eCH-0224 – Modèles d'architecture Identity Federation impliquant un Broker

Nom	Modèles d'architecture Identity Federation impliquant un Broker
eCH-nombre	eCH-0224
Catégorie	Norme
Stade	Défini
Version	1.0
Statut	Approuvé
Date de décision	2020-06-04
Date de publication	2020-07-29
Remplace la version	-
Condition préalable	eCH-0107 V3.0, eCH-0170 V2.0, eCH-0219 V1.0
Annexes	-
Langues	Allemand (original), français (traduction)
Auteurs	Groupe spécialisé IAM Annett Laube-Rosenpflanzer, BFH TI, annett.laube@bfh.ch Marc Kunz, BFH TI, marc.kunz@bfh.ch Gerhard Hassenstein, BFH TI, gerhard.hassenstein@bfh.ch Bojan Leimer, BFH TI, bojan.leimer@bfh.ch
Editeur / distribution	Association eCH, Mainaustrasse 30, case postale, 8034 Zurich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Condensé

Cette norme définit les modèles d'architecture basés sur un Broker pour les systèmes d'Identity Federation en cyberadministration. Les divers cas d'utilisation et les scénarii G2C, G2G et G2B servent à illustrer la manière dont le choix d'un modèle d'Identity Federation est dicté par les différentes exigences en matière de protection de la vie privée et de confidentialité en particulier. Les modèles de Broker possibles sont présentées en détail mais indépendamment des considérations technologiques.

Sommaire

Condensé 1
Remarque 3
1 Statut 4
2 Introduction 4
2.1 But du document 4
2.2 Classification 5
2.3 Champ d'application 5
2.4 Groupe cible 6
2.5 Délimitation 6
2.6 Caractère normatif des chapitres 7
3 Vue d'ensemble de l'Identity Federation 8
3.1 Confiance 10
3.2 Confidentialité 10
3.3 Session Handling 11
3.3.1 Single Sign-on (SSO) 12
3.3.2 Single Logout (SLO) 12
4 4 Scénarii dans la cyberadministration 13
4.1 Government to Citizen (G2C) 13
4.2 Government to Government (G2G) 13
4.3 Government to Business (G2B) 14
5 Cas d'application 14
5.1 Authentification pure 14
5.1.1 E-Identities indépendantes 15
5.1.2 E-Identities reliées 15
5.2 Authentification avec transmission d'attributs 15
5.2.1 Durée de vie des valeurs d'attribut 15
5.2.2 Nombre de sources 16
5.2.3 Provenance des données 16
5.2.4 Qualité des attributs 16
5.3 Identificateurs techniques utilisés dans les cas d'application 16
5.3.1 Identificateur réparti (Distributed ID) 17
5.3.2 Identificateur technique lié au Relying Party (Persistent ID) 17
5.3.3 Identificateur technique aléatoire unique (Transient ID) 17
6 Exigences 18
6.1 Exigences imposées au système IAM fédéré 18
6.2 Exigences du Stakeholder: bénéficiaire de prestations 19
6.3 Exigences du Stakeholder: Fournisseur de prestations 21
6.4 Exigences du Stakeholder: direction 23
7 Sélection du modèle d'Identity Federation 24
7.1 Influence des exigences 24
7.2 Influence des scénarii 26
7.3 Systèmes n'impliquant pas de Broker 27

7.4 Broker Double Blinding 28
7.5 Sources ouvertes Broker 30
7.6 Protection de la confidentialité Broker 31
8 Modèles de Broker 33
8.1 Notions de base concernant les modèles de Broker 33
8.1.1 Sections de protocole 33
8.1.2 Session Handling 37
8.1.3 Processus 38
8.2 Broker Double Blinding 41
8.2.1 Affectation des processus 42
8.3 Sources ouvertes Broker 43
8.3.1 Affectation des processus 43
8.4 Protection de la confidentialité Broker 44
8.4.1 Affectation des processus 45
9 Application de la norme eCH-0170 aux Identity Federations impliquant un Broker 47
9.1 Niveau de confiance de l'authentification (NDCA) 47
9.2 Niveau de confiance de l'enregistrement (NCDE) 47
9.3 Niveau de confiance du pilotage (NCDP) 47
9.4 Niveau de confiance de la fédération (NDCF) 47
10 Exclusion de responsabilité - droits de tiers 49
11 Droits d'auteur 49
Annexe A – Références & bibliographie 50
Annexe B – Collaboration & vérification 51
Annexe C – Abréviations et glossaire 51
Annexe E – Liste des illustrations 52
Annexe F – Liste des tableaux 52
Annexe G – Modèles de Tokenbased Identity Federation impliquant un Broker 53

Remarque

En vue d'une meilleure lisibilité et compréhension, seul le genre masculin est utilisé pour la désignation des personnes dans le présent document. Cette formulation s'applique également aux femmes dans leurs fonctions respectives.

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.

2 Introduction

Une Identity Federation en cyberadministration permet aux autorités de mettre leurs prestations à la disposition – en ligne – des collaborateurs d'autres autorités et des citoyens ainsi que des organisations et entreprises de leur pays (voir glossaire IAM [1] 2.62). Les autorités délèguent alors l'authentification et la confirmation d'attributs à différents prestataires de services IAM. Cette délégation repose sur une confiance mutuelle, elle-même basée sur des accords juridiques, organisationnels/architecturaux et techniques

Une Identity Federation est constituée de ses participants (Relying Parties et prestataires de services IAM, tels qu'IdP, AP et Broker), qui forment ensemble une communauté avec un IAM Management et un IAM Steering communs. Les Relying Parties utilisent les services IAM proposés par les prestataires de services IAM. Au moment de l'exécution, les processus «Authentifier le sujet» et «Compléter et confirmer l'E-Identity» sont généralement pris en charge par les prestataires de services IAM. L'autorisation du sujet pour accéder à une ressource (processus «Autoriser l'accès») relève de la seule compétence des Relying Parties et ne peut être déléguée aux prestataires de services IAM.

2.1 But du document

Ce document vient concrétiser les principes de conception généraux d'un système IAM (eCH-0107 [2]) et définit les modèles d'architecture pour les Identity Federations, qui satisfont au mieux aux exigences actuelles en matière de cyberadministration.

A cette fin, les scénarii envisagés (voir chapitre 4) et les cas d'application (voir chapitre 5) sont circonscrits en fonction de leur pertinence, les exigences générales stipulées par eCH-0107 [2] sont mises en œuvre et complétées par les exigences relatives à la protection de la sphère privée des sujets (voir chapitre 6).

Des exigences plus strictes permettent de limiter le volume à quelques modèles d'Identity Federation seulement et d'établir des critères de sélection (chapitre 7).
Le choix de modèles impliquant un Broker (intermédiaire) constitue le meilleur moyen de remplir les obligations imposées.

Ces modèles de Broker sont décrits en détail dans la suite du document afin d'établir un cadre architectural et technique pour une éventuelle implémentation.

Le dernier chapitre traite de l'application du modèle de qualité à des fins d'authentification des sujets (eCH-0170 [3]).

2.2 Classification

La norme eCH-0107 [2] regroupe les concepts et documents auxiliaires complémentaires relatifs aux solutions IAM fédérées. Les concepts sont des descriptions concrètes, de ce à quoi ressemble une proposition de solution IAM, et comportent des concepts partiels et des architectures devant être pris en compte pour la mise en œuvre. Ces concepts sont étayés par des documents auxiliaires, qui fournissent des informations complémentaires et sont pertinents pour plus d'un concept. Les modèles de qualité et de maturité représentés sont des exemples de document auxiliaire sans être exhaustifs.

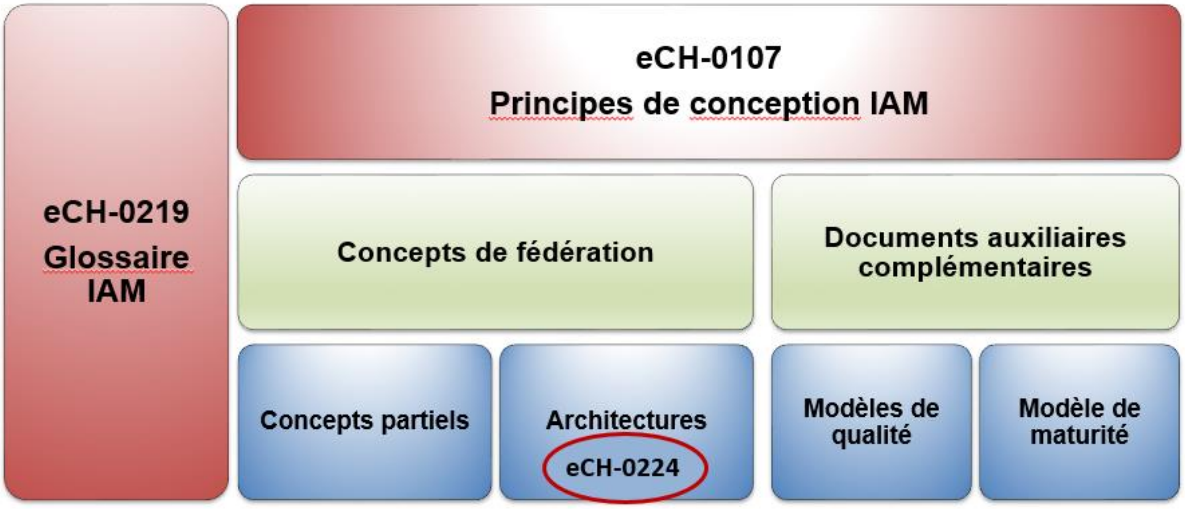

Figure:1 Classification de la norme eCH-0224

La présente norme eCH-0224 décrit les modèles d'architecture pour l'Identity Federation impliquant un Broker. L'architecture STIAM décrite dans la norme eCH-0168 [4] est ainsi complétée d'autres architectures qui sont mises en relation entre elles.
Il est en outre fait référence à la norme eCH-0170 [3] qui définit le modèle de qualité pour l'authentification des sujets.
La terminologie propre à cette norme est expliquée et définie par la norme eCH-0219 [1].

2.3 Champ d'application

Le document décrit les exigences, l'architecture et les directives d'implémentation des systèmes d'Identity Federation impliquant un Broker dans la cyberadministration. Les systèmes d'Identity Federation sont abordés principalement dans les contextes interorganisations. A cet égard, l'utilisation de ces mêmes systèmes au sein d'une organisation est simplement recommandée.

Le document décrit les exigences, les architectures et les directives en priorité pour les nouveaux systèmes. Il peut toutefois être également utilisé pour les systèmes IAM existants.

La description dans cette norme est faite sans considération technologique, d'autres normes se chargeant de l'appliquer à des technologies concrètes.

La norme permet, à l'aide de différents critères de sélection, d'opter pour l'un des modèles impliquant un Broker aujourd'hui utilisables en cyberadministration. Les directives relatives à l'implémentation de ce modèle laissent toutefois une marge de manœuvre, qui est susceptible d'être encore réduite lors de l'implémentation.

2.4 Groupe cible

Ce document conceptuel s'adresse principalement:

- aux architectes d'affaires qui spécifient et conçoivent les systèmes d'Identity Federation,
- aux architectes logiciels qui conseillent leurs clients lors de la conception et la réalisation d'un système d'Identity Federation
- aux responsables de la protection des données, qui veulent étendre les systèmes d'Identity Federation à la confidentialité et à la protection de la sphère privée,
- à ceux/celles que l'IAM intéresse et qui disposent de connaissances techniques.

2.5 Délimitation

Les modèles d'Identity Federation présentés dans ces pages reposent principalement sur les exigences de la cyberadministration. Ils peuvent cependant être appliqués à d'autres domaines.

Trois scénarii (voir chapitre 4) avec plusieurs cas d'utilisation (voir chapitre 5) peuvent être identifiés pour les systèmes d'Identity Federation dans la cyberadministration. Seuls ces scénarii et cas d'application sont pris en compte dans la présente norme. Ainsi, la transmission de données, documents ou signatures électroniques, par exemple, n'est pas traitée.

Des personnes physiques agissent pour le compte de sociétés (personnes morales). Les processus et la mise en œuvre technique de la manière, dont les droits sont transférés à une personne physique, ne sont pas traités dans cette norme.

La norme décrit des modèles d'Identity Federations dans lesquels les participants communiquent entre eux à l'aide d'un Broker central. Les modèles dans lesquels plusieurs Brokers ou systèmes d'Identity Federation sont en relation à des fins de communication (on parle alors de modèles d'interfédération) ne sont pas pris en compte. De même, l'intégration au sein d'Identity Frameworks internationaux, tels que STORK [5] et eIDAS [6], n'est pas abordée.

L'utilisation du Holder of Key (HoK) est brièvement évoquée dans la présente norme. Celle-ci étant peu répandue et les conditions imposant un tel HoK étant relativement rares, aucune spécification détaillée n'est donnée. La norme définit les procédures compatibles avec un niveau de confiance allant jusqu'à VS3 selon eCH-0170 [3] (resp. FAL 2 selon NIST 800-63C [7]).

La présente norme ne décrit que succinctement le Session Handling, dont la mise en œuvre, fortement tributaire de la technologie, n'entre dans le cadre de la norme.

Plusieurs services sont reliés en entre eux dans les architectures de service (SOA et Microservices) et les E-Identities des sujets doivent être transmis (délégation). La délégation de confirmations d'authentification et d'attributs n'est pas considérée dans cette norme.

Dans le cas où un système IAM est mis en œuvre conformément à la LSIE [8], les dispositions légales, ainsi que leurs ordonnances et dispositions d'application, doivent être respectées avant que les directives définies dans les normes eCH puissent être appliquées. En cas de conflit, la LSIE [8] prime.

2.6 Caractère normatif des chapitres

Les chapitres de la présente norme sont de nature soit normative soit descriptive. Le tableau suivant définit la classification des chapitres.

Chapitre	Description
2 Introduction	**Descriptif**
3 Vue d'ensemble Identity Federation	**Descriptif**
4 Scénarii cyberadministration	**Normatif**
5 Cas d'utilisation	**Normatif**
6 Exigences	**Normatif**
7 Sélection du modèle d'Identity Federation	**Normatif**
8 Modèles de Broker	**Normatif**
9 Application de la norme eCH-0170 aux Identity Federations impliquant un Broker	**Descriptif**

Les annexes A et C sont également normatives. Toutes les autres annexes de cette norme sont descriptives.

3 Vue d'ensemble de l'Identity Federation

Contrairement aux solutions IAM isolées, incluant des identités indépendantes les unes des autres, dans une fédération d'identités, une application délègue certains des services (l'identification et l'authentification d'un sujet par exemple) à des instances spécialisées (acteurs). Une Identity Federation regroupe des participants impliqués qui constituent une communauté (métadomaines) (voir Figure 4 dans eCH-0107 [2]). Cette communauté disposer d'un IAM Management (direction) et d'un IAM Steering (pilotage) commun, s'accordant sur des sur des exigences et directives communes (IAM-Policy)[1]. Les activités d'administration de l'IAM-Policy sont décrites en détail dans la norme eCH-0107 [2] pour le processus «Administration de l'IAM-Policy» (chapitre 6.4.1).

On peut distinguer entre une Identity Federation directe et une Identity Federation impliquant un Broker. Dans le cas d'une Identity Federation directe (ou simple), un Identity Provider (ou un ensemble d'IdP similaires) associé à divers fournisseurs d'applications constituent une communauté en convenant de règles et d'exigences communes (règles d'identification, niveaux d'authentification, attributs à concilier, etc.) Ce type d'Identity Federation forme une communauté fermée. Tout fournisseur d'applications reste libre de prendre part à plusieurs communautés (facebook, Google, twitter, etc.) en qualité de participant, chaque utilisateur se prévalant toutefois d'une identité indépendante au sein de chaque communauté. Une telle pratique est aujourd'hui courante sur les réseaux sociaux, comme en atteste l'exemple qui suit.

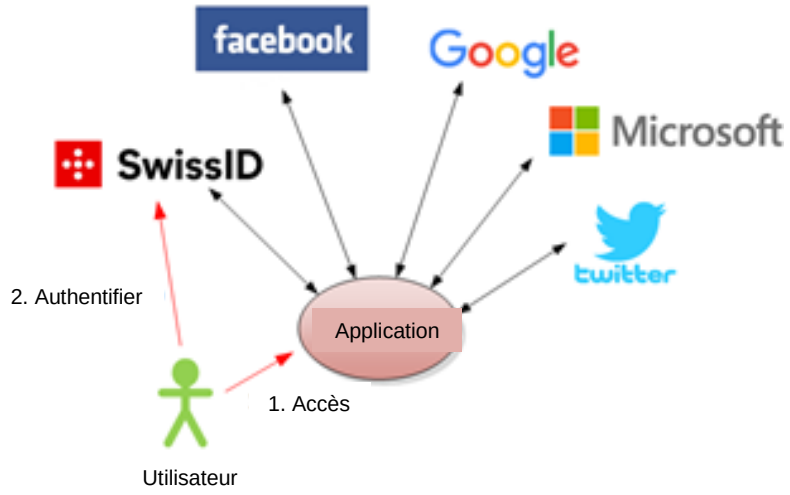

Figure 2: Identity Federation simple (directe)

Une Identity Federation impliquant un Broker fournit généralement ses prestations à plusieurs communautés. Les services du Broker reposent sur un corps de règles qui sont contraignantes pour toutes les communautés affiliées et s'appliquent également au Broker. Toute sous-communauté peut se doter de directives plus spécifiques et plus strictes, sous réserve toutefois que celles-ci n'enfreignent pas les directives générales applicables à l'ensemble des communautés.
Une Identity Federation impliquant un Broker déleste les applications et les Identity Providers de certaines tâches et charges et facilite la participation à une communauté, puisqu'aussi bien fournisseurs que consommateurs d'identité peuvent limiter leur communication à un partenaire unique (le Broker), même si utilisateur ait aussi la possibilité de s'authentifier auprès

[1] Un même participant peut aussi figurer dans plusieurs sous-communautés.

de plusieurs IdP. Pour plus de renseignements concernant les avantages et les inconvénients des systèmes d'Identity Federation, se reporter au chapitre 7 .

