eCH-0174 - Vermittlerbasierte Identity Federations - Implementierung mit SAML 2.0

Name	Vermittlerbasierte Identity Federations - Implementierung mit SAML 2.0
eCH-Nummer	eCH-0174
Kategorie	Standard
Reifegrad	Implementiert
Version	2.0.0
Status	Genehmigt
Beschluss am	2021-11-24
Ausgabedatum	2021-11-17
Ersetzt Version	1.0 – Major Change
Voraussetzungen	eCH-0224 v1.0
Beilagen	-
Sprachen	Deutsch (Original), Französisch (Übersetzung)
Autoren	Fachgruppe IAM Annett Laube-Rosenpflanzer, BFH, annett.laube@bfh.ch Gerhard Hassenstein, BFH, gerhard.hassenstein@bfh.ch Sven Bracklo, BFH, sven.bracklo@bfh.ch
Herausgeber / Vertrieb	Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Zusammenfassung

Dieser Standard beschreibt die technische Umsetzung der vermittlerbasierten Identity Federation Modelle aus dem Standard eCH-0224 mit Hilfe von SAML 2.0, parallel zum Standard eCH-0225, der die Umsetzung mit OIDC beschreibt. Ziel ist die Sicherstellung von Interoperabilität vor allem für Relying Parties in den Szenarien G2G, G2B und G2C. Dazu werden die notwendigen Services und Protokolle beschrieben. Der Standard richtet sich damit vorwiegend an IT-Architekten und Entwickler von Komponenten in der Identity Federation.

Inhaltsverzeichnis

1 Einleitung 6
1.1 Status 6
1.2 Einleitung 6
1.3 Anwendungsgebiet 6
1.4 Einordnung 6
1.5 Zielgruppe 8
1.6 Abgrenzung 8
1.7 Normativer Charakter der Kapitel 9
2 Identity Federation basierend auf SAML 10
2.1 SAML-Services 10
2.2 Authentifizierung mit und ohne Attributabfrage über SSO-Service 11
2.3 Authentifizierung mit Attributabfrage über AQS-Service 12
2.4 Signierung und Verschlüsselung 12
2.5 Technische Identifikatoren 13
2.6 User Consent 14
2.7 Protokolle 14
2.7.1 Authentifizierung ohne Attributabfrage 14
2.7.2 Authentifizierung mit Attributabfrage über AttributeConsumingServiceIndex 17
2.7.3 Authentifizierung mit Attributabfrage über Attribute Query 20
3 Richtlinien 23
3.1 Allgemeine Richtlinien 23
3.2 Richtlinien für alle Messages 25
3.3 Richtlinien für Authentication Requests 25
3.4 Richtlinien für Attribute Queries 26
3.5 Richtlinien für Responses 26
3.6 Richtlinien für Assertions 27
4 Schnittstellen der Vermittlermodelle 29
4.1 Authentifizierung 29

4.2 Authentifizierung mit Attributübermittlung 29
4.2.1 Vermittler Double-Blinding 29
4.2.2 Vermittler Offene Quellen 30
5 Schnittstellen für die Relying Party (RP) 31
5.1 Authentifizierung 31
5.1.1 Authentifizierungsanfrage an den Vermittler 31
5.1.2 Authentifizierungsbestätigung vom Vermittler 32
5.2 Authentifizierung mit Attributübergabe 33
5.2.1 Authentifizierungs- und Attributanfrage an den Vermittler 34
5.2.2 Authentifizierungs- und Attributbestätigungen vom Vermittler 34
6 Schnittstellen für Vermittler 37
6.1 Authentifizierung 38
6.1.1 Authentifizierungsanfrage von der Relying Party (RP) 38
6.1.2 Authentifizierungsanfrage an den Identity Provider (IdP) 39
6.1.3 Authentifizierungsbestätigung vom Identity Provider (IdP) 40
6.1.4 Authentifizierungsbestätigung an die Relying Party (RP) 41
6.2 Authentifizierung mit Attributanfrage über AttributeConsumingServiceIndex 42
6.2.1 Authentifizierungs- und Attributanfrage von der Relying Party (RP) 42
6.2.2 Authentifizierungs- und Attributanfragen an Identity & Attribute Provider (IdP/AP) .. 42
6.2.3 Authentifizierungs- und Attributbestätigungen vom IdentityProvider & Attribute (IdP/AP) 42
6.2.4 Authentifizierungs- und Attributbestätigungen an die Reyling Party (RP) 44
6.3 Authentifizierung mit Attributübergabe über Attribute Query 46
6.3.1 Authentifizierungs- und Attributanfrage von der Relying Party (RP) 46
6.3.2 Authentifizierungsanfrage an den Identity & Attribute Provider (IdP/AP) 46
6.3.3 Authentifizierungsbestätigung vom Identity & Attribute Provider (IdP/AP) 46
6.3.4 Attributanfrage an den Identity & Attribute Provider (IdP/AP) 46
6.3.5 Attributbestätigung vom Identity & Attribute Provider (IdP/AP) 48
6.3.6 Authentifizierungs- und Attributbestätigungen an die Relying Party (RP) 49
7 Schnittstellen für Identity & Attribute Provider (IdP/AP) 50
7.1 Authentifizierung 51
7.1.1 Authentifizierungsanfrage vom Vermittler 51

7.1.2 Authentifizierungsbestätigung an den Vermittler ... 52
7.2 Authentifizierung mit Attributanfrage über AttributeConsumingServiceIndex ... 53
7.2.1 Authentifizierungs- und Attributanfrage vom Vermittler ... 53
7.2.2 Authentifizierungs- und Attributbestätigung an den Vermittler ... 53
7.3 Authentifizierung mit Attributanfrage über Attribute Query ... 55
7.3.1 Authentifizierungsanfrage vom Vermittler ... 55
7.3.2 Authentifizierungsbestätigung an den Vermittler ... 55
7.3.3 Attributanfrage vom Vermittler ... 55
7.3.4 Attributbestätigung an den Vermittler ... 55
8 Metadaten ... 57
8.1 Community-Metadaten ... 57
8.1.1 Relying Party ... 57
8.1.2 IdP & IdP/AP ... 58
8.2 SAML-Metadaten ... 58
8.2.1 SAML-Metadaten-Richtlinien ... 60
8.2.2 Allgemeine Vorgaben zu `<md:EntityDescriptor>` Elementen ... 60
8.2.3 Vorgaben zu Vermittler Metadaten ... 61
8.2.4 Vorgaben zu IdP/AP Metadaten ... 63
9 Sicherheitsüberlegungen ... 64
10 Haftungsausschluss/Hinweise auf Rechte Dritter ... 65
11 Urheberrechte ... 65
Anhang A – Referenzen und Bibliographie ... 66
Anhang B – Mitarbeit & Überprüfung ... 68
Anhang C – Abkürzungen und Glossar ... 68
Anhang D – Änderungen gegenüber Vorversion ... 69
Anhang E – Abbildungsverzeichnis ... 71
Anhang F – Verzeichnis der Listings ... 71
Anhang G – Tabellenverzeichnis ... 72

Hinweis

Aus Gründen der besseren Lesbarkeit und Verständlichkeit wird im vorliegenden Dokument bei der Bezeichnung von Personen ausschliesslich die maskuline Form verwendet. Diese Formulierung schliesst Frauen in ihrer jeweiligen Funktion ausdrücklich mit ein.

Notation

Die Schlüsselworte MUSS *(MUST)*, DARF NICHT *(MUST NOT)*, ERFORDERLICH *(REQUIRED)*, SOLLTE *(SHOULD)*, SOLLTE NICHT *(SHOULD NOT)*, EMPFOHLEN *(RECOMMENDED)*, KANN *(MAY)* und OPTIONAL in diesem Dokument sind zu interpretieren wie in IETF RFC 2119 [1] beschrieben.

Die in diesem Dokument aufgeführten Präfixe, referenzieren folgende XML-Namensräume:

Präfix	XML-Namensraum
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

Tabelle 1: Präfixe und referenzierte XML-Namensräume

1 Einleitung

1.1 Status

Genehmigt: Das Dokument wurde vom Expertenausschuss genehmigt. Es hat für das definierte Einsatzgebiet im festgelegten Gültigkeitsbereich normative Kraft.

1.2 Einleitung

Eine Identity Federation im E-Government ermöglicht es Behörden ihre Leistungen online den Mitarbeitern anderer Behörden und den Bürgern sowie Organisationen und Unternehmen ihres Landes zur Verfügung zu stellen (siehe eCH-0219 IAM Glossar [2] Kapitel 2.62). Die Behörden delegieren dazu die Authentifizierung und die Bestätigung von Attributen an verschiedene IAM-Dienstanbieter. Grundlage der Delegation sind organisatorische/architektonische und technische Vereinbarungen oder Gesetze und Verordnung.

Im Standard eCH-0224 [3] wurde anhand von geschärften Anforderungen aus dem E-Government zusammen mit Anforderungen zum Schutz der Privatsphäre der Subjekte, der Raum der möglichen Identity Federation Systeme auf den folgenden drei vermittlerbasierten Modellen eingeschränkt:

- Vermittler Double Blinding,
- Vermittler Offene Quellen,
- Vermittler Vertraulichkeitsschutz.

Die Umsetzung dieser Modelle wird mit Hilfe von SAML 2.0 [4] in diesem Standard beschrieben. Die Umsetzung mit OIDC [1] wurde bereits im Standard eCH-0225 [6] beschrieben.

1.3 Anwendungsgebiet

Der Standard beschreibt die Umsetzung der vermittlerbasierten Identity Federation Modelle aus eCH-0224 . Er ist eine Richtlinie zur Implementierung der notwendigen Schnittstellen und Protokolle für die einzelnen Identity Federation Komponenten, um die Interoperabilität zwischen verschiedenen Anbietern sicherzustellen.

Ziel ist die Sicherstellung von **Interoperabilität** zwischen den verschiedenen Komponenten vermittlerbasierter Identity Federations, vor allem für Relying Parties, in den Szenarien G2G, G2B und G2C. Dazu werden die notwendigen Schnittstellen und Protokolle pro Komponente (RP, Vermittler, IdP/AP) definiert und besonders auf die notwendigen Anpassungen bzw. Erweiterungen von SAML hingewiesen.

1.4 Einordnung

Unter dem Standard eCH-0107 [7] positionieren sich Konzepte für föderierte IAM-Lösungen und ergänzende Hilfsmittel. Die Konzepte sind konkrete Beschreibungen, wie ein IAM-Lösungsvorschlag

aussieht, und beinhalten Teilkonzepte und Architekturen, die für die Umsetzung berücksichtigt werden müssen. Den Konzepten werden Hilfsmittel zur Seite gestellt, die ergänzende Informationen zur Verfügung stellen. Diese können für mehr als ein Konzept relevant sein. Die in diesem Dokument dargestellten Qualitäts- und Maturitätsmodelle sind Beispiele für solche Hilfsmittel. Die Liste dieser Hilfsmittel ist nicht abschliessend.

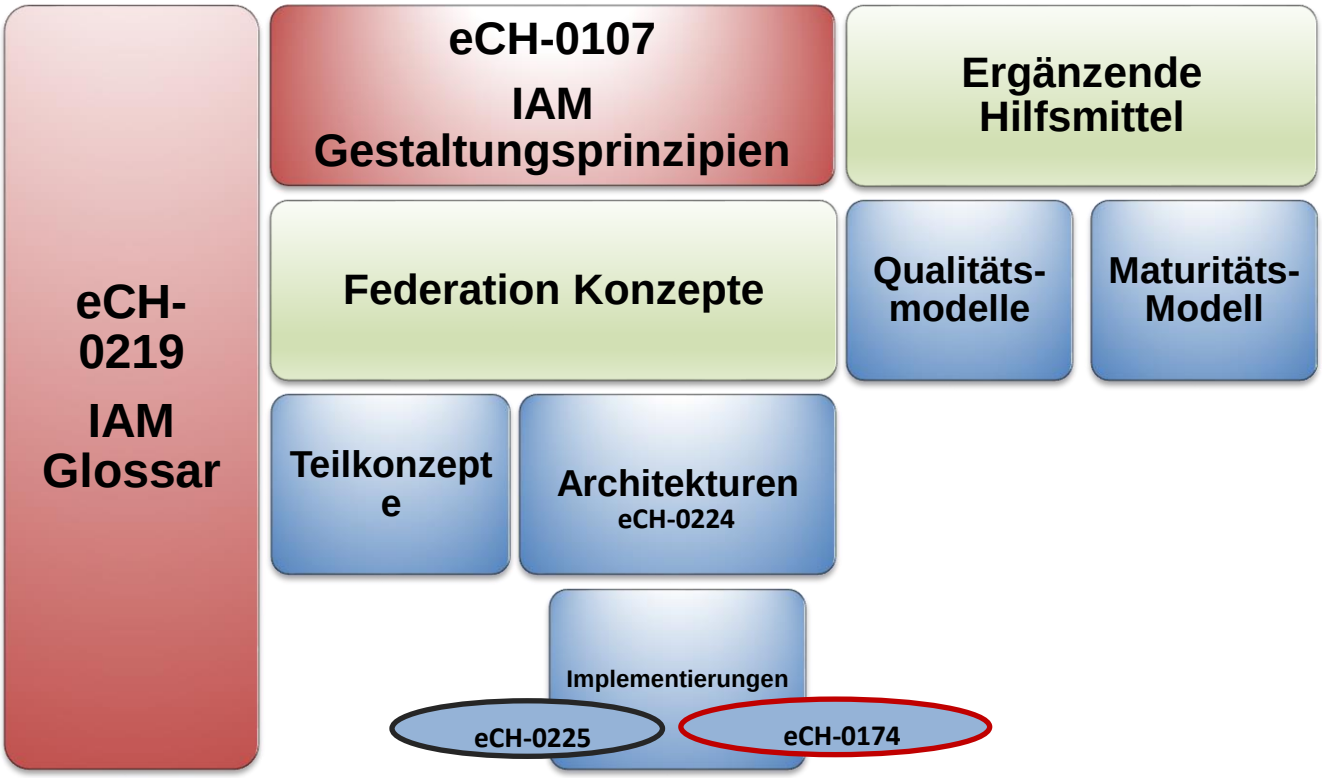

Abbildung 1: Einordnung des Standards eCH-0174 v2.0.0

Während V1.0 dieses Standards nur die Implementierung des STIAM-Modells beschrieben hat, enthält V2.0.0 die Implementierung von vermittlerbasierten Identity Federation Modelle aus eCH-0224 [2] auf der technologischen Basis von SAML 2.0 [4]. Dabei werden nur Varianten beschrieben, die bereits in der Praxis umgesetzt wurden.

Die Umsetzung der Identity Federation Modelle aus eCH-0224 [3] mit OIDC [5] ist im Standard eCH-0225 [6] beschrieben.

In der Version 2.0.0 wurden daraufhin alle STIAM-Begriffe wurden systematisch durch die im eCH-0224 [3] verwendete Terminologie ersetzt. Da die Unabhängigkeit von den STIAM-Standards (eCH-167 [8], eCH-0168 [9] und eCH-0169 [10]) ein Ziel der aktualisierten Version dieses Standards war, wurden Teile vom eCH-0168 in aktualisierter Form übernommen (Details zu den Änderungen gegenüber der Vorversion befinden sich in Anhang D).

1.5 Zielgruppe

Der Standard richtet sich vorwiegend an IT-Architekten und Entwickler von Identity Federations oder einzelnen Komponenten (RP, Vermittler, IdP, IdP/AP) von Identity Federation Systemen im E-Government. Er setzt Kenntnis der Vermittlermodelle aus eCH-Standard eCH-0224 [3] sowie fundiertes Wissen über den SAML 2.0 Standard [4] voraus.

Kapitel 2 definiert die Grundlagen eines Identity Federation Systems mit SAML 2.0 und sollte von IT-Architekten und Entwicklern studiert werden.

In Kapitel 3 werden zusätzliche Anforderungen an eine Identity Federation auf der Basis von SAML 2.0 im E-Government nach eCH-0224 [3] und eCH-0107 [7] definiert. Daneben werden die Richtlinien für Implementierungen der SAML-Messages beschrieben.

Kapitel 4 gibt einen Überblick über die Schnittstellen der Vermittlermodelle. Dieses Kapitel ist für IT-Architekten sowie Entwickler gleichermassen wichtig.

Die Kapitel 5, 6 und 7 definieren die Schnittstellen der Komponenten und richten sich vorwiegend an Entwickler, die die entsprechenden Schnittstellen implementieren. Es werden pro Komponente die zu implementierenden Schnittstellen beschrieben. die dadurch entstehenden Wiederholung von Schnittstellen (z.B. Kap. 5.1.1 - Authentifizierungsanfrage an den Vermittler und Kap. 6.1.1 Authentifizierungsanfrage von der Relying Party (RP)) ist beabsichtigt, um den Lesefluss pro Komponente zu vereinfachen und die Protokolle aus Sicht der jeweiligen Komponente zu präsentieren. IT-Architekten sollten diese Kapitel studieren, um das Zusammenspiel der Komponenten im Detail zu verstehen.

Kapitel 8 beschreibt die notwenigen Metadaten für eine Identity Federation basierend auf SAML 2.0 und ist daher vor allem für IT-Architekten sowie Entwickler interessant.

1.6 Abgrenzung

Dieser Standard beschreibt die Umsetzung der in eCH-0224 [3] definierten Anforderungen mit den heute üblichen technischen Mitteln auf der Basis von SAML 2.0 [4]. Es werden ausschliesslich die vermittlerbasierten Identity Federation Modelle «Double Blinding» und «Offene Quellen» aus eCH-0224 berücksichtigt. Andere Modelle oder Varianten von SAML 2.0 werden nicht adressiert.

1.7 Normativer Charakter der Kapitel

Die Kapitel des vorliegenden Standards sind von normativem oder auch deskriptivem Charakter. Folgende Tabelle definiert die Einordnung der Kapitel.

Kapitel	Beschreibung
1 Einleitung	**Deskriptiv**
2 Identity Federation basierend auf SAML	**Normativ**
3 Richtlinien	**Normativ**
4 Schnittstellen der Vermittlermodelle	**Normativ**
5 Schnittstellen für die Relying Party (RP)	**Normativ**
6 Schnittstellen für Vermittler	**Normativ**
7 Schnittstellen für Identity & Attribut Provider (IdP/AP)	**Normativ**
8 Metadaten	**Normativ**
9 Sicherheitsüberlegungen	**Deskriptiv**

2 Identity Federation basierend auf SAML

Dieses Dokument beschreibt eine Implementierung der in Standard eCH-0224[3] beschriebenen Architekturmodelle mit SAML 2.0[4], mit den folgenden **Einschränkungen**:

Es werden nur Prozesse zur Laufzeit beschrieben.

