eIDAS-Node Migration Guide

Version 1.4

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

Table of contents

List of tables

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 v1.3 to eIDAS-Node v1.4.

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.
- Chapter 3 — *Changes*: Contains detailed information about the changes that should be taken into consideration when migrating to eIDAS-Node version 1.4.

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, including:

- configuration changes; and
- changes to common code.

2. Prerequisites

Before starting your migration to eIDAS-Node version 1.4 you should have:

- already implemented eIDAS-Node version 1.3;
- downloaded the eIDAS-Node v1.4 Integration Package; and
- downloaded the latest documentation.

3. Changes

3.1. Summary of changes

In eIDAS-Node version 1.4 there are several changes that affect your installation. The main changes are:

- WebLogic 12.2 family support (see section 3.2);
- SPType propagation to Proxy Service/IdP (see section 3.3);
- Correction to LegalPerson data set attributes (see section 3.4); and
- Limiting the size of IdP supplied attribute values (see section 3.5).

3.2. WebLogic 12.2 family support

Table 1: WebLogic 12.2 family support — Quick reference of changes

Subject	Item	Description
Node	`weblogic.xml`	Added extra application classloader preferred packages.
	Resource location	Renamed '`resources`' folder to '`resource`'.

Changes have been made to the eIDAS-Node in order to support WebLogic 12.2 family. Tests were made with version 12.2.1.2.0.

To avoid conflict with the Oracle embedded OpenSAML new packages/resources have been added to `weblogic.xml`. The '`resources`' folder containing javascripts, images and stylesheets has been renamed to '`resource`' because of a class loading problem. Please be sure to amend your firewall or proxy rules.

Please note: In Demo Tools the folder name remains '`resources`'.

3.3. SPType propagation to Proxy Service/IdP

Table 2: SPType propagation — Quick reference of changes

Subject	Item	Description
Node	Code changes	Propagate `SPType` to Specific

eIDAS-Node version 1.3 came with an improvement of propagating `SPType` using the `LightRequest` interface. There was a scenario when the `SPType` was not presented to MS-Specific Proxy Service, namely when it was provided by the Metadata and not the Request. This has been fixed, the Proxy Service will always present `SPType` in the `LightRequest` regardless of the way the Connector supplies it.

3.4. Correction to LegalPerson data set attributes

Table 3: Correction to LegalPerson data set attributes — Quick reference of changes

Subject	Item	Description
Node	Code changes	Added the correct attributes along with temporary logic to pick the ones supported by the other party.
Demo Tools	Configuration	Added the correct attributes to SP configuration, disabled the incorrect ones by default on the select attributes page.

There were two eIDAS core attributes mistakenly defined in eIDAS-Node version 1.3 and prior versions.

- http://eidas.europa.eu/attributes/legalperson/LegalPersonAddress was defined as http://eidas.europa.eu/attributes/legalperson/LegalAddress

- http://eidas.europa.eu/attributes/legalperson/VATRegistrationNumber was defined as http://eidas.europa.eu/attributes/legalperson/VATRegistration.

They both belong to `LegalPerson` data set and they are both optional.

In order to preserve business continuity, the solution introduces a temporary logic into eIDAS-Node v1.4 which will be backward compatible with previous versions, because:

- as a Connector, it checks the metadata of the Proxy Service for whether the erroneous or the correct ones are supported, and issues a Request accordingly;

- as a Proxy Service it will issue a Response with attributes presented in the original Request; and

- as a Proxy Service it will present both sets in the list of supported attributes in the Metadata.