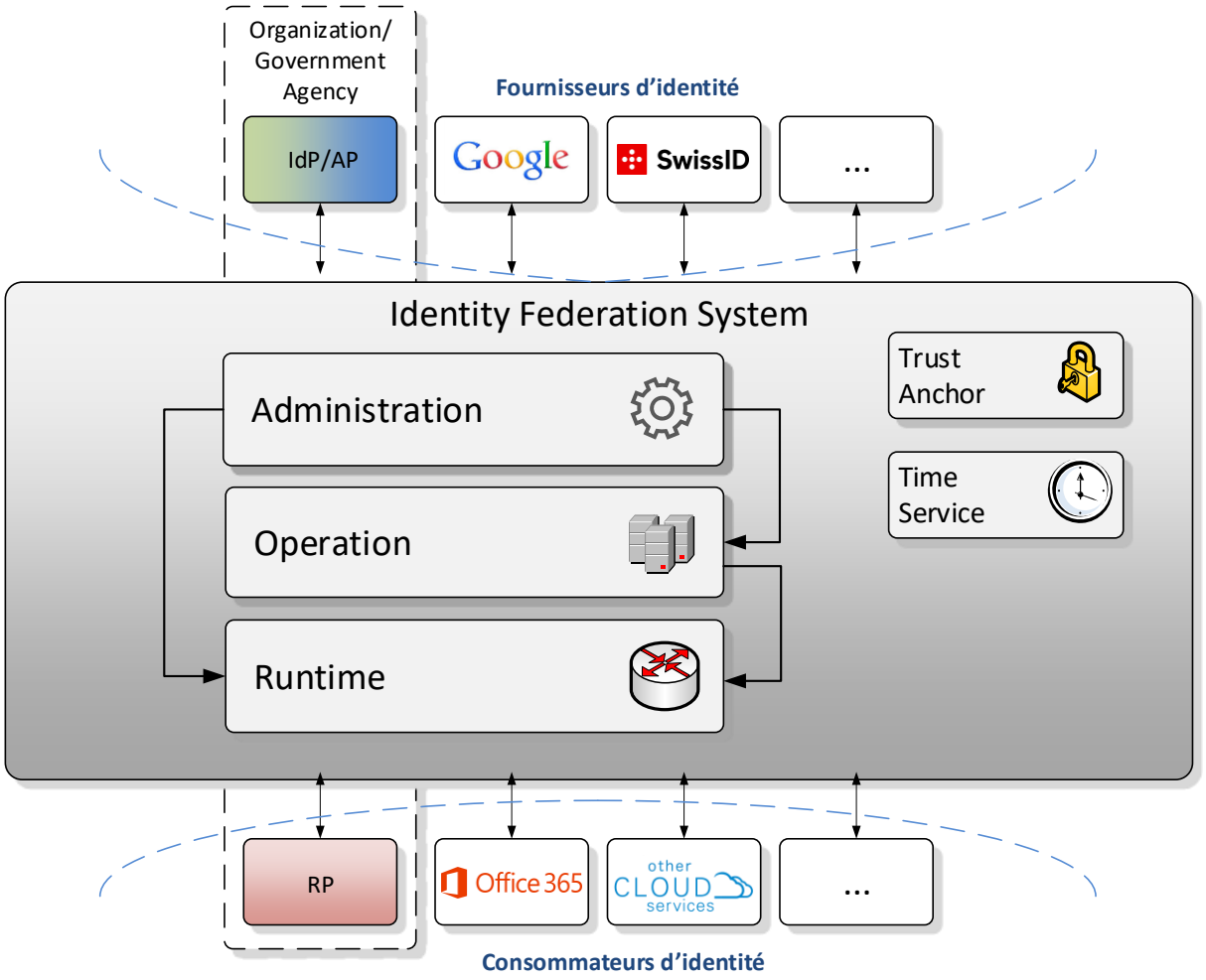

Figure 3: Structure grossière d'un système d'Identity Federation impliquant un Broker

Un système d'Identity Federation impliquant un Broker met tous les services nécessaires à la disposition des participants d'une communauté selon leurs exigences et directives (IAM-Policy).

Ces services peuvent être répartis en trois groupes:

- *Administration*: ce groupe comporte les processus de la période de définition et l'établissement (processus d'affaires *Définir l'IAM* et *Diriger l'IAM*) selon la norme eCH-0107 [2],
- *Operation:* le groupe couvre l'exploitation à proprement parler et le processus d'affaires *Soutenir les processus centraux.*
- *Runtime: o*n trouve ici tous les processus de la période d'exécution (processus d'affaires *Contrôler l'accès*).

Trust Anchor et Time Service sont stipulés selon eCH-0107 [2] dans les processus *Administration de l'IAM-Policy* respectivement *Diriger l'IAM Management*.

L'implémentation de ces services n'est pas sans incidence sur le périmètre de fonctionnement du système global.

3.1 Confiance

Une Identity Federation repose sur la confiance mutuelle entre les partenaires concernant le respect des directives convenues (IAM-Policy) (sur la base du principe-8 eCH-0107 [2]). La confiance se décline en deux catégories: l'intégrité et la disponibilité.

Les facteurs d'intégrité et de disponibilité sont présentés succinctement ci-après:

- Intégrité
  - **Authenticité:** l'origine et l'intégrité des confirmations d'authentification ou d'attribut reçues doivent pouvoir être suivies (traçabilité). Cela peut être fait par exemple en signant les confirmations (voir IAM-9 eCH-0107 [2]).
  - **Intégrité des données**: l'intégrité des données couvre l'exactitude des données. L'absence totale de manipulation des données par des personnes/entités non autorisées doit être garantie. Les signatures sont le moyen le plus courant d'y parvenir (voir IAM-9 eCH-0107 [2]).
  - **Traçabilité**: il doit pouvoir être possible de déterminer qui a traité des données précises, quand et de quelle manière.

- Disponibilité
  - **Disponibilité du système**: La disponibilité du système couvre le degré de fonctionnalité des composants centraux (Broker, IdP, AP). Cela signifie que ces composants devraient être à tout moment opérationnels et que le traitement des données se déroule correctement. La direction IAM peut, pour s'en assurer, avoir recours à des mesures organisationnelles et techniques. De la disponibilité souhaitée pour ces composants dépendent les exigences imposées au système IAM en charge de l'exécution.
  - **Fiabilité**: La fiabilité ou l'intégrité du système porte sur le fonctionnement correct des composants. La direction IAM peut imposer et surveiller l'intégrité demandée pour le système par des mesures organisationnelles et techniques.

3.2 Confidentialité

Dans une Identity Federation en cyberadministration, la protection de la sphère privée et des données revêt une importance particulière (voir aussi les exigences LB-13, LB-17 et LE-10 eCH-0107 [2]). Certaines des données traitées permettent d'identifier la personne (nom, prénom, date de naissance par exemple). Ce document part du principe selon lequel aucune donnée particulièrement digne d'être protégée (selon la LPD [9] art. 3.c) n'est utilisée pour l'authentification. Dans le cas d'un recours à des données particulièrement dignes d'être protégées, d'autres mesures, qui ne sont pas traitées dans le présent document, doivent être définies et mises en œuvre[2].
De manière générale, on désigne cet aspect de protection par le terme **confidentialité**: on peut parler de confidentialité lorsque des informations ne sont accessibles qu'aux personnes autorisées.
Cette confidentialité peut être préservée au moyen de mesures légales/organisationnelles et/ou techniques. Les mesures d'ordre technique ont pour elles de rendre une utilisation abusive des données plus difficile, dans le cas où les mesures légales/organisationnelles devaient se révéler trop peu efficaces.

[2] La nécessité d'un recours à des données particulièrement dignes d'être protégées doit être étudiée au cas par cas. En fonction du contexte et des combinaisons de données, des mesures de protection spécifiques peuvent s'imposer.

L'exigence relative à la confidentialité porte sur la transmission de confirmations d'authentification et d'attributs, par l'expéditeur (IdP, IdP/AP, AP) au destinataire (RP). La confidentialité de la transmission d'attributs présuppose que le niveau de confiance de l'authentification du sujet et du RP soit acceptable.

De manière générale, une Client Platform est considérée comme peu sûre et il faut veiller à ce qu'elle ne reçoive aucune information concernant l'utilisateur (au choix par un cryptage ou une transmission en utilisant un Back Channel). Voir également la norme eCH-0170 [3], chap. 8.2.3.

Dans les modèles d'architecture avec Broker en particulier, les confirmations d'authentification et d'attributs entre expéditeur et destinataire doit être transmises avec prudence, car toutes les confirmations d'authentification et d'attributs passent par le Broker, [3] qui pourrait alors utiliser les informations pour en déduire des habitudes comportementales. D'ordinaire, les confirmations d'authentification ne contiennent pas de données à caractère personnel au sens où l'entend la LPD [9] art 3.a et ne sont donc pas particulièrement critiques (l'Identifier peut faire exception à cette règle, dès lors qu'il n'est pas aléatoire et a un rapport avec). A l'inverse, les confirmations d'attributs contiennent des renseignements concernant les personnes.

3.3 Session Handling

Une Identity Federation regroupe de multiples sessions distinctes mises en place entre la Client Platform et les différents services IAM. Ces sessions doivent être différenciées les unes des autres:

- Les sessions auprès de l'IdP ou du Broker permettent le Single Sign-On (SSO) et réduisent ainsi les opérations d'authentification des sujets.
- Les sessions auprès du Discovery Service peuvent automatiser la sélection d'IdP, de sorte que les sujets soient amenés à faire un choix uniquement la première fois.
- Les sessions auprès du Relying Party permettent de s'authentifier une seule fois pour les différentes (https-)Requests (pour les diverses ressources) d'un User Client. Ces sessions peuvent grandement varier d'une application à l'autre.
- Les Attribute Providers sont d'ordinaire ‚stateless' et n'établissent pas de sessions.

Si elles coexistent, ces sessions n'en sont pas moins indépendantes les unes des autres: cela signifie que le fait qu'une session se déroule ne signifie pas systématiquement qu'une autre a lieu en même temps. Certaines sessions cependant peuvent être reliées entre elles, par des Identifiers communs par exemple.

L'existence de différentes sessions partiellement dépendantes rend les SSO, SLO et Step-Up-Authentication très compliqués, la technologie utilisée exerçant une influence majeure à cet égard. C'est la raison pour laquelle la présente norme se contente d'une description succincte des propriétés les plus importantes. La mise en œuvre concrète du Session Handling est l'objet d'autres normes eCH portant sur la technologie et s'appuyant sur cette norme.

[3] On parle dans ce cas précis d'un Broker considéré comme «honest but curious». En d'autres termes, le protocole est correctement implémenté (le Broker est honnête/honest), mais il pourrait être tenté de consulter les données passant par lui et de les utiliser à ses propres fins (il est curieux/curious).

3.3.1 Single Sign-on (SSO)

Suite à une authentification, le sujet peut accéder à la ressource protégée. Dans le cas où le sujet, au cours d'une période définie et limitée, souhaite accéder à une ressource d'un autre Relying Party au sein de la même communauté, il ne lui est pas nécessaire de s'authentifier de nouveau. Dans le cas où des attributs sont transmis, le consentement du sujet peut, le cas échéant, être imposé.

Le Relying Party peut toutefois exiger une authentification du sujet avant que ce dernier n'accède à ses ressources, et ainsi contourner le SSO.

3.3.1.1 Step-Up Authentication

La Step-Up Authentication constitue un cas particulier de SSO. Le sujet est déjà authentifié, mais souhaite à présent accéder à une ressource auprès du même ou d'un autre Relying Party, qui impose un niveau d'authentification plus strict. Dans ce cas de figure, le Relying Party envoie une nouvelle Request ou une Request renouvelée et l'utilisateur doit choisir l'un des IdP possibles, comme lors de l'authentification initiale, et s'authentifier auprès de ce dernier. Il faut alors une Identity Mapping (voir chap. 8.1.3.2) et Identity Linking (voir chap. 8.1.3.7). Dans le cas où la Step-Up Authentication est réalisée auprès du même IdP, ces deux fonctionnalités ne sont pas nécessaires.

Dans le cas où cela est nécessaire, les attributs demandés par la nouvelle ressource doivent être fournis dans la qualité souhaitée par un AP approprié.

3.3.1.2 Step-Down Authentication

La Step-Down Authentication constitue un cas particulier de SSO., au même titre que la Step-Up Authentication
On parle de Step-Down Authentication lorsque l'utilisateur a déjà été authentifié auprès d'un RP avec un niveau élevé et qu'il souhaite à présent accéder à un RP exigeant une qualité d'authentification moindre et que cette qualité est la seule qu'il est en mesure de traiter. Au sein d'un même Relying Party, ce cas d'utilisation se limite à une opération SSO, dans le cadre de laquelle l'authentification élevée déjà effectuée est réutilisée.
Le Step-Down peut poser problème lorsqu'une qualité d'authentification déjà existante impose des exigences supplémentaires à un RP (des attributs cryptés par exemple), auxquelles ce dernier n'est pas en mesure de répondre. Le Broker doit alors procéder aux adaptations de rigueur afin de remédier à ces obstacles techniques

Exemple: le sujet est déjà authentifié avec le niveau de confiance 3 et souhaite accéder à une ressource dont le niveau de confiance requis est 1. Le Broker accepte la confirmation d'authentification (de niveau de confiance 3) de l'IdP. Le Broker transforme la confirmation d'authentification en une confirmation de niveau de confiance 1 et la transmet au RP.

3.3.2 Single Logout (SLO)

Le Single Logout permet au sujet de se déconnecter de toutes les sessions au sein d'une communauté (IdP mais aussi RP). Le sujet devrait avoir la possibilité de le faire de manière aussi simple et transparente que possible.

Les Relying Parties impliquées doivent pour cela mettre à disposition des interfaces prenant en charge le Single Logout. Dans le cas où le processus de déconnexion (Logout) devait

ne pas fonctionner ou ne pas être pris en charge par un Relying Party, le sujet doit en être informé en conséquence.

4 4 Scénarii dans la cyberadministration

Un système d'Identity Federation dans la cyberadministration peut couvrir les scénarii suivants:

- Government to Citizen (G2C),
- Government to Government (G2G),
- Government to Business (G2B).

4.1 Government to Citizen (G2C)

Définition: dans un scénario Government to Citizen (G2C), les personnes physiques (citoyens ou habitants dans le rôle de personne civile, c.à.d. un acteur sans lien avec les autorités) utilisent, en ligne, les prestations spécifiques d'une autorité (RP). A cette fin, l'autorité délègue une partie des prestations IAM nécessaires à des prestataires de services IAM.

Il faut à cet égard utiliser, autant que possible, les E-Identities (et donc les IdP/AP) des individus qu'ils possèdent déjà et qui satisfont aux exigences des autorités. Les individus auraient donc la possibilité d'avoir recours aux mêmes E-Identities pour les prestations des autorités communales, cantonales et fédérales. Les E-Identities peuvent être gérées par les autorités ou des acteurs privés.

Exemples:

- Une personne devrait être identifiée par l'IdP/AP cantonal, qui connaît son adresse résidentielle, afin de pouvoir accéder à une application d'un autre canton, qui demande cette adresse résidentielle. L'application vérifie les confirmations d'authentification et d'attributs reçues avant d'accorder l'accès à ses ressources.
- Une personne utilise une E-Identity de niveau de confiance élevé (SuisseID par exemple) afin de commander un extrait du registre des poursuites.

4.2 Government to Government (G2G)

Définition: dans un scénario Government to Government (G2G), les employés ou les services d'une autorité (commune, canton, Confédération) utilisent, en ligne, les prestations spécifiques d'autres autorités et, dans certains circonstances, celles de leur propre autorité. A cette fin, l'autorité délègue une partie des prestations IAM nécessaires à la prestation spécifique, à des prestataires de services IAM.

Les employés et les services agissent alors pour le compte de l'autorité, comme en attestent des attributs confirmés. Les attributs confirmés peuvent également être utilisés par le RP à des fins de justifications d'entrée/d'accès.

L'employé ou le service est authentifié par un Identity Provider compétent de l'autorité (d'origine).

