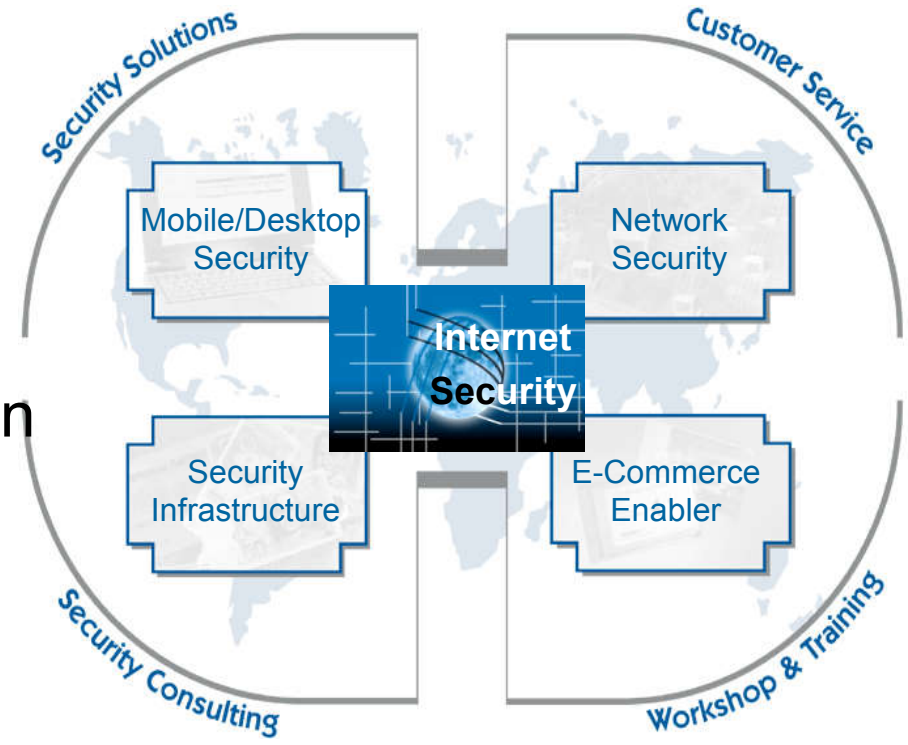
Network Security

Secure Communication in Virtual Enterprises with Encryption, Digital Signature and Firewall

