

# MS-SPECIFIC EIDAS PROXY-SERVICE KONFIGURATION

Version 1.2 vom 22.05.2024

Thomas Lenz – [thomas.lenz@egiz.gv.at](mailto:thomas.lenz@egiz.gv.at)

Thomas Zefferer – [thomas.zefferer@a-sit.at](mailto:thomas.zefferer@a-sit.at)

## Inhaltsverzeichnis

|   |   |
|---|---|
| Inhaltsverzeichnis                                | 1 |
| 1. Konfiguration                                  | 1 |
| 1.1. <b>Allgemeine Hinweise zur Konfiguration</b> | 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   |
|--|--|
| <a href="#">/public/secure/*</a>             | Endpunkte für Prozessmanagement und ErrorHandling am MS-Proxy-Service      |
| <a href="#">/eidas/light/idp/post</a>        | Endpunkte für Kommunikation mit eIDAS Referenzimplementierung              |
| <a href="#">/eidas/light/idp/redirect</a>    | Endpunkte für Kommunikation mit eIDAS Referenzimplementierung              |
| <a href="#">/sp/idaustria/eidas/metadata</a> | SAML2 Metadaten des ID Austria Clients im MS-Proxy-Service                 |
| <a href="#">/sp/idaustria/eidas/post</a>     | SAML2 POST-Binding Endpunkt des ID Austria Clients im MS-Proxy-Service     |
| <a href="#">/sp/idaustria/eidas/redirect</a> | SAML2 Redirect-Binding Endpunkt des ID Austria Clients im MS-Proxy-Service |
| <a href="#">/actuator/*</a>                  | 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          | <b>Default:</b><br>ms_proxyservice    | Applikationsname                                       |
| spring.boot.admin.client.enabled | true / false<br><b>Default:</b> 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<br><b>Default:</b><br>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<br><b>Default:</b> 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://<br>abcde.at/<br>ms_proxyService                               | URL unter welcher das MS-Proxy-Service erreichbar ist  |
| eidas.ms.context.url.request.validation | true/false<br><b>Default:</b> 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<br><b>Default:</b><br>trueAktiviert den Clusterbetriebsmode | Aktiviert den Clusterbetriebsmode  |
| eidas.ms.core.error.handling.config     | <b>Default:</b><br>./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"> <li>• Mapping von internen auf externe Fehlercodes. Die externen FehlerCodes sind jene die dem SP oder dem Benutzer auf der Fehlerseite angezeigt werden.</li> <li>• Erstellung von Fehlertickets für interne Fehlercodes</li> <li>• Konfiguration von LogLevels i zentralen Fehlerhändling für interne Fehlercodes</li> </ul> |

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

| Name                                 | Wert(e)                            | Beschreibung  |
|--------------------------------------|------------------------------------|---|
| eidas.ms.webcontent.static.directory | <b>Default:</b><br>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        | <b>Default:</b><br>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       | <b>Default:</b><br>properties/mess | Dieses Verzeichnis stellt die primäre Quelle für Message Properties für i18n  |

ages

(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

### 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 | <b>Default:</b><br>HmacSHA256 | Algorithmus zur Integritätssicherung von PendingRequestIds   |
| eidas.ms.core.pendingrequestid.digist.secret    | pendingReqIdSecret            | Secret zur Generierung und Validierung von Einmalzugriffstoken.<br><b>Hinweis:</b> 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]<br><b>Default:</b> 15 | Response Timeout, Maximale Zeitspanne in Sekunden bis der Server eine Anfrage beantwortet.                                |
| eidas.ms.client.http.connection.timeout.connection | [sec]<br><b>Default:</b> 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]<br><b>Default:</b> 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 | <b>Default:</b><br>misc/idaAttributeMapping.json                               | Pfad zur externen Mapping Konfiguration zwischen eIDAS Attributen und ID Austria Attributen.   |
| eidas.ms.auth.eIDAS.node_v2.proxy.entityId         | <b>Default:</b><br>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 | <b>z.B.:</b><br>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<br><b>Default:</b> POST   | HTTP Methode welche zur Weiterleitung an den eIDAS Node verwendet wird   |
| eidas.ms.auth.eIDAS.node_v2.proxy.forward.errors   | true/false<br><b>Default:</b> false  | Aktiviert / Deaktiviert die Rückgabe von Fehlern an den eIDAS Node. Falls  |

