eIDAS-Node eID Error and Event Logging v2.6

eIDAS eID Implementation

Exported on 04/15/2022

Table of Contents

Document history

Version	Date	Modification reason	Modified by
1.0	06/10/2017	Extracted from Installation Manual	DIGIT
2.0	11/04/2018	• Editorial improvements • Update to Error Codes and Error Messages	DIGIT
2.1	06/07/2018	• Reuse of document policy updated and version changed to match the corresponding Release.	DIGIT
2.3	20/06/2019	Added information regarding the new implementation of message logging. Other updates to existing examples regarding Zulu time improvement.	DIGIT
2.4	06/12/2019	• Editorial improvements • Minor Updates	DIGIT
2.5	11/12/2020	eIDAS-Node 2.5 release	DIGIT
2.6	04/2022	eIDAS-Node 2.6 release	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.

List of abbreviations

The following abbreviations are used within this document.

Abbreviation	Meaning
eIDAS	electronic Identification and Signature. The Regulation (EU) N°910/2014[1] governs electronic identification and trust services for electronic transactions in the internal market to enable secure and seamless electronic interactions between businesses, citizens and public authorities.
IdP	Identity Provider. An institution that verifies the citizen's identity and issues an electronic ID.
MS	Member State
SAML	Security Assertion Markup Language
SP	Service Provider

List of definitions

The following definitions are used within this document.

Term	Meaning
Audit	A function which seeks to validate that controls are in place, adequate for their purposes, and which reports inadequacies to appropriate levels of management.
Audit log	An audit log is a chronological sequence of audit records, each of which contains evidence directly as a result of the execution of a business process or system function
eIDAS-Node	An eIDAS-Node is an application component that can assume two different roles depending on the origin of a received request. See eIDAS-Node Connector and eIDAS-Node Proxy Service.

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

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.

This document provides information on the eID implementation of error and event logging as a building block for generating an audit trail of activity on the eIDAS Network. It describes the files that are generated, the file format, the components that are monitored and the events that are recorded. It is also presents points that should be considered when planning, implementing and operating an auditing environment.

1.1 Purpose

The purpose of this document is to describe the strategy for logging of errors and events in the eIDAS-Node.

1.2 Document Structure

This document is divided into the following sections:

- Chapter 1 – *Introduction:* this section.
- Chapter 2 – *What is an audit trail?* Introduces the concept of an audit trail and discusses the forensics and diagnosis of audit trail analysis.
- Chapter 3 – *Standards, frameworks and best practices* provides a brief introduction to industry standards and guidelines that should be considered when implementing a logging and auditing scheme.
- Chapter 4 – *Log generation* shows the format and describes the information attributes that are contained in a log record.
- Chapter 5 – *Logging configuration settings* discusses log management requirements and recommendations.
- Chapter 6 – *Log files* describes the locally stored log files and presents a matrix of which events are logged, in which log file and which response would be triggered.
- Chapter 7 – *eIDAS-Node* messages logging provides information about the information stored in the logs regarding incoming and outgoing messages.
- Chapter 8 – *Operational considerations* contains information that should be taken into account when implementing a logging process.
- Chapter 9 – *References* contains a list of reference material with links.
- Appendix A – *eIDAS-Node Error Codes and Error Messages* contains a list of error code and associated message properties.
- Appendix B – Full Logging examples

1.3 Other technical reference documentation

We recommend that you also familiarise yourself with the following eID technical reference documents which are available on **Digital Home > eID :**

- *eIDAS-Node Installation, Configuration and Integration Quick Start Guide* describes how to quickly install a Service Provider, eIDAS-Node Connector, eIDAS-Node Proxy Service and IdP from the distributions in the release package. The distributions provide preconfigured eIDAS-Node modules for running on each of the supported application servers.
- *eIDAS-Node Installation and Configuration Guide* describes the steps involved when implementing a Basic Setup and goes on to provide detailed information required for customisation and deployment.
- *eIDAS-Node National IdP and SP Integration Guide* provides guidance by recommending one way in which eID can be integrated into your national eID infrastructure.
- *eIDAS-Node Demo Tools Installation and Configuration Guide* describes the installation and configuration settings for Demo Tools (SP and IdP) supplied with the package for basic testing.

- *eIDAS-Node and SAML* describes the W3C recommendations and how SAML XML encryption is implemented and integrated in eID. Encryption of the sensitive data carried in SAML 2.0 Requests and Assertions is discussed alongside the use of AEAD algorithms as essential building blocks.
- *eIDAS-Node Security Considerations* describes the security considerations that should be taken into account when implementing and operating your eIDAS-Node scheme.
- *eIDAS-Node Error Codes* contains tables showing the error codes that could be generated by components along with a description of the error, specific behaviour and, where relevant, possible operator actions to remedy the error.

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 What is an audit trail?

A log is a record of the events occurring within an organisation's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network.

An audit trail consists of a number of log records providing documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure or event.

In a stand-alone system, all the security relevant activities in individual components can be isolated. This allows us to maintain a time-ordered list of all actions and events (e.g. audit trail) that happened in the system and enabling us to audit the system by simply following the information trail in a single place, obeying to a defined notation and in a specific timeline.

The number, volume and variety of different systems operating in an eIDAS-Network's distributed architecture has created the need for security log management and safeguards to help protect the confidentiality, integrity, and availability of service and the data therein. With this in mind, an audit trail must meet two very important requirements:

- The possibility of reconstructing an entire transaction by linking all related request/response identifiers throughout the complete path of the request processing, from Service Provider to eIDAS-Node to Identity Provider and back.
- The association between an incoming request and all subsequently-related outgoing request(s), as well as the corresponding replies

In order to meet these requirements the eIDAS-Node implementation is required to record and retain audit-logging information sufficient to answer the following questions:

- Who performed the logging (the main component or an external module/party)?
- What activity was performed? (e.g. Input, Process, Output)
- Who or what performed the activity, including where or on what system the activity was performed from (subject)?
- What the activity was performed on (object)?
- When was the activity performed?
- What tool(s) was used to perform the activity?
- What was the status (such as success/failure), outcome, or result of the activity?

2.1 Forensics and diagnostics

Analysis of the audit trail will help to identify use and abuse of the eIDAS Network, including the following conditions:

- Sequencing failure
- Excessive use
- Data changes
- Fraud and other criminal activities
- Suspicious, unacceptable or unexpected behaviour
- Modifications to configuration
- Application code file and/or memory changes input validation failures e.g. protocol violations, unacceptable encodings, invalid parameter names and values
- Output validation failures e.g. database record set mismatch, invalid data encoding
- Authentication successes and failures
- Authorisation (access control) failures
- Session management failures e.g. cookie session identification value modification

- Application errors and system events e.g. syntax and runtime errors, connectivity problems, performance issues, third party service error messages, file system errors, file upload virus detection, configuration changes
- Application and related systems start-ups and shut-downs, and logging initialisation (starting, stopping or pausing)
- Use of higher-risk functionality e.g. network connections, addition or deletion of users, changes to privileges, assigning users to tokens, adding or deleting tokens, use of systems administrative privileges, access by application administrators, all actions by users with administrative privileges, access to payment cardholder data, use of data encrypting keys, key changes, creation and deletion of system-level objects, data import and export including screen-based reports, submission of user-generated content - especially file uploads
- Legal and other opt-ins e.g. permissions for mobile phone capabilities, terms of use, terms & conditions, personal data usage consent, permission to receive marketing communications

3 Standards, frameworks and best practices

Standards and frameworks like COBIT (Control Objectives for Information and Related Technology) by the Technology IT Governance Institute and the Information Systems Audit and Control Association (ISACA) and ITIL (Information Technology Infrastructure Library) provide information on IT governance and auditing. However there is little regulatory guidance on the specific controls, the standard of due care means doing at least what one's peers are doing as well as following security best practices frameworks as proposed by COBIT, BITS, COSO and standards including ISO 17799 and NIST SP 800-53 and ISF Standard of Good Practice, ISO / ISO 27002.

