EGIZ

www.egiz.gv.at
E-Mail: post@egiz.gv.at
Telefon: ++43 (316) 873 5514
Fax: ++43 (316) 873 5520
Inffeldgasse 16a / 8010 Graz / Austria

Integration von MOA-ID in Online-Applikationen

Applikationsintegration

Version 1.1, 08. August 2012

Thomas Zefferer – thomas.zefferer@egiz.gv.at

Zusammenfassung: Dieses Dokument fasst die wichtigsten Aspekte einer Integration von MOA-ID in Online-Applikationen zusammen. Fokus wird dabei vor allem auf praxisbezogene Aspekte gelegt. Zum besseren Verständnis werden die einzelnen Schritte, die für eine Verwendung von MOA-ID im Rahmen von Online-Applikationen nötig sind, anhand konkreter Beispiele und Umsetzungsvorschläge illustriert.

Das vorliegende Dokument bietet dazu zunächst eine allgemeine Beschreibung eines Authentifizierungsvorgangs mit MOA-ID, zeigt die einzelnen Prozessschritte dieses Vorgangs und identifiziert die in den Authentifizierungsprozess involvierten Komponenten. Im Anschluss wird gezeigt, welche Vorkehrungen auf Seiten einer Online-Applikation getroffen werden müssen, um die von MOA-ID bereitgestellte Funktionalität nutzen zu können. Im Speziellen werden die Implementierung einer entsprechenden Bürgerkartenauswahl, nötige Schritte zum Aufruf von MOA-ID aus Online-Applikationen, oder auch die abschließende Übertragung der von MOA-ID ermittelten Authentifizierungsdaten an die Online-Applikation diskutiert.

Inhaltsverzeichnis:

Revision History

Version	Datum	Autor(en)	
0.1	02.08.2012	Thomas Zefferer	Initialversion
1.0	03.08.2012	Herbert Leitold	Interner Review
1.1	03.08.2012	Arne Tauber	Editorielle Änderungen

1 Einleitung

Im österreichischen E-Government spielen die MOA-Komponenten (Module für Online-Applikationen) eine zentrale Rolle. Diese implementieren häufig wiederkehrende Funktionen und ermöglichen damit eine einfache Integration dieser Funktionen in Online-Applikationen. Für die sichere bürgerkartenbasierte Authentifizierung von Benutzerinnen und Benutzern kommt die Komponente MOA-ID zur Anwendung. Diese Komponente implementiert eine vollständige sichere Authentifizierung von Benutzerinnen und Benutzern und ermöglicht Online-Applikationen einen authentifizierten Zugriff auf Ressourcen durchzusetzen. In diesem Dokument soll die Integration von MOA-ID in Java-basierte Online-Applikationen näher erläutert und anhand konkreter Beispiele illustriert werden.

Abbildung 1 zeigt den typischen Ablauf einer MOA-ID-basierten Anmeldung an einer Online-Applikation. In den Anmeldevorgang sind dabei grundsätzlich folgende Komponenten involviert:

- Online-Applikation: Dabei handelt es sich um eine serverseitige Web-Applikation, die für den Zugriff auf bestimmte Ressourcen (Web-Seiten, etc.) eine sichere Authentifizierung von Benutzerinnen und Benutzern voraussetzt.
- Browser: Der Zugriff auf die Web-Applikation erfolgt über einen Web-Browser.
- MOA-ID: Diese Komponenten implementiert den Authentifizierungsprozess und stellt der Online-Applikation nach erfolgter Authentifizierung entsprechende Authentifizierungsdaten zur Verfügung, anhand derer die Online-Applikation die Benutzerin bzw. den Benutzer eindeutig identifizieren kann.
- Bürgerkartenumgebung: Die Bürgerkartenumgebung (BKU) implementiert die SecurityLayer-Schnittstelle und bietet damit Zugriff auf die Bürgerkarte der Benutzerin bzw. des Benutzers.

