Talgildur samleiki

Undirskjal 6 – Kort ID

APRIL 2016

TALGILDU FØROYAR
01100110 01101111

KortID loysn úr ESTLANDI OG ÍSLANDI

Introduction

In the following sections the the card id solution used in Estonia and Iceland is described. The solution uses a smartcard to establish the identity of a person. The solution is part of a public-key infrastructure (PKI) and therefore requires the components in a PKI to be available. A general overview of PKI is found elsewhere.

The description of the Icelandic card id is very high-level whereas the description of the Estonia solution is more thorough. The reason is that more time has been allocated to the Estonian solution and that the Icelandic solution is more complex in the sense it supports cards from multiple vendors and that it is already know evident that the Icelandic solution will not be chosen due to its complexity and support burden.

Estonian Card ID solution

In Estonia a Card ID solution has been in operation since 2002. The Swiss company Trüb, now a part of Gemalto, has been providing the cards. The card id solution that the Faroese Government is considering is the one used in Estonia. One of the main reasons for considering this solution is that it is a proven technology and very widely used in Estonia. Other countries have also based their national identity card on technologies form Trüb. The solution uses two pins – one for authentication and one for signing.

Icelandic Card ID solution

The Icelandic Card ID solution is from 2008. The icelandic banks own the the Icelandic CA (Auðkenni). Certificates were issues on bank cards and the banks themselves determine what type of cards they procure. The Icelandic solution relies on driver software and browser plug-in from Nexus. The software supports multiple card vendors, but as always, not everything works equally well together. As as result, the support burden of the Icelandic card solutions has been substantial. The solution uses the same pin for authentication and signing.

Adoption among Icelandic persons has been modest, but the card is a popular solution in the work-place.

Technical overview of the Estonian card id solution

Card and drivers

SmartCard

The information in this section is mainly derived from (Trüb Baltic AS, 2013).

Smart cards are special kind of chip card that contain a microprocessor and non-volatile memory. Smart cards support cryptographic operations such as genereating private/public key pairs. It is not possible to extract a private key from a smart card – only operations that use the private key are available for use.

There a number of different vendors that produce smart cards and their microprocessor platforms. In order to shield some of the differences between the smart card vendors and provide portability, Trüb has selected smart cards that support Java Card Platform. Trüb has produced a Java applet that interacts with the smart card's microprocessor to perform PKI related functions such as cryptographic operations.

Smart Cards contain a number of data objects. Below is an overview of the data objects on the card.

Table 1-1 The functions of EstEID security chip objects in the card application

Object	Function description
PIN1	The authorisation of the cardholder: 1) for getting access to the authentication key procedures. 2) for the execution of the following operations: a) the generation of new key pairs b) the loading of certificates
PIN2	For getting access to signature key.
PUK	The unblocking of PIN codes when they have been blocked after number of allowed consecutive incorrect entries.
Authentication certificate	The certificate for cardholder identification.
Signature certificate	The certificate calculating and checking the cardholder's electronic signature.
Authentication key pair (x2)	▪ Key pair that is actively used for cardholder authentication procedures. ▪ Optional idle key pair for a potential future replacement of active authentication key pair.
Signature key pair (x2)	▪ Key pair that is actively used for digital signing procedures. ▪ Optional idle key pair for a potential future replacement of active signature key pair.
Cardholder personal data file	Includes the cardholder's personal data.
CMK_PIN	3DES key which is used to secure the PIN code replacement procedure.
CMK_KEY	3DES key which is used to authorise the new key pair generation.
CMK_CERT	3DES key which is used to form the secure command series to load the user certificates.

Drivers

In order to use the card, a computer/tablet needs to have drivers to communicate with the Java applet on the card. The drivers are automatically installed the first time the card is accessed from computer via a card reader. The drivers allow applications to communicate and invoke services that the Java applet on the card. Drivers are available for Windows, Mac OS X and Linux. The Estonian government sponsors the development of drivers.

Application support

For applications to use the smart card they must be able to communicate with a device on the computer/tablet. For regular applications installed on the computer/tablet this no problem as those applications have access to local devices. On the other hand, browser-based applications do not have access to local devices without using a browser plug-in. Different browsers have different plug-in architectures which means that for a specific solution such as the one in Estonia there must several plug-ins available in order to support the main browsers on the market (Firefox, Internet Explorer, Chrome, Safari, etc). The Estonian Government sponsors the development of plug-ins for a range of browsers.