Note: The eIDAS-Node logs may contain person identification data, hence these logs should be handled and protected appropriately in accordance with the European privacy regulations [Dir. 95/46/EC] and [Reg. 2016/679].

[Reg. 2016/679] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[Dir. 95/46/EC] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

4 Log generation

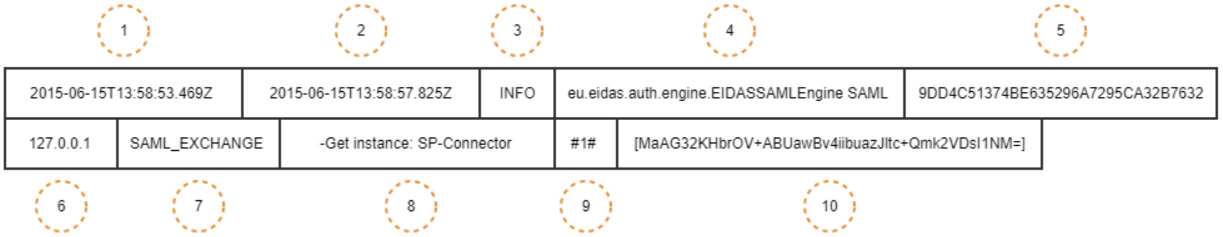
The following table shows the information attributes that are contained in a log record.

Table 1: Log record attributes

Name	See Figure 1	Description
Date time	1	The date time of the logging event in Zulu Time, also known as Coordinated Universal Time (UTC) format.
Thread	2	Outputs the name of the server processing thread that generated the logging event.
Level	3	Outputs the level of the logging event. • **ERROR**: some type of failure has occurred, users are probably being affected (or will soon be) and the fix probably requires human intervention. • **WARN**: an unexpected technical or business event occurred, users may be affected, but probably no immediate human intervention is required. Support personnel will want to review these issues a soon as possible to understand what the impact is. Basically any issue that needs to be tracked but may not require immediate intervention. • **INFO**: things we want to see at high volume in case we need to forensically analyse an issue. Typical business exceptions can go here (e.g. login failed due to bad credentials). • **DEBUG**: used for entry/exit of most non-trivial methods and detailed information on the flow through the system. This will be written to logs only. • **TRACE**: this would be for extremely detailed and potentially high volume logs that you do not typically want enabled even during normal development.
ClassName	4	Outputs location information of the caller's (Java) class which generated the logging event.
sessionId	5	If available the session Id.
IpAddress	6	If available the Remote IP address.
Even	7	If available, the type of logging event.
Message	8	The content of the message

Name	See Figure 1	Description
EventNumber	9	Sequential increasing number of the event
Hash	10	A hash generated of the line log content guaranteeing integrity

The following is an example of log content showing three log records.



2015-06-15T13:58:53.469Z	2015-06-15T13:58:57.825Z	INFO	eu.eidas.auth.engine.EIDASSAMLEngine SAML	9DD4C51374BE635296A7295CA32B7632
127.0.0.1	SAML_EXCHANGE	-Get instance: SP-Connector	#1#	[MaAG32KHbrOV+ABUawBv4iibuazJltc+Qmk2VDsI1NM=]

```
2015-06-15T13:58:57.825Z [http-bio-8080-exec-2] DEBUG eu.eidas.auth.engine.EIDASSAMLEngine -9DD4C51374BE6
35296A7295CA32B7632 -127.0.0.1 SAML_EXCHANGE -null #2# [/
d5F9UqFZy3OY37PA500TGpepPczdUzbJigiZxGIa2E=]
2015-06-15T13:59:07.212Z [http-bio-8080-exec-2] INFO  eu.eidas.node.auth.connector.AUCONNETORSAML -9DD4C5
1374BE635296A7295CA32B7632 -127.0.0.1 SAML_EXCHANGE -Connector - Processing SAML Request with ID _a4352
6c05fc8168879b5789ba0d62744 #3# [AeRp3ofGkl3gcIEH4QypViREHPB9Kw+hFFpt1DdUKGc=]
```

Figure 1: Example of log content

Notes: The following shows the attribute delimiters and their meaning

# is used as a field delimiter

[ ] delimits optional components

Important: Additional attributes may be added in future phases of this project.

Figure 2 below show examples of log records on an eIDAS-Node.

```
2015-06-15T13:58:53.469Z [http-bio-8080-exec-2] INFO  eu.eidas.auth.engine.EIDASSAMLEngine SAML_EXCHANGE -9
DD4C51374BE635296A7295CA32B7632 -127.0.0.1 -Get instance: SP-Connector  #1#
[MaAG32KHbrOV+ABUawBv4iibuazJltc+Qmk2VDsI1NM=]
2015-06-15T13:59:07.212Z [http-bio-8080-exec-2] INFO  eu.eidas.node.auth.connector.AUCONNECTORSAML
 SAML_EXCHANGE -9DD4C51374BE635296A7295CA32B7632 -127.0.0.1 -Connector - Processing SAML Request with
ID _a43526c05fc8168879b5789ba0d62744 #3# [AeRp3ofGkl3gcIEH4QypViREHPB9Kw+hFFpt1DdUKGc=]
...
2015-06-15T13:59:07.393Z [http-bio-8080-exec-2] INFO  eu.eidas.auth.engine.EIDASSAMLEngine SAML_EXCHANGE -9
DD4C51374BE635296A7295CA32B7632 -127.0.0.1 -Get instance: Connector-Service  #15# [lJCReY/
HA7Kcc9HyKuJww2qFRvjSxkQfmw/1sBGnxH8=]
2015-06-15T13:59:07.529Z [http-bio-8080-exec-2] INFO  eu.eidas.node.auth.connector.AUCONNECTORSAML
 SAML_EXCHANGE -9DD4C51374BE635296A7295CA32B7632 -127.0.0.1 -Connector - Processing SAML Request with
ID _a43526c05fc8168879b5789ba0d62744 #16# [zsSBlcAwF8Lg1Ig7u2S//OtoklvnnLZnAPcWX6Quci8=]
...
```

```
2015-06-15T13:59:08.445Z [http-bio-8080-exec-2] INFO  eu.eidas.auth.engine.EIDASSAMLEngine SAML_EXCHANGE -9
DD4C51374BE635296A7295CA32B7632 -127.0.0.1 -Get instance: Service  #29# [/
K59pCfDIfHDTBiQKc1n5VLKBtdOprWsEumnndh8TIQ=]
2015-06-15T13:59:08.697Z [http-bio-8080-exec-2] INFO  eu.eidas.node.auth.service.AUSERVICESAML
 SAML_EXCHANGE -9DD4C51374BE635296A7295CA32B7632 -127.0.0.1 -Service - Processing SAML Request with ID _d
41ae1dc063c7e4a87f17e57fdbc1329 #31# [rkLbukPhl+5ia+wzzJyVY2DHHfz2JlXPvpT1CmHRZgw=]
```

Figure 2: Log records on IT-eIDAS-Node

In cases where, the information to be logged is generated by other than an eIDAS-Node, sanitizing can be applied. The string, with information, will be escaped if it contains any of the following characters Carriage Return (ASCII 13, \r) and/or Line Feed (ASCII 10, \n) and CRLF. Furthermore, a suffix will be added to the original string to signal the modification of the original information.