Dipl.-Ing. Norbert Pohlmann

Chief Marketing Director



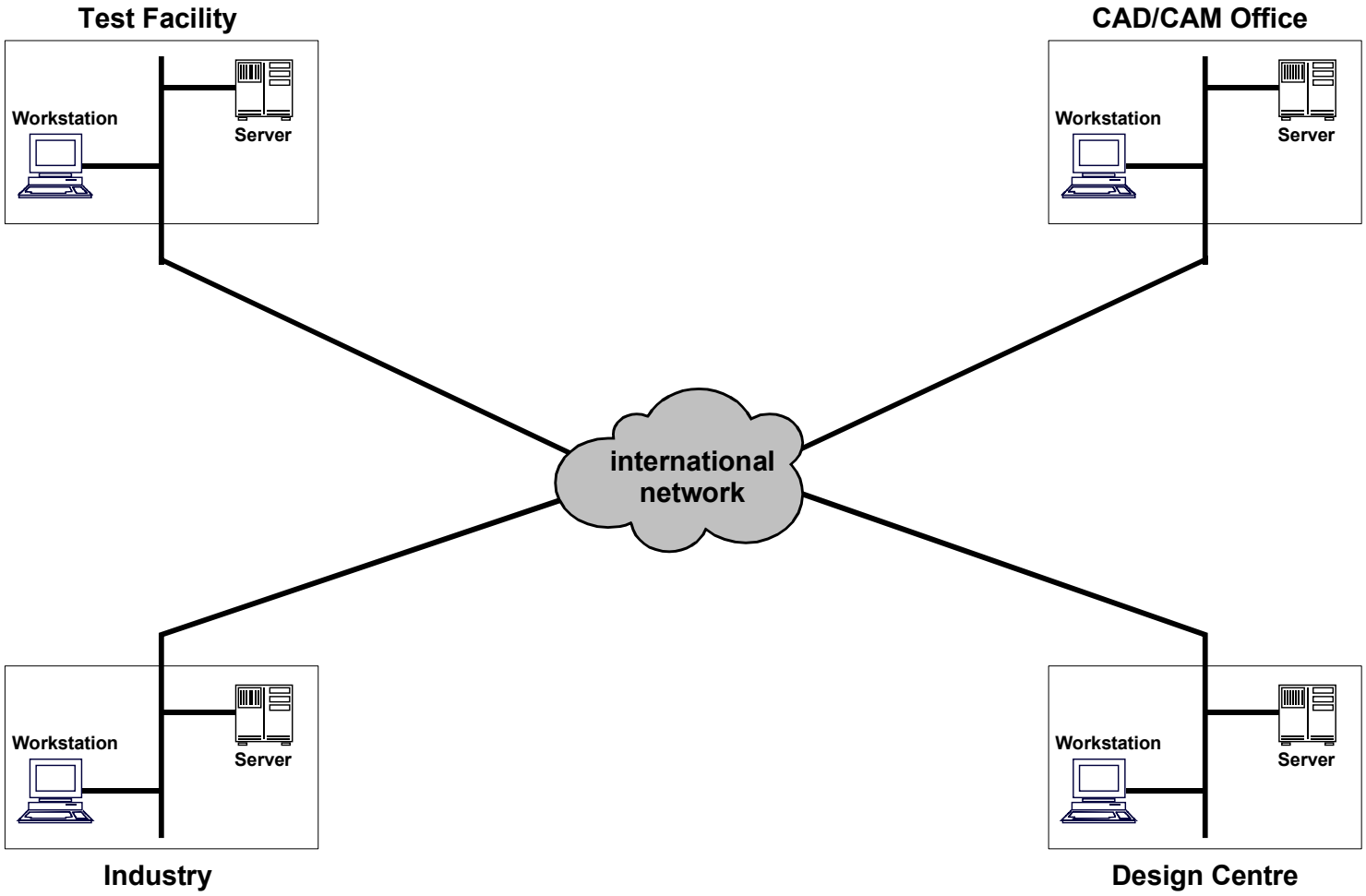
utimaco®
safeware

Contents

- Security needs for Concurrent Multidisciplinary Engineering
- Security Concepts
  - Encryption (Black-Box-Solution)
  - Digital Signature
  - Firewall-System
- Combined Solutions

utimaco® safeware

Concurrent Multidisciplinary Engineering



Security Needs for Concurrent Multidisciplinary Engineering (1)

- confidentiality
  - know-how protection
  - competitors try to gain access to the development results
- non-repudiation
  - to secure that the right information are received to be worked with
  - responsilbility for the result (wrong results may cause tremendous damages)
- integrity of data
  - no manipulation during transmission
  - no virus - infection

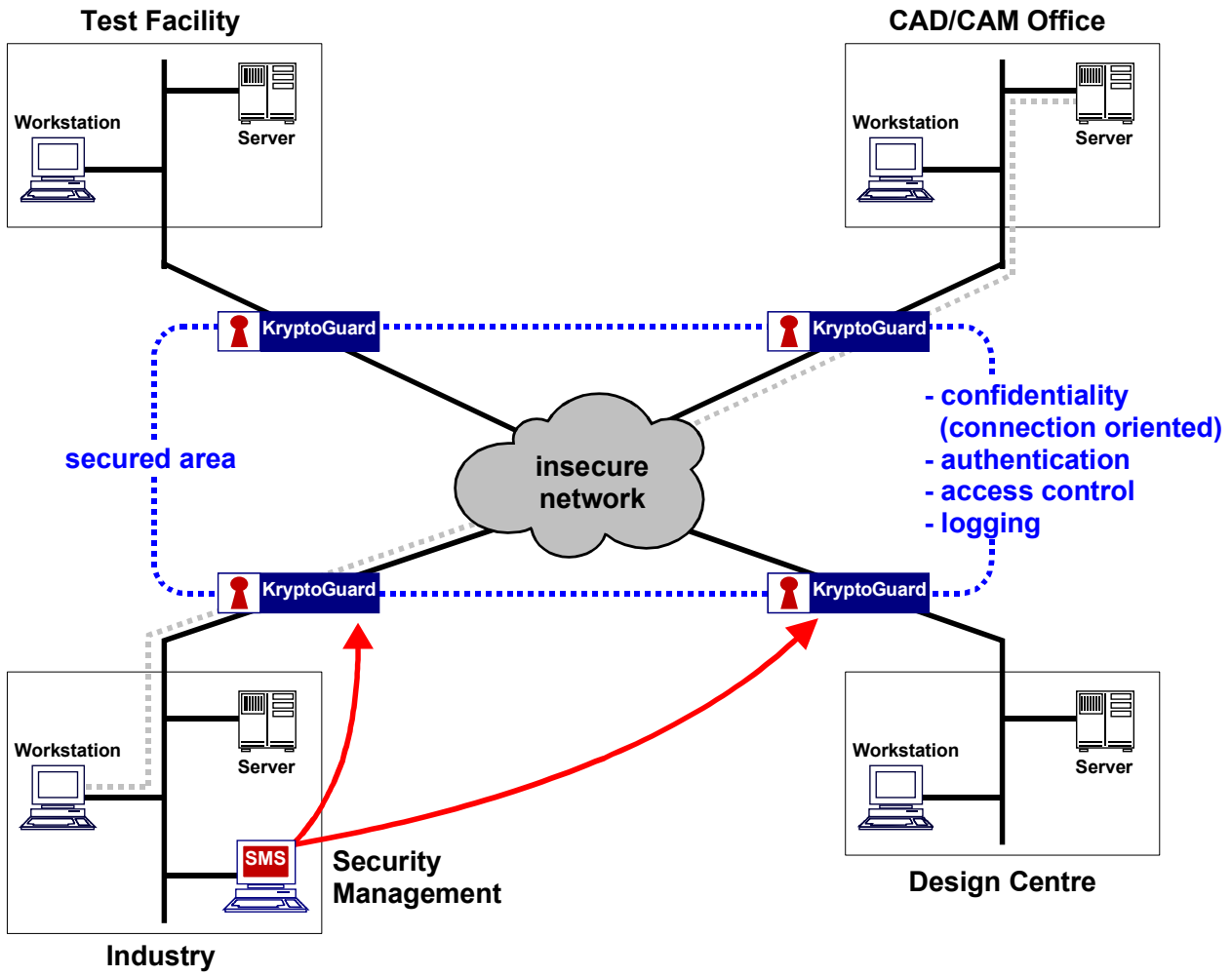
utimaco safeware

Security Needs for Concurrent Multidisciplinary Engineering (2)

