



www.sk.ee

Embedding digital signature technology to other systems - Estonian practice

Urmo Keskel
SK, DigiDoc Product Manager

E-stonia?

SK

- Population: 1.35M
- Internet usage: 54%
- Internet banking: 72%
- Mobile penetration: 92%
- 1000+ Free Internet Access points
- **PKI penetration: >67%**
- **Biggest national eID card roll-out in Europe !**



ID-card Project



- Started in 1997
- Law on personal identification documents: Feb, 1999
- Digital Signature Act: March, 2000
- Government accepted plan for launching ID-card: May, 2000
- First card issued: Jan 28, 2002
- May 2006: >850 000 active cards



The Card



➤ “Compulsory”
for all residents

➤ Contains:

- Personal data file
- Certificate for authentication
(along with e-mail address
Forename.Surname@eesti.ee)
- Certificate for digital signature



Digital Signature - concepts



- Public sector is obliged to accept digitally signed documents
- Digital signature is universal
 - Open user group
 - Any relation – government, business, private
- Focus on document concept
 - Equivalent to what we are doing on paper
- Innumerable quantity of “applications”



Digitally signed document



- Fortunately enough, there is commonly accepted format of digitally signed documents in Estonia (DigiDoc – with extension .ddoc)
- It is impossible to convert digital signature from one format to another
 - Signature value depends on content
 - Signature can be created only by owner of a private key



Document format



- Based on XML-DSIG standard
- Contains subset of ETSI TS 101 903 (XAdES) extensions
 - Place, time and of signature
 - Role of signature holder
 - Validity confirmation and certificate of OCSP responder



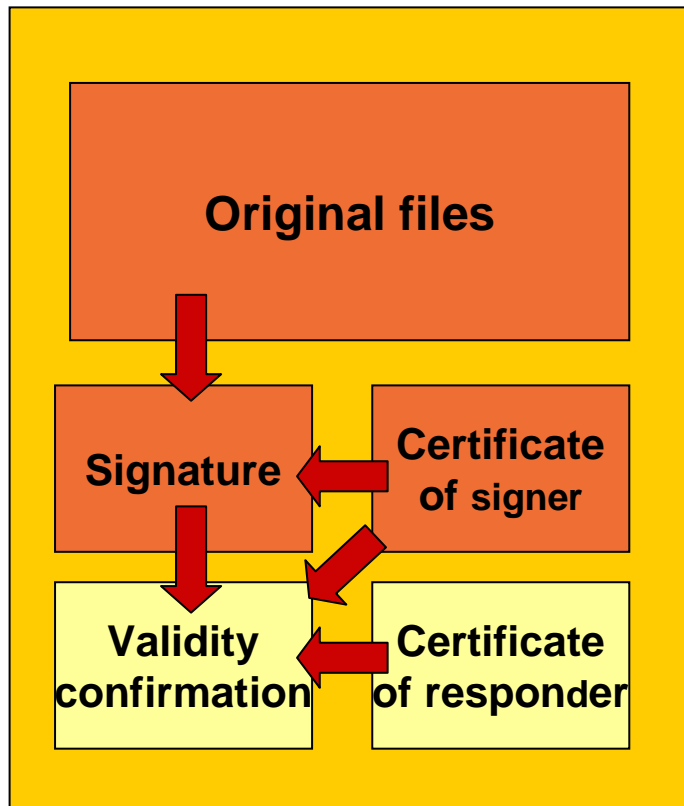
Document format (2)



- Multiple original documents can be signed at once
- Original document can be embedded or detached
- Original document can be XML or any binary format
- Multiple signatures are supported
- Just one validity confirmation per signature



