



Nets Norway AS
Haavard Martinsens Vei 54
NO-0045 Oslo

T +47 22 89 89 89
F +47 22 81 64 54
www.nets.eu

Foretaksregisteret NO 990 224 978

E-Ident Integration guide

Version: 2.7
Date: 18.12.2015

Contents

1. Introduction	4
Purpose	4
Intended audience	4
Document conventions	4
Referenced documentation	5
Terms and definitions	5
Acronym	6
Change log	7
2. Integration process	8
Preproduction configuration	8
Production configuration	9
Merchant certificates	9
eID providers	9
3. E-Ident integration	11
Introduction	11
4. Identification	12
Introduction	12
Identification request	13
Single sign-on	17
SAML request	18
SAML response	19
SAML error response	19
Log out sequence	20
Status request	21
5. Visual presentation	24
Normal GUI	24
Reduced GUI	25
6. CSS style guide	27
Introduction	27
eID selection	28
Status page	29
7. Configuration	30
Network address and protocols	30
Recommended eID provider dimensions	30
System property timeouts	31
8. Appendix 1	32
CSS Style sheet elements	32
SAML response example	34
SOAPFault response example	35
E-Ident SAML WSDL	36
E-Ident assertion attributes	37
Basic E-Ident requirements	38
9. Appendix 2 – eID providers	40
Introduction	40
How to enable a new eID	40
BankID (NO)	41
Information	41
Test certificate	41

Production certificate	41
BankID 2.0 (without Java)	42
Known issue	44
“BankID på mobil” (NO)	45
Information	45
Test certificate	45
Production certificate	45
CSS	45
Pre-set mobile phone number and birthdate	45
BankID (SE)	46
Information	46
Test certificate and clients	46
Production certificate	46
Autostart and PresetID in BankID	47
Differentiate between the different end user certificate	48
Known issue	48
Telia e-legitimation (SE)	49
Information	49
Test certificate	49
Production certificate	49
User test certificates	50
Known issues	50
Buypass (NO)	50
Information	50
NemID – personal (POCES) and employee (MOCES) certificates (DK)	51
Information	51
PID/RID cpr-service	52
Existing NemID Service Provider	52
New NemID Service Provider	54
Test users	56
NemID JS client and CSS styling	56
CPR input page	57

1. Introduction

Purpose

The E-Ident service is a platform that provides Merchant sites with an infrastructure for identifying End users. The identification data that E-Ident exposes to merchant applications may be used to determine End user authentication, and even authorization.

E-Ident provides:

- electronic identification using well known eID providers such as BankID, NemID
- an eID provider independent interface for end user identification
- Single sign-on

E-Ident is part of the Nets Signing and Identification Services portfolio.

For a detailed description of supported functions, please refer to the "*E-Ident Functional description*" documentation.

Intended audience

This document is intended for technical staff at the Merchant who will integrate to E-Ident. This document assumes that the reader has sufficient knowledge of how web applications work and also understands concepts such as requests, sessions, authentication, electronic ID, SAML, and SOAP.

Document conventions

To increase readability and enhance the separation of concepts, special terms, expressions, and references are formatted in different type (font and decoration). The following conventions are used throughout this document.

Code examples are formatted in proportional width text using the courier new font. Font sizes for code examples may vary for beautification purposes. Application and protocol parameter names also follow the same formatting.

```
<a href="https://authentication.site/" class="link">Log in</a>
```

E-Ident artifacts will always be in italics (except when in tables and illustrations). These will also have mixed case wherever they are used.

```
Global Logout Service (GLS)
```

References to other documentation are formatted in quoted italics like "*Nets Signing and Identification Services Technical configuration Form*". These references will also be listed in a references table in the beginning of this document.

Referenced documentation

Document	Description
SAML bindings	http://www.oasis-open.org/committees/download.php/3405/oasis-sstc-saml-bindings-1.1.pdf
SAML assertion	http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf
SAML documentation	http://www.oasis-open.org/committees/download.php/3400/oasis-sstc-saml-1.1-pdf-xsd.zip
Nets E-Ident Merchant technical verification test	A suite of tests that merchants must execute to verify conformance with E-Ident. The test is performed against merchant applications before the merchant can be activated for production.
Nets Signing and Identification Services Technical configuration Form	The configuration form includes all necessary configuration details that are needed to enable Merchants in the customer test and production system.

Terms and definitions

Term	Description
Artifact Receiver	An URL to the Merchant resource that will process a SAML artifact after authentication
Cookies	Small data tokens stored in the web browser that are used to transfer data between web sessions
End user	In E-Ident terminology, the End user is the client executing an identification sequence. Interchangeable with both browser (user agent) and human user
eID provider	A service that manages and verifies identity information
Merchant	A registered entity that provides valuable services, both online and offline, to End users. The principal interested in the identity of End users. In SAML terminology, this is the relying party
Single sign-on	A feature that allows valid identity information to be shared between multiple Merchants
SSO Cluster	A contract between different Merchants intending to implement single sign-on within their sites
E-Ident	E-Ident is a part of the Nets Signing and Identification Services portfolio. E-Ident provides Merchant sites with End user identification through different eID providers. In SAML terminology, this is the asserting party
E-Signing	E-Signing is a part of the Nets Signing and Identification Services portfolio. This is a service for signing electronic documents.
Nets Signing and Identification Services	This is a portfolio consisting of the services E-Ident, E-Signing, ID-Rights and E-Archive

Acronym

Acronym	Description
CN	Common Name
CoC	Certificate of Conformity
CSS	Cascading style sheet
DN	Distinguished Name
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Secure HTTP
PID	Personal Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
SAML	Security Assertion Markup Language
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
SSN	Social security number
SSO	Single sign-on
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTF-8	A character encoding format of ISO 10646 (RFC 3629)
XML	eXtensible Markup Language
XMLDSIG	XML Digital Signature

Change log

Version	Description	Date
2.0	Corrected the information about Telia e-legitimation, and updated the information about BankID (SE), NemID (DK) and BankID on mobile phones (NO).	12.05.2014
2.1	Added information about BankID 2.0 in section BankID (NO) in chapter 9. Updated also the information about NemID in the same chapter.	16.06.2014
2.2	Added information about BankID (NO) test users and new NemID links.	12.08.2014
2.3	Added information about no_bankid parameter, added valid values for the IDPROVIDER attribute, updated the information about BankID (NO) and added information about NemID JS.	18.09.2014
2.4	Updated the NemID JS information.	17.10.2014
2.5	Updated the NemID JS information and some minor error corrections.	13.11.2014
2.6	Added extra information about the "NemID_clientmode" parameter.	10.12.2014
2.7	Updated the information about BankID test certificate and production certificate, replaced preproduction with customer test and some minor error corrections.	18.12.2015

2. Integration process

A Merchant must be a registered entity in Nets Signing and Identification Services before the services provided by E-Ident are accessible.

Nets Signing and Identification Services has two environments available for customers: the customer test environment for implementation and testing purposes, and the production environment.

Note that updates to the customer test environment are usually performed during normal working hours. A notice to customers will be sent 1-2 days prior to the planned update.¹

Merchant configurations in both environments are done on Wednesdays. All configuration data must be available for Nets Signing and Identification Services by noon the previous Friday.

It is also a requirement that E-Ident Merchants have registered with a supported eID provider. Refer to section Merchant certificates for more details.

Preproduction configuration

The following data must be available to Nets Signing and Identification Services before customer test configuration:

- Merchant test certificate from eID provider
- A completed "*Nets Signing and Identification Services Technical configuration form*"

All configuration data should be sent to Nets Signing and Identification Services support at the following e-mail address:

support.esecurity@nets.eu

After configuration, the Merchant will receive data (merchant eID and access code) that will allow for integration with E-Ident to develop and test their own system.

After the implementation and testing of the Merchant's system, the "*Nets E-Ident Merchant technical verification test*" must be completed and approved. This must be done some time before the production configuration. Please notify Nets Signing and Identification Services after completing the technical verification.

¹ Notifications are sent to e-mail addresses defined in the "Notification regarding service operation" field in the "*Nets Signing and Identification Services Technical configuration form*"

Production configuration

The following data must be available to Nets Signing and Identification Services before Production configuration:

- Merchant certificate from eID provider
- *"Nets Signing and Identification Services Technical configuration form"* updated with production data
- Approved *"Nets E-Ident Merchant technical verification test "*

After configuration, the Merchant will receive data (a merchant eID and access code) that will allow for integration with E-Ident production system.

Merchant certificates

When filling the *"Nets Signing and Identification Services Technical configuration form"*, a Merchant needs to specify:

- Contact information for the Merchant
- Required eID provider and eID provider settings
- Dates for desired customer test and production deployment
- Static content such as web site logos, help texts, etc.

The configuration form requires that Merchants have valid agreements with eID providers and that the rules and regulations outlined by eID providers have been fulfilled. The rules and regulations may include (but not limited) to:

- Access to sensitive private data (passwords, SSN numbers)
- Access to critical software and infrastructure
- Handling and exchange of personal data (names, addresses)

eID providers

E-Ident provides Merchants with a common interface allowing Merchant applications utilize different eID providers to identify End users. Merchants can register with one or more supported eID providers, and offer End users any combination of those registered eID providers.

The following eID providers are supported by E-Ident:

- BankID (Norway)
- BankID on mobile phones (*"BankID på mobil"*) (Norway)
- Buypass Smartkort (Norway)
- NemID POCES (Denmark)
- NemID MOCES (Denmark)
- BankID (Sweden) including Mobile BankID and Nordea e-

legitimation

- Telia e-legitimation (Sweden)

The different eID providers are all designed in their own proprietary ways and will behave and interact differently with the End users. They also implement various techniques to verify End user identities (such as passwords, code generating tokens, client certificates, smart cards, etc.).

See Appendix 2 – eID providers for more information about how to obtain a Merchant certificate from the different eID providers.

3. E-Ident integration

Introduction

Merchant sites that rely on E-Ident to provide End user identification must conform to communication and data exchange protocols described in this document.

For authentication or authorisation purposes, the Merchant website must implement mechanisms that enforce access control to protected, valuable or sensitive content. Such mechanisms may include features such as session management and federation, user identification, authorization and tracking, logout or session termination.