- access control
  - strangers should not have access to the computers or networks to be protected
- access-right management
  - only authorised people should have access to the computer
- authentication
  - only communication protocols and services which are permitted should be used
- logging
  - security relevant events can be logged and analysed
  - events can be logged and thus be used as evidence

utimaco safeware

Encryption with the help of a Black-Box Solution (Security System with Packet Filter)



utimaco safeware

Security Services which are provided with this kind of Black-Box Solution

- confidentiality of data (setting up VPNs)
  - it is impossible to read data in plaintext
- authentication
  - implicit by means of encryption
  - explicit by means of authentication mechanisms
- access control
  - only logical connections, which are permitted, can be set up
  - strangers cannot have access to end system
- access-right management
  - only communication protocols and services which are permitted, can be used
- logging
  - security relevant events can be logged and analysed

utimaco safeware

Security System with Packet Filtering

advantages

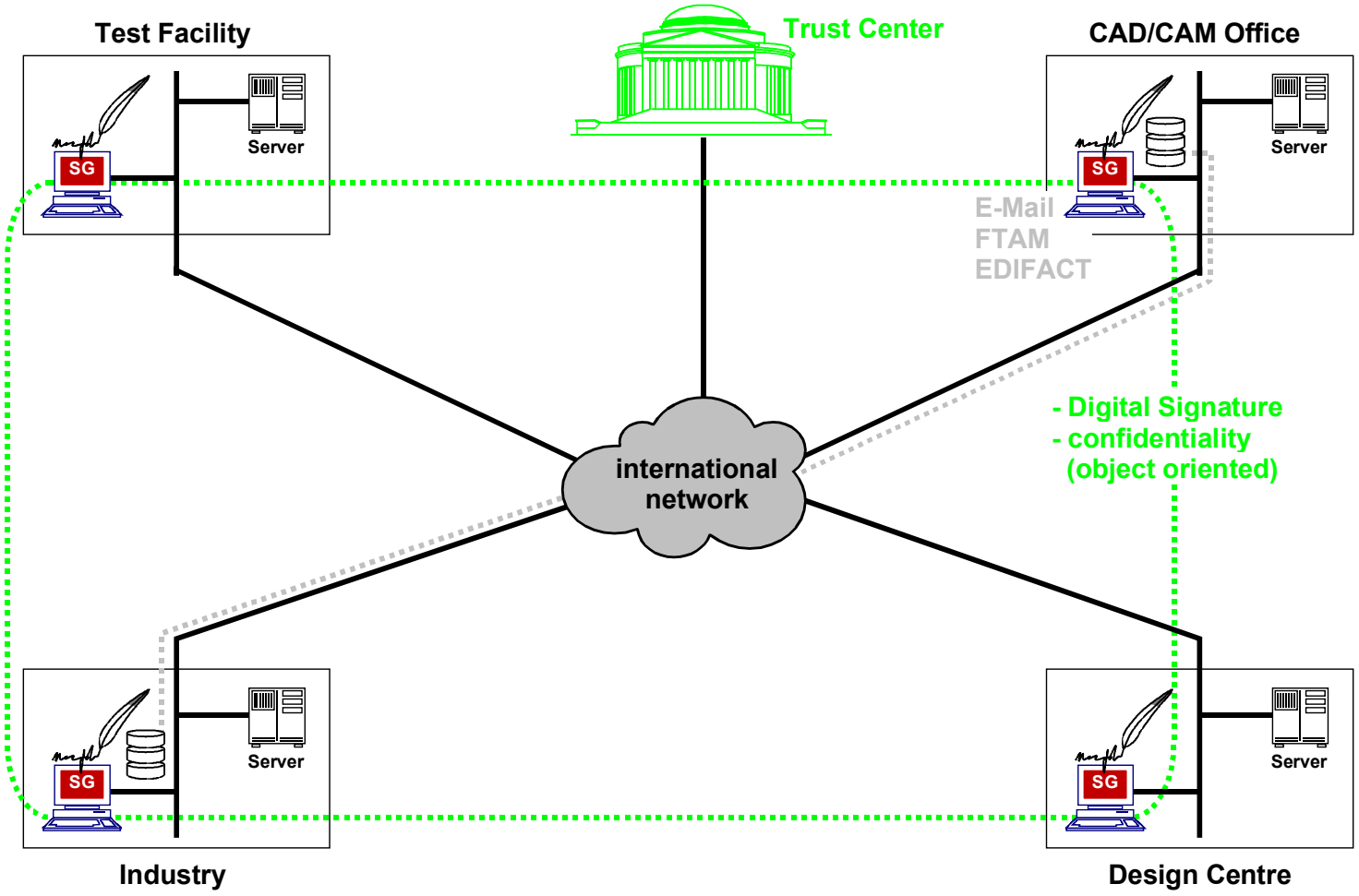
- black box solution
  - transparant security
    - easy to integrate
    - no change of application necessary
    - independent of computer system and operating system
    - supports all kinds of communications:
      - **session oriented (Telnet etc.)**
      - **store and forward (e-mail)**
  - combines easy handling with clearly defined responsibilities

