Dokumentation

Anonymous Credentials – Claim-based authentication

Version 1.0, 04.12.2013

Bernd Zwattendorfer – bernd.zwattendorfer@egiz.gv.at

Zusammenfassung: Anonymous Credentials vermeiden einerseits die Verkettung von unterschiedlichen Authentifizierungsprozessen einer Bürgerin bzw. eines Bürgers, andererseits ermöglichen sie die Offenlegung nur von Teilen einer Identität, ohne die gesamte Identität einer Bürgerin bzw. eines Bürgers zu offenbaren. Dies ist vor allem in datenschutzrechtlicher Hinsicht interessant, und somit auch für einen Einsatz im E-Government. In diesem Projekt wird eine konzeptionelle Architektur vorgestellt, wie Anonymous Credentials im Rahmen einer Bürgerinnen- bzw. Bürger-Authentifizierung Verwendung finden könnten. Zusätzlich werden für eine mögliche Implementierung taugliche Technologien vorgestellt sowie die Architektur anhand unterschiedlicher Kriterien evaluiert.

E-Government Innovationszentrum
Inffeldgasse 16/a, A-8010 Graz
Tel. +43 316 873 5514
Fax. +43 316 873 5520
E-Mail post@egiz.gv.at
www.egiz.gv.at

Das E-Government Innovationszentrum ist eine gemeinsame Einrichtung des Bundeskanzleramtes und der TU-Graz

BUNDESKANZLERAMT ÖSTERREICH

TU Graz
Graz University of Technology

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Die eindeutige Identifizierung und sichere Authentifizierung von Bürgerinnen bzw. Bürgern spielt eine wichtige Rolle im österreichischen e-Government. Die Identifizierung wird dabei über die Personenbindung erreicht, eine von der Stammzahlregisterbehörde signierte und somit authentische Datenstruktur, die persönliche Daten der Bürgerin bzw. des Bürgers enthält. Zu den Daten, die in der Personenbindung gespeichert sind, zählen die Stammzahl, Vor- und Nachname, Geburtsdatum, und der öffentliche Schlüssel des Schlüsselpaars auf der Bürgerkarte zum Erstellen von qualifizierten Signaturen. Die qualifizierte Signatur dient auch zur Authentifizierung von Bürgerinnen bzw. Bürgern in e-Government Prozessen bzw. bei Online Applikationen. Den Prozess der Identifizierung und Authentifizierung bei Online Applikationen übernimmt üblicherweise das Open Source-Modul MOA-ID.

Obwohl die Personenbindung aufgrund der Stammzahl eine eindeutige Identifizierung der Bürgerin bzw. des Bürgers zulässt, hat die Struktur der Personenbindung gewisse Nachteile. Egal bei welcher Online Applikation sich eine Bürgerin bzw. ein Bürger anmeldet, es müssen immer die komplette Personenbindung und somit alle persönlichen Daten an die Online Applikation bzw. MOA-ID übertragen werden. Bei einigen Applikationen ist dies jedoch nicht notwendig bzw. möchte vielleicht eine Bürgerin bzw. ein Bürger nicht alle persönlichen Daten Preis gegeben. So wäre es beispielsweise denkbar, dass bei behördlichen Meinungsumfragen oder Petitionen nur Personen eines bestimmten Alters (z.B. Personen ab 60) abstimmberechtigt sind. In diesem Fall wäre es vollkommen ausreichend, nur die Information „älter über 60“ an die Online Applikation zu übertragen, nicht jedoch das gesamte Geburtsdatum einer Bürgerin bzw. eines Bürgers. Der Vorgang so einer Authentifizierung wird als claim-basierte Authentifizierung bezeichnet. Sogenannte Anonymous Credentials sind speziell für die Realisierung claim-basierter Authentifizierung ausgelegt.

In diesem Projekt wurde deshalb untersucht, inwiefern Anonymous Credentials für eine Identifizierung und Authentifizierung im österreichischen E-Government geeignet sind. Ziel dabei ist, dass Bürgerinnen und Bürger einerseits nur wirklich benötigte Attribute an die Online Applikation übertragen müssen, und andererseits selbst wählen bzw. bestimmen können, welche Attribute an eine Online Applikation übertragen werden. Abschnitt 2 stellt unterschiedliche Anonymous Credentials Systeme vor. Abschnitt 3 konzipiert eine Architektur für einen Einsatz zur Identifizierung und Authentifizierung von Bürgerinnen bzw. Bürgern. Diese Architektur wird anschließend anhand unterschiedlicher Kriterien in Abschnitt 4 evaluiert. Das Projekt wird abschließend in Abschnitt 5 zusammengefasst.

2 Anonymous Credentials (AC)

Anonymous Credential Systems erlauben die Authentifizierung nur auf Basis von anonymen Attributen (Credentials), sprich die komplette Identität einer Person muss nicht Preis gegeben werden. Anonymous Credentials erlauben z.B. nur die Bekanntgabe des Alters als authentisches Attribut, ohne dabei das Geburtsdatum offenzulegen. Prinzipiell kann zwischen One-Show und Multi-Show Anonymous Credential Systemen unterschieden werden. Bei One-Show Systemen wird immer der gleiche mathematische Wert für ein Attribut offengelegt, Personen sind daher trotzdem linkbar. Bei Multi-Show Systemen wird bei jeder Offenlegung eines Attributs ein anderer mathematischer Wert erzeugt, sodass die Linkbarkeit einer Person verhindert werden kann. Im Folgenden werden die bekanntesten Anonymous Credentials Systeme vorgestellt.

