SWITCH

The Swiss Education & Research Network

The new PostZertifikat: first hands-on experience

Kaspar Brand <brand@switch.ch>

2nd SWITCHpki RAO Meeting

Berne, 18 April 2007

The PostZertifikat – it's available, finally

SWITCH
The Swiss Education & Research Network

Launched at press conference on 4 April 2007

What you get:

- Siemens CardOS V4.3B smartcard (Infineon SLE66CX322P processor chip, 32 KByte memory)
- Omnikey CardMan 6121 USB smartcard reader
- software (drivers for smartcard reader and smartcard)
- a 4-page "user manual"

… all stuffed into a nice yellow cardboard box ("Starter-Kit"), which is produced by industrious employees wearing white coats…
[https://postzertifikat.ch/f_5537_download_movies.php?file=2]

What you also get:

- three pre-generated 2048-bit RSA keys
- a 6-digit transport PIN
- a passphrase for revoking these keys

A closer look at the smartcard

SWITCH
The Swiss Education & Research Network

Looking at the private keys through Cryptoki (PKCS#11)…

CKA_LABEL	SwissSign_nonRep	SwissSign_digSig	SwissSign_dataEnc
CKA_SIGN	TRUE	TRUE	TRUE
CKA_DECRYPT	FALSE	TRUE	TRUE
CKA_UNWRAP	FALSE	TRUE	TRUE
CKA_LOCAL	**TRUE**	**TRUE**	**TRUE**
CKA_EXTRACTABLE	**FALSE**	**FALSE**	**FALSE**
CKA_NEVER_EXTRACTABLE	**TRUE**	**TRUE**	**TRUE**
CKA_SECONDARY_AUTH	TRUE	FALSE	FALSE

CKA_SIGN: key supports signatures where the signature is an appendix to the data
CKA_DECRYPT: key supports decryption
CKA_UNWRAP: key supports unwrapping (i.e. can be used to unwrap other keys)
CKA_LOCAL: key was either generated locally or copied from a key with CKA_LOCAL == TRUE
CKA_EXTRACTABLE: key is extractable and can be wrapped
CKA_NEVER_EXTRACTABLE: key never had CKA_EXTRACTABLE == TRUE
CKA_SECONDARY_AUTH: key requires a secondary authentication to take place before its use is allowed

What you get if all checks succeeded

SWITCH
The Swiss Education & Research Network

Three certificates, all with the same issuer/subject:

```
Issuer: C=CH, O=SwissSign AG, CN=Swiss Post Platinum CA - G2
Subject: C=CH, O=Your Org, CN=Your Name/emailAddress=you@example.org
```

Valid for 3 years

With different key usages:

nonRep (not for certificates issued to organizations, where **`CN=Your Org`**)

```
X509v3 Key Usage: critical
  Non Repudiation
X509v3 Subject Alternative Name:
  email:you@example.org
```

digSig

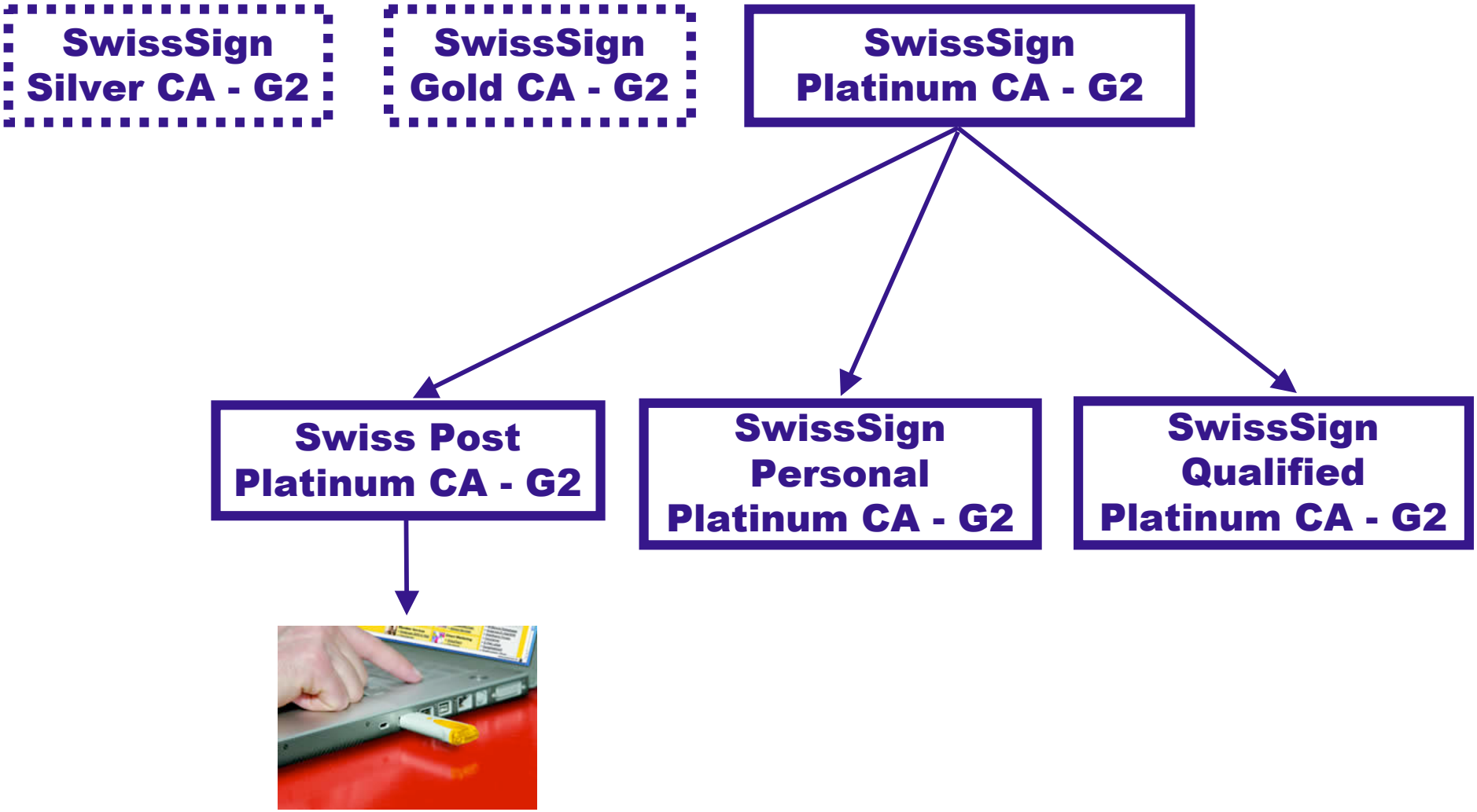
```
X509v3 Key Usage: critical
  Digital Signature, Key Agreement
X509v3 Extended Key Usage:
  E-mail Protection, TLS Web Client Authentication, Microsoft Smartcardlogin
X509v3 Subject Alternative Name:
  email:you@example.org
```

