



MS-SPECIFIC EIDAS PROXY-SERVICE KONFIGURATION

Version 1.0 vom 23.08.2022
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/](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 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.err orcodes	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

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: true	Aktiviert die Legacyunterstützung des AuthHandlers, entsprechend eGovernmentgesetz vor E-ID Einführung. Ist die Legacyunterstützung 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 entspricht 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-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/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

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

eidas.ms.core.pendingrequestid.digit.algorithm

Default:
HmacSHA256
pendingReqIdSecret

eidas.ms.core.pendingrequestid.digit.secret

einmaliger Verwendung wird das Token durch den widerrufen.
Algorithmus zur Integritätssicherung von PendingRequestIds

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
<u>eidas.ms.client.http.connection.timeout.socket</u>	[sec] Default: 15	Response Timeout, Maximale Zeitspanne in Sekunden bis der Server eine Anfrage beantwortet.
<u>eidas.ms.client.http.connection.timeout.connection</u>	[sec] Default: 15	Connection-Pool Timeout. Maximale Zeitspanne in Sekunden bis vom internen HTTP Connection-Pool eine Verbindung frei wird.
<u>eidas.ms.client.http.connection.timeout.request</u>	[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
<u>eidas.ms.auth.eIDAS.proxy.attribute.mapping.config</u>	Default: misc/idaAttributeMapping.json	Pfad zur externen Mapping Konfiguration zwischen eIDAS Attributen und ID Austria Attributen.
<u>eidas.ms.auth.eIDAS.node_v2.proxy.entityId</u>	Default: ownSpecificProxy	Name des MS-Proxy-Service in der Kommunikation mit dem eIDAS Node aus der Referenzimplementierung
<u>eidas.ms.auth.eIDAS.node_v2.proxy.forward.endpoint</u>		Endpunkt des eIDAS Nodes der Referenzimplementierung an welchen der Anmeldeprozess nach erfolgreicher ID Austria Anmeldung weitergeleitet wird
<u>eidas.ms.auth.eIDAS.node_v2.forward.method</u>	GET / POST Default: POST	HTTP Methode welche zur Weiterleitung an den eIDAS Node verwendet wird
<u>eidas.ms.auth.eIDAS.proxy.mandates.enabled</u>	true/false Default: true	Aktiviert die Unterstützung von Anmeldung in Vertretung am MS-Proxy-Service
<u>eidas.ms.auth.eIDAS.proxy.mandates.profiles.natural.default</u>	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
<u>eidas.ms.auth.eIDAS.proxy.mandates.profiles.legal.default</u>	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

eidas.ms.modules.idaustriaauth.trustore.type	jks / pkcs12	Response des ID Austria System verwendet wird. Definiert den TrustStore Type welcher für SAML2 Kommunikation mit dem ID Austria Systems verwendet werden soll.
eidas.ms.modules.idaustriaauth.trustore.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.trustore.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	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> 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.

1.2.9. 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	Default: TODO	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		Komma-separierte Liste von ID Austria Attributen welche zusätzlich am IDA System angefragt werden müssen
eidas.ms.advanced.attributes.ejustice.value.x	Default: TODO	Mappt das im Anmeldevorgang ausgewählte Vollmachtenprofil auf den Attributwert des ejustice Attributes. Bei Definition mehrerer Mappings mux das ‚x‘ durch eine eindeutige Id ersetzt werden. Beispiel für einen Konfigurationswert: TODO

1.2.10. Spezifische Konfigurationen für eIDAS-Connectoren

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

eidas.ms.connector.x.mandates.enabled	X	zugeordnet ist. Z.B.: ES, EU, ... Aktiviert die Unterstützung von 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