle forme le requérant est-il présent lors de l'identification? Peut-on constater que la personne physique existe bien et est personnellement présente?
------------	--

Remarques:

- Lors de l'enregistrement, le requérant doit être personnellement présent et ne peut être représenté.
- Si le requérant n'a pas l'exercice de ses droits civils selon l'article 13 CC, c'est à dire qu'il est mineur ou incapable de discernement, le représentant légal doit donner son consentement.
- Les modalités pour le facteur *Présence* correspondent aux valeurs (*remote*, *in person* et *virtual in-person*) pour les *Presence Requirements* dans NIST 800-63-3A [16] – chapitre 4.4 – 4.8.
- En Suisse, l'ordonnance OSCSE Art 7.2 [10] s'applique pour la modalité *Virtual In-Person*: *les fournisseurs reconnus peuvent délivrer des certificats réglementés dans le cadre d'un processus de vérification d'identité par le biais d'une communication audiovisuelle en temps réel, répondant aux exigences de la loi du 10 octobre 1997 sur le blanchiment d'argent.*

Niveau	Modalités	Description
PP.a	Pas de présence	Aucune présence n'est requise.
PP.b	Online	Le requérant est présent en ligne via un réseau (Internet, téléphone).
PP.c	Virtual In-Person	En complément du niveau PP.b: Le système utilisé dispose de mesures, suffisantes du point de vue de la technologie et des procédures, qui permettent de rendre la présence en ligne quasi équivalente à une présence physique au moyen d'une communication en temps réel.
PP.d	In-Person (physique)	La présence physique personnel du requérant est requise lors de l'enregistrement.

Tableau 14: Modalités du facteur *Présence*

Exemple:

- Niveau PP.a
 - Enregistrement par E-Mail ou Ticket-System
- Niveau PP.b
 - Enregistrement en ligne par application Web ou Smartphone-App
 - Enregistrement par téléphone par le biais de renseignements techniques ou personnels (ex. renseignements vérifiables concernant la personne)
- Niveau PP.c
 - Identification vidéo selon les conditions-cadre de la FINMA en matière de droit relatif à la surveillance
- Niveau PP.d
 - Le requérant se présente personnellement devant la RA.

5.2.1.2 Facteur Justificatif

Le facteur *Justificatif (Identity Evidence, IE)* classe les justificatifs présentés lors de l'enregistrement selon leur qualité. La RA est compétente pour vérifier la validité et l'authenticité des justificatifs et de leur source.

Si plusieurs justificatifs sont utilisés, le critère doit être déterminé au cas par cas pour chaque justificatif.

Questions:	Le justificatif est-il authentique et valide? Le justificatif provient-il d'une source fiable et reconnue?
------------	---

Remarques:

- Les modalités pour le facteur *Justificatif* correspondent aux valeurs (*unacceptable, weak/adequate, strong, superior*) pour *Identity Evidence* dans NIST 800-63-3A [16] – chapitre 5.3.1.1 (Identity Evidence).
- Les niveaux IE.b, IE.c et IE.d correspondent aux exigences pour le niveau de sécurité *faible, significatif et élevé* dans eIDAS 2015/1502 [7], section 2.1.2.
- En Suisse, la loi SCSE ((943.03), article 9 [9] ainsi que l'ordonnance OSCSE (943.032) art 5.1 [10] s'appliquent pour le niveau le plus élevé: le requérant doit personnellement présenter à la RA un document d'identité, valide en Suisse au moment de l'enregistrement (c'est à dire non expiré).

Niveau	Modalités	Description
IE.a	Aucun justificatif	Aucun justificatif n'est présenté. ou les justificatifs ne sont pas concluants, car l'instance émettrice n'a manifestement procédé à aucune vérification d'identité.
IE.b	Justificatif présenté	<i>Il peut être supposé que le justificatif est authentique ou existe selon une source fiable et que le justificatif est à première vue valide.</i> ¹⁰ Le justificatif contient au moins un identificateur, qui identifie sans ambiguïté le sujet à qui il appartient. Le processus de délivrance du justificatif est structuré de manière à ce que l'on puisse supposer qu'il a été délivré pour le bon sujet. Le justificatif contient des caractéristiques de sécurité, qui ne peuvent être reproduites qu'avec des connaissances spéciales.
IE.c	Justificatif reconnu et vérifié	En complément du niveau IE.b, l'une des alternatives suivantes doit être remplie. 1) Le justificatif est reconnu et valide dans le contexte donné. et le justificatif a été vérifié afin de constater son authenticité, ou une source fiable a connaissance qu'il existe et se rapporte à un sujet existant réellement. 2) Un document d'identité valide a été présenté (original ou copie) 3) La présentation d'un justificatif électronique d'une E-Identity certifiée ou notifiée valide et de qualité égale ou supérieure, constitue également un justificatif valide.
IE.d	Justificatif de caractéristiques physiques	En complément du niveau IE.c, l'une des alternatives suivantes doit être remplie. 1) Le justificatif doit être reconnu par l'Etat et l'original être présenté. Le justificatif doit permettre la comparaison d'une ou de plusieurs caractéristiques physiques de la personne (photo ou caractéristiques biométriques) et celles-ci doivent être vérifiées – dans la mesure où elles sont accessibles. 2) La présentation d'un justificatif électronique d'une E-Identity certifiée ou notifiée valide et de qualité égale ou supérieure, constitue également un justificatif valide.

Tableau 15: Modalités du facteur *Justificatifs*

¹⁰ eIDAS 2015/1502 [5], Section 2.1.2. Niveau de sécurité faible.

Exemples:

- Niveau IE.a
 - Document de source inconnue, sans tampon d'un établissement public
- Niveau IE.b
 - Carte de crédit
 - Permis de conduire
 - Certificat de naissance
 - SwissPass CFF
 - Carte d'assuré d'une caisse d'assurance maladie
 - Carte d'étudiant ou de salarié
- Niveau IE.c
 - SwissPass CFF et vérification positive par le personnel en charge du contrôle
 - Carte d'étudiant avec photo et validité, délivré par un établissement public dans le domaine de l'éducation
 - Copie d'une pièce d'identité reconnue par l'Etat
 - Permis de conduire
- Niveau IE.d
 - Pièces d'identité reconnues par l'Etat

5.2.1.3 Facteur Validation des renseignements

Le facteur *Validation des renseignements (Identity Validation, IV)* décrit avec quatre modalités, comment la RA peut, à l'aide des justificatifs présentés, vérifier l'exactitude des données indiquées lors du dépôt de la demande.

Question:	<p>Le lien entre le requérant (sujet), qui présente les justificatifs, et l'identité déclarée du sujet peut-il être établi?</p> <p>Les renseignements fournis par le requérant concordent-ils avec les données figurant dans les justificatifs présentés?</p>
-----------	---

Remarques:

- Les niveaux pour le facteur *Validation des renseignements* correspondent aux valeurs (*unacceptable, weak/adequate, strong, superior*) dans NIST 800-63-3A [16] – chapitre 5.4.1 (Identity Verification)
- Les niveaux IV.b, IV.c et IV.d correspondent aux exigences pour les niveaux de sécurité *faible, significatif* et *élevé* dans eIDAS 2015/1502 [7], section 2.1.2.
- L'annexe H répertorie les exigences supplémentaires relatives aux différents types de validation en fonction de la forme de présence du requérant.
- Selon l'application et le contexte, il est possible de demander et de contrôler d'autres attributs ne permettant pas l'identification sujet.

Niveau	Modalités	Description
IV.a	Pas de validation	Il n'est pas possible, ni souhaitable de vérifier les renseignements.
IV.b	Validation adéquate	Le requérant peut prouver qu'il a accès aux justificatifs. Les renseignements du requérant sont vérifiés à l'aide des données des justificatifs présentés.
IV.c	Validation forte	En complément du niveau IV.b: Des précautions ont été prises en vue de réduire le risque que l'identité du requérant ne concorde pas avec l'E-Identity déclarée.
IV.d	Validation la plus forte	En complément du niveau IV.c: un justificatif doit contenir des caractéristiques physiques. et le lien entre le requérant et les justificatifs a été établi en comparant la personne et les renseignements biométriques disponibles ou accessibles du justificatif le plus fort. et le lien entre le requérant et l'E-Identity déclarée a été vérifié au moyen d'une adresse postale.

Tableau 16: Modalités facteur *Validation des renseignements*

Exemples:

- Niveau IV.c
 - La vérification de caractéristiques physiques ou d'autres renseignements redondants (déclaration technique par la personne) peut être effectuée par des questions correspondantes par téléphone ou d'autres outils électroniques (questionnaires) par exemple.

5.2.1.4 Facteur Non-répudiabilité

Le facteur *Non-répudiabilité (Nonrepudiation, NP)* décrit si et comment au moment du dépôt de la demande, des données biométriques ont été collectées afin de pouvoir prouver la présence d'un sujet à un moment ultérieur.

Questions:	Est-il possible, à un moment ultérieur (après validation de l'identité), de prouver qu'un requérant était bien présent lors de l'enregistrement? Est-il possible d'empêcher que le sujet ne conteste la présence lors de l'enregistrement (et ainsi la délivrance d'un moyen d'authentification)?
------------	--

Remarques:

- Voir également NIST 800-63-3A [16] – chapitre 4.6.7
- En Suisse, l'ordonnance OSCSE 943.032 art 11.31[10] s'applique pour le niveau le plus élevé: les justificatifs pour l'identification des requérants doivent être conservés pendant onze années.

Niveau	Modalités	Description
NP.a	Pas de collecte	Aucune donnée biométrique n'est collectée lors du dépôt de la demande.
NP.b	Copie d'une pièce d'identité	Au moment de la vérification de l'identité, une copie d'un justificatif authentique et valide, qui contient les caractéristiques physiques, est créée.
NP.c	Collecte de données biométriques	Au moment de la vérification de l'identité, des données biométriques (ex. empreintes digitales ou portraits) sont collectées et enregistrées afin de documenter la présence du requérant.

Tableau 17: Modalités du facteur *Non-répudiabilité*

Exemples:

- Niveau NP.b
 - Copie d'une pièce d'identité

5.2.1.5 Facteur Procuration

Question:	La personne physique est-elle habilitée à agir au nom de l'organisation?
-----------	--

Remarques:

- aucune

Niveau	Modalités	Description
PA.a	Pas de procuration	Aucune procuration, ni déclaration de consentement n'est présentée.
PA.b	Procuration	L' article 5.2 de l'OSCSE [10] prévoit qu'une déclaration de consentement soit présentée: <ol style="list-style-type: none"> 1. Les personnes qui sont enregistrées au registre du commerce ont l'autorisation de signature conformément à cet enregistrement (signature individuelle, collective etc.). 2. Les personnes qui ne sont pas enregistrées au registre du commerce doivent fournir une déclaration constatant le consentement de la part du/des personnes habilitées à signer selon l'enregistrement au registre du commerce ou conformément à la représentation commerciale sur la base de l'article 32 et suivants du CO. 3. Concernant les administrations publiques: selon les bases légales en vigueur au niveau fédéral, cantonal et communal

Tableau 18: Modalités du facteur *Procuration*

5.2.2 Identification des personnes physiques

Le critère Identification des personnes physiques décrit comment une personne physique est identifiée. Il résume les facteurs suivants selon le schéma représenté dans le Tableau 19 (voir également Figure 11):

- Facteur Présence: chapitre 5.2.1.1
- Facteur Justificatif: chapitre 5.2.1.2
- Facteur Validation des renseignements: chapitre 5.2.1.3
- Facteur Non-répudiabilité: chapitre 5.2.1.4

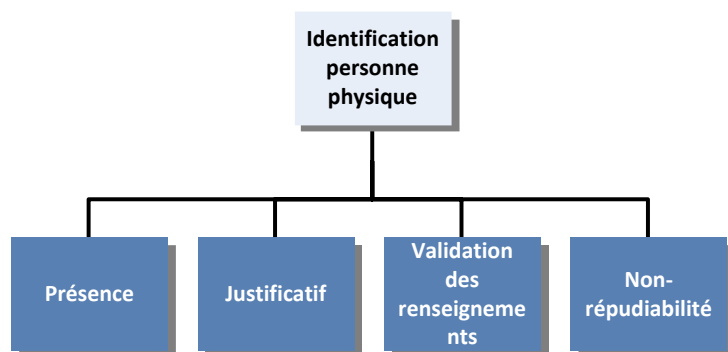


Figure 11: Facteurs relatifs au critère *Identification des personnes physiques*

Questions:	<p>Comment l'identité d'une personne physique, pour qui a été délivrée une identité électronique, a-t-elle été vérifiée?</p> <p>Selon quels points de vue les attributs facultatifs ont-ils été vérifiés?</p>
------------	---

Remarques:

- Les niveaux IDN2, IDN3 et IDN4 correspondent au niveau de sécurité *faible, significatif et élevé* dans eIDAS 2015/1502 [7], section 2.1.2 (justificatif et vérification d'identité (personne physique)).