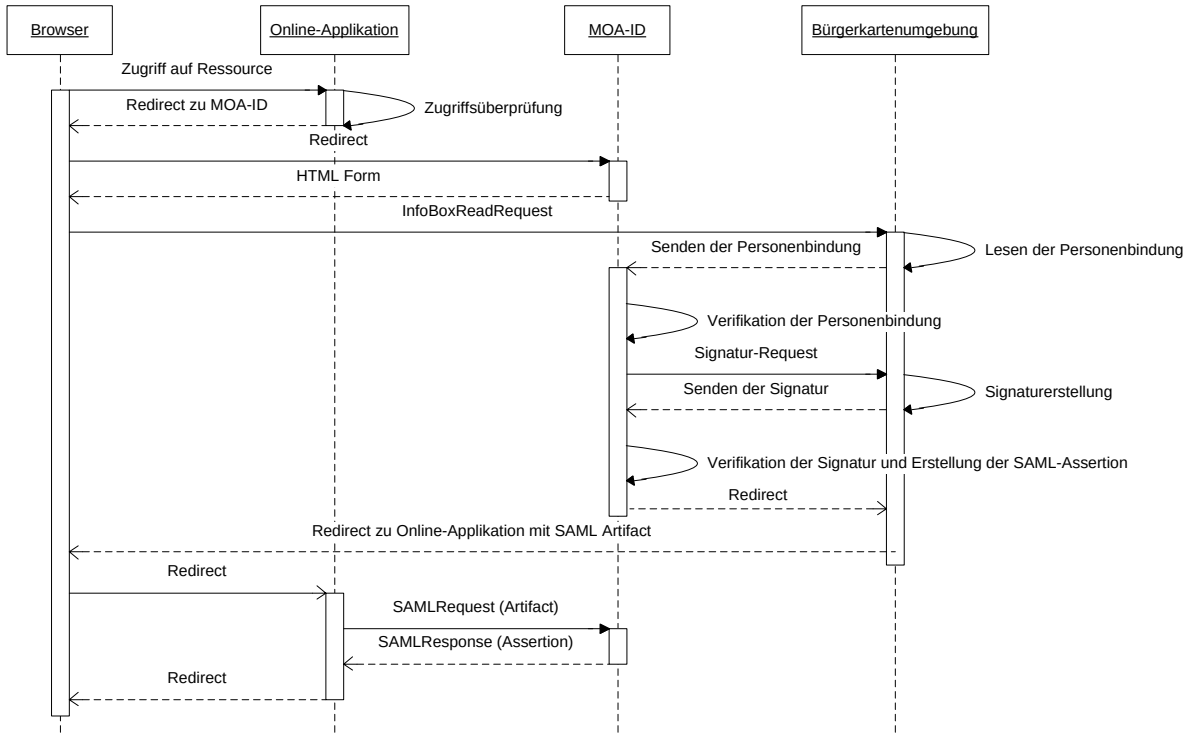

Abbildung 1. Ablauf einer MOA-ID basierten Anmeldung an einer Online-Applikation.

Eine Anmeldung an der Online-Applikation über MOA-ID gliedert sich grundsätzlich in folgende Schritte:

1) Die Benutzerin bzw. der Benutzer fordert über den Browser Zugriff auf eine Ressource der Online-Applikation an.
2) Die Online-Applikation überprüft, ob ein Zugriff auf die angeforderte Ressource nur für authentifizierte Benutzerinnen und Benutzer vorgesehen ist.
3) Ist eine Authentifizierung vorgesehen, wird die Benutzerin bzw. der Benutzer auf eine entsprechende Anmeldeseite der Online-Applikation weitergeleitet.
4) Über einen entsprechenden HTTP-POST-Request wird die Authentifizierungskomponente MOA-ID aufgerufen.
5) MOA-ID schickt in der Antwort auf diesen Request einen InfoBoxReadRequest gemäß SecurityLayer-Spezifikation zum Lesen der Personenbindung an den Browser.
6) Dieser Request wird im Anschluss vom Browser an die Bürgerkartenumgebung gesendet.
7) Die Bürgerkartenumgebung verarbeitet den erhaltenen Request und liest die Personenbindung von der Bürgerkarte der Benutzerin bzw. des Benutzers aus.
8) Die Personenbindung wird über die DataURL (siehe SecurityLayer-Spezifikation) an MOA-ID übertragen.
9) Die Signatur der Personenbindung wird von MOA-ID verifiziert.
10) MOA-ID sendet als Antwort auf die Personenbindung einen Signatur-Request über die offene DataURL-Verbindung als Antwort an die Bürgerkartenumgebung.
11) Die Bürgerkartenumgebung verarbeitet den Request und veranlasst die Signaturerstellung durch die Bürgerkarte der Benutzerin bzw. des Benutzers.
12) Die erstellte Signatur wird über die DataURL an MOA-ID übertragen.
13) MOA-ID verifiziert die erhaltene Signatur und erstellt eine SAML-Assertion, die relevante Authentifizierungsdaten enthält.
14) Über die Bürgerkartenumgebung wird die Benutzerin bzw. der Benutzer zurück zur Online-Applikation weitergeleitet (Redirect). Der Redirect enthält ein eindeutiges SAML-Artifact, über das die SAML-Assertion innerhalb einer gewissen Zeit bei MOA-ID abgeholt werden kann.
15) Die Online-Applikation extrahiert das SAML-Artifact und holt damit die SAML-Assertion von MOA-ID ab.
16) Auf Basis der Authentifizierungsinformation in der SAML Assertion gewährt bzw. verweigert die Applikation der Benutzerin bzw. dem Benutzer den Zugriff auf die geschützte Ressource.

