Visual Representation of Certificate Based eID

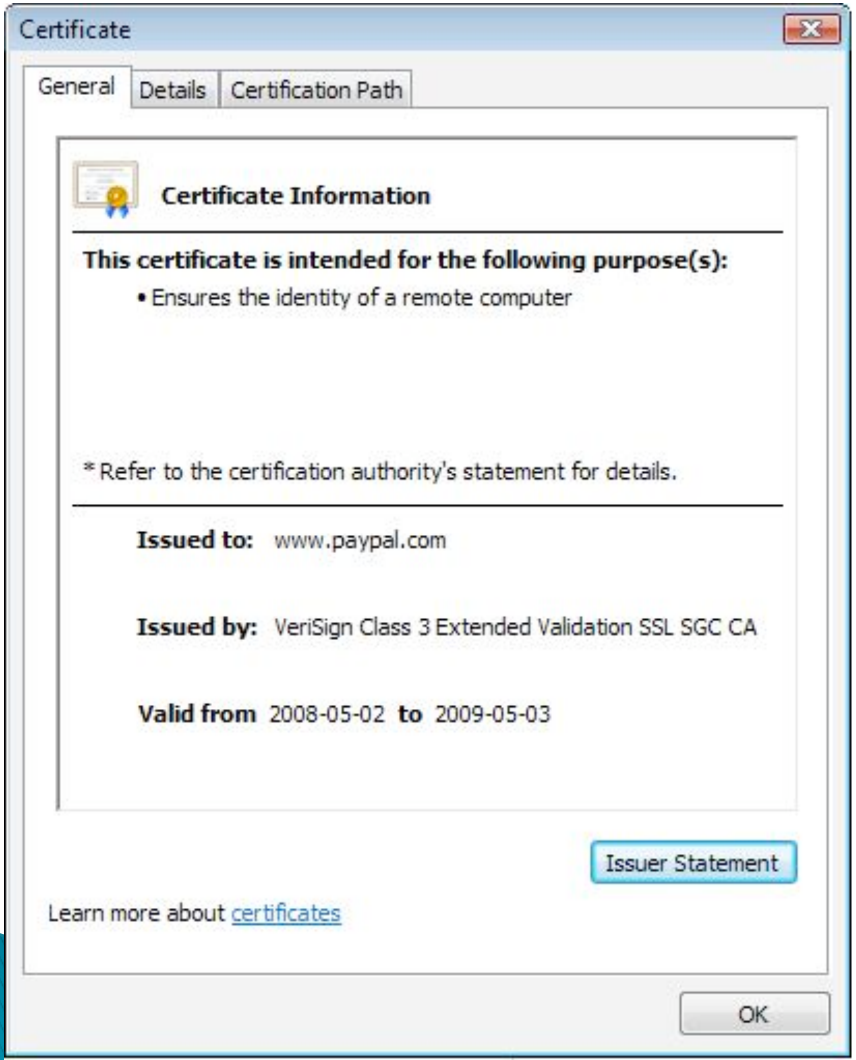
Stefan Santesson
AAA-sec.com

What is the problem

- The need for humans to know WHO they are dealing with
  - Software publisher
  - Web merchant
  - Authority asking for private information

We have deployed the most sophisticated math to verify credentials…… But NO way to translate that verification to human intelligible information!

