

MS-SPECIFIC EIDAS NODE KONFIGURATION

Version 1.6.0 vom 22.05.2024

Thomas Lenz – thomas.lenz@egiz.gv.at

Thomas Zefferer – thomas.zefferer@a-sit.at

Inhaltsverzeichnis

Inhaltsverzeichnis	1
1. Konfiguration	1
1.1. Allgemeine Hinweise zur Konfiguration	1
1.2. Konfigurationsparameter	2
2. Änderungsübersicht	7

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
/sp/idaustria/metadata	SAML2 Metadaten des ID Austria Clients im MS-Connector
/sp/idaustria/post	SAML2 POST-Binding Endpunkt des ID Austria Clients im MS-Connector
/sp/idaustria/redirect	SAML2 Redirect-Binding Endpunkt des ID Austria Clients im MS-Connector
/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 Releasepaket.

Die Pfad zur Konfiguration muss mittels Java SystemD Parameter

- `-Deidas.ms.configuration=/path/to/configuration`

festgelegt werden.

Für die Kommunikation mit dem eIDAS Node benötigt das MS-Proxy-Service auch eine Referenz auf die eIDAS Node Konfiguration. Der hierfür benötigte Konfigurationsteil aus der eIDAS Node ist ebenfalls in der Standardkonfiguration im Verzeichnis config/eIDAS/ beigelegt. Der Pfad zu dieser Konfiguration muss mittels der JAVA SystemD Parameter:

- `-DSPECIFIC_CONNECTOR_CONFIG_REPOSITORY=/path/to/configuration/eIDAS/`

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	Aktiviert oder deaktiviert den SpringBoot

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.int o.techlog	true / false Default: true	Aktiviert / Deaktiviert das Logging von MDS Daten in den technischen Log
eidas.ms.revisionlog.write.MDS.int o.revisionlog	true / false Default: true	Aktiviert / Deaktiviert das Logging von MDS Daten in den Revisionslog
eidas.ms.revisionlog.logIPAddressO fUser	true / false Default: true	Aktiviert / Deaktiviert das Logging der IP 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.validat ion	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 den Clusterbetriebsmode
eidas.ms.core.error.handling.config	Default: ./misc/misc/err or_conf.yaml	Pfad auf die Mapping-Tabelle zur Konfiguration des zentralen Fehlerhändlings. Diese Konfiguration bietet folgende Parameter: <ul style="list-style-type: none"> • Mapping von internen auf externe Fehlercodes. Die externen FehlerCodes sind jene die dem SP oder dem Benutzer auf der Fehlerseite angezeigt werden. • Erstellung von Fehlertickets für interne Fehlercodes • Konfiguration von LogLevels i zentralen Fehlerhändling für interne Fehlercodes

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

Name	Wert(e)	Beschreibung
eidas.ms.webcontent.static.director y	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 generierten HTML GUI des MS-Connector hinterlegt. Diese Templates werden im Anmeldeprozess dynamisch geladen und verarbeitet
eidas.ms.webcontent.properties	Default:	Dieses Verzeichnis stellt die primäre

	properties/messages	Quelle für Message Properties für i18n (Multi-Language) 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 <i>true</i> , 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.lightToken.connector.request.issuer.name	Default: specificCommunicationDefinitionConnectorRequest	Issuename für die Erstellung von Zugriffstoken für die Weiterleitung des Anmeldevorgangs vom MS-Connector an den eIDAS Node
eidas.ms.auth.eIDAS.node_v2.lightToken.connector.request.secret	Default: mySecretConnectorRequest	Passwort für die Erstellung von Zugriffstoken für die Weiterleitung des Anmeldevorgangs vom MS-Connector an den eIDAS Node Hinweis: Muss mit der Konfiguration am

