Bulk strategies for qualified electronic signatures and time stamps

Detlef Hühnlein
secunet Security Networks AG

Developers Track [DEV-301]
Thursday, February 26th 2004

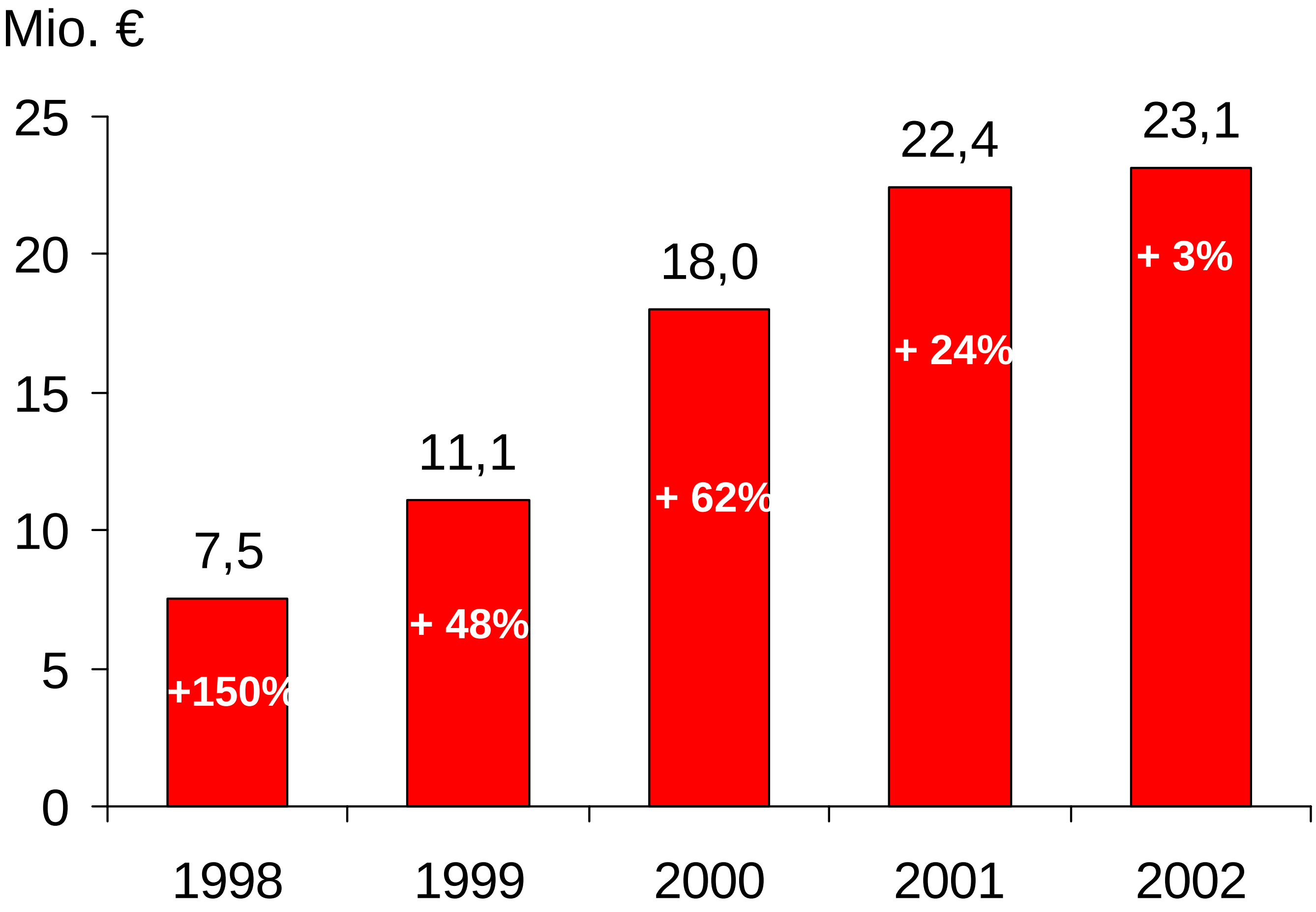
Agenda

- **Introduction**
- Background
  - Electronic signatures and time stamps in Europe
  - The need for bulk strategies
- Electronic signatures
- Time stamps
- Further applications
- Conclusion

