
Fedict eID Applet

Developer's Guide

Integrating the eID Applet within your web applications.

Frank Cornelis

6 Jan 2010

Copyright © 2008-2010 Fedict

Abstract

This developer's guide serves as an entry point for integrating the eID Applet in your web applications. The target audience is web developers and web application architects.

1. Introduction	1
1.1. Mac OS X	2
1.2. Linux	2
2. eID Applet	3
3. eID Applet Service	4
3.1. eID Identification	6
3.2. eID Authentication	12
3.3. eID Signatures	17
3.4. eID Administration	18
3.5. eID Applet Kiosk Mode	19
3.6. Generic eID Applet Service settings	20
4. eID Applet Web Application Deployment	23
5. eID Applet Protocol	24
5.1. eID Applet Protocol Messages	24
A. eID Applet Developer's Guide License	33
B. eID Applet License	34
C. Revision history	34

1. Introduction

The Fedict eID Applet is a browser component that exposes the functionality of an eID card to your web applications. In [Figure 1, "eID Applet Screenshot"](#) you find a screen shot of the eID Applet.

Please insert your eID card...



Figure 1. eID Applet Screenshot

The main features of the eID Applet are:

- Easy to integrate within an existing web application.
- Security and privacy of the citizen is protected.
- Interactive eID card handling.
- Support of CCID secure pinpad readers.

The eID Applet uses Java applet technology. This minimized the client web browser requirements.



eID Applet Source Code

The eID Applet source code is available at [eID Applet Google Code](http://code.google.com/p/eid-applet/) [http://code.google.com/p/eid-applet/].



eID Applet Support

Best-effort support on the eID Applet is provided via the [eID Applet Google Group](http://groups.google.com/group/eid-applet) [http://groups.google.com/group/eid-applet] mailing list. Feel free to join in.

1.1. Mac OS X

Because Apple only supports the Java 6 runtime on their Mac OS X operating systems since Snow Leopard, the identification functionality will not work for Mac OS X 10.4 and 10.5.

The strategy is to no longer support operating systems, but to support a specific Java platform. For the eID Applet this is the Java 6 platform (for eID identification that is. eID authentication and eID signature creation can also run using a Java 1.5 JRE). We can only give advice on how to configure Java 6 on your operating system.

1.2. Linux

1.2.1. Fedora 9, 10, 11, 12

The Fedora operating system comes by default with the IcedTea JRE which is based on the OpenJDK. If the Firefox browser uses this JRE the eID Applet still has some difficulties to run.

Please download the official Sun Java 6 JRE and enable it in the Firefox browser. The Firefox plugins can be configured via symbolic links under: `/usr/lib/mozilla/plugins`. Remove the IcedTea JRE link via: `rm /usr/lib/mozilla/plugins/libjavaplugin.so`. Afterwards add a symbolic link to the Sun JRE plugin, which can be found under: `$JAVA_HOME/jre/plugin/i386/ns7/libjavaplugin_oji.so`. Check the installed plugins in Firefox by navigating to: `about:plugins`.

1.2.2. Ubuntu 9.04, 9.10

Under Linux Ubuntu you can install the Sun JRE 1.6 via the following command: `sudo apt-get install sun-java6-jdk sun-java6-plugin`

2. eID Applet

The eID Applet should be used within a web page as shown in the following example:

```
<script src="https://www.java.com/js/deployJava.js"></script>
<script>
  var attributes = {
    code : 'be.fedict.eid.applet.Applet.class',
    archive : 'eid-applet-package.jar',
    width : 400,
    height : 300
  };
  var parameters = {
    TargetPage : 'identity-result.jsp',
    AppletService : 'applet-service',
    BackgroundColor : '#ffffff'
  };
  var version = '1.6';
  deployJava.runApplet(attributes, parameters, version);
</script>
```

Notice that we are using the Deployment Toolkit to load the eID Applet. This avoids browser compatibility issues and features an automatic installation of the required Java browser plugin.

The web application in which the eID Applet is embedded should use SSL for securing the communication between the web browser and the web application server. The eID Applet will not proceed when it detects a non SSL browser session.

The eID Applet will also not proceed when it detects that it has insufficient privileges to do so. This implies that the eID Applet JAR has to be signed and trusted by the citizen. The eID Applet that ships with an officially released eID Applet SDK has been signed by Fedict. In case of a security breach with the eID Applet, Fedict can revoke the corresponding code signing certificate to guarantee maximal safety of the citizen.

The available eID Applet parameters are summarized in [Table 1, “eID Applet Parameters”](#).

Table 1. eID Applet Parameters

Parameter	Required	Description
TargetPage	required	Indicates the page to which the eID Applet navigates after performing the requested eID operation. For example: <code>result.jsp</code>
AppletService	required	Points to the eID Applet Service server-side component that will handle the communication between the eID Applet and the (servlet) web application container. For example: <code>applet-service</code>
BackgroundColor	optional	The background color that is used by the eID Applet user interface. The default background color is white. For example: <code>#ffffff</code>
ForegroundColor	optional	The foreground color that is used by the eID Applet user interface. The default foreground color is black. For example: <code>#000000</code>
Language	optional	The language that is used by the eID Applet user interface for internationalization of the status messages. If it is not provided, the eID Applet defaults to the JRE runtime locale settings. For example: <code>nl</code>
RemoveCardCallback	optional	When the eID Applet runs in kiosk mode, a web developer can use this parameter to set a Javascript callback. The callback function will be invoked on an eID card removal event.
MessageCallback	optional	Via this parameter a web developer can configure a Javascript callback. This callback function will be invoked everytime the eID Applet displays an info message.



Javascript

The eID Applet cannot be accessed from Javascript for cross-site scripting security reasons.

3. eID Applet Service

The eID Applet requires a server-side service component to communicate the identity or authentication data from the web browser to the server using a secure channel. We call this component the eID Applet Service. The eID Applet SDK comes with eID Applet Service servlet components to ease integration of the eID Applet within servlet container Java EE based web

applications. The eID Applet Service components require at least a servlet version 2.4 container and a JRE version 1.5. The eID Applet and eID Applet Service architecture has been depicted in [Figure 2, “eID Applet Architecture”](#).