Exemples:

- Un employé du canton de Zurich souhaite consulter les informations d'une application fédérale. Il doit pour cela s'authentifier auprès de l'IdP cantonal. L'application fédérale accorde l'accès à l'employé après avoir vérifié les confirmations d'authentification et d'attributs reçues.
- Le service cantonal des contributions souhaite accéder aux données actuelles d'adresse des communes afin d'automatiser l'envoi de documents de nature fiscale.

4.3 Government to Business (G2B)

Définition: dans un scénario Government to Business, une personne physique agit pour le compte d'une organisation n'agissant pas elle-même, et utilise, en ligne, les prestations spécifiques d'une autorité (RP). A cette fin, l'autorité délègue les prestations IAM nécessaires aux prestataires de services IAM.

La personne physique doit par exemple être inscrite, selon la norme eCH-0170 [3] chapitre 6.2.1, pour la période de définition et associée à l'organisation qui n'agit pas elle-même. Pour la période d'exécution, le RP peut consulter l'Enterprise Attribute correspondant afin de confirmer l'appartenance à l'organisation.

Dans la mesure du possible, les E-Identities déjà présentes devraient être utilisées. Les E-Identities peuvent être gérées par les autorités ou des acteurs privés.

Exemples:

- Un entrepreneur souhaite adapter l'entrée de son entreprise dans le registre du commerce. Il lui faut pour cela s'authentifier avec un niveau de confiance élevé et peuvent fournir des attributs attestant qu'il est habilité à procéder à cette adaptation.

5 Cas d'application

Dans une Identity Federation de cyberadministration, on distingue, du point de vue du RP, deux cas d'application caractéristiques de la période d'exécution. Ces deux cas peuvent se retrouver dans tous les scénarii présentés au chapitre 4:

- **Authentification pure:** voir chapitre 5.1,
- **Authentification avec transmission d'attributs:** voir chapitre 5.2.

Les cas d'application définis ci-dessous sont des variantes du processus de période d'exécution *Confirmer l'E-Identity*, spécifié par la norme eCH-0107 [2]. Les différences entre les cas d'application concernent les différentes caractéristiques du sous-processus *Compléter l'E-Identity*..

5.1 Authentification pure

Dans le cas d'application Authentification pure, le processus partiel Compléter l'E-Identity est totalement supprimé. Le sujet est authentifié uniquement par un IdP. L'authentification doit avoir pour résultat un identificateur technique et la qualité de l'authentification. Seule la confirmation d'authentification est transmise. Aucune information ni attribut permettant d'identifier le sujet ne doit figurer dans la confirmation d'authentification.

5.1.1 E-Identities indépendantes

Un sujet peut posséder plusieurs E-Identities et s'en servir pour accéder à une ressource. Chacune des E-Identities du sujet doit être indépendante des autres, au sens où une ressource ne doit pas pouvoir constater que deux E-Identities distinctes appartiennent à un même sujet.

5.1.2 E-Identities reliées

Un sujet peut posséder plusieurs E-Identities associées. Les E-Identities sont associées lorsqu'une ressource reconnaît un sujet, bien qu'il utilise une autre E-Identity lors d'un nouvel accès.

5.2 Authentification avec transmission d'attributs

Outre le cas d'utilisation 'Authentification pure' (voir chapitre 5.1), pour lequel seuls une information sur le statut relatif à l'authentification effectuée et un identificateur technique sont retournés, une certaine quantité d'attributs sont demandés et livrés lors de l'authentification avec transmission des attributs.

Le processus 'Compléter l'E-Identity' (eCH-0107 [2]chapitre 6.1.4) est donc un processus partiel du processus Authentifier le sujet.

Le cas échéant, le sujet doit valider les attributs (User Consent). Se reporter au chapitre 8.1.3.3 pour de plus amples renseignements.

Exemple G2C:

- Un RP amorce la transmission d'une identité lorsqu'il veut créer localement un nouvel utilisateur pour le sujet et veut compléter les attributs de ce dernier. Le RP délègue l'authentification du sujet à un IdP/AP.
- Utilisation de BE-Login pour une déclaration de revenus ou demande de bourses d'études.

Exemple G2G:
Un agent d'une autorité cantonale souhaite accéder au RP de la Confédération. Pour ce faire, l'agent est authentifié auprès de l'IdP du canton. Les attributs 'Canton' et 'Fonction' sont transmis. L'agent ne doit pas valider ces attributs, car il s'agit d'Enterprise Attributes.

Les propriétés suivantes des attributs ne sont pas sans incidence sur le type de transmission des attributs et doivent être prises en compte lors de l'évaluation d'un système IAM.

Recommandation: Recommandation: les propriétés ou la qualité d'un attribut DEVRAIENT figurer dans la confirmation d'attribut au RP.

5.2.1 Durée de vie des valeurs d'attribut

Les attributs sont classés en deux catégories approximatives selon leur durée de vie:

- attributs pour lesquels les valeurs changent rarement (nom, prénom, date de naissance par exemple).
- attributs pour lesquels les valeurs doivent être régulièrement contrôlées (attributs en découlant comme l'âge du sujet, l'appartenance à un canton par exemple).

5.2.2 Nombre de sources

Les attributs peuvent être obtenus auprès d'une ou de plusieurs sources. Dans le cas où les attributs sont transmis depuis plusieurs sources, une Attribute Aggregation s'impose. Plus il y a de sources impliquées, plus un système IAM est complexe.

5.2.3 Provenance des données

L'utilisation des attributs pour le RP n'est pas sans incidence sur les exigences en matière de confirmations d'attribut. Lorsque l'on utilise par exemple des attributs pour les confirmations d'entrée et d'accès, il peut être important de connaître la source des attributs.

Exemples:

- sans importance: pointure
- exigé: appartenance à un canton

5.2.4 Qualité des attributs

Les attributs peuvent être de différente qualité. Il incombe au pilotage IAM de la communauté de définir comment doit être établie la qualité des attributs. La qualité des attributs peut dépendre de la qualité de l'authentification, de la source (provenance des données), etc. Le niveau de qualité d'un attribut doit être transféré au RP en tant que partie de la confirmation de l'attribut.

Exemples:

- Attribut non confirmé: titre (ou civilité)
- Attribut confirmé: adresse résidentielle (adresse du domicile du sujet confirmée par la Poste)
- Attribut officiellement confirmé: date de naissance

5.3 Identificateurs techniques utilisés dans les cas d'application

Trois types distincts **d'identificateurs techniques**[4] peuvent être utilisés dans une confirmation d'authentification. Le choix de l'identificateur à utiliser est déterminé en fonction des exigences du Relying Party et des exigences en matière de respect de la vie privée du sujet. Indépendamment de ces trois types d'identificateurs techniques, il ne devrait pas être possible de déduire qui est le sujet. Les identificateurs techniques ne désignent explicitement **pas** les identificateurs spécifiques (numéro AVS par exemple). Le cas échéant, ceux-ci sont transférés au RP en tant qu'attributs.

Recommandation: Un identificateur technique DEVRAIT toujours être une séquence de caractères aléatoire et NE DEVRAIT PAS contenir de données à caractère personnel conformément à l'article 3.a [8] de la LPD. Pour de plus amples renseignements concernant les identificateurs techniques, se reporter au SAML Core 2.0 [10] chapitre 8.3.

[4] Dans SAML, l'identificateur technique est le paramètre 'NameID'. Dans OIDC, l'identificateur technique est le paramètre 'sub'.

5.3.1 Identificateur réparti (Distributed ID)

Après l'authentification, le même identificateur doit être émis pour chaque Relying Party et chaque sujet. Il est ainsi possible de reconnaître un sujet auprès de plusieurs Relying Parties.

Lorsque l'on utilise cet identificateur, les Relying Parties impliqués au sein de la communauté peuvent facilement établir des habitudes comportementales et corréler les données des sujets.

Recommandation: les identificateurs techniques répartis NE DEVRAIENT PAS être utilisés.

5.3.2 Identificateur technique lié au Relying Party (Persistent ID)

Après l'authentification, un identificateur différent mais toujours le même doit être émis pour chaque Relying Party et chaque sujet. Il est ainsi possible pour un Relying Party de reconnaître un sujet. Mais comme un autre Relying Party reçoit un autre identificateur du même sujet, il est plus difficile de corréler les données.

Recommandation: un identificateur lié au RP DEVRAIT être utilisé lorsque le Relying Party souhaite délocaliser l'authentification, mais reconnaître le sujet lors de son prochain accès.

Exemple G2C: commande de carte de stationnement dans la commune

5.3.3 Identificateur technique aléatoire unique (Transient ID)

Un identificateur différent doit être utilisé pour chaque authentification du sujet.
Le sujet ne peut ainsi être reconnu dans le cadre de l'authentification d'un RP en cas d'accès à plusieurs reprises. Cet identificateur est également utile si l'accès à une ressource ne devrait être accordé que sur la base d'attributs.

Recommandation: un identificateur technique aléatoire unique DEVRAIT être utilisé lorsque le sujet également ne doit pas être reconnu en cas d'accès à plusieurs reprises ou si l'accès à une ressource ne devrait être accordé que sur la base d'attributs.

Exemple G2C:
consultation en ligne sur les addictions (www.safezone.ch par exemple)

Exemple G2G:
Une application fédérale n'est accessible qu'aux agents du canton. L'identité de l'agent n'est pas pertinente dans ce cas de figure.

6 Exigences

Les exigences relatives à un système IAM fédéré de cyberadministration sont décrites dans la norme eCH-0107 [2]. Ce chapitre aborde ces exigences et les illustre. Seuls les scénarii pertinents pour la cyberadministration (G2C, G2B et G2G, voir chapitre 4) et les cas d'application du chapitre 5 sont pris en compte. En outre, une étape sera franchie vers la mise en place de Identity Federations et, par conséquent, seules des technologies établies et le plus faible obstacle possible à l'entrée des RP seront exigés.

Les exigences peuvent parfois se révéler **contradictoires**. La classification des exigences au moyen des termes DOIT, DEVRAIT et PEUT se fait du point de vue du Stakeholder concerné. Les chapitres 7 et 8 exposent les mises en pratique possibles et les exigences pouvant être mises en œuvre concernant la vie privée. Les exigences sont (la plupart du temps) définies indépendamment d'un scénario. Selon le contexte et le scénario, certaines exigences peuvent être omises. Le pilotage d'IAM de la communauté (voir 224-Dir-1) doit décider quel modèle d'intermédiaire est utilisé pour répondre aux exigences.

Les nouvelles exigences et les exigences plus strictes sont réparties dans quatre groupes de typologies distincts:

- B… Business (exigences d'affaires),
- D… Data (informations et données),
- A… Application (application),
- T… Technology (technologie).

Les termes DOIT et NE DOIT PAS spécifient les exigences à remplir pour se conformer à la norme. Les exceptions doivent être décidées par le pilotage d'IAM de la communauté (voir 224-Dir-1).

Les termes DEVRAIENT et NE DEVRAIENT PAS indiquent que, parmi plusieurs possibilités, l'une est recommandée comme particulièrement appropriée sans en mentionner ni exclure les autres, ou qu'une certaine approche est privilégiée mais pas impérativement nécessaire, ou que (pour la forme négative) une certaine possibilité ou approche est déconseillée mais pas interdite.

Le terme PEUT renvoyer à une possibilité facultative.

6.1 Exigences imposées au système IAM fédéré

Désignation	Type	Description	Justification / référence
224-IAM-1	B	Seuls les scénarii G2C, G2B ou G2G DOIVENT être pris en charge. Plusieurs scénarii peuvent être pris en charge simultanément.	Restriction des scénarii
224-IAM-2	T	Le système IAM fédéré DOIT prendre en charge les applications dans les navigateurs Web (Chrome, Firefox etc.) et DEVRAIT prendre en charge les applications mobiles (application pour iOS et Android).	IAM-4

Désignation	Type	Description	Justification / référence
224-IAM-3	T	Les technologies[5] utilisées pour les protocoles du système IAM fédéré DOIVENT être bien établies.	IAM-4, 224-Dir-1 224-Dir-2
224-IAM-4	A/D	Dans un système d'Identity Federation, un modèle de qualité pour l'authentification DOIT être implémenté par tous les participants du système IAM et prévaloir.	IAM-2, 224-Dir-3
224-IAM-4.1	A/D	eCH-0170 [2] DEVRAIT être utilisé comme modèle de qualité pour l'authentification.	IAM-2
224-IAM-5	A/D	Les attributs DEVRAIENT pouvoir être évalués selon un modèle de qualité facile à comprendre (exemple: attributs non confirmés; attributs confirmés; attributs officiellement confirmés).	IAM-2, 224-Dir-4
224-IAM-6	B/A/T	Les RP, IdP et AP DOIVENT être intégrés conformément aux directives définies.	Principe 8
224-IAM-7	B/A	Il DEVRAIT être possible d'utiliser plusieurs sous-communautés dans un même système d'Identity Federation, dans la mesure où celles-ci imposent des exigences compatibles avec le système global.[6]	IAM-4
224-IAM-8	A	L'instance interrogée (Broker, IdP, IdP/AP ou AP) DOIT pouvoir identifier sans ambigüité l'instance interrogatrice (Broker ou RP) au moyen de la demande d'authentification ou d'attribut.[7]	Trust

Tableau 1: Exigences imposées au système IAM

6.2 Exigences du Stakeholder: bénéficiaire de prestations

Il existe, dans un système IAM fédéré, différentes exigences fondamentales devant être prises en compte lors de la conception de l'architecture IAM.

[5] Les seules technologies actuellement établies pour les protocoles dans un système d'Identity Federation sont SAML et OIDC. Le pilotage d'IAM de la communauté décide des technologies à considérer comme établies.

[6] Une communauté dispose d'une IAM-Policy commune qui, si elle peut être durcie, ne peut être assouplie dans les sous-communautés. Cela permet de s'assurer que les exigences sont compatibles et peuvent être implémentées dans un système IAM.

[7] L'identification comprend l'enregistrement et la reconnaissance de l'instance interrogatrice (authentification) selon les processus et les règles de Compliance prédéfinis.

La vie privée doit être protégée dans le scénario G2C. Dans le G2B également, la vie privée doit être prise en compte, sauf si aucune donnée permettant d'identifier une personne n'est échangée.

Concernant l'implémentation d'un système IAM, les exigences relatives à la vie privée doivent être mises au clair et des mesures organisationnelles et techniques correspondantes être mises en œuvre afin de protéger la vie privée des personnes physiques au sein du système IAM.

Ces exigences peuvent parfois se révéler contradictoires. Les chapitres 7 et 8 exposent les mises en pratique possibles et les exigences pouvant être mises en œuvre concernant la vie privée.

Désignation	Type	Description	Justification / référence
224-LB-1	B	La vie privée des personnes physiques DOIT être protégée.[8]	LB-2, LB-2.1, LB-13
224-LB-2	B	Une personne physique DOIT pouvoir accéder à une E-ressource, sans que les fournisseurs d'identité du système IAM ne puissent s'en rendre compte.[9]	Non-traçabilité (RP)
224-LB-3	B	Une personne physique DOIT pouvoir accéder à une E-ressource, sans que cette E-ressource ne sache quels fournisseurs d'identité ont été utilisés dans le système IAM. [10]	Non-traçabilité (IdP), principe Need to Know, minimisation des données
224-LB-4	B	Une personne physique DOIT pouvoir accéder à plusieurs reprises aux E-ressources de plusieurs RP (indépendants), sans que les RP ou des tiers non-autorisés puissent relier entre eux ces événements.	Non-associativité
224-LB-5	B	Les informations permettant d'identifier les personnes voire les informations sensibles [11]concernant une personne DOIVENT être protégées de telle manière que seules les RP autorisés, les organes autorisés (contrôle interne) et	Confidentialité

[8] Les différents aspects de la sphère privée (voir. eCH-0107 [2] chap. 9) devraient être évalués dans une mise en œuvre concrète au moyen d'une analyse des risques et des menaces.

[9] Il faut s'assurer que les fournisseurs d'identité ne soient pas informés des RP utilisant le sujet. Cette précaution permet de garantir que les fournisseurs d'identité, jugés «honest but curious», n'établissent d'habitudes comportementales concernant les habitudes d'utilisation.

[10] Il faut s'assurer que le RP n'est pas informé de l'IdP auprès duquel le sujet s'est authentifié et de l'AP ayant confirmé les attributs. De la sorte, on garantit que le RP ne reçoive aucune information dont il n'a pas besoin pour s'acquitter de ses fonctions.

[11] Selon le contexte, l'affectation des droits ou la combinaison d'attributs particuliers peut se révéler une question sensible.

