



# Digitaliseringsstyrelsen

## KFOBS Signature Validation Certificates

Signature validation in NemLog-in and Signing Service

Version: 1.1

ID: 32309

2016-08-29

|  |          |
|--|----------|
| <b>DESCRIPTION .....</b>                                   | <b>3</b> |
| 1.1 OVERVIEW .....   | 3        |
| 1.2 SIGNATURE VALIDATION .....                             | 3        |
| 1.3 SIGNATURE VALIDATION OF NEMLOG-IN ASSERTIONS .....     | 3        |
| 1.3.1 IdP certificates – OIOSAML.....                      | 3        |
| 1.3.2 IdP certificates – Virk legacy .....                 | 4        |
| 1.4 SIGNATURE VALIDATION – SECURITY TOKEN SERVICE .....    | 4        |
| 1.4.1 Bootstrap Token Case.....                            | 4        |
| 1.4.2 WSC/WSP verification of response and assertion ..... | 5        |
| 1.4.3 WSP/WSC verification flows.....                      | 5        |
| 1.5 SIGNATURE VALIDATION – SIGNING SERVICE .....           | 6        |
| <b>2 REFERENCES .....</b>                                  | <b>7</b> |
| <b>3 CHANGE LOG .....</b>                                  | <b>8</b> |

# Description

## 1.1 Overview

The purpose of this document is to guide the service providers on which certificate to use to perform signature validation of the responses from NemLog-in and Signing Service. The validation of responses is related to implementation of *NemLog-in*, *Attribute service*, *Security Token Service* (a part of NemLog-in) and *Signing Service*. The certificates are listed below and the services has been linked to the certificate which should be used to verify the signature.

## 1.2 Signature validation

All the responses from NemLog-in and Signing Service are XML responses. All the responses sent from NemLog-in and Signing Service will be signed by NemLog-in and Signing Service certificates. As a service provider you must use the *public certificate* to verify that the responses returned has been issued by *NemLog-in / Signing service* and not been modified – this will prevent for instance “man in the middle attacks”. Please note that all service providers are required to implement this check in their integration to *NemLog-in* and *Signing Service*.

## 1.3 Signature validation of NemLog-in assertions

The *NemLog-in* assertion is the decrypted response from *NemLog-in*. Once you as service provider receives the token you must verify the signature by using the certificate from the IdP metadata.

### 1.3.1 IdP certificates – OIOSAML

When an IT-system receives an assertion from NemLog-in then the assertion must be verified to ensure that it originates from *NemLog-in* by using the certificate stored in the IDP metadata file.

Note there are two sets of IdP Metadata, which each contain a set of certificate, one for test and one for production. The link below is the direct for download the IdP certificate stored in the metadata as a base64 certificate file.

Production: <https://test-nemlog-in.dk/Testportal/Prod-nemlog-in-2-2014.xml>

Test: <https://test-nemlog-in.dk/Testportal/Test-nemlog-in-2.xml>

### 1.3.2 IdP certificates – Virk legacy

This section describes the scenario, where the service provide uses the virk profile.

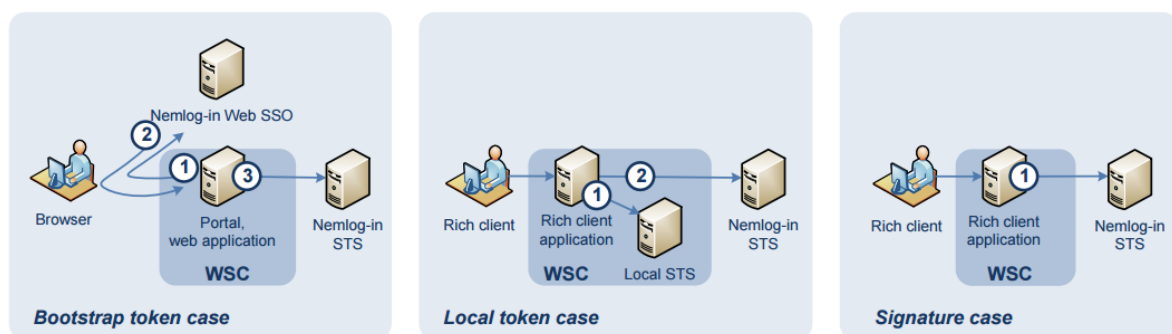
Note there are two sets of IdP Metadata, which each contain a set of certificate, one for test and one for production. The link below is the direct for download the IdP certificate stored in the metadata as a base64 certificate file.

