eIDAS-Node Migration Guide

Version 1.4.2

Document history

Version	Date	Modification reason	Modified by
1.4 Pre release	31/08/2017	Origination	DIGIT
1.4 Official release	06/10/2017	Minor update to section 3.7	DIGIT
1.4.1 Official release	15/06/2018	Document Version changed to correspond with the release. Reuse of document policy updated.	DIGIT
1.4.2	06/08/2018	Migration guide updated to describe changes made by removing vulnerability EID-631: Issuer URL in SAML AuthnRequest can be manipulated.	DIGIT (CB)

Disclaimer

This document is for informational purposes only and the Commission cannot be held responsible for any use which may be made of the information contained therein. References to legal acts or documentation of the European Union (EU) cannot be perceived as amending legislation in force or other EU documentation.

The document contains a brief overview of technical nature and is not supplementing or amending terms and conditions of any procurement procedure; therefore, no compensation claim can be based on the contents of the present document.

Table of contents

1. Introduction

This document is intended for a technical audience consisting of developers, administrators and those requiring detailed technical information on how to configure, build and deploy the eIDAS-Node application.

The purpose of this document is to facilitate migration from eIDAS-Node v1.4.1 to eIDAS-Node v1.4.2.

1.1. Document structure

This document is divided into the following sections:

Chapter 1 — *Introduction*: this section.

Chapter 2 — *Prerequisites*: Identifies any prerequisites that are required before migrating your eIDAS-Node to version 1.4.2.

Chapter 3 — *Changes*: Contains detailed information about the changes that should be taken into consideration when migrating to eIDAS-Node version 1.4.2.

1.2. Document aims

The main aim of this document is to provide information on all the changes requiring your action when migrating to eIDAS-Node version 1.4.2, including:

configuration changes; and

changes to common code.

2. Prerequisites

Before starting your migration to eIDAS-Node version 1.4.2 you should have:

already implemented eIDAS-Node version 1.4.1;
downloaded the eIDAS-Node v1.4.2 Integration Package; and
downloaded the latest documentation.

3. Changes

3.1. Summary of changes

In eIDAS-Node version 1.4.2 there are several changes that affect your installation. The main changes are:

Remove vulnerability EID-631: Issuer URL in SAML AuthnRequest can be manipulated

3.2. Validate issuer of SAML request (and SAML response)

This change validates the issuer of the metadata. **A node with an inexistent or empty whitelist for a component will not retrieve any metadata for that component.**

Specifically, the following 4 checks are performed during the EIDAS authentication flow:

The SAML Requests issued from SP's to Connector have the issuer checked against **sp.metadata.location.whitelist**

The SAML Requests issued from Connector(s) to Proxy have the issuer checked against **connector.metadata.location.whitelist**

The SAML Responses issued from IdP (s) to Proxy have the issuer checked against **idp.metadata.location.whitelist**

The SAML Responses issued from Proxy(s) to Connector have the issuer checked against a dynamic whitelist built from values of all the keys following the **pattern service1.metadata.url ... service8.metadata.url**

3.2.1. Code changes

```
EIDAS-Node\src\main\java\eu\eidas\node\auth\connector\AUCONNECTORSAML.java
EIDAS-Node\src\main\java\eu\eidas\node\auth\service\AUSERVICESAML.java
EIDAS-Specific\src\main\java\eu\eidas\node\auth\specific\SpecificEidasConnector.java
EIDAS-Specific\src\main\java\eu\eidas\node\auth\specific\SpecificEidasService.java
EIDAS-Node\src\main\webapp\WEB-INF\applicationContext.xml
      Changes necessary to retrieve and populate corresponding metadata url whitelists that
      the node is allowed to contact back to retrieve metadata necessary to verify SAML
      request / SAML response signatures (based on sp.metadata.location.whitelist,
      sp.metadata.location.whitelist, idp.metadata.location.whitelist
EIDAS-SAMLEngine\src\main\java\eu\eidas\auth\engine\ProtocolEngine.java
EIDAS-SAMLEngine\src\main\java\eu\eidas\auth\engine\ProtocolEngineI.java
      Core changes in the Protocol Engine to take into account the whitelists above when un-
      marshalling the SAML Request and Response and verify the signature of their originating
      issuer.
```

```
EIDAS-Commons\src\main\java\eu\eidas\util\WhitelistUtil.java
      Utility class for parsing a semicolumn separated list of ascii strings that represent a
      SET OF the urls.
```

3.2.2. Configuration changes

eidas.xml additions: semicolumn separated urls as values for following new keys

```
<entry key="connector.metadata.location.whitelist">
http://localhost:8080/EidasNode/ConnectorMetadata;
http://eidasnode:8888/EidasNode/ConnectorMetadata;

</entry>

<entry key="sp.metadata.location.whitelist">

http://localhost:8080/SP/metadata

</entry>

<entry key="idp.metadata.location.whitelist">

        http://localhost:8080/IdP/metadata

</entry>
```

3.3. Other fixes/improvements

No additional changes were made.