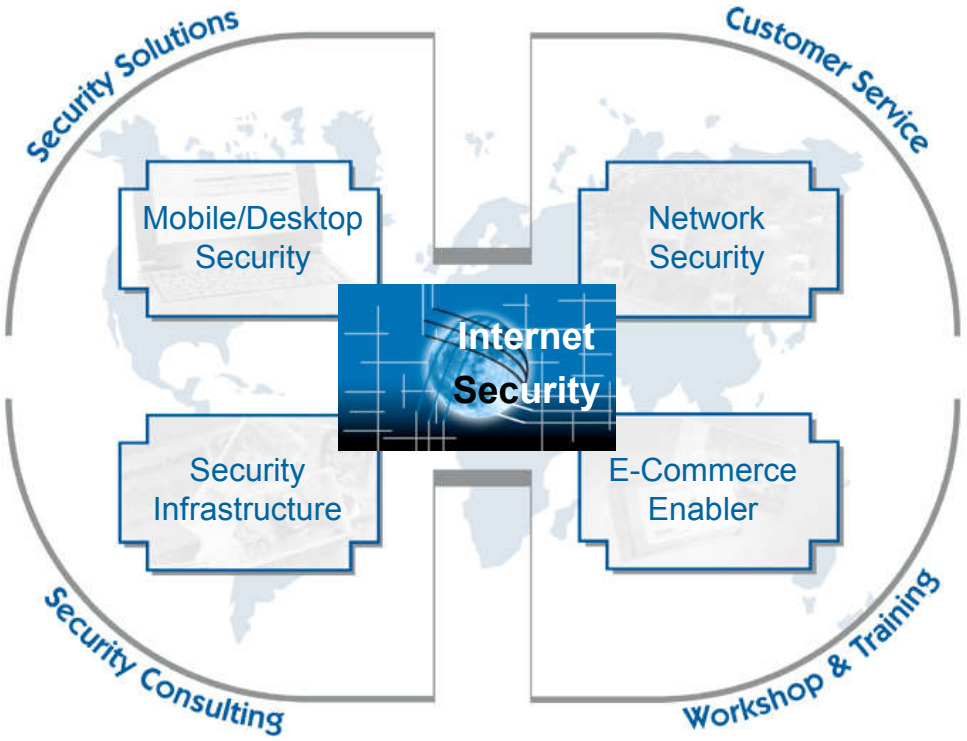
Secure E-Mail Communication in Organisations



Dipl.-Ing. Norbert Pohlmann
CMO, Utimaco Safeware AG

utimaco® safeware

Why do we need Security?

- Changes in (e-)business process
  - Information society
- Assets are available as bits and bytes (e-@ssets)
- Hackers are forcing us to protect our information
  - Hacking is considered as „sport“
  - No moral
- Data has become the most important economic good
  - This means increasing vulnerability of companies
  - Economic espionage is very lucrative

e-@ssets

E-Mail: Chances & Risks

- E-mail is the most frequently used application on the Internet
- Offers fast exchange of information for the communication partners without changing media
- Information via e-mail and their attachment could represent several mio.$
  - drafts of agreements
  - business transactions
  - merges
- Risk: information is send in plaintext

Do you know Bad Aibling?

- Bad Aibling:

- 50 km south east of Munich
- Health resort with 16.000 inhabitants
- nice view on the Tölzer mountains and the river Inn
- oldest Bavarian health resort for mud-baths

http://www.kur-online.de/indxd.htm

Do you know Bad Aibling?

- Bad Aibling:
- US Air force territory with interception station, reporting to the NSA