5 Logging configuration settings

The deployer or host of the eIDAS-Node and related specific components should ensure that other jurisdiction or organisation specific, guidelines, and procedures with respect to logging and to incorporate and support these log management requirements and recommendations; also comply with functional and operational requirements. The following table provides examples of the types of logging configuration settings to be specified in policies, which are MS specific.

Table 2: Logging configuration settings

Category	Low Impact Systems	Moderate Impact Systems	High Impact Systems
How long to retain log data	1 to 2 weeks	1 to 3 months	3 to 12 months , in absence of specific legal requirements
How often to rotate logs	Optional (if performed, at least every week or every 25 MB)	Every 6 to 24 hours, or every 2 to 5 MB	Every 15 to 60 minutes, or every 0.5 to 1.0 MB
If the organisation requires the system to transfer log data to the log management infrastructure, how frequently that should be done	Every 3 to 24 hours	Every 15 to 60 minutes	At least every 5 minutes
How often log data needs to be analysed locally (through automated or manual means)	Every 1 to 7 days	Every 12 to 24 hours	At least 6 times a day
Whether log file integrity checking needs to be performed for rotated logs	Optional	Yes	Yes
Whether rotated logs need to be encrypted	Optional	Optional	Yes
Whether log data transfers to the log management infrastructure need to be encrypted or performed on a separate logging network	Optional	Yes is feasible	Yes

6 Log files

Each eIDAS Node is configured to generate four different locally stored log files for tracing activities:

- **The Application System log:** (eIDASNodeSystem) contains all the events occurring at the application level (e.g. server start/stop, change of configuration).
- **The Application Security log**: (eIDASNodeSecurity) contains all the security related events.
- **The Message Exchange log:** (eIDASNodeSAMLExchange) contains the details about exchanged messages.
- **The Debug Message Exchange log**: (eIDASNodeFullMsgExchange) contains the full content of the messages that are exchanged by the Node.
- **The Application Detailed log**: (eIDASNodeDetail) contains the more detailed information at destination to the technical team for forensics, investigation and debugging purposes.

The locations of the audit files are by default configured to use a Java system properties variable called LOG_HOME.

A value can be assigned to this variable by using: *-DLOG_HOME="<myDirectoryName>"* at server start-up.

If modification of the environment variable is not possible, the value of this variable could also be assigned by adding the following line in the *logback.xml* file *<property name="LOG_HOME" value ="<myDirectoryName>" />*

The following table shows a matrix of which events are logged, in which log file and which response would be triggered.

Table 3: Event log matrix

		Record in log file						Response type			
Event	**System**	**Detailed**	**Security**	**MessageExchg**	**Console**	**Appl. server log**	**Threshold level (see Table 1)**	**Immediate**	**Routine**	**Forensics - historic**	**Comment**
SAML request processing \ [EVT-1\]		√		√	√		Info		√		Normal processing of the SAML messages
SAML Response processing \ [EVT-2\]		√		√	√		Info		√		Normal processing of the SAML messages
OpenSAML Error \[EVT-3\]		√		√	√		Error	√			Error occurs in the OpenSAML product library

		Record in log file						Response type			
Event	**System**	**Detailed**	**Security**	**MessageExchg**	**Console**	**Appl. server log**	**Threshold level (see Table 1)**	**Immediate**	**Routine**	**Forensics - historic**	**Comment**
Configuration change \ [EVT-4\]	√				√				√	√	Configuration change via management console
Configuration reload \ [EVT-5\]	√				√				√	√	
Application startup \ [EVT-6\]	√					√			√	√	Start of application filters
Application shutdown \ [EVT-4\]	√					√			√	√	Start of application filters
Console alerts \[EVT-5\]	√	√			√			√		√	

		Record in log file						Response type			
Event	**System**	**Detailed**	**Security**	**MessageExchg**	**Console**	**Appl. server log**	**Threshold level (see Table 1)**	**Immediate**	**Routine**	**Forensics - historic**	**Comment**
Exceptions Application errors and system events e.g. syntax and runtime errors, connectivity problems, performance issues, file system errors \ [EVT-6\]		√			√			√			
Unauthorised access attempt to management console \ [EVT-7\]		√	√		√			√			
Input validation failures \ [EVT-8\]		√	√		√				√		Could hide an attack
Output validation failures \ [EVT-9\]		√	√		√				√		Could hide an attack

		Record in log file						Response type			
Event	**System**	**Detailed**	**Security**	**MessageExchg**	**Console**	**Appl. server log**	**Threshold level (see Table 1)**	**Immediate**	**Routine**	**Forensics - historic**	**Comment**
Session management failures e.g. cookie session identification value modification \ [EVT-10\]		√	√		√			√			Could hide an attack
Content security violation \ [EVT-11\]		√	√		√			√			Could hide an attack
Sequencing failure (like SAML Response without being preceded by SAML Request) \[EVT-12\]		√	√		√			√			Could hide an attack
Excessive use (like SAML request limitation exceeded) \ [EVT-13\]		√	√		√			√			Could hide an attack

		Record in log file						Response type			
Event	**System**	**Detailed**	**Security**	**MessageExchg**	**Console**	**Appl. server log**	**Threshold level (see Table 1)**	**Immediate**	**Routine**	**Forensics - historic**	**Comment**
Certificate not valid \ [EVT-13\]		√	√		√			√			Could hide an attack
Signature not valid \ [EVT-14\]		√	√		√			√			Could hide an attack

6.1 Event detailed error codes and associated actions

For full information on eIDAS-Node error codes and associated actions, refer to the *eIDAS-Node Error Codes* document.

7 eIDAS-Node messages logging

The incoming and outgoing Light Requests/Light Responses and eIDAS Requests and Responses to the eIDAS Node are logged in 8 points as depicted in the below Figure 3.

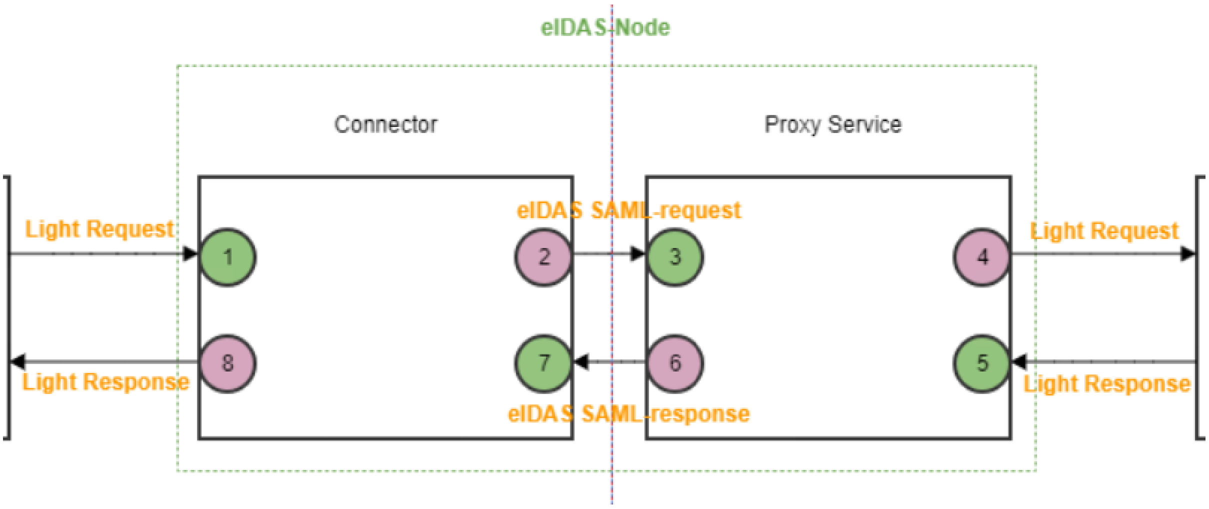


Figure 3: Message Logging diagram

7.1 Enabling of the logging

To enable the logging, the following entries may be set in the eidas.xml configuration file.

