

# KFOBS Nemlog-in Delivery2

Log viewer guide

Version: 3.0

ID: 32309

2016-06-30

# Contents

<b>1</b>	<b>INTRODUCTION .....</b>	<b>3</b>
<b>2</b>	<b>HOW TO USE LOG VIEWER .....</b>	<b>4</b>
<b>3</b>	<b>LOGGING AND DEBUGGING LOGINS (SSO) .....</b>	<b>9</b>
<b>4</b>	<b>LOGGING AND DEBUGGING LOGOUTS (SLO).....</b>	<b>13</b>
<b>5</b>	<b>LOGGING AND DEBUGGING ATTRIBUTE QUERY WEB SERVICE CALLS .....</b>	<b>17</b>
<b>6</b>	<b>LOGGING AND DEBUGGING SECURE TOKEN SERVICE (STS).....</b>	<b>20</b>
<b>7</b>	<b>LOGGING AND DEBUGGING SIGNING SERVICE .....</b>	<b>22</b>
<b>8</b>	<b>CONTACT NEMLOG-IN SUPPORT.....</b>	<b>25</b>
<b>9</b>	<b>CHANGELOG .....</b>	<b>26</b>

# 1 Introduction

Nemlog-in generates a series of logs (events) related to login, logout and Attribute Query calls. Log viewer is a tool that can be used to speed up the log searching and thus contribute to the overall debugging.

The log viewer does not replace the Nemlog-in support function, but it is recommended that the tool be used as a starting point before contacting Nemlog-in support. Refer to section ["Contact Nemlog-in support"](#) for information that can make debugging more efficient.

The log viewer also supports the other components Signing Service and Security Token Service.

## 2 How to use log viewer

This section describes how searches are performed in the log viewer.

All searches are performed on a basis of date ranges for Web SSO login, Web SSO Logout, Attribute Query, Secure Token service and Signing Service. Optional "Request Id" can be used to highlight the messages related to the optional request Id provided.

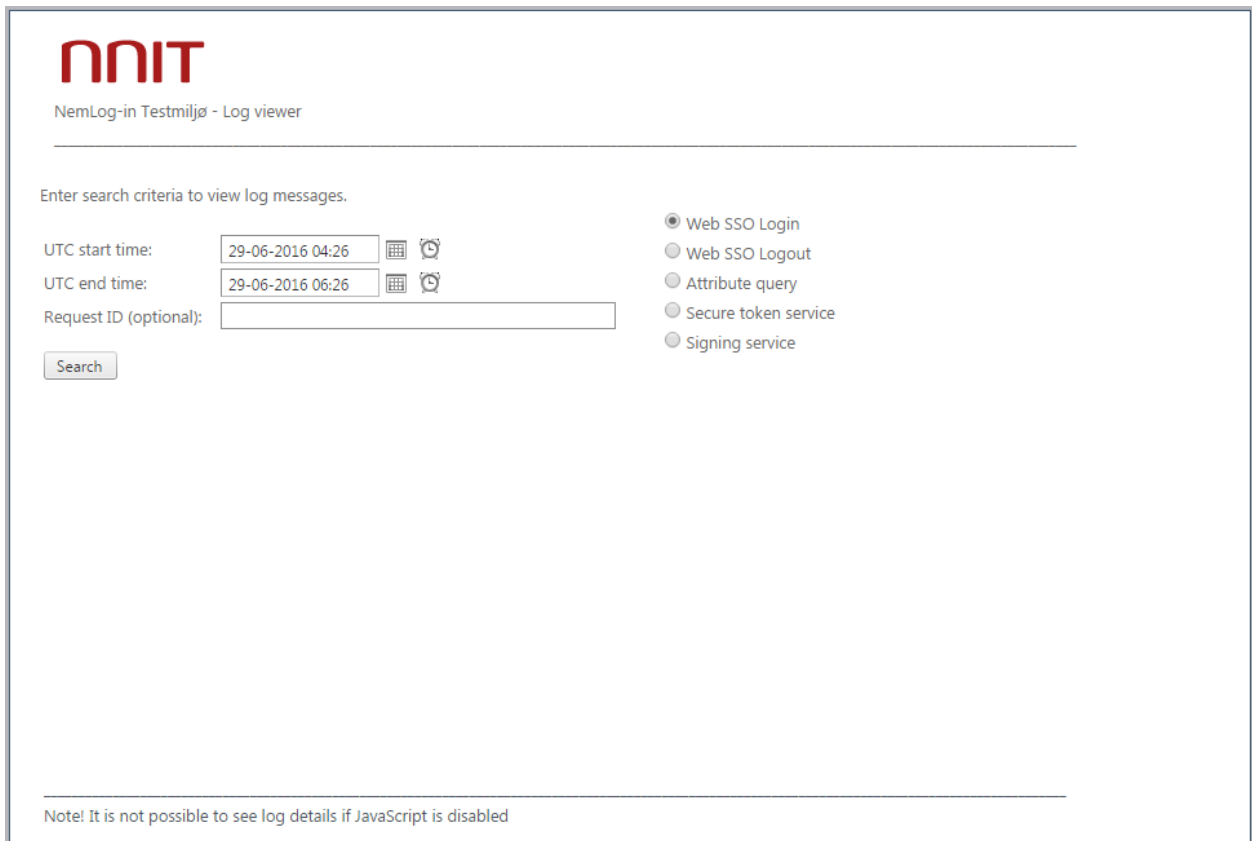
- For WebSSO login, specify the "ID" attribute in the <AuthnRequest> message as Request Id input to highlight related logs.
- For WebSSO logout, specify the "ID" attribute in the <LogoutRequest> message as Request Id input to highlight related logs.
- For Attribute Query, specify the value of CorrelationId in the message as Request Id input to highlight related logs.
- For Secure Token Service, specify the value of CorrelationId in the message as Request Id input to highlight related logs.
- For Signing service, specify the value of CorrelationId in the message as Request Id input to highlight related logs.

