Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-SIT

Seidlgasse 22 / 9, 1030 Wien
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

Inffeldgasse 16a, 8010 Graz
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461 ZVR: 948166612 UID: ATU60778947

MS-SPECIFIC EIDAS NODE KONFIGURATION

Version 1.1 vom 05.04.2022
Thomas Lenz – thomas.lenz@egiz.gv.at
Thomas Zefferer – thomas.zefferer@a-sit.at

Inhaltsverzeichnis

1. Konfiguration

Dieses Dokument beschreibt Konfigurationsparameter des österreichspezifischen eIDAS Connector.

1.1. Allgemeine Hinweise zur Konfiguration

Die nachfolgenden Kapitel beschreiben allgemeine Konfigurationsrichtlinien für den österreichspezifischen eIDAS Connector.

1.1.1. Referenzen auf Dateien und Verzeichnisse

Pfade auf Dateien und Verzeichnisse werden als relativ zum jeweilig in der Konfiguration angegebenen configRootDirectory interpretiert sofern diese nicht mit *file:* beginnen.

Beispiele:

ConfigRootDirector: eidas.ms.core.configRootDir=file:/test/config/

Konfigurationspfad	Absoluter Pfad über den die Ressource geladen wird
gui/templates/	file:/test/config/gui/templates/
/gui/templates/	file:/test/config/gui/templates/
file:/gui/templates/	file:/gui/templates/
file:/gui/test/test1.html	file:/gui/test/test1.html
gui/test/test1.html	file:/test/config/gui/test/test1.html

1.1.2. Öffentliche Endpunkte am MS-Connector

Der MS-Connector stellt öffentliche benötigte Services an folgenden End-Punkten zur Verfügung.

Endpunkt	Beschreibung
/pvp/metadata	SAML2 Metadaten des MS-Connector
/pvp/post	SAML2 POST-Binding Endpunkt des MS-Connector
/pvp/redirect	**SAML2 Redirect-Binding Endpunkt des MS-Connector**
/myHomeCountry	Endpunkt für Länderauswahl
/eidas/light/sp/post	Endpunkte für Kommunikation mit eIDAS Referenzimplementierung
/eidas/light/sp/redirect	Endpunkte für Kommunikation mit eIDAS Referenzimplementierung
/actuator/*	Spring Actuator HealthCheck und Infos

1.2. Konfigurationsparameter

Die Applikation im ‚war' enthält eine Basiskonfiguration mit Defaultwerten diese ist jedoch von sich aus nicht lauffähig. Eine Standardkonfiguration befindet sich im Verzeichnis config/ des Releasepacket.
Die Pfad zur Konfiguration muss mittels Java SystemD Parameter
-Deidas.ms.configuration=/path/to/configuration
festgelegt werden.

Die Anwendungskonfiguration mit minimal erforderlichen Konfigurationsparametern befindet sich unter config/default_config.properties. Nachfolgend sind alle möglichen Konfigurationsparameter im Detail beschrieben.

Der Applikation ist eine intere Logging-Konfiguration beigelegt welche auf Systemkonsole des Applikationsservers schreibt. Eine externe Loggingkonfiguration kann mittels Java SystemD Parameter -Dlogging.config=file:/path/to/configuration/logback_config.xml festgelegt werden.

1.2.1. SpringBoot Module

Name	Wert(e)	Beschreibung
spring.application.name	**Default:** ms_connector	Applikationsname
spring.boot.admin.client.enabled	true / false **Default:** false	Aktiviert oder deaktiviert den SpringBoot Admin Client

