SOFSEM 2008

High Tatras, Slovakia,
Jan. 19 – 25, 2008

Strong Authentication over Lock-Keeper

Feng Cheng, Christoph Meinel

Hasso-Plattner-Institute,

University of Potsdam, Germany

Strong Authentication over Lock-Keeper

- Introduction
- Background:
  - Strong Authentication
  - Physical Separation and Lock-Keeper
- **Lock-Keeper Strong Authentication Framework**
  - Motivations, **Framework** and benefits
- **Security Enhancement of Lock-Keeper Web Service Module**
  - Architecure, User Scenario and Experiment Results
- Conclusions

Introduction (1)

- Compare to user-password authentication, **Strong Authentication** meets the increased security requirements, which enables organizations to verify user identities with high degree of certainty

- Existing Strong Authentication solutions: physical token (smart card), X.509, SAML-Token, and biometric authentication, etc.

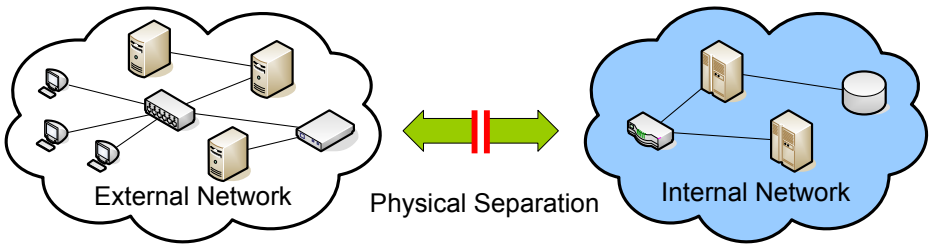
- A centralized Identity and Access Management (IAM) system is usually required to store and manage the credential-related components, e.g. user profiles, privacies or certificates, policies

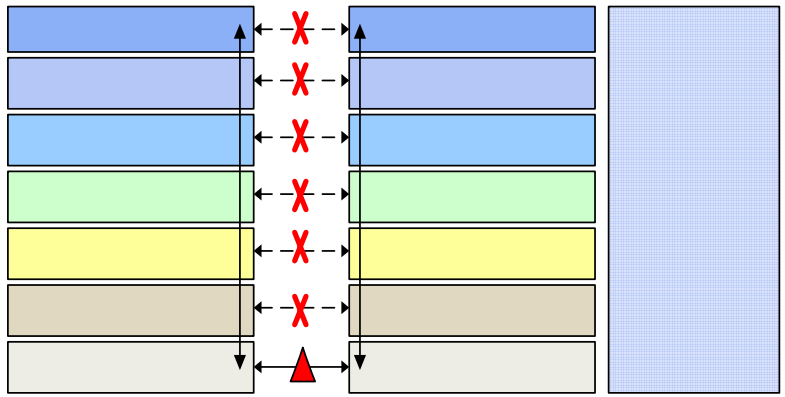
- The possibility to attack the IAM and its protected resources comes along while the IAM host exposes connections to outside.

- To protect the IAM system and its hosted authentication procedure against those malicious attacks has been a main task

Introduction (2)

- Physical Separation has been recognized as an efficient method to guarantee the **highest level** security and prevent **online network attacks**
- It can be used to protect the sensitive IT-Infrastructure or its components, such as IAM part for most Strong Authentication frameworks
- An integrated Strong Authentication framework is also required by most “Physical Separation” protected applications, such as web services, etc.
- So, we propose an advance authentication framework to combine Strong Authentication and **Physical Separation**





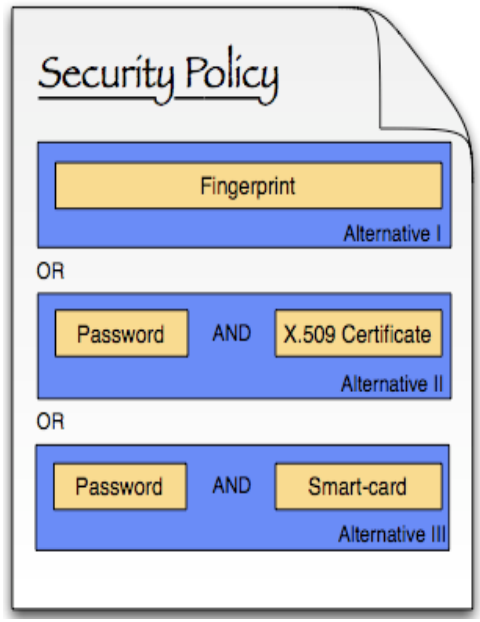
Background (1) – Strong Authentication

- The traditional weak authentication method, e.g. user-password
  - only requires the information of "**something you know**" from users
  - is vulnerable to such attacks as Keystroke Monitoring, Dictionary Attacks, Network Sniffing, Man-in-Middle attack, Social Engineering attack, etc.
- The **strong authentication** demands many additional information
  - **Something you are**
  - **Something you have**
  - **Something you can do**
  - **… …**

- Strong Authentication is also defined as **two / multiple factors** authentication.

Background (2) – Strong Authentication

- With the rapid growth of **e-Commerce**, **e-Banking** and **e-Government**, more and more organizations have deployed strong authentication solutions to protect their online resources and services
- Strong Authentication is always realized and performed in **loosely coupled** network environment, such as **Service Oriented Architectures** (**SOA**).
- Serveral **assistant techniques, standards and even products** have been developed, e. g.:
  - X.509, SAML,SSO, IAM, LDAP, JAAS, RSA SecurID, Kerberos, IPSEC, SSL/TLS, Windows live ID, OpenID, OpenSSO, ...
- How to **securely** set up these technologies in a certain exsiting IT-Infrastructure as well as **reliably** perform the authentication proceadures is a problem.



Background (3) – Physical Separation

- Attacks targeted on the whole private network has been the most dangerous challenge of security.
  - **online attack** and offline attacks
  - known attacks and **unknown attacks**
  - **Insider attacks** and outsider attacks
- If you are connected to the network, you would be **always** at the risk of being attacked.
- **The ultimate method to secure a network is to disconnect it**
- The main task is to separate the private network at both logical and physical levels, and simultaneously permit secure data exchange **– Physical Separation.**

Background (4) – Physical Separation

Related Works: Known Implementations of „Physical Separation“

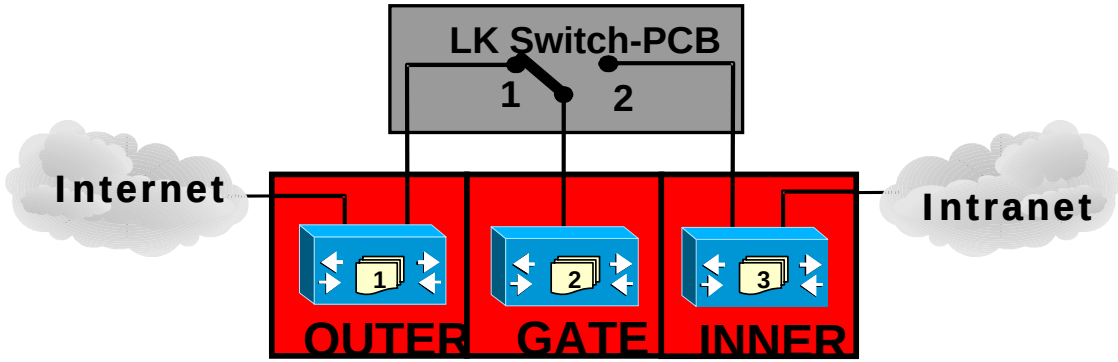
- **NRL Pump – from US Naval Research Laboratory (NRL)**
  - It cannot really separate the two communicated sections in the physical layer because both the high (destination) and low (source) “processes” share a same “communication buffer”
- **Air-Gap Technology** includes
  - Two independent computers, a connection switch and a shared “Memory Bank”
  - Whale’s **e-Gap** system is successful in providing VPN solution (taken over by Microsoft in 2006)
- “**Security Guard**” (SG)
  - The SG grants a “one way traffic” between two systems and a kind of “Human Review”, which is a central part of this structure
  - A special hardware is required to realize the one-way controller
- **Others**: Physical Separation Card, Shared SCSI Device, …

