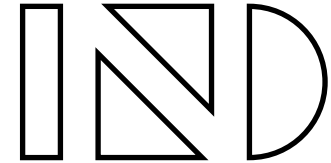


University of Stuttgart

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



# An Evolutionary Approach to Multilaterally Secure Services in ISDN / IN

*Reiner Sailer*

## Structure:

- ❑ Introduction
- ❑ Exemplary Authentication Service
- ❑ Architectural Enhancements of ISDN / IN
- ❑ 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**

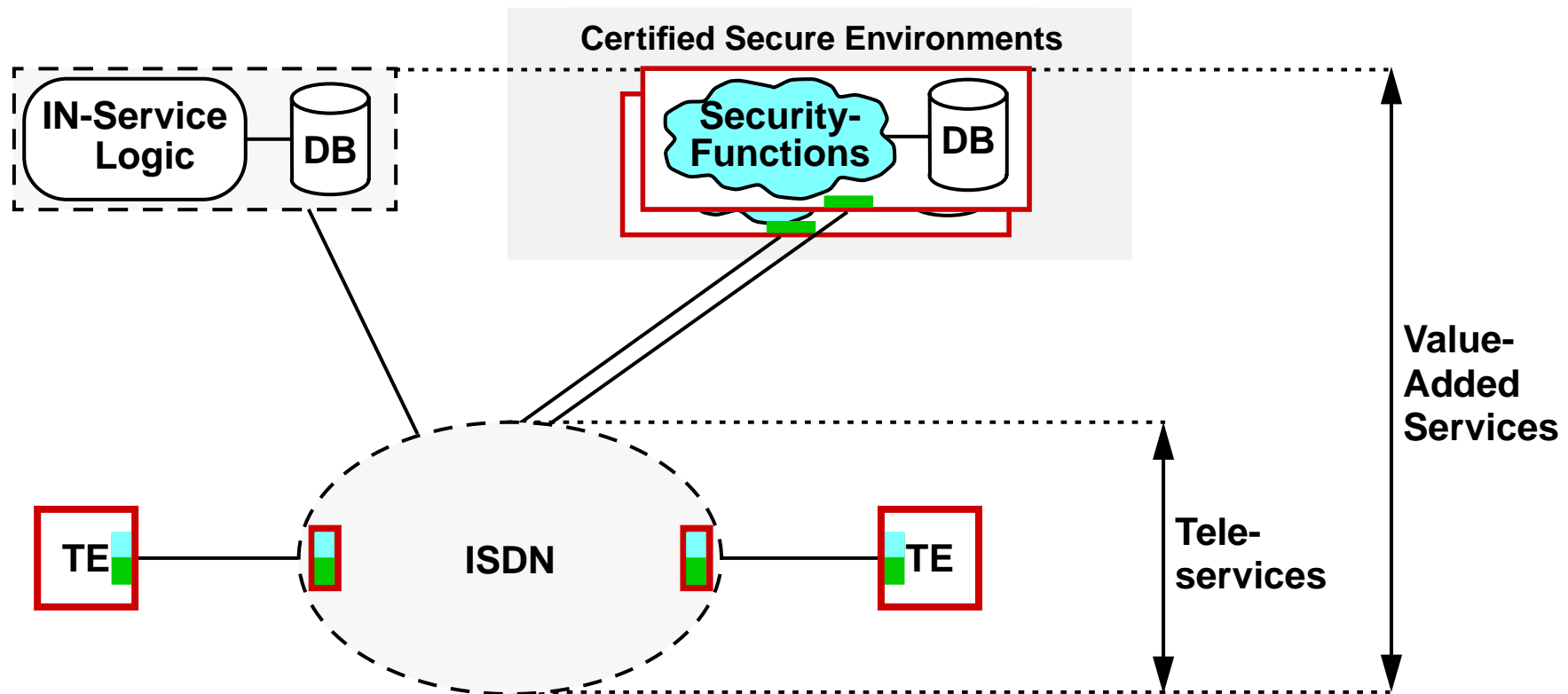
## Challenges

- ❑ **assessment & rating**
  - **separation of security relevant functions**
  - **secure runtime environments**
- ❑ **synchronization** of distributed security functions
- ❑ **combination** of security functions with telecommunication services

