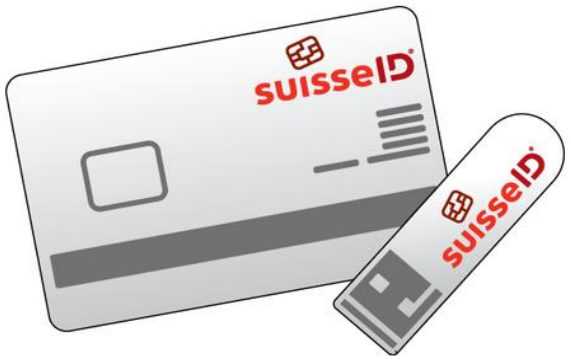


SuisseID als PKI-Ersatz für KMU?

Masterarbeit MAS Information Security 18
Hochschule Luzern/IWI

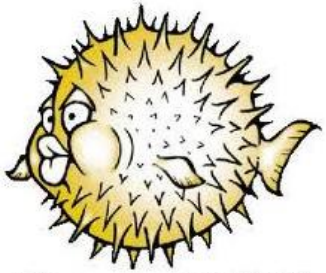
Stephan Rickauer

Beer-Talk, 31. Oktober 2013

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Who is /me?



Vorstellung

Stephan Rickauer

- Seit 2011 bei Compass als IT Security Analyst
- Vom Unix-Engineering zur IT-Security
- Kompetenzen
  - Empirische Sicherheitsprüfungen
  - IT-Security
  - IT-Forensik

Hobbys

- Shitokai Karate
- Action Sports
- Sci-Fi
- Free Software («as in speech»)

Nach Feierabend...

Agenda

Übersicht, Ziele und Zusammenfassung

Einführung PKI und SuisseID

Exemplarische Betriebsabläufe am Beispiel Compass

Migrationsuntersuchung SuisseID

Vergleiche: PKI versus SuisseID

Fazit / Ergebnisse

Dank & Fragen und Antworten

Übersicht, Ziele und Zusammenfassung

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Übersicht, Ziele und Zusammenfassung

Idee: ***"Kann man die SuisseID in einer KMU im professionellen Umfeld als Ersatz zu einer eigenen Public Key Infrastructure betreiben?"***

Gibt es Funktionseinbussen?

Lohnt sich der Aufwand?

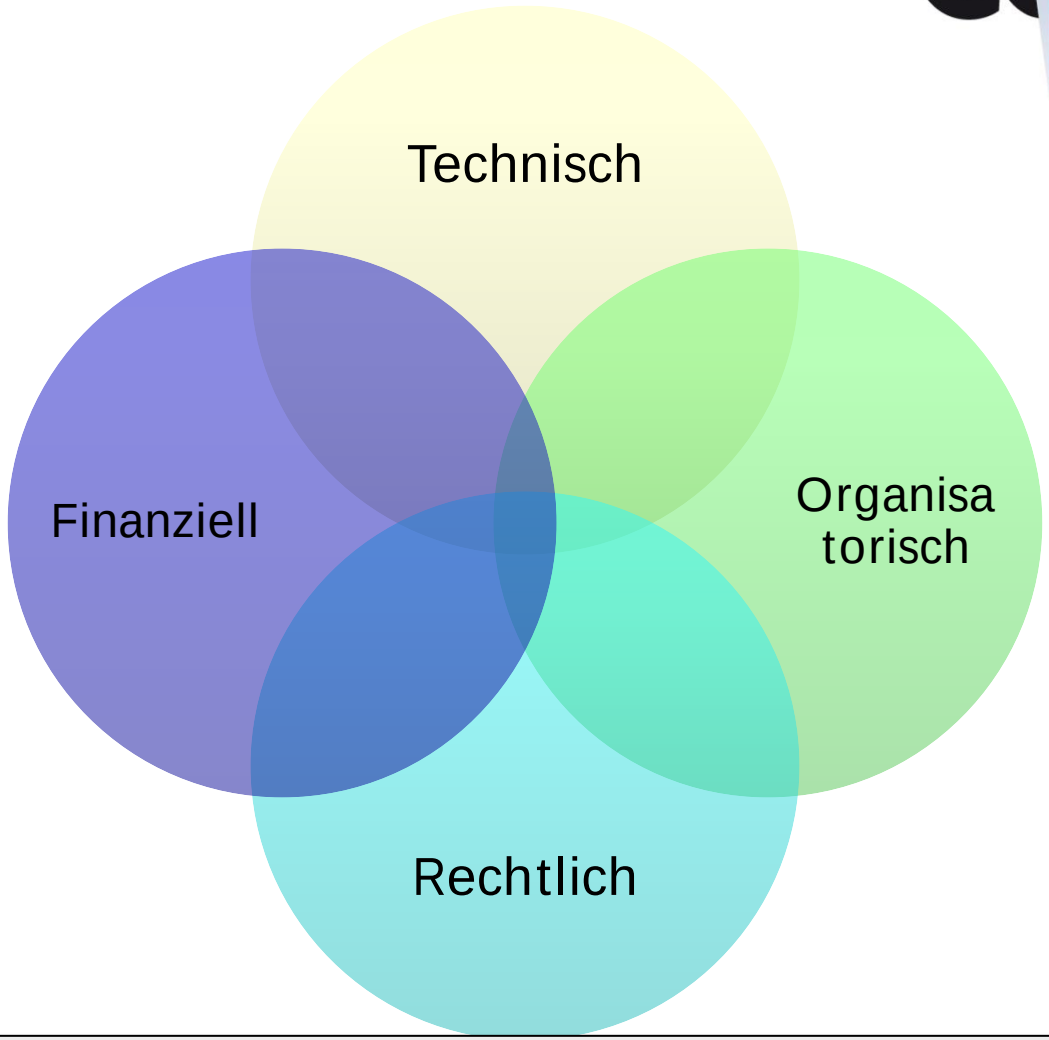
Welche Kosteneinsparung sind möglich?