Key	Description
saml.audit	Activated the logging of information regarding incoming outgoing LightRequest/LightResponse, eIDAS Request and Response. If true logs information about the mentioned incoming requests and responses and does not log if false. Default value: true (This logging is activated by default).
full.message.logging	Activate the logging of the full content of the incoming or outgoing message (LightRequest, LightResponse, eIDAS Request and eIDAS Response). If true, logging will be executed, if false or not present the logging will not be executed. This functionality should only be used for debug purposes.

7.2 Selection of the logging file

The locations of the audit files are by default configured to use a Java system properties variable called LOG_HOME.

A value can be assigned to this variable by using: *-DLOG_HOME="<myDirectoryName>"* at server start-up.

If modification of the environment variable is not possible, the value of this variable could also be assigned by adding the following line in the *logback.xml* file
<property name="LOG_HOME" value ="<myDirectoryName>" />

7.3 Description of the logging entries

Note: The eIDAS-Node logs may contain person identification data; hence, these logs should be handled and protected appropriately in accordance with the European privacy regulations [Dir. 95/46/EC] and [Reg. 2016/679].

[Reg. 2016/679] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

At each of these points, information regarding the message is logged with different entries. The following table describes the logging entries:

Entry	Description	Remarks
Timestamp	Current time.	UTC (Zulu)
OpType	Operation type can be receives or sends.	
NodeId	The Id of the node from which this message was received (in case of OpType receives) or to which it will be sent (in case of OpType sends).	For eIDAS Requests and eIDAS Responses to the EntityId.
Origin	The origin of the incoming message. (e.g., HTTP referer header.)	N/A for OpType sends
Destination	The destination of the message	
flowId	The Id of the eIDAS flow. Used to relate messages from the same eIDAS authentication process.	The same eIDAS authentication flow will have 2 different flowIds one for Connector and another for Proxy-Service.
msgId	Id of the message	
msgHash	Hash of the message	Uses SHA512.
bltHash	Hash of the Binary Light Token	Uses Sha512. Only logged for Light Request and Light Responses.

Entry	Description	Remarks
inResponseTo	Id of request to which the response is related.	Only logged for Responses.
statusCode	Status code of the response.	Only logged for Responses.

The correlation of requests and responses can be done using the entries: *msgId*, *flowId*, and *inResponseTo*.

One example of the values logged for all the 8 points is as follows. Note that the line hashes were not included for more readability as you would find in *eIDASNodeDetail* or in *eIDASNodeSAMLExchange* files.

Point 1

Timestamp	2019-06-17T13:36:30.269Z,
OpType	eIDAS Connector receives request from Specific Connector,
NodeId	specificConnector,
Origin	http://localhost:8080/SpecificConnector/ServiceProvider,
Destination	http://localhost:8080/EidasNode/SpecificConnectorRequest,
flowId	_teeF25P50axuRHOk5uP1K_678N9D5oP1j_khKNqjuV59yOeHFqmocWSJoIZACjD,
msgId	87cc1ae7-10df-4237-acf2-ac4957c4f899,
msgHash	ENshi09fT2f6Z5hwUj8DCF9SQmdkOJ7wiZVS9yJNskV+Obrs2kMoe3S1GokcaffUOCVOhOIw4dsT8a94pLTTMw==,
bltHash	6MA9YGjgD22SYyoLqJJDxD4y1xiTM0rA8Azv9RYLCpyL6LaSqwOZx9mAvIPZCfTxMVn/7vCycFjjExTPn8GqgQ==

Point 2

Timestamp	2019-06-17T13:36:30.840Z,
OpType	eIDAS Connector sends request to eIDAS Proxy Service,
NodeId	http://localhost:8081/EidasNode/ServiceMetadata,[2]

[2] http://localhost:8081/EidasNode/ServiceMetadata,Origin

Origin	N/A,
Destination	http://localhost:8081/EidasNode/ColleagueRequest,[3]
flowId	_teeF25P50axuRHOk5uP1K_678N9D5oP1j_khKNqjuV59yOeHFqmocWSJoIZACjD,
msgId	_0at.n7PwAPBqTvJd0pV1X-DV.NxNtwHWIpSiAYi2hpqiPWxfwEJLvTgwzGEHJ9N,
msgHash	0oFuUvWD9FNGhIvltp2LrOEPQLoRnYNhhDksaDmqObipFoTVet6cytx1658Mjb4ub9mwam4ctK7L2JvvcniPnQ==

Point 3

Timestamp	2019-06-17T13:36:31.490Z,
OpType	eIDAS Proxy Service receives request from eIDAS Connector,
NodeId	http://localhost:8080/EidasNode/ConnectorMetadata,[4]
Origin	http://localhost:8080/EidasNode/SpecificConnectorRequest,[5]
Destination	http://localhost:8081/EidasNode/ColleagueRequest,[6]
flowId	_dKIqa0LWWcAzxNR67B4vh5r0.Cv-28vRyOH.B3VV5sTLt3Pn.ViOVmoJaxqQOfF,
msgId	_0at.n7PwAPBqTvJd0pV1X-DV.NxNtwHWIpSiAYi2hpqiPWxfwEJLvTgwzGEHJ9N,
msgHash	0oFuUvWD9FNGhIvltp2LrOEPQLoRnYNhhDksaDmqObipFoTVet6cytx1658Mjb4ub9mwam4ctK7L2JvvcniPnQ==

Point 4

Timestamp	2019-06-17T13:36:31.635Z,

[3] http://localhost:8081/EidasNode/ColleagueRequest,flowId
[4] http://localhost:8080/EidasNode/ConnectorMetadata,Origin
[5] http://localhost:8080/EidasNode/SpecificConnectorRequest,Destination
[6] http://localhost:8081/EidasNode/ColleagueRequest,flowId

OpType	eIDAS Proxy Service sends request to Specific Proxy Service,
NodeId	specificProxyService,
Origin	N/A,
Destination	http://localhost:8081/SpecificProxyService/ProxyServiceRequest,[7]
flowId	_dKIqa0LWWcAzxNR67B4vh5r0.Cv-28vRyOH.B3VV5sTLt3Pn.ViOVmoJaxqQOfF,
msgId	_GfAaa-Kz2X.gdywQuGMwd133hYM3TdgC6nrZ1r6qCr2elzRxFagueLd8VYTnGWR,
msgHash	utu1Z4sHax2W/0mZd4jx44TGpdKuJj7HKv7VlJ/PHL7fx5joUFUl7u0+mcEdE9BDPRk672VlLxhAgOgwMTwpGg==,
bltHash	uU8WCpZQejNKFXjiSHoRQnZPe19VcB1YsR7D5MiSNZlEZCy1/6rmanPs7rx8zZ2/O4IzI8ub74vSi34m9FZXEw==

Point 5

Timestamp	2019-06-17T13:37:18.970Z,
OpType	eIDAS Proxy Service receives response from Specific Proxy Service,
NodeId	specificProxyService,
Origin	http://localhost:8081/SpecificProxyService/AfterCitizenConsentResponse,[8]
Destination	http://localhost:8081/EidasNode/SpecificProxyServiceResponse,[9]
flowId	_dKIqa0LWWcAzxNR67B4vh5r0.Cv-28vRyOH.B3VV5sTLt3Pn.ViOVmoJaxqQOfF,
msgId	3e1b6aee-fa0b-44a3-add0-09d81826cd66,

