

MS-SPECIFIC EIDAS PROXY-SERVICE KONFIGURATION

Version 1.3 vom 18.10.2024

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 Proxy-Service.

1.1. Allgemeine Hinweise zur Konfiguration

Die nachfolgenden Kapitel beschreiben allgemeine Konfigurationsrichtlinien für das österreichspezifische eIDAS Proxy-Service.

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-Proxy-Service

Das MS-Proxy-Service stellt öffentliche benötigte Services an folgenden End-Punkten zur Verfügung.

Endpunkt	Beschreibung
/public/secure/*	Endpunkte für Prozessmanagement und ErrorHandling am MS-Proxy-Service
/eidas/light/idp/post	Endpunkte für Kommunikation mit eIDAS Referenzimplementierung
/eidas/light/idp/redirect	Endpunkte für Kommunikation mit eIDAS Referenzimplementierung
/sp/idaustria/eidas/metadata	SAML2 Metadaten des ID Austria Clients im MS-Proxy-Service
/sp/idaustria/eidas/post	SAML2 POST-Binding Endpunkt des ID Austria Clients im MS-Proxy-Service
/sp/idaustria/eidas/redirect	SAML2 Redirect-Binding Endpunkt des ID Austria Clients im MS-Proxy-Service
/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-proxy.configuration=/path/to/configuration/default_config.properties* 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_PROXY_SERVICE_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 interne 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_proxyservice	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.revisionlog.logIPAddressOfUser	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_proxyService	URL unter welcher das MS-Proxy-Service 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-Proxy-Service Applikation. Alle relativen Pfade werden als relativ zu diesem Pfad interpretiert.
eidas.ms.context.use.clustermode	true/false Default: trueAktiviert den Clusterbetriebsmode	Aktiviert den Clusterbetriebsmode
eidas.ms.core.error.handling.config	Default: ./misc/misc/error_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.directory	Default: webcontent/	Alle in diesem Verzeichnis hinterlegten Daten werden statisch im Kontext der MS-Proxy-Service 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-Proxy-Service hinterlegt. Diese Templates werden im Anmeldeprozess dynamisch geladen und verarbeitet
eidas.ms.webcontent.properties	Default: properties/mess	Dieses Verzeichnis stellt die primäre Quelle für Message Properties für i18n

ages

(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

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.digit.algorithm	Default: HmacSHA256	Algorithmus zur Integritätssicherung von PendingRequestIds
eidas.ms.core.pendingrequestid.digit.secret	pendingReqIdSecret	Secret zur Generierung und Validierung von Einmalzugriffstoken. Hinweis: Wird das MS-Proxy-Service im Cluster betrieben (mehr als eine Instanz) muss dieser Parameter auf allen Instanzen des MS-Proxy-Service identisch sein.

1.2.6. HTTP Client Basisparameter

Name	Wert(e)	Beschreibung
eidas.ms.client.http.connection.timeout.socket	[sec] Default: 15	Response Timeout, Maximale Zeitspanne in Sekunden bis der Server eine Anfrage beantwortet.
eidas.ms.client.http.connection.timeout.connection	[sec] Default: 15	Connection-Pool Timeout. Maximale Zeitspanne in Sekunden bis vom internen HTTP Connection-Pool eine Verbindung frei wird.
eidas.ms.client.http.connection.timeout.request	[sec] Default: 15	Request Timeout, Maximale Zeitspanne in Sekunden bis der Server eine Anfrage annimmt.

1.2.7. eIDAS Node Integration

Name	Wert(e)	Beschreibung
eidas.ms.auth.eIDAS.proxy.attribute.mapping.config	Default: misc/idaAttributeMapping.json	Pfad zur externen Mapping Konfiguration zwischen eIDAS Attributen und ID Austria Attributen.
eidas.ms.auth.eIDAS.node_v2.proxy.entityId	Default: ownSpecificProxy	Name des MS-Proxy-Service in der Kommunikation mit dem eIDAS Node aus der Referenzimplementierung
eidas.ms.auth.eIDAS.node_v2.proxy.forward.endpoint	z.B.: https://eidas.bmi.gv.at/EidasNode/SpecificProxyServiceResponse	Endpunkt des eIDAS Nodes der Referenzimplementierung an welchen der Anmeldeprozess nach erfolgreicher ID Austria Anmeldung weitergeleitet wird
eidas.ms.auth.eIDAS.node_v2.proxy.forward.method	GET / POST Default: POST	HTTP Methode welche zur Weiterleitung an den eIDAS Node verwendet wird
eidas.ms.auth.eIDAS.node_v2.proxy.forward.errors	true/false Default: false	Aktiviert / Deaktiviert die Rückgabe von Fehlern an den eIDAS Node. Falls