dataEnc

```
X509v3 Key Usage: critical
  Key Encipherment, Data Encipherment
X509v3 Extended Key Usage:
  E-mail Protection, Microsoft Encrypted File System
```

SwissSign's Platinum CA hierarchy

SWITCH
The Swiss Education & Research Network



Pricing of the PostZertifikat

SWITCH
The Swiss Education & Research Network

- Three types of certificates available
- Valid for 3 years, yearly fee depends on the type of certificate
- Mobile RA offering for all certificate types
- Enterprise RA option available for certificates with an organization name entry (O=)

	Natürliche Personen	Natürliche Personen mit Organisationseintrag	Organisationen
Kauf Starter-Kit	90.-	90.-	90.-
Jährliche Nutzungsgebühr	35.-	60.-	90.-

Optionen:

Mobile Registrierungsstelle: Grundpauschale pro Einsatztag	200.-	200.-	200.-
Mobile Registrierungsstelle: Stundenansatz [1]	78.-	78.-	78.-
Ausbildung einer eigenen Registrierungsstelle [2]	---	1'800.-	---
Restore nach der M of N Methode	1'500.-	1'500.-	1'500.-

[1] Pro Stunde kann eine mobile Registrierungsstelle ca. 4-5 Personen bedienen.
[2] Diese Pauschale ist für die Ausbildung von max. 3 Personen vorgesehen.

Supported operating systems/applications

SWITCH
The Swiss Education & Research Network

Browser / Email Client / Betriebssystem	Internet Explorer 6.0 und höher	Outlook	Firefox 2.0.0.x und höher	Mozilla 1.0 und höher	Thunderbird	Opera	IncaMail
Windows 2000	X	X	X	X	X	X	X
Windows XP Ho	X	X	X	X	X	X	X
Windows XP Pro	X	X	X	X	X		X
Windows Vista	O	O	O	O	O		O
Linux SuSE 10			X		O		O
Linux Red Hat			O		O		O
Mac OS X PPC[1]			X		O		O
Mac OS X Intel			O		O		O

X = supported / O = not yet available

➔ Support for several OS/application combos missing due to lack of suitable drivers (either smartcard reader and/or smartcard)

Other things to note

SWITCH
The Swiss Education & Research Network

Only available as a hardware token

Not a qualified certificate according to ZertES (only an “advanced” one). Quoting from the German AGB:

> *Bei den Postzertifikaten handelt es sich **nicht um qualifizierte Zertifikate** im Sinne des Bundesgesetzes über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES). […] Die auf einem PostZertifikat beruhende elektronische Signatur ist – abweichende gesetzliche oder vertragliche Regelungen vorbehalten – nach schweizerischem Recht **nicht der eigenhändigen Unterschrift gleichgestellt** (vgl. Artikel 14bis des Obligationenrechtes).*
>
> [**“not on a par with the personal signature”** according to the Swiss Code of Obligations]

For the encryption certificate, a key escrow option can be selected at registration time. Access to the escrowed copy is possible either through a user-selected passphrase or by the “M of N method”

In theory (AGB section 20.3), Swiss Post can cancel the contract within 1 week’s notice, for no specific reason (will invalidate the certificates issued so far)…

Some room for improvement left…

SWITCH
The Swiss Education & Research Network

When the Mac installer has done its duty…

(Clicking **OK** will **`shutdown -r now`**, i.e. reboot immediately)

The Swiss Education & Research Network