Background (5) – Lock-Keeper

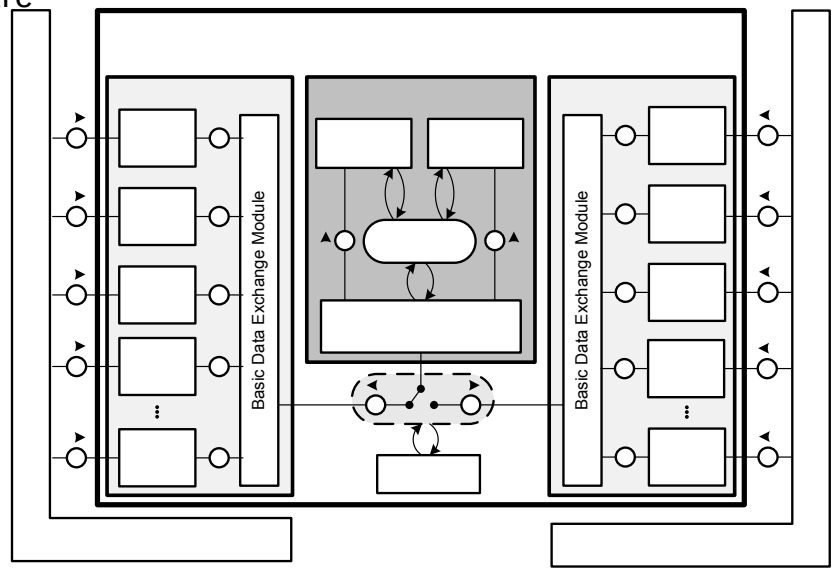
Lock-Keeper, which is a new implementation of PS-Idea, consists of

- 3/4 active **SBC**-based (Single Board Computer) Units and a patented **switch PCB**

LK Switch-PCB



- Lock-Keeper **SDE (Secure Data Exchange)** Software
  - Several Application Modules (INNER/OUTER)
    - File eXchange (File-X)
    - Mail eXchange (Mail-X)
    - Web Services (WS)
    - Database Replication (DB-Rep)
    - ... ...
  - Basic SDE Module (GATE)
    - Application-level Data Exchange
    - No Server running on GATE
    - Pull-Push mechanism
  - Security Module (GATE)



Background (6) – Lock-Keeper

- There is the traditional conflict of **security and usability**. Lock-Keeper is a solution for high level security requirement.
- It's not proposed to replace the conventional network firewall.
- In 2005, we started a cooperation with "Civil and National Security" Department of Siemens Switzerland
- Siemens Switzerland has started to produce the commercial version of the Lock-Keeper (OEM).

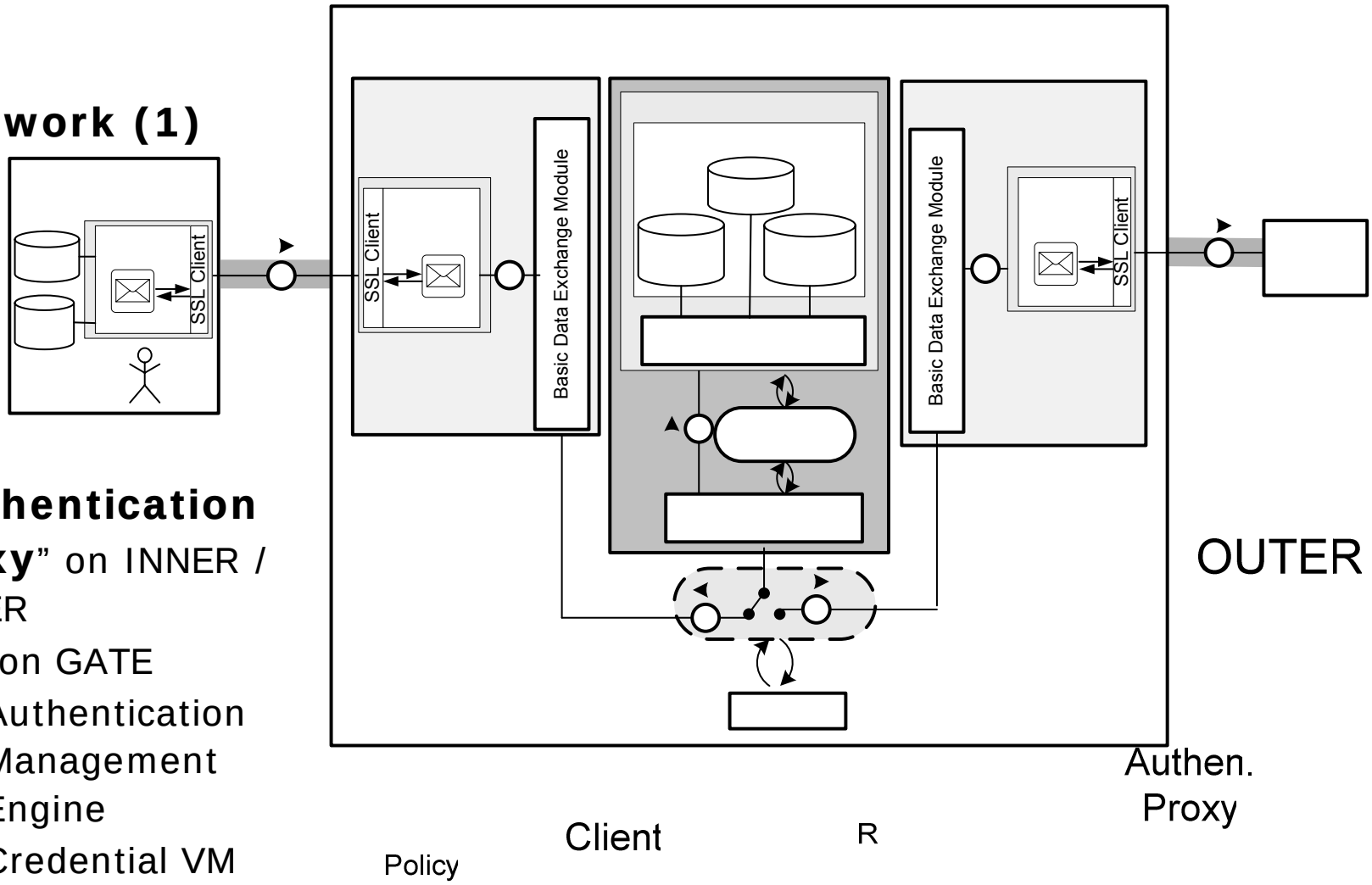
Lock-Keeper Strong Authentication Framework (1)

Our Motivations to combine Strong Authentication with Physical Separation:

- **Credentials** required by the strong authentication, such as user information databases, privacy database and certificate store, etc., should be saved safely – impossible to be directly accessed
- The **authentication methods** or cryptography algorithms can be flexibly deployed on GATE – impossible to be changed or abused.
- The authentication operations and procedures should be performed unaffectedly in an isolated environment – "**offline authentication**".
- The **internal resources** including all the internal hosts and the network infrastructure should be protected well while normal network services are provided simultaneously.
- This Lock-Keeper Authentication Framework is required to make it possible for Lock-Keeper to support more web based applications and proffer protection for more practical scenarios – significantly improve the **Lock-Keeper's usability.**

Lock-Keeper Strong Authentication Framework (2)

Framework (1)



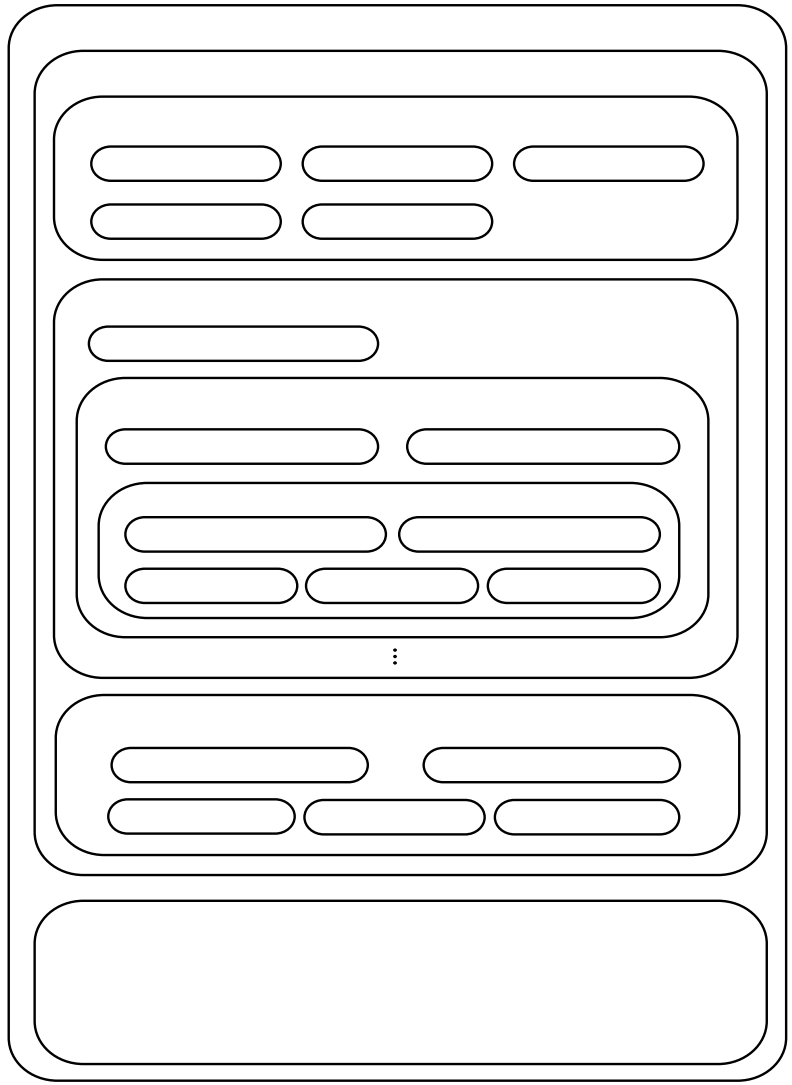
- "**Authentication Proxy**" on INNER / OUTER
- **IAM** on GATE
  - Authentication Management Engine
  - Credential VM

Lock-Keeper Strong Authentication Framework (3)

Framework (2)

"Authentication Proxy" on OUTER / INNER

- External users communicate with the "***Authentication Proxy***" using **normal** network connections.
- The proxy will parse the data traffic, i.e. network-level packets, belongs to this received request and then reconstruct into the application-level **LKMC** (Lock-Keeper Message Container):
  - a message body
  - a message header

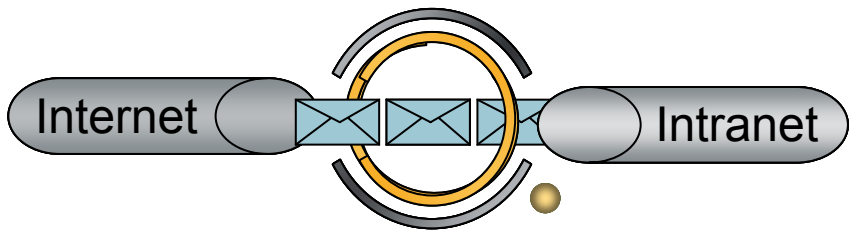


Lock-Keeper Strong Authentication Framework (4)

Framework (3)

"Authentication Proxy" on OUTER / INNER

- After being preprocessed on OUTER, the LKMC is transferred to GATE through the Lock-Keeper "***Basic Data Exchange Module***".
- As soon as it completely arrives at GATE, the "***Authentication Management Engine***" will pass it to the IAM system.
- The "*Authentication Proxy*" on INNER forwards the LKMC message to the protected service host (i.e. **the internal server**), which is located in the internal network.
- Then the response message can be generated after the invocation of requested applications.
- Similar to the incoming request message, the **outgoing response** message is also required to be issued, signed, and encrypted by the internal server and GATE as well.

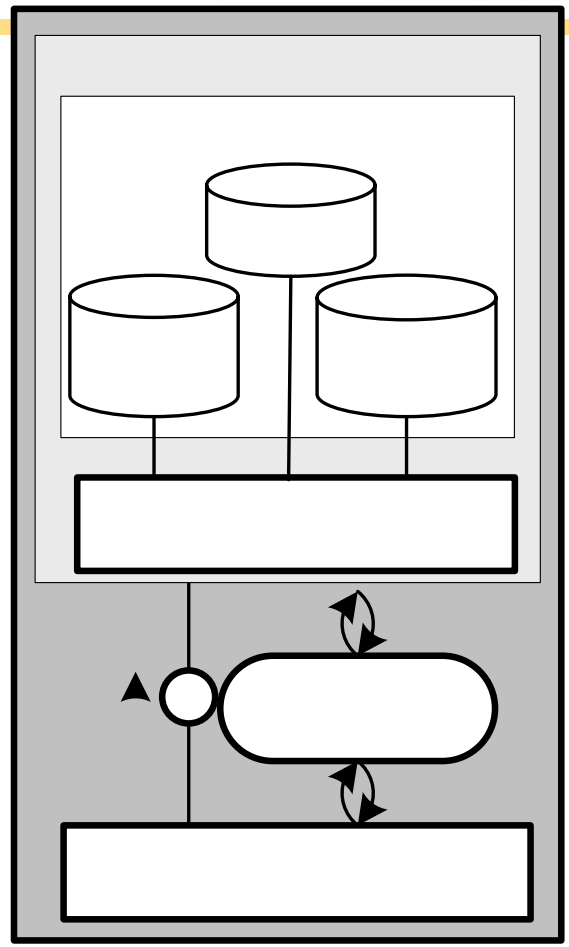


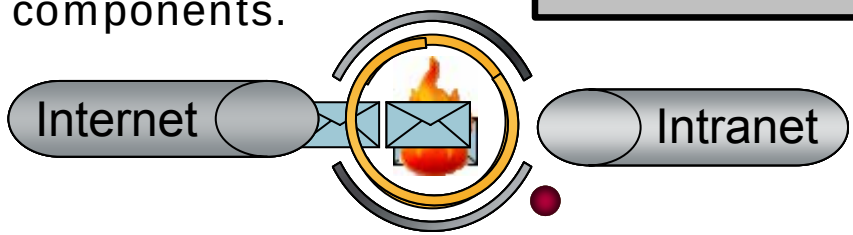
Lock-Keeper Strong Authentication Framework (5)

Framework (4)

IAM System on GATE

- The LKMC message is required to be authenticated by the IAM System on GATE, which is designed based on "***Strong Authentication***".
- The whole authentication procedure is started and controlled by the "***Authentication Management Engine***", which
  - decrypts the LKMC
  - extracts authentication information.
- Then, further authentication operations can be performed by communications between the "*Authentication Management Engine*" and the corresponding credential components.