Modalités	Description	Présence	Justificatif	Validation des renseignements	Non-répudiabilité
IDN1	Toutes les informations concernant l'identité sont auto-déclaratives et non vérifiées.	PP.a	IE.a	IV.a	NP.a
IDN2	Les informations concernant l'identité sont vérifiées à l'aide de justificatifs authentiques et valides. Le requérant peut être présent physiquement ou en ligne.	PP.b, PP.c ou PP.d	IE.b	IV.b	NP.a
IDN3	En complément du niveau IDN2: les justificatifs ont été validés de manière forte. Au moment de la vérification, la copie d'un justificatif avec les caractéristiques physiques a été créé.	PP.b, PP.c ou PP.d	1x IE.c ou 2 x IE.b	IV.c	NP.b
IDN4	En complément du niveau IDN3: le requérant doit être présent physiquement ou «virtual in-person» Les renseignements biométriques figurant dans les justificatifs sont vérifiés. Au moment de la vérification, la présence du requérant a été documenté.	PP.c ou PP.d	IE.d	IV.d	NP.c

Tableau 19: Modalités du critère *Identification des personnes physiques*

5.2.3 Identification des personnes morales

Question:	La personne morale existe-t-elle? Comment l'existence de la personne morale a-t-elle été vérifiée? Selon quels points de vue, les attributs ont-ils été vérifiés?
-----------	--

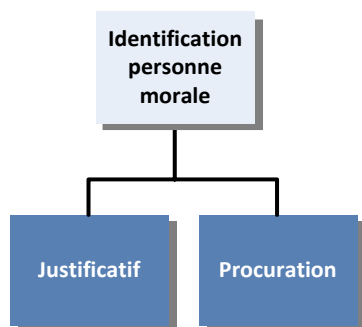


Figure 12: Facteurs relatifs au critère *Identification des personnes morales*

Le critère Identification de personnes morales décrit comme une personne morale (organisation) est identifiée. Il repose sur les facteurs *Justificatif* et *Procuration* (voir également Tableau 20):

- Facteur Justificatif: chapitre 5.2.1.4
- Facteur Procuration: chapitre 5.2.1.5

Remarques:

- Le niveau IDJ2 correspond au niveau de sécurité *faible* et IDJ3 correspond au niveau de sécurité *élevé* dans eIDAS 2015/1502 [5], section 2.1.3 Justificatif et vérification d'identité (personne morale)).

Modalités	Description	Justificatif	procuration
IDJ1 (auto-déclaratif)	Toutes les informations concernant l'identité sont auto-déclaratives et non vérifiées.	IE.a	PA.a
IDJ2 (vérifié)	Les informations concernant l'identité proviennent d'un justificatif valide et ont été validées.	IE.b	PA.a
IDJ3 (reconnu)	En complément du niveau IDJ2, les points suivants doivent être remplis: les informations concernant l'identité proviennent de justificatifs valides et reconnus. Les justificatifs ont été vérifiés. Le justificatif doit contenir un identificateur sans ambiguïté, le nom et la forme juridique de la personne morale.	IE.c	PA.a

Modalités	Description	Justificatif	procuration
IDJ4 (mandataire)	En complément du niveau IDJ3, les points suivants doivent être remplis: le justificatif doit être un extrait du registre du commerce actuel et certifié. ¹¹ Une déclaration de consentement doit être présentée.	IE.c	PA.b

Tableau 20: Modalités du critère *Identification de personnes morales*

5.2.4 Lien entre personne physique et morale

Question:	La personne physique a-t-elle le droit d'agir pour le compte de personne morale? Selon quelle précision le lien a-t-il été vérifié auprès d'une source fiable?
-----------	---

Remarques:

- Pour le niveau L4, il doit y avoir une entrée dans le registre du commerce en Suisse, voir OSCSE [10], Article 5.2
- eIDAS 2015/1502 [7], section 2.1.4 règle la question du cycle de vie d'un lien conformément aux procédures reconnues au niveau national.
- Ce lien nécessite des attributs supplémentaires afin de déterminer la fonction ou la (sous-)organisation de la personne physique au sein de la période morale.

Niveau	Modalités	Description
L1	Pas de vérification	Le lien entre la personne physique et la personne morale n'est pas vérifié.
L2	Lien simple	Le lien a été créé selon les procédures reconnues au niveau national.
L3	Lien avec inscription	Le lien a été créé selon les procédures reconnues au niveau national, ce qui a entraîné l'inscription du lien dans une source fiable.
L4	Lien avec identifiant unique	Le lien a été contrôlé, au moyen d'un identifiant sans ambiguïté utilisé dans l'environnement national, qui représente la personne morale, ainsi qu'au moyen d'informations émanant d'une source fiable, que les personnes physiques représentent sans ambiguïté.

Tableau 21: Modalités du critère *Lien entre personne physique et morale*

¹¹ D'après l'OSCSE [9], article 5.2

5.2.5 Transmission du moyen d'authentification

Questions:	<p>Comment assure-t-on que seul le bon sujet reçoit le mode/facteur d'authentification?</p> <p>Comment empêche-t-on que des personnes non autorisées puissent détenir le moyen d'authentification?</p> <p>En cas de livraison par la poste:</p> <p style="padding-left: 40px;">L'adresse postale indiquée par le requérant est-elle valable?</p> <p style="padding-left: 40px;">L'adresse postale peut-elle être attribuée à la prétendue identité électronique?</p>
------------	--

Le critère *Transmission du moyen d'authentification* décrit le processus de transmission pour un moyen d'authentification ou un facteur d'authentification.

Le critère peut être omis lorsque le CSP associe un moyen d'authentification à l'E-Identity du sujet, que ce dernier détient ou contrôle déjà (un mot de passe par exemple).

Si l'on utilise, pour une authentification, un moyen d'authentification avec plusieurs facteurs d'authentification ou plusieurs moyens d'authentification, le critère pour chaque moyen d'authentification ou chaque facteur d'authentification doit être déterminé individuellement. Le niveau de qualité global résulte alors du niveau le plus faible des différentes évaluations.

Le critère dépend du facteur *Address-Verification* (représenté dans le Tableau 22), lorsque la livraison s'effectue par la poste. Ce facteur (voir également NIST 800-63-3A [16] – *Address Confirmation, AC*) décrit si et comment les renseignements relatifs à une adresse postal ont été contrôlés.

Remarques:

- Les niveaux 2, 3 et 4a, 4b correspondent au niveau de sécurité faible, significatif et élevé dans eIDAS 2015/1502 [7], section 2.2.2 (délivrance, livraison et activation)
- Dans ISO 29115 [2], chap. 10.2.2.1 définit des *Controls* supplémentaires pour *Credential Issuance*.

Niveau	Modalités	Description	Address-Verification ¹²
1	Livraison simple	La livraison garantit une bonne certitude que le moyen d'authentification est affecté au bon sujet. Des processus sont définis et documentés.	Aucune vérification: Les renseignements sur l'adresse sont fournis à titre déclaratif et ne sont pas contrôlés.

¹² La vérification de l'adresse n'est pertinente qu'en cas de livraison par courrier.

Niveau	Modalités	Description	Address-Verification ¹²
2	Livraison sûre	<p>En complément du niveau 1:</p> <p><i>Après la délivrance, le moyen d'authentification est livré d'une manière selon laquelle il peut être supposé qu'il n'atteigne que le sujet à qui il est destiné.</i>¹³</p> <p>Dans le cas d'une livraison à domicile, le moyen d'authentification doit être protégé contre les modifications (<i>tampering</i>) au moyen d'une signature numérique.</p>	<p>Aucune vérification:</p> <p>Les renseignements sur l'adresse sont fournis à titre déclaratif et ne sont pas contrôlés.</p>
3	Livraison personnelle	<p>En complément du niveau 2:</p> <p><i>Après la délivrance, le moyen d'authentification est livré d'une manière permettant de supposer que seul le sujet à qui il appartient peut le détener.</i>¹⁴</p> <p>Si le moyen d'authentification n'est pas remis personnellement, l'existence et l'appartenance de l'adresse au sujet doivent être vérifiées.</p>	<p>Validation adéquate:</p> <p>Les renseignements sur l'adresse proviennent d'un justificatif valide approprié.</p>
4a	Avec processus d'activation pour le moyen d'authentification	<p>En complément du niveau 3:</p> <p><i>Dans le cadre du processus d'activation, l'on contrôle que seul le sujet, à qui il appartient, puisse détenir le moyen d'authentification.</i>¹⁵</p> <p>Dans le cas d'une livraison à domicile, l'on doit utiliser un canal sûr et le sujet (ou un représentant autorisé) doit confirmer la réception.</p> <p>Le processus d'activation ne doit être actif que pendant une durée déterminée (10 min max. en cas de livraison numérique du code d'activation; 7 jours max. en cas de livraison par courrier en Suisse; 21 jours max. pour l'étranger).</p>	<p>Validation forte:</p> <p>Les renseignements sur l'adresse proviennent d'un justificatif valide approprié et sont vérifiés de manière adaptée.</p>

¹³ eIDAS 2015/1502 [7], section 2.2.2. niveau de sécurité faible.

¹⁴ eIDAS 2015/1502 [7], section 2.2.2. niveau de sécurité significatif.

¹⁵ eIDAS 2015/1502 [7], section 2.2.2. niveau de sécurité élevé.

Niveau	Modalités	Description	Address-Verification ¹²
4b	Remise en main propre	Le moyen d'authentification est directement remis au sujet présent physiquement et en personne, par une instance habilitée par un CSP. L'identité du sujet est vérifiée au moyen d'une comparaison des caractéristiques physiques avec un justificatif approprié (validation forte IV.c). La réception fait l'objet d'un accusé de réception.	-

Tableau 22: Modalités du critère *Transmission du moyen d'authentification*

Exemples:

- Niveau 1
 - Le mot de passe (moyen d'authentification) est envoyé à l'adresse E-mail mentionné au moment de l'inscription.
- Niveau 2
 - Le nom d'utilisateur (identificateur) et le mot de passe (moyen d'authentification) sont envoyés séparément, au moins l'un des deux devant être envoyé par courrier à l'adresse mentionnée au moment de l'inscription.
 - Un lien pour le téléchargement du moyen d'authentification est envoyé à l'adresse E-mail mentionnée au moment de l'inscription. Les liens ne sont plus valables au bout d'un certain temps (ex. 24 heures).
- Niveau 3
 - Le justificatif pour les renseignements sur l'adresse peuvent être des attestations de domicile, des factures d'électricité ou d'eau.
 - Le moyen d'authentification est envoyé par lettre recommandée à l'adresse mentionnée au moment de l'inscription et vérifiée.
 - Le moyen d'authentification est téléchargé une fois saisi le mot de passe remis physiquement lors de l'inscription.
- Niveau 4a
 - Le moyen d'authentification est envoyé au sujet par lettre recommandée à l'adresse mentionnée au moment de l'inscription et vérifiée, il n'est activé qu'après validation de l'E-Identity par un processus d'activation.

- Niveau 4b
 - Le moyen d'authentification est mis à la disposition du sujet par lettre recommandée avec la mention complémentaire «en main propre»¹⁶.
 - Le moyen d'authentification est remis personnellement au sujet par une instance compétente (ex. remise des papiers d'identité par le service des pièces d'identités compétent en Allemagne¹⁷).