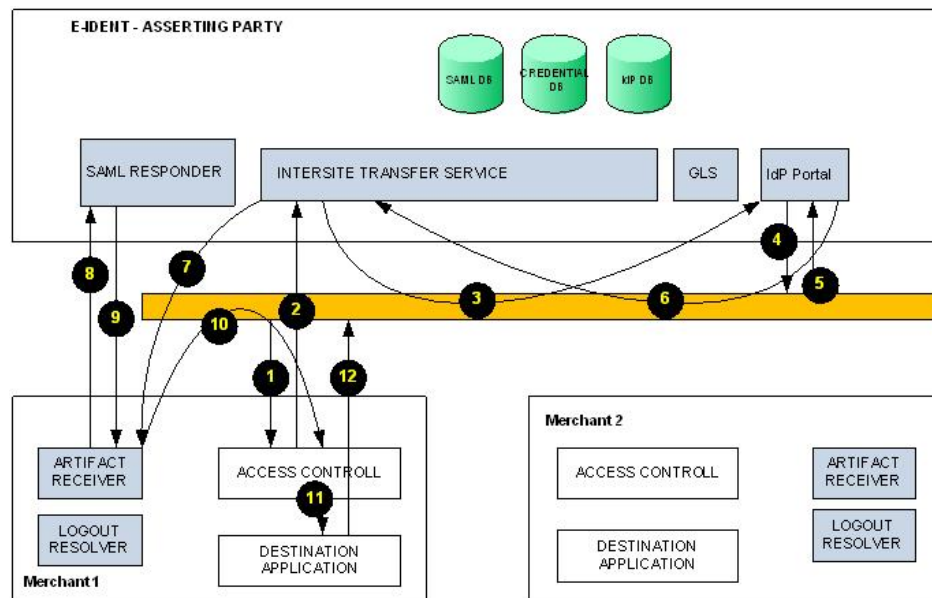
A new or unidentified session that attempts to access the protected content must be detected by the Merchant web application and the request channeled through an identification sequence. The identification sequence is initiated by the Merchant application, but the actual identification and assertion process is managed by E-Ident.

E-Ident presents the End user with a list of available eID providers. Alternatively, an identification dialog for a pre-selected eID provider is displayed in cases where only one eID provider is supported.

After identification, End user credentials (assertion data) are stored in the E-Ident database. The merchant application can access the asserted End user data using the SAML protocol which is an XML-based framework for exchanging user authentication, entitlement, and attribute information.

4. Identification

Introduction



The figure above illustrates the identification sequence for a Merchant site (Merchant 1) that has outsourced the identification process to E-Ident.

The flow of interaction is:

1. The End user accesses merchant 1 web site.
2. Merchant 1 web site performs an access check and determines that the user must be authenticated. The user browser is redirected to E-Ident *Inter-site Transfer Service (ITS)* to begin identification.
3. The *ITS* initiates a new session for the End user and redirects the request to *Identity Provider Portal (IdPP)*.
4. *IdPP* presents the End user with appropriate eID provider dialog for collection of End user identity credentials.
5. The user supplies identity credentials for verification.
6. *IdPP* verifies the provided identity credentials and directs the request to the *ITS*.
7. The *ITS* generates a SAML artifact that is sent to the Merchant artifact receiver.
8. The Artifact receiver uses the artifact to retrieve the assertion generated in step 7 above (see section SAML request).

9. The SAML responder replies with a SAML response (section SAML response) containing the assertion.
10. The Artifact Receiver then sends the browser the intended target resource
11. Merchant 1 authenticates the End user and grants access to protected resources
12. The resource is displayed in the web browser.

Identification request

To initiate a log in sequence, Merchants sites create an identification request that is sent to the *ITS (Inter-site Transfer Service)*. The request instructs the *ITS* to prepare an identification sequence for the End user. The request syntax follows.

ITS base URL	https://ti-pp.bbs.no/its/index.html
--------------	---------------------------------------------------------------------------------------

The base URL accepts the following parameters:

Parameter	Description	Constraints
mid	Merchant identifier. This is an ID assigned to the Merchant upon configuration and must be used in subsequent requests to E-Ident	Required: yes
TARGET	Data sent back to the artifact receiver after identification. Merchants can use this to carry session specific data tokens such as name or URL of resource user intended to access, or a session ID	Required: yes Parameter name must be in upper case
deflect	Name of a target frame. The named frame is the one assigned to render the artifact receiver after identification	Required: no Default: <code>_top</code> Regular expression: <code>[_a-zA-Z0-9]{1,12}</code>
locale	Language used to provide user with information during identification. If not provided, then E-Ident uses the language specified by the web browser. If no supported languages are available in the browser, or the parameter, then Norwegian is used by default	Required: no Supported language codes: <code>nb_NO</code> <code>en_GB</code> <code>da_DK</code> <code>sv_SE</code>

<p>presetid</p>	<p>A pre-selected user ID. Merchant can use this to limit identification to the given ID. The ID can be SSN, PID or other PIN.</p> <p>Note that not all eID providers support presetid</p>	<p>Required: no Encoding: Base64</p>
<p>start</p>	<p>A Merchant URL that points to a start page. The start page is used as an exit strategy for users that opt out of the identification sequence (for example, choosing to cancel the identification process midway or after a status message is displayed by E-Ident).</p> <p>Note that the start URL is not used if a status URL is provided as the status URL will be used to present status messages in place of E-Ident.</p> <p>This parameter overrides the URL issued to E-Ident during configuration</p>	<p>Required: no Format: URL Range: only URLs to trusted domains are allowed by ITS. Trusted domains must be provided in the "Nets Signing and Identification Services Technical configuration form"</p>
<p>status</p>	<p>The URL is used to provide End users with clear messages in cases where an unexpected event occurs. Unexpected events can be errors during identification, change of status, or other relevant information not associated with a successful identification.</p> <p>E-Ident always appends a status code to the provided URL, so this URL must allow a status code to be appended to it.</p> <p>Example: If the event <code>uid.expired</code> occurs, and the URL is defined as being <code>http://merchant/statusurl.html?su=</code> (notice how this URL works well with the appended status code), then the actual URL requested will be <code>http://merchant/statusurl.html?su=uid.expired</code></p> <p>This parameter overrides the URL issued to E-Ident during configuration.</p>	<p>Required: no Format: URL Range: only URLs to trusted domains are allowed by ITS (see start URL constraints above)</p>

style	<p>A Merchant with a specific typographic, layout, or colour scheme can provide the URL to a CSS style sheet. If provided, the given style sheet will be used when rendering web pages in a browser.</p> <p>This parameter overrides the URL issued to E-Ident during configuration</p> <p>Note: style is ignored if the wi parameter is set to "n".</p>	<p>Required: no</p> <p>Format: URL</p> <p>Range: only URLs to trusted domains are allowed by ITS (see start URL constraints above)</p>
wi	<p>Web interface hint. For normal GUI, set the value of this parameter to "n" (without quotation marks). For reduced GUI, use "r"</p>	<p>Required: no</p> <p>Default: n</p>
for- cepki- vender	<p>A comma separated list of eID provider. The list limits the eID providers made available to the End user for identification. See the next table for a mapping between eID and the constraint.</p>	<p>Required: no</p> <p>One or more of: no_bidnc, no_bankid no_bidmob, no_bp, dk_nemid_js, dk_nemid-opensign, se_bankid, se_telia</p>

Mapping of eID to forcepkivendor parameters:

eID	forcepkivendor parameter
BankID (NO)	no_bidnc / no_bankid*
BankID on mobile phones ("BankID på mobil") (NO)	no_bidmob
Buypass Smartkort (NO)	no_bp
NemID with key card (DK)	dk_nemid_js
NemID with key file (DK)	dk_nemid-opensign
BankID (SE)	se_bankid
Telia e-legitimation (SE)	se_telia

*New customers should start using the "no_bankid" parameter. If you, after starting to use BankID 2.0 (without Java) still want to use BankID Java applet in some cases, the "no_bidnc" parameter must be used. If no parameter is given for BankID (NO) or "no_bankid", the BankID 2.0 client will be loaded.

Example URL in HTML:

```
<a href=
  "https://ti-pp.bbs.no/its/index.html?mid=123&TARGET=mytarget"
>LOG IN</a>
```

It is recommended that the TARGET parameter value be URL-encoded as it might contain characters that can interfere with the way the ITS URL is processed. The characters that must be encoded include:

Character	URL Encoding	Usage
?	%3F	Query string delimiter
&	%26	Query string parameter separator
#	%23	HTML anchor

In addition to the listed request parameters, incoming requests may also contain extra parameters that are specific for selected ID providers.

Parameter	Description	Constraints	eID provider
dob6	6-digit date of birth for "BankID på mobil" (NO)	Required: no Encoding: Base64	"BankID på mobil" (NO)
celnr8	8-digit mobile/cell number for "BankID på mobil" (NO)	Required: no Encoding: Base64	"BankID på mobil" (NO)
autostart	Used to inform the service if it shall try to start the eID client automatically. (If the user is using the device where the eID client is located)	Required: no Encoding: true false	BankID (SE)
nemid_clientmode	The NemID JS client can either be shown in a standard or in a limited mode. The standard mode includes administration possibilities for the user like activation for new user. Some customers might notice that the content of their iFrame is moved slightly when pressing the	Required: no (default=standard) Encoding: standard limited	NemID JS (DK)

	question mark button in the NemID client. This could be prevented by using this parameter with "limited" as the value.		
--	------------------------------------------------------------------------------------------------------------------------	--	--

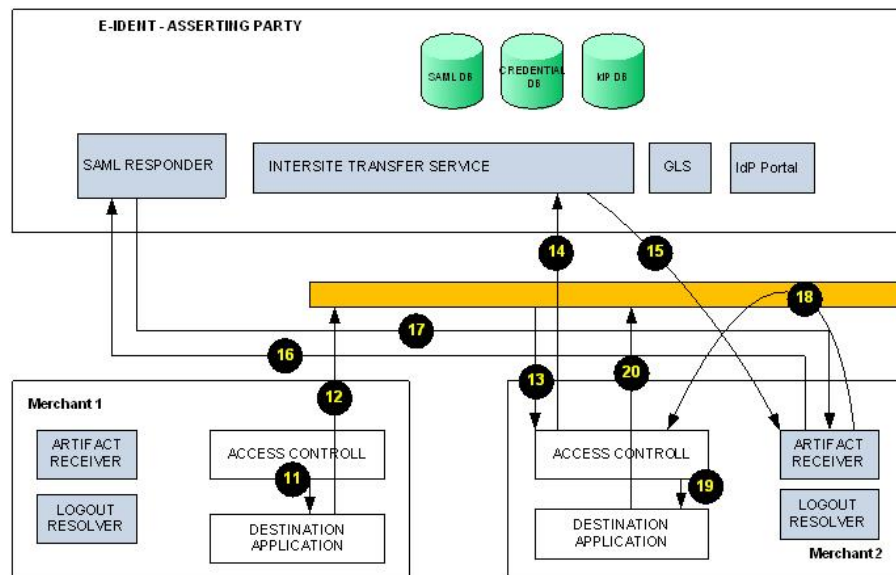
Single sign-on

Single sign-on (SSO) allows registered Merchant sites to share asserted End user attributes without requiring them (the End users) to identify themselves again to each of the Merchant sites. SSO is not enabled by default, but Merchants opting to provide End users with this ability have to enter into a mutual SSO agreement.