2.1 U-Prove

U-Prove [1] ist eine von Stefan Brands [Brands00] entwickelte und von Microsoft übernommene Technologie. [Paquin13] beschreibt U-Prove als eine innovative Technologie, die es Benutzerinnen bzw. Benutzern erlaubt, nur minimale – aber von einer vertrauenswürdigen Entität – zertifizierte Attribute bei Interaktion mit Online Service Providern zu verwenden. Die zentrale Einheit von U-Prove ist ein sogenanntes U-Prove Token, welches authentische und kryptographisch geschützte Attribute enthält. Dieses U-Prove Token wird bei Interaktion mit einem Service Provider zum Nachweis von gewissen Attributen verwendet [Paquin13a]. Das Token und dessen Attribute werden dabei vom Service Provider verifiziert. U-Prove Tokens werden üblicherweise von einem sogenannten Issuer für eine Benutzerin bzw. einen Benutzer ausgestellt. Der Issuer überprüft dabei zuvor die Echtheit der Attribute, bevor sie in ein Token gespeichert werden.

Der Widerruf von ausgestellten Tokens erfolgt über Blacklists. In das Token wird üblicherweise ein eindeutiger Identifikator kodiert, welcher bei Widerruf auf diese Blacklists gesetzt wird. U-Prove Tokens können entweder von der Benutzerin bzw. vom Benutzer selbst widerrufen werden, oder beispielsweise wenn ein Service Provider aufhört, dieses U-Prove Token zu akzeptieren.

Die wesentlichen Eigenschaften von U-Prove sind Unlinkbarkeit sowie die gezielte Offenlegung von Attributen. Unlinkbarkeit heißt in diesem Fall, dass kein Zusammenhang zwischen unterschiedlichen U-Prove Tokens, die derselben Benutzerin

[1] http://research.microsoft.com/en-us/projects/u-prove/

bzw. demselben Benutzer zugeordnet sind, feststellbar sind. Nichtsdestotrotz sind Benutzerinnen bzw. Benutzer mit ein und denselben Token linkbar, da immer nur der gleiche mathematische Wert für ein Attribut offengelegt wird (One-Show System). Bei der gezielten Offenlegung von Attributen ist es Benutzerinnen und Benutzern möglich, selbst festzulegen, welche Attribute einem Service Provider veröffentlicht werden und welche nicht.

2.2 Idemix

Identity Mixer[2] (Idemix) ist ein von IBM entwickeltes Anonymous Credential System. Ähnlich wie bei U-Prove erhält hier eine Benutzerin bzw. ein Benutzer ein Credential von einem Issuer, der damit der Benutzerin bzw. dem Benutzer bestimmte Attribute attestiert. Wird eines dieser Attribute als Nachweis bei einem Service Provider benötigt, so wird vom Benutzer das vom Issuer ausgestellte Credential in ein neues Credential transformiert, welches jedoch nur eine bestimmte und vom Service Provider nötige Untermenge an Attributen enthält. Dabei kann die Benutzerin bzw. der Benutzer den Service Provider überzeugen, dass sie bzw. er bestimmte Attribute besitzt oder Eigenschaften erfüllt, ohne vollständige Informationen Preis zu geben. Im Gegensatz zu U-Prove kann eine Transformation beliebig oft erfolgen, und die Benutzerin bzw. der Benutzer bleibt trotzdem unlinkbar (Multi-Show System).

Der Widerruf erfolgt bei Idemix im Gegensatz zu U-Prove zumeist auf Basis von Whitelists. Wenn also ein Benutzerin bzw. ein Benutzer nachweisen muss, dass ihr bzw. sein sein Credential nicht widerrufen wurde, so muss er einfach nachweisen, dass ein bestimmter Identifikator des Credentials auf einer Whitelist steht. Es gibt jedoch noch einige andere Möglichkeiten für Widerrufsmechanismen in Idemix (auch Blacklists). Einen guten Überblick dazu gibt [LKD+11].

2.3 ABC4Trust

ABC4Trust[3] ist ein von der EU finanziertes Projekt, welches als Ziel die Entwicklung und Pilotierung eines Frameworks hat, das unterschiedliche Anonymous Credential Systeme miteinander vereint. Derzeit werden vom ABC4Trust-Framework U-Prove und Idemix unterstützt. Die folgende Abbildung 1 zeigt die allgemeine Architektur des ABC4Trust-Frameworks und die Interaktionen der einzelnen involvierten Entitäten [CKL+12].