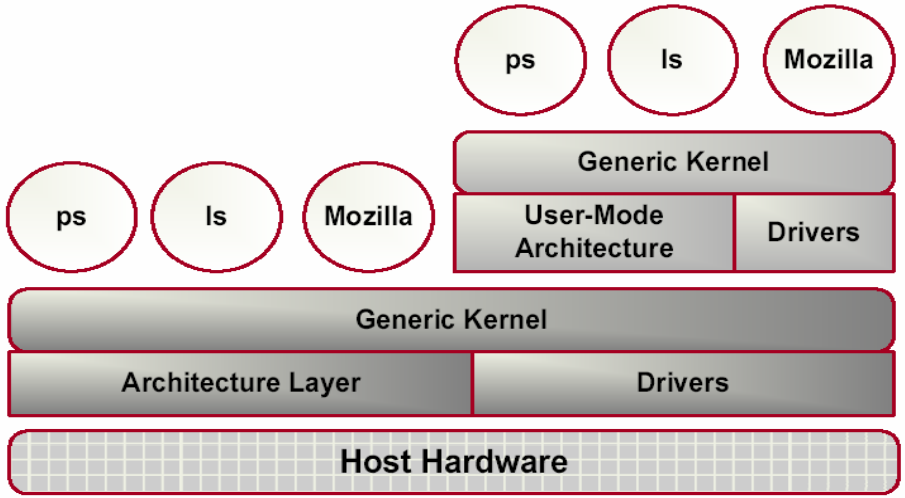


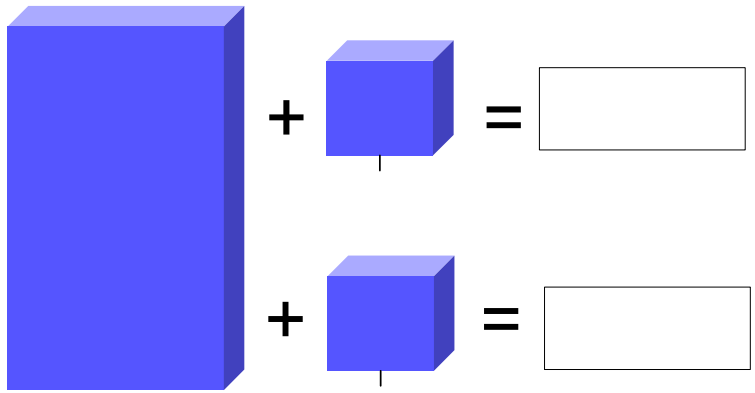
Lock-Keeper Strong Authentication Framework (6)

Framework (5)

IAM System on GATE – Virtual Machine (VM) Technology

- **Offline Authentication**
  - Physical Separation
  - VM Isolation
- **Offline Maintaining**
  - **Copy-On-Write (COW):** **D**ifferent VMs can share **the same unchangeable base Image-File**, and the difference can be saved in independent small-size COW file.

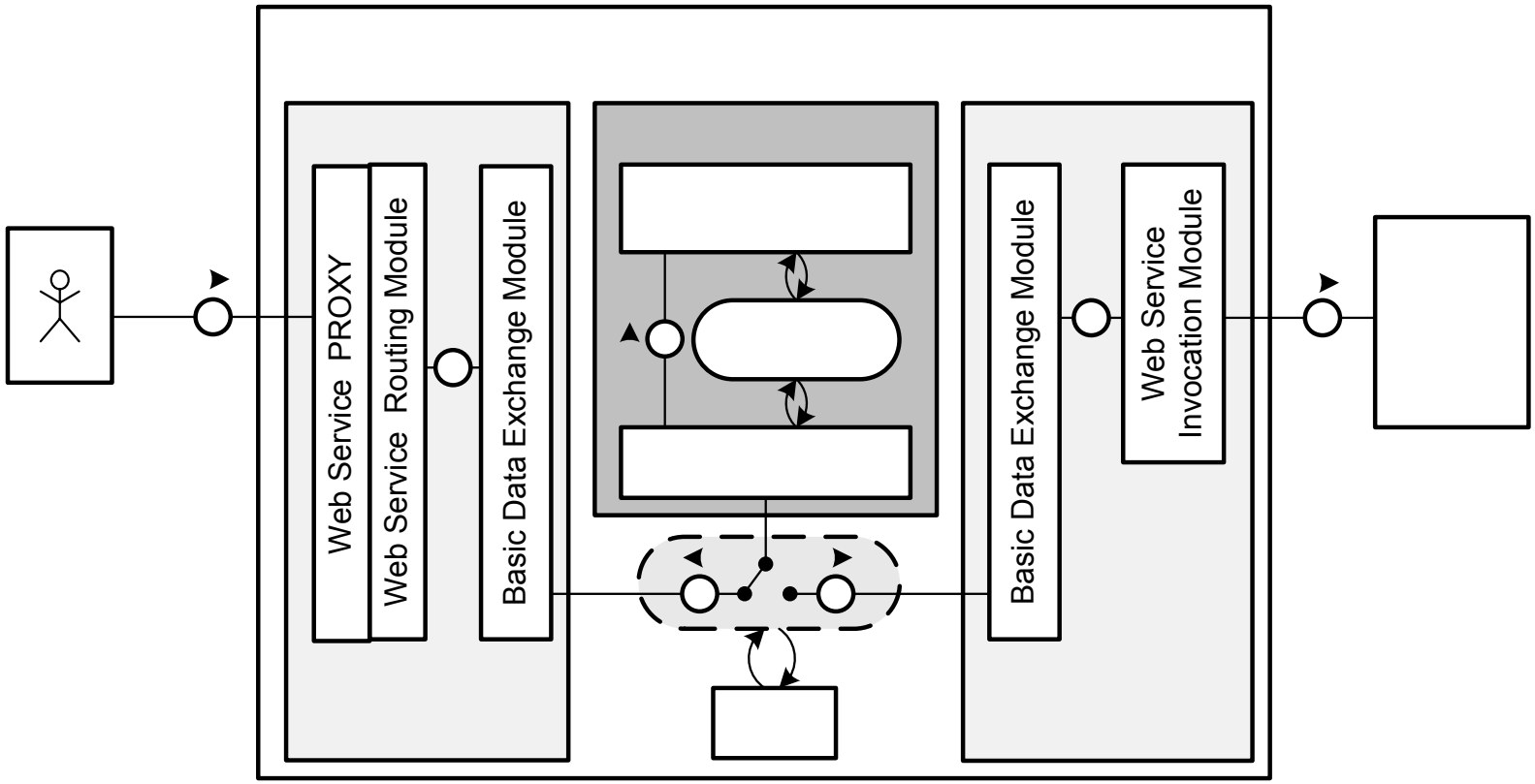




Security Enhancement of Lock-Keeper Web Service Module (1)