disadvantages

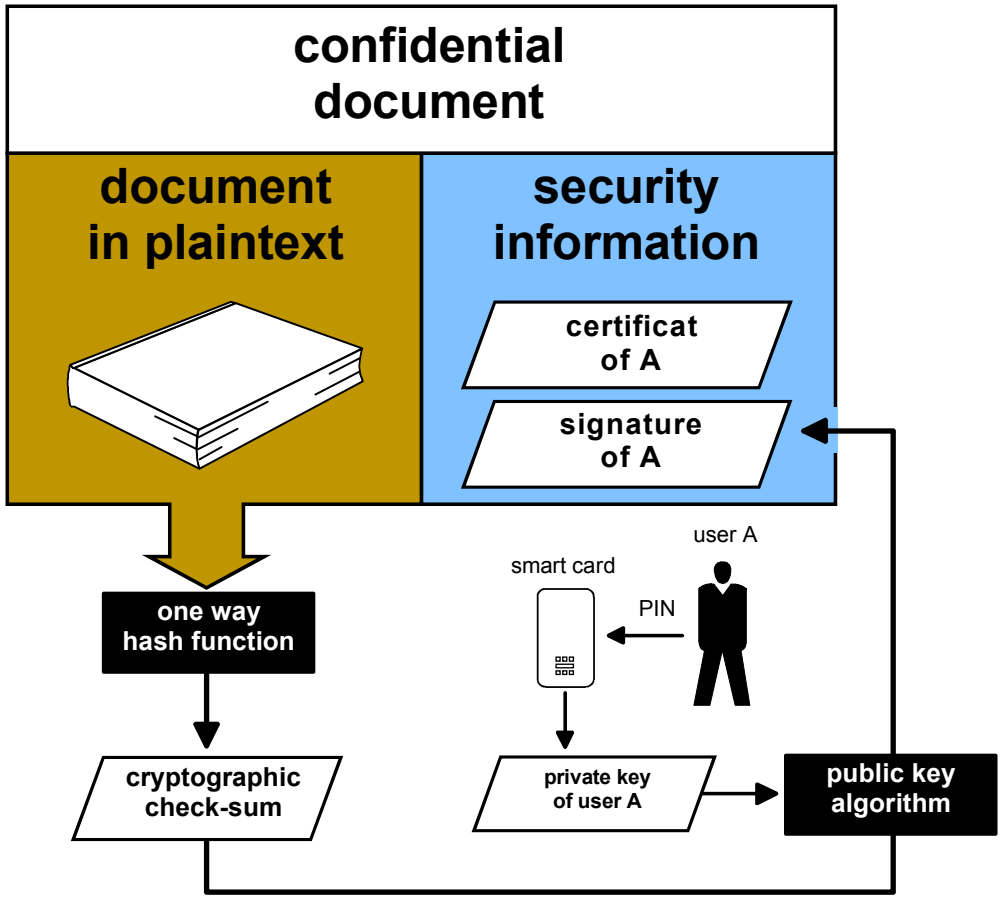
- key management
  - either one organisation (normaly the company which pays) has to take over responsibility
  - or all have to employ the same product
    (Problem presently: no standard or trustworthy infrastructure is available)
- no non-repudiation
  - has to be realised via other mechanisms
- no control on application level