Obwohl der gesamte Authentifizierungsprozess einigermaßen komplex erscheint, gestaltet sich eine Integration von MOA-ID in eine Web-Applikation relativ einfach. Der größte Teil der Funktionalität (Kommunikation mit Bürgerkartenumgebung, etc.) wird ausschließlich von MOA-ID implementiert und muss bei einer Integration in Web-Applikationen nicht näher betrachtet werden.

Die folgenden Abschnitte beschreiben den o.g. Authentifizierungsprozess aus Sicht der Online-Applikation. Anhand einer konkreten Java-basierten Web-Applikation wird dabei eine typische Integration von MOA-ID illustriert.

2 Auswahl der Bürgerkartenumgebung

Als ersten Schritt im Rahmen einer MOA-ID basierten Authentifizierung von Benutzerinnen und Benutzern muss die Online-Applikation eine Auswahlseite anbieten, über die Benutzerinnen und Benutzer die von ihnen präferierte Bürgerkartenausprägung auswählen können. Derzeit stehen hierfür die Alternativen „Chipkarte“ und „Handy-Signatur“ zur Verfügung. Bei einer Verwendung von Chipkarten können Benutzerinnen und Benutzer außerdem zwischen der Verwendung einer lokal installierten Bürgerkartenumgebung oder eines Java-Applet-basierten Ansatzes wählen.

MOA-ID unterstützt Applikationsbetreiber bei der Integration einer entsprechenden Auswahlseite. So enthält MOA-ID ein Template in Form einer HTML-Datei, das als Auswahlseite in Online-Applikationen integriert werden kann. Abbildung 2 zeigt das von MOA-ID bereitgestellte Template. Dieses kann einfach entsprechend den Bedürfnissen und des Layouts der Online-Applikation angepasst werden. Die Dokumentation zur Anpassung dieses Templates befindet sich unter [5].

