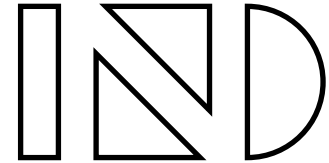


University of Stuttgart

INSTITUTE OF
COMMUNICATION NETWORKS
AND COMPUTER ENGINEERING
Prof. Dr.-Ing. Dr. h. c. mult. P. J. Kühn



Security Services in an Open Service Environment – Considering Network Integrity

Reiner Sailer

Structure:

- ❑ Introduction
- ❑ Open Security Services
- ❑ Network Integrity Aspects
- ❑ Conclusions & Outlook

Introduction

Multilateral security

The **security needs of all parties** that are affected by a telecommunication service **are taken into account in a balanced way**

Superordinate goals

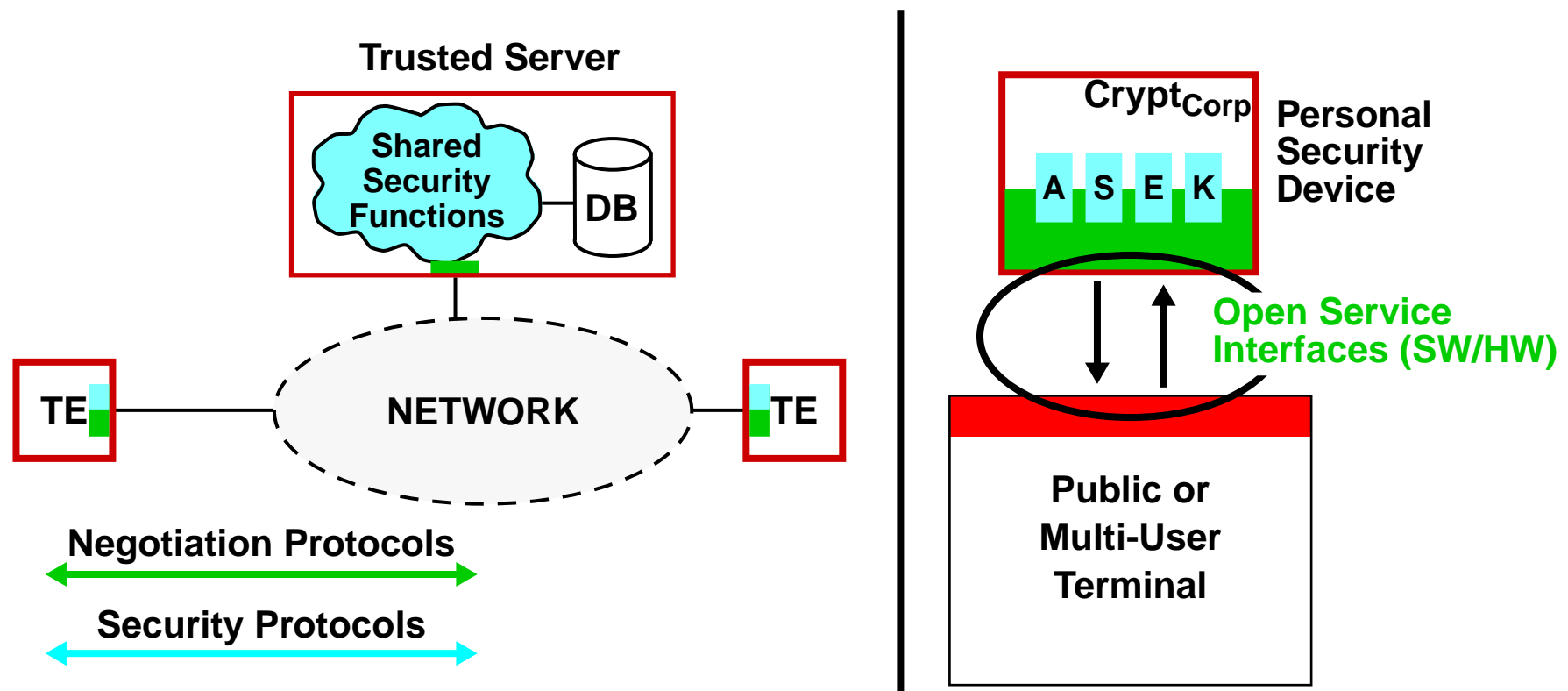
- ❑ **empowering users & enabling applications**
- ❑ **saving huge investments in existing network infrastructures**

