eIDAS-Node Migration Guide

Version 1.4.4

Document history

Version	Date	Modification reason	Modified by
1.0	14.12.2018	Migration description to eIDAS-Node v1.4.4 (from eIDAS-Node v1.4.3).	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 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

References

[1] SAML Core 2.0, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15/03/2005, http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

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 v1.4.3 to eIDAS-Node v1.4.4.

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 1.4.4.

Chapter 3 — *Changes*: Contains detailed information about the changes that should be taken into consideration when migrating to eIDAS-Node version 1.4.4.

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 1.4.4, including:

configuration changes; and

changes to common code.

2. Prerequisites

Before starting your migration to eIDAS-Node version 1.4.4 you should have:

already implemented eIDAS-Node version 1.4.3;
downloaded the eIDAS-Node v1.4.4 Integration Package; and
downloaded the latest documentation.

3. Changes

3.1. Summary of changes

In eIDAS-Node version 1.4.4 there are several changes that affect your installation.

(EID-652) Problem in validation of entityID of SP

(EID-671) Host header poisoning

(EID-408) Arbitrary data injection in audit trail log, (EID-658) Interference with audit trail

(EID-694) CVE-2014-3625

(EID-695) CVE-2015-0201

(EID-696) CVE-2015-3192

(EID-697) CVE-2015-5211

(EID-698) CVE-2016-5007

(EID-699) CVE-2018-1270

(EID-700) CVE-2018-1271

(EID-701) CVE-2018-1272

(EID-702) CVE-2012-0881

(EID-730) Vulnerable version of JQuery

3.2. Whitelist of SAML Request/Response issuers are now considered holding URIs instead of URLs

Motivated by (EID-652) Problem in validation of entityID of SP

Until now the whitelisted issuers were considered by the EIDAS nodes as being URLs. But this was a non compliant SAML assumption as according to 8.3.6 Entity Identifier of SAML Core 2.0 documentation [1], such an identifier must be defined as a URI of no more than 1024 characters.

3.2.1. Code changes

eu.eidas.util.WhitelistUtil

To validate URI the WhitelistUtil class is doing 2 things:

1. For URI syntactic verification, It uses the create method from the java URI class. This method verifies if the checked URI violates the RFC 2396 directive.
2. To fully achieve SAML 2.0 compliancy It also checks that the whitelisted URIs are no more than 1024 characters.

WhitelistUtil logging has also been adapted. For each URI failing validation check a WARN message is printed in the log files with a corresponding stacktrace:

1. For a URI syntax error the logged Exception is an IllegalArgumentExxception caused by a java.net.URISyntaxException.
2. For a too long URI the logged exception is an IllegalArgumentExxception with the message: "Non SAML compliant URI. URI is more than 1024 characters in length".

For more information on the java URI class and its validation process , please see the corresponding Javadoc and if needed the RFC 2396 directive.

3.3. eIDAS-Node should log SAML messages for the exchanges with SP and IdP

For EIDAS-Node 1.4.4 we need to be able to track all the SAML messages that are generated and then sent by the Node/Specific and to capture the points in EIDAS-Node when the messages generated by the SP and IdP are received by the Node/Specific.

SAML messages are also logged for specific cases when the normal flow not successful for example Cancel Colleague Request, Cancel Colleague Response, choosing an invalid LoA, failed authentication at the IdP.

For the complete structure of all the SAML messages logged by the Node/Specific we are recommending to read eID Error and Event Logging document.

