Spezifikation

MOA-ID 1.9.98-SNAPSHOT Dokumentation

PreRelease Dokumentation MOA-ID 1.9.98-SNAPSHOT

Version 0.7, 29.01.2014

Thomas Lenz – Thomas.lenz@egiz.gv.at
Andreas Fitzek – andreas.fitzek@egiz.gv.at

Zusammenfassung: Dieses Dokument beschreibt die Einrichtung und Verwendung von MOA-ID 1. 9.98-SNAPSHOT. Diese MOA-ID Version ist ein PreRelease von MOA-ID 2.0 und integriert bereits SAML2 im PVP2 S-Profil, Single Sign-On und eine datenbankbasierte Konfiguration- und Session-Verwaltung.

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

1 MOA-ID 3
1.1 MOA-ID Installation 3
1.2 MOA-ID Basiskonfiguration 3
1.2.1 Properties 3
1.3 MOA-ID Konfiguration in der Datenbank 6
1.3.1 Allgemeine MOA-ID Konfiguration 6
1.3.2 Online-Applikationskonfiguration 10
1.3.3 Import und Export von XML Konfigurationen 14
1.4 Einsprungspunkte 14
2 MOA-ID Konfigurationstool 16
2.1 Properties 16
2.2 Verwendung 18
2.2.1 Initialiserung 18
2.2.2 Usermanagement: 18
3 Installation MOA-ID und MOA-ID Konfigurationstool 20
3.1 Schritte 20
3.1.1 Installation des JDK 20
3.1.2 Installation von TOMCAT 20
3.1.3 Installation der IAIK JCE 20
3.1.4 Installation einer Datenbank 20
3.1.5 Konfiguration des Tomcat 20
3.1.6 Konfiguration von MOA-ID 21
3.1.7 Konfiguration des MOA-ID Konfigurationstools 21
3.1.8 Initialisierung des MOA-ID Konfigurationstools 21
3.2 Konfiguration der MOA-ID Instanz 22
3.2.1 Neue Konfiguration anlegen 22
3.2.2 Migrationsstrategie von 1.5.1 auf 2.0 22

1 MOA-ID

1.1 MOA-ID Installation

MOA-ID 1.9.98-SNAPSHOT ist ähnlich zu konfigurieren wie MOA-ID 1.5.1. Hierzu kann die Dokumentation von MOA-ID 1.5.1 unter [MOA-DOC] herangezogen werden. Das *moa-id-auth.war* ist in den *webpps* Ordner des jeweiligen Tomcat zu kopieren. (Erfolgreiche Tests mit Tomcats in den Versionen 6 und 7).
Die Konfiguration besteht aus zwei Teilen. Ein Teil der Konfiguration liegt wie bei MOA-ID 1.5.1 im *conf* Ordner des Tomcats. Hierbei handelt es sich um Basiseinstellungen für MOA-ID, Keys zum Signieren, Zertifikate für SSL Verbindungen und Templates, welche von MOA-ID für den Anmeldevorgang verwendet werden. Die beiden Ordner */conf/moa-id* und *conf/moa-spss* beinhalten eine Basiskonfiguration, welche als Ausgangskonfiguration verwendet werden kann (siehe Kapitel 1.2). Der zweite Teil der Konfiguration wird in einer Datenbank abgelegt und kann über das Konfigurations-Tool (siehe Kapitel 1.3) konfiguriert werden.

1.2 MOA-ID Basiskonfiguration

Die Konfiguration der Basiseinstellungen einer jeden MOA-ID Instanz erfolgt mittels einer properties Datei. Diese Hauptkonfigurationsdatei liegt im Ordner /conf/moa-id und wird mit Hilfe der Umgebungsvariable „moa.id.configuration“ festgelegt. Die Basiskonfiguration beinhaltet eine solche Datei mit dem Name „moa-id.properties“ welche als Ausgangskonfiguration genutzt werden kann. Die Tabelle in Kapitel 1.2.1 beschreibt alle Parameter dieser Konfigurationsdatei.

Zusätzlich wird für den Betrieb der Zugriff auf eine Datenbank benötigt, in welcher ein Großteil der Konfiguration, die Session Daten und bei Bedarf auch eine Anmeldestatistik abgelegt werden. Als Datenbank wird mySQL empfohlen (wurde mit mySQL getestet), der Einsatz eines alternativen Datenbanksystems ist jedoch ebenfalls möglich. Für den Betrieb werden zwei getrennte Datenbank Schema benötig, da die Konfiguration und die Session Informationen getrennt abgelegt werden. Der Datenbankzugriff wird ebenfalls über die properties Datei konfiguriert.

1.2.1 Properties

Die Datei „moa-id.properties” enthält die folgenden Eigenschaften.

Name	Beispielswert	Beschreibung
configuration.moasession.key	MeinNEUERMOASESSIONKEY	PassPhrase mit dem die Session Daten in der Datenbank verschlüsselt werden (optional)