eidas.ms.auth.eIDAS.node_v2.lightToken.connector.request.algorithm	Default: SHA-256	eIDAS-Node übereinstimmen Hash Algorithmus für die Erstellung von Zugriffstoken für die Weiterleitung des Anmeldevorgangs vom MS-Connector an den eIDAS Node Hinweis: Muss mit der Konfiguration am eIDAS-Node übereinstimmen
eidas.ms.auth.eIDAS.node_v2.lightToken.connector.response.issuer.name	Default: specificCommunicationDefinitionConnectorResponse	Issuername für die Erstellung von Zugriffstoken für die Rückleitung des Anmeldevorgangs vom eIDAS-Node an den MS-Connector
eidas.ms.auth.eIDAS.node_v2.lightToken.connector.response.secret	Default: mySecretConnectorResponse	Passwort für die Erstellung von Zugriffstoken für die Rückleitung des Anmeldevorgangs vom eIDAS-Node an den MS-Connector Hinweis: Muss mit der Konfiguration am eIDAS-Node übereinstimmen
eidas.ms.auth.eIDAS.node_v2.lightToken.connector.response.algorithm	Default: SHA-256	Hash Algorithmus für die Erstellung von Zugriffstoken für die Rückleitung des Anmeldevorgangs vom eIDAS-Node an den MS-Connector Hinweis: Muss mit der Konfiguration am eIDAS-Node übereinstimmen
eidas.ms.auth.eIDAS.node_v2.incoming.lightRequest.max.number.characters	Default: 65535	Maximale Anzahl von Zeichen des Request zwischen eIDAS Node der Referenzimplementierung und des MS-Connector
<i>eidas.ms.auth.eIDAS.node_v2.incoming.lightResponse.max.number.characters</i>	Default: 65535	Maximale Anzahl von Zeichen der Response zwischen eIDAS Node der Referenzimplementierung und des MS-Connector
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.proxyservices.privatesp. notsupported	Default: DE,EE,ES	Komma separierte Liste von Länderkürzel für welche eine Anmeldung von privaten Service-Providern nicht unterstützt. Die Unterstützung von privaten Service-Providern ergibt sich aus den Notifizierungsunterlagen der jeweiligen Länder und bilateral aus Tests.
eidas.ms.auth.eIDAS.node_v2.workarounds.useRequestIdAsTransactionIdentifier	true / false Default: true	Falls Active wird die SAML2 RequestId zur Sessionsynchronisation 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).

eidas.ms.auth.eIDAS.node_v2.loa.requested.minimum

Default:
http://eidas.eur
opa.eu/LoA/high

eidas.ms.auth.eIDAS.node_v2.requested.namelformat

Default: null

eidas.ms.auth.eIDAS.node_v2.requested.namelformat.
{countryCode}

Default: null

Hinweis: War erforderlich a manche eIDAS Nodes diesen Parameter als „required“ markiert hatten ob es in der eIDAS Spezifikation nicht vorgesehen war. Mindest LoA welcher für die Authentifizierung erforderlich ist.

SAML2 Namelformat welches für die Anfrage an ausländische eIDAS Proxy-Services verwendet wird.

SAML2 Namelformat welches für die Anfrage an einem länderspezifischen ausländische eIDAS Proxy-Services verwendet wird.

{countryCode} LänderCode (z.B. de)

1.2.7. Matching allgemein

Name	Wert(e)	Beschreibung
eidas.ms.auth.eIDAS.matching.byaddress.enable	true / false Default: true	Aktiviert/ Deaktiviert die Matching-Möglichkeit via Adresssuche
eidas.ms.auth.eIDAS.matching.byaddress.maxresults	Default: 250	Maximale Anzahl von angezeigten Adressen bei Adresssuche