Reiner Sailer, 7<sup>th</sup> International Conference on Computer Communications And Networks (IC3N), Lafayette, LA, October 1998

## Add-On Approach to a Security Enhanced Service Environment in ISDN/IN

- ❑ security functions & secure environments
- ❑ negotiation & security service protocols



Reiner Sailer, 7<sup>th</sup> International Conference on Computer Communications And Networks (IC3N), Lafayette, LA, October 1998

## **General requirements for the negotiation of security services**

- ❑ **algorithms, message and parameter types, protocols, fall back mechanisms, reference points (user, network operator, service provider)**

## **Authentication services**

- ❑ **exchange of authentication tokens (challenges, responses)**
- ❑ **retrieval of public key certificates & certificate/key revocation lists**

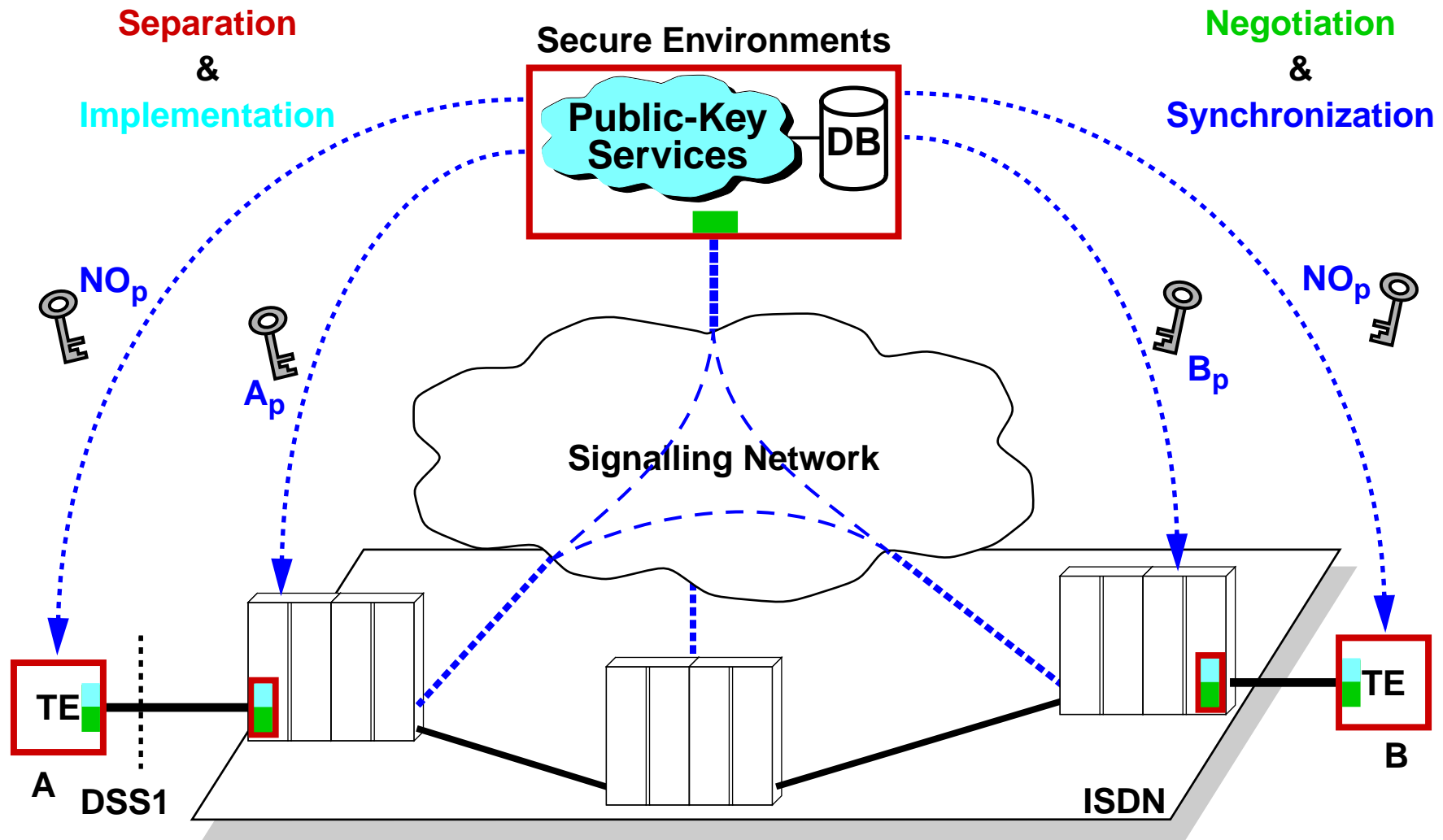
## **Encryption services**

- ❑ **key exchange, key agreement, key change**
- ❑ **synchronization, resynchronisation of encryption and decryption**

## **Anonymity services**

- ❑ **negotiation of mechanisms to conceal the relationship of persons with a particular communication event**

Reiner Sailer, 7<sup>th</sup> International Conference on Computer Communications And Networks (IC3N), Lafayette, LA, October 1998



Reiner Sailer, 7<sup>th</sup> International Conference on Computer Communications And Networks (IC3N), Lafayette, LA, October 1998

## ISDN Infrastructure and **SAP<sup>ISDN</sup>**

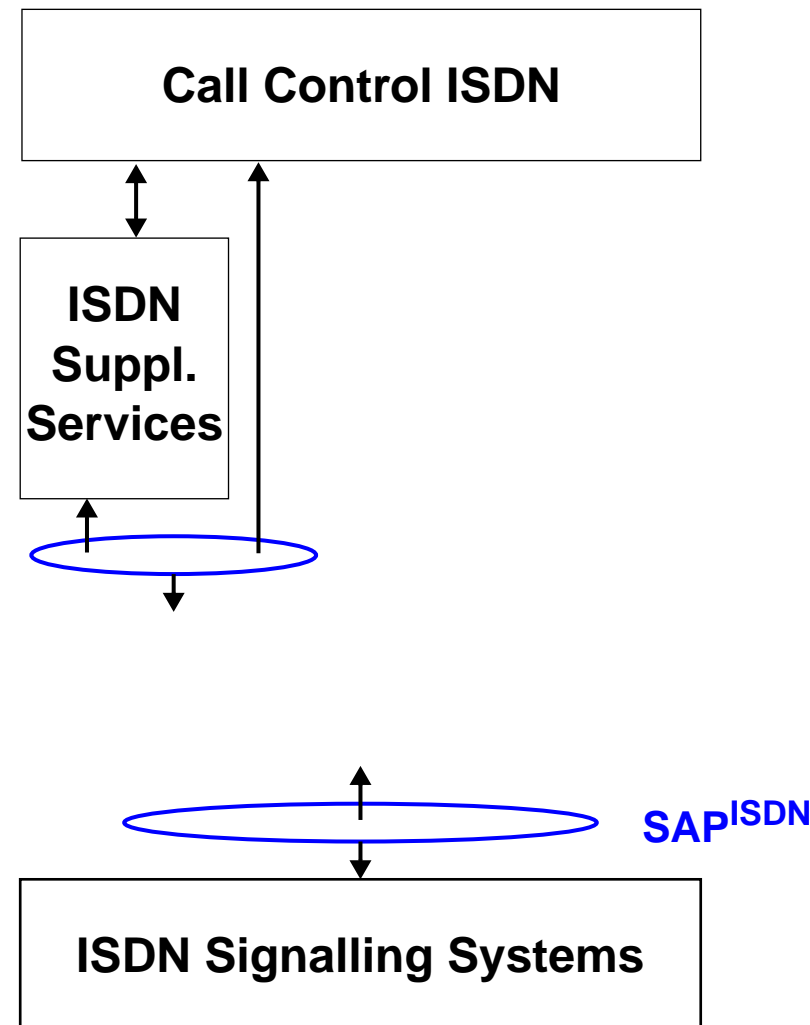
- ❑ exchange of security control data (using DSS1 and SS7)