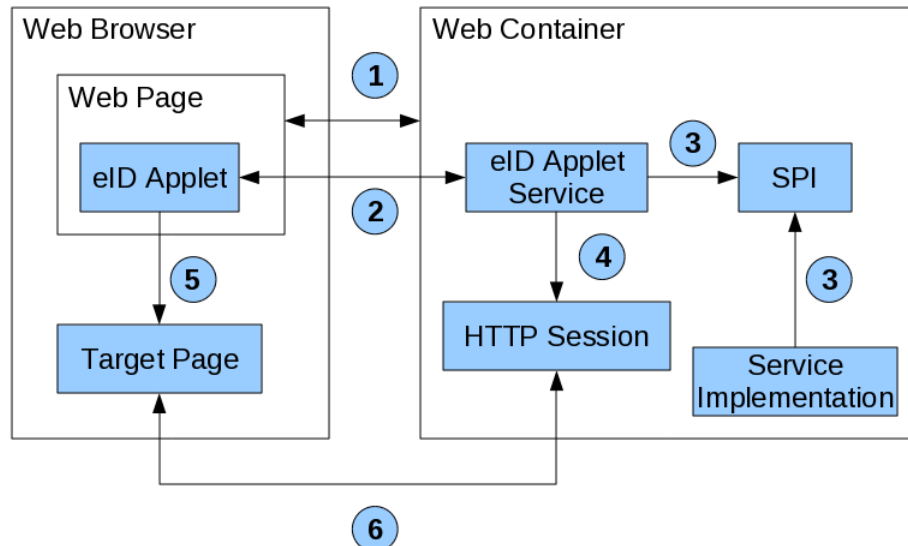


Figure 2. eID Applet Architecture

During the first step (1) the web browser loads the web page containing a reference to the eID Applet. The web browser continues by loading the eID Applet via the JRE web browser plugin. After the eID Applet has been loaded, it initiates a protocol run (2) with the server-side eID Applet Service. For some eID operations the web developer is required to configure service provider components. These service provider components are invoked (3) by the eID Applet Service during a protocol run. At the end of a protocol run (4) the eID Applet Service pushes some attributes into the HTTP session context of the web application container. Finally (5) the eID Applet makes the web browser to navigate to the target page. The target page can now access the eID identity items (6) made available by the eID Applet service.



eID Applet Service implementations

For the moment we only fully support Java EE servlet containers out of the box. At the same time this serves as the reference implementation. Depending on the success of the eID Applet SDK, we will also provide backends for other web application frameworks. We already have initial support for the ASP.NET web application environment and for the PHP environment.



eID Applet Service HTTP session

When using web frameworks like JBoss Seam you might stumble on conversation preservation issues because of the redirect executed by the

eID Applet at the end of the performed eID operation. When using a conversation scoped JBoss Seam managed bean, you can preserve the conversation across the eID Applet screen flow by adding the following HTTP parameter to the TargetPage applet parameter: `TargetPage : 'your-target-page.seam?conversationId=#{conversation.id}'`,

3.1. eID Identification

By default the eID Applet Service will operate the eID Applet to make it perform an eID identification. This is also known as data capture. Via this eID operation your web application is capable of reading out the identity data (i.e. name, first name, date of birth, ...) of the user his eID card.

The eID Applet Service Servlet can be configured via your `web.xml` web deployment descriptor as shown in the following example:

```
<servlet>
  <servlet-name>AppletServiceServlet</servlet-name>
  <servlet-class>be.fedict.eid.applet.service.AppletServiceServlet</servlet-class>
</servlet>
<servlet-mapping>
  <servlet-name>AppletServiceServlet</servlet-name>
  <url-pattern>/applet-service</url-pattern>
</servlet-mapping>
```



eID Applet Service dependencies

The eID Applet Service, which can be found in the `eid-applet-service-x.x.x.jar` artifact, has some 3rd party dependencies. These artifacts are located under the `lib/` directory inside the eID Applet SDK package. Depending on your Java EE runtime environment you should place these JAR files under the `META-INF/lib` directory of your web application.



eID Applet Service availability

One can always check for eID Applet Service availability by manually browsing to the location of the eID Applet Service servlet as configured in your `web.xml` Java EE web deployment descriptor.

After a successful identification took place, the `AppletServiceServlet` eID Applet Service will push at least the `eid.identity` attribute, which holds the parsed identity fields,

to the servlet container session. The `eid.identity` session attribute is of Java type `be.fedict.eid.applet.service.Identity`. More information on the exposed attributes can be found in the Javadoc API documentation of the eID Applet Service artifact.



eID Session Attributes

To ease integration of the eID Applet Service in web frameworks like JBoss Seam we have provided a top-level `eid` session attribute and getters on all exposed session attribute types. The top-level `eid` session attribute is of Java type `be.fedict.eid.applet.service.EIdData`. This means that the identity is available via both `eid.identity` session attribute and invocation of the `getIdentity()` method on the `eid` session attribute. This way we cover as much Java web frameworks as possible.

3.1.1. eID Address

During an eID identification operation the address on the eID card can be retrieved by setting the following `init-param` on the `AppletServiceServlet`:

```
<init-param>
  <param-name>IncludeAddress</param-name>
  <param-value>true</param-value>
</init-param>
```

After a successful eID identification, the eID address will be available via the `eid.address` session attribute within the servlet container session context. The `eid.address` session attribute is of Java type `be.fedict.eid.applet.service.Address`.

3.1.2. eID Photo

During an eID identification operation the citizen's photo on the eID card can be retrieved by setting the following `init-param` on the `AppletServiceServlet`:

```
<init-param>
  <param-name>IncludePhoto</param-name>
  <param-value>true</param-value>
</init-param>
```

After a successful eID identification, the photo will be available via the `eid.photo` session attribute within the servlet container session context. The eID photo is of Java type `byte[]` and in JPEG image format.

We provide a `PhotoServlet` to ease visualization of the eID photo within your web application. Configure the `PhotoServlet` as follows:

```
<servlet>
  <servlet-name>PhotoServlet</servlet-name>
  <servlet-class>be.fedict.eid.applet.service.PhotoServlet</servlet-class>
</servlet>
<servlet-mapping>
  <servlet-name>PhotoServlet</servlet-name>
  <url-pattern>/photo.jpg</url-pattern>
</servlet-mapping>
```

After a successful eID identification you can display the eID photo by putting next HTML tag in your web page:

```

```

3.1.3. eID Certificates

If you need to have explicit access to the eID citizen certificates, you can instruct the eID Applet to extract the certificates via the following eID Applet Service servlet configuration:

```
<init-param>
  <param-name>IncludeCertificates</param-name>
  <param-value>true</param-value>
</init-param>
```

After a successful eID identification, the certificates will be available as session attributes of Java type `java.security.cert.X509Certificate`. The authentication certificate will be available as `eid.certs.authn` session attribute. The non-repudiation (i.e. signature) certificate will be available as `eid.certs.sign` session attribute. The Citizen CA certificate will be available as `eid.certs.ca` session attribute. The Root CA certificate will be available as `eid.certs.root` session attribute.