1. Es werden nur die Funktionalitäten beschrieben, die für eine lauffähige Lösung auf SAML 2.0 minimal erforderlich sind, d.h. auf alle optionalen Anforderungen und auf Protokolle neben dem SAML 2.0 Web Browser SSO Profile mit HTTP Binding (HTTP POST bzw. HTTP redirect) und SAML 2.0 Assertion Query/Request Profile wird verzichtet.

   Daher wird auch auf die Beschreibung von Single-Logout-Protokollen verzichtet.[1]

2. Es wird davon ausgegangen, dass als Quelle nur ein einzelner IdP/AP verwendet wird, der jeweils Authentifizierungs- und (optional) Attribute-Bestätigungen ausstellt. Eine Trennung von IdP und AP ist zwar theoretisch möglich, kommt aber in der Praxis kaum vor.
3. Der Vermittler unterstützt kein Identity-Linking (siehe auch eCH-0224[3], Kap. 8.1.3.7). Identity-Linking muss daher, wenn gefordert, von der Relying Party umgesetzt werden.
4. Es ist keine Back-Channel-Kommunikation, z.B. mit dem SAML Artifact Resolution Protocol [11] vorgesehen, da es in der Praxis nicht verwendet wird bzw. einen zu hohen Aufwand bei der Implementierung verursachen würde.
5. Eine Umsetzung vom SAML V2.0 Holder-of-Key Web Browser SSO Profile[12], das auf Identity Federations nicht einfach anzuwenden ist, wird in diesem Standard nicht weiter behandelt. Daher ist eine Verwendung der Vertrauensstufe 4 nach eCH-0170 v2.0[13] für die Qualität der Authentifizierung der Subjekte nicht möglich.

2.1 SAML-Services

Im Folgenden werden die SAML-Services beschrieben, die von den verschiedenen Komponenten unterstützt werden müssen bzw. sollen, um die in diesem Dokument beschriebenen Protokolle zu implementieren.

Die SAML-Profiles [14] (Web Browser SSO und Assertion Query/Request) definieren die folgenden Services:

- **Single Sign-On Service (SSO):** Der SSO Service beschreibt einen SAML Protokoll-Endpunkt, der einen Authentication Request (`<samlp:AuthnRequest>`) entgegennimmt.
- **Attribute Query Service (AQS):** Der Attribute Query Service beschreibt einen SAML Protokoll-Endpunkt, der eine Attribut-Abfrage (`<samlp:AttributeQuery>`) entgegennimmt.
- **Assertion Consumer Service (ACS):** Der Assertion Consumer Service beschreibt einen

[1] Auf Grund der komplexen Problematik von Single-Logout (SLO) und der engen Verbindung zum Session-Handling sollte diese Thematik in einen eigenen Standard beleuchtet werden.

SAML Protokoll-Endpunkt, der die Antwort (`<samlp:Response>`) auf einen Authentication Request (`<samlp:AuthnRequest>`) oder auf eine Attribut-Abfrage (`<samlp:AttributeQuery>`) entgegennimmt.

Tabelle 2 zeigt in der Übersicht, welche SAML-Services von welcher Komponente implementiert werden müssen bzw. sollten.

		SAML-Service		
		SSO	**ACS**	**AS**
Komponente	**Vermittler**	MUSS	MUSS	-[2]
	IdP und IdP/AP	MUSS	-	KANN[3]
	Relying Party	-	MUSS	-

Tabelle 2: Zuordnung von Komponenten zu SAML-Services

2.2 Authentifizierung mit und ohne Attributabfrage über SSO-Service

Abbildung 2 zeigt den Ablauf einer Authentifizierung ohne und mit Attributabfrage über den SSO-Service. Die Attributabfrage wird dabei mittels `AttributeConsumingServiceIndex` im Authentication Request (`<samlp:AuthnRequest>`) gesteuert.[4]

Eine Relying Party sendet einen Authentication Request (1) an den SSO-Service des Vermittlers. Dieser agiert als Proxy und sendet einen neuen Request (2) an den SSO des authentisierenden IdP. Der IdP authentifiziert das Subjekt, generiert eine Response und sendet diese an den ACS des Vermittlers zurück (3). Die Response enthält eine Authentifizierungsbestätigung und optional Attribute. Der Vermittler validiert die Response vom IdP und generiert eine neue Response, die er der anfragenden Relying Party zurücksendet (4).

[2] Um die Interoperabilität der Identity Federation zur erhöhen, wird auf den AQS beim Vermittler verzichtet. Der Vermittler muss keine Attributaggregation vornehmen und erhält Attribute aus derselben Quelle, bei der sich ein Benutzer authentisiert hat. Die Relying Party (RP) muss daher nur Authentication Request/Response unterstützen.

[3] Während primär die Authentifizierung mit Attributanfrage über den `AttributeConsumingServiceIndex` per SSO-Service vorgesehen ist, können mit dem AQS-Service ebenfalls IdP/APs unterstützt werden, welche Attributanfragen über die `<samlp:AttributeQuery>` verwenden.

[4] Alternativ wäre auch ein Extended AuthnRequest möglich, wie früher von der SuisseID gemäss Suisse-ID Spezifikation Kapitel 4.10.1.3. https://www.ech.ch/index.php/de/dokument/2aa44bb4-e35e-4266-9d69-c8e0d6721cb3 unterstützt. Da keine weiteren IdPs bekannt sind, die dieses Protokoll verwenden, wird auf eine Beschreibung in diesem Standard verzichtet.

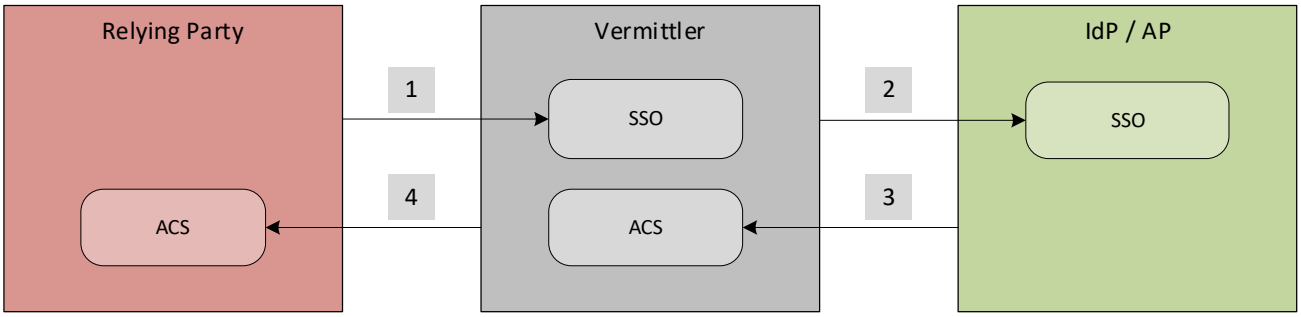

Abbildung 2: Interaktion der SAML-Services bei einem Authentication Request (mit und ohne Attributabfrage)

2.3 Authentifizierung mit Attributabfrage über AQS-Service

Abbildung 3 zeigt den Ablauf einer Authentifizierung mit Attributabfrage über den AS des IdP/APs.

Eine Relying Party sendet einen Authentication Request (1) an den SSO-Service des Vermittlers. Dieser agiert als Proxy und sendet einen neuen Request (2) an den SSO des authentisierenden IdP. Der IdP authentifiziert das Subjekt, generiert eine Response und sendet diese an den ACS des Vermittlers zurück (3). Nachdem der Vermittler die Identität des Subjekts kennt, wird zeitnah eine Attributabfrage an den AS des IdP/APs gesendet (4). Der IdP/AP liefert die gewünschten Attribute an den Vermittler zurück (5), welcher diese optional aggregiert oder umwandelt, bevor er sie an die anfragende Relying Party (RP) zusammen mit der Authentifizierungsbestätigung zurücksendet (6).

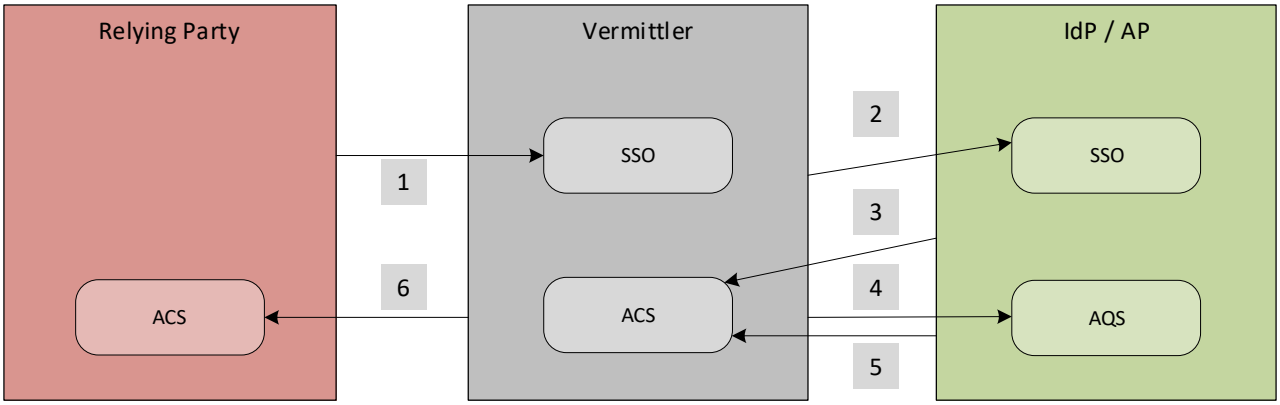

Abbildung 3: Interaktion der SAML-Services bei einem Authentication Request mit AttributeQuery

2.4 Signierung und Verschlüsselung

Die anfragenden Messages (Requests) MÜSSEN und die Antworten (Reponses) SOLLTEN[5] von den jeweiligen Komponenten vor dem Versenden signiert werden (siehe Abbildung 4). Eine Ausnahme ist die Response-Message beim Vermittlermodel Offene Quellen Variante 1 (siehe Kapitel 4.2.2): Da die

[5] Das Signieren von Response und Assertion erhöht die Komplexität, bietet aber einige Sicherheitsvorteile, wie das Verhindern des Einfügens in oder Änderns von Nachrichten (siehe Sections 6.1.3/6.1.5 in [19]).

Original-Assertion vom IdP/AP übernommen wird, MUSS die Response-Message vom Vermittler signiert werden.

Die in der Message enthaltene Assertion MUSS ebenfalls signiert sein; je nach Vermittlermodell wird die originale Signatur vom IdP/AP weitergegeben oder der Vermittler signiert die Assertion neu (siehe Kapitel 4.2).

Damit die RP die originalen Signaturen der Assertions prüfen kann, muss sie über den Public Key des IdP/APs verfügen. Im Normalfall erhält sie diesen aus den SAML-Metadaten der Domäne[6] (oft auch Gemeinschaft genannt), die über den Vermittler verteilt werden können (siehe Kapitel 8.2). In Ausnahmefällen kann der Public Key auch als Teil der Assertion zur Laufzeit mitgeschickt werden.

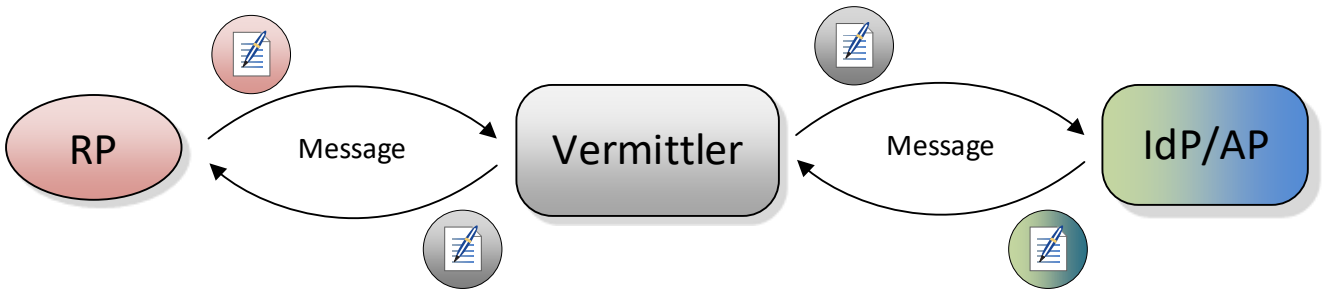

Abbildung 4: Übersicht der Signierung der Messages zwischen den Schnittstellen

Abhängig von den Qualitätsanforderungen SOLLTE die Assertion zwischen Vermittler und RP verschlüsselt werden. Zwischen Vermittler und IdP/AP MUSS die Assertion verschlüsselt werden.

Da es sich bei den SAML-Messages und den SAML-Assertions um XML-Strukturen handelt, wird bezüglich Verschlüsselung bzw. Signaturen auf die W3C Empfehlungen zur XML Encryption [15] und XML Signature [16] verwiesen. Best Practices findet man auch im Standard eCH-0091 [17].

2.5 Technische Identifikatoren

Wie in Standard eCH-0224 [3] Kapitel 5.3 definiert, SOLLTE eine Relying Party einen gebundenen technischen Identifikator (Persistent ID) verwenden, wenn das Subjekt bei einem erneuten Zugriff anhand dieses Identifikators (und nicht durch seine Attribute) wiedererkannt werden soll. Anderenfalls SOLLTE ein einmaliger zufälliger Identifikator (Transient ID) verwendet werden. Andere technische Identifikatoren SOLLTEN nicht verwendet werden. Die Informationen, welchen Typ von Identifikator die RP verwenden möchte, wird in den Metadaten (siehe Kap. 8), speziell im SPSSODescriptor der RP hinterlegt,

Diese Anforderungen haben Auswirkungen auf den Vermittler und die Verwendung der technischen Identifikatoren auf den Protokollstrecken zwischen RP und Vermittler (P1) sowie zwischen Vermittler und IdP/AP (P2) [7].

Verlangt die RP einen einmaligen zufälligen Identifikator (Transient ID) MUSS der Vermittler einen

[6] Begriff aus dem IAM-Glossar [2].

[7] Falls die Attribute aus mehreren Quellen bezogen werden (was für diesen Standard ausgeschlossen ist), kann es erforderlich sein, auf der Protokollstrecke P2 einen verteilten Identifikator (Distributed ID) zu verwenden.

solchen Identifikator vom gewählten IdP/AP ebenfalls verlangen oder für den Fall, dass der IdP/AP keine Transient IDs unterstützt, selbst einen einmaligen zufälligen Identifikator generieren.

Im Vermittlermodell Double Blinding DARF der Vermittler unter keinen Umständen den erhaltenen Identifier an die RP weiterreichen.

2.6 User Consent

Bevor der Vermittler eine Attributbestätigung an die RP übermittelt, MUSS das Subjekt die Attribute freigeben. Siehe Richtlinie 6 - Freigabe der Attribute (User Consent) (Kapitel 3.1, S 24).

Aus technischer Sicht gibt es zwei verschiedene Möglichkeiten, den User Consent einzuholen: *Ohne Attributwerte* oder *Mit Attributwerten* (siehe eCH-0224 [3] Kapitel 8.1.3.3). Die Domäne entscheidet, welche Variante verwendet werden soll und schafft die dazu notwendigen rechtlichen Grundlagen. In Abbildung 6 und Abbildung 7 sind die entsprechenden Abläufe graphisch dargestellt.

Für die Variante *Ohne Attributwerte* MUSS der Vermittler den User Consent **vor der Abfrage** der Attribute beim IdP/AP einholen. Gibt der Benutzer sein Einverständnis zur Attributabfrage nicht, MUSS das Protokoll an dieser Stelle mit einer entspr. Fehlermeldung an die RP abgebrochen werden.

Für die Variante *Mit Attributwerten* MUSS der Vermittler den User Consent **nach der Abfrage** der Attribute beim IdP/AP einholen. Gibt der Benutzer sein Einverständnis zur Attributabfrage nicht, MUSS das Protokoll an dieser Stelle mit einer entspr. Fehlermeldung an die RP abgebrochen werden.

2.7 Protokolle

Im Folgenden wird die Protokollübersicht zur Authentifizierung **OHNE** und **MIT** Attributabfrage des Subjekts beim IdP/AP erläutert. Sie basieren auf dem SAML Web Browser SSO Profile mit HTTP POST Binding bzw. Assertion Query/Request. Die Protokollabschnitte und verwendeten Messages werden im Kapitel 4 und in den Kapiteln der Schnittstellen 5, 6 und 7 detailliert beschrieben.

Für die Authentifizierung mit Attributabfrage MUSS der Vermittler die beiden Varianten mit AttributeConsumingServiceIndex und Attribute-Query unterstützen. Die Authentifizierung mit Attributanfrage zwischen RP und Vermittler MUSS über den AttributConsumingServiceIndex geschehen, die Attributanfrage zwischen Vermittler und IdP/AP MUSS zusätzlich über die Attribute-Query möglich sein.[8]

2.7.1 Authentifizierung ohne Attributabfrage

Abbildung 5 zeigt die Übersicht des Protokollverlaufs einer Authentifizierung ohne Attributabfrage.

[8] Durch die Variante der Attribute-Query wird gewährleistet, dass IdP/APs, die keinen `<samlp:AttributeConsumingServiceIndex>` unterstützen, ebenfalls in das System eingegliedert werden können.

