Security Architecture of SEMPER

Torben Pedersen
Cryptomathic

Outline

- Goals of the architecture
- Overview of the architecture
- Service blocks - general structure
- Lower layers - individual service blocks
- Why are the goals obtained?

SEMPER overview

User requirements (customer / merchant)

Evaluation of trials

Legal aspects

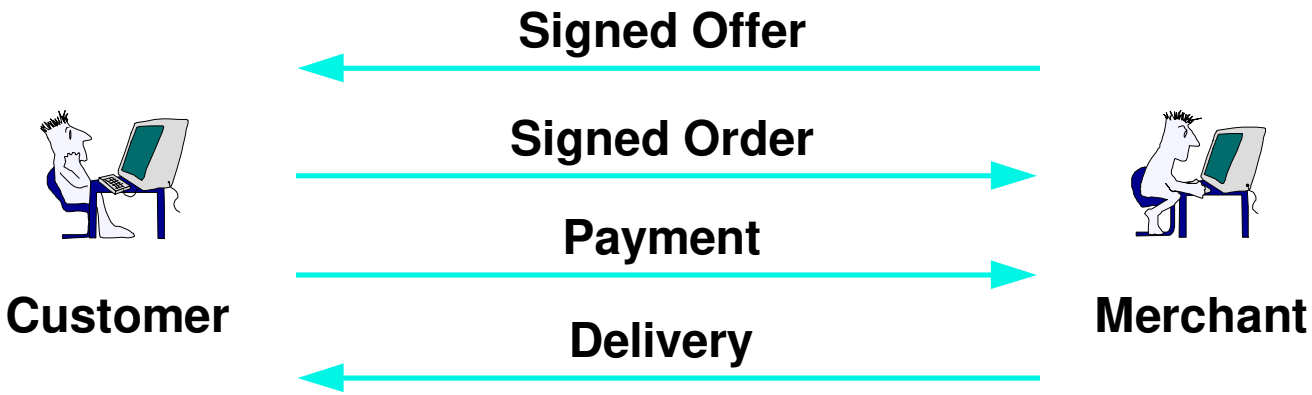
Making a security architecture

Implementing the architecture

Integrating business applications

Scenarios

Initial



Security requirements:

- authentication / non-repudiation
- secure payment
- confidentiality

Additional services

- Fair exchange (e.g., soft goods for delivery)
- Multiple customers (auction)

Security requirements

- Fairness
- Privacy
- “Multi-party security”

Goals of Architecture

Support secure implementation of

- **Envisaged scenarios**
- **Required services**

Openness

- **Independent of specific tools (e.g., payment systems)**
- **Possible to build new applications on top**
- **Public definition (allowing independent verification)**