The binding requirements for such an agreement are beyond the scope of this document, but the following issues are among the items covered:

- two or more member Merchants
- common requirements for identification attributes (assertions)

A SSO enabled identification is transparent to the Merchant and requires no special treatment by Merchant applications. The request and valid parameters are identical to those of an ordinary identification sequence as described in section Identification request above.



The figure above illustrates a single sign-on (SSO) sequence. This is a continuation of the log in identification request described at the beginning of chapter 4. Steps 11 and 12 are described in the previous section.

This sequence is only relevant where Merchant 2 is in the same SSO clus-

ter as Merchant 1, and that the End user is already logged into Merchant 1 (and wishes to access a restricted resource on Merchant site 2).

13. The End user requests for a protected resource in Merchant 2 web site.
14. Merchant 2 cannot register that the request has been authenticated and redirects the End user to E-Ident for identification.
15. *ITS* detects that the End user had already provided their credentials (through Merchant 1 login). *ITS* generates an assertion for the End user and a corresponding artifact.
16. The Artifact Receiver uses the artifact from step 15 above to retrieve an assertion (section SAML request).
17. The SAML responder returns a SAML response (section SAML response) containing the assertion.
18. The Artifact Receiver then sends the browser the intended `TARGET` resource.
19. Merchant 2 authenticates the End user and grants access to the targeted resource
20. The resource is displayed in the web browser.

SAML request

After the End user identification, a SAML artifact is generated that can be used to access the identification details of the End user (name, date of birth, roles and privileges, for instance).

This artifact, together with the `TARGET` that the Merchant provided in the initial log in request, is sent to the Merchant artifact resolver URL. The resolver URL is preconfigured by the Merchant and provided during configuration (see the *"Nets Signing and Identification Services Technical configuration form"*).

The SAML request is used to get a SAML assertion that contains attributes describing the user. The artifact must be provided in the SAML request (ArtifactRequest) within the SAML AssertionArtifact XML element of the SOAP message. Refer to the *"SAML assertion"* documentation for more details.

E-Ident only supports the AssertionArtifact request. Here is a sample request:

```
<?xml version="1.0"?>
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:ns1="urn:oasis:names:tc:SAML:1.0:protocol"
xmlns:ns2="http://www.w3.org/2000/09/xmldsig#"
xmlns:ns3="urn:oasis:names:tc:SAML:1.0:assertion">
  <soapenv:Body>
    <ns1:Request MinorVersion="1" MajorVersion="1"
RequestID="CFB7892DC7F7CD3F954DDC721BDBAF7DB2E51C62">
      <ns1:AssertionArtifact>AACAKo1eAGQeNw1SRkVR3Cg</ns1:AssertionArtifact>
    </ns1:Request>
  </soapenv:Body>
</soapenv:Envelope>
```

The SAML request requires that the merchant application provides basic access authentication credentials. Invalid credentials will get an HTTP response with an error code and an empty SAML response.

SAML response

With the SAML response, the Merchant website is now able to obtain details about the identified End user.

The details obtained from the *SAMLResponse* depend on eID provider policies, personal information access regulations, and on the assertion templates configured for the Merchant.

If a corresponding assertion is found for the artifact, a SAML assertion with the status Success is returned by E-Ident. The response will contain all asserted attributes of the authenticated user, as well as information on the assertion validity, and the method used for identification.

If no assertion could be found for the artifact, a SAML response is returned that does not contain any asserted attributes (the status will still be set to Success).

If there is an error with the artifact, for example if the artifact has expired, the SAML response contains a status message. The assertion retrieved might contain the following attributes:

Name	Description
Certificate	The certificate in Base64 encoding
PID	Personal Identifier
SSN	Social security number, or other equivalent

SAML error response

An error message can be returned for various reasons. The error message type is either a SOAPFault or a SAML message with a status message describing the error. The format of the SAML message is described in the "SAML assertion" documentation.

Error messages are triggered by the following events:

Trigger	Error message type
Merchant sent an expired SAML artifact	SAML
SOAP XML received not well formed or cannot be vali-	SOAPFault

dated against schemas	
SAML XML received not well formed	SOAPFault
SAML XML cannot be validated against schemas	SAML

Log out sequence

Log out allows a Merchant website to terminate an authenticated End user session. To initiate the log out process, the *Global Logout Service (GLS)* has to be invoked by the Merchant website.

GLS base URL	https://ti-pp.bbs.no/gls/logout.html
--------------	-----------------------------------------------------------------------------------------

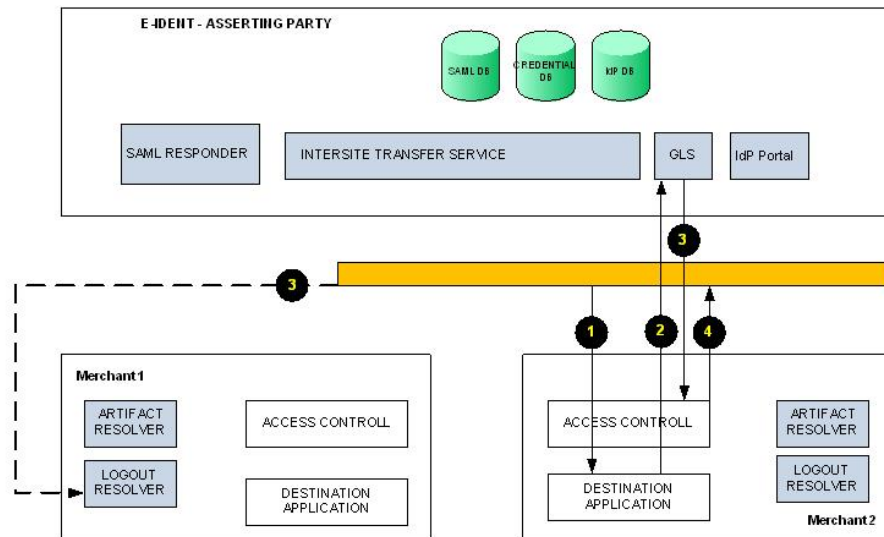
The base URL accepts the following parameters:

Parameter name	Description	Constraints
mid	Merchant identifier. This is an ID assigned to the Merchant upon configuration and must be used in subsequent requests to E-Ident.	Required: yes
nexturl	After log out, the End user will be directed to the URL pointed to by the <code>nexturl</code> parameter. If not provided, E-Ident presents the user with a generic log out page.	Required: no Format: URL
deflect	Name of a target frame. The named frame is the one assigned to render the artifact receiver after identification.	Required: no Default: <code>_top</code> Regular expression: <code>[_a-zA-Z0-9]{1,12}</code>

During log out, *GLS* will perform a call to the Merchant logout URL provided at configuration time. The logout URL allows the Merchant website to clean up any session context data for the affected End user (session invalidation, logging, etc.). The logout URL is not presented to the End user and should therefore not publish any content.

If a `nexturl` parameter is provided, the End user is eventually directed to that URL after the *GLS* is done cleaning up the session.

The `deflect` parameter (when provided) instructs *GLS* to direct the display of `nexturl` to a named frame. This is used if the Merchant wishes to display `nexturl` in a different frame (for example another browser window, the parent frame or get rid of all frames altogether)



The figure above illustrates a log out sequence.

1. The End user has access to some protected content in Merchant site 2.
2. Merchant 2 provides a log out link to *GLS*.
3. The *GLS* creates a record of the valid identification that exists for the current user and invokes *logout* URLs for all Merchants with active user identifications. If merchant 2 and merchant 1 are in the same SSO cluster, then both *logoutURLs* are invoked.
4. If the Merchant has provided a *nexturl*, the browser is then sent to that URL.

Status request

Whenever an unexpected event occurs, a status message can be displayed to the End user. This status message provides the End user with a simple explanation of the cause (sometimes a suitable remedial action is also provided).

Status codes are displayed whenever the normal identification sequence is interrupted, such as when an error occurs or when the End user chooses to cancel the process.

If the *status* parameter is set, either in the *LoginRequest* or upon configuration, E-Ident does not show a status page to the End user, but instead, redirects the browser to the Merchant *status* URL. A status code is appended to the *status* URL.

Example: If the status URL is set to <https://merchant/statusurl.html?su=> and the identification fails, the End user is redirected to <https://merchant/statusurl.html?su=authfailed>.

The list of message labels used by E-Ident is given below.

Label	Description
authfailed	The logon was not successful.
Cancel	The End user cancelled the log in process.
Generalerror	A general error has occurred. This is the default error label.
merchant404	There is an error with the configuration of the selected Merchant and eID provider combination.
ua.nobrowser	The browser of the End user is not supported.
ua.nocookies	The End user browser does not support Cookies, which is required.
ua.nojava	The End user browser does not support Java, which is required.
ua.nojavascript	The End user browser does not support JavaScript, which is required.
ua.noos	The operating system of the End user is not supported.
ua.oldos	The operating system of the End user is not supported.
ua.oldjava	The End user needs to upgrade the Java version installed in the browser.
ua.oldjs	The End user needs to upgrade the JavaScript version running in the browser.
ua.unsupported.version	The browser version of the End user is not supported.
ua.unsupported.charset	The browser of the End user supports only character encodings that are not supported by E-Ident.
uid.blocked	The ID of the End user has been blocked.
uid.revoked	The ID of the End user has been revoked.
uid.expired	The ID of the End user has expired.

wrongmobdob	A wrong mobile phone number or date of birth has been supplied. This status code is related to "BankID på mobil".
-------------	-------------------------------------------------------------------------------------------------------------------

Note: Some status codes (such as merchant404) are never sent to the Merchant status URL but handled internally by E-Ident.