1.2.2. Logging

Name	Wert(e)	Beschreibung
eidas.ms.core.logging.level.info.errorcodes	CSV Liste **Default:** auth.21	Liste von CSV getrennten internen StatusCodes, welche im Fehlerfall anstatt mit LogLevel „INFO" anstatt „WARN" geloggt werden sollen
eidas.ms.technicallog.write.MDS.into.techlog	true / false **Default:** true	Aktiviert / Deaktivert das Logging von MDS Daten in den technischen Log
eidas.ms.revisionlog.write.MDS.into.revisionlog	true / false **Default:** true	Aktiviert / Deaktivert das Logging von MDS Daten in den Revisionslog
eidas.ms.revisionlog.logIPAddressO	true / false	Aktiviert / Deaktivert das Logging der IP

fUser	**Default:** true	Adresse der aufrufenden Stelle in den Revisionslog

1.2.3. Basiskonfigurationsparameter

Name	Wert(e)	Beschreibung
eidas.ms.context.url.prefix	https:// abcde.at/ ms_connector	URL unter welcher der MS_Connector erreichbar ist
eidas.ms.context.url.request.validation	true/false **Default:** false	Validierung ob die eingehenden http Requests dem URL Prefix des Konfigurationsparameters „eidas.ms.context.url.prefix“ entsprechen
eidas.ms.configRootDir=file:./	file:./	Absoluter Pfad, beginnend mit file:…, zum Konfigurationsverzeichnis der MS_Connector Applikation. Alle relativen Pfade werden als relativ zu diesem Pfad interpretiert.
eidas.ms.context.use.clustermode	true/false **Default:** true	Aktiviert die Legacyunterstützung des AuthHandlers, entsprechend eGovernmentgesetz vor E-ID Einführung. Ist die Legacyuntersützung aktiviert werden Handy-Signatur, XML Personenbindungen, XML AuthBlöcke, Stammzahlen, … identisch zu aktuell noch verwendeten MOA-ID Instanzen verarbeitet. Ohne Legacyunterstützung werden ausschließlich Identifikations- und Authentifizierungsinformationen entsprecht dem E-ID unterstützt.

1.2.4. Pfade auf GUI spezifische Elemente (Template, i18n, …)

Name	Wert(e)	Beschreibung
eidas.ms.webcontent.static.directory	**Default:** webcontent/	Alle in diesem Verzeichnis hinterlegten Daten werden statisch im Kontext der MS-Connector Applikation unter „/static/…“ eingebunden. Anwendungsfälle sind statische CSS, JS, oder Bilder welche in anderen Templates referenziert werden.
eidas.ms.webcontent.templates	**Default:** templates/	In diesem Verzeichnis sind Templates für alle dynamisch genierten HTML GUI des MS-Connector hinterlegt. Diese Templates werden im Anmeldeprozess dynamisch geladen und verarbeitet
eidas.ms.webcontent.properties	**Default:** properties/messages	Dieses Verzeichnis stellt die primäre Quelle für Message Properties für i18n (Multi-Langure) Unterstützung dar und Umfasst ein Minimalset an Properties für Deutsch und Englisch. **Hinweis:** Alle Properties welche nicht in über dieses Verzeichnis aufgelöst werden können werden entsprechend den in der Applikation hinterlegten Default Properties auf Englisch verarbeitet
eidas.ms.webcontent.templates.countryselection	**Default:** countrySelection.html	Definiert den Namen des GUI Templates für die Länderauswahl

1.2.5. Validierung von Einmalzugriffstoken (PendingRequestIDs)

Name	Wert(e)	Beschreibung
eidas.ms.core.pendingrequestid.maxlifetime	Default: 300	Dieser Parameter definiert den Gültigkeitszeitraum des Einmalzugriffstoken während eines laufenden Prozesses in Sekunden. Nach

		einmaliger Verwendung wird das Token durch den widerrufen.
eidas.ms.core.pendingrequestid.digist.algorithm	**Default:** HmacSHA256	Algorithmus zur Integritätssicherung von PendingRequestIds
eidas.ms.core.pendingrequestid.digist.secret	pendingReqIdSecret	Secret zur Generierung und Validierung von Einmalzugriffstoken. **Hinweis:** Wird der MS-Connector im Cluster betrieben (mehr als eine Instanz) muss dieser Parameter auf allen Instanzen des MS-Connector identisch sein.

