EGIZ E-Government Innovationszentrum

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

Konzept und Spezifikation MOA-ID 1.5.2

Update Spezifikation Module für Online Applikationen - ID

Version 1.5.2, 29.06.2012

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

Klaus Stranacher – Klaus.Stranacher@egiz.gv.at

Zusammenfassung: Dieses Dokument enthält ein Update zur Spezifikation von MOA-ID 1.4 vom 02.08.2007 [MOA-ID 1.4]. Dieses Update betrifft die folgenden Abschnitte dieser Spezifikation:

- Abschnitt 4.4 (AUTH-Block) → Umsetzung ab MOA-ID Version 1.5.1
- Abschnitt 4.5 (Anmeldedaten) → Umsetzung ab MOA-ID Version 1.5.2

Inhaltsverzeichnis:

Revision History

Version	Datum	Autor(en)	
1.0	26.07.2010	Bernd Zwattendorfer	Initialversion
1.1	25.10.2010	Bernd Zwattendorfer	Zusätzliches Attribute „targetFullName“
1.2	11.10.2011	Klaus Stranacher	Update für Online-Vollmachten
1.3	26.02.2012	Klaus Stranacher	Update Attribut „sourceID“
1.5.2	26.09.2012	Bernd Zwattendorfer	Update der Anmeldedaten für STORK-Attribute

1 Authentisierungskomponente

1.1 AUTH-Block

Der AUTH-Block ist eine Datenstruktur, die von der Authentisierungskomponente und vom Security-Layer mittels eines XSLT Stylesheets aufgebaut wird, und enthält ab MOA-ID Version 1.5.1 folgende Informationen:

Daten zur Person:

- Vor- und Nachname aus der Personenbindung
- Geburtsdatum aus der Personenbindung

Daten zur Anwendung:

- Name der Anwendung
- Staat

Technische Parameter:

- URL der Anwendung
- Bereich oder Identifier der Anwendung
- Identifikator des Benutzers (bPK)
- Referenzwert für Vollmachtenservice (bei Anmeldung mit Vollmacht)
- Datum
- Uhrzeit

Ab MOA-ID Version 1.5.1 zusätzlich verfügbare Werte werden in den AUTH-Block als <saml:Attribute> Elemente eingefügt.

1.1.1 <saml:Attribute>

1.1.1.1 Name der Anwendung

`<saml:Attribute>` hat folgende Attribute:

Name	Beschreibung
`AttributeName`	oaFriendlyName
`AttributeNamespace`	`http://reference.e-government.gv.at/namespace/moa/20020822#`

`<saml:Attribute>` für den Namen der nachfolgenden Applikation enthält genau ein `<saml:AttributeValue>` mit dem Namen der Anwendung als `xs:string`. Der Name der Anwendung wurde vorher als Attribut in der Konfigurationsdatei konfiguriert.

1.1.1.2 Bereichsspezifisches Personenkennzeichen (bPK)

`<saml:Attribute>` für das bereichsspezifische Personenkennzeichen hat folgende Attribute:

Name	Beschreibung
`AttributeName`	bPK

AttributeNamespace	http://reference.e-government.gv.at/namespace/moa/20020822#

<saml:Attribute> für das bereichsspezifische Personenkennzeichen enthält genau ein <saml:AttributeValue> mit dem Kindelement <pr:Identification>, welches das bereichsspezifische Personenkennzeichen sowie den dafür definierten Typen enthält. Für dieses Attribut ergibt sich damit die folgende Struktur:

```
<saml:Attribute AttributeName='bPK' AttributeNamespace='http://ref…'>
  <saml:AttributeValue>
    <pr:Identification>
      <pr:Value>fWlgvP6sDcXHK+OTgHGEf44mEvw=</pr:Value>
      <pr:Type>urn:publicid:gv.at:cdid+bpk</pr:Type>
    </pr:Identification>
  </saml:AttributeValue>
</saml:Attribute>
```

1.1.1.3 Identifier der Anwendung (MOA-WID-Modus)

<saml:Attribute> für den Identifier der Anwendung hat folgende Attribute:

Name	Beschreibung
AttributeName	IdentityLinkDomainIdentifierType
AttributeNamespace	http://reference.e-government.gv.at/namespace/moa/20020822#

<saml:Attribute> für den Identifier der Anwendung enthält genau ein <saml:AttributeValue> mit dem Identifier der Anwendung (z.B. Firmenbuchnummer, Vereinsnummer, etc.).