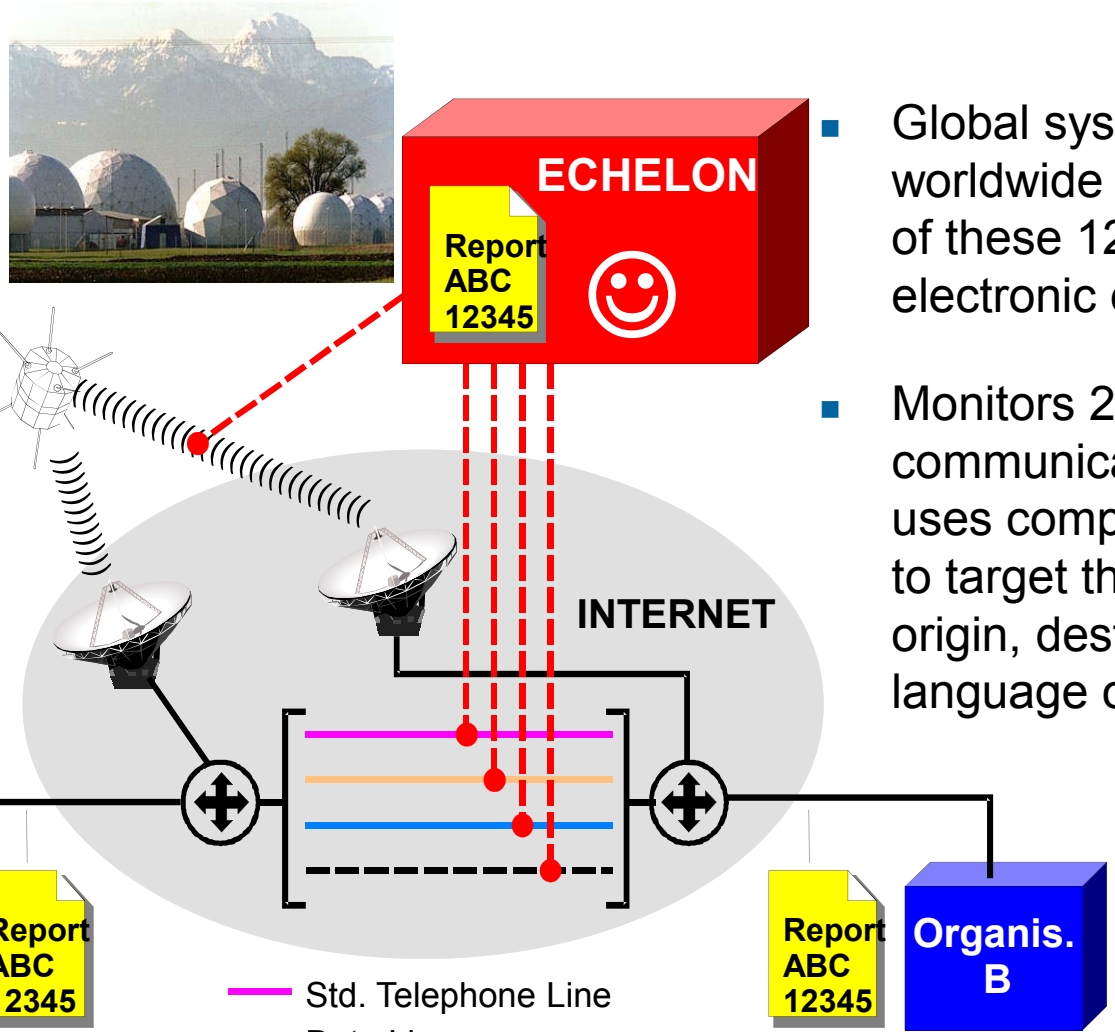
- Task of the National Security Agency: Interception and decoding of all kinds of foreign communication, which might be of interest for US security

- budget six times higher than the CIA‘s
- the world biggest employer of mathematicans

http://www.aib.de

- The „war of information“ is still on, even if you don´t see it!