[7] http://localhost:8081/SpecificProxyService/ProxyServiceRequest,flowId

[8] http://localhost:8081/SpecificProxyService/AfterCitizenConsentResponse,Destination

[9] http://localhost:8081/EidasNode/SpecificProxyServiceResponse,flowId

msgHash	04IClOQQSWaeZ/5kUxDFYJw7qVZgOKuvrnfwYEbwgbkqhxkNBUG4XajPDd1zc4S7NTerGEOvJdZ8e2TmM9GDkQ==,
bltHash	LCb+tPt+fSlGgc9l3KRbiRljLkaXnlRiNFj1WyBLSh6g4Cb2N8LETdtdKuOk9yLhUcGRk/wxRKMAPJyzA+23MA==,
inResponseTo	_GfAaa-Kz2X.gdywQuGMwd133hYM3TdgC6nrZ1r6qCr2elzRxFagueLd8VYTnGWR,
statusCode	urn:oasis:names:tc:SAML:2.0:status:Success

Point 6

Timestamp	2019-06-17T13:37:21.168Z,
OpType	eIDAS Proxy Service sends response to eIDAS Connector,
NodeId	ttp://localhost:8080/EidasNode/ConnectorMetadata,[10]
Origin	N/A,
Destination	http://localhost:8080/EidasNode/ColleagueResponse,[11]
flowId	_dKIqa0LWWcAzxNR67B4vh5r0.Cv-28vRyOH.B3VV5sTLt3Pn.ViOVmoJaxqQOfF,
msgId	_e1hSsKlpJ.OW-wCEzbgnbGc2lhd1PTKXwYgtz8Id9.UCpWlmUBt.jAFtWRAAckd,
msgHash	9drKEZ8ixvQ8ycKCMVl6t5xwE8QiI7sZuQYrHqFXLZJuDAHlFYwCM6dQiEWxUE8yHzHrYNWxf1v4/7vr+dXjHQ==,
inResponseTo	_0at.n7PwAPBqTvJd0pV1X-DV.NxNtwHWIpSiAYi2hpqiPWxfwEJLvTgwzGEHJ9N,
statusCode	urn:oasis:names:tc:SAML:2.0:status:Success

Point 7

[10] http://localhost:8080/EidasNode/ConnectorMetadata,Origin
[11] http://localhost:8080/EidasNode/ColleagueResponse,flowId

Timestamp	2019-06-17T13:37:21.896Z,
OpType	eIDAS Connector receives response from eIDAS Proxy Service,
NodeId	http://localhost:8081/EidasNode/ServiceMetadata,[12]
Origin	http://localhost:8081/EidasNode/SpecificProxyServiceResponse,[13]
Destination	http://localhost:8080/EidasNode/ColleagueResponse,[14]
flowId	_teeF25P50axuRHOk5uP1K_678N9D5oP1j_khKNqjuV59yOeHFqmocWSJoIZACjD,
msgId	_e1hSsKlpJ.OW-wCEzbgnbGc2lhd1PTKXwYgtz8Id9.UCpWlmUBt.jAFtWRAAckd,
msgHash	9drKEZ8ixvQ8ycKCMVl6t5xwE8QiI7sZuQYrHqFXLZJuDAHlFYwCM6dQiEWxUE8yHzHrYNWxf1v4/7vr+dXjHQ==,
inResponseTo	_0at.n7PwAPBqTvJd0pV1X-DV.NxNtwHWIpSiAYi2hpqiPWxfwEJLvTgwzGEHJ9N,
statusCode	urn:oasis:names:tc:SAML:2.0:status:Success

Point 8

Timestamp	2019-06-17T13:37:23.241Z,
OpType	eIDAS Connector sends response to Specific Connector,
NodeId	specificConnector,
Origin	N/A,
Destination	http://localhost:8080/SpecificConnector/ConnectorResponse,[15]
flowId	_teeF25P50axuRHOk5uP1K_678N9D5oP1j_khKNqjuV59yOeHFqmocWSJoIZACjD,

[12] http://localhost:8081/EidasNode/ServiceMetadata,Origin
[13] http://localhost:8081/EidasNode/SpecificProxyServiceResponse,Destination
[14] http://localhost:8080/EidasNode/ColleagueResponse,flowId
[15] http://localhost:8080/SpecificConnector/ConnectorResponse,flowId

msgId	_Ji1R-U_ikNrfdI7PrWm6hITG6NcKz3ltC6l-IOE.qs9rU6HA7VnKGr058.4KbBO,
msgHash	FEM2e5zTV77egP5wQRcREeOwoAmLwjx26hGtC+alhkUThcSot+O5KPceYKuvNhjEsOI8QfUOHp5kmkSo/sFG0w==,
bltHash	pRdaV0JKhp+gPofrwBHWbpX8PE3lWidr/pVOTd0UD0oXtmNJBvM56FdJhF5HoP+C0ok94gUDQYXLf1B6uT8mgA==,
inResponseTo	87cc1ae7-10df-4237-acf2-ac4957c4f899,
statusCode	urn:oasis:names:tc:SAML:2.0:status:Success

For more details on the logging points and an example of an end-to-end logging trail eIDAS Connector (country A) ↔ eIDAS ProxyService (country B) for the messages, please refer to *Message logging improvements in eIDAS-Node v2.3* https://ec.europa.eu/digital-building-blocks/wikis/x/hCUIBQ.
The URLs with ec.europa.eu domain in this document are only accessible to the experts registered with the eIDAS eID Implementation community.

7.4 Description of the full message logging

This functionality should only be used for debug purposes.

The full message logging is printing the full content of the request or response incoming into or outgoing from the Node in a specific logging file (cfr. Section 6 Log files).

The content of the log is the xml content of the request or response preceded by a line containing the timestamp and the logger class.

An example of the content logged by the *ConnectorOutgoingEidasRequestLogger* is available in the Appendix B. Full Logging examples.

8 Operational considerations

- Audit facilities should be designed with their specific use(s) in mind, not simply adapted from existing system logs.
- Member States should create and maintain an audit log management structure, including policy, procedures, rules and tools.
- Audit log files should be periodically saved and moved to another storage space. The periodicity may be influenced by the classification of the data, but should be defined either according to a fixed size (e.g. every time the log reaches 1Mb) and / or according to a fixed period of time (e.g. per day, per week).
- Attacks on systems should be prevented by the use of technical preventive controls. These controls should be preferred above procedural preventive controls if possible. Both measures should be used in conjunction with examination of the audit data.
- Member States should consider the use of a Security Event management system due to the large volume of security events.
- Member States should not solely rely on unauthorised events or breaches of policy, but should additionally consider proactive monitoring.
- Member States should consider the use of Security Information and Event Management (SIEM) technology to help the automation and collection of auditable events.
- Audit records should contain a time stamp. Ensure that each system's clock is synchronised to a common time source so that its timestamp will match those generated by other systems.
- The privacy of personal data must be protected.
- Measures should be implemented in order that deleting or modifying logs of own activities should be detected and alerted immediately.
- Administrators should not be able to erase or de-activate logs of activities.
- Audit events should be protected from modification by using digital signatures to sign audit records.
- Audit events should be archived to 'write-once 'media to protect the archive from modification or deletion.
- Where audit records are subject to cryptographic authentication the input data to the authentication computation should include an accurate timestamp.
- Archived audit log files should be protected by appropriate logical and physical security mechanisms.
- The capture of customer sensitive data in audit logs should be avoided. If necessary sensitive data should be anonymised, tokenised or encrypted to avoid data breaches.
- Where audit data are encrypted, the appropriate decryption software and keys must be available and properly maintained, under appropriate access control, for the whole of the lifetime of the encrypted data. Proper maintenance should include periodic testing and adequate back-up to cater for loss of stored encryption keys.
- Audit records should be created in a simple standard format.
- Where audit data are compressed, the appropriate decompression software must be available and properly maintained for the whole of the lifetime of the compressed data. Proper maintenance should include periodic testing.
- The audit trails must be stored in a long-term support and a tamper evident format, such that illicit addition, modification or deletion of any audit trail can be detected.