Authentication

Authentication using a browser is done be selecting the correct certificate used for authenticating the user. A plug-in helper script is used in the browser access the smart card. Authentication in web environment is carried out using standard TLS/SSL protocol with Client Authentication, supported by most of the browsers used (IE, Mozilla, Safari, Chrome). The protocol implies that the Service Provider will receive full certificate of the user. When the browser requests a cryptographic operation on the card, such as encrypting as hash using the private key, the card software requires that the user enters the pin for the key. The pin can either be entered on a card reader with keypad or the computer's operating system presents the users with a dialog for entering the pin.

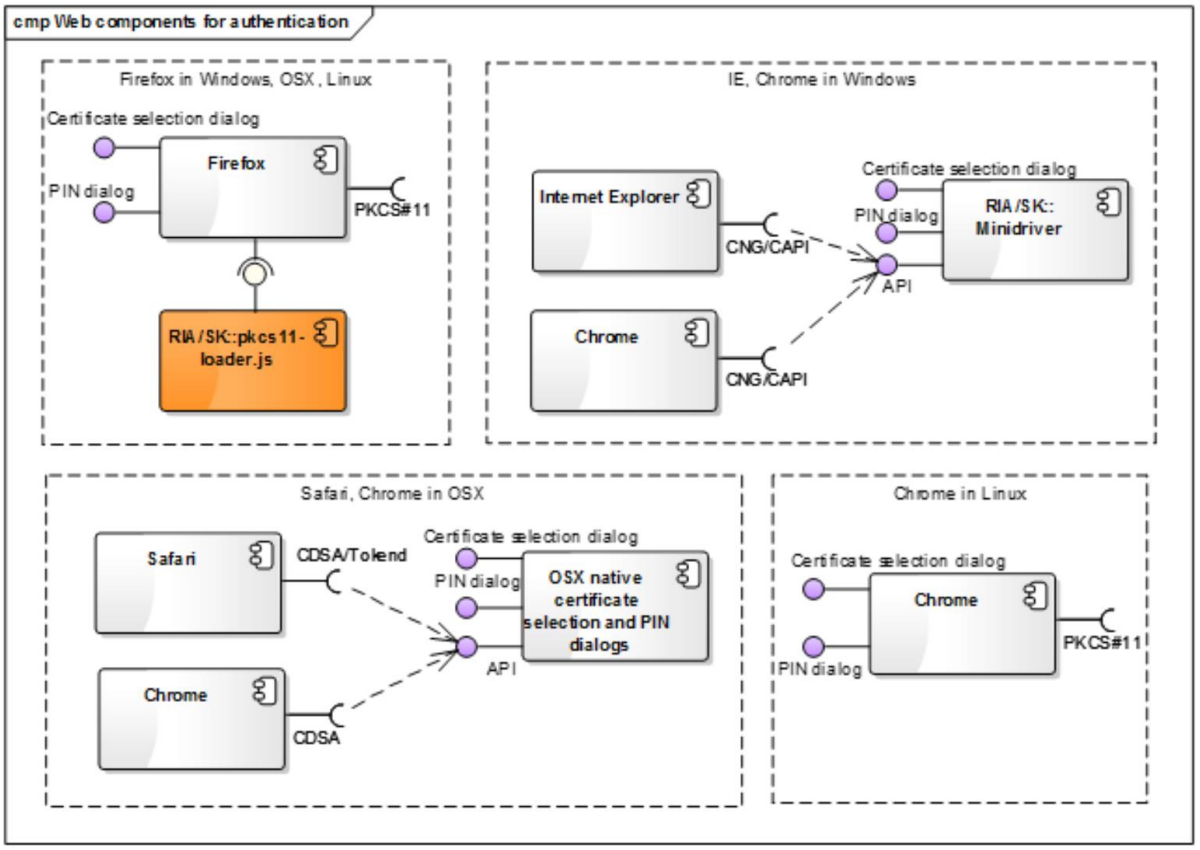

Figure: Web authentication components

Signing

The signing process consists of the computation of a hash of the object to be signed. The computed hash is encrypted using the user's private key and shipped together with the object being signed. The recipient of the document is able to verify the signature by computing the hash of the object and using the signer's public key to decrypting the hash and compare it to the calculated hash.

The object being signed typically represents an action (eg. a money transfer, an update of information etc.)