This is NOT intelligible



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

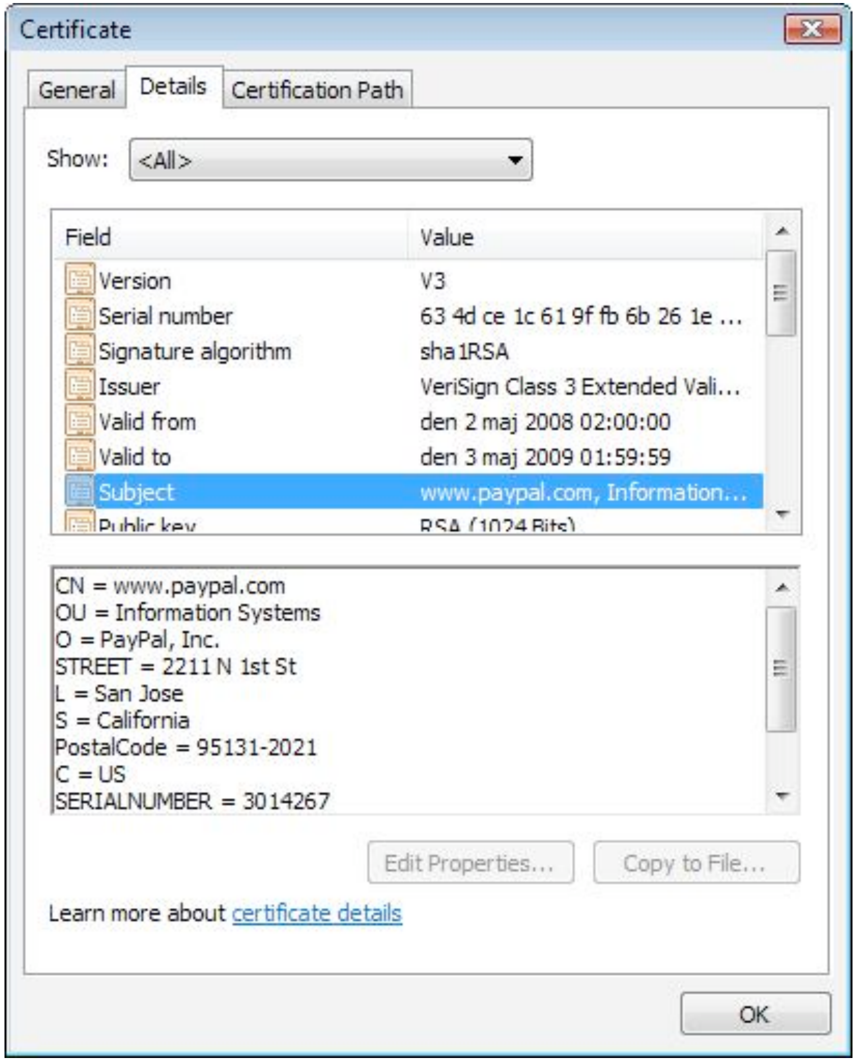
* Refer to the certification authority's statement for details.

Issued to: www.paypal.com

Issued by: VeriSign Class 3 Extended Validation SSL SGC CA

Valid from 2008-05-02 **to** 2009-05-03

Learn more about certificates



Show: <All>

Field	Value
Version	V3
Serial number	63 4d ce 1c 61 9f fb 6b 26 1e ...
Signature algorithm	sha1RSA
Issuer	VeriSign Class 3 Extended Vali...
Valid from	den 2 maj 2008 02:00:00
Valid to	den 3 maj 2009 01:59:59
Subject	www.paypal.com, Information...
Public key	RSA (1024 Bits)

```
CN = www.paypal.com
OU = Information Systems
O = PayPal, Inc.
STREET = 2211 N 1st St
L = San Jose
S = California
PostalCode = 95131-2021
C = US
SERIALNUMBER = 3014267
```