[2] http://idemix.wordpress.com/
[3] https://abc4trust.eu/

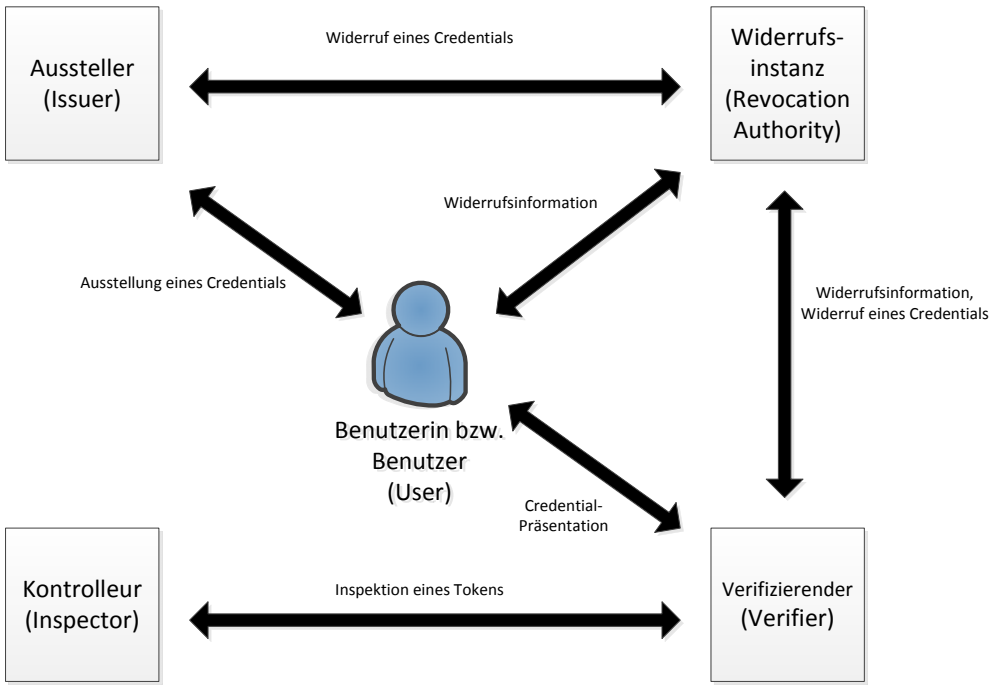

Abbildung 1 - Architektur des ABC4Trust-Frameworks [CKL+12]

Im Folgenden werden nun die einzelnen Entitäten und deren Funktionen genauer beschrieben [CKL+12]:

Benutzerin bzw. Benutzer:

Eine Benutzerin bzw. ein Benutzer kann mehrere Credentials von unterschiedlichen Issuern ausgestellt bekommen. Diese Credentials bzw. eine Transformation oder Subset dieser Credentials können dann einem oder mehreren Verifizierenden präsentiert werden. Die Benutzerin bzw. der Benutzer kann dabei selektieren, welche Informationen präsentiert werden und welche nicht. Die Benutzerin bzw. der Benutzer hat auch die Möglichkeit mit der Widerrufsinstanz zu kommunizieren, um Informationen über die Gültigkeit ihres bzw. seines Credentials zu erhalten.

Aussteller:

Der Aussteller oder Issuer übergibt Benutzerinnen bzw. Benutzern entsprechende Credentials. Vor Ausstellung muss der Issuer jedoch die Korrektheit der Attribute bzw. Informationen, die im Credential enthalten sein sollen, überprüfen. Dies benötigt in den meisten Fällen eine Identifizierung und Authentifizierung der Benutzerin bzw. des Benutzers. Der Issuer kommuniziert auch mit der Widerrufsinstanz bezüglich des Widerrufs eines Credentials.

Verifizierender:

Ein Verifizierender regelt üblicherweise den Zugriff auf geschützte Ressourcen und benötigt für einen Zugriff von einer Benutzerin bzw. einem Benutzer bestimmte Informationen. Der Verifizierende beschreibt die Richtlinien für einen Zugriff in der sogenannten „Presentation Policy“. Die Benutzerin bzw. der Benutzer generiert ein sogenanntes „Presentation Token“ aus ihrem bzw. seinem Credentials, das alle notwendigen Informationen sowie kryptographischen Beweise gemäß der Presentation Policy beinhaltet. Ein Verifizierender kommuniziert auch mit der Widerrufsinstanz, entweder zum Widerruf eines Credentials oder um Widerrufsinformationen abzurufen.

Widerrufsinstanz:

Die Widerrufsinstanz ist verantwortlich um Credentials zu widerrufen, damit diese nicht mehr länger gültig sind und nicht mehr zur Erstellung eines Presentation Tokens verwendet werden können. Benutzerinnen bzw. Benutzer aber auch Verifizierende müssen immer die aktuellen Widerrufsinformationen der Widerrufsinstanz abfragen, um Presentation Token genieren bzw. überprüfen zu können.

Kontrolleur:

Ein Kontrolleur oder Inspector ist eine vertrauenswürdige Kontrollinstanz, die unter bestimmten Umständen ein Presentation Token de-anonymisieren kann. Um dies zu ermöglichen, muss ein Verifizierender bereits in der Presentation Policy festlegen, welche Attribute von welchem Kontrolleur und unter welchen Umständen inspiziert werden können. Der Benutzerin bzw. dem Benutzer ist daher von Anfang an bewusst, dass unter gewissen Umständen eine Kontrollinstanz seine Attribute einsehen kann.

In dem Architekturbild in Abbildung 1 sind die einzelnen Entitäten jeweils getrennt dargestellt, es kann jedoch eine Entität auch mehrere Funktionen übernehmen. So kann beispielsweise die Rolle des Ausstellers mit den Rollen der Widerrufsinstanz und des Kontrolleurs zusammenfallen.

3 Architektur und Konzept

Dieser Abschnitt beschreibt im Wesentlichen ein architektonisches Konzept, wie Anonymous Credential Systeme auch im österreichischen E-Government eingesetzt werden könnten. Hauptaspekt ist dabei, dass Bürgerinnen bzw. Bürgern die Möglichkeit geboten wird, nicht alle Identitätsdaten sondern nur Teile davon bei Online Applikationen Preis zu geben. Um dies realisieren zu können, werden die Attribute, die derzeit auf der Personenbindung gespeichert sind, als Credential modelliert. Weiters wird davon ausgegangen, dass wiederum MOA-ID die Identifizierung und Authentifizierung von Bürgerinnen und Bürgern an Online Applikationen übernimmt.