Ändert sich der Benutzerkomfort?

Wie wird das Sicherheitsniveau beeinflusst?

Existieren rechtliche Konsequenzen?

Vorgehen



Compass Security Schweiz AG

Einführung zu PKI und SuisseID

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Einführung zu PKI und SuisseID

Public Key Infrastrukturen (PKI):

- Asymmetrisches Kryptosystem als Grundlage
- Unternehmensweite, einheitliche Infrastruktur-Lösung zur zertifikatsbasierten Authentisierung, Verschlüsselung, Signierung
- Oft in Zusammenschluss mit Single-Sign-On (SSO) zur zentralen Einmal-Authentisierung
- Fortgeschrittene Zertifikate/Signaturen
- Zertifkate als Soft- oder Hardtoken (USB, Smartcard etc.)

Einführung zu PKI und SuisseID (2)

SuisseID:

- Standardisierter, elektronischer Identitätsnachweis

Wie PKI, aber:

- Qualifiziertes Zertifkat (QS) und Authentisierungs-Zertifkat (IAC)
- Hardware als USB-Stick und Smartcard
- Gesetzlich annerkannte, digitale Unterschrift
- **"Sicher"**
- Soll keine Verschlüsselung ermöglichen
- Ausstellung nur durch Anbieter von Zertifizierungsdiensten

Fortgeschritten vs. Qualifiziert

- Fortgeschritten:
  - Zertifikat ausschliesslich dem Inhaber zugeordnet
  - Zertifikat ermöglicht eindeutige Identifikation des Inhabers
  - Wird mit Mitteln erzeugt, die unter seiner alleinigen Kontrolle stehen
  - Ermöglicht das Erkennen von signierten und nachträglich veränderten Dokumenten

- Qualifiziert
  - Sichere Signaturerstellungseinheit gemäss ZertES
  - Ausstellung durch akkreditierte Zertifizierungsdienste (CSP)
  - Schlüsselpaar muss auf Signaturerstellungseinheit erzeugt werden (TAV)
  - Signaturerstellungseinheit muss unter Kontrolle des Zertifikatsinhabers sicher betrieben werden (TAV)

OpenSC

```
$ opensc-tool.exe --list-readers
# Detected readers (pcsc)
Nr.  Card  Features  Name
0    Yes             ACS CCID USB Reader 0
1    Yes             AKS ifdh 0
2    Yes             AKS ifdh 1
3    Yes             AKS VR 0
```

```
C:\>opensc-tool.exe --reader 0 --name
Unsupported card
```

```
$ opensc-tool --reader 0 --atr
3b:fa:18:00:02:c1:0a:31:fe:58:4b:53:77:69:73:73:53:69:67:6e:89
```