Basic challenges

- ❑ **assessment & rating** of security enhanced services
- ❑ **synchronization** of distributed security functions
- ❑ **combination** of security functions with telecommunication services
- ❑ **open protocols & interfaces** for flexible and global use

Add-on approach to a security enhanced service environment in ISDN/IN

- standardized **negotiation & security protocols**
- standardized **service access points** promote replaceable security devices



Reiner Sailer, 14th Annual Computer Security Applications Conference, Phoenix, AZ, December 1998

ISDN Infrastructure and **SAP^{ISDN}**

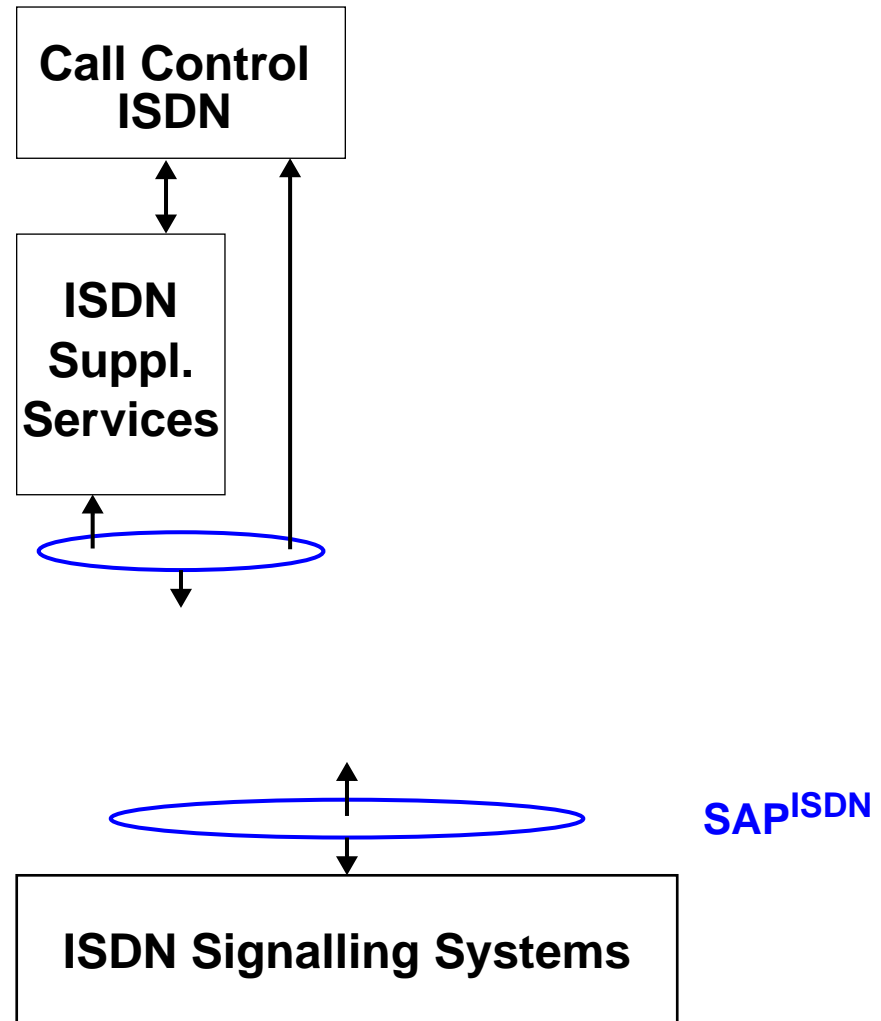
- exchange of security control data (using DSS1 and SS7)

Security Adaptation Layer (SAL)

- separation (access control)
- provision of standardized **SAP^{SEC}**
- linking of **SSS** and ISDN services

Security Supplementary Services

- negotiation using **SAP^{Sec}** & encapsulation of sec. functions
- **synchronization** by standardized protocols (using **Sec-PDUs**)