utimaco safeware

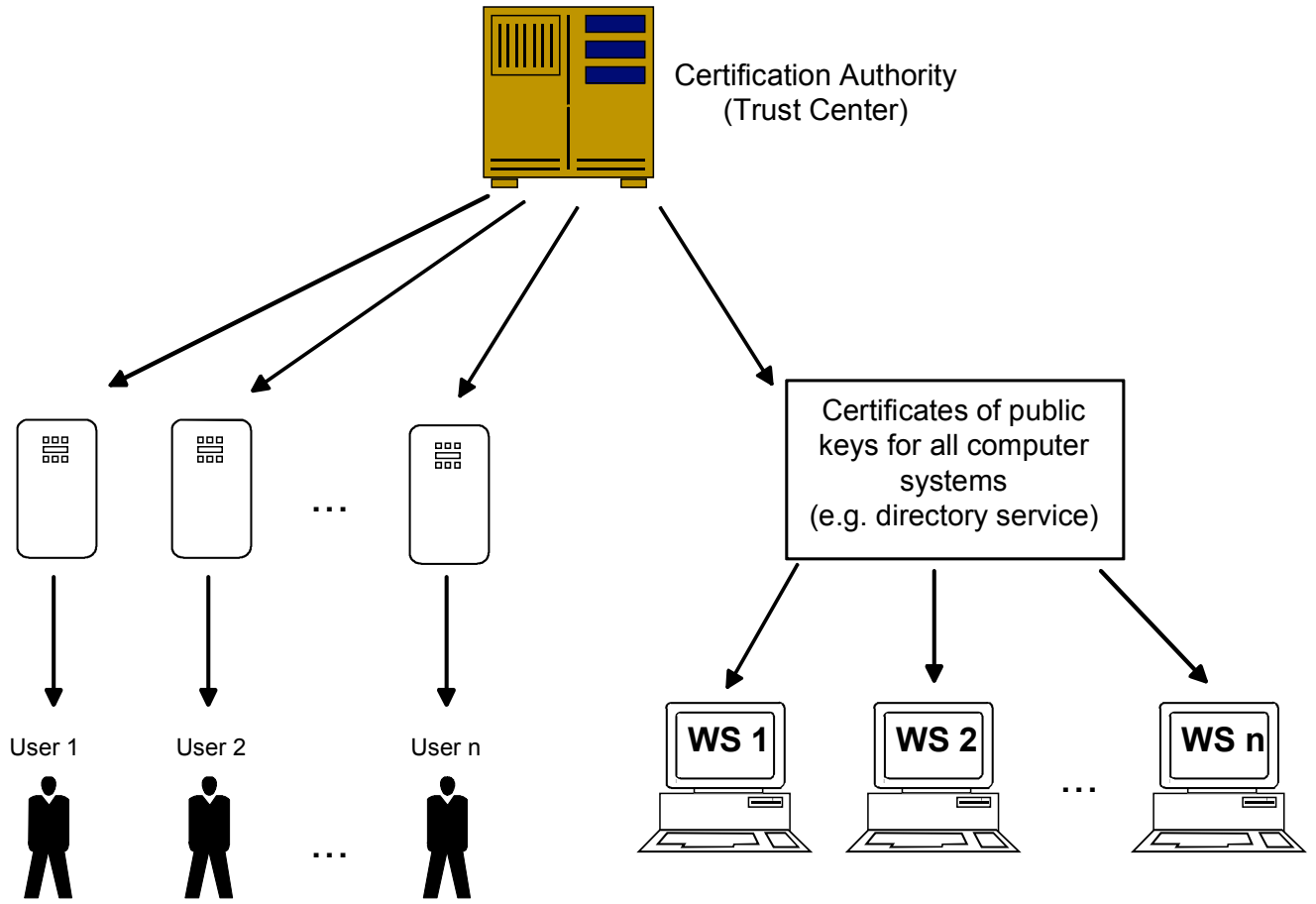
Digital Signature and Object Encryption



Signature Function



Certification Authorities



Digital Signature and Object Encryption

advantages

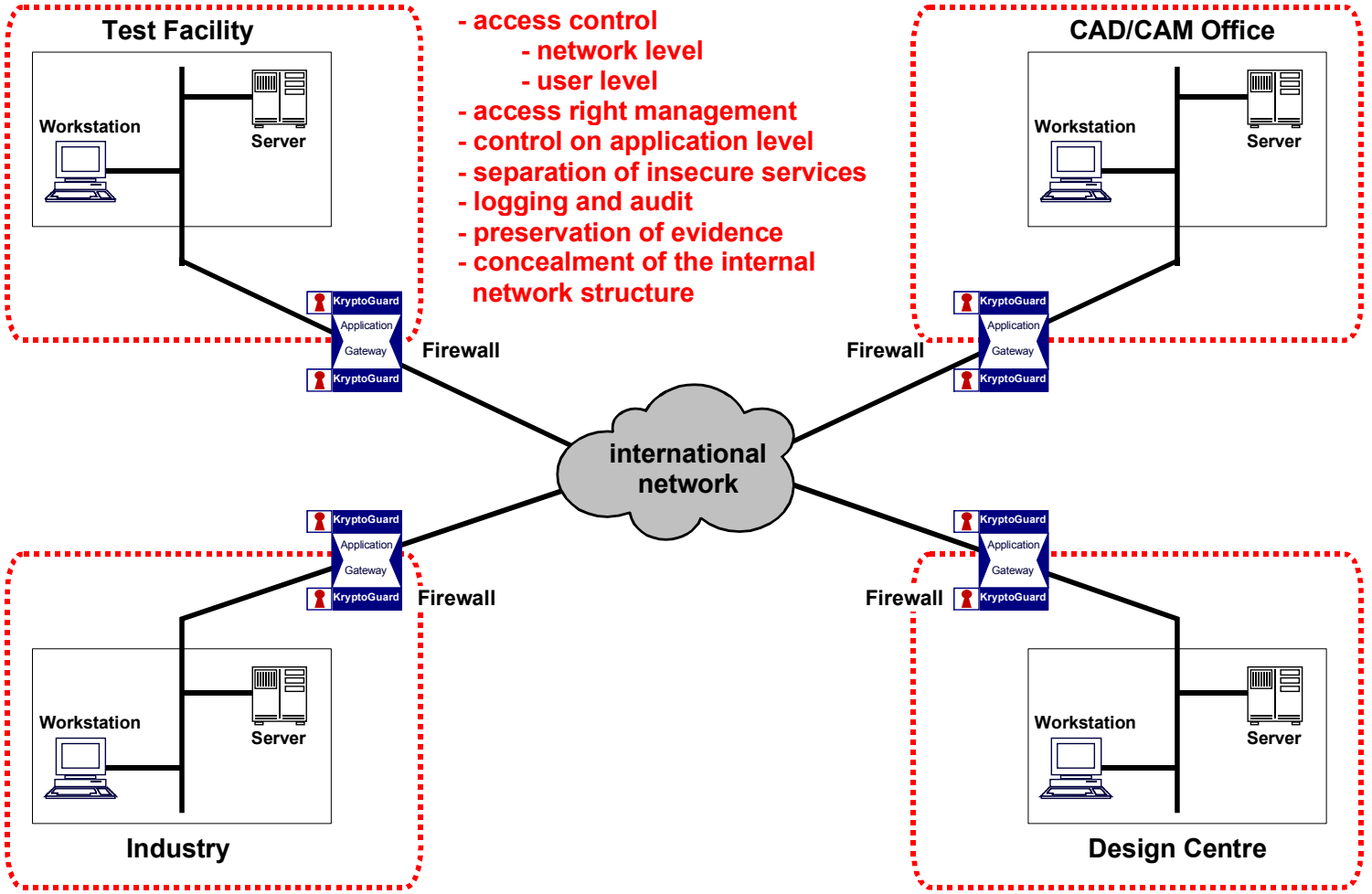
- integrated into application
- legaly recognised signature (as a signature under a document)
- secures only what needs to be secured (selection possible)
- requirements:
  - secure, trustworthy infrastructure
    - supplied by Signature Law (in Germany)

