eCH-0174 – Identity Federations impliquant un Broker – Implémentation avec SAML 2.0

Nom	Identity Federations impliquant un Broker – Implémentation avec SAML 2.0
eCH-nombre	eCH-0174
Catégorie	Norme
Degré de maturité	Implémenté
Version	2.0.0
Statut	Approuvé
Date de décision	2021-11-24
Date de publication	2021-11-24
Remplace la version	1.0 – Major Change
Conditions préalables	eCH-0224 v1.0
Annexes	-
Langues	Allemand (original), français (traduction)
Auteurs	Groupe spécialisé IAM Annett Laube-Rosenpflanzer, BFH, annett.laube@bfh.ch Gerhard Hassenstein, BFH, gerhard.hassenstein@bfh.ch Sven Bracklo, BFH, sven.bracklo@bfh.ch
Éditeur / 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

La présente norme décrit l'implémentation technique des modèles d'Identity Federation impliquant un Broker tirés de la norme eCH-0224 en utilisant SAML 2.0, parallèlement à la norme eCH-0225 qui en décrit l'implémentation avec OIDC. L'objectif est de garantir l'interopérabilité, en particulier pour les Relying Parties dans les scénarios G2G, G2B et G2C. Les services et protocoles nécessaires sont décrits à cette fin. La norme s'adresse en priorité aux architectes informatiques et aux développeurs des composants de l'Identity Federation.

Sommaire

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.

Notation

Les mots clé DOIT (MUST), NE DOIT PAS (MUST NOT), REQUIS (REQUIRED), DEVRAIT (SHOULD), NE DEVRAIT PAS (SHOULD NOT), RECOMMANDÉ (RECOMMENDED), PEUT (MAY) et FACULTATIF dans ce document doivent être interprétés selon la description faite dans la RFC IETF 2119 [1].

Les préfixes énumérés dans ce document référencent les espaces de noms XML suivants:

Préfixe	Espace de nom XML
saml:	urn:oasis:names:tc:SAML:2.0:assertion
samlp:	urn:oasis:names:tc:SAML:2.0:protocol
md:	urn:oasis:names:tc:SAML:2.0:metadata
ds:	http://www.w3.org/2000/09/xmldsig#
mdattr:	urn:oasis:names:tc:SAML:metadata:attribute

Tableau 1: Préfixes et espaces de nom XML référencés

1 Introduction

1.1 Statut

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

1.2 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 eCH-029 glossaire IAM [2] chapitre 2.62). Les autorités délèguent alors l'authentification et la confirmation d'attributs à différents prestataires de services IAM. La délégation est fondée sur les accords organisationnels/architecturaux et techniques ou les législations/règlementations.

Dans la norme eCH-0224 [3], la place réservée aux systèmes d'Identity Federation impliquant un Broker a été restreinte aux trois modèles qui suivent, sur la base d'exigences plus rigoureuses de cyberadministration ainsi que des exigences de protection de la sphère privée des sujets:

- Broker Double Blinding,
- Broker Sources ouvertes
- Broker Protection de la confidentialité.

La présente norme décrit la mise en œuvre de ces modèles au moyen de SAML 2.0 [4]. La mise en œuvre avec OIDC [5] a déjà été décrite dans la norme eCH-0225 [6].

1.3 Champ d'application

La norme décrit la mise en œuvre des modèles d'Identity Federation impliquant un Broker tirés de la norme eCH-0224 [3]. Il s'agit d'une directive portant sur l'implémentation des interfaces et protocoles nécessaires pour les différents composants de l'Identity Federation afin de garantir l'interopérabilité entre les différents prestataires.

L'objectif est ici de garantir **l'interopérabilité** entre les différents composants des Identity Federations impliquant un Broker, en particulier pour les Relying Parties dans les scénarios G2G, G2B et G2C. Les interfaces et protocoles nécessaires pour chaque composant (RP, Broker, IdP/AP) sont définis, et l'accent est mis en particulier sur les adaptations et extensions nécessaires de SAML.

1.4 Classification

La norme eCH-0107 [7] 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 four-

nissent des informations complémentaires. Ces derniers peuvent être pertinents pour plus d'un concept. Les modèles de qualité et de maturité représentés ici sont des exemples de document auxiliaire. La liste de documents auxiliaires n'est pas exhaustive.

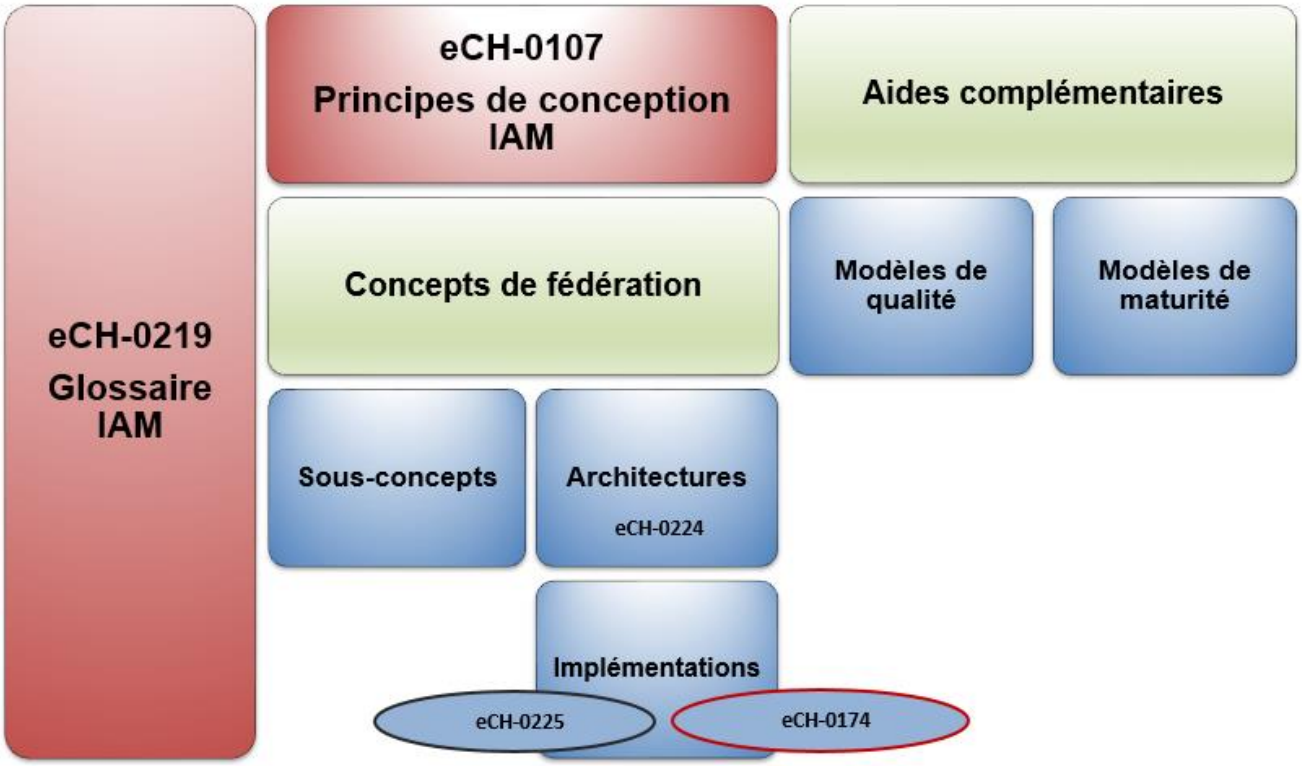

Figure 1: Classification de la norme eCH-0174 v2.0.0

Alors que la version V1.0 de la présente norme se contentait de décrire l'implémentation du modèle STIAM, la version V2.0.0 couvre aussi l'implémentation de modèles d'Identity Federations impliquant un Broker tirés de la norme eCH-0224 [3] sur la base technologique de SAML 2.0 [4]. Seules les variantes déjà mises en œuvre dans la pratique y sont décrites.

La mise en œuvre des modèles d'Identity Federations de la norme eCH-0224 [3] avec OIDC [5] est décrite dans la norme eCH-0225 [6].

Dans la version 2.0.0, toute la terminologie STIAM a ensuite été systématiquement remplacée par celle utilisée dans la norme eCH-0224 [3]. La version actualisée de la présente norme ayant notamment pour objectif l'indépendance vis-à-vis des normes STIAM (eCH-167 [8], eCH-0168 [9] et eCH-0169 [10]), certaines parties ont été reprises de eCH-0186 sous une forme actualisée (les détails sur les modifications par rapport à la version antérieure se trouvent en annexe D).

1.5 Groupe cible

La norme est destinée en priorité aux architectes et développeurs informatiques d'Identity Federations ou de composants individuels (RP, Broker, IdP/AP) de systèmes d'Identity Federations dans

la cyberadministration. Elle présuppose une connaissance des modèles de Broker de la norme eCH-0224 [3] ainsi que de solides connaissances de la norme SAML [4].

Le chapitre 2 définit les principes fondamentaux d'un système d'Identity Federation avec SAML 2.0 et devrait être étudié par les architectes informatiques et développeurs.

Le chapitre 3 définit les exigences supplémentaires pour une Identity Federation ayant pour base le SAML 2.0 dans la cyberadministration conformément aux normes eCH-0224 [3] et eCH-0107 [7]. Les directives pour les implémentations des SAML Messages sont décrites en parallèle.

Le chapitre 4 offre une vue d'ensemble des interfaces des modèles de Broker. Ce chapitre est également important pour les architectes informatiques et les développeurs.

Les chapitres 5, 6 et 7 définissent les interfaces des composants et s'adressent en priorité aux développeurs qui implémentent les interfaces correspondantes. Les interfaces à mettre en œuvre sont décrites pour chaque composant. La répétition des interfaces qui en résulte (chap. 5.1.1 Demande d'authentification au Broker et chap. 6.1.1 Demande d'authentification du Relying Party (RP) par exemple) a pour but de simplifier le flux de lecture pour chaque composant et de présenter les protocoles du point de vue du composant correspondant. Les architectes informatiques se doivent de lire ce chapitre afin de bien saisir les interactions entre les composants.

Le chapitre 8 décrit les métadonnées nécessaires pour une Identity Federation basée sur SAML 2.0 et revêt donc un intérêt particulier pour les architectes informatiques et les développeurs.

1.6 Délimitation

Cette norme décrit la mise en œuvre des exigences définies par la norme eCH-0224 [3] avec les moyens techniques actuels ayant pour base le SAML 2.0 [4]. Seuls les modèles d'Identity Federations impliquant un Broker «Double Blinding» et «Sources ouvertes» de la norme eCH-0224 sont pris en compte. Les autres modèles ou variantes de SAML 2.0 ne sont pas abordés.

1.7 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
1 Introduction	**Descriptif**
2 Identity Federation basée sur SAML	**Normatif**
3 Directives	**Normatif**
4 Interfaces des modèles de Broker	**Normatif**
5 Interfaces pour le Relying Party (RP)	**Normatif**
6 Interfaces pour Broker	**Normatif**
7 Interfaces pour Identity & Attribut Provider (IdP/AP)	**Normatif**
8 Métadonnées	**Normatif**
9 Sécurité	**Descriptif**

2 Identity Federation basée sur SAML

Ce document offre une description de la mise en œuvre des modèles d'architecture décrits dans la norme eCH-0224 [3] avec SAML 2.0 [4], avec les **restrictions** suivantes:

Les seuls processus décrits sont ceux correspondants à la période d'exécution.

1. Seules sont décrites les fonctionnalités minimales requises pour une solution STIAM opérationnelle avec SAML 2.0, c.à.d. toutes les exigences facultatives et les protocoles autres que SAML 2.0 Web Browser SSO Profile avec HTTP Binding (HTTP POST ou HTTP redirect) et SAML 2.0 Assertion Query/Request Profile ne sont pas pris en compte.

   Par conséquent, la description des protocoles Single Logout est également laissée de côté.[1]

2. On part du principe qu'un seul IdP/AP est utilisé comme source qui émet des confirmations d'authentification et (à titre facultatif) d'attributs. Bien que possible en théorie, la séparation de l'IdP et de l'AP se produit rarement dans la pratique.

3. Le Broker ne prend en charge aucun Identity Linking (voir également eCH-0224 [3], chap. 8.1.3.7). L'Identity Linking doit donc être mis en œuvre par le Relying Party, lorsque requis.

4. Il n'y a pas de communication par Back Channel de prévu, par exemple avec le SAML Artifact Resolution Protocol [11], car elle n'est pas utilisée dans la pratique ou que la mise en œuvre impliquerait une charge de travail démesurée.

5. Une mise en œuvre du SAML V2.0 Holder-of-Key Web Browser SSO Profile [12], qui n'est pas facilement applicable aux Identity Federations, n'est pas discutée plus avant dans la présente norme. Par conséquent, il n'est pas possible d'utiliser le niveau de confiance 4 selon la norme eCH-0170 v2.0 [13] pour la qualité de l'authentification des sujets.

2.1 Services SAML

Les services SAML, qui doivent ou devraient être pris en charge par les différents composants, afin de mettre en œuvre les protocoles décrits dans ce document, sont décrits dans la suite du document.

Les profils SAML [14] (Web Browser SSO et Assertion Query/Request) définissent les services suivants:

- **Single Sign-On Service (SSO):** le SSO Service décrit un point final du protocole SAML qui reçoit une Authentication Request (`<samlp:AuthnRequest>`).
- **Attribute Query Service (AQS):** l'Attribute Query Service décrit un point final de protocole SAML qui reçoit une demande d'attributs (`<samlp:AttributeQuery>`).
- **Assertion Consumer Service (ACS):** l'Assertion Consumer Service décrit un point final du protocole SAML qui reçoit la réponse (`<samlp:Response>`) à une Authentication Request

[1] Compte tenu de la complexité de la problématique du Single Logout (SLO) et du lien étroit avec le Session Handling, cette question devrait faire l'objet d'une norme dédiée.

(<samlp:AuthnRequest>) ou à une demande d'attributs (<samlp:AttributeQuery>).

Le tableau 2 présente une vue d'ensemble des services SAML qui doivent ou devraient être implémentés et par quels composants STIAM.

		Service SAML		
		SSO	**ACS**	**AS**
Composant	**Broker**	DOIT	DOIT	-[2]
	IdP et IdP/AP	DOIT	-	PEUT[3]
	Relying Party	-	DOIT	-

Tableau 2: Affectation des composants aux services SAML

2.2 Authentification avec et sans demande d'attributs via le service SSO

La figure 2 illustre le déroulement d'une authentification sans et avec demande d'attributs via le service SSO. La demande d'attributs est pilotée au moyen de l'AttributeConsumingServiceIndex dans l'Authentication Request (<samlp:AuthnRequest>).[4]

Un Relying Party envoie une Authentication Request (1) au service SSO du Broker. Celui-ci agit comme un proxy et envoie une nouvelle Request (2) au SSO de l'IdP authentifiant. L'IdP authentifie le sujet, génère une Response et la renvoie à l'ACS du Broker (3). La Response contient une confirmation d'authentification et, à titre facultatif, des attributs. Le Broker valide la Response de l'IdP et génère une nouvelle Response, qu'il renvoie au Relying Party requérant (4).

[2] Afin d'accroître l'interopérabilité de l'Identity Federation, l'AQS pour le Broker n'est pas pris en compte. Le Broker ne doit alors plus procéder à une Attribute Aggregation et reçoit les attributs de la source auprès de laquelle s'est authentifié l'utilisateur. Le Relying Party (RP) ne doit donc prendre en charge que l'Authentication Request/Response.

[3] Bien que destiné principalement à l'authentification avec une demande d'attributs via le service SSO AttributeConsumingServiceIndex, le service AQS peut également être utilisé afin de prendre en charge les IdP/AP qui utilisent des demandes d'attributs via le service <samlp:AttributeQuery> via SSO.

[4] À titre alternatif, un Extended AuthnRequest serait également possible, tel que précédemment pris en charge par SuisseID selon la spécification Suisse-ID chapitre 4.10.1.3. https://www.ech.ch/index.php/de/dokument/2aa44bb4-e35e-4266-9d69-c8e0d6721cb3. Faute d'IdP connu pour utiliser ce protocole, la présente norme n'en propose pas de description.

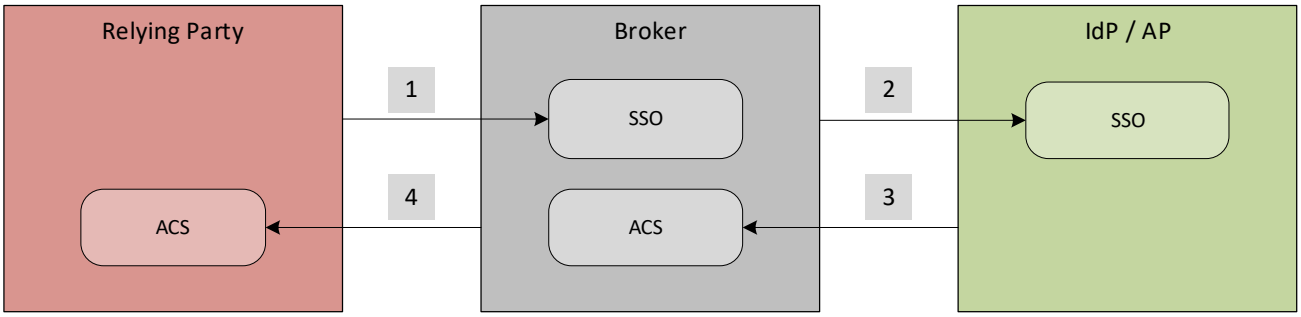

Figure 2: Interaction des services SAML pour une Authentication Request (avec et sans demande d'attributs)

2.3 Authentification avec demande d'attributs via le service AQS

La Figure 3 illustre le déroulement d'une Authentification avec demande d'attributs via l'AS de l'IdP/AP.

Un Relying Party envoie une Authentication Request (1) au service SSO du Broker. Celui-ci agit comme un proxy et envoie une nouvelle Request (2) au SSO de l'IdP authentifiant. L'IdP authentifie le sujet, génère une Response et la renvoie à l'ACS du Broker (3). Après que le Broker connaît l'identité du sujet, une demande d'attributs est envoyée à l'AS de l'IdP/AP (4). L'IdP/AP renvoie les attributs souhaités au Broker (5), qui peut les agréger ou les convertir, avant de les renvoyer au Relying Party (RP) requérant accompagnés de la confirmation d'authentification (6).