3.1 Architektur

Abbildung 2 zeigt die generelle Architektur für die Realisierung einer Bürgerinnen- bzw. Bürger-Authentifizierung unter Verwendung von Anonymous Credentials.

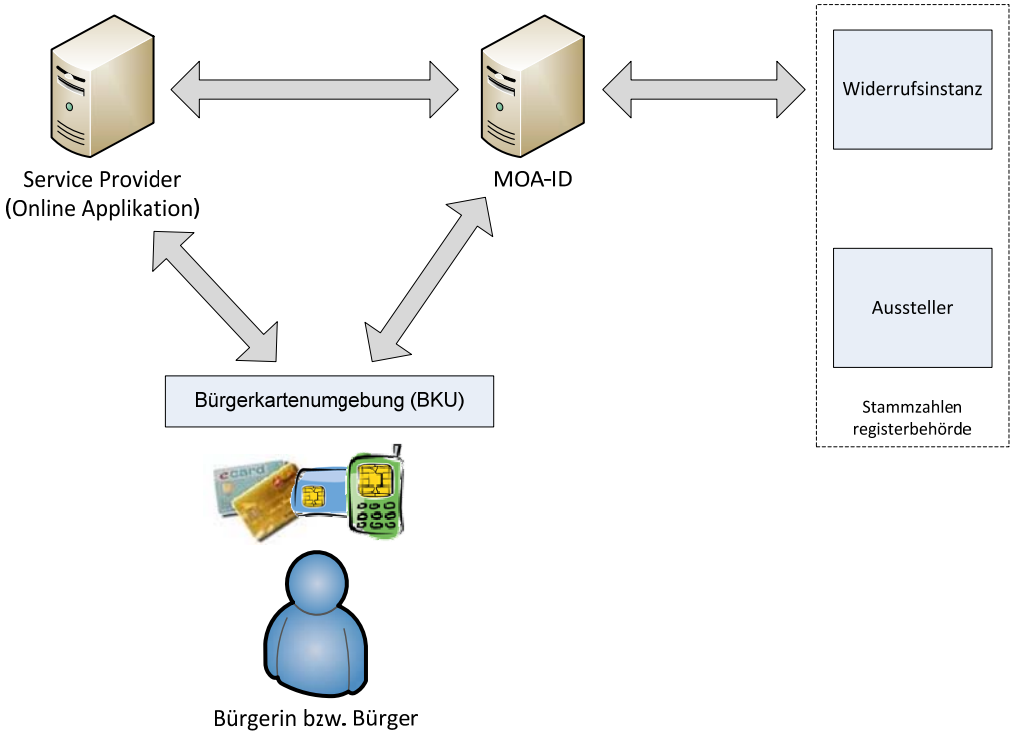

Abbildung 2 - Generelle Architektur

Die in Abbildung 2 dargestellte Architektur entspricht im Wesentlichen der bisherigen Architektur unter Verwendung von MOA-ID zur Identifizierung und Authentifizierung von Bürgerinnen und Bürgern. Einziger Unterschied ist, dass anstatt der bisher verwendeten Technologien Anonymous Credentials eingesetzt werden. Kurz zusammengefasst wird folgender Anwendungsfall damit abgebildet.

Eine Bürgerin bzw. ein Bürger möchte sich mit ihrer bzw. seiner Bürgerkarte bei einer Online Applikation anmelden. Sie bzw. er möchte aber nicht seine kompletten Identitätsdaten offenlegen, sondern nur eine Untermenge der Daten bei der Anmeldung Preis geben. Die Bürgerkarte unterstützt diese Funktion, da sie mit Anonymous Credentials modelliert und dementsprechend so von der Stammzahlenregisterbehörde ausgestellt wurde. Um zu überprüfen ob die für eine Anmeldung notwendigen Credentials noch gültig sind, wird die Bürgerin bzw. der Bürger von der Online Applikation an MOA-ID weitergeleitet. MOA-ID kontaktiert die Widerrufsinstanz und überprüft, ob die präsentierten Credentials nicht widerrufen wurden. Diese Widerrufsinformation wird zurück an die Online Applikation übermittelt. Nachdem angenommen wird, dass die Credentials gültig sind, können Online Applikation und Bürgerin bzw. Bürger insofern interagieren, dass die Bürgerin bzw. der Bürger der Online Applikation entsprechende Credentials über die gewünschten Attribute liefert.

Die einzelnen in diesem Anwendungsfall beteiligten Entitäten werden nun etwas genauer beschrieben.

Bürgerin bzw. Bürger:

Eine Bürgerin bzw. ein Bürger möchte sich wie gewohnt mit ihrer bzw. seiner Bürgerkarte bei einer Online Applikation anmelden. Die Attribute der Bürgerkarte sind in diesem Fall als Anonymous Credential modelliert.

Online Applikation:

Die Online Applikation ist eine behördliche Anwendung, für deren Zugriff authentische Attribute benötigt werden. Die Online Applikation benötigt jedoch nur eine bestimmte Menge von Attributen, beispielsweise nur das Alter der Bürgerin bzw. des Bürgers.

MOA-ID:

An MOA-ID werden wie bisher Funktionen zur Identifizierung und Authentifizierung von der Online Applikation ausgelagert. In diesem Fall übernimmt MOA-ID speziell die Überprüfung von Widerrufsinformationen.

Widerrufsinstanz:

Die Widerrufsinstanz hat eine Blacklist gespeichert, die angibt, welche Credentials widerrufen sind. Sie wird von der Stammzahlenregisterbehörde betrieben.

Aussteller:

Der Aussteller ist auch die Stammzahlenregisterbehörde. Diese stellt Bürgerinnen und Bürgern Bürgerkarten auf Basis von Anonymous Credentials aus.