8.1 Retention period

- MS should ensure that audit retention is part of the organisation's overall retention policy.
- Where the execution of sensitive security-related actions cannot be made subject to dual control, then that execution should be monitored in a timely fashion.
- MS should determine which data is classified as audit data and should protect and preserve this data appropriately.
- Personal notes should be kept by incident investigators throughout the whole course of an investigation and those notes should themselves be protected and preserved in the same manner as audit data.

- Audit records used during an investigation must be preserved at least until the end of the investigation and for any subsequent prosecution irrespective of their normal retention period.
- Follow the organisation's incident response policy to investigate an audit log incident.
- System configuration information should be modified, if necessary, to prevent an event from overwhelming the system.

9 References

[1] ISO/IEC 27002 - Information technology -- Security techniques -- Code of practice for information security management, section 10.10, 2005 ([www.iso.org[16]|http://www.iso.org])

[2] BSI PD008: Legal Admissibility and Evidential Weight of Information Stored Electronically, British Standards Institution, 1999

[3] COBIT (Control Objectives for Information and related Technology) from Information Systems Audit and Control Association ([http://www.isaca.org/cobit.htm|http://www.isaca.org/cobit.htm])

[4] ICT-PSP/2007/1 – STORK 1 : D5.7.3 Functional Design for PEPS, MW models and interoperability

[5] K. Kent, M. Souppaya. Guide to Computer Security Log Management. Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-92, September 2006 <ac:structured-macro ac:name="anchor" ac:schema-version="1" ac:macro-id="6fdaad1a-3019-435c-bf72-a9e154d794d9"><ac:parameter ac:name="">SANS_ConsensusPolicyResource</ac:parameter></ac:structured-macro>

[6] SANS Consensus Policy Resource Community - Information Logging Standard, [http://www.sans.org/security-resources/policies/server-security|http://www.sans.org/security-resources/policies/server-security]

[7] EC council - The use of audit trails in security systems [http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/the-use-of-audit-trails-in-security-systems-guidelines-for-european-banks/|http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/the-use-of-audit-trails-in-security-systems-guidelines-for-european-banks/]

[8] AUDIT Trails - NIST publication http://csrc.nist.gov/publications/nistbul/itl97-03.txt

[9] ENISA: Privacy Features of European eID Card Specification, Version 1.0.1, January 2009, <span style="color: #0000ff">+

<a href="http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_privacy_features_eID.pdf+" class="external-link" rel="nofollow">http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_privacy_features_eID.pdf+</a></span(see page 3)>

[10] EC council - The use of audit trails in security systems [http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/the-use-of-audit-trails-in-security-systems-guidelines-for-european-banks/|http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/the-use-of-audit-trails-in-security-systems-guidelines-for-european-banks/]

[11] AUDIT Trails - NIST publication http://csrc.nist.gov/publications/nistbul/itl97-03.txt

[12] NIST: An Introduction to Computer Security: The NIST Handbook, NIST Special Publication 800-12, December 1997, [http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf|http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf] <ac:structured-macro ac:name="anchor" ac:schema-version="1" ac:macro-id="f3d816c9-ae6f-4498-860f-498e84e5191c"><ac:parameter ac:name="">Common_Criteria</ac:parameter></ac:structured-macro>

[13]Common Criteria: Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 4, September.2012 Part 2: Security Functional Components, [http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf|http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf]

[16] http://www.iso.org

10 Appendix A: eIDAS-Node Error Codes and Error Messages

The following table provides a list of eIDAS-Node errors and related error messages.

Table 4: Error Codes and Error Messages

Key	Description
sProviderAction.invalidCountry.code	Invalid Country selected by the Citizen error message on the ServiceProvider interface.
sProviderAction.invalidCountry.message	Invalid SP Domain error message on the ServiceProvider interface.
sProviderAction.invalidSaml.code	Invalid SP Saml request error code on the ServiceProvider interface.
sProviderAction.invalidSaml.message	Invalid SP Saml request error message on the ServiceProvider interface.
sProviderAction.invalidSPProviderName.code	Invalid SP Provider Name error code on the ServiceProvider interface.
sProviderAction.invalidSPProviderName.message	Invalid SP Provider Name error message on the ServiceProvider interface.
sProviderAction.invalidRelayState.code	Invalid SP Relay State parameter error code on the ServiceProvider interface.
sProviderAction.invalidRelayState.message	Invalid SP Relay State parameter error message on the ServiceProvider interface.
sProviderAction.invalidAttr.code	Invalid SP personal attribute list error code on the ServiceProvider interface.
sProviderAction.invalidAttr.message	Invalid SP personal attribute list error message on the ServiceProvider interface.
sProviderAction.errorCreatingSAML.code	Generating SAML Token error code on the ServiceProvider interface.
sProviderAction.errorCreatingSAML.message	Generating SAML Token error message on the ServiceProvider interface.
internalError.code	Generic error code.

Key	Description
internalError.message	Generic error message.
attrList.code	Invalid attribute list error code on Specific code.
attrList.message	Invalid attribute list error message on Specific code.
invalid.sessionId.code	Invalid session id error code.
invalid.sessionId.message	Invalid session id error code.
invalid.session.code	Invalid session error code.
invalid.session.message	Invalid session error code.
callback.code	Invalid eIDAS-Node Proxy Service callback URL error code on CitizenConsent interface.
callback.message	Invalid eIDAS-Node Proxy Service callback URL error message on CitizenConsent interface.
idp.url.code	Invalid IdP redirect URL error code.
idp.url.message	Invalid IdP redirect URL error message.
IdPSAMLResponse.code	Invalid IdP's SAML Response error code.
IdPSAMLResponse.message	Invalid IdP's SAML Response error message.
serviceSAMLResponse.code	Invalid Proxy Service's SAML Response error code.
serviceSAMLResponse.message	Invalid Proxy Service's SAML Response error message.
authenticationFailed.code	Authentication Failed error code on IdPResponse Interface.
authenticationFailed.message	Authentication Failed error message on IdPResponse Interface.
username.code	Authentication Failed error code on specific code.

Key	Description
username.message	Authentication Failed error message on specific code.
invalidAttributeList.code	Invalid Attribute List error code on Specific Code or IdP Response.
invalidAttributeList.message	Invalid Attribute List error message on Specific Code or IdP Response.
invalidAttributeValue.code	Invalid Attribute Value error code on Specific Code.
invalidAttributeValue.message	Invalid Attribute Value error message on Specific Code.
attVerification.mandatory.code	No consent given error code on the CitizenConsent interface.
attVerification.mandatory.message	No consent given to mandatory error message on the CitizenConsent interface.
hash.error.code	Hash generation error code.
hash.error.message	Hash generation error message.
qaaLevel.code	Invalid QAALevel error code on Specific Code or IdP Response.
qaaLevel.message	Invalid QAALevel error message on Specific Code or IdP Response.
colleagueRequest.invalidSAML.code	Invalid SAML Token error code on the ColleagueRequest interface.
colleagueRequest.invalidSAML.message	Invalid SAML Token error message on the ColleagueRequest interface.
colleagueRequest.invalidCountry.code	Invalid Citizen Country error code on the ColleagueRequest interface.
colleagueRequest.invalidCountry.message	Invalid Citizen Country error code on the ColleagueRequest interface.