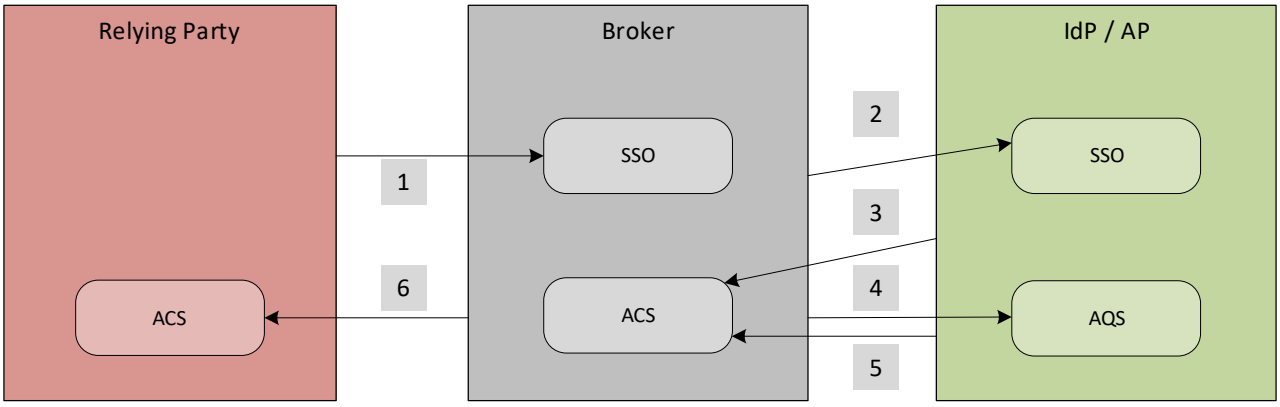

Figure 3: Interaction des services SAML pour une Authentication Request avec Attribute Query)

2.4 Signature et chiffrement

Les messages requérants (Requests) DOIVENT et les réponses (Responses) DEVRAIENT être signés par les composants concernés avant l'envoi (voir Figure 4). Une exception est le Response Message pour le modèle de Broker Sources ouvertes variante 1 (voir chapitre 4.2.2): L'Original Assertion étant reprise par l'IdP/AP, le Response Message DOIT être signé par le Broker.[5]

[5] Si la signature de la Response et de l'Assertion rend les choses plus complexes, elle n'est pas sans avantages en matière de sécurité, comme notamment la prévention de l'insertion dans ou la modification des messages (voir rubriques 6.1.3/6.1.5 in [19]).

L'Assertion contenue dans le message DOIT également être signée; en fonction du modèle de Broker, la signature originale est transmise par l'IdP/AP ou le Broker signe à nouveau l'Assertion (voir chapitre 4.2).

Pour que le RP puisse vérifier les signatures originales des Assertions, il doit disposer de la Public Key de l'IdP/AP. D'ordinaire, il l'obtient dans les métadonnées SAML du domaine[6] (souvent appelé également communauté) qui peuvent être distribuées via le Broker (voir chapitre 8.2). À titre exceptionnel, la Public Key peut également être envoyée comme partie de l'Assertion pour la période d'exécution.

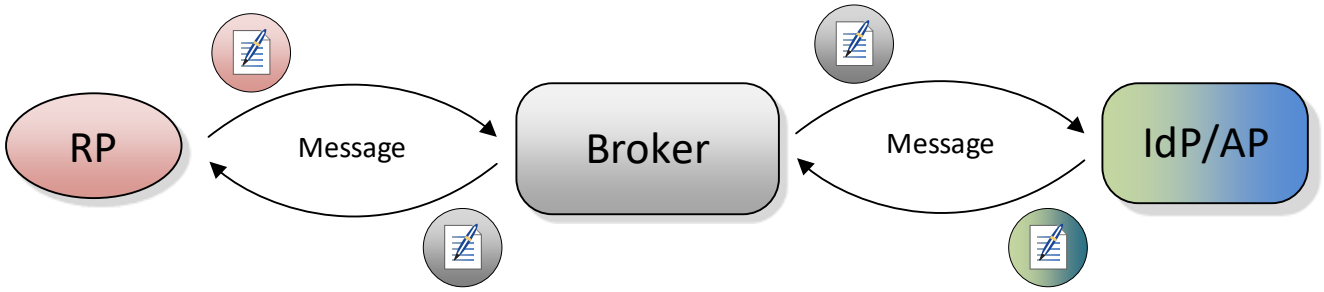

Figure 4: Vue d'ensemble de la signature des Messages entre les interfaces

En fonction des exigences de qualité, l'Assertion entre le Broker et le RP DEVRAIT être chiffrée. L'Assertion DOIT être chiffrée entre le Broker et l'IdP/AP.

Les SAML Messages et les SAML Assertions étant des structures XML, renvoi est fait concernant le chiffrement ou les signatures aux recommandations W3C concernant l'Encryption XML [15] et la signature XML [16]. La norme eCH-0091 [17] contient également des Best Practices.

2.5 Identificateurs techniques

Tel que défini dans la norme eCH-0224 [3] chapitre 5.3, un Relying Party DEVRAIT utiliser un identificateur technique lié (Persistent ID) lorsque le sujet doit être reconnu au moyen de cet identificateur (et non de ses attributs) en cas de nouvel accès. Dans le cas contraire, un identificateur aléatoire unique (Transient ID) DEVRAIT être utilisé. Les autres identificateurs techniques NE DEVRAIENT PAS être utilisés. Les informations concernant le type d'identificateur, que le RP souhaite utiliser, sont stockées dans les métadonnées (voir chapitre 8), notamment dans le SPSSODescriptor du RP,

Ces exigences ne sont pas sans incidence sur le Broker et l'utilisation des identificateurs techniques sur les itinéraires du protocole entre le RP et le Broker (P1) ainsi que le Broker et l'IdP/AP (P2) [7].

Si le RP requiert un identificateur aléatoire unique (Transient ID), le Broker DOIT également demander un tel identificateur à l'IdP/AP sélectionné ou créer lui-même un identificateur aléatoire unique dans l'éventualité où l'IdP/AP ne prendrait pas en charge les Transient ID.

Dans le modèle de Broker Double Blinding, le Broker NE DOIT en aucune circonstance transmettre

[6] Terminologie tirée du glossaire IAM [2]..

[7] Dans le cas où les attributs proviennent de sources multiples (ce qui est exclu dans le cas de cette norme), un recours à un identificateur réparti (Distributed ID) sur l'itinéraire du protocole P2 peut s'imposer.

au RP l'identificateur reçu.

2.6 User Consent

Avant que le Broker envoie une confirmation d'attributs au RP, le sujet DOIT valider les attributs. Voir Directive 6 – Validation des attributs (User Consent) (chapitre 3.1, p 24).

Du point de vue technique, il existe deux possibilités distinctes d'obtenir l'User Consent: *Sans valeurs d'attribut* ou *avec valeurs d'attribut* (voir eCH-0224 [3] chapitre 8.1.3.3). Le domaine statue sur la variante à utiliser et jette les bases juridiques nécessaires à cet effet. La Figure 6 et la Figure 7 illustrent les procédures correspondantes.

Pour la variante *Sans valeurs d'attribut.* le Broker DOIT obtenir l'User Consent **avant la demande** des attributs auprès de l'IdP/AP. Si l'utilisateur ne consent pas à la demande d'attributs, le protocole DOIT être interrompu à ce stade avec une annonce d'erreur correspondante au RP.

Pour la variante *Avec valeurs d'attribut,* le Broker DOIT obtenir l'User Consent **après la demande** des attributs auprès de l'IdP/AP. Si l'utilisateur ne consent pas à la demande d'attributs, le protocole DOIT être interrompu à ce stade avec une annonce d'erreur correspondante au RP.

2.7 Protocoles

La suite du document expose une vue d'ensemble des protocoles pour l'authentification **SANS** et **AVEC** demande d'attributs du sujet à l'IdP/AP. Ils sont basés sur le SAML Web Browser SSO Profile avec HTTP POST Binding ou Assertion Query/Request. Les sections de protocole et les messages utilisés sont décrits en détail au chapitre 4 et dans les chapitres des interfaces 5, 6 et 7.

Pour l'authentification avec demande d'attributs, le Broker DOIT prendre en charge les deux variantes avec AttributeConsumingServiceIndex et Attribute-Query. L'authentification avec demande d'attributs entre le RP et le Broker DOIT être effectuée via l'AttributConsumingServiceIndex, la demande d'attributs entre le Broker et l'IdP/AP DOIT en outre être possible via l'Attribute-Query.[8]

2.7.1 Authentification sans demande d'attributs

La Figure 5 propose une vue d'ensemble du déroulement du protocole d'une authentification sans demande d'attributs.

[8] La variante de l'Attribute-Query permet de garantir que les IdP/AP, qui ne prennent en charge aucun `<samlp:AttributeConsumingServiceIndex>`, puissent également être intégrés au système.

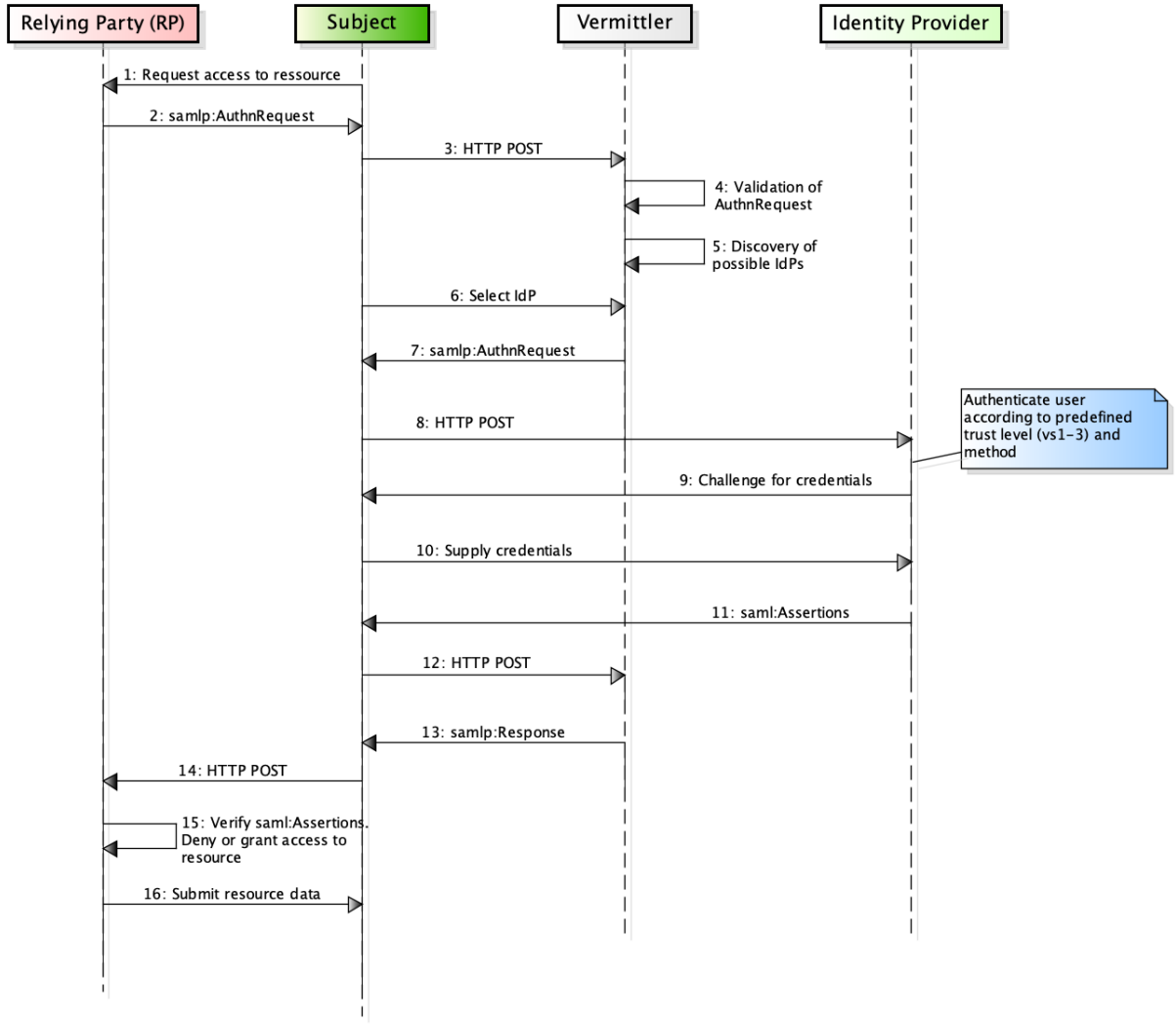

Figure 5: Protocole d'authentification sans transmission d'attributs

Tableau de référence pour la Figure 5:

Étape	Description	Interface	Chapitre
1, 2	L'utilisateur souhaite accéder à une ressource du RP. Le RP renvoie au Browser de l'utilisateur une <samlp:AuthnRequest> sous une forme HTML self-submitting.	Relying Party	5.1.1
3, 4, 5, 6, 7	Transmission de la <samlp:AuthnRequest> au service SSO du Broker. Le Broker valide la Request et détermine les IdPs appropriés à partir du <samlp:AttributeConsumingServiceIndex>. Si plusieurs IdP répondent aux critères, l'utilisateur DOIT sélectionner un IdP souhaité. Le Broker crée ensuite une nouvelle <samlp:AuthnRequest> qui est renvoyée au Browser de l'utilisateur.	Broker	6.1.1, 6.1.2

Étape	Description	Interface	Chapitre
8, 9, 10, 11	Le Browser envoie la <samlp:AuthnRequest> au service SSO de l'IdP. L'utilisateur s'authentifie auprès de l'IdP. En cas d'authentification réussie, l'IdP crée une <samlp:Response> avec <saml:AuthnStatement> et <saml:Assertion> et la renvoie au Browser de l'utilisation.	IdP	7.1.1, 7.1.2
12, 13	Le Browser transmet la <saml:Assertion> au Broker. Le Broker crée une nouvelle <samlp:Response> avec une <saml:Assertion>, y compris un <saml:AuthnStatement>, et la renvoie au Browser.	Broker	6.1.3, 6.1.4
14, 15, 16	Le Browser envoie la <samlp:Response> au Relying Party (RP), qui vérifie à présent la <samlp:Response> du Broker et, partant de là, accorde ou refuse l'accès à la ressource.	Relying Party	5.1.2

Tableau 3: Tableau de référence pour le protocole d'authentification sans transmission d'attributs

2.7.2 Authentification avec demande d'attributs via l'AttributeConsumingServiceIndex

La Figure 6 propose la vue d'ensemble du déroulement du protocole d'une authentification avec demande d'attributs à l'aide de l'`<samlp:AttributeConsumingServiceIndex>`. Si le déroulement du protocole est le même que celui illustré par la Figure 5, la `<samlp:AuthnRequest>` et la `<samlp:Response>` en particulier diffèrent toutefois, et à cela s'ajoute l'obtention de l'User Consent. L'User Consent DOIT être obtenu avant ou après la confirmation d'authentification et d'attributs.

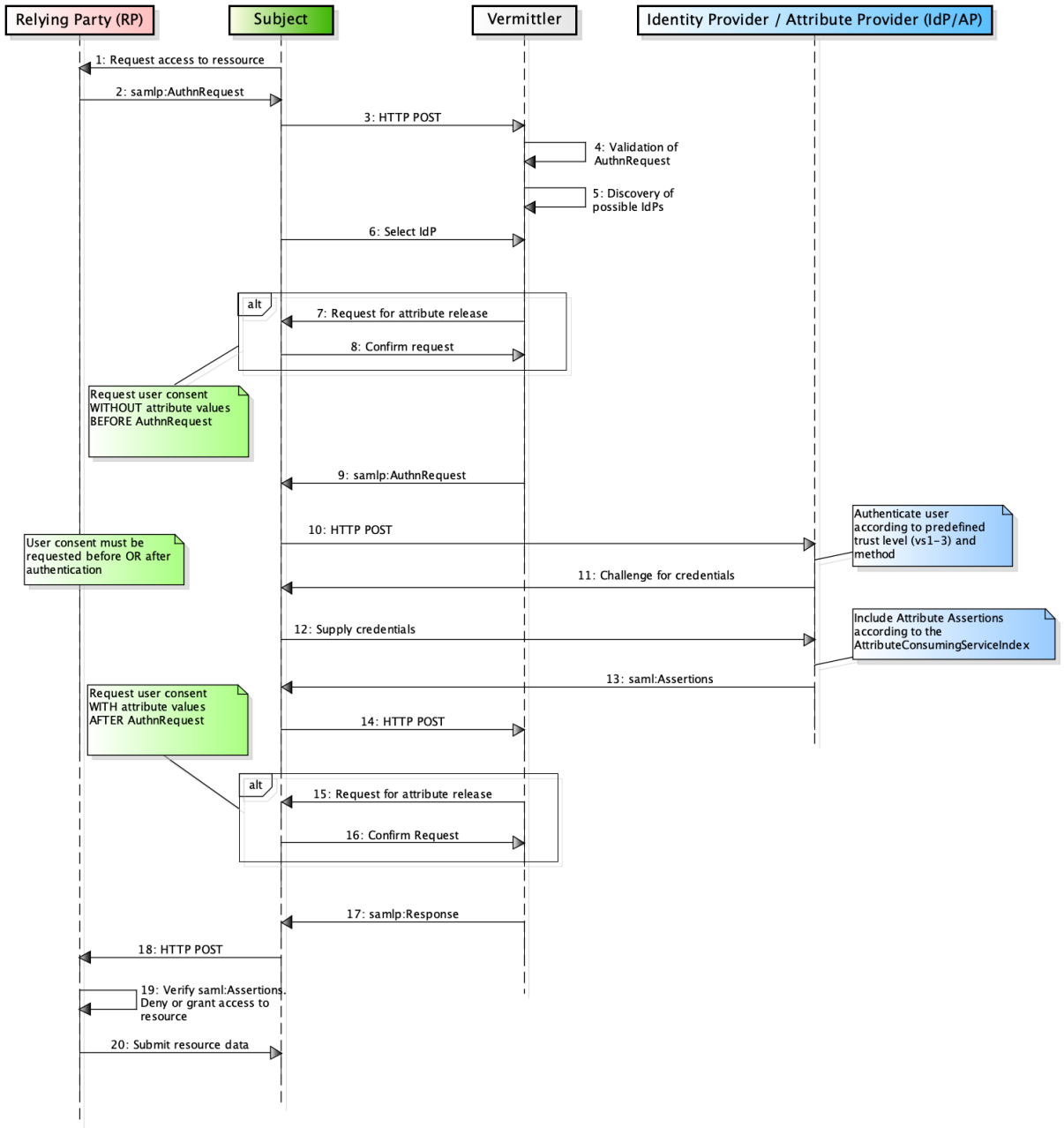

Figure 6: Protocole d'authentification avec transmission d'attributs par AttributeConsumingServiceIndex

Tableau de référence pour la Figure 6:

Étape	Description	Interface	Chapitre
1, 2	L'utilisateur souhaite accéder à une ressource du RP. Le RP renvoie au Browser de l'utilisateur une <samlp:AuthnRequest> sous une forme HTML self-submitting.	RP	5.2.1
3, 4, 5, 6	Transmission de la <samlp:AuthnRequest> au service SSO du Broker. Le Broker valide la Request et détermine les IdP/AP appropriés à partir du <samlp:AttributeConsumingServiceIndex>. Si plusieurs IdP/AP répondent aux critères, l'utilisateur DOIT sélectionner un IdP/AP souhaité.	Broker	6.2.1,
7, 8, 9	***Facultatif*** Dans l'éventualité où l'User Consent devrait être obtenu avant la demande d'authentification et d'attributs, le Broker envoie une demande pour la validation des attributs demandés pour l'utilisateur. Le Broker crée une nouvelle <samlp:AuthnRequest> avec un <samlp:AttributeConsumingServiceIndex> correspondant aux attributs exigés (et le cas échéant validés) qui est renvoyée au Browser de l'utilisateur.	Broker	6.2.2
10, 11, 12, 13	Le Browser envoie la <samlp:AuthnRequest> au service SSO de l'IdP/AP. L'utilisateur s'authentifie auprès de l'IdP/AP. En cas de succès de l'authentification, l'IdP/AP crée une <samlp:Response> avec une <saml:Assertion>, qui contient un <saml:AuthnStatement> et un <saml:AttributeStatement>, et la renvoie au navigateur.	IdP/AP	7.2.1, 7.2.2
14, 15, 16, 17	Le Browser transmet la <saml:Response> au Broker. ***Facultatif*** Dans le cas où l'User Consent devrait être obtenu après la réception des attributs, le Broker envoie à l'utilisateur une demande de validation des attributs, y compris les valeurs d'attribut tirées de la confirmation d'attributs. L'utilisateur confirme la demande. Le Broker crée une <samlp:Response> avec une <saml:Assertion>, qui contient le <saml:AuthnStatement> et le <saml:AttributeStatement> de la Response précédente de l'IdP/AP. La <samlp:Response> est transmise au Broker.	Broker	6.2.3, 6.2.4
18, 19,	Le Browser envoie la <samlp:Response> au Relying Party, qui vérifie alors la <samlp:Response> du Broker et, partant de	RP	5.2.2

Étape	Description	Interface	Chapitre
20	là, accorde ou refuse l'accès à la ressource.		