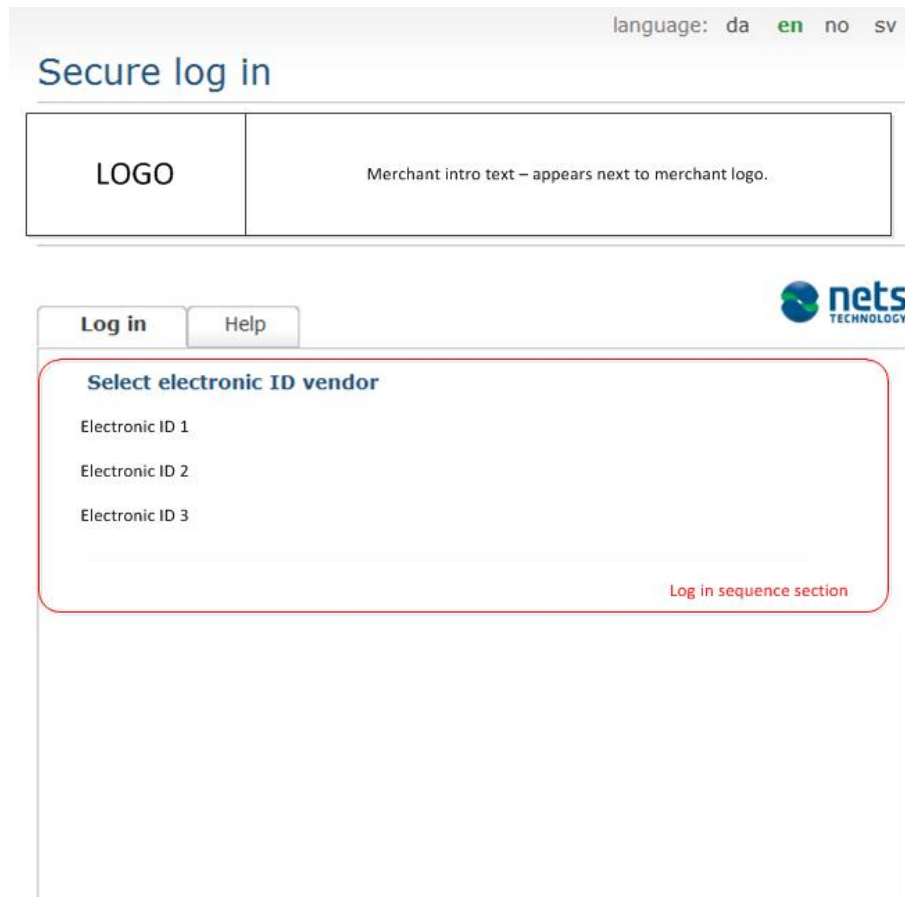
5. Visual presentation

The identification request allows Merchants to configure how the log in sequence is rendered. Merchant sites may provide presentation hints to E-Ident. These hints are used to determine how the log in pages are displayed (layout, font types, colours, etc.).

E-Ident has two presentation modes: *normal GUI* mode, and *reduced GUI* mode.

Normal GUI

The *normal GUI* mode is the standard presentation mode. In *normal GUI*, the log in sequence is rendered within a E-Ident layout (colours, fonts, and graphics).



language: da en no sv

Secure log in

LOGO	Merchant intro text – appears next to merchant logo.
------	------------------------------------------------------

Log in Help

Select electronic ID vendor

- Electronic ID 1
- Electronic ID 2
- Electronic ID 3

Log in sequence section

nets TECHNOLOGY

The layout presented to the End user contains elements that identify the Merchant (a Merchant logo, and introductory text). The Merchant is required to provide both the logo, and introductory text during configuration.

The screenshot above illustrates how *normal GUI* might look like with a

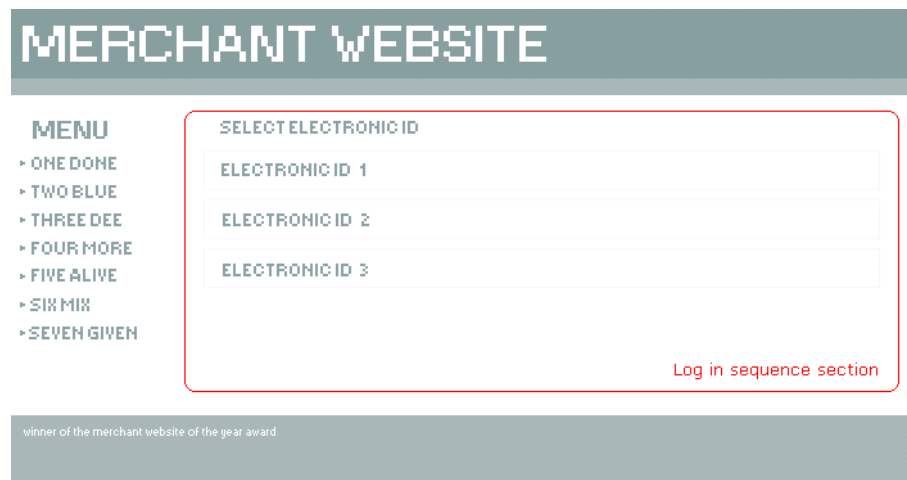
Merchant logo and accompanying text. All other page elements (including the language selection tabs at the very top) are standard E-Ident assets.

The following table lists the parameters required to specify normal GUI:

Parameter	Description
wi	For normal GUI, set the value of this parameter to "n" (without quotation marks)

Reduced GUI

In *reduced GUI* mode, Merchants have greater control over the look and feel of the identification sequence.



In *reduced GUI*, E-Ident allows Merchants to embed the log in sequence within the Merchant website. Notice how the font type and colour within the sequence has been matched to that of the Merchant site in the previous screenshot.

The following table lists the parameters required to specify *reduced GUI*:

Parameter	Description
wi	For reduced GUI, set the value of this parameter to "r" (without quotation marks)
style	Full URL to the Merchant style sheet. When provided, the style sheet will override all other style sheets such as E-Ident default style, and the Merchant style sheet provided during configuration. The style sheet will be used throughout the log in sequence
deflect	Name of a target frame (default is <code>_top</code>)

In addition to selecting *reduced GUI*, the Merchant is also required to provide some screen real estate for E-Ident (i.e. the Merchant site must provide E-Ident with an area within which to run). This can be accomplished

by using frames, iframes or layers.

The *deflect* parameter is used to specify which named frame (a window, a frame) the target URL will be displayed in. When not specified, the *deflect* has an assigned value of `_top`.

A simple iframe can be set up with similar HTML code:

```
<iframe
  name="E-Ident "
  src="https://ti-pp.bbs.no/its/index.html?mid=merchantid&wi=r&..."
  height="512"
  width="640">
</iframe>
```

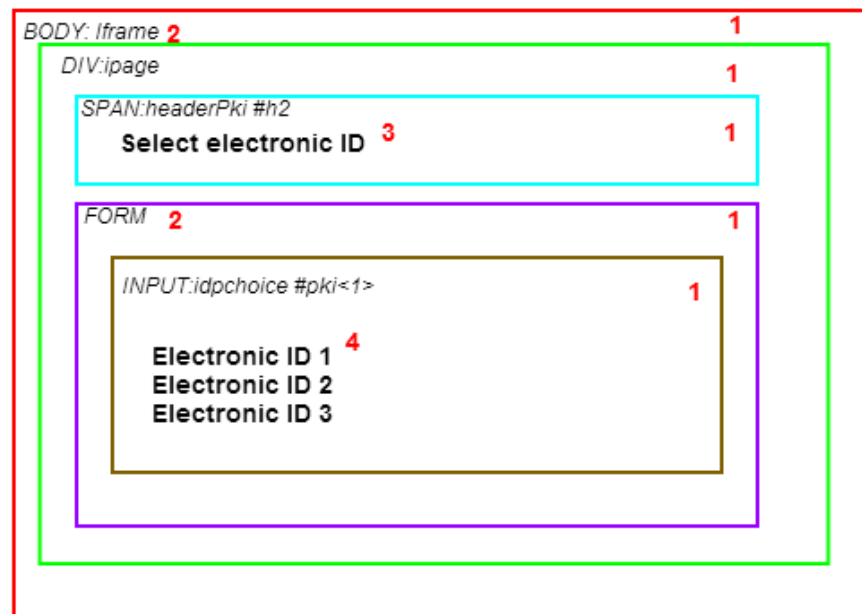
Please refer to the CSS style guide chapter for details of how the style sheets can be configured for E-Ident.

6. CSS style guide

Introduction

This section describes CSS style elements used in E-Ident. These styles can be modified by Merchant websites that wish to provide custom styles to End users.

In all diagrams and figures, the various page components and sections will be marked in colorful frames (1), as illustrated in the figure below.

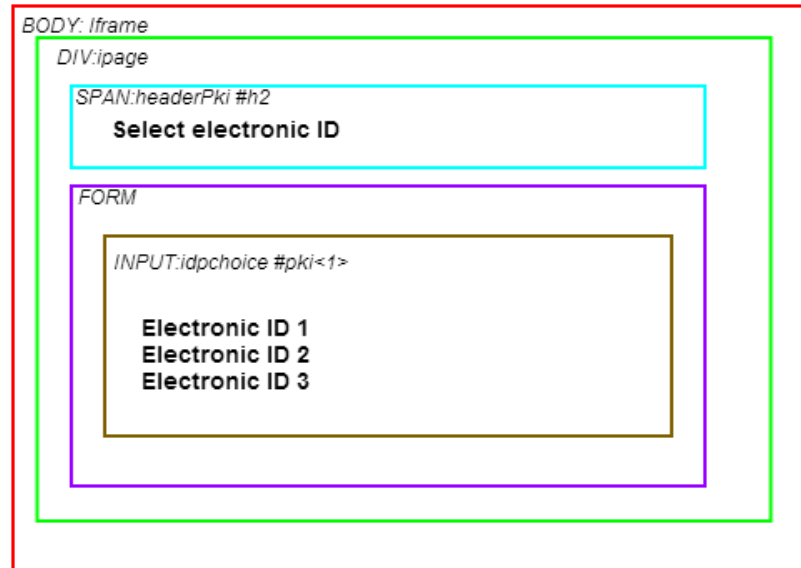


Each colored frame is represented in the HTML code as a block tag (2). A block tag could be either a `BODY`, `DIV`, `TABLE`, `FORM`. If the HTML tag has a CSS style assigned to it, that will be indicated together with the HTML tag (for instance, the `BODY` in the diagram above has a CSS style class named `iframe`).

Some page sequences have static content which is rendered as part of the page. (3) is in this case a static content element. In the diagram, the content has been laid out using the `SPAN` HTML tag. (4) is the main page content.

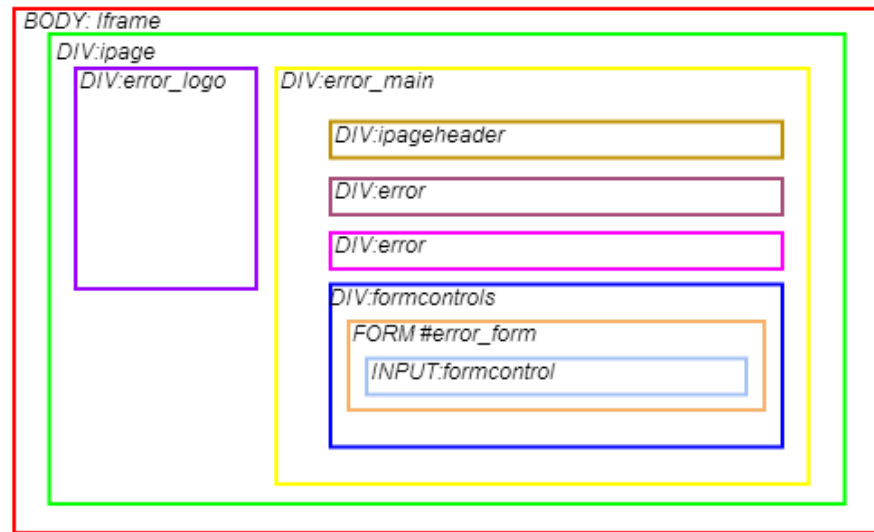
eID selection

E-Ident displays an eID provider selection page if the Merchant supports more than one eID provider. The eID selection page is skipped if there is only one valid eID provider for the current request.