5.2.6 Prolongation/remplacement du moyen d'authentification

Questions:	<p>Dans quelles conditions un moyen d'authentification encore valide peut-il être prolongé ou un moyen d'authentification révoqué être remplacé?</p> <p>Comment peut-on garantir lors de la prolongation/du remplacement que le sujet existe encore et que les renseignements fournis (concernant l'adresse par exemple) sont encore exacts?</p>
------------	--

Le critère Prolongation/remplacement du moyen d'authentification évalue le processus,

- comment la validité d'un moyen d'authentification arrivant à expiration mais encore valide peut être prolongée (voir la colonne Prolongation dans le Tableau 29)
ou
- un moyen d'authentification révoqué peut être remplacé (voir la colonne Remplacement dans le Tableau 29)

Si plusieurs moyens d'authentification sont utilisés pour authentification, le critère doit être déterminé individuellement pour chaque moyen d'authentification. Le niveau de qualité global résulte ensuite du niveau le plus faible des différentes évaluations.

Remarques:

- Les niveaux CN1 et CN2 correspondent au niveau de sécurité faible et élevé dans eIDAS 2015/1502 [7], section 2.2.4 (prolongation et remplacement)
- Les exigences concernant *CredentialSecureRenewal* dans ISO 29115 [2] chapitre 10.2.2.1 ont été prises en compte.
- La rénovation d'un mot de passe à l'aide d'une adresse E-Mail valide est un cas particulier de remplacement de moyen d'authentification et correspond au niveau CN1.

¹⁶ La Poste suisse propose un service de remplacement correspondant pour les lettres recommandées, avec vérification de l'identité du destinataire. Voir <https://www.post.ch/de/geschaeflich/themen-a-z/zusatzleistungen/zusatzleistungen-briefe-inland/eigenhaendig>.

¹⁷ Voir http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/eperso.pdf?__blob=publicationFile.

Niveau	Modalités	Description	
		Prolongation	Remplacement
CN1	Prolongation après présentation/remplacement simple	Le CSP dispose de processus définis et documentés relatifs à la prolongation/au remplacement du moyen d'authentification.	
		Le moyen d'authentification encore valide est présenté lors de la demande de prolongation. Si le moyen d'authentification actuel a déjà expiré, une prolongation n'est plus possible. Toutes les interactions doivent passer par des canaux sûrs.	En cas de remplacement, un nouveau moyen d'authentification est simple-ment livré (voir critère <i>Transmission du moyen d'authentification</i> niveau 1).
CN2	Prolongation après présentation/ remplacement sûr	Comme pour CN1.	En cas de remplacement, un nouveau moyen d'authentification est livré de manière sûre (voir critère <i>Transmission du moyen d'authentification</i> niveau 2).
CN3	Prolongation après présentation/ remplacement personnel	En complément du niveau CN2: Le sujet doit être à nouveau identifié selon IDN2 ou IDJ2.	
		Comme pour CN2.	En cas de remplacement, un nouveau moyen d'authentification est personnellement livré (voir critère <i>Transmission du moyen d'authentification</i> niveau 3).

Niveau	Modalités	Description	
		Prolongation	Remplacement
CN4	Prolongation/remplacement après vérification	En complément du niveau CN3: <i>en cas de prolongation ou de remplacement sur la base de moyens d'identifications électroniques valides, les données d'identité sont contrôlées au moyen d'une source fiable.</i> ¹⁸	
		ou pour les personnes physiques, un justificatif du niveau IE.d doit être remis et les renseignements être validés selon le niveau IV.d. Pour les personnes morales, il faut en outre vérifier le lien avec la personne physique selon le niveau L4.	
			Le moyen d'authentification remplacé est remis en main propre (voir critère <i>Transmission du moyen d'authentification</i> niveau 4).

Tableau 23: Modalités du critère *Prolongation/remplacement du moyen d'authentification*

6 Modèle de qualité du pilotage

Le modèle de qualité du pilotage est déterminé par l'évaluation du critère *Piloter l'IAM* (voir Annexe G.3 pour une description du processus).

Le modèle de qualité du pilotage contient trois critères (voir Figure 13).

6.1 Niveaux de confiance du pilotage (NDCP)

Les niveaux de confiance du pilotage (NDCP) découlent des trois critères suivants (voir Figure 13):

- Surveillance (chapitre 6.2.1),
- Responsabilité (chapitre 6.2.2),
- Maturité (chapitre 6.2.3).

¹⁸ eIDAS 2015/1502 [5], section 2.2.4. niveau de sécurité élevé.

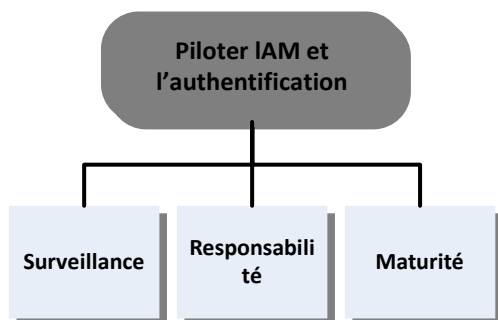


Figure 13: Critères pour le modèle de qualité du pilotage

Le niveau de confiance du pilotage (NDCP) est déterminé par la modalité la plus faible des critères.

Niveau de confiance du pilotage (NDCP)	Surveillance	Responsabilité	Maturité
1	Interne selon norme propre ou pas du tout	Aucune responsabilité	Initial
2	Interne selon règles/normes prédéfinies	Responsabilité limitée	Défini
3	Audit externe	Responsabilité selon la loi	Géré, mesuré
4	Audit par instance accréditée	Responsabilité + peine conventionnelle	Optimisé, intégré

Tableau 24: Détermination du niveau de confiance du pilotage (NDCP)

6.2 Critères du pilotage

6.2.1 Surveillance

Questions:	<p>Dans quelle mesure les prestataires de service sont-ils dignes de confiance?</p> <p>De quelle qualité sont les processus des prestataires de service?</p> <p>Comment les prestataires sont-ils surveillés?</p>
------------	---

Les processus de mise à disposition des services sont variés et divergent notamment en termes de qualité. Si les processus s'appuient sur des normes et que la mise en œuvre des processus est en outre vérifiée, la qualité des processus des prestataires de service augmente. Plus la qualité des processus internes est élevée, plus le potentiel de risque d'attaques et d'erreurs est faible.

Si, lors de l'authentification du sujet, plusieurs prestataires de service sont impliqués, le critère doit être déterminé au cas par cas pour chaque prestataire de service. Le niveau le plus faible détermine ensuite la qualité globale de ce critère.

Remarques:

- Les niveaux 2, 3 et 4 correspondent au niveau de sécurité faible, significatif et élevé dans eIDAS 2015/1502 [7], section 2.4.7 (respect et vérification)
- En Suisse, l'ordonnance OSCSE SR 943.032 [10] s'applique pour le niveau 4.
- Les niveaux correspondent au critère *Surveillance Attribute-Authority* dans la norme eCH-0171 [5], qui ne décrit toutefois que la surveillance de l'Attribute-Authority.

Niveau	Modalités	Description
1	Interne selon norme propre ou pas du tout	Le prestataire de service ne s'oriente par rapport à aucune norme ou des normes élaborées en interne. Il n'y a pas de vérification du respect par une instance interne.
2	Interne selon règles/normes prédéfinies	Le prestataire de service s'oriente par rapport à des normes publiquement accessibles et utilisées de manière répandue. La vérification du respect des normes est régulièrement effectuée par une instance interne.
3	Audit indépendant	Le prestataire de service s'oriente par rapport à des normes publiquement accessibles et utilisées de manière répandue. La vérification du respect des normes est régulièrement effectuée par une instance indépendante.
4	Audit par une instance accréditée	Le prestataire de service s'oriente par rapport à des normes, dont le respect et la vérification sont effectués par une instance officiellement accréditée. <i>Si le système est directement géré par un service d'Etat, les vérifications sont effectuées selon la réglementation nationale.</i> ¹⁹

Tableau 25: Modalités du critère *Surveillance*

6.2.2 Responsabilité

Question:	Quelle est la portée de la responsabilité des prestataires de service?
-----------	--

Le critère *Responsabilité du prestataire de service* montre dans quelle mesure il est obligé de répondre des services qu'il met à disposition. Plus l'obligation/la volonté d'assumer une responsabilité est élevée, plus la qualité est grande.

¹⁹ eIDAS 2015/1502 [7], section 2.4.7. niveau de sécurité élevé.

Remarques:

- Les niveaux correspondent également au critère *Responsabilité de l'Attribute-Authority* dans la norme eCH-0171 [5], qui se contente toutefois de décrire la responsabilité de l'Attribute-Authority.
- Le niveau utilisé pour l'administration fédérale est toujours le 4.

Niveau	Modalités	Description
1	Aucune responsabilité	Toute responsabilité est déclinée par contrat ou les CGV dans la mesure où la législation le permet.
2	Responsabilité limitée	La responsabilité est limitée par contrat ou les CGV dans la mesure où la législation le permet.
3	Responsabilité selon la loi	Les dispositions en matière de responsabilité s'appliquent à la responsabilité du prestataire de service (partie générale du Code des obligations (art. 97 et suivants), selon le SCSE [9]).
4	Responsabilité + peine conventionnelle	En complément du niveau 3, la mise en œuvre des droits à dédommagement est facilitée par l'accord sur une peine conventionnelle cumulée raisonnable selon l'article 163 et suivants du CO.

Tableau 26: Modalités du critère *Responsabilité*

6.2.3 Maturité

Questions:	<p>Quel est le degré de maturité du système d'enregistrement et d'authentification?</p> <p>Dans quelle mesure le prestataire de service est-il à même d'intégrer ses propres constatations, comme les incidents de sécurité par exemple?</p> <p>Dans quelle mesure le prestataire de service est-il en mesure d'adapter bien et rapidement ses processus sur la base de nouvelles constatations (propres ou externes)?</p>
------------	--

Les définitions de processus et leur application pour la fourniture de services varient pour chaque prestataire de service et divergent en termes de niveau de détail. Si ces processus s'appuient sur des normes et que la mise en œuvre des processus fait en outre l'objet de vérifications, la qualité des processus des prestataires de service augmente. Plus la qualité des processus internes est élevée, plus le potentiel de risque d'attaques et d'erreurs est faible. Plus la qualité de la capacité de changement de ces processus est élevée, plus la confiance dans ce prestataire de service est élevée.

Si, plusieurs prestataires de service sont impliqués dans l'authentification du sujet, le critère doit être déterminé au cas par cas pour chaque prestataire de service. Le niveau le plus faible détermine alors la qualité globale de ce critère.

Les niveaux suivants du degré de maturité dans le modèle de maturité eCH-0172 [22] sont utilisés pour définir les niveaux pour le critère *Maturité*:

- Degré de maturité niveau 1: initié, adhoc et degré de maturité niveau 2: correspond au niveau 1,
- Degré de maturité niveau 3: défini, correspond au niveau 2,
- Degré de maturité niveau 4: géré, mesuré, correspond au niveau 3,
- Degré de maturité niveau 5: optimisé, intégré, correspond au niveau 4.

Dans le cas où, lors de la classification d'un prestataire de service, l'évaluation ne peut être effectuée, il faut supposer que les processus ont été au moins définis, mais n'ont éventuellement pas été documentés. Cette supposition s'explique par le fait qu'il s'agit en grande partie d'opérations automatisées.

Niveau	Modalités	Description
1	Initial	Les processus sont adhoc et non organisés (degré de maturité 1) ou suivent déjà un modèle régulier (degré de maturité 2).
2	Défini	En complément du niveau 1: Les processus sont documentés et communiqués. Il existe un logging pour les opérations d'enregistrement et d'authentification et il y a des règles et des processus d'alerte pour les authentifications qui échouent.
3	Géré, mesuré	En complément du niveau 2: Les processus sont surveillés et mesurés. Il existe des règles relatives à l'enregistrement des catégories d'utilisateur, à la force de l'authentification, découlant du besoin de protéger les ressources, des règles d'authentification pour l'utilisation de Federated IAM..
4	Optimisé, intégré	En complément du niveau 3: Les Good Practices (les règles relatives à la détermination du niveau de qualité selon une norme (STORK-QAA, eCH, ...)) sont appliquées, les processus sont automatisés (il existe une infrastructure de répertoire centralisée pour l'identification et l'authentification pour la période d'exécution) et améliorés au moyen de contrôles systématiques des processus.