configuration.monitoring. active	true / false	Aktiviert das Monitoring Servlet
configuration.monitoring.test. identitylink.url	/test/idl/test_identitylink.xml	URL zu einem IdentityLink der für den IdentityLink Test verwendet wird.
configuration.advanced-logging.active	true / false	Aktiviert das erweiterte Zugriffsstatistic Logging in die Datenbank
service.onlinemandates. acceptedServerCertificates	certs/…	Ordner mit speziellen Serverzertifikaten (optional)
service.onlinemandates. clientKeyStore	keys/vollmachten-service.p12	PKCS12 KeyStore für den Zugriff zum Online-Vollmachten Service. (optional)
service.onlinemandates. clientKeyStorePassword	test	Passwort für den Keystore des Online-Vollmachten Service (optional)
service.foreignidentities. acceptedServerCertificates	certs/…	Ordner mit speziellen Serverzertifikaten (optional)
service.foreignidentities. clientKeyStore=keys	keys/szrgw.p12	PKCS12 KeyStore für den Zugriff zum SZR-Gateway Service. (optional)
service.foreignidentities. clientKeyStorePassword	test	Passwort für den Keystore des SZR-Gateway Service (optional)
protocols.pvp2.idp.ks.file	keys/pvp2.p12	Java Keystore Datei oder PKCS12 KeyStore die den Asymetrischen Schluessel fuer MOA-ID als Identity Provider enthaelt.
protocols.pvp2.idp.ks. kspassword	s3cr3t	Java Keystore Key Passwort
protocols.pvp2.idp.ks.metadata.alias	metadata	Alias des Schluessels im Keystore (Metadatensignature)
protocols.pvp2.idp.ks.metadata.keypassword	s3cr3t	Key Passwort (Metadatensignature)
protocols.pvp2.idp.ks.assertion.sign.alias	assertion	Alias des Schluessels im Keystore (Assertionsignature)
protocols.pvp2.idp.ks.assertion.sign.keypassword	123456	Key Passwort (Assertionsignature)
protocols.oauth20.jwt.ks.file	ecc_test/sinful.p12	Keystore zur Signature des OpenID Connect Tokkens
protocols.oauth20.jwt.ks.key	openID	Alias des OpenID Connect Keys

.name		
protocols.oauth20.jwt.ks.password		Passwort des OpenID Connect Keystores
protocols.oauth20.jwt.ks.key.password		Passwort des OpenID Connect Keys
moasession.hibernate.dialect	org.hibernate.dialect.MySQLDialect	MOA-Session Hibernate Datenbank Dialekt (aktuell mySQL)
moasession.hibernate.connection.url	jdbc:mysql://localhost/moa-id-session?charSet=utf-8	URL zum MOA-Session Datenbank Schema
moasession.hibernate.connection.driver_class	com.mysql.jdbc.Driver	Hibernate Connection zum MOA-Session Datenbank Schema (aktuell mySQL)
moasession.hibernate.connection.username	moasession	Benutzername für den Zugriff zum MOA-Session Datenbank Schema
moasession.hibernate.connection.password	password	Passwort für den Zugriff zum MOA-Session Datenbank Schema
configuration.hibernate.dialect	org.hibernate.dialect.MySQLDialect	MOA-Konfiguration Hibernate Datenbank Dialekt (aktuell mySQL)
configuration.hibernate.connection.url	jdbc:mysql://localhost/moa-id-config?charSet=utf-8&autoReconnect=true	URL zum MOA- Konfiguration Datenbank Schema
configuration.hibernate.connection.driver_class	com.mysql.jdbc.Driver	Hibernate Connection zum MOA-Konfiguration Datenbank Schema (aktuell mySQL)
configuration.hibernate.connection.username	moaconfig	Benutzername für den Zugriff zum MOA- Konfiguration Datenbank Schema
configuration.hibernate.connection.password	password	Passwort für den Zugriff zum MOA- Konfiguration Datenbank Schema
advancedlogging.hibernate.dialect	org.hibernate.dialect.MySQLDialect	Statisticlogger Hibernate Datenbank Dialekt (aktuell mySQL)
advancedlogging.hibernate.connection.url	jdbc:mysql://localhost/moa-id-statistic?charSet=utf-8&autoReconnect=tru	URL zum MOA- Statisticlogger Datenbank Schema

	e	
advancedlogging.hibernate.connection.driver_class	com.mysql.jdbc.Driver	Hibernate Connection zum MOA- Statisticlogger Datenbank Schema (aktuell mySQL)
advancedlogging.hibernate.connection.username	moaconfig	Benutzername für den Zugriff zum MOA- Statisticlogger Datenbank Schema
advancedlogging.hibernate.connection.password	password	Passwort für den Zugriff zum MOA- Statisticlogger Datenbank Schema

1.3 MOA-ID Konfiguration in der Datenbank

Alle weiteren Konfigurationsparameter welche bereits aus der MOA-ID 1.5.1 Konfiguration bekannt sind werden mit Hilfe des MOA-ID Konfigurationstools konfiguriert. Die Einrichtung des Konfigurationstools wird in Kapitel 2 beschrieben.

1.3.1 Allgemeine MOA-ID Konfiguration

Die allgemeine MOA-ID Konfiguration umfasst alle Bereiche der aus MOA-ID 1.5.1 bekannten Konfiguration mit Ausnahme der Online-Applikationen. Die nachfolgenden Tabellen beschreiben alle Bereiche der allgemeinen Konfiguration. Bei Elementen die bereits aus der MOA-ID 1.5.1 Konfiguration bekannt sind wird auf den dementsprechenden XML Identifier aus der MOA-ID 1.5.1 Konfiguration verwiesen. Nach einer Änderung an der allgemeinen Konfiguration von MOA-ID muss müssen die MOA-ID Instanzen, welche diese Konfiguration verwenden, neu gestartet werden.

1.3.1.1 Default BKUs

Hiermit werden die URLs zu den Bürgerkartenumgebungen (BKUs) definiert die von MOA-ID für einen Anmeldevorgang verwendet werden, sollte in einer Online-Applikation keine BKUs definiert sein (siehe Kapitel 1.3.2.3). Dieser Bereich ersetzt das XML-Element *<TrustedBKUs>* aus der 1.5.1 MOA-ID Konfiguration, da somit die verwendeten BKUs fix über die Konfiguration vorgeben werden. Wird für SAML1 die BKU Auswahl als POST Parameter mitübergeben so muss dieser mit den hinterlegten BKUs übereinstimmen.