1.2.8. SZR Anbindung

Name	Wert(e)	Beschreibung
eidas.ms.auth.eIDAS.szcclient.useTestService	true / false	Aktiviert/ Deaktiviert die Verwendung des SZR Testsystems
eidas.ms.auth.eIDAS.szcclient.endpoint.prod		URL auf das SZR Produktivsystem
eidas.ms.auth.eIDAS.szcclient.endpoint.test		URL auf das SZR Testsystem
eidas.ms.auth.eIDAS.szcclient.ssl.keystore.type	jks / pkcs12	Definiert den Keystore Type welcher für den Zugriff auf das Service verwendet werden soll Hinweis: wird kein Type angegeben so wird der KeyStore ignoriert
eidas.ms.auth.eIDAS.szcclient.ssl.keystore.path		Pfad zum Software KeyStore, welcher für die SSL Client Authentifizierung am SZR verwendet werden soll
eidas.ms.auth.eIDAS.szcclient.ssl.keystore.password		Passwort des KeyStores für die SSL Client Authentifizierung
eidas.ms.auth.eIDAS.szcclient.ssl.keystore.alias		Name des Schlüssels im KeyStore welcher für den SSL Zugriff verwendet wird.
eidas.ms.auth.eIDAS.szcclient.ssl.keystore.password		Passwort des Schlüssels im KeyStore welcher für den SSL Zugriff verwendet wird.
eidas.ms.auth.eIDAS.szcclient.ssl.truststore.type	jks / pkcs12	Definiert den Truststore Type er für die Validierung des SSL Serverzertifikate verwendet werden soll Hinweis: wird kein Type angegeben so wird der KeyStore ignoriert
eidas.ms.auth.eIDAS.szcclient.ssl.truststore.path		Pfad zum Software KeyStore (jks) der als TrustStore für SSL Serverzertifikate des SZR verwendet werden soll
eidas.ms.auth.eIDAS.szcclient.ssl.truststore.password		Passwort für den Zugriff auf den TrustStore
eidas.ms.auth.eIDAS.szcclient.timeout.connection	Sekunden Default: 15	Connection Timeout für den Zugriff auf das SZR
eidas.ms.auth.eIDAS.szcclient.timeout.response	Sekunden Default: 30	Response Timeout bei SZR Zugriff
eidas.ms.auth.eIDAS.szcclient.parameters		Verfahrenskennzeichen falls die bPK des

ms.vkz		Benutzer via SZR abgefragt werden soll. Hinweis: Diese Funktion wird mit der Umstellung auf den ID Austria nicht mehr benötigt.
eidas.ms.auth.eIDAS.szcrlclient.param.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.szcrlclient.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.szcrlclient.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.szcrlclient.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.szcrlclient.param.setPlaceOfBirthIfAvailable	true / false Default: true	Aktiviert / deaktiviert die Übermittlung von eIDAS PlaceOfBirth als PersInfo an das SZR
eidas.ms.auth.eIDAS.szcrlclient.param.setBirthNameIfAvailable	true / false Default: true	Aktiviert / deaktiviert die Übermittlung des eIDAS BirthName als PersInfo an das SZR
eidas.ms.auth.eIDAS.szcrlclient.debug.logfullmessages	true / false Default: false	Aktiviert / deaktiviert das Logging der vollen SZR Kommunikation. Hinweis: hierfür muss auch der Logger auf der Klasse <i>at.asitplus.eidas.specific.modules.auth.eidas.v2.utils.LoggingHandler</i> auf 'trace' liegen.
eidas.ms.auth.eIDAS.szcrlclient.debug.useDummySolution	true / false Default: false	Aktiviert / deaktiviert das SZR Dummy Hinweis: NUR FÜR REINES ENTWICKLUNGS-SETUP

1.2.9. ZMR Anbindung

Name	Wert(e)	Beschreibung
eidas.ms.auth.eIDAS.zmrclient.endpoint		URL auf die zu verwendete ZMR Instanz
eidas.ms.auth.eIDAS.zmrclient.ssl.keyStore.type	jks / pkcs12	Definiert den Keystore Type welcher für den Zugriff auf das Service verwendet werden soll. Hinweis: wird kein Type angegeben so wird der KeyStore ignoriert
eidas.ms.auth.eIDAS.zmrclient.ssl.keyStore.path		Pfad zum Software KeyStore, welcher für die SSL Client Authentifizierung verwendet werden soll
eidas.ms.auth.eIDAS.zmrclient.ssl.keyStore.password		Passwort des KeyStores für die SSL Client Authentifizierung
eidas.ms.auth.eIDAS.zmrclient.ssl.key.alias		Name des Schlüssels im KeyStore welcher für den SSL Zugriff verwendet wird.
eidas.ms.auth.eIDAS.zmrclient.ssl.key.password		Passwort des Schlüssels im KeyStore welcher für den SSL Zugriff verwendet wird.
eidas.ms.auth.eIDAS.zmrclient.ssl.trustStore.type	jks / pkcs12	Definiert den Truststore Type er für die Validierung des SSL Serverzertifikate verwendet werden soll. Hinweis: wird kein Type angegeben so wird der KeyStore ignoriert