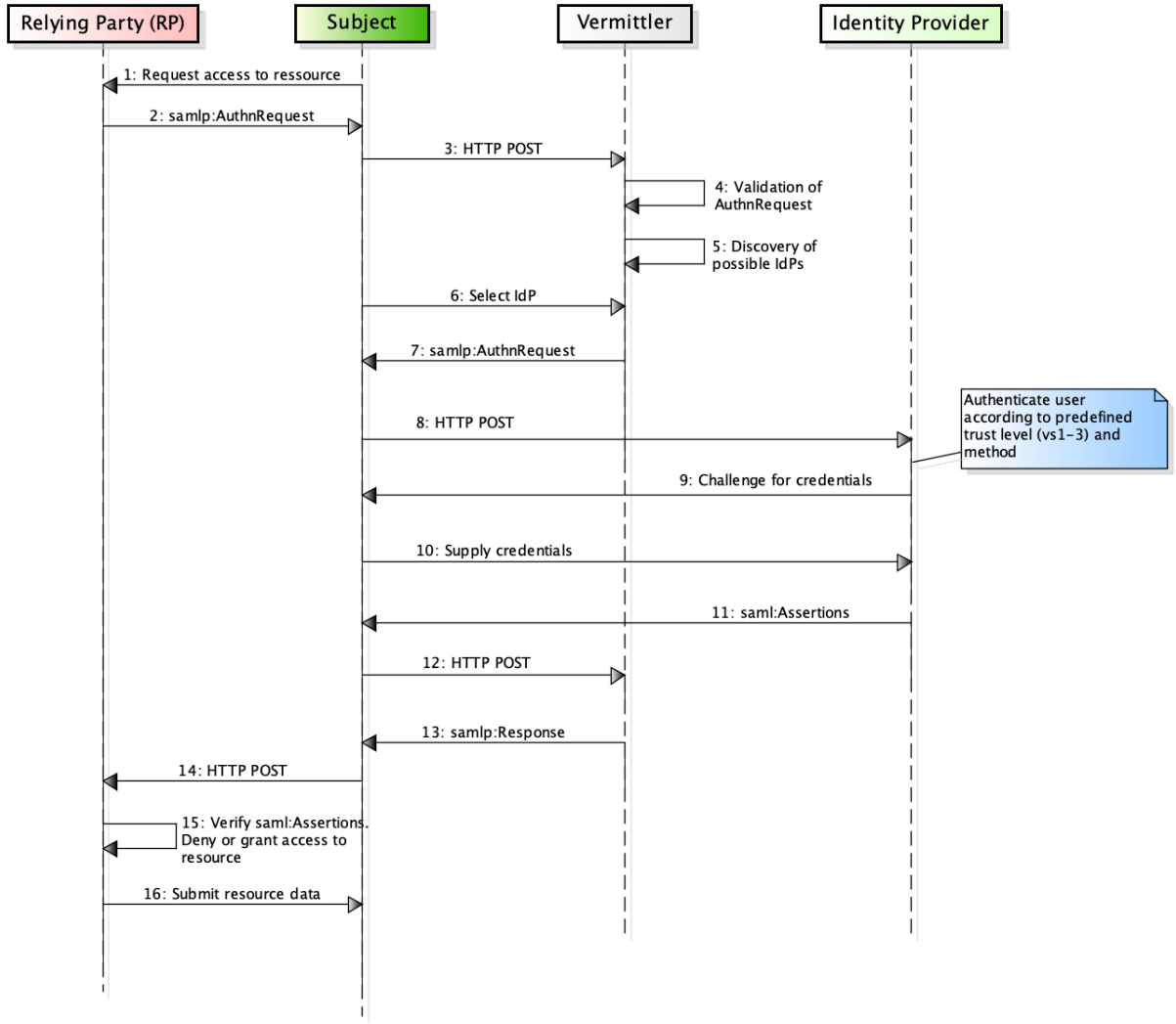

Abbildung 5: Authentifizierungs-Protokoll ohne Attributübermittlung

Referenz-Tabelle zu Abbildung 5:

Schritt	Beschreibung	Schnittstelle	Kapitel
1, 2	Der Benutzer möchte auf eine Ressource der RP zugreifen. Die RP sendet einen <samlp:AuthnRequest> in einer self-submitting HTML Form zurück an den Browser des Benutzers.	Relying Party	5.1.1
3, 4, 5, 6, 7	Weiterleitung des <samlp:AuthnRequest> an den SSO-Service des Vermittlers. Der Vermittler validiert den Request und ermittelt anhand des <samlp:AttributeConsumingServiceIndex> die geeigneten IdPs. Wenn mehrere IdPs die Kriterien erfüllen, MUSS der Benutzer einen gewünschten IdP auswählen. Anschliessend erstellt der Vermittler einen	Vermittler	6.1.1, 6.1.2

Schritt	Beschreibung	Schnittstelle	Kapitel
	neuen <samlp:AuthnRequest>, der zurück an den Browser des Benutzer gesendet wird.		
8, 9, 10, 11	Der Browser sendet den <samlp:AuthnRequest> an den SSO-Service des IdPs. Der Benutzer authentisiert sich gegenüber dem IdP. Bei erfolgreicher Authentisierung erzeugt der IdP eine <samlp:Response> mit <saml:AuthnStatement> und <saml:Assertion> und sendet diese an den Browser des Benutzers zurück.	IdP	7.1.1, 7.1.2
12, 13	Der Browser leitet die <saml:Assertion> an den Vermittler weiter. Der Vermittler erzeugt eine neue <samlp:Response> mit einer <saml:Assertion> inklusive einem <saml:AuthnStatement> und sendet diese zurück an den Browser.	Vermittler	6.1.3, 6.1.4
14, 15, 16	Der Browser sendet die <samlp:Response> an die Relying Party (RP), die nun die <samlp:Response> des Vermittlers verifiziert und anhand dessen den Zugriff auf die Ressource gewährt oder verweigert.	Relying Party	5.1.2

Tabelle 3: Referenz-Tabelle zum Authentifizierungs-Protokoll ohne Attributübermittlung

2.7.2 Authentifizierung mit Attributabfrage über AttributeConsumingServiceIndex

Abbildung 6 zeigt die Übersicht des Protokollverlaufs einer Authentifizierung mit Attributabfrage mithilfe des `<samlp:AttributeConsumingServiceIndex>`. Der Protokollverlauf ist gleichzusetzen mit dem Verlauf aus Abbildung 5, jedoch unterscheiden sich insbesondere der `<samlp:AuthnRequest>` und `<samlp:Response>` und es kommt die Einholung des User Consents hinzu. Der User Consent MUSS vor oder nach der Authentifizierungs- und Attributbestätigung eingeholt werden.

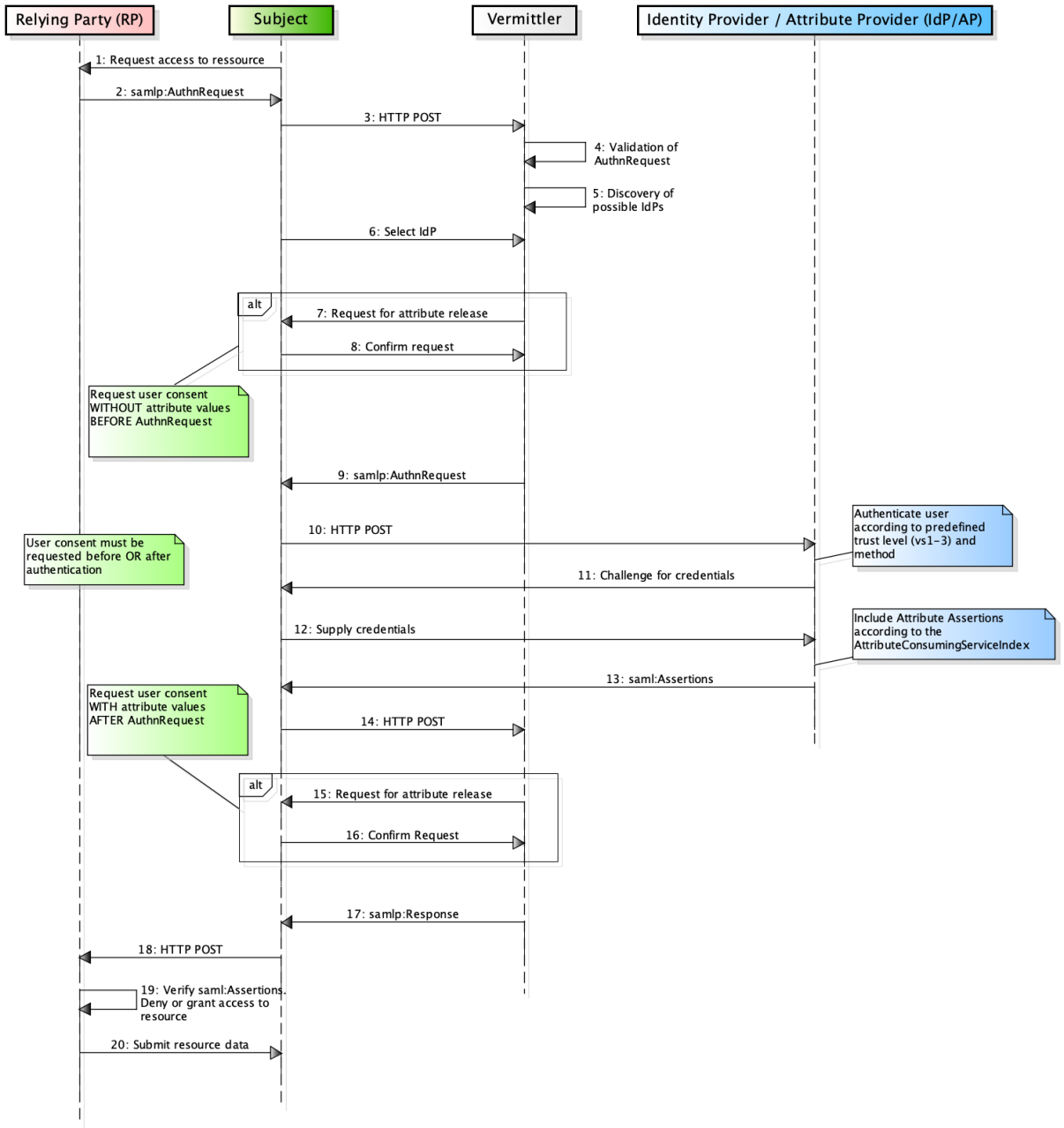

Abbildung 6: Authentifizierungs-Protokoll mit Attributübermittlung durch AttributeConsumingServiceIndex

Referenz-Tabelle zu Abbildung 6:

Schritt	Beschreibung	Schnittstelle	Kapitel
1, 2	Der Benutzer möchte auf eine Ressource vom RP zugreifen. Die RP sendet einen <samlp:AuthnRequest> in einer self-submitting HTML Form zurück an den Browser des Benutzers.	RP	5.2.1
3, 4, 5, 6	Weiterleitung des <samlp:AuthnRequest> an den SSO-Service des Vermittlers. Der Vermittler validiert den Request und ermittelt anhand des <samlp:AttributeConsumingServiceIndex> die geeigneten IdP/APs. Wenn mehrere IdP/APs die Kriterien erfüllen, MUSS der Benutzer einen gewünschten IdP/AP auswählen.	Vermittler	6.2.1,
7, 8, 9	***Optional*** Falls der User Consent vor der Authentifizierungs- & Attributanfrage eingeholt werden soll, sendet der Vermittler eine Anfrage zur Freigabe der angefragten Attribute zum Benutzer. Der Vermittler erstellt einen neuen <samlp:AuthnRequest> mit einem den angeforderten (und ggf. freigegebenen) Attributen entsprechenden <samlp:AttributeConsumingServiceIndex>, der zurück an den Browser des Benutzer gesendet wird.	Vermittler	6.2.2
10, 11, 12, 13	Der Browser sendet den <samlp:AuthnRequest> an den SSO-Service des IdP/APs. Der Benutzer authentisiert sich gegenüber dem IdP/AP. Bei erfolgreicher Authentisierung erzeugt der IdP/AP eine <samlp:Response> mit einer <saml:Assertion>, die eine <saml:AuthnStatement> und <saml:AttributeStatement> enthält, und sendet diese an den Browser zurück.	IdP/AP	7.2.1, 7.2.2
14, 15, 16, 17	Der Browser leitet die <saml:Response> an den Vermittler weiter. ***Optional*** Falls der User Consent nach Erhalt der Attribute eingeholt werden soll, sendet der Vermittler dem Benutzer eine Anfrage zur Freigabe der Attribute inklusive Attributwerte aus der Attributbestätigung. Der Benutzer bestätigt die Anfrage. Der Vermittler erstellt eine <samlp:Response> mit einer <saml:Assertion>, welche das <saml:AuthnStatement> und <saml:AttributeStatement> aus der vorherigen Response vom IdP/AP beinhaltet. Die <samlp:Response> wird an den	Vermittler	6.2.3, 6.2.4

Schritt	Beschreibung	Schnittstelle	Kapitel
	Browser weitergeleitet.		
18, 19, 20	Der Browser sendet die <samlp:Response> an die Relying Party, die nun die <samlp:Response> des Vermittlers verifiziert und anhand dessen den Zugriff auf die Ressource gewährt oder verweigert.	RP	5.2.2

Tabelle 4: Referenz-Tabelle zum Authentifizierungs-Protokoll mit Attributübermittlung durch AttributeConsumingServiceindex

2.7.3 Authentifizierung mit Attributabfrage über Attribute Query

Abbildung 7 zeigt die Übersicht des Protokollverlaufs einer Authentifizierung mit der Attributabfrage durch eine Attribute Query. Der Protokollverlauf unterscheidet sich insbesondere durch die zusätzliche Attributanfrage nach der erfolgreichen Authentifizierung. Der User Consent MUSS vor der Attributanfrage oder nach der Attributbestätigung eingeholt werden.

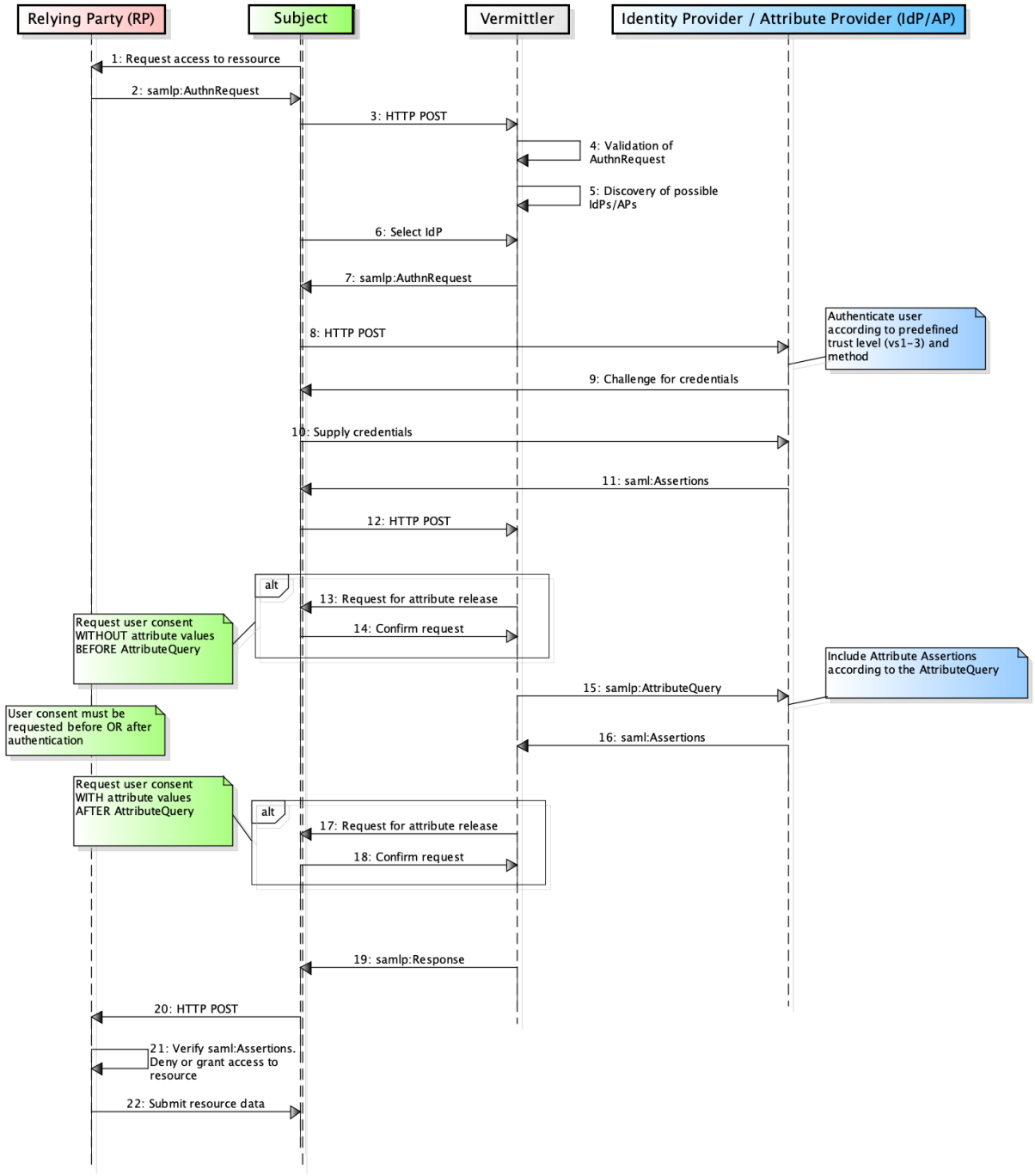

Abbildung 7: Authentifizierungs-Protokoll mit Attributübermittlung durch Attribute-Query

Referenz-Tabelle zu Abbildung 7:

Schritt	Beschreibung	Schnittstelle	Kapitel
1, 2	Der Benutzer möchte auf eine Ressource vom RP zugreifen. Die RP sendet einen <samlp:AuthnRequest> in einer self-submitting HTML Form zurück an den Browser des Benutzers.	Relying Party	5.2.1
3, 4, 5, 6, 7	Weiterleitung des <samlp:AuthnRequest> an den SSO-Service des Vermittlers. Der Vermittler validiert den Request und ermittelt anhand des <samlp:AttributeConsumingServiceIndex> die geeigneten IdP/APs. Wenn mehrere IdP/APs die Kriterien erfüllen, MUSS der Benutzer einen gewünschten IdP/AP auswählen. Anschliessend erstellt der Vermittler einen neuen <samlp:AuthnRequest> OHNE <AttributeConsumingServiceIndex>[9], den er zurück an den Browser des Benutzers sendet.	Vermittler	6.3.1, 6.3.2
8, 9, 10, 11	Der Browser sendet die <samlp:AuthnRequest> an den SSO-Service des gewählten IdP/APs. Der Benutzer authentisiert sich gegenüber dem IdP. Bei erfolgreicher Authentisierung erzeugt der IdP eine <samlp:Response> mit <saml:Assertion> und <saml:AuthnStatement> und sendet diese an den Benutzer zurück.	IdP/AP	7.3.1, 7.3.2
12, 13, 14, 15	Nachdem der Benutzer sich authentisiert hat, leitet der Browser die <saml:Assertion> weiter an den Vermittler. ***Optional*** Falls der User Consent vor der Attributanfrage eingeholt werden soll, sendet der Vermittler eine Anfrage zur Freigabe der angefragten Attribute zum Benutzer. Anschliessend erstellt der Vermittler aus den von der RP geforderten Attribute eine Attribute-Query und sendet diese an den IdP/AP.	Vermittler	6.3.3, 6.3.4
16	Der IdP/AP empfängt die <samlp:AttributeQuery> und erzeugt eine <samlp:Response> mit <saml:Assertion> und <saml:AttributeStatement> und sendet diese zurück an den Vermittler.	IdP/AP	7.3.3, 7.3.4
17, 18, 19	***Optional*** Falls der User Consent nach Erhalt der Attribute eingeholt	Vermittler	6.3.5,

[9] Wird der `<AttributeConsumingServiceIndex>` nicht angegeben, wird der Default wirksam, der einer Authentifizierung ohne Attributanfrage entsprechen muss.