If the SAML message is recognized by Nemlog-in and there are messages logged, then the log viewer will present the log results.

## 2.1 Searching the logs

In the log viewer page, select a date range, category, and an optional "Request Id" to view the logs. If no ID is given, the search result will contain all the logs in the given date range.

The log viewer (<https://logviewer.test-nemlog-in.dk/>)



The screenshot shows the 'NemLog-in Testmiljø - Log viewer' interface. At the top left is the 'nnit' logo. Below it, the text 'NemLog-in Testmiljø - Log viewer' is displayed. A horizontal line separates the header from the main content area. The main content area contains the instruction 'Enter search criteria to view log messages.' Below this, there are three input fields: 'UTC start time' with the value '29-06-2016 04:26', 'UTC end time' with the value '29-06-2016 06:26', and 'Request ID (optional)'. Each time field has a calendar icon and a clock icon. To the right of these fields is a list of radio buttons for log categories: 'Web SSO Login' (selected), 'Web SSO Logout', 'Attribute query', 'Secure token service', and 'Signing service'. A 'Search' button is located below the 'Request ID' field. At the bottom of the interface, a note states: 'Note! It is not possible to see log details if JavaScript is disabled'.

## 2.2 Viewing logs

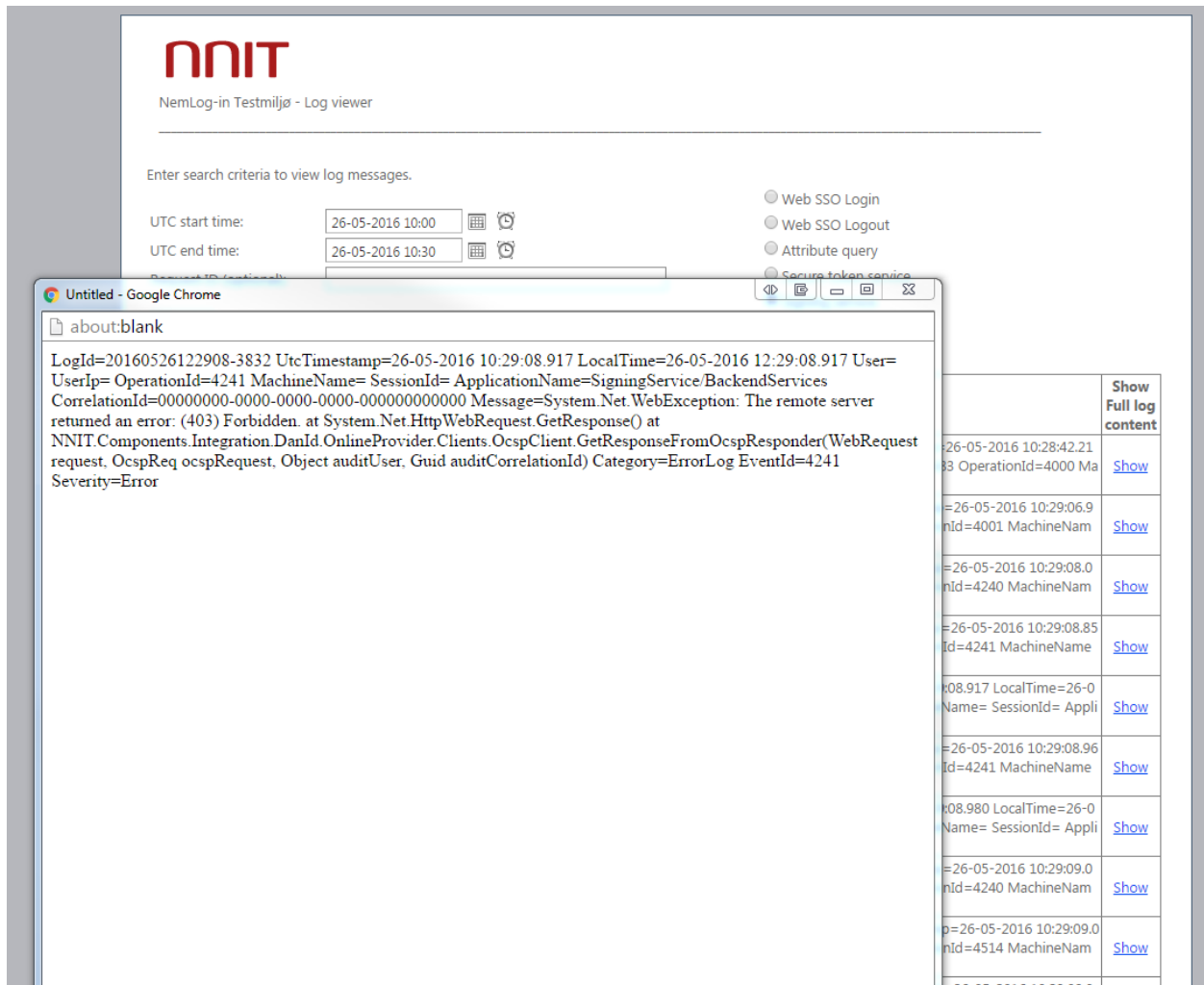
If there are log messages that matches the date range and the log category, the log viewer will display these messages as illustrated by the image below.