3.1.4. Output to PDF

The eID Applet SDK comes with a servlet component that allows you to output the eID identity data to PDF. This can be useful if you want to print the eID identity data from within your web application pages. The PDF servlet can be configured as follows:


```

<servlet>
  <servlet-name>PdfServlet</servlet-name>
  <servlet-class>be.fedict.eid.applet.service.PdfServlet</servlet-class>
</servlet>
<servlet-mapping>
  <servlet-name>PdfServlet</servlet-name>
  <url-pattern>/identity.pdf</url-pattern>
</servlet-mapping>

```

After a successful eID identification, the PDF is available via:

```

<a href="identity.pdf" target="_blank">View as PDF</a>

```

3.1.5. Google Earth

The eID Applet Service also comes with a servlet for visualizing the eID identity data via Google Earth. *Figure 3, “eID Identity in Google Earth”* shows a screenshot of an eID identity visualized via Google Earth.

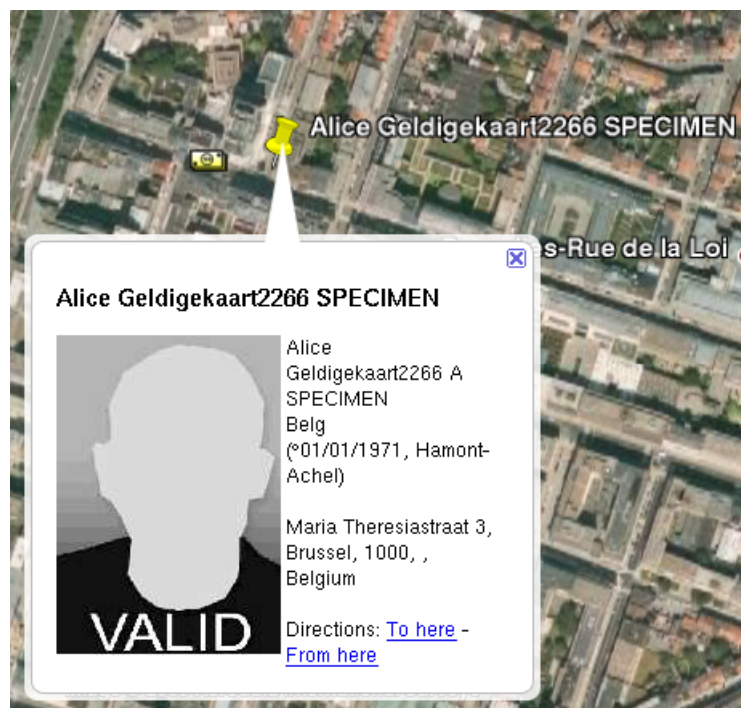


Figure 3. eID Identity in Google Earth

The servlet is configured as follows:

```
<servlet>
  <servlet-name>KmlServlet</servlet-name>
  <servlet-class>be.fedict.eid.applet.service.KmlServlet</servlet-class>
</servlet>
<servlet-mapping>
  <servlet-name>KmlServlet</servlet-name>
  <url-pattern>/identity.kmz</url-pattern>
</servlet-mapping>
```

After a successful eID identification, the Google Earth KMZ file is available via:

```
<a href="identity.kmz" target="_blank">View in Google Earth</a>
```

3.1.6. JSON

The eID Applet SDK comes with a servlet to support eID identity data retrieval inside your web application via JSON. The JSON servlet is configured as follows:

```
<servlet>
  <servlet-name>JSONServlet</servlet-name>
  <servlet-class>be.fedict.eid.applet.service.JSONServlet</servlet-class>
</servlet>
<servlet-mapping>
  <servlet-name>JSONServlet</servlet-name>
  <url-pattern>/identity.js</url-pattern>
</servlet-mapping>
```

The retrieved JSON data object has the following structure:

```
{
  identity: {
    name: "SPECIMEN",
    firstName: "Alice Geldigekaart",
    dateOfBirth: "Fri Jan 01 00:00:00 CET 1971",
    gender: "FEMALE"
  },
  address: {
    streetAndNumber: "Meirplaats 1 bus 1",
    municipality: "Antwerpen",
    zip: "2000"
  }
}
```

```
}
}
```

3.1.7. Identity Data Integrity

During an eID identification operation the eID Applet Service can perform integrity verification on the retrieved eID identity data. This feature prevents malicious parties to alter critical identity data.

To enable this functionality as part of an eID identification operation, you need to implement the `IdentityIntegrityService` interface. This service provider interface (SPI) can be found in the `eid-applet-service-spi` artifact. The corresponding service component (EJB3) session bean should be registered somewhere in JNDI. The JNDI location of this service component needs to be communicated to the eID Applet Service via the following `init-param` on the `AppletServiceServlet` :

```
<init-param>
  <param-name>IdentityIntegrityService</param-name>
  <param-value>your/location/in/jndi/IdentityIntegrityServiceBean</param-value>
</init-param>
```



Java EE Application Classpath

In an EJB Java EE application the `eid-applet-service-spi` artifact should be moved from your web application `WEB-INF/lib` WAR artifact to the EAR scoped classpath. Depending on your used Java EE application server it should be registered in `application.xml` as a Java module or moved to the `lib/` directory of your EAR to avoid classpath issues in your application server.



Java EE 6 Web Profile support

To support the coming Java EE 6 Web Profile we already foresee the usage of two types of service component lookups. The first one is JNDI based. This type of service lookup allows you to utilize EJB3 session beans as service provider interface implementation. The second type is via simple Java class name references. This type of service lookup is meant for lightweight servlet container environment. For example the `SignatureService` interface implementing component can be referred to via both `SignatureService` `init-param` and via `SignatureServiceClass` `init-param`. The `SignatureService` `init-param` will trigger a JNDI lookup of the signature service. The `SignatureServiceClass`

`init-param` will trigger a class instantiation using the default constructor of the given class.

The identity integrity service prevents malicious parties from altering the identity data. However, this does not prevent malicious parties to replace the identity data with that of another citizen. To prevent replacement of identity data, one can use a so called authenticated eID identification.

If the eID identification is preceded with an eID authentication then the eID Applet Service is able to link the authenticated national registry number with the one found in the eID identity file during identity integrity verification. This makes for a bullet-proof eID identification that cannot be forged.