Schritt	Beschreibung	Schnittstelle	Kapitel
	werden soll, sendet der Vermittler dem Benutzer eine Anfrage zur Freigabe der Attribute inklusive Attributwerte aus der Attributbestätigung. Der Vermittler erstellt eine <samlp:Response> mit einer <saml:Assertion>, welche das <saml:AuthnStatement> **und** <saml:AttributeStatement> aus den vorherigen Responses vom IdP/AP beinhaltet.		6.3.6
18, 19, 20	Der Browser sendet die <samlp:Response> an die Relying Party (RP), die nun die <samlp:Response> des Vermittlers verifiziert und anhand dessen den Zugriff auf die Ressource gewährt oder verweigert.	Relying Party	5.2.2

Tabelle 5: Referenz-Tabelle zum Authentifizierungs-Protokoll mit Attributübermittlung durch Attribute Query

3 Richtlinien

Basierend auf den Anforderungen für eine Identity Federation im E-Government nach eCH-0224 [3] und eCH-0107 [3] MÜSSEN für diesen Standard zusätzlich die folgenden Richtlinien eingehalten werden.

Aus diesen Richtlinien resultieren Einschränkungen bzw. Erweiterungen des SAML-Standards [4]. Ausserdem wird definiert, welche Anforderung mit welcher technischen Massnahme erfüllt wird.

Zusätzlich SOLLTEN die gängigen SAML Standard und Implementation Guidelines, z.B.[18] und [19], eingehalten werden.

3.1 Allgemeine Richtlinien

Richtlinie 1 – Authentifizierung der anfragenden Instanz: Die angefragte Instanz MUSS die anfragende Komponente vor dem Retournieren von Authentifizierungs- oder Attributinformationen eines Subjektes authentifizieren.

Die anfragende Instanz MUSS ihre Anfrage signieren.

Die angefragte Instanz MUSS die Signatur der erhaltenen Message prüfen und mit den SAML-Metadaten abgleichen.

Erfüllte Anforderungen: 224-LE-5, IAM-11 und LB-15.

Richtlinie 2 – Authentizität und Integrität der Antwort: Alle retournierten SAML-Messages und Assertions MÜSSEN von der ausstellenden Instanz signiert werden.

Ist die abnehmende Instanz der Vermittler, MUSS dieser die Signatur prüfen. Die RP SOLLTE in ihrem eigenen Interesse eine Prüfung der Signatur vornehmen.

Erfüllte Anforderung: IAM-9

Richtlinie 3 – Vertraulichkeitsschutz der Assertions: Zum Schutz der Privatsphäre des Subjekts SOLLTE die ausstellende Instanz (Quelle) die Authentication und Attribute Assertions so ausstellen, dass nur die berechtigte Instanz die Attribute einsehen kann.

Die Authentication und Attribute Assertions SOLLTEN verschlüsselt werden. Ist die empfangende Instanz der Vermittler, MÜSSEN alle Assertions verschlüsselt werden.

Wenn der Vermittler als ausstellende Instanz die Assertions verschlüsselt, muss die RP in der Lage sein, diese entsprechend zu verarbeiten.

Erfüllte Anforderung: 224-LB-4

Richtlinie 4 – Qualitätsmodell für die Authentifizierung: Für die Qualität der Authentifizierung der Subjekte MÜSSEN die Vertrauensstufen nach eCH-0170 v2.0 [13] verwenden werden:

- *urn:ech.ch/ech0170v2/vs1*: Vertrauensstufe 1 (Kein oder minimales Vertrauen),
- *urn:ech.ch/ech0170v2/vs2*: Vertrauensstufe 2 (Geringes Vertrauen),
- *urn:ech.ch/ech0170v2/vs3*: Vertrauensstufe 3 (Beträchtliches Vertrauen),
- *urn:ech.ch/ech0170v2/vs4*: Vertrauensstufe 4 (Hohes Vertrauen)[10].

Die RP MUSS die geforderte Vertrauensstufe bei der Registrierung in ihren Metadaten (siehe Kapitel 8.1.1) festlegen und KANN (falls sie unterschiedliche Vertrauensstufen benötigt) diese in der Authentifizierungsanfrage mitsenden.

Der Vermittler KANN in der Authentifizierungsanfrage die geforderte Vertrauensstufe mitsenden.

Der IdP MUSS die verfügbaren Vertrauensstufen in den Metadaten definieren (siehe Kap. 8.1.2). Falls mehrere Vertrauensstufen möglich sind, MUSS der IdP die verwendete Vertrauensstufe in der Authentifizierungsbestätigung (Authentication Assertion) mitsenden.

Der Vermittler MUSS in jedem Fall die Vertrauensstufe in der Authentifizierungsbestätigung mitsenden. Die Vertrauensstufe in der Authentifizierungsbestätigung erhält der Vermittler entweder zur Laufzeit von der Authentifizierungsbestätigung des IdP oder aus den zur Definitionszeit definierten Metadaten des IdP.

Erfüllte Anforderungen: 224-IAM-4, 224-IAM-4.1

Richtlinie 5 – Qualitätsmodell für die Attributbestätigung: Für die Qualität der Attributbestätigung der Subjekte MUSS das folgende oder ein gleichwertiges Modell verwendet werden.

- *urn.ech.ch/ech0224v1/aq1*: Attributqualität 1 (nicht bestätigte Attribute),
- *urn.ech.ch/ech0224v1/aq2*: Attributqualität 2 (bestätigte Attribute),
- *urn.ech.ch/ech0224v1/aq3*: Attributqualität 3 (staatlich bestätigte Attribute).

Die RP MUSS bei der Registrierung der Ressource beim Vermittler mitteilen, welche Attribute in welcher Qualität sie verlangt.

Der Vermittler MUSS in der Attributbestätigung die Qualität der Attribute an die RP mitsenden. Die Qualität der Attribute erhält der Vermittler entweder zur Laufzeit von der Attributbestätigung des IdP/AP oder aus den zur Definitionszeit definierten Metadaten der IdP/AP.

Erfüllte Anforderung: 224-IAM-5

Richtlinie 6 – Freigabe der Attribute (User Consent): Wenn die Einholung des User Consent beim IdP/AP deaktiviert werden kann, MUSS der Vermittler das Einverständnis des Subjekts einholen, dass die ausgewählten Attribute an die RP übermittelt werden dürfen.

Der IdP/AP SOLLTE NICHT den „User Consent“ vom Subjekt einholen.
Erfüllte Anforderung: 224-LB-6

[10] Vertrauensstufe 4 erfordert eine Umsetzung vom SAML V2.0 Holder-of-Key Web Browser SSO Profile [12], das auf Identity Federations nicht einfach anzuwenden ist und deshalb in diesem Standard nicht weiter behandelt wird.

3.2 Richtlinien für alle Messages

In diesem Abschnitt werden die Richtlinien für die SAML-Messages festgelegt.

- Das `ID` Attribut im Wurzelelement MUSS in jeder Message vorhanden sein. Der Wert MUSS in der Message eindeutig sein. Er wird als Referenz bei der Signatur der Message verwendet.
- Das `Destination` Attribut im Wurzelelement jeder Message MUSS immer vorhanden sein. Dessen Wert MUSS die URL sein, an die die Message gesendet wird.
- Das `IssueInstant` Attribut im Wurzelelement jeder Message MUSS immer vorhanden sein. Dessen Wert gibt den Zeitpunkt der Erstellung der Message an. Dieser MUSS in UTC codiert werden.
- Das `Version` Attribut im Wurzelelement jeder Message MUSS immer vorhanden sein. Dessen Wert MUSS `2.0` sein.
- Der Wert des `<saml:Issuer>` Elements MUSS in jeder Message mit dem `EntityID` Attribut aus den Metadaten derjenigen Entität übereinstimmen, welche die Message erstellt hat.
- Alle Messages MÜSSEN mit einem in der Domäne anerkannten Zertifikat (Applikationszertifikat) digital signiert sein (d.h. ein `<ds:Signature>` Element enthalten).[11]

3.3 Richtlinien für Authentication Requests

- Das `<samlp:AuthnRequest>` Element MUSS die Wurzel des Authentication Requests sein.
- Das <samlp:AuthnRequest> Element MUSS mit einem in der Community anerkannten Zertifikat digital signiert sein (ein <ds:Signature> Element muss enthalten sein).
- Das `<samlp:AuthnRequest>` Element MUSS die Attribute `AssertionConsumerServiceURL` und `ProtocolBinding` enthalten.

  Der Wert von `AssertionConsumerServiceURL` MUSS mit dem `AssertionConsumerService` Element aus den Metadaten derjenigen Entität übereinstimmen, welche den Authentication Request erstellt hat.
- Der Wert des `ProtocolBinding` Attributes MUSS `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST` sein.
- Das `<samlp:AuthnRequest>` Element KANN ein `ForceAuthn` Attribut enthalten.
- Das `<samlp:AuthnRequest>` Element KANN ein `<samlp:NameIDPolicy>` Element enthalten. Der Wert dessen `Format` Attribut MUSS `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` oder `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` sein. Falls er persistent ist, MUSS im `<samlp:NameIDPolicy>` Element das `AllowCreate` Attribut vorhanden sein, und dessen Wert MUSS auf `true` gesetzt werden.

[11] Detaillierte Informationen zu den verschiedenen Zertifikatsklassen und deren Verwendung im E-Government findet man im eCH-0048 - PKI-Zertifikatsklassen [23].

Wenn das <samlp:NameIDPolicy> Element weggelassen wird, gilt das urn:oasis:names:tc:SAML:2.0:nameid-format:transient Format als Default.

- Der Authentication Request SOLLTE das AttributeConsumingServiceIndex Attribut enthalten. Falls dieses nicht vorhanden ist, gilt der Default.
- Der Authentication Request KANN ein <saml:Subject> Element mit einem nameID Element für den Fall eines Session-Refreshing oder einer Step-Up-Authentifizierung enthalten.
- Der Authentication Request KANN ein <samlp:RequestedAuthnContext> Element mit einem <saml:AuthnContextClassRef> Element enthalten, wenn eine Authentisierung mit einem höheren Level erwünscht wird als in den Metadaten gefordert wird. Der Wert des <saml:AuthnContextClassRef> Elements MUSS eine der Vertrauensstufen nach eCH-0170 v2.0 [13] sein, z.B.
  - *urn:ech.ch/ech0170v2/vs1*: Vertrauensstufe 1 (Kein oder minimales Vertrauen),
  - *urn:ech.ch/ech0170v2/vs2*: Vertrauensstufe 2 (Geringes Vertrauen),
  - *urn:ech.ch/ech0170v2/vs3*: Vertrauensstufe 3 (Beträchtliches Vertrauen).
- Der Authentication Request SOLLTE KEINE weiteren Elemente (z.B. Conditions, Scope, …) enthalten, ausser es ist explizit für die Domäne abgestimmt und definiert.

3.4 Richtlinien für Attribute Queries

- Das <samlp:AttributeQuery> Element MUSS die Wurzel des Attribute Query Requests sein.
- Das <samlp:AttributeQuery Element MUSS mit einem in der Community anerkannten Zertifikat digital signiert sein (ein <ds:Signature> Element muss enthalten sein).
- Das <samlp:AttributeQuery> Element MUSS ein <saml:Subject> Element ent-halten. Dieses MUSS ein <saml:NameID> enthalten. Dessen Format DARF NICHT urn:oasis:names:tc:SAML:2.0:nameid-format:transient sein.
- Das <samlp:AttributeQuery> Element MUSS ein oder mehrere <Attribute> Elemente enthalten.
- Das <samlp:AttributeQuery> DARF NICHT zwei oder mehrere <Attribute> Elemente enthalten, die dieselben Name und NameFormat Attribute haben.

3.5 Richtlinien für Responses

- Das <samlp:Response> Element MUSS die Wurzel der Response Message sein.
- Das <saml:Response> Element SOLLTE mit einem in der Community anerkannten Zertifikat digital signiert sein (ein <ds:Signature> Element muss enthalten sein).
- Das <Response> Element MUSS ein InResponseTo Attribut enthalten.

  Das InResponseTo Attribut MUSS mit der ID der Abfrage, für welche die Response erstellt wurde, übereinstimmen.
- Das <samlp:Response> Element MUSS ein <samlp:Status> Element enthalten und dieses

wiederum ein <samlp:StatusCode>.