Name	Beispielswert	Beschreibung
Online BKU	https://demo.egiz.gv.at/demoportal_bkuonline/https-security-layer-request	URL zu einer Online-BKU Instanz
Handy BKU	https://www.handy-signatur.at/mobile/https-security-	URL zur Handy-BKU Instanz

	layer-request/default.aspx	
Lokale BKU	https://127.0.0.1:3496/https-security-layer-request	URL zur lokalen BKU Instanz

1.3.1.2 SecurtiyLayer Request Templates

Hierbei handelt es sich um jede Templates welche bei MOA-ID 1.5.1 im StartAuthentication Request an MOA-ID übergeben wurden. (http POST Parameter „template"). Diese Templates werden nun fix bei MOA-ID hinterlegt und müssen nicht mehr im Request mitübergeben werden. Aus Sicherheitsgründen können nur mehr die bei MOA-ID 2.0 hinterlegten Templates verwendet werden, wobei aus Kompatibilitätsgründen weiterhin getrennte Templates definiert werden können.

Name	Beispielswert	Beschreibung
Online BKU	http://demo.egiz.gv.at/demoportal_moaid-2.0/template_onlineBKU.html	URL zum jeweiligen SecurityLayer Request Template für die Online-BKU
Handy BKU	http://demo.egiz.gv.at/demoportal_moaid-2.0/template_handyBKU.html	URL zum jeweiligen SecurityLayer Request Template für die Handy-BKU
Lokale BKU	http://demo.egiz.gv.at/demoportal_moaid-2.0/template_localBKU.html	URL zum jeweiligen SecurityLayer Request Template für die lokale BKU

1.3.1.3 Zertifikatsprüfung

Hierbei handelt es sich um Parameter die bereits aus der MOA-ID 1.5.1 Konfiguration bekannt sind. Die nachfolgende Tabelle gibt einen Link auf das entsprechende XML-Element aus der MOA-ID 1.5.1 Konfiguration. Diese kann für weitere Informationen herangezogen werden.

Name	MOA-ID 1.5.1 XML-Element
CertStoreDirecorty	<GenericConfiguration name="DirectoryCertStoreParameters.RootDir"
TrustManagerRevocation Checking	<GenericConfiguration name="TrustManager.RevocationChecking“
TrustedCACertificates:	<TrustedCACertificates>
ChainingMode	<ChainingModes systemDefaultMode=

1.3.1.4 Session TimeOuts

Hiermit werden die Zeiträume definiert in denen eine Single Sign-On Session gültig ist und eine Online-Applikation die Assertion mittels Redirect-Binding abholen muss. Alle Zeiträume müssen in Sekunden angegeben werden.

Name	Beschreibung
Assertion	Zeitraum in Sekunden in der eine Online-Applikation die Assertion abholen muss bevor diese ungültig wird.
SSO Session authentifiziert	Maximale Zeitspanne einer SSO Session. Nach Ablauf dieser Zeitspanne muss sich der Benutzer auf jeden Fall neu authentifizieren
SSO Session letzter Zugriff	Zeitspanne seit dem letzten Zugriff mit einer gültigen SSO Session. Nach Ablauf dieser Zeitspanne muss sich der Benutzer neu authentifizieren.

1.3.1.5 MOA-SP Konfiguration

Hiermit wird der Zugriff zu MOA-SP/SS zur Signaturprüfung konfiguriert. Alle Elemente waren auch bereits in der MOA-ID 1.5.1 Konfiguration enthalten.

Name	MOA-ID 1.5.1 XML-Element
Personenbindung Trustprofil	MOA-SP/VerifyIdentityLink/TrustProfileID
Authentfizierungsblock Trustprofil	MOA-SP/VerifyAuthBlock/TrustProfileID
Authentfizierungsblock Transformationen	MOA-SP/VerifyAuthBlock/VerifyTransformsInfoProfileID
MOA-SP Service URL	MOA-SP/ConnectionParameter/URL

1.3.1.6 Externe Services

Hiermit werden die URLs zum Online-Vollmachten Service und zum SZR-Gateway konfiguriert. Beide Konfigurationsparameter waren auch bereits in der MOA-ID 1.5.1 Konfiguration enthalten.

1.3.1.7 Singe Sign-On (SSO)

MOA-ID 2.0 unterstützt Single Sign-On. In diesem Bereich können SSO spezifische Parameter konfiguriert werden.

Name	Beispielswert	Beschreibung
URL-Prefix	https://demo.egiz.gv.at/demoportal_moaid-2.0/	URL-Prefix der MOA-ID Instanz
Service	EGIZ MOAID 2.0 Beta	Name des Betreibers

Name		
Service Target	BF	Bereich dem der MOA-ID Betreiber zugeordnet wird.
AuthBlockText	Ich #NAME# stimme am #DATE# um #TIME# einer Anmeldung mittels Single Sign-On zu.	Zusätzlicher Text im AuthBlock der vom Benutzer signiert wird.

Der Inhalt des Elements AuthBlockText wird im AuchBlock, welcher vom Benutzer im Anmeldevorgang signiert wird, dargestellt. Die Schlüsselwörter #NAME#, #DATE# und #TIME# werden hierbei von MOA-ID durch die jeweiligen Informationen zum Anmeldezeitpunkt ersetzt.

- #NAME# → Vor- und Familienname (z.B. Max Mustermann)
- #DATE# → Aktuelles Datum (z.B 07.08.2013)
- #TIME# → Aktuelle Uhrzeit (z.B. 10:35)

1.3.1.8 Protokolle

Hierbei handelt es sich um authentifizierungsprotokollspezifische Einstellungen die in MOA-ID 2.0 neu hinzukommen sind. Dieser Bereich ist in zwei Teilabschnitte unterteilt.

1. LegacyModus
   In MOA-ID 2.0 wird die Bürgerkartenauswahl standardmäßig von MOA-ID bereitgestellt und somit erfolgt diese im Kontext von MOA-ID 2.0. Dem zu Folge müssen die aus MOA-ID 1.5.1 bekannten StartAuthentication Parameter (target, bkuURL, template, usemandate) nicht mehr im StartAuthentication Request übergeben werden und es kann ein standardkonformes Authentifizierungsprotokoll verwendet werden.
   Soll die Bürgerkartenauswahl weiterhin, wie in MOA-ID 1.5.1 im Kontext der Online-Applikation erfolgen muss für das jeweilige Protokoll der Legacy Modus aktiviert werden. Wird der Legacy Modus verwendet müssen jedoch die bkuURL, das Template und der target mit den bei MOA-ID 2.0 hinterlegten Parametern übereinstimmten.