disadvantages

- no access control
  - no access-right management
- not combinable with session-oriented communication

as envelope and manual signature

Firewall System

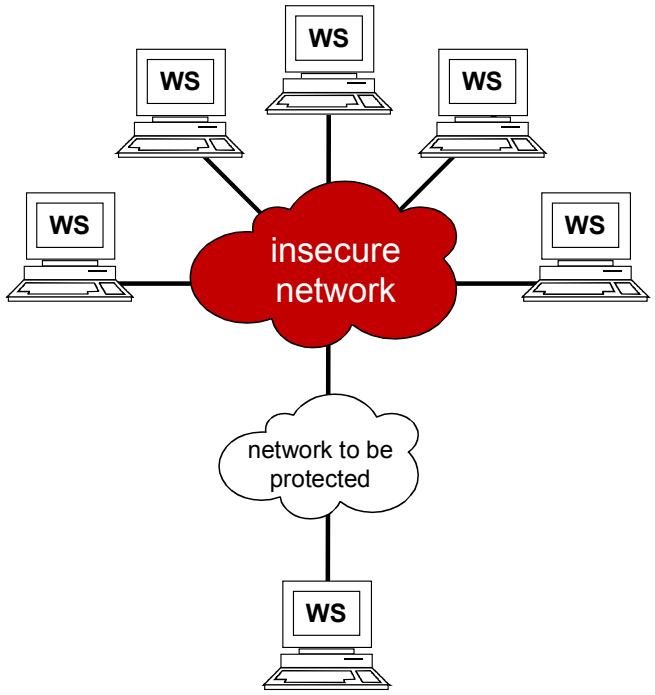


A public network is not a “one-way street”

Risks in public networks:

What are the problems?

- High-tech spies steal someone’s know-how and sell it profitably to competitors.
- Hackers intrude into the local networks of public authorities and companies and manipulate data or smuggle in wrong information.
- Netsurfers paralyze the whole computer system of a company and cause economic damages amounting to millions.