Architecuture (1) – Overview

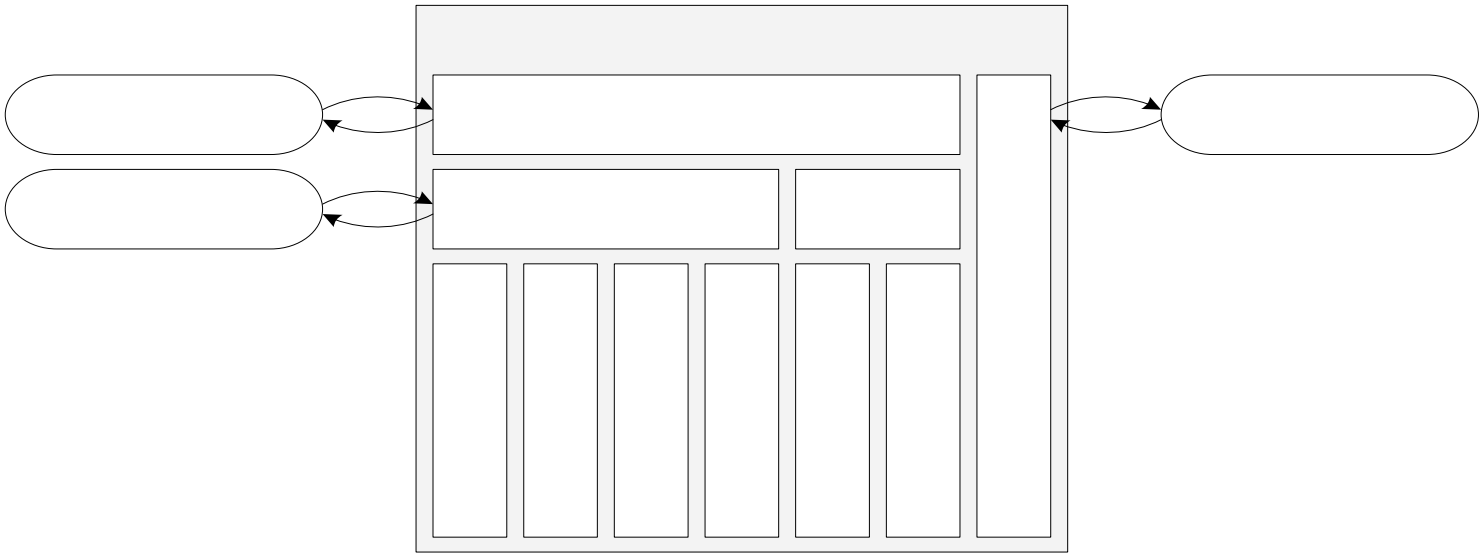
- **Our Web Service Module requires authentication**



Security Enhancement of Lock-Keeper Web Service Module (2)

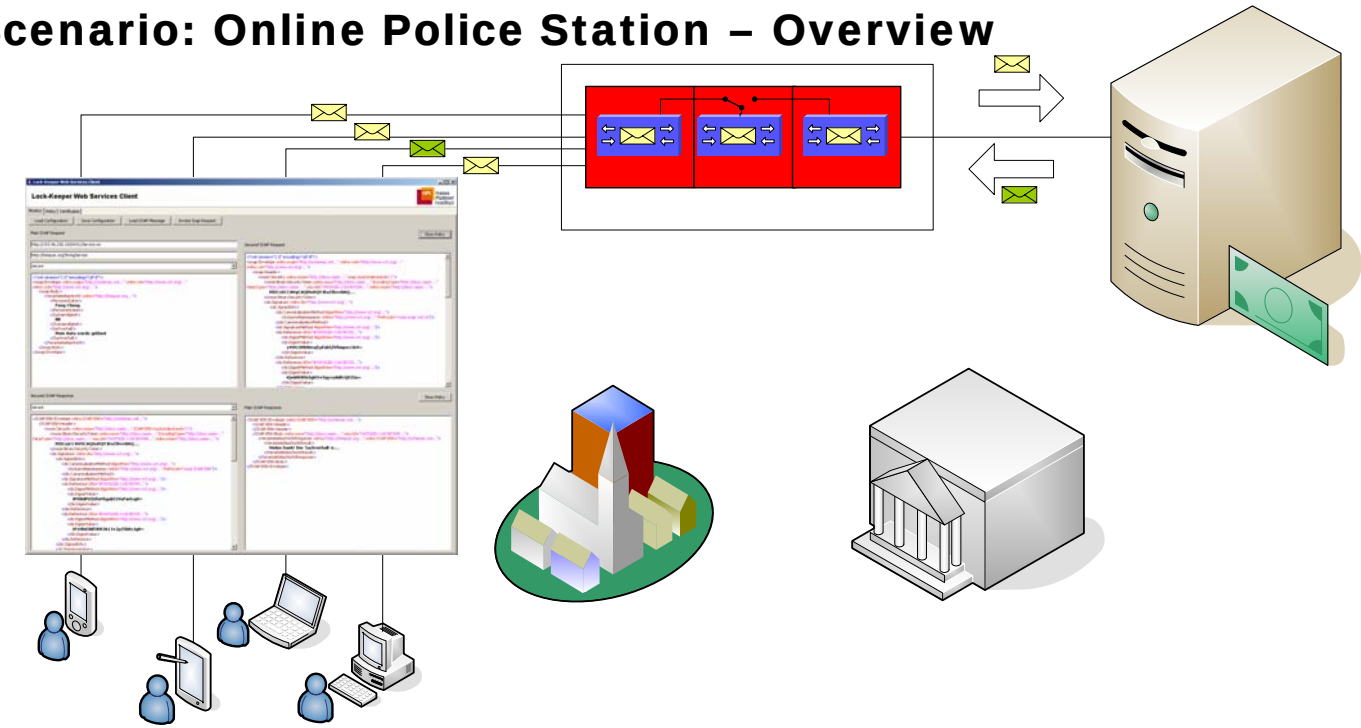
Architecuture (2)

- **Implement "Authentication Proxy"**
  - **"Web Service Proxy" and "Web Service Routing Module" on OUTER**
  - **"Web Service Invocation Module" on INNER**
- **Implement "Strong Authentication"**
  - **SOAP Verification on GATE: WS-Policy, WS-Security, … …**