3.3.1. Code changes

New values have been introduced to define operation types describing SAML messages:

EIDAS-Commons\src\main\java\eu\eidas\auth\commons\EIDASValues.java

New utilities classes for logging have been created in common module:

EIDAS-Commons\src\main\java\util\logging\LoggingMarkerMDC.java

EIDAS-Commons\src\main\java\util\logging\LoggingSanitizer.java

Two new classes, each with its own implementation, have been added to deal with processing of HttpRequests and append SAML messages into the log files:

EIDAS-Node\src\main\java\eu\eidas\node\auth\LoggingUtil.java

EIDAS-Specific\src\main\java\eu\eidas\node\auth\specific\LoggingUtil.java

A new servlet class has been implemented in order to capture outgoing messages from the Proxy-Service to the Connector:

EIDAS-Node\src\main\java\eu\eidas\node\service\LogSamlServlet.java

Several classes have been modified in order to call the logging methods from LoggingUtil classes:

EIDAS-Node\src\main\java\eu\eidas\node\auth\connector\AUCONNECTORSAML.java

EIDAS-Node\src\main\java\eu\eidas\node\auth\service\AUSERVICE.java

EIDAS-Node\src\main\java\eu\eidas\node\auth\service\AUSERVICESAML.java

EIDAS-Node\src\main\java\eu\eidas\node\connector\ColleagueResponseServlet.java

EIDAS-Node\src\main\java\eu\eidas\node\connector\ConnectorControllerService.java

EIDAS-Node\src\main\java\eu\eidas\node\connector\ServiceProviderServlet.java

EIDAS-Node\src\main\java\eu\eidas\node\service\IdPResponseServlet.java

EIDAS-Node\src\main\java\eu\eidas\node\service\ServiceControllerService.java

EIDAS-Specific\src\main\java\eu\eidas\node\auth\specific\SpecificEidasService.java

EIDAS-Specific\src\main\java\eu\eidas\node\auth\specific\SpecificEidasConnector.java

EIDAS-
Specific\src\main\java\eu\eidas\node\specificcommunication\SpecificConnectorImpl.java

Some servlets were modified to forward to the new introduced servlet LogSamlServlet, such as:

EIDAS-Node/src/main/java/eu/eidas/node/service/ColleagueRequestServlet.java

EIDAS-Node/src/main/java/eu/eidas/node/service /ServiceExceptionHandlerServlet

EIDAS-Node/src/main/java/eu/eidas/node/service/IdPResponseServlet.java

New classes were introduced to allow storing and retrieving to and from cache, SAML Logging message's data:

EIDAS-Node/src/main/java/eu/eidas/node/logging/AbstractLogSamlCaching.java

EIDAS-Node/src/main/java/eu/eidas/node/logging/DistributedLogSamlCaching.java

EIDAS-Node/src/main/java/eu/eidas/node/logging/ILogSamlCachingService.java

EIDAS-Node/src/main/java/eu/eidas/node/logging/LogSamlHolder.java

EIDAS-Node/src/main/java/eu/eidas/node/logging/SimpleLogSamlCaching.java

Several properties have been added in the beans:

EIDAS-Specific\src\main\resources\specificApplicationContext.xml

EIDAS-Node\src\main\webapp\WEB-INF\applicationContext.xml

Several test classes have been adapted to the new implementation:

EIDAS-Specific\src\test\java\eu\eidas\node\specificcommunication\SpecificConnectorImplTest.java

EIDAS-Specific\src\test\java\eu\eidas\node\specificcommunication\SpecificProxyServiceImplTest.java

EIDAS-Node/src/test/java/eu/eidas/node/auth/service/tests/AUSERVICECitizenTestCase.java

EIDAS-Node/src/test/java/eu/eidas/node/auth/service/tests/AUSERVICESAMLTestCase.java

EIDAS-Node/src/test/java/eu/eidas/node/auth/service/tests/AUSERVICETestCase.java

Also a new parameter, originatingResponseId, was added to ISERVICESAMLService and ISERVICEService interface methods generateSamlTokenFail. A new method was added to LoggingUtil to retrieve IAuthentication response from http request. Similar change to the signature of sendFailure at AUSERVICE was implemented, adding originatingResponseId parameter.

The old methods prepareReqLoggerBean, prepareRespLoggerBean, saveLog, getLoggerBean were removed from AUCONNECTORSAML and AUSERVICESAML and due to that:

signature of checkAntiReplay checkServiceCountryToCitizenCountry and checkResponseLoA methods in AUCONNECTORSAML and of checkAntiReplay at AUSERVICESAML were changed removing unused parameters.