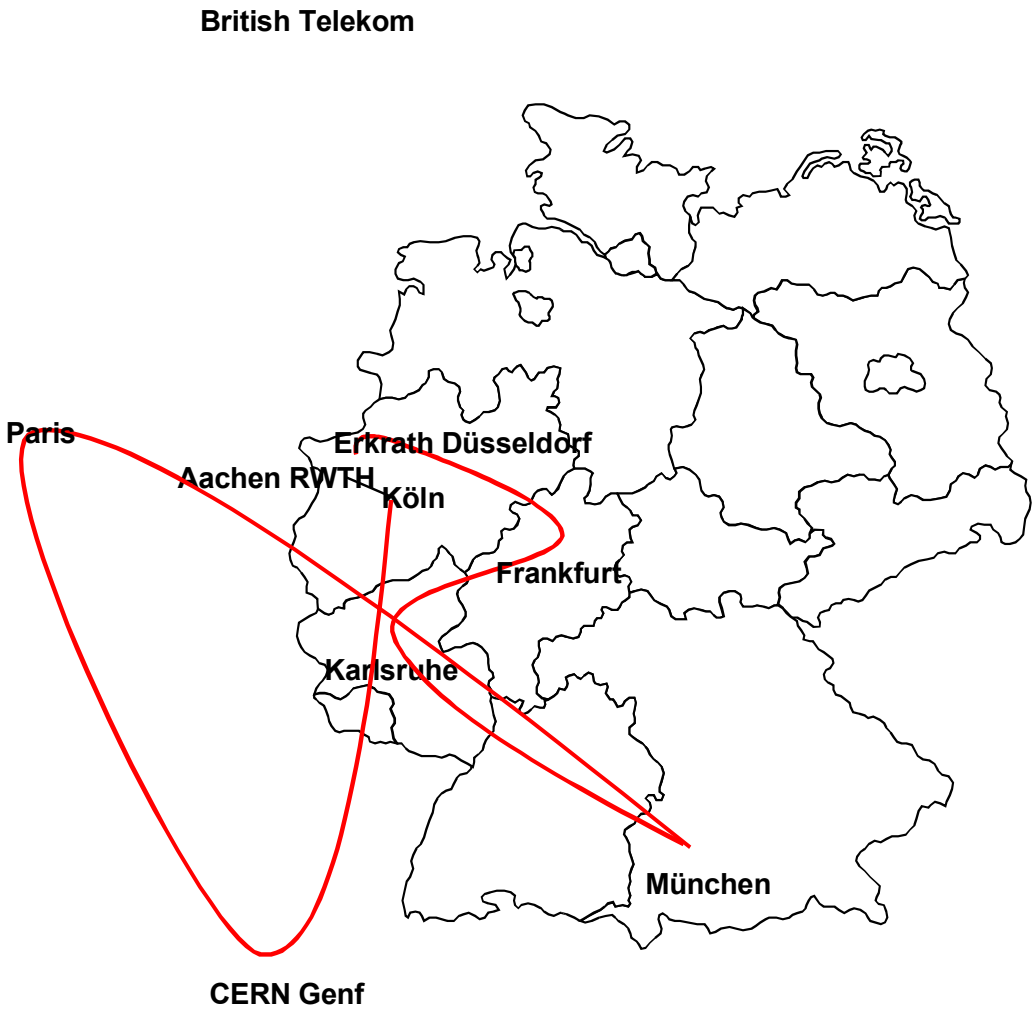
ECHELON



- Global system with worldwide stations (among of these 120 satellites) for electronic eavesdropping
- Monitors 2.000.000 communications per hour, uses computerised systems to target those of interest by origin, destination, language or key words

utimaco safeware

Path of an E-Mail



scratch

1. Router.KryptoKom.de
2. local.aachen.core.csl-gmbh.net
3. local2.erkrath.core.csl-gmbh.net
4. xip2.erkrath.core.csl-gmbh.net
5. cisco.csl-gmbh.net
6. frankfurt.core.xlink.net
7. langen.core.xlink.net
8. karlsruhe.core.xlink.net
9. muenchen.core.xlink.net
10. Munich-EBS.EBONE.NET
11. Paris-EBS2.EBONE.NET
12. Cern-EBS1.Ebone.NET
13. CH-s2.dante.bt.net
14. Ch-f0-0.eurocore.bt.net
15. DE-s1-0.eurocore.bt.net
16. De-f0-dante.bt.net
17. ipgate2.win-ip.dfn.de
18. ipgate21.win-ip.dfn.de
19. ZR-Koeln1.WiN-IP.DFN.DE
20. RWTH-Achen1.WiN-IP.DFN.DE
21. cisco-bwin.rz.rwth-aachen.de
22. informat-05.rz.RWTH-Aachen.DE
23. terpi.Informatik.RWTH-Achen.DE

E-Mail Communication: Risks

- Monitoring of e-mail in plaintext
- Smuggling in of non-authentic information
- Tampering with data
- Interruption of message flow
- Recognition of message flow

utimaco safeware

Basics of E-Mail-Security

Confidentiality	• encryption • access and rights control
Integrity	• digital signature • check sum
Authenticity	• encryption • user login • certificates
Reliability	• digital signature • certificates • timestamp
Availability	• hardware mirroring • backup of data

utimaco safeware

Conceptional E-Mail Security

utimaco safeware

Security Policy (1)