Inhalt der SuisseID (pkcs15-tool)

```
Private RSA Key [SwissSign_nonRep]

Private RSA Key [SwissSign_digSig]

Private RSA Key [SwissSign_dataEnc]

Public RSA Key [SwissSign_nonRep]

Public RSA Key [SwissSign_digSig]

Public RSA Key [SwissSign_dataEnc]

X.509 Certificate [SwissSign Platinum CA - G2]

X.509 Certificate [SwissSign SuisseID Platinum CA 2010 - G2]

X.509 Certificate [StephanAndreasRickauerAuthentication]

X.509 Certificate [SwissSign Qualified Platinum CA 2010 - G2]

X.509 Certificate [StephanAndreasRickauerQualifiedSignature]
```

Exemplarische Betriebsabläufe am Beispiel Compass Security AG

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Exemplarische Betriebsabläufe

Organisatorisches

1. Strafregisterauszug
2. Betreibungsregister-Auszug

Technisches

1. Authentisierung
2. Digitales und manuelles Signieren
3. Verschlüsselung

Exemplarische Betriebsabläufe (2)

Dienst	Produkt	Kategorie
Betriebssystem-Authentisierung	Windows / OS X	Authentisierung
Webbasierte Zugänge	Externe Website	
	Compass Website	
Remote Access Services	OpenSSH	
	OpenVPN	
	Subversion (Versionskontrolle)	
Spezielle Zugänge	Filebox	
	Abacus-Cloud	
	SuissseTax ESTV (MwSt.)	
E-Mail-Signierung	Outlook S/MIME	Signieren
Datei-Signierung	Offerten, PDFs usw.	
Full-Disk Encryption	PGP WDE / BitLocker	Verschlüsseln
Dateibasierte Verschlüsselung	PGP Desktop	

Migrationsuntersuchung SuisseID

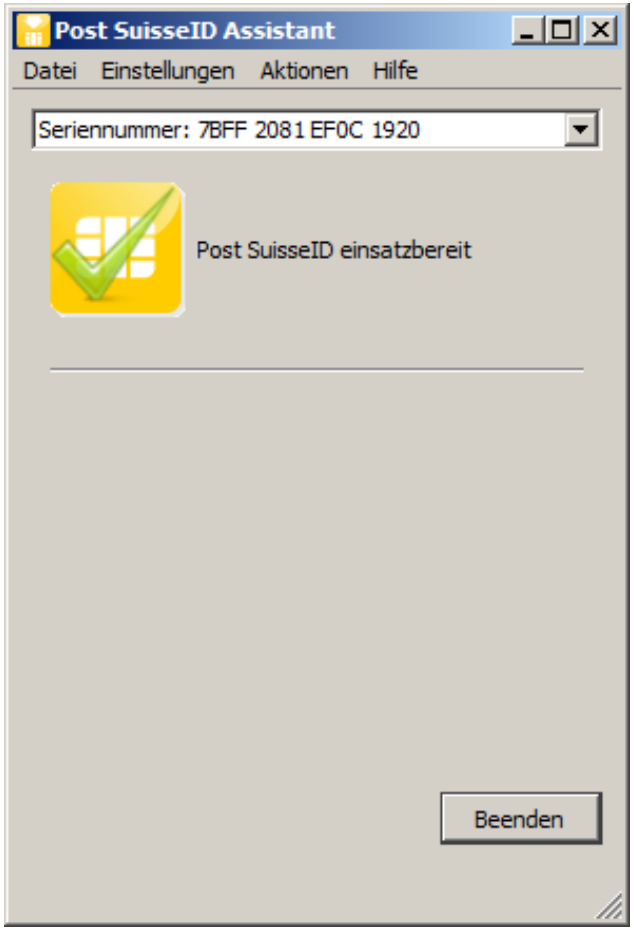
Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Migrationsuntersuchung (Organ.)

Organisatorisches

1. Antrag SuisseID
2. Installation SuisseID-Software
3. Strafregisterauszug
4. Betreibungsregister-Auszug



Migrationsuntersuchung (Authent.)