Tableau 27: Modalités du critère *Maturité*

7 Modèle de qualité de la fédération

Le modèle de qualité de la fédération est déterminé par l'évaluation des critères du processus *Fédérer l'identité* (se reporter à l'Annexe G.1.2. pour une description du processus).

7.1 Niveaux de confiance de la fédération (NDCF)

Les niveaux de confiance de la fédération (NDCF) découlent des 4 critères suivants (voir Figure 14):

- Justificatif de détention de la confirmation d'authentification (chapitre 7.2.1).
- Authenticité de la confirmation d'authentification (chapitre 7.2.2),
- Protection de la confidentialité de la confirmation d'authentification (chapitre 7.2.3),
- Forme de transmission de la confirmation d'authentification (chapitre 7.2.4),

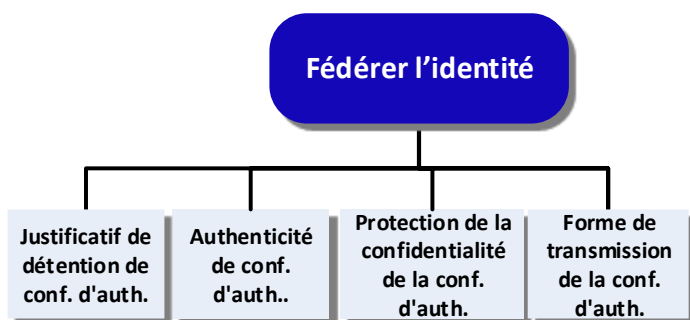


Figure 14: Critères pour le modèle de qualité de la fédération

Le niveau de confiance de la fédération (NDCF) est ici déterminé par la modalité des critères.

Niveaux de confiance de la fédération (NDCF)	Justificatif de détention de la conf. auth.	Authenticité	Protection de la confidentialité	Forme de transmission
1	Porteur	Signature numérique	Aucun	Indépendant
2	Porteur	Signature numérique	Cryptage	Front Channel
			Aucun	Back Channel
3	Contrôlable par RP	Signature numérique	Cryptage	Indépendant

Tableau 28: Niveaux de confiance de la fédération (NDCF)

Exemples:

- VSF1: SuisseID, Standard SAML Web SSO profile, OpenID Connect Implicit Client Profile
- VSF2:
 - (Front Channel): SwitchAAI
 - (Back Channel): SAML Artifact Binding, OpenID Connect ID Token
- VSF3:
 - SAML Holder of Key Profile

7.2 Critères de la fédération

7.2.1 Justificatif de détention de la confirmation d'authentification

Questions:	La confirmation d'authentification permet-elle d'identifier suffisamment le sujet? La confirmation d'authentification représente-t-elle le sujet référencé (abonné) de manière sûre? Y a-t-il une protection contre les attaques de type usurpation d'identité? Le porteur de la confirmation d'authentification est-il également l'abonné (le sujet qui s'est authentifié au préalable)?
------------	--

Remarque:

- Correspond à l'*assertion détention category* de NIST 800-63C [18]

Modalités	Description
Porteur - Bearer (B)	L'identité du sujet est uniquement confirmée par la confirmation d'authentification. Le RP doit partir du principe que la confirmation d'authentification a été délivrée pour le sujet porteur. Cela représente la forme la plus faible de confirmation d'authentification dans un système d'identité fédéré. Quand un assaillant est capable d'intercepter une telle confirmation d'authentification et de la présenter lui-même au RP, il est en mesure d'accéder à une ressource protégée en utilisant une fausse identité.
Contrôlable par RP - Holder-of-Key (HoK)	La confirmation d'authentification contient une référence à un moyen d'authentification (authentificateur), dont la détention identifie encore plus le sujet. Le RP peut ainsi demander au porteur de s'authentifier à nouveau.

Tableau 29: Modalités du critère Justificatif de détention de la confirmation d'authentification

7.2.2 Authenticité de la confirmation d'authentification

Questions:	<p>L'origine et l'intégrité de la confirmation d'authentification peuvent-elles être prouvées?</p> <p>La confirmation d'authentification est-elle authentique?</p> <p>L'émetteur peut-il être identifié sans ambiguïté?</p> <p>L'émetteur peut-il contester avoir délivrer la confirmation d'authentification?</p>
------------	--

Remarques:

- L'authenticité d'une confirmation d'authentification est en règle générale garantie par une signature numérique asymétrique. D'autres moyens peuvent également être envisagés (ex. avec des algorithmes symétriques), lorsque le RP se trouve en position de pouvoir constater, de manière suffisante, l'origine d'une confirmation d'authentification. Les assertions relatives à des procédures concrètes ne sont pas l'objet de cette norme.
- L'authenticité fait partie de l'*assertion protection category* dans NIST SP 800-63C [18].

Modalités	Description
Aucune mesure	Aucune mesure n'a été prise afin de sécuriser l'authenticité de la confirmation d'authentification.
Mesures de sécurisation de l'authenticité (signature numérique)	Des mesures suffisantes ont été prises afin de sécuriser l'authenticité de la confirmation d'authentification.

Tableau 30: Modalités du critère *Authenticité de la confirmation d'authentification*

Exemples:

- Dans le cas de SAML, la confirmation d'authentification est signée (authentication assertion) avec une clé privée de l'IdP. La clé publique correspondante est publiée et accessible au RP.
- Dans le cas de Kerberos, le ticket est crypté de manière symétrique avec une clé, échangée au préalable entre le service destinataire (RP) et le Key Distribution Center (IdP).

7.2.3 Protection de la confidentialité de la confirmation d'authentification

Question:	La confirmation d'authentification est protégée de manière à ce que des tiers non autorisés ne puissent consulter les informations contenues?
-----------	---

Remarques:

- Le cryptage fait partie de l'*assertion protection category* dans NIST SP 800-63C [18]
- Le cryptage contribue à la sécurité. Les données peuvent être protégées contre la transmission par rapport aux éléments d'acheminement (navigateur par exemple)
- Les assertions relatives à des procédures concrètes ne sont pas l'objet de cette norme.

Modalités	Description
Aucun cryptage	La confirmation d'authentification n'est pas cryptée.
Cryptage	Le Payload de la confirmation d'authentification a été crypté par l'IdP avec la clé publique du RP. ²⁰

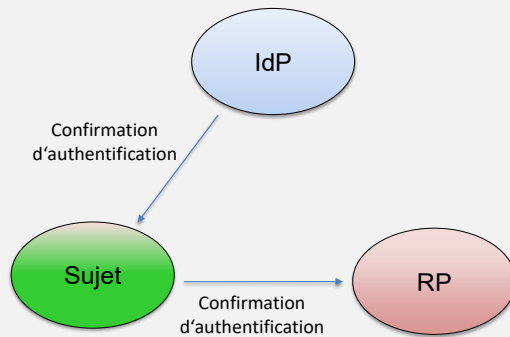
Tableau 31: Modalités du critère *Cryptage de la confirmation d'authentification*

7.2.4 Forme de transmission de la confirmation d'authentification

Question:	La confirmation d'authentification est-elle transmise de manière à ce que des tiers non autorisés ne puissent consulter les informations contenues?
-----------	---

Remarque:

- La forme de transmission fait partie de l'*assertion protection category* dans NIST SP 800-63C [18].

Modalités	Description
Front Channel	<p>Concernant la transmission par Front Channel, l'IdP génère, une fois l'authentification primaire réussie, une confirmation d'authentification et l'envoie au sujet (ou à la Client Application de ce dernier). Le sujet présente cette assertion au RP, afin de s'authentifier auprès de lui ou d'obtenir son autorisation.</p>  <p>Figure 15: Transmission par Front Channel</p>

²⁰ Pour des raisons de performance, dans le cas de la cryptographie asymétrique, on ne chiffre pas le Payload total, mais l'on a recours à une cryptographie hybride: la cryptographie hybride consiste pour l'expéditeur (IdP) à générer une clé symétrique aléatoire (Session-Key). Avec cette Session-Key, les données à protéger sont chiffrées de manière symétrique. La Session-Key est ensuite encryptée de façon asymétrique avec la clé publique du destinataire (RP) [27] [21].

Modalités	Description
Back Channel	<p>Concernant la transmission par Back Channel, l'IdP transmet une référence (ex. sous la forme HTTP Redirect URL) au sujet. La référence elle-même ne contient <i>aucune</i> information relative au sujet. Le sujet transmet cette référence au RP. Au moyen de cette référence, le RP peut se procurer la confirmation d'authentification auprès de l'IdP dans le délai autorisé et avec l'autorisation correspondante via un Back-Channel.</p> <p>Figure 16: Transmission par Back Channel</p>

Tableau 32: Modalités du critère *Forme de transmission de la confirmation d'authentification*

8 Comparaison avec les normes internationales

Dans ce chapitre, l'on compare les modèles des normes internationales (NIST SP 800-63-3 [3], règlement eIDAS 910/2014 [1], ISO/IEC 29115 [2]) avec les niveaux de confiance définis dans cette norme.

La comparaison exposée par le Tableau 33 offre une vue d'ensemble de la façon dont les niveaux de confiance peuvent être classés de manière grossière.

Niveau de confiance (NDC)	NIST	eIDAS 910/2014	ISO/IEC 29115
VS1	AAL 1 IAL 1 FAL 1	-	LoA1
VS2	AAL 1 - FAL 2	faible ²¹	LoA2
VS3	AAL 2 IAL 2 FAL 2	significatif	LoA3

²¹ eIDAS exige au niveau „faible“ uniquement un facteur pour l'authentification. Pour l'enregistrement comme pour le pilotage, eIDAS exige au moins un justificatif ou un audit interne. C'est la raison pour laquelle eIDAS classera grossièrement 'faible' comme VS2.

Niveau de confiance (NDC)	NIST	eIDAS 910/2014	ISO/IEC 29115
VS4	AAL 3 IAL 3 FAL 3	élevé	LoA4

Tableau 33: Vue d'ensemble de la comparaison des niveaux de confiance

Chaque norme internationale ne couvre pas tous les modèles partiels définis dans la présente norme. C'est la raison pour laquelle les différentes étapes sont mises en regard et les différences mises en évidence dans les chapitres qui suivent. Les seuls critères évoqués à cet égard sont ceux qui sont pertinents pour l'évaluation qualitative.

Les niveaux de confiance sont comparés à leurs équivalents dans les normes internationales. Les différences sont marquées (d'un astérisque *) et décrites.

8.1 Modèle de qualité de l'authentification

Le niveau de sécurité eIDAS et le Level of Assurance ISO/IEC 29115 correspondent aux niveaux de confiance de l'authentification définis dans cette norme, d'après le Tableau 34.

Niveau de confiance de l'authentification (NDCA)	NIST SP 800-63-3	eIDAS 910/2014	ISO/IEC 29115
VSA1	AAL 1*	faible	LoA2
VSA2	AAL 1*	significatif	LoA3
VSA3	AAL 2*	élevé	LoA3
VSA4	AAL 3*	élevé	LoA4

Tableau 34: Comparaison du modèle de qualité de l'authentification

Différences par rapport à NIST SP 800-63B

Dans NIST SP 800-63B [13], le critère *Reauthentication* et *Assertion* (correspond au critère *Justificatif de détention de la confirmation d'authentification*), employé dans cette norme pour déterminer les niveaux de confiance de la fédération (NDCF), est également utilisé pour la détermination de l'AAL.

8.2 Modèle de qualité de l'enregistrement

8.2.1 Enregistrement pour les personnes physiques

Niveau de confiance de l'enregistrement pour les personnes phys. (NDCPP)	NIST SP 800-63-3	eIDAS 910/2014	ISO/IEC 29115
VSRN1	IAL 1	-	LoA1
VSRN2	-	faible	LoA2*
VSRN3	IAL 2*	significatif	LoA3
VSRN4	IAL 3*	élevé	LoA4

Tableau35: Comparaison du modèle de qualité de l'enregistrement des personnes physiques

Différences par rapport à NIST SP 800-63B

NIST SP 800-63B ne prend en charge que 3 Identity Assurance Level (IAL1, IAL2 et IAL3), qui correspondent aux niveaux de confiance VSRN1, VSRN3 et VSRN4.