- **Analysis of communication structures**
  - Partner for e-mail communication
  - Analysis of need for secure E-Mail communication
  - Wishes of and influence on partners

- **Analysis of need for protection**
  - Definition of security classes with regard to
    - Confidentiality
    - Integrity
    - Authenticity

utimaco safeware

Examples of security classes with regard to confidentiality

Security class	Applies if	example
"low" damage potential	• Available for all • Controlled distribution • Easy to recover in case of loss	• Internal directories and rules • Statistics without strategic and data protection meaning • Company data /data for the public
"middle" damage potential	• Damage is restricted to responsibility of one organisational unit (not within the whole organisation) • General rule for customers and employees	• Data within one part of the organisation (personal data, customer data, etc.) • Host data on PCs (File-Transfer)
"high" damage potential	• Influence on all parts of the organisation • Damage to all parts of the organisation (image, etc.)	• Strategic information and financial data • Confidential personal data or customer data • agreements

Security policy (2)

- Extention of rules and regulations regarding the e-mail use for confidential documents and data
- Set-up of guidelines for e-mail exchange with regard to security classes:

Security class (damage potential)	Sending via E-Mail
„low	Possible, no encryption
„medium“	Possible, but encryption requiered
„high	Possible, but encryption requiered **Alternatively** No exchange via e-mail

Security policy (3)

- Developing a information recovery concept (message recovery, key recovery)
- User trainings
- operation instructions/ guide lines
  - handling of encryption and digital signature
  - key handling
  - case of emergency

Public Key Infrastructure

- **Policy**
  - security concepts
  - user guidelines
  - operation instruction / tasks
- **RA - Registration Authority**
  - identification (incl. registration) according to policy
- **CA - Certification Authority**
  - key generation for certification authorities
  - certification for public keys
  - personalisation of transport media for certificates, key pair etc.
  - time stamp services
  - optional generation of keys for users
- **DIR - Directory Services**
- **PKI enabled application**
  - E-mail
  - ...

utimaco safeware

Current Standards

- **Exchange format**
  - PGP
  - S/MIME
- **Certification format**
  - X.509 Version 3
- **revocation lists**
  - X.509 CRL Version 2
- **directory service**
  - LDAP Version 3

PKI-interfaces

PKIX-protocol

Token

PKCS#11

programming interface (smartcards, ...)

PKCS#12

standards for storing private keys, certificates, user information

PKCS#13

elliptic curves encryption standard (RSA)

utimaco safeware

Decision Criteria for Product Choice (1)

- **Security**
  - strong encyption
    (symmetric > **112 Bit**,
    asymmetric 768, **1024**, 2048, ... **Bit**)
  - recognized standards instead of depending on one vendors
  - danger of trap doors in software
- **Availability**
  - legal permission of local applications (export or import rights)
- **Reliability**
  - independent tests
  - established, commercial products

utimaco safeware

Decision Criteria for Product Choice(2)

- **Software-Ergonomcs**
  - easy to learn
  - simple, intuitive handling in accordance with standards
  - easy to integrate in e-Mail products
    (i.e. MS Outlook, Lotus Notes, Groupwise, ...)
  - encryption/signature speed
- **Key / certificate management**
  - X.509-certificate
  - SmartCards
  - LDAP-binding
- **Interoperability**
  - „Inhomogenity“ of communicating parties

Decision Criteria for Product Choice(3)

- **Software-Maintenance-Concepts**
  - updates (extra costs?)
  - expenditure for client updates
- **Costs**
  - investments
    - hardware
    - software
    - installation
    - trainings
  - running costs
    - administration
    - maintenance