Element	Description	Defaults
BODY: iframe	HTML body tag (root element for styling)	Width: 100%
DIV: ipage	Page parent tag contains all other content items.	
SPAN: headerPki #h2	HTML span tag with h2 as CSS id and headerPki as class.	
FORM	A form houses all listed eIDs.	
INPUT: idpchoice #pki<1>	Each eID provider element is an HTML input tag with pki<eID provider number> as CSS id.	
INPUT: idpchoice_ hover	The idpchoice_hover class is invoked when the mouse passes over an item in the eID provider list	

Status page



Element	Description
DIV: error_logo	Icon next to status message
DIV: error_main	Container for error messages and buttons
DIV: ipageheader	Message heading just above the status message (some messages do not have headings)
DIV: error	Status message text
DIV: formcontrols	Form control elements (input buttons and submit buttons)
FORM #error_form	Form for input buttons
INPUT: formcontrol	Input buttons

Please refer to the full CSS style sheet elements table in the appendix.

7. Configuration

Network address and protocols

Service	Protocol	URL (customer test system)
ITS	HTTPS	https://ti-pp.bbs.no/its/index.html
GLS	HTTPS	https://ti-pp.bbs.no/gls/logout.html
SAML 1.1 Responder	SOAP over HTTPS	https://ti-pp.bbs.no/saml1resp/getassertion

Service	Protocol	URL (production system)
ITS	Secure HTTPS	https://ti.bbs.no/its/index.html
GLS	Secure HTTPS	https://ti.bbs.no/gls/logout.html
SAML 1.1 Responder	SOAP over HTTPS	https://ti.bbs.no/saml1resp/getassertion

Note: All HTTPS servers listen on standard secure SSL port 443.

Recommended eID provider dimensions

eID provider	Minimum dimensions in pixels (width x height)
BankID NO	400 x 280
BankID on mobile phones (NO)	480 x 280 (regular GUI will be shown) 479 (or lower) x 280 (a smaller, responsive GUI will be shown)
Buypass	400 x 300
NemID with key card	200 x 250
NemID with key file	500 x 200

Mobile BankID	400 x 628
---------------	-----------

System property timeouts

Property	Timeout	Usage
ART_MAX_AGE	3	SAML artifact lifetime specifies the time limit within which the artifact can be used to retrieve an assertion.
GID_IDLE_TIMEOUT	30	The maximum time allowed between consecutive E-Ident requests within the same session. When GID_IDLE_TIMEOUT elapses, a new session is created.
GID_MAX_AGE	1440	The maximum length of time a E-Ident session can be kept active.

All time units are in minutes.

8. Appendix 1

CSS Style sheet elements

Style sheet elements	Description/usage
.iframe	This class is assigned to all HTML body tags in E-Ident
.ipage	Each page has a master div tag with an ipage class
.idpchoice	The eID provider selection page displays each ID as a form button. Each button uses this class
.idpchoice:hover, .idpchoice_hover	Class used for eID provider choices that are in focus (onMouseOver)
.form_a	HTML links within a form
.formcontrols	Parent class for form controls (all form controls are placed within a single div using this class)
.formcontrol	Each form control is assigned this class
.formcontrol:hover	Class used for form controls that are in focus
.error_main	Alert box for displaying status messages
.error	Status message or error message
.error_logo	Icon next to status message
.info	Info box
#h0 #h1 #h2 #h3 #h4	Heading text classes (number grows as the heading size decreases. Normal heading size is h3)
#t0 #t1 #t2 #t3 #t4	Normal text classes (number grows as the text size decreases. Normal text size is t3)
#w0 #w1 #w2 #w3 #w4	Warning text classes (number grows as the warning size decreases. Normal text size is w3)
#n0 #n1 #n2 #n3 #n4	Highlighted text classes (number grows as the highlight text size decreases. Highlight text size is n3)

.main	Main container for page
.ipageheader	Header inside iframe
.logo	eID provider logo container
.formheader	Header inside form
.status	Status messages inside form
.info_body	DIV container for information to the user and input fields.
.body	Information text
.text	Input fields with text or number input
#ssn #cpr	Input fields for ssn and cpr.
.button_holder	Div container for the buttons
.bidmobil	"BankID på mobil" (NO): Parent class for form controls (all form controls are placed within a single div using this class)
.bidtext	"BankID på mobil" (NO): Input fields for text.
#bidmob_mobilen0	"BankID på mobil" (NO): Input field for mobile number.
#bidmob_mobilealias	"BankID på mobil" (NO): Input field for date of birth.
.bidbutton	"BankID på mobil" (NO): formcontrol will be assigned this class.
.err_img	"BankID på mobil" (NO): error icon.
.err_text	"BankID på mobil" (NO): error text.
.ref_code	"BankID på mobil" (NO): reference code.

.ref_label	"BankID på mobil" (NO): reference label.
.work_img	"BankID på mobil" (NO): loading icon.
.ref_text	"BankID på mobil" (NO): reference text.
.instructions	"BankID på mobil" (NO): Instructions for user.
#nemid_index_html	NemID JS: ID of the IDP's HTML tag
#nemid_iframe	NemID JS: ID of the iframe that contains the NemID client
#nobank-id_index_html	BankID 2.0: ID of the IDP's HTML tag
#bid_client	BankID 2.0: ID of the div that contains the BankID 2.0 client

SAML response example

```
<?xml version="1.0"?>
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:ns1="urn:oasis:names:tc:SAML:1.0:protocol"
xmlns:ns2="http://www.w3.org/2000/09/xmldsig#"
xmlns:ns3="urn:oasis:names:tc:SAML:1.0:assertion">
  <soapenv:Body>
    <ns1:Response IssueInstant="2010-06-21T09:13:03.414Z" MinorVersion="1" MajorVersion="1" InResponseTo="CFB7892DC7F7CD3F954DDC721BDBAF7DB2E51C62" ResponseID="TI2-CFB7892DC7F7CD3F954DDC721BDBAF7DB2E51C62">
      <ns1:Status>
        <ns1:StatusCode Value="ns1:Success"/>
      </ns1:Status>
      <ns3:Assertion IssueInstant="2010-06-21T09:13:03.445Z"
Issuer="https://dev-ti.bbsas.no/saml1resp/"
AssertionID="TI2-9974DDD950FA6E04FAE3AE1E3194D035691B122E"
MinorVersion="1" MajorVersion="1">
        <ns3:Conditions NotOnOrAfter="2010-06-21T09:43:02.000Z" NotBefore="2010-06-21T09:13:02.000Z"/>
        <ns3:AuthenticationStatement AuthenticationInstant="2010-06-21T09:13:03.445Z" AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:X509-PKI">
          <ns3:Subject>
            <ns3:NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">SERIALNUMBER=PID: 1111-2222-3-444444444 + CN=Testperson 123456789 Testsen, O=Ingen organisatorisk tilknytning, C=DK</ns3:NameIdentifier>
          <ns3:SubjectConfirmation>
            <ns3:ConfirmationMethod>
              urn:oasis:names:tc:SAML:1.0:cm:artifact
            </ns3:ConfirmationMethod>
          </ns3:SubjectConfirmation>
        </ns3:AuthenticationStatement>
      </ns3:Assertion>
    </ns1:Response>
  </soapenv:Body>
</soapenv:Envelope>
```

```

</ns3:Subject>
</ns3:AuthenticationStatement>
<ns3:AttributeStatement>
  <ns3:Subject>
    <ns3:NameIdentifier
      Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
      SERIALNUMBER=PID: 1111-2222-3-4444444444 + CN=Testperson 123456789
      Testsen, O=Ingen organisatorisk tilknytning, C=DK
    </ns3:NameIdentifier>
  </ns3:Subject>
  <ns3:Attribute AttributeNameSpace="urn:bbs:esec:adames:ti2:saml:1.1:attributeNamespace:uri"
    AttributeName="DK_SSN">
    <ns3:AttributeValue
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xsi:type="xs:string">123456789</ns3:AttributeValue>
    </ns3:Attribute>
  <ns3:Attribute AttributeNameSpace="urn:bbs:esec:adames:ti2:saml:1.1:attributeNamespace:uri"
    AttributeName="DK_DAN_PID">
    <ns3:AttributeValue
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xsi:type="xs:string">1111-2222-3-4444444444</ns3:AttributeValue>
    </ns3:Attribute>
  </ns3:AttributeStatement>
</ns3:Assertion>
</ns1:Response>
</soapenv:Body>
</soapenv:Envelope>

```

SOAPFault response example

```

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>
    <SOAP-ENV:Fault>
      <faultcode>SOAP-ENV:Client</faultcode>
      <faultstring>
        SOAP Processing Error. Received invalid SOAP message. No SAML artifacts found in the message.
      </faultstring>
    </SOAP-ENV:Fault>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

Example of a SOAPFault returned when an invalid SAML artifact is provided when querying for an assertion.

E-Ident SAML WSDL

WSDL of the web service

```
<?xml version="1.0" encoding="UTF-8"?>
<definitions xmlns="http://schemas.xmlsoap.org/wsdl/"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:tns="http://www.bbs.no/esec/adames/ti2/saml11/2010/06#"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:saml="urn:oasis:names:tc:SAML:1.0:protocol"

targetNamespace="http://www.bbs.no/esec/adames/ti2/saml11/2010/06#">
  <types>
    <xsd:schema>
      <xsd:import namespace="urn:oasis:names:tc:SAML:1.0:protocol"
schemaLocation="oasis-sstc-saml-schema-protocol-1.1.xsd"/>
    </xsd:schema>
  </types>
  <message name="request">
    <part name="parameters" element="saml:Request"/>
  </message>
  <message name="response">
    <part name="parameters" element="saml:Response"/>
  </message>
  <portType name="GetAssertion">
    <operation name="getassertion">
      <input message="tns:request"/>
      <output message="tns:response"/>
    </operation>
  </portType>
  <binding name="GetAssertionPortBinding" type="tns:GetAssertion">
    <soap:binding style="document"
transport="http://schemas.xmlsoap.org/soap/http"/>
    <operation name="getassertion">
      <soap:operation/>
      <input>
        <soap:body use="literal"/>
      </input>
      <output>
        <soap:body use="literal"/>
      </output>
    </operation>
  </binding>