Test: <https://test-nemlog-in.dk/Testportal/Test-nemlog-in-2Virk.xml>

Production: <https://test-nemlog-in.dk/Testportal/Prod-nemlog-in-2Virk-2014.xml>

## 1.4 Signature validation – Security Token Service

As a service provider there is a couple of scenarios where you can get an assertion in return from Security Token Service. There are 3 different scenarios of Security Token Service. Bootstrap Token Case, Signature case and Local Token Case. <sup>1</sup>



Figur 1: Flow in STS for each scenario

### 1.4.1 Bootstrap Token Case

In the bootstrap scenario you will need to use to verify the assertion received from NemLog-in by using the *IdP metadata* certificate described in section 1.3.1. You will need to validate the NemLog-in assertion as you usually do in the NemLog-in Web SSO scenario. Furthermore you will need to validate the signature from the STS. The validation is the same for all 3 scenarios. More details in the next section.

<sup>1</sup> References - Link to STS documentation for more information

### 1.4.2 WSC/WSP verification of response and assertion

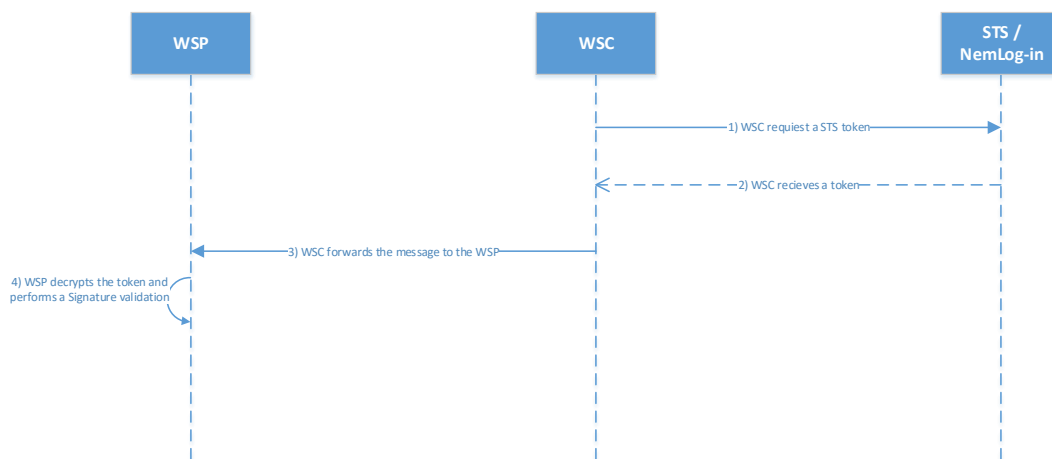
For all the scenarios you will need to verify the *assertion* and the *response* from STS/NemLog-in.

**WSC:** The WSC makes a request to NemLog-in/STS and receives a response which includes a signature in which can tell if the issued token was sent from NemLog-in/STS. Before sending it to the WSP. The WSC should perform a [XMLDSIG](#) verification of the response

**WSP:** The WSP decrypts the assertion received from the WSC and performs a XMLDSIG of the decrypted *assertion*

### 1.4.3 WSP/WSC verification flows

As described in section 1.4.2 here is the flow



**Figur 2: STS flows**

- 1) The WSC requests a token
- 2) The token received from STS needs to be verified that it has been issued by NemLog-in
- 3) The WSC forwards the token to the WSP
- 4) The WSP decrypts the token and validates that the assertion has been sent by NemLog-in/STS

Test: <https://test-nemlog-in.dk/Testportal/certifikater/TestSTSCertificate.zip>

Produktion: <https://test-nemlog-in.dk/Testportal/certifikater/ProductionSTSCertificate.zip>

## 1.5 Signature validation – Signing Service

The signature validation in Signing Service is required. To validate the signature of Signing Service the service provider needs to perform a validation of the response received. See the Signing Service documentation for more information<sup>2</sup> section 7. Note that signing service also got a service in which you can verify your signature proof. More of that in section 9.

Test: <https://test-nemlog-in.dk/Testportal/certifikater/SSTestSigning.zip>

Produktion: <https://test-nemlog-in.dk/Testportal/certifikater/SSProduktionSigning.zip>

---

<sup>2</sup> References - Link to Signing Service

## 2 References

- Link to STS documentation: <https://test-nemlog-in.dk/Testportal/dokumenter/NemLog-in2%20-%20STS.pdf>
- Link to Signing Service: <https://test-nemlog-in.dk/Testportal/dokumenter/NemLog-in2%20-%20signing%20service.pdf>

## 3 Change log

| Date       | Version | Description of Changes | Initials |
|------------|---------|------------------------|----------|
| 2016-08-24 | 1.0     | Initiel version        | KSLR     |
| 2016-08-29 | 1.1     | Approved               | TMLN     |