1. Betriebssystem-Authentisierung
   1. Windows sehr gut dokumentiert
   2. Mac OS X, Proof-of-Concept
   3. Linux, prinzipiell möglich, out-of-scope
2. Webbasiert, Drittanbieter
   1. CSNC-Wiki => SSL
   2. Revoziierung via CRL oder OSCP
   3. OpenID und Clavid
3. Webbasiert, Compass-eigen
   1. Hacking-Lab => Identity Provider
   2. Filebox => SuisseID Java SDK

4. Remote Access Services
    1. OpenSSH
        1. Windows
        2. OS X
        3. Linux
        4. Schlüssel-Revokation

    1. OpenVPN => bereits zertifikatsbasiert, kein Problem

    2. Subversion => SSH basiert

5. Spezielle Zugänge
    1. Abacus vi / Abaweb => bereits SuisseID-tauglich
    2. Mehrwertsteuer-Abrechnung (SuisseTax) => eingestellt

Migrationsuntersuchung (Signatur)

Digitales Signieren

1. E-Mail-Signatur

2. Offerten, Berichte und Verträge
   1. Einzelsignatur
   2. Multisignatur
   3. Zertifizierung
   4. Problem Medienbruch

Migrationsuntersuchung (Verschl.)

Verschlüsselung

1. Festplattenverschlüsselung
   1. PKCS#11-Unterstützung fehlt
   2. Private Key des Verschlüsselungsschlüssels der SuisseID nicht nutzbar

2. Dateibasierte und E-Mail-Verschlüsselung
   1. Nur mit Softtoken (QuoVadis)

Versuch: «Verschlüsselung trotz Hinternissen»

Migrationsuntersuchung (BCM)

Backup-Prozesse

Business-Continuity

- Vollständiger Ausfall (Verlust, Diebstahl etc.)
- Vergessen des PINs
- Ablauf der Gültigkeit

Vergleiche PKI vs. SuisseID

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Technische Machbarkeit (Auth.)

Kategorie	Details	Ohne PKI	Eigene PKI	SuisseID / ext. PKI
Betriebssystem	Windows	Ja, Benutzername und Passwort oder Fingerprint	Möglich	Möglich
	Mac	Ja, Benutzername und Passwort oder Fingerprint	Möglich	Möglich
Webbasierte Authentisierung	CSNC-Wiki	Nicht möglich	Möglich	Möglich
	Projectile	Möglich	Nicht möglich, aber via SSL lösbar	Nicht möglich, aber via SSL lösbar
	SBB-Portal	Möglich	Nicht möglich	Nicht möglich
	Swisscom-Login	Möglich	Nicht möglich	Nicht möglich
	Social Media	Möglich	Teilweise via Clavid-IDP möglich	Teilweise via Clavid-IDP möglich
	Hacking-Lab	Möglich	Nicht möglich	Lösbar
	Filebox	Möglich	Nicht möglich	Lösbar
Remote-Access	OpenSSH	Möglich	Möglich	Möglich
	OpenVPN	Nicht sinnvoll möglich	Möglich	Möglich
	Subversion	Möglich	Möglich	Möglich

Technische Machbarkeit (2)

Kategorie	Details	Ohne PKI	Eigene PKI	SuisseID / ext. PKI
E-Mails	Outlook / Mac Mail	Nicht möglich	Nicht möglich	Möglich
Dokumente	SwissSigner	Nicht möglich	Nicht möglich	Möglich

Tabelle 6: Technische Machbarkeit der Signierung

Kategorie	Details	Ohne PKI	Eigene PKI	SuisseID / ext. PKI
E-Mails	Outlook / Mac Mail	Nicht möglich	Nicht möglich	Nicht möglich, nur mit Softtoken
Festplatte	PGP WDE / FileVault	Nicht möglich	Möglich (Win)	Nicht möglich, nur mit Softtoken (Win)
Dateien	PGP Desktop	Nicht möglich	Möglich	Nicht möglich, nur mit Softtoken
Backup		N/A	Möglich	Nicht möglich, nur mit Softtoken

Tabelle 7: Technische Machbarkeit der Verschlüsselung

Benutzerfreundlichkeit (Auth.)