No.	Log time	Event Id	Event type	Log contents	Show Full log content
1	26-05-2016 10:28:56	4000	HandlePageRequest	LogId=12f1ca4f-09fc-4563-9e78-f60d791ded5d UtcTimestamp=26-05-2016 10:28:42.212 LocalTime=26-05-2016 12:28:42.212 User= UserIp=10.98.134.83 OperationId=4000 MachineName= SessionId=t5iorjnsfpfxjoava1k2...	<a href="#">Show</a>
2	26-05-2016 10:29:07	4001	InitializeService	LogId=c27ed588-a316-45a2-a46b-2af7797937a1 UtcTimestamp=26-05-2016 10:29:06.995 LocalTime=26-05-2016 12:29:06.995 User= UserIp= OperationId=4001 MachineName= SessionId= ApplicationName=SigningService/...	<a href="#">Show</a>
3	26-05-2016 10:29:08	4240	DanIdIsCertificateValid	LogId=2e9141ec-82eb-4109-b278-7e299861fd2f UtcTimestamp=26-05-2016 10:29:08.089 LocalTime=26-05-2016 12:29:08.089 User= UserIp= OperationId=4240 MachineName= SessionId= ApplicationName=SigningService/...	<a href="#">Show</a>
4	26-05-2016 10:29:08	4241	GetResponseFromOcspResponder	LogId=961a45cf-e224-476c-8bf1-4e5751816d01 UtcTimestamp=26-05-2016 10:29:08.855 LocalTime=26-05-2016 12:29:08.855 User= UserIp= OperationId=4241 MachineName= SessionId= ApplicationName=SigningService/...	<a href="#">Show</a>
5	26-05-2016 10:29:08	4241	GetResponseFromOcspResponder	LogId=20160526122908-3832 UtcTimestamp=26-05-2016 10:29:08.917 LocalTime=26-05-2016 12:29:08.917 User= UserIp= OperationId=4241 MachineName= SessionId= ApplicationName=SigningService/BackendServices C...	<a href="#">Show</a>
6	26-05-2016 10:29:08	4241	GetResponseFromOcspResponder	LogId=961a45cf-e224-476c-8bf1-4e5751816d01 UtcTimestamp=26-05-2016 10:29:08.964 LocalTime=26-05-2016 12:29:08.964 User= UserIp= OperationId=4241 MachineName= SessionId= ApplicationName=SigningService/...	<a href="#">Show</a>
7	26-05-2016 10:29:09	4240	DanIdIsCertificateValid	LogId=20160526122909-6340 UtcTimestamp=26-05-2016 10:29:08.980 LocalTime=26-05-2016 12:29:08.980 User= UserIp= OperationId=4240 MachineName= SessionId= ApplicationName=SigningService/BackendServices C...	<a href="#">Show</a>
8	26-05-2016 10:29:09	4240	DanIdIsCertificateValid	LogId=2e9141ec-82eb-4109-b278-7e299861fd2f UtcTimestamp=26-05-2016 10:29:09.027 LocalTime=26-05-2016 12:29:09.027 User= UserIp= OperationId=4240 MachineName= SessionId= ApplicationName=SigningService/...	<a href="#">Show</a>

It is possible to view the entire contents of the log message by clicking the "Show" link next to the log item.


### 2.2.1 Viewing log details

The image below illustrates the display of the complete log details.



### 2.2.2 Identifying related logs



To identify logs related to each other, the optional Request Id can be supplied in order to highlight the logs as illustrated by the image below.





NemLog-in Testmiljø - Log viewer

---

Enter search criteria to view log messages.

UTC start time:   

UTC end time:   

Request ID (optional):

- Web SSO Login
- Web SSO Logout
- Attribute query
- Secure token service
- Signing service