The logic is temporarily implemented, it is planned to be removed when the last affected eIDAS-Node version (v1.3) is no longer supported. Starting from that future version, the old, erroneous set will no longer be supported. The following diagram illustrates how continuity is achieved:
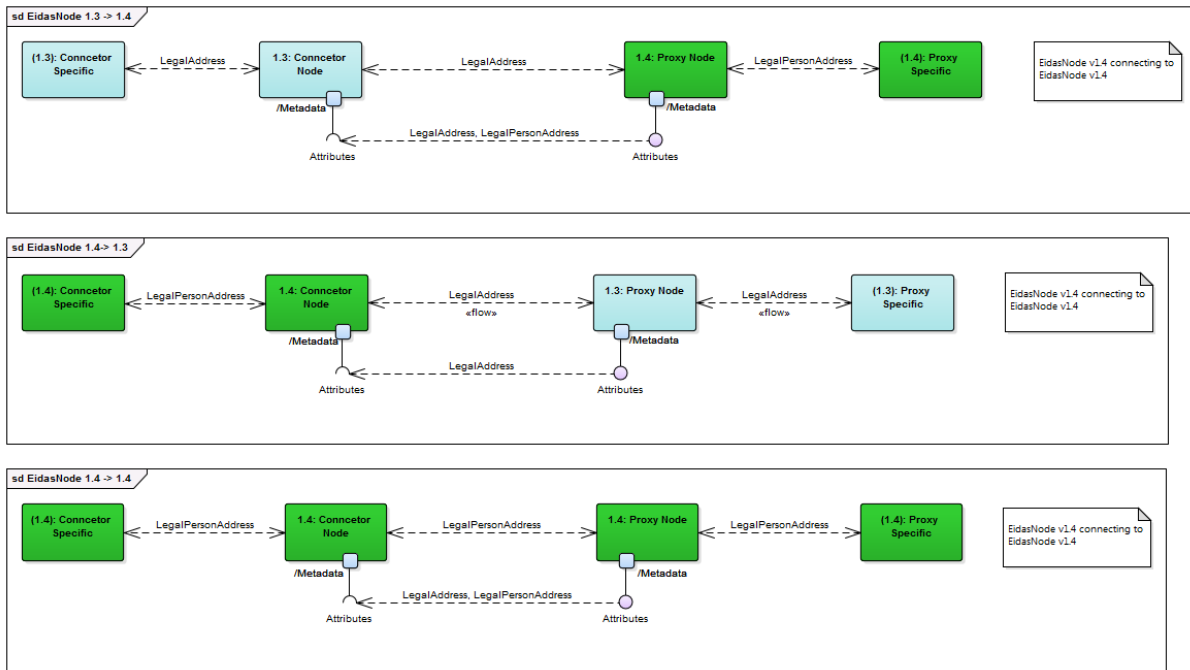
The MS-Specific part MUST supply the correct attributes in the `LightRequest` and the `LightResponse` to the eIDAS-Node. The eIDAS-Node will only send these correct attributes to the MS-Specific as well. So the usage of erroneous attributes is restricted to the Network, and the eIDAS-Node hides the switching logic. Therefore the custom MS-Specific or component connecting to the MS-Specific from national infrastructure has to be amended.

3.5.   Limiting the size of IdP supplied attribute values

Table 4: Limiting the size of IdP supplied attribute values — Quick reference of changes

Subject	Item	Description
Node	Code changes	Re-implemented missing check to Proxy Service
Node	Configuration	`max.attrValue.size` in `eidasParameters.properties`

There is a basic check implemented for IdP supplied attribute values. Proxy Service validates attribute value size supplied in `LightResponse` against a value supplied by the configuration. Attempt with any larger attribute will result in an exception.

3.5.1.   Configuration changes

The `max.attrValue.size` setting from `eidasParameters.properties` file, limits the attribute value size in bytes in the `LightResponse`.

3.6.   Use of SamlEngineClock

Table 5: Use of SamlEngineClock — Quick reference of changes

Subject	Item	Description
Node	Code changes	Code is using `ProtocolEngine` configured clock

It is possible to configure a clock implementation in `ProtocolEngine` configuration (e.g: `SamlEngine.xml`). In eIDAS-Node v1.3 and previous versions this clock was not being used in several parts of the code, causing different timestamps in SAML messages. This correction takes advantage of the provided clock when constructing SAML messages.

3.6.1.   Code changes

If you are using your own `ProtocolProcessor` implementation, you need to amend some methods. The `ProtocolProcessorI` interface has been modified in order to supply a timestamp (created by engine clock) to `ProtocolProcessor` where time is needed. Methods affected:

- `marshallRequest`;
- `marshallResponse`;
- `marshallErrorResponse`.

The old methods are still there, marked as `@Deprecated`. Those are commented to be removed, which will happen in a future version.

3.7.   Other fixes/improvements need no action

- Thread safety bug has been fixed in `DocumentBuilderFactory`;
- Removal of deprecated `PersonalAttributeList`, `PersonalAttribute`, `PersonalAttributeString` and `AttributeUtil` classes. If any of these are used in the MS-Specific part, it needs to be upgraded to classes provided by `AttributeRegistry`;
- Backslash '\' characters have been replaced with normal slash '/' in the sample configuration to support UNIX type systems;
- The code and configuration related to old DE and AT plugins was removed;
- Changed behaviour of `FileMetadataLoader` to ignore all files that are not well-formed XML or have .xml extension and log it when this occurs;
- JBoss 6 is no longer supported.
- Added missing `AddressID` element to `PostalAddress`, to be compliant with Cora ISA Vocabulary version 0.3.