Kategorie	Details	Ohne PKI	Eigene PKI	SuisseID / ext. PKI
Betriebs-system	Windows	2	3	3
	Mac	2	3	3
Webbasierte Authentisierung	CSNC-Wiki	2	3	3
	Projectile	2	2 (Autorisierung weiterhin via PJT)	2 (Autorisierung weiterhin via PJT)
	SBB-Portal	2	N/A	N/A
	Swisscom-Login	2	N/A	N/A
	Social Media	1	2	2
	Hacking-Lab	2	N/A	3
	Filebox	2	N/A	3
Remote-Access	OpenSSH	2	3	3
	OpenVPN	N/A	3	3
	Subversion	2	3	3

Benutzerfreundlichkeit (2)

Kategorie	Details	Ohne PKI	Eigene PKI	SuisseID / ext. PKI
E-Mails	Outlook & Mac Mail	N/A	N/A	2 / 3
Dokumente	SwissSigner	N/A	N/A	2

Tabelle 9: Benutzerfreundlichkeit des Signierens

Kategorie	Details	Ohne PKI	Eigene PKI	SuisseID / ext. PKI
E-Mails	Outlook / Mac Mail	N/A	N/A	3 (mit Softtoken)
Festplatte	PGP WDE / FileVault	N/A	3	2 (mit Softtoken)
Dateien	PGP Desktop	N/A	3	2 (mit Softtoken)
Backup		N/A	2	2 (mit Softtoken)

Tabelle 10: Benutzerfreundlichkeit des Verschlüsselns

Sicherheitsniveau (Auth.)

Kategorie	Details	Ohne PKI	Eigene PKI	SuisseID / ext. PKI
Betriebssystem	Windows	1	2	2
	Mac	1	2	2
Webbasierte Authentisierung	CSNC-Wiki	1	2	2
	Projectile	1	3	3
	SBB-Portal	1	N/A	N/A
	Swisscom-Login	1	N/A	N/A
	Social Media	1	N/A	2
	Hacking-Lab	1	N/A	2
	Filebox	2	N/A	3
Remote-Access	OpenSSH	1	2	2
	OpenVPN	N/A	2	2
	Subversion	1	2	2

Sicherheitsniveau (2)

Kategorie	Details	Ohne PKI	Eigene PKI	SuisseID / ext. PKI
E-Mails	Outlook / Mac Mail	N/A	N/A	3
Dokumente	SwissSigner	N/A	N/A	3

Tabelle 12: Sicherheitsniveau des Signierens

Kategorie	Details	Ohne PKI	Eigene PKI	SuisseID / ext. PKI
E-Mails	Outlook / Mac Mail	N/A	N/A	3 (mit Token)
Festplatte	PGP WDE / FileVault	N/A	3 (mit Token)	3 (mit Token)
Dateien	PGP Desktop	N/A	3 (mit Token)	3 (mit Token)

Tabelle 13: Sicherheitsniveau des Verschlüsselns

Fazit / Ergebnisse

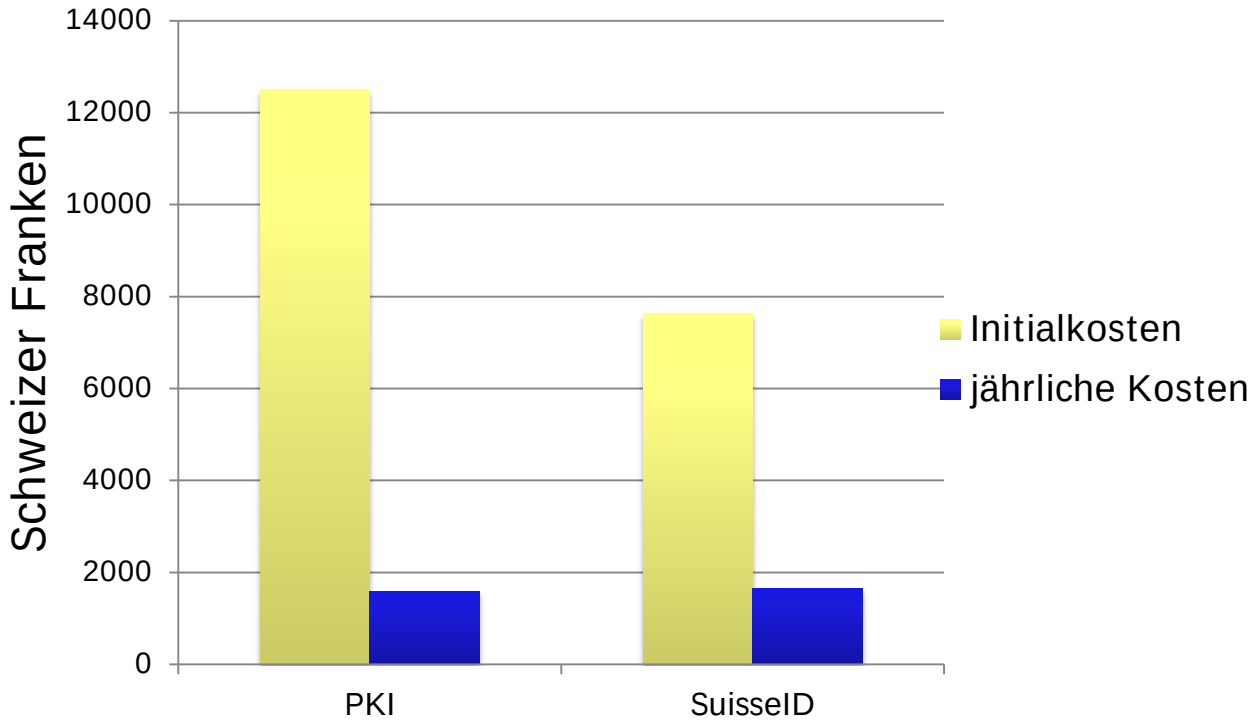
Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Fazit / Ergebnisse