1.1.1.4 Referenzwert für Vollmacht (bei Anmeldung mit Vollmacht)

<saml:Attribute> für den Referenzwert der Vollmacht hat folgende Attribute:

Name	Beschreibung
AttributeName	mandateReferenceValue
AttributeNamespace	http://reference.e-government.gv.at/namespace/moa/20020822#

<saml:Attribute> für den Referenzwert der Vollmacht enthält genau einen Text mit dem Referenzwert.

1.2 Anmeldedaten (Zusätzliche SAML Attribute)

Die Anmeldedaten werden in Form einer SAML-Assertion dargestellt, die, basierend auf dem signierten AUTH-Blocks und der vorher übersendeten zugehörigen Personenbindung, von der Authentisierungskomponente der nachfolgenden Applikation zur Verfügung gestellt wird. Die Liste der Informationen, die in dieser SAML-Assertion enthalten sein können, ist in Abschnitt 4.5 (Anmeldedaten) in der Spezifikation von MOA-ID 1.4 vom 02.08.2007 [MOA-ID 1.4] beschrieben. Die folgenden Unterkapitel spezifizieren jene Attribute, die zusätzlich zu diesen Attributen in neueren MOA-Versionen übertragen werden könnnen.

1.2.1 SourceID

MOA-Version: ab 1.5.1
`<saml:Attribute>` für die sourceID (sourceID kann als optionaler Parameter beim MOA-ID Aufruf angegeben werden) folgende Attribute:

Name	Beschreibung
`AttributeName`	sourceID
`AttributeNamespace`	`http://reference.e-government.gv.at/namespace/moa/20020822#`

`<saml:Attribute>` für die sourceID enthält genau jene der beim MOA-ID Aufruf angegeben wird. Fehlt dieser Parameter, entfällt diese `<saml:Attribute>`.

1.2.2 STORK Attribute

MOA-Version: ab 1.5.2
Wegen der in MOA-ID 1.5.2 integrierten STORK[1]-Funktionalität wird diese Liste durch die von STORK spezifizierten Informationen bzw. Attribute erweitert. Im Falle der Authentifizierung einer ausländischen BürgerIn über STORK und MOA-ID können bei Bedarf zusätzliche SAML Attribute in der SAML-Assertion an die Applikation mitüberliefert werden. Diese Attribute müssen bei einer entsprechen STORK Authentifizierung angefragt werden und können in der MOA-ID Konfiguation konfiguriert werden. Details zu diesen überlieferten Attributen können in der STORK-Spezifikation [STORK D5.8.3b] nachgelesen werden. Im Folgenden Abschnitt werden alle möglichen STORK Attribute mit einer kurzen Beschreibung bzw. einem Verweis zur entsprechenden STORK Spezifikation aufgelistet

1.2.3 <saml:Attribute>

Die folgende Tabelle enthält alle STORK-Attribute, die im Rahmen einer STORK Authentifizierung von ausländischen BürgerInnen angefragt werden bzw. in der SAML-Assertion enthalten sein können.

Friendly Name	Name	Name Format	Beschreibung
Inherited Family Name	http://www.stork.gov.eu/1.0/inheritedFamilyName	UTF-8	[STORK D5.7.3]
Adopted Family Name	http://www.stork.gov.eu/1.0/adoptedFamilyName	UTF-8	[STORK D5.7.3]
Gender	http://www.stork.gov.eu/1.0/gender	„M“ oder „F“	[STORK D5.7.3]
Country of Birth	http://www.stork.gov.eu/1.0/countryCodeOfBirth	ISO-3166-3	[STORK D5.7.3]
Nationality	http://www.stork.gov.eu/1.0/nationalityCode	Country code	[STORK D5.7.3]
Marital Status	http://www.stork.gov.eu/1.0/maritalStatus	S = Single M = Married P = Separated D = Divorced W = Widowed	[STORK D5.7.3]
Text Residence Address	http://www.stork.gov.eu/1.0/textResidenceAddress	UTF-8 (with new lines)	[STORK D5.7.3]
Canonical Residence Address	http://www.stork.gov.eu/1.0/canonicalResidenceAddress	XML	see 6.4.1
eMail Address	http://www.stork.gov.eu/1.0/eMail	e-mail	[STORK D5.7.3]