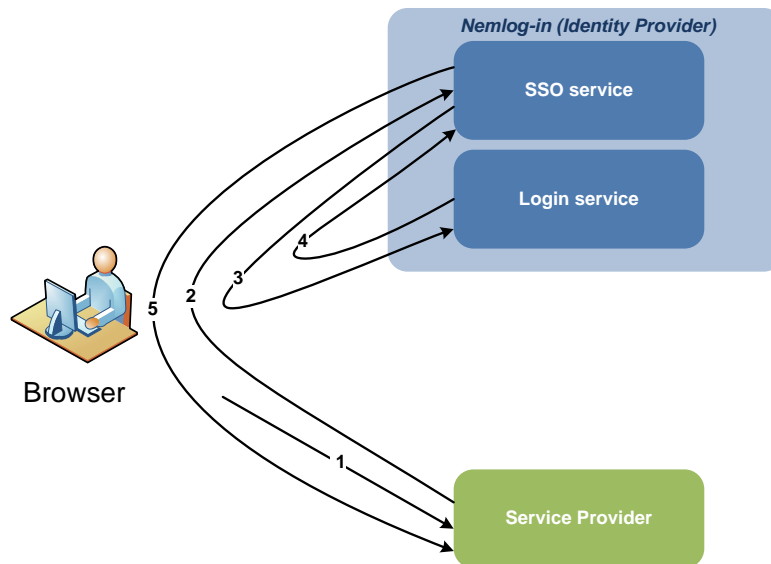
No.	Log time	Event Id	Event type	Log contents	Show Full log content
1	26-05-2016 10:28:56	4000	HandlePageRequest	LogId=12f1ca4f-09fc-4563-9e78-f60d791ded5d UtcTimestamp=26-05-2016 10:28:42.212 LocalTime=26-05-2016 12:28:42.212 User= UserIp=10.98.134.83 OperationId=4000 MachineName= SessionId=t5iorjnsfpxfoava1k2...	<a href="#">Show</a>
2	26-05-2016 10:29:07	4001	InitializeService	LogId=c27ed588-a316-45a2-a46b-2af7797937a1 UtcTimestamp=26-05-2016 10:29:06.995 LocalTime=26-05-2016 12:29:06.995 User= UserIp= OperationId=4001 MachineName= SessionId= ApplicationName=SigningService/...	<a href="#">Show</a>
3	26-05-2016 10:29:08	4240	DanIdsCertificateValid	LogId=2e9141ec-82eb-4109-b278-7e299861fd2f UtcTimestamp=26-05-2016 10:29:08.089 LocalTime=26-05-2016 12:29:08.089 User= UserIp= OperationId=4240 MachineName= SessionId= ApplicationName=SigningService/...	<a href="#">Show</a>
4	26-05-2016 10:29:08	4241	GetResponseFromOcspResponder	LogId=961a45cf-e224-476c-8bf1-4e5751816d01 UtcTimestamp=26-05-2016 10:29:08.855 LocalTime=26-05-2016 12:29:08.855 User= UserIp= OperationId=4241 MachineName= SessionId= ApplicationName=SigningService/...	<a href="#">Show</a>
5	26-05-2016 10:29:08	4241	GetResponseFromOcspResponder	LogId=20160526122908-3832 UtcTimestamp=26-05-2016 10:29:08.917 LocalTime=26-05-2016 12:29:08.917 User= UserIp= OperationId=4241 MachineName= SessionId= ApplicationName=SigningService/BackendServices C...	<a href="#">Show</a>
6	26-05-2016 10:29:08	4241	GetResponseFromOcspResponder	LogId=961a45cf-e224-476c-8bf1-4e5751816d01 UtcTimestamp=26-05-2016 10:29:08.964 LocalTime=26-05-2016 12:29:08.964 User= UserIp= OperationId=4241 MachineName= SessionId= ApplicationName=SigningService/...	<a href="#">Show</a>
7	26-05-2016 10:29:09	4240	DanIdsCertificateValid	LogId=20160526122909-6340 UtcTimestamp=26-05-2016 10:29:08.980 LocalTime=26-05-2016 12:29:08.980 User= UserIp= OperationId=4240 MachineName= SessionId= ApplicationName=SigningService/BackendServices C...	<a href="#">Show</a>
8	26-05-2016 10:29:09	4240	DanIdsCertificateValid	LogId=2e9141ec-82eb-4109-b278-7e299861fd2f UtcTimestamp=26-05-2016 10:29:09.027 LocalTime=26-05-2016 12:29:09.027 User= UserIp= OperationId=4240 MachineName= SessionId= ApplicationName=SigningService/...	<a href="#">Show</a>
9	26-05-2016 10:29:09	4514	ServiceProviderCertificateValidationError	LogId=254c3bba-ee0b-41eb-9eab-563e1a2b7100 UtcTimestamp=26-05-2016 10:29:09.042 LocalTime=26-05-2016 12:29:09.042 User= UserIp= OperationId=4514 MachineName= SessionId= ApplicationName=SigningService/...	<a href="#">Show</a>



### 3 Logging and debugging logins (SSO)

This section describes the logs made available as a result of a successful login.

The image illustrates the login process:



The login process consists of the following steps:

- 1) User requests a protected resource from a Service Provider.
- 2) Service Provider sends <AuthnRequest> (1) to Nemlog-in for the authentication of the user which is received by Nemlog-in service SSO .
- 3) Nemlog-in SSO service sends new <AuthnRequest> (2) to Nemlog-in login service where the user is presented to the login page if the user does not already logged in Nemlog-in.
- 4) Nemlog-in Log service sends <AuthnResponse> (1) to Nemlog-in SSO service, which issued SAML assertion.
- 5) Nemlog-in SSO service sends <AuthnResponse> (2) with assertiveness to Service Provider.

A complete login process will result in the following order of logs listed in the table below:

EventId	Description	Time
3110	<AuthnRequest> (1) is verified and accepted by Nemlog-in	Upon receipt of step 2 (SSO service)
3600	The content of <AuthnRequest> (1)	Upon receipt of step 2 (SSO service)

3601	<AuthnRequest> (2) sent from the SSO service.	Before sending step 3 (SSO service)
3210	<AuthnRequest> (2) received by the Login service	Upon receipt of step 3 (Login service)
3211/3212	3211 = User has been properly authenticated by login on the login page (login without SSO). 3212 = User has been correctly re-authenticated by login with SSO.	Before sending step 4 (Login service)
3602	<AuthnResponse> (1) received from Log service	Upon receiving step 4 (SSO service)
3604	Decrypted <AuthnResponse> (1) assertion received from Login service	Upon receiving step 4 (SSO service)
3605	Decrypted assertion to Service Provider.	Before sending step 5 (SSO service)
3603	<AuthnResponse> (2) with encrypted assertion to the Service Provider.	Before sending step 5 (SSO service)

Table 1: logging with complete login

## 3.1 Troubleshooting logins

This section describes possible errors occurring in a not completed login, to assist with your own debugging.