Les différences entre les niveaux de confiance et l'Identity Assurance Level reposent principalement sur la qualité et le nombre de justificatifs et ont été par conséquent adaptés, dans cette norme, au contexte suisse (présentation d'une pièce d'identité).

NIST n'accepte pas la présentation, comme justificatif, d'un justificatif électronique d'une E-Identity notifiée ou certifiée valide, de qualité égale ou supérieure.

Différences par rapport à ISO/IEC 29115

ISO requiert déjà au LoA2 un justificatif avec une photo du sujet. La transmission devrait être effectuée selon le critère 5.2.5 Transmission du moyen d'authentification au niveau 3 (Transmission personnelle).

8.2.2 Enregistrement des personnes morales

Seul eIDAS traite et évalue la qualité de l'enregistrement des personnes morales. La comparaison avec les niveaux de confiance de l'enregistrement pour les personnes morales est représentée au Tableau 36.

Les Non-Person Entities (NPE) décrites dans ISO/IEC 29115 ne doivent pas être considérées comme équivalentes aux personnes morales.

NIST SP 800-63-3 ne traite pas la question des personnes morales.

Niveau de confiance de l'enregistrement pour les personnes mor. (NDCPM)	NIST SP 800-63-3	eIDAS 910/2014	ISO/IEC 29115
VSRJ1	-	-	-
VSRJ2	-	faible	-
VSRJ3	-	élevé	-
VSRJ4	-	-	-

Tableau 36: Comparaison du modèle de qualité de l'enregistrement des personnes morales

8.3 Modèle de qualité du pilotage

Le niveau de sécurité eIDAS et le Level of Assurance ISO 29115 correspondent aux niveaux de confiance du pilotage (NDCP), qui ont été définis dans cette norme (voir Tableau 37).

Dans NIST SP 800-63-3, les mesures de sécurité sont définies d'après NIST SP 800-53 [23], en fonction de la valeur, en termes de protection, des données à gérer.

Niveau de confiance du pilotage (NDCP)	NIST SP 800-63-3*	eIDAS 910/2014	ISO/IEC 29115
NDCP1	-	-	LoA 1
NDCP2	-	faible	LoA 2
NDCP3	-	significatif	LoA 3
NDCP4	-	élevé	LoA 4

Tableau 37: Comparaison du modèle de qualité du pilotage

8.4 Modèle de qualité de la fédération

Les niveaux de confiance de la fédération (NDCF) correspondent au Federation Assurance Level (FAL) du NIST SP 800-63C [18] (voir Tableau 38).

Ni le règlement eIDAS 910/2014 [1], ni l'ISO/IEC 29115 [2] ne prennent en compte la qualité de l'authentification dans une Identity Federation, en tant que modèle de qualité autonome. On part donc du principe ceux-ci sont intégrés pour eIDA et ISO.

Niveau de confiance de la fédération (NDCF)	NIST SP 800-63-3*	eIDAS 910/2014	ISO/IEC 29115
VSF1	FAL 1	-	-
VSF2	FAL 2	-	-
VSF3	FAL 3	-	-

Tableau 38: Comparaison du modèle de qualité de la fédération

Différences par rapport à NIST SP 800-63C

A la différence de la norme NIST, VSF2 fait la distinction entre Front-Channel et Back-Channel. Jusqu'à ce niveau de confiance, nous considérons la transmission cryptée d'une Assertion via le navigateur (Front Channel) et d'une Assertion non cryptée via un canal sûr entre l'IdP et le RP comme équivalentes en termes de protection de la confidentialité.

9 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.

10 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] R. Bernold, G. Hassenstein, A. Laube-Rosenpflanzler, A. Spichiger, and M. Topfel, "eCH-0107 Gestaltungsprinzipien für die Identitäts- et Zugriffsverwaltung (IAM)," 2013.
- [2] M. Topfel, T. Jarchow, A. Spichiger, and R. Bernold, "eCH-0171 Qualitätsmodell der Attributwertbestätigung zur eID," 2014.
- [3] B. Hulsebosch, G. Lenzin, and H. Eertink, "STORK: D2.3 - Quality authenticator scheme," 2007.
- [4] D. A. S. Europ, I. Parlement de, CONSEIL DE Europ, et I. Union, "RÈGLEMENT (UE) n° 910/2014 DU PARLEMENT ET DU CONSEIL EUROPÉEN du," vol. 2014, n° 910, 2015.
- [5] Union européenne, "Règlement d'exécution (UE) n° 2015/1502 de la Commission du 8 septembre 2015," n° septembre, 2012.
- [6] P. Editors, W. Fumy, M. De Soete, E. J. Humphreys, K. Naemura, and K. Rannenber, "ITU-T Recommendation X . 1254 | International Standard ISO / IEC DIS 29115 Information technology — Security Techniques — Entity Authentication Assurance Framework," 2011.
- [7] J. L. F. Paul A. Grassi, "DRAFT NIST Special Publication 800-63-3," 2016. [Online]. Available: <https://pages.nist.gov/800-63-3/sp800-63-3.html>. [Accessed: 01-Sep-2016].
- [8] R. Kissel, "Glossary of Key Information Security Terms Glossary of Key Information Security Terms," *Nist*, vol. NISTIR 729, n° révision 2, 2013.
- [9] Le Conseil fédéral suisse, "Ordonnance sur les services de certification dans le domaine des signatures électroniques et des autres applications des certificats numériques," 2016.
- [10] P. Madsen, E. Maler, S. Microsystems, T. Wisniewski, T. Nadalin, S. Cantor, and J. Hodges, "SAML V2.0 Executive Overview," no. April, pp. 1–7, 2005.
- [11] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, W. E. Burr, D. F. Dodson, and R. A. Perlner, "NIST Special Publication 800-63-2 Electronic Authentication Guideline."
- [12] "DRAFT Strength of Function for Authenticators - Biometrics." [Online]. Available: <https://pages.nist.gov/SOFA/SOFA.html>. [Accessed: 03-Nov-2016].
- [13] J. P. R. Paul A. Grassi, Elaine M. Newton, Ray A. Perlner, Andrew R. Regenscheid, William E. Burr, James L. Fenton, "DRAFT NIST Special Publication 800-63B," 2016. [Online]. Available: <https://pages.nist.gov/800-63-3/sp800-63b.html>. [Accessed: 22-Aug-2016].
- [14] J. L. F. Paul A. Grassi, Jamie M. Danker, William E. Burr, "DRAFT NIST Special Publication 800-63A," 2016. [Online]. Available: <https://pages.nist.gov/800-63-3/sp800-63a.html>. [Accessed: 01-Sep-2016].
- [15] S. K. S. Paul A. Grassi, James L. Fenton, Justin P. Richer, "DRAFT NIST Special Publication 800-63C." [Online]. Available: <https://pages.nist.gov/800-63-3/sp800-63c.html>. [Accessed: 01-Sep-2016].
- [16] H. Häni and U. Kienholz, "eCH-0172 Modèle de maturité IAM," 2014.
- [17] Joint Task Force Transformation Initiative, "Security and Privacy Controls for Federal Information Systems and Organizations [SP 800-53]," 2015.
- [18] "Measuring Strength of Identity Proofing," 2016.
- [19] A. Laube-rosenpflanzler, G. Hassenstein, S. Agosti, M. Vinzens, U. Pfenninger, and D. Leiser, "eCH-0168 SuisseTrustIAM technique Architektur und Prozesse," 2014.

- [20] T. Polk, K. Mckay, and S. Chokhani, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations [SP 800-52]," 2014.
- [21] "Cryptographie hybride." [Online]. disponible:
https://fr.wikipedia.org/wiki/Cryptographie_hybride.

Annexe B - Collaboration & vérification

Buff Raffael	Abraxas Informatik AG
Gruoner Torsten	Administration fédérale – DFF – UPIC
Hassenstein Gerhard	Haute Ecole Spécialisée Bernoise
Heerkens Marc	Administration fédérale – EFD – UPIC
Kunz Marc	Haute Ecole Spécialisée Bernoise
Laube-Rosenpflanzner Annett	Haute Ecole Spécialisée Bernoise
Schlunegger Yves	CSC Switzerland GmbH
Selzam Thomas	Haute Ecole Spécialisée Bernoise
Spichiger Andreas	Haute Ecole Spécialisée Bernoise

Annexe C - Abréviations et glossaire

C.1 Abréviations

AAL	Authentication Assurance Level
CA	Credential Authority
CSP	Credential Service Provider
eIDAS	Règlement (UE) n° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur
UE	Union européenne
FAL	Federation Assurance
FIDO	Fast IDentity Online
HoK	Holder of Key
HTTP	Hypertext Transfer Protocol
HW-MFA	Hardware Multifactor Authentication
IAL	Identity Assurance Level
IAM	Identity and Access Management
IdP	Identity Provider
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
KDC	Kerberos Distribution Center
LoA	Level of Assurance
MFA	Multi Factor Authentication

NIST	National Institute of Standards and Technology
nPA	neuer Personalausweis (nouvelle carte d'identité)
OIDC	OpenID Connect
OTP	One-time Password
PIN	Numéro d'identification personnel
RA	Register Authority / autorité d'enregistrement
RP	Relaying Party
SAML	Security Assertion Markup Language
SFA	Single Factor Authentication
SMS	Short Message Service
SR	Recueil systématique du droit fédéral
SSO	Single Sign-on
STORK	Secure idenTity acrOss boRders linKed
TGT	Ticket Granting Ticket
TSP	Trust Service Provider
IDE	Unique identifier
URL	Uniform Resource Locator
NDC	Niveau de confiance
NDCA	Niveau de confiance de l'authentification
NDCF	Niveau de confiance de la fédération
NDCE	Niveau de confiance de l'enregistrement
NDCPM	Niveau de confiance de l'enregistrement pour les personnes morales
NDCPP	Niveau de confiance de l'enregistrement pour les personnes physiques
NDCP	Niveau de confiance du pilotage
CC	Code civil suisse

C.2 Glossaire

Authentificateur	Représentation fonctionnelle du moyen d'authentification du monde réel. La fonction d'un authentificateur permet de produire une valeur de sortie à partir d'une valeur de saisie et d'une valeur secrète.
Authentification	Opération de vérification d'une E-Identity déclarée.
Confirmation d'authentification	Confirmation de l'authentification réussie d'un sujet.

Facteur d'authentification	Informations et/ou processus, qui peuvent être utilisés pour l'authentification d'un sujet. Les facteurs d'authentification peuvent reposer sur quatre caractéristiques distinctes (dépendant de la détention, dépendant des connaissances, inhérent ou basé sur le comportement) ou combinaisons des celles-ci.
Moyen d'authentification	Quelque chose qu'un sujet détient et dont il a le contrôle (une clé cryptographique, un secret ou une caractéristique biométrique).
Justificatif	Document ou objet provenant d'une source fiable, qui contient les renseignements concernant le requérant.
Caractéristique biométrique	Une caractéristique biométrique est une caractéristique physique d'une personne, qui peut être utilisée à des fins d'identification.
Certificate Authority / Certification authority (CA)	Une Certificate Authority est un Credential Service Provider (CSP) spécial, qui délivre, renouvelle et révoque des certificats numériques (Public Key certificate, X.509 par exemple) comme moyen d'authentification.
Client Platform	Le système ou l'appareil depuis lequel le sujet initie un processus d'authentification.
Credential	Un Credential représente une quantité de données, par laquelle une E-Identity est liée à un moyen d'authentification, qui est détenu et contrôlé par le sujet.
Credential Service Provider (CSP)	Une entité, qui agit comme éditeur digne de confiance de certificats numériques et d'autres tokens de sécurité (moyens d'authentification).
E-Identity	Représentation d'un sujet. Une E-Identity (identité numérique) a un identificateur (nom sans ambiguïté), dans la plupart des cas avec une quantité d'attributs supplémentaires, qui peuvent être attribués sans ambiguïté à un sujet à l'intérieur d'un espace de nom. Un sujet peut avoir plusieurs E-Identities.
Moyen d'identification électronique	Contient des facteurs d'authentification, des attributs pour les personnes et a une validité. Lors d'une authentification, le processus global Authentifier le sujet est effectué par des moyens d'identification électroniques. Il englobe ainsi le moyen d'authentification, le Credential et l'IdP.
Système d'identification électronique	Terme tiré d'eIDAS 910/2014 [1]: un «système d'identification électronique» est un système pour l'identification électronique, dans le cadre duquel des moyens d'identification électronique sont délivrés pour des personnes physiques ou morales ou des personnes morales, qui représentent des personnes morales. Un système d'identification électronique notifié doit remplir toutes les conditions prérequisées répertoriées dans eIDAS 910/2014 [1] Article 7.