- Bei einem erfolgreichen Authentication Request MUSS das <samlp:Response> Element ein <saml:Assertion> Element enthalten.
- Ist der Authentication Request nicht erfolgreich, MUSS im <samlp:StatusCode> Element eine Fehlermeldung nach SAML 2.0 [4] vorhanden sein und die Assertion fällt weg. Das Element <samlp:Status> KANN zusätzlich ein <samlp:StatusDetail> und <samlp:StatusMessage> Element enthalten. Dabei muss beachtet werden, dass keine unnötigen Informationen über den Benutzer oder die Art des Fehlers in die zusätzlichen Elemente eingebunden werden.

```
<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: Beispiel einer SAML Response (Success)

3.6 Richtlinien für Assertions

In diesem Abschnitt werden die Richtlinien für die SAML-Assertions festgelegt.

- Das <saml:Assertion> Element MUSS ein ID und IssueInstant Attribut enthalten.
- Das <saml:Assertion> Element MUSS ein <saml:Issuer> Element enthalten. Dessen Wert MUSS mit dem EntityID Attribut aus den Metadaten übereinstimmen und von derjenigen Komponente stammen, welche die Assertion erstellt hat.
- Das <saml:Assertion> Element MUSS mit einem in der Domäne anerkannten Zertifikat digital signiert sein (<ds:Signature> Element enthalten).
- Das <saml:Assertion> Element MUSS ein <saml:Subject> Element enthalten. Dieses MUSS ein <saml:NameID> und <saml:SubjectConfirmation> Element enthalten.
  Das <saml:SubjectConfirmation> Element MUSS ein Method Attribut haben. Dessen Wert MUSS urn:oasis:names:tc:SAML:2.0:cm:bearer sein.
  Das <saml:SubjectConfirmation> Element MUSS ein <saml:SubjectConfirmationData> Element haben. Dieses MUSS ein InResponseTo, Recipient and NotOnOrAfter Attribut haben.
- Das <saml:Assertion> Element MUSS ein <saml:Conditions> Element enthalten. Dieses MUSS ein NotBefore und NotOnOrAfter Attribut haben. Ausserdem MUSS dieses ein <saml:AudienceRestriction> Element enthalten, welches ein <saml:Audience> Element

hat. Dessen Wert MUSS mit dem `EntityID` Attribut aus den Metadaten der Entität übereinstimmen, für welche die Assertion erstellt wurde.

- Das `<Assertion>` Element MUSS genau ein `<saml:AuthnStatement>` Element und/oder ein `<saml:AttributeStatement>` Element beinhalten.
- Das `<saml:AuthnStatement>` Element MUSS ein `AuthnInstant` und ein `SessionIndex` Attribut, sowie ein `<saml:AuthnContext>` Element enthalten.
- Das `<saml:AuthnContext>` Element MUSS ein `<saml:AuthnContextClassRef>` Element enthalten. Dessen Wert MUSS einer der folgenden Vertrauensstufe nach eCH-0170 v2.0 [13] sein:
  - `urn:ech.ch/ech0170v2/vs1`: Vertrauensstufe 1 (Kein oder minimales Vertrauen),
  - `urn:ech.ch/ech0170v2/vs2`: Vertrauensstufe 2 (Geringes Vertrauen),
  - `urn:ech.ch/ech0170v2/vs3`: Vertrauensstufe 3 (Beträchtliches Vertrauen).
- Das `<saml:AttributeStatement>` Element MUSS ein `Name` und `NameFormat` Attribut, sowie ein `<samlAttributeValue>` Element enthalten.
- Das `<saml:AttributeValue>` Element MUSS ein `xsi:type` Attribut beinhalten und als Wert das entsprechende Attribut beinhalten. Ebenfalls MUSS die Attributqualität, z.B. als Attribut `ech0224:aq` mit den Werten nach eCH-0224 v1.0 [3], angegeben werden.
- Das `<saml:AttributeStatement>` Element MUSS ein oder mehrere `<saml:Attribute>` Elemente enthalten und diese KÖNNEN ein oder mehrere `<saml:AttributeValue>` Elemente sowie eine Angabe zur Quelle (`<saml:OriginalIssuer>`) haben.

4 Schnittstellen der Vermittlermodelle

In diesem Kapitel wird definiert, wie die zwei Vermittlermodelle **Offene Quellen** und **Double-Blinding** aus dem eCH-Standard eCH-0224 [3] mit den entsprechenden Schnittstellenbeschreibungen umgesetzt werden. Es werden hier nur die Schnittstellen zwischen den Akteuren für die Laufzeitprozesse spezifiziert. Weitere Tätigkeiten der Akteure befinden sich in eCH-0224 ab Kapitel 8.

Im Kapitel 4.1 befindet sich die Übersicht der Schnittstellen für die *Authentifizierung* und es wird auf die entsprechende Schnittstellendefinition der Akteure verwiesen.

Im Kapitel 4.2 befindet sich die Übersicht der Schnittstellen für die *Authentifizierung mit Attributübergabe*. Da sich die Vermittlermodelle bei der Attributübergabe unterscheiden, werden sie einzeln spezifiziert.

4.1 Authentifizierung

Bei einem Vermittlermodell erfolgt die Authentifizierung (ohne Attributabfrage) in beiden Protokoll-Abschnitten prinzipiell gleich. Jede Komponente MUSS die Anfrage bzw. Bestätigung signieren. Der Vermittler MUSS in diesem Fall die Authentifizierungsbestätigung vom IdP/AP in eine neue, vom Vermittler signierte Response einfügen. Abbildung 8 zeigt eine Übersicht der Authentifizierung.

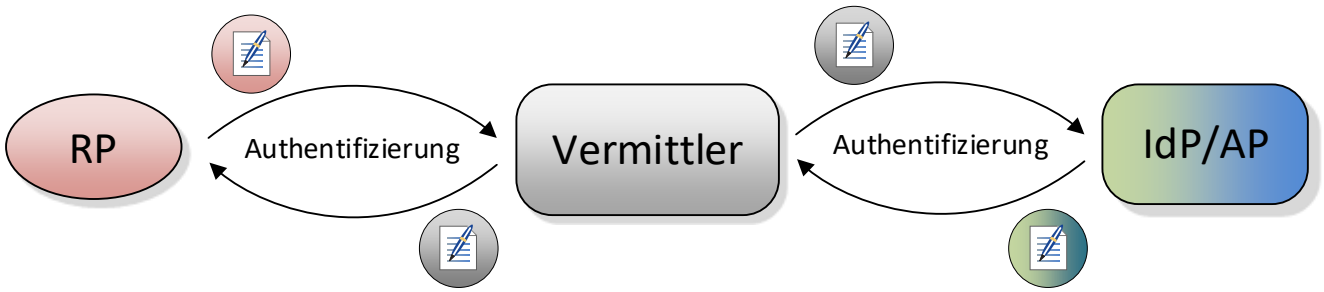

Abbildung 8: Übersicht der Schnittstellen zur Authentifizierung

4.2 Authentifizierung mit Attributübermittlung

Die Signierung und Verschlüsselung der Assertion hängt vom Vermittlermodell ab.

4.2.1 Vermittler Double-Blinding

Die detaillierte Beschreibung des Vermittlermodells Double-Blinding befindet sich im eCH-0224 [3], Kapitel 8.2.

Abbildung 9 zeigt, wie die Komponenten die Authentication und Attribute Assertion signieren. Der Vermittler MUSS die erhaltene Assertion neu signieren, sodass die RP bzw. der IdP/AP keine Kenntnis voneinander erhalten.

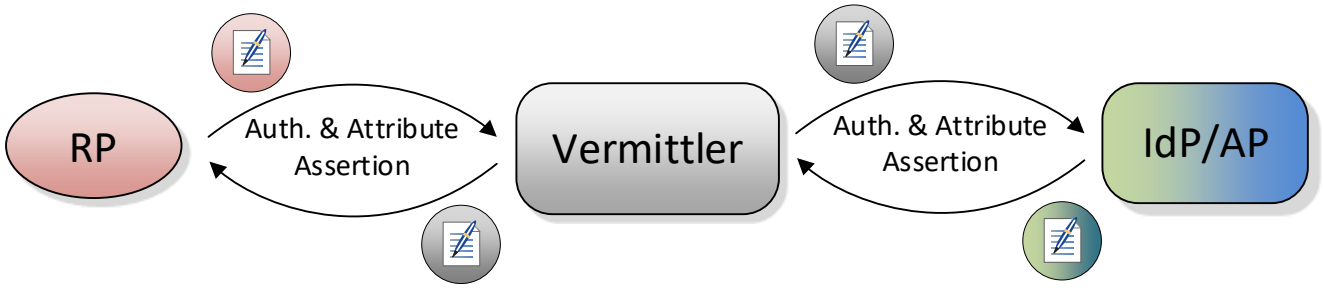

Abbildung 9: Übersicht der Assertion-Übermittlung bei Double-Blinding

4.2.2 Vermittler Offene Quellen

Die detaillierte Beschreibung des Vermittlermodells Offene Quellen befindet sich im eCH-0224 [3], Kapitel 8.3.

Variante 1 – *Signaturübermittlung*

Die RP MUSS die Quelle der Assertion identifizieren können.

Der Vermittler MUSS die Signatur des IdP/APs unverändert lassen (siehe Abbildung 10). So kann die RP anhand der Signatur den IdP/AP identifizieren.

Die Signaturübermittlung wird nur bei der Authentifizierung über den AttributeConsumingServiceIndex (siehe Kapitel 2.7.2) unterstützt.[12]

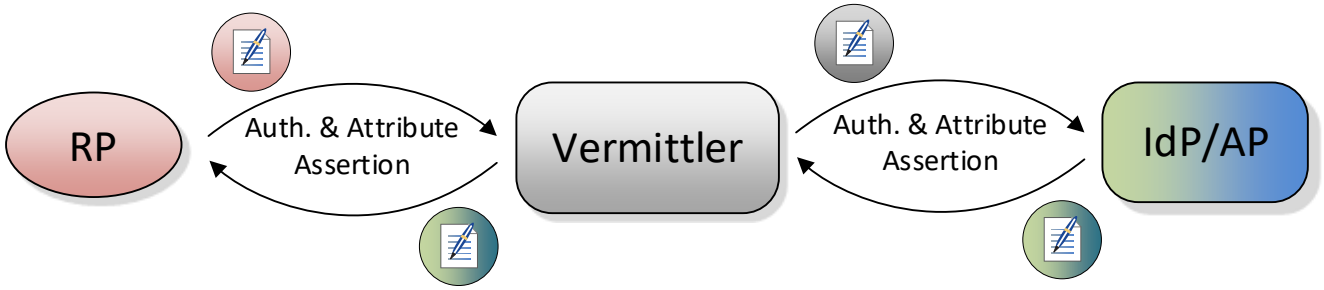

Abbildung 10: Übersicht der Assertion-Übermittlung bei Offene Quellen durch Signaturübermittlung

Variante 2 *– Identifikation per Attribut*

Der Vermittler MUSS die Assertion, wie in Abbildung 9 skizziert, neu signieren und MUSS in der Assertion mit Hilfe eines zusätzlichen Attributes den IdP/AP erkenntlich machen.

Dafür MUSS der Vermittler das Attribut `AuthenticatingAuthority` hinzufügen, der Wert MUSS die `EntityID` des entsprechenden IdP/APs sein. Ein Beispiel für eine solche Assertion befindet sich in Listing 5.

[12] Die Authentifizierung mit Attributabfrage über Attribute Query resultiert in zwei verschiedenen Assertions (Authentifizierungs- und Attributbestätigung) beim Vermittler. Der Vermittler MUSS beide Assertions zu einer neuen Assertion zusammenfügen, sodass keine Signatur vom IdP/AP übernommen werden kann.

5 Schnittstellen für die Relying Party (RP)

In diesem Kapitel werden die Schnittstellen zur RP spezifiziert. Der Ablauf der Authentifizierung ohne Attributübergabe ist in Kapitel 4.1 und eine Authentifizierung mit Attributübergabe in Kapitel 4.2 definiert. Die Authentifizierung und die Attributübergabe MUSS immer über den Vermittler laufen.

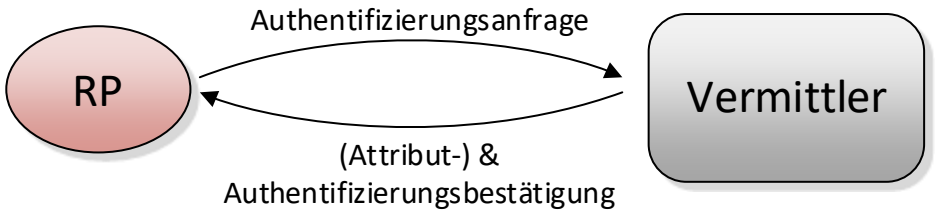

Abbildung 11: Übersicht der Schnittstellen von der RP

Die Tabelle 6 zeigt, in welchem Kapitel die entsprechende Anfrage (bzw. Antwort) der RP spezifiziert werden.

Authentifizierung	Authentifizierungsanfrage	Kapitel 5.1.1
	Authentifizierungsbestätigung	Kapitel 5.1.2
Authentifizierung mit Attributübergabe	Authentifizierungs- und Attributanfrage	Kapitel 5.2.1
	Authentifizierungs- und Attributbestätigungen	Kapitel 5.2.2

Tabelle 6: Kapitelübersicht der Schnittstellen der RP

5.1 Authentifizierung

Die RP MUSS eine Authentifizierungsanfrage an den Vermittler senden und bekommt eine `<samlp:Response>` Message zurück. Das Resultat einer erfolgreichen Authentifizierung MUSS eine Authentication Assertion sein.

5.1.1 Authentifizierungsanfrage an den Vermittler

Die RP erzeugt einen `<samlp:AuthnRequest>` (Listing 2). Der `<samlp:AuthnRequest>` enthält im Normalfall einen `<samlp:AttributeConsumingServiceIndex>`, der ein definiertes Set von Attributen identifiziert. Bei einer Authentifizierung ohne Attributanfrage wird der Wert auf Default gesetzt oder diese Angabe nicht gemacht, sodass vom Default ausgegangen wird[13]. Der `<samlp:AuthnRequest>`

[13] Damit ein Authentication Request ohne Attribut-Abfrage durchgeführt werden kann, muss der entsprechende `md:AttributeConsumingService` ohne Attribute in den Metadaten des Vermittlers definiert sein. Der Default des

wird signiert und an den SSO-Service des Vermittlers gesendet.

```
<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: Authentifizierungsanfrage von der RP zum Vermittler

5.1.2 Authentifizierungsbestätigung vom Vermittler

Der Attribute Consumer Service (ACS) der RP empfängt eine `<samlp:Response>` vom Vermittler (Listing 3). Die `<samlp:Response>` beinhaltet eine `<saml:Assertion>`, die ein `<saml:AuthnStatement>` enthält. Die RP MUSS die Signaturen der `<samlp:Response>` und `<saml:Assertion>` verifizieren und kann die Antwort des Vermittlers für den Zugriffsentscheid auf die Ressource verwenden.

Bei einer erfolgslosen Authentifizierung des Benutzers MUSS die `<samlp:Response>` eine Fehlermeldung nach den Richtlinien für Responses (Kapitel 3.5) beinhalten.

`<samlp:AttributeConsumingServiceIndex>` wird in den Metadaten (siehe Kapitel 8) definiert.

```
<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: Authentifizierungsbestätigung vom Vermittler zur RP

5.2 Authentifizierung mit Attributübergabe

Die RP MUSS eine Authentifizierungsanfrage an den Vermittler senden und bekommt eine `<samlp:Response>` Message zurück. Das Resultat einer erfolgreichen Authentifizierung MUSS eine Assertion sein, die bei erfolgreicher Authentifizierung ein AuthnStatement und die geforderten Attribute enthält. Die Attributanfrage zwischen RP und Vermittler MUSS über den `<samlp:AttributeConsumingServiceIndex>` geschehen.

5.2.1 Authentifizierungs- und Attributanfrage an den Vermittler

Die RP erzeugt einen `<samlp:AuthnRequest>` (Listing 4). Der `<samlp:AuthnRequest>` enthält einen `<samlp:AttributeConsumingServiceIndex>`, der ein definiertes Set von Attributen identifiziert. Der `<samlp:AuthnRequest>` wird signiert und an den SSO-Service des Vermittlers gesendet.

```
<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: Authentifizierungs- & Attributanfrage von der RP zum Vermittler

5.2.2 Authentifizierungs- und Attributbestätigungen vom Vermittler

Bevor der Vermittler die Attributbestätigung an die RP übermittelt, MUSS das Subjekt die Attribute freigeben. Siehe Richtlinie 6 - Freigabe der Attribute (User Consent).

Der Assertion Consuming Service (ACS) des RPs empfängt eine `<samlp:Response>`.

Die `<samlp:Response>` MUSS vom Vermittler signiert sein, für die Signierung der `<saml:Assertion>` ist das Vermittlermodell entscheidend:

Variante Double-Blinding (Kapitel 4.2.1)

Die RP DARF NICHT erkennen können, welcher IdP/AP die Assertion erzeugt hat.

Dazu MUSS die `<saml:Assertion>` vom Vermittler signiert sein.

Variante Offene-Quellen (Kapitel 4.2.2)

Die RP MUSS erkennen können, welcher IdP/AP die Assertion erzeugt hat.

Dazu MUSS die `<saml:Assertion>` vom IdP/AP signiert sein ODER in der Authentifizierungsbestätigung dem Attribut `<saml:AuthnContext>` ein weiteres Attribut `<saml:AuthenticatingAuthority>` (Listing 5) mit der EntityId des IdP/APs als Wert beinhalten. Da die Validierung der Signaturen von `<saml:Assertion>` und `<saml:Response>` mit unterschiedlichen Signaturzertifikaten bei RPs problematisch sein kann, ist die Lösung mit dem zusätzlichen Attribut zu bevorzugen.

```
<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 mit AuthenticatingAuthority-Attribut (Offene Quellen)

Listing 6 zeigt eine Authentifizierungs- und Attributbestätigung nach dem Vermittlermodell Double-Blinding.

Die RP MUSS die Signaturen der `<samlp:Response>` und `<saml:Assertion>` verifizieren und kann die Antwort des Vermittlers für den Zugriffsentscheid auf die Ressource verwenden.

```
<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
                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 6: Authentifizierungs- und Attributbestätigung vom Vermittler zur RP (Double-Blinding Model)

6 Schnittstellen für Vermittler

Der Vermittler ist der Protokoll-Endpunkt von RP und IdP/AP. Grundsätzlich sieht die RP den Vermittler als IdP/AP. Der IdP/AP sieht den Vermittler als RP.

Der Vermittler ist Bindeglied zwischen den Identitätslieferanten und -konsumenten. Die Authentifizierung und die Attributübergabe MUSS immer über den Vermittler laufen.

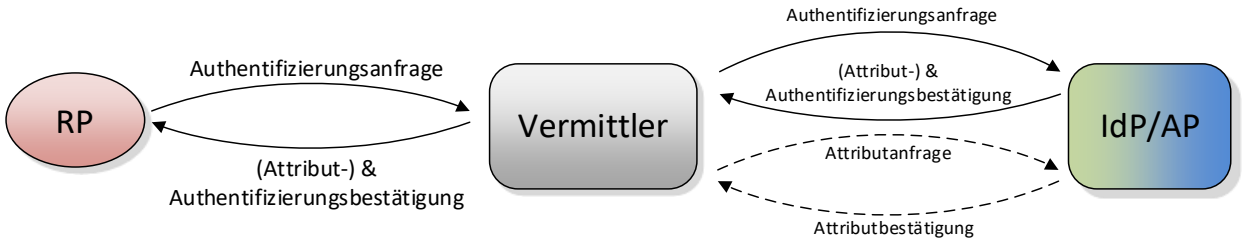

Abbildung 12: Übersicht der Schnittstellen vom Vermittler

In den folgenden Kapiteln werden die Schnittstellen spezifiziert. Dabei werden pro Anwendungsfall die ausgetauschten Nachrichten aus Sicht des Vermittlers definiert.

Die Tabelle 7 zeigt, in welchem Kapitel die entsprechende Anfrage (bzw. Antwort) des Vermittlers spezifiziert werden. Für die Attributübermittlung MUSS der Vermittler auf der Protokollstrecke zum IdP/AP sowohl die Attributübergabe mittels Attribute Query wie auch per AttributeConsumingServiceIndex unterstützen.

Authentifizierung		Authentifizierungsanfrage von der RP	Kapitel 6.1.1
		Authentifizierungsanfrage an den IdP	Kapitel 6.1.2
		Authentifizierungsbestätigung vom IdP	Kapitel 6.1.3
		Authentifizierungsbestätigung an die RP	Kapitel 6.1.4
Authentifizierung mit Attributübergabe	Attribute Consuming ServiceIndex	Authentifizierungs- und Attributanfrage von der RP	Kapitel 6.2.1
		Authentifizierungs- und Attributanfrage an den IdP/AP	Kapitel 6.2.2
		Authentifizierungs- und Attributbestätigung an den Vermittler	Kapitel 6.2.3
		Authentifizierungs- und Attributbestätigung an die RP	Kapitel 6.2.4
	Attribute Query	Authentifizierungs- und Attributanfrage von der RP	Kapitel 6.3.1
		Authentifizierungsanfrage an den IdP/AP	Kapitel 6.3.2
		Authentifizierungsbestätigung vom IdP/AP	Kapitel 6.3.3
		Attributanfrage an den IdP/AP	Kapitel 6.3.4
		Attributbestätigung vom IDP/AP	Kapitel 6.3.5
		Authentifizierungs- und Attributbestätigung an die RP	Kapitel 6.3.6

Tabelle 7: Kapitelübersicht der Schnittstellen des Vermittlers

6.1 Authentifizierung

Der Vermittler MUSS eine Authentifizierungsanfrage von der RP empfangen. Anhand dieser MUSS der Vermittler eine Authentifizierungsanfrage an den IdP/AP senden und bekommt eine `<samlp:Response>` Message zurück. Im Erfolgsfall MUSS die Reponse-Message eine Authentication Assertion enthalten. Der Vermittler MUSS die Message und Authentication Assertion neu signieren und an die RP senden.

6.1.1 Authentifizierungsanfrage von der Relying Party (RP)

Der SSO-Service des Vermittlers empfängt einen `<samlp:AuthnRequest>` von einer RP (siehe Listing 7).

Der Vermittler ermittelt die Relying Party (RP-ID) des Absenders anhand des `<saml:Issuer>` Elements in seiner Datenbasis (`<md:entityID>` Eintrag). Die Signatur der `<samlp:AuthnRequest>` wird mittels X.509 Zertifikat des RPs aus der Datenbasis verifiziert. Der Vermittler erstellt anhand der mitgelieferten `<samlp:AttributeConsumingServiceIndex>`[14] eine Liste von möglichen Authentifizierungsdiensten (IdPs) zusammen. Dabei sind je nach Ressourcen Definition folgende Szenarien möglich:

a) Die Ressource hat einen (oder mehrere) IdPs (IdP-ID) vorgegeben, die den definierten QAA-Level erfüllen. Der Vermittler zeigt auf seiner Webseite dem Benutzer die vordefinierten IdPs zur Wahl an oder leitet ihn direkt zum einzig möglichen IdP weiter.
b) Die Ressource hat einen erwünschten Authentifizierungslevel (QAA-Level) vorgegeben. Anhand dieses Werts erstellt der Vermittler eine Liste der in Frage kommenden IdPs und gibt diese dem Benutzer zur Auswahl.