Bürgerkartenumgebung:

Die Bürgerkartenumgebung regelt den Zugriff auf Credentials bzw. die Transformation von Credentials auf der Bürgerkarte.

3.2 Verwendete Technologien

Um diese vorgestellte Architektur umsetzen zu können, ist die Verwendung folgender Technologien denkbar.

3.2.1 Idemix

Idemix wurde bereits in Abschnitt 2.2 vorgestellt. Idemix wurde als Anonymous Credential System ausgewählt, da es von ABC4Trust unterstützt, aktuelle Java Implementierungen vorhanden sind, und da es ein Multi-Show System ist. Im Rahmen einer Implementierung sollte somit Idemix zur Modellierung von Bürgerkarten-Attributen verwendet werden. Somit wird Idemix in der Bürgerkartenumgebung und der Bürgerkarte selbst verwendet. Abbildung 3 illustriert die Komponenten, bei denen Idemix zur Anwendung kommt.

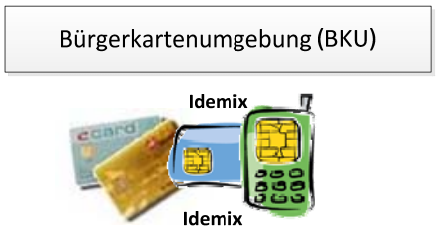

Abbildung 3 - Komponenten, die Idemix verwenden

Idemix unterstützt unterschiedliche Ansätze zur Widerrufsprüfung. In diesem konkreten Konzept wird Verifiable Encryption (VE) in Zusammenhang mit Blacklists verwendet. Verifiable Encryption bedeutet, dass z.B. eine Bürgerin bzw. ein Bürger eine Eigenschaft einer Nachricht nachweisen kann, obwohl die Nachricht in verschlüsselter Form vorliegt. Im Rahmen dieses Konzept wird ein eindeutiger Identifikator des Credentials verschlüsselt. Eine Bürgerin bzw. ein Bürger kann dann nachweisen, dass der verschlüsselte Wert korrekt ist, ohne jedoch den Identifikator offenlegen zu müssen.

3.2.2 ABC4Trust

ABC4Trust wurde ebenfalls bereits in Abschnitt 2.3 vorgestellt. ABC4Trust wird speziell für das Protokoll für den Datenaustausch zwischen Online Applikation und Bürgerkartenumgebung, und MOA-ID und Bürgerkartenumgebung verwendet. Dabei werden jeweils zwischen diesen beiden Entitäten eine Presentation Policy und ein Presentation Token ausgetauscht. Die Presentation Policy gibt dabei an, welche Credentials bzw. Attribute von der Bürgerkarte benötigt werden. Die Bürgerkartenumgebung berechnet bzw. transformiert dann die entsprechenden Credentials und Attribute und liefert diese in Form eines Presentation Tokens an die anfragende Entität zurück. Abbildung 4 illustriert die Komponenten, bei denen ABC4Trust zur Anwendung kommt.

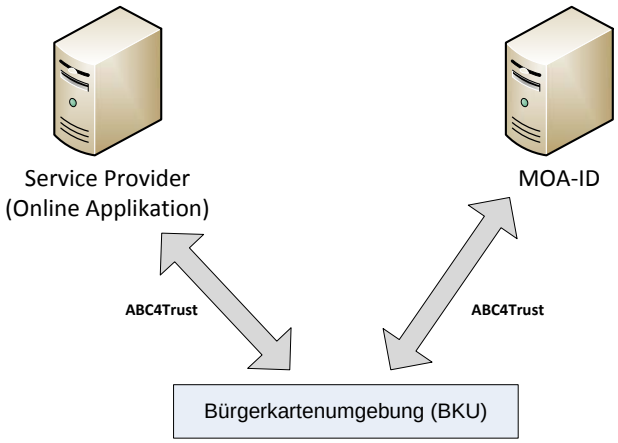

Abbildung 4 - Komponenten, die ABC4Trust verwenden

3.2.3 SAML

SAML [4] (Security Assertion Markup Language) ist eine XML-basierte Auszeichnungssprache, die speziell für den sicheren Austausch von Identitäts- und Authentifizierungsdaten entwickelt wurde. Die derzeitige MOA-ID Implementierung verwendet auch SAML für den Austausch von Daten der Bürgerin bzw. des Bürgers zwischen MOA-ID und der Online Applikation. Auch in dieser konzeptionellen Architektur wird SAML für den Austausch von Daten zwischen diesen beiden Komponenten verwendet. Im Speziellen werden Widerrufsinformationen ausgetauscht. Abbildung 5 illustriert die Schnittstelle, wo SAML zum Einsatz kommt.

[4] http://saml.xml.org

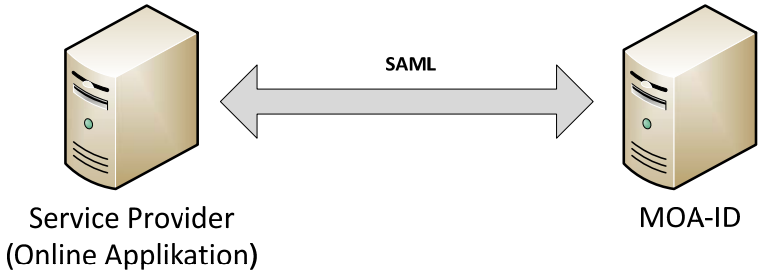

Abbildung 5 - Komponenten, die SAML verwenden

3.2.4 SOAP

SOAP[5] ist ein auf XML-basiertes Protokoll für den simplen Austausch von Daten bzw. Nachrichten zwischen Systemen im Rahmen von Web Services. SOAP-Nachrichten können beliebige XML-Nachrichten für den Austausch beinhalten. Im Rahmen dieser Architektur wird die Widerrufsprüfung (die Kommunikation zwischen MOA-ID und der Widerrufsinstanz) als Web Service abgebildet. Abbildung 6 illustriert die Schnittstelle, wo SOAP zum Einsatz kommt.