1.2.6. eIDAS Node Integration

Name	Wert(e)	Beschreibung
eidas.ms.auth.eIDAS.eid.testidentity.default	true / false **Default:** false	Wenn *true*, wird die eIDAS Identität als Test-Identität entsprechend dem national verwendeten PVP2 Attribute-Profil und dem Attribute EID-IDENTITY-STATUS-LEVEL markiert. **Hinweis:** In Hinblick auf das Staging im ID Austria System sollte dem eIDAS Test-System Test-Identitäten und dem eIDAS Prod.-System Identitäten auf Produktionslevel zugeordnet werden.
eidas.ms.auth.eIDAS.node_v2.entityId	**Default:** ownSpecificConnector	Name des MS-Connectors in der Kommunikation mit dem eIDAS Node aus der Referenzimplementierung
eidas.ms.auth.eIDAS.node_v2.forward.endpoint		Endpunkt des eIDAS Nodes der Referenzimplementierung an welchen der Anmeldeprozess nach der Länderauswahl weitergeleitet wird
eidas.ms.auth.eIDAS.node_v2.forward.method	GET / POST **Default:** POST	HTTP Methode welche zur Weiterleitung an den eIDAS Node verwendet wird
eidas.ms.auth.eIDAS.node_v2.countrycode	**Default:** AT	Ländercode des MS-Connector Betreibers
eidas.ms.auth.eIDAS.node_v2.publicSectorTargets	**Default:** urn:publicid:gv.at:cdid\+.*	RegEx zur Unterscheidung von öffentlichen / private Service-Providern auf Basis des im MS-Connector Request übermittelten bPK Bereichs des Service-Providers. Alle SP's welche auf diese RegEx matchen werden als Public markiert
eidas.ms.auth.eIDAS.node_v2.workarounds.useRequestIdAsTransactionIdentifier	true / false **Default:** true	Falls Active wird die SAML2 RequestId zur Sessionsyncronisation verwendet. Ansonsten der SAML2 RelayState. **Hinweis:** Aktiv wegen fehlerhafter Unterstützung von SAML2 Relaystate auf machen eIDAS Nodes
eidas.ms.auth.eIDAS.node_v2.requesterId.useHashedForm	true / false **Default:** true	Die eIDAS Spezifikation 1.2 fordert die Übertragung eines eindeutigen SP Identifier für private Service-Provider. Falls aktiv wird der Sha256 Hash des eindeutigen SP Identifiers anstatt des Plaintext Identifiers als RequesterId verwendet.
eidas.ms.auth.eIDAS.node_v2.requesterId.lu.useStaticRequesterForAll	true / false **Default:** true	Aktiviert / Deaktiviert die Verwendung einer statischen „RequesterID" und „ProviderName" für alle Requests an LU. **Hinweis:** Da bei LU in die Generierung des PersonalIdentifier ProviderName/RequesterId einfließen ist ohne statischen Wert kein Matching möglich
eidas.ms.auth.eIDAS.node_v2.workarounds.addAlwaysProviderName	true / false **Default:** false	Setzt den „ProviderName" bei allen Requests (öffentliche und private Sps). **Hinweis:** War erforderlich a manche eIDAS Nodes diesen Parameter als „required" markiert hatten ob es in der

		eIDAS Spezifikation nicht vorgesehen war.
eidas.ms.auth.eIDAS.node_v2.loa.requested.minimum	**Default:** http://eidas.europa.eu/LoA/high	Mindest LoA welcher für die Authentifizierung erforderlich ist.
eidas.ms.auth.eIDAS.node_v2.requested.nameIdFormat	**Default:**null	SAML2 NameIdFormat welches für die Anfrage an ausländische eIDAS Proxy-Services verwendet wird.