Moment de définition	Le système IAM est mis en place et configuré au cours de la période de définition. Les identités électroniques sont en outre établies La période de définition englobe ainsi les processus de mise à disposition de toutes les informations nécessaires pour tous les composants impliqués ainsi que les composants eux-mêmes.
Fédération / Fédération	Une fédération est une collaboration entre différentes entités d'un système IAM par delà les limites des organisations et des systèmes, sans duplication ni réplique des données d'utilisateur nécessaires à cela (E-Identities).
Identification	L'identification est une opération pour la période de définition, qui consiste à vérifier l'identité du sujet au moyen de justificatifs.
Document d'identité	a) Passeport, b) Carte d'identité suisse c) Carte d'identité reconnue pour l'entrée sur le territoire de la Suisse
Identity Provider (IdP)	Entité qui vérifie pour la période d'exécution l'identité électronique du sujet. On vérifie que le sujet détient et contrôle le moyen d'authentification et qu'il existe bien un lien entre le sujet et les moyens d'authentification utilisés à l'aide des Credentials.
Personne morale	Les personnes morales sont des organisations selon l'article 52 et suivant du CC ainsi que selon les dispositions applicables du droit des sociétés du CO.
Caractéristique physique	Caractéristique d'une personne, comme la taille et la couleur des yeux.
Période d'exécution	Les processus électroniques, par lesquels un sujet peut accéder aux ressources d'un Relying Party, ont lieu pour la période d'exécution.
Autorité d'enregistrement / Registration Authority (RA)	Une entité, qui enregistre suffisamment d'informations concernant un sujet pour pouvoir vérifier son identité.
Sujet	Une personne physique, une organisation ou un service, qui accède ou souhaite accéder à une ressource. Un sujet est représenté par des E-Identities.
Unité IDE	Les unités IDE désignent toutes les entreprises et institutions, qui reçoivent une IDE. Les entités IDE sont définies en vertu de l'article 3.c de la loi fédérale sur le numéro d'identification des entreprises.
Source fiable	N'importe quelle source d'information, qui est considérée comme digne de confiance pour une situation concrète.
Administrations	Administration désigne une collectivité publique (offices et autorités, le cas échéant organismes privés mandatés pour de telles tâches), qui s'acquittent de tâches de l'Etat qui lui sont confiées par la loi.

Annexe D - Modifications par rapport à la version précédente

La présente norme remplace la norme eCH-0170 v1.0. La version révisée inclut d'importants nouvelles constatations et concepts, en particulier provenant des normes NIST SP 800-63-3 [3], eIDAS ordonnance 910/2014 [1] et ISO/IEC 29115 [2]).

Ainsi les parties fondamentales du document eCH-0170 ont été retravaillées en profondeur dans la version 2.0. Les différences ont été élaborées dans un outil. On peut ainsi repérer les critères de la version 1.0 comparables à la version 2.0. La suite du document répertorie les modifications générales et renvoie aux contenus correspondant dans eCH-0170 version 1.0.

Fondamentalement:

- La structure des chapitres a été fondamentalement retravaillée et rapprochée de celle de eCH-171. Ainsi la représentation des modèles de qualité a-t-elle été harmonisée dans un souci d'améliorer la lisibilité.
- V1.0 reposait exclusivement sur les constatations du projet UE STORK. Celles-ci ont été prises en compte lors de l'élaboration du règlement eIDAS et le sont donc également dans cette norme.
- Outre le règlement eIDAS, ISO/IEC 29155 et NIST 800-63-3 ont également été pris en compte lors de l'élaboration de cette norme. La subdivision en modèles partiels en particulier y trouve ses origines.
- Outre la qualité de l'authentification des sujets physiques, V2.0 prend également en considération celle des sujets moraux.

Chapitre 2 Introduction [eCH-0170 v1.00 chapitre 1]

- L'introduction a été complètement retravaillée et repose sur le modèle de processus et d'information de eCH-107 [4]. Ces modèles ont été nettement étendus.

Chapitre 3 Terminologie [nouveau]

- La terminologie a été nettement étendue et retravaillée en se référant à eCH-107 [4], le glossaire correspondant se trouvant en Annexe C.2.

Chapitre 4 Modèle de qualité [eCH-0170 v1.00 chapitre 3]

- Le nouveau modèle de qualité se compose de niveaux de confiance et comporte 4 modèles partiels.

Chapitre 5, 6, 7 et 8 [eCH-0170 v1.00 chapitre 4]

- Ces chapitres décrivent les modèles partiels, les critères correspondants et leur composition par rapport aux niveaux de confiance.

Chapitre 9 Comparaison avec les normes internationales [nouveau]

- Dans ce chapitre, le modèle de qualité est mis en regard des normes internationales eIDAS, ISO/IEC 29115 et NIST 800-63-3.

Modifications de la version 2.0 à 2.01

Référence croisée manquante au chapitre 2.2, ajoutée.

Transfert vers la mise en page en cours.

Annexe E - Liste des illustrations

Figure 1: Classification de la norme de la norme eCH-0170	9
Figure 2: Modèle de processus Authentification d'un sujet.....	10
Figure 3: Architecture de l'information.....	13
Figure 4: Schéma de fonctionnement d'un moyen d'authentification.....	18
Figure 5: Modèle d'une Identity Federation	23
Figure 6: Définition du <i>sujet</i>	25
Figure 7: Composition du modèle de qualité	27
Figure 8: Vue d'ensemble de tous les critères.....	32
Figure 9: Critères pour le modèle de qualité de l'authentification	35
Figure 10: Critères pour le modèle de qualité de l'enregistrement.....	39
Figure 11: Facteurs relatifs au critère <i>Identification des personnes physiques</i>	47
Figure 12: Facteurs relatifs au critère <i>Identification des personnes morales</i>	49
Figure 13: Critères pour le modèle de qualité du pilotage	57
Figure 14: Critères pour le modèle de qualité de la fédération	61
Figure 15: Transmission par Front Channel	64
Figure 16: Transmission par Back Channel.....	65
Figure 17: Cartographie des processus	81
Figure 18: Processus <i>Authentifier le sujet</i>	81
Figure 19: Processus <i>Fédérer l'identité</i>	82
Figure 20: Processus <i>Enregistrer un sujet</i>	84
Figure 21: Processus <i>Piloter l'IAM</i>	87

Annexe F - Liste des tableaux

Tableau 1: Code de couleur dans le document.....	11
Tableau 2: Vue d'ensemble du caractère normatif des chapitres	16
Tableau 3: Exemples de moyen d'authentification et de Credential associé.....	19
Tableau 4: Parties du modèle de qualité et niveaux de confiance correspondants.....	27
Tableau 5: Niveaux de confiance du modèle de qualité pour l'authentification des sujets	30
Tableau 6: Composition des niveaux de confiance aux niveaux des modèles partiels	31
Tableau 7: Conditions préalables pour les Identity Federation Systems.....	34
Tableau 8: Niveaux de confiance de l'authentification (NDCA).....	35
Tableau 9: Modalités du critère <i>Moyen d'authentification</i>	37
Tableau 10: Modalités du critère <i>Certification du moyen d'authentification</i>	37
Tableau 11: Modalités du critère <i>réauthentification</i>	38
Tableau 12: Détermination du NDCE pour les personnes physiques	40
Tableau 13: Détermination du NDCE pour les personnes morales	40
Tableau 14: Modalités du facteur <i>Présence</i>	41
Tableau 15: Modalités du facteur <i>Justificatifs</i>	43
Tableau 16: Modalités facteur <i>Validation des renseignements</i>	45
Tableau 17: Modalités du facteur <i>Non-réputabilité</i>	46
Tableau 18: Modalités du facteur <i>Procuration</i>	47
Tableau 19: Modalités du critère <i>Identification des personnes physiques</i>	48
Tableau 20: Modalités du critère <i>Identification de personnes morales</i>	50
Tableau 21: Modalités du critère <i>Lien entre personne physique et morale</i>	50
Tableau 22: Modalités du critère <i>Transmission du moyen d'authentification</i>	53
Tableau 23: Modalités du critère <i>Prolongation/remplacement du moyen d'authentification</i> ..	56
Tableau 24: Détermination du niveau de confiance du pilotage (NDCP)	57
Tableau 25: Modalités du critère <i>Surveillance</i>	58
Tableau 26: Modalités du critère <i>Responsabilité</i>	59

Tableau 27: Modalités du critère <i>Maturité</i>	60
Tableau 28: Niveaux de confiance de la fédération (NDCF).....	61
Tableau 29: Modalités du critère Justificatif de détention de la confirmation d'authentification	62
Tableau 30: Modalités du critère <i>Authenticité de la confirmation d'authentification</i>	63
Tableau 31: Modalités du critère <i>Cryptage de la confirmation d'authentification</i>	64
Tableau 32: Modalités du critère <i>Forme de transmission de la confirmation d'authentification</i>	65
Tableau 33: Vue d'ensemble de la comparaison des niveaux de confiance	66
Tableau 34: Comparaison du modèle de qualité de l'authentification	66
Tableau 35: Comparaison du modèle de qualité de l'enregistrement des personnes physiques	67
Tableau 36: Comparaison du modèle de qualité de l'enregistrement des personnes morales	68
Tableau 37: Comparaison du modèle de qualité du pilotage	68
Tableau 38: Comparaison du modèle de qualité de la fédération	68
Tableau 39: Exigences relatives à la transmission de la confirmation d'authentification.....	84

Annexe G - Processus

Le processus d'authentification conditionne un grand nombre d'activités. Concernant l'évaluation de la qualité de l'authentification d'un sujet, la confirmation même mais aussi les processus associés à l'élaboration sont également pris en compte.

La Figure 17 montre les processus pour l'exécution, la définition et le pilotage d'une authentification. Seuls les processus pertinents pour le classement qualitatif de l'authentification sont pris en compte.

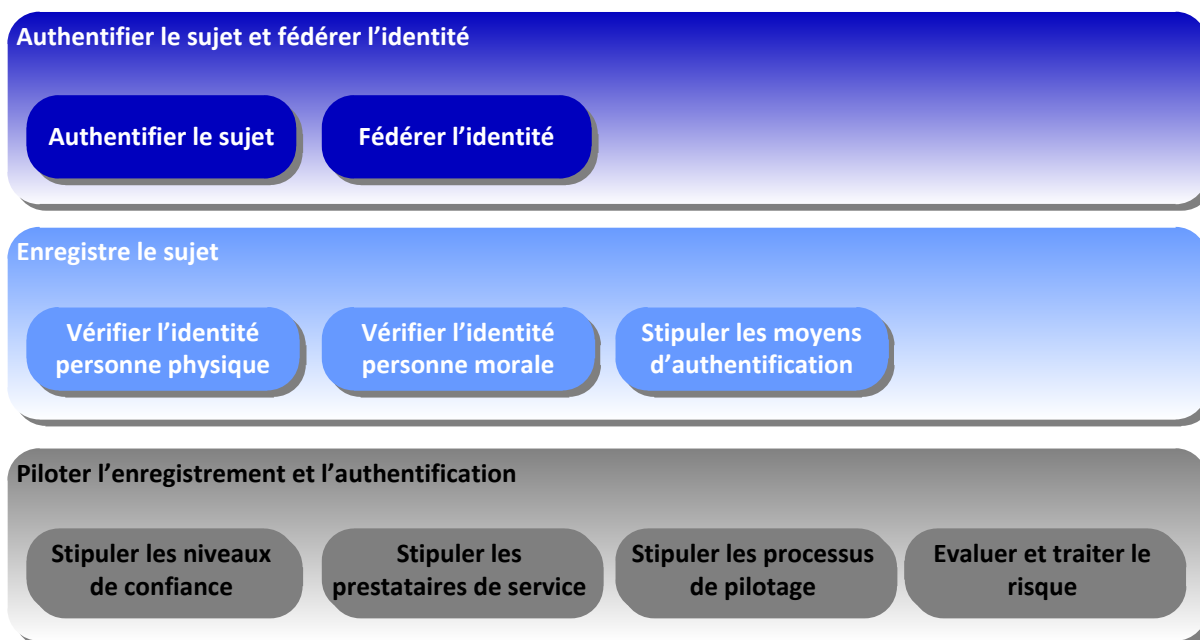


Figure 17: Cartographie des processus

G.1 Authentifier le sujet et fédérer l'identité

G.1.1 Authentifier le sujet

Le processus *Authentifier le sujet* permet de vérifier rapidement pour la période d'exécution l'E-Identity d'un sujet par un Identity Provider en ayant recours à un moyen d'authentification (voir Figure 18).