|   |  |   |
|---|--|---|
| eidas.ms.auth.eIDAS.node_v2.lightToken.proxyService.request.issuer.name         | <b>Default:</b><br>specificCommunicationDefinitionProxyServiceRequest  | deaktiviert werden alle Fehler am MS-ProxyService ausgegeben.<br>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              | <b>Default:</b><br>mySecretProxyServiceRequest                         | Passwort für die Erstellung von Zugriffstoken für die Weiterleitung des Anmeldevorgangs vom eIDAS-Node an das MS-ProxyService<br><b>Hinweis:</b> Muss mit der Konfiguration am eIDAS-Node übereinstimmen  |
| eidas.ms.auth.eIDAS.node_v2.lightToken.proxyService.request.algorithm           | <b>Default:</b> SHA-256  | Hash Algorithmus für die Erstellung von Zugriffstoken für die Weiterleitung des Anmeldevorgangs vom eIDAS-Node an das MS-ProxyService<br><b>Hinweis:</b> Muss mit der Konfiguration am eIDAS-Node übereinstimmen  |
| eidas.ms.auth.eIDAS.node_v2.lightToken.proxyService.response.issuer.name        | <b>Default:</b><br>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             | <b>Default:</b><br>mySecretProxyServiceResponse                        | Passwort für die Erstellung von Zugriffstoken für die Rückleitung des Anmeldevorgangs vom MS-ProxyService an den eIDAS-Node<br><b>Hinweis:</b> Muss mit der Konfiguration am eIDAS-Node übereinstimmen  |
| eidas.ms.auth.eIDAS.node_v2.lightToken.proxyService.response.algorithm          | <b>Default:</b> SHA-256  | Hash Algorithmus für die Erstellung von Zugriffstoken für die Rückleitung des Anmeldevorgangs vom MS-ProxyService an den eIDAS-Node<br><b>Hinweis:</b> Muss mit der Konfiguration am eIDAS-Node übereinstimmen  |
| eidas.ms.auth.eIDAS.node_v2.incoming.lightRequest.max.number.characters         | <b>Default:</b> 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> | <b>Default:</b> 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<br><b>Default:</b> true                                     | Aktiviert die Unterstützung von Anmeldung in Vertretung am MS-Proxy-Service   |
| eidas.ms.auth.eIDAS.proxy.mandates.profiles.natural.default                     | CSV Liste<br><b>Default:</b><br>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:<br><a href="https://eid.oesterreich.gv.at/authHandler/public/mis/info">https://eid.oesterreich.gv.at/authHandler/public/mis/info</a>  |
| eidas.ms.auth.eIDAS.proxy.mandates.profiles.legal.default                       | CSV Liste<br><b>Default:</b><br>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:<br><a href="https://eid.oesterreich.gv.at/authHandler/public/mis/info">https://eid.oesterreich.gv.at/authHandler/public/mis/info</a> |

### 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](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](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](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](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.<br><b>Hinweis:</b> 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.<br><b>Hinweis:</b> 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/<br>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.<br><b>Hinweis:</b> 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  | <b>P-Stage:</b><br><a href="https://eid.oesterreich.gv.at/auth/idp/shibboleth">https://eid.oesterreich.gv.at/auth/idp/shibboleth</a><br><br><b>Q-Stage:</b><br><a href="https://eid2.oesterreich.gv.at/auth/idp/shibboleth">https://eid2.oesterreich.gv.at/auth/idp/shibboleth</a> | SAML2 EntityID des ID Austria System<br><b>Hinweis:</b> 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<br>eidas.ms.configuration.pvp.enable.entitycategories | true / false<br><b>Default:</b> true<br>true / false<br><b>Default:</b> false  | Aktiviert die XML Schemavalidierung für SAML2 Metadaten und SAML2 Requests<br>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   |  | <b>Hinweis:</b> Als <contactType> wird immer ‚technical‘ gesetzt.<br>SurName entsprechend SAML2 Metadatenspezifikation 2.3.2.2 Element <ContactPerson>  |
| eidas.ms.pvp2.metadata.contact.email   |  | <b>Hinweis:</b> Als <contactType> wird immer ‚technical‘ gesetzt.<br>EmailAddress entsprechend SAML2 Metadatenspezifikation 2.3.2.2 Element <ContactPerson>   |
|  |  | <b>Hinweis:</b> 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>

**Hinweis:** Die für eJustice benötigte Funktionalität wurde bereits konzeptionell berücksichtigt jedoch fehlen aus aktueller Sicht die finale Abstimmung für die Konfiguration und die Inbetriebnahme. Somit können diese Parameter bis auf weiteres unberücksichtigt bleiben und es können die Defaultwert aus der Beispielkonfiguration übernommen werden.