## Security Adaptation Layer (SAL)

- ❑ separation (access control)
- ❑ provision of standardized **SAP<sup>SEC</sup>**
- ❑ linking of **SSS** and ISDN services

## Security Supplementary Services

- ❑ negotiation & encapsulation of security functions (using **SAP<sup>Sec</sup>**)
- ❑ **synchronization** by standardized protocols (SSS-PDUs)



Reiner Sailer, 7<sup>th</sup> International Conference on Computer Communications And Networks (IC3N), Lafayette, LA, October 1998

## ISDN Infrastructure and **SAP<sup>ISDN</sup>**

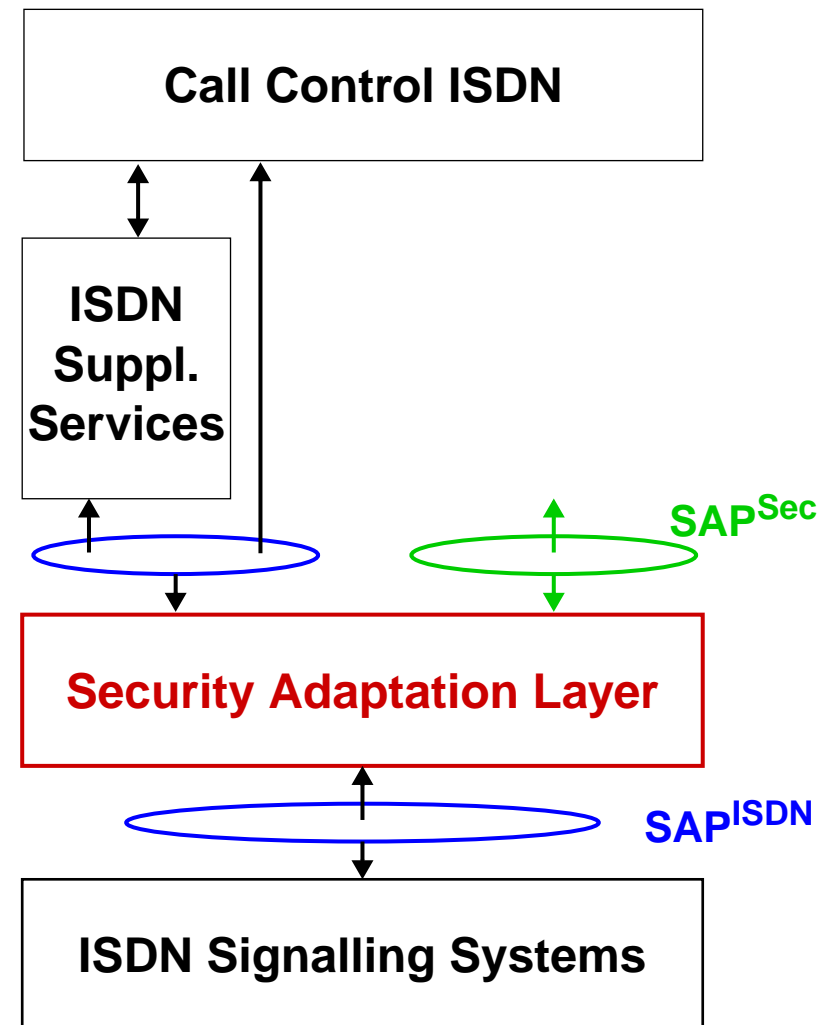
- ❑ exchange of security control data (using DSS1 and SS7)

### Security Adaptation Layer (SAL)

- ❑ separation (access control)
- ❑ provision of standardized **SAP<sup>SEC</sup>**
- ❑ linking of **SSS** and ISDN services

### Security Supplementary Services

- ❑ negotiation & encapsulation of security functions (using **SAP<sup>Sec</sup>**)
- ❑ **synchronization** by standardized protocols (SSS-PDUs)



Reiner Sailer, 7<sup>th</sup> International Conference on Computer Communications And Networks (IC3N), Lafayette, LA, October 1998