2. PVP2 Konfiguration
   Dieser Bereich beinhaltet PVP2 spezifische Konfigurationsparameter.

Name	Beispielwert	Beschreibung
PVP2 Service URL-Prefix	https://moaid.egiz.gv.at	Issuer Name den MOA-ID als Identity Provider nutzen soll

PVP Service Name	https://moaid.egiz.gv.at/moa-id-auth/	Oeffentliche URL unter der MOA-ID erreichbar ist
Kurzbezeichnung - Organisation	EGIZ	Name der Organisation die MOA-ID betreibt (fuer Metadaten von MOA-ID)
Vollständiger Name - Organisation	EGIZ	Anzeigename der Organisation die MOA-ID betreibt (fuer Metadaten von MOA-ID)
URL der Organisation - Organisation	http://www.egiz.gv.at	URL der Organisation die MOA-ID betreibt (fuer Metadaten von MOA-ID)
Familienname	Mustermann	Nachname der Kontakt-person in den Metadaten von MOA-ID
Vorname	Max	Vorname der Kontakt-person in den Metadaten von MOA-ID
Mailadresse	max@test.com	Mailadresse der Kontakt-person in den Metadaten von MOA-ID
Telefonnummer	+43 0142525261	Telefonnummer der Kontaktperson in den Metadaten von MOA-ID
Unternehmen	E-Government Innovationszentrum	Unternehmen der Kontaktperson in den Metadaten von MOA-ID
Type des Kontakts	technical	SAML2 spezifischer Typ des Kontaktperson in den Metadaten von MOA-ID

1.3.1.9 SecurityLayer Transformationen

Hiermit wird die SecurityLayer Transformation angegeben welche von MOA-ID 2.0 verwendet werden soll. Das entsprechende Element in der MOA-ID 1.5.1 Konfiguration lautete <AuthComponent/SecurityLayer/TransformsInfo>. Über das Datei-Upload Feld kann die zu verwendende Transformation hochgeladen werden. Diese befindet sich in der MOA-ID Defaultkonfiguration im Ordner */conf/moa-id/transforms/ TransformsInfoAuthBlockTable_DE_new.xml*

1.3.2 Online-Applikationskonfiguration

Die Konfiguration der Online-Applikationen erfolgt über ein getrenntes Formular. Die anschließende Aufstellung beschreibt die einzelnen Konfigurationspunkte. Online

Applikationen können direkt eingetragen werden ohne dass ein Neustart der MOA-ID Instanzen notwendig ist.

Name	Beispielswert	Beschreibung
Online-Applikation ist aktiviert		Die Online-Applikation ist aktiv und wird von MOA-ID 2.0 verwendet
Eindeutiger Identifikatior	https://demo.egiz.gv.at/demoportal_demologin/	PublicURLPrefix in MOA-ID 1.5.1
Name der Online-Applikation	Demo Application Simple	FriendlyName in MOA-ID 1.5.1
Privatwirtschaftliche Applikation		Type in MOA-ID 1.5.1 (businessService / publicService)

1.3.2.1 Privatwirtschaftlicher Bereich

Name	Beispielswert	Beschreibung
Identificationsnummer	FN+468924i	Stammzahl des Wirtschaftsunternehmens

1.3.2.2 Öffentlicher Bereich

Name	Beispielswert	Beschreibung
Bereich (Target)	BF	Geschäftsbereich der Online-Applikation
Bezeichnung des Bereichs	Bildung und Forschung	Bezeichnung des Bereichs der Online-Applikation sollte kein automatisches Mapping durch MOA-ID möglich sein
Sub-Bereich		Hiermit kann der Bereich der Online-Applikation näher spezifiziert werden.

Zusätzlich gibt es für Benutzer mit Administratorrechten die Möglichkeit eine freidefinierbare Bereichskennung für Testzwecke zu konfigurieren.

1.3.2.3 BKU Konfiguration

Hiermit können onlineapplikationsspezifische Bürgerkartenumgebungen definiert werden. Werden keine Bürgerkartenumgebungen definiert wird die Default Konfiguration (siehe Kapitel 1.3.1.1) verwendet. Zusätzlich gibt es weitere BKU spezifische Einstellungen.

Name	Beispielswert	Beschreibung
KeyBoxIdentifier		OnlineApplication/@keyBoxIdentifier in MOA-ID 1.5.1
Security-LayerTemplates		Zusätzliche SecurityLayer Request Template URLs, welche für diese Onlineapplikation als WhiteList freigeschalten werden.

Wenn die Option SecurityLayerTemplates (Legacy Request) ausgewählt wurde können drei zusätzliche SecurtityLayer Request Templates für diese Onlineapplikation definiert werden. Diese hier definierten Templates dienen als zusätzliche WhiteList für Templetes welche im „*StartAuthentication*“ Request mit dem Parameter „*template*“ übergeben werden. Somit können nur bei MOA-ID hinterlegte SL Templates verwendet werden.

1.3.2.4 Vollmachten

Dieses Element beinhaltet eine (Komma-separierte) Liste von Vollmachten-Profilen, die festlegen mit welchen Vollmachtstypen man sich bei der Online-Applikation anmelden kann. Unter https://vollmachten.stammzahlenregister.gv.at/mis/ finden Sie eine Liste der unterstützen Vollmachten-Profile. Hierzu muss jedoch das Vollmachten Service konfiguriert werden (siehe Kapitel 1.2.1 und 1.3.1.6)

Name	Beispielswert	Beschreibung
Vollmachten(ja/nein)		Vollmachtenanmeldung erlauben
Profile	Zustellung,ELGABilateral, DVR	Liste von Vollmachten –Profile die durch Komma getrennt werden
Nur Vollmachten-anmeldung erlauben		Es ist nur eine Anmeldung mittels Online-Vollmacht möglich

1.3.2.5 Single Sign-On

Hiermit können onlineapplikationsspezifische SSO Einstellungen konfiguriert werden.