Es ist möglich, weitere allgemeine Regeln zur IdP-Auswahl auf dem Vermittler zu definieren, z.B. basierend auf IP-Range oder User Agent.

```
<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: Authentifizierungsanfrage von der RP zum Vermittler

[14] Der `<samlp:AttributeConsumingServiceIndex>` ist bei einer Authentifizierung ohne Attribute auf den Default zu setzen. Ist er nicht vorhanden, ist vom Default auszugehen.

6.1.2 Authentifizierungsanfrage an den Identity Provider (IdP)

Der Vermittler erstellt anhand der von der RP empfangenen `<samlp:AuthnRequest>` einen neuen Request (siehe Listing 8). Der neue Request beinhaltet den Vermittler als `<saml:Issuer>` und den gewählte IdP als `<samlp:Destination>`.

Die `<samlp:AuthnRequest>` wird durch den Vermittler signiert und an den SSO-Service des IdPs geschickt.

```
<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: Authentifizierungsanfrage vom Vermittler zum IdP

6.1.3 Authentifizierungsbestätigung vom Identity Provider (IdP)

Der Assertion Consumer Service (ACS) des Vermittlers empfängt eine `<samlp:Response>` des IdPs (Listing 9).

Der Vermittler MUSS die Signaturen der `<samlp:Response>` und `<saml:Assertion>` verifizieren. Der Vermittler MUSS überprüfen, ob die Vertrauensstufe der Authentifizierung im Attribut `<saml:AuthContextClassRef>` vorhanden ist. Ist das Attribut nicht vorhanden, MUSS der Vermittler die Vertrauensstufe vom IdP aus den hinterlegten Metadaten einfügen.

```
<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: Authentifizierungsbestätigung vom IdP zum Vermittler

6.1.4 Authentifizierungsbestätigung an die Relying Party (RP)

Der Vermittler erstellt anhand der von der IdP empfangenen `<samlp:Response>` eine neue Response (Listing 10). Die neue Response beinhaltet den Vermittler als `<saml:Issuer>` und die relevante RP als `<samlp:Destination>`.

Der Vermittler signiert die `<samlp:Response>` und die `<saml:Assertion>` neu und sendet diese an den Assertion Consuming Service (ACS) der 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: Authentifizierungsbestätigung vom Vermittler zur RP

6.2 Authentifizierung mit Attributanfrage über AttributeConsumingServiceIndex

Der Vermittler MUSS eine Authentifizierungsanfrage von der RP empfangen. Die Authentifizierungsanfrage MUSS den `<saml:AttributeConsumingServiceIndex>` beinhalten.

Der Vermittler MUSS eine neue Authentifizierungsanfrage mit dem entsprechenden `<saml:AttributeConsumingServiceIndex>` an den gewählten IdP/AP senden. Nach erfolgreicher Authentifizierung MUSS der Vermittler eine `<samlp:Response>` Message mit einer Authentication und Attribute Assertion vom IdP/AP zurückerhalten.

Anschliessend MUSS der Vermittler die Authentication und Attribute Assertion in eine `<samlp:Response>` Message einfügen und zurück an die RP senden.

Der Vermittler MUSS den User Consent zur Attributübermittlung an die RP einholen. Dazu MUSS der Vermittler die Erlaubnis entweder vor der Authentifizierungs- und Attributanfrage an den IdP/AP ODER nach der Authentifizierungs- und Attributbestätigung vom IdP/AP einholen. Falls der User Consent nach Erhalt der Attribute eingeholt werden soll, MUSS der Vermittler zusätzlich dem Benutzer die Werte der Attribute anzeigen (siehe Kapitel 2.6).

6.2.1 Authentifizierungs- und Attributanfrage von der Relying Party (RP)

Der Vorgang nach Erhalt einer `<samlp:AuthnRequest>` von einer RP ist gleich wie in Kapitel 6.1.1. Der AttributeConsumingServiceIndex wird in diesem Fall **NICHT** den Default beinhalten (siehe Listing 11). Der Vermittler stellt nun eine Liste von IdP/APs zusammen, die zusätzlich die geforderten Attribute des Benutzers anbieten können.

```
<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: Authentifizierungsanfrage mit AttributeConsumingServiceIndex vom RP zum Vermittler

6.2.2 Authentifizierungs- und Attributanfragen an Identity & Attribute Provider (IdP/AP)

Der Vorgang zum Senden einer `<samlp:AuthnRequest>` an den IdP/AP ist gleich wie in Kapitel 6.1.2. Der `<saml:AttributeConsumingServiceIndex>` ist in diesem Fall **NICHT** der Default, sodass der IdP/AP die entsprechenden Attribute mitliefert.

6.2.3 Authentifizierungs- und Attributbestätigungen vom IdentityProvider & Attribute (IdP/AP)

Der Vorgang zum Empfangen einer `<samlp:Response>` vom IdP/AP ist gleich wie in Kapitel 6.1.3. Die Response beinhaltet in diesem Fall ein `<saml:AuthnStatement>` und ein `<saml:AttributeStatement>` mit einem oder mehreren `<saml:Attribute>` Elementen (siehe 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: Authentifizierungs- & Attributbestätigung vom IdP/AP zum Vermittler

6.2.4 Authentifizierungs- und Attributbestätigungen an die Reyling Party (RP)

Der Vermittler erstellt nun aus der `<samlp:Response>` vom IdP/AP (Listing 12) eine neue Authentifizierungs- und Attributbestätigung.

Die neue `<samlp:Response>` beinhaltet eine `<saml:Assertion>`, die die Elemente `<saml:AuthnStatement>` und `<AttributeStatement>` aus der Bestätigung vom IdP/AP beinhaltet. Die anfragende Relying Party wird als `<samlp:Destination>` festgelegt.

Die `<samlp:Response>` wird vom Vermittler neu signiert, die Signierung der `<saml:Assertion>` ist jedoch abhängig vom Vermittlermodell:

Variante Double-Blinding (Kapitel 4.2.1)

Der IdP/AP DARF NICHT für die RP erkennbar sein.

Der Vermittler MUSS die `<samlp:Response>` und `<saml:Assertion>` neu signieren.

Variante Offene-Quellen (Kapitel 4.2.2)

Der IdP/AP MUSS für die RP erkennbar sein.

Der Vermittler MUSS die Signatur vom IdP/AP der `<saml:Assertion>` belassen ODER der Authentifizierungsbestätigung in dem Attribut `<saml:AuthnContext>` ein weiteres Attribut `<saml:AuthenticatingAuthority>` mit der `EntityID` des IdP/APs als Wert hinzufügen (siehe 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: Authentifizierungsbestätigung mit AuthenticatingAuthority (Offene Quellen)

Listing 14 zeigt eine `<samlp:Response>` nach dem Vermittlermodell Double-Blinding. Die Authentifizierungs- und Attributbestätigung wird an den Attribute Consumer Service (ACS) der Relying Party gesendet.

```
<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
                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 14: Authentifizierungs- & Attributbestätigung vom Vermittler zur RP (Double Blinding)

6.3 Authentifizierung mit Attributübergabe über Attribute Query

Der Vermittler MUSS eine Authentifizierungsanfrage von der RP empfangen. Die Authentifizierungsanfrage MUSS einen `<saml:AttributeConsumingServiceIndex>` beinhalten.

Der Vermittler MUSS eine neue Authentifizierungsanfrage (ohne Attributanfrage) an den IdP/AP senden und MUSS bei einer erfolgreichen Authentifizierung eine `<samlp:Response>` Message mit einer Authentication Assertion erhalten. Anschliessend MUSS der Vermittler eine Attributanfrage an den IdP/AP senden und MUSS eine `<samlp:Response>` Message mit einer Attribute Assertion erhalten. Der Vermittler MUSS die erhaltenen Assertions zu einer Authentication und Attribut Assertion zusammenfügen und in einer `<samlp:Response>` Message zurück an die RP senden.

Der Vermittler MUSS den User Consent zur Attributübermittlung an die RP einholen. Dazu MUSS der Vermittler die Erlaubnis entweder vor der Attributanfrage an den IdP/AP ODER nach der Attributbestätigung vom IdP/AP einholen. Falls der User Consent nach Erhalt der Attribute eingeholt werden soll, MUSS der Vermittler zusätzlich dem Benutzer die Werte der Attribute anzeigen (siehe Kapitel 2.6).

6.3.1 Authentifizierungs- und Attributanfrage von der Relying Party (RP)

Der Vorgang nach Erhalt einer `<samlp:AuthnRequest>` von einer RP ist gleich wie in Kapitel 6.1.1. Der AttributeConsumingServiceIndex wird in diesem Fall **NICHT** den Default beinhalten (siehe Listing 11). Der Vermittler stellt nun eine Liste an IdP/APs zusammen, die zusätzlich zur geforderten Vertrauensstufe der Authentifizierung die geforderten Attribute anbieten.

6.3.2 Authentifizierungsanfrage an den Identity & Attribute Provider (IdP/AP)

Der Vorgang zum Senden eines `<samlp:AuthnRequest>` an den IdP/AP ist gleich wie in Kapitel 6.1.2. Der `<saml:AttributeConsumingServiceIndex>` wird jedoch **NICHT** aus der `<samlp:AuthnRequest>` von der RP übernommen, sondern MUSS auf den Default gesetzt werden.

6.3.3 Authentifizierungsbestätigung vom Identity & Attribute Provider (IdP/AP)

Der Vorgang zum Empfangen einer `<samlp:Response>` vom IdP/AP ist gleich wie in Kapitel 6.1.3.

6.3.4 Attributanfrage an den Identity & Attribute Provider (IdP/AP)

Nach Erhalt der Authentifizierungsbestätigung erstellt der Vermittler eine `<samlp:AttributeQuery>` (Listing 15). Die geforderten Attribute ermittelt der Vermittler durch den `<saml:AttributeConsumingServiceIndex>` aus der `<samlp:AuthnRequest>` von der RP.

Die Attribute werden als `<saml:Attribute>` der `<samlp:AttributeQuery>` beigefügt. Anschliessend wird die `<samlp:AttributeQuery>` vom Vermittler signiert und an den Attribute Query Service (AQS) des Attribute Providers (AP) gesendet.

```
<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: Attributanfrage vom Vermittler zum IdP/AP

6.3.5 Attributbestätigung vom Identity & Attribute Provider (IdP/AP)

Der Attribute Consumer Service (ACS) des Vermittlers empfängt eine `<samlp:Response>` (Listing 16) vom 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
                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 16: Attributbestätigung vom IdP/AP zum Vermittler

6.3.6 Authentifizierungs- und Attributbestätigungen an die Relying Party (RP)

Der Vermittler erstellt nun aus der Authentifizierungs- und der Attributbestätigung vom IdP/AP eine neue Response.

Die neue `<samlp:Response>` beinhaltet eine `<saml:Assertion>`, die die Elemente `<saml:AuthnStatement>` (Listing 9) und `<AttributeStatement>` (Listing 16) aus den vorher erhaltenen Responses zusammenfügt. Die anfragende Relying Party wird als `<samlp:Destination>` festgelegt.

Abhängig vom Vermittlermodell MUSS der Vermittler die Identifizierung des IdP/AP gegenüber der RP ermöglichen bzw. verbieten:

Variante Double-Blinding (Kapitel 4.2.1)

Der IdP/AP DARF NICHT für die RP erkennbar sein.

Der Vermittler MUSS die `<samlp:Response>` und `<saml:Assertion>` neu signieren.

Variante Offene-Quellen (Kapitel 4.2.2)[15]

Der IdP/AP MUSS für die RP erkennbar sein.

Der Vermittler MUSS in der Authentifizierungsbestätigung dem Attribut `<saml:AuthnContext>` ein weiteres Attribut `<saml:AuthenticatingAuthority>` mit dem IdP/AP als Wert hinzufügen (siehe Listing 13).

Listing 14 zeigt eine `<samlp:Response>` nach dem Vermittlermodell Double-Blinding. Die Authentifizierungs- und Attributbestätigung wird an den Attribute Consumer Service (ACS) der Relying Party gesendet.

[15] Die Variante der Signaturübermittlung wird bei der Authentifizierung mit Attributübergabe über die Attribute Query NICHT unterstützt. Der Vermittler MUSS eine neue `<saml:Assertion>` erstellen und signieren, um beide `<saml:Assertion>` vom IdP/AP zusammenfügen zu können.

7 Schnittstellen für Identity & Attribute Provider (IdP/AP)

In diesem Kapitel werden die Schnittstellen zum IdP/AP spezifiziert. Der Ablauf der Authentifizierung über eine Vermittlerinfrastruktur ist in Kapitel 4.1 und eine Authentifizierung mit Attributübergabe in Kapitel 4.2 definiert.

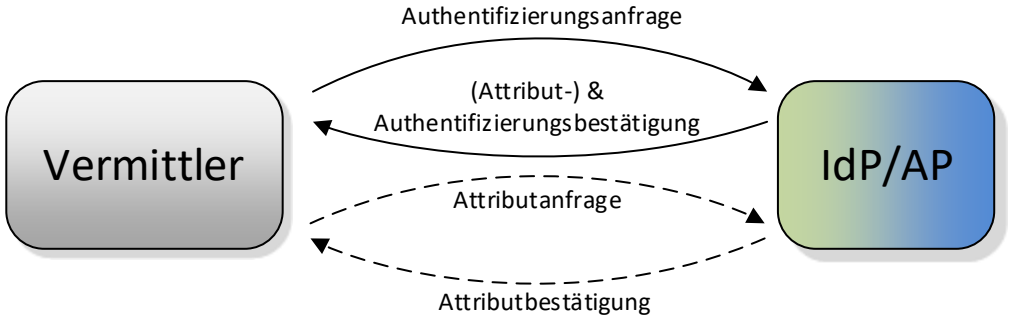

Abbildung 13: Übersicht der Schnittstellen vom Identity & Attribute Provider

In den folgenden Kapiteln werden die Schnittstellen für den IdP/AP spezifiziert. Dabei werden pro Anwendungsfall die ausgetauschten Nachrichten aus Sicht des Identity- & Attribute Providers definiert.

Die Tabelle 8 zeigt, in welchem Kapitel die entsprechenden Anfragen (bzw. Antwort) des IdP/APs spezifiziert werden. Für die Attributübermittlung MUSS der IdP/AP entweder die Attribute Query oder die Attributanfrage mittels `AttributeConsumingServiceIndex` unterstützen.

Authentifizierung		Authentifizierungsanfrage vom Vermittler	Kapitel 7.1.1
		Authentifizierungsbestätigung an den Vermittler	Kapitel 7.1.2
Authentifizierung mit Attributübergabe	Attribute Consuming-ServiceIndex	Authentifizierungs- und Attributanfrage vom Vermittler	Kapitel 7.2.1
		Authentifizierungs- und Attributbestätigung an den Vermittler	Kapitel 7.2.2
	Attribute Query	Authentifizierungsanfrage vom Vermittler	Kapitel 7.3.1
		Authentifizierungsbestätigung an den Vermittler	Kapitel 7.3.2
		Attributanfrage vom Vermittler	Kapitel 7.3.3
		Attributbestätigung an den Vermittler	Kapitel 7.3.4

Tabelle 8: Kapitelübersicht der Schnittstellen des IdP/APs

7.1 Authentifizierung

Der IdP/AP MUSS eine Authentifizierungsanfrage vom Vermittler empfangen. Der IdP/AP MUSS den Benutzer auffordern, sich zu authentifizieren. Bei erfolgreicher Authentifizierung MUSS der IdP/AP eine `<samlp:Response>` Message mit einer Authentication Assertion zurück an den Vermittler senden.

7.1.1 Authentifizierungsanfrage vom Vermittler

Der SSO-Service des IdP/APs empfängt einen `<samlp:AuthnRequest>` (Listing 17). Der IdP/AP MUSS den Benutzer auffordern, sich zu authentisieren.[16]

Nach erfolgreicher Authentisierung wird der Benutzer vom IdP/AP authentifiziert. In den seltenen Ausnahmefällen, bei denen der IdP/AP das Einverständnis vom Benutzer selbst einholt, wird dies in den Metadaten des IdP/APs vermerkt und der Vermittler holt kein weiteres Einverständnis ein.

```
<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: Authentifizierungsanfrage vom Vermittler zum IdP/AP

Bei einer erfolgslosen Authentifizierung[17] des Benutzers MUSS der IdP/AP eine `<samlp:Response>` erstellen, die eine Fehlermeldung nach den Richtlinien für Responses (Kapitel 3.5) beinhaltet.

[16] Die Authentisierungsmethode ist dem IdP zu überlassen, muss aber der ausgewiesenen Vertrauensstufe entsprechen. Gängige Methoden sind u.a. Username/Password, PKI basierend, 2FA, etc.

[17] Der IdP/AP definiert, wann eine Authentifizierung als erfolglos betrachtet wird. Darunter können z.B. Fehlauthentifizierung, Zeitüberschreitung, Abbruch des Benutzers oder Überschreitung der maximalen Anzahl an Versuchen fallen.

7.1.2 Authentifizierungsbestätigung an den Vermittler

Der IdP erzeugt eine `<samlp:Response>`, welche ein `<saml:AuthnStatement>` in einer `<saml:Assertion>` enthält (Listing 18).
Die `<samlp:Response>` und `<saml:Assertion>` werden vom IdP/AP signiert und zurück an den ACS des Vermittlers gesendet.

```
<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: Authentifizierungsbestätigung vom IdP/AP zum Vermittler

7.2 Authentifizierung mit Attributanfrage über AttributeConsumingServiceIndex

Der IdP/AP MUSS eine Authentifizierungsanfrage von dem Vermittler empfangen. Der IdP/AP MUSS den Benutzer auffordern, sich zu authentifizieren. Bei erfolgreicher Authentifizierung MUSS der IdP/AP eine `<samlp:Response>` Message mit einer Authentication und Attribute Assertion zurück an den Vermittler senden.