Désignation	Type	Description	Justification / référence
		la personne physique elle-même puisse les consulter.	
224-LB-6	B	La personne physique DOIT donner son consentement avant que les confirmations d'attribut soient transmises à un RP avec les attributs personnels.	Consentement /transmission, Reg-1
224-LB-7	B	Les fournisseurs d'identité, Brokers et RP DOIVENT pouvoir à tout moment accéder aux données en vertu de la législation en vigueur en matière de protection des données et des règles cantonales de protection des données.	Droit d'accès, Reg-1
224-LB-8	B	Il DOIT être garanti que les RP reçoivent uniquement les informations concernant les personnes physiques pour lesquelles ils disposent des autorisations correspondantes.	Droit d'interrogation
224-LB-9	B	Les informations transmises pour une opération d'authentification particulière et leurs métadonnées DOIVENT pouvoir être présentées par les fournisseurs d'identité, Brokers et RP pour une période donnée définie par le pilotage d'IAM (de la communauté).	Traçabilité
224-LB-10	B	Une personne physique PEUT demander aux fournisseurs d'identité, Broker et RP que ses données soient supprimées. La suppression est possible dès lors que les données ne sont plus nécessaires pour s'acquitter de la tâche prévue et que l'opération ne va pas à l'encontre d'obligations légales de conservation.	Droit à l'oubli, Reg-1

Tableau 2: Exigences du bénéficiaire de prestations

6.3 Exigences du Stakeholder: Fournisseur de prestations

Désignation	Type	Description	Justification / référence
224-LE-1	B	Dans G2C: les sujets dans le système IAM DOIVENT être des personnes physiques. Dans G2G: le sujet DOIT être une personne physique ou un service dans le cadre de son appartenance à une autorité	Restriction des scénarii

Désignation	Type	Description	Justification / référence
224-LE-2	B/D	Surtout G2G: les confirmations d'attribut DEVRAIENT provenir d'AP dignes de confiance.[12]	Restriction des scénarii
224-LE-3	B	L'intégration au système IAM fédéré DOIT être possible pour le RP moyennant une contribution minime.[13]	Simplicité pour le RP
224-LE-3.1	B	Le RP DEVRAIT communiquer uniquement avec une composante (IdP ou Broker).	
224-LE-3.2	B	Le RP DEVRAIT prendre en charge uniquement une variante de protocole (Version, Flow, ...) et ne DEVRAIT pas avoir à procéder à des transformations de protocole.	
224-LE-3.3	B	Le RP DEVRAIT pouvoir déléguer autant de processus que possible (Discovery, User Consent, Identity/Attribut-Mapping & -Transformation…).	LE-11
224-LE-3.4	A	La demande et la réponse d'authentification, ainsi que les demandes et confirmations d'attributs DOIVENT être définies selon un format spécifique. Tous les participants peuvent se fier au fait que le format remplit bien les exigences minimales (contient par exemple une signature, un identificateur, correspond à un schéma d'attributs donné etc.).	Simplicité pour le RP, IAM-4, 224-Dir-5
244-LE-4	B/A	La RP PEUT exiger que la sélection des IdP puisse être limitée.	LE-5
224-LE-5	B	Un RP PEUT exiger que l'origine des confirmations d'authentification et d'attributs des sujets en remontant jusqu'à leur source (IdP, IdP/AP ou AP) puisse être contrôlée.	Provenance des données
224-LE-6	B	Un RP PEUT exiger que l'authenticité et l'intégrité des confirmations d'attributs des sujets en remontant jusqu'à leur source (IdP, IdP/AP ou AP) puissent être contrôlées.	Intégrité des données

[12] Lorsque le système d'Identity Federation est utilisé au sein d'une organisation, cette exigence peut être assouplie

[13] Une intégration simple peut par exemple signifier un jour-personne. Il s'agit uniquement de la configuration de la connexion, et non de la mise en œuvre des interfaces et de leurs protocoles.

Désignation	Type	Description	Justification / référence
224-LE-7	B	Le RP PEUT exiger qu'un même identificateur technique soit toujours retourné pour un sujet, indépendamment de l'IdP utilisé.	Simplicité pour le RP (pas d'Identity Linking/Mapping pour le RP) 224-Dir-1

Tableau 3: Exigences du prestataire de services

6.4 Exigences du Stakeholder: direction

Désignation	Type	Description	Justification / référence
224-Führ-1	B	Le pilotage d'IAM (de la communauté) DOIT décider quelles exigences des différents Stakeholders peuvent être raisonnablement remplies, et DOIT remédier aux contradictions.[14]	Principe 9 Dir-5
224-Führ-2	B	Le pilotage d'IAM (de la communauté) PEUT définir des exceptions pour les (anciens) systèmes existants.	Principe 9
224-Führ-3	B	Le pilotage d'IAM (de la communauté) DOIT définir un modèle de qualité pour l'authentification qui réponde aux exigences de tous les Stakeholders.	LE-7 Reg-2
224-Führ-4	B	Le pilotage d'IAM (de la communauté) PEUT définir un modèle de qualité pour les attributs qui réponde aux exigences de tous les Stakeholders.	LE-7 Reg-2
224-Führ-5	B	Le pilotage d'IAM (de la communauté) DOIT définir les formats de la demande et la réponse d'authentification, ainsi que les demandes et confirmations d'attributs, afin que les exigences de tous les Stakeholders soient remplies.	Principe 9 IAM-4, Dir-2

Tableau 4: Exigences du Stakeholder: Direction

[14] L'évaluation des exigences peut être effectuée en fonction des critères suivants: rentabilité (budget, coûts, délais), respect des normes, convivialité, soutien des systèmes existants etc.

7 Sélection du modèle d'Identity Federation

Les exigences parfois contradictoires du chapitre 6, en particulier concernant la protection de la sphère privée, ont une forte incidence sur la conception du modèle d'Identity Federation. Ce chapitre traite des exigences concernées et leur répercussion sur le choix du modèle. La Figure 4 offre une illustration graphique du processus de sélection.
La combinaison de plusieurs modèles de Broker est autorisée. Le «Broker Double Blinding» et les «Sources ouvertes Broker» sont faciles à combiner. La communauté doit décider, conformément aux exigences des parties concernées, quels modèles d'Identity Federation devraient être utilisés et comment les parties doivent être impliquées.

7.1 Influence des exigences

Exigence 224-LE-3 (intégration RP simple)

Cette exigence ne peut être réalisée que par les systèmes IAM impliquant un Broker selon le modèle Hub-'n'-Spoke (voir eCH-0107 [2] chap. 4.1). Dans ces systèmes impliquant un Broker, la complexité entre *n* Relying Parties et *m* IdP/AP est réduite et le RP ne communique plus qu'avec **un** composant, le Broker central. Ce dernier assume également des charges centrales telles que le Metadata Management, le Discovery Service, les requêtes d'User Consent etc.

Directive: Dans la cyberadministration, on DOIT avoir recours à un système d'Identity Federation impliquant un Broker. L'un des modèles de Broker («Broker Double Blinding», Sources ouvertes Broker», «Protection de la confidentialité Broker») ou une **combinaison** de ces modèles DOIT être réalisé.

Protection de la confidentialité au niveau du Broker - exigence 224-LB-5

La protection de la confidentialité au niveau du Broker signifie que celui-ci protège les confirmations d'authentification et d'attributs qui passent par lui, contre toute utilisation abusive. Cette protection de la confidentialité peut être réalisée de manière **juridique/organisationnelle** ou **technique**.

Directive: dans le cas d'une réalisation technique de la protection de la confidentialité, on DOIT avoir recours au modèle «Protection de la confidentialité Broker».

Dans ce modèle, les confirmations d'attribut, qui peuvent, le cas échéant, contenir des données sensibles et personnelles, ne sont transmises au Broker que cryptées pour le destinataire final (RP) et ne peut peuvent par conséquent pas être consultées par celui-ci. Toutefois, une telle situation n'est pas sans effet sur d'autres exigences relatives à la protection de la sphère privée, telles 224-LB-2 (Non-traçabilité RP) et 224-LB-3 (Non-traçabilité IdP), qui ne peuvent plus être satisfaites qu'avec des mesures techniques supplémentaires (certificats anonymes de courte durée par exemple), qui ne sont pas décrites dans la présente norme..

Dans le cas d'une réalisation juridique/organisationnelle, d'autres critères doivent entrer en ligne de compte lors du choix du modèle d'Identity Federation, comme le scénario mis en œuvre ou les exigences relatives à la protection de la sphère privée du sujet.

Exigence 224-LB-2 (non-traçabilité RP)

Cette exigence devrait être remplie lorsque la protection de la sphère privée du sujet est importante.
Au moment de satisfaire à cette exigence, il faut s'assurer que les fournisseurs d'identité ne puissent constater quelle ressource (quel RP) utilise le sujet. L'exigence est automatiquement remplie dès lors que la protection de la confidentialité n'est pas réalisée techniquement au niveau du Broker.

Directive: lorsque la non-traçabilité (RP) est exigée, on DOIT réaliser soit un «Broker Double Blinding», soit un «Sources ouvertes Broker».

Exigence 224-LB-3 (non-traçabilité IdP)

Cette exigence devrait être remplie lorsque la protection de la sphère privée du sujet est importante. Au moment de satisfaire à cette exigence, il faut s'assurer que le RP n'est pas en mesure de déterminer où le sujet s'est authentifié et quel AP a confirmé les attributs. Satisfaire l'exigence 224-LB-3 empêche de remplir l'exigence 224-LE-5 (provenance des données).

Directive: lorsque la non-traçabilité (IdP) est demandée, on DOIT réaliser un «Broker Double Blinding».

Exigence 224-LE-5 (provenance des données)

Cette exigence demande à ce qu'un RP puisse contrôler la provenance des confirmations d'authentification et d'attributs et – selon l'implémentation – la provenance des confirmations (en contrôlant la signature du système source ou au moyen d'un attribut par exemple). Si cette exigence est remplie, un «Blinding» unilatéral, tout au plus, est possible, car le RP connaît toujours les systèmes sources (224-LB-3 ne peut être remplie).

Directive: lorsque la provenance des données est demandée, on DOIT réaliser un «Sources ouvertes Broker».

Exigence 224-LE-6 (intégrité des données)

Le RP peut contrôler l'intégrité et l'exhaustivité des confirmations d'authentification et d'attributs à partir de la source (en contrôlant par exemple une signature du système source). Cette exigence ne peut être satisfaite que lorsque l'exigence 224-LE-5 (provenance des données) l'est également. L'exigence 224-LB-3 ne peut être remplie.

Directive: lorsque l'intégrité des données est demandée, l'exigence concernant la provenance des données DOIT également être remplie. On DOIT réaliser un «Sources ouvertes Broker».

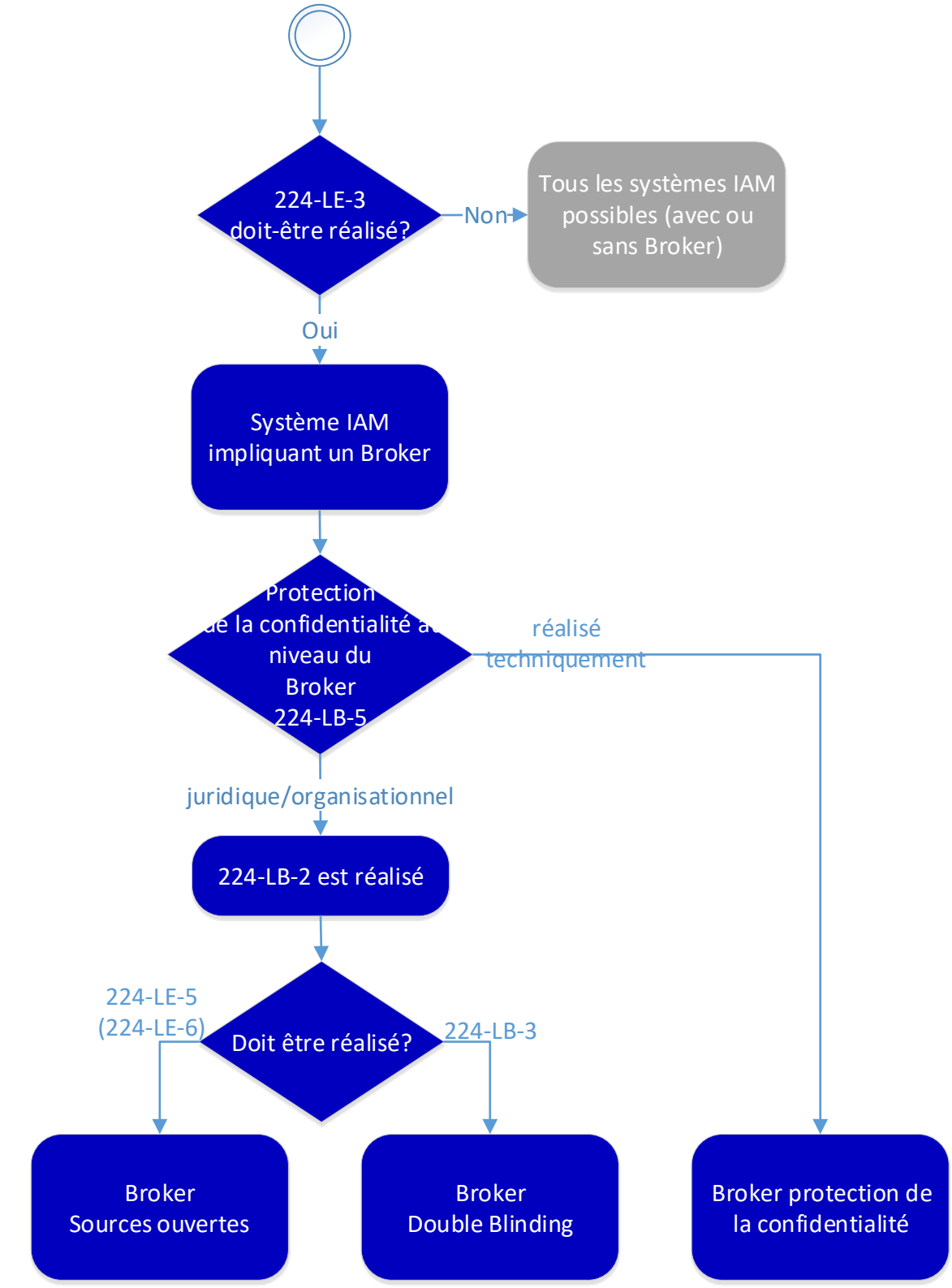

Figure 4: Arbre de décision pour la sélection de modèles d'Identity Federation

7.2 Influence des scénarii

Scénario G2G

Dans un scénario G2G, dans lequel on ne confirme d'ordinaire que des Enterprise Attributes des employés des autorités avec les résultats d'authentification et que ceux-ci ne sont utilisés que pour décider des entrées et accès, la protection de la sphère privée du sujet est moins pertinente dans la plupart des cas. Il est bien souvent important à cet égard de connaître la provenance des confirmations (224-LE-5).

Recommandation G2G: dans le cas d'un scénario G2G, on DEVRAIT utiliser un «Sources ouvertes Broker».

Scénario G2B

Dans le scénario G2B, la protection de la sphère privée joue un rôle, quoique moindre, comparé au cas du G2C. En effet, seuls les Enterprise Attributes pour la décision sur les entrées et accès devraient normalement être utilisés – comme dans G2G. Les données à caractère personnel des personnes représentant l'organisation ne devraient donc pas être demandées. L'exigence 224-LB-5 (confidentialité) ne doit par conséquent pas être remplie. Contrairement à l'exigence 224-LB-2 (non-traçabilité RP), qui doit être remplie afin d'exclure toute utilisation abusive.

Recommandation G2B: pour un scénario G2B, on DEVRAIT avoir recours à un «Sources ouvertes Broker» ou un «Broker Double Blinding», en fonction de la décision relative à la réalisation de 224-LE-5 (provenance des données).

Scénario G2C

Les exigences relatives à la protection de la sphère privée 224-LB-2 (non-traçabilité RP) et 224-LB-3 (non-traçabilité IdP), ainsi que 224-LB-5 (confidentialité) s'excluent en cas de respect de 224-IAM-3 (technologies établies). Une réalisation de toutes ces exigences n'est possible qu'à l'aide de «Modèles Token-based d'Identity Federation» (les attributs sont placés dans l'environnement du sujet - voir Annexe G), dont la mise en œuvre se révélerait très fastidieuse en l'état actuel de la technique (Q2 2018) (contradictions avec le principe 9 eCH-0107 [2]) [2]).

Directive G2C avec confidentialité: lorsque l'exigence 224-LB-5 (confidentialité) doit être remplie dans le scénario G2C, on DOIT réaliser une «Protection de la confidentialité Broker».

Directive G2C avec non traçabilité RP: lorsque l'exigence 224-LB-2 (non-traçabilité RP) doit être remplie dans un scénario G2C, on DOIT avoir recours à un «Sources ouvertes Broker» ou un «Broker Double Blinding», en fonction de la décision relative à la réalisation de 224-LE-5 (provenance des données) et 224-LB-3 (non-traçabilité IdP).

7.3 Systèmes n'impliquant pas de Broker

Une Identity Federation sans Broker peut se révéler judicieux dans les circonstances suivantes:

- l'Identity Federation est utilisée au sein d'une organisation. Dans ces circonstances, il n'y a pas de non-respect des exigences 224-LB-2 (non-traçabilité RP) et 224-LB-3 (non-traçabilité IdP) ou la traçabilité est partiellement requise. Le scénario G2C s'en

trouve ainsi exclu, car un scénario impliquant le citoyen dépasse toujours les limites de l'organisation.
- D'ordinaire, le respect de l'exigence 224-LE-3 (intégration RP simple) passe par un recours à un Broker. Si, toutefois, seul un ou quelque IdP sont utilisés dans la Identity Federation, la simplification au moyen d'un Broker n'est plus une nécessité.
- Si le règlement eCH-0170 exige un niveau de confiance 4, avoir recours à un intermédiaire peut rendre difficile, voire impossible, la mise en œuvre de la sécurité accrue, telle que requise (procédure Holder of Key par exemple).