secunet Security Networks AG

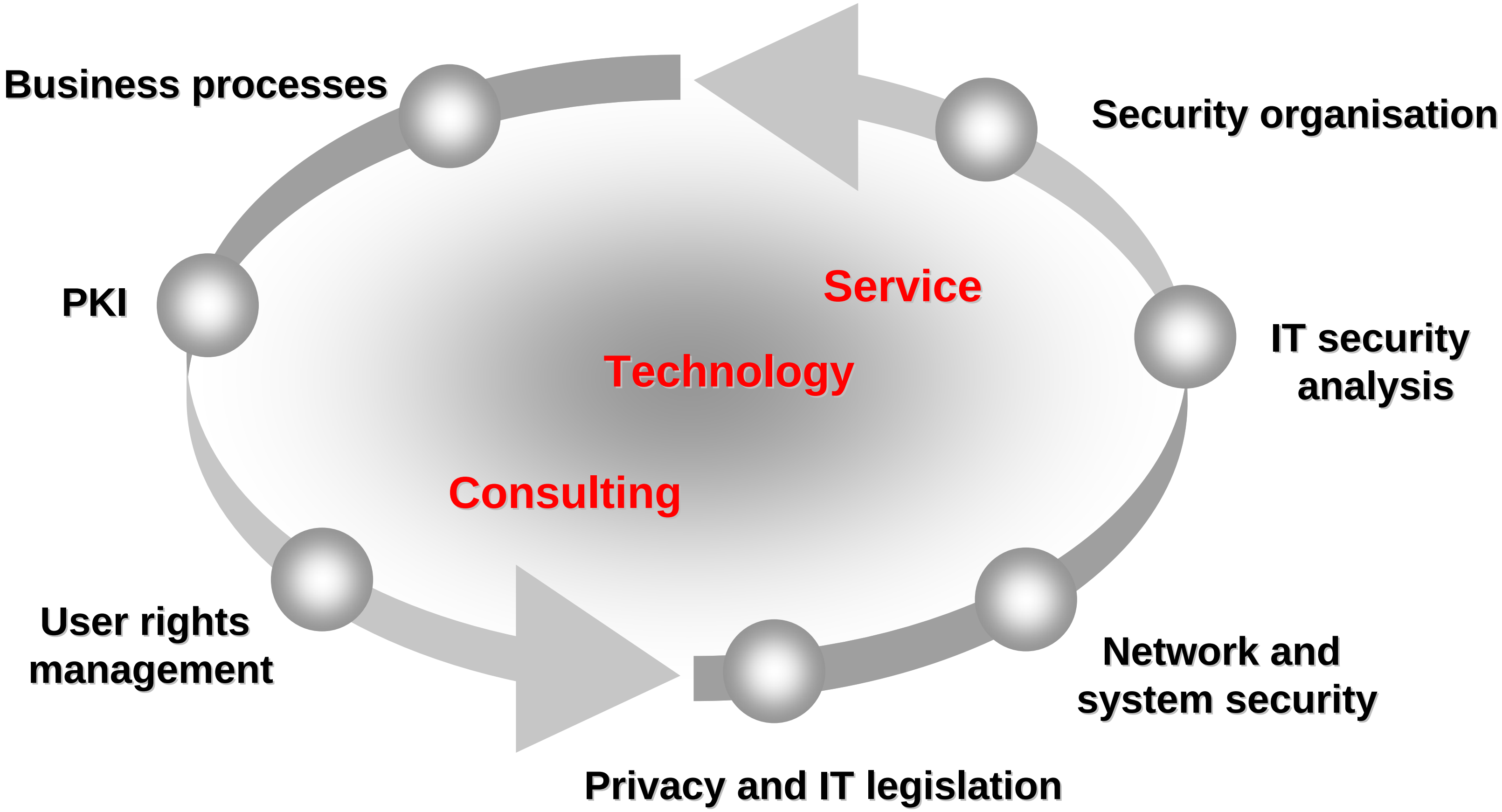
- founded in Dec 1996
- IPO: Nov 9, 1999
- shareholders:
  - Giesecke & Devrient (47%)
  - RWTÜV AG (30%)
  - Free float (23%)
- turnover in 2002: 23,1 Mio. € (+ Secartis)
- 180 employees (+ Secartis)