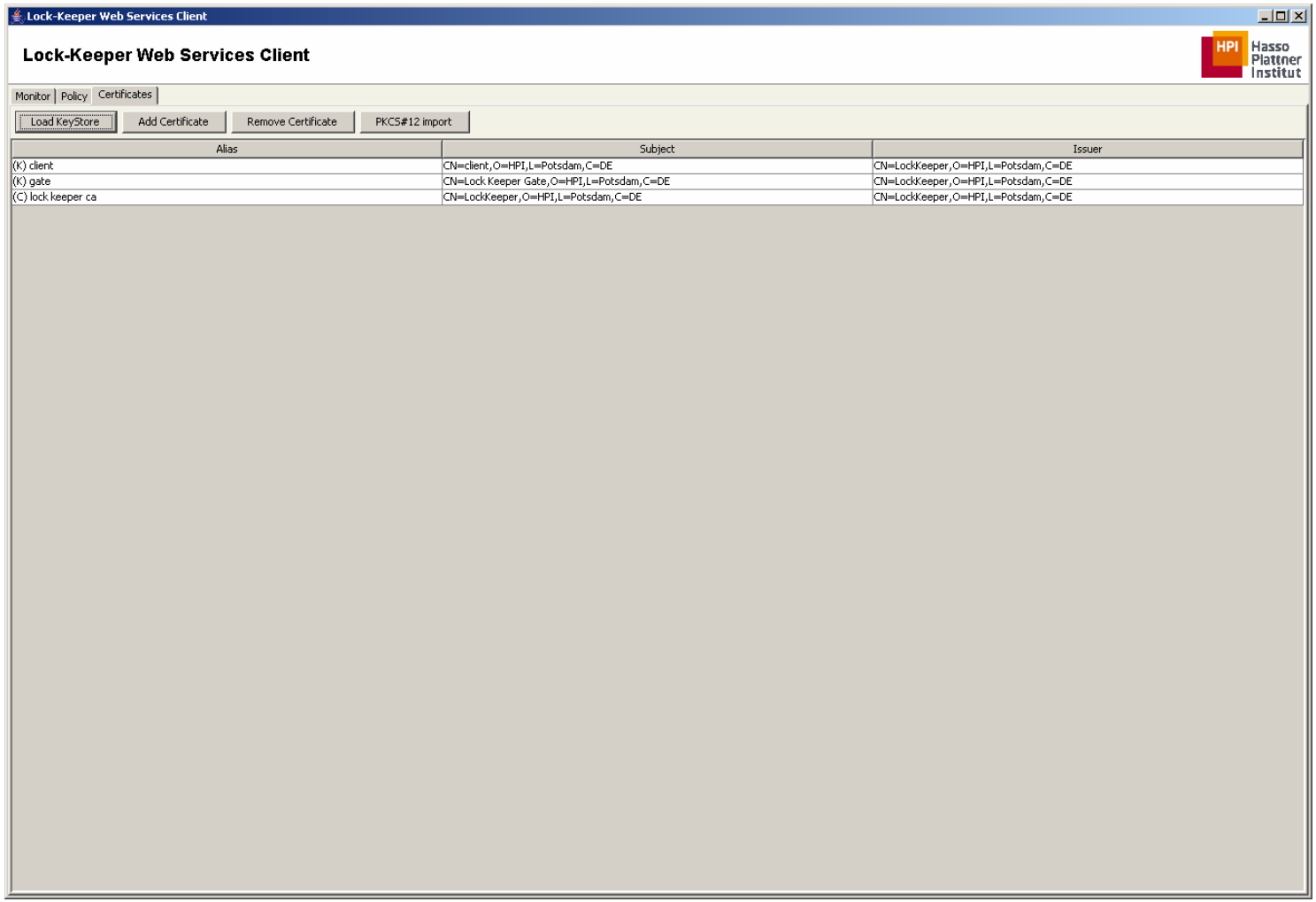
Security Enhancement of Lock-Keeper Web Service Module (3)

User Scenario: Online Police Station – Overview



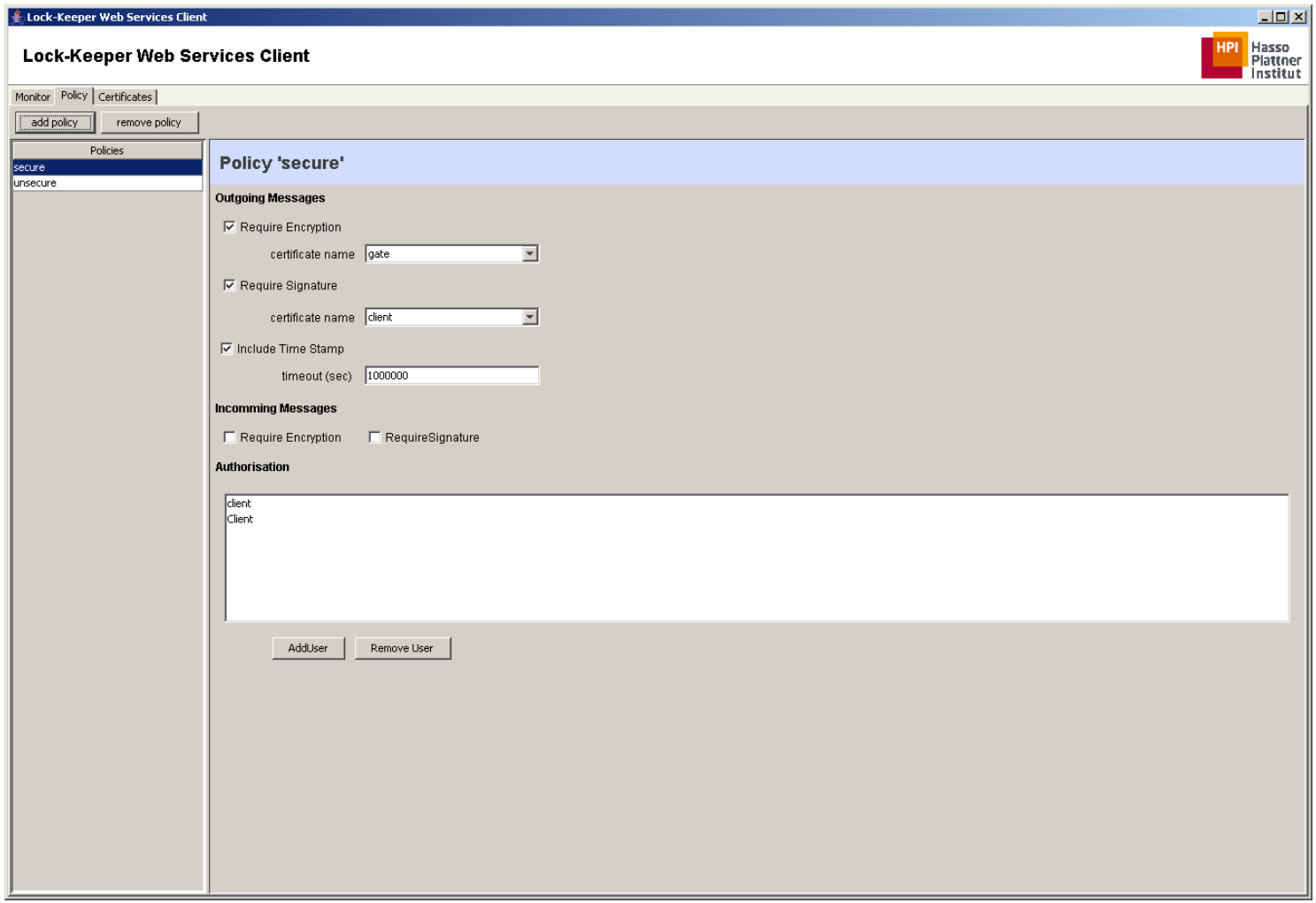
Security Enhancement of Lock-Keeper Web Service Module (4)