Tableau 4: Tableau de référence pour le protocole d'authentification avec transmission d'attributs par AttributeConsumingServiceindex.

2.7.3 Authentification avec demande d'attributs via une Attribute Query

La Figure 7 propose la vue d'ensemble du déroulement du protocole d'une authentification avec demande d'attributs par une Attribute Query. Le déroulement du protocole diffère notamment par la demande d'attributs supplémentaire après une authentification réussie. L'User Consent DOIT être obtenu avant la demande d'attributs ou après la confirmation d'attributs.

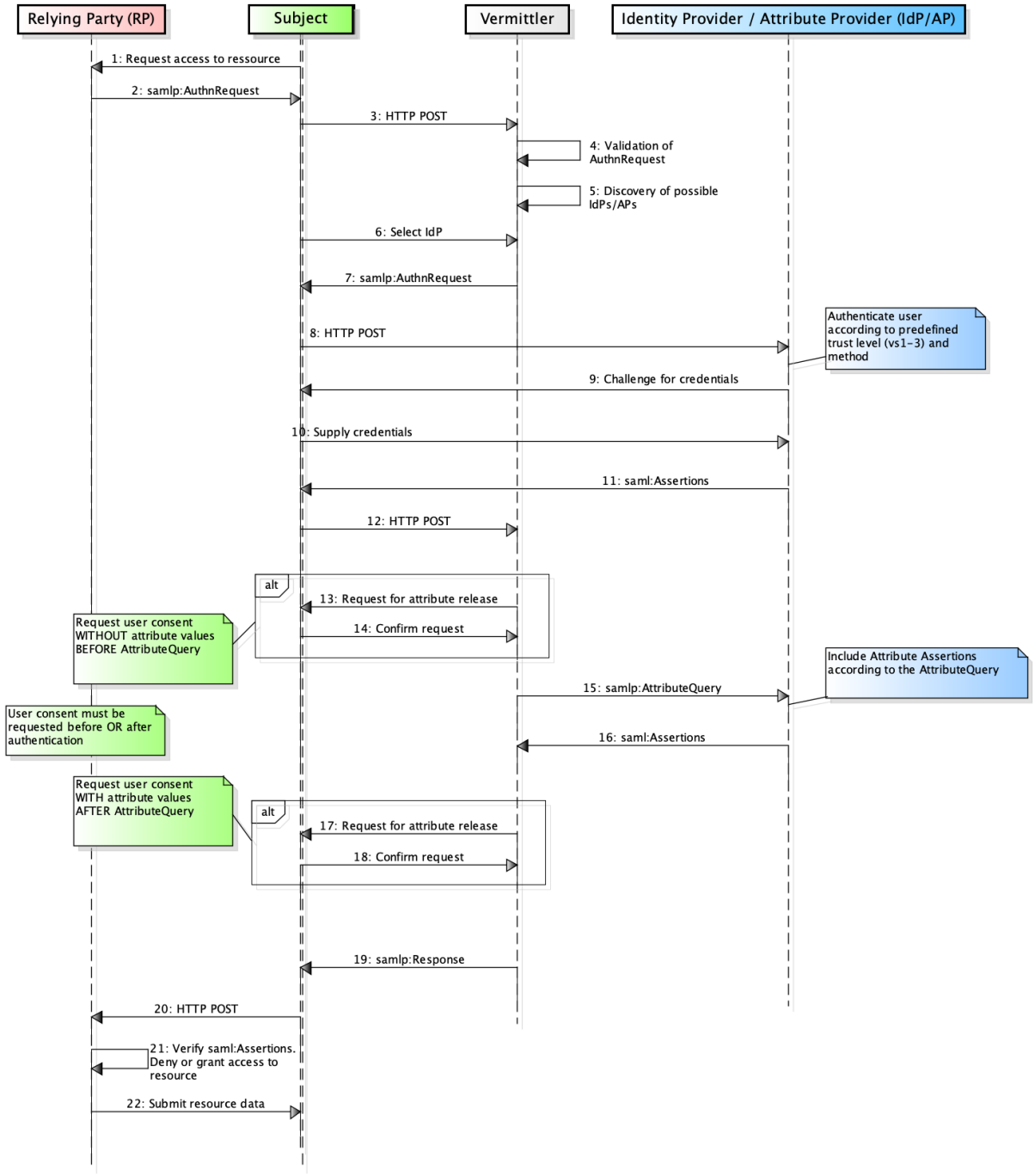

Figure 7: Protocole d'authentification avec transmission d'attributs par Attribute-Query

Tableau de référence pour la Figure 7:

Étape	Description	Interface	Chapitre
1, 2	L'utilisateur souhaite accéder à une ressource du RP. Le RP renvoie au Browser de l'utilisateur une <samlp:AuthnRequest> sous une forme HTML self-submitting.	Relying Party	5.2.1
3, 4, 5, 6, 7	Transmission de la <samlp:AuthnRequest> au service SSO du Broker. Le Broker valide la Request et détermine les IdP/AP appropriés à partir du <samlp:AttributeConsumingServiceIndex>. Si plusieurs IdP/AP répondent aux critères, l'utilisateur DOIT sélectionner un IdP/AP souhaité. Le Broker crée ensuite une nouvelle <samlp:AuthnRequest> SANS <AttributeConsumingServiceIndex>[9], qu'il renvoie au navigateur de l'utilisateur.	Broker	6.3.1, 6.3.2
8, 9, 10, 11	Le Browser envoie la <samlp:AuthnRequest> au service SSO de l'IdP/AP sélectionné. L'utilisateur s'authentifie auprès de l'IdP. En cas d'authentification réussie, l'IdP crée une <samlp:Response> avec <saml:Assertion> et <saml:AuthnStatement> et la renvoie à l'utilisateur.	IdP/AP	7.3.1, 7.3.2
12, 13, 14, 15	Une fois que l'utilisateur s'est authentifié, le Browser transmet la <saml:Assertion> au Broker. ***Facultatif*** Dans l'éventualité où l'User Consent devrait être obtenu avant la demande d'attributs, le Broker envoie une demande pour la validation des attributs demandés pour l'utilisateur. Le Broker crée ensuite une Attribute-Query à partir des attributs exigés par le RP et l'envoie à l'IdP/AP.	Broker	6.3.3, 6.3.4
16	L'IdP/AP reçoit la <samlp:AttributeQuery> et crée une <samlp:Response> avec <saml:Assertion> et <saml:AttributeStatement> et la renvoie au Broker.	IdP/AP	7.3.3, 7.3.4
17, 18, 19	***Facultatif*** Dans le cas où l'User Consent devrait être obtenu après la réception des attributs, le Broker envoie à l'utilisateur une demande de validation des attributs, y compris les valeurs d'attribut tirées de la confirmation d'attributs.	Broker	6.3.5, 6.3.6

[9] Si l'`<AttributeConsumingServiceIndex>` n'est pas indiqué, le Default, qui doit correspondre à une authentification sans demande d'attributs, prend effet.

Étape	Description	Interface	Chapitre
	Le Broker crée une <samlp:Response> avec une <saml:Assertion>, qui contient le <saml:AuthnStatement> **et** le <saml:AttributeStatement> des Responses précédentes de l'IdP/AP.		
18, 19, 20	Le Browser envoie la <samlp:Response> au Relying Party (RP), qui vérifie à présent la <samlp:Response> du Broker et, partant de là, accorde ou refuse l'accès à la ressource.	Relying Party	5.2.2

Tableau 5: Tableau de référence pour le protocole d'authentification avec transmission d'attributs par Attribute Query.

3 Directives

Partant des exigences pour une Identity Federation en cyberadministration selon les normes eCH-0224 [3] et eCH-0107 [7], les directives suivantes DOIVENT également être respectées pour cette norme.

Ces directives impliquent des restrictions ou des extensions concernant la norme SAML [4]. Il est en outre défini quelle mesure technique doit permettre de satisfaire quelle exigence.

Les SAML Standard & Implementation Guidelines courantes, ex. [18] et [19], DEVRAIENT par ailleurs être respectées.

3.1 Directives générales

Directive 1 – Authentification de l'instance requérante: l'instance ayant reçu la demande DOIT authentifier les composants requérants avant de renvoyer les informations d'authentification ou d'attribut d'un sujet.

L'instance requérante DOIT signer sa demande.

L'instance interrogée DOIT vérifier la signature du message reçu et comparer avec les métadonnées SAML.

Exigences satisfaites: 224-LE-5, IAM-11 et LB-15.

Directive 2 – Authenticité et intégrité de la réponse: tous les SAML Messages et Assertions renvoyés DOIVENT être signés par l'instance émettrice.

Si le Broker est l'instance d'acceptation, il DOIT vérifier la signature. Le RP DEVRAIT, dans son propre intérêt, effectuer une vérification de la signature.

Exigence satisfaite: IAM-9

Directive 3 – Protection de la confidentialité des Assertions: Afin de protéger la vie privée du sujet, l'instance émettrice (source) DEVRAIT émettre les Authentication et Attribute Assertions de telle manière que seule l'instance autorisée puisse les consulter.

Les Authentication et Attribute Assertions DEVRAIENT être chiffrées. Si l'instance réceptrice est le Broker, toutes les Assertions DOIVENT être chiffrées.

Si le Broker en tant qu'instance émettrice chiffre les Assertions, le RP doit être en mesure de les traiter en conséquence.

Exigence satisfaite: 224-LB-4

Directive 4 – Modèle de qualité pour l'authentification: pour la qualité de l'authentification des sujets, les niveaux de confiance selon eCH-0170 v2.0 [13] DOIVENT être utilisés:

- *urn:ech.ch/ech0170v2/vs1*: Niveau de confiance 1 (confiance nulle ou minimale),
- *urn:ech.ch/ech0170v2/vs2*: Niveau de confiance 2 (confiance faible),
- *urn:ech.ch/ech0170v2/vs3*: Niveau de confiance 3 (confiance notable),
- *urn:ech.ch/ech0170v2/vs4*: Niveau de confiance 4 (confiance élevée)[10].

Le RP DOIT définir le niveau de confiance nécessaire lors de l'enregistrement dans ces métadonnées (voir chapitre 8.1.1) et PEUT l'envoyer dans la demande d'authentification (si elle a besoin de plusieurs niveaux de confiance).

Le Broker PEUT envoyer le niveau de confiance demandé dans la demande d'authentification.

L'IdP DOIT définir les niveaux de confiance disponibles dans les métadonnées (voir chap. 8.1.2). Si plusieurs niveaux de confiance sont possibles, l'IdP DOIT envoyer également le niveau de confiance utilisé dans la confirmation d'authentification (Authentication Assertion).

Le Broker DOIT dans tous les cas envoyer le niveau de confiance conjointement dans la confirmation d'authentification. Le Broker obtient le niveau de confiance dans la confirmation d'authentification soit pour la période d'exécution de la confirmation d'authentification de l'IdP soit à partir des métadonnées de l'IdP définies pour la période de définition.

Exigences satisfaites: 224-IAM-4, 224-IAM-4.1

Directive 5 – Modèle de qualité pour la confirmation d'attributs: pour la qualité de la confirmation d'attributs des sujets, le modèle suivant ou un modèle équivalent DOIT être utilisé.

- *urn.ech.ch/ech0224v1/aq1*: Qualité d'attribut 1 (attributs non confirmés),
- *urn.ech.ch/ech0224v1/aq2*: Qualité d'attribut 2 (attributs confirmés),
- *urn.ech.ch/ech0224v1/aq3*: Qualité d'attribut 3 (attributs officiellement confirmés).

Le RP DOIT indiquer au Broker la qualité exigée pour quel attribut lors de l'enregistrement de la ressource.

Le Broker DOIT envoyer conjointement la qualité des attributs au RP dans la confirmation d'attributs. Le Broker reçoit la qualité des attributs soit pour la période d'exécution de la confirmation d'attributs de l'IdP/AP soit à partir des métadonnées de l'IdP/AP définies pour la période de définition.

Exigence satisfaite: 224-IAM-5

Directive 6 – Validation des attributs (User Consent): Lorsque l'obtention de l'User Consent auprès de l'IdP/AP peut être désactivée, le Broker DOIT obtenir le consentement du sujet pour que les attributs sélectionnés puissent être transmis au RP.

L'IdP/AP NE DEVRAIT PAS obtenir l'«User Consent» du sujet.
Exigence satisfaite: 224-LB-6

[10] Le niveau de confiance 4 nécessite une mise en œuvre du SAML V2.0 Holder-of-Key Web Browser SSO Profile [12], dont l'utilisation sur les Identity Federations n'est pas simple et ne sera donc pas traitée plus avant dans la présente norme.

3.2 Directives pour tous les messages

Cette rubrique établit les directives pour les SAML Messages.

- L'attribut `ID` dans l'élément racine DOIT figurer dans chaque message. La valeur dans le message DOIT être sans ambigüité. Elle est utilisée comme référence lors de la signature du message.
- L'attribut `Destination` dans l'élément racine de chaque message DOIT toujours être présent. Sa valeur DOIT être l'URL à laquelle le message est envoyé.
- L'attribut `IssueInstant` dans l'élément racine de chaque message DOIT toujours être présent. Sa valeur indique le moment de la création du message. Celle-ci DOIT être codée en UTC.
- L'attribut `Version` dans l'élément racine de chaque message DOIT toujours être présent. Sa valeur DOIT être `2.0`.
- La valeur de l'élément `<saml:Issuer>` DOIT concorder dans chaque message avec l'attribut `EntityID` provenant des métadonnées de l'entité, qui a créé le Message .
- Tous les messages DOIVENT être signés numériquement avec l'un des certificats (certificat d'application) reconnus dans le domaine (c'est-à-dire contenir un élément `<ds:Signature>`).[11]

3.3 Directives pour les Authentication Requests

- L'élément `<samlp:AuthnRequest>` DOIT être la racine de l'Authentication Request.
- L'élément <samlp:AuthnRequest> DOIT être signé numériquement avec l'un des certificats reconnus dans la Community (un élément <ds:Signature> doit être contenu).
- L'élément `<samlp:AuthnRequest>` DOIT contenir les attributs `AssertionConsumerServiceURL` et `ProtocolBinding`.

  La valeur d'`AssertionConsumerServiceURL` DOIT concorder avec l'élément `AssertionConsumerService` des métadonnées de l'entité qui a créé l'Authentication Request.
- La valeur de l'attribut `ProtocolBinding` DOIT être `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`.
- L'élément `<samlp:AuthnRequest>` PEUT contenir un attribut `ForceAuthn`.
- L'élément `<samlp:AuthnRequest>` PEUT contenir un élément `<samlp:NameIDPolicy>`. La valeur dont l'attribut `Format` DOIT être `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` ou `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`. Si elle est persistante, l'attribut `AllowCreate` doit figurer dans l'élément <samlp:NameIDPolicy> et dont la valeur DOIT être réglée sur

[11] Des renseignements détaillés concernant les différentes classes de certificats et leur utilisation dans la cyberadministration figurent dans la norme eCH-0048 - Classes de certificats PKI [23]..

Si l'élément `<samlp:NameIDPolicy>` est abandonné, le format `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` est considéré comme Default (par défaut).

- L'Authentication Request DEVRAIT contenir l'attribut `AttributeConsumingServiceIndex`. Dans l'éventualité où cette option ne serait pas disponible, la valeur par défaut s'applique.
- L'Authentication Request PEUT contenir un élément `<saml:Subject>` avec un élément `nameID` pour le cas d'un Session Refreshing ou d'une Step Up Authentification.
- L'Authentication Request PEUT contenir un élément `<samlp:RequestedAuthnContext>` avec un élément `<saml:AuthnContextClassRef>`, lorsque l'authentification requise doit présenter un niveau plus élevé que dans les métadonnées. La valeur de l'élément `<saml:AuthnContextClassRef>` DOIT être l'un des niveaux de confiance selon la norme eCH-0170 v2.0 [13] par exemple
  - *urn:ech.ch/ech0170v2/vs1*: Niveau de confiance 1 (confiance nulle ou minimale),
  - *urn:ech.ch/ech0170v2/vs2*: Niveau de confiance 2 (confiance faible),
  - *urn:ech.ch/ech0170v2/vs3*: Niveau de confiance 3 (confiance notable).
- L'Authentication Request ne DEVRAIT contenir AUCUN élément supplémentaire (Conditions, Scope, etc.), sauf si explicitement convenu et défini pour le domaine.

3.4 Directives pour les Attribute Queries

- L'élément `<samlp:AttributeQuery>` DOIT être la racine de l'Attribute Query Request.
- L'élément `<samlp:AttributeQuery` DOIT être signé numériquement avec l'un des certificats reconnus dans la Community (un élément <ds:Signature> doit être contenu).
- L'élément `<samlp:AttributeQuery>` DOIT contenir un élément `<saml:Subject>`. Celui-ci DOIT contenir un `<saml:NameID>`. Le format de ce dernier NE DOIT PAS être `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`.
- L'élément `<samlp:AttributeQuery>` DOIT contenir un ou plusieurs éléments `<Attribute>` .
- L'élément `<samlp:AttributeQuery>` NE DOIT PAS contenir un ou plusieurs éléments `<Attribute>` , qui ont les mêmes attributs `Name` et `NameFormat`.

3.5 Directives pour Responses

- L'élément `<samlp:Response>` DOIT être la racine du Response Message.
- L'élément `<saml:Response>` DEVRAIT être signé numériquement avec l'un des certificats reconnus dans la Community (un élément `<ds:Signature>` doit être contenu).
- L'élément `<Response>` DOIT contenir un attribut `InResponseTo`.

  L'attribut `InResponseTo` DOIT concorder avec l'`ID` de la demande, pour laquelle la Response a été créée.

- L'élément `<samlp:Response>` contenir un élément`<samlp:Status>` et celui-ci doit contenir un `<samlp:StatusCode>`.