ISDN Infrastructure and **SAP^{ISDN}**

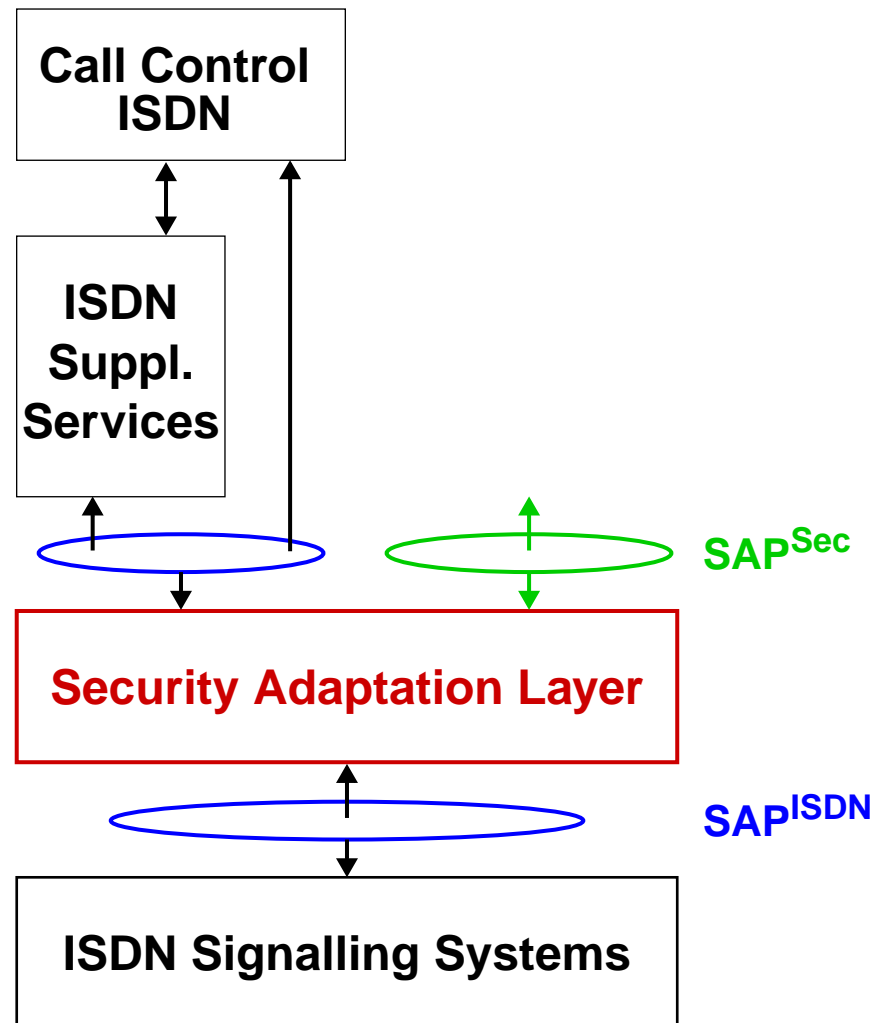
- exchange of security control data (using DSS1 and SS7)

Security Adaptation Layer (SAL)

- separation (access control)
- provision of standardized **SAP^{SEC}**
- linking of **SSS** and ISDN services

Security Supplementary Services

- negotiation using **SAP^{Sec}** & encapsulation of sec. functions
- **synchronization** by standardized protocols (using **Sec-PDUs**)



ISDN Infrastructure and **SAP^{ISDN}**

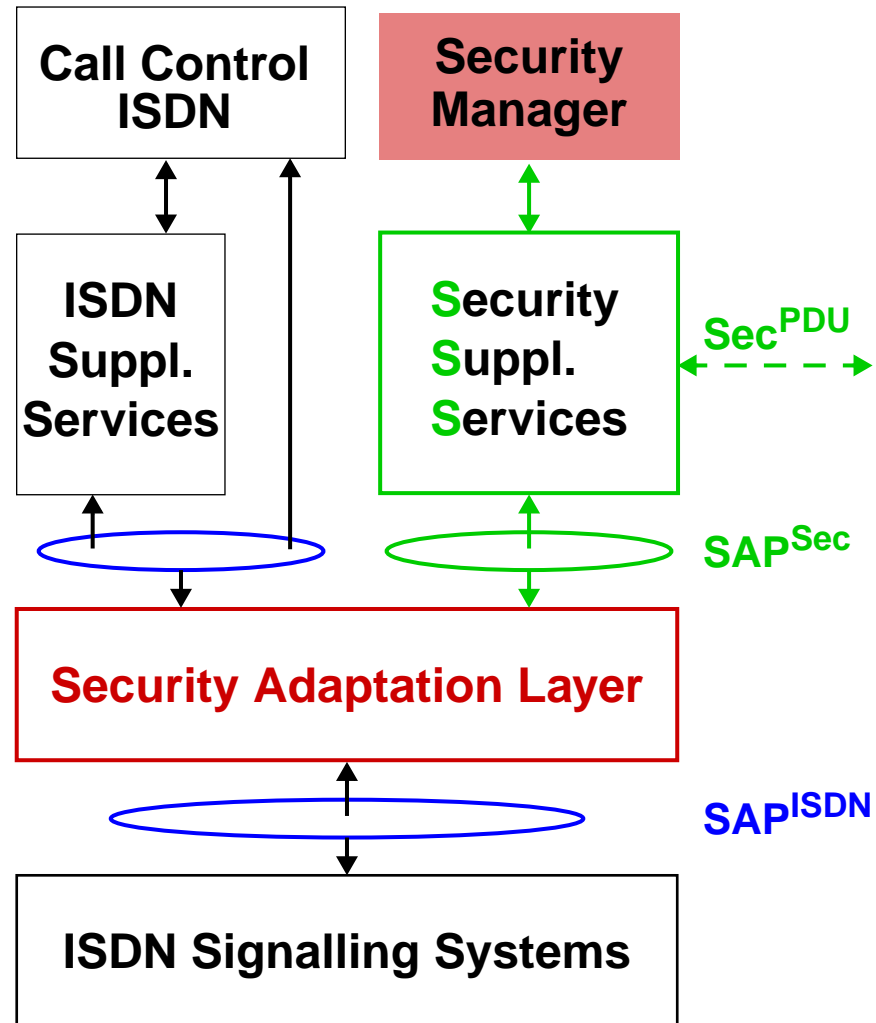
- exchange of security control data (using DSS1 and SS7)