1.2.7. SZR Anbindung

Name	Wert(e)	Beschreibung
eidas.ms.auth.eIDAS.szrclient.useTestService	true / false	Aktiviert/ Deaktiviert die Verwendung des SZR Testsystems
eidas.ms.auth.eIDAS.szrclient.endpoint.prod		URL auf das SZR Produktivsystem
eidas.ms.auth.eIDAS.szrclient.endpoint.test		URL auf das SZR Testsystem
eidas.ms.auth.eIDAS.szrclient.ssl.keyStore.path		Pfad zum Software KeyStore, welcher für sie SSL Client Authentifizierung am SZR verwendet werden soll
eidas.ms.auth.eIDAS.szrclient.ssl.keyStore.password		Passwort des KeyStores für die SSL Client Authentifizierung
eidas.ms.auth.eIDAS.szrclient.ssl.trustStore.path		Pfad zum Software KeyStore (jks) der als TrustStore für SSL Serverzertifikate des SZR verwendet werden soll
eidas.ms.auth.eIDAS.szrclient.ssl.trustStore.password		Passwort für den Zugriff auf den TrustSTore
eidas.ms.auth.eIDAS.szrclient.timeout.connection	Sekunden **Default:** 15	Connection Timeout für den Zugriff auf das SZR
eidas.ms.auth.eIDAS.szrclient.timeout.response	Sekunden **Default:** 30	Response Timeout bei SZR Zugriff
eidas.ms.auth.eIDAS.szrclient.params.vkz		Verfahrenskennzeichen falls die bPK des Benutzes via SZR abgefragt werden soll. **Hinweis:** Diese Funktion wird mit der Umstellung auf den ID Austria nicht mehr benötigt.
eidas.ms.auth.eIDAS.szrclient.params.useSZRForbPKCalculation	true / false **Default:** false	Aktiviert / Deaktiviert die Berechnung der bPK via SZR **Hinweis:** Diese Funktion wird mit der Umstellung auf den ID Austria nicht mehr benötigt.
eidas.ms.auth.eIDAS.szrclient.eidasbind.mds.inject	true / false **Default:** false	Aktiviert / Deaktiviert das Einfügen des MDS in die “eidasBind” falls die Anmeldung im ID Austria Mode erfolgt **Hinweis:** Ist nach Produktivsetzung des ID Austria nicht mehr erforderlich.
eidas.ms.auth.eIDAS.szrclient.workarounds.eidmapping.revisionlog.active	true / false **Default:** true	Aktiviert / deaktiviert das Logging von konvertierten PersonalIdentifier im Revisionslog **Hinweis:** DE PersonalIdentifier werden aktuell konvertiert da es im ERnP eine Längenbeschränkung auf 54 Zeichen gibt
eidas.ms.auth.eIDAS.szrclient.workarounds.use.getidentitylink.for.ida	true / false **Default:** true	Aktiviert / deaktiviert den Workaround für die Eintragung in das ERnP im ID Austria Betriebsmodus. Falls aktiv erfolgt die Eintragung in das ERnP via SZR auf unter Verwendung der Operation getIdentitylinkEidas
eidas.ms.auth.eIDAS.szrclient.params.setPlaceOfBirthIfAvailable	true / false **Default:** true	Aktiviert / deaktiviert die Übermittlung von eIDAS PlaceOfBirth als PersionInfo an das SZR
eidas.ms.auth.eIDAS.szrclient.params.setBirthNameIfAvailable	true / false **Default:** true	Aktiviert / deaktiviert die Übermittlung des eIDAS BirthName als PersionInfo an das SZR
eidas.ms.auth.eIDAS.szrclient.debug.logfullmessages	true / false **Default:** false	Aktiviert / deaktiviert das Logging der vollen SZR Kommunikation.