7.2.1 Authentifizierungs- und Attributanfrage vom Vermittler

Der Vorgang nach Erhalt einer `<samlp:AuthnRequest>` von dem Vermittler ist gleich wie in Kapitel 7.1.1. Zusätzlich werden durch den `<saml:AttributeConsumingServiceIndex>` die definierten Attribute ermittelt und überprüft, ob der Benutzer über diese Attribute verfügt.

7.2.2 Authentifizierungs- und Attributbestätigung an den Vermittler

Der IdP/AP erzeugt nun die Authentifizierungs- und Attributbestätigung, welche eine `<saml:Assertion>` mit `<saml:AuthnStatement>` und `<saml:AttributeStatement>` beinhaltet (Listing 19). Das `<saml:AttributeStatement>` enthält die aus der `<samlp:AuthnRequest>` angeforderten Attribute als `<saml:Attribute>` mit `<saml:AttributeValue>`.

Die `<samlp:Response>` und `<saml:Assertion>` werden vom IdP/AP signiert und zurück an den Attribute Consumer Service (ACS) des Vermittlers gesendet.

```
<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 19: Authentifizierungs- und Attributbestätigung vom IdP/AP zum Vermittler

7.3 Authentifizierung mit Attributanfrage über Attribute Query

Der IdP/AP MUSS eine Authentifizierungsanfrage von dem Vermittler empfangen. Der IdP/AP MUSS den Benutzer auffordern, sich zu authentifizieren. Bei erfolgreicher Authentifizierung MUSS der IdP/AP eine `<samlp:Response>` Message mit einer Authentication Assertion zurück an den Vermittler senden. Nach der Übermittlung der Authentifizierungsbestätigung MUSS der IdP/AP eine Attributanfrage vom Vermittler empfangen. Der IdP/AP MUSS eine `<samlp:Response>` Message mit einer Attribute Assertion erzeugen und zurück an den Vermittler senden.

7.3.1 Authentifizierungsanfrage vom Vermittler

Der Vorgang zum Empfangen einer `<samlp:Response>` vom Vermittler ist gleich wie in Kapitel 7.1.1.

7.3.2 Authentifizierungsbestätigung an den Vermittler

Das Erzeugen der Authentifizierungsbestätigung ist gleich wie in Kapitel 7.1.2.

7.3.3 Attributanfrage vom Vermittler

Der Attribute Query Service (AQS) des IdP/APs empfängt eine `<samlp:AttributeQuery>` (Listing 20). Die geforderten Attribute sind als `<saml:Attribute>` gelistet. Der IdP/AP überprüft, ob der Benutzer über die im `<saml:Attribute>` definierten Attribute verfügt.

```
<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: Attributanfrage vom Vermittler zum IdP/AP

7.3.4 Attributbestätigung an den Vermittler

Der IdP/AP erstellt anhand der gelisteten Attribute in der Attribute Query (Listing 20) eine `<samlp:Response>` (Listing 21). Für die Response stellt der IdP/AP eine `<saml:Assertion>` zusammen, welche ein `<saml:AttributeStatement>` mit `<saml:Attribute>` und `<saml:AttributeValue>` Elementen beinhaltet. Die `<saml:Assertion>` und `<samlp:Response>` werden vom IdP/AP signiert und an den ACS des Vermittlers gesendet.

Falls die angefragten Attribute nicht übermittelt werden können, MUSS eine `<samlp:Response>` mit nach `<samlp:StatusCode>` gemäss Kapitel 3.5 zum Vermittler gesendet werden.

```
<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
                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 21: Attributbestätigung vom IdP/AP zum Vermittler

8 Metadaten

Jede Komponente der Domäne (Vermittler, IdPs, IdP/APs, RPs), die über SAML-Services verfügt, muss die zu diesen Services notwendigen Informationen in der Datenbasis (Metadaten) des Vermittlers ablegen.[18] Diese komponentenspezifischen Informationen werden in der Regel manuell über ein GUI von einer dazu autorisierten Person eingegeben.[19]

Es werden die Metainformationen aller SAML-Komponenten von den zuständigen Administratoren erfasst.

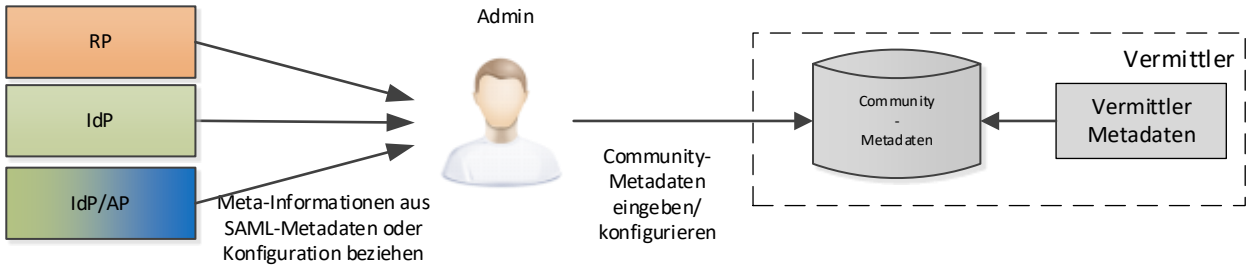

Abbildung 14: Erfassen der Meta-Informationen beim Vermittler

In einer Datenbasis (Komponenten-Management) des Vermittlers werden neben den SAML-Metadaten noch weitere Informationen zu den einzelnen Komponenten abgelegt. Hier werden die Anforderungen der Ressourcen der RPs erfasst und die Angebote der IdPs bzw. IdP/APs erfasst.

8.1 Community-Metadaten

In den Community-Metadaten werden die einzelnen Komponenten einer Organisation, also IdP, IdP/AP und Relying Party (RP), verwaltet. Ausserdem werden im Falle einer Relying Party die Anforderungen der Ressourcen sowie bei einem IdP/AP die angebotenen Vertrauensstufen der Authentifizierung und der Attribute geführt. Alternativ können sich die Teilnehmer einer Domäne auch auf eine Vertrauensstufe einigen, die dann für alle gilt.

8.1.1 Relying Party

Für eine Relying Party muss ein Service Provider Service definieren werden, welcher die Authentication und Attribute Assertions entgegennimmt. Unterhalb des Service Providers, können eine oder mehrere Ressourcen definiert werden.

Für den Service Provider Service wird definiert:

[18] Fall die Identity Federation mehrere Domänen umfasst, MÜSSEN die Metadaten der einzelnen Domänen getrennt verwaltet und publiziert werden.

[19] Alternativ könnten diese Informationen auch auf der Komponente lokal erzeugt und in den Vermittler über eine vorgegebene Schnittstelle hochgeladen werden. Diese Uploadfunktion und die Verarbeitung dieser Metadaten auf dem Vermittler sind optional.

- SAML-Metadaten: Meta-Daten der RP, inklusive der Schlüsselinformationen[20] zum Verschlüsseln und Verifizieren der Signatur,
    - AssertionConsumerService: URI des Service Provider Services,[21]
- (Optional) Angabe, ob verschlüsselte Assertions unterstützt werden.

Für jede Ressource wird definiert:

- Geforderte Vertrauensstufe[22] der Authentifizierung entspr. eCH-0170 [13],
- Liste der angeforderten Attribute, ggf. mit Attributqualität (siehe auch Richtlinie 5 in Kapitel 3.1)[23],
- (optional) Priorisierte Liste der akzeptierten IdP/APs.

8.1.2 IdP & IdP/AP

Für einen IdP wird definiert:

- SAML-Metadaten: Meta-Daten des IdP, inklusive der Schlüsselinformationen zum Verschlüsseln und Verifizieren der Signatur,
    - Endpoints für den AuthenticationService und optional für den SingleLogoutService
- Unterstützte Vertrauensstufen bei der Authentifizierung

Agiert ein IdP als IdP/AP müssen zusätzlich definiert werden:

- SAML-Metadaten des Attribute Query Service
- Angebotene Attribute mit ihrer Qualität nach dem in Richtlinie 5 (siehe Kapitel 3.1) vorgeschlagenem Qualitätsmodell.

8.2 SAML-Metadaten

Der Vermittler muss über die Metainformationen der SAML-Services aller Komponenten der Domäne verfügen (siehe auch [20]). Die peripheren SAML-Komponenten benötigen aber auch bestimmte Informationen einzelner Komponenten:

- Die RPs müssen die Metainformationen der SSO-Services des Vermittlers kennen.
    - Beim Vermittlermodel Offene Quellen mit Signaturübermittlung müssen die RPs auch die Public Keys der IdP/APs zur Überprüfung der Signatur der Assertions kennen.

---

[20] Auch die Verfahren zum Schlüsselaustausch etc. müssen in der Domäne geregelt werden. Ein Beispiel einer entspr. Guideline findet befindet sich bei Switch: https://www.switch.ch/aai/guides/sp/certificate-rollover/ .

[21] Falls SingleLogout unterstützt werden soll, kann URI für den SingleLogoutService des Service Providers angegeben werden.

[22] Im Normalfall werden nur die Vertrauensstufen VS1 bis VS3 verwendet, da die Vertrauensstufe 4 zusätzliche Anforderungen sowohl an die RP wie auch die anderen Komponenten in der Domäne stellt.

[23] Für jedes geforderte Attribut-Set muss in den SAML-Metadaten ein entspr. `<md:AssertionConsumerService>` Elemente definiert werden. Das Default `<md:AssertionConsumerService>` Element sollte einer Authentifizierung ohne Attribute entsprechen.

- Die IdPs und IdP/APs müssen die Metainformationen der ACS-Services des Vermittlers kennen.

Da alle peripheren Komponenten SAML 2.0 unterstützen, kann die Verteilung dieser Metainformationen mittels SAML-Metadaten erfolgen. Die Aufbereitung der notwendigen SAML-Metadaten erfolgt durch einen Metadata-Aggregator-Dienst.[24] Dazu muss dieser Dienst periodisch die Informationen zum Vermittler und den angeschlossen IdPs und IdP/APs signiert publizieren. Anschliessend können diese SAML-Metadaten von den Mitgliedern der Domäne abgeholt, validiert und bei sich integriert werden.

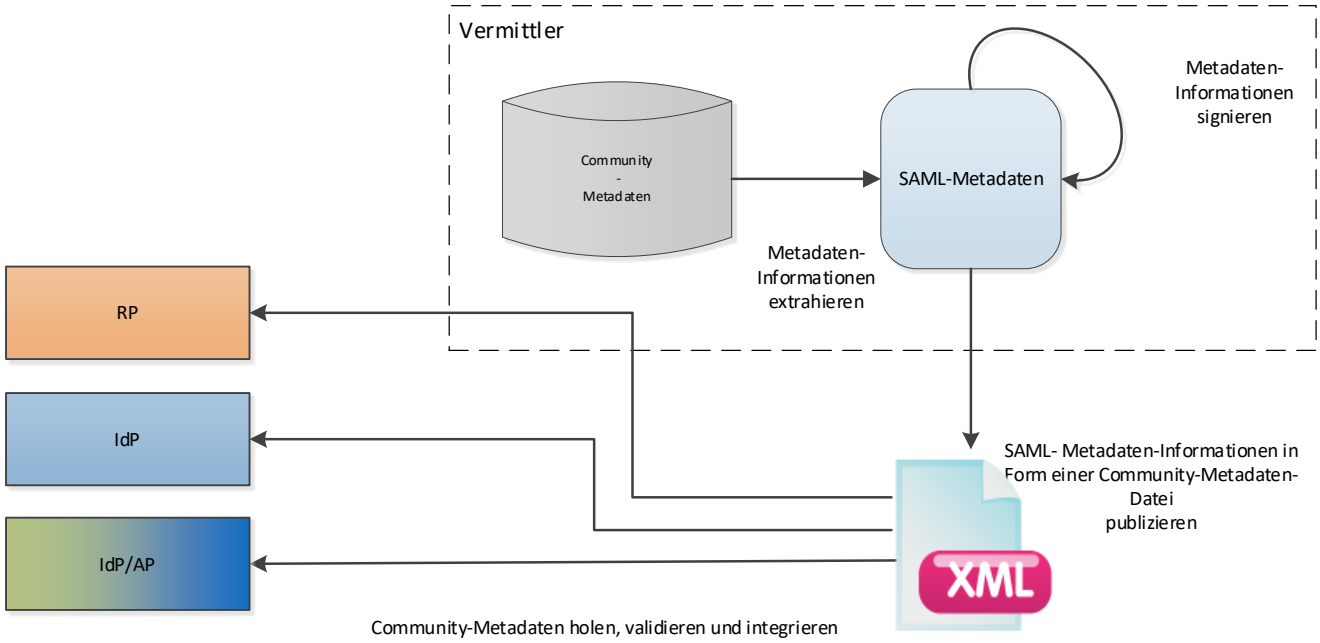

Abbildung 15: Publizierung der SAML-Metadaten

Auf diese Weise verfügen die Mitglieder der Domäne über alle notwendigen Informationen, um mit dem Vermittler über SAML 2.0 kommunizieren zu können.

Die SAML-Metadaten enthalten alle notwendigen Informationen über die SAML-Services des Vermittlers und der IdPs bzw. IdP/AAs. Sie werden periodisch vom Metadata-Aggregator-Dienst erstellt, signiert und publiziert.

Listing 22 zeigt ein Beispiel einer vom Metadata-Aggregator-Dienst publizierten SAML-Metadaten-Datei.

Eine SAML-Metadaten-Datei enthält ein `<md:EntitiesDescriptor>` Element, welches die `<md:EntityDescriptor>` des Vermittlers (SSO und ACS) sowie die SSO aller IdPs bzw. IdP/APs enthält. Das `validUntil` Attribut gibt die Gültigkeitszeit der SAMLCommunity-Metadaten-Datei und das `cacheDuration` Attribut die maximale Länge der Zeit an, während die Komponenten der Domäne die SAML-Metadaten-Datei speichern sollten.

[24] Der Metadata-Aggregator-Dienst kann auch unabhängig vom Vermittler als separate Komponente implementiert werden.

```
<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>

    <!-- Vermittler -->
    <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: SAML-Metadaten-Datei

8.2.1 SAML-Metadaten-Richtlinien

In der Folge werden die zu publizierenden SAML-Metadaten näher beschrieben. Sie enthalten unter anderem Informationen über:

Die Adresse und den Namen der Entität (Komponente).
Die Endpunktkonfigurationen der Entität (URL).
Die Public-Key-Zertifikate zur Prüfung signierter SAML-Nachrichten.
Die Public-Key-Zertifikate zur Prüfung signierter SAML-Assertions.
SAML-Attribute, die von der Entität konsumiert/erzeugt werden können.

8.2.2 Allgemeine Vorgaben zu `<md:EntityDescriptor>` Elementen

- Die Vermittler Metadaten Definition MUSS mit einem `<md:EntityDescriptor>` Element beginnen.
- Das `<md:EntityDescriptor>` Element MUSS ein `entityID` Attribut haben. Dessen Wert MUSS eine URI sein, welche in der Domäne eindeutig ist und als Identifikator verwendet wird.
- Im `<md:EntityDescriptor>` Element MUSS ein `<Extensions>` Element mit den vom Vermittler oder IdP/AP unterstützten *Authentication Assurance Level* gemäss *SAMLV2.0 Identity Assurance Profiles* [11] angeben werden.
- Das `<md:EntityDescriptor>` Element KANN ein oder mehrere Elemente vom Typ `<md:IDPSSODescriptor>`, `<md:SPSSODescriptor>` oder `<md:AttributeAuthority-Descriptor>` enthalten.
- Das `<md:EntityDescriptor>` Element KANN ein `<md:Organization>` Element enthalten, welches wiederum ein `<md:OrganizationName>` und eine `<md:OrganizationURL>` aufweist.
- Ein `<md:OrganizationDisplayName>` Element und ein `<md:ContactPerson>` Element sind

OPTIONAL.

8.2.3 Vorgaben zu Vermittler Metadaten

IDPSSODescriptor:

Der IDPSSODescriptor beschreibt die SSO-Metainformationen des Vermittlers.

- Das `<md:EntityDescriptor>` Element des Vermittlers MUSS ein Element vom Typ `<md:IDPSSODescriptor>` und ein Element vom Typ `<md:SPSSODescriptor>` enthalten.
- Das `<md:IDPSSODescriptor>` Element MUSS ein `protocolSupportEnumeration` Attribut haben, dessen Wert MUSS `urn:oasis:names:tc:SAML:2.0:protocol` sein.
- Das `WantAuthnRequestsSigned` Attribut des `<md:IDPSSODescriptor>` Elementes MUSS auf `true` gesetzt werden. Dies bedeutet, dass die RP den Authentication Request (`<samlp:AuthnRequest>`) signieren MÜSSEN, sonst wird dieser vom Vermittler nicht akzeptiert.
- Das `<md:KeyDescriptor>` Element für Signatur MUSS im `<md:IDPSSODescriptor>` vorhanden sein. Dessen `<ds:KeyInfo>` MUSS ein `<ds:X509Data>` Element enthalten, und dieses wiederum ein `<ds:X509Certificate>`.
- Das `<md:IDPSSODescriptor>` Element MUSS ein oder mehrere `<md:SingleSignOnService>` Elemente enthalten.
- Das `<md:IDPSSODescriptor>` Element KANN ein oder mehrere `<md:SingleLogOutService>` Elemente enthalten.[25]
- Das `<md:IDPSSODescriptor>` Element MUSS mehrere `<md:NameIDFormat>` Elemente enthalten. Es MÜSSEN `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` und `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` unterstützt werden [14].

SPSSODescriptor:

Der SPSSODescriptor beschreibt die Service Provider Metainformationen des Vermittlers.

- Das `<md:SPSSODescriptor>` Element des Vermittlers MUSS ein `protocolSupportEnumeration` Attribut haben, dessen Wert MUSS `urn:oasis:names:tc:SAML:2.0:protocol` sein.
- Das `WantAssertionsSigned` Attribut des `<md:SPSSODescriptor>` Elementes MUSS auf `true` gesetzt werden.
- Das `AuthnRequestsSigned` Attribut des `<md:SPSSODescriptor>` Elementes MUSS auf `true` gesetzt sein.
- Das `<md:KeyDescriptor>` Element für Signatur MUSS im `<md:SPSSODescriptor>` vorhanden sein. Dessen `<ds:KeyInfo>` MUSS ein `<ds:X509Data>` Element enthalten, und dieses wiederum ein `<ds:X509Certificate>`.
- Das `<md:SPSSODescriptor>` Element MUSS ein oder mehrere `<md:AssertionConsumerService>` Elemente[26] enthalten. Das `index` Attribut MUSS in jedem `<md:AssertionConsumerService>` Element vorhanden sein. Das Protocol Binding `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST` MUSS unterstützt werden.
- Das `<md:SPSSODescriptor>` Element MUSS mindestens ein `<md:NameIDFormat>` Element enthalten. Es MÜSSEN `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` und

[25] Eine Beschreibung der Umsetzung von SLO in einer Identity Federation würde den Rahmen des Standards sprengen und wird daher nicht berücksichtigt.