Name	Beispielswert	Beschreibung
Single Sign-On verwenden		Gibt an ob die Online-Applikation SSO unterstützt. Wird dieses Element nicht gewählt muss sich der Benutzer auch bei einer gültigen SSO Session bei jeder Anmeldung authentifizieren.
Zusätzliche Userabfrage		Wird dieses Element gewählt erhält der Benutzer eine

		zusätzliche Abfrage im Falle einer SSO Anmeldung.
Single Log-Out URL		URL zu einem Service der Online-Applikation über die diese vom Log-Out des Users informiert werden kann.

Die Single- Log-Out Funktionalität ist in der aktuellen Version noch nicht implementiert, da die hierfür benötige Spezifikation noch im Entwurf befinden. Da eine Umsetzung geplant ist, ist das dafür erforderliche Konfigurationsfeld bereits enthalten.

1.3.2.6 SAML1 Konfiguration

Hierbei handelt es sich um die gleichnamigen <OnlineApplication/AuthComponent> Attribute aus der MOA-ID 1.5.1 Konfiguration. Durch Auswahl der einzelnen Attribute werden diese in der SAML1 Assertion an die Online-Applikation übertragen.

1.3.2.7 PVP2.x Konfiguration

Dieser Abschnitt konfiguriert applikationsspezifische Einstellungen für PVP2.x. Wenn durch die Online-Applikation PVP2.x zur Authentifizierung verwendet werden soll, müssen diese Elemente konfiguriert werden.

Name	Beispielswert	Beschreibung
URL zu den Metadaten:	http://demo.egiz.gv.at/demologin-pvp2-sso/metadata/demoportal-pvp2-sso.mdxml	URL unter der MOA-ID 2.0 die Metadaten der Online-Applikation beziehen kann. Diese Metadaten müssen durch die Online-Applikation signiert werden.
Infos zum Zertifikat:	CN=Sample PVP App,OU=Unknown,O=Unknown,L=Unknown,ST=Unknown,C=Unknown	Wenn bereits ein Zertifikat hinterlegt ist, wird hier der SubjectName des Zertifikats ausgegeben.
Zertifikat hochladen		Zertifikat mit dem die Metadaten der Online-Applikation signiert sind. Dieses wird benötigt um die Metadaten zu verifizieren.

1.3.2.8 Zusätzliche allgemeine Einstellungen

Hierbei handelt es sich um einige allgemeine Konfigurationsparameter.

Name	Beispielswert	Beschreibung
AuthblockText:	Siehe Kapitel 1.3.1.7	Ein zusätzlicher Test der im

		AuthBlock dargestellt wird. Dieser wird jedoch nur dargestellt, wenn die Online-Applikation nicht SSO unterstützt, da ansonst der SSO AuthBlock verwendet wird.
bPk/wbPk ausblenden	True/False	Blendet für diese Online-Applikation die bPk/wbPK im Authblock aus.
Login-Fenster Konfiguration		Diese Menüpunkt bietet zusätzliche Einstellungen für eine Anpassung der Bürgerkartenauswahl welche von MOA-ID 2.0 generiert wird.

1.3.3 Import und Export von XML Konfigurationen

Über diese Funktionalität besteht die Möglichkeit eine bestehende MOA-ID 1.5.1 Konfiguration in MOA-ID 2.0 zu importieren. Zusätzlich ist es möglich die MOA-ID 2.0 Konfiguration in ein XML Dokument zu exportieren oder in eine bestehende MOA-ID 2.0 XML Konfiguration zu importieren.

Hierbei ist jedoch zu beachten dass bei einem Import die aktuell vorhandene Konfiguration vollständig gelöscht und durch die importierte Konfiguration ersetzt wird. Es wird empfohlen ein Backup einer eventuell vorhandenen MOA-ID 2.0 Konfiguration zu erstellen, bevor eine neue Konfiguration importiert wird. Hierfür kann die Exportfunktion verwendet werden.

Nähere Informationen zur Migration einer MOA-ID 1.5.1 Konfiguration auf die neue MOA-ID 2.0 Konfiguration finden Sie in Kapitel 3.

1.4 Einsprungspunkte

MOA-ID 1.9.95-SNAPSHOT bietet zusätzlich zu MOA-ID 1.5.1 noch folgende Endpunkte an (als Prefix fuer all diese Endpunkt dient die unter „idp.public.url“ definierte URL):

- pvp2/metadata: Unter dieser URL stellt MOA-ID die SAML2 Metadaten zur Verfuegung
- pvp2/redirect: Dieser Endpunkt bietet das Redirect Binding in SAML2 an. Dieser Endpunkt ist auch in den Metadaten angeführt.
- pvp2/post: Dieser Endpunkt bietet das Post Binding in SAML2 an. . Dieser Endpunkt ist auch in den Metadaten angeführt.
- LogOut: Dieser Endpunkt bietet eine LogOut Funktionalität für Single Sign-On. Es kann ein URL als http-GET Parameter (?redirect=http://demo…..) übergeben an.

Wird eine URL Übergeben erfolgt nach der LogOut Operation ein Redirect auf angegebene Seite. (Beispiel: https://labda.iaik.tugraz.at:8443/moa-id-auth/LogOut?redirect=https://labda.iaik.tugraz.at:5553/demologin/)

- MonitoringServlet: Dieser Endpunkt bietet eine Monitoring Funktionalität für MOA-ID. Hierfür muss jedoch das Monitoring in der Konfiguration aktiviert werden. (Siehe Kapitel x). Werden alle implementierten Tests erfolgreich abgearbeitet antwortet das Servlet mit http Statuscode 200. Sollte während des Testvorgangs ein Fehler aufgetreten sein antwortet das Service mit http Statuscode 500 und liefert zusätzlich eine Fehlerbeschreibung mit.