For some applications that need eID identification of citizen B after eID authentication of citizen A, you might want to disable this feature. Do so via:

```
<init-param>
  <param-name>SkipNationalNumberCheck</param-name>
  <param-value>true</param-value>
</init-param>
```

3.1.8. Privacy Service

The application can define an identity data usage description by means of a privacy service component. To enable this functionality as part of an eID identification operation, you need to implement the `PrivacyService` interface. This service provider interface (SPI) can be found in the `eid-applet-service-spi` artifact. The corresponding service component (EJB3) session bean should be registered somewhere in JNDI. The JNDI location of this service component needs to be communicated to the eID Applet Service via the following `init-param` on the `AppletServiceServlet` :

```
<init-param>
  <param-name>PrivacyService</param-name>
  <param-value>your/location/in/jndi/PrivacyServiceBean</param-value>
</init-param>
```

3.2. eID Authentication

The eID Applet can be used to authenticate an end user via the eID card. eID based entity authentication is much safer than a simple password based authentication scheme since the eID card makes a two-factor authentication possible.



eID Applet Authentication Configuration

There are many different eID Applet configurations possible for eID Authentication. The optimal configuration highly depends on your web application requirements. In case of doubt contact us at the [eID Applet Google Group](http://groups.google.com/group/eid-applet) [http://groups.google.com/group/eid-applet] mailing list for additional advice.

To perform an eID authentication, you need to implement the `AuthenticationService` interface. This interface can be found as part of the `eid-applet-service-spi` artifact. This service component (EJB3) session bean should be registered somewhere in JNDI. The JNDI location of this service component needs to be set via the following `init-param` on the `AppletServiceServlet` :

```
<init-param>
  <param-name>AuthenticationService</param-name>
  <param-value>your/location/in/jndi/AuthenticationServiceBean</param-value>
</init-param>
```

After a successful authentication the `eid.identifier` session attribute will contain a unique identifier (the national registration number) for the user. The `eid.identifier` session attribute is of Java type `java.lang.String`. To respect the citizen's privacy, the national registration number should not be abuse for linking identity data. Profiling based on eID data linking is forbidden by law.



Mac OS X

Because not every version of Mac OS X supports the Java 6 runtime, we made the eID Applet to also operate on a Java 5 runtime for the basic eID authentication (and eID signature) operations.



Sun JRE

Because the eID Applet is using the `SunPKCS11` security provider we need the Sun JRE as browser applet runtime for eID authentication (and eID signature) via the eID Applet. These days the OpenJDK JRE also comes with an (almost working) `SunPKCS11` security provider.



eID Middleware

The eID Applet is using the PKCS#11 library for eID authentication (and eID signatures). This requires that the eID Middleware has been installed on the client system.

If no PKCS#11 library has been found and the applet browser runtime is Java 6, then the eID Applet will fallback to the Java 6 Smart Card I/O API to generate the authentication (or in case of eID signature the non-repudiation) digital signature via the direct PC/SC smart card interface.

By default the eID Applet will sign a sequence similar to (salt, challenge) using the authentication private key of the citizen's eID card. The challenge is send over SSL by the eID Applet Service. The salt value is produced by the eID Applet itself. The salt value prevents that the eID Applet is forced into signing a given server-side value. To prevent a certain type of man-in-the-middle attack we can make the eID Applet to sign a sequence similar to (salt, hostname, challenge) . This feature can be enabled by setting the following `init-param` on the `AppletServiceServlet` :

```
<init-param>
  <param-name>Hostname</param-name>
  <param-value>www.PutYourSiteHostnameHere.be</param-value>
</init-param>
```



Hostname verification

It is strongly advised to enable this hostname verification feature to reduce security vulnerability.

To prevent DNS attacks one can even make the eID Applet sign the IP address of the server. This feature can be enabled by setting the following `init-param` on the `AppletServiceServlet` :

```
<init-param>
  <param-name>InetAddress</param-name>
  <param-value>1.2.3.4</param-value>
</init-param>
```

If you enable both `Hostname` and `InetAddress` features at the same time, the eID Applet will be signing a sequence similar to (salt, hostname, IP address, challenge) . The hostname and IP address are the same as seen by the web browser.

3.2.1. Non-reversible Citizen Identifier

After a successful eID authentication took place, the `eid.identifier` session attribute will contain the national registry number. In some cases the national registry number cannot be used as is for unique user identifier. The eID Applet Service features Non-Reversible Citizen Identifiers (NRCID) to transform the national registry number into an application domain specific identifier. The NRCID is based on the HMAC-SHA1 of the National Registry Number, optionally appended with an application identifier and/or organization identifier. This feature can be enabled by setting the following `init-param` on the `AppletServiceServlet` :

```
<init-param>
  <param-name>NRCIDSecret</param-name>
  <param-value>place-your-application-secret-here</param-value>
</init-param>
```

The secret should be hexadecimal encoded and at least 128 bits (16 bytes) long. Thus the hexadecimal encoded secret should be at least 32 characters long.

The optional application identifier and organization identifier can be specified via the `NRCIDAppId` and `NRCIDOrgId` init parameters.

3.2.2. Secure Channel Binding

Tunneled entity authentication protocols like the one implemented by the eID Applet are subject to man-in-the-middle attacks without proper secure channel binding put in place. Cryptographic end-point channel binding has been implemented by means of digesting the TLS server certificate as part of the authentication signature. This option can be activated via the following `init-param` on the `AppletServiceServlet` :

```
<init-param>
  <param-name>ChannelBindingServerCertificate</param-name>
  <param-value>/path/to/your/server/certificate.der</param-value>
</init-param>
```

The server certificate should be in DER encoded format or in PEM format.



Server Certificate Channel Binding

It is strongly advised to activate server certificate cryptographic channel binding to have equivalent security properties compared to mutual TLS entity authentication.

Besides server certificate channel binding the eID Applet also supports unique channel binding using the TLS session identifier. This option can be activated via the following `init-param` on the `AppletServiceServlet` :

```
<init-param>
  <param-name>SessionIdChannelBinding</param-name>
  <param-value>true</param-value>
</init-param>
```

This will make the authentication signature to also digest the TLS session identifier.



Channel Binding

Secure channel binding based on unique channel binding using the TLS session identifier alone is not enough! Always use at least server certificate cryptographic channel binding. You can combine this with (unsecure) unique channel binding using the TLS session identifier if appropriate.