Document format (3)



```
C:\Documents and Settings\tarvi\Desktop\tarvi.xml - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Home Search Favorites Media
Address C:\Documents and Settings\tarvi\Desktop\tarvi.xml
Google Search Web Search Site Page Info Up Highlight

<?xml version="1.0" encoding="UTF-8" ?>
- <SignedDoc format="DIGIDOC-XML" version="1.1">
  <DataFile ContentType="EMBEDDED_BASE64" Filename="tarvi.txt" Id="D0" MimeType="text/plain"
    Size="120">//5TAHkAcwB0AGUAbQAgAEkAbgBmAG8AcbtAGEAdABpAG8AbgAgAHIAZQBwAG8A
    cgB0ACAAdwByAGkAdAB0AGUAbgAgAGEAdAA6ACAAMQA5AC4AMQAxAC4AMgAwADAA
    MgAgADEANGA6ADEAOQA6ADEAOQANAaAoA</DataFile>
  - <Signature Id="S0" xmlns="http://www.w3.org/2000/09/xmldsig#">
    - <SignedInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
    - <Reference URI="#D0">
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <DigestValue>k1mloxQifof9vtNmwlXT2X2/XtQ=</DigestValue>
    </Reference>
    - <Reference URI="#S0-SignedProperties">
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <DigestValue>788QSk95mMKw4mSgECZsMIILgvM=</DigestValue>
    </Reference>
    </SignedInfo>
    <SignatureValue Id="S0-SIG">AT7kfBjsyl/CojRopoiqIFd52D3j1LdpV68TfMq4gqdfbtLiWGSg5IWig5+F2wit
    dlfngS7/vkc1QW8Hr1h8IOapn4I3cjpFgFfx4yJHBuKJYMK+Sarx/LDPSIVbQGdR3
    tffgYnj8OPToGDVJZ+AHxZmu93Hb5I0ZYHSEZvN8Fo0=</SignatureValue>
  - <KeyInfo>
    - <KeyValue>
      - <RSAKeyValue>
        <Modulus>j4evKjrrMxhOZ1DLTFn1r04gpqqKhMU2sroZjKm0vC/p1lksrB0GVmRIYyubqs5o
        FGaWZ9exuZUgx7pyjSZr7dmoF+nd3HCWzKxmMVV9xbsEji6HTYe7oQdlpAAwzyjc
        ZWox/y4UUc0Zqr7q+PfENP6vxGX1psEYt/yVzmr7J9M=</Modulus>
        <Exponent>PBnY/w==</Exponent>
      </RSAKeyValue>
    </KeyValue>
    - <X509Data>
      <X509Certificate>MIID7zCCAtAgAwIBAgIEPFEniJANBgkqhkiG9w0BAQUFAADBMRgwFgYJKoZIhvcN
```