  <service name="GetAssertionService">
    <port name="GetAssertionPort" bind-
ing="tns:GetAssertionPortBinding">
      <soap:address loca-
tion="https://ti.bbs.no/saml11resp/getassertion"/>
    </port>
  </service>
</definitions>
```

Please note that the SOAP address location for customer test environment will vary from the URL provided in the above example.

E-Ident assertion attributes

The following table lists all available assertion attributes that may be returned in a SAML response. Not all attributes are available in all SAML responses. The list of returned attributes is specific to the eID provider used for identification.

Attribute	Description/Usage	eID provider
IDPROVIDER	The ID provider used for identification	ALL. See valid values in a table below this table.
CERTPOLICYOID	A policy identifier for the End user certificate	ALL
CN	Common Name from End user certificate	ALL
DN	Distinguished Name from End user certificate	ALL
CERTIFICATE	The X509 certificate of the identified End user	ALL
NOTAFTER	Certificate validity end time	ALL
NOTBEFORE	Certificate validity begin time	ALL
FIRSTNAME	End user first name (from certificate)	ALL (where available)
SURNAME	End user surname (from certificate)	ALL (where available)
GIVENNAME	End user given name (from certificate)	ALL (where available)
C	Country code	ALL (where available)
DOB	Date of birth where available	
DK_SSN	Danish SSN	NemID
NO_SSN	Norwegian SSN	Norwegian BankID
NO_CEL8	8-digit mobile/cell number (provided by merchant or user)	Norwegian BankID Mobile
NO_DOB6	6-digit date of birth (provided by merchant or user)	Norwegian BankID Mobile

DK_DAN_PID	DanID PID	DanID
NO_BID_PID	Norwegian BankID PID	Norwegian BankID
NO_BP_FIRSTNAME	Buypass first name	Buypass smartcard
NO_BP_LASTNAME	Buypass surname	Buypass smartcard
NO_BP_BUYPASSID	Buypass ID	Buypass smartcard
SE_BID_SECURITYLEVEL	Swedish BankID security level	Swedish BankID
SE_SSN	Swedish SSN	Swedish BankID

The following table gives the valid values for the IDPROVIDER attribute:

eID provider	IDPROVIDER value
BankID Java applet	no_bidnc
BankID client without Java	no_bankid
"BankID på mobil" (NO)	no_bidmob
NemID JS client (DK)	dk_nemid_js
NemID OpenSign applet (DK)	dk_nemid-opensign
Buypass Smartcard (NO)	no_bp
Telia e-legitimation (SE)	se_telia
BankID (SE)/Mobile BankID /Nordea e-legitimation	se_bankid

Basic E-Ident requirements

E-Ident uses HTTP cookies to temporarily store session data. The stored data is only used to manage the state of the current session and has a lifetime ranging from a few seconds to at least a whole day. No sensitive, private, or critical information is stored in the HTTP cookies, and it is only used when SSO and the Global Logout possibility shall be used. For all other needs E-Ident will enforce URL rewrite instead of cookies.



For browsers that do not support 3rd party cookies (when E-Ident are used with reduced GUI) E-Ident will enforce URL rewrite instead of cookies. SSO and Global Logout are not supported in this mode.

E-Ident requires that web browsers also have been enabled to run Java applets and Javascript.

9. Appendix 2 – eID providers

Introduction

This appendix aims to list information regarding the different eID providers.

eID provider	How to obtain merchant ID
NemID POCES (DK)	https://www.nets-danid.dk/
NemID MOCES (DK)	https://www.nets-danid.dk/
BankID (NO)	http://www.bankid.no
“BankID på mobil” (NO)	http://www.bankid.no
BankID (SE)/Mobile BankID /Nordea e-legitimation	http://www.bankid.com http://www.nordea.se/e-legitimation
Telia e-legitimation (SE)	http://eid.trust.telia.com
Buypass Smartcard (NO)	http://www.buypass.no

How to enable a new eID

To enable a new eID for your Merchant site, the following steps should be fulfilled:

- Send an updated version of the “Nets Signing and Identification Services Technical configuration form” to support. If the eID should be added to your existing Merchant site, please state existing site and your MerchantID. Complete the applicable fields in the chapter regarding eID’s.
- Specific eID details like eID information, merchant certificates and test certificates are provided later in this chapter.

BankID (NO)

Information

To enable BankID (NO) in your Merchants application you need an agreement with a bank issuing BankID (NO) for a merchant certificate. More information:

<https://www.bankid.no/BankID-for-ditt-nettsted/>

Note: In the order form received from the bank, remember to check the "enable SSN" box if you are going to use SSN in your application.

Test certificate

Nets eSecurity support will issue a test merchant certificate to you if not otherwise stated. In cases where others are issuing the certificate, please send the activation link and code for the certificate to Nets eSecurity support: support.esecurity@nets.eu, (or you can make the bank forward the information directly). Nets Signing and Identification Services will activate the certificate and do the configuration.

End user test certificates can be ordered from Nets eSecurity support at support.esecurity@nets.eu. If you need a specific SSN (preferably a fictive as this is test), please provide that together with the request for a test user certificate.

Production certificate

Nets through the Signing and Identification Services are resellers of BankID merchant certificates, and this can be ordered either separately or together with E-Ident. If ordered through Nets, you will in an information letter be asked to complete a form with information needed to create a BankID "brukerstedsavtale" with BankID Norge. The form shall be returned to support.esecurity@nets.eu, and based on the form Nets will register this order at BankID. After the registration you will be asked to confirm and sign the order. When the order is signed with BankID Norge, Nets will receive the activation information for your BankID merchant certificate from your bank. The merchant certificate will be activated and connected to your E-Ident configuration.

If you haven't ordered the BankID merchant certificate through Nets, you will receive an activation link and code from your bank or another reseller of BankID merchant certificates. Contact Nets Signing and Identification Services support to get the name and number of the person that shall receive the certificate information. The certificate information shall be sent to Nets Signing and Identification Services in two different channels (e.g activation link in an e-mail and activation code by sms).

If your bank requires a CoC (Certificate of Confirmation) before issuing the merchant certificate, please contact support. Nets Signing and Identification Services will send a CoC to your bank.

**BankID 2.0
(without Java)**

From the 2.0 release of BankID, the BankID client is independent of Java. The E-Ident service is updated to support the new BankID client without Java. This section will explain what to do to start using the new BankID client and customer impact.

Migration and getting started

Migration to BankID 2.0 from BankID Java applet:

System	What to do
Customer test	<p>Customers may be migrated to BankID 2.0 from the 23rd June. Migration of the customer's merchant site is done upon request to support.esecurity@nets.eu. Please supply us with your MerchantID / MID and the preferred time for migration. If BankID Java applet should be available after the configuration, please let us know. See the IE8 work-around for information regarding this.</p> <p>Migration in customer test is done consecutively and within 1-2 working days from the request.</p>
Production	<p>Nets will schedule weekly migrations of customers in production. This will be every Tuesday during day time from the time it is available in production. Please notify Nets eSecurity support five days prior to migration.</p> <p>The first migration will be right after the production release of BankID 2.0 for those of Nets' customers that want to start using BankID 2.0 immediately. To be a part of the first migration, please notify Nets eSecurity support at least 10 working days before.</p> <p>Other migration times than Tuesdays may be agreed with Nets. Please notify Nets eSecurity support as soon as possible about your preferred time schedule.</p> <p>When notifying Nets about your preferred production time, please include the MerchantID(s) /MID(s). If BankID Java applet should be available after the configuration, please let us know. See the IE8 workaround for information regarding this.</p> <p>A roll-back procedure of your migration will be in place. Notify Nets eSecurity support as soon as possible if you are in need of a roll-back of the migration.</p>

Customer impact

The migration to BankID 2.0 may be done without any specific changes in the interface between the customer and the E-Ident service. The following should however be considered:

1. The use of BankID 2.0 and Internet Explorer 8. It will not be possible to use IE 8 together with the BankID 2.0 client. A solution to use IE8 together with the "old" BankID Java applet will be added prior to production.
2. There will be no changes to the forcepkivendor parameter.

3. Migration to BankID 2.0 will impact graphical appearance and platform support. Nets strongly advises the customers to use the customer test facilities to test migrated systems before opening for the production system. The recommended and minimum IFRAME sizes from BankID are:
 - a. Large screen (Desktop/tablet): 396px (w) by 280px (h) (recommended) / 370px (w) by 204px (h) (minimum)
 - b. Small screen (Smartphone) (only minimum sizes): 320px (w) by 350px (h) (portrait) / 480px (w) by 200px (h) (landscape)
4. The optional small applet in E-Ident is now set to the minimum IFRAME size. Customers need to configure their applications with this IFRAME size.
5. The IDPROVIDER attribute in the SAML artifact has been changed from no_bidnc to no_bankid when BankID 2.0 has been used. The no_bidnc parameter will be returned when the BankID with Java Applet has been used.
6. Some customers may experience that the BankID client has been cropped inside the IFRAME. This is solved by adjusting your CSS file. See the "CSS file adjustment" section on the next page.

IE 8 workaround

IE 8 is not supported with BankID 2.0. To be able to still support IE 8 a workaround to load the "old" BankID Java Applet will be made available. This functionality is not available in the first release of BankID 2.0 support in E-Ident. Please make sure to notify our support that you want both BankID 2.0 and BankID Java Applet to be available.

If your Merchant configuration is made available with both BankID 2.0 and BankID Java Applet, the parameter "forcepkivendor" must be used to determine which client to start. The "no_bidnc" will start the BankID Java Applet, while "no_bankid" will start the BankID 2.0 client. If the "forcepkivendor" parameter is not given, BankID 2.0 will be started. The user will never get the possibility to select between BankID 2.0 client and BankID Java Applet. If the "Select" page from E-Ident is shown to the end user, only one choice for BankID will appear, and this is the newest version of BankID.

Note: If you today are using the "forcepkivendor" parameter, your implementation must be changed so that the "no_bidnc" parameter is not sent as default. If you have not specified that the BankID Java Applet shall be

available for your configuration, both “forcepkivendor” parameters (“no_bidnc” and “no_bankid”) will start the BankID 2.0 client.

See more about the “forcepkivendor” parameter in chapter 4 of this document.

CSS file adjustment

The BankID 2.0 client must be styled with CSS to display properly. The default styling has CSS rule that set the proper sizes. If you override styling, your style sheet must be updated for the new BankID client. Styling can be overridden either by setting av style URL in the merchant configuration or by sending a style parameter when starting identification.

The default CSS styling sets width and height to 100%. The client will then expand to fill the container (iframe), regardless of the container size.

When overriding styling, the sample CSS below will produce the same effect as the default styling.