3.2.3. Explicit PIN entry

The eID card offers caching of the PIN authorization when creating an authentication signature. Some applications might require a PIN entry upon each authentication request. This can be achieved by performing an eID card logoff right before the creation of the authentication signature. Activate this feature via the following `init-param` on the `AppletServiceServlet` :

```
<init-param>
  <param-name>PreLogoff</param-name>
  <param-value>true</param-value>
</init-param>
```

3.2.4. Authenticated Identification

It is possible to combine an eID authentication operation with an eID identification operation. Activate the eID identification as part of the eID authentication via the following `init-param` on the `AppletServiceServlet` :

```
<init-param>
  <param-name>IncludeIdentity</param-name>
  <param-value>true</param-value>
</init-param>
```


Also include the eID address via the following `init-param` on the `AppletServiceServlet` :

```
<init-param>
  <param-name>IncludeAddress</param-name>
  <param-value>true</param-value>
</init-param>
```

Also include the eID photo via the following `init-param` on the `AppletServiceServlet` :

```
<init-param>
  <param-name>IncludePhoto</param-name>
  <param-value>true</param-value>
</init-param>
```

The identity integrity service can also be activated when combining eID authentication with eID identification.

3.3. eID Signatures

The eID Applet can also be used to create digital signatures using the non-repudiation eID certificate. The supported signature algorithms are SHA1-RSA-PKCS1 , SHA224-RSA-PKCS1 , SHA256-RSA-PKCS1 , SHA384-RSA-PKCS1 , SHA512-RSA-PKCS1 , RIPEMD128-RSA-PKCS1 , RIPEMD160-RSA-PKCS1 , and RIPEMD256-RSA-PKCS1 .



Legally Binding eID Digital Signatures

Please be aware that the eID digital signatures are legally binding by law. Don't make the citizen sign digital documents unless it is absolutely necessary from a legal point of view for the correct functioning of your business work flow.

To use this functionality you need to implement the `SignatureService` interface. This interface can be found in the `eid-applet-service-spi` artifact. This service component (EJB3) session bean should be registered somewhere in JNDI. The JNDI location of this service component needs to be set via the following `init-param` on the `AppletServiceServlet` :

```
<init-param>
  <param-name>SignatureService</param-name>
  <param-value>your/location/in/jndi/SignatureServiceBean</param-value>
</init-param>
```

The eID Applet Service can be configured to perform two basic types of digital signatures:

- The digest value to be signed originates solely from the `SignatureService` implementing service component.
- The eID Applet first sends over a set of digest values calculated from local files. These files are selected by the citizen via an eID Applet file user interface. Out of this set of digest values the `SignatureService` implementing service component then calculates a super digest value. This digest value is signed using the eID Applet.

The supported file digest algorithms are SHA-1 , SHA-256 , SHA-384 , and SHA-512 .

This type of digital signature operation can be used to construct for example XML Signatures, XAdES Signatures or PDF Signatures.

The type of digital signature created by the eID Applet is completely determined by the implementation of the `SignatureService` SPI. We provide several base implementation of the `SignatureService` SPI as part of the `eid-applet-service-signer` artifact. The most important signature service implementations provided by the eID Applet SDK are:

- ODF 1.2 signatures (supported by OpenOffice.org 3.1)
- Office OpenXML (supported by Microsoft Office 2007)



PKI Validation

The eID Applet Service does not perform any PKI validation. So the signature service component, authentication service component and the identity integrity component need to implement PKI validation of the citizen certificates itself. PKI validation is out of scope of the provided eID Applet Service.

A PKI validation module tailored for the Belgian eID PKI is available at the [jTrust Google Code](http://code.google.com/p/jtrust/) [http://code.google.com/p/jtrust/] site.

3.4. eID Administration

The eID Applet allows for some administrative eID tasks like changing the PIN and unblocking the PIN. This feature has been implemented to break the hard dependency on the eID Middleware.

The eID PIN change administrative task can be executed by setting the following `init-param` on the `AppletServiceServlet` :

```
<init-param>
  <param-name>ChangePin</param-name>
  <param-value>true</param-value>
```

```
</init-param>
```

The eID unblock PIN administrative task can be executed by setting the following `init-param` on the `AppletServiceServlet` :

```
<init-param>
  <param-name>UnblockPin</param-name>
  <param-value>true</param-value>
</init-param>
```

3.5. eID Applet Kiosk Mode

Some web applications require explicit management of the (authenticated) user session. For this type of web applications we have foreseen a so-called Kiosk Mode. In this mode the eID Applet will notify the web application in case the eID card has been removed from the smart card reader. The web developer can use this notification to trigger for example a session cleanup at the server-side.

The eID Applet Kiosk Mode can be activated by setting the following `init-param` on the `AppletServiceServlet` :

```
<init-param>
  <param-name>Kiosk</param-name>
  <param-value>true</param-value>
</init-param>
```

The web developer can install the notification callback as follows inside a web page:

```
<script src="https://www.java.com/js/deployJava.js"></script>
<script>
  var attributes = {
    code : 'be.fedict.eid.applet.Applet.class',
    archive : 'eid-applet-package.jar',
    width : 1,
    height : 1,
    mayscript : 'true'
  };
  var parameters = {
    AppletService : 'applet-kiosk-service',
    RemoveCardCallback : 'removeCardCallback'
  };
  var version = '1.5';
```

```
    deployJava.runApplet(attributes, parameters, version);
</script>
<script>
    function removeCardCallback() {
        alert('eID card removal has been detected by the web page.');
```

As you can see the web developer can install a Javascript callback function by setting the `RemoveCardCallback` eID Applet parameter. In our example we simply display a Javascript pop-up. Of course more complex operations are possible here. One might imagine a use case where the callback method invokes a server-side component via AJAX.



mayscript

Don't forget the `mayscript: 'true'` attribute, else the eID Applet will not be able to invoke Javascripts inside the browser window.

3.6. Generic eID Applet Service settings

The settings listed in this section apply to eID identification operations, eID authentication operations, eID signature operations, and eID administration operations.

3.6.1. Secure Client Environment

The eID Applet offers functionality to check whether the client environment is secure enough given the application requirements. In case the eID Applet Service detects an insecure client environment the eID Applet can:

- show an error message and abort the requested eID operation.
- show a warning message and ask the citizen whether he/she wants to continue or not.

To activate this functionality you need to implement the `SecureClientEnvironmentService` interface. This interface can be found in the `eid-applet-service-spi` artifact. This service component (EJB3) session bean should be registered somewhere in JNDI. The JNDI location of this service component needs to be set via the following `init-param` on the `AppletServiceServlet` :

```
<init-param>
  <param-name>SecureClientEnvironmentService</param-name>
  <param-value>your/location/in/jndi/SecureClientEnvironmentServiceBean</param-value>
</init-param>
```

Additional client environment information can be pushed to the eID Applet Service by adding the following eID Applet parameters within your web page eID Applet configuration:

```
NavigatorUserAgent : navigator.userAgent,
NavigatorAppName : navigator.appName,
NavigatorAppVersion : navigator.appVersion
```



Java 6

This eID Applet feature requires a Java 6 browser runtime or an installed eID Middleware PKCS#11 library.