The ResponseCarryingServiceException constructor was refactored to take issuer of request as parameter. Several Jsp pages were changed

EIDAS-Node/src/main/webapp/citizenConsent.jsp

EIDAS-Node/src/main/webapp/presentConsent.jsp

EIDAS-Node/src/main/webapp/presentSamlResponseError.jsp

Hidden input field logSamlToken was added to allow LogSamlServlet to receive the information necessary to log the messages and other existing ones removed.

Renaming of enum constants at

EIDAS-Node/src/main/java/eu/eidas/node/NodeParameternames.java.

A new constant was added at

EIDAS-Node/src/main/java/eu/eidas/node/NodeViewNames.java

3.3.2. Configuration changes

A new cache was introduced named proxyServiceLogSamlCacheService, at

EIDAS-Config\server\hazelcast.xml.

Two new properties were added to

EIDAS-Config\server\eidas.xml

saml.audit was introduced in order to activate or deactivate logging of SAML messages and nonDistributedLogSaml. Retention was added to fine tune retention period of SimpleLogSamlCaching cache, set by default with the same value as for the distributed version proxyServiceLogSamlCacheService set in hazelcast.xml.

3.4. CSP report handler uri.

Motivated by (EID-671) Host header poisoning.

Until now, the CSP report handler URI was obtained from various sources taken out of the HTTP Request. This could be a vulnerability as the Node was trusting information coming from the outside world contained in the HTTP Request. To solve this issue, the new property security.header.CSP.report.uri was added in the eidas.xml.

Note: If this property is not defined, the following warning message will be displayed in the log files: "*Node configuration has no URI defined for the CSP reporting feature. CSP violation will not be reported*".

3.5. Upgrading Apache Xerces library to avoid potential Dos attack.

This was motivated by (EID-702).

As mentioned in CVE-2012-0881, Apache Xerces library 2.11 is vulnerable to Denial of Services. To avoid the risk of CVE-2012-0881, Apache Xerces library was upgraded to 2.12. Please upgrade, if appropriate, Apache Xerces libraries in your server configuration.

3.6. Other fixes/improvements

3.6.1. Implemented CRLF protection for audit logs.

As already implemented in the 2.x branch, and motivated by EID-408 & EID-658, the LoggingSanitizer was implemented that contains removeCRLFInjection method to prevent CRLF injection. This method is executed in AUCONNECTORSAML.java and AUSERVICESAML.java for some fields that are external to the node and whose content, potentially containing CRLF injection, are printed into log files.

3.6.2. Upgrade spring version from 4.1.0 to 4.3.18.

This was motivated by issues (EID-694, EID-695, EID-696, EID-697, EID-698, EID-699, EID-700, EID-701).

This upgrading of the spring framework was needed to solve some vulnerabilities existing in previous releases of the spring framework, see https://www.cvedetails.com

3.6.3. Fixed missing relayState when user cancels consent on Response attribute values.

Corrected the relayState if check code in citizenConsent.jsp so that in the case of user consent cancel in Response attributes, the relayState is included in the form if it is not null.

3.6.4. Upgrading Vulnerable version JQuery 1.11.3 to 3.3.1.

This was motivated by (EID-730).

Upgraded /EidasNode/resource/skin0/js/jquery-1.11.3.min.js to jquery-3.3.1.js

The JQuery library at version 1.11.3 had multiple known security issues. For more information, see:

https://github.com/jquery/jquery/issues/2432
http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/
https://nvd.nist.gov/vuln/detail/CVE-2015-9251
http://research.insecurelabs.org/jquery/test/

.

3.6.5. EIDAS-SpecificCommunicationDefinition wrong jar name

The jar produced at the EIDAS-SpecificCommunicationDefinition module had the wrong name. The wrong finalName element was removed from the pom so that the eidas-specific-communication-definition.jar is produced as expected.