



eIDAS-Node Migration Guide

For Version 2.3.1

Document history

Version	Date	Modification reason	Modified by
1.0	07/08/2019	Information how to migrate to eIDAS-Node v2.3.1 from eIDAS-Node v2.3.0	DIGIT

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 information of a technical nature and does not supplement or amend the terms and conditions of any procurement procedure; therefore, no compensation claim can be based on the contents of this document.

© European Union, 2019

Reuse of this document is authorised provided the source is acknowledged. The Commission's reuse policy is implemented by Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents.

Table of contents

DOCUMENT HISTORY	2
TABLE OF CONTENTS	4
1. INTRODUCTION	5
1.1. Document structure	5
1.2. Document aims	5
2. PREREQUISITES	6
3. CHANGES	7
3.1. Summary of changes	7
3.2. 201907-01 vulnerability	7
3.2.1. Code changes	7
3.3. Other fixes/improvements requiring no action	8
3.3.1. EIDAS Metadata VERSION 2.3.1 update	8
3.3.2. Keystore folder for the 2.3.1 Release needs to be updated	8

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 to eIDAS-Node v2.3.1 from eIDAS-Node v2.3.

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 2.3.1.

Chapter 3 — *Changes*: Contains detailed information about the changes that should be taken into consideration when migrating to eIDAS-Node version 2.3.1.

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 2.3.1, including:

- configuration changes; and
- changes to code.

Disclaimer: The users of the eIDAS-Node sample implementation remain fully responsible for its integration with back-end systems (Service Providers and Identity Providers), testing, deployment and operation. The support and maintenance of the sample implementation, as well as any other auxiliary services, are provided by the European Commission according to the terms defined in the European Union Public License (EUPL) at https://joinup.ec.europa.eu/sites/default/files/custom-page/attachment/eupl_v1.2_en.pdf

2. Prerequisites

Before starting your migration to eIDAS-Node version 2.3.1 you should have:

- already implemented eIDAS-Node version 2.3;
- downloaded the eIDAS-Node v2.3.1 Integration Package; and
- downloaded the latest documentation.

3. Changes

3.1. Summary of changes

In the eIDAS-Node version 2.3.1 there are changed to address:

- (EID-956) 201907-01 vulnerability

For other fixes and improvements requiring no action, please see section 3.3.

3.2. 201907-01 vulnerability

A fix was implemented to resolve the 201907-01 vulnerability.

3.2.1. Code changes

The following files were changed:

EIDAS-Encryption/src/main/java/eu/eidas/auth/engine/xml/opensaml/CertificateUtil.java

EIDAS-SAMLEngine/src/main/java/eu/eidas/auth/engine/core/impl/AbstractProtocolSigner.java

Special cases for checking trust chain based on issuer in AbstractProtocolSigner.java method checkValidTrust were removed as well as unnecessary methods getIssuerCertificate and hasCredential.

It was also implemented the adding of all signature certificates to the to be trusted signature credential before trust chain validation using new method getAllSignatureCertificates on CertificateUtil to allow better validation of trust chain.

Related to this change new Junit test were added for checking certificate trust at CertificateUtilTest.java and also new test certificates replaced the previous ones.

TestEidasNodeMetadataTrustChain.java tests were adapted to new keystores so several new keystores were added at:

EIDAS-Node/src/test/resources/keystore/eIDASkeystores/

eidaskystore_Connector_CC_TrustedIntermediate.jks

eidaskystore_Connector_CC_TrustedIntermediateTrustedRoot.jks

eidaskystore_Connector_CC_TrustedLeaf.jks

eidaskystore_Connector_CC_TrustedRoot.jks

metadata.jks

metadata_TC_WITHOUT_INTERMEDIATE_CA_CERTIFICATE.jks

metadata_TC_WITHOUT_ROOT_CA.jks

metadataPlusExtraCertificate.jks

metadataSingleCertificate.jks

and previous xml files at EIDAS-Node/src/test/resources/keystore were updated

SignModule_METADATA_INTERMEDIATE_CA_ROOT_CA_TRUST.xml

SignModule_METADATA_INTERMEDIATE_CA_TRUST.xml

SignModule_METADATA_NODE_CERT_TRUST.xml

SignModule_METADATA_ROOT_CA_TRUST.xml

SignModule_METADATA_SINGLE_CERTIFICATE.xml

SignModule_METADATA_TC.xml

SignModule_METADATA_TC_WITHOUT_INTERMEDIATE_CA_CERTIFICATE.xml

SignModule_METADATA_TC_WITHOUT_ROOT_CA_CERTIFICATE.xml

SignModule_METADATA_TC_WRONG_ORDER_EXTRA_CERTIFICATE.xml

related to this tests were update accordingly.

3.3. Other fixes/improvements requiring no action

3.3.1. **EIDAS Metadata VERSION 2.3.1 update**

In eidas.xml eidas.application.identifier value was updated to 2.3.1

3.3.2. **Keystore folder for the 2.3.1 Release needs to be updated**

A new eidasKeyStore_METADATA_TC keystore was added to the demo configuration EIDAS-Config/keystore folder which, lead to the update of the existing eidasKeyStore_Connector_XX.jks and eidasKeyStore_Service_XX.jks keystores, basically the rootcametadata trusted certificate was updated. At demo configuration folder EIDAS-Config/server, the SignModule_Connector.xml and SignModule_Service.xml files also needed to be updated to the new private key in eidasKeyStore_METADATA_TC keystore