Key	Description
colleagueRequest.errorCreatingSAML.code	Generating SAML Response error code on the ColleagueRequest interface.
colleagueRequest.errorCreatingSAML.message	Generating SAML Response error code on the ColleagueRequest interface.
colleagueRequest.attrNull.code	Invalid personal attribute list error code on the ColleagueRequest interface.
colleagueRequest.attrNull.message	Invalid personal attribute list error message on the ColleagueRequest interface.
colleagueRequest.invalidDestUrl.code	Invalid Citizen Consent URL error code on the ColleagueRequest interface.
colleagueRequest.invalidDestUrl.message	Invalid Citizen Consent URL error code on the ColleagueRequest interface.
serviceRedirectUrl.code	Invalid Proxy Service Redirect configuration URL error code on the ServiceProvider interface.
serviceRedirectUrl.message	Invalid Proxy Service Redirect configuration URL error message on the ServiceProvider interface
colleagueResponse.invalidSAML.code	Invalid SAML Token error code on the ColleagueResponse interface.
colleagueResponse.invalidSAML.message	Invalid SAML Token error message on the ColleagueResponse interface.
auRequestIdError.code	The SAML Response Id is either null or not valid error code.
auRequestIdError.message	The SAML Response Id is either null or not valid error message.
audienceRestrictionError.code	SAML Conditions are not compliant error code.
audienceRestrictionError.message	SAML Conditions are not compliant error message.

11 Appendix B: Full Logging examples

This section is dedicated to examples of the full logging of requests and responses.

- Full logging of an Outgoing Eidas Request from the Connector

Full logging output of the ConnectorOutgoingEidasRequestLogger.

```
2020-01-03T14:05:27.848Z [default task-1] INFO
eu.eidas.logging.full.ConnectorOutgoingEidasRequestLogger
FULL_MESSAGE_EXCHANGE -127.0.0.1: #1#
[hxdHUI9A3ccwpKrOJ4L1pYG3LO2vlIHLCAgJyM5tRK0=]
< saml2p :AuthnRequest  xmlns:ds = "http://www.w3.org/2000/09/
xmldsig#"   xmlns:eidas = "http://eidas.europa.eu/saml-extensions"
 xmlns:saml2 = "urn:oasis:names:tc:SAML:2.0:assertion"   xmlns:saml2p =
urn:oasis:names:tc:SAML:2.0:protocol"   Consent = "urn:oasis:names:tc:
SAML:2.0:consent:unspecified"   Destination = "http://cef-eid-
build-1:8085/EidasNode/ColleagueRequest"   ForceAuthn = "true"   ID = "
_cjDLF_aH1QfI9yA10MXMKpzPEHXDGTAuzPaOWvP9Vz25jMWEj_LEDqa44RPTDh8"
 IsPassive = "false"   IssueInstant = "2020-01-03T14:05:27.155Z"
 ProviderName = "DEMO-SP-CC"   Version = "2.0" >< saml2 :Issuer  Format
urn:oasis:names:tc:SAML:2.0:nameid-format:entity" > http://cef-eid-
build-1:8085/EidasNode/ConnectorMetadata </ saml2 :Issuer>< ds :Signat
ure>< ds :SignedInfo>< ds :CanonicalizationMethod  Algorithm = "http:/
/www.w3.org/2001/10/xml-exc-c14n#" />< ds :SignatureMethod  Algorithm =
http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256" />< ds :Reference
 URI =
 "#_cjDLF_aH1QfI9yA10MXMKpzPEHXDGTAuzPaOWvP9Vz25jMWEj_LEDqa44RPTDh8" ><
 ds :Transforms>< ds :Transform  Algorithm = "http://www.w3.org/
2000/09/xmldsig#enveloped-signature" />< ds :Transform  Algorithm = "h
ttp://www.w3.org/2001/10/xml-exc-c14n#" /></ ds :Transforms>< ds :Dige
stMethod  Algorithm = "http://www.w3.org/2001/04/xmlenc#sha256" />< ds
DigestValue>3N2C3RjqWjGUwEY2TPxT4q+Q/Wb65bwUEn1Tp7dtrz8=</ ds :DigestV
alue></ ds :Reference></ ds :SignedInfo>< ds :SignatureValue>KUlYiczRP
qBKOFN6qlUqVc67WWyekQuJ07abNY/HlzZU70q8QFFZVqlhfGPUe8eoMA64zFm/
XEvSF+H/++A+9Q==</ ds :SignatureValue>< ds :KeyInfo>< ds :X509Data>< d
s
 :X509Certificate>MIICTjCCAfSgAwIBAgIULqql9qk8a7BYHcg4hQH60G9385QwCgYIK
oZIzj0EAwIwfDELMAkGA1UEBhMCQkUxEDAOBgNVBAgMB0JlbGdpdW0xETAPBgNVBAcMCEJ
ydXNzZWxzMRswGQYDVQQKDBJFdXJvcGVhbiBDb21pc3Npb24xDjAMBgNVBAsMBURJR0lUM
RswGQYDVQQDDBJsb2NhbC1rYS1kZW1vLWNlcnQwHhcNMTkxMDA3MTI1MzI0WhcNMjQxMDA
1MTI1MzI0WjB8MQswCQYDVQQGEwJCRTEQMA4GA1UECAwHQmVsZ2l1bTERMA8GA1UEBwwIQ
nJ1c3NlbHMxGzAZBgNVBAoMEkV1cm9wZWFuIENvbWlzc2lvbjEOMAwGA1UECwwFRElHSVQ
xGzAZBgNVBAMMEmxvY2FsLWthLWRlbW8tY2VydDBaMBQGByqGSM49AgEGCSskAwMCCAEBB
wNCAAR6GPfWZsxJ+r9KgVSdCAJkeu+Mq7YV8APo4/ydKRBIRAHwdIR7/
WvP6G7E9XBkmkeS1RSUMyisx/
```

```
 pYrP+5jphro1MwUTAdBgNVHQ4EFgQUpdHaept65uZTZ3LCIHsuw5RnvpIwHwYDVR0jBBgw
FoAUpdHaept65uZTZ3LCIHsuw5RnvpIwDwYDVR0TAQH/BAUwAwEB/
zAKBggqhkjOPQQDAgNIADBFAiASunseDrp7znsk6U8ot5JnzUjH6LjZf43oglr0hJNGWgI
hAJut1Fg9FNXAWUKWh7RiLI4ZWgMxHNqsTcwFiVNMqgmp</ ds :X509Certificate></
 ds :X509Data></ ds :KeyInfo></ ds :Signature>< saml2p :Extensions>< ei
das :RequestedAttributes>< eidas :RequestedAttribute  FriendlyName = "
D-2012-17-EUIdentifier"   Name = "http://eidas.europa.eu/attributes/
legalperson/D-2012-17-EUIdentifier"   NameFormat = "urn:oasis:names:tc
:SAML:2.0:attrname-format:uri"   isRequired = "false" />< eidas :Reque
stedAttribute  FriendlyName = "EORI"   Name = "http://eidas.europa.eu/
attributes/legalperson/EORI"   NameFormat = "urn:oasis:names:tc:SAML:2
.0:attrname-format:uri"   isRequired = "false" />< eidas :RequestedAtt
ribute  FriendlyName = "LEI"   Name = "http://eidas.europa.eu/
attributes/legalperson/LEI"   NameFormat = "urn:oasis:names:tc:SAML:2.
0:attrname-format:uri"   isRequired = "false" />< eidas :RequestedAttr
ibute  FriendlyName = "LegalName"   Name = "http://eidas.europa.eu/
attributes/legalperson/LegalName"   NameFormat = "urn:oasis:names:tc:S
AML:2.0:attrname-format:uri"   isRequired = "true" />< eidas :Requeste
dAttribute  FriendlyName = "LegalAddress"   Name = "http://
eidas.europa.eu/attributes/legalperson/LegalPersonAddress"
 NameFormat = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
 isRequired = "false" />< eidas :RequestedAttribute  FriendlyName = "Le
galPersonIdentifier"   Name = "http://eidas.europa.eu/attributes/
legalperson/LegalPersonIdentifier"   NameFormat = "urn:oasis:names:tc:
SAML:2.0:attrname-format:uri"   isRequired = "true" />< eidas :Request
edAttribute  FriendlyName = "SEED"   Name = "http://eidas.europa.eu/
attributes/legalperson/SEED"   NameFormat = "urn:oasis:names:tc:SAML:2
.0:attrname-format:uri"   isRequired = "false" />< eidas :RequestedAtt
ribute  FriendlyName = "SIC"   Name = "http://eidas.europa.eu/
attributes/legalperson/SIC"   NameFormat = "urn:oasis:names:tc:SAML:2.
0:attrname-format:uri"   isRequired = "false" />< eidas :RequestedAttr
ibute  FriendlyName = "TaxReference"   Name = "http://eidas.europa.eu/
attributes/legalperson/TaxReference"   NameFormat = "urn:oasis:names:t
c:SAML:2.0:attrname-format:uri"   isRequired = "false" />< eidas :Requ
estedAttribute  FriendlyName = "VATRegistration"   Name = "http://
eidas.europa.eu/attributes/legalperson/VATRegistrationNumber"
 NameFormat = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
 isRequired = "false" />< eidas :RequestedAttribute  FriendlyName = "Bi
rthName"   Name = "http://eidas.europa.eu/attributes/naturalperson/
BirthName"   NameFormat = "urn:oasis:names:tc:SAML:2.0:attrname-
format:uri"   isRequired = "false" />< eidas :RequestedAttribute
 FriendlyName = "CurrentAddress"   Name = "http://eidas.europa.eu/
attributes/naturalperson/CurrentAddress"   NameFormat = "urn:oasis:nam
es:tc:SAML:2.0:attrname-format:uri"   isRequired = "false" />< eidas :
RequestedAttribute  FriendlyName = "FamilyName"   Name = "http://
```

```
eidas.europa.eu/attributes/naturalperson/CurrentFamilyName"
NameFormat = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
isRequired = "true" />< eidas :RequestedAttribute  FriendlyName = "Fir
stName"   Name = "http://eidas.europa.eu/attributes/naturalperson/
CurrentGivenName"   NameFormat = "urn:oasis:names:tc:SAML:2.0:attrname
-format:uri"   isRequired = "true" />< eidas :RequestedAttribute
FriendlyName = "DateOfBirth"   Name = "http://eidas.europa.eu/
attributes/naturalperson/DateOfBirth"   NameFormat = "urn:oasis:names:
tc:SAML:2.0:attrname-format:uri"   isRequired = "true" />< eidas :Requ
estedAttribute  FriendlyName = "Gender"   Name = "http://
eidas.europa.eu/attributes/naturalperson/Gender"   NameFormat = "urn:o
asis:names:tc:SAML:2.0:attrname-format:uri"   isRequired = "false" /><
idas :RequestedAttribute  FriendlyName = "PersonIdentifier"   Name = "
http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier"
NameFormat = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
isRequired = "true" />< eidas :RequestedAttribute  FriendlyName = "Pla
ceOfBirth"   Name = "http://eidas.europa.eu/attributes/naturalperson/
PlaceOfBirth"   NameFormat = "urn:oasis:names:tc:SAML:2.0:attrname-
format:uri"   isRequired = "false" />< eidas :RequestedAttribute
FriendlyName = "LegalAdditionalAttribute"   Name = "http://
eidas.europa.eu/attributes/legalperson/LegalAdditionalAttribute"
NameFormat = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
isRequired = "false" />< eidas :RequestedAttribute  FriendlyName = "Ad
ditionalAttribute"   Name = "http://eidas.europa.eu/attributes/
naturalperson/AdditionalAttribute"   NameFormat = "urn:oasis:names:tc:
SAML:2.0:attrname-format:uri"   isRequired = "false" /></ eidas :Reque
stedAttributes></ saml2p :Extensions>< saml2p :NameIDPolicy
AllowCreate = "true"   Format = "urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified" />< saml2p :RequestedAuthnContext  Comparison = "m
inimum" >< saml2 :AuthnContextClassRef> http://eidas.europa.eu/LoA/
low </ saml2 :AuthnContextClassRef></ saml2p :RequestedAuthnContext></
saml2p :AuthnRequest> #2#
[HKA8HqNhTMylytox5txoC19ThvfqIvX6ZX9L39A0S9c=]
```