Turnover

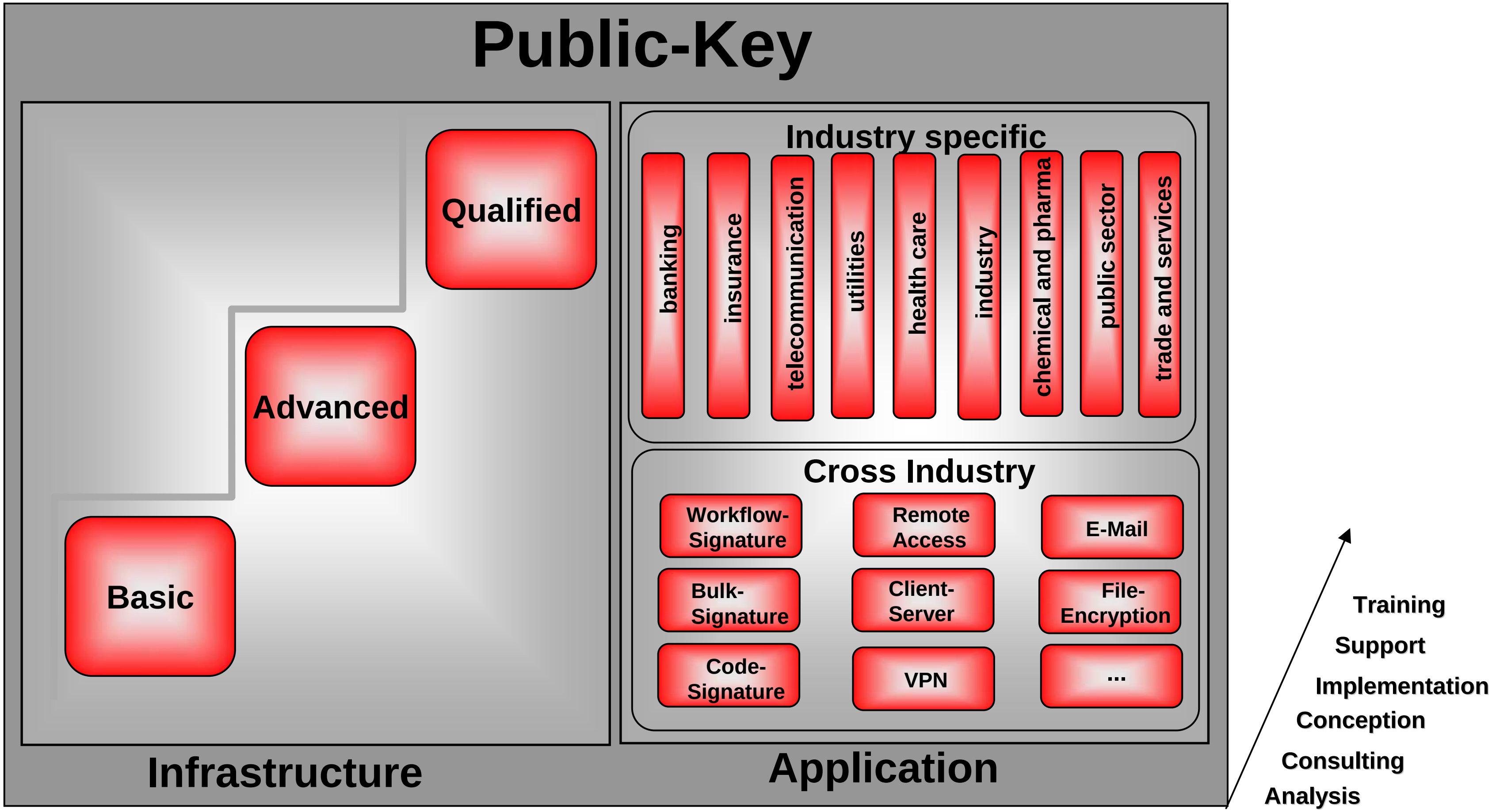


Mio. €
25
20
15
10
5
0
7,5
+150%
11,1
+ 48%
18,0
+ 62%
22,4
+ 24%
23,1
+ 3%
1998
1999
2000
2001
2002

secunet Portfolio



PKI-Portfolio



Public-Key

Qualified

Advanced

Basic

Infrastructure

Industry specific

banking

insurance

telecommunication

utilities

health care

industry

chemical and pharma

public sector

trade and services

Cross Industry

Workflow-Signature

Remote Access

E-Mail

Bulk-Signature

Client-Server

File-Encryption

Code-Signature

VPN

...

Application

Training

Support

Implementation

Conception

Consulting

Analysis

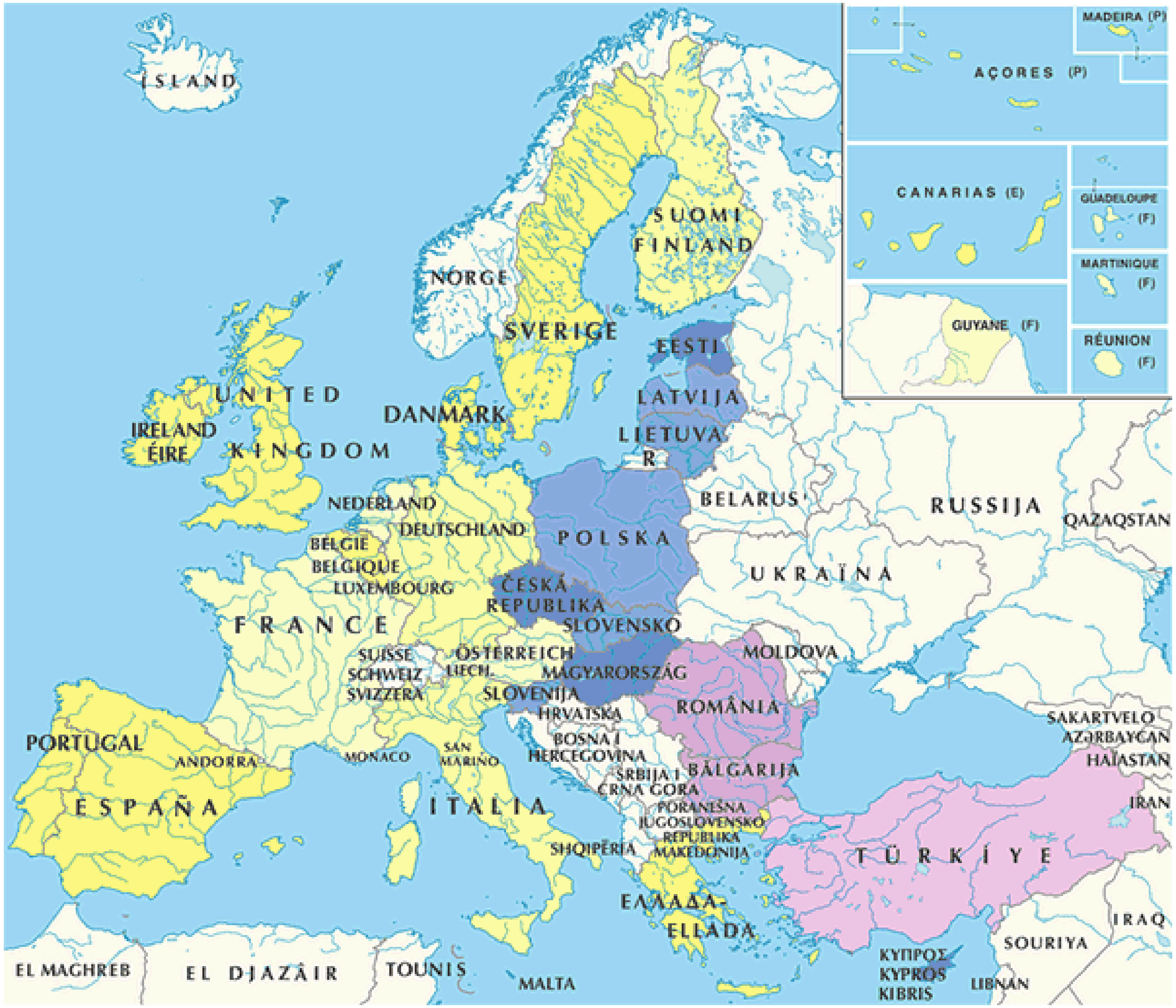
PKI Highlights

- More than 300 successful PKI-related projects
- Implementation of infrastructures of all (22) accredited CSPs issuing qualified certificates and times stamps in Germany
- Specification of Greek accreditation and supervision scheme for CSPs issuing qualified certificates
- MultiSign solution family for electronic (bulk) signatures
- SINAVPN solution family for highly secure communication
  - BSI-Approval for „STRENG GEHEIM“ (TOP SECRET)
  - Application in all (>200) German embassies

Agenda

- Introduction
- **Background**
  - **Electronic signatures and time stamps in Europe**
  - The need for bulk strategies
- Electronic signatures
- Time stamps
- Further applications
- Conclusion