WS Client: Certificates Panel



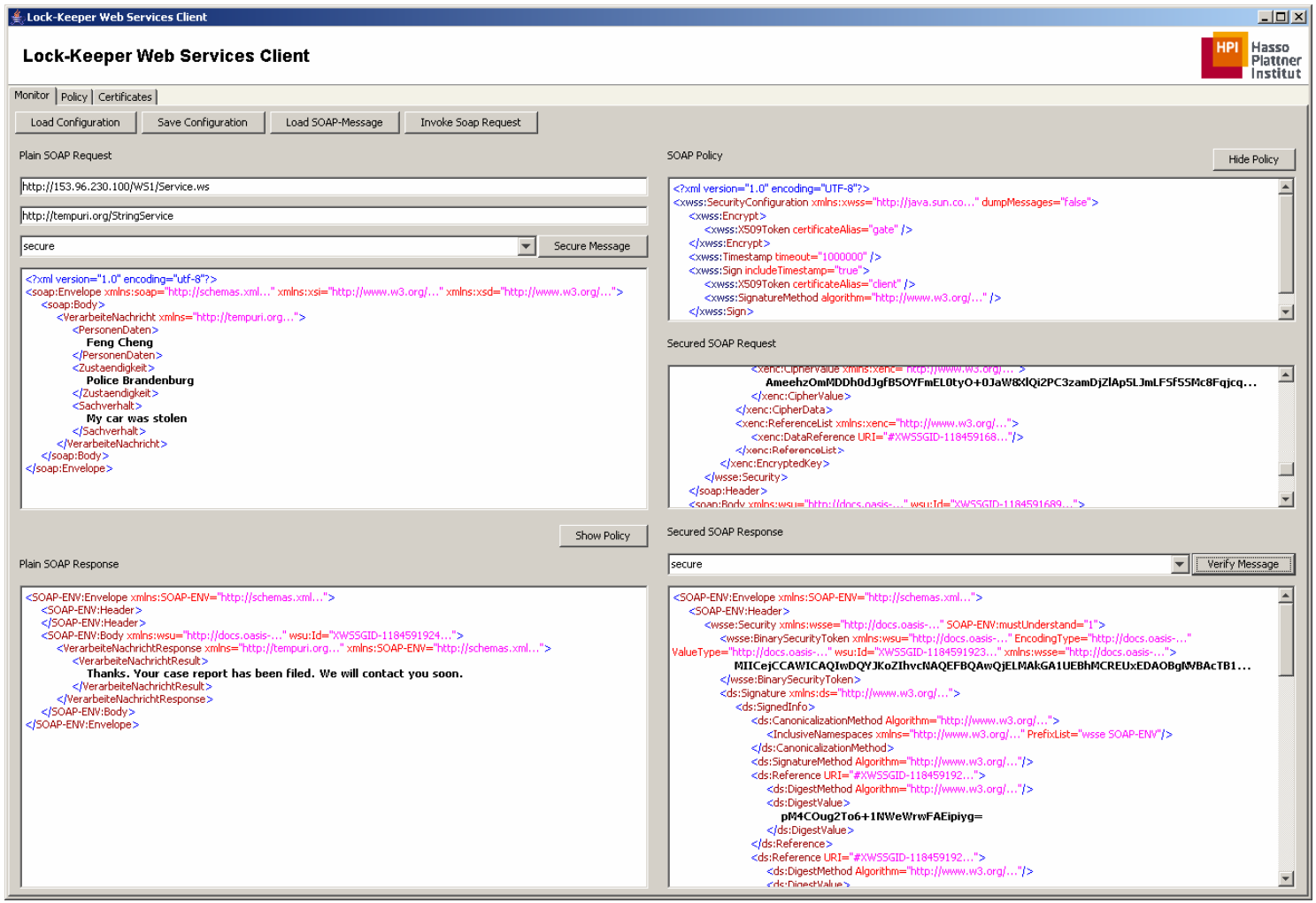
Security Enhancement of Lock-Keeper Web Service Module (5)

WS Client – Policy Panel



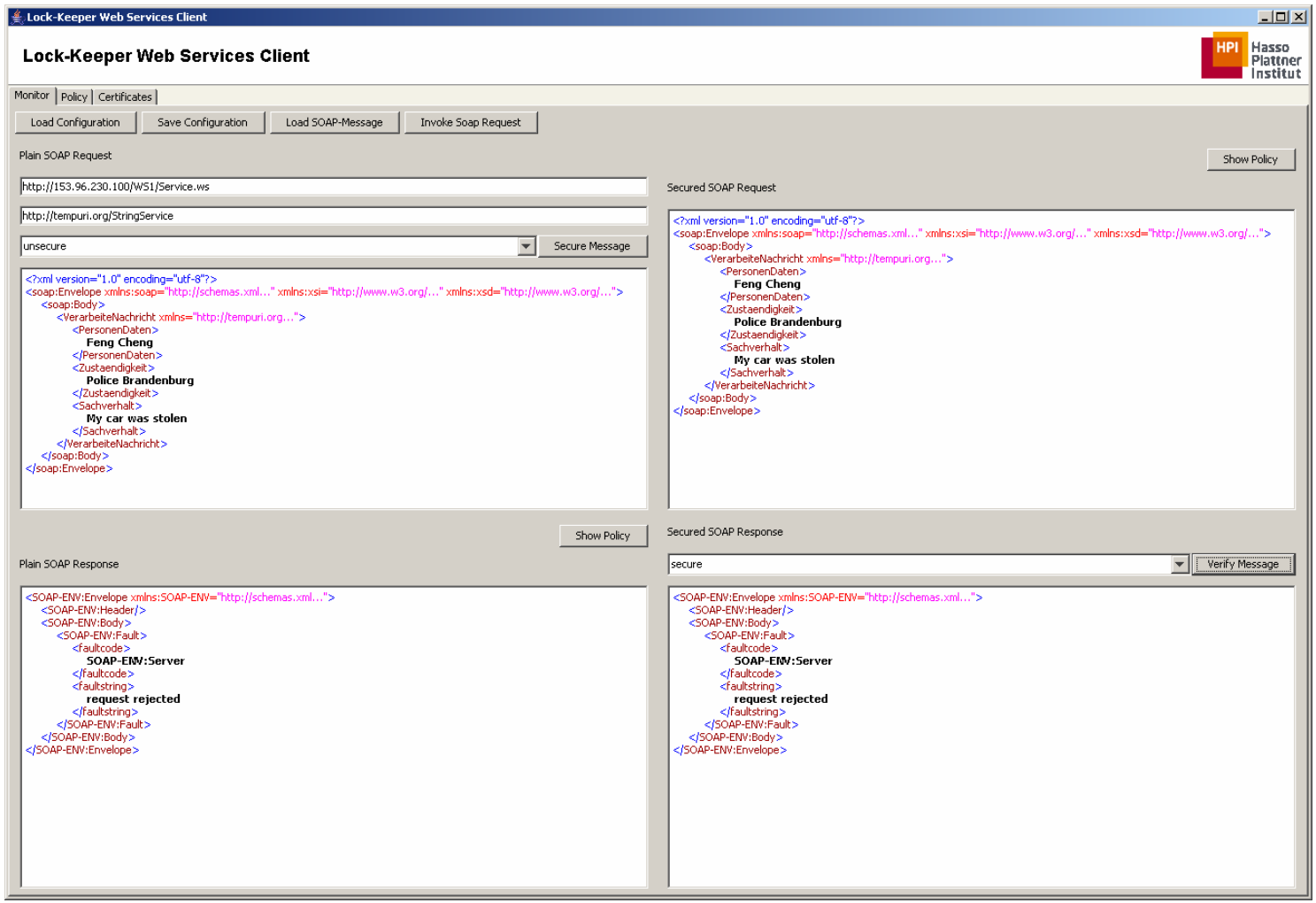
Security Enhancement of Lock-Keeper Web Service Module (6)