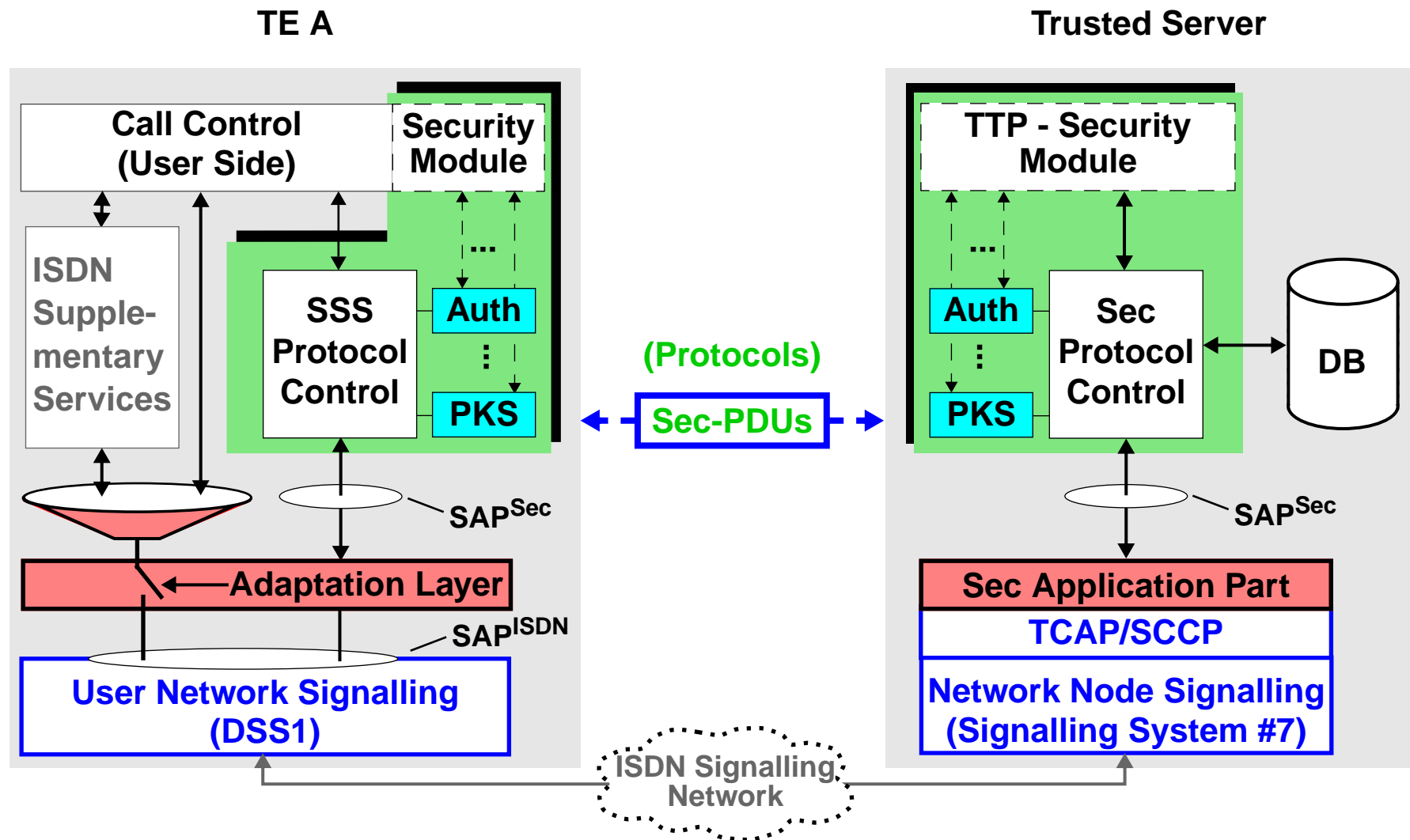
Security Adaptation Layer (SAL)