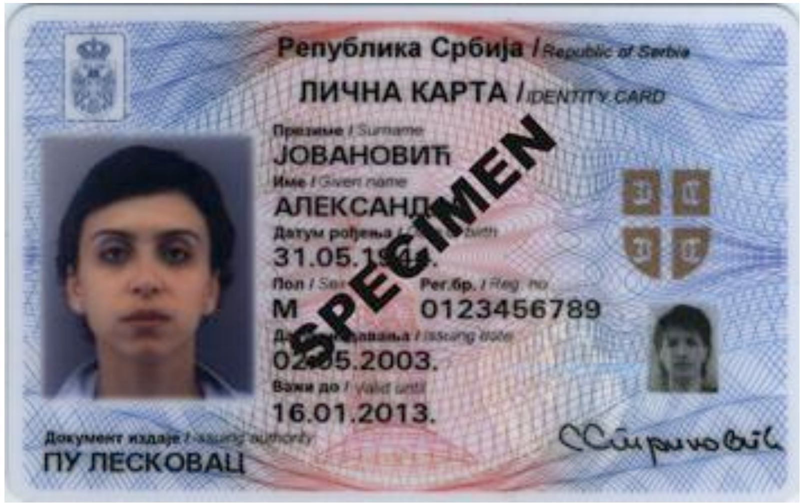
Learn more about certificate details

But this is

DIM DIOLCH

004972203
SECURITY: 02
LEVEL: 4

12345 67809



Република Србија / Republic of Serbia

ЛИЧНА КАРТА / IDENTITY CARD

Презиме / Surname
JОВАНОВИЋ

Име / Given name
АЛЕКСАНД

Датум рођења / Date of birth
31.05.19

Пол / Sex
M

Рег.бр. / Reg. no
0123456789

Датум издавања / Issuing date
02.05.2003.

Важи до / Valid until
16.01.2013.

Документ издаје / Issuing authority
ПУ ЛЕСКОВАЦ

What is stopping us

- No common visual design
- No common set of attributes
- Lack of semantics and labels (country, serialNumber)
- Lack of localization

Certificates do not provide sufficient data

RFC 3709 Logotypes

- Adds logotype images through URL and hash
  - Community
  - Issuer Organization
  - Subject Organization

BUT..

- No graphical design
- No selection of attributes
- No semantics or display labels

BUT RFC 3709....

- Is extensible
- Allow definition of new image types

So......

- What if we turn the whole visual representation of the eID into one combined and scalable image?

Possible solution

- July 1 2008, Portable Document Format (PDF) becomes ISO 32000-1:2008

- Three choices
  - Keep RFC 3709 intact
    - Just define new RFC 3709 otherLogos type, binding a complete visual certificate image to the certificate
  - Update RFC 3709
  - Define new extension

Open issues

- Allow embedded certificate image?
- Extensibility
- MIME Media Type for PDF
- Metadata (language and scaling)

Use Case

BankID

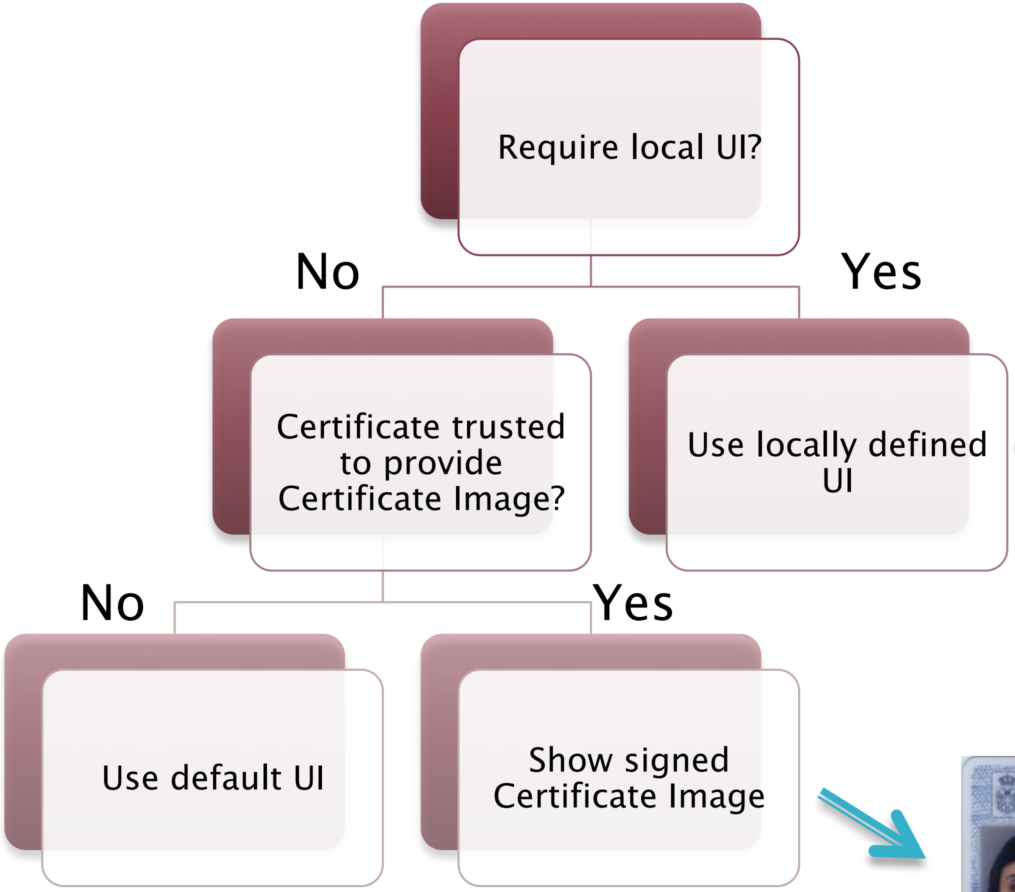
- National eID provider in Sweden
- 1.5 million users
- Usable in 300 Services
- Supported by national legislation
- Customized applications for trust, session and UI control
- Certificate image could enhance
  - Identification of Services
  - General User acceptance of technology
  - Selection and recognition of certified eID