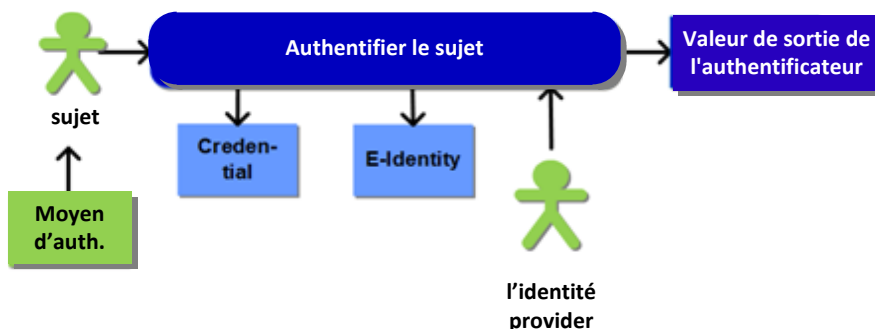


Figure 18: Processus *Authentifier le sujet*

Ce processus correspond à l'*Entity Authentication Phase* dans ISO 29115 [2], l'*Electronic Authentication Phase* (phase d'authentification électronique) dans STORK [6], la phase *Authentication* dans eIDAS [7] et la *Digital Authentication* dans NIST SP 800-63B [15].

Authentifier le sujet	Vérification de l'E-Identity déclarée d'un sujet par l'Identity Provider.
-----------------------	---

Activités:

- Le sujet utilise un moyen d'authentification qui est mis à sa disposition et dont il a le contrôle.
- Le moyen d'authentification génère, à l'aide d'un authentificateur, une valeur de sortie à partir des renseignements fournis par le sujet (secret et autres valeurs saisies facultatives).
- Le moyen d'authentification envoie la valeur de sortie générée à un IdP à des fins de vérification.
- L'IdP contrôle la valeur de sortie générée par le Credential de l'E-Identity déclarée. Si la vérification est positive, l'authentification est réussie.
- En fonction du niveau de sécurité exigé, le RP doit à nouveau faire authentifier le sujet au bout d'une durée déterminée (en fonction de ses propres directives) par l'IdP (réauthentification).

Critères de qualité:

- Chapitre 4.2.1 Moyen d'authentification
- Chapitre 4.2.2 Certification du moyen d'authentification
- Chapitre 4.2.3 Réauthentification

G.1.2 Fédérer l'identité

Concernant le processus *Fédérer l'identité*, une fois le sujet authentifié avec succès, le résultat est transféré pour la période d'exécution sous la forme d'une confirmation d'authentification par l'IdP au RP (voir Figure 19).

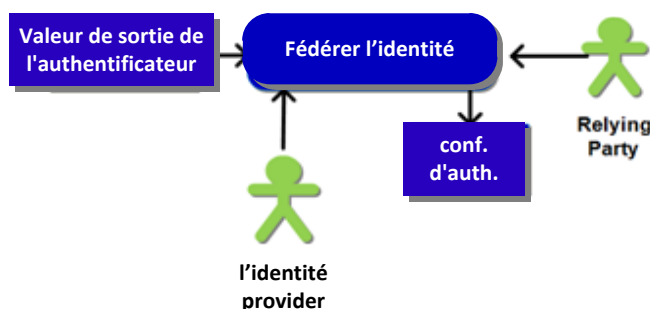


Figure 19: Processus *Fédérer l'identité*

Ce processus n'est pas mentionné de façon explicite dans ISO 29115 [2], dans STORK [6] et dans eIDAS [7]. Il correspond au *Federation Process* dans NIST SP 800-63C [18].

Fédérer l'identité	Transmission d'une confirmation d'authentification de l'IdP au RP
--------------------	---

Activités:

- L'IdP vérifie si le RP est autorisé à demander une confirmation d'authentification.
- (facultatif) l'IdP obtient le consentement du sujet pour la transmission de la confirmation d'authentification au service requérant (RP).
- L'IdP génère la confirmation d'authentification avec estampille temporelle, signature et cryptage facultatif.
- L'IdP transfère la confirmation d'authentification au RP.
- Le RP vérifie l'actualité et l'authenticité de la confirmation d'authentification.

Le tableau suivant présente les principales exigences de sécurité permettant de mesurer si les critères sont pertinents dans le contexte de la transmission d'une confirmation d'authentification.

Exigence	Description	Moyen	Critères
Origine et intégrité sécurisées d'une confirmation d'authentification	Un RP peut vérifier si une confirmation d'authentification a été délivrée par un IdP digne de confiance et si celle-ci a été entretemps manipulée sous quelque forme que ce soit.	Signature numérique d'importantes informations par l'émetteur, qu'une partie de confiance (RP) peut vérifier à la réception d'une confirmation d'authentification.	Authenticité de la confirmation d'authentification
Confidentialité de la confirmation d'authentification transférée et des informations d'identité	Les informations d'authentification et d'identité à transmettre doivent être protégées contre tout accès par des tiers non autorisés.	Par des moyens cryptographiques ou par la sélection d'une connexion directe et sécurisée de communication.	Protection de la confidentialité de la confirmation d'authentification Forme de transmission de la confirmation d'authentification

Exigence	Description	Moyen	Critères
Vérification du lien des abonnés à la confirmation d'authentification	Un RP doit avoir la possibilité de contrôler si une confirmation d'authentification remise a été délivrée pour l'abonné par l'IdP et ainsi que le porteur est également l'abonné.	Lien cryptographique d'une confirmation d'authentification à un secret, que connaît uniquement le sujet préalablement authentifié (abonné) en tant que porteur légitime.	Justificatif de détention de la confirmation d'authentification

Tableau 39: Exigences relatives à la transmission de la confirmation d'authentification.

Critères de qualité:

- Chapitre 7.2.1 Justificatif de détention de la confirmation d'authentification
- Chapitre 7.2.2 Authenticité de la confirmation d'authentification
- Chapitre 7.2.3 Protection de la confidentialité de la confirmation d'authentification
- Chapitre 7.2.4 Forme de transmission de la confirmation d'authentification

G.2 Enregistrer un sujet

Le processus *Enregistrer un sujet* couvre toutes les activités de vérification de l'identité d'un sujet et l'attribution ou le classement du moyen d'authentification pour une E-Identity (voir Figure 20). Le processus se compose de 2 sous-processus: le processus *Vérifier l'identité* pour lequel on établit une distinction entre la vérification personnes physiques et morales, et le processus *Stipuler le moyen d'authentification*, qui ne commence qu'une fois le processus *Vérifier l'identité* achevé avec succès.

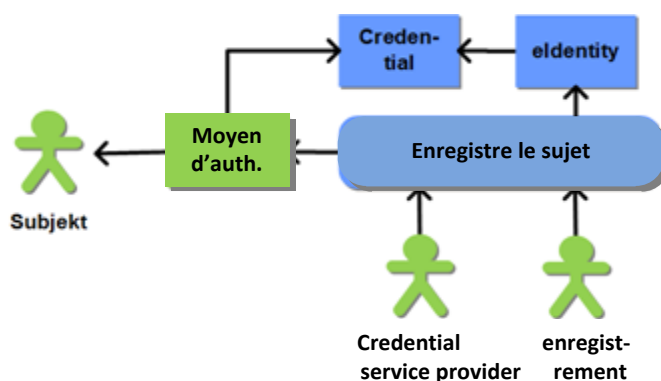


Figure 20: Processus *Enregistrer un sujet*

G.2.1 Vérifier l'identité de la personne physique

Ce processus correspond à la phase *Vérification et justificatif d'identité (personne physique)* dans eIDAS [7], chap. 2.1.2.

Vérifier identité personne physique	Vérification de l'existence du sujet, constatation de l'identité et validation sur la base de justificatifs par la RA
-------------------------------------	---

Activités:

- La RA recueille les données personnelles requises et examine le cas échéant les justificatifs.
- (facultatif) La RA valide les données collectées en les comparant aux renseignements figurant dans les justificatifs.
- (facultatif) La RA prend les données d'adresse dans un justificatif approprié et les contrôle.
- (facultatif) La présence du sujet pendant le dépôt de la demande fait l'objet d'une consignation par écrit.

Critères de qualité:

- Chapitre 5.2.2 Identification des personnes physiques.

G.2.2 Vérifier l'identité d'une personne morale

Ce processus correspond à la phase *Justificatif et vérification d'identité (personne morale)* et *Association de moyens d'identification électroniques de personnes physiques et morales* dans eIDAS [7], chap. 2.1.3 et chap. 2.1.4.

Vérifier l'identité personne morale	Vérification de l'existence du sujet, constatation de l'identité et validation sur la base des justificatifs par la RA, lien entre la personne physique et la personne morale
-------------------------------------	---

Activités:

- La RA vérifie l'identité de la personne physique (voir chapitre G.2.1)
- La RA collecte les données nécessaires pour la personne morale et examine le cas échéant les justificatifs.²²
- (facultatif) La RA valide les données collectées en les comparant aux renseignements figurant dans les justificatifs.
- (facultatif) La RA vérifie le lien entre la personne physique et morale en comparant avec les justificatifs.

²² Si plusieurs personnes physiques sont associées à une personne morale, l'identification de la personne morale ne doit pas être répétée dans chacun des cas.

Critères de qualité:

- Chapitre 5.2.2 Identification des personnes physiques
- Chapitre 5.2.3 Identification des personnes morales
- Chapitre 5.2.4 Lien entre personne physique et morale

G.2.3 Stipuler le moyen d'authentification

Ce processus correspond aux phases *Délivrance, livraison et activation* ainsi que *Prolongation et remplacement* dans eIDAS [7], chap. 2.2.2 et chap. 2.2.4. Ce processus ne démarre qu'une fois le processus *Vérifier l'identité* achevé avec succès.

Stipuler le moyen d'authentification	Le CSP fait délivrer par la RA un moyen d'authentification sur la base de la vérification d'identité et le transmet au sujet.
--------------------------------------	---

Activités:

- Le CSP délivre le moyen d'authentification ou associe un moyen d'authentification existant à l'E-Identity du sujet.
- (facultatif) Le CSP transmet le moyen d'authentification au sujet. Cette activité est omise lorsque:
 - le sujet détermine lui-même le moyen d'authentification (ex. mot de passe),
 - le moyen d'authentification est délivré par un tiers et transmis au sujet,
 - le CSP associe un moyen d'authentification à l'E-Identity du sujet, que ce dernier détient ou contrôle déjà.
- (facultatif) Le sujet active le moyen d'authentification dans un processus d'activation.
- (facultatif) Le sujet peut en demander un nouveau auprès du CSP avant l'expiration de la validité du moyen d'authentification.

Critères de qualité:

- (facultatif) Chapitre 5.2.5 Transmission du moyen d'authentification
- Chapitre 5.2.6 Prolongation/remplacement du moyen d'authentification

G.3 Piloter l’IAM

Le processus *Piloter l’IAM* contient les fonctions Management, Governance, Risk et Compliance dans le contexte de l’authentification des sujets (voir Figure 21).