Europe


ÍSLAND
NORGE
SVERIGE
SUOMI
FINLAND
EESTI
LATVIJA
LIETUVA
R
DANMARK
UNITED
KINGDOM
IRELAND
ÉIRE
NEDERLAND
BELGIE
BELGIQUE
LUXEMBOURG
DEUTSCHLAND
POLSKA
ČESKÁ REPUBLIKA
SLOVENSKO
BELARUS
RUSSIJA
QAZAQSTAN
UKRAÏNA
MOLDOVA
FRANCE
SUISSE
SCHWEIZ
SVIZZERA
LIECH.
ÖSTERREICH
MAGYARORSZÁG
SLOVENIJA
HRVATSKA
ROMÂNIA
BOSNA I HERCEGOVINA
SRBIJA I CRNA GORA
BĂLGARIJA
PORTUGAL
ANDORRA
ESPAÑA
MONACO
SAN MARINO
ITALIA
PORANEŠNA JUGOSLOVENSKO REPUBLIKA MAKEDONIJA
SHQIPËRIA
ΕΛΛΑΔΑ-ELLADA
TÜRKİYE
SAKARTVELO
AZƏRBAYCAN
HAÏASTAN
IRAN
IRAQ
SOURIYA
ΚΥΠΡΟΣ
KYPROS
KIBRIS
LIBNAN
EL MAGHREB
EL DJAZÂIR
TOUNIS
MALTA
MADEIRA (P)
AÇORES (P)
CANARIAS (E)
GUADELOUPE (F)
MARTINIQUE (F)
GUYANE (F)
RÉUNION (F)

Electronic signatures in Europe

- 1997 – First laws on electronic signatures (Italy, Germany)
- 1999 – Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
- 2001 – Implementation into national law until July 19th 2001
- Today – 15 different signature laws implementing 1999/93/EC
- Tomorrow – (at least) 10 more to come

1999/93/EC

- Defines
  - (advanced) electronic signature
  - (qualified) certificate
  - (secure) signature-creation device
- „Qualified electronic signatures“
  - are advanced electronic signatures, which are based on a qualified certificate (QC) and created by a secure-signature-creation device (SSCD)
  - are deemed equivalent to handwritten signatures (Art. 5 1. (a))

Advanced electronic signatures

- Electronic signature
  - Means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication

- Advanced electronic signature is an electronic signature, which
  - Is uniquely linked to the signatory
  - Is capable of identifying the signatory
  - Is created using means the signatory can maintain under his sole control
  - Is linked to the data to which it relates such that any subsequent change of the data is detectable

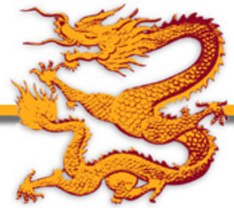
Qualified certificate

- is a certificate which meets the requirements of 1999/93/EC Annex I
  - Qualified certificate profile is specified in RFC 3039 and ETSI TS 101 862
- and is issued by certification-service-provider which meets the requirements of 1999/93/EC Annex II
  - CEN CWA 14167: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures
    - Part 1: System Security Requirements
    - Part 2: Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)
  - Policy requirements for certification authorities issuing qualified certificates are specified in ETSI TS 101 456
  - Conformity assessment of CSPs is adressed in CEN CWA 14172

Secure Signature Creation Device

- Must
  - satisfy the requirements of 1999/93/EC Annex III
  - Ensure that signature keys are unique
  - Ensure that signature forgeries are not possible
  - Ensure the secrecy of the signature keys
    - Protection against the use of others
    - Protection against the signatory (!)
- CEN CWA 14169 – Secure Signature-Creation Devices with CC EALevel 4+, where the augmentation „+“ is defined in Section 4.5
  - Strength of functions is high
  - Vulnerability assessment
    - AVA_MSU.3 (analysis and testing of insecure states)
    - AVA_VLA.4 (highly resistant)

Time Stamps



- Not explicitely adressed by 1999/93/EC, but
  - requirement for CSP issuing qualified certificates to „ensure that the date and time when a certificate is issued or revoked can be determined precisely“ (Annex II (c))
  - definitions in national signature laws, like §2 Nr. 14 SigG (German Signature Act) for example:
    - A „Qualified Time Stamp“ is an electronic attestation of a CSP, meeting the requirements of SigG, that certain electronic data were presented to it at a certain point in time.
- Standardized in
  - RFC 3161 – Time Stamping Protocol
  - ETSI TS 101 861 – Time Stamping Profile
  - ETSI TS 102 023 – Policy Requirements for Time-Stamping Authorities

Agenda

- Introduction
- **Background**
  - — Electronic signatures and time stamps in Europe
  - — **The need for bulk strategies**
- Electronic signatures
- Time stamps
- Further applications
- Conclusion

Some use cases in Germany

- Qualified electronic signatures
  - Official notices which require the written form (e.g. notice of assessment (§157 AO))
  - Electronic archiving of records for social insurance organisations (§36 SRVwV)
  - Electronic invoices (§14 UStG)
- Qualified time stamps
  - Re-signing qualified electronic signatures (§17 SigV)
  - ...

Millions of signatures / time stamps

How about using HSMs?