Tableau 5: Conformité aux exigences d'une Identity Federation n'impliquant pas de Broker.

Exigence	Degré de satisfaction	Remarque
224-LB-2 (Non-traçabilité RP)	non réalisé	
224-LB-3 (Non-traçabilité IdP)	non réalisé	
224-LB-5 (Protection de la confidentialité)	possible	
224-LE-3 (Intégration RP simple)	non réalisé	Réalisable uniquement si un ou plusieurs IdP sont utilisés
224-LE-5 (Provenance des données)	possible	
224-LE-6 (Intégrité des données)	possible	

Directive: Les scénarios imposant le respect de l'exigence 224-LB-2 (non-traçabilité RP) ou 224-LB-3 (non-traçabilité) NE DEVRAIENT PAS utiliser un modèle sans Broker.

7.4 Broker Double Blinding

Un «Broker Double Blinding» doit entièrement séparer les sections de protocole P1 et P2. La section de protocole P1 décrit la communication entre le RP et le Broker, P2 la communication entre le Broker et les IdP, les AP ainsi que les IdP/AP.
Tous les participants au système IAM font confiance au Broker pour qu'il respecte la nature confidentielle des informations passant par lui et qu'il n'en fasse pas un usage abusif. Cette confiance est fondée de manière juridique/organisationnelle.
Le Broker réalise un *Double Blinding*, ce qui signifie que le RP ne se voit confier aucune information susceptible de lui permettre de déduire auprès de quel IdP le sujet a été authentifié et de quels APs proviennent les éventuels attributs. En outre, l'IdP ou l'IdP/AP et les AP utilisés ne reçoivent aucune information concernant le RP auquel souhaite accéder le sujet.

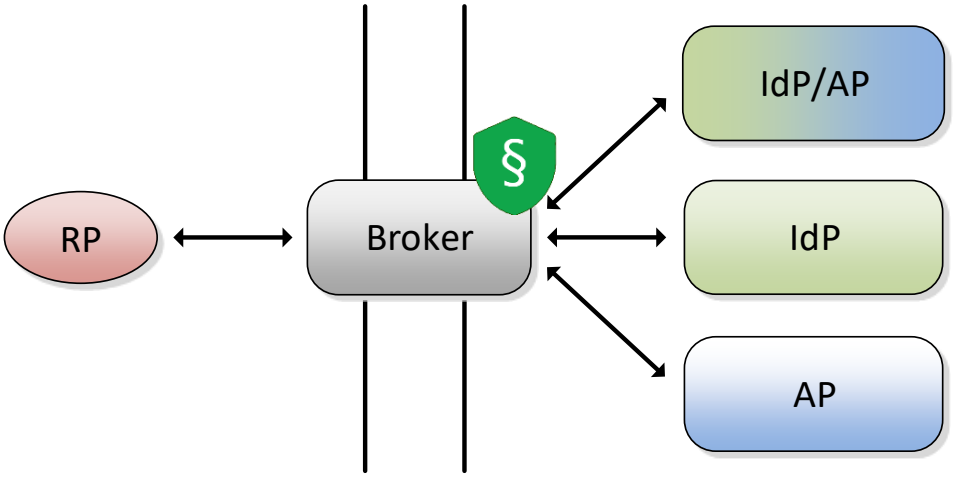

Figure 5: Broker Double Blinding

Le tableau suivant répertorie les exigences pertinentes pour une décision ainsi que leur degré de réalisation selon le chapitre 6.

Tableau 6: Réalisation des exigences du «Brokers Double Blinding»

Exigence	Degré de satisfaction	Remarque
224-LB-2 (Non-traçabilité RP)	réalisé	
224-LB-3 (Non-traçabilité IdP)	réalisé	
224-LB-5 (Protection de la confidentialité)	jurid./organisat. uniquement	Le Broker «voit» les confirmations d'attribut
224-LE-3 (Intégration RP simple)	réalisé	
224-LE-5 (Provenance des données)	non réalisé	
224-LE-6 (Intégrité des données)	non réalisé	

Le modèle «Broker Double Blinding» peut être utilisé pour tous les scénarios.

Directive: les scénarii, qui insistent sur la réalisation de l'exigence 224-LE-5 (provenance des données) ou 224-LE-6 (intégrité des données), NE DOIVENT PAS utiliser le modèle «Broker Double Blinding».

Ce modèle est également utilisé pour le STIAM en Identity Proxying Mode (IP-Mode) (voir eCH-0168 [4], chapitre 3.4.1).

7.5 Sources ouvertes Broker

Un «Sources ouvertes Broker» fonctionne selon un mode semblable à celui d'un «Broker Double Blinding» (voir chapitre 7.4).
Le Broker se contente de réaliser un «Blinding» unilatéral:

- L'IdP ou l'IdP/AP et les AP utilisés ne reçoivent, comme auparavant, aucune information concernant le RP auquel le sujet souhaite accéder.
- Toutefois, le Broker transmet au RP, sous une forme visible, l'information sur l'IdP auprès duquel le sujet a été authentifié et de quels AP proviennent les attributs. Cela peut également se produire uniquement pour l'IdP ou les AP sélectionnés.

Lors de la divulgation des sources, une distinction doit être établie entre *Visibilité* et *Vérifiabilité*.

- **Visibilité** signifie que le Broker indique au RP d'où provient la réponse d'origine. Cela peut être fait sous la forme d'un attribut par exemple.
- **Vérifiabilité** signifie que le RP peut vérifier la source et l'intégrité des attributs au moyen d'une signature. Les attributs signés à l'origine sont transmis par le Broker au RP. S'il est autorisé, ce comportement n'est pas traité plus avant dans cette norme.

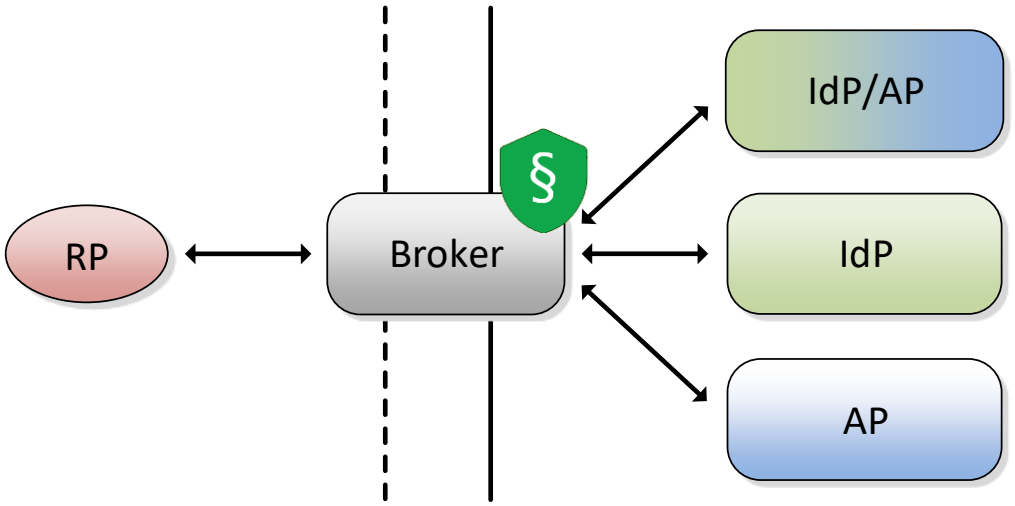

Figure 6: Sources ouvertes Broker

Le tableau suivant répertorie les exigences pertinentes pour une décision ainsi que leur degré de réalisation selon le chapitre 6.

Tableau 7: Réalisation des exigences des «Sources ouvertes Broker»

Exigence	Degré de satisfaction	Remarque
224-LB-2 (Non-traçabilité RP)	réalisé	
224-LB-3 (Non-traçabilité IdP)	non réalisé	
224-LB-5 (Protection de la confidentialité)	jurid./organisat. uniquement	Le Broker «voit» les confirmations d'attribut

224-LE-3 (intégration RP simple)	réalisé	
224-LE-5 (provenance des données)	réalisé	
224-LE-6 (Intégrité des données)	possible	Avec les confirmations d'attribut, qui sont signées par l'IdP/AP ou l'AP.

Le modèle «Sources ouvertes Broker» convient donc essentiellement aux scénarii G2G. Il peut être utilisé pour les scénarii G2B et G2C, lorsque la réalisation des exigences 224-LB-3 (protection de la sphère privée) n'est pas imposée.

Directive: le modèle «Sources ouvertes Broker» NE DOIT PAS être utilisé lorsque l'exigence 244-LB-3 (protection de la sphère privée) est imposée.

7.6 Protection de la confidentialité Broker

Dans le cas de la «Protection de la confidentialité Broker», la confidentialité des confirmations d'attributs doit être réalisée techniquement par cryptage. Le Broker ne peut donc pas accéder aux valeurs d'attribut ni les modifier.
Les attributs doivent être signés par la source (IdP/AP ou AP) et cryptés pour le RP. Le RP peut ainsi déterminer qui a fourni les attributs.
La réalisation technique de la protection de la confidentialité empêche le «Blinding» entre le RP et les Attribute Providers (IdP/AP et AP), comme dans les deux autres modèles[15].

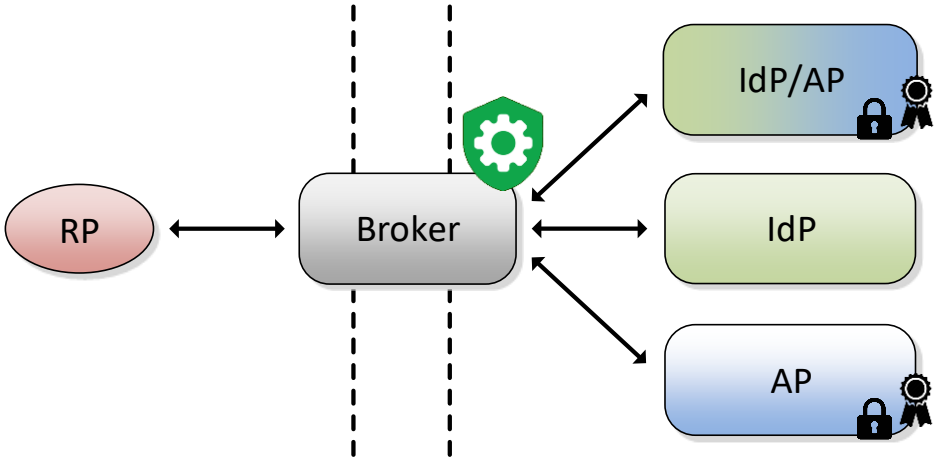

Figure 7: Protection de la confidentialité Broker

Le tableau suivant répertorie les exigences pertinentes pour une décision ainsi que leur degré de réalisation selon le chapitre 6.

Tableau 8: Réalisation des exigences du «Protection de la confidentialité Broker»

Exigence	Degré de satisfaction	Remarque

[15] Sauf si des certificats anonymisés de courte durée sont utilisés pour le cryptage des données. Cette approche n'est pas abordée plus avant dans la présente norme.

224-LB-2 (Non-traçabilité RP)	non réalisé	
224-LB-3 (Non-traçabilité IdP)	non réalisé	
224-LB-5 (Protection de la confidentialité)	réalisé techniquement au niveau du Broker	
224-LE-3 (Intégration RP simple)	en partie réalisé	La protection de la confidentialité accroît la charge de travail du RP
224-LE-5 (Provenance des données)	réalisé	
224-LE-6 (Intégrité des données)	réalisé	

Le modèle «Protection de la confidentialité Broker» convient aux scénarii G2C, lorsque la «protection de la sphère privée» est moins pertinente. L'inconvénient est que les RP et les IdP peuvent ensuite établir des modèles simples sur les habitudes comportementales des sujets.

Dans les scénarii G2G, le modèle peut être utilisé lorsque la réalisation de l'exigence 224-LE-5 (provenance des données) et 224-LE-6 (intégrité des données) est requise. Concernant G2B, le modèle est peu adapté faute de réalisation de l'exigence 224-LB-2.

Directive: le modèle «Protection de la confidentialité Broker» NE DOIT PAS être utilisé, lorsque l'exigence 224-LB-2 ou 224-LB-3 est imposée.

8 Modèles de Broker

Ce chapitre définit les modèles de Broker dans le détail. Il commence par une introduction des notions importantes avant de spécifier les modèles «Broker Double Blinding», «Sources ouvertes Broker», et «Protection de la confidentialité Broker».

8.1 Notions de base concernant les modèles de Broker

Les chapitres suivants spécifient les concepts de base. Les explications portent, d'une part, sur les sections de protocole entre RP, Broker et IdP/AP (AP) et, d'autre part, sur les processus pertinents et les activités spécifiques.

8.1.1 Sections de protocole

La communication entre les composants est répartie entre deux sections de protocole distinctes. Comme sur la Figure 8, la section P1 décrit la communication entre le RP et le Broker. P2 décrit la communication entre le Broker et les IdP, les AP ainsi que les IdP/AP. Dans P3, la communication se déroule sans Broker, directement entre RP et IdP/AP ou AP.

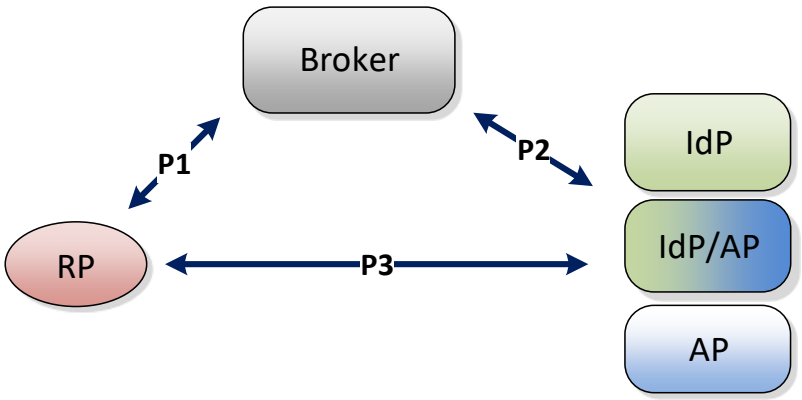

Figure 8: Sections de protocole

Quel que soit le procédé, les éléments suivants sont requis: Metadata Management, Trust Management et IdP-Discovery. Le plus simple consiste à confier ces tâches au Broker. Dans tous les cas, les confirmations d'authentification et d'attributs doivent être signées (voir eCH-0107 [2] Exigences IAM-7, IAM-9 et IAM-11). Il est ainsi possible de contrôler l'authenticité et l'intégrité des confirmations.

8.1.1.1 Section de protocole entre RP et Broker (P1)

Deux possibilités sont envisagées pour la section de protocole entre RP et Broker:

1. Toute la communication entre le RP et le Broker s'effectue via la Client Platform (navigateur par exemple) du sujet.
2. Seul le processus d'authentification s'effectue via la Client Platform. Toutes les étapes de communication qui suivent s'effectuent via Back-Channel.

Les deux procédés présentent des avantages et des inconvénients qui sont présentés dans les chapitres qui suivent. Le choix du procédé à mettre en œuvre doit reposer sur une évaluation par la communauté selon l'exigence en matière de sécurité et le domaine d'application.

8.1.1.1.1 Confirmation d'authentification et d'attributs via Front-Channel

Lors de ce procédé, toute la communication s'effectue via la Client Platform (navigateur par exemple) du sujet. Le sujet est authentifié via la Client Platform. A cet égard, les confirmations d'authentification et les éventuelles confirmations d'attribut sont transmises au RP via la Client Platform. Il s'agit d'un mode simple d'authentification d'un sujet.

Quelques aspects de sécurité doivent être observés. La communication se déroulant intégralement via la Client Platform, il faut évaluer dans quelle mesure doit être protégée la communication. Par principe, la Client Platform peut consulter et manipuler la communication.

Deux mesures peuvent en principe être prises en guise de contremesure. Une sécurisation au niveau du transport ou du contenu. La seule protection efficace contre une Client Platform curieuse ou compromise est le cryptage de la confirmation d'authentification et d'attributs au niveau du contenu. La protection offerte par le cryptage et l'authentification au niveau du transport (TLS par exemple) est confinée au canal de communication.

Ce procédé n'est pas recommandé lorsque le Broker ne peut pas identifier sans ambigüité le RP lors de la demande d'authentification et d'attributs, car le Broker n'est alors pas en mesure de contrôler si le RP est bien habilité à solliciter des confirmations d'authentification et d'attributs. Dans ce cas de figure, le procédé présenté au chapitre 8.1.1.1.2 devrait être utilisé.

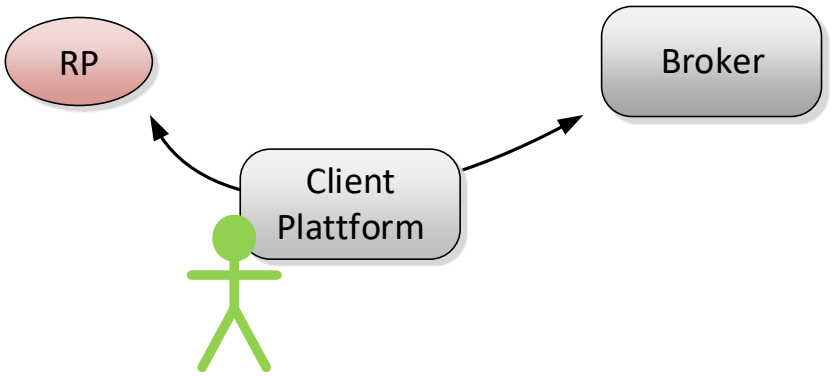

Figure 9: Section de protocole P1 – Front-Channel

Une fois reçue la confirmation d'authentification et d'attributs, le RP doit valider les signatures.