- Full logging of an Outgoing LightResponse from the Connector

Full logging output of the ConnectorOutgoingEidasLightResponseLogger.

```
2020-02-06T10:17:17.943Z [http-nio-8080-
exec-1] INFO  eu.eidas.logging.full.ConnectorOutgoingLightResponseLogg
er FULL_MESSAGE_EXCHANGE -172.17.0.1:  #11# [4LWthojFVqXLpv8tcMM2whTMO
dMeuj7DPqb5+6D/rGg=]
```

```
<? xml  version = "1.0"  encoding = "UTF-8"  standalone = "yes" ?><
ightResponse >    < id >_RX8QrnJIcr7v1n4Z.PvTeKL6owCLsakmS-
tt2KaFtW3ItuNAkKvItj6q3-_QVZc</ id >    < relayState >8e201975-
c953-4bc1-bdf8-37677cf0039a</ relayState >    < issuer > http://
localhost:8080/EidasNode/ConnectorMetadata </ issuer >    < subject >0
123456</ subject >    < subjectNameIdFormat >urn:oasis:names:tc:SAML:1
.1:nameid-format:unspecified</ subjectNameIdFormat >    < status >
    < failure >false</ failure >        < statusCode >urn:oasis:names:
tc:SAML:2.0:status:Success</ statusCode >        < statusMessage >urn:
oasis:names:tc:SAML:2.0:status:Success</ statusMessage >    </ status >
    < inResponseToId >fd8e8c53-592a-48ea-999c-4cd4230aa10b</
 inResponseToId >    < levelOfAssurance > http://eidas.europa.eu/LoA/
low </ levelOfAssurance >    < attributes >        < attribute >
      < definition > http://eidas.europa.eu/attributes/legalperson/
LegalName </ definition >            < value >Current Legal Name</
 value >        </ attribute >        < attribute >            < defini
tion > http://eidas.europa.eu/attributes/legalperson/
LegalPersonIdentifier </ definition >            < value >CA/CB/
125457487Company</ value >        </ attribute >        < attribute >
          < definition > http://eidas.europa.eu/attributes/
naturalperson/CurrentFamilyName </ definition >            < value >Ga
rcia</ value >        </ attribute >        < attribute >            <
efinition > http://eidas.europa.eu/attributes/naturalperson/
CurrentGivenName </ definition >            < value >javier</ value >
       </ attribute >        < attribute >            < definition > h
ttp://eidas.europa.eu/attributes/naturalperson/DateOfBirth </
 definition >            < value >1965-01-01</ value >        </
 attribute >        < attribute >            < definition > http://
eidas.europa.eu/attributes/naturalperson/PersonIdentifier </
 definition >            < value >CA/CB/12345</ value >        </
 attribute >    </ attributes ></ lightResponse > #12# [MkB9q0hjCn0SBRD
QCczjz1ju3sT3tZ5y4zsqfzZaOYo=]
```