Infrastructure

PKI

- Certificate
- Secret Key

Smartcard reader

- CardMan Family

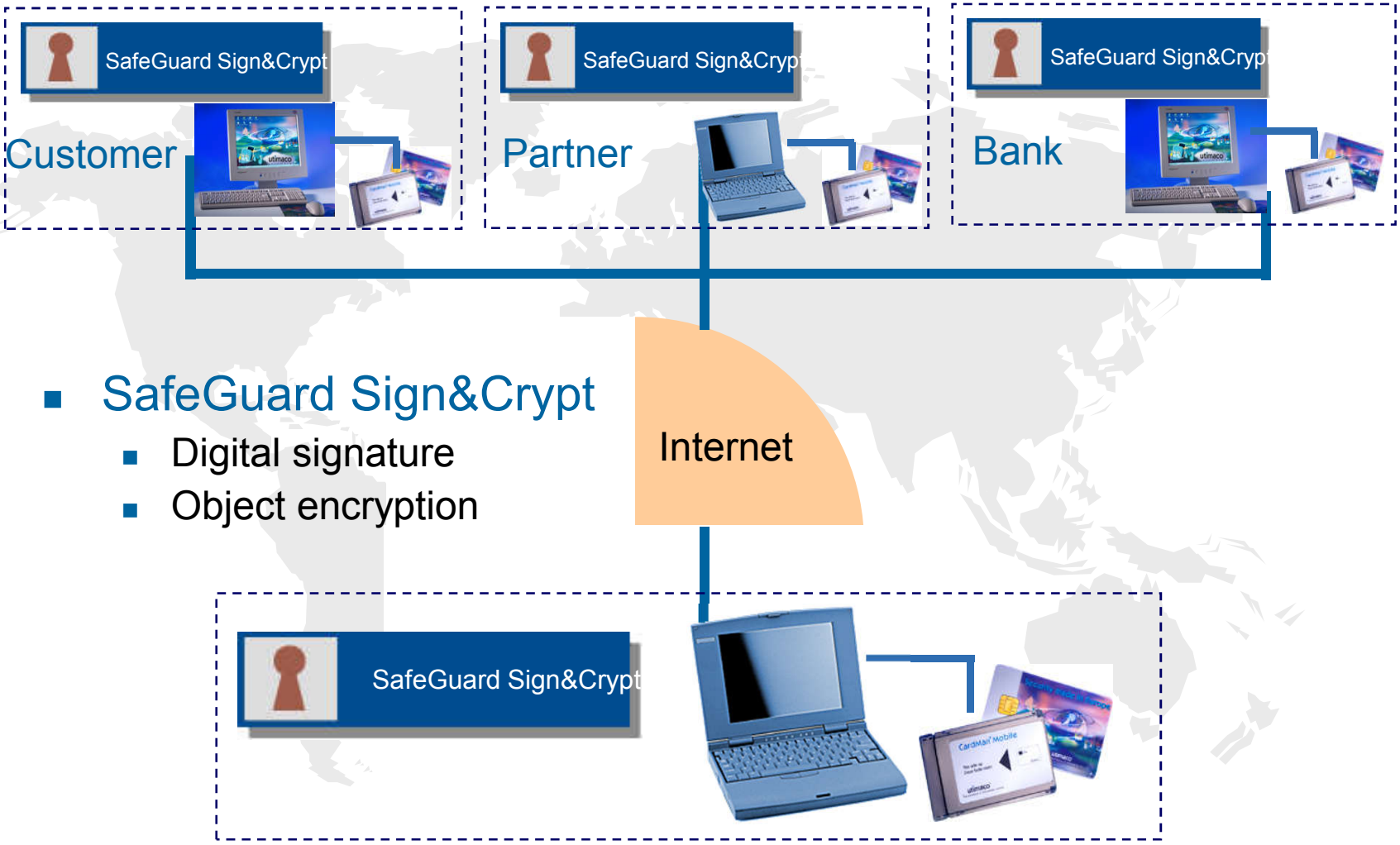
SPM

- Security Policy Manager

Security solutions for our customer

utimaco safeware

Digital Signature & E-Mail Security



- SafeGuard Sign&Crypt
  - Digital signature
  - Object encryption

Security solutions for our customer

utimaco safeware

User Awareness

- Approx. 45 % of all computer breakdowns are caused by users, their mistakes in operating or carelessness (KES 1998)
- User Trainings
  - product related trainings
  - realizing the security policy
  - awareness
- User with awareness
  - comprehend information and IT-systems as a value which needs to be protected
  - understands IT-security as a part of his task/duty and as a quality feature

Measure catalog for e-Mail security in enterprises

time

- Setting up an internal help-office
- Establish backup-processes
- User trainings
- Step-by-step concept for installation (Roll-Out)
- Training for security administrators
- Establish a useful PKI
- Product choice
- Developing a security policy

E-Mail-security - without compromises!

„You have to protect your data
from your little sister or the secret service,
everything in between doesn‘t make sense.“

Bruce Schneier

Utimaco Safeware AG

Your global partner for IT-security

www.utimaco.de

info.de@utimaco.de

utimaco safeware