### 3.1.1 Troubleshooting using reported errors

The following table describes errors that can be displayed using the Log viewer:

EventId	Description	Possible actions
3100	<AuthnRequest> is rejected by throttling module because the Service Provider has reached its maximum number of requests for a period.	Try sending the request later.
3200/3202	Typical error on the user's end when submitting credentials to the Nemlog-in login page. The error is probably due to: <ul style="list-style-type: none"> <li>Error in applets on the login page.</li> <li>Error in verifying user's information from DanID (OOAPI)</li> <li>User entered incorrect information</li> </ul>	Try to log in again. If the error recurs, it is probably a more general error in the login applets. Check for announcements of any service interruptions.
3213	Error with login applets on Nemlog-in login pages (after the user submits the credentials). Can often be linked to logging 3202.	Same procedure as log 3202

### 3.1.2 Troubleshooting with no reported errors

In some cases the entire log chain is not shown in the log viewer. Here is what you need to look for in case the chain breaks or a log is missing:

#### There are no logs recorded on <AuthnRequest>

Nr.	Description	Possible actions
1	<b>There are problems with &lt;AuthnRequest&gt; signature</b>	
	Signed with certificate other than the one registered in Nemlog-in	Verify the metadata from Nemlog-in. If possible, register new metadata.
	Error in signature due to incomplete or invalid information.	Verify the requirements for signature in SAML 2.0 and XMLDSIG
	Error in signature due to wrong cryptography	Verify that one of the following signature algorithms are used: RSA-SHA1 and RSA-SHA256
	The certificate is expired or revoked	Verify by using the certificate metadata validator in the Nemlog-in test environment - <a href="https://test-nemlog-in/testportal/">https://test-nemlog-in/testportal/</a>
2	<b>There are problems with the structure of &lt;AuthnRequest&gt; message</b>	
	SAML message does not comply with OIOSAML / SAML	Verify requirements <AuthnRequest> idp SAML 2.0 and OIOSAML Web SSO

#### The last log is eventId 3110:

Nr.	Description	Possible Actions
1	<b>There is an internal error in Nemlog-in</b>	
	The <AuthnRequest> has been approved and therefore there is probably an internal error in Nemlog-in	Try to log in again. If the problem keeps recurring, contact Nemlog-in support.

#### The last log is eventId 3600 or 3601:

Nr.	Description	Possible actions
1	<b>There is an internal error in Nemlog-in</b>	
	The <AuthnRequest> has been approved and therefore there is probably an internal error in Nemlog-in	Try to log in again. If the problem keeps recurring, contact Nemlog-in support.

#### The last log is eventId 3210:

Nr.	Description	Possible actions
1	<b>There is an error in connection with the provision of user identity</b>	

	There is an error in submitting the user credentials at login or re-authentication by SSO.	Try to log in again. If the problem keeps recurring, contact Nemlog-in support.
--	--	--

**Last log is eventId 3211 or 3212:**

Nr.	Description	Possible actions
<b>1</b>	<b>There is an internal error in Nemlog-in</b>	
	User's identity has been determined, but the SSO service has not received <AuthnResponse> (1).	Try to log in again. If the problem keeps recurring, contact Nemlog-in support.

**Last log is eventId 3602 or 3604:**

Nr.	Description	Possible actions
<b>1</b>	<b>There is an internal error in Nemlog-in</b>	
	SSO service has received <AuthnResponse> (1), but could not issue any assertion to the Service Provider.	Try to log in again. If the problem keeps recurring, contact Nemlog-in support.

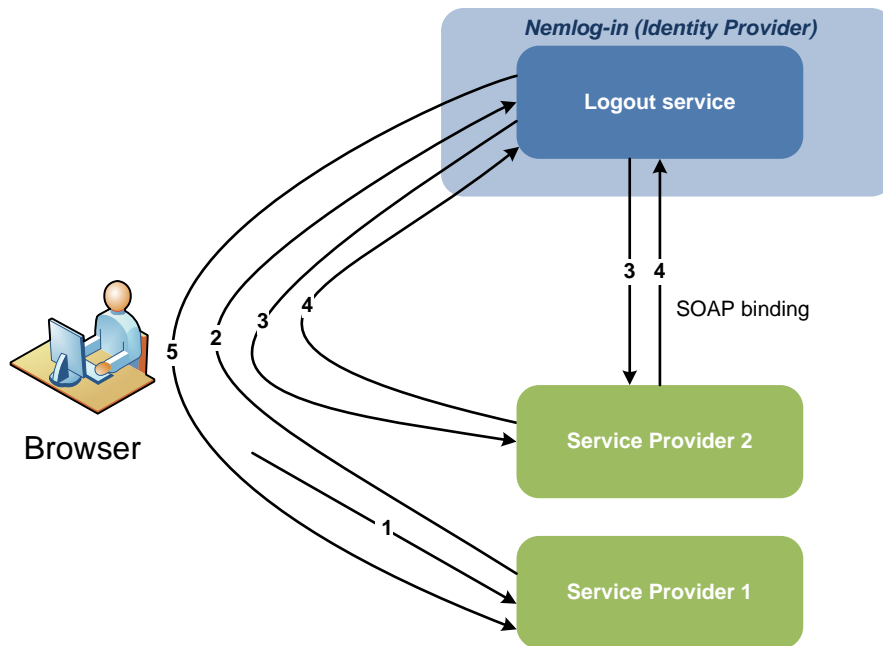
**Last log is eventId 3605:**

Nr.	Description	Possible actions
<b>1</b>	<b>There is an internal error in Nemlog-in</b>	
	SSO service has correctly issued an assertion to the Service Provider, but could not send <AuthnResponse> (2) to the Service Provider.	Try to log in again. If the problem keeps recurring, contact Nemlog-in support.