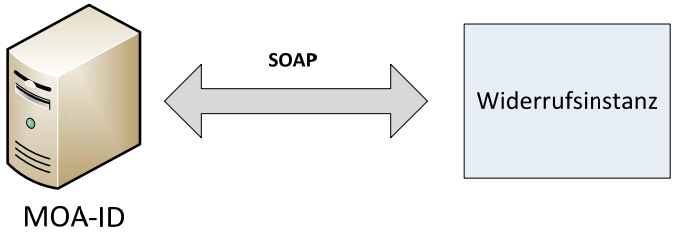

Abbildung 6 - Komponenten, die SOAP verwenden

3.3 Identifizierungs- und Authentifizierungsablauf

Dieser Unterabschnitt beschreibt einen Identifizierungs- und Authentifizierungsablauf unter Verwendung der zuvor vorgestellten Technologien. Die einzelnen Prozessschritte werden im Sequenz-Diagramm in Abbildung 7 dargestellt.

[5] http://www.w3.org/TR/soap/

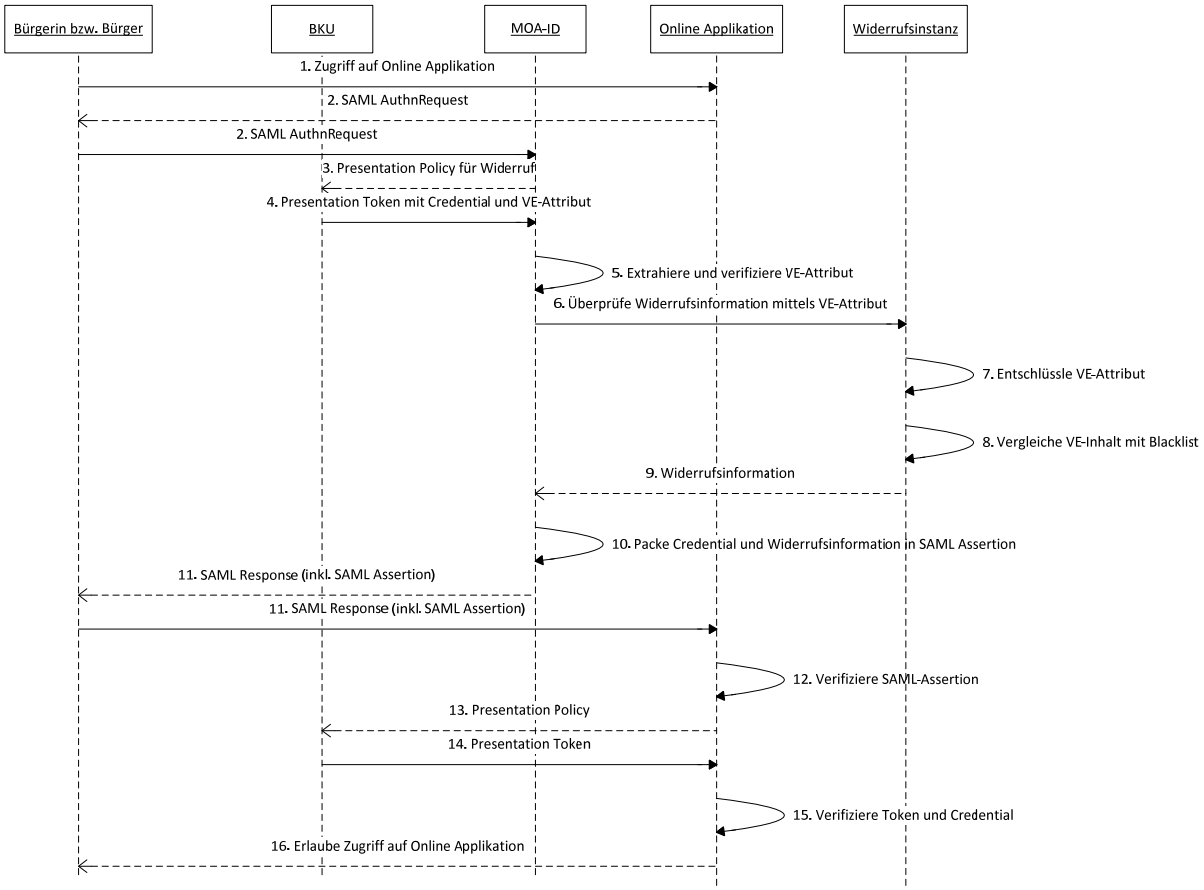

Abbildung 7 - Identifizierungs- und Authentifizierungsablauf unter Verwendung von Anonymous Credentials

1. Eine Bürgerin bzw. ein Bürger möchte auf eine geschützte Ressource einer Online Applikation zugreifen.
2. Nachdem die Bürgerin bzw. der Bürger noch nicht authentifiziert ist, wird diese bzw. dieser zur Authentifizierung an MOA-ID weitergeleitet. Die Online Applikation erstellt dazu einen SAML AuthnRequest.
3. MOA-ID verifiziert den SAML AuthnRequest und generiert eine Presentation Policy. Diese Presentation Policy enthält die Anfrage, dass die Bürgerin bzw. der Bürger nachweisen soll, dass seine Credentials nicht widerrufen sind. Die Presentation Policy wird von MOA-ID an die Bürgerkartenumgebung (BKU) gesandt.
4. Um zu beweisen, dass die Credentials der Bürgerin bzw. des Bürgers nicht widerrufen sind, wird Verifiable Encryption (VE) eingesetzt. Der eindeutige Identifikator des Credentials wird also von der Bürgerin bzw. vom Bürger verschlüsselt (VE-Attribut) und zusammen mit dem eigentlichen Credential in ein Presentation Token verpackt, welches anschließend an MOA-ID retourniert wird.