Experiment Results (1)

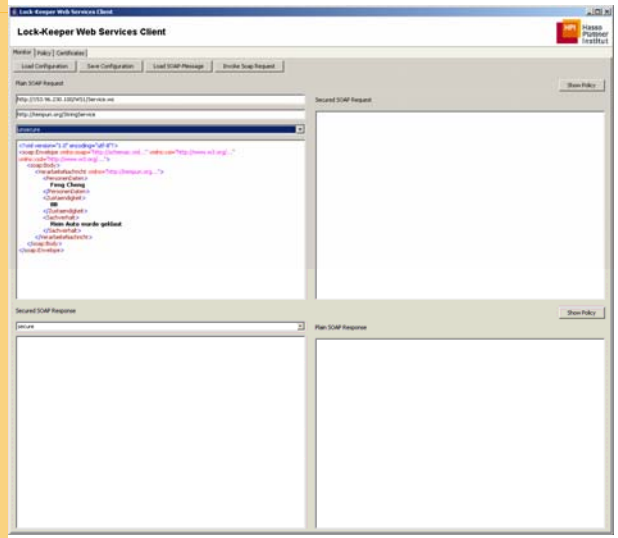


Security Enhancement of Lock-Keeper Web Service Module (7)

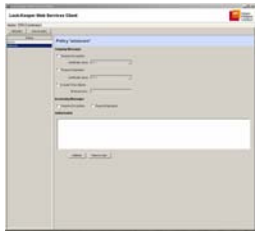
Experiment Results (2)

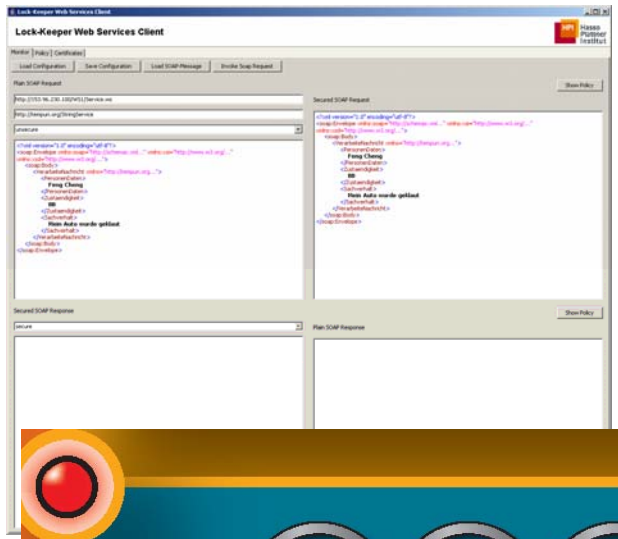


Security Enhancement of Lock-Keeper Web Service Module (8)

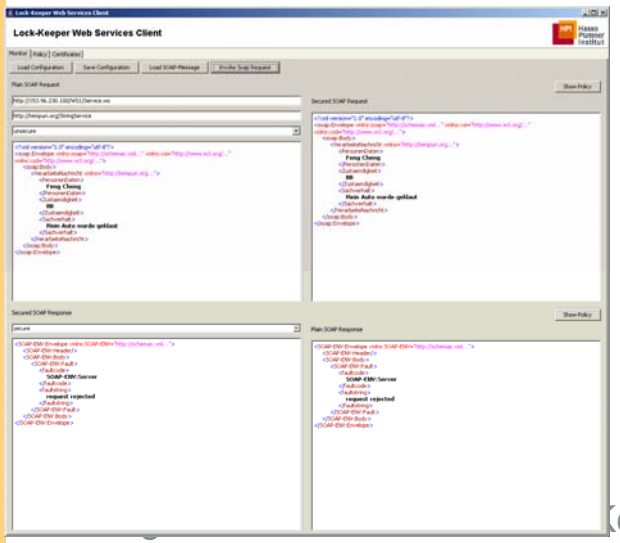


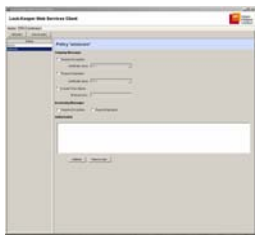
US-Policy



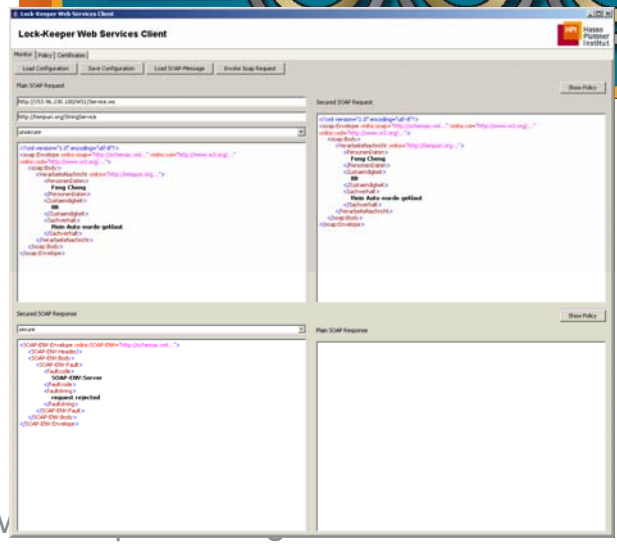


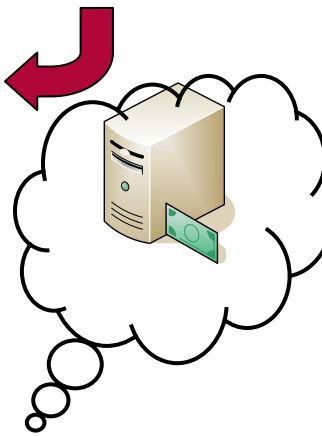
WS-Invoking





US-Policy





Conlcusions (1) – Short Summary

- An advanced Lock-Keeper Strong Authentication Framework is proposed
- Several benefits on the combination of the Strong Authentication technology with Physical Separation technology are presented
  - all the authentication components, user profile, privacy and policy are protected well on GATE, which are impossible to be actively accessed from outside.
  - The whole authentication procedure is performed on GATE and impossibly to be affected, which demonstrates the idea of "**Offline Authentication**".
  - The *Credential VM* in the integrated IAM system can be easily and securely updated, which realizes the concept of "**Offline Maintaining**"
  - Both incoming request and outgoing response are required to be verified so that the **insider attacks** can be prevented.
- an enhanced Lock-Keeper Web Service Module is implemented based on the proposed framework.
  - significantly improve the usability of Lock-Keeper
  - Practically demonstrate the applicability of our proposed authentication approach

Conlcusions (2) – Future Work

- The Lock-Keeper can be used as a suitable host for the **federated authentication** proxy to exchange and translate the different authentication information required by different organizations.
- Other special authentication and access control schemes can also be integrated in Lock-Keeper to enhance security of existing applications.
- Development of a unified authentication client, e.g. a plug-in or extension for normal web browsers, also makes great senses to popularize this idea.

Thanks for your attention!

For more information:

Chair of Internet Technologies and Systems
Hasso Plattner Institute at University of Potsdam
P.O.Box 900460, D-14440, Potsdam, Germany

http://www.hpi.uni-potsdam.de