8.1.1.1.2 Confirmation d'authentification et d'attributs via Back-Channel

Le sujet est authentifié à l'aide de la Client Platform (navigateur par exemple). Une fois l'authentification réussie, une référence est envoyée au RP via la Client Platform en lieu et place d'une confirmation d'authentification ou d'attributs. Cette référence ne doit contenir aucune donnée permettant de retrouver l'identité du sujet. Le RP peut désormais demander la confirmation d'authentification ou d'attributs auprès du Broker via le Back-Channel.

Ce procédé présente l'avantage que la Client Platform ne voit aucune donnée du sujet et qu'il n'est donc pas nécessaire de prendre des mesures particulières destinées à les protéger.
Le Broker peut également vérifier via ce Back-Channel sûr, si le RP est habilité à solliciter des confirmations d'authentification et d'attributs. La communication via le Back-Channel doit

être protégée au niveau du transport (au moyen de TLS par exemple), car elle se déroule directement entre le RP et le Broker.

L'inconvénient de ce procédé est le fait que le RP doit implémenter légèrement plus de logique en raison d'une nouvelle requête, pour pouvoir recevoir les confirmations d'authentification et d'attributs.

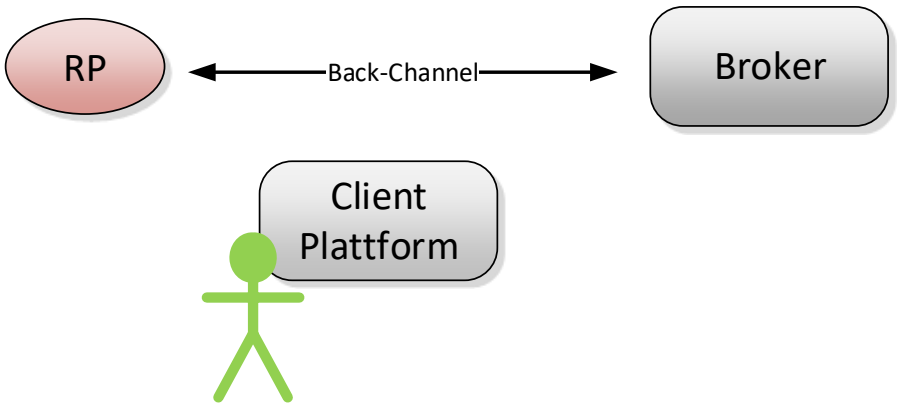

Figure 10: Section de protocole P1 - Back-Channel

Une fois reçue la confirmation d'authentification et d'attributs, le RP doit valider les signatures.

8.1.1.2 Section de protocole entre Broker et IdP, AP et IdP/AP (P2)

Ce chapitre décrit la façon dont se déroule la communication entre le Broker et les IdP, AP et IdP/AP impliqués. Il existe différentes variantes pouvant être utilisées en fonction de la situation initiale, des exigences de sécurité et du champ d'application.

8.1.1.2.1 Authentification et requête d'attributs depuis une source

Dans le cadre de ce procédé, le sujet est authentifié et des attributs peuvent être transmis.

Comme pour la section de protocole P1, on trouve là encore deux possibilités de transmettre les confirmations d'authentification et d'attributs.

La confirmation d'authentification et d'attributs peut être transmise au Broker par Front-Channel via la Client Platform (comme au chapitre 8.1.1.1.1).

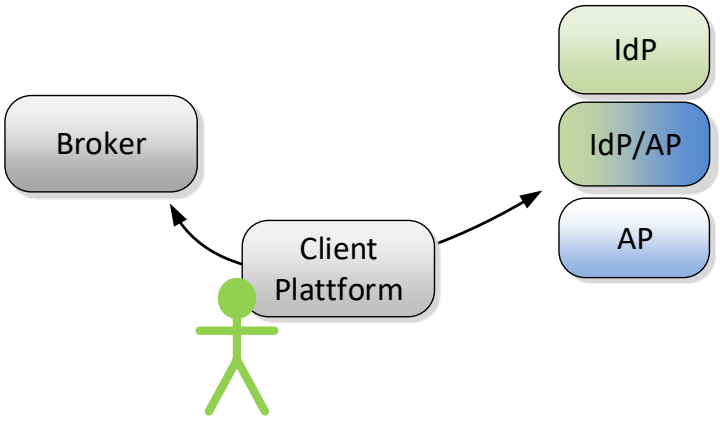

Figure:11 Section de protocole P2 – Front-Channel

Dans la deuxième possibilité, une référence peut être envoyée au Broker via la Client Platform. A l'aide de la référence, le Broker peut solliciter la confirmation d'authentification et d'attributs auprès de l'IdP (comme au chapitre 8.1.1.1.2).

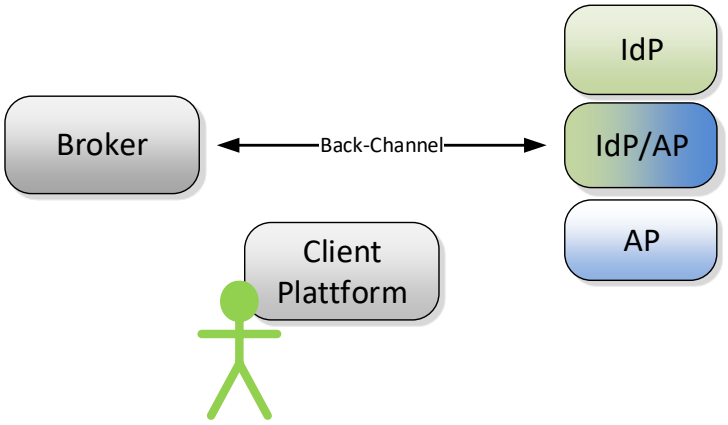

Figure 12: Section de protocole P2 - Back-Channel

Dans les deux cas, le Broker doit vérifier les signatures de confirmation. L'un des deux procédés possibles doit être réalisés.

8.1.1.2.2 Requête d'attributs auprès de plusieurs sources

Ce procédé consiste à authentifier le sujet et à compiler et à transmettre les attributs de plusieurs sources. Une agrégation d'attributs est alors nécessaire. Les E-Identities utilisées ici doivent être préalablement associées lors de la période de définition.

Il existe deux variantes distinctes concernant la manière et l'auteur de l'agrégation des attributs. Le choix de la variante à utiliser dépend du modèle de Broker utilisé et la décision correspondante doit être prise en fonction de la situation initiale, des exigences de sécurité et du champ d'application.

Le Broker agrège les attributs

Après l'authentification (voir chapitre 8.1.1.2.1) il faut décider des AP à interroger au moyen des métadonnées. Le Broker adresse une de-mande d'attributs aux AP correspondants en passant par un canal direct (Back-Channel).

Les AP doivent étudier les demandes d'attributs au moyen des mesures appropriées. Une fois le contrôle réussi, les AP génèrent des confirmations d'attribut et les envoient au Broker.

Le Broker doit ensuite agréger les confirmations d'attribut.

Le Broker transmet les références d'attributs
Cette variante est utilisée dans le modèle «Protection de la confidentialité Broker».

Après l'authentification (voir chapitre 8.1.1.2.1) il faut décider des AP à interroger au moyen des métadonnées. Le Broker génère des références correspondantes et doit les envoyer au RP. Le RP doit ensuite interroger directement les AP à l'aide de la référence (voir 8.1.1.3).

8.1.1.3 Section de protocole entre RP et IdP/AP ou AP (P3)

Cette section de protocole est utilisée uniquement lorsque le RP se procure les attributs directement auprès de la source des attributs (protection de la confidentialité Broker)

Si le RP reçoit une référence (sous forme d'URI et d'Access Token par exemple) du Broker, celui-ci peut solliciter, via un Back-Channel, des attributs directement auprès d'un IdP/AP ou d'un AP. L'IdP/AP ou l'AP doit vérifier l'authenticité de la référence avant de transmettre les attributs au RP. Le RP doit valider la signature à la réception de la confirmation d'attributs.

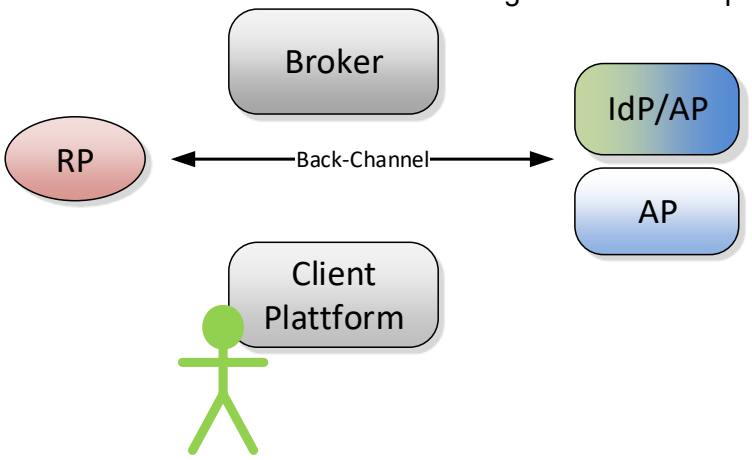

Figure 13: Section de protocole P3

8.1.2 Session Handling

Selon les exigences et le cas d'application de l'Identity Federation, le Broker peut être implémenté de différentes manières:

- **Stateless**: Le Broker ne conserve par principe aucune donnée pour la période d'exécution. Le Broker répond aux demandes d'authentification par des confirmations d'authentification (dans OIDC avec Authentication Code Flow par exemple), mais ne tient pas de session concernant une authentification réussie. Le Single Sign-On peut être rendu possible au niveau de l'IdP. Un Single Logout n'est pas possible. Lorsque le Broker est exploité en mode stateless, il n'est pas possible de couvrir l'intégralité des cas d'application. Seuls les cas d'application Authentification et Transmission d'identité peuvent être réalisés.
- **Stateful**: le Broker contrôle les sessions. Tous les cas d'application peuvent être couverts (les attributs de plusieurs sources peuvent être agrégés par exemple). Le Broker peut ainsi répondre à plusieurs demandes d'authentification émanant de divers

RP, sans que le sujet ne doive à nouveau s'authentifier auprès de l'IdP. L'User Consent peut être géré de manière centralisée par le Broker. En fonction des données traitées et enregistrées, d'autres directives en matière de protection des données doivent être prises en compte.

8.1.3 Processus

Les processus de base d'un IAM fédéré ont déjà été décrits en détail dans les principes de conception pour la gestion des identités et des accès (eCH-0107 [2]). Les paragraphes qui suivent se réfèrent aux différents processus d'un système d'Identity Federation avec les parties correspondantes dans les normes eCH-0107 [2] et eCH-0170 [3]. Lorsque cela est nécessaire, les activités des processus sont concrétisées ou étayées au moyen d'exemples.

Les processus suivants doivent être pris en compte dans une Identity Federation impliquant un Broker.

Période d'exécution:

- Confirmer l'E-Identity (eCH-0107 chapitre 6.1.1)
  - Transformation de la confirmation d'authentification.
  - Identity Mapping (regroupement d'identités)
  - Obtention de l'User Consent
  - Transformation de confirmation d'attribut
  - Attribute Aggregation
  - Transformation de protocole
- IdP Discovery (eCH-0107 chapitre 6.1.2)
- Authentifier le sujet (eCH-0107 chapitre 6.1.3)
- Compléter l'E-Identity (eCH-0107 chapitre 6.1.4)
  - Confirmation d'attribut
- Autoriser l'entrée (eCH-0107 chapitre 6.1.5)
- Autoriser l'accès et publier les attributs (eCH-0107 chapitre 6.1.6)

Période de définition:

- Définir l'E-Identity (eCH-0107 chapitre 6.2.1)
  - Identity Linking
  - Enregistrement Step-Up
- Définir les attributs (eCH-0107 chapitre 6.2.2)
- Définir les moyens d'authentification (eCH-0107 chapitre 6.2.3)
- Définir les règles d'entrée pour les E-ressources (eCH-0107 chapitre 6.2.5)
- Définir les règles d'accès pour les E-ressources (eCH-0107 chapitre 6.2.6)

Etablissement:

- Diriger la direction IAM
  - Metadata Management

Les activités relatives aux systèmes d'Identity Federation impliquant un Broker sont définies ci-après.

8.1.3.1 Transformation de confirmation d'authentification

Processus: Confirmer l'E-Identity

Un Broker doit transformer la confirmation d'authentification et d'attributs en fonction des différentes exigences. La transformation d'identificateur est une singularité à cet égard. Un Broker devrait l'adapter dans tous les cas de figure (voir chapitre 5).

8.1.3.2 Identity Mapping (regroupement d'identités)

Processus: Confirmer l'E-Identity

Une application, qui autorise plusieurs services d'authentification (solutions cloud ou login via les réseaux sociaux par exemple), peut gérer un Identity Linking (voir à ce sujet le chapitre 8.1.3.7).
Dès qu'un Broker se trouve entre le RP et l'IdP, le RP ne peut plus exécuter lui-même l'Identity Mapping en fonction des identificateurs obtenus du Broker que dans certaines conditions. En cas de besoin, le RP devrait déléguer l'Identity Mapping au Broker.

8.1.3.3 Obtention de l'User Consent

Processus: Confirmer l'E-Identity

Il existe généralement deux possibilités distinctes d'obtenir l'User Consent. Il faut en appliquer une:

- **Sans valeurs d'attribut**: le Broker obtient l'User Consent auprès des AP **avant** la requête d'attributs. Le sujet peut ainsi accepter la quantité d'attributs, mais ne reçoit aucune information concernant les valeurs d'attribut.
- **Avec valeurs d'attribut**: le Broker obtient l'User Consent auprès des AP **après** la requête d'attributs. Le sujet reçoit les informations complètes concernant les valeurs d'attribut.

Le sujet doit par principe valider la quantité définie d'attributs pour une ressource au moins une fois. Il est possible d'enregistrer quand quelle quantité d'attributs a été validée pour quelle ressource du sujet. Le sujet peut ainsi accéder à une ressource sans avoir à donner à nouveau son consentement[16].

Dès que la ressource nécessite une autre quantité d'attributs, le sujet doit avoir la possibilité de donner à nouveau son consentement.

Le consentement peut être obtenu à partir de plusieurs composantes pour le sujet. La communauté doit décider quel composant l'User Consent reprend, ainsi que la manière dont l'User Consent sera présenté au sujet et sous quelle forme le consentement sera enregistré.

Il est également possible de demander des attributs lorsque le sujet n'est (plus) impliqué (offline access). Il faut pour ce faire obtenir le consentement du sujet concernant l'opération. Ex.: dans le cas de l'envoi d'une newsletter, l'adresse e-mail actuelle du sujet est demandée avant que l'e-mail soit envoyé.

Dans le cas des Entreprise Attributes (voir glossaire IAM [1]), qui ont été implicitement validés par le sujet (parce que, faute de quoi, le sujet ne peut accomplir sa tâche d'office par exemple), aucun consentement du sujet n'est requis.

[16] Si le consentement ne peut être enregistré, le sujet doit le redonner à chaque demande.

8.1.3.4 Transformation de confirmations d'attribut

Processus: Confirmer l'E-Identity

Le contexte, dans lequel un attribut revêt une importance particulière pour une application, doit être prescrit par la communauté. Les participants doivent s'entendre sur le contenu et la sémantique d'une information d'attribut.
Il existe plusieurs approches différentes visant à éviter que les informations d'attribut ne perdent de leur importance dans un environnement d'Identity Federation et à permettre qu'elles soient correctement préparées par un AP et lues et interprétées correctement par un RP.
Lorsqu'une transformation de confirmations d'attribut se révèle nécessaire, au moins l'une des approches suivantes doit être mise en œuvre:

- ***Rapprochement par un schéma commun*** (schéma LDAP par exemple). Aucune logique de transformation à cet égard.
- Transformation d'un attribut entre l'éditeur et le consommateur. La communauté prescrit dans quel cadre une transformation peut ou doit avoir lieu, sans altérer l'importance d'un attribut.
    - ***Transformation du nom d'attribut:*** sur la voie de la transmission, le nom d'un attribut doit être adapté selon des règles précises par une instance dûment habilitée (‚title' → ‚hasFunction' par exemple)
    - **Transformation de la valeur d'attribut:** sur la voie de la transmission, la valeur d'un attribut doit être adaptée selon des règles précises par une instance dûment habilitée, sans altérer l'importance. (un transfert de date de '02.14PM' → '14:14' ou une décomposition: ‚Adresse=Bernstrasse 42' → ‚Strasse=Bernstrasse' + ‚Hausnummer=42' par exemple).

8.1.3.5 Attribut Aggregation

Processus: Confirmer l'E-Identity

Le terme *Attribute Aggregation* désigne le processus consistant à demander des attributs concernant une E-Identity connue auprès de plusieurs sources et à les compiler. Peu importe alors qu'un AP soit également IdP ou non. Ce processus peut être utilisé.