		Hinweis: hierfür muss auch der Logger auf der Klasse *at.asitplus.eidas.specific.modules.auth.eidas.v2.utils.LoggingHandler* auf 'trace' liegen.
eidas.ms.auth.eIDAS.szrclient.debug.useDummySolution	true / false **Default:** false	Aktiviert / deaktiviert das SZR Dummy **Hinweis:** NUR FÜR REINES ENTWICKLUNGS-SETUP

1.2.8. eIDAS Requested Attributes

Name	Wert(e)	Beschreibung
eidas.ms.auth.eIDAS.node_v2.attributes.requested.onlynatural.{index}	CSV aus 'Attribute-FriendlyName' und 'isRequired' flag	Set von Attributen welche Allgemein angefragt werden, bestehend aus FriendlyName des eIDAS Attributes und einem Flag (true/false) ob das Attribute verpflichtend oder Optional ist. 1. {index} Eindeutiger Index (z.B. 0, 1, ...)
eidas.ms.auth.eIDAS.node_v2.attributes.requested.{countryCode}.onlynatural.{index}	CSV aus 'Attribute-FriendlyName' und 'isRequired' flag	Set von Attributen welche welche für ein spezifisches Land zusätzlich angefragt werden, bestehend aus FriendlyName des eIDAS Attributes und einem Flag (true/false) ob das Attribute verpflichtend oder Optional ist. 2. {index} Eindeutiger Index (z.B. 0, 1, ...) 3. {countryCode} LänderCode (z.B. de)
eidas.ms.auth.eIDAS.node_v2.attributes.requested.representation.{index}	CSV aus 'Attribute-FriendlyName' und 'isRequired' flag	Set von Attributen welche Allgemein bei Vertretungen angefragt werden, bestehend aus FriendlyName des eIDAS Attributes und einem Flag (true/false) ob das Attribute verpflichtend oder Optional ist. 4. {index} Eindeutiger Index (z.B. 0, 1, ...)

1.2.9. ID Austria – AuthBlock

Name	Wert(e)	Beschreibung
eidas.ms.auth.eIDAS.authblock.keystore.type	jks / pkcs12	Definiert den Keystore Type welcher zur Signatur des ID Austria AuthBlocks verwendet werden soll
eidas.ms.auth.eIDAS.authblock.keystore.path	keys/ authblock.jks	Pfad zum Software KeyStore im Falle von ‚jks' oder ‚pkcs12' KeyStoretypen.
eidas.ms.auth.eIDAS.authblock.keystore.password	password	Password des Software KeyStores im Falle von ‚jks' oder ‚pkcs12' KeyStoretypen.
eidas.ms.auth.eIDAS.authblock.key.alias	metadata	Name des Schlüssels im KeyStore welcher zur Signatur des ID Austria AuthBlocks verwendet wird.
eidas.ms.auth.eIDAS.authblock.key.password	password	Passwport des Schlüssels im KeyStore welcher zur Signatur des ID Austria AuthBlocks verwendet wird.

1.2.10. SAML2 Endpunkt für ID Austria und MOA-ID

Name	Wert(e)	Beschreibung
eidas.ms.pvp2.keystore.type	jks / pkcs12	Definiert den Keystore Type welcher für SAML2 Kommunikation verwendet werden soll
eidas.ms.pvp2.keystore.path	keys/junit.jks	Pfad zum Software KeyStore im Falle von ‚jks' oder ‚pkcs12' KeyStoretypen.
eidas.ms.pvp2.keystore.password	password	Password des Software KeyStores im Falle von ‚jks' oder ‚pkcs12' KeyStoretypen.
eidas.ms.pvp2.key.metadata.alias	metadata	Name des Schlüssels im KeyStore welcher zur Erstellung von signierten SAML2 Metadaten verwendet wird.