- En cas d'Authentication Request réussie, l'élément `<samlp:Response>` DOIT contenir un élément `<saml:Assertion>` .
- Si l'Authentication Request échoue, une annonce d'erreur selon SAML 2.0 [4] DOIT figurer dans l'élément `<samlp:StatusCode>` et l'Assertion est abandonnée. L'élément `<samlp:Status>` PEUT en outre contenir un élément `<samlp:StatusDetail>` et `<samlp:StatusMessage>`. Il faut à cet égard veiller à ne pas inclure dans les éléments supplémentaires des informations inutiles concernant l'utilisateur ou la nature de l'erreur.

```
<samlp:Response
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="lnqw-xqap-xydg-kxsr"
    InResponseTo="mkqs-ezew-qplo-snrt"
    Version="2.0"
    IssueInstant="2020-12-05T09:23:59Z"
    Destination="https://saml-rp.example.com/SAML/ACS/Browser">
        <saml:Issuer>https://vermittler.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
       <samlp:StatusMessage>...</samlp:StatusMessage>
       <samlp:StatusDetail Value="urn:oasis:names:tc:SAML:2.0:status:Responder">
              ...
       </samlp:StatusDetail>
    </samlp:Status>
</samlp:Response>
```

Listing 1: Exemple de SAML Response (Success)

3.6 Directives pour les Assertions

Cette rubrique établit les directives pour les SAML Assertions.

- L'élément `<saml:Assertion>` DOIT contenir un attribut `ID` et `IssueInstant` .
- L'élément `<saml:Assertion>` DOIT contenir un élément `<saml:Issuer>` . Sa valeur DOIT concorder avec l'attribut `EntityID` provenant des métadonnées et être issue du composant qui a créé l'Assertion.
- L'élément `<saml:Assertion>` DOIT être signé numériquement avec l'un des certificats reconnus dans le domaine (élément `<ds:Signature>` contenu).
- L'élément `<saml:Assertion>` DOIT contenir un élément `<saml:Subject>` . Celui-ci DOIT contenir un élément `<saml:NameID>` et `<saml:SubjectConfirmation>` .
  L'élément `<saml:SubjectConfirmation>` DOIT avoir un attribut `Method` Attribut. Sa valeur DOIT être `urn:oasis:names:tc:SAML:2.0:cm:bearer`.
  L'élément `<saml:SubjectConfirmation>` DOIT avoir un élément `<saml:SubjectConfirmationData>`. Celui-ci DOIT avoir un attribut `InResponseTo`, `Recipient` et `NotOnOrAfter`.
- L'élément `<saml:Assertion>` DOIT contenir un élément `<saml:Conditions>` . Celui-ci DOIT avoir un attribut `NotBefore` et `NotOnOrAfter` . Celui-ci DOIT en outre contenir un élément `<saml:AudienceRestriction>`, qui a un élément `<saml:Audience>`. Sa valeur DOIT concorder avec l'attribut `EntityID` provenant des métadonnées de l'entité pour laquelle a été créée l'Assertion.
- L'élément `<Assertion>` DOIT contenir un élément `<saml:AuthnStatement>` et/ou un élément `<saml:AttributeStatement>`.

- L'élément `<saml:AuthnStatement>` DOIT contenir un`AuthnInstant` et un attribut `SessionIndex` ainsi qu'un élément `<saml:AuthnContext>`.
- L'élément `<saml:AuthnContext>` DOIT contenir un élément `<saml:AuthnContextClassRef>`. Sa valeur DOIT être l'un des niveaux de confiance suivants selon la norme eCH-0170 v2.0 [13]:
  - `urn:ech.ch/ech0170v2/vs1`: Niveau de confiance 1 (confiance nulle ou minimale),
  - `urn:ech.ch/ech0170v2/vs2`: Niveau de confiance 2 (confiance faible),
  - `urn:ech.ch/ech0170v2/vs3`: Niveau de confiance 3 (confiance notable).
- L'élément `<saml:AttributeStatement>` DOIT contenir un attribut `Name` et `NameFormat`, ainsi qu'un élément `<samlAttributeValue>`.
- L'élément `<saml:AttributeValue>` DOIT contenir un attribut `xsi:type` et comme valeur l'attribut correspondant. De même, la qualité de l'attribut DOIT être indiquée, par exemple comme attribut `ech0224:aq` avec les valeurs selon eCH-0224 v1.0 [3].
- L'élément `<saml:AttributeStatement>` DOIT contenir un ou plusieurs éléments `<saml:Attribute>` et ceux-ci PEUVENT avoir un ou plusieurs éléments `<saml:AttributeValue>` ainsi qu'un renseignement concernant la source (`<saml:OriginalIssuer>`).

4 Interfaces des modèles de Broker

Ce chapitre définit la façon dont deux modèles de Broker **Sources ouvertes** et **Double Blinding** de la norme 0224 [3] sont mis en œuvre avec les descriptions d'interface correspondantes. Seules les interfaces entre les acteurs pour les processus de période d'exécution sont ici spécifiées. Les autres activités des acteurs sont présentées dans la norme eCH-0224 à partir du chapitre 8.

Le chapitre 4.1

Le chapitre 4.2

4.1 Authentification

Dans le cas d'un modèle de Broker, l'authentification (sans demande d'attributs) s'effectue en principe de la même manière dans les deux sections de protocole. Chaque composant DOIT signer la demande ou la confirmation. Dans ce cas de figure, le Broker DOIT insérer la confirmation d'authentification de l'IdP/AP dans une nouvelle Response signée par le Broker. La Figure 8 offre une vue d'ensemble de l'authentification.

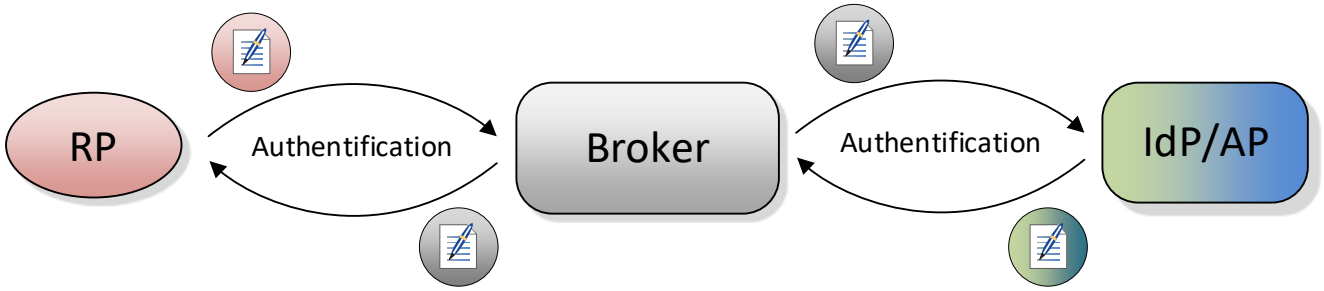

Figure 8: Vue d'ensemble des interfaces pour l'authentification

4.2 Authentification avec transmission d'attributs

La signature et le chiffrement de l'assertion dépendent du modèle de Broker.

4.2.1 Broker Double Blinding

La description détaillée du modèle de Broker Double Blinding se trouve dans le document eCH-0224 [3] au chapitre 8.2.

La Figure 9 illustre la façon dont les composants signent l'Authentication & Attribute Assertion. Le Broker DOIT à nouveau signer l'Assertion reçue, de sorte que le RP ou l'IdP/AP n'aient pas connaissance l'un de l'autre.

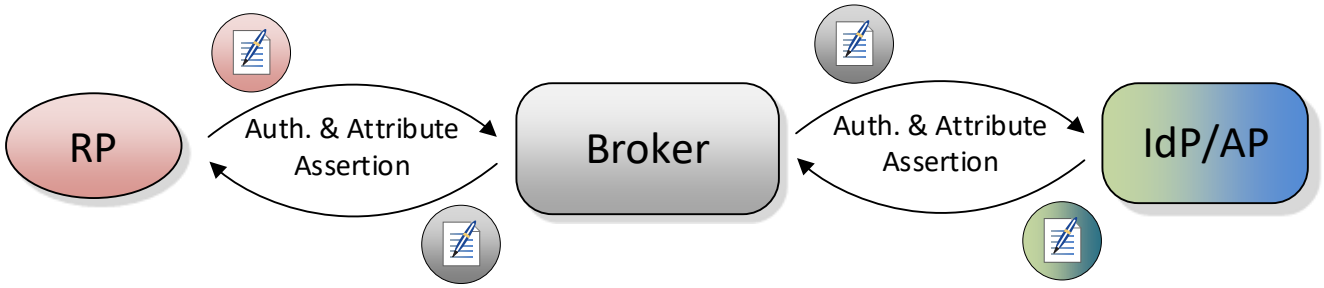

Figure 9: Vue d'ensemble de la transmission d'Assertion en cas de Double Blinding

4.2.2 Sources ouvertes Broker

La description détaillée du modèle de Broker Sources ouvertes se trouve dans le document eCH-0224 [3] au chapitre 8.3.

Variante 1 – *Transmission de signature*

Le RP DOIT pouvoir identifier la source de l'Assertion.

Le Broker DOIT laisser la signature de l'IdP/AP inchangée (voir Figure 10). Le RP peut identifier l'IdP/AP à partir de la signature.

La transmission de signature est prise en charge uniquement concernant l'authentification via l'AttributeConsumingServiceIndex (voir chapitre 2.7.2).[12]

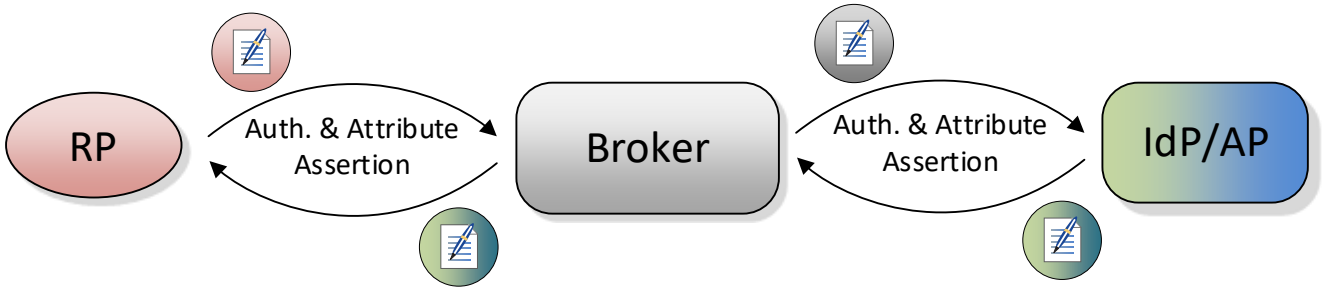

Figure 10: Vue d'ensemble de la transmission d'Assertion pour les sources ouvertes par transmission de signature

Variante 2 *– Identification par attribut*

Le Broker DOIT à nouveau signer l'Assertion, tel qu'illustré par la Figure 9, et DOIT permettre l'identification de l'IdP/AP dans l'Assertion à l'aide d'un attribut supplémentaire.

Pour ce faire, le Broker DOIT ajouter l'Attribut `AuthenticatingAuthority`, la valeur DOIT être l'`EntityID` de l'IdP/AP correspondant. Le Listing 5 propose un exemple d'une telle Assertion.

[12] L'authentification avec demande d'attributs via l'Attribute Query se traduit par deux Assertions distinctes (confirmation d'authentification et d'attributs) auprès du Broker. Le Broker DOIT combiner les deux Assertions en une nouvelle Assertion, afin qu'aucune signature ne puisse être reprise par l'IdP/AP.

5 Interfaces pour le Relying Party (RP)

Ce chapitre spécifie les interfaces avec le RP. La procédure d'authentification sans transmission d'attributs est définie au chapitre 4.1 et l'authentification avec transmission d'attributs au chapitre 4.2. L'authentification et la transmission des attributs DOIVENT toujours passer par le Broker.

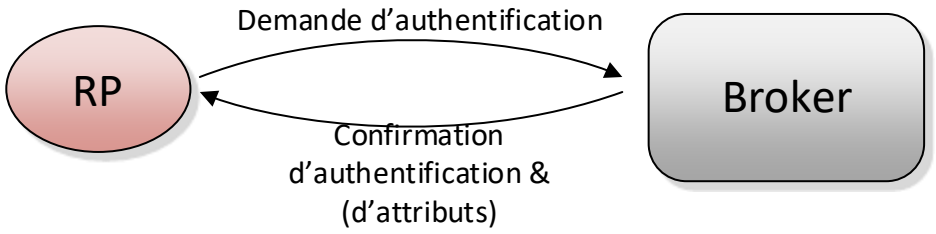

Figure 11: Vue d'ensemble des interfaces du RP

Le Tableau 6 indique dans quel chapitre est spécifiée la demande (ou réponse) correspondante du RP.

Authentification	Demande d'authentification	Chapitre 5.1.1
	Confirmation d'authentification	Chapitre 5.1.2
Authentification avec transmission d'attributs	Demande d'authentification et d'attributs	Chapitre 5.2.1
	Confirmations d'authentification et d'attributs	Chapitre 5.2.2

Tableau 6: Vue d'ensemble des chapitres des interfaces des RP

5.1 Authentification

La RP DOIT envoyer une demande d'authentification au Broker et reçoit en retour un message `<samlp:Response>`. Le résultat d'une authentification réussie DOIT être une Authentication Assertion.

5.1.1 Demande d'authentification au Broker

Le RP crée une `<samlp:AuthnRequest>` (Listing 2). La `<samlp:AuthnRequest>` contient d'ordinaire un `<samlp:AttributeConsumingServiceIndex>`, qui identifie un jeu défini d'attributs. En cas d'authentification sans demande d'attributs, la valeur est réglée sur Default ou ce renseignement n'est pas fourni, de sorte que l'on part en principe de Default[13]. La `<samlp:AuthnRequest>` est signée et envoyée au service SSO du Broker.

[13] Pour qu'une Authentication Request sans demande d'attributs puisse être effectuée, le `md:AttributeConsu-`

```
<samlp:AuthnRequest
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="ewda-e1df-xydg-xwsq"
    Version="2.0"
    IssueInstant="2020-12-05T09:21:59Z"
    Destination="https://vermittler.example.com/SAML/SSO/Browser"
    AssertionConsumerServiceURL="https://saml-rp.example.com/SAML/ACS/POST"
    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    AttributeConsumingServiceIndex="1">
    <saml:Issuer>https://saml-rp.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
</samlp:AuthnRequest>
```

Listing 2: Demande d'authentification du RP au Broker

5.1.2 Confirmation d'authentification du Broker

L'Attribute Consumer Service (ACS) du RP reçoit une `<samlp:Response>` du Broker (Listing 3). La `<samlp:Response>` contient une `<saml:Assertion>`, qui contient un `<saml:AuthnStatement>`. Le RP DOIT vérifier les signatures de la `<samlp:Response>` et la `<saml:Assertion>` et peut utiliser la réponse du Broker pour la décision concernant l'accès à la ressource.

En cas d'échec de l'authentification de l'utilisateur, la `<samlp:Response>` DOIT contenir une annonce d'erreur selon les directives concernant les Responses (chapitre 3.5).

`mingService` correspondant doit être défini sans attributs dans les métadonnées du Broker. Le Default du `<samlp:AttributeConsumingServiceIndex>` est défini dans les métadonnées (voir chapitre 8).

```
<samlp:Response
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="lnqw-xqap-xydg-kxsr"
    InResponseTo="ewda-e1df-xydg-xwsq"
    Version="2.0"
    IssueInstant="2020-12-05T09:23:59Z"
    Destination="https://saml-rp.example.com/SAML/ACS/Browser">
        <saml:Issuer>https://vermittler.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value=
              "urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <saml:Assertion
        xmlns:xs="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:ech-0174="http://www.ech.ch/ech0174v2"
        ID="lnqw-xqap-xydg-kxsr"
        Version="2.0"
        IssueInstant="2020-12-05T09:27:05Z">
        <saml:Issuer>https://vermittler.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
        <saml:Subject>
            <saml:NameID Format=
                "urn:oasis:names:tc:SAML:2.0:nameidformat:transient">
                wdrt-6gre-wcbp-ubwq-234gz
            </saml:NameID>
            <saml:SubjectConfirmation
                Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData
                    NotOnOrAfter="2020-12-05T09:37:05Z"
                    Recipient="https://saml-rp.example.com/SAML/ACS/POST"
                    InResponseTo="mkqs-ezew-qplo-snrt"/>
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions
            NotBefore="2020-12-05T09:27:05Z"
            NotOnOrAfter="2020-12-05T09:37:05Z">
            <saml:AudienceRestriction>
                <saml:Audience>
                    https://saml-rp.example.com
                </saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement
            AuthnInstant="2020-12-05T09:23:50Z"
            SessionIndex="234122">
            <saml:AuthnContext>
                <saml:AuthnContextClassRef>
                    urn:ech.ch/ech0170v2/vs1
                </saml:AuthnContextClassRef>
            </saml:AuthnContext>
        </saml:AuthnStatement>
    </saml:Assertion>
</samlp:Response>
```

Listing 3: Confirmation d'authentification du Broker au RP

5.2 Authentification avec transmission d'attributs

Le RP DOIT envoyer une demande d'authentification au Broker et reçoit un message `<samlp:Response>`. Le résultat d'une authentification réussie DOIT être une Assertion qui, en cas d'authentification réussie, contient un AuthnStatement et les attributs requis. La demande d'attributs entre le RP et le Broker DOIT se faire via le `<samlp:AttributeConsumingServiceIndex>`.

5.2.1 Demande d'authentification et d'attributs au Broker

Le RP créé une <samlp:AuthnRequest> (Listing 4). Le <samlp:AuthnRequest> contient un <samlp:AttributeConsumingServiceIndex>, qui identifie un jeu défini d'attributs. La <samlp:AuthnRequest> est signée et envoyée au service SSO du Broker.

```
<samlp:AuthnRequest
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="ewda-e1df-xydg-xwsq"
    Version="2.0"
    IssueInstant="2020-12-05T09:21:59Z"
    Destination="https://vermittler.example.com /SAML/SSO/Browser"
    AssertionConsumerServiceURL="https://saml-rp.example.com/SAML/ACS/POST"
    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    AttributeConsumingServiceIndex="2">
    <saml:Issuer>https://saml-rp.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
</samlp:AuthnRequest>
```

Listing 4: Demande d'authentification et d'attributs du RP au Broker

5.2.2 Confirmations d'authentification et d'attributs du Broker

Avant que le Broker n'envoie la confirmation, d'attribut au RP, le sujet DOIT valider les attributs. Voir Directive 6 – Validation des attributs (User Consent).

L'Assertion Consuming Service (ACS) du RP reçoit une <samlp:Response>.

La <samlp:Response> DOIT être signée par le Broker, le modèle de Broker étant déterminant pour la signature de la <saml:Assertion>:

Variante Double Blinding (chapitre 4.2.1)

Le RP NE DOIT PAS pouvoir reconnaître l'IdP/AP qui a créé l'Assertion.

À cette fin, la <saml:Assertion> DOIT être signée par le Broker.