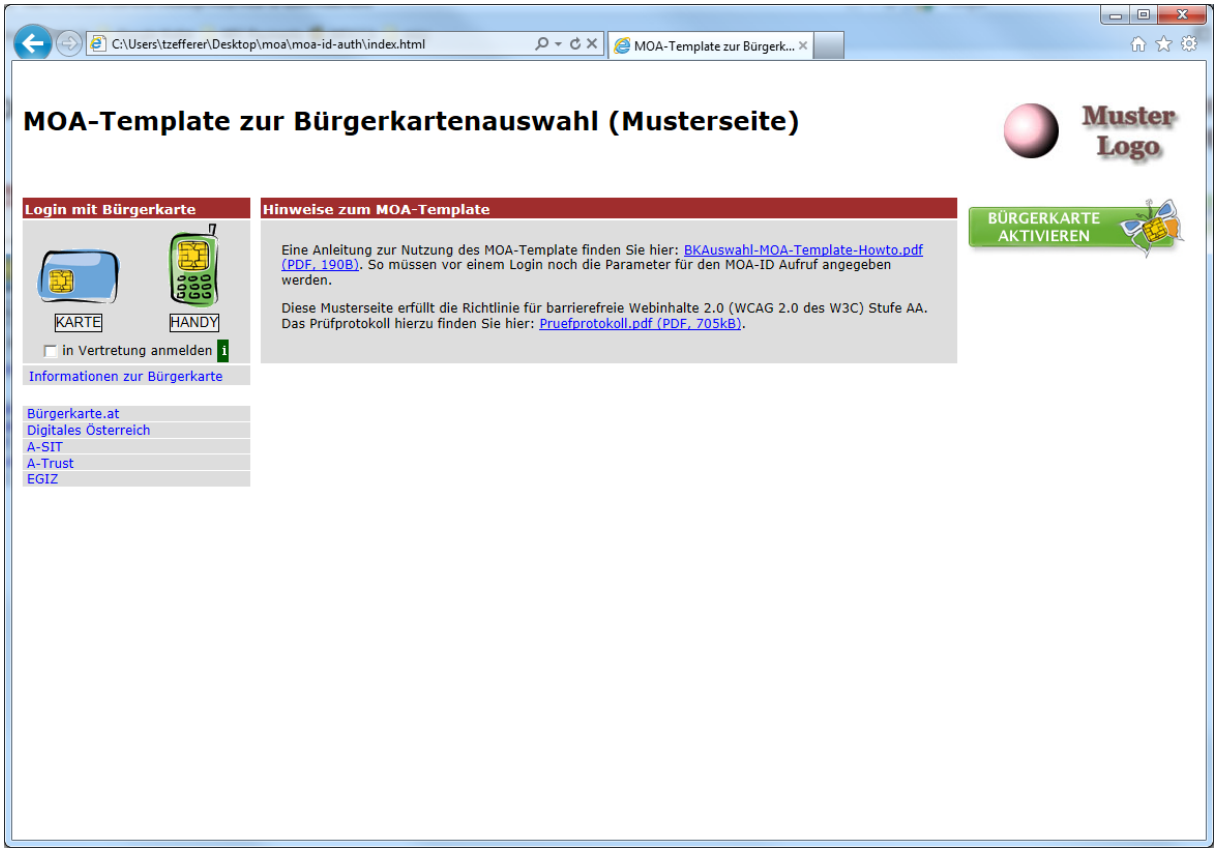

Abbildung 2. Von MOA-ID bereitgestelltes Template zur Integration einer Auswahlseite für präferierte Bürgerkarten-Ausprägungen.

Lässt sich das gesamte in Abbildung 2 dargestellte Template nicht oder nur schwer in ein bestehendes Layout integrieren, so kann optional auch nur ein Teil des Templates verwendet werden. So könnte etwa der oben dargestellte Bereich „Login mit Bürgerkarte“ – d.h. die eigentliche Bürgerkartenauswahl – über einen HTML-IFRAME in eine bestehende Applikation integriert werden.

Natürlich kann die gesamte Funktionalität des angebotenen Templates auch vom Applikationsbetreiber selbst implementiert werden, um eine optimale und nahtlose Integration in bestehende Applikationen zu gewährleisten. In diesem Fall kann das von MOA-ID angebotene Template zumindest als Vorlage dienen.

3 Aufruf der MOA-ID Authentisierungskomponente

Unabhängig von der durch die Benutzerin bez. den Benutzer ausgewählten Bürgerkartenausprägung muss zum Start der MOA-ID-basierten Authentifizierung ein entsprechender Request an MOA-ID gesendet werden. Dies muss in Form eines HTTP-POST-Requests erfolgen. Listing 1 zeigt einen beispielhaften Aufruf von MOA-ID unter der Annahme, dass die Handy-Signatur als Bürgerkarte ausgewählt wurde.

Listing 1. Aufruf von MOA-ID über HTTP-POST.

```
<form method="POST" name="moaidform" id="moa" action="https://moadomain.at/moa-id-
auth/StartAuthentication?OA=https://appdomain.at/application/moaid-servlet/">
    <input type="hidden" name="Template"
value="https://appdomain.at/application/login_template/template_handyBKU.html">
    <input type="hidden" name="bkuURI" value="https://www.handy-signatur.at/mobile/https-security-
layer-request/default.aspx">
</form>
```

Als „action“-Attribut des HTML-FORM Tags muss die URL, unter der MOA-ID erreichbar ist, angegeben werden. MOA-ID kann dabei am gleichen oder auch auf einem externen Server betrieben werden. Wichtig ist, dass das Servlet „StartAuthentication“ von MOA-ID explizit als aufzurufende URL angegeben wird. Der angegebenen URL muss zudem der URL-Parameter „OA“ angefügt werden. Dieser definiert jene URL, an die MOA-ID nach erfolgter Authentifizierung das SAML-Artifact zur Abholung der SAML-Assertion überträgt. In dem in Listing 1 gezeigten Beispiel muss die Online-Applikation also unter /moaid-servlet ein Servlet bereitstellen, das von MOA-ID aufgerufen werden kann und das das SAML-Artifact entgegennehmen kann (siehe dazu auch Abschnitt 4).

Darüber hinaus können die beiden Input-Parameter „Template“ und „bkuURI“ angegeben werden. Über den Parameter „Template“ wird eine URL definiert, unter der sich MOA-ID ein für die Anmeldung benötigtes Template von der Online-Applikation abholen kann. Über dieses Template können optional diverse Parameter für die Integration der Handy-Signatur (bzw. der jeweils ausgewählten BKU) angegeben werden.