3.6.2. eID Card Removal

The eID Applet can ask the citizen for eID card removal after performing the selected eID operation. This option can be used to limit the window of opportunity for malware to abuse the eID card.

The eID card removal can be activated by setting the following `init-param` on the `AppletServiceServlet` :

```
<init-param>
  <param-name>RemoveCard</param-name>
  <param-value>true</param-value>
</init-param>
```

3.6.3. eID Card Logoff

After an eID authentication, eID signature, or eID administration task (i.e. PIN change) the eID card will re-use the PIN authorization for future eID authentication operations. This feature was originally implemented on the eID JavaCard Applet (which is located inside the eID chip) to allow for mutual authenticated SSL without the need to re-enter the PIN on each SSL session renewal. Although this makes sense in the context of SSL, it actually makes for a serious eID security weakness: SSO should be handled at the IdP level, not at the card level. Only an IdP can have notion of trust domains between different web applications. Luckily the eID card foresees in an eID card logoff. This eID logoff feature can be enabled during both eID authentication or eID signature operations by setting the following `init-param` on the `AppletServiceServlet` :

```
<init-param>
  <param-name>Logoff</param-name>
  <param-value>true</param-value>
```

```
</init-param>
```

This feature requires a Java 6 browser runtime as it is using the Smart Card I/O API. If no Java 6 runtime is available this feature will default to an eID card removal as this yields the same result.



Enable eID card logoff

It is strongly advised to enable the eID card logoff feature to prevent abuse of the authentication functionality of the eID card.

3.6.4. Auditing

To comply with certain regulations one might need to have an audit trace of the activities performed on the eID Applet Service by clients. The eID Applet Service offers auditing support by means of the SPI design pattern.

To activate the audit functionality you need to implement the `AuditService` interface. This interface can be found in the `eid-applet-service-spi` artifact. This service component (EJB3) session bean should be registered somewhere in JNDI. The JNDI location of this service component needs to be set via the following `init-param` on the `AppletServiceServlet` :

```
<init-param>
  <param-name>AuditService</param-name>
  <param-value>your/location/in/jndi/AuditServiceBean</param-value>
</init-param>
```

3.6.5. Alternative UI

The eID Applet offers its own user interface for interactive handling of eID card events. As some web application technologies (like Flex) like to construct their own user interface we created a Javascript based callback mechanism so that these web technologies can visualize the info messages themselves.

The web developer can install the info message callback inside a web page as follows:

```
<script src="https://www.java.com/js/deployJava.js"></script>
<script>
  var attributes = {
    code : 'be.fedict.eid.applet.Applet.class',
    archive : 'eid-applet-package.jar',
    width : 1,
    height : 1,
```

```

    mayscript : 'true'
  };
  var parameters = {
    AppletService : 'applet-service',
    MessageCallback : 'messageCallback'
  };
  var version = '1.6';
  deployJava.runApplet(attributes, parameters, version);
</script>
<script>
  function messageCallback(status, message) {
    document.getElementById('appletMessage').innerHTML = '<b>' + status + ': ' + message
    + '</b>';
  }
</script>
<div id="appletMessage">Message placeholder</div>

```

As you can see the web developer can install a Javascript callback function by setting the `MessageCallback` eID Applet parameter. The `status` parameter can be either `NORMAL` or `ERROR`. In our example we simply display the incoming message via some dynamic HTML. Of course more complex visualizations are possible here.



mayscript

Don't forget the `mayscript: 'true'` attribute, else the eID Applet will not be able to invoke Javascripts inside the browser window.

4. eID Applet Web Application Deployment

You can deploy your eID Applet enabled web application over a lot of different network topologies, depending on the setup of your infrastructure. The easiest configuration is a setup where you terminate the SSL on the Application Server itself. Another option is to use an AJP proxy. An example of how to configure the Apache HTTPD AJP proxy is given below:

```

LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
ProxyPass /eid-applet-test/ ajp://localhost:8009/eid-applet-test/
ProxyPass /eid-applet-beta/ ajp://localhost:8009/eid-applet-beta/

```

This AJP proxy can then terminate the SSL without the Application Service noticing this.

Some configuration use non-AJP aware reverse proxies. An example on how to configure the Apache HTTPD as a reverse proxy is given below:

ProxyRequests Off

```
<Proxy *>
    Order deny,allow
    Allow from all
</Proxy>

<Location /eid-applet-test/>
    ProxyPass http://localhost:8080/eid-applet-test/
    ProxyPassReverse http://localhost:8080/eid-applet-test/
</Location>
```

Because the Application Server no longer receives the SSL information as provided by the AJP protocol, the eID Applet Service can no longer detect whether it's using a secure connection or not. The eID Applet Service can be configured to skip the secure connection check using the following `init-param` on the `AppletServiceServlet` :

```
<init-param>
  <param-name>SkipSecureConnectionCheck</param-name>
  <param-value>true</param-value>
</init-param>
```

Further it is important to have a servlet container session cookie without the `HttpOnly` flag set. Else the eID Applet Service will push the eID identity credentials in the wrong Application Server HTTP session.

5. eID Applet Protocol

In this section we will elaborate on the eID Applet protocol used in the communication between the eID Applet and the eID Applet Service. If you use the eID Applet Service servlet implementation that comes with the eID Applet SDK you actually don't need to know the details of the eID Applet protocol. However, this information can be useful for web application developers that use other web frameworks than a Java EE servlet container based framework.

The eID Applet Protocol is based on the HTTP protocol using the POST method. Parameters are passed as HTTP headers and for binary data the HTTP body is used. The messages should be transported over a secure SSL connection.

5.1. eID Applet Protocol Messages

The following documentation has been generated automatically.

5.1.1. HelloMessage

This message starts a communication session between eID Applet and eID Applet Service. It sets the protocol state to: INIT

Table 2. HelloMessage HTTP headers

Header name	Required	Value
X-AppletProtocol-Type	true	HelloMessage
X-AppletProtocol-Language	false	Some String value.
X-AppletProtocol-Version	true	1

Allowed eID Applet Service response messages are: [Section 5.1.9, “IdentificationRequestMessage”](#) [Section 5.1.10, “CheckClientMessage”](#) [Section 5.1.12, “AuthenticationRequestMessage”](#) [Section 5.1.13, “AdministrationMessage”](#) [Section 5.1.14, “SignRequestMessage”](#) [Section 5.1.15, “FilesDigestRequestMessage”](#) [Section 5.1.16, “KioskMessage”](#) [Section 5.1.17, “SignCertificatesRequestMessage”](#)

5.1.2. ClientEnvironmentMessage

This message is only accepted if the eID Applet Service protocol state is: ENV_CHECK

Table 3. ClientEnvironmentMessage HTTP headers

Header name	Required	Value
X-AppletProtocol-Type	true	ClientEnvironmentMessage
X-AppletProtocol-JavaVersion	true	Some String value.
X-AppletProtocol-JavaVendor	true	Some String value.
X-AppletProtocol-OSName	true	Some String value.
X-AppletProtocol-OSArch	true	Some String value.
X-AppletProtocol-OSVersion	true	Some String value.
X-AppletProtocol-NavigatorUserAgent	false	Some String value.
X-AppletProtocol-NavigatorAppName	false	Some String value.
X-AppletProtocol-NavigatorAppVersion	false	Some String value.
X-AppletProtocol-Version	true	1

HTTP body should contain the data.