5. MOA-ID extrahiert das VE-Attribut aus dem Presentation Token und verifiziert das VE-Attribut. MOA-ID kann jedoch nur dessen Gültigkeit – genauer gesagt den von der Bürgerin bzw. Bürger erstellten Nachweis dafür – überprüfen aber nicht dessen Inhalt einsehen.
6. Zur Überprüfung, ob das mitgelieferte Credential gültig ist, wird das VE-Attribut via Web Service an die Widerrufsinstanz übermittelt.
7. Die Widerrufsinstanz entschlüsselt[6] das VE-Attribut und extrahiert den darin enthaltenen Identifikator.
8. Die Widerrufsinstanz überprüft, ob der Identifikator auf einer von der Widerrufsinstanz gewarteten Blacklist steht. Alle Identifikatoren von Credentials, die auf dieser Blacklist stehen, sind widerrufen.
9. Die Widerrufsinstanz retourniert als Web Service-Antwort die entsprechende Widerrufsinformation, im Wesentlichen nur die Information, ob das präsentierte Credential widerrufen ist oder nicht. In diesem Szenario wird weiters davon ausgegangen, dass das präsentierte Credential noch gültig ist.
10. MOA-ID packt das von der Bürgerin bzw. dem Bürger präsentierte Credential sowie die dazugehörige Widerrufsinformation in eine SAML Assertion. Die SAML Assertion bzw. die SAML Response wird von MOA-ID signiert.
11. MOA-ID übermittelt die SAML Response zurück an die Online Applikation.
12. Die Online Applikation verifiziert die SAML Assertion bzw. SAML Response.
13. Die Online Applikation sendet eine Presentation Policy an die BKU mit jenen gewünschten Werten, die für eine Authentifizierung benötigt werden. Dies kann z.B. nur das Alter der Bürgerin bzw. des Bürgers sein.
14. Die BKU erstellt die notwendigen Attribute und sendet diese gemeinsam mit dem Credential verpackt in einem Presentation Token an die Online Applikation.
15. Die Online Applikation verifiziert die präsentierten Attribute auf deren Gültigkeit. Zusätzlich wird überprüft, ob das in diesem Schritt präsentierte Credential und das bei MOA-ID zur Widerrufsprüfung präsentierte und von MOA-ID via SAML Assertion übermittelte Credential identisch ist.
16. Sind beide Überprüfungen erfolgreich, so kann die Online Applikation Zugriff auf die gewünschte Ressource gewähren.

[6] Das VE-Attribut kann von der Widerrufsinstanz entschlüsselt werden, da diese unter der Obhut der Stammzahlenregisterbehörde steht und die Stammzahlenregisterbehörde für die Ausstellung des Credentials verantwortlich war.

4 Evaluierung

In diesem Abschnitt wird das zuvor beschriebene Konzept anhand unterschiedlicher Kriterien evaluiert.

4.1.1 Wiederverwendung existierender Infrastruktur

Die Verwendung von Anonymous Credentials bedingt den vollständigen Austausch der Personenbindung, da hier eine komplett andere Technologie Verwendung findet. Bereichsspezifische Personenkennzeichen (bPKs) können entweder für alle staatlichen Tätigkeitsbereiche als Attribute im Credential modelliert, oder anhand von sogenannten Scope-Exclusive Pseudonyms [CKL+11] abgebildet werden. Zusätzlich müssen sowohl MOA-ID als auch die Online Applikation das Kommunikationsprotokoll von ABC4Trust unterstützen.

4.1.2 Konformität zum aktuellen Prozessfluss

Der beschriebene Prozessfluss im Vergleich zum aktuellen Identifizierungs- und Authentifizierungsprozessfluss unter Verwendung von MOA-ID ist etwas unterschiedlich. So überprüft MOA-ID im beschriebenen Fall nur, ob das präsentierte Credential widerrufen ist oder nicht. Die Verifikation der Gültigkeit der eigentlichen Attribute erfolgt direkt bei der Online Applikation und nicht wie bisher bei MOA-ID.

4.1.3 Skalierbarkeit

Die Widerrufsprüfung von Anonymous Credentials basierend auf Multi-Show Systemen ist sehr komplex und rechenintensiv. Speziell für eine große Anzahl an Benutzerinnen bzw. Benutzern - wie z.B. die österreichische Bevölkerung - ist der Einsatz nur bedingt geeignet. Generell würde sich eine Migration einzelner Komponenten (z.B. MOA-ID) in eine Cloud anbieten, da Engpässe in der Skalierbarkeit so leichter vermieden werden könnten.

4.1.4 Praktikabilität

Die Berechnung von Beweisen für bestimmte Attribute in Multi-Show Systemen ist sehr rechenintensiv. Nachdem diese Berechnungen in der Bürgerkartenumgebung der Bürgerin bzw. des Bürgers durchgeführt werden müssen, ist mit dementsprechend langen Wartezeiten inmitten des Authentifizierungsprozesses zu rechnen.