eidas.ms.auth.eIDAS.node_v2.lightToken.proxyService.request.issuer.name	Default: specificCommunicationDefinitionProxyServiceRequest	deaktiviert werden alle Fehler am MS-ProxyService ausgegeben. Issuername für die Erstellung von Zugriffstoken für die Weiterleitung des Anmeldevorgangs vom eIDAS-Node an das MS-ProxyService
eidas.ms.auth.eIDAS.node_v2.lightToken.proxyService.request.secret	Default: mySecretProxyServiceRequest	Passwort für die Erstellung von Zugriffstoken für die Weiterleitung des Anmeldevorgangs vom eIDAS-Node an das MS-ProxyService Hinweis: Muss mit der Konfiguration am eIDAS-Node übereinstimmen
eidas.ms.auth.eIDAS.node_v2.lightToken.proxyService.request.algorithm	Default: SHA-256	Hash Algorithmus für die Erstellung von Zugriffstoken für die Weiterleitung des Anmeldevorgangs vom eIDAS-Node an das MS-ProxyService Hinweis: Muss mit der Konfiguration am eIDAS-Node übereinstimmen
eidas.ms.auth.eIDAS.node_v2.lightToken.proxyService.response.issuer.name	Default: specificCommunicationDefinitionProxyServiceResponse	Issuername für die Erstellung von Zugriffstoken für die Weiterleitung des Anmeldevorgangs vom MS-ProxyService an den eIDAS-Node
eidas.ms.auth.eIDAS.node_v2.lightToken.proxyService.response.secret	Default: mySecretProxyServiceResponse	Passwort für die Erstellung von Zugriffstoken für die Rückleitung des Anmeldevorgangs vom MS-ProxyService an den eIDAS-Node Hinweis: Muss mit der Konfiguration am eIDAS-Node übereinstimmen
eidas.ms.auth.eIDAS.node_v2.lightToken.proxyService.response.algorithm	Default: SHA-256	Hash Algorithmus für die Erstellung von Zugriffstoken für die Rückleitung des Anmeldevorgangs vom MS-ProxyService an den eIDAS-Node 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-ProxyService
<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-ProxyService
<u>eidas.ms.auth.eIDAS.proxy.mandates.enabled</u>	true/false Default: true	Aktiviert die Unterstützung von Anmeldung in Vertretung am MS-Proxy-Service
eidas.ms.auth.eIDAS.proxy.mandates.profiles.natural.default	CSV Liste Default: GeneralvollmachtBilateral	Liste von komma-separierten Vollmachtenprofilen welche für die Anmeldung in Vertretung für eine natürliche Person erlaubt sind. Eine Liste aller Profile findet sich unter: https://eid.oesterreich.gv.at/authHandler/public/mis/info
eidas.ms.auth.eIDAS.proxy.mandates.profiles.legal.default	CSV Liste Default: Einzelvertretungsbefugnis	Liste von komma-separierten Vollmachtenprofilen welche für die Anmeldung in Vertretung für eine juristische Person erlaubt sind. Eine Liste aller Profile findet sich unter: https://eid.oesterreich.gv.at/authHandler/public/mis/info

1.2.8. ID Austria Anbindung

Aus Sicht des MS-Proxy-Service sind folgende Registrierungsparameter auf jeden Fall

notwendig:

- Eindeutige Identifier:
 - P-Stage:
https://eidas.bmi.gv.at/ms_proxyservice/sp/idaustria/eidas/metadata
 - T-Stage:
https://eidas-test.bmi.gv.at/ms_proxyservice/sp/idaustria/eidas/metadata
- bPK-Bereich: ZP-eidas
- 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)
 - Vollmachtenattribute werden automatisch mit der Aktivierung von Vertretungen inkludiert
- Anmeldung in Vertretung erlauben
 - Vollmachtenprofile entsprechend den in der MS-Proxy-Service hinterlegten Profile
- SAML2 Metadaten
 - Die für die Registrierung benötigten SAML2 Metadaten werden automatisch generiert und können unter den folgenden Endpunkten abgerufen werden.
 - P-Stage:
https://eidas.bmi.gv.at/ms_proxyservice/sp/idaustria/eidas/metadata
 - T-Stage:
https://eidas-test.bmi.gv.at/ms_proxyservice/sp/idaustria/eidas/metadata