- Chrysalis Luna® CA3 version 3.97
  - Common Criteria EAL 4+
  - Augmentation „+“ is ALC_FLR.2 (Flaw Reporting Procedures)
- SSCD requires „+“ to be
  - Strength of functions is high
  - Vulnerability assessment
    - AVA_MSU.3 (analysis and testing of insecure states)
    - AVA_VLA.4   (highly resistant)

Currently SSCD = Smart Card

Agenda

- Introduction
- Background
  - Electronic signatures and time stamps in Europe
  - The need for bulk strategies
- **Electronic signatures**
- Time stamps
- Further applications
- Conclusion

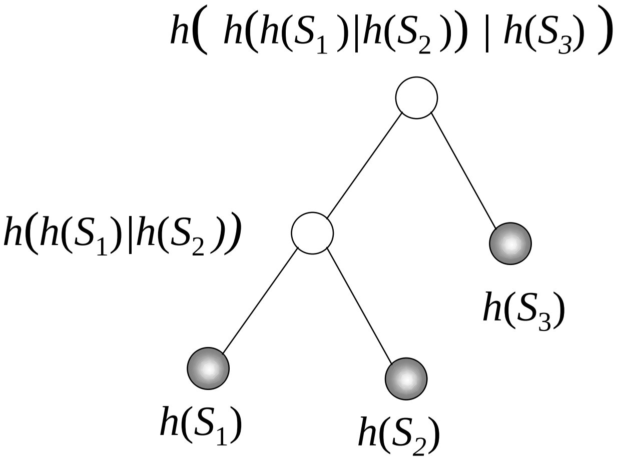
Bulk strategy – Parallelization

- Benchmark
  - TCOS 2.0 cards
  - 200k data
  - Directory polling interface
  - PKCS#7 signatures

# SSCDs	Sig. / min.	Sig. / day	Ideal / day
1	46	66.240	66.240
2	79	113.760	132.480
4	132	190.080	264.960
8	199	286.560	529.920
16	376	540.889	1.059.840
32	717	1.032.943	2.119.680
64	1.401	2.017.052	4.239.360
128	2.768	3.985.269	8.478.720
256	5.501	7.921.703	16.957.440

Bulk strategy – Batch signature

- Batch signature due to Pavlovsky / Boyd / Merkle



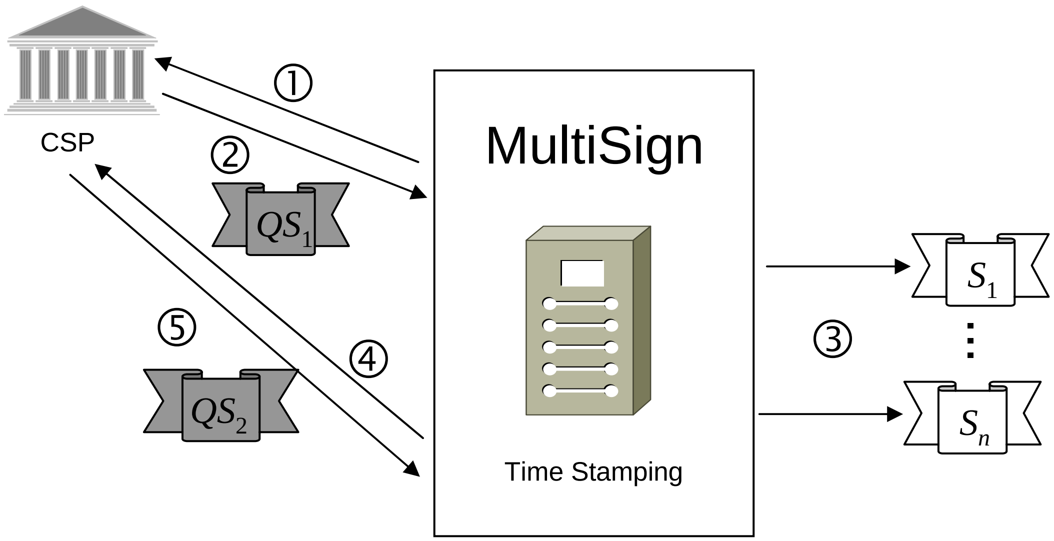
- Proposed Syntax:

```
reducedHashtree SEQUENCE OF Node
Node ::= SEQUENCE {
   direction BIT STRING {L (0), R  (1)},
   hashvalue         OCTET STRING }
```

Agenda

- Introduction
- Background
  - Electronic signatures and time stamps in Europe
  - The need for bulk strategies
- Electronic signatures
- **Time stamps**
- Further applications
- Conclusion

Interval-qualified (IQ) time stamps



① Requesting qualified time stamp via TSP (RFC3161)