The controversial issue

- What if a CA issues a certificate with conflicting information ?
  - Image claims I’m John Doe
  - Attributes claim I’m Jane Doe

- Society tolerates that some crimes are possible to commit as long as we can detect, trace and prosecute them.
- Relying Party trust policy is always in control

Typical UI policy



Require local UI?

No

Yes

Certificate trusted to provide Certificate Image?

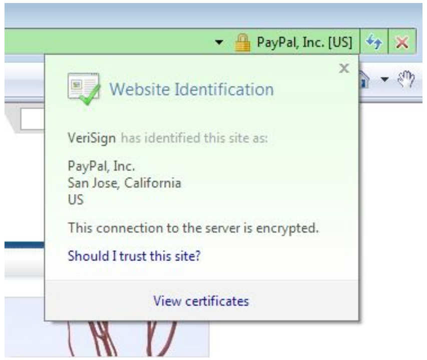
Use locally defined UI

No

Yes

Use default UI

Show signed Certificate Image



Website Identification

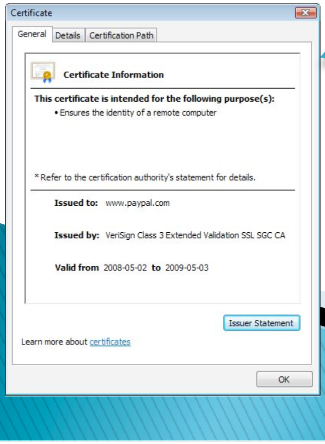
VeriSign has identified this site as:

PayPal, Inc.
San Jose, California
US

This connection to the server is encrypted.

Should I trust this site?

View certificates



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

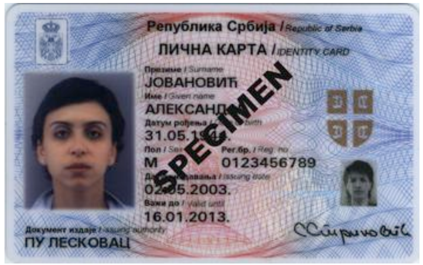
* Refer to the certification authority's statement for details.

Issued to: www.paypal.com

Issued by: VeriSign Class 3 Extended Validation SSL SGC CA

Valid from 2008-05-02 **to** 2009-05-03

Learn more about certificates



Република Србија / Republic of Serbia

ЛИЧНА КАРТА / IDENTITY CARD

Презиме / Surname
JOBAHOBИЋ

Име / Given name
АЛЕКСАНД

Датум рођења / Date of birth
31.05.19

Пол / Sex
M

Рег.бр. / Reg. no
0123456789

Датум издавања / Issuing date
02.05.2003.

Важи до / Valid until
16.01.2013.

Документ издаје / Issuing authority
ПУ ЛЕСКОВАЦ

Path Forward

- Investigate interest
- Editors
- Develop first draft
- Request to develop standard in PKIX

Visual eID Project

http://AAA-sec.com/visualeid/

stefan@AAA-sec.com