## 4 Logging and debugging logouts (SLO)

This section describes the logs made available as a result of a successful logout.

The image below illustrates the logout process:



In the above example, the user logged is logged in to two Service Providers.

The steps in the logout process are:

- 1) User logs out from Service Provider (1).
- 2) Service Provider (1) sends <LogoutRequest> (1) to Nemlog-in to start the Single Log-Out (SLO).
- 3) Nemlog-in sends <LogoutRequest> (2) to participating Service Provider (2), which also implements the logout locally.
- 4) Service Provider (2) sends <LogoutResponse> (1) to Nemlog-in, internally marks the Service Provider (2) for logged out<sup>1</sup>.
- 5) NemLog-in marks Service Provider (1) as logged out and sends <LogoutResponse> (2).

---

<sup>1</sup> Step 3 + 4 can be made via HTTP Redirect or HTTP Post over the user's browser or as a back-channel call via SOAP interface. The Service Provider configured bindings determines this method

A complete logout process will result in the order of the logs that are listed in the table below:

EventId	Description	Time
3900	<LogoutRequest> (1) is verified and accepted by Nemlog-in	Upon receiving step 2
3901	The logging is carried out for each service providers participating in the user's session.	Upon receiving step 2
3905	<LogoutRequest> (2) from Nemlog-in (SOAP binding).	Before sending step 3
3904	<LogoutRequest> (2) from the failed Nemlog-in (SOAP binding).	Before sending step 3
3902	<LogoutResponse> (1) from Service Provider (2) (SOAP binding).	Upon receiving step 4
3906	<LogoutResponse> (1) from Service Provider (2) failed. (SOAP binding).	Upon receiving step 4
3911	<LogoutRequest> (2) from Nemlog-in (HTTP Redirect / Post bindings)	Before sending step 3
3912	<LogoutResponse> (1) from Service Provider (2) (HTTP Redirect/Post bindings).	Upon receiving step 4
3913	This represents logging session logout of Nemlog-in itself.	Before sending step 5
3919	<LogoutResponse> (2) from Nemlog-in	Before sending step 5

Table 2: logs of a complete logout

## 4.1 Troubleshooting logout

This section describes the possible errors that could occur during logout, to assist in debugging.

The search starts from the last log that is registered for a given logout on the basis of logging in Table 2 in the previous section.

### There are no logs recorded <LogoutRequest> (1)

Nr.	Description	Possible actions
1	<b>There are problems with &lt;LogoutRequest&gt; (1) signature</b>	
	Signed with certificate other than that of what is registered in Nemlog-in	Verify the metadata from Nemlog-in. If possible, register new metadata.
	Error in signature due to incomplete or invalid information.	Verify the requirements for signature in SAML 2.0 and XMLDSIG
	Error in signature due to wrong cryptography	Verify that one of the following

		signature algorithms are used: RSA-SHA1 and RSA-SHA256
	The certificate is expired or revoked	Verify certificate metadata validator on Nemlog-in test environment
<b>2</b>	<b>There are problems with the structure of &lt;LogoutRequest&gt; message</b>	
	SAML message does not comply OIOSAML / SAML	Verify requirements <LogoutRequest> in SAML 2.0 and OIOSAML Web SSO

**Last log is eventId 3900:**

Nr.	Description	Possible actions
<b>1</b>	<b>There is an internal error in Nemlog-in</b>	
	Nemlogin received <LogoutRequest> (1), but could not implement logout.	Try to log off again. If the problem keeps occurring, contact Nemlog-in support.

**Last log is eventId 3911/3912:**

Nr.	Description	Possible actions
<b>1</b>	<b>An error has occurred in the login chain</b>	
	If Nemlog-in experience problems sending or receiving messages over HTTP Redirect / Post bindings, the logout process will be interrupted and thus are no additional logs. Such errors are typically caused by problems with the user's browser or that a service provider does not respond correctly.	Try to log off again. If the problem keeps occurring, contact Nemlog-in support.

**Last log is eventId 3913:**

Nr.	Description	Possible actions
<b>1</b>	<b>Nemlog-in could not send &lt;LogoutResponse&gt; (2)</b>	
	User has been logged out of Nemlog-in itself, but could not send <LogoutResponse> (2) to the Service Provider (1). Such errors are typically caused by problems with the user's browser or the Service Provider does not respond correctly.	Try to log off again. If the problem keeps occurring, contact Nemlog-in support.

**Troubleshooting the known bugs**

The table below describes possible causes of known errors in the logout process.