- separation (access control)
- provision of standardized **SAP^{SEC}**
- linking of **SSS** and ISDN services

Security Supplementary Services

- negotiation using **SAP^{Sec}** & encapsulation of sec. functions
- **synchronization** by standardized protocols (using **Sec-PDUs**)






Reiner Sailer, 14th Annual Computer Security Applications Conference, Phoenix, AZ, December 1998

**Network integrity aspects concerning
the exchange of security control data**

Architectural refinements

- **Security Services, Security Adaptation Layer**
- **Negotiation of security services and combination with existing services**

 **R. Sailer: An Evolutionary Approach to Multilaterally Secure Services in ISDN / IN.
7th ICCCN, Lafayette LA, October 1998.**

Reiner Sailer, 14th Annual Computer Security Applications Conference, Phoenix, AZ, December 1998

Incoming inspection of control data that enters a signalling network via:

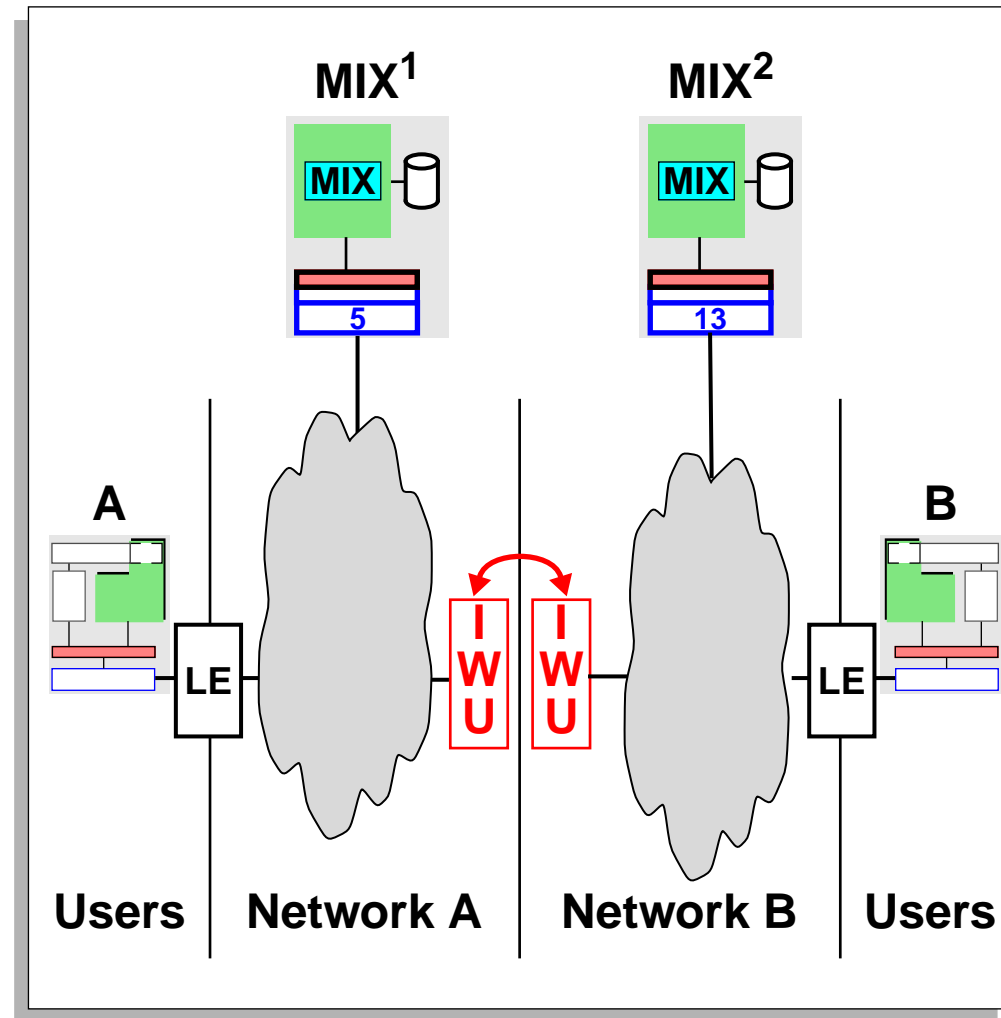
- User Network Interfaces
- Network Node Interfaces

