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

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

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

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

DVR: 1035461 ZVR: 948166612 UID: ATU60778947

MS-SPECIFIC EIDAS PROXY-SERVICE KONFIGURATION

Version 1.2 vom 16.12.2022
Thomas Lenz – thomas.lenz@egiz.gv.at
Thomas Zefferer – thomas.zefferer@a-sit.at

Inhaltsverzeichnis

1. Konfiguration

Dieses Dokument beschreibt Konfigurationsparameter des österreichspezifischen eIDAS 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 Releasepacket.
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:

- *-DEIDAS_CONFIG_REPOSITORY=/path/to/configuration/eIDAS/*
- *-DSPECIFIC_CONNECTOR_CONFIG_REPOSITORY=/path/to/configuration/eIDAS/*
- *-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	Aktiviert oder deaktiviert den SpringBoot

	Default: false	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 / Deaktivert 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:** true	Aktiviert die Legacyunterstützung des AuthHandlers, entsprechend eGovernmentgesetz vor E-ID Einführung. Ist die Legacyuntersützung aktiviert werden Handy-Signatur, XML Personenbindungen, XML AuthBlöcke, Stammzahlen, ... identisch zu aktuell noch verwendeten MOA-ID Instanzen verarbeitet. Ohne Legacyunterstützung werden ausschließlich Identifikations- und Authentifizierungsinformationen entsprecht dem E-ID unterstützt.

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

Name	Wert(e)	Beschreibung
eidas.ms.webcontent.static.directory	**Default:** webcontent/	Alle in diesem Verzeichnis hinterlegten Daten werden statisch im Kontext der MS-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 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 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.endpoin	**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.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 deaktiviert werden alle Fehler am MS-ProxyService ausgegeben.
eidas.ms.auth.eIDAS.proxy.mandates.enabled	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-Berech: 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 Vertetungen 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	Passwport 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 Metadatensignaturzertifikate 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 Austira 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.organisation.name		OrganizationName entsprechend SAML2 Metadatenspezifikation 2.3.2.1 Element <Organisation>
eidas.ms.pvp2.metadata.organisation.friendyname		OrganizationDisplayName entsprechend SAML2 Metadatenspezifikation 2.3.2.1 Element <Organisation>
eidas.ms.pvp2.metadata.organisation.url		OrganizationURL entsprechend SAML2 Metadatenspezifikation 2.3.2.1 Element <Organisation>
eidas.ms.pvp2.metadata.contact.givenname		GivenName entsprechend SAML2 Metadatenspezifikation 2.3.2.2 Element <ContactPerson> **Hinweis:** Als <contactType> wird immer

		‚technical' gesetzt.
eidas.ms.pvp2.metadata.contact.surname		SurName entsprechend SAML2 Metadatenspezifikation 2.3.2.2 Element <ContactPerson> **Hinweis:** Als <contactType> wird immer ‚technical' gesetzt.
eidas.ms.pvp2.metadata.contact.email		EmailAddress entsprechend SAML2 Metadatenspezifikation 2.3.2.2 Element <ContactPerson> **Hinweis:** Als <contactType> wird immer ‚technical' gesetzt.

1.2.9. 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
eidas.ms.advanced.attributes.ejusticerole.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.ejusticerole.mandate.mode	**Default:** forceLegal	Vollmachtenbetriebsmodus am IDA System entsprechend der Liste von Vollmachtenprofile. **Hinweis:** folgende Werte stehen zur Verfügung. • 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.ejusticerole.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.ejusticerole.value.x	eJusticePortalVip1=VIP1 **Default:**	Mappt das im Anmeldevorgang ausgewählte Vollmachtenprofil auf den Attributwert des eJustice Attributes. Bei Definiton mehrerer Mappings mux das ‚x'

		durch eine eindeutige Id ersetzt werden. **Beispie für einen Konfigurationswert:** TODO

1.2.10. 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 **Bsp:** true/false
eidas.ms.connector.x.mandates.natural	X (falls Vertretungen aktiv)	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-Connectorerlaubt 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