SEMPER

Security Architecture of SEMPER

Browser/ Server

Third Parties

WWW Integration

Tinguin

Business Applications

Commerce Managers

Transfer and Exchange Managers

Payment Block

Certificate Block

Statement Block

Tinguin Block

Prefer. Block

Access Control

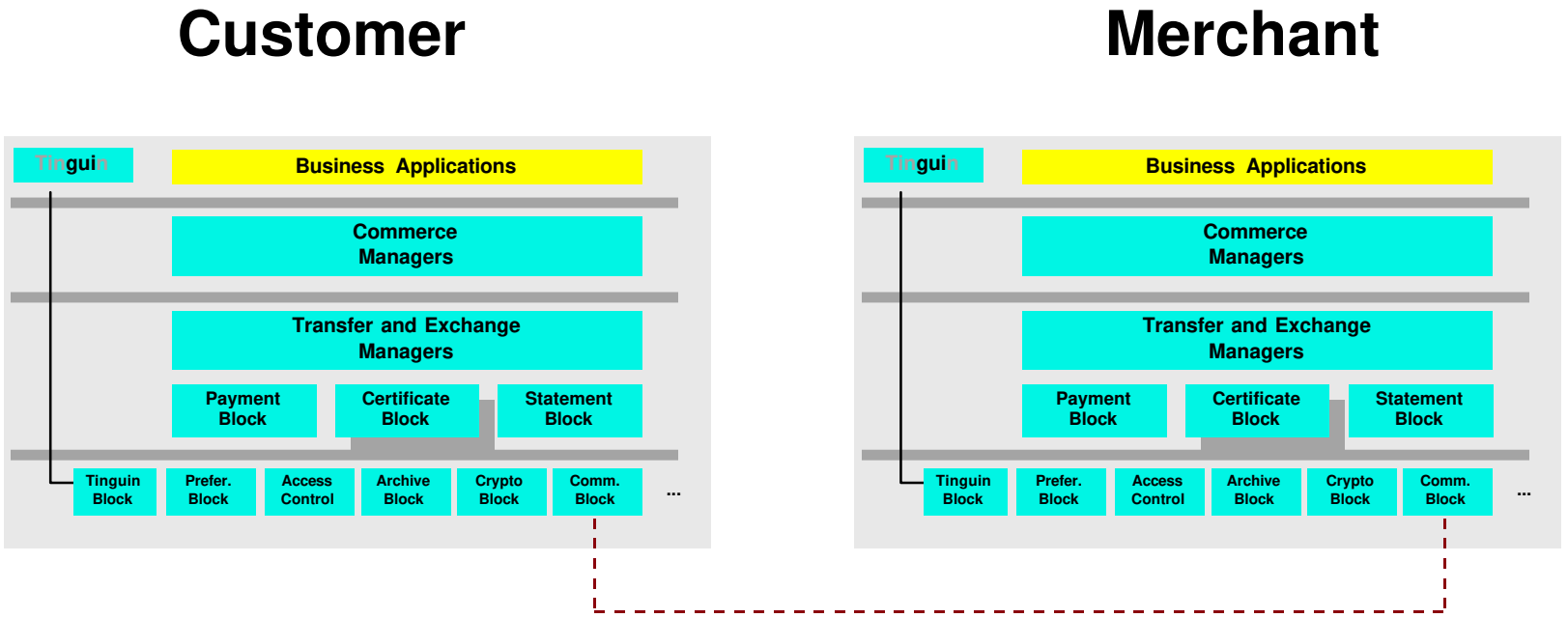
Archive Block

Crypto Block

Comm. Block

...