Body content: A list of strings containing the names of the smart card readers.

Allowed eID Applet Service response messages are: [Section 5.1.9, “IdentificationRequestMessage”](#) [Section 5.1.11, “InsecureClientMessage”](#) [Section 5.1.12, “AuthenticationRequestMessage”](#) [Section 5.1.13, “AdministrationMessage”](#) [Section 5.1.14, “SignRequestMessage”](#) [Section 5.1.15, “FilesDigestRequestMessage”](#) [Section 5.1.17, “SignCertificatesRequestMessage”](#)

5.1.3. AuthenticationDataMessage

This message is only accepted if the eID Applet Service protocol state is: AUTHENTICATE

Table 4. AuthenticationDataMessage HTTP headers

Header name	Required	Value
X-AppletProtocol-Type	true	AuthenticationDataMessage
X-AppletProtocol-SignatureValueSize	true	Some Integer value.
X-AppletProtocol-SaltValueSize	true	Some Integer value.
X-AppletProtocol-SessionIdSize	false	Some Integer value.
X-AppletProtocol-AuthnCertFileSize	true	Some Integer value.
X-AppletProtocol-CaCertFileSize	true	Some Integer value.
X-AppletProtocol-RootCaCertFileSize	true	Some Integer value.
X-AppletProtocol-IdentityFileSize	false	Some Integer value.
X-AppletProtocol-AddressFileSize	false	Some Integer value.
X-AppletProtocol-PhotoFileSize	false	Some Integer value.
X-AppletProtocol-IdentitySignatureFileSize	false	Some Integer value.
X-AppletProtocol-AddressSignatureFileSize	false	Some Integer value.
X-AppletProtocol-NationalRegistryCertFileSize	false	Some Integer value.
X-AppletProtocol-Version	true	1

HTTP body should contain the data.

Body content: Contains concatenation of salt value, optional session id, signature value, and authn cert chain.

Allowed eID Applet Service response messages are: [Section 5.1.18, “FinishedMessage”](#)

5.1.4. SignatureDataMessage

This message is only accepted if the eID Applet Service protocol state is: SIGN

Table 5. SignatureDataMessage HTTP headers

Header name	Required	Value
X-AppletProtocol-Type	true	SignatureDataMessage
X-AppletProtocol-SignatureValueSize	true	Some Integer value.
X-AppletProtocol-SignCertFileSize	false	Some Integer value.
X-AppletProtocol-CaCertFileSize	false	Some Integer value.
X-AppletProtocol-RootCaCertFileSize	false	Some Integer value.
X-AppletProtocol-Version	true	1

HTTP body should contain the data.

Body content: Contains concatenation of signature value and sign cert chain.

Allowed eID Applet Service response messages are: [Section 5.1.18, “FinishedMessage”](#)

5.1.5. FileDigestsDataMessage

This message is only accepted if the eID Applet Service protocol state is: DIGEST

Table 6. FileDigestsDataMessage HTTP headers

Header name	Required	Value
X-AppletProtocol-Type	true	FileDigestsDataMessage
X-AppletProtocol-Version	true	1

HTTP body should contain the data.

Body content: List of string triples containing (digest algo, digest value in hex, description)

Allowed eID Applet Service response messages are: [Section 5.1.14, “SignRequestMessage”](#)

5.1.6. ContinueInsecureMessage

This message is only accepted if the eID Applet Service protocol state is: INSECURE

Table 7. ContinueInsecureMessage HTTP headers

Header name	Required	Value
X-AppletProtocol-Type	true	ContinueInsecureMessage
X-AppletProtocol-Version	true	1

Allowed eID Applet Service response messages are: [Section 5.1.9, “IdentificationRequestMessage”](#) [Section 5.1.12, “AuthenticationRequestMessage”](#) [Section 5.1.13, “AdministrationMessage”](#) [Section 5.1.14, “SignRequestMessage”](#) [Section 5.1.15, “FilesDigestRequestMessage”](#)

5.1.7. SignCertificatesDataMessage

This message is only accepted if the eID Applet Service protocol state is: SIGN_CERTS

Table 8. SignCertificatesDataMessage HTTP headers

Header name	Required	Value
X-AppletProtocol-Type	true	SignCertificatesDataMessage
X-AppletProtocol-SignCertFileSize	false	Some Integer value.
X-AppletProtocol-CaCertFileSize	false	Some Integer value.
X-AppletProtocol-RootCaCertFileSize	false	Some Integer value.
X-AppletProtocol-Version	true	1

HTTP body should contain the data.

Body content: The non-repudiation certificate chain.

Allowed eID Applet Service response messages are: [Section 5.1.14, “SignRequestMessage”](#)

5.1.8. IdentityDataMessage

This message is only accepted if the eID Applet Service protocol state is: IDENTIFY

Table 9. IdentityDataMessage HTTP headers

Header name	Required	Value
X-AppletProtocol-Type	true	IdentityDataMessage
X-AppletProtocol-IdentityFileSize	true	Some Integer value.
X-AppletProtocol-AddressFileSize	false	Some Integer value.

Header name	Required	Value
X-AppletProtocol-PhotoFileSize	false	Some Integer value.
X-AppletProtocol-IdentitySignatureFileSize	false	Some Integer value.
X-AppletProtocol-AddressSignatureFileSize	false	Some Integer value.
X-AppletProtocol-RrnCertFileSize	false	Some Integer value.
X-AppletProtocol-RootCertFileSize	false	Some Integer value.
X-AppletProtocol-AuthnCertFileSize	false	Some Integer value.
X-AppletProtocol-SignCertFileSize	false	Some Integer value.
X-AppletProtocol-CaCertFileSize	false	Some Integer value.
X-AppletProtocol-Version	true	1

HTTP body should contain the data.

Body content: Concatenation of identity file, optional address file, optional photo file, optional identity signature file, optional address signature file, and optional national registry certificate and root certificate.