**Registered an eventId 3904:**

Nr.	Description	Possible actions
-----	-------------	------------------

<b>1</b>	<b>Nemlog-in could not send &lt;LogoutRequest&gt; (2)</b>	
	<p>The error is caused by the Service Provider not responding to the request sent from Nemlog-in. It could be caused by:</p> <ul style="list-style-type: none"> <li>• SOAP endpoint does not exists / is not responding</li> <li>• DNS error (hostname cannot be resolved)</li> <li>• NNIT FW is preventing the call</li> </ul>	<p>Try to log off again. If the problem keeps occurring, contact Nemlog-in support.</p>

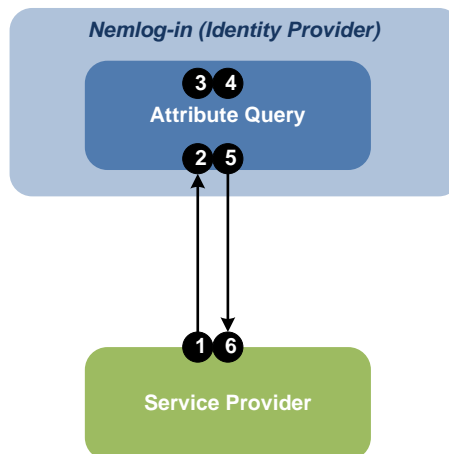
**Registered an eventId 3906:**

Nr.	Description	Possible actions
<b>1</b>	<b>Nemlog-in could not interpret &lt;LogoutResponse&gt; (1)</b>	
	<p>The error may occur because the SOAP message does not meet SAML.</p>	<p>Try to log off again. If the problem keeps occurring, contact Nemlog-in support.</p>



## 5 Logging and debugging Attribute Query web service calls

This section describes the logs made available as a result of the Attribute Query query. The image below illustrates the process:



The steps in the process are:

- 1) Service Provider sends <Attribute Query> query (1) for Attribute Query.
- 2) Attribute Query receives, validates and authenticates the request.
- 3) Attribute Query retrieves requested attributes from the relevant attribute sources (Certifikatkilde, Brugerttighedssystem, CPR-online).
- 4) Attribute Query issuer assertion with delivered attributes.
- 5) Attribute Query sends response message if necessary, including signed and encrypted assertion, to Service Provider.
- 6) Service Provider receives response.

The table below lists the order of the logs generated by Attribute Query query:

EventId	Description	Time
3700	<Attribute Query> query (1) is verified and accepted by Nemlog-in	Upon receiving step 2
3711	One or more attributes could not be delivered. Query will still process the other requested attributes. Note that logging 3711 will only occur if there are	Upon receiving step 3

	attributes that cannot be delivered.	
3712	An attribute source is used to retrieve the attributes. Note that there will often be several 3712 logs in the same query.	Before sending step 3
3760	Attributes supplied by the source attribute FBRS (Nemlog-in's Brugerrettighedsystem).	Before sending step 3
3771	Privileges / proxies provided by the attribute source FBRS (Nemlog-in's Brugerrettighedsystem).	Upon receiving step 3
3750/3751	Social Security number provided by the source attribute CPR online. 3750 is logged using personal certificate. 3751 is logged using the employee certificate.	Upon receiving step 3
3713	The complete assertion is issued to Service Provider.	Before sending step 4
3714	Complete response message is sent to the Service Provider including encrypted assertion.	Upon receiving step 5

*Table 3: Logs of complete query*

## 5.1 Troubleshooting the Attribute Query web service calls

This section describes possible error situations to assist with your debugging.

There will usually only be one of the listed logs in the table below and a logging 3714 with response status code.

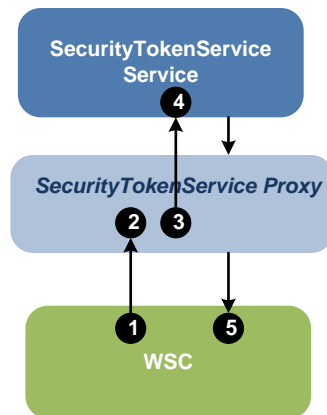
EventId	Description	Possible actions
3701	<AttributeQuery> request could not be authenticated: In OIOSAML variant, this means that the signature could not be verified. In Virk variant, this means that the username and password could not be verified.	Verify that the signature or username / password are correct.  Verify that NemLog-in received metadata for Service Provider.
3702	EntityId in <Attribute Query> request could not be accepted. Entity Id is not registered in Nemlog-in.	Verify that the entityId is correct.  Verify that NemLog-in received metadata for Service Provider.
3703	Parts of <Attribute Query> request could not be interpreted (message formatted correctly).	Verify the message format
3704	One or more elements and / or attributes in the <Attribute Query> query are missing or illegal	Verify the message format

	(message formatted incorrectly).	
3710	The user certificate used by the Subject identifier is not recognized by NemLog-in's local certificate cache.	When the user logs on Nemlog-in Web SSO certificate will be updated in NemLog-in's local cache after a shorter period.

## 6 Logging and debugging Secure token service (STS)

This section describes the logs made available as a result of a Web service consumer calling Secure Token Service.

The image below illustrates the process:



1. A WSC sends a <RequestSecurityToken> request to the STS, which is intercepted by the SecurityTokenServiceProxy (hereafter referred to as Proxy).
2. The Proxy invokes the WSTrustBinding module for reading the request. The module validates the request formatting and returns the request as a Request envelope type.
3. The Proxy invokes the ValidateRequest module for complete request validation and authentication in accordance with rules defined in the STS processing rules specification.
4. The Proxy invokes the SecurityTokenServiceService (referred Service from hereafter) for processing the now validated request.
5. The Proxy returns the response to WSC.