eidas.ms.auth.eIDAS.zmrclient.ssl.trustStore.path		Pfad zum Software KeyStore (jks) der als TrustStore für SSL Serverzertifikate des SZR verwendet werden soll
eidas.ms.auth.eIDAS.zmrclient.ssl.trustStore.password		Passwort für den Zugriff auf den TrustStore
eidas.ms.auth.eIDAS.zmrclient.timeout.connection	Sekunden Default: 15	Connection Timeout für den Zugriff auf das ZMR
eidas.ms.auth.eIDAS.zmrclient.timeout.response	Sekunden Default: 30	Response Timeout bei ZMR Zugriff
eidas.ms.auth.eIDAS.zmrclient.request.organisation.behoerdennr		Behördennummer, welche für die Kommunikation mit dem ZMR verwendet werden soll
eidas.ms.auth.eIDAS.zmrclient.request.update.reason.code	Default: PERS_AENDERN	ZMR Code, welche für Änderungen am ZMR verwendet werden soll
eidas.ms.auth.eIDAS.zmrclient.request.update.reason.text	Default: KITT for eIDAS Matching true / false Default: false	Begründung, welche bei Änderungen am ZMR verwendet werden soll
eidas.ms.auth.eIDAS.zmrclient.debug.logfullmessages		Vollständiger Trace-Log der Anfragen und Antworten von/an das ZMR. Hinweis: hierbei muss auch das LogLevel für die Klasse: <i>at.asitplus.eidas.specific.modules.auth.eidas.v2.utils.LoggingHandler</i> auf <i>trace</i> erhöht werden.
eidas.ms.auth.eIDAS.zmrclient.request.update.with.bpk.only	true / false Default: false	Wenn aktiv, erfolgt die Identifikation einer Person im Falle eines ZMR Updates nur auf Basis der bPK-ZP. Wenn nicht aktiv, werden zusätzlich Vorname, Nachname und Geburtsdatum an das ZMR gesendet.

1.2.10. ERnP Anbindung

Hinweis: Für einen vollständigen Trace-Log der Anfragen und Antworten von/an das ERnP muss das LogLevel für die Klasse: *org.apache.http.wire* auf *debug* erhöht werden.

Name	Wert(e)	Beschreibung
eidas.ms.auth.eIDAS.ernpclient.endpoint		URL auf die zu verwendete ZMR Instanz
eidas.ms.auth.eIDAS.ernpclient.ssl.keyStore.type	jks / pkcs12	Definiert den Keystore Type welcher für den Zugriff auf das Service verwendet werden soll. Hinweis: wird kein Type angegeben so wird der KeyStore ignoriert
eidas.ms.auth.eIDAS.ernpclient.ssl.keyStore.path		Pfad zum Software KeyStore, welcher für die SSL Client Authentifizierung verwendet werden soll
eidas.ms.auth.eIDAS.ernpclient.ssl.keyStore.password		Passwort des KeyStores für die SSL Client Authentifizierung
eidas.ms.auth.eIDAS.ernpclient.ssl.key.alias		Name des Schlüssels im KeyStore welcher für den SSL Zugriff verwendet wird.
eidas.ms.auth.eIDAS.ernpclient.ssl.key.password		Passwort des Schlüssels im KeyStore welcher für den SSL Zugriff verwendet wird.
eidas.ms.client.http.connection.timeout.request	Sekunden Default: 15	Connection Timeout für den Zugriff auf das ERnP
eidas.ms.client.http.connection.timeout.socket	Sekunden Default: 30	Response Timeout bei ERnP Zugriff
eidas.ms.auth.eIDAS.ernpclient.request.organisation.behoerdennr		Behördennummer, welche für die Kommunikation mit dem ERnP verwendet werden soll
<u>eidas.ms.auth.eIDAS.ernpclient.api.person.add.gender</u>	Default: Keine Angabe	Wert des „Geschlecht“ Attributes bei Neueintragung in das ERnP. Hinweis: Der hier angegebene textuelle Wert muss mit den erlaubten Werten aus der ERnP Spezifikation übereinstimmen