Variante sources ouvertes (chapitre 4.2.2)

Le RP DOIT pouvoir reconnaître l'IdP/AP qui a créé l'Assertion.

L'<saml:Assertion> DOIT être signée par l'IdP/AP OU l'attribut supplémentaire <saml:AuthenticatingAuthority> (Listing 5) avec l'EntityId de l'IdP/AP comme valeur DOIT être joint à l'attribut <saml:AuthnContext> dans la confirmation d'authentification. La validation des signatures de <saml:Assertion> et <saml:Response> avec différents certificats de signature pouvant poser problème pour les RP, on préfèrera la solution avec l'attribut supplémentaire.

```
<saml:AuthnStatement
       AuthnInstant="2020-12-05T09:23:50Z"
       SessionIndex="234122">
            <saml:AuthnContext>
                <saml:AuthnContextClassRef>
                   urn:ech.ch/ech0170v2/vs3
                </saml:AuthnContextClassRef>
               <saml:AuthenticatingAuthority>
                      https://saml-idp-ap.example.com
               </saml:AuthenticatingAuthority>
            </saml:AuthnContext>
</saml:AuthnStatement>
```

Listing 5: Authentication Assertion avec AuthenticatingAuthority-Attribut (Sources ouvertes)

Le Listing 6 illustre une confirmation d'authentification et d'attributs selon le modèle de Broker Double Blinding.

Le RP DOIT vérifier les signatures de la `<samlp:Response>` et la `<saml:Assertion>` et peut utiliser la réponse du Broker pour la décision concernant l'accès à la ressource.

```
<samlp:Response
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="we34-bhou-pyaq-gbhf"
    InResponseTo="ewda-e1df-xydg-xwsq"
    Version="2.0"
    IssueInstant="2020-12-05T09:23:59Z"
    Destination="https://saml-rp.example.com/SAML/ACS/Browser">
        <saml:Issuer>https://vermittler.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <saml:Assertion
        xmlns:xs="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:ech-0174="http://www.ech.ch/ech0174v2"
        ID="we34-bhou-pyaq-gbhf"
        Version="2.0"
        IssueInstant="2020-12-05T09:27:05Z">
        <saml:Issuer>https://vermittler.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
        <saml:Subject>
            <saml:NameID Format=
                "urn:oasis:names:tc:SAML:2.0:nameidformat:transient">
                wdrt-6gre-wcbp-ubwq-234gz
            </saml:NameID>
            <saml:SubjectConfirmation
                Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData
                    NotOnOrAfter="2020-12-05T09:37:05Z"
                    Recipient="https://saml-rp.example.com/SAML/ACS/POST"
                    InResponseTo="ewda-e1df-xydg-xwsq"/>
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions
            NotBefore="2020-12-05T09:27:05Z"
            NotOnOrAfter="2020-12-05T09:37:05Z">
            <saml:AudienceRestriction>
                <saml:Audience>https://saml-rp.example.com</saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement
            AuthnInstant="2020-12-05T09:23:50Z"
            SessionIndex="234122">
            <saml:AuthnContext>
                <saml:AuthnContextClassRef>
                    urn:ech.ch/ech0170v2/vs1
                </saml:AuthnContextClassRef>
            </saml:AuthnContext>
        </saml:AuthnStatement>
        <saml:AttributeStatement>
            <saml:Attribute
                Nom=
                "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                <saml:AttributeValue
                      xsi:type="xs:StringMaxLength255MinLenght1"
                      ech0224:aq="2">
                    hans@example.com
                </saml:AttributeValue>
            </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>
```

Listing 6: Confirmation d'authentification et d'attributs du Broker au RP (Double Blinding Model)

6 Interfaces pour Broker

Le Broker est le point final de protocole du RP et de l'IdP/AP. En principe, le RP considère le Broker comme IdP/AP. L'IdP/AP considère le Broker comme RP.

Le Broker est le lien entre les fournisseurs et les consommateurs d'identité. L'authentification et la transmission des attributs DOIVENT toujours passer par le Broker.

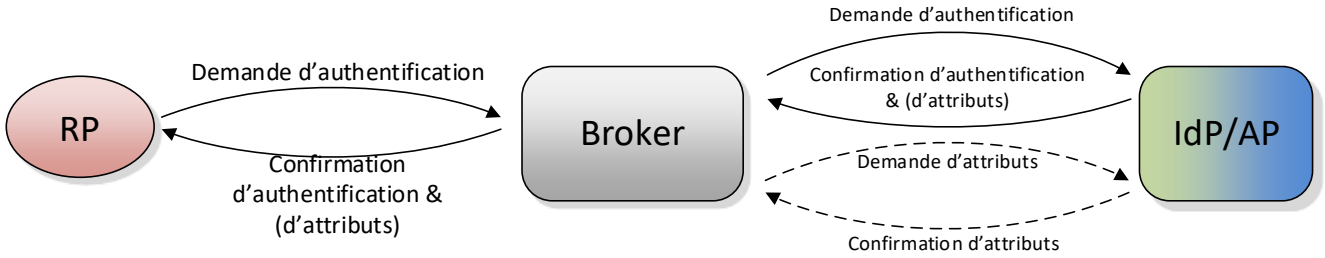

Figure 12: Vue d'ensemble des interfaces du Broker

Les chapitres suivants spécifient les interfaces. Les messages échangés par application sont définis du point de vue du Broker.

Le Tableau 7 indique dans quel chapitre est spécifiée la demande (ou réponse) correspondante du Broker. Pour la transmission d'attributs, le Broker DOIT prendre en charge la transmission d'attributs au moyen tant de l'Attribute Query que de l'AttributeConsumingServiceIndex sur l'itinéraire du protocole vers l'IdP/AP.

Authentification		Demande d'authentification du RP	Chapitre 6.1.1
		Demande d'authentification à l'IdP	chapitre 6.1.2
		Confirmation d'authentification de l'IdP	chapitre 6.1.3
		Confirmation d'authentification au RP	chapitre 6.1.4
Authentification avec transmission d'attributs	Attribute Consuming ServiceIndex	Demande d'authentification et d'attributs du RP	Chapitre 6.2.1
		Demande d'authentification et d'attributs à l'IdP/AP	Chapitre 6.2.2
		Confirmation d'authentification et d'attributs au Broker	Chapitre 6.2.3
		Confirmation d'authentification et d'attributs au RP	Chapitre 6.2.4
	Attribute Query	Demande d'authentification et d'attributs du RP	Chapitre 6.3.1
		Demande d'authentification à l'IdP/AP	Chapitre 6.3.2
		Confirmation d'authentification de l'IdP/AP	Chapitre 6.3.3
		Demande d'attributs à l'IdP/AP	Chapitre 6.3.4
		Confirmation d'attributs de l'IDP/AP	Chapitre 6.3.5
		Confirmation d'authentification et d'attributs au RP	Chapitre 6.3.6

Tableau 7: Vue d'ensemble des chapitres des interfaces du Broker

6.1 Authentification

Le Broker DOIT recevoir une demande d'authentification du RP. À l'aide de celui-ci, le Broker DOIT envoyer une demande d'authentification à l'IdP/AP et reçoit un message `<samlp:Response>` en retour. En cas de succès, le Response Message DOIT contenir une Authentication Assertion. Le Broker DOIT à nouveau signer le Message et l'Authentication Assertion et les envoyer au RP.

6.1.1 Demande d'authentification du Relying Party (RP)

Le service SSO du Broker reçoit une `<samlp:AuthnRequest>` d'un RP (voir Listing 7).

Le Broker détermine le Relying Party (RP-ID) de l'expéditeur à partir de l'élément `<saml:Issuer>` dans sa base de données (entrée `<md:entityID>`). La signature de la `<samlp:AuthnRequest>` est vérifiée au moyen du certificat X.509 du RP à partir de la base de données. Le Broker dresse une liste des services d'authentification possibles (IdP) à partir du `<samlp:AttributeConsumingServiceIndex>`[14] fourni. En fonction de la définition des ressources, les scénarios possibles sont les suivants:

a) La ressource a prescrit un (ou plusieurs) IdP (IdP-ID), qui satisfont au QAA Level défini. Sur son site Web, le Broker montre à l'utilisateur les IdP prédéfinis au choix ou le transmet directement au seul IdP possible.
b) La ressource a prescrit un niveau d'authentification (QAA-Level) souhaité. Sur la base de cette valeur, le Broker dresse une liste d'IdP envisageables et la soumet à l'utilisateur pour qu'il fasse son choix.

Il est possible de définir d'autres règles générales pour la sélection de l'IdP pour le Broker, en fonction de l'IP Range ou de l'User Agent par exemple.

```
<samlp:AuthnRequest
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="ewda-e1df-xydg-xwsq"
    Version="2.0"
    IssueInstant="2020-12-05T09:21:59Z"
    Destination="https://vermittler.example.com/SAML/SSO/Browser"
    AssertionConsumerServiceURL="https://saml-rp.example.com/SAML/ACS/POST"
    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    AttributeConsumingServiceIndex="1">
    <saml:Issuer>https://saml-rp.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
</samlp:AuthnRequest>
```

Listing 7: Demande d'authentification du RP au Broker

[14] l'`<samlp:AttributeConsumingServiceIndex>` doit être réglée sur Default en cas d'authentification sans attribut. s'il ne figure pas, la valeur à prendre en compte est Default.

6.1.2 Demande d'authentification à l'Identity Provider (IdP)

Le Broker crée, à partir de la `<samlp:AuthnRequest>` reçue par le RP, une nouvelle Request (voir Listing 8). La nouvelle Request contient le Broker en tant que `<saml:Issuer>` et l'IdP sélectionné en tant que `<samlp:Destination>`.

La `<samlp:AuthnRequest>` est signée par le Broker et envoyée au service SSO de l'IdP.

```
<samlp:AuthnRequest
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="mkqs-ezew-qplo-snrt"
    Version="2.0"
    IssueInstant="2020-12-05T09:22:30Z"
    Destination="https://saml-idp-ap.example.com/SAML/SSO/Browser"
    AssertionConsumerServiceURL="https://vermittler.example.com/SAML/ACS/Browser"
    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    AttributeConsumingServiceIndex="1">
    <saml:Issuer>https://vermittler.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
</samlp:AuthnRequest>
```

Listing 8: Demande d'authentification du Broker à l'IdP

6.1.3 Confirmation d'authentification de l'Identity Provider (IdP)

L'Assertion Consumer Service (ACS) du Broker reçoit une `<samlp:Response>` de l'IdP (Listing 9).

Le Broker DOIT vérifier les signatures de la `<samlp:Response>` et de la `<saml:Assertion>`. Le Broker DOIT vérifier si le niveau de confiance de l'authentification figure bien dans l'attribut `<saml:AuthContextClassRef>`. Si l'attribut n'est pas présent, le Broker DOIT insérer le niveau de confiance de l'IdP à partir des métadonnées enregistrées.

```
<samlp:Response
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="lnqw-xqap-xydg-kxsr"
    InResponseTo="mkqs-ezew-qplo-snrt"
    Version="2.0"
    IssueInstant="2020-12-05T09:23:59Z"
    Destination="https://vermittler.example.com/SAML/ACS/Browser">
        <saml:Issuer>https://saml-idp-ap.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <saml:Assertion
        xmlns:xs="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:ech-0174="http://www.ech.ch/ech0174v2"
        ID="we34-bhou-pyaq-gbhf"
        Version="2.0"
        IssueInstant="2020-12-05T09:27:05Z">
        <saml:Issuer>https://saml-idp-ap.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
        <saml:Subject>
            <saml:NameID Format=
                "urn:oasis:names:tc:SAML:2.0:nameidformat:transient">
                wdrt-6gre-wcbp-ubwq-234gz
            </saml:NameID>
            <saml:SubjectConfirmation
                Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData
                    NotOnOrAfter="2020-12-05T09:37:05Z"
                    Recipient="https://vermittler.example.com/SAML/ACS/POST"
                    InResponseTo="mkqs-ezew-qplo-snrt"/>
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions
            NotBefore="2020-12-05T09:27:05Z"
            NotOnOrAfter="2020-12-05T09:37:05Z">
            <saml:AudienceRestriction>
                <saml:Audience>
                    https://vermittler.example.com
                </saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement
            AuthnInstant="2020-12-05T09:23:50Z"
            SessionIndex="234122">
            <saml:AuthnContext>
                <saml:AuthnContextClassRef>
                    urn:ech.ch/ech0170v2/vs1
                </saml:AuthnContextClassRef>
            </saml:AuthnContext>
        </saml:AuthnStatement>
    </saml:Assertion>
</samlp:Response>
```

Listing 9: Confirmation d'authentification de l'IdP au Broker

6.1.4 Confirmation d'authentification au Relying Party (RP)

Le Broker crée une nouvelle Response à partir de la `<samlp:Response>` reçue par l'IdP (Listing 10). La nouvelle Response contient le Broker en tant que `<saml:Issuer>` et le RP pertinent en tant que `<samlp:Destination>`.

Le Broker signe à nouveau la `<samlp:Response>` et la `<saml:Assertion>` et l'envoie à l'Assertion Consuming Service (ACS) du Relying Party.

```
<samlp:Response
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="lnqw-xqap-xydg-kxsr"
    InResponseTo="ewda-e1df-xydg-xwsq"
    Version="2.0"
    IssueInstant="2020-12-05T09:23:59Z"
    Destination="https://saml-rp.example.com/SAML/ACS/Browser">
        <saml:Issuer>https://vermittler.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value=
              "urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <saml:Assertion
        xmlns:xs="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:ech-0174="http://www.ech.ch/ech0174v2"
        ID="lnqw-xqap-xydg-kxsr"
        Version="2.0"
        IssueInstant="2020-12-05T09:27:05Z">
        <saml:Issuer>https://vermittler.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
        <saml:Subject>
            <saml:NameID Format=
                "urn:oasis:names:tc:SAML:2.0:nameidformat:transient">
                wdrt-6gre-wcbp-ubwq-234gz
            </saml:NameID>
            <saml:SubjectConfirmation
                Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData
                    NotOnOrAfter="2020-12-05T09:37:05Z"
                    Recipient="https://saml-rp.example.com/SAML/ACS/POST"
                    InResponseTo="mkqs-ezew-qplo-snrt"/>
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions
            NotBefore="2020-12-05T09:27:05Z"
            NotOnOrAfter="2020-12-05T09:37:05Z">
            <saml:AudienceRestriction>
                <saml:Audience>
                    https://saml-rp.example.com
                </saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement
            AuthnInstant="2020-12-05T09:23:50Z"
            SessionIndex="234122">
            <saml:AuthnContext>
                <saml:AuthnContextClassRef>
                    urn:ech.ch/ech0170v2/vs1
                </saml:AuthnContextClassRef>
            </saml:AuthnContext>
        </saml:AuthnStatement>
    </saml:Assertion>
</samlp:Response>
```

Listing 10: Confirmation d'authentification du Broker au RP

6.2 Authentification avec demande d'attributs via le AttributeConsumingServiceIndex

Le Broker DOIT recevoir une demande d'authentification du RP. La demande d'authentification DOIT contenir le `<saml:AttributeConsumingServiceIndex>`.

Le Broker DOIT envoyer une nouvelle demande d'authentification avec le `<saml:AttributeConsumingServiceIndex>` correspondant à l'IdP/AP sélectionné. Une fois l'authentification réussie, le Broker DOIT recevoir en retour un message `<samlp:Response>` avec une Authentication et Attribute Assertion de l'IdP/AP.

Le Broker DOIT ensuite insérer l'Authentication et Attribute Assertion dans un message `<samlp:Response>` et le renvoyer au RP.

Le Broker DOIT obtenir l'User Consent pour la transmission d'attributs auprès du RP. Pour ce faire, le Broker DOIT obtenir l'autorisation soit avant la demande d'authentification et d'attributs à l'IdP/AP, SOIT après la confirmation d'authentification et d'attributs de l'IdP/AP. Dans le cas où l'User Consent devait être obtenu après la réception des attributs, le Broker DOIT en outre afficher les valeurs des attributs pour l'utilisateur (voir chapitre 2.6).

6.2.1 Demande d'authentification et d'attributs du Relying Party (RP)

La procédure à suivre une fois reçue une `<samlp:AuthnRequest>` d'un RP est la même que celle du chapitre 6.1.1. Dans ce cas de figure, le AttributeConsumingServiceIndex ne contient **PAS** le Default (voir Listing 11). Le Broker dresse à présent une liste d'IdP/AP qui peuvent fournir en plus les attributs requis de l'utilisateur.

```
<samlp:AuthnRequest
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="ewda-e1df-xydg-xwsq"
    Version="2.0"
    IssueInstant="2020-12-05T09:21:59Z"
    Destination="https://vermittler.example.com/SAML/SSO/Browser"
    AssertionConsumerServiceURL="https://saml-rp.example.com/SAML/ACS/POST"
    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    AttributeConsumingServiceIndex="2">
    <saml:Issuer>https://saml-rp.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
</samlp:AuthnRequest>
```

Listing 11: Demande d'authentification avec AttributeConsumingServiceIndex du RP au Broker

6.2.2 Demandes d'authentification et d'attributs à l'Identity & Attribute Provider (IdP/AP)

La procédure d'envoi d'une `<samlp:AuthnRequest>` à l'IdP/AP est la même qu'au chapitre 6.1.2. Dans ce cas de figure, le `<saml:AttributeConsumingServiceIndex>` n'est **PAS** le Default, de telle sorte que l'IdP/AP fournisse également les attributs correspondants.

6.2.3 Confirmations d'authentification et d'attributs de l'IdentityProvider & Attribute (IdP/AP)

La procédure de réception d'une `<samlp:Response>` de l'IdP/AP est la même qu'au chapitre 6.1.3. La Response contient dans ce cas de figure un `<saml:AuthnStatement>` et un `<saml:AttributeStatement>` avec un ou plusieurs éléments `<saml:Attribute>` (voir Listing 12).

```
<samlp:Response
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="lnqw-xqap-xydg-kxsr"
    InResponseTo="mkqs-ezew-qplo-snrt" Version="2.0"
    IssueInstant="2020-12-05T09:23:59Z"
    Destination="https://vermittler.example.com/SAML/ACS/Browser">
        <saml:Issuer>https://saml-idp-ap.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <saml:Assertion
        xmlns:xs="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:ech-0174="http://www.ech.ch/ech0174v2"
        ID="we34-bhou-pyaq-gbhf" Version="2.0"
        IssueInstant="2020-12-05T09:27:05Z">
        <saml:Issuer>https://saml-idp-ap.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
        <saml:Subject>
            <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameidformat:transient">
                wdrt-6gre-wcbp-ubwq-234gz
            </saml:NameID>
            <saml:SubjectConfirmation
                Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData
                    NotOnOrAfter="2020-12-05T09:37:05Z"
                    Recipient="https://saml-rp.example.com/SAML/ACS/POST"
                    InResponseTo="mkqs-ezew-qplo-snrt"/>
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions
            NotBefore="2020-12-05T09:27:05Z" NotOnOrAfter="2020-12-05T09:37:05Z">
            <saml:AudienceRestriction>
                <saml:Audience>
                    https://vermittler.example.com
                </saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement
            AuthnInstant="2020-12-05T09:23:50Z"
            SessionIndex="234122">
            <saml:AuthnContext>
                <saml:AuthnContextClassRef>
                    urn:ech.ch/ech0170v2/vs1
                </saml:AuthnContextClassRef>
            </saml:AuthnContext>
        </saml:AuthnStatement>
        <saml:AttributeStatement>
            <saml:Attribute
               Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                <saml:AttributeValue
                      xsi:type="xs:StringMaxLength255MinLenght1"
                      ech0224:aq="2">
                    hans@example.com
                </saml:AttributeValue>
            </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>
```

Listing 12: Confirmation d'authentification & d'attributs de l'IdP/AP au Broker

6.2.4 Confirmations d'authentification et d'attributs au Relying Party (RP)

Le Broker crée à présent une nouvelle confirmation d'authentification et d'attributs à partir de la `<samlp:Response>` de l'IdP/AP (Listing 12).