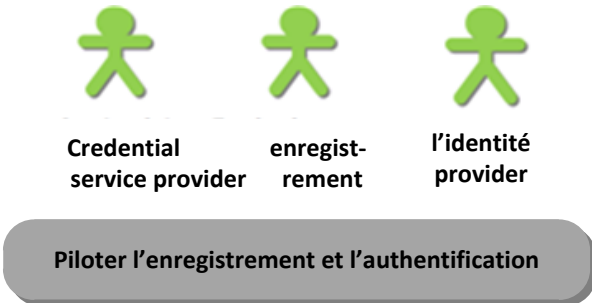


Figure 21: Processus *Piloter l’IAM*

G.3.1 Stipuler les niveaux de confiance

Stipuler les niveaux de confiance	Stipuler comment la qualité de l’authentification peut être vérifiée et comparée.
-----------------------------------	---

Activités:

- Stipuler les critères de qualité pour le modèle de qualité.
- Définir le modèle de qualité pour l’authentification des sujets et dont la subdivision en niveaux de confiance.
- Stipuler comment les niveaux de confiance peuvent être transmis entre l’IdP et le RP.

Remarque:

- La norme eCH-0170 définit tant les critères de qualité qu’un modèle de qualité avec ses niveaux de confiance. La norme sert ainsi de base à ce processus.

Critères de qualité:

- Aucun

G.3.2 Stipuler les prestataires de service

Stipuler les prestataires de service	Stipuler les prestataires IAM du système IAM et structure des relations de confiance entre ceux-ci
--------------------------------------	--

Activités:

- Stipulation de l'organisation (Stakeholders) et des relations en ceux-ci (coopération)
- Définition des relations de confiance entre les Stakeholders
- Mise à jour et échange des métadonnées

Critères de qualité:

- Chapitre 6.2.1 Surveillance
- Chapitre 6.2.2 Responsabilité

G.3.3 Stipuler les processus de pilotage

Stipuler les processus de pilotage	Définition de la traçabilité de tous les processus. Stipuler les processus et les règles pour l'authentification processus complétés (révocation, remplacement etc.)
------------------------------------	---

Activités:

- Définition de la traçabilité de l'ensemble des processus (dépôt des documents pertinents par exemple) et de leur audit.
- Stipuler les délais de conservation des données pertinentes pour chaque étape du processus (voir également ISO 29115 [2] chapitre «Record-keeping/recording»)
- Stipulation des processus et règles pour la révocation/déprovisionnement des moyens d'authentification
- Stipulation des processus et règles pour le remplacement des moyens d'authentification
- Stipulation de la disponibilité (Service Level Agreements) des différents prestataires de service
- Stipulation du cycle de vie d'un lien entre personnes physiques et morales (ex. activation, suspension, renouvellement, dénonciation) (voir également eIDAS 2015/1502 [7], section 2.1.4)
- Stipulation du modèle de maturité et niveaux de maturité

Remarque:

- La norme eCH-0172 [22] définit les niveaux de maturité IAM notamment pour le classement par la maturité des processus du pilotage et est complétée par un document auxiliaire avec des questions concrètes afin de déterminer cette maturité. D'autres modèles de maturité pourraient également être pris en considération, mais ils sont plutôt génériques, comme CMMI for Services v1.3 et l'évaluation SCAMPI pour ce modèle par exemple.

Critères de qualité:

- Chapitre 6.2.1 Surveillance
- Chapitre 6.2.3 Maturité

G.3.4 Evaluer et gérer les risques

Evaluer et gérer les risques	Définition des opérations de traitement des risques (estimation et adressage des risques)
------------------------------	---

Activités selon eCH-0107 [4], chap.6.3.2:

- Analyse du besoin de protection: l'analyse du besoin de protection garantit des exigences adaptées en matière de sécurité (autant de sécurité que nécessaire, pas autant que possible).
- Exécution et consignation de l'analyse des risques.
- Elaboration d'un concept de protection des données et de l'information.
- Amélioration continue du concept de sécurité: définie dans la norme ISO 27001. En raison de la situation actuelle, des mesures sont planifiées, mises en œuvre, contrôlées et optimisées de façon périodique. Ce processus d'amélioration est une procédure efficace, qui a fait ses preuves et est aujourd'hui devenue un élément essentiel des Best Practice.
- [FACULTATIF] Gestion des risques basée sur un système de gestion de la sécurité des informations (ISMS) selon ISO 27001.
- [FACULTATIF] Gestion des risques basée sur un Framework comme COBIT.

Critères de qualité:

- Chapitre 6.2.2 Responsabilité
- Chapitre 6.2.3 Maturité

Annexe H - Exigences relatives aux moyens d'authentification

Cette annexe décrit, de manière succincte, les moyens d'authentification les plus courants.

Chacun de ces moyens d'authentification doit remplir certaines exigences afin de satisfaire aux critères des niveaux de confiance. La présente norme ne comporte pas de définition de ces exigences, se reporter aux normes et recommandations courantes.

De plus amples renseignements tels les moyens d'authentification pouvant utilisés sont disponibles dans NIST SP 800-63B [15] chapitre 10.2.

H.1 Memorized Secrets

Type: Single-Factor Authenticator

Synonyme: secrets enregistrés

Les *Memorized Secrets*, généralement appelés mots de passe ou PIN, sont des valeurs gardées secrètes, qui sont le plus souvent sélectionnées par l'utilisateur et enregistrées dans sa mémoire ou dans un autre lieu de stockage sûr. Elles doivent être suffisamment complexes et aléatoires afin de ne pas pouvoir être devinées par un assaillant ou calculées d'une autre manière. Les *Password Policies* stipulent les règles relatives à la longueur, la complexité, le mix de caractères, la durée avant expiration et la réutilisation et définit ainsi la force des Memorized Secrets.

Exemples: mot de passe ou PIN

Les exigences sont décrites dans le détail dans les sources suivantes:

- Voir également NIST SP 800-63B [15], chapitre 5.1.1 et Appendice A.

H.2 Look-Up Secrets

Type: Single-Factor Authenticator

Synonyme: secret consultable

Les *Look-Up Secrets* contiennent une liste de valeurs (alpha)numériques, qui ont été échangées auparavant entre le sujet et le Credential Service Provider (CSP). Pour l'authentification, l'utilisateur doit indiquer une valeur particulière figurant dans cette liste.

Les valeurs échangées doivent être générées de manière aléatoire. Elles ne doivent être utilisées qu'une seule fois et posséder une entropie suffisamment élevée.

Exemples: listes de décompte (engl. *tally sheet*) ou blocs TAN

Les exigences sont décrites dans le détail dans les sources suivantes:

- Voir également NIST SP 800-63B [15], chapitre 5.1.2.

H.3 Out of Band Authenticators

Type: Single-Factor Authenticator

Synonyme: canal externe

Out of Band est un appareil physique avec une adresse unique, capable de recevoir les secrets sélectionnés par le CSP, pour une seule utilisation.

L'appareil est détenu par le sujet et devrait pouvoir être contacté via un canal privé propre, qui est utilisé indépendamment du canal primaire pour le deuxième facteur d'authentification.

L'Out of Band Authenticator peut fonctionner selon 2 modes distincts:

1. Le sujet présente au service authentifiant via le canal de communication principal, le secret qu'il a reçu via le deuxième canal.
2. Le sujet renvoie directement au service authentifiant une réponse via le deuxième canal de communication.

Exemples: téléphone portable/Smartphone avec numéro de portable et procédure SMS-TAN

Les exigences sont décrites dans le détail dans les sources suivantes:

- Voir également NIST SP 800-63B [15], chapitre 5.1.3.

H.4 OTP Devices

Type: en fonction de l'implémentation: Single-Factor Authenticator ou (hardware based) Multi-Factor Authenticator

Synonyme: générateur de mot de passe à usage unique

Un Single-Factor OTP Device est un logiciel ou un appareil, qui génère spontanément un mot de passe à usage unique selon un algorithme spécifique (par événement, sur une base temporelle). L'appareil ou l'application contient un secret intégré (clé), qui est utilisé une fois pour la génération du mot de passe utilisé. L'heure actuelle ou un compteur incrémental peuvent servir de valeur de saisie.

Exemples: SecureID-Token, Google Authenticator, SafeNet mobilePass

Pour activer l'algorithme, le Multi-Factor OTP Device a besoin d'un deuxième facteur (connaissances ou détention) sur l'appareil. Ce deuxième facteur d'authentification peut être un Keypad intégré, un capteur biométrique (ex. empreintes digitales) ou une interface informatique directe (ex. USB).

Exemples: SecureID-Token avec Keypad, HID ActivID Token

Les exigences sont décrites dans le détail dans les sources suivantes:

- Voir également NIST SP 800-63B [15], chapitre 5.1.4 (single-factor) et 5.1.5 (multi-factor).

H.5 Single Factor Cryptographic Devices

Type: Single-Factor Authenticator

Synonyme: appareils de cryptage à facteur unique

Un *single-factor cryptographic device* est un appareil physique, qui effectue des calculs cryptographiques au moyen d'une saisie fournie à l'appareil. L'appareil n'a besoin pour cela d'aucune activation via un second facteur d'authentification. Pour générer la valeur de sortie, l'appareil utilise une clé symétrique ou asymétrique stockée dans sa mémoire. L'authentification est accomplie par le justificatif de détention de l'appareil.

Un *single-factor cryptographic device* contient également des logiciels intégrés. Le Credential Service Provider (CSP) est compétent pour ces derniers et contrôle le mode de fonctionnement des logiciels.

Exemple: Yubikey U2F

Les exigences sont décrites dans le détail dans les sources suivantes:

- Voir également NIST SP 800-63B [15], chapitre 5.1.6.

H.6 Multi-Factor Cryptographic Software

Type: Multi-Factor Authenticator

Synonyme: logiciel de cryptage multifacteurs

Un *multi-factor software cryptographic authenticator* est une clé cryptographique, qui est enregistrée sur un disque dur ou un support de données semblable. Un tel Authenticator doit être activé au moyen d'un deuxième facteur d'authentification. L'authentification est accomplie par le justificatif de détention et le contrôle de la clé cryptographique. Cet Authenticator combine 2 facteurs d'authentification: détention (clé cryptographique) avec un autre secret (détention ou détention), qui est utilisé pour l'activation.

Exemple: Soft-Token (fichier PKCS#12)

Les exigences sont décrites dans le détail dans les sources suivantes:

- Voir également NIST SP 800-63B [15], chapitre 5.1.7.

H.7 Multi-Factor Cryptographic Devices

Type: hardware based Multi-Factor Authenticator

Synonyme: appareils de cryptage multifacteurs

Un *multi-factor cryptographic device* est un appareil physique, qui contient une clé cryptographique protégée. Il doit être activé au moyen d'un deuxième facteur d'authentification (connaissances ou détention). L'authentification est accomplie par le justificatif de détention et le contrôle de la clé cryptographique.

Un *multi-factor cryptographic device* contient également des logiciels intégrés. Le Credential Service Provider (CSP) est compétent pour ces derniers et contrôle le mode de fonctionnement des logiciels.

Exemples: SmartCard, SuisseID

Les exigences sont décrites dans le détail dans les sources suivantes:

- Voir également NIST SP 800-63B [15], chapitre 5.1.8.

Annexe I - Exigences relatives au facteur Validation des renseignements

Cette annexe répertorie les exigences supplémentaires relatives au facteur *Validation des renseignements*. Pour des exigences plus détaillées, se reporter aux normes et recommandations habituelles.

Divers facteurs influent sur la qualité de la validation. Il s'agit notamment de:

- Niveau de formation des vérificateurs,
- Disponibilité de documents falsifiés,
- Complexité du cadre juridique lors de l'utilisation de types de documents les plus divers,
- Utilisation d'appareils pour la vérification automatisée de documents, ex. pour les passeports ou cartes d'identité électroniques,

Les exigences détaillées sont décrites dans les sources suivantes:

- NIST Measuring Strength of Identity Proofing [24], chapitre 3.1
- NIST 800-63A [16], chapitre 5.4.3 détaille les exigences relatives à la vérification en cas de présence *virtual-in-person*.
- eIDAS 2015/1502 [7] définit au chapitre 2.4.5 les exigences relatives aux institutions et au personnel, en vigueur pour tous les niveaux de sécurité