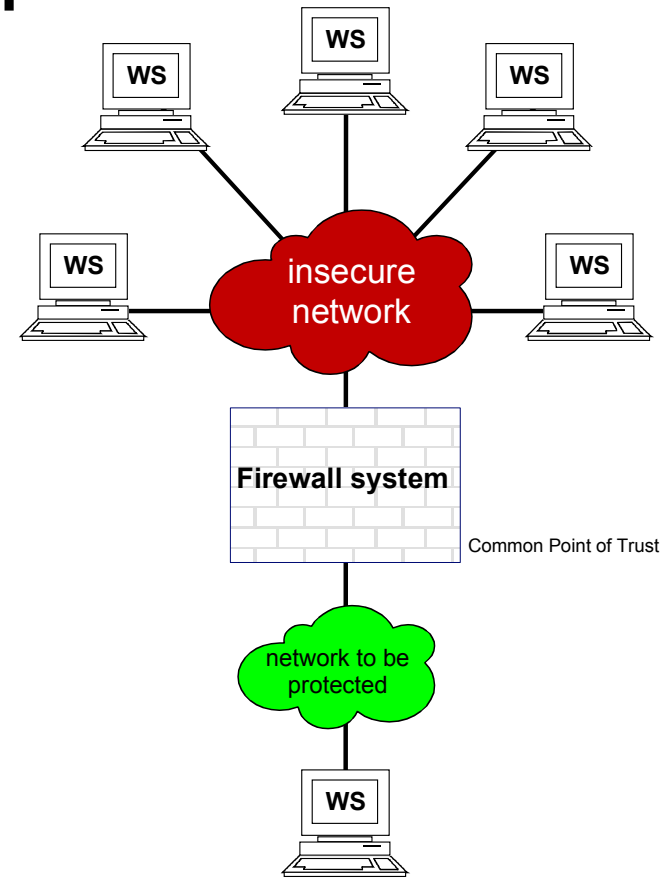


utimaco safeware

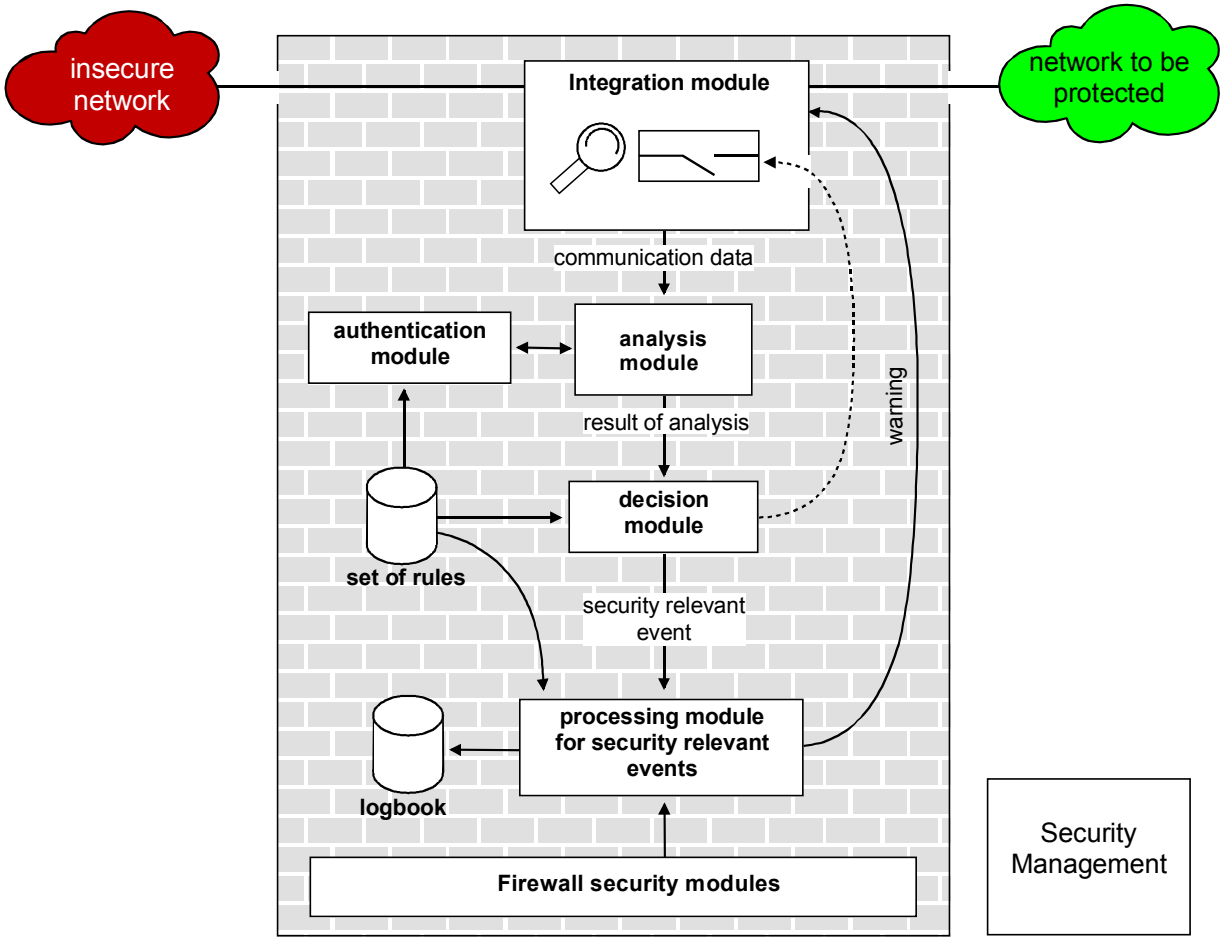
Integration of a Firewall System

Objectives of a Firewall System

- access control on network level
- access control on user level
- access-right management
- control on application level
- separation of insecure services
- logging and audit
- preservation of evidence
- concealment of the internal network structure