8.1.3.6 Transformation de protocole

Processus: Confirmer l'E-Identity
Les systèmes d'Identity Federation impliquant un Broker séparent la partie fournisseurs d'informations des consommateurs d'informations. Le même protocole, mais également des protocoles différents peuvent être appliqués sur les deux sections de protocole (P1, P2) (SAML ↔ SAML ou OIDC ↔ OIDC par exemple).
Lorsque des protocoles sont utilisés sur les sections de protocole (P1, P2) dans un système d'Identity Federation impliquant un Broker, le Broker doit les traduire resp. les adapter. Ceci dépend des propriétés et des capacités des partenaires de communication périphériques.

8.1.3.7 Identity Linking

Processus: Définir l'E-Identity

L'administration des E-Identities associées (LinkedID) via l'Identity Linking est un composant du processus *Définir l'E-Identity*. Cette opération peut être effectuée par un sujet lui-même

ou par une organisation qui y est habilitée. En reliant les E-Identities par le sujet, il doit être garanti que le sujet s'authentifie de telle manière que le niveau d'authentification corresponde à la plus haute qualité des E-Identities associées.
L'Identity Linking contient l'activation/la désactivation d'un lien entre deux E-Identities déjà existantes et les attributs qui y sont associés, mais pas la création, l'échange et la suppression d'attributs.

Les E-Identities peuvent être associées de différentes manières. Quand un Identity Linking est utilisé, il faut utiliser l'un des types suivants:

- Un identificateur commun (shared identifier).
- Protocole (Linking Protocole) pour relier les E-Identities. De manière caractéristique, le lien figure dans un tableau de linking vers le Broker.

8.1.3.8 Enregistrement Step-Up

Processus: Définir l'E-Identity

L'enregistrement Step-Up permet d'évaluer une E-Identity en termes de qualité. Pour ce faire, le processus 'Définir l'E-Identity' est à nouveau amorcé et le sujet est identifié par un RA selon le niveau de confiance souhaité et ses moyens de preuve sont à nouveau vérifiés. D'autres facteurs d'authentification peuvent venir s'y greffer en tant que moyen d'authentification et/ou d'autres moyens d'authentification peuvent être émis pour le sujet.
Un enregistrement Step-Up doit avoir l'un des résultats suivants:

- L'E-Identity atteint un niveau de confiance accrue après un enregistrement réussi.
- Le sujet contient une autre E-Identity qui correspond au niveau de confiance supérieur.

8.1.3.9 Metadata Management

Processus: Diriger la direction IAM

Un Metadata Management (gestion des métadonnées) doit être pris en charge par la direction de l'Identity Federation. Elle décide la manière dont les métadonnées sont structurées dans le système IAM et par quelles interfaces les métadonnées sont transmises aux participants.
Les partenaires participants devraient avoir la possibilité de se procurer des métadonnées des interfaces spécifiques. Par ailleurs (en fonction des exigences du système IAM), la direction devrait offrir des possibilités de saisir les métadonnées (un RP peut par exemple saisir une E-Ressource et décider de la qualité devant être exigée pour l'authentification et les attributs).

8.2 Broker Double Blinding

Dans le cas du «Broker Double Blinding», les sections de protocole doivent être totalement séparés les unes des autres. Le Broker est le point final du protocole pour les deux sections de protocole. Les RP et IdP/AP ne se connaissent pas directement. Ceci implique pour les participants de faire pleinement confiance au Broker.

Procédure: le RP souhaite faire authentifier le sujet avec un niveau de confiance précis et envoie une demande correspondante au Broker. Le Broker doit contrôler la demande et montre au sujet (sous réserve de contrôle réussi) les IdP qui remplissent les exigences de la demande. Après que le sujet a choisi un IdP, le sujet doit être transmis à l'IdP choisi. Le sujet doit être authentifié par l'IdP.
Après l'authentification du sujet, le Broker doit recevoir une confirmation d'authentification (et les éventuelles confirmations d'attribut provenant de la même source ou d'autres sources) signées par l'IdP. Le Broker doit valider la signature. Une fois la vérification réussie, le Broker doit supprimer la/les signature(s) d'origine et, de nouveau, signer lui-même la confirmation d'authentification (et le cas échéant la confirmation d'attribut) avant de l'envoyer.

Avant de signer, le Broker peut effectuer d'autres activités:

- Identity Mapping & transformation de la confirmation d'authentification.
  Pour rendre difficile toute corrélation des E-Identities pour les RP, un identificateur technique aléatoire unique ou un identificateur technique lié au RP devrait être utilisé pour chaque RP (voir chapitre 5.3.3 et 5.3.2).
- Attribute Aggregation & transformation des confirmations d'attribut
- Transformation de protocole

Les confirmations d'authentification ou d'attributs doivent être transmises au RP selon le chapitre 8.1.1.1.

8.2.1 Affectation des processus

Dans le cas du «Broker Double Blinding», le Broker peut assumer de nombreuses tâches. Parmi celles-ci figurent le Metadata Management, le Trust Management, Access Definition, Discovery, Transformation des données d'identité, Attribute Aggregation, Attribute Transformation, Transformation de protocole et Autoriser l'entrée. Il semble opportun que la validation des attributs par le sujet (User Consent) soit également confiée au Broker. A titre d'alternative, l'User Consent peut être pris en charge par l'IdP et (si possible) par l'AP.

Identity Linking et Identity Mapping peuvent être pris en charge par le Broker, si cela est nécessaire et demandé.

La charge d'intégration pour le RP pour ce type de Broker est très faible, car il doit définir uniquement les droits d'accès au cours de la période de définition et autoriser l'accès au moyen des droits d'accès au cours de la période d'exécution.

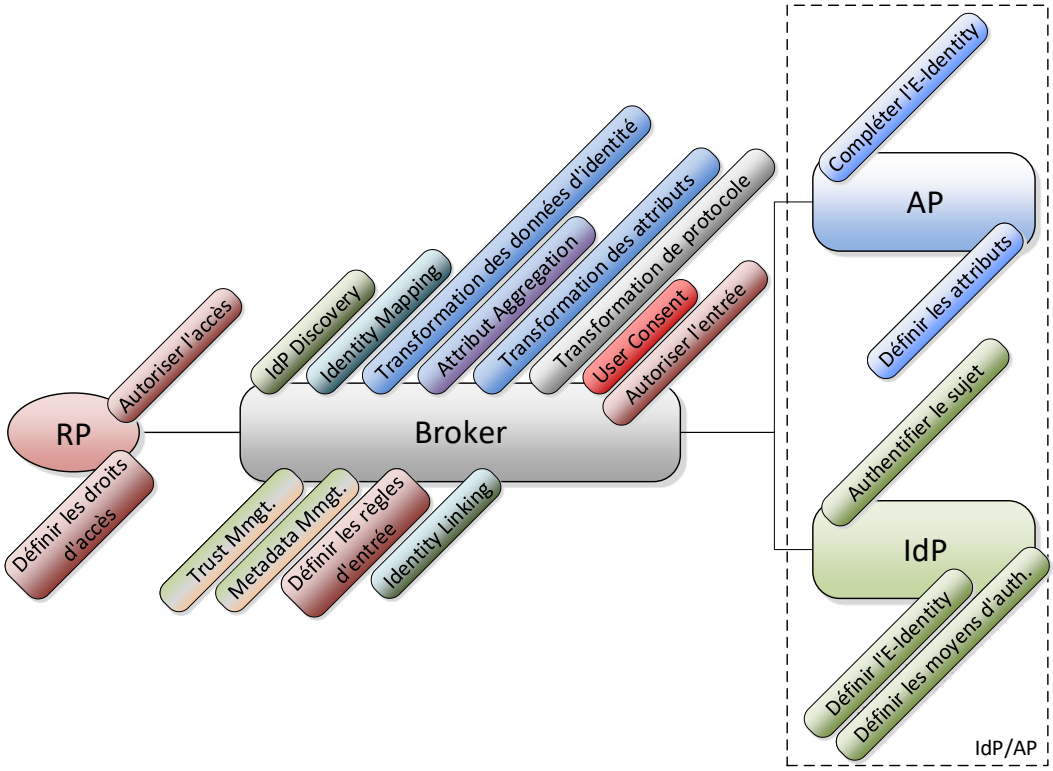

Figure 14: Affectation de processus Broker Double Blinding

8.3 Sources ouvertes Broker

En fonction de l'exigence, il est souhaitable que le RP souhaite recevoir plus d'informations con-cernant les confirmations d'authentification et d'attribut.

Dans le cas de ce modèle, les sources de l'authentification et des attributs doivent être divul-guées au RP. Le RP peut suivre par quel IdP le sujet a été authentifié et quel IdP/AP ou AP constitue la source de l'attribut.

Le déroulement est semblable à la description du Double Blinding selon le chapitre 8.2. De plus, le Broker doit insérer la source d'authentification et/ou des attributs dans les confirma-tions (comme attribut par exemple) dans la section de protocole P1. Le RP peut ainsi, au choix, suivre par quel IdP a été authentifié le sujet et de quel AP proviennent les attributs

Dans le cas où les sources des attributs devraient être vérifiables, le Broker doit transmettre la confirmation d'attributs d'origine au RP. Le RP peut ensuite vérifier la véracité et l'authenti-cité de la confirmation d'attribut au moyen de la signature. Dans ce cas de figure, le Broker n'a pas la possibilité de transformer les attributs.

8.3.1 Affectation des processus

Dans le cas où seules les sources peuvent être tendues visibles à l'aide d'attributs, l'affecta-tion des processus correspond au chapitre 8.2.1.

La Figure 15 présente l'affectation des processus et des activités lorsque seule la confirma-tion de l'attribut doit être **vérifiable**. A la différence du «Broker Double Blinding», le Broker n'a pas la capacité de transformer les attributs et peut, le cas échéant, être repris par le RP.

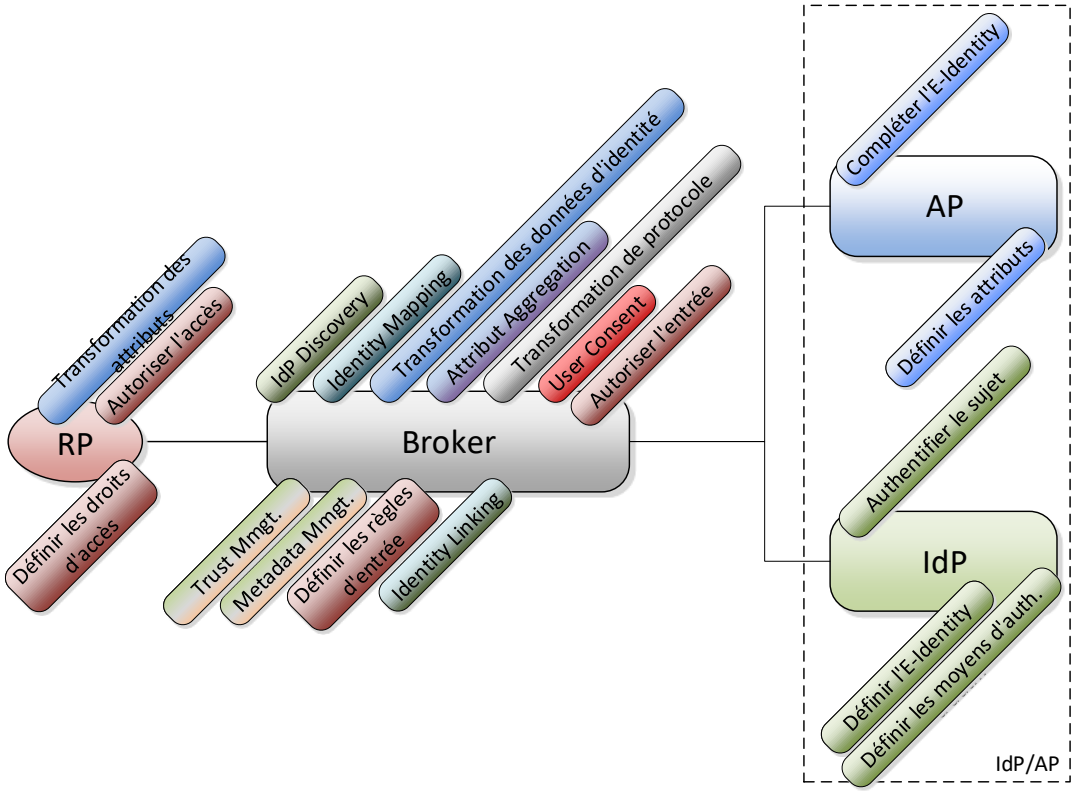

Figure 15: Affectation Sources ouvertes Broker

8.4 Protection de la confidentialité Broker

La protection de la confidentialité consiste à ne pas faire confiance au Broker concernant la consultation et la transformation des informations sur les attributs. C'est la raison pour laquelle les confirmations d'attribut doivent être transmises par l'AP sous une forme confidentielle pour le RP. Le Broker ne doit pas se trouver en mesure de voir les valeurs d'attribut et de les transformer.[17]

La transmission de la confirmation d'authentification s'effectue comme pour le modèle «Sources ouvertes Broker».

Les répercussions sur les participants et les processus sont les suivantes:

- Afin de préserver la confidentialité des attributs par rapport au Broker, il y a deux possibilités au choix. Il faut en appliquer une:
  - Les attributs sont cryptés par l'AP pour le RP.
  - Le RP reçoit du Broker des références auprès desquelles les attributs peuvent être directement prélevées (via la section de protocole P3).
- Dans le cas où les attributs sont transmis cryptés au RP via le Broker, l'AP doit savoir pour quel RP les attributs sont cryptés. Ceci peut se faire via les métadonnées ou avoir lieu durant la période d'exécution.
- Le consentement du sujet concernant la transmission d'attributs (User Consent) doit être obtenu soit par le Broker, soit par l'IdP/AP. Dans le cas où c'est le Broker qui

[17] Dans le cas où la confirmation d'authentification ne devrait pas être visible par le Broker non plus, le Broker ne peut discerner les processus IdP Discovery et Administration des métadonnées, car il ne peut pas de lui-même reconnaître l'identité du sujet.

s'en charge, ce dernier doit obtenir le consentement du sujet avant que les attributs soient sollicités auprès de l'AP avec protection de la confidentialité. Le sujet ne voit toutefois que les noms d'attribut, pas les valeurs d'attribut.

Lorsque des attributs avec protection de la confidentialité sont transmis entre l'AP et le RP, il n'est en principe plus possible de maintenir un Double Blinding, car l'expéditeur (AP) peut à coup sûr déterminer l'identité des destinataires (RP). Pour que cela reste possible, l'on peut par exemple utiliser des certificats anonymisés. L'AP ne peut alors plus reconnaître le RP au moyen des informations dans le certificat et le Double Blinding être ainsi préservé. Cette forme, comme d'autres formes de préservation du Double Blinding, en dépit de la protection de la confidentialité, est relativement fastidieuse à mettre en œuvre (contradiction avec l'exigence 224-LE-3) et ne sont, à ce titre, pas traitées plus avant dans la présente norme.

Dans le cas de la protection de la confidentialité Broker, il faut éviter un Blinding unilatéral. Soit l'on doit divulguer à qui les AP transmettent les données et, pour les RP, de qui proviennent les données, soit l'AP et le RP ignorent tous deux le destinataire des données ou la source des données.

Dans tous les cas, le Broker n'a aucune possibilité de transformer les attributs.

8.4.1 Affectation des processus

Dans le cas où les attributs sont transmis cryptés via le Broker, les processus doivent être affectés comme selon la Figure 16.

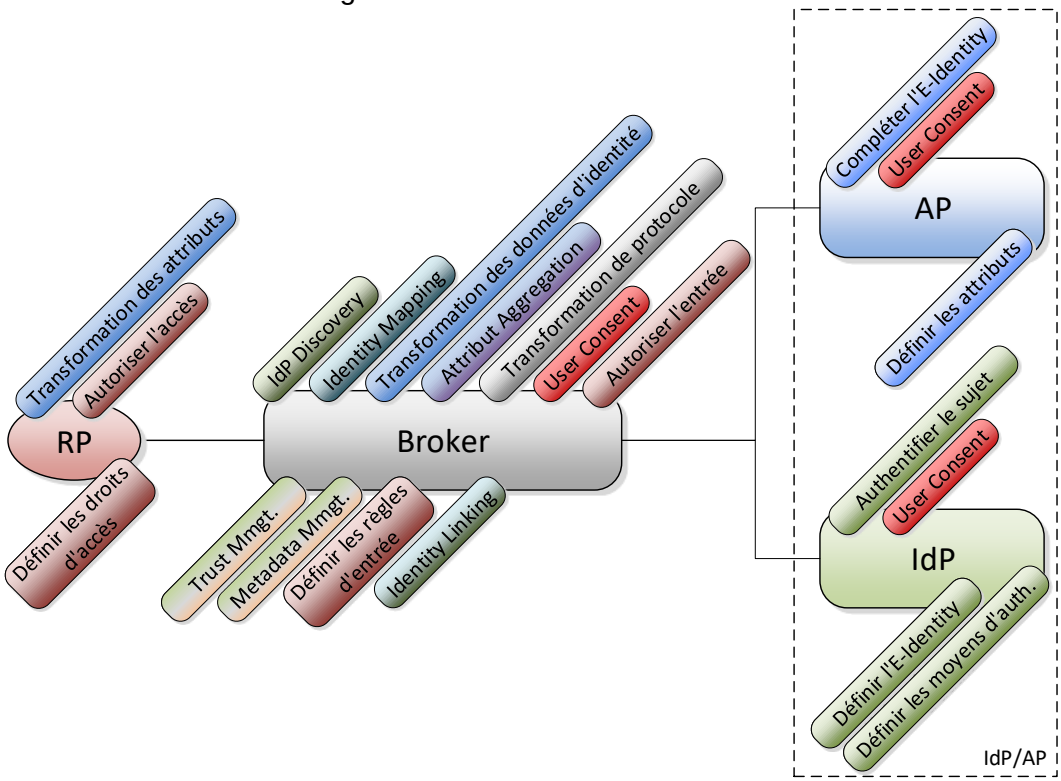

Figure 16: Protection de la confidentialité Broker (attributs cryptés)[18]

[18] «User Consent» doit être effectué soit par le Broker soit par l'IdP et l'AP.