Allowed eID Applet Service response messages are: [Section 5.1.18, “FinishedMessage”](#)

5.1.9. IdentificationRequestMessage

Table 10. IdentificationRequestMessage HTTP headers

Header name	Required	Value
X-AppletProtocol-Type	true	IdentificationRequestMessage
X-AppletProtocol-IncludeAddress	false	Some boolean value.
X-AppletProtocol-IncludePhoto	false	Some boolean value.
X-AppletProtocol-IncludeIntegrityData	false	Some boolean value.
X-AppletProtocol-RemoveCard	false	Some boolean value.
X-AppletProtocol-IncludeCertificates	false	Some boolean value.

Header name	Required	Value
X-AppletProtocol-IdentityDataUsage	false	Some String value.
X-AppletProtocol-Version	true	1

This message will perform an eID Applet protocol state transition to: IDENTIFY

5.1.10. CheckClientMessage

Table 11. CheckClientMessage HTTP headers

Header name	Required	Value
X-AppletProtocol-Type	true	CheckClientMessage
X-AppletProtocol-Version	true	1

This message will perform an eID Applet protocol state transition to: ENV_CHECK

5.1.11. InsecureClientMessage

Table 12. InsecureClientMessage HTTP headers

Header name	Required	Value
X-AppletProtocol-Type	true	InsecureClientMessage
X-AppletProtocol-WarnOnly	false	Some boolean value.
X-AppletProtocol-Version	true	1

This message will perform an eID Applet protocol state transition to: INSECURE

5.1.12. AuthenticationRequestMessage

Table 13. AuthenticationRequestMessage HTTP headers

Header name	Required	Value
X-AppletProtocol-Type	true	AuthenticationRequestMessage
X-AppletProtocol-RemoveCard	false	Some boolean value.
X-AppletProtocol-IncludeHostname	false	Some boolean value.
X-AppletProtocol-IncludeInetAddress	false	Some boolean value.
X-AppletProtocol-Logoff	false	Some boolean value.
X-AppletProtocol-PreLogoff	false	Some boolean value.
X-AppletProtocol-SessionIdChannelBinding	false	Some boolean value.

Header name	Required	Value
X-AppletProtocol-ServerCertificateChannelBinding	false	Some boolean value.
X-AppletProtocol-IncludeIdentity	false	Some boolean value.
X-AppletProtocol-IncludeAddress	false	Some boolean value.
X-AppletProtocol-IncludePhoto	false	Some boolean value.
X-AppletProtocol-IncludeIntegrityData	false	Some boolean value.
X-AppletProtocol-Version	true	1

HTTP body should contain the data.

Body content: The challenge to be signed using the authentication certificate. If IncludeHostname is set, then prefix the challenge with the server hostname before signing.

This message will perform an eID Applet protocol state transition to: AUTHENTICATE

5.1.13. AdministrationMessage

This message stops a communication session between eID Applet and the eID Applet Service.

Table 14. AdministrationMessage HTTP headers

Header name	Required	Value
X-AppletProtocol-Type	true	AdministrationMessage
X-AppletProtocol-ChangePin	false	Some boolean value.
X-AppletProtocol-UnblockPin	false	Some boolean value.
X-AppletProtocol-RemoveCard	false	Some boolean value.
X-AppletProtocol-Logoff	false	Some boolean value.
X-AppletProtocol-Version	true	1

5.1.14. SignRequestMessage

Table 15. SignRequestMessage HTTP headers

Header name	Required	Value
X-AppletProtocol-Type	true	SignRequestMessage
X-AppletProtocol-DigestAlgo	true	Some String value.
X-AppletProtocol-Description	false	Some String value.
X-AppletProtocol-RemoveCard	false	Some boolean value.

Header name	Required	Value
X-AppletProtocol-Logoff	false	Some boolean value.
X-AppletProtocol-Version	true	1

HTTP body should contain the data.

Body content: The digest value to be signed using the non-repudiation certificate

This message will perform an eID Applet protocol state transition to: SIGN

5.1.15. FilesDigestRequestMessage

Table 16. FilesDigestRequestMessage HTTP headers

Header name	Required	Value
X-AppletProtocol-Type	true	FilesDigestRequestMessage
X-AppletProtocol-DigestAlgo	true	Some String value.
X-AppletProtocol-Version	true	1

This message will perform an eID Applet protocol state transition to: DIGEST

5.1.16. KioskMessage

This message stops a communication session between eID Applet and the eID Applet Service.

Table 17. KioskMessage HTTP headers

Header name	Required	Value
X-AppletProtocol-Type	true	KioskMessage
X-AppletProtocol-Version	true	1

5.1.17. SignCertificatesRequestMessage

Table 18. SignCertificatesRequestMessage HTTP headers

Header name	Required	Value
X-AppletProtocol-Type	true	SignCertificatesRequestMessage
X-AppletProtocol-Version	true	1

This message will perform an eID Applet protocol state transition to: SIGN_CERTS

5.1.18. FinishedMessage

This message stops a communication session between eID Applet and the eID Applet Service.

Table 19. FinishedMessage HTTP headers

Header name	Required	Value
X-AppletProtocol-Type	true	FinishedMessage
X-AppletProtocol-Version	true	1

A. eID Applet Developer's Guide License



This document has been released under the Creative Commons license.



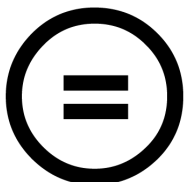
You are free to Share — to copy, distribute and transmit the work.



You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).



You may not use this work for commercial purposes.



You may not alter, transform, or build upon this work.

More information about the Creative Commons license conditions can be found at [Creative Commons organization](http://creativecommons.org/) [http://creativecommons.org/].

B. eID Applet License

The eID Applet source code has been released under the GNU LGPL version 3.0.

This is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License version 3.0 as published by the Free Software Foundation. This software is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details. You should have received a copy of the GNU Lesser General Public License along with this software; if not, see <http://www.gnu.org/licenses/>.

C. Revision history

Table C.1. Revision history

Date	Author	Description
26 Jan 2009	Frank Cornelis	Initial version.
22 Apr 2009	Frank Cornelis	1.0.0-beta-1
29 May 2009	Frank Cornelis	1.0.0-beta-2
24 Jul 2009	Frank Cornelis	1.0.0-beta-3
18 Sep 2009	Frank Cornelis	1.0.0-beta-4
22 Nov 2009	Frank Cornelis	1.0.0-rc-1
16 Dec 2009	Frank Cornelis	1.0.0-rc-2
6 Jan 2010	Frank Cornelis	1.0.0-rc-3