2 MOA-ID Konfigurationstool

Hierbei handelt es sich ebenfalls um eine Java basierte Web-Applikation. Die Datei *moa-id-configuration.war* ist in den *webpps* Ordner des jeweiligen Tomcat zu kopieren. (Erfolgreiche Tests mit Tomcats in den Versionen 6 und 7).

Diese Hauptkonfigurationsdatei liegt im Ordner /conf/ und wird mit Hilfe der Umgebungsvariable „moa.id.webconfig" festgelegt. Die Basiskonfiguration beinhaltet eine solche properties Datei mit dem Name „moa-id.properties" welche als Ausgangskonfiguration genutzt werden kann. Die Tabelle in Kapitel 2.1 beschreibt alle Parameter die über diese Datei gesetzt werden können

2.1 Properties

Name	Beispielswert	Beschreibung
general.login.deaktivate	true / false	Hiermit kann der Login deaktiviert oder aktiviert werden
hibernate.dialect	org.hibernate.dialect.MySQLDialect	MOA-Konfiguration Hibernate Datenbank Dialekt (aktuell mySQL)
hibernate.connection.url	jdbc:mysql://localhost/moa-id-config?charSet=utf-8&autoReconnect=true	URL zum MOA- Konfiguration Datenbank Schema
hibernate.connection.driver_class	com.mysql.jdbc.Driver	Hibernate Connection zum MOA-Konfiguration Datenbank Schema (aktuell mySQL)
hibernate.connection.username	moaconfig	Benutzername für den Zugriff zum MOA- Konfiguration Datenbank Schema
hibernate.connection.password	password	Passwort für den Zugriff zum MOA- Konfiguration Datenbank Schema
general.publicURLContext	https://demo.egiz.gv.at/moa-id-configuration/	Public URL Prefix des MOA-ID Konfigurationstools
general.mail.host		Adresse eines SMTP Servers zum Versand von Statusmeldungen
general.mail.host.port		Port des SMTP Servers (optional)
general.mail.host.username		Benutzername für den SMTP Server (optional)
general.mail.host.password		Passwort für den SMTP Server

		(optional)
general.mail.from.name		Absendername für Statusmeldungen
general.mail.from.address		Absendeadresse für Statusmeldungen
general.mail.admin.adress	thomas.lenz@egiz.gv.at	Mailadresse des Administrators
general.login.pvp2.isactive	true / false	Aktiviert den PVP2 Login für das MOA-ID Konfigurations-tool. Hierfür müssen jedoch auch
general.moaid.instance.url	https://labda.iaik.tugraz.at:8443/moa-id-auth/	URL des MOA-ID IDPs
general.login.pvp2.isactive	true /false	PVP 2.1 Authentifizierung aktivieren / deaktivieren
general.login.pvp2.idp.metadata.url	https://labda.iaik.tugraz.at:8443/moa-id-auth/pvp2/metadata	URL der MOA-ID IDP Metadaten
general.login.pvp2.idp.metadata.certificate	configs/moa_idp.crt	Signaturzertifikat der MOA-ID IDP Metadaten
general.login.pvp2.idp.metadata.entityID	https://labda.iaik.tugraz.at:8443/moa-id-auth	EntityID des MOA-ID IDP
general.login.pvp2.idp.sso.logout.url	https://labda.iaik.tugraz.at:8443/moa-id-auth/LogOut?redirect=	SSO LogOut URL des MOA-ID IDP
general.login.pvp2.metadata.entities.name	MOA-ID 2.x Configuration Tool	EnitiyName des Konfigurations-tools (Metadaten)
general.login.pvp2.keystore.url	configs/pvp.p12	Keystore mit Keys zum Signieren und Verschlüsseln
general.login.pvp2.keystore.password	123456	Keystore Passwort
general.login.pvp2.keystore.type	PKCS12	Keystoreformat
general.login.pvp2.keystore.metadata.key.alias	metadata	Alias des Signaturekeys der Metadaten
general.login.pvp2.keystore.metadata.key.password	123456	Passwort des Signaturekeys der Metadaten
general.login.pvp2.keystore.authrequest.encryption.key.alias	encryption	Alias des Keys zur Verschlüsselung der Assertion
general.login.pvp2.keystore.authrequest.encryption.key.password	123456	Passwort des Keys zur Verschlüsselung der Assertion

general.login.pvp2.keystore.authrequest.key.alias	authrequest	Alias des Keys zur Signierung des AuthRequests
general.login.pvp2.keystore.authrequest.key.password	123456	Passwort des Keys zur Signierung des AuthRequests
general.userrequests.cleanup.delay	18	Zeit zur Verifikation von Mailaddressen bei Benutzeraccountanfragen [h]

2.2 Verwendung

2.2.1 Initialiserung

Für den ersten Start muss der Login deaktiviert werden (general.login.deaktivate Property = true). Anschließend kann die Benutzerverwaltung des MOA-ID Konfigurationstools unter der folgenden Adresse aufgerufen werden, wobei die der erste Teil durch die dementsprechende Serveradresse ersetzt werden muss.

… /moa-id-configuration/secure/usermanagementInit.action

Mit Hilfe dieser Benutzerverwaltung kann ein neuer Benutzer angelegt und ein Kennwort für den Benutzer vergeben werden. Zusätzlich muss dieser Benutzer als aktiv (Benutzer ist aktiv) markiert und als Admin (Benutzer ist Admin) freigeschalten werden. Nach dem speichern wird der neu angelegte Benutzer in der Liste von vorhandenen Benutzern dargestellt.