1.2.11. ID Austria Anbindung für Matching

Eine mögliche Matching Variante stellt das Matching über einen bestehenden ID Austria dar. Hierfür ist eine Registrierung am ID Austria System erforderlich. Aus Sicht des MS-Connectors sind folgende Registrierungsparameter auf jeden Fall notwendig:

- Eindeutige Identifier:
 - P-Stage: https://eid.as.bmi.gv.at/ms_connector/sp/idaustria/metadata
 - T-Stage: https://eid.as-test.bmi.gv.at/ms_connector/sp/idaustria/metadata
- bPK-Bereich: ZP
- Attribute:
 - Ausstellungsland
 - Vorname (wird für öffentliche SP's per Default übertragen)
 - Familienname (wird für öffentliche SP's per Default übertragen)
 - Geburtsdatum (wird für öffentliche SP's per Default übertragen)
 - bPK (wird per Default übertragen)
 - Authentifizierungslevel des Bürgers (wird per Default übertragen)
- SAML2 Metadaten
 - Die für die Registrierung benötigten SAML2 Metadaten werden automatisch generiert und können unter den folgenden Endpunkten abgerufen werden.
 - P-Stage: https://eid.as.bmi.gv.at/ms_connector/sp/idaustria/metadata
 - T-Stage: https://eid.as-test.bmi.gv.at/ms_connector/sp/idaustria/metadata

Name	Wert(e)	Beschreibung
eid.as.modules.idaustriaclient.keystore.type	jks / pkcs12	Definiert den Keystore Type welcher für SAML2 Kommunikation mit dem ID Austria Systems im Zuge des Matching Vorgangs verwendet werden soll
eid.as.modules.idaustriaclient.keystore.path	keys/junit.jks	Pfad zum Software KeyStore im Falle von ‚jks‘ oder ‚pkcs12‘ KeyStoretypen.
eid.as.modules.idaustriaclient.keystore.password	password	Password des Software KeyStores im Falle von ‚jks‘ oder ‚pkcs12‘ KeyStoretypen.
eid.as.modules.idaustriaclient.metadata.sign.alias	metadata	Name des Schlüssels im KeyStore welcher zur Erstellung von signierten SAML2 Metadaten das ID Austria Matching Clients verwendet wird.
eid.as.modules.idaustriaclient.metadata.sign.password	password	Passwort des Schlüssels im KeyStore welcher zur Erstellung von signierten SAML2 Metadaten das ID Austria Matching Clients verwendet wird.
eid.as.modules.idaustriaclient.request.sign.alias	sign	Name des Schlüssels im KeyStore welcher zur Signatur von SAML2 Requests an das ID Austria System verwendet wird. Hinweis: Das Zertifikat zu diesem Schlüssel ist in den SAML2 Metadaten hinterlegt.
eid.as.modules.idaustriaclient.request.sign.password	password	Password des Schlüssels im KeyStore welcher zur Signatur von SAML2 Requests an das ID Austria System verwendet wird.
eid.as.modules.idaustriaclient.response.encryption.alias	encrypt	Name des Schlüssels im KeyStore welcher zur Verschlüsselung der SAML2 Response des ID Austria System verwendet wird. Hinweis: Das Zertifikat zu diesem Schlüssel ist in den SAML2 Metadaten hinterlegt.
eid.as.modules.idaustriaclient.response.encryption.password	password	Password des Schlüssels im KeyStore welcher zur Verschlüsselung der SAML2 Response des ID Austria System verwendet wird.
eid.as.modules.idaustriaclient.truststore.type	jks / pkcs12	Definiert den TrustStore Type welcher für SAML2 Kommunikation mit dem ID Austria Systems im Zuge des Matching Vorgangs verwendet werden soll.
eid.as.modules.idaustriaclient.truststore.path	keys/teststore.jks	Pfad zum Software TrustStore im Falle von ‚jks‘ oder ‚pkcs12‘ TrustStoretypen. Dieser TrustStore dient zur Validierung des