4.1.5 Erweiterbarkeit

Die Möglichkeit der Erweiterung hängt von der Modellierung der bPKs als Anonymous Credentials ab. Wird jedes bPK als eigenständiges Attribut modelliert, so muss bei Hinzukommen eines neuen staatlichen Sektors und somit bPKs der Bürgerin bzw. dem Bürger ein neues Credential ausgestellt werden. Wird hingegen auf den in [CKL+11]

beschriebenen Ansatz von Scope-Exclusive Pseudonyms gesetzt, so kann ein ähnliches sektor-spezifisches Modell wie bisher mit Stammzahl und daraus Ableitung der bPKs realisiert werden.

4.1.6 Änderungen in der BKU

Für den Einsatz von Anonymous Credentials muss die Funktionalität der BKU grundlegend geändert werden. So muss diese einerseits Anonymous Credentials unterstützen und andererseits das Kommunikationsprotokoll von ABC4Trust implementieren.

4.1.7 Vertrauen in MOA-ID

MOA-ID muss kein großes Vertrauen entgegen gebracht werden, da es nie persönliche Attribute der Bürgerin bzw. des Bürgers zu Gesicht bekommt. Es sieht nur das Credential der Bürgerin bzw. des Bürgers, jedoch nicht dessen Inhalt. MOA-ID könnte somit auch in einer Public Cloud deployed werden. Nichtsdestotrotz muss in diesem Fall überprüft bzw. festgestellt werden können, dass MOA-ID in der Cloud korrekt arbeitet.

5 Zusammenfassung und Fazit

Anonymous Credential Systeme sind im Wesentlichen dafür ausgelegt, eine Verkettung von unterschiedlichen Identifizierungs- und Authentifizierungsprozessen der ein und derselben Benutzerin bzw. des Benutzers zu vermeiden (Unlinkbarkeit). Zusätzlich ermöglichen sie nicht alle Identitätsdaten, sondern nur ein bestimmtes Subset von Attributen einer Bürgerin bzw. eines Bürgers, bei Anmeldungen bei einer Online Applikation offenzulegen. Diese Eigenschaft erhöht natürlich den Datenschutz für Bürgerinnen und Bürger.

Im Rahmen dieses Projekts wurde untersucht, inwiefern Anonymous Credentials auch für einen Einsatz im österreichischen E-Government geeignet sind. Zu diesem Zweck wurde ein Konzept und eine Architektur entwickelt, wie Anonymous Credentials zur Authentifizierung bei Online Applikationen herangezogen werden könnten. Für eine mögliche zukünftige Implementierung wurden bereits entsprechende Technologien ausgewählt, die Verwendung finden könnten. Die auf Basis dieser Technologien entwickelte Architektur wurde anschließend anhand unterschiedlicher Kriterien evaluiert.

In der Evaluierung hat sich gezeigt, dass eine Umsetzung der Architektur mit den derzeit vorhandenen technologischen Mitteln noch nicht praktikabel ist. Zu rechenintensiv sind Berechnungen rund um ein Credential, die alle in der Bürgerkartenumgebung der Bürgerin bzw. des Bürgers durchgeführt werden müssten. Nichtsdestotrotz sind Anonymous Credentials aufgrund deren Möglichkeiten zur Wahrung des Datenschutzes von Bürgerinnen und Bürgern ein Versprechen für die Zukunft für einen Einsatz im E-Government.

Dokumentenhistorie

Version	Datum	Autor(en)	Anmerkung
0.1	28.11.2013	Bernd Zwattendorfer	Dokumenterstellung
0.2	29.11.2013	Bernd Zwattendorfer	Kapitel 1 und 2
0.3	02.12.2013	Bernd Zwattendorfer	Kapitel 3 und 4
0.4	03.12.2013	Bernd Zwattendorfer	Finaler Draft
0.5	04.12.2013	Arne Tauber	Kommentare
1.0	04.12.2013	Bernd Zwattendorfer	Finale Version

Referenzen

[Brands00] Stefan Brands: *"Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy"*, 2000, http://www.credentica.com/the_mit_pressbook.html

[CKL+12] Jan Camenisch, Ioannis Krontiris, Anja Lehmann, Gregory Neven, Christian Paquin, Kai Rannenberg: "H2.1-ABC4Trust Architecture for Developers", ABC4Trust, 2012, https://abc4trust.eu/download/ABC4Trust-H2.1-Architecture-for-Developers.pdf

[CKL+11] Jan Camenisch, Ioannis Krontiris, Anja Lehmann, Gregory Neven, Christian Paquin, Kai Rannenberg, Harald Zwingelberg: "D2.1 Architecture for Attribute-based Credential Technologies – Version 1", 2011

[LKD+11] J. Lapon, M. Kohlweiss, B. De Decker und V. Naessens: „Analysis of Revocation Strategies for Anonymous Idemix Credentials", CMS 2011, 2011, pp. 3–17

[Paquin13] Christian Paquin: *"U-Prove Technology Overview V1.1"* - Revision 2, 2013, http://research.microsoft.com/pubs/166980/U-Prove%20Technology%20Overview%20V1.1%20Revision%202.pdf

[Paquin13a] Christian Paquin, *"U-Prove Cryptographic Specification V1.1"* - Revision 2, 2013, http://research.microsoft.com/pubs/166969/U-Prove%20Cryptographic%20Specification%20V1.1%20Revision%202.pdf