| Name  | Wert(e)  | Beschreibung  |
|---|--|---|
| <a href="#">eidas.ms.advanced.attributes.ejustice.mandate.profiles</a>          | eJusticePortalVIP1<br><b>Default:</b>  | Liste von Vollmachtenprofilen über welche Rollen für eJustice Anwendungen abgebildet werden. Diese Liste wird an das IDA System übergeben.  |
| <a href="#">eidas.ms.advanced.attributes.ejustice.mandate.mode</a>              | <b>Default:</b><br>forceLegal  | Vollmachtenbetriebsmodus am IDA System entsprechend der Liste von Vollmachtenprofile.<br><b>Hinweis:</b> folgende Werte stehen zur Verfügung. <ul style="list-style-type: none"><li>• legal: ohne Vertretung oder Vertretung für juristische Personen</li><li>• natural: ohne Vertretung oder Vertretung für natürliche Personen</li><li>• forceLegal: nur Vertretung für juristische Personen</li><li>• forceNatural: nur Vertretung für natürliche Personen</li><li>• all: ohne Vertretung und mit Vertretung erlaubt</li><li>• forceAll: nur Vertretung erlaubt</li><li>• none: keine Vertretung erlaubt</li></ul> |
| <a href="#">eidas.ms.advanced.attributes.ejustice.additional.ida.attributes</a> | <b>Default:</b><br>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  |
| <a href="#">eidas.ms.advanced.attributes.ejustice.value.x</a>                   | eJusticePortalVIP1=VIP1<br><b>Default:</b>   | 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.<br><br><b>Beispiel für einen Konfigurationswert:</b><br>TODO   |

### 1.2.10. Zentrales Fehlerhandling

Das MS-ProxyService implementiert ein zentrales Fehlerhandling 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<br>2. no_ticket<br>3. errorpage  | Definiert das Verhalten bezüglich Fehlertickets für dieses Set. Folgende Optionen stehen zur Verfügung:<br>1. <b>ticket</b> Zeigt eine Fehlerseite mit Fehlerticket und bietet die optionale Rückleitung an den Service-Provider sofern diese verfügbar ist.<br>2. <b>no_ticket</b> Rückleitung an den Service-Provider sofern möglich. Falls nicht, Anzeige einer Fehlerseite ohne Fehlerticket<br>3. <b>errorpage</b> Zeigt immer eine Fehlerseite ohne Fehlerticket und bietet die optionale Rückleitung an den Service-Provider sofern diese Verfügbar ist. |
| externalCode          | <b>1002</b>                                | Definiert den externen ErrorCode welcher diesem Set zugeordnet ist. Der externe ErrorCode wird sowohl in der GUI angezeigt als auch dem Service-Provider returniert.<br><b>Hinweis:</b> wird kein externen ErrorCode angegeben wird der interne weitergereicht.   |
| logLevel              | 1. ERROR<br>2. WARN<br>3. INFO<br>4. DEBUG | Definiert den LogLevel mit welchem dieses Set von Fehlern im technischen Log geloggt wird   |
| internalCode          | - auth.39<br>- 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.<br><b>Hinweis:</b> Es kann nur ein Konfigurationsset mit <i>defaultConfig=true</i> geben  |
| writeThrowable        | true/false<br><b>Default:</b> true         | Wenn <i>false</i> , werden für diese internen Fehlercodes keine Stacktraces geloggt sondern nur die Fehlermeldung.  |
| useInternalAsExternal | true/false                                 | Wenn <i>true</i> , werden die   |

|  |                       |   |
|--|-----------------------|---|
|  | <b>Default:</b> false | internen Fehlercodes direkt als externe Fehlercodes weitergereicht sofern kein <i>externalCode</i> definiert ist.<br><b>Hinweis:</b> Falls kein <i>externalCode</i> definiert wurde und dieses Flag auf <i>false</i> steht, wird als <i>externalCode</i> immer StatusCode 9199 verwendet. |
|--|-----------------------|---|

### 1.2.11. 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.enabled        | X                               | Aktiviert die Unterstützung von Anmeldung in Vertretung am MS-Proxy-Service für diesen eIDAS-Connector  |
| eidas.ms.connector.x.mandates.natural        | X<br>(falls Vertretungen aktiv) | <b>Bsp:</b> true/false<br>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:<br><a href="https://eid.oesterreich.gv.at/authHandler/public/mis/info">https://eid.oesterreich.gv.at/authHandler/public/mis/info</a> |
| eidas.ms.connector.x.mandates.legal          | X<br>(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:<br><a href="https://eid.oesterreich.gv.at/authHandler/public/mis/info">https://eid.oesterreich.gv.at/authHandler/public/mis/info</a>                          |
| eidas.ms.connector.x.auth.idaustria.entityId |                                 | SAML2 EntityID des ID Austria System auf welches für diesen eIDAS-Connector weitergeleitet werden soll.<br><b>Hinweis:</b> 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 |