eidas.ms.modules.idaustriaclient.truststore.password

eidas.ms.modules.idaustriaclient.idaustria.idp.entityId

eidas.ms.modules.idaustriaclient.idaustria.idp.metadataUrl

trustIda

P-Stage:
<https://eid.oesterreich.gv.at/auth/idp/shibboleth>

Q-Stage:
<https://eid2.oesterreich.gv.at/auth/idp/shibboleth>

Vertrauensverhältnisses der SAML2 Metadaten des ID Austria Systems.
Hinweis: Der in der Beispielkonfiguration beigelegte Truststore beinhaltet bereits die aktuellen SAML2 Metadaten signaturzertifikate des ID Austria Systems.
Password des Software TrustStores im Falle von ‚jks‘ oder ‚pkcs12‘ TrustStoretypen.
SAML2 EntityID des ID Austria System
Hinweis: Die EntityID stellt gleichzeitig auch die URL auf die SAML2 Metadaten des ID Austria Systems dar.

URL auf die SAML2 Metadaten des ID Austria System, sofern diese nicht identisch zur EntityId ist.

1.2.12. 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, ...)
eidas.ms.auth.eIDAS.node_v2.attributes.requested.representation.{index}	CSV aus 'Attribute-FriendlyName' und 'isRequired' flag	3. {countryCode} LänderCode (z.B. de) 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, ...)

1.2.13. 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	Passwort des Schlüssels im KeyStore

password		welcher zur Signatur des ID Austria AuthBlocks verwendet wird.
eidas.ms.auth.eIDAS.authblock.us	true / false	Aktiviert das Legacyformat für den AuthBlock, welcher an das ID Austria System übermittelt wird.
e.legacy.version	Default: false	Hinweis: Das AuthBlock Format muss mit dem ID Austria System abgestimmt sein da der AuthBlock am IDA System validiert wird.

1.2.14. 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	Passwort 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 Responses des zentralen eIDAS Knoten verwendet wird.
eidas.ms.pvp2.key.signing.password	password	Hinweis: Das Zertifikat zu diesem Schlüssel ist in den SAML2 Metadaten hinterlegt. Passwort des Schlüssels im KeyStore welcher zur Signatur von SAML2 Responses 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.organization.name		OrganizationName entsprechend SAML2 Metadatenspezifikation 2.3.2.1 Element <Organisation>
eidas.ms.pvp2.metadata.organization.friendlyname		OrganizationDisplayName entsprechend SAML2 Metadatenspezifikation 2.3.2.1 Element <Organisation>
eidas.ms.pvp2.metadata.organization.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>
eidas.ms.pvp2.metadata.contact.suriname		Hinweis: Als <contactType> wird immer ‚technical‘ gesetzt. SurName entsprechend SAML2 Metadatenspezifikation 2.3.2.2 Element <ContactPerson>
eidas.ms.pvp2.metadata.contact.email		Hinweis: Als <contactType> wird immer ‚technical‘ gesetzt. EmailAddress entsprechend SAML2 Metadatenspezifikation 2.3.2.2 Element <ContactPerson>
		Hinweis: Als <contactType> wird immer ‚technical‘ gesetzt.

1.2.15. Erlaubte ID Austria 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
<code>eidas.ms.sp.x.uniqueID=http://test.com/test</code>	X	(Eindeutige Id wie SAML2 EntityId)
<code>eidas.ms.sp.x.pvp2.metadata.truststore</code>	X	Pfad zum Software KeyStore (jks) der als TrustStore zur Validierung des SAML2 Metadatensignaturzertifikats dieses SP verwendet werden soll
<code>eidas.ms.sp.x.pvp2.metadata.truststore.password</code>	X	Passwort für den Zugriff auf den TrustStore
<code>eidas.ms.sp.x.friendlyName</code>		FriendlyName für diese SP sofern dieser nicht via SAML2 Request übermittelt wird
<code>eidas.ms.sp.x.pvp2.metadata.url</code>		URL auf die SAML2 Metadaten des SP falls diese nicht mit der uniqueID übereinstimmt
<code>eidas.ms.sp.x.policy.allowed.requested.targets</code>		RegEx mit erlaubten bPK Bereichen für diesen SP Hinweis: Defaultmäßig sind alle Bereiche zulässig

1.2.16. Zentrales Fehlerhandling

Der MS-Connector implimentiert ein zentrales Fehlerhandling über welches sich das Verhalten im Fehlerfall konfigurieren lässt. Die Konfiguration wird mittels Property `eidas.ms.core.error.handling.config` an den MS-Connector übergeben. Die Konfiguration bietet folgende Konfigurationsmöglichkeiten wobei sich die gesamte Konfiguration aus mehreren Sets aus Konfigurationseinträgen zusammensetzen kann.