Structure of an active Firewall element



Firewall System

advantages

- every organisation is responsible for its own security
- no unauthorised access to the computer to be protected
- access-right management
- preservation of evidence
- independant of terminals and operating system

disadvantages

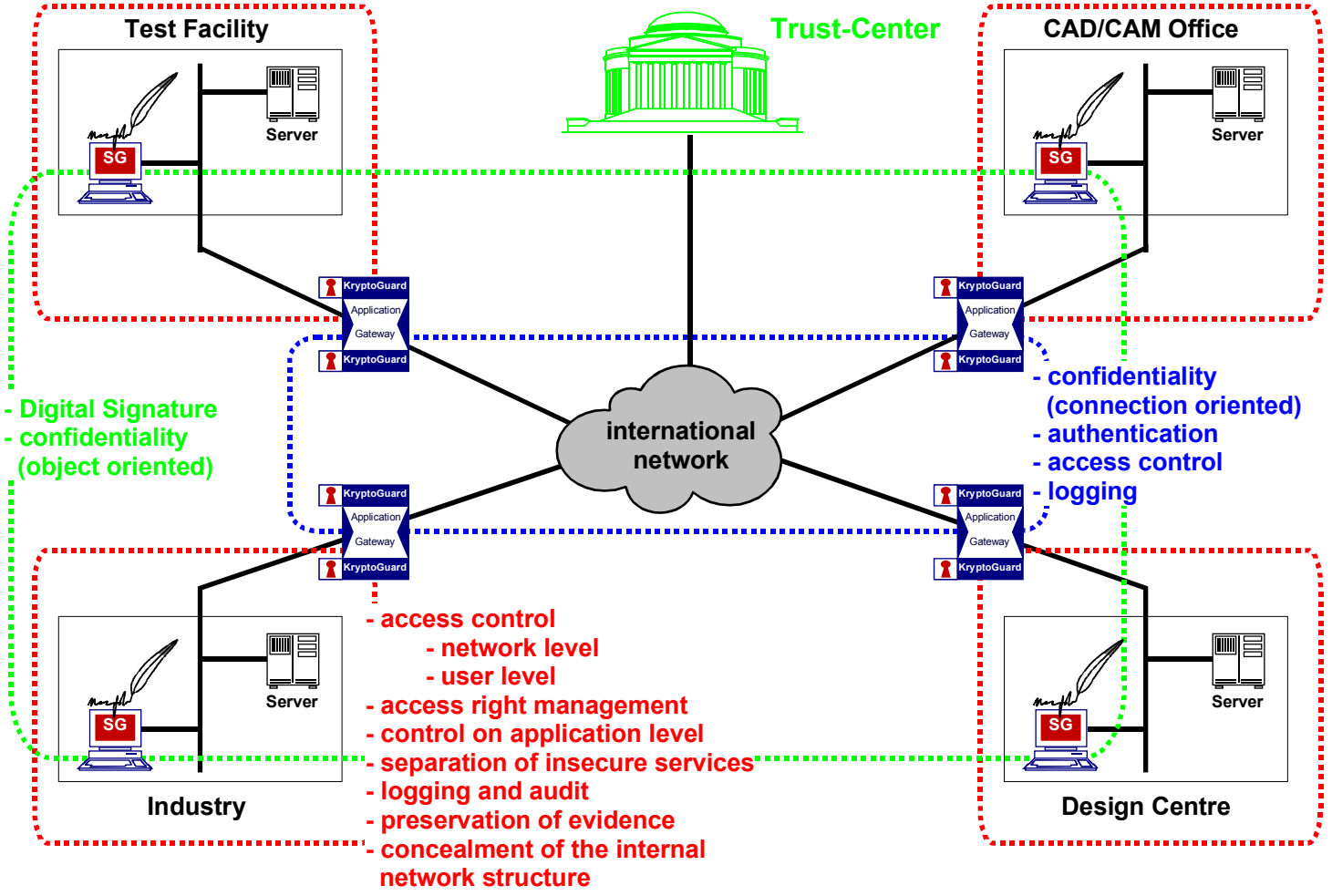
- integrity of data and confidentiality have to be realised via other means
- no non-repudiation

as firewall

and doorman

utimaco safeware

Combinations



Summary

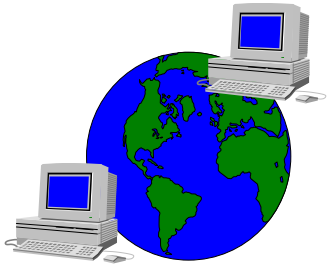
- Solutions for the realisation of secure Concurrent Multidisciplinary Engineering are available
- Combination of different concepts fulfills all security needs
- Organisations with its own responsibility are able to act independently
- When using SmardCards they can be employed for digitale signature as well as for authentication with the Firewall system

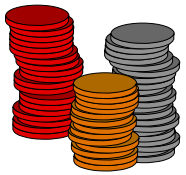
utimaco® safeware

Why Security?

- Information society: fundamental changes
  - Increasing number of work processes are done via IT-systemsnetworks

    ⇒ network a new object for attackers
  - Increasing value of information stored on IT-systems
    - The value of complete documentation of R&D units can easily exceed millions $
  - Secure and reliable paymend and transactions via insecure networks (e.g. Internet)
  - Lack of appropriate moral





utimaco safeware

Why Security?

- Requirements for security
  - selfprotection against espionage necessary
  - legal regulations have to be fulfilled

utimaco safeware