Templates, die für die einzelnen Bürgerkarten-Implementierungen verwendet werden können, werden ebenfalls von MOA-ID bereitgestellt und können einfach in die Online-Applikation übernommen werden. Das von MOA-ID zur Verfügung gestellte Template für die Verwendung der Handy-Signatur ist in Listing 2 dargestellt. Ähnliche vorbereitete Templates existieren auch für die Verwendung chipkartenbasierter Bürgerkartenausprägungen.

Listing 2. Template für die Verwendung der Handy-Signatur.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html lang="de">
    <head>
        <title></title>
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
        <script language="javascript" type="text/javascript">
            function onAnmeldeSubmit() {
                document.CustomizedForm.submit();
                document.CustomizedForm.Senden.disabled=true;
            }
        </script>
    </head>
    <body onLoad="onAnmeldeSubmit()">
        <form name="CustomizedForm" action="<BKU>" method="post" enctype="multipart/form-data<>">
            <input class="button" type="hidden" value="Starte Authentisierung" name="Senden">
            <input type="hidden" name="XMLRequest" value="<XMLRequest>">
            <input type="hidden" name="DataURL" value="<DataURL>">
            <input type="hidden" name="PushInfobox" value="<PushInfobox>">

            <!-- Angabe der Parameter fuer die Handy-BKU -->
            <input type="hidden" name="appletWidth" value="210">
            <input type="hidden" name="appletHeight" value="149">

            <!-- [OPTIONAL] Aendern Sie hier die Hintergrundfarbe der Handy-BKU -->
```

```
                <input type="hidden" name="backgroundColor" value="#DDDDDD">

                <input type="hidden" name="redirecttarget" value="_parent">
            </form>

            <form name="CustomizedInfoForm" action="<BKU>" method="post">
                <input type="hidden" name="XMLRequest" value="<CertInfoXMLRequest>">
                <input type="hidden" name="DataURL" value="<CertInfoDataURL>">
            </form>
            <form name="DummyForm" action="<BKU>" method="post">
            </form>
        </body>
</html>
```

Neben dem Parameter „Template“ kann beim Aufruf von MOA-ID auch der Input-Parameter „bkuURI“ angegeben werden. Dieser definiert die URL zu der von der Benutzerin bzw. vom Benutzer ausgewählten Bürgerkartenumgebung (Handy-Signatur, etc.). In dem in Listing 1 gezeigten Beispiel verweist dieser Parameter auf die von A-Trust betriebene Handy-Signatur-Instanz.

Nach dem Absenden des in Listing 1 gezeigten Web-Formulars an MOA-ID wird der Authentifizierungsvorgang automatisch gestartet und durchgeführt. Die Online-Applikation ist in die Authentifizierung der Benutzerin bzw. des Benutzers nicht unmittelbar involviert. Diese muss lediglich (etwa über ein HTML-IFRAME Tag) die GUI-Komponente der gewählten Bürgerkartenumgebung einbinden. Bei Verwendung des von MOA-ID bereitgestellten Templates wird dies von diesem Template übernommen.

4 Abholen der SAML-Assertion

Nach erfolgter Authentifizierung durch MOA-ID unter Verwendung der Bürgerkarte ist MOA-ID in Besitz der nötigen Authentifizierungsdaten. Diese sind in einer SAML-Assertion entsprechend strukturiert. Zum endgültigen Abschluss des Authentifizierungsprozesses muss diese SAML-Assertion nun an die Online-Applikation übertragen werden. Dazu wird die Benutzerin bzw. der Benutzer mit einem SAML-Artifact Parameter an die Online-Applikation weitergeleitet. Das SAML-Artifact kann einer SAML-Assertion eindeutig zugordnet werden. Die Online-Applikation kann dieses SAML-Artifact verwenden, um die SAML-Assertion in MOA-ID abzuholen.

Zur Übertragung des SAML-Artifacts leitet MOA-ID die Benutzerin bzw. den Benutzer and die Online-Applikation weiter, die wie in Listing 1 dargestellt durch den URL-Parameter „OA“ festgelegt wurde. Hinter dieser URL verbirgt sich in der Regel ein Servlet der Online-Applikation, welches in weiterer Folge das SAML-Artifact ausliest. Listing 3 zeigt anhand eines konkreten Beispiels, wie das SAML-Artifact aus dem von MOA-ID gesendeten Request über den Identifier „SAMLArtifact“ ausgelesen werden kann.

Listing 3. Auslesen des SAML-Artifacts.

```
Protected void doPost(HttpServletRequest request, HttpServletResponse response) throws
ServletException, IOException {

    String artifact = request.getParameter("SAMLArtifact");


    // Further processing follows here...