Si des références sont transmises au RP, l'agrégation des attributs doit être prise en charge par le RP (voir Figure 17).

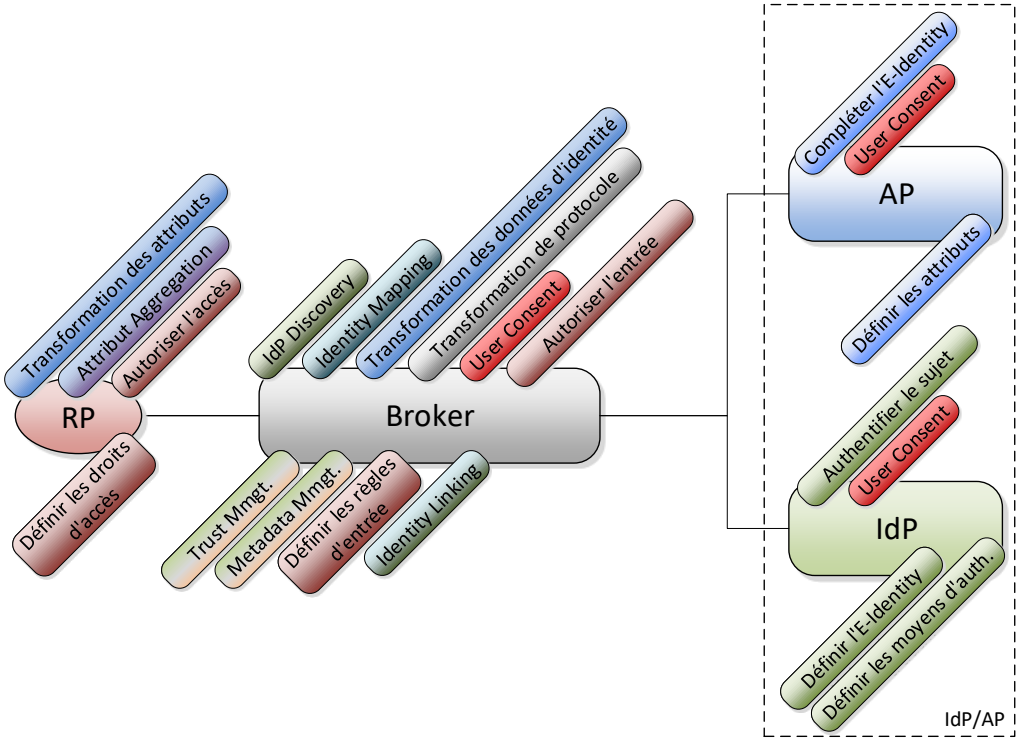

Figure 17: Protection de la confidentialité Broker (référence aux attributs)[19]

[19] «User Consent» doit être effectué soit par le Broker soit par l'IdP ou l'AP.

9 Application de la norme eCH-0170 aux Identity Federations impliquant un Broker

La norme eCH-0170 [3] définit un modèle de qualité pour l'authentification d'un sujet pour des systèmes IAM simples, composés de l'IdP et du RP (sans Broker). Les sections suivantes décrivent, pour chacun des modèles partiels, les répercussions sur un modèle de qualité de l'intégration d'un Broker.

9.1 Niveau de confiance de l'authentification (NDCA)

Dans un système IAM impliquant un Broker, un sujet est aussi toujours authentifié par un IdP. C'est la raison pour laquelle, lors de la détermination du niveau de confiance, les critères *Moyen d'authentification* et *Certification du moyen d'authentification* doivent être appliqués aux IdP utilisés.

Concernant le critère *Réauthentification*, le Broker doit être pris en compte. Si le Broker est responsable des User Sessions, il doit amorcer la réauthentification, lorsque la durée de la session d'authentification conformément à la version a été dépassée. Dans ce cas précis, le Broker doit solliciter une nouvelle authentification auprès de l'IdP selon la version.

9.2 Niveau de confiance de l'enregistrement (NCDE)

Concernant la détermination des niveaux de confiance de l'enregistrement, l'IdP utilisé (resp. la RA de l'IdP) est étudié. L'influence du Broker sur la qualité de l'enregistrement n'existe que s'il permet un Identity-Linking.

9.3 Niveau de confiance du pilotage (NCDP)

Concernant la détermination du niveau de confiance du pilotage, tous les prestataires de services IAM impliqués (IdP y compris RA et Broker) sont pris en compte. Les prestataires de services IAM doivent remplir les critères d'un niveau afin d'être classés en conséquence. Le résultat global du niveau de confiance du pilotage correspond au plus petit niveau des prestataires de services pris en compte.

9.4 Niveau de confiance de la fédération (NDCF)

Les NDCF 1 et NDCF 2 peuvent être aisément atteints dans une Identity Federation avec un Broker. On considère que le Broker bénéficie toujours de la confiance concernant l'authentification. Il est donc le point final du protocole pour la signature ainsi que pour le cryptage.

Les confirmations d'authentification sont toujours signées (critère «Authenticité de la confirmation d'authentification»). L'IdP signe la confirmation d'authentification pour le Broker. Le Broker vérifie la signature et signe à nouveau la confirmation d'authentification pour le RP (la signature de l'IdP n'est pas transmise). Le RP contrôle ensuite la signature.

Dans le cas où la confirmation d'authentification est cryptée (critère «protection de la confidentialité de la confirmation d'authentification»), l'IdP la crypte pour le Broker. Le Broker décrypte la confirmation d'authentification et la crypte à nouveau pour le RP.

Le NDCF 3, qui requiert la mise en œuvre du principe[20] de Holder-of-Key, pose problème. Dès lors que le NDCF 3 se révèle nécessaire, le Broker ne devrait plus procéder qu'à l'IdP-Discovery. Le RP amorcerait alors l'authentification directement auprès de l'IdP. Il convient à cet égard de veiller ce qu'il n'y ait plus aucun Blinding. L'IdP connaît le RP et le RP connaît l'IdP. Un éventuel Identity Linking et Identity Mapping doivent éventuellement être effectués sur le RP. Le Broker ne peut pas transformer l'E-Identity.

[20] . La preuve de la clé (ou secret) devrait être contrôlée sur les deux sections de protocole (P1 et P2). Pour le sujet, cela impliquerait de devoir s'authentifier à trois reprises. Du point de vue de l'expérience utilisateur, une telle situation n'est pas souhaitable et devrait donc être évitée.

10 Exclusion de responsabilité - droits de tiers

Les normes élaborées par l'Association **eCH** et mises gratuitement à la disposition des utilisateurs ainsi que les normes de tiers adoptées, ont seulement valeur de recommandations. L'Association **eCH** ne peut en aucun cas être tenue pour responsable des décisions ou mesures prises par un utilisateur sur la base des documents qu'elle met à disposition. L'utilisateur est tenu d'étudier attentivement les documents avant de les mettre en application et au besoin de procéder aux consultations appropriées. Les normes **eCH** ne remplacent en aucun cas les consultations techniques, organisationnelles ou juridiques appropriées dans un cas concret.
Les documents, méthodes, normes, procédés ou produits référencés dans les normes **eCH** peuvent le cas échéant être protégés par des dispositions légales sur les marques, les droits d'auteur ou les brevets. L'obtention des autorisations nécessaires auprès des personnes ou organisations détentrices des droits relève de la seule responsabilité de l'utilisateur.
Bien que l'Association **eCH** mette tout en œuvre pour assurer la qualité des normes qu'elle publie, elle ne peut fournir aucune assurance ou garantie quant à l'absence d'erreur, l'actualité, l'exhaustivité et l'exactitude des documents et informations mis à disposition. La teneur des normes **eCH** peut être modifiée à tout moment sans préavis.
Toute responsabilité relative à des dommages que l'utilisateur pourrait subir par suite de l'utilisation des normes **eCH** est exclue dans les limites des règlementations applicables.

11 Droits d’auteur

Tout auteur de normes **eCH** en conserve la propriété intellectuelle. Il s'engage toutefois à mettre gratuitement, et pour autant que ce soit possible, la propriété intellectuelle en question ou ses droits à une propriété intellectuelle de tiers à la disposition des groupes de spécialistes respectifs ainsi qu'à l'Association **eCH** pour une utilisation et un développement sans restriction dans le cadre des buts de l'association.
Les normes élaborées par les groupes de spécialistes peuvent, moyennant mention des auteurs **eCH** respectifs, être utilisées, développées et déployées gratuitement et sans restriction.
Les normes **eCH** sont complètement documentées et libres de toute restriction relevant du droit des brevets ou de droits de licence. La documentation correspondante peut être obtenue gratuitement.
Les présentes dispositions s’appliquent exclusivement aux normes élaborées par **eCH**, non aux normes ou produits de tiers auxquels il est fait référence dans les normes **eCH**. Les normes incluront les références appropriées aux droits de tiers.

Annexe A – Références & bibliographie

[1] A. Laube-Rosenpflanzer, A. Spichiger, M. Kunz, T. Kessler, and A. Müller, “eCH-0219 IAM Glossar,” version 1.0, 2019 [Online]. Available: http://www.ech.ch/dokument/b1a76129-0c3e-4021-a6ff-c3123554fd95

[2] A. Laube-Rosenpflanzer, A. Spichiger, M. Kunz, T. Kessler, T. Gruoner, and M. Heerkens, “eCH-0107 Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM),” version 3.0, 2019 [Online]. Available: https://www.ech.ch/dokument/167ccf46-b902-4b58-88f2-eed05ed58c05

[3] A. Laube-Rosenpflanzer, G. Hassenstein, M. Kunz, T. Gruoner, A. Spichiger, and T. Selzam, “eCH-0170 Qualitätsmodell zur Authentifizierung von Subjekten,” version 2.0, 2017 [Online]. Available: https://www.ech.ch/alfresco/s/ech/download?nodeid=54cce841-215f-4887-9382-25620dcbf9b1

[4] A. Laube-rosenpflanzer, G. Hassenstein, S. Agosti, M. Vinzens, U. Pfenninger, and D. Leiser, “eCH-0168 SuisseTrustIAM technische Architektur und Prozesse,” version 1.0, 2014 [Online]. Available: https://www.ech.ch/alfresco/s/ech/download?nodeid=31499686-813d-4589-b794-11015fbf2059

[5] “Stork 2.0.” [Online]. Available: https://www.eid-stork2.eu/

[6] Parlement et Conseil de l'Union européenne, «RÈGLEMENT (UE) no. 910/2014 DU PARLEMENT ET DE CONSEIL EUROPÉEN du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, (eIDAS),» 2015.

[7] S. K. S. Paul A. Grassi, James L. Fenton, Justin P. Richer, “DRAFT NIST Special Publication 800-63C,” 2017 [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63c.html. [Accessed: 22-Jun-2017]

[8] Département fédéral de la justice et de la police DFJP, «Loi E-ID.» [Online]. Available: https://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/e-id.html

[9] L’Assemblée fédérale de la Confédération suisse, «LPD: Loi fédérale sur la protection des données du 19 juin 1992 (état le 1 janvier 2014), 235.1,» version 1992, pp. 1–24, 2014 [Online]. Available: https://www.admin.ch/opc/fr/classified-compilation/19920153/201401010000/235.1.pdf

[10] S. Cantor, J. Kemp, R. Philpott, and E. Maler, “Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0,” *OASIS Stand.*, 2005 [Online]. Available: https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[11] K. Kane, K. Easterbrook, G. Zaverucha, and C. Paquin, “U-Prove - Microsoft Research.” [Online]. Available: https://research.microsoft.com/en-us/projects/u-prove/

[12] J. Camenisch and M. Dubovitskaya, “IBM Research - Zurich, Identity Mixer.” [Online]. Available: https://www.zurich.ibm.com/identity_mixer/

Annexe B – Collaboration & vérification

Gruoner Torsten	UPIC
Emmenegger Adrian	SwissSign
Hangartner Nick	SwissSign
Hassenstein Gerhard	ICTM / Haute école spécialisée de Berne
Hefti Esther	Chancellerie d'Etat du canton de Zurich
Kunz Marc	ICTM / Haute école spécialisée de Berne
Laube-Rosenpflanzer Annett	ICTM / Haute école spécialisée de Berne
Leimer Bojan	ICTM / Haute école spécialisée de Berne
Voge Mario	SwissSign

Annexe C – Abréviations et glossaire

AP	Attribute Provider
G2B	Government to Business
G2C	Government to Citizen
G2G	Government to Government
IAM	Identity and Access Management
IdP	Identity Provider
IdP/AP	Identity Provider/Attribute Provider
LDAP	Lightweight Directory Access Protocol
OIDC	OpenID Connect
RP	Relying Party
SAML	Security Assertion Markup Language
SLO	Single Logout
SOA	Service oriented architecture
SSO	Single Sign-On
TLS	Transport Layer Security
URI	Uniform Resource Indicator
NCDA	Niveau de confiance de l'authentification
NCDF	Niveau de confiance de la fédération
NCDE	Niveau de confiance du pilotage
NCDP	Niveau de confiance du pilotage

Annexe E – Liste des illustrations

Figure:1 Classification de la norme eCH-0224 5
Figure 2: Identity Federation simple (directe) 8
Figure 3: Structure grossière d'un système d'Identity Federation impliquant un Broker 9
Figure 4: Arbre de décision pour la sélection de modèles d'Identity Federation 26
Figure 5: Broker Double Blinding 29
Figure 6: Sources ouvertes Broker 30
Figure 7: Protection de la confidentialité Broker 31
Figure 8: Sections de protocole 33
Figure 9: Section de protocole P1 – Front-Channel 34
Figure 10: Section de protocole P1 - Back-Channel 35
Figure:11 Section de protocole P2 – Front-Channel 36
Figure 12: Section de protocole P2 - Back-Channel 36
Figure 13: Section de protocole P3 37
Figure 14: Affectation de processus Broker Double Blinding 43
Figure 15: Affectation Sources ouvertes Broker 44
Figure 16: Protection de la confidentialité Broker (attributs cryptés) 45
Figure 17: Protection de la confidentialité Broker (référence aux attributs) 46

Annexe F – Liste des tableaux

Tableau 1: Exigences imposées au système IAM 19
Tableau 2: Exigences du bénéficiaire de prestations 21
Tableau 3: Exigences du prestataire de services 23
Tableau 4: Exigences du Stakeholder: Direction 23
Tableau 5: Conformité aux exigences d'une Identity Federation n'impliquant pas de Broker. 28
Tableau 6: Réalisation des exigences du «Brokers Double Blinding» 29
Tableau 7: Réalisation des exigences des «Sources ouvertes Broker» 30
Tableau 8: Réalisation des exigences du «Protection de la confidentialité Broker» 31

Annexe G – Modèles de Tokenbased Identity Federation impliquant un Broker

Les modèles d'Identity Federation Token-based impliquant un Broker offrent une protection maximale de la vie privée d'un sujet.
Dans le cadre d'une procédure en ligne classique (SAML et OIDC par exemple), l'identification et des attributs sont rapidement communiqués au moyen d'un Software-Token. A l'inverse, les méthodes dites ‚token-based', ou encore ‚claims-based' voire ‚credential-based' reposent sur le principe consistant à enregistrer ou à sauvegarder les données sensibles dans l'environnement du sujet. L'exemple le plus parlant à cet égard est le ‚*neue deutsche Personalausweis*' (nPA, la nouvelle carte d'identité allemande). Les données d'identification des personnes sont fournies par une source officielle et enregistrées sur la carte d'identité électronique. Un processus de sélection doit permettre au prestataire de services (Relying Party) une autorisation par rapport à la carte. L'utilisateur est toujours intégré dans un tel processus de sélection, en ayant la pleine maîtrise des cartes des données sélectionnées sur la carte. La carte d'identité électronique joue ainsi le rôle d'Identity Provider personnel décalé sous forme de Hardware-Token, qui contient des données persistantes d'identification de la personne. Microsoft U-Prove [11] et Identity-Mixer (Idemix en abrégé) par IBM [12] sont deux autres variantes de systèmes ‚token-based' d'Identity Federation, axés pour leur part sur la protection de la sphère privée du sujet.