## ISDN Infrastructure and **SAP<sup>ISDN</sup>**

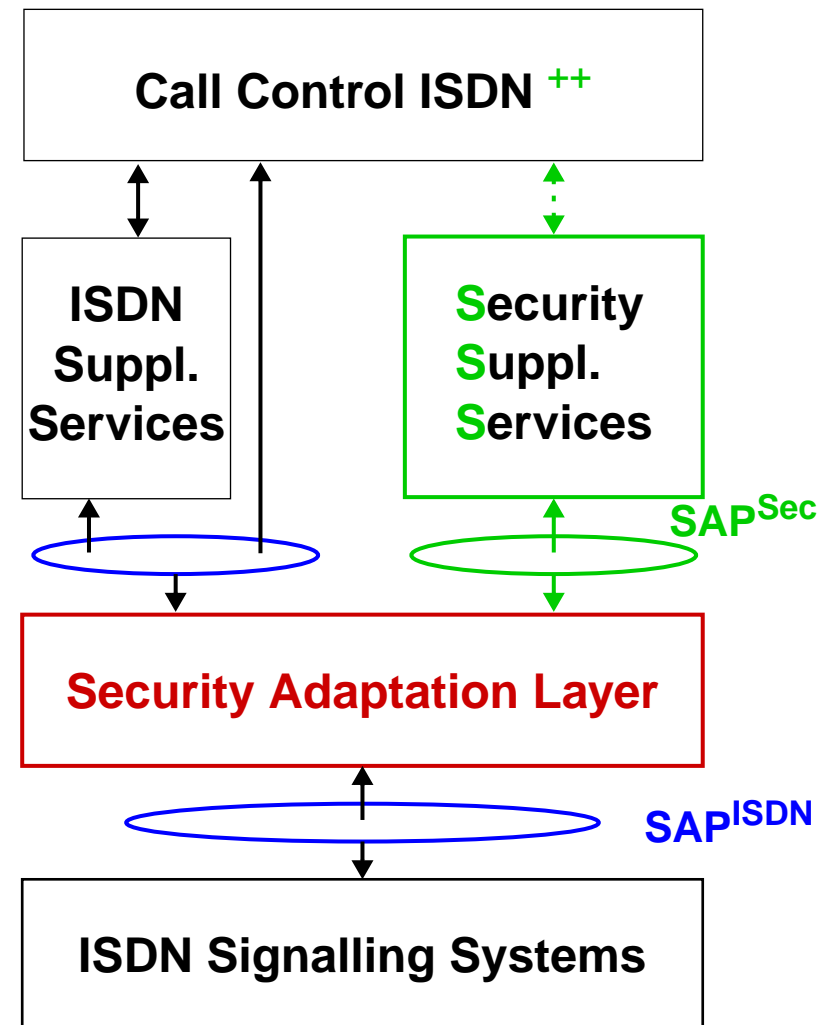
- ❑ exchange of security control data (using DSS1 and SS7)

## Security Adaptation Layer (SAL)

- ❑ separation (access control)
- ❑ provision of standardized **SAP<sup>SEC</sup>**
- ❑ linking of **SSS** and ISDN services