Uniform Architecture



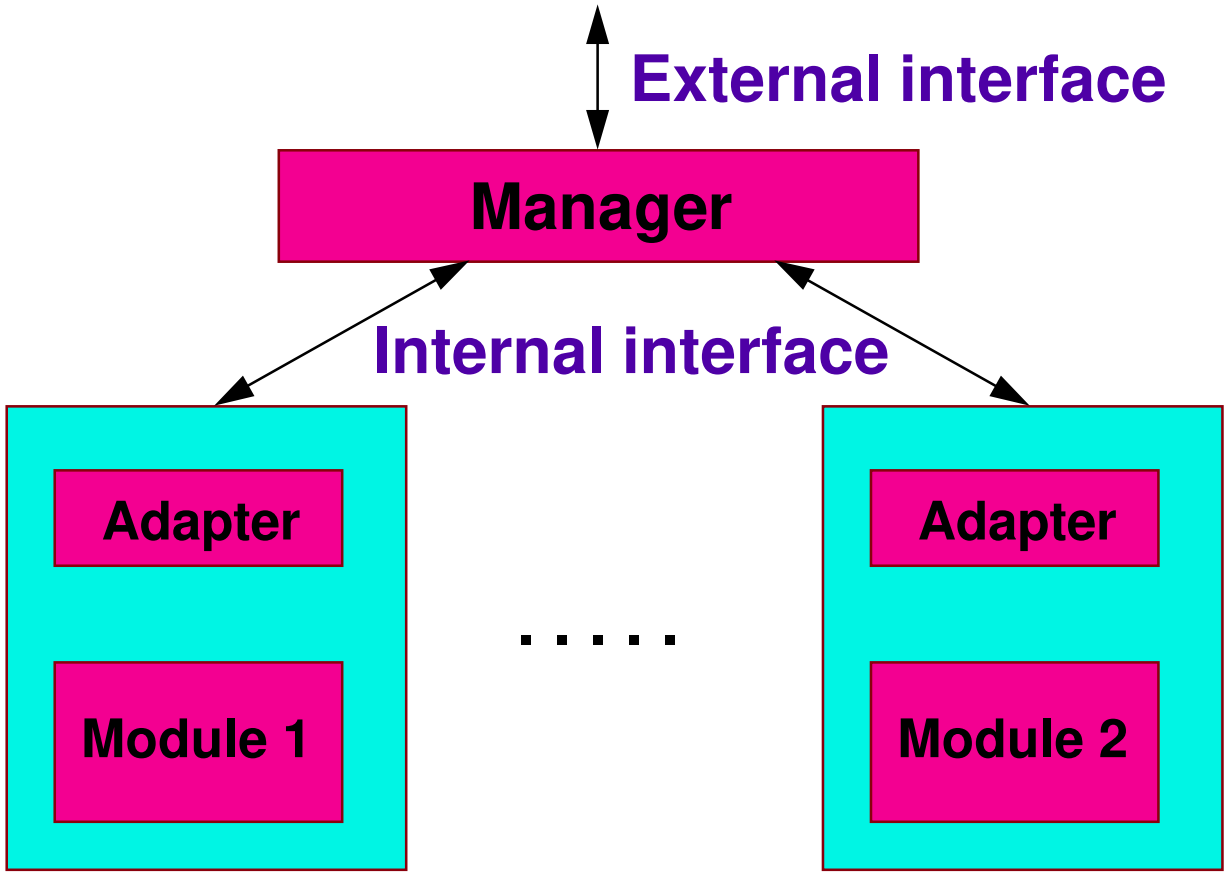
Transfers and Exchanges

Electronic transaction is composed of a number of transfers and exchanges

Commerce layer offers high level transfers and exchanges:

- **Get_offer**
- **Order**
- **Pay_and_deliver**

Structure of Service Block



Service Block Defines two Interfaces

External interface

Used by other SEMPER components

Internal interface

Used by manager to call module

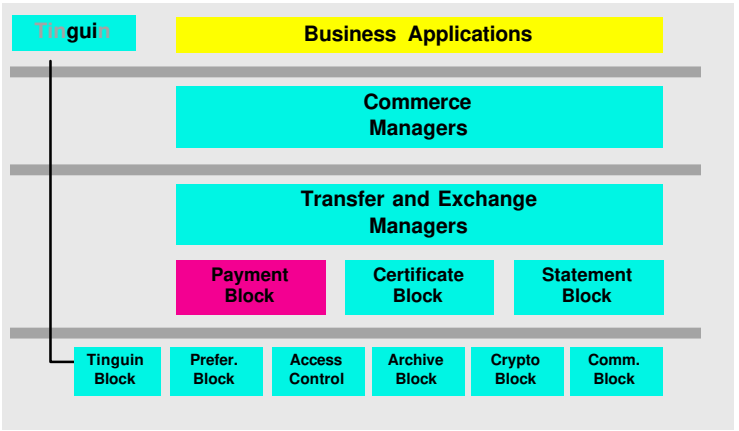
Adapter needed if module does not support interface

Requirement:

Possible to add/change module

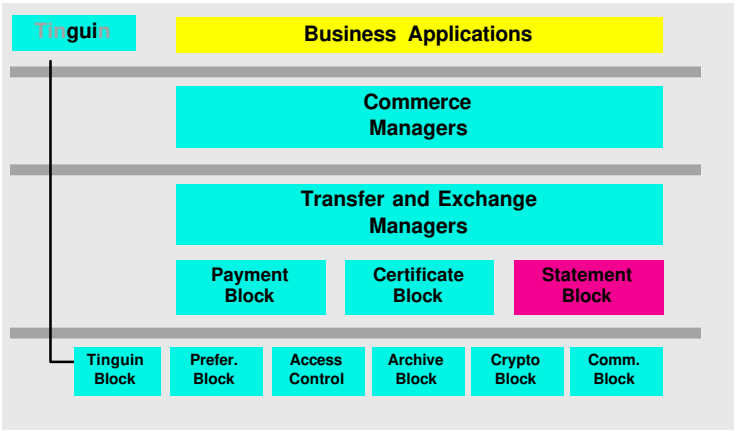
Define general internal interface for each block