Name	Wert(e)	Beschreibung
eidas.ms.modules.idaustriaauth.keystore.type	jks / pkcs12	Definiert den Keystore Type welcher für SAML2 Kommunikation mit dem ID Austria Systems verwendet werden soll
eidas.ms.modules.idaustriaauth.keystore.path	keys/junit.jks	Pfad zum Software KeyStore im Falle von ‚jks‘ oder ‚pkcs12‘ KeyStoretypen.
eidas.ms.modules.idaustriaauth.keystore.password	password	Password des Software KeyStores im Falle von ‚jks‘ oder ‚pkcs12‘ KeyStoretypen.
eidas.ms.modules.idaustriaauth.metadata.sign.alias	metadata	Name des Schlüssels im KeyStore welcher zur Erstellung von signierten SAML2 Metadaten das ID Austria Clients verwendet wird.
eidas.ms.modules.idaustriaauth.metadata.sign.password	password	Passwort des Schlüssels im KeyStore welcher zur Erstellung von signierten SAML2 Metadaten das ID Austria Clients verwendet wird.
eidas.ms.modules.idaustriaauth.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.
eidas.ms.modules.idaustriaauth.request.sign.password	password	Passwort des Schlüssels im KeyStore welcher zur Signatur von SAML2 Requests an das ID Austria System verwendet wird.
eidas.ms.modules.idaustriaauth.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.
eidas.ms.modules.idaustriaauth.response.encryption.password	password	Passwort des Schlüssels im KeyStore welcher zur Verschlüsselung der SAML2 Response des ID Austria System verwendet wird.
eidas.ms.modules.idaustriaauth.truststore.type	jks / pkcs12	Definiert den TrustStore Type welcher für SAML2 Kommunikation mit dem ID Austria Systems verwendet werden soll.

eidas.ms.modules.idaustriaauth.truststore.path	keys/ teststore.jks	Pfad zum Software TrustStore im Falle von ‚jks‘ oder ‚pkcs12‘ TrustStoretypen. Dieser TrustStore dient zur Validierung des 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.
eidas.ms.modules.idaustriaauth.truststore.password	trustIda	Password des Software TrustStores im Falle von ‚jks‘ oder ‚pkcs12‘ TrustStoretypen.
eidas.ms.modules.idaustriaauth.idp.entityId	P-Stage: https://eid.oesterreich.gv.at/auth/idp/shibboleth Q-Stage: https://eid2.oesterreich.gv.at/auth/idp/shibboleth	SAML2 EntityID des ID Austria System Hinweis: Die EntityID stellt gleichzeitig auch die URL auf die SAML2 Metadaten des ID Austria Systems dar.
eidas.ms.modules.idaustriaauth.idp.metadataUrl		URL auf die SAML2 Metadaten des ID Austria System, sofern diese nicht identisch zur EntityId ist.
eidas.ms.configuration.pvp.scheme.validation eidas.ms.configuration.pvp.enable.entitycategories	true / false Default: true true / false Default: false	Aktiviert die XML Schemavalidierung für SAML2 Metadaten und SAML2 Requests 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.surname		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.

1.2.9. BORIS Attribute für ejustice

Sektorspezifische eIDAS Attribute-Konfiguration für die Unterstützung von ejustice Anwendungen der Europäischen Kommission Diese Konfiguration kommt nur dann zum Einsatz wenn die folgenden sektorspezifischen eIDAS Attribute vom eIDAS-Connector angefordert werden:

- <http://e-justice.europa.eu/attributes/naturalperson/eJusticeNaturalPersonRole>
- <http://e-justice.europa.eu/attributes/legalperson/eJusticeLegalPersonRole>