[26] Das Default `<md:AssertionConsumerService>` Element sollte einer Authentifizierung ohne Attribute entsprechen. Weitere solche Elemente müssen für die geforderter Attribut-Sets der angeschlossenen RPs definiert werden.

`urn:oasis:names:tc:SAML:2.0:nameid-format:transient` unterstützt werden [14].

```
<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">
             Vermittler Provider
         </md:OrganizationName>
         <md:OrganizationDisplayName xml:lang="en">
             Vermittler 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: Beispiel eines Vermittler EntityDescriptors

8.2.4 Vorgaben zu IdP/AP Metadaten

Das `<md:EntityDescriptor>` Element eines IdP/APs MUSS ein `<md:IDPSSODescriptor>` Element mit den folgenden Angaben (vgl. dazu Listing 24) und KANN ein `<md:AttributeAuthority-Descriptor>` Element enthalten.

- Das `<md:IDPSSODescriptor>` Element MUSS ein `protocolSupportEnumeration` Attribut haben, dessen Wert MUSS `urn:oasis:names:tc:SAML:2.0:protocol` sein.
- Das `WantAuthenticationRequestsSigned` Attribut des `<md:IDPSSODescriptor>` Elementes MUSS auf `true` gesetzt werden.
- Das `<md:KeyDescriptor>` Element für Signatur MUSS im `<md:IDPSSODescriptor>` vorhanden sein. Dessen `<ds:KeyInfo>` MUSS ein `<ds:X509Data>` Element enthalten, und dieses wiederum ein `<ds:X509Certificate>`.
- Das `<md:IDPSSODescriptor>` Element MUSS ein oder mehrere `<md:SingleSignOnService>` Elemente enthalten. Das HTTP-POST Protocol Binding MUSS unterstützt sein.
- Das `<md:IDPSSODescriptor>` Element KANN mehrere `<md:NameIDFormat>` Elemente enthalten. Es MUSS `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` und KANN `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` unterstützt werden [14].

Optional kann ein `<md:AttributeAuthorityDescriptor>` definiert sein, wenn der IdP/AP AttributQueries unterstützt.

- Das `<md:AttributeAuthorityDescriptor>` Element MUSS ein `protocolSupportEnumeration` Attribut haben, dessen Wert MUSS `urn:oasis:names:tc:SAML:2.0:protocol` sein.
- Das `<md:KeyDescriptor>` Element für Signatur MUSS im `<md:AttributeAuthority-Descriptor>` vorhanden sein. Dessen `<ds:KeyInfo>` MUSS ein `<ds:X509Data>` Element enthalten, und dieses wiederum ein `<ds:X509Certificate>`
- Das `<md:AttributeAuthorityDescriptor>` Element MUSS mindestens ein `<md:AttributeService>` Element enthalten.

```
<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: Beispiel eines IdP/AP EntityDescriptor

9 Sicherheitsüberlegungen

Die Speicherung und Übertragung von Personendaten darf nur auf Grund und im Rahmen von bestehenden rechtlichen Grundlagen erfolgen und hat die gesetzlichen Datenschutzbestimmungen zu befolgen. Die nötigen Vorkehrungen sind zu treffen, dass die Daten fehlerfrei übertragen und vor, während und nach der Übertragung nur von dazu autorisierten Personen eingesehen und verändert werden können.

Falls ein IAM-System gemäss BGEID [21] oder ähnlicher Gesetze umgesetzt wird, müssen die gesetzlichen Bestimmungen, sowie die dazugehörigen Verordnungen und Ausführungsbestimmungen eingehalten werden, bevor die in den eCH-Standards definierten Richtlinien angewendet werden können.

10 Haftungsausschluss/Hinweise auf Rechte Dritter

eCH-Standards, welche der Verein **eCH** dem Benutzer zur unentgeltlichen Nutzung zur Verfügung stellen oder welche **eCH** referenzieren, haben nur den Status von Empfehlungen. Der Verein **eCH** haftet in keinem Fall für Entscheidungen oder Massnahmen, welche der Benutzer auf Grund dieser Dokumente trifft und / oder ergreift. Der Benutzer ist verpflichtet, die Dokumente vor deren Nutzung selbst zu überprüfen und sich gegebenenfalls beraten zu lassen. **eCH**-Standards können und sollen die technische, organisatorische oder juristische Beratung im konkreten Einzelfall nicht ersetzen.

In **eCH**-Standards referenzierte Dokumente, Verfahren, Methoden, Produkte und Standards sind unter Umständen markenrechtlich, urheberrechtlich oder patentrechtlich geschützt. Es liegt in der ausschliesslichen Verantwortlichkeit des Benutzers, sich die allenfalls erforderlichen Rechte bei den jeweils berechtigten Personen und/oder Organisationen zu beschaffen.

Obwohl der Verein **eCH** all seine Sorgfalt darauf verwendet, die **eCH**-Standards sorgfältig auszuarbeiten, kann keine Zusicherung oder Garantie auf Aktualität, Vollständigkeit, Richtigkeit bzw. Fehlerfreiheit der zur Verfügung gestellten Informationen und Dokumente gegeben werden. Der Inhalt von **eCH**-Standards kann jederzeit und ohne Ankündigung geändert werden.

Jede Haftung für Schäden, welche dem Benutzer aus dem Gebrauch der **eCH**-Standards entstehen ist, soweit gesetzlich zulässig, wegbedungen.

11 Urheberrechte

Wer **eCH**-Standards erarbeitet, behält das geistige Eigentum an diesen. Allerdings verpflichtet sich der Erarbeitende, sein betreffendes geistiges Eigentum oder seine Rechte an geistigem Eigentum anderer, sofern möglich, den jeweiligen Fachgruppen und dem Verein **eCH** kostenlos zur uneingeschränkten Nutzung und Weiterentwicklung im Rahmen des Vereinszweckes zur Verfügung zu stellen.

Die von den Fachgruppen erarbeiteten Standards können unter Nennung der jeweiligen Urheber von **eCH** unentgeltlich und uneingeschränkt genutzt, weiterverbreitet und weiterentwickelt werden.

eCH-Standards sind vollständig dokumentiert und frei von lizenz- und/oder patentrechtlichen Einschränkungen. Die dazugehörige Dokumentation kann unentgeltlich bezogen werden.

Diese Bestimmungen gelten ausschliesslich für die von **eCH** erarbeiteten Standards, nicht jedoch für Standards oder Produkte Dritter, auf welche in den **eCH**-Standards Bezug genommen wird. Die Standards enthalten die entsprechenden Hinweise auf die Rechte Dritter.

Anhang A – Referenzen und Bibliographie

[1]	IETF, «RFC 2119,» 1997. [Online]. Available: http://www.ietf.org/rfc/rfc2119.txt.
[2]	eCH, «eCH-0219 IAM Glossar, Version 1.0,» 30 November 2018. [Online]. Available: https://ech.ch/de/standards/60491.
[3]	eCH, «eCH-0224 Vermittlerbasierte Identity Federation Architekturmodelle, Version 1.0,» 05 Juni 2020. [Online]. Available: https://ech.ch/de/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 Vermittlerbasierte Identity Federations – Implementierung mit OIDC,» 2020.
[7]	eCH, «eCH-0107 Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM), Version 3.0,» 07 Februar 2019. [Online]. Available: https://ech.ch/de/standards/60198.
[8]	eCH, «eCH-0167 SuisseTrustIAM Rahmenkonzept,» 6 Juni 2014. [Online]. Available: https://ech.ch/de/standards/60432.
[9]	eCH, «eCH-0168 SuisseTrustIAM technische Architektur und Prozesse,» 27 November 2014. [Online]. Available: https://ech.ch/de/standards/60577.
[10]	eCH, «eCH-0169 SuisseTrustIAM-Geschäftsarchitektur V1.0,» 4 September 2014. [Online]. Available: https://ech.ch/de/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 eID Qualitätsmodell, Version 2.0,» 13 September 2017. [Online]. Available: https://ech.ch/de/standards/60593.
[14]	OASIS, «Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 – Errata Composite,» 07 September 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 XML-Signatur und Verschlüsselung V2.0.0,» 2' April 2021. [Online].

	Available: https://ech.ch/de/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]	Eidgenössisches Justiz- und Polizeidepartement EJPD, «Bundesgesetz über elektronische Identifizierungsdienste (BGEID),» [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 PKI-Zertifikatsklassen V2.0,» 30 11 2018. [Online]. Available: https://ech.ch/de/standards/60507.

Anhang B – Mitarbeit & Überprüfung

Bracklo Sven	Berner Fachhochschule
Hassenstein Gerhard	Berner Fachhochschule
Kunz Marc	Mitglied eCH FG IAM
Laube-Rosenpflanzer Annett	Berner Fachhochschule

Anhang C – Abkürzungen und Glossar

ACS	Assertion Consumer Service
AQS	Attribute Query Service
AP	Attribute Provider
HoK	Holder-of-Key
IAM	Identity und 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

Dieses Dokument verwendet grundsätzlich die Begriffsdefinitionen aus eCH-0219 [2].

Anhang D – Änderungen gegenüber Vorversion

Der vorliegende Standard beschreibt die Implementierung von vermittlerbasierten Identity Federation Modelle aus eCH-0224 [3]. Version 1.0 basierte auf dem Architektur-Modell von SuisseTrust Identity and Access Management (STIAM) beschrieben in eCH-0168 [9].

Aufgrund des veränderten Architekturmodell wurde auch die Kapitelstruktur verändert und der Standard wurde ähnlich aufgebaut wie der eCH-0225 [6], der die OIDC-Implementierung der vermittlerbasierten Identity Federation Modelle aus eCH-0224 beschreibt.

Nachfolgend werden die generellen Änderungen aufgeführt und auf die jeweiligen Inhalte in eCH-0174 Version 1.00 verwiesen.

Grundsätzliches:

V2.0.0 beschränkt sich konsequent auf die Implementierung von vermittlerbasierten Identity Federation Modelle aus eCH-0224, dabei werden nur Varianten beschrieben, die bereits in der Praxis umgesetzt wurden.
Der Titel des Standards wurde entsprechend angepasst.
Alle STIAM-Begriffe wurden systematisch durch die im eCH-0224 [3] verwendete Terminologie ersetzt.
Da die Unabhängigkeit von den STIAM-Standards, wie eCH-0168 [9], ein Ziel der aktualisierten Version dieses Standards war, wurden Teile vom eCH-0168 in aktualisierter Form übernommen.

Kapitel	Seite	Anpassung	RFC Nr.
1.2	6	Einleitung [eCH-0174 V1.0 Kapitel 1] Die Einleitung wurde komplett überarbeitet und an den neuen Inhalt angepasst.	-
0	10	Identity Federations basierend auf SAML [eCH-0174 V1.0 Kapitel 3 und 4] • Kapitel 2 beschreibt die verschiedenen SAML-Services, die von den einzelen Komponenten zur Verfügung gestellt werden müssen, sowie die Interaktionen dieser Services, wobei nur die Laufzeit-Prozesse der Vermittlermodelle aus eCH-0224 betrachtet werden. • Die folgenden Protokolle aus dem eCH-0174 v1.0 wurden nicht in die Version v2.0 übernommen, da diese ohne praktische Bedeutung sind. - Zur Laufzeit: ○ Single Logout - Zur Definitionszeit: ○ IdP-Linking, ○ AA-Linking, ○ RP-Linking.	-

Kapitel	Seite	Anpassung	RFC Nr.
3	23	**Richtlinien [eCH-0174 V1.0 Kapitel 2 und 6]** Das Kapitel enthält die in eCH-0174 V1.0 Kapitel 2 definierten Anforderungen soweit nicht bereits in eCH-0107 v3.0 [7] bzw. eCH-0224 [3] vorhanden sind. Es werden Richtlinien definiert, die eingehalten werden müssen, um den Anforderungen an eine Identity Federation im E-Government nach eCH-0224 [3] und eCH-0107 [7] zu genügen. Die Richtlinien für die SAML-Message wurden weitgehend aus dem Standard eCH-0174 V1.0 übernommen und in einigen wenigen Punkte angepasst. Auf die Messages für Single Logout (Request und Response) wurde verzichtet, da diese ohne praktische Bedeutung sind.	-
4	29	**Schnittstellen der Vermittlermodelle [neu]** Kapitel 4 definiert die Schnittstellen für zwei Vermittlermodelle **Offene Quellen** und **Double-Blinding** aus dem eCH-Standard eCH-0224 [3].	-
5, 6, 7	31, 37, 50	**Schnittstellen für die RP, Vermittler und IdP/AP [neu]** Folgend der Vorlage des eCH-Standards eCH-0225 [6] wurden die Schnittstellen für die drei Komponenten jeweils in einem eigenen Kapitel beschrieben.	-
8	57	**Metadaten [eCH-0174 V1.0 Kapitel 5]** Das Kapitel beschreibt die notwendigen Community- und SAML-Metadaten einer Identity Federation, die mit SAML V2.0 implementiert wird. Die Informationen zu den Community-Metadaten wurden in verkürzter und angepasster Form aus dem eCH-0168 [9] Kapitel 9 übernommen. Die SAML-Metadaten entsprechen den Angaben aus eCH-0174 V1.0 in aktualisierter Form.	-

Tabelle 9 Änderungen gegenüber Vorversion

Nicht übernommen aus eCH-0174 V1.0 wurde Kapitel 7 - Erweiterungen und Spezialfälle, da diese heute ohne praktische Bedeutung sind.

Anhang E – Abbildungsverzeichnis

Abbildung 1: Einordnung des Standards eCH-0174 v2.0.0 7

Abbildung 2: Interaktion der SAML-Services bei einem Authentication Request (mit und ohne Attributabfrage) 12

Abbildung 3: Interaktion der SAML-Services bei einem Authentication Request mit AttributeQuery 12

Abbildung 4: Übersicht der Signierung der Messages zwischen den Schnittstellen..... 13

Abbildung 5: Authentifizierungs-Protokoll ohne Attributübermittlung 15

Abbildung 6: Authentifizierungs-Protokoll mit Attributübermittlung durch AttributeConsumingServiceIndex 17

Abbildung 7: Authentifizierungs-Protokoll mit Attributübermittlung durch Attribute-Query..... 20

Abbildung 8: Übersicht der Schnittstellen zur Authentifizierung..... 29

Abbildung 9: Übersicht der Assertion-Übermittlung bei Double-Blinding 30

Abbildung 10: Übersicht der Assertion-Übermittlung bei Offene Quellen durch Signaturübermittlung 30

Abbildung 11: Übersicht der Schnittstellen von der RP 31

Abbildung 12: Übersicht der Schnittstellen vom Vermittler 37

Abbildung 13: Übersicht der Schnittstellen vom Identity & Attribute Provider 50

Abbildung 14: Erfassen der Meta-Informationen beim Vermittler..... 57

Abbildung 15: Publizierung der SAML-Metadaten..... 59

Anhang F – Verzeichnis der Listings

Listing 1: Beispiel einer SAML Response (Success) 27

Listing 2: Authentifizierungsanfrage von der RP zum Vermittler 32

Listing 3: Authentifizierungsbestätigung vom Vermittler zur RP..... 33

Listing 4: Authentifizierungs- & Attributanfrage von der RP zum Vermittler 34

Listing 5: Authentication Assertion mit AuthenticatingAuthority-Attribut (Offene Quellen)..... 35

Listing 6: Authentifizierungs- und Attributbestätigung vom Vermittler zur RP (Double-Blinding Model) 36
Listing 7: Authentifizierungsanfrage von der RP zum Vermittler 38
Listing 8: Authentifizierungsanfrage vom Vermittler zum IdP 39
Listing 9: Authentifizierungsbestätigung vom IdP zum Vermittler 40
Listing 10: Authentifizierungsbestätigung vom Vermittler zur RP 41
Listing 11: Authentifizierungsanfrage mit AttributeConsumingServiceIndex vom RP zum Vermittler 42
Listing 12: Authentifizierungs- & Attributbestätigung vom IdP/AP zum Vermittler 43
Listing 13: Authentifizierungsbestätigung mit AuthenticatingAuthority (Offene Quellen) 44
Listing 14: Authentifizierungs- & Attributbestätigung vom Vermittler zur RP (Double Blinding)45
Listing 15: Attributanfrage vom Vermittler zum IdP/AP 47
Listing 16: Attributbestätigung vom IdP/AP zum Vermittler 48
Listing 17: Authentifizierungsanfrage vom Vermittler zum IdP/AP 51
Listing 18: Authentifizierungsbestätigung vom IdP/AP zum Vermittler 52
Listing 19: Authentifizierungs- und Attributbestätigung vom IdP/AP zum Vermittler 54
Listing 20: Attributanfrage vom Vermittler zum IdP/AP 55
Listing 21: Attributbestätigung vom IdP/AP zum Vermittler 56
Listing 22: SAML-Metadaten-Datei 60
Listing 23: Beispiel eines Vermittler EntityDescriptors 62
Listing 24: Beispiel eines IdP/AP EntityDescriptor 64

Anhang G – Tabellenverzeichnis

Tabelle 1: Präfixe und referenzierte XML-Namensräume 5
Tabelle 2: Zuordnung von Komponenten zu SAML-Services 11
Tabelle 3: Referenz-Tabelle zum Authentifizierungs-Protokoll ohne Attributübermittlung 16

Tabelle 4: Referenz-Tabelle zum Authentifizierungs-Protokoll mit Attributübermittlung durch AttributeConsumingServiceindex 19

Tabelle 5: Referenz-Tabelle zum Authentifizierungs-Protokoll mit Attributübermittlung durch Attribute Query 22

Tabelle 6: Kapitelübersicht der Schnittstellen der RP 31

Tabelle 7: Kapitelübersicht der Schnittstellen des Vermittlers 37

Tabelle 8: Kapitelübersicht der Schnittstellen des IdP/APs 50

Tabelle 9 Änderungen gegenüber Vorversion 70