## Security Supplementary Services

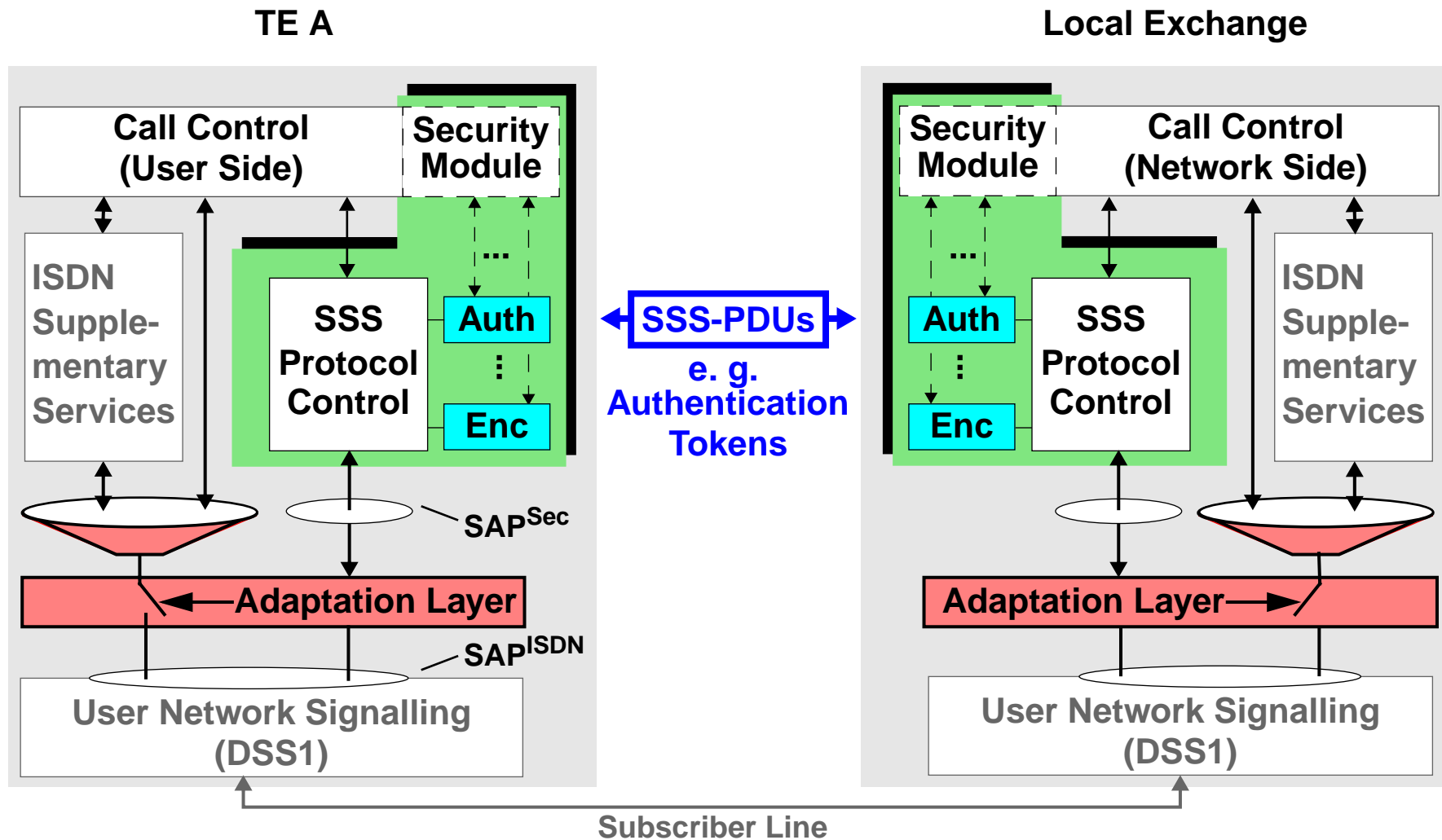
- ❑ negotiation & encapsulation of security functions (using **SAP<sup>Sec</sup>**)
- ❑ **synchronization** by standardized protocols (SSS-PDUs)



Reiner Sailer, 7<sup>th</sup> International Conference on Computer Communications And Networks (IC3N), Lafayette, LA, October 1998