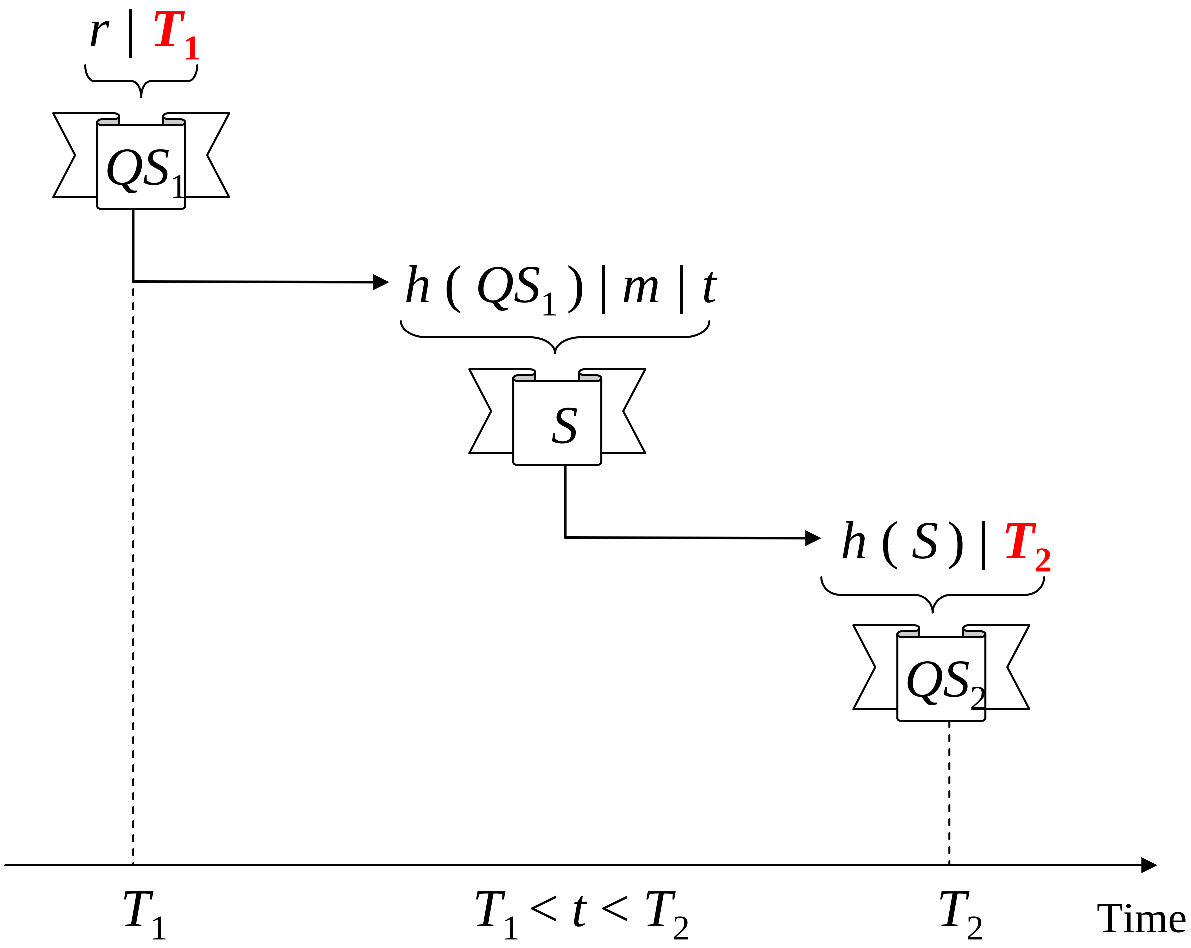
② Obtaining time stamp with time T_1

③ Creation of an arbitrary number of TSP- oder CMS-(RFC 3369) based time stamps with time t_i, such that one is able to prove that $T_1 < t_i < T_2$

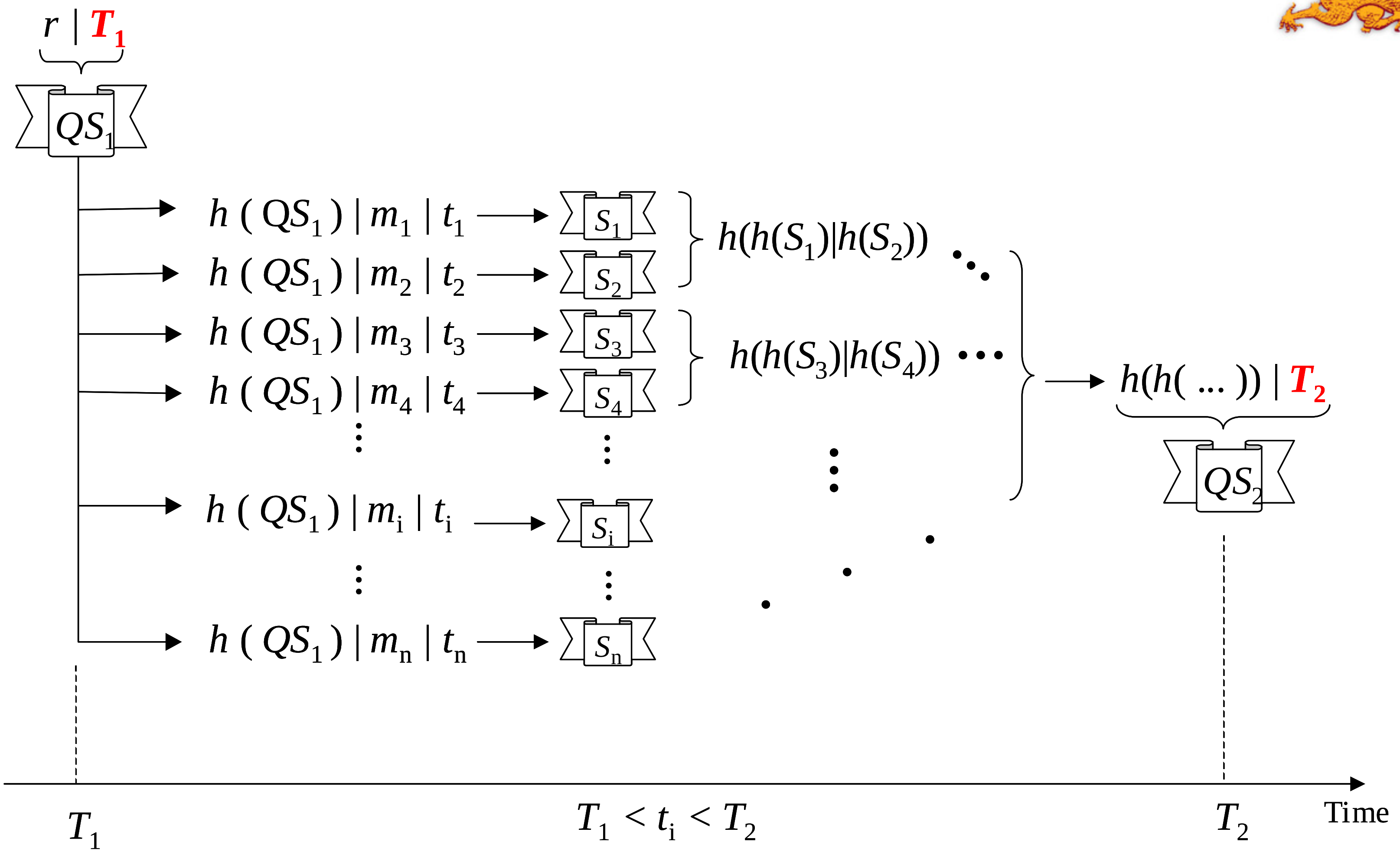
④ Requesting qualified time stamp via TSP