Below is a diagram covering the web components in the ID-software of Estonia (Architecture of ID-software, 2016)

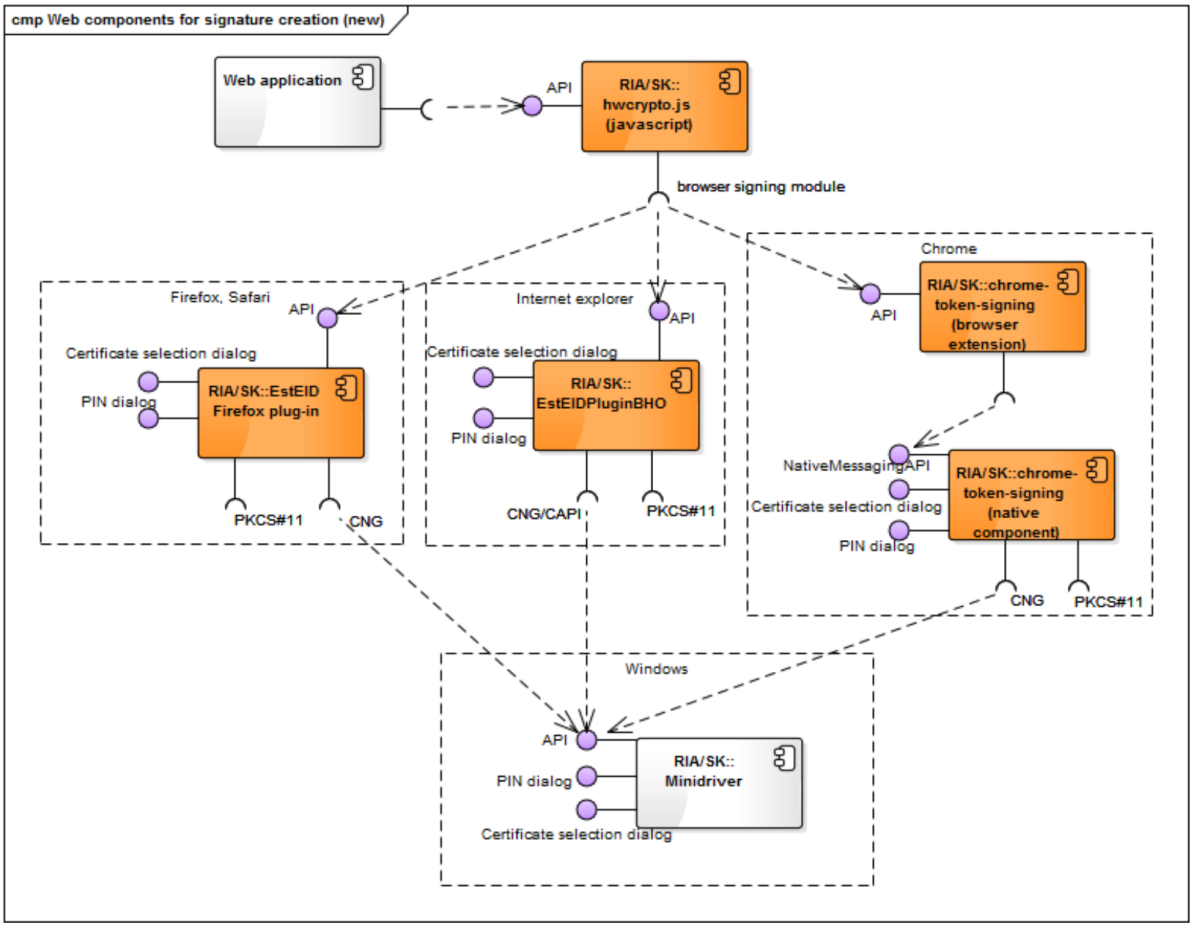

Figure: Components for signature creation in web environment

When a user makes an action that requires his signature, the action needs to be represented and signed in order to be evidence of the user's action.

As illustrated in the diagram below, the Estonia solution uses the same framework for as is used for signing documents (DigiDoc). This raises the question how the Faroese Government should proceed when digital signature is not in scope for this project?