[1] http://eid-stork.eu/

Title	http://www.stork.gov.eu/1.0/title	UTF-8	[STORK D5.7.3]
Residence Permit	http://www.stork.gov.eu/1.0/residencePermit	UTF-8	[STORK D5.7.3]
Pseudonym	http://www.stork.gov.eu/1.0/pseudonym	UTF-8	[STORK D5.7.3]
Age	http://www.stork.gov.eu/1.0/age	Numeric	[STORK D5.7.3]
Is AgedOver	http://www.stork.gov.eu/1.0/isAgeOver	Requested age boundary if true, empty if false	Abschnitt 5.1.4.8.1.1 von [STORK D5.8.3b]
Citizen QAA Level	http://www.stork.gov.eu/1.0/citizenQAALevel	Numeric {1:4}	Zwischen 1 und 4
Fiscal Number	http://www.stork.gov.eu/1.0/fiscalNumber	UTF-8	

`<saml:Attribute>` kommt in der SAML-Assertion mehrmals vor um die oben erwähnten STORK Informationen darzustellen. Jedes `<saml:Attribute>` enthält genau ein `<saml:AttributeValue>`.

Name	Beschreibung
`AttributeName`	http://www.stork.gov.eu/1.0/inheritedFamilyName http://www.stork.gov.eu/1.0/adoptedFamilyName http://www.stork.gov.eu/1.0/gender http://www.stork.gov.eu/1.0/countryCodeOfBirth http://www.stork.gov.eu/1.0/nationalityCode http://www.stork.gov.eu/1.0/maritalStatus http://www.stork.gov.eu/1.0/textResidenceAddress http://www.stork.gov.eu/1.0/canonicalResidenceAddress http://www.stork.gov.eu/1.0/eMail http://www.stork.gov.eu/1.0/title http://www.stork.gov.eu/1.0/residencePermit http://www.stork.gov.eu/1.0/pseudonym http://www.stork.gov.eu/1.0/age http://www.stork.gov.eu/1.0/isAgeOver http://www.stork.gov.eu/1.0/citizenQAALevel http://www.stork.gov.eu/1.0/fiscalNumber
`AttributeNamespace`	`urn:eu:stork:names:tc:STORK:1.0:assertion`

Die folgenden Attribute sind zwar auch in STORK spezifiziert, werden jedoch entweder nicht benötigt oder nicht in den Anmeldedaten als separates `<saml:Attribute>` übertragen, sondern befinden sich an anderen Stellen der SAML-Assertion.

Friendly Name	Name	Name Format	Beschreibung
eIdentifier	http://www.stork.gov.eu/1.0/eIdentifier	CC/CC/Base64	[STORK D5.7.3] Nicht benötigt, bPK wird aus Stammzahl der Personenbindung berechnet und befindet sich im NameIdentifer element im Subject (siehe Abschnitt 4.5.3 von [MOA-ID 1.4])
Given Name	http://www.stork.gov.eu/1.0/givenName	UTF-8	[STORK D5.7.3] Wird im PersonData Attribute übertragen, siehe Abschnitt 4.5.5.1 von [MOA-ID 1.4])
Surname	http://www.stork.gov.eu/1.0/surname	UTF-8	[STORK D5.7.3] Wird im PersonData Attribute übertragen, siehe Abschnitt 4.5.5.1 von [MOA-ID 1.4])

Date of Birth	http://www.stork.gov.eu/1.0/dateOfBirth	Date	[STORK D5.7.3] Sofern vorhanden, wird es im PersonData Attribute übertragen, siehe Abschnitt 4.5.5.1 von [MOA-ID 1.4])
Signed Document	http://www.stork.gov.eu/1.0/signedDoc	Abschnitt 6.5 von [STORK D5.8.3b]	Abschnitt 6.5 von [STORK D5.8.3b] Dieses Attribut wird automatisch von MOA-ID angefragt. Die erhaltene Signatur des Bürgers wird optional als AUTHBlock im SubjectConfirmationData Element übertragen. (siehe Abschnitt 4.5.4 von [MOA-ID 1.4])

Referenzen

[MOA-ID 1.4]	ARGE Spezifikation MOA: *Spezifikation Module für Online Applikationen - ID*. Version 1.4, August 2007.
[STORK D5.7.3]	STORK Konsortium: D5.7.3 Functional Design for PEPS, MW models and interoperability, 2011. https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1874
[STORK D5.8.3b]	STORK Konsortium: *D5.8.3b Interface Specification*, STORK Deliverable, 2011. https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1880