⑤ Obtaining qualified time stamp with time T_2

Relative temporal order



Construction of IQ time stamps



$\underbrace{r \mid T_1}$

QS_1

$h\,(QS_1) \mid m_1 \mid t_1 \longrightarrow S_1$

$h\,(QS_1) \mid m_2 \mid t_2 \longrightarrow S_2$

$h\,(QS_1) \mid m_3 \mid t_3 \longrightarrow S_3$

$h\,(QS_1) \mid m_4 \mid t_4 \longrightarrow S_4$

$h\,(QS_1) \mid m_i \mid t_i \longrightarrow S_i$

$h\,(QS_1) \mid m_n \mid t_n \longrightarrow S_n$

$h(h(S_1)|h(S_2))$

$h(h(S_3)|h(S_4))$

$\longrightarrow \underbrace{h(h(\,\dots\,)) \mid T_2}$

QS_2

T_1

$T_1 < t_i < T_2$

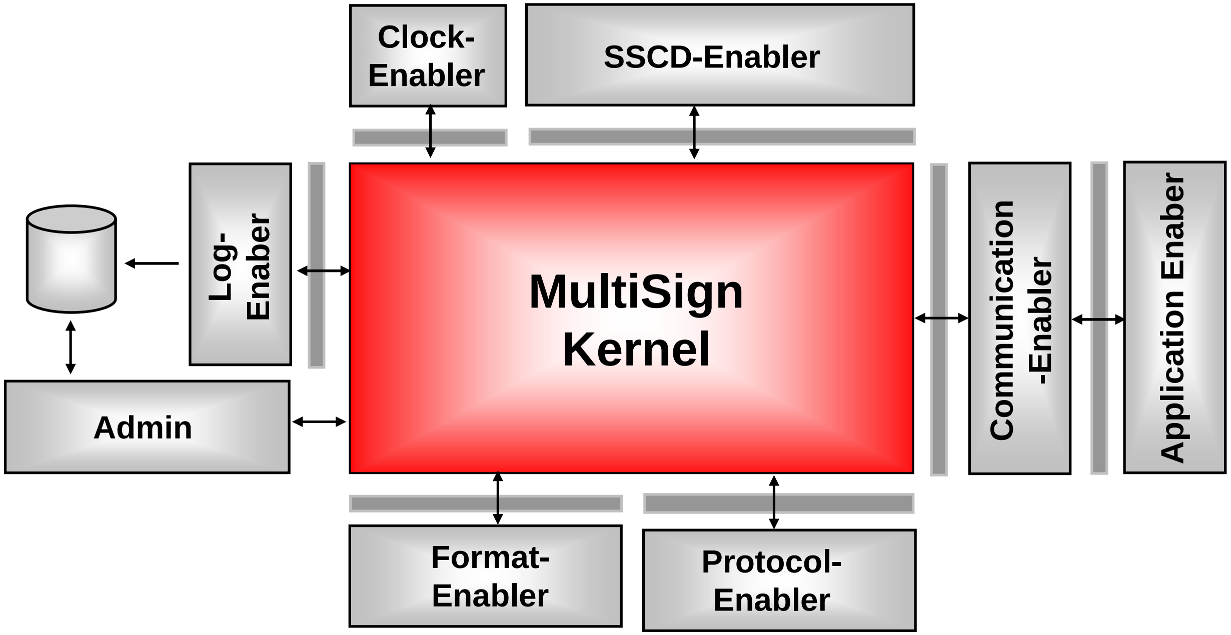
T_2

Time

Agenda

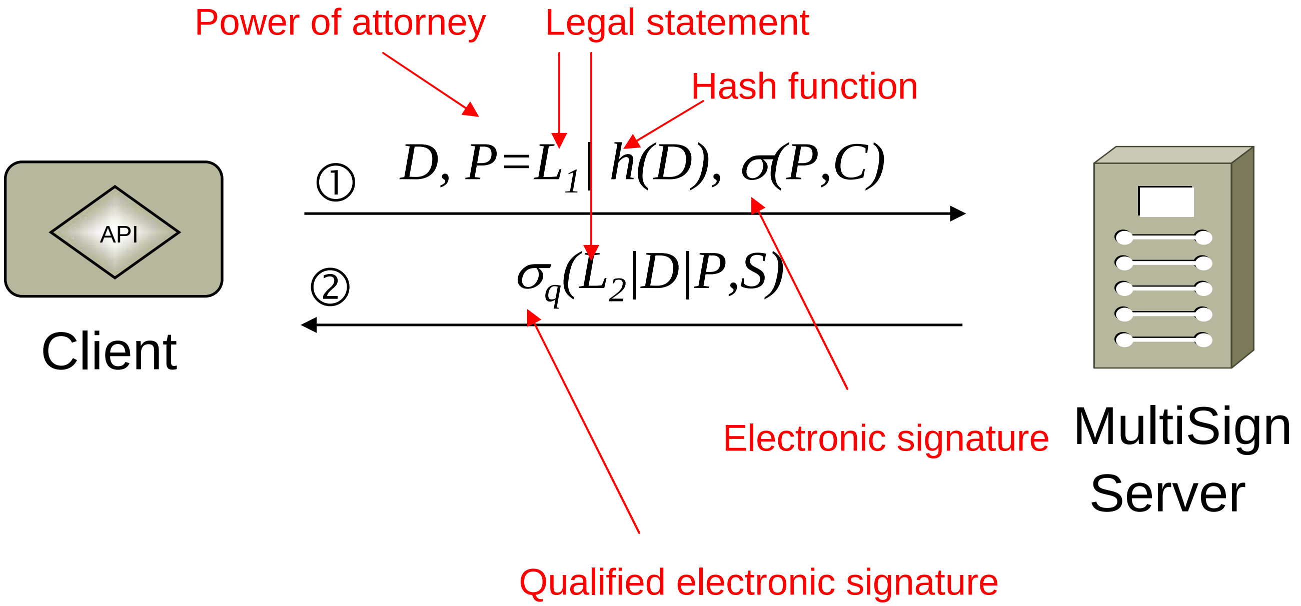
- Introduction
- Background
  - Electronic signatures and time stamps in Europe
  - The need for bulk strategies
- Electronic signatures
- Time stamps
- **Further applications**
- Conclusion