Danach ist die Initialisierung des MOA-ID Konfigurationstools abgeschlossen und die Web-Applikation kann mit aktivierter Authentifizierung (general.login.deaktivate Property = false) neu gestartet werden.

2.2.2 Usermanagement:

Alle Benutzer die Admin–Rechte besitzen haben vollen Zugriff auf die MOA-ID Konfiguration. Benutzer ohne Admin-Rechten stehen folgende Operationen nicht oder nur eingeschränkt zur Verfügung.

- **Online-Applikationen bearbeiten:** Ein Benutzer ohne Admin-Rechte kann nur jene Online-Applikationen bearbeiten die von ihm erstellt wurden. Das bearbeiten anderer Online-Applikationen ist nicht möglich.
- **Online Applikation anlegen:** Ein Benutzer ohne Admin-Rechte kann Online-Applikationen anlegen. Die Funktionen „Online-Applikation aktivieren“ (siehe 1.3.2) steht jedoch nicht zur Verfügung. Somit muss die Online-Applikation von

einem Admin aktiv geschalten werden. Zusätzlich kann die Funktion „Zusätzliche Userabfrage“ (siehe 1.3.2.5) nicht deaktiviert werden.

- **Benutzerverwaltung:** Ein Benutzer ohne Admin-Rechte kann keine neuen Benutzer erstellen. Dieser kann jedoch seinen Benutzeraccount bearbeiten und gegeben falls löschen. Beim Löschen eines Benutzeraccounts werden Online-Applikationen die von diesem erstellt wurden jedoch nicht automatisch gelöscht.

3 Installation MOA-ID und MOA-ID Konfigurationstool

Die nachfolgende Aufstellung beschreibt die einzelnen Installationsschritte einer MOA-ID 2.0 Instanz und des MOA-ID Konfigurationstools.

3.1 Schritte

3.1.1 Installation des JDK

Für den Betrieb ist eine JDK in der Mindestversion 1.5 erforderlich. Es wird jedoch eine aktuelle JDK Version empfohlen. MOA-ID und das MOA-ID Konfigurationstool wurden erfolgreich mit JDK Versionen 1.6 und 1.7 getestet. Installieren Sie eine JDK in ein von Ihnen gewähltes Verzeichnis. Das Wurzelverzeichnis wird in weiterer Folge $JAVA_HOME bezeichnet.

3.1.2 Installation von TOMCAT

Installieren sie einen TOMCAT in ein von ihnen gewähltes Verzeichnis. Das Tomcat Wurzelverzeichnis wird im weiteren Verlauf als $CATALINA_HOME bezeichnet. MOA-ID und das MOA-ID Konfigurationstool wurden erfolgreich mit den Tomct Versionen 6 und 7 getestet.

3.1.3 Installation der IAIK JCE

Die Dateien aus dem Verzeichnis *ext* im Pre-Release Packet müssen in das Verzeichnis $JAVA_HOME/jre/lib/ext kopiert werden. Zusätzlich müssen die sogenannten Unlimited Strength Jurisdiction Policy Files für die verwendete Java Version heruntergeladen, entpackt und ins Verzeichnis $JAVA_HOME/jre/lib/securtiy kopiert werden.

3.1.4 Installation einer Datenbank

Für den Betrieb von MOA-ID 2.0 wird eine Datenbank empfohlen. Als Datenbank wird mySQL empfohlen (wurde mit mySQL getestet), der Einsatz eines alternativen Datenbanksystems ist jedoch ebenfalls möglich. Für den Betrieb werden zwei getrennte Datenbank Schema benötig, da die Konfiguration und die Session Informationen getrennt abgelegt werden. Erstellen Sie zwei Datenbank Schemas welche von MOA-ID verwendet werden sollen. Deren Namen können z.B. auf *moa-id-session* für Sessiondaten und *moa-id-config* für die Konfiguration lauten. Beliebige andere Namen für die Datenbank Schema sind jedoch auch möglich.

3.1.5 Konfiguration des Tomcat

Das Pre-Release Packet enthält zwei weitere Verzeichnisse welche in weiterer Folge als $MOA_ID, darin sind alle MOA-ID spezifischen Dateien enthalten, und als $MOA_ID_CONFIG bezeichnet werden.

- Kopieren Sie die Datei $MOA_ID/moa-id-auth.war in das Verzeichnis $CATALINA_HOME/webapps.
- Kopieren Sie die Datei $MOA_ID_CONFIG/moa-id-configuration.war in das Verzeichnis $CATALINA_HOME/webapps
- Kopieren Sie den Inhalt von $MOA_ID/conf/ nach $CATALINA_HOME/conf
- Kopieren Sie den Inhalt von $MOA_ID_CONFIG/conf/ nach $CATALINA_HOME/conf
- Die endorsed Libraries für Tomcat müssen aus dem Verzeichnis *endorsed* im Pre-Release Packet in das Verzeichnis $CATALINA_HOME/endorsed kopiert werden.
- Folgende JAVA System Properties sind mindestens zu setzten
    - moa.id.configuration
      Pfad zur MOA-ID Konfiguration. ($CATALINA_HOME\conf\moa-id\moa-id.properties)
    - moa.spss.server.configuration
      Pfad zur MOA-SPSS Konfiguration ($CATALINA_HOME\conf\moa-spss\MOASPSSConfiguration.xml)
    - moa.id.webconfig
      Pfad zur MOA-ID Konfigurationstool Konfiguration ($CATALINA_HOME\conf\moa-id-config\moa-id.properties
- Alle weiteren Einstellungsparameter sind identisch zu MOA-ID 1.5.1 und können dieser Konfigurationsbeschreibung entnommen werden. (z.B. SSL Parameter, …)

3.1.6 Konfiguration von MOA-ID

Die Datei $CATALINA_HOME\conf\moa-id\moa-id.properties enthält die Basiskonfiguration für MOA-ID. Passen Sie diese Konfiguration nach Ihren Gegebenheiten an. Eine Beschreibung der einzelnen Konfigurationsparameter finden Sie in Kapitel 1.2.1.