}
```

Mit Hilfe des auf diese Weise erhaltenen SAML-Artifacts kann in weiterer Folge die SAML-Assertion von MOA-ID abgeholt werden. MOA-ID bietet dazu eine entsprechende Web-Service-Schnittstelle an. Diese Schnittstelle ist unter folgender URL erreichbar:

https://moadomain.at/moa-id-auth/services/GetAuthenticationData

Die Online-Applikation muss also einen entsprechenden Client implementieren, der das SAML-Artifact an die von MOA-ID bereitgestellte Web-Service-Schnittstelle überträgt, um die dazugehörige SAML-Assertion abzuholen. Der Aufbau des entsprechenden R equests sowie der erhaltenen Response folgt dabei dem SAML 1.0 Standard.

Listing 4 illustriert einen SAML-Request zum Abholen einer SAML-Assertion, die über das SAML-Artifact „AAH5hs8aaZSFYHya0/cmtJ3QAR7rf54uhIsEcDMZFmmZ1/Qldrdf4JSK“ referenziert wird. Der SAML-Request ist bereits in einen SOAP-Request eingebettet, welcher in weiterer Folge an MOA-ID gesendet werden kann.

Listing 4. Beispielhafter SAML-Request zur Abholung des SAML-Assertion von MOA-ID.

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
    <soapenv:Header/>
    <soapenv:Body>
        <samlp:Request IssueInstant="2009-11-30T13:31:42.033+01:00" MajorVersion="1" MinorVersion="0"
RequestID="d889b63cd2a41b2d" xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol">
            <samlp:AssertionArtifact>AAH5hs8aaZSFYHya0/cmtJ3QAR7rf54uhIsEcDMZFmmZ1/Qldrdf4JSK
            </samlp:AssertionArtifact>
        </samlp:Request>
    </soapenv:Body>
</soapenv:Envelope>
```

Der von der Online-Applikation zu implementierende Client muss also aus dem erhaltenen SAML-Artifact einen spezifikationskonformen SAML-Request generieren, diesen in einen SOAP-Request einbetten und im Anschluss an die Web-Service-Schnittstelle von MOA-ID senden.

5 Extrahierung der Authentisierungsdaten

Kann MOA-ID zum übermittelten SAML-Artifact eine zugehörige SAML-Assertion finden, wird diese an die Online-Applikation in der Antwort auf den übermittelten Web-Service-Request übertragen. Die erhaltene SAML-Response folgt so wie der SAML-Request dem SAML 1.0 Standard.

Listing 5 zeigt eine beispielhafte SAML-Response. Für die Online-Applikation von besonderem Interesse ist dabei das Element „<saml:Assertion>“, welches die eigentlichen Authentifizierungsdaten enthält. Dieses, bzw. die in diesem Element enthaltenen Daten müssen daher von der Online-Applikation je nach Bedarf extrahiert werden. Die für eine Identifizierung der Benutzerin bzw. des Benutzers besonders relevanten Daten sind in Listing 5 hervorgehoben. So enthält die SAML-Assertion neben dem eindeutigen Identifier (in diesem Beispiel offensichtlich ein bPK, bei einer Verwendung im privaten Sektor würde die Assertion ein wbPK enthalten) auch Vorname, Zuname und Geburtsdatum der authentifizierten Person. Diese Daten können schlussendlich von der Online-Applikation zur eindeutigen Identifizierung der Benutzerin bzw. des Benutzers herangezogen werden.

Listing 5. Beispiel einer von MOA-ID erhaltenen SAML-Response.