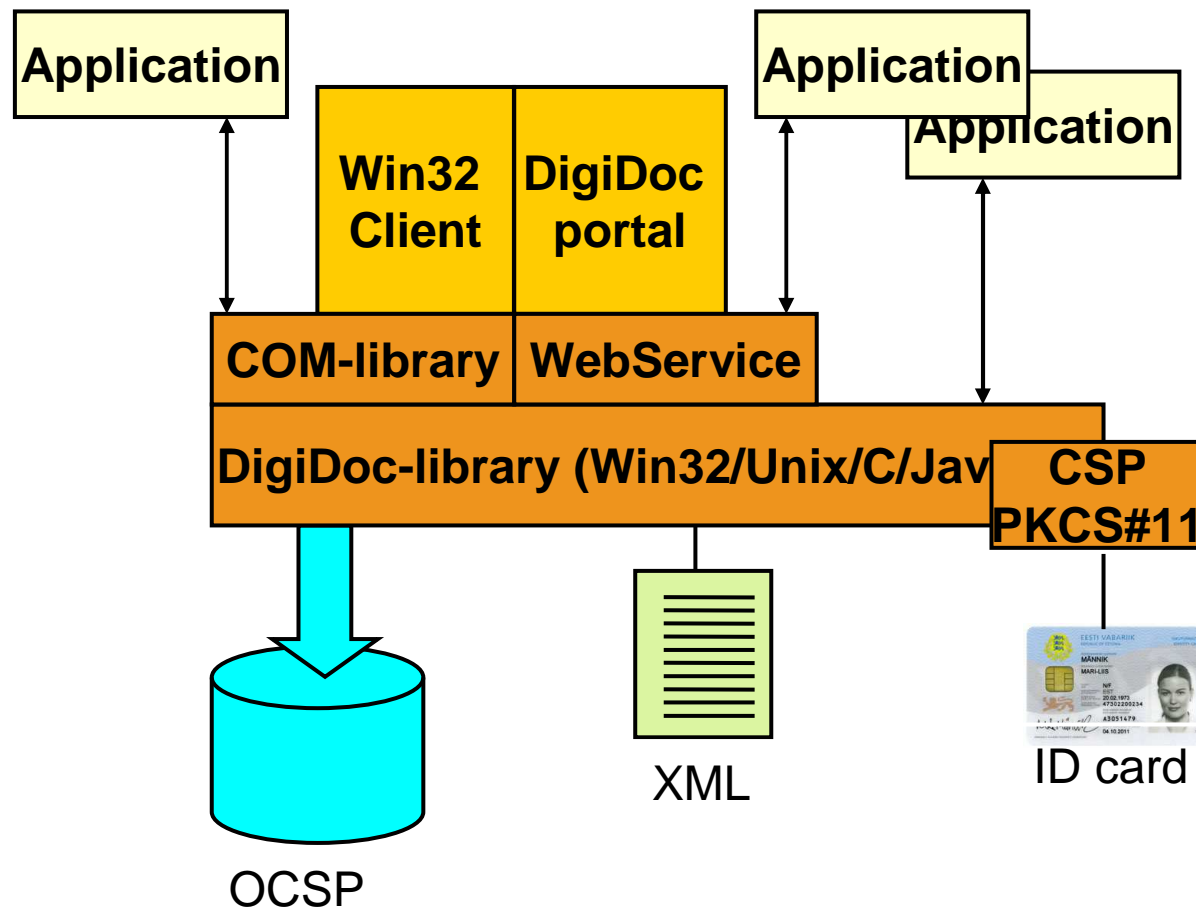
DigiDoc – not just a document format!



- DigiDoc is environment for providing digitally signed documents
- Contains:
 - Document format
 - WWW-portal for creating and verifying digital signatures
 - Client applications
 - Programming libraries
- Distributed as a free system



DigiDoc Architecture



DigiDoc Portal



- Simple WWW-application for everyone:
 - Downloading/uploading of document
 - Signing documents
 - Sending document to another portal user
 - Verification

Puhkus Tarvi 03-2006.ddoc [Download file](#) [Confirmation page](#) [Delete](#)

Files

Filename	Type	Size	
Puhkus Tarvi 03-2006.doc	application/msword	539 KB	

Signatures

Signer	Time	Signature
MARTENS, TARVI, 36903260223	21.03.2006 17:25:11	OK
MILVA, TARMO, 36801200230	21.03.2006 21:02:29	OK
KESKEL, URMO, 38002240232	22.03.2006 11:37:26	OK
JÄRV, AIN, 36810170217	23.03.2006 11:30:40	OK

Shared for signing

From	To
TARVI MARTENS 36903260223	URMO KESKEL 38002240232



DigiDoc Client



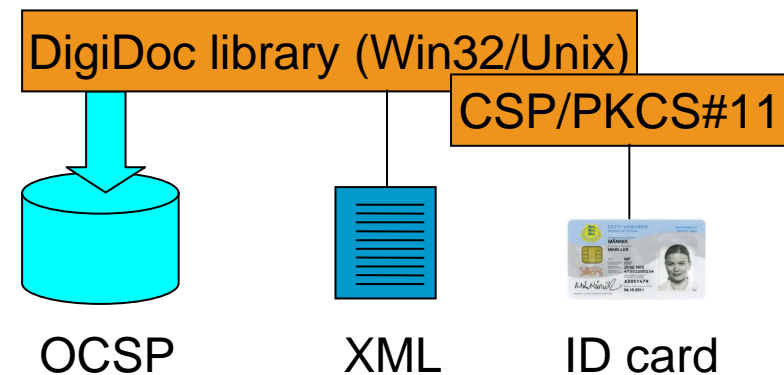
- Provides the same functionality as portal
 - Signing and obtaining validity confirmation
 - Verification of signed document
- Does not require uploading document to some server
- Tested with Estonian, Finnish and Belgium national ID-cards