La nouvelle `<samlp:Response>` contient une `<saml:Assertion>` qui contient les éléments `<saml:AuthnStatement>` et `<AttributeStatement>` provenant de la confirmation de l'IdP/AP. Le Relying Party requérant est défini comme `<samlp:Destination>`.

La `<samlp:Response>` est désormais signée par le Broker, la signature de la `<saml:Assertion>` dépend toutefois du modèle de Broker:

Variante Double Blinding (chapitre 4.2.1)

L'IdP/AP NE DOIT PAS être identifiable par le RP.

Le Broker DOIT à nouveau signer la `<samlp:Response>` et la `<saml:Assertion>`.

Variante sources ouvertes (chapitre 4.2.2)

L'IdP/AP DOIT être identifiable par le RP.

Le Broker DOIT laisser la signature de l'IdP/AP de la `<saml:Assertion>` OU ajouter à la confirmation d'authentification dans l'attribut `<saml:AuthnContext>` un attribut supplémentaire `<saml:AuthenticatingAuthority>` avec l'`EntityID` de l'IdP/AP en tant que valeur (voir Listing 13).

```
<samlp:Response>
        ...
        <saml:Assertion>
                ...
                <saml:AuthnStatement
                        AuthnInstant="2020-12-05T09:23:50Z"
                        SessionIndex="234122">
                             <saml:AuthnContext>
                                 <saml:AuthnContextClassRef>
                                    urn:ech.ch/ech0170v2/vs3
                                 </saml:AuthnContextClassRef>
                                <saml:AuthenticatingAuthority>
                                        https://saml-idp-ap.example.com
                                </saml:AuthenticatingAuthority>
                        </saml:AuthnContext>
                </saml:AuthnStatement>
        </saml:Assertion>
</samlp:Response>
```

Listing 13: Confirmation d'authentification avec AuthenticatingAuthority (sources ouvertes)

Le Listing 14 illustre une `<samlp:Response>` selon le modèle de Broker Double Blinding. La confirmation d'authentification et d'attributs est envoyée à l'Attribute Consumer Service (ACS) du Relying Party.

```
<samlp:Response
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="we34-bhou-pyaq-gbhf"
    InResponseTo="ewda-e1df-xydg-xwsq"
    Version="2.0"
    IssueInstant="2020-12-05T09:23:59Z"
    Destination="https://saml-rp.example.com/SAML/ACS/Browser">
        <saml:Issuer>https://vermittler.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <saml:Assertion
        xmlns:xs="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:ech-0174="http://www.ech.ch/ech0174v2"
        ID="we34-bhou-pyaq-gbhf"
        Version="2.0"
        IssueInstant="2020-12-05T09:27:05Z">
        <saml:Issuer>https://vermittler.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
        <saml:Subject>
            <saml:NameID Format=
                "urn:oasis:names:tc:SAML:2.0:nameidformat:transient">
                wdrt-6gre-wcbp-ubwq-234gz
            </saml:NameID>
            <saml:SubjectConfirmation
                Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData
                    NotOnOrAfter="2020-12-05T09:37:05Z"
                    Recipient="https://saml-rp.example.com/SAML/ACS/POST"
                    InResponseTo="mkqs-ezew-qplo-snrt"/>
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions
            NotBefore="2020-12-05T09:27:05Z"
            NotOnOrAfter="2020-12-05T09:37:05Z">
            <saml:AudienceRestriction>
                <saml:Audience>
                    https://saml-rp.example.com
                </saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement
            AuthnInstant="2020-12-05T09:23:50Z"
            SessionIndex="234122">
            <saml:AuthnContext>
                <saml:AuthnContextClassRef>
                    urn:ech.ch/ech0170v2/vs1
                </saml:AuthnContextClassRef>
            </saml:AuthnContext>
        </saml:AuthnStatement>
        <saml:AttributeStatement>
            <saml:Attribute
                Nom=
                "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                <saml:AttributeValue
                      xsi:type="xs:StringMaxLength255MinLenght1"
                      ech0224:aq="2">
                    hans@example.com
                </saml:AttributeValue>
            </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>
```

Listing 14: Confirmation d'authentification & d'attributs du Broker au RP (Double Blinding)

6.3 Authentification avec transmission des attributs via une Attribute Query

Le Broker DOIT recevoir une demande d'authentification du RP. La demande d'authentification DOIT contenir un `<saml:AttributeConsumingServiceIndex>`.

Le Broker DOIT envoyer une nouvelle demande d'authentification (sans demande d'attributs) à l'IdP/AP et DOIT, en cas d'authentification réussie, recevoir un message `<samlp:Response>` avec une Authentication Assertion. Le Broker DOIT ensuite envoyer une demande d'attributs à l'IdP/AP et DOIT recevoir un message `<samlp:Response>` avec une Attribute Assertion. Le Broker DOIT combiner les Assertions reçues en une Authentication et Attribute Assertion et les renvoyer au RP dans un message `<samlp:Response>`.

Le Broker DOIT obtenir l'User Consent pour la transmission d'attributs auprès du RP. Pour ce faire, le Broker DOIT obtenir l'autorisation SOIT avant la demande d'attributs à l'IdP/AP, SOIT après la confirmation d'attributs de l'IdP/AP. Dans le cas où l'User Consent devait être obtenu après la réception des attributs, le Broker DOIT en outre afficher les valeurs des attributs pour l'utilisateur (voir chapitre 2.6).

6.3.1 Demande d'authentification et d'attributs du Relying Party (RP)

La procédure à suivre une fois reçue une `<samlp:AuthnRequest>` d'un RP est la même que celle du chapitre 6.1.1. Dans ce cas de figure, le AttributeConsumingServiceIndex ne contient **PAS** le Default (voir Listing 11). Le Broker dresse à présent une liste d'IdP/AP, qui, outre le niveau de confiance de l'authentification exigé, proposent également les attributs exigés.

6.3.2 Demande d'authentification à l'Identity & Attribute Provider (IdP/AP)

La procédure d'envoi d'une `<samlp:AuthnRequest>` à l'IdP/AP est la même qu'au chapitre 6.1.2. L'`<saml:AttributeConsumingServiceIndex>` n'est toutefois **PAS** repris de la `<samlp:AuthnRequest>` par le RP, mais DOIT être réglé sur Default.

6.3.3 Confirmation d'authentification de l'Identity & Attribute Provider (IdP/AP)

La procédure de réception d'une `<samlp:Response>` de l'IdP/AP est la même qu'au chapitre 6.1.3.

6.3.4 Demande d'attributs à l'Identity & Attribute Provider (IdP/AP)

Une fois reçue la confirmation d'authentification, le Broker crée une `<samlp:AttributeQuery>` (Listing 15). Le Broker détermine les attributs exigés via le `<saml:AttributeConsumingServiceIndex>` provenant de la `<samlp:AuthnRequest>` du RP.

Les attributs sont joints à la `<samlp:AttributeQuery>` comme `<saml:Attribute>`. La `<samlp:AttributeQuery>` est ensuite signée par le Broker et envoyée à l'Attribute Query Service (AQS) de l'Attribute Provider (AP).

```
<samlp:AttributeQuery
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:ech-0174 ="http://www.ech.ch/ech0174v2"
    ID="aafe-we23-enzz-d3et"
    Version="2.0"
    IssueInstant="2020-12-05T09:26:05Z"
    Destination="https://saml-idp-ap.example.com/SAML/AS/Browser">
    <saml:Issuer>https://vermittler.example.ch</saml:Issuer>
   <ds:Signature>...</ds:Signature>
   <saml:Subject>
       <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:
         nameid-format:unspecified">
         2347-0987-4few-cf643-jtf12swe
       </saml:NameID>
   </saml:Subject>
   <saml:Attribute
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
      ech0224:aq="2">
    </saml:Attribute>
</samlp:AttributeQuery>
```

Listing 15: Demande d’attributs du Broker à l’IdP/AP

6.3.5 Confirmation d'attributs de l'Identity & Attribute Provider (IdP/AP)

L'Attribute Consumer Service (ACS) du Broker reçoit une `<samlp:Response>` (Listing 16) de l'IdP/AP.

```
<samlp:Response
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="lnqw-xqap-xydg-kxsr"
    InResponseTo="aafe-we23-enzz-d3et"
    Version="2.0"
    IssueInstant="2020-12-05T09:23:59Z"
    Destination="https://vermittler.example.com/SAML/ACS/Browser">
        <saml:Issuer>https://saml-idp-ap.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <saml:Assertion
        xmlns:xs="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:ech-0174="http://www.ech.ch/ech0174v2"
        ID="lnqw-xqap-xydg-kxsr"
        Version="2.0"
        IssueInstant="2020-12-05T09:27:05Z">
        <saml:Issuer>https://saml-idp-ap.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
        <saml:Subject>
            <saml:NameID Format=
                "urn:oasis:names:tc:SAML:2.0:nameidformat:transient">
                wdrt-6gre-wcbp-ubwq-234gz
            </saml:NameID>
            <saml:SubjectConfirmation
                Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData
                    NotOnOrAfter="2020-12-05T09:37:05Z"
                    Recipient="https://saml-rp.example.com/SAML/ACS/POST"
                    InResponseTo="aafe-we23-enzz-d3et"/>
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions
            NotBefore="2020-12-05T09:27:05Z"
            NotOnOrAfter="2020-12-05T09:37:05Z">
            <saml:AudienceRestriction>
                <saml:Audience>
                    https://vermittler.example.com
                </saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AttributeStatement>
            <saml:Attribute
                Nom=
                "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                <saml:AttributeValue
                      xsi:type="xs:StringMaxLength255MinLenght1"
                      ech0224:aq="2">
                    hans@example.com
                </saml:AttributeValue>
            </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>
```

Listing 16: Confirmation d'attributs de l'IdP/AP au Broker

6.3.6 Confirmations d'authentification et d'attributs au Relying Party (RP)

Le Broker crée à présent une nouvelle Response à partir de la confirmation d'authentification et d'attributs de l'IdP/AP.

La nouvelle `<samlp:Response>` contient une `<saml:Assertion>`, qui combine les éléments `<saml:AuthnStatement>` (Listing 9) et `<AttributeStatement>` (Listing 16) à partir des Responses précédemment reçues. Le Relying Party requérant est défini comme `<samlp:Destination>`.

Selon le modèle de Broker, le Broker DOIT autoriser ou interdire l'identification de l'IdP/AP au RP:

Variante Double Blinding (chapitre 4.2.1)

L'IdP/AP NE DOIT PAS être identifiable par le RP.

Le Broker DOIT à nouveau signer la `<samlp:Response>` et la `<saml:Assertion>`.

Variante sources ouvertes (chapitre 4.2.2)[15]

L'IdP/AP DOIT être identifiable par le RP.

Dans la confirmation d'authentification, le Broker DOIT ajouter à l'attribut `<saml:AuthnContext>` un attribut supplémentaire `<saml:AuthenticatingAuthority>` avec l'IdP/AP comme valeur (voir Listing 13).

Le Listing 14 illustre une `<samlp:Response>` selon le modèle de Broker Double Blinding. La confirmation d'authentification et d'attributs est envoyée à l'Attribute Consumer Service (ACS) du Relying Party.

[15] La variante de transmission de signature n'est PAS prise en charge concernant l'authentification avec transmission des attributs via l'Attribute Query. Le Broker DOIT créer et signer une nouvelle `<saml:Assertion>` afin de pouvoir combiner les deux `<saml:Assertion>` de l'IdP/AP.

7 Interfaces pour l'Identity & Attribute Provider (IdP/AP)

Ce chapitre spécifie les interfaces avec l'IdP/AP. La procédure d'authentification via une infrastructure de Broker est définie au chapitre 4.1 et l'authentification avec transmission d'attributs au chapitre 4.2.

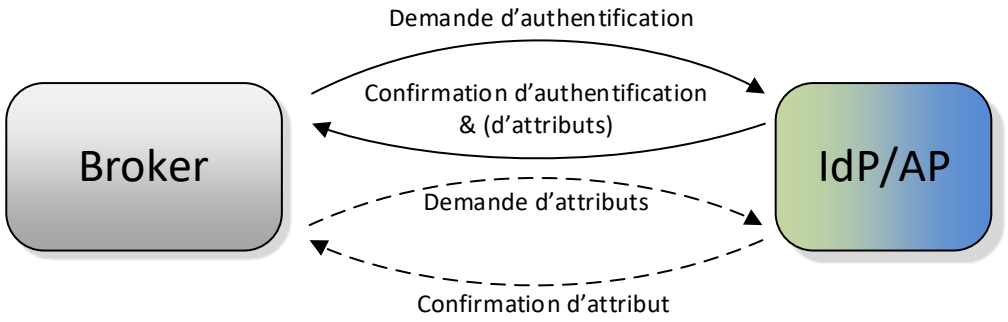

Figure 13: Vue d'ensemble des interfaces de l'Identity & Attribute Provider

Les chapitres suivants spécifient les interfaces pour l'IdP/AP. Les messages échangés par application sont définis du point de vue de l'Identity & Attribute Provider.

Le Tableau 8 indique dans quel chapitre sont spécifiées les demandes (ou réponses) correspondante de l'IdP/AP. Concernant la transmission d'attributs, l'IdP/AP DOIT prendre en charge soit l'Attribute Query soit la demande d'attributs au moyen du `AttributeConsumingServiceIndex`.

Authentification		Demande d'authentification du Broker	Chapitre 7.1.1
		Confirmation d'authentification du Broker	chapitre 7.1.2
Authentification avec transmission d'attributs	Attribute Consuming-ServiceIndex	Demande d'authentification et d'attributs du Broker	Chapitre 7.2.1
		Confirmation d'authentification et d'attributs au Broker	Chapitre 7.2.2
	Attribute Query	Demande d'authentification du Broker	Chapitre 7.3.1
		Confirmation d'authentification du Broker	Chapitre 7.3.2
		Demande d'attributs du Broker	Chapitre 7.3.3
		Confirmation d'attributs au Broker	Chapitre 7.3.4

Tableau 8: Vue d'ensemble des chapitres des interfaces de l'IdP/AP

7.1 Authentification

L'IdP/AP DOIT recevoir une demande d'authentification du Broker. L'IdP/AP DOIT enjoindre l'utilisateur de s'authentifier. En cas de succès de l'authentification, l'IdP/AP DOIT renvoyer un message `<samlp:Response>` au Broker avec une Authentication Assertion.

7.1.1 Demande d'authentification du Broker

Le service SSO de l'IdP/AP reçoit une `<samlp:AuthnRequest>` (Listing 17). L'IdP/AP DOIT enjoindre l'utilisateur de s'authentifier.[16]

Après une authentification réussie, l'utilisateur est authentifié par l'IdP/AP. Dans les rares cas exceptionnels où l'IdP/AP obtient le consentement de l'utilisateur lui-même, cela est noté dans les métadonnées de l'IdP/AP et le Broker ne demande pas d'autre consentement.

```
<samlp:AuthnRequest
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="mkqs-ezew-qplo-snrt"
    Version="2.0"
    IssueInstant="2020-12-05T09:22:30Z"
    Destination="https://saml-idp-ap.example.com/SAML/SSO/Browser"
    AssertionConsumerServiceURL="https://vermittler.example.com/SAML/ACS/Browser"
    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST">
    <saml:Issuer>https://vermittler.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
</samlp:AuthnRequest>
```

Listing 17: Demande d'authentification du Broker à l'IdP/AP

En cas d'échec de l'authentification[17] de l'utilisateur, l'IdP/AP DOIT créer une `<samlp:Response>` qui contient une annonce d'erreur selon les directives pour les Responses (chapitre 3.5).

[16] La méthode d'authentification doit être laissée à l'appréciation de l'IdP, mais doit correspondre au niveau de confiance assigné. Les méthodes courantes sont notamment Username/Password, basé sur PKI, 2FA, etc.

[17] L'IdP/AP définit quand une authentification est considérée comme échouée. Il peut s'agir, par exemple, d'une mauvaise authentification, d'un dépassement de délai, d'une annulation de l'utilisateur ou d'un dépassement du nombre maximal de tentatives.

7.1.2 Confirmation d'authentification du Broker

L'IdP crée une `<samlp:Response>` qui contient un `<saml:AuthnStatement>` dans une `<saml:Assertion>` (Listing 18).
La `<samlp:Response>` et la `<saml:Assertion>` sont signées par l'IdP/AP signe et renvoyées à l'ACS du Broker.

```
<samlp:Response
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="lnqw-xqap-xydg-kxsr"
    InResponseTo="mkqs-ezew-qplo-snrt"
    Version="2.0"
    IssueInstant="2020-12-05T09:23:59Z"
    Destination="https://vermittler.example.com/SAML/ACS/Browser">
        <saml:Issuer>https://saml-idp-ap.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <saml:Assertion
        xmlns:xs="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:ech-0174="http://www.ech.ch/ech0174v2"
        ID="we34-bhou-pyaq-gbhf"
        Version="2.0"
        IssueInstant="2020-12-05T09:27:05Z">
        <saml:Issuer>https://saml-idp-ap.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
        <saml:Subject>
            <saml:NameID Format=
                "urn:oasis:names:tc:SAML:2.0:nameidformat:transient">
                wdrt-6gre-wcbp-ubwq-234gz
            </saml:NameID>
            <saml:SubjectConfirmation
                Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData
                    NotOnOrAfter="2020-12-05T09:37:05Z"
                    Recipient="https://vermittler.example.com/SAML/ACS/POST"
                    InResponseTo="mkqs-ezew-qplo-snrt"/>
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions
            NotBefore="2020-12-05T09:27:05Z"
            NotOnOrAfter="2020-12-05T09:37:05Z">
            <saml:AudienceRestriction>
                <saml:Audience>
                    https://vermittler.example.com
                </saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement
            AuthnInstant="2020-12-05T09:23:50Z"
            SessionIndex="234122">
            <saml:AuthnContext>
                <saml:AuthnContextClassRef>
                    urn:ech.ch/ech0170v2/vs1
                </saml:AuthnContextClassRef>
            </saml:AuthnContext>
        </saml:AuthnStatement>
    </saml:Assertion>
</samlp:Response>
```

Listing 18: Confirmation d'authentification de l'IdP/AP au Broker

7.2 Authentification avec demande d'attributs via le AttributeConsumingServiceIndex

L'IdP/AP DOIT recevoir une demande d'authentification du Broker. L'IdP/AP DOIT enjoindre l'utilisateur de s'authentifier. En cas d'authentification réussie, l'IdP/AP DOIT renvoyer un message `<samlp:Response>` au Broker avec une Authentication et Attribute Assertion.