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion" InResponseTo="-525973270146282894"
    IssueInstant="2009-02-24T13:38:32+01:00" MajorVersion="1" MinorVersion="0"
    ResponseID="6125563722598650316">
    <samlp:Status>
        <samlp:StatusCode Value="samlp:Success"> </samlp:StatusCode>
        <samlp:StatusMessage>Anfrage erfolgreich beantwortet</samlp:StatusMessage>
    </samlp:Status>
    <saml:Assertion xmlns:pr="http://reference.e-government.gv.at/namespace/persondata/20020228#"
        xmlns:si="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" AssertionID="-1780069874206367983"
        IssueInstant="2009-02-24T13:37:30+01:00" Issuer="http://localhost:8080/moa-id-auth/"
        MajorVersion="1" MinorVersion="0" xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
        <saml:AttributeStatement>
            <saml:Subject>
                <saml:NameIdentifier NameQualifier="urn:publicid:gv.at:cdid+bpk"
                    >FyOkEWMooLy8L1zwNicKAhf/vPU=</saml:NameIdentifier>
                <saml:SubjectConfirmation>
                    <saml:ConfirmationMethod>http://reference.e-
government.gv.at/namespace/moa/20020822#cm</saml:ConfirmationMethod>
                    <saml:SubjectConfirmationData/>
                </saml:SubjectConfirmation>
            </saml:Subject>
            <saml:Attribute AttributeName="PersonData"
                AttributeNamespace="http://reference.e-
government.gv.at/namespace/persondata/20020228#">
                <saml:AttributeValue>
                    <pr:Person
                        xmlns:pr="http://reference.e-government.gv.at/namespace/persondata/20020228#"
                        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                        xsi:type="pr:PhysicalPersonType">
                        <pr:Identification>
                            <pr:Value/>
                            <pr:Type>urn:publicid:gv.at:baseid</pr:Type>
                        </pr:Identification>
                        <pr:Name>
                            <pr:GivenName>XXXKarin Stella</pr:GivenName>
                            <pr:FamilyName primary="undefined">XXXKunz</pr:FamilyName>
                        </pr:Name>
                        <pr:DateOfBirth>1900-01-01</pr:DateOfBirth>
                    </pr:Person>
                </saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute AttributeName="isQualifiedCertificate"
                AttributeNamespace="http://reference.e-government.gv.at/namespace/moa/20020822#">
                <saml:AttributeValue>false</saml:AttributeValue>
```

```
            </saml:Attribute>
            <saml:Attribute AttributeName="bkuURL"
                AttributeNamespace="http://reference.e-government.gv.at/namespace/moa/20020822#">
                <saml:AttributeValue>http://localhost:3495/http-security-layer-
request</saml:AttributeValue>
            </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>
```

Anmerkung: Für Anwendungen der Privatwirtschaft (wbPK) sollte die Online-Applikation neben dem eindeutigen Identifikationsbegriff wbPK über Vergleich der Personendaten (Name, Geburtsdaten) mit den in der Online-Applikation hinterlegten Daten die Plausibilität dieser Zuordnung überprüfen. Dies um Fehlzuordnungen, die in wbPK-Anwendungen aus der Manifestbildung und Behandlung der Stammzahl/wbPK in der Personenbindungssignatur möglich sind, technisch auszuschließen (die Personendaten sind trotz der Signaturmanifeste immer von der Stammzahlenregisterbehörde signiert). Zusätzlich können für eine revisionssichere Dokumentation des Anmeldevorgangs die von der Bürgerin bzw. dem Bürger mit qualifizierter Signatur (und damit rechtssicher) unterschriebenen Anmeldedaten archiviert werden (siehe dazu auch folgendes Kapitel).

6 Revisionssichere Dokumentation

MOA-ID speichert – je nach konfiguriertem Log-Level mehr oder weniger detailliert – Informationen zu den Anmeldevorgängen in einer konfigurierbaren Log-Datei. Für eine revisionssichere Dokumentation jedes einzelnen Anmeldevorganges kann die Online-Applikation die von der Bürgerin bzw. vom Bürger qualifiziert signierten Anmeldedaten anfordern. Dazu muss in der Konfiguration der Online-Applikation in MOA-ID das Attribut „provideAUTHBlock“ auf den Wert „true“ gesetzt werden. Listing 6 zeigt eine beispielhafte Konfiguration einer Online-Applikation in MOA-ID. Gemäß dieser Konfiguration werden die von der Benutzerin bzw. vom Benutzer signierten Anmeldedaten über die SAML-Response an die Online-Applikation übertragen.

Listing 6. Beispielhafte Konfiguration einer Online-Applikation in MOA-ID.

```
<OnlineApplication
    friendlyName="Demo-Applikation"
    publicURLPrefix="https://appdomain.at/application/moaid-login/"
    type="businessService" >

    <AuthComponent
        provideAUTHBlock="true"
        provideCertificate="false"
        provideIdentityLink="false"
        provideStammzahl="false"
        slVersion="1.2" >

        <IdentificationNumber>

            <pr:Vereinsnummer xmlns:pr="http://reference.e-
government.gv.at/namespace/persondata/20020228#" >
0123456789
            </pr:Vereinsnummer>
        </IdentificationNumber>
    </AuthComponent>