Name	Wert(e)	Beschreibung
eidas.ms.advanced.attributes.ejustice.mandate.profiles	eJusticePortalVip1 Default:	Liste von Vollmachtenprofilen über welche Rollen für ejustice Anwendungen abgebildet werden. Diese Liste wird an das IDA System übergeben.
eidas.ms.advanced.attributes.ejustice.mandate.mode	Default: forceLegal	Vollmachtenbetriebsmodus am IDA System entsprechend der Liste von Vollmachtenprofile. Hinweis: folgende Werte stehen zur Verfügung. <ul style="list-style-type: none">• legal: ohne Vertretung oder Vertretung für juristische Personen• natural: ohne Vertretung oder Vertretung für natürliche Personen• forceLegal: nur Vertretung für juristische Personen• forceNatural: nur Vertretung für natürliche Personen• all: ohne Vertretung und mit Vertretung erlaubt• forceAll: nur Vertretung erlaubt• none: keine Vertretung erlaubt
eidas.ms.advanced.attributes.ejustice.additional.ida.attributes	Default: urn:oid:1.2.40.0.10.2.1.1.261.76,urn:oid:1.2.40.0.10.2.1.1.261.84,urn:oid:1.2.40.0.10.2.1.1.261.100	Komma-separierte Liste von ID Austria Attributen welche zusätzlich am IDA System angefragt werden müssen
eidas.ms.advanced.attributes.ejustice.value.x	eJusticePortalVip1=VIP1 Default:	Mappt das im Anmeldevorgang ausgewählte Vollmachtenprofil auf den Attributwert des ejustice Attributes. Bei Definition mehrerer Mappings muss das ‚x‘ durch eine eindeutige Id ersetzt werden. Beispiel für einen Konfigurationswert: eJusticePortalVip1=VIP1

1.2.10. PowerOfRepresentationScope Attribute für SDG/OOTS

Sektorspezifische eIDAS Attribute-Konfiguration für die Unterstützung von SDG/OOTS Anwendungen. Diese Konfiguration kommt nur dann zum Einsatz wenn das folgende sektorspezifische eIDAS Attribute vom eIDAS-Connector angefordert wird:

- <http://data.europa.eu/p4s/attributes/PowerOfRepresentationScope>

Hinweis: Die für SDG/OOTS benötigte Funktionalität wurde bereits konzeptionell berücksichtigt jedoch fehlen aus aktueller Sicht die finale Abstimmung für die Konfiguration und die Inbetriebnahme auf der Produktivumgebung. Die im Handbuch und in der Beispielkonfiguration hinterlegten Parameter entsprechend spiegeln das abgestimmte Verhalten für die Test-Umgebung wider.

Name	Wert(e)	Beschreibung
eidas.ms.advanced.attributes.oots.powerofrepresentation.enabled eidas.ms.advanced.attributes.ejustice.mandate.mode	true / false Default: false Default: forceLegal	Aktiviert / Deaktiviert die Unterstützung des sektorspezifischen OOTS Attributes. Vollmachtenbetriebsmodus am IDA System entsprechend der Liste von Vollmachtenprofile. Hinweis: folgende Werte stehen zur Verfügung. <ul style="list-style-type: none">• legal: ohne Vertretung oder Vertretung für juristische Personen• natural: ohne Vertretung oder Vertretung für natürliche Personen• forceLegal: nur Vertretung für juristische Personen• forceNatural: nur Vertretung für natürliche Personen• all: ohne Vertretung und mit Vertretung erlaubt• forceAll: nur Vertretung erlaubt• none: keine Vertretung erlaubt
eidas.ms.advanced.attributes.oots.powerofrepresentation.additional.ida.attributes	Default: urn:oid:1.2.40.0.10.2.1.1.261.76,urn:oid:1.2.40.0.10.2.1.1.261.84,urn:oid:1.2.40.0.10.2.1.1.261.100	Komma-separierte Liste von ID Austria Attributen welche zusätzlich am IDA System angefragt werden müssen
eidas.ms.advanced.attributes.oots.powerofrepresentation.scopes	Default:	Mapping von SDG/OOTS spezifischen Scopes auf österreichische Vollmachtenprofile. Das Mapping erfolgt auf Basis eines JSON Konfigurationsparameter. scope: Scope Identifier laut SDG/OOTS Spezifikation profile: Österreichisches Vollmachtenprofile für diesen Scope mode: folgende Werte stehen zur Verfügung. <ul style="list-style-type: none">• legal: ohne Vertretung oder Vertretung für juristische Personen• natural: ohne Vertretung oder Vertretung für natürliche Personen• forceLegal: nur Vertretung für juristische Personen• forceNatural: nur Vertretung für natürliche Personen• all: ohne Vertretung und mit Vertretung erlaubt• forceAll: nur Vertretung erlaubt• none: keine Vertretung erlaubt