Kosten und Aufwände

- PKI in der Anschaffung teurer, SuisseID im Betrieb
- Kosten SuisseID steigen mit Anzahl Mitarbeiter



Fazit / Ergebnisse (2)

Neue Risiken und Chancen

- Rechtlich gültiges Signieren nur mit SuisseID
- Verschlüsselung mit SuisseID nur über Umwege (Softtoken)
- Angriff auf PC mit Malware möglich => Klasse-3-Leser
- Business Continuity problematisch
- KnowHow auch bei SuisseID erforderlich, zur Anbindung der Dienste

Fazit / Ergebnisse (3)

Notwendige Schritte zur Lösung offener Probleme

- Verschlüsselung mittels HSM
- Kosten zu hoch bei grossen Stückzahlen
- SuisseID-Unterstützung externer Portale

Fragen und Antworten

Mein Dank gilt allen, die mich bei der Erstellung dieser Masterarbeit unterstützt haben, insbesondere Walter Sprenger, Armand Portmann, Marc Fischer, Roger Blum, Corsin Camichel, Lisa Meike Rüppel, Rebecca Gross und Paul Kalkbrenner.

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Manche Sachen muss man nicht testen.

Andere schon.

Appendix

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Verschlüsselungs-Versuche

Schlüssel vorhanden, aber nicht benutzbar?

```
# pkcs15-tool -D | grep -A8 "Public RSA Key \[SwissSign_dataEnc"
Using reader with a card: ACS ACR38U-CCID 00 00
Public RSA Key [SwissSign_dataEnc                ]
        Object Flags   : [0x2], modifiable
        Usage          : [0x51], encrypt, wrap, verify
        Access Flags   : [0x10], local
        ModLength      : 2048
        Key ref        : -1
        Native         : no
        Path           : 3f00501550754b03
        ID             : 17e6264ab81d8bf29eccd7786dcb58c6d20ccdcb

# pkcs15-tool -r 17e6264ab81d8bf29eccd7786dcb58c6d20ccdcb
Using reader with a card: ACS ACR38U-CCID 00 00
Certificate with ID '17e6264ab81d8bf29eccd7786dcb58c6d20ccdcb' not found.
```

Export generiert PKCS#8-**Format ...**

```
$ certtool --pubkey-info --load-pubkey SwissSign_dataEnc.pubkey -d 2
Setting log level to 2
|<2>| p11: loaded provider 'gnome-keyring-module' with 0 slots
Loading certificate list...
|<2>| ASSERT: mpi.c:58
|<2>| ASSERT: mpi.c:255
|<2>| ASSERT: gnutls_pubkey.c:731
certtool: importing --load-pubkey: SwissSign_dataEnc.pubkey: ASN1 parser: Error
in TAG.
```

Verschlüsselungsversuche (2)