```
#nobankid_index_html {
    height: 100%;
    overflow-y: hidden; /* make sure no scroll bar is shown */
}

#nobankid_index_html .iframe,
#nobankid_index_html .iframe .ipage {
    height: 100%;
}

#nobankid_index_html .iframe .ipage .main {
    height: 100%;
    min-height: 200px;
}
```

Known issue

With the BankID-app it is not always possible to detect if the app is installed on the device used for identification. It is also a known issue regarding automatic start of the BankID-app when using Android OS.

When the app is closing, E-Ident tries to redirect the user back to the browser. However, it is not guaranteed that the user is redirected back to the same browser as the one that started the session. The merchant implementation must support that the end user are redirected back in a new web browser, eg cookies cannot be used.

“BankID på mobil” (NO)

Information

To enable BankID on mobile phones (NO) in your Merchant application you need an agreement with a bank issuing BankID (NO) for a merchant certificate (“Brukerstedssertifikat”). When ordering the BankID merchant certificate make sure to order BankID on mobile phones as well.

To be able to use BankID on mobile phones you also need an agreement with the phone suppliers. Your bank will supply you with the information you need.

More information:

<https://www.bankid.no/>

Test certificate

For issuance of a BankID merchant test certificate, see the Test certificate section in the BankID (NO) part earlier in this chapter. Remember to order BankID on mobile phones when you order a BankID (NO) merchant test certificate.

For End user test certificate you need a dedicated mobile phone with a SIM-card for test purposes. Contact BankID Norge to retrieve a SIM-card. After receiving the SIM-card, contact BankID support (support@bankid.no) to register the SIM-card in BankID preproduction.

Production certificate

For issuance of a BankID merchant certificate, see the Production certificate section in the BankID (NO) part earlier in this chapter. When ordering the BankID merchant certificate make sure to order BankID on mobile phones as well.

CSS

The BankID on mobile phones GUI pages have some specific CSS elements. See the HTML code in test for the different styling options. All elements are also described in Appendix 1.

Pre-set mobile phone number and birthdate

The end user’s mobile phone number and birthdate may be preset at the Merchant’s own site prior to calling the E-Ident service. The mobile phone number and birthdate can be appended to the SAML request to E-Ident. See the Identification request section of chapter 4 for more information.

BankID (SE)

Information

To enable BankID (SE) in your Merchants application you need an agreement with a bank issuing BankID (SE). See <https://www.bankid.com> for banks that issues BankID and general information about BankID.

BankID (SE) is issuing End user certificates in different ways (<http://www.bankid.com/sv/Vad-ar-BankID/BankID-pa-flera-satt/>). "BankID på kort", "BankID på fil" and "Mobilt BankID" are all supported through E-Ident. From April 2014, Nordea e-legitimation certificates are supported through BankID (SE) in E-Ident as well instead of as an own eID implementation in E-Ident.

Test certificate and clients

Nets Signing and Identification Services has a test merchant certificate and test user certificates that the Merchant can use. This will be distributed to you during configuration of the test Merchant site. You may also get end user test certificates from your bank.

To test identification using Mobilt BankID, a test version of the "BankID säkerhetsapp" must be downloaded from <http://www.bankid.com/rp/info/> and a test certificate to the given phone. See chapter 7 of the document "BankID Relying Party Guidelines v2.x" at the page <http://www.bankid.com/rp/info/>. In the table you will find information about the test version of BankID Security App for Android, iOS and Windows 8.

To test identification on a PC, you need to download the latest BankID security program (BISP 5.x or higher) from <https://install.bankid.com/>. It is the same version of the BISP program that shall be used in both test and production. However, to use it in test you need to do some configurations on your PC. See chapter 7 of the document "BankID Relying Party Guidelines v2.x" at the page <http://www.bankid.com/rp/info/>. In the table you will find information about the test version of BankID Security Application for PCs (Windows and OS X). A CavaServerSelector.txt file has been added to the E-Signing document package.

Production certificate

These steps should be followed to retrieve a certificate:

- Merchant: Fill in the needed information in chapter 6.4 in the "*Nets Signing and Identification Services Technical configuration form*". This is information that Nets will be using when generating a certificate request (*.p10 file) on behalf of the customer. Send in the complete form or an updated form to Nets Signing and Identification Services support support.esecurity@nets.eu.
- Nets: Based on the information in the above form, Nets will generate a *.p10 file. When generating a *.p10 file the private and public key pair is generated and stored safely at Nets. After generating

the file, Nets will e-mail this to the Merchant.

- Merchant: E-mail the certificate request to your bank. The certificate the merchant gets in return must be forwarded to Nets Signing and Identification Services support support.esecurity@nets.eu.
- Nets: Configures your Merchant site with support for BankID (Sweden).

To support the use of Mobile BankID, the merchant certificate must include a display name. Most certificates issued after 31.12.2012 have been issued with this element.

Autostart and PresetID in BankID

BankID has two different clients. One client for PC and MAC, this is called "security program" and one for mobile devices (iOs, android, winPhone) called app.

All authentication operations must first be initialized towards the BankID infrastructure. Hence, the client will after startup connect to BankID infrastructure to check if the user has any pending operation. There are two methods of registering an operation in BankID, with or without SSN (Social Security Number/Person number). The differences between these two methods are how the client will be started. The client can be started with a reference or without. If you start the client with a reference the client will contact the BankID infrastructure and fetch the operation linked to this reference. If the client is not started with a reference the client will connect to the BankID infrastructure and check if there are any operations linked to the user's SSN. In practice, these two different methods are used to start the client on the device the user has initialized the operation, or to start the client on another device (e.g. sitting on a PC, but wants to use BankID on the phone). If you want to start the client on another device the SSN must be used.

To realize the use of this functionality, the E-Ident service uses the two parameters "autostart" and "presetid". See section Identification request in chapter 4 for information about these parameters.

The following rules applies when using the autostart and presetid parameters:

Autostart	Presetid	Behaviour
False (default)	Null (default)	<p>This will be the behavior if the customer only switches over to the new eID without doing anything at their site.</p> <p>The user will be presented with a choice of using this device or another device (if another device is selected the end-user must provide the SSN) for both identification and signing. See BankID's demo implementation of this page:</p>

		https://demo.bankid.com/nyademobanken/Logon.aspx
False	xxxxxxx	<p>This means that the end-user wants to start the client on another device.</p> <p>The end-user will be presented a message; "Launch your BankID Security App.")"</p> <p>The customer should give the end-user an option to either start the client on this device or on another device.</p>
True	Null	<p>The client will be auto started on current device.</p> <p>The customer should give the end-user an option to either start the client on this device or on another device.</p>
True	xxxxxxx	<p>The client will be auto started on current device.</p> <p>The customer should give the end-user an option to either start the client on this device or on another device, and it should send the appropriate autostart parameter.</p>

Differentiate between the different end user certificate

To differentiate between the different end user certificate types, the Merchant can use the "CERTPOLICYOID" parameter from the assertion. A list of all available certificate policy oid's is available in the latest version of the document "BankID Relying Party Guidelines" on www.bankid.com/rp/info.

Known issue

With the Mobile BankID app it is not always possible to detect if the app is installed on the device used for identification.

When the app is closing, E-Ident tries to redirect the user back to the browser. However, it is not guaranteed that the user is redirected back to the same browser as the one that started the session. The merchant implementation must support that the end user are redirected back in a new web browser, eg cookies cannot be used.

Telia e-legitimation (SE)

Information

To use Telia e-legitimation in E-Ident the Merchant must have an agreement with Telia and it needs to apply for a certificate ("Förlitande certifikat") from <http://eid.trust.telia.com>. Below is a short description on how to retrieve certificates for test and for production. For more information about the eID, please see Telia's web site.

Telia e-legitimation uses a client installed on the end user's computer to handle end user certificates i.e the NetID client.

Test certificate

To obtain a test certificate, the following steps should be followed:

- Merchant: Fill in the needed information in chapter 6.6 in the "Nets Signing and Identification Services Technical configuration form". This is information that Nets will use to generate a certificate request (*.p10 file) on behalf of the customer. Send the complete form or an updated form to support at support.esecurity@nets.eu.
- Nets: Based on the information in the above form, Nets will generate a *.p10 file (CSR file). When generating a *.p10 file the private and public key pair is generated and stored safely at Nets. After generating the file, Nets will e-mail this to the Merchant.
- Merchant: Go into Telia's web site (<https://cve.preprod.trust.telia.com/TeliaForlitande>) and apply for a "Förlitande certifikat". Mark the check box "Jag har en CSR", and copy the content of the .p10 file to the CSR field. Merchant will receive a certificate back from Telia.
- E-mail the certificate to support.esecurity@nets.eu. Nets will now configure your Merchant site with the support for Telia e-legitimation.

Production certificate

To obtain a production certificate, the following steps should be followed:

- Merchant: Fill in the needed information in chapter 6.6 in the "Nets Signing and Identification Services Technical configuration form". This is information that Nets will use to generate a certificate request (*.p10 file) on behalf of the customer. Send the complete form or an updated form to support at support.esecurity@nets.eu.
- Nets: Based on the information in the above form, Nets will generate a *.p10 file (CSR file). When generating a *.p10 file the private and public key pair is generated and stored safely at Nets. After generating the file, Nets will e-mail this to the Merchant.
- Merchant: Go into Telia's web site

(<https://cve.trust.telia.com/TeliaForlitande>) and apply for a "För-litande certifikat". Mark the check box "Jag har en CSR", and copy the content of the .p10 file to the CSR field. Merchant will receive a certificate back from Telia.

- E-mail the certificate to support.esecurity@nets.eu. Nets will now configure your Merchant site with the support for Telia e-legitimation.

User test certificates

A set of user test certificates may be obtained from this site:

- <https://eid.trust.telia.com/Testcertifikat/Teliae-legmjukt.aspx>

Note: You need to install a client like the NetID client. It can be obtained from <https://cve.trust.telia.com/TeliaElegNG/>

Known issues

E-Ident always attempts to display clear messages to the end user when unexpected events occur (such as cancellations or error messages). However, when using Telia e-legitimation, such messages cannot be displayed to the end user due to the nature of the electronic ID infrastructure. The communication between E-Ident and Telia e-legitimation is built upon SSL which is terminated prematurely when identification errors occur, and therefore denying the web browser access to an appropriate end user message. Because of this `Status URL` and `Start URL` in combination with `Teli-aID` does not have any effect.

It is not possible to change the language of the pop-up boxes Telia e-legitimation uses.

Buypass (NO)

Information