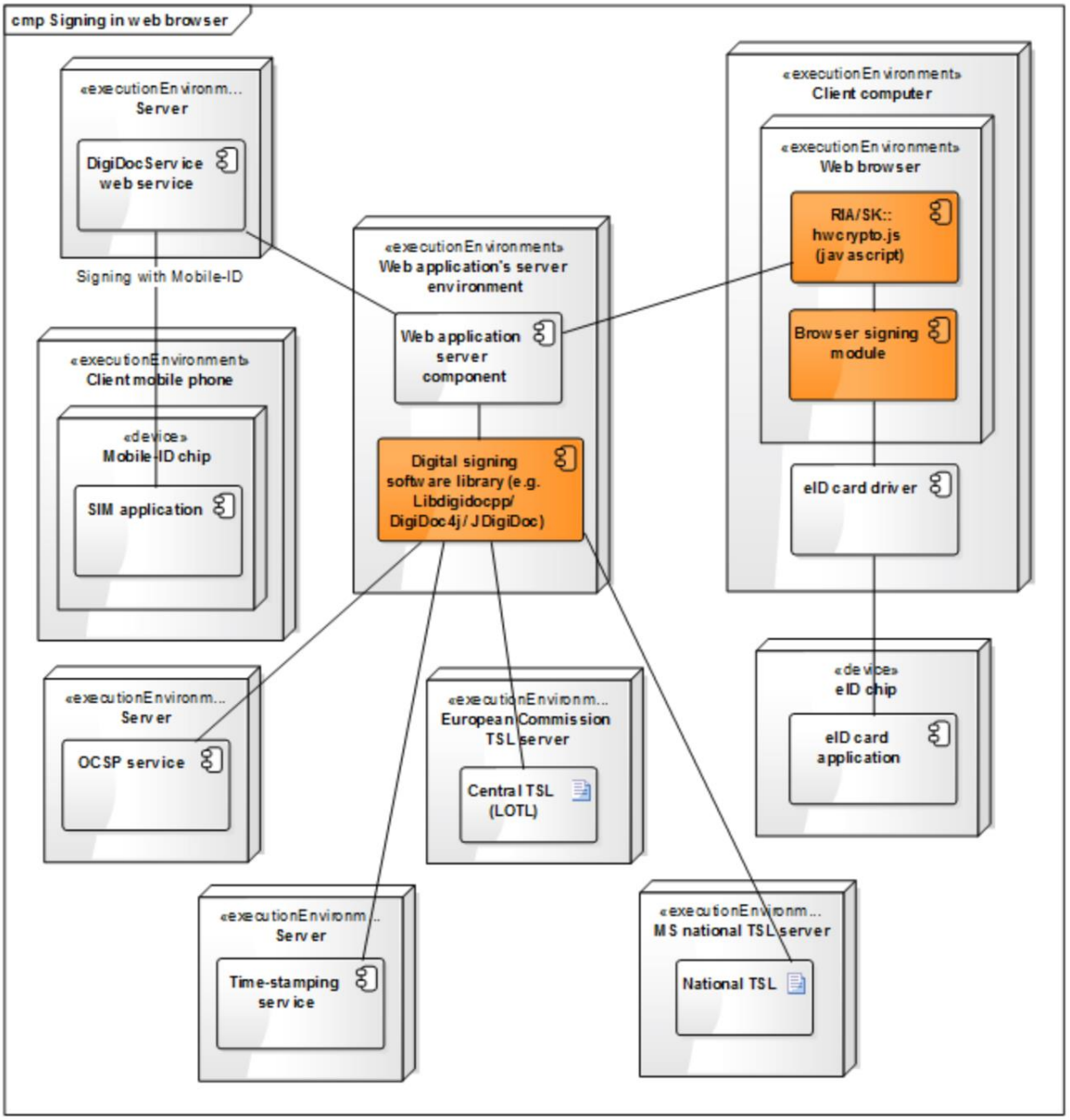

Figure: Signing in web browser via a web application

Summary

The Card ID solution used in Estonia is one component in Estonias electronic Identity system. The solutions requires a Public Key Infrastructure and comprises the following compenents:

- Card readers
- Java applet on the smart card
- Operating system drivers for the smart card
- Plug-ins to web browsers in order to use smart cards

- Utility application for computers to read smart card and update PIN codes
- Procedures and systems for personalising smart cards

The card id solution is a proven technology and in Estonia about 1.2m cards have been issued.

Although seemingly simple, there are quite a few software components in use on the client in order to make the system work.

Since operating systems and browsers continously evolve, there will be a need for updating plug-ins and drivers supporting the card id solution.

The card id solution does not mandate any how service providers use certificates, but there is a need to provide libraries/frameworks/guidelins for service providers to interact with elements in the PKI.