MultiSign Architecture



Empowered signatures

- Suppose that there is a Client *without* SSCD who needs to file an official document D which requires the written form



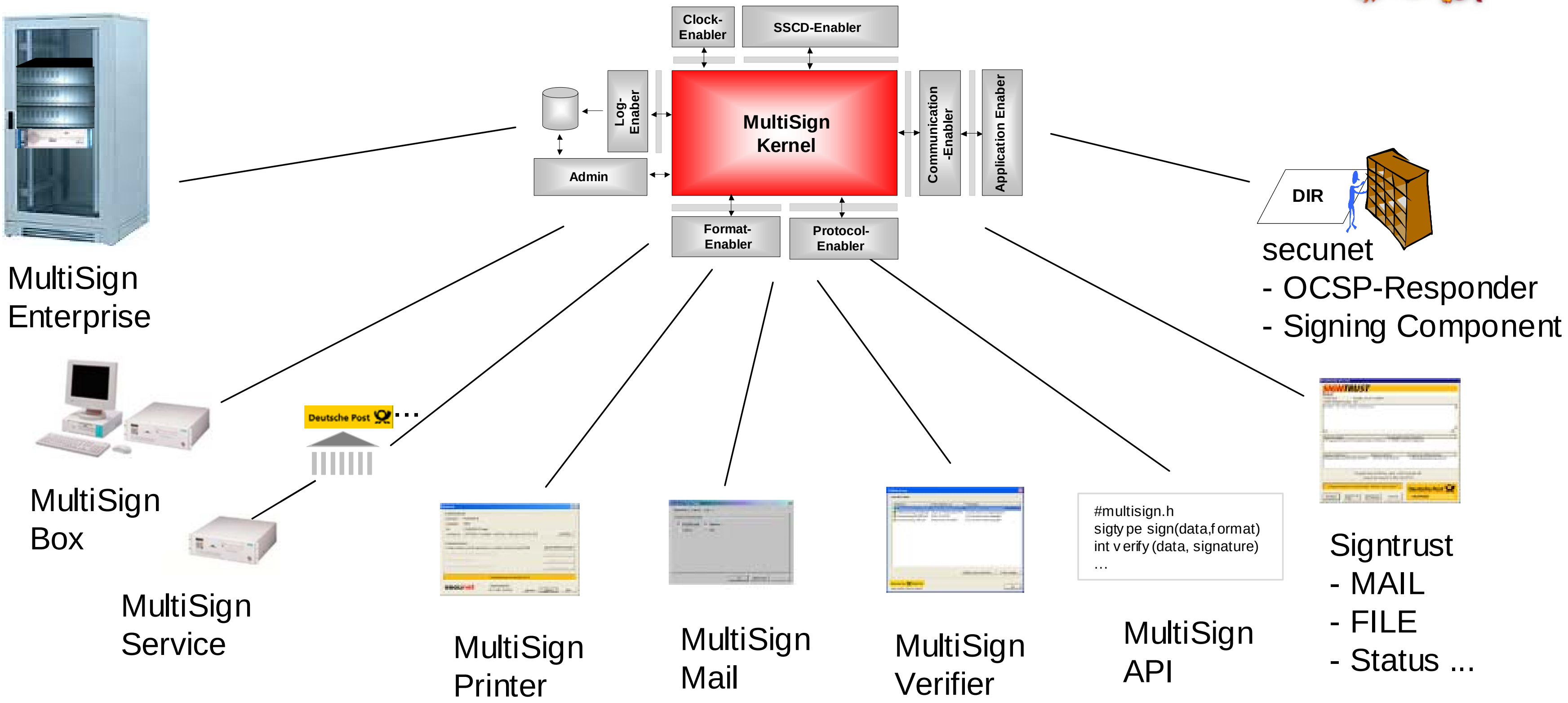
Agenda

- Introduction
- Background
  - Electronic signatures and time stamps in Europe
  - The need for bulk strategies
- Electronic signatures
- Time stamps
- Further applications
- **Conclusion**

Conclusion

- Qualified electronic signatures
  - are necessary to replace the written form
  - need SSCD and qualified certificate (QC)
- Bulk strategies for electronic signatures to cover high volumes
  - Parallelization of SSCDs
  - Batch signature approach
- Interval-qualified time stamps
- Empowered signatures for Clients without SSCD or QC

MultiSign Suite



Clock-Enabler

SSCD-Enabler

Log-Enaber

Admin

MultiSign Kernel

Communication-Enabler

Application Enaber

Format-Enabler

Protocol-Enabler

DIR

secunet
- OCSP-Responder
- Signing Component

MultiSign Enterprise

MultiSign Box

Deutsche Post …

MultiSign Service

```
#multisign.h
sigty pe sign(data,f ormat)
int v erify (data, signature)
…
```

MultiSign Printer

MultiSign Mail

MultiSign Verifier

MultiSign API

Signtrust
- MAIL
- FILE
- Status ...

Thanks for your attention!

Questions?

Detlef Hühnlein
secunet Security Networks AG
Im Teelbruch 116
45219 Essen
Germany
Tel: +49 9571 896479
Fax: +49 9571 896482
E-Mail: detlef.huehnlein@secunet.com
Internet: http://www.secunet.com