7.2.1 Demande d'authentification et d'attributs du Broker

La procédure à suivre une fois reçue une `<samlp:AuthnRequest>` du Broker est la même que celle du chapitre 7.1.1. En outre, le `<saml:AttributeConsumingServiceIndex>` détermine les attributs définis et vérifie que l'utilisateur dispose bien de cet attribut.

7.2.2 Confirmation d'authentification et d'attributs au Broker

L'IdP/AP crée à présent la confirmation d'authentification et d'attributs, qui contient une `<saml:Assertion>` avec `<saml:AuthnStatement>` et `<saml:AttributeStatement>` (Listing 19). L'élément `<saml:AttributeStatement>` contient les attributs exigés dans la `<samlp:AuthnRequest>` en tant que `<saml:Attribute>` avec la `<saml:AttributeValue>`.

La `<samlp:Response>` et la `<saml:Assertion>` sont signées par l'IdP/AP et renvoyées à l'Attribute Consumer Service (ACS) du Broker.

```
<samlp:Response
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="lnqw-xqap-xydg-kxsr"
    InResponseTo="mkqs-ezew-qplo-snrt"
    Version="2.0"
    IssueInstant="2020-12-05T09:23:59Z"
    Destination="https://vermittler.example.com/SAML/ACS/Browser">
        <saml:Issuer>https://saml-idp-ap.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <saml:Assertion
        xmlns:xs="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:ech-0174="http://www.ech.ch/ech0174v2"
        ID="we34-bhou-pyaq-gbhf"
        Version="2.0"
        IssueInstant="2020-12-05T09:27:05Z">
        <saml:Issuer>https://saml-idp-ap.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
        <saml:Subject>
            <saml:NameID Format=
                "urn:oasis:names:tc:SAML:2.0:nameidformat:transient">
                wdrt-6gre-wcbp-ubwq-234gz
            </saml:NameID>
            <saml:SubjectConfirmation
                Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData
                    NotOnOrAfter="2020-12-05T09:37:05Z"
                    Recipient="https://saml-rp.example.com/SAML/ACS/POST"
                    InResponseTo="mkqs-ezew-qplo-snrt"/>
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions
            NotBefore="2020-12-05T09:27:05Z"
            NotOnOrAfter="2020-12-05T09:37:05Z">
            <saml:AudienceRestriction>
                <saml:Audience>
                    https://vermittler.example.com
                </saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement
            AuthnInstant="2020-12-05T09:23:50Z"
            SessionIndex="234122">
            <saml:AuthnContext>
                <saml:AuthnContextClassRef>
                    urn:ech.ch/ech0170v2/vs1
                </saml:AuthnContextClassRef>
            </saml:AuthnContext>
        </saml:AuthnStatement>
        <saml:AttributeStatement>
            <saml:Attribute
                Nom=
                "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                <saml:AttributeValue
                      xsi:type="xs:StringMaxLength255MinLenght1"
                      ech0224:aq="2">
                    hans@example.com
                </saml:AttributeValue>
            </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>
```

Listing 19: Confirmations d’authentification et d’attributs de l’IdP/AP au Broker

7.3 Authentification avec demande d'attributs via une Attribute Query

L'IdP/AP DOIT recevoir une demande d'authentification du Broker. L'IdP/AP DOIT enjoindre l'utilisateur de s'authentifier. En cas de succès de l'authentification, l'IdP/AP DOIT renvoyer un message `<samlp:Response>` au Broker avec une Authentication Assertion. Une fois la confirmation d'authentification transmise, l'IdP/AP DOIT recevoir une demande d'attributs du Broker. L'IdP/AP DOIT créer un message `<samlp:Response>` avec une Attribute Assertion et la renvoyer au Broker.

7.3.1 Demande d'authentification du Broker

La procédure de réception d'une `<samlp:Response>` du Broker est la même qu'au chapitre 7.1.1.

7.3.2 Confirmation d'authentification du Broker

La création de la confirmation d'authentification est la même qu'au chapitre 7.1.2.

7.3.3 Demande d'attributs du Broker

L'Attribute Query Service (AQS) de l'IdP/AP reçoit une `<samlp:AttributeQuery>` (Listing 20). Les attributs requis sont répertoriés en tant que `<saml:Attribute>`. L'IdP/AP vérifie si l'utilisateur dispose des attributs définis dans les `<saml:Attributes>`.

```
<samlp:AttributeQuery
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:ech-0174 ="http://www.ech.ch/ech0174v2"
    ID="aafe-we23-enzz-d3et"
    Version="2.0"
    IssueInstant="2020-12-05T09:26:05Z"
    Destination="https://saml-idp-ap.example.com/SAML/AS/Browser">
    <saml:Issuer>https://vermittler.example.ch</saml:Issuer>
   <ds:Signature>...</ds:Signature>
   <saml:Subject>
       <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:
         nameid-format:unspecified">
         2347-0987-4few-cf643-jtf12swe
       </saml:NameID>
   </saml:Subject>
   <saml:Attribute
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
      ech0224:aq="2">
    </saml:Attribute>
</samlp:AttributeQuery>
```

Listing 20: Demande d'attributs du Broker à l'IdP/AP

7.3.4 Confirmation d'attributs au Broker

L'IdP/AP crée une `<samlp:Response>` (Listing 21) à partir de la liste des attributs répertoriés dans l'Attribute Query (Listing 20). Pour la Response, l'IdP/AP compile une `<saml:Assertion>`, qui contient un `<saml:AttributeStatement>` avec des éléments `<saml:Attribute>` et `<saml:AttributeValue>`. La `<saml:Assertion>` et `<samlp:Response>` sont signées par l'IdP/AP et envoyées à l'ACS du Broker.

Dans le cas où les attributs demandés ne sont pas transmis, une `<samlp:Response>` DOIT être envoyée avec après le `<samlp:StatusCode>` selon le chapitre 3.5 au Broker.

```
<samlp:Response
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="lnqw-xqap-xydg-kxsr"
    InResponseTo="aafe-we23-enzz-d3et"
    Version="2.0"
    IssueInstant="2020-12-05T09:23:59Z"
    Destination="https://vermittler.example.com/SAML/ACS/Browser">
        <saml:Issuer>https://saml-idp-ap.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <saml:Assertion
        xmlns:xs="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:ech-0174="http://www.ech.ch/ech0174v2"
        ID="lnqw-xqap-xydg-kxsr"
        Version="2.0"
        IssueInstant="2020-12-05T09:27:05Z">
        <saml:Issuer>https://saml-idp-ap.example.com</saml:Issuer>
        <ds:Signature>...</ds:Signature>
        <saml:Subject>
            <saml:NameID Format=
                "urn:oasis:names:tc:SAML:2.0:nameidformat:transient">
                wdrt-6gre-wcbp-ubwq-234gz
            </saml:NameID>
            <saml:SubjectConfirmation
                Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData
                    NotOnOrAfter="2020-12-05T09:37:05Z"
                    Recipient="https://saml-rp.example.com/SAML/ACS/POST"
                    InResponseTo="aafe-we23-enzz-d3et"/>
            </saml:SubjectConfirmation>
        </saml:Subject>
            <saml:Conditions
            NotBefore="2020-12-05T09:27:05Z"
            NotOnOrAfter="2020-12-05T09:37:05Z">
            <saml:AudienceRestriction>
                <saml:Audience>
                    https://vermittler.example.com
                </saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AttributeStatement>
            <saml:Attribute
                Nom=
                "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                <saml:AttributeValue
                      xsi:type="xs:StringMaxLength255MinLenght1"
                      ech0224:aq="2">
                    hans@example.com
                </saml:AttributeValue>
            </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>
```

Listing 21: Confirmation d'attributs de l'IdP/AP au Broker

8 Métadonnées

Chaque composant du domaine (Broker, IdP, IdP/AP, RP) qui dispose de services SAML doit déposer les informations nécessaires à ces services dans la base de données (métadonnées) du Broker.[18] Ces informations spécifiques aux composants sont généralement saisies manuellement via une GUI par une personne habilité à le faire.[19]

Les métainformations de tous les composants SAML sont collectées par les administrateurs compétents.

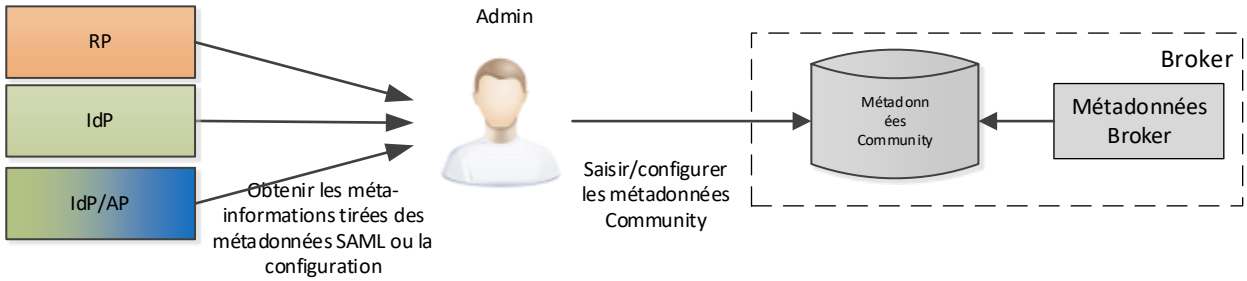

Figure 14: Collecte de métainformations auprès du Broker.

Outre les métadonnées SAML, des informations supplémentaires relatives aux différents composants sont enregistrés dans une base de données (gestion des composants) du Broker. C'est ici que sont enregistrées les exigences en matière de ressources des RP et les offres des IdP ou des IdP/AP.

8.1 Métadonnées Community

Les différents composants d'une organisation, soit IdP, IdP/AP et Relying Party (RP) sont gérés dans les métadonnées Community. En outre, les exigences relatives aux ressources dans le cas d'un Relying Party et les niveaux de confiance proposés pour l'authentification et les attributs dans le cas d'un IdP/AP sont conservés. À titre d'alternative, les participants d'un domaine peuvent convenir d'un niveau de confiance qui s'applique alors à tous.

8.1.1 Relying Party

Pour une Relying Party, il faut définir un Service Provider Service qui reçoit les Authentication et Attribute Assertions. Une ou plusieurs ressources peuvent être définies sous le Service Provider.

Pour le Service Provider Service, les points définis sont les suivants:

- Métadonnées SAML: les métadonnées du RP, y compris les informations sur les clés[20] pour le

[18] Dans le cas où l'Identity Federation comprend plusieurs domaines, les métadonnées de chaque domaine DOIVENT être gérées et publiées séparément.

[19] À titre d'alternative, ces informations pourraient aussi être générées localement au niveau du composant et téléchargées dans le Broker via une interface spécifiée. Cette fonction d'upload et le traitement de ces métadonnées au niveau du Broker sont facultatifs.

[20] ainsi que la procédure pour l'échange de clés etc., doivent être réglées dans le domaine. Un exemple de directive correspondante est disponible sur le site de Switch: https://www.switch.ch/aai/guides/sp/certificate-rollover/.

chiffrement et la vérification de la signature,

- AssertionConsumerService: URI du Service Provider Service,[21]

- (facultatif) Indique si les Assertions chiffrées sont prises en charge.

Pour chaque ressource, on définit:

- Niveau de confiance requis[22] de l'authentification selon la norme eCH-0170 [13],
- Liste des attributs demandés, le cas échéant, avec qualité d'attribut (voir également la directive 5 au chapitre 3.1)[23],
- (facultatif) Liste hiérarchisée des IdP/AP acceptés.

8.1.2 IdP & IdP/AP

Pour un IdP, les points suivants sont définis:

- Métadonnées SAML: les métadonnées de l'IdP, y compris les informations sur les clés pour le chiffrement et la vérification de la signature,
  - les points finaux pour l'AuthenticationService et, à titre facultatif, pour le SingleLogoutService
- Niveau de confiance soutenu lors de l'authentification

Si un IdP agit en tant que IdP/AP, les points suivants doivent également être définis:

- les métadonnées SAML du Attribute Query Service
- les attributs proposés avec leur qualité selon le modèle de qualité proposé dans la directive 5 (voir chapitre 3.1).

8.2 Métadonnées SAML

Le Broker doit disposer des métainformations des services SAML de tous les composants du domaine (voir également [20]). Les composants SAML périphériques exigent toutefois aussi certaines informations de la part des différents composants:

- Les RP doivent connaître les métainformations des services SSO du Broker.
  - Dans le modèle de Broker Sources ouvertes avec transmission de signature, les RP doivent également connaître les Public Keys des IdP/AP pour vérifier la signature des Assertions.
- Les IdP et les IdP/AP doivent connaître les métainformations des ACS Services du Broker.

Tous les composants périphériques prenant en charge SAML 2.0, ces métainformations peuvent être

[21] L'URI peut être indiqué pour le SingleLogoutService du Service Provider, dans le cas où le SingleLogout doit être pris en charge,

[22] En cas normal, seuls les niveaux de confiance VS1 à VS3 sont utilisés, car le niveau de confiance 4 impose des exigences supplémentaires tant au RP qu'aux autres composants dans le domaine.

[23] Pour chaque jeu d'attribut exigé, un élément `<md:AssertionConsumerService>` correspondant doit être défini dans les métadonnées SAML. L'élément Default `<md:AssertionConsumerService>` devrait correspondre à une authentification sans attribut.

distribuées au moyen de métadonnées SAML. La préparation des métadonnées SAML nécessaires est effectuée par un Metadata Aggregator Service.[24] Il faut à cette fin que ce service publie périodiquement les informations sous forme signée, relatives au Broker et aux IdP et IdP/AP connectés. Ces métadonnées SAML peuvent ensuite être récupérées par les membres du domaine, validées et intégrées par ces derniers.

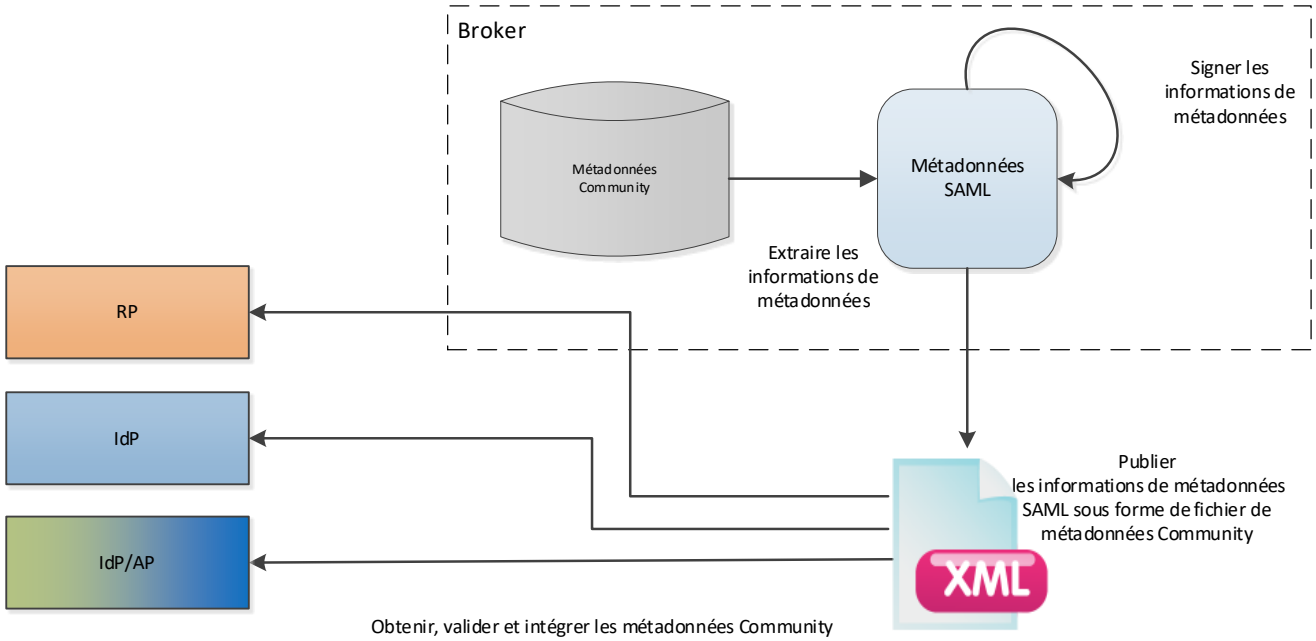

Figure 15: Publication des métadonnées SAML

De cette façon, les membres du domaine ont à leur disposition toutes les informations nécessaires pour pouvoir communiquer avec le Broker via SAML 2.0.

Les métadonnées SAML contiennent toutes les informations nécessaires concernant les services SAML du Broker et les IdP ou IdP/AA. Elles sont créées, signées et publiées selon un rythme périodique par le Metadata Aggregator Service.

Le Listing 22 présente un exemple de fichier de métadonnées SAML publié par le Metadata Aggregator Service.

Un fichier de métadonnées SAML contient un élément `<md:EntitiesDescriptor>`, qui contient le `<md:EntityDescriptor>` du Broker (SSO et ACS) ainsi le SSO de tous les IdP ou IdP/AP. L'attribut `validUntil` indique la période de validité du fichier de métadonnées de la SAML Community et l'attribut `cacheDuration` la durée maximale de la période, au cours de laquelle les composants de domaine devraient enregistrer le fichier de métadonnées SAML.

[24] Le Metadata Aggregator Service peut également être mis en œuvre en tant que composant séparé, indépendamment du Broker.

```
<md:EntitiesDescriptor
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    validUntil="2017-02-20T23:00:00Z"
    cacheDuration="PT24H"
    ID="csxy-3wwa-qy01-ewda-e1df-xydg">

    <ds:Signature>...</ds:Signature>

    <!-- Broker -->
    <md:EntityDescriptor
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="eenl-4ftv-7uqa-lmg3-q123-vsaq"
    entityID="https://vermittler.example.com">
     ...
    </md:EntityDescriptor>

    <!-- IdP/AP -->
    <md:EntityDescriptor
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="eenl-2rxp-7uqa-q123-tecm"
    entityID="https://saml-idp-ap.example.com">
     ...
    </md:EntityDescriptor>
</md:EntitiesDescriptor>
```

Listing 22: Fichier de métadonnées SAML

8.2.1 Directives concernant les métadonnées SAML

Les métadonnées SAML à publier sont décrites plus avant ci-dessous. Elles contiennent notamment des informations sur:

L'adresse et le nom de l'entité (composant).
Les configurations de point final de l'entité (URL).
Les certificats Public Key pour vérifier les SAML Messages signés.
Les certificats Public Key pour vérifier les SAML Assertions signées.
Attributs SAML qui peuvent être consommés/générés par l'entité.