</OnlineApplication>
```

MOA-ID liefert die signierten Anmeldedaten dann zusammen mit der SAML-Assertion in der entsprechenden SAML-Response. Die signierten Authentifizierungsdaten sind dabei im Element „saml:SubjectConfirmationData“ enthalten. Listing 7 illustriert die Integration der signierten Authentifizierungsdaten in die SAML-Response. Aus Gründen der Übersichtlichkeit wurde nicht der gesamte AUTH-Block dargestellt.

Listing 7. SAML-Response mit signierten Authentifizierungsdaten.

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response InResponseTo="b7a82c9ff0c8c9d2" IssueInstant="2012-08-03T09:09:58+02:00"
MajorVersion="1" MinorVersion="0" ResponseID="-5655510743788571087"
xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion" xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol">
    <samlp:Status>
        <samlp:StatusCode Value="samlp:Success"></samlp:StatusCode>
        <samlp:StatusMessage>Anfrage erfolgreich beantwortet</samlp:StatusMessage>
    </samlp:Status>
    <saml:Assertion AssertionID="3171569170319627500" IssueInstant="2012-08-03T09:09:58+02:00"
Issuer="https://appdomain.at/moa-id-auth/" MajorVersion="1" MinorVersion="0"
xmlns:pr="http://reference.e-government.gv.at/namespace/persondata/20020228#"
xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion" xmlns:si="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <saml:AttributeStatement>
            <saml:Subject>
                <saml:NameIdentifier
NameQualifier="urn:publicid:gv.at:wbpk+VR+0123456789">e0C5zZDkaaqIk3Bn123tPb4t5AE=
                </saml:NameIdentifier>
                <saml:SubjectConfirmation>
                    <saml:ConfirmationMethod>http://reference.e-
government.gv.at/namespace/moa/20020822#cm
                    </saml:ConfirmationMethod>
                    <saml:SubjectConfirmationData>
```

```
                        <saml:Assertion AssertionID="any" IssueInstant="2012-08-03T09:09:50+02:00"
Issuer="Max Mustermann" MajorVersion="1" MinorVersion="0" xmlns:pr="http://reference.e-
government.gv.at/namespace/persondata/20020228#" xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">

[…]

                        </saml:Assertion>
                    </saml:SubjectConfirmationData>
                </saml:SubjectConfirmation>
            </saml:Subject>
            <saml:Attribute AttributeName="PersonData" AttributeNamespace="http://reference.e-
government.gv.at/namespace/persondata/20020228#">
                <saml:AttributeValue>
                    <pr:Person si:type="pr:PhysicalPersonType" xmlns:pr="http://reference.e-
government.gv.at/namespace/persondata/20020228#" xmlns:si="http://www.w3.org/2001/XMLSchema-instance">
                        <pr:Identification>
                            <pr:Value/>
                            <pr:Type>urn:publicid:gv.at:wbpk+VR+0123456789</pr:Type>
                        </pr:Identification>
                        <pr:Name>
                            <pr:GivenName>Max</pr:GivenName>
                            <pr:FamilyName primary="undefined">Mustermann</pr:FamilyName>
                        </pr:Name>
                        <pr:DateOfBirth>1981-08-30</pr:DateOfBirth>
                    </pr:Person>
                </saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute AttributeName="isQualifiedCertificate"
AttributeNamespace="http://reference.e-government.gv.at/namespace/moa/20020822#">
                <saml:AttributeValue>true</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute AttributeName="bkuURL" AttributeNamespace="http://reference.e-
government.gv.at/namespace/moa/20020822#">
                <saml:AttributeValue>https://moccadomain.at/bkuonline/https-security-layer-request
                </saml:AttributeValue>
            </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>
```

Bei einer Speicherung der auf diese Weise erhaltenen Authentifizierungsdaten ist zu beachten, dass aus der Natur der elektronischen Signatur die signierten Daten im Zuge des Speichervorgangs in keiner Weise verändert werden dürfen, da die Signatur dann nicht mehr prüfbar ist.

Referenzen

[1] Dokumentation MOA-ID, http://joinup.ec.europa.eu/site/moa-idspss/moa-id-1.5.1/doc/moa_id/moa.htm

[2] Spezifikation MOA-ID, http://joinup.ec.europa.eu/site/moa-idspss/moa-id-1.5.1/doc/MOA_ID_1.4_20070802.pdf

[3] Konzept und Spezifikation MOA-ID 1.5 – Update Spezifikation Module für Online Applikationen – ID, http://joinup.ec.europa.eu/site/moa-idspss/moa-id-1.5.1/doc/MOA_ID_1.5_Anhang.pdf

[4] Die österreichische Bürgerkarte, http://www.buergerkarte.at/konzept/securitylayer/spezifikation/aktuell/

[5] Dokumentation zur Nutzung des MOA-Template für eine integrierte Bürgerkartenauswahl bei MOA-ID, https://joinup.ec.europa.eu/sites/default/files/BKAuswahl-MOA-Template-Howto.pdf