Security control information

- transported by the network
⇒ contributes to **signalling load**
- processed by network nodes
⇒ contributes to **service control**

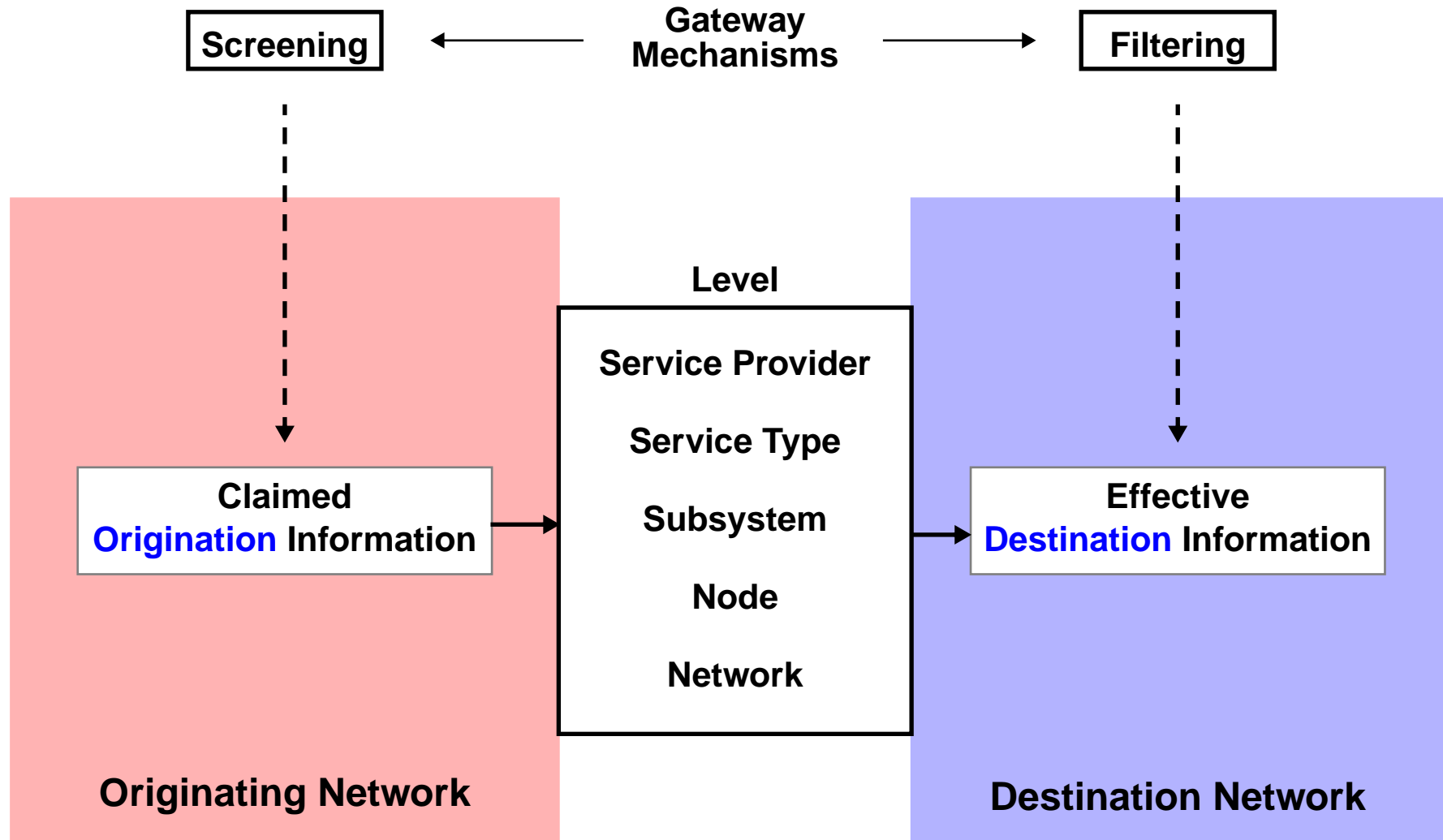
but might be protected against interpretation regarding NOs

