End-To-End Secured Credentialing over the Internet

This presentation describes an Open Source/Open Hardware project that aims establishing a standard for distributing digital credentials such as PKI certificates, OTP seeds, and Information Cards.

A user may have a cryptographic container that is “strong”, be it in the form of a smart card or embedded in a mobile device.

If the user needs to receive an authentication key over the Internet, relevant issuer questions include:

- Is the key container FIPS 140-2 certified or similar?
- Are keys actually created in or stored in the container?

The use-case for this may not be entirely obvious but the fact is that the majority of keys used in mobile phones will be deployed OTA (Over The Air). Currently the primary method are statically configured passwords which neither banks nor government agencies consider satisfactory.

To accomplish E2ES (End To End Security), the described scheme (which consists of a cryptographic module SKS, and a matching provisioning protocol KeyGen2), defines a security architecture with a device certificate at its core. The device certificate is necessary for vouching for the container's identity, type, certification etc.

However, E2ES provisioning requires multiple steps which is why the device certificate together with two other keys performing an SP800-56A ECC CDH primitive is used to create an authenticated secret session key.

With the session key the issuer “orders” the key container creating key-pairs, accepting PIN and PUK definitions etc. all signed by MACs. Secret data transferred between the container and the issuer is encrypted using a derived key. Generated keys are attested by another derived key.

Robustness is assured by performing the entire provisioning session as a transaction.

Successful operation returns a signed “receipt” to the issuer.

Device certificates eliminate enrollment passwords.

Key containers are provisioned using a [future] standard Internet browser.

Author:

Anders Rundgren
PrimeKey Solutions
Skype: anders.rundgren.com
Cell: +46 70 720 91 02
Mail: anders@primekey.se

Stockholm: 2011-08-08