Buypass merchant certificates must be ordered from Buypass Smartkort (www.buypass.no). Buypass will issue two sets of certificates. The keystore certificates (used to secure communication between Buypass and E-Ident) will be sent by registered mail to Nets, and the password will be sent to a defined person in Nets. The Buypass merchant certificate (used to seal the SDO) will be sent by e-mail to the person ordering the certificates and the password is sent registered to either the person ordering it or a defined person in Nets. The last part must be agreed between the merchant and Nets.

NemID – personal (POCES) and employee (MOCES) certificates (DK)

Information

NemID with both personal (POCES) and employee (MOCES) certificates are supported through the E-Ident service. Information about these eID's can be found at NemID's webpages:

- <http://www.nets.eu/dk-da/Produkter/Sikkerhed/NemID-tjenesteudbyder/Pages/default.aspx>
- <http://www.nets.eu/dk-da/Produkter/Sikkerhed/medarbejdersignatur/Pages/default.aspx>

The NemID eID are offering two different clients for End users. One is the JS client (replaces the OTP applet) and the other is the OpenSign applet. The JS client and OpenSign applet again offers the possibility to identify with either personal (POCES) or employee (MOCES) certificates.

If the End user shall be presented with a list of possible eID's to identify himself with it is recommended to use the following description in “”:

- “NemID med nøglekort” (the JS client)
- “NemID med nøglefil” (the OpenSign applet)

To be able to offer identification using NemID (Personal certificate/POCES) and/or NemID Medarbejdersignatur ((Employee certificate/MOCES), Nets need to configure your Merchant site with a NemID Virksomhedssignatur (organization certificate/ VOCES).

The next sections list the steps you need to complete to be configured in the E-Ident service with NemID.

- First, you need to enter into an agreement about the PID/CPR service. This applies to all customers. See the section about PID/CPR-service.
- Secondly, you need to order test and production certificates. If you are not a NemID service provider, you will also need to enter into an agreement to be a service provider. The process of ordering test and production certificates are slightly different whether you are an existing service provider or a new. When continue reading, if you are already an existing NemID Service Provider, continue to read and follow the steps in the sections about PID/CPR-service and Existing NemID Service Provider. If you are a new NemID Service Provider, continue to read and follow the steps in the sections about PID/CPR-service and New NemID Service Provider.

PID/RID cpr-service

NemID offers a PID/RID²cpr-service that can match a user's PID/RID with a CPR number. The service is provided by the Agency for Digitisation. Access to the PID/CPR-service requires that Service Providers enter into an agreement with associated conditions for use of the service. The use of the service is free of charge, and all customers using the E-Ident service should enter into an agreement about the PID/RID cpr-service.

To get access to the PID/RID cpr-service, please go to and follow the steps:

- <http://www.nets.eu/dk-da/Produkter/Sikkerhed/NemID-tjenesteudbyder/supplerende-produkter/PID-RID-cpr-tjenester/Pages/default.aspx#tab3>

General information about the service can be found here:

- <http://www.nets.eu/dk-da/Produkter/Sikkerhed/NemID-tjenesteudbyder/supplerende-produkter/PID-RID-cpr-tjenester/Pages/default.aspx#tab1>

Existing NemID Service Provider

As an existing NemID Service Provider you need to order new certificates, both test- and production certificates, only for use in the E-Ident service. New certificates are required to ensure that the identification is coming through the E-Ident service.

Test company certificate (called test virksomhedscertifikat (test-VOCES))

Please follow the below steps to retrieve a test-VOCES:

1. Contact your administrator³ in relation to the existing NemID test environment and have the administrator issue a new test-VOCES. Please note the following when ordering the test certificate:
 - a. Add support.esecurity@nets.eu as the technical contact person. Nets eSecurity support will receive an e-mail with a link to download your certificate.
 - i. If you add yourself as technical contact, please forward the link you will receive in an e-mail to support.esecurity@nets.eu. **Please do not install the certificate from the link.**
 - b. When the test-VOCES is issued an installation code will be shown. Please note this code and e-mail it to sup-

² PID and RID is unique identifiers in respectively personal and employee certificates.

³ Information about your test administrator may be received from tusupport@danid.dk

port.esecurity@nets.eu.

2. In order to activate the test-VOCES, you have to apply for access to the test environment at: <http://www.nets.eu/dk-da/Service/kundeservice/nemid-tu/Pages/Adgang-til-testsystem.aspx>
 - a. The UID number of the test-VOCES can be found in the NemID Selfservice at: https://www.medarbejdersignatur.dk/produkter/nemid_medarbejdersignatur/log_paa_nemid_selvbetjening/log_paa_med_noeglefil/index.html, see "Øvrige signaturer", "Administrer Virksomhedssignatur". This can be done by a company administrator.
 - b. The Friendly name has to be different from any existing test-VOCES.
 - c. Choose access to the PID and/or RID services.
 - d. Add the IP-address of the pre-production environment of the E-Ident Service. These are: 91.102.24.1 and 91.102.24.115.
3. When the test-VOCES is activated, the technical contact will receive information by e-mail, regarding access to the test environment. If support.esecurity@nets.eu has been set as the technical contact in step 1 above, the e-mail will be sent directly to support. If not, please forward the e-mail with the access information to support.esecurity@nets.eu

Production Company Certificate (called Virksomhedscertifikat (production-VOCES)):

1. The production-VOCES shall be ordered by the company administrator in the NemID Selfservice at: https://www.medarbejdersignatur.dk/produkter/nemid_medarbejdersignatur/log_paa_nemid_selvbetjening/log_paa_med_noeglefil/index.html⁴. When ordering the certificate, please note the following:
 - a. Add support.esecurity@nets.eu as the technical contact person.
 - b. When the production-VOCES is issued, an installation code will be shown. Please note this code, and e-mail sup-

⁴ Pricing information for NemID production certificate for existing NemID Service providers is found here: <http://www.nets.eu/dk-da/Produkter/Sikkerhed/medarbejdersignatur/Pages/Priser-uden-Pro-pakken.aspx>

port.esecurity@nets.eu with a request for a mobile phone number to send the code to. When you receive the phone number, please send a SMS with the code and the name of your company.

2. In order to activate the production-VOCES, you have to apply for access to the production environment at: <http://www.nets.eu/dk-da/Service/kundeservice/nemid-tu/Pages/Adgang-til-produktionssystem.aspx>
 - a. The UID number can be found in the NemID Selfservice at: https://www.medarbejdersignatur.dk/produkter/nemid_medarbejdersignatur/log_paa_nemid_selvbetjening/log_paa_med_noeglefil/index.html, see "Øvrige signaturer", "Administrer Virksomhedssignatur". This can be done by a company administrator.
 - b. The Friendly name has to be different from any existing production-VOCES
 - c. Choose access to the PID and/or RID services.
3. When the production-VOCES is activated, you will receive information by e-mail, regarding access to the production environment. An e-mail containing the link to the production-VOCES, along with the access information to production environment shall be forwarded to Nets eSecurity support at support.esecurity@nets.eu.
4. You will receive a code to access the link from your NemID administrator. Please contact Nets eSecurity support at support.esecurity@nets.eu to receive a mobile phone number to send the code to.

After receiving both the test-VOCES and the production-VOCES, Nets eSecurity will download the certificates and add these to your Merchant configuration.

New NemID Service Provider

In order to use the E-Ident service and support NemID for signing, you need to order a test Company Certificate (called a test-VOCES), and a production Company Certificate (called a production-VOCES). In addition, you need to enter into a NemID Service Provider Agreement.

Production Company Certificate (called production-VOCES)

1. A production-VOCES shall be ordered by the company administrator⁵ in the NemID Selfservice at: https://www.medarbejdersignatur.dk/produkter/nemid_medarbejdersignatur/log_paa_nemid_selvbetjening/log_paa_med_noeglefil/in

⁵ If you are not aware of who your company administrator are, log on to the NemID self-service site with your MOCES certificate.

[dex.html](#)⁶ When ordering the production-VOCES, please note the following:

- a. Add support.esecurity@nets.eu as the technical contact person.
- b. When the production-VOCES is issued, an installation code will be shown. Please note this code, and e-mail support.esecurity@nets.eu with a request for a mobile phone number to send the code to. When you receive the phone number, please send a SMS with the code and the name of your company.

NemID Service Provider Agreement and test Company Certificate (called test-VOCES)

1. In order to become a NemID Service Provider you need to enter into a Service Provider Agreement with Nets DanID, so that both parties are aware of, and agree with, the conditions and obligations that apply for NemID.
 - a. Enter into the agreement at: <http://www.nets.eu/dk-da/Produkter/Sikkerhed/NemID-tjenesteudbyder/Pages/default.aspx#tab4>
2. While concluding the Service Provider Agreement, a test-VOCES is also issued as well as access to the test and production environments.
 - a. The UID number can be found in the NemID Selfservice at: https://www.medarbejdersignatur.dk/produkter/nemid_medarbejdersignatur/log_paa_nemid_selvbetjening/log_paa_med_noeglefil/index.html , see "Øvrige signaturer", "Administrer Virksomhedssignatur". This can be done by a company administrator.
 - b. Choose access to the PID and/or RID services.
3. Add the IP-addresses of the pre-production environment of the E-Ident Service. These are: 91.102.24.1 and 91.102.24.115. When the test-VOCES and the production-VOCES have access to the associated environment, you will receive information by e-mail, regarding access to the associated environments. Forward the e-mail(s) to support.esecurity@nets.eu. **Do not install the test- or production-VOCES certificates.**

After receiving the test- and production VOCES, Nets eSecurity will down-

⁶ Pricing information for new service providers: <http://www.nets.eu/dk-da/Produkter/Sikkerhed/medarbejdersignatur/Pages/Priser-uden-Pro-pakken.aspx>

load the certificates and add these to your Merchant configuration.

Test users

NemID test users can be ordered here:

- <https://applek.danid.dk/testtools/> (username=oces, password=nemid4all). Fill in a fictive CPR, standard address, zip and city. Check for POCES Qualified and Standard OTP Device.

More information can also be found in the document "Vejledning i brug af test tools":

- <http://www.nets.eu/dk-da/Service/kundeservice/nemid-tu/tjenesteudbyderpakkeJS/Pages/default.aspx>

NemID JS client and CSS styling

The NemID JS client can either be shown in a standard or in a limited mode. The standard mode includes administration possibilities for the user like activation possibility for new NemID users. The mode is controlled using a parameter called "nemid_clientmode". In E-Ident this is appended to the authentication request. The minimum recommended IFRAME sizes are:

- 200 x 250 (width x height)

CSS file adjustment

The NemID JS client must be styled with CSS to display properly. The default styling has CSS rule that set the proper sizes. If you override styling, your style sheet must be updated for the new NemID client. Styling can be overridden either by setting a style URL in the merchant configuration or by sending a style parameter when starting identification.

The default CSS styling sets width and height to 100%. The client will then expand to fill the container (iframe), regardless of the container size.

When overriding styling, the sample CSS below will produce the same effect as the default styling.

```
#nemid_index_html {
    height: 100%;
}

#nemid_iframe {
    width: 100%;
    height: 100%;
    min-width: 500px;
    min-height: 450px;
}
```


CPR input page

It is possible to retrieve the CPR (Danish social security number) of an end user through the identification process in E-Ident. To retrieve the CPR number, an optional page can be presented to the user after the log on process with NemID is completed. The default page looks like this:

Enter CPR for authentication:

Proceed

The page can be styled using CSS. See the HTML code in test for styling options.

The CPR the end user enters will be matched with the PID from the end user's certificate in the PID/CPR service from NemID. The usage of this functionality requires an agreement with NemID regarding this service. See information earlier in this chapter about the PID/CPR service. If the CPR matches the PID, the CPR is returned in the SAML assertion. If the matching fails, the user will get an error.