The table below lists the order of the logs generated by Secure Token Service:

EventId	Description	Time
3800	< RequestSecurityToken > request is received by SecurityTokenServiceProxy	Upon receiving step 2 (STS proxy)
3801	Incoming request is validated	Upon receiving step 2 (STS proxy)
3806	Requester entity	Upon receiving step 2 (STS proxy)
3813	Attribute policy enforced	Before sending step 4 (STS proxy)
3812	Attribute provider invocation	Upon receiving step 4 (STS service)
3860	Attribute retrieval	Upon receiving step 4 (STS service)
3870/3871	Privilege retrieval from (PID/RID)	Upon receiving step 4 (STS service)
3850/3851	CPR retrieval from PID/RID	Upon receiving step 4 (STS service)
3814	DanID certificate check	Upon receiving step 4 (STS service)
3815	Persistent pseudonym invocation	Upon receiving step 4 (STS service)
3816	Session status invocation	Upon receiving step 4 (STS service)
3817	FBRS organization invocation	Upon receiving step 4 (STS service)
3872	Assertion issued	Before sending step 5 (STS proxy)
3804	Response message	Before sending step 5 (STS proxy)

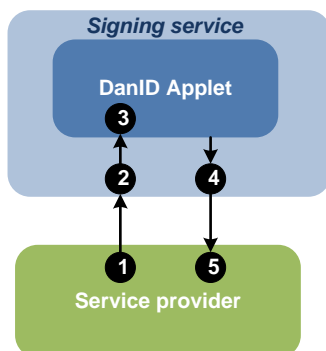
## 6.1 Troubleshooting Security Token Service calls

This section describes the possible error situations, to assist with your debugging.

EventId	Description	Possible actions
3802	<RequestSecurityToken> request is not readable	Verify the message format
3803	<RequestSecurityToken> request is not valid	Verify the message format
3805	Internal processing error	Try to call STS again. If the problem keeps occurring, contact Nemlog-in support.

## 7 Logging and debugging Signing service

This section describes the logs made available as a result of a call to the Signing service. The image below illustrates the process:



The steps in the process are:

- 1) Service Provider redirects to signing service for signing.
- 2) Signing service initializes and displays the DanID java/JavaScript applet UI to perform the signing.
- 3) DanID Java/JavaScript applet performs the signing process and returns the result to Signing service.
- 4) Signing service performs additional checking, like certificate revocation, and sends the result back to the service provider.
- 5) Service provider receives the result of the signing service process.

The table below lists the order of the logs generated by Signing service:

EventId	Description	Time
4000	Signing Service Web initialized	Upon receipt of step 2 (Signing service)
4001	Call to signing service backend	Before sending step 3 (DanID)
4240	DanID certificate check	Upon receipt of step 3(DanID)
4241	DanID certificate revocation check	Upon receipt of step 3(DanID)
4003	Return from backend	Before sending step 4 (Signing service)

4004	Return values to SP	Before sending step 5(Service provider)
------	---------------------	---

## 7.1 Troubleshooting Signing service calls

This section describes the possible error situations to can assist with your debugging.

EventId	Description	Possible actions
4506	SessionHijackDetected	Check connection to signing service for session hijacking
4516	Unknown URL parameter	Redirection post to signing service has unrecognized URL parameter. Check service provider settings.
4519	Critical POST parameter missing	Redirection post to signing service is missing critical POST parameters. Check service provider settings.
4518	Cookie not valid	Enable cookies on browser
4507	InputValidationFailedSignTextFormat	Check the correctness of the POST parameters sent to the signing service
4503	Service Configuration error	Try to call Signing service. If the problem keeps occurring, contact Nemlog-in support.
4511	Service provider not registered	Verify that the service provider has been provisioned to the signing provisioning service.
4512	Invalid fingerprint	Check the correctness of the POST parameters sent to the signing service
4513	Unsupported Digest Algorithm	Check the correctness of the POST parameters sent to the signing service
4514	ServiceProviderCertificateValidationError	Verify that the service provider's certificate is valid.
4604	Failed to sign proof	Check the correctness of the POST parameters sent to the signing service
4603	Failed to store proof set	Try to call Signing service. If the problem keeps occurring, contact Nemlog-in support.

--	--	--



## 8 Contact Nemlog-in support

When contacting Nemlog-in support, it is important that you have as much as possible of the following information available:

- Provide the Service Provider information
  - Provide entityId (preferred)
  - Provide Service Provider name
- Provide SAML message identification
  - Provide <AuthnRequestID> for WebSSO login errors
  - Provide <LogoutRequestID> for WebSSO logout errors
  - Provide <AttributeQueryID> for Attribute Query errors
  - Provide <CorrelationID> for Secure token Service errors
  - Provide <CorreclationID> for Signing service errors
- Provide eventId
  - Provide the last eventId reported with Log viewer (if possible).

## 9 Changelog

Date	Version	Description of Changes	Initials
04.12.2012	0.a	Document created	MWL
10.12.2012	0.b	Document ready for review	MWL
12.12.2012	0.c	Document reviewed	OAR
14.12.2012	1.0	Document approved	MWL
17.07.2013	1.a	Document updated with delivery b+c including <ul style="list-style-type: none"><li>• Added events for NemLog-in</li><li>• Attribute Query events</li></ul>	MWL
19.07.2013	2.0	Approved by DIGST	MWL
29.06.2016	2.a	Document updated after release of log viewer 2.0	SMCP
30.06.2016	3.0	Document approved by DIGST	KSLR