Name	Wert(e)	Beschreibung
<code>action</code>	<ul style="list-style-type: none">• <code>ticket</code>• <code>no_ticket</code>• <code>errorpage</code>	Definiert das Verhalten bezüglich Fehlerticket für dieses Set. Folgende Optionen stehen zur Verfügung: <ul style="list-style-type: none">• ticket Zeigt eine Fehlerseite mit Fehlerticket und bietet die optionale Rückleitung an den Service-Provider sofern diese verfügbar ist.• no_ticket Rückleitung an den Service-Provider sofern möglich. Falls nicht, Anzeige einer Fehlerseite ohne Fehlerticket• errorpage Zeigt immer eine Fehlerseite ohne Fehlerticket und bietet die optionale Rückleitung an den Service-Provider sofern diese

		Verfügbar ist.
externalCode	1002	Definiert den externen ErrorCode welcher diesem Set zugeordnet ist. Der externe ErrorCode wird sowohl in der GUI angezeigt als auch dem Service-Provider returniert. Hinweis: wird kein externen ErrorCode angegeben wird der interne weitergereicht.
logLevel	<ul style="list-style-type: none"> • ERROR • WARN • INFO • DEBUG 	Definiert den LogLevel mit welchem dieses Set von Fehlern im technischen Log geloggt wird
internalCode	<ul style="list-style-type: none"> - auth.39 - auth.40 	Eine Liste von internen Fehlercodes welche diesem Konfigurationsset zugeordnet sind. Diese weisen somit ein identisches Verhalten bezüglich <i>action</i> , <i>externalCode</i> und <i>logLevel</i> auf.
defaultConfig	true/false	Definiert dieses Set als Default und spiegelt somit das Defaultverhalten im Fehlerfall wider. Hinweis: Es kann nur ein Konfigurationsset mit <i>defaultConfig=true</i> geben
writeThrowable	true/false Default: true	Wenn <i>false</i> , werden für diese internen Fehlercodes keine Stacktraces geloggt sondern nur die Fehlermeldung.
useInternalAsExternal	true/false Default: false	Wenn <i>true</i> , werden die internen Fehlercodes direkt als externe Fehlercodes weitergereicht sofern kein <i>externalCode</i> definiert ist. Hinweis: Falls kein <i>externalCode</i> definiert wurde und dieses Flag auf <i>false</i> steht, wird als <i>externalCode</i> immer StatusCode 9199 verwendet.

2. Änderungsübersicht

Datum	Beschreibung	Autor
20.01.2021	Initialversion für MS-Connector 1.2.0	Thomas Lenz
12.05.2021	Finalisierung für MS-Connector 1.2.0	Thomas Lenz
25.06.2021	Konfiguration für NameldFormat erweitert	Thomas Lenz
05.04.2022	Finalisierung für MS-Connector 1.2.4	Thomas Lenz
19.05.2022	Finalisierung für MS-Connector 1.3.0	Thomas Lenz
05.07.2022	Finalisierung für MS-Connector 1.3.1	Thomas Lenz
26.08.2022	Finalisierung für MS-Connector 1.3.3	Thomas Lenz
21.11.2022	Finalisierung für MS-Connector 1.3.5	Thomas Lenz
02.03.2023	Finalisierung für MS-Connector 1.3.8	Thomas Lenz

11.10.2023	Finalisierung für MS-Connector 1.4.0
14.03.2024	Finalisierung für MS-Connector 1.5.0
22.05.2024	Finalisierung für MS-Connector 1.6.0

Thomas Lenz
Thomas Lenz
Thomas Lenz