8.2.2 Règles générales concernant les éléments `<md:EntityDescriptor>`

- La définition des métadonnées Broker DOIT commencer par un élément `<md:EntityDescriptor>` .
- L'élément `<md:EntityDescriptor>` DOIT avoir un attribut `entityID`. Sa valeur DOIT être un URI, sans équivoque dans le domaine, qui doit être utilisée comme identificateur.
- Dans l'élément`<md:EntityDescriptor>`, un élément `<Extensions>` doit être indiqué avec l'*Authentication Assurance Level* pris en charge par le Broker ou l'IdP/AP, selon *SAMLV2.0 Identity Assurance Profiles* [11].
- L'élément `<md:EntityDescriptor>` PEUT contenir un ou plusieurs éléments de type `<md:IDPSSODescriptor>`, `<md:SPSSODescriptor>` ou `<md:AttributeAuthorityDescriptor>` .
- L'élément `<md:EntityDescriptor>` PEUT contenir un élément `<md:Organization>` qui à son tour présente un `<md:OrganizationName>` et un `<md:OrganizationURL>` .
- Un élément `<md:OrganizationDisplayName>` et un élément`<md:ContactPerson>` sont FACULTATIFS.

8.2.3 Règles concernant les métadonnées Broker

IDPSSODescriptor:

L'IDPSSODescriptor décrit les métainformations SSO du Broker.

- L'élément `<md:EntityDescriptor>` du Broker DOIT contenir un élément de type `<md:IDPSSODescriptor>` et un élément de type `<md:SPSSODescriptor>`.
- L'élément `<md:IDPSSODescriptor>` DOIT avoir un attribut `protocolSupportEnumeration`, dont la valeur DOIT être `urn:oasis:names:tc:SAML:2.0:protocol`.
- L'attribut `WantAuthnRequestsSigned` de l'élément `<md:IDPSSODescriptor>` DOIT être réglé sur `true`. Cela signifie que les RP DOIVENT signer l'Authentication Request (`<samlp:AuthnRequest>`), faute de quoi elle n'est pas acceptée par le Broker.
- L'élément `<md:KeyDescriptor>` pour la signature DOIT être présent dans le `<md:IDPSSODescriptor>`. Sa `<ds:KeyInfo>` DOIT contenir un élément `<ds:X509Data>` et ce dernier un `<ds:X509Certificate>`.
- L'élément `<md:IDPSSODescriptor>` DOIT contenir un ou plusieurs éléments `<md:SingleSignOnService>`.
- L'élément `<md:IDPSSODescriptor>` DOIT contenir un ou plusieurs éléments `<md:SingleLogOutService>`.[25]
- L'élément `<md:IDPSSODescriptor>` DOIT contenir plusieurs éléments `<md:NameIDFormat>`. `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` et `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` DOIVENT être pris en charge [14].

SPSSODescriptor:

Le SPSSODescriptor décrit les métainformations Service Provider du Broker.

- L'élément `<md:SPSSODescriptor>` du Broker DOIT avoir un attribut `protocolSupportEnumeration`, dont la valeur DOIT être `urn:oasis:names:tc:SAML:2.0:protocol`.
- L'attribut `WantAssertionsSigned` de l'élément`<md:SPSSODescriptor>` DOIT être placé sur `true`.
- L'attribut `AuthnRequestsSigned` de l'élément`<md:SPSSODescriptor>` DOIT être réglé sur `true`.
- L'élément `<md:KeyDescriptor>` pour la signature DOIT figurer dans `<md:SPSSODescriptor>`. Sa `<ds:KeyInfo>` DOIT contenir un élément `<ds:X509Data>` et ce dernier un `<ds:X509Certificate>`.
- L'élément `<md:SPSSODescriptor>` DOIT contenir un ou plusieurs éléments `<md:AssertionConsumerService>`[26]. L'attribut `index` DOIT figurer dans chaque élément `<md:AssertionConsumerService>`. Le Protocol Binding `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST` DOIT être pris en charge.
- L'élément `<md:SPSSODescriptor>` DOIT contenir au moins un élément `<md:NameIDFormat>` . `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` et `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` DOIVENT être pris en charge [14].

[25] Une description de la mise en œuvre de SLO dans une Identity Federation dépasserait le cadre de la norme et n'est donc pas incluse.

[26] L'élément Default `<md:AssertionConsumerService>` devrait correspondre à une authentification sans attributs. D'autres éléments doivent être définis pour les jeux d'attributs requis des RP connectés.

```
<md:EntityDescriptor
   xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
   xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute"
   ID="eenl-4ftv-7uqa-lmg3-q123-vsaq"
   entityID="https://vermittler.example.com">
   <md:IDPSSODescriptor
        WantAuthnRequestsSigned="true"
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <md:KeyDescriptor use="signing">
            <ds:KeyInfo> ... </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:NameIDFormat>
           urn:oasis:names:tc:SAML:2.0:nameid-format:transient
        </md:NameIDFormat>
        <md:NameIDFormat>
           urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
        </md:NameIDFormat>
        <md:SingleSignOnService
           Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
           Location="https://vermittler.example.com/SAML/SSO/Browser"/>
        <md:SingleSignOnService
           Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
           Location="https://vermittler.example.com/SAML/SSO/Browser"/>
   </md:IDPSSODescriptor>
   <md:SPSSODescriptor
        AuthnRequestsSigned="true"  WantAssertionsSigned="true"
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <md:KeyDescriptor use="signing">
            <ds:KeyInfo> ... </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:NameIDFormat>
            urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
        </md:NameIDFormat>
        <md:AssertionConsumerService isDefault="true"  index="1"
                 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                 Location="https://saml-idp-ap.example.com/SAML/ACS/POST"/>
        <md:AttributeConsumingService index="1" isDefault="true">
            <md:ServiceName xml:lang="en">vermittler.example.com</md:ServiceName>
        </md:AttributeConsumingService>
   </md:SPSSODescriptor>
  <md:Organization>
        <md:OrganizationName xml:lang="en">
            Broker Provider
        </md:OrganizationName>
        <md:OrganizationDisplayName xml:lang="en">
            Broker Service Provider Example Name
        </md:OrganizationDisplayName>
        <md:OrganizationURL xml:lang="en">
            https://vermittler.example.com
        </md:OrganizationURL>
  </md:Organization>
  <md:ContactPerson contactType="administrative">
        <md:GivenName>Hans</md:GivenName>
        <md:SurName>Muster</md:SurName>
        <md:EmailAddress>hansm@gov.ch</md:EmailAddress>
  </md:ContactPerson>

</md:EntityDescriptor>
```

Listing 23: Exemple d’un Broker EntityDescriptors

8.2.4 Règles concernant les métadonnées IdP/AP

L'élément `<md:EntityDescriptor>` d'un IdP/AP DOIT contenir un élément `<md:IDPSSODescriptor>` avec les renseignements suivants (voir à ce sujet Listing 24) et PEUT contenir un élément `<md:AttributeAuthorityDescriptor>` .

- L'élément `<md:IDPSSODescriptor>` DOIT avoir un attribut `protocolSupportEnumeration`, dont la valeur DOIT être`urn:oasis:names:tc:SAML:2.0:protocol`.
- L'attribut `WantAuthenticationRequestsSigned` de l'élément `<md:IDPSSODescriptor>` DOIT être réglé sur `true`.
- L'élément `<md:KeyDescriptor>` pour la signature DOIT être présent dans le `<md:IDPSSODescriptor>`. Sa `<ds:KeyInfo>` DOIT contenir un élément `<ds:X509Data>` et ce dernier un `<ds:X509Certificate>`.
- L'élément `<md:IDPSSODescriptor>` DOIT contenir un ou plusieurs éléments `<md:SingleSignOnService>`. Le HTTP-POST Protocol Binding DOIT être pris en charge.
- L'élément PEUT `<md:IDPSSODescriptor>` contenir plusieurs éléments `<md:NameIDFormat>`. `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` DOIT être pris en charge et `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` PEUT être pris en charge [14].

À titre facultatif, un `<md:AttributeAuthorityDescriptor>` peut être défini lorsque l'IdP/AP prend en charge les AttributQueries.

- L'élément `<md:AttributeAuthorityDescriptor>` DOIT avoir un attribut `protocolSupportEnumeration`, dont la valeur DOIT être `urn:oasis:names:tc:SAML:2.0:protocol`.
- L'élément `<md:KeyDescriptor>` pour la signature DOIT figurer dans le `<md:AttributeAuthorityDescriptor>`. Sa `<ds:KeyInfo>` DOIT contenir un élément `<ds:X509Data>` et ce dernier un `<ds:X509Certificate>`
- L'élément `<md:AttributeAuthorityDescriptor>` DOIT contenir au moins un élément `<md:AttributeService>`.

```
<md:EntityDescriptor
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
       xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute"

             ID="eenl-2rxp-7uqa-q123-tecm"
             entityID="https://idp.gov.ch">

  <md:IDPSSODescriptor
           WantAuthnRequestsSigned="true"
           protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

           <md:KeyDescriptor use="signing">
               <ds:KeyInfo>
                  <ds:X509Data>
                        <ds:X509Certificate>
                              ...
                        </ds:X509Certificate>
                   </ds:X509Data>
               </ds:KeyInfo>
           </md:KeyDescriptor>

           <md:NameIDFormat>
               urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
         </md:NameIDFormat>

           <md:SingleSignOnService
               Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
               Location="https://saml-idp-ap.example.com/SAML/SSO/Browser"/>
     </md:IDPSSODescriptor>

  <md:AttributeAuthorityDescriptor
          protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
              <md:KeyDescriptor use="signing">
              <ds:KeyInfo>
                  <ds:X509Data>
                      <ds:X509Certificate>
                          ...
                      </ds:X509Certificate>
                  </ds:X509Data>
              </ds:KeyInfo>
          </md:KeyDescriptor>
      <md:AttributeService
              Location="https://saml-idp-ap.example.com/AAService"
              Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
      ...
  </md:AttributeAuthorityDescriptor>
</md:EntityDescriptor>
```

Listing 24: Exemple d'un IdP/AP EntityDescriptor

9 Sécurité

L'enregistrement et le transfert de données à caractère personnel ne sont autorisés que sur la base et dans le cadre des principes légaux en vigueur et doivent se conformer aux dispositions légales en matière de protection des données. Les mesures nécessaires doivent être prises afin que les données puissent être transférées sans erreur et avant, pendant et après le transfert, ne puissent être consultées et modifiées que par des personnes qui y sont habilitées.

Dans le cas où un système IAM est mis en œuvre conformément à la LSIE [21] ou aux lois semblables, 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.

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 réglementations 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 et bibliographie

[1]	IETF, «RFC 2119,» 1997. [Online]. Available: http://www.ietf.org/rfc/rfc2119.txt.
[2]	eCH, «eCH-0219 Glossaire IAM, version 1.0,» 30 novembre 2018. [Online]. Available: https://ech.ch/fr/standards/60491.
[3]	eCH, «eCH-0224 Modèles d'architecture Identity Federation impliquant un Broker, version 1.0,» 5 juin 2020. [Online]. Available: https://ech.ch/fr/standards/60586.
[4]	OASIS, «Security Assertion Markup Language (SAML) V2.0 Technical Overview,» 25 March 2008. [Online]. Available: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html.
[5]	J. B. M. J. B. d. M. a. C. M. N. Sakimura, «OpenID Connect Core 1.0 incorporating errata set 1,» 8 November 2014. [Online]. Available: https://openid.net/specs/openid-connect-core-1_0.html.
[6]	eCH, «eCH-0225 Identity Federations impliquant un Broker – Implémentation avec OIDC,» 2020.
[7]	eCH, «eCH-0107 Principes de conception pour l'administration des identité et des accès (IAM), version 3.0,» 7 février 2019. [Online]. Available: https://ech.ch/fr/standards/60198.
[8]	eCH, «eCH-0167 Concept cadre SuisseTrustIAM,» 6 juin 2014. [Online]. Available: https://ech.ch/fr/standards/60432.
[9]	eCH, «eCH-0168 Architecture et processus SuisseTrustIAM,» 27 novembre 2014. [Online]. Available: https://ech.ch/fr/standards/60577.
[10]	eCH, «eCH-0169 Architecture administrative de SuisseTrustIAM V1.0,» 4 septembre 2014. [Online]. Available: https://ech.ch/fr/standards/60409.
[11]	«SAML V2.0 Identity Assurance Profiles Version 1.0,» 2010. [Online]. Available: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.pdf.
[12]	OASIS, 10 August 2010. [Online]. Available: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-holder-of-key-browser-sso.pdf.
[13]	eCH, «eCH-0170 Modèle de qualité eID, version 2.0,» 13 septembre 2017. [Online]. Available: https://ech.ch/fr/standards/60593.
[14]	OASIS, «Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 – Errata Composite,» 07 septembre 2012. [Online]. Available: https://www.oasis-open.org/committees/download.php/56777/sstc-saml-core-errata-2.0-wd-07-diff.pdf.
[15]	B. D. E. S. K. Y. a. M. N. Takeshi Imamura, «XML Encryption Syntax and Processing Version 1.1,» 11 April 2013. [Online]. Available: https://www.w3.org/TR/xmlenc-core1/.
[16]	J. B. B. F. B. L. a. E. S. Mark Bartel, «XML Signature Syntax and Processing Version 1.1,» 11 April 2013. [Online]. Available: https://www.w3.org/TR/xmldsig-core/.

[17]	eCH, «eCH-0091 Norme de signature et de chiffrement XML V2.0.0,» 2 avril 2021. [Online]. Available: https://ech.ch/fr/standards/60522.
[18]	OASIS, «SAML Implementation Guidelines,» 27 Augst 2004. [Online]. Available: https://www.oasis-open.org/committees/download.php/8958/sstc-saml-implementation-guidelines-draft-01.pdf.
[19]	OASIS, «Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0,» 15 March 2005. [Online]. Available: http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf.
[20]	OASIS (Rainer Hörber), «SAML V2.0 Metadata Guide,» 08 01 2014. [Online]. Available: https://www.oasis-open.org/committees/download.php/51890/SAML%20MD%20simplified%20overview.pdf.
[21]	Département fédéral de la justice et de la police DFJP, «Loi fédérale sur les services d'identification électronique (LSIE),» [Online]. Available: https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/e-id.html.
[22]	OASIS, «Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard,» March 2005. [Online]. Available: http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.
[23]	eCH, «eCH-0048 Classes de certificat PKI V2.0,» 30 11 2018. [Online]. Available: https://ech.ch/fr/standards/60507.

Annexe B – Collaboration & vérification

Bracklo Sven	Haute école spécialisée de Berne
Hassenstein Gerhard	Haute école spécialisée de Berne
Kunz Marc	Membre eCH FG IAM
Laube-Rosenpflanzer Annett	Haute école spécialisée de Berne

Annexe C – Abréviations et glossaire

ACS	Assertion Consumer Service
AQS	Attribute Query Service
AP	Attribute Provider
HoK	Holder-of-Key
IAM	Identity and Access Management
IdP	Identity Provider
SSO	Single-Sign-on
SLO	Single Logout
SAML	Security Assertion Markup Language
URL	Uniform Resource Locator
URI	Uniform Resource Indicator
UTC	Coordinated Universal Time
RP	Relying Party

Ce document utilise essentiellement les définitions terminologiques de la norme eCH-0219 [2].

Annexe D – Modifications par rapport à la version précédente

La présente norme décrit la mise en œuvre des modèles d'Identity Federations impliquant un Broker figurant dans la norme eCH-0224 [3]. La version 1.0 reposait sur le modèle d'architecture de Suisse-Trust Identity and Access Management (STIAM) décrit dans eCH-0168 [9]..

En raison du changement de modèle architectural, la structure des chapitres a elle aussi été modifiée et la norme a été structurée de manière semblable à la norme eCH-0225 [6], qui décrit la mise en œuvre OIDC des modèles d'Identity Federations impliquant un Broker de la norme eCH-0224.

Les modifications générales sont énumérées ci-dessous et font référence aux contenus respectifs de la version 1.00 de la norme eCH-0174.

Principes:

La version V2.0.0 est donc cantonnée à la mise en œuvre des modèles d'Identity Federations impliquant un Broker de la norme eCH-0224, les variantes décrites étant déjà mises en œuvre dans la pratique.
Le titre de la norme a été modifié en conséquence.
Toute la terminologie STIAM a été systématiquement remplacée par celle utilisée dans la norme eCH-0224 [3].
La version actualisée de la présente norme ayant notamment pour objectif l'indépendance vis-à-vis des normes STIAM, telles que eCH-0168 [9], certaines parties ont été reprises de eCH-0168 sous une forme actualisée.

Chapitre	Page	Adaptation	No. RFC
1.2	6	Introduction [eCH-0174 V1.0 chapitre 1] L'introduction a été entièrement retravaillée et adaptée au nouveau contenu.	-
0	10	Identity Federations basées sur SAML [eCH-0174 V1.0 chapitre 3 et 4] • Le chapitre 2 décrit les différents services SAML que doivent fournir les différents composants, ainsi que les interactions de ces services, seuls les processus de la période d'exécution des modèles de Broker de la norme eCH-0224 étant pris en compte. • Les protocoles suivants tirés de la norme eCH-0174 v1.0 n'ont pas été repris dans la version v2.0, car ceux-ci ne revêtent aucune importance pratique. - Concernant la période d'exécution: ○ Single Logout - Concernant la période de définition: ○ IdP Linking,	-

Chapitre	Page	Adaptation	No. RFC
		○ AA Linking, ○ RP Linking.	
3	23	**Directives [eCH-0174 V1.0 chapitre 2 et 6]** Le chapitre contient les exigences définies dans la norme eCH-0174 V1.0 chapitre 2, sous réserve qu'elles ne figurent pas déjà dans la norme eCH-0107 v3.0 [7] ou eCH-0224 [3]. Des directives, qui doivent être respectées, afin de satisfaire aux exigences imposées à une Identity Federation en cyberadministration selon la norme eCH-0224 [3] et eCH-0107 [7], sont définies. Les directives pour le SAML Message ont été largement reprises de la norme eCH-0174 V1.0 et adaptées sur quelques points. Les messages pour Single Logout (Request et Response) ont été abandonnés, car ceux-ci ne revêtent aucune importance pratique.	-
4	29	**Interfaces des modèles de Broker [nouveau]** Le chapitre 4 définit les interfaces pour deux modèles de Broker **Sources ouvertes** et **Double Blinding** de la norme eCH eCH-0224 [3]..	-
5, 6, 7	31, 37, 50	**Interfaces pour les RP, Broker et IdP/AP [nouveau]** Suivant le modèle de la norme eCH-0225 [6], les interfaces pour les trois composants ont été décrites chacune dans un chapitre distinct.	-
8	57	**Métadonnées [eCH-0174 V1.0 Chapitre 5]** Le chapitre décrit les métadonnées Community et SAML nécessaires d'une Identity Federation implémentée avec SAML V2.0. Les informations concernant les métadonnées Community ont été reprises sous une forme abrégée et adaptée de la norme eCH-0168 [9] Chapitre 9. Les métadonnées SAML correspondent aux renseignements de eCH-0174 V1.0 sous une forme actualisée.	-

Tableau 9: Modifications par rapport à la version précédente

Le chapitre 7 - Extensions et cas particuliers n'a pas été repris de la norme eCH-0174 V1.0, car ceux-ci ne revêtent aucune importance aujourd'hui.

Annexe E – Liste des illustrations

Annexe F – Liste des listings

Annexe G – Liste des tableaux