# Architectural Enhancements

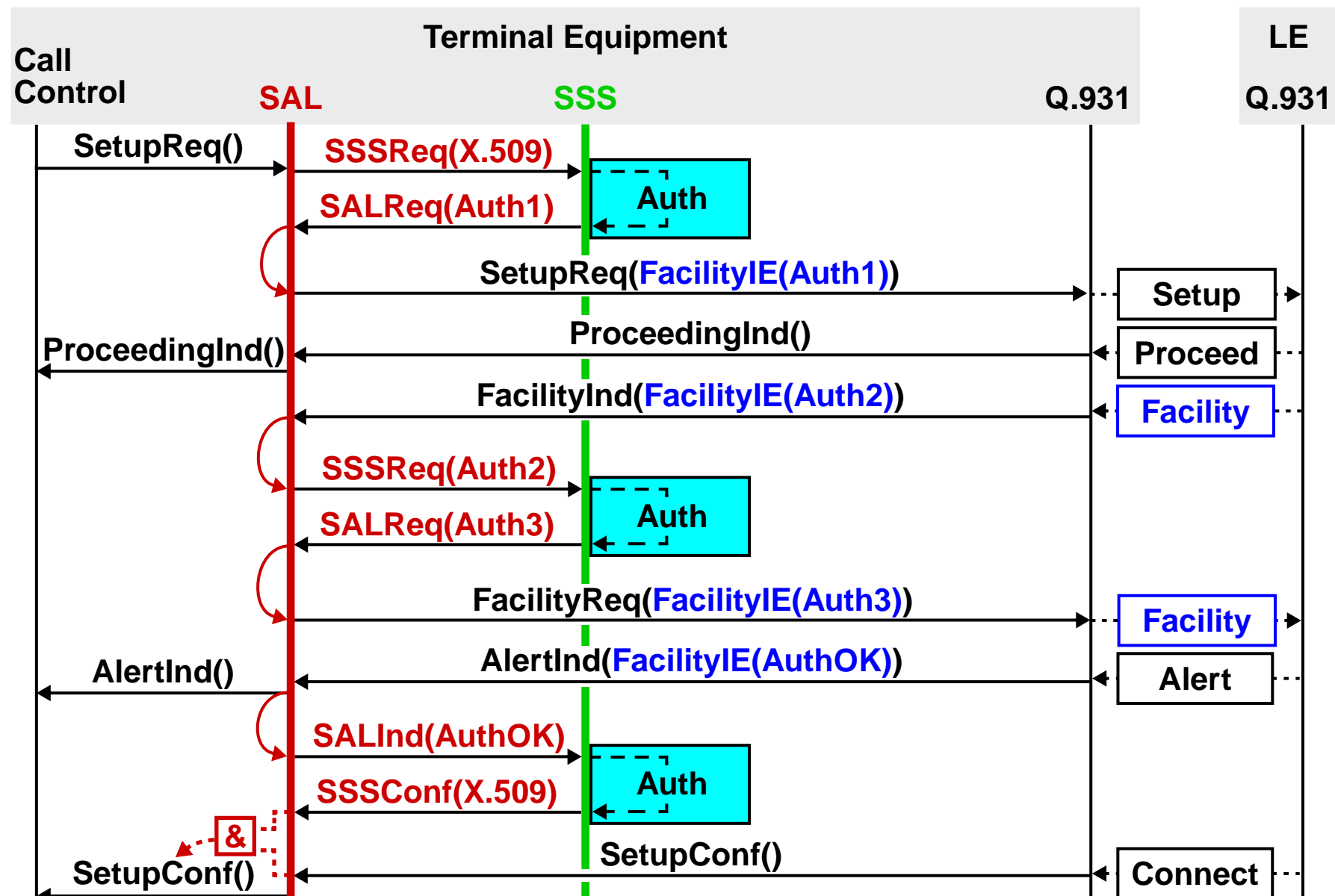
# Implementation



Reiner Sailer, 7<sup>th</sup> International Conference on Computer Communications And Networks (IC3N), Lafayette, LA, October 1998