Payment Block



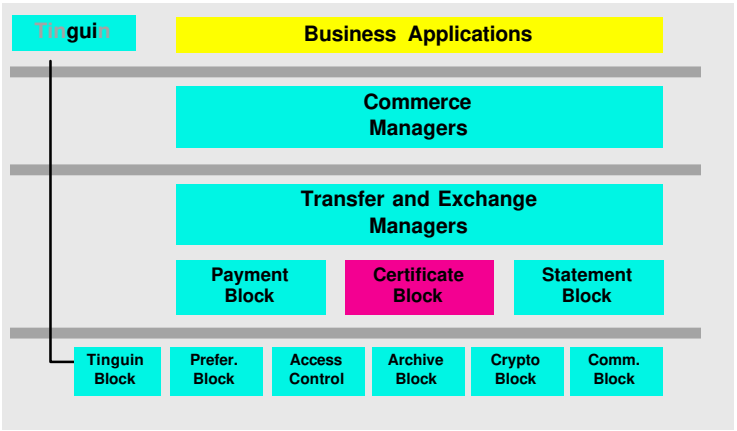
- **Management of purse and till**
- **Module corresponds to (implementation of a payment system) - different types supported**

Statement Block



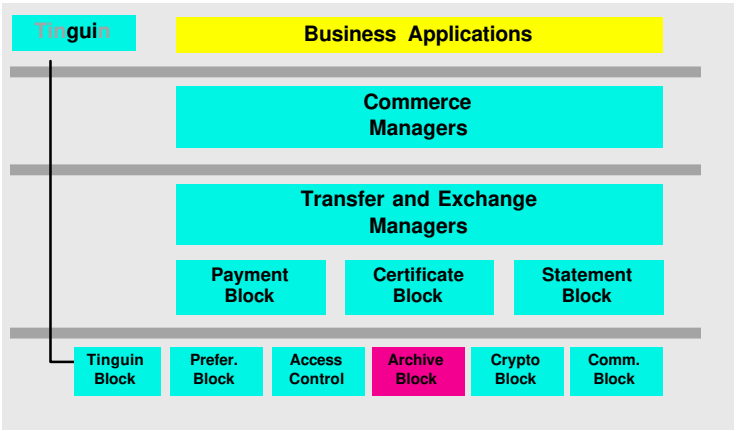
- Secure messages (statements)
- Module: key exchange

Certificate Block



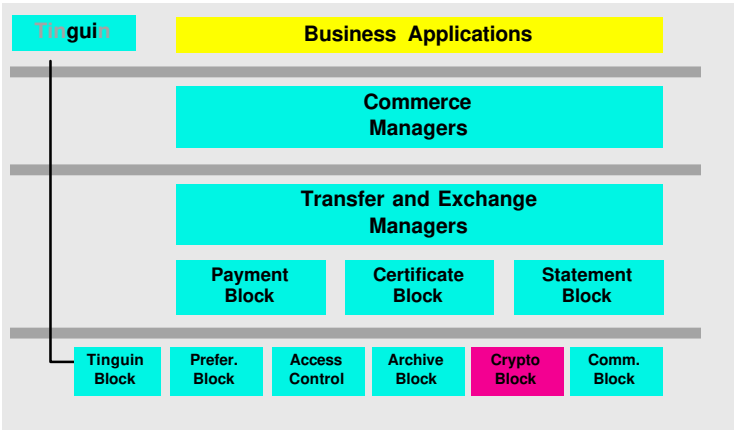
- Registration, certification, certificates
- Module:
  - Actual certificate
  - Registration / certification

Archive Block



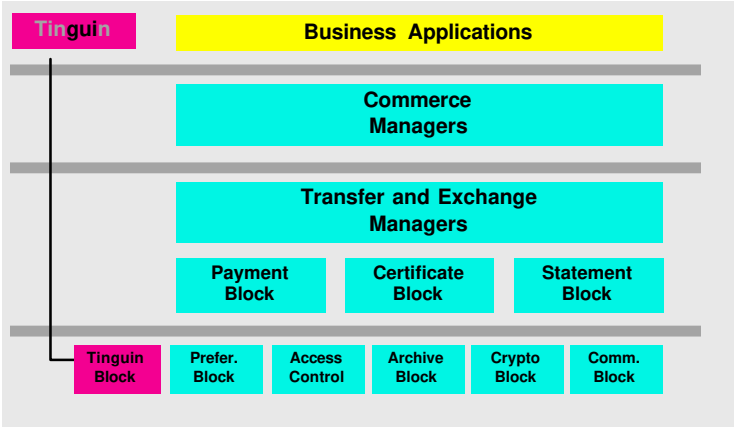
- **Functionality for (secure) storage**
- **Module: database**