3.1.7 Konfiguration des MOA-ID Konfigurationstools

Die Datei $CATALINA_HOME\conf\moa-id-config\moa-id.properties enthält die Basiskonfiguration für das MOA-ID Konfigurationstool. Passen Sie diese Konfiguration nach Ihren Gegebenheiten an. Eine Beschreibung der einzelnen Konfigurationsparameter finden Sie in Kapitel 2.1.

3.1.8 Initialisierung des MOA-ID Konfigurationstools

Nachdem alle Basiseinstellungen abgeschlossen sind kann die restliche Konfiguration mittels des MOA-ID Konfigurationstools erfolgen. Nach dem Start der Tomcat Instanz kann wie in Kapitel 2.2.1 beschrieben das Konfigurationstool initialisiert und ein neuer Benutzer angelegt werden. Anschließend kann die Authentifizierung am

Konfigurationstool wieder aktiviert und das Tool zur Konfiguration von MOA-ID 2.0 verwendet werden.

3.2 Konfiguration der MOA-ID Instanz

Für die Konfiguration der MOA-ID Instanz mittels des Konfigurationstools stehen zwei Varianten zur Verfügung. Die MOA-ID Instanz kann entweder von Grund auf neu konfiguriert werden oder es kann eine bestehende MOA-ID 1.5.1 Konfiguration importiert werden.

3.2.1 Neue Konfiguration anlegen

Wenn keine bestehende Konfiguration importiert wird kann direkt mit der Konfiguration der neuen Instanz begonnen werden. Zuerst ist die allgemeine MOA-ID Konfiguration laut Kapitel 1.3.1 zu erstellen. Danach können die gewünschten Online-Applikation laut Kapitel 1.3.2 eingetragen werden. Nach einer Änderung der allgemeinen Konfiguration muss die MOA-ID Instanz neu gestartet werden.

3.2.2 Migrationsstrategie von 1.5.1 auf 2.0

Es besteht auch die Möglichkeit eine bestehende MOA-ID 1.5.1 Konfiguration zu importieren. Da nicht alle neuen Konfigurationsparameter automatisiert aus der MOA-ID 1.5.1 Konfiguration erstellt werden können sind mehrere Schritte notwendig.

1. Importieren einer bestehenden MOA-ID 1.5.1 Konfiguration mithilfe der Import Funktion des MOA-ID Konfigurationstools. Danach sollte sowohl die allgemeine Konfiguration als auch die Online-Applikationen eingetragen sein.
2. Überprüfen ob bei den Online-Applikationen die korrekten BKU URLs eingetragen wurden. (siehe Kapitel 1.3.2.3). Sollten die BKU URLs korrekt sein kann mit Schritt 4 fortgesetzt werden.
3. Sollten die BKU-URLs der Online-Applikationen nicht korrekt importiert worden sein können in der allgemeinen Konfiguration die DefaultBKUs (siehe Kapitel 1.3.1.1) gesetzt werden. Wenn anschließend die bestehende MOA-ID 1.5.1 Konfiguration erneut importiert wird, werden diese DefaultBKUs bei den Online-Applikationen eingetragen.
4. Allgemeine Konfiguration: Folgende Punkte der allgemeinen Konfiguration müssen auf jeden Fall kontrolliert und eventuell angepasst werden.
    1. SecurityLayer Request Templates (siehe Kapitel 1.3.1.2)
    2. Single Sign-On Einstellungen (siehe Kapitel 1.3.1.7)
    3. PVP2 Konfiguration
    4. SecurtiyLayer Transformation: Sollte die SecurityLayer Transformation (siehe Kapitel 1.3.1.9) nicht korrekt importiert worden sein (Dateiname ist leer) so muss diese neu hochgeladen werden. Die korrekte Transformation

befindet sich im Verzeichnis ($CATALINA_HOME\conf\moa-id-config\transforms\TransformsInfoAuthBlockTable_DE_new.xml)

5. Online-Applikationen: Je nachdem welche Authentifizierungsprotokolle verwendet werden oder wenn Single Sign-On nicht unterstützen werden soll sind Änderungen an der Online-Applikationskonfiguration erforderlich. Hierfür die jeweilige Online-Applikation aus der Liste der Online-Applikationen auswählen und die jeweiligen Parameter anpassen.
    1. Single Sign-On: Standardmäßig ist Single Sign-On aktiviert. Nähere Details zur SSO Konfiguration finden Sie in Kapitel 1.3.2.5.
    2. PVP2 Konfiguration: Soll für die Authentifizierung das PVP2.1 Protokoll verwendet werden, so müssen die PVP2 spezifischen Parameter bei der jeweiligen Online-Applikation eingetragen werden. Nähere Details zu den PVP2 Parametern finden Sie in Kapitel 1.3.2.7.
6. Wenn alle Änderungen und Anpassungen abgeschlossen wurden muss die MOA-ID Instanz neu gestartet werden. Anschließend sollte eine Anmeldung an MOA-ID 2.0 für die registrierten Online-Applikationen bereits möglich sein.

Dokumentenhistorie

Version	Datum	Autor(en)	Anmerkung
0.1	27.06.2013	Andreas Fitzek	Initial Version
0.2	07.08.2013	Thomas Lenz	SSO, Database, Konfigurationstool
0.3	06.09.2013	Thomas Lenz	OA spezifische SL Templates, Monitoring Servlet
0.4	03.10.2013	Thomas Lenz	Um neue Funktionalität erweitert
0.5	04.11.2013	Thomas Lenz	Um neue Funktionalität erweitert
0.6	15.11.2013	Thomas Lenz	PreRelease 1.9.97
0.7	29.01.2014	Thomas Lenz	PreRelease 1.9.98

Referenzen

[MOA-DOC] http://joinup.ec.europa.eu/site/moa-idspss/