OpenSSH-Konvertierung als Lösung?

```
$ ssh-keygen -f SwissSign_dataEnc.sshpub -e -m PEM > SwissSign_dataEnc.pubkey2
$ cat SwissSign_dataEnc.pubkey2
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAhAQhMH29zPCdgnMJSsTlbtLz0vvyW6iWvd2zuGrdsPR4donwit8T
ui0sOgl0JlMndGBtS4DMw0R3/1aJ0iHM2ZxU5ZEH9voh4h+Hy4zHp80K/iKCh+S0
g8FCm66KGKgOYYE1juHug2jHur6YARXe65oBdMKHRrvwdPJyvT08eMYrkTel1niB
88ShYIn+dkRbBUDjex+H29vzLXkqtRaYnqADV40GPRGq89PpZPBshK/mT7opxmfx
zcPsbLhXYPKYyMwTTabago2I61Q49bPv+wLxYBjkovGeWBtma3W4qvc6ofFgRena
KZkgkCRIUlPNMp5tTPJE4LPUdyweUtzIMwIDAQAB
-----END RSA PUBLIC KEY-----
```

```
$ openssl asn1parse -in SwissSign_dataEnc.pubkey2
    0:d=0  hl=4 l= 266 cons: SEQUENCE
    4:d=1  hl=4 l= 257 prim: INTEGER
:840421307DBDCCF09D8273094AC4E56ED2F3D2FBF25BA896BDDDB3B86ADDB0F4787689F08ADF13BA
2D2C3A097426532774606D4B80CCC34477FF5689D221CCD99C54E59107F6FA21E21F87CB8CC7A7CD0
AFE228287E4B483C1429BAE8A18A80E6181358EE1EE8368C7BABE980115DEEB9A0174C28746BBF074
F272BD3D3C78C62B9137A5D67881F3C4A16089FE76445B0540E37B1F87DBDBF32D792AB516989EA00
3578D063D11AAF3D3E964F06C84AFE64FBA29C667F1CDC3EC6CB85760F298C8CC134DA6DA828D88EB
5438F5B3EFFB02F16018E4A2F19E581B666B75B8AAF73AA1F16045E9DA2999209024485253CD329E6
D4CF244E0B3D4772C1E52DCC833
  265:d=1  hl=2 l=   3 prim: INTEGER           :010001
```

```
$ openssl rsautl -in sig -verify -asn1parse -inkey SwissSign_dataEnc.pubkey2 -
pubin
unable to load Public Key
```

Verschlüsselungsversuche (3)

OpenSSL-Ansatz

```
OpenSSL> rsautl -decrypt -engine pkcs11 -inkey slot_0-
b6efd1c9c5da0d4b70e18b580bd22757d53d79aa -keyform engine -in cipher.txt -out
deciphered.txt
engine "pkcs11" set.
PKCS#11 token PIN:
key not found.
PKCS11_get_private_key returned NULL
cannot load Private Key from engine
3073407176:error:26096080:engine routines:ENGINE_load_private_key:failed loading
private key:eng_pkey.c:126:
unable to load Private Key
error in rsautl
```

Deliverables

Nr.	Frage / Punkt	Erklärung	Ja	Noch nicht
1.	Business-Continuity-Plan vorhanden?	Bei Ausfall der SuisseID muss ein BCM-Plan existieren, so dass MA weiterhin arbeiten können.		
2.	Angestrebtes Sicherheitsniveau im Unternehmen definiert?	Entscheidet über den Einsatz von Klasse-1- oder Klasse-3-Kartenlesern.		
3.	Verschlüsselungsproblematik relevant für das Unternehmen und entsprechend adressiert?	Mit der SuisseID kann nicht verschlüsselt und alternative Konzepte müssen gefunden werden.		
4.	Anzubindende Dienste für die Smartcard-basierte Authentisierung definiert?	Welche Dienste sollen via Smartcard zugänglich sein?		
5.	Anzubindende Dienste für das Smartcard-basierte Signieren definiert?	Welche Dokumente sollen via SuisseID signiert werden? Wer erhält diese Ermächtigung? Werden E-Mails ebenfalls immer signiert?		
6.	Kann das Knowhow zur Anbindung der SuisseID in die technischen Unternehmensprozesse bereitgestellt werden?	Die technische Anbindung zur Smartcard-Authentisierung- und Signierung ist nicht trivial und muss durch Spezialisten durchgeführt und gepflegt werden.