(e. g. encrypted Sec-PDUs for anonymity services)

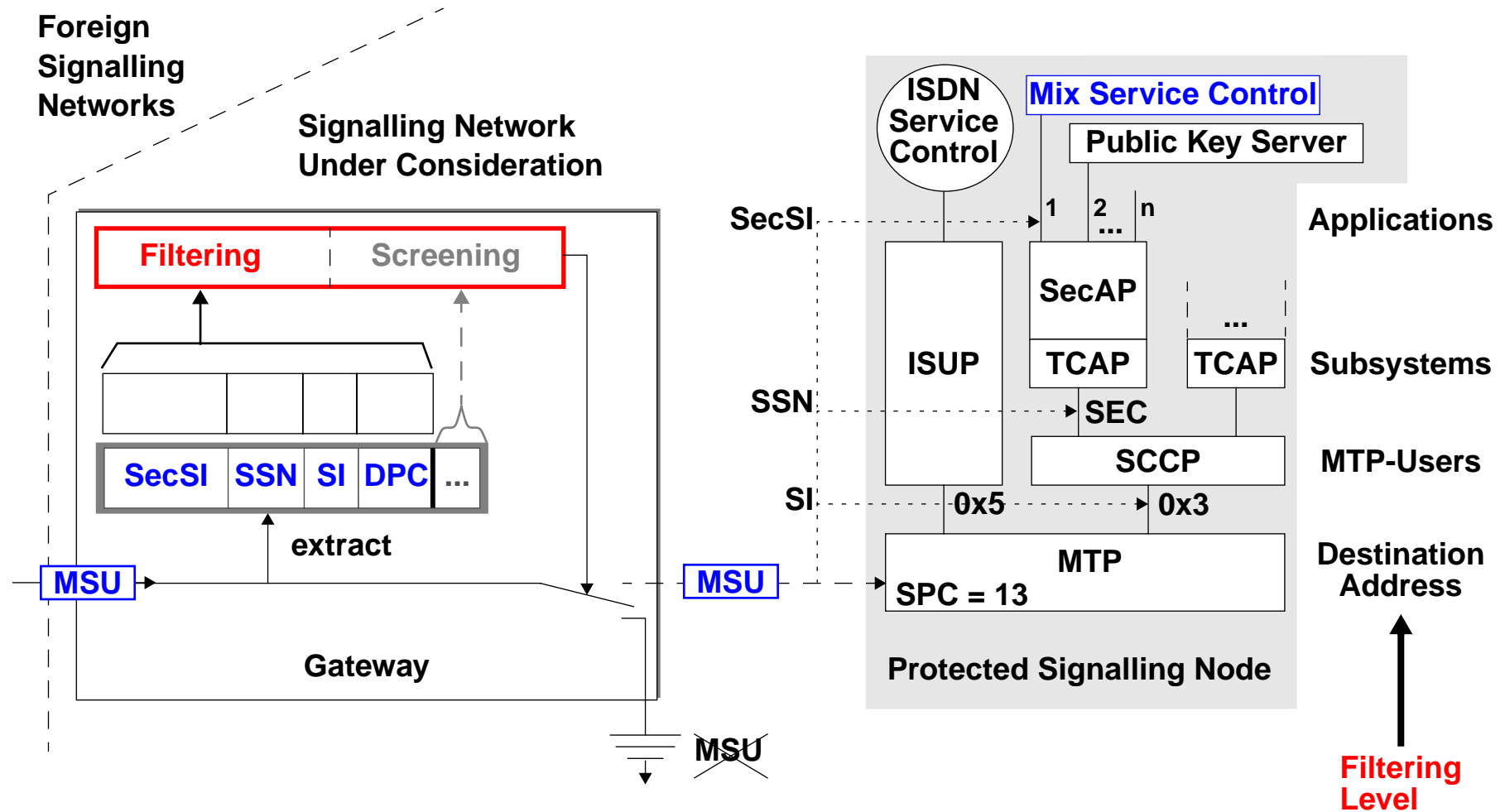


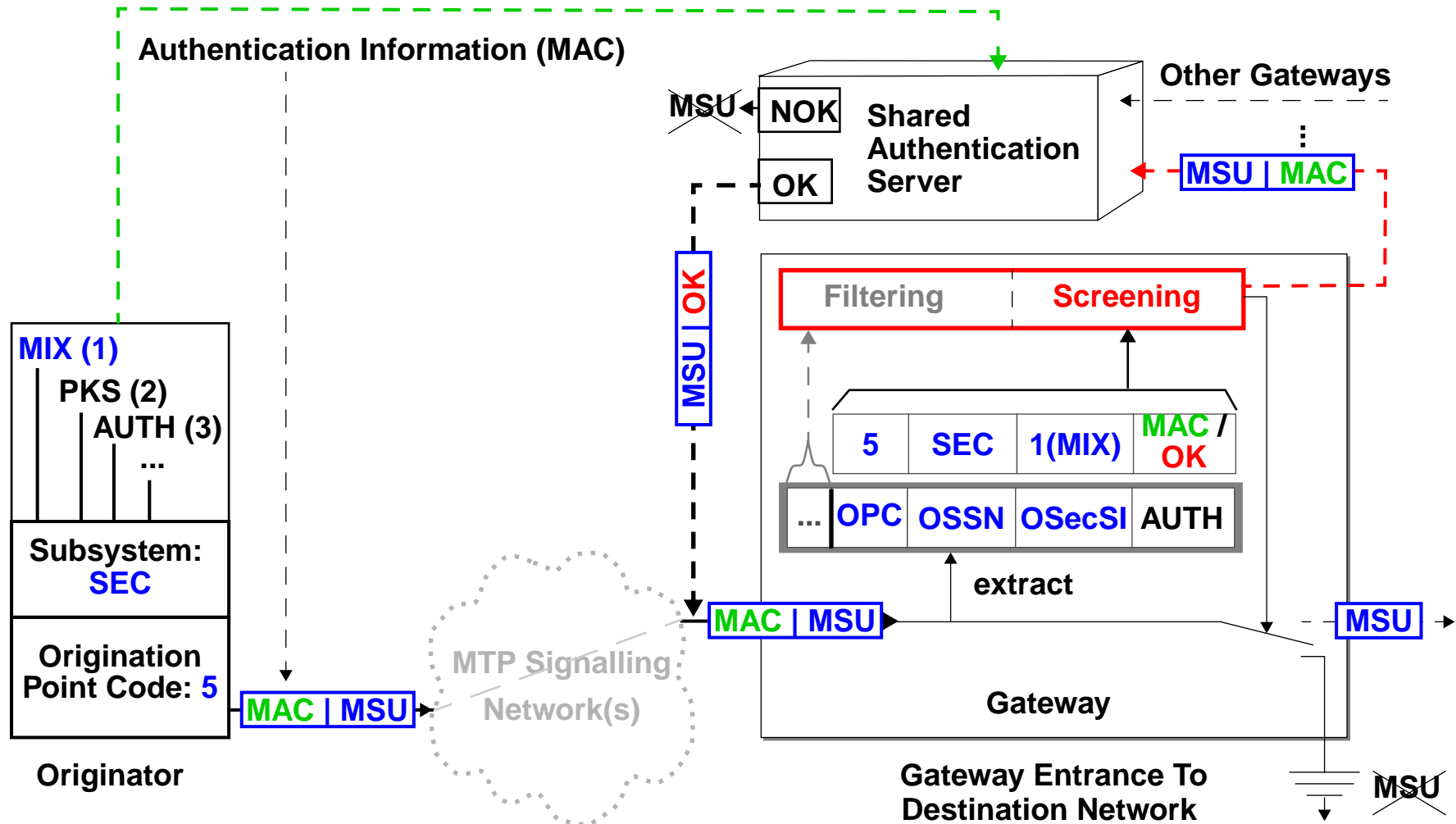
Network Integrity

Basic Mechanisms



Reiner Sailer, 14th Annual Computer Security Applications Conference, Phoenix, AZ, December 1998





Reiner Sailer, 14th Annual Computer Security Applications Conference, Phoenix, AZ, December 1998

Conclusions & Outlook

✓ Challenges

Initial implementation of end-to-end open security services

- ❑ intel-based PCs running Linux, ISDN interface cards, ISDN-PBX
- ❑ **SAP^{Sec}** implemented as standardized hw/sw driver interface
- ❑ **High Layer Compatibility** parameter for **SSS** compatibility check
- ❑ **synchronization by User To User Signalling** (interim solution)

Long term requirements

- ❑ means for addressing network internal servers via the UNI
- ❑ means for verifying data that serves as a basis for filtering and screening
- ❑ means for the efficient exchange of security control data
- ❑ **SecAP** interworking at network boundaries for global security services
- ❑ **standardized security protocols** (e. g. **Public Key Certificate Retrieval, Authentication, Encryption, Anonymity**)