Crypto Block



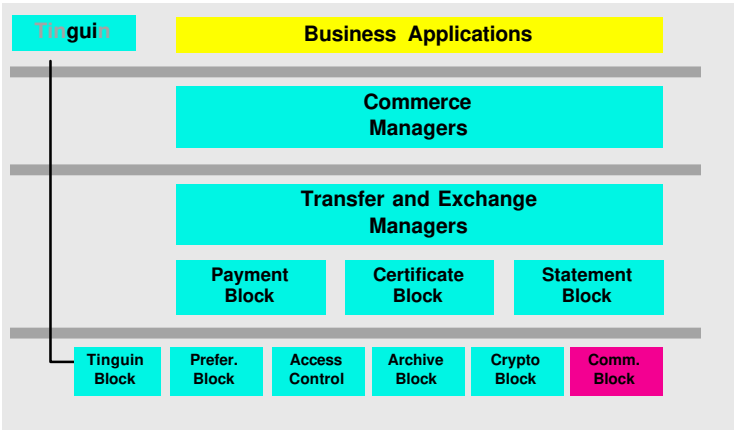
- **Provides functionality for cryptographic functions**
- **Module: cryptographic tool (e.g., chip card)**

TINGUIN



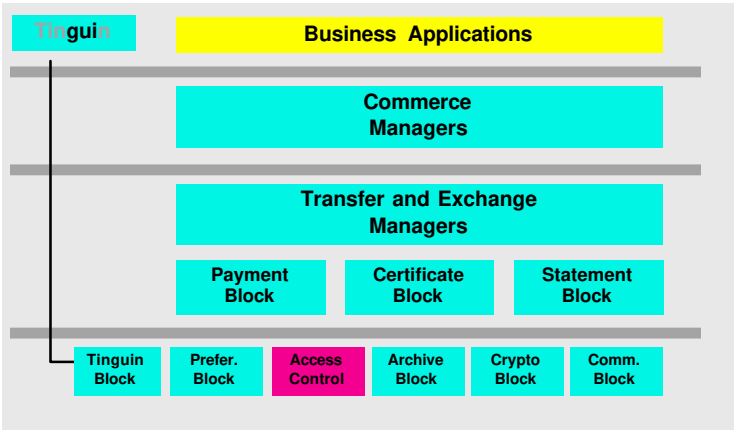
- **Functionality for (secure) user interface**
- **Module: display and keyboards**

Communication Manager



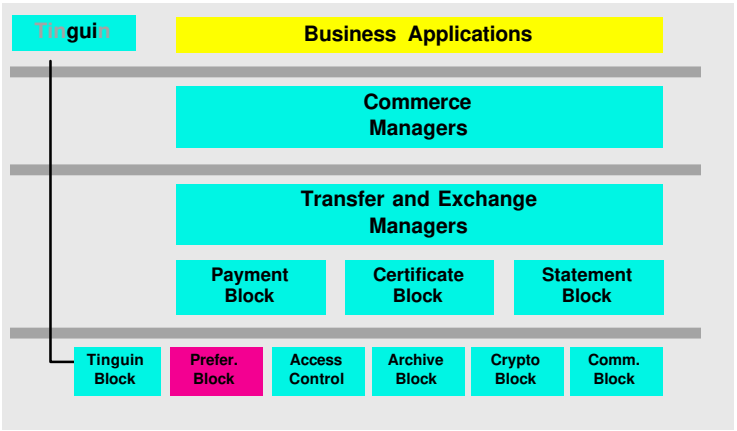
- **Functionality for communication**

Access Manager



- Functionality for (local) access control
- Access control to software (external software limited access to SEMPER software)

Preference Manager



- Local configuration of user software
- Handling user preferences

Conclusion

Security of services:

- **SEMPER provides a set of high level secure services**
- **Access control prevents misuse of services on lower layer**

Openness

- **Service block structure provides independence of specific tools**
- **Open design**
- **Integrating business applications - to be seen**