# Architectural Enhancements

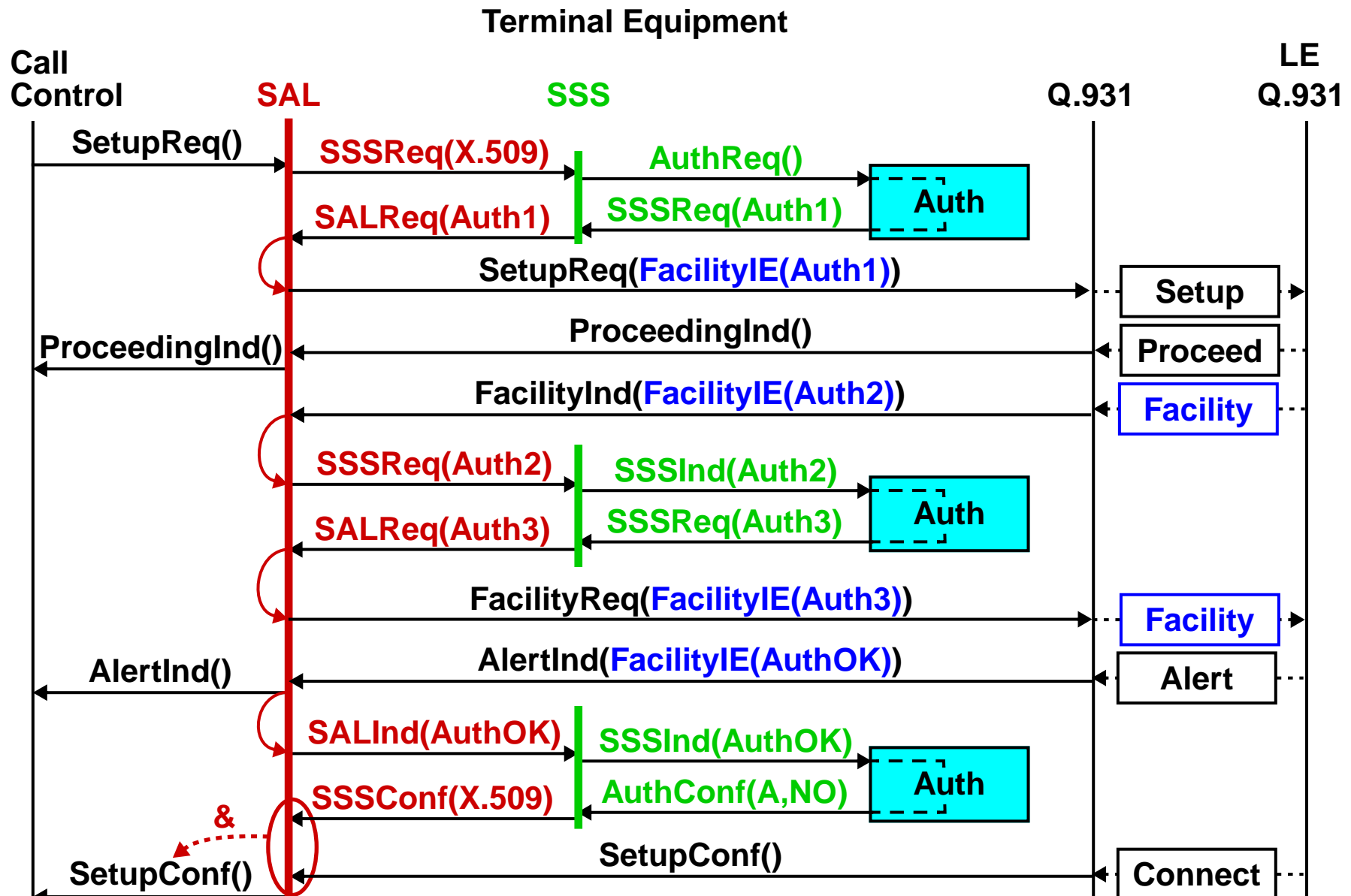
# Example



Reiner Sailer, 7<sup>th</sup> International Conference on Computer Communications And Networks (IC3N), Lafayette, LA, October 1998

# Architectural Enhancements

# Example (II)



Reiner Sailer, 7<sup>th</sup> International Conference on Computer Communications And Networks (IC3N), Lafayette, LA, October 1998

# Conclusions & Outlook

---

## ✓ Challenges

### Initial implementation

- ❑ intel-based PCs running Linux, ISDN Interface Cards, ISDN-PBX
- ❑ addressing (public key certificate) servers by E.164 ISDN number
- ❑ High Layer Compatibility parameter for SSS compatibility check
- ❑ synchronization by User To User Signalling

### Long term requirements

- ❑ means for addressing network internal servers via the UNI (e. g. URLs like [sss.cryptocom.org](http://sss.cryptocom.org))
- ❑ translation of URL-Global Title Addresses into MTP-addresses of SS7
- ❑ means for the efficient exchange of security control data
- ❑ standardized SSS protocols (e. g. Public Key Certificate Retrieval, Authentication, Encryption, Anonymity)

Reiner Sailer, 7<sup>th</sup> International Conference on Computer Communications And Networks (IC3N), Lafayette, LA, October 1998