eidas.ms.pvp2.key.metadata.password	password	Passwport des Schlüssels im KeyStore welcher zur Erstellung von signierten SAML2 Metadaten verwendet wird.
eidas.ms.pvp2.key.signing.alias	sign	Name des Schlüssels im KeyStore welcher zur Signatur von SAML2 Respones des zentralen eIDAS Knoten verwendet wird. **Hinweis:** Das Zertifikat zu diesem Schlüssel ist in den SAML2 Metadaten hinterlegt.
eidas.ms.pvp2.key.signing.password	password	Passwort des Schlüssels im KeyStore welcher zur Signatur von SAML2 Respones verwendet wird.
eidas.ms.pvp2.metadata.validity	xx [Stunden] **Default:** 24	Gültigkeitszeitraum der vom MS-Connector generierten SAML2 Metadaten
eidas.ms.configuration.pvp.scheme.validation	true / false **Default:** true	Aktiviert die XML Schemavalidierung für SAML2 Metadaten und SAML2 Requests
eidas.ms.configuration.pvp.enable.entitycategories	true / false **Default:** false	Aktiviert die Unterstützung von SAML2 EntityCategories, entsprechend dem PVP2 S-Profil
eidas.ms.pvp2.metadata.organisation.name		OrganizationName entsprechend SAML2 Metadatenspezifikation 2.3.2.1 Element <Organisation>
eidas.ms.pvp2.metadata.organisation.friendyname		OrganizationDisplayName entsprechend SAML2 Metadatenspezifikation 2.3.2.1 Element <Organisation>
eidas.ms.pvp2.metadata.organisation.url		OrganizationURL entsprechend SAML2 Metadatenspezifikation 2.3.2.1 Element <Organisation>
eidas.ms.pvp2.metadata.contact.givenname		GivenName entsprechend SAML2 Metadatenspezifikation 2.3.2.2 Element <ContactPerson> **Hinweis:** Als <contactType> wird immer ‚technical' gesetzt.
eidas.ms.pvp2.metadata.contact.surname		SurName entsprechend SAML2 Metadatenspezifikation 2.3.2.2 Element <ContactPerson> **Hinweis:** Als <contactType> wird immer ‚technical' gesetzt.
eidas.ms.pvp2.metadata.contact.email		EmailAddress entsprechend SAML2 Metadatenspezifikation 2.3.2.2 Element <ContactPerson> **Hinweis:** Als <contactType> wird immer ‚technical' gesetzt.

1.2.11. Erglaubte ID Austria und MOA-ID Instanzen

Neue Service Provider können einfach durch das Einfügen eines Sets von Konfigurationseigenschaften hinzugefügt werden. Das x in eidas.ms.sp.x.uniqueID muss ersetzt werden, um eine eindeutige Id für dieses Set von Konfigurationswerten zu erhalten.

Name	Required	Beschreibung
eidas.ms.sp.x.uniqueID=http://test.com/test	X	(Eindeutige Id wie SAML2 EntityId)
eidas.ms.sp.x.pvp2.metadata.truststore	X	Pfad zum Software KeyStore (jks) der als TrustStore zur Validierung des SAML2 Metadatensignaturzertifikats dieses SP verwendet werden soll
eidas.ms.sp.x.pvp2.metadata.truststore.password	X	Passwort für den Zugriff auf den TrustStore
eidas.ms.sp.x.friendlyName		FriendlyName für diese SP sofern dieser nicht via SAML2 Request übermittelt wird
eidas.ms.sp.x.pvp2.metadata.url		URL auf die SAML2 Metadaten des SP falls diese nicht mit der uniqueID übereinstimmt

eidas.ms.sp.x.policy.allowed.requested.targets		RegEx mit erlaubten bPK Bereichen für diesen SP **Hinweis:** Defaultmäßig sind alle Bereiche zulässig
eidas.ms.sp.x.policy.hasBaseIdTransferRestriction	true / false **Default:** true	Erlaubt das Ausliefern der Stammzahl an die MOA-ID Instanz des SP.
eidas.ms.sp.x.newEidMode	true / false **Default:** false	Aktiviert den ID Austria Mode für diesen SP. In diesem Fall werden anstatt der XML Personenbindung und der Stammzahl, ein eidasBind und ein technischer AuthBlock an den SP übermittelt

2. Änderungsübersicht

Datum	Beschreibung	Autor
20.01.2021	Initialversion für MS-Connector 1.2.0	Thomas Lenz
12.05.2021	Finialisierung für MS-Connector 1.2.0	Thomas Lenz
25.06.2021	Konfiguration für NameIdFormat erweitert	Thomas Lenz
05.04.2022	Finalisierung für MS-Connector 1.2.4	Thomas Lenz