DigiDoc libraries



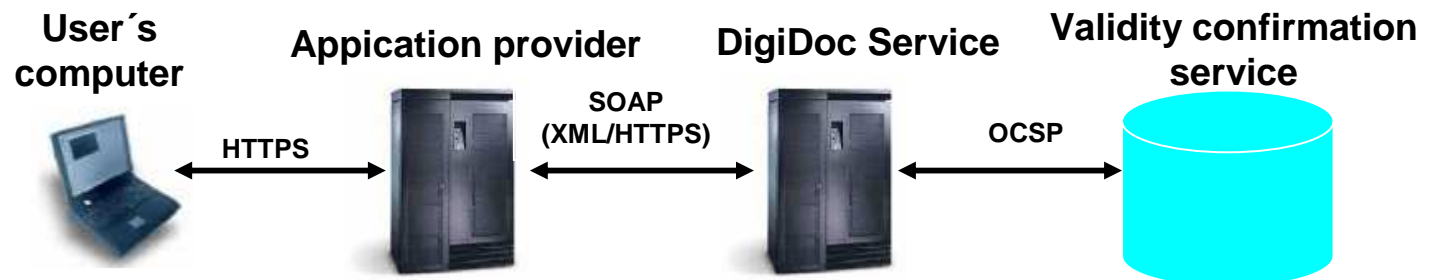
- Signing through PKCS#11 and CSP
- Handling of validity confirmation
- Handling of XML document
- Verification
- Encryption/decryption
- Win32/Unix, C code
- DLL & COM under Windows
- Java implementation
- Distributed under LGPL terms



DigiDocService



- Simple SOAP-based protocol
 - “I have a file here, make it signed”
 - “I have got a signed file. What’s inside it?”
- Best for integration of digital signature handling capability – libraries a changing rapidly, the protocol remains more stable
- Especially is designed for web-applications, but not only



DigiDocService(2)



- Platform independent – SOAP protocol is used
- Easy integration
 - Demo application and thin client library for Java
 - Demo application and thin client library for PHP
- Platform independent for end-user
 - Includes ActiveX add-on for Internet Explorer
 - Includes Java Applet for Mozilla/Firefox
- No need to worry about library updates



What to choose?



- Usually DigiDocService is the best solution for WWW based systems
- For complex systems there may be a need for libraries (for example for encryption/decryption)
- For verification only and data file extracting the integration of libraries may be the optimal solution



What kind of systems need digital signing functionality?



Some examples of applications:

- Internet banking
 - Document management systems
 - E-services: signing contracts, applications, orders and etc
 - Book-keeping software
 - E-voting and gallup systems
 - ...
- ➔ 80% of systems are web-based



Different integration levels



- No integration - Digital signatures are created and verified by using DigiDoc Client or WWW portal.
- Integration for verification only
- Signing and verification both are implemented



Current situation in Estonia



- Almost all document management systems support digital signing and digital signature verification
- All governmental institutions (should) accept digitally signed files, but only few of them have integrated signing into their systems
- Some banks allow to sign payment orders
- Signing contracts on e-services are getting day by day more popular
- I-voting in October 2005 (municipal government elections)



Hot topics in Estonia



- Achieving the digital signatures interoperability within Europe is a big challenge
- Usually there are no rules for archiving electronic documents
- Legislation of company signatures (so called digital stamps) is in progress
- Soon it should be possible to create a qualified signature by mobile phone



Morale



- PKI stands for Public Key **Infrastructure**
- There are no services nor applications before **The Infrastructure** is built
 - Roads generate no benefit, transportation does
 - People do not buy cars unless there are roads
- **Infrastructure first**



Additional information



- DigiDoc contsepts: www.openxades.org
- DigiDoc technology: www.sk.ee
- ID-card practices: www.id.ee
- Govermental e-services: www.eesti.ee



Contact point:
urmo@sk.ee





www.sk.ee

Thank You!