Beispielkonfiguration für OOTS Scope Mapping:

```
[
  {"scope": "X1", "profile": "Einzelvertretungsbefugnis", "mode": "legal"},
  {"scope": "X2", "profile": "Einzelvertretungsbefugnis", "mode": "legal"},
  {"scope": "X3", "profile": "Einzelvertretungsbefugnis", "mode": "legal"},
  {"scope": "X4", "profile": "Einzelvertretungsbefugnis", "mode": "legal"},
  {"scope": "X5", "profile": "Einzelvertretungsbefugnis", "mode": "legal"},
  {"scope": "X6", "profile": "Einzelvertretungsbefugnis", "mode": "legal"},
  {"scope": "X10", "profile": "Einzelvertretungsbefugnis", "mode": "legal"},
  {"scope": "X11", "profile": "Einzelvertretungsbefugnis", "mode": "legal"},
  {"scope": "atInternal!Default!Scope",
    "profile": "Einzelvertretungsbefugnis", "mode": "legal", "default": true}]
```

1.2.11. Zentrales Fehlerhändling

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

Name	Wert(e)	Beschreibung
action	1. ticket 2. no_ticket 3. errorpage	<p>Definiert das Verhalten bezüglich Fehlertickets für dieses Set. Folgende Optionen stehen zur Verfügung:</p> <ol 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	<p>Definiert den externen ErrorCode welcher diesem Set zugeordnet ist. Der externe ErrorCode wird sowohl in der GUI angezeigt als auch dem Service-Provider returniert.</p> <p>Hinweis: wird kein externen ErrorCode angegeben wird der interne weitergereicht.</p>

logLevel	1. ERROR 2. WARN 3. INFO 4. DEBUG	Definiert den LogLevel mit welchem dieses Set von Fehlern im technischen Log geloggt wird
internalCode	- 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.

1.2.12. Spezifische Konfigurationen für eIDAS-Connectoren

Der MS-Proxy-Service implementiert kein WhiteListing von erlaubten ausländischen eIDAS-Connectoren. Sollte ein WhiteListing erwünscht sein muss dieses über den EIDAS-Node umgesetzt werden.

Allgemein werden alle Anmeldeparameter dynamisch aus dem Authentifizierungsrequest des anfragenden eIDAS-Connectors extrahiert und die Defaultkonfiguration angewendet. In manchen Fällen kann es jedoch notwendig werden das Prozessparameter für einen spezifische eIDAS-Connector angepasst werden müssen, da z.B. der CountryCode der anfragenden Stelle nicht korrekt aus den Anfrageinformationen extrahiert werden kann. Das x in eidas.ms.connector.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 (SAML2 EntityId) des eIDAS-Connectors für welchen dieses Konfigurationselement gilt
eidas.ms.connector.x.countryCode	X	CountryCode oder Kennenzeichen der länderübergreifenden Organisation, welche diesem eIDAS-Connector zugeordnet ist. Z.B.: ES, EU, ...
eidas.ms.connector.x.mandates.en	X	Aktiviert die Unterstützung von

abled

Anmeldung in Vertretung am MS-Proxy-Service für diesen eIDAS-Connector

eidas.ms.connector.x.mandates.natural

X
(falls
Vertretungen
aktiv)

Bsp: true/false

Liste von komma-separierten Vollmachtenprofilen welche für die Anmeldung in Vertretung für eine natürliche Person für diesen eIDAS-Connector erlaubt sind. Eine Liste aller Profile findet sich unter:

<https://eid.oesterreich.gv.at/authHandler/public/mis/info>

eidas.ms.connector.x.mandates.legal

X
(falls
Vertretungen
aktiv)

Liste von komma-separierten Vollmachtenprofilen welche für die Anmeldung in Vertretung für eine juristische Person für diesen eIDAS-Connector erlaubt sind. Eine Liste aller Profile findet sich unter:

<https://eid.oesterreich.gv.at/authHandler/public/mis/info>

eidas.ms.connector.x.auth.idaustria.entityId

SAML2 EntityID des ID Austria System auf welches für diesen eIDAS-Connector weitergeleitet werden soll.

Hinweis: Die EntityID stellt gleichzeitig auch die URL auf die SAML2 Metadaten des ID Austria Systems dar.

2. Änderungsübersicht

Datum	Beschreibung	Autor
23.08.2022	Initialversion für MS-Proxy-Service 1.0.0	Thomas Lenz
30.11.2022	Anpassungen für v1.0.1	Thomas Lenz
16.12.2022	Anpassungen für v1.0.2	Thomas Lenz
14.03.2024	Anpassungen für v1.1.0	Thomas Lenz
22.05.2024	Anpassungen für v1.2.0	Thomas Lenz
18.10.2024	Anpassungen für v1.3.0 OOTS PowerOfRepresentationScope Attribut	Thomas Lenz