Information Security of Patient-Centred Services Utilising the German Nationwide Health Information Technology Infrastructure

Ali Sunyaev

HealthSec '12
3rd USENIX Workshop on Health Security and Privacy
Bellevue, WA
August 7th, 2012

Assistant Professor Dr. Ali Sunyaev
Information Systems and Information Systems Quality
University of Cologne

Agenda

- Patient-Centred Services
- German Health Information Technology Infrastructure (HTI)
  - Overview of Smart Cards
  - HTI Timeline
  - HTI Introduction Phases
  - HTI Components
  - High-Level HTI Architecture
- Utilisation of HTI Security Features for Provision of Patient-Centred Services
- Conclusion

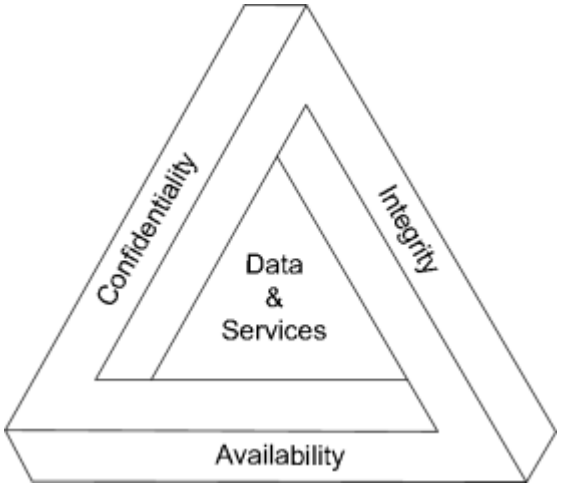


Patient-Centred Services

- Fulfill needs of patients
- Not bound to requirements of care providers
- Personalisation through access to patients' information
- Patient empowerment
- Can be provided by anyone, who can finance the required resources
- Can provide any functionality patients deem useful

- **Handling of sensitive medical information!**

Patient-Centred Services



⇒ **Need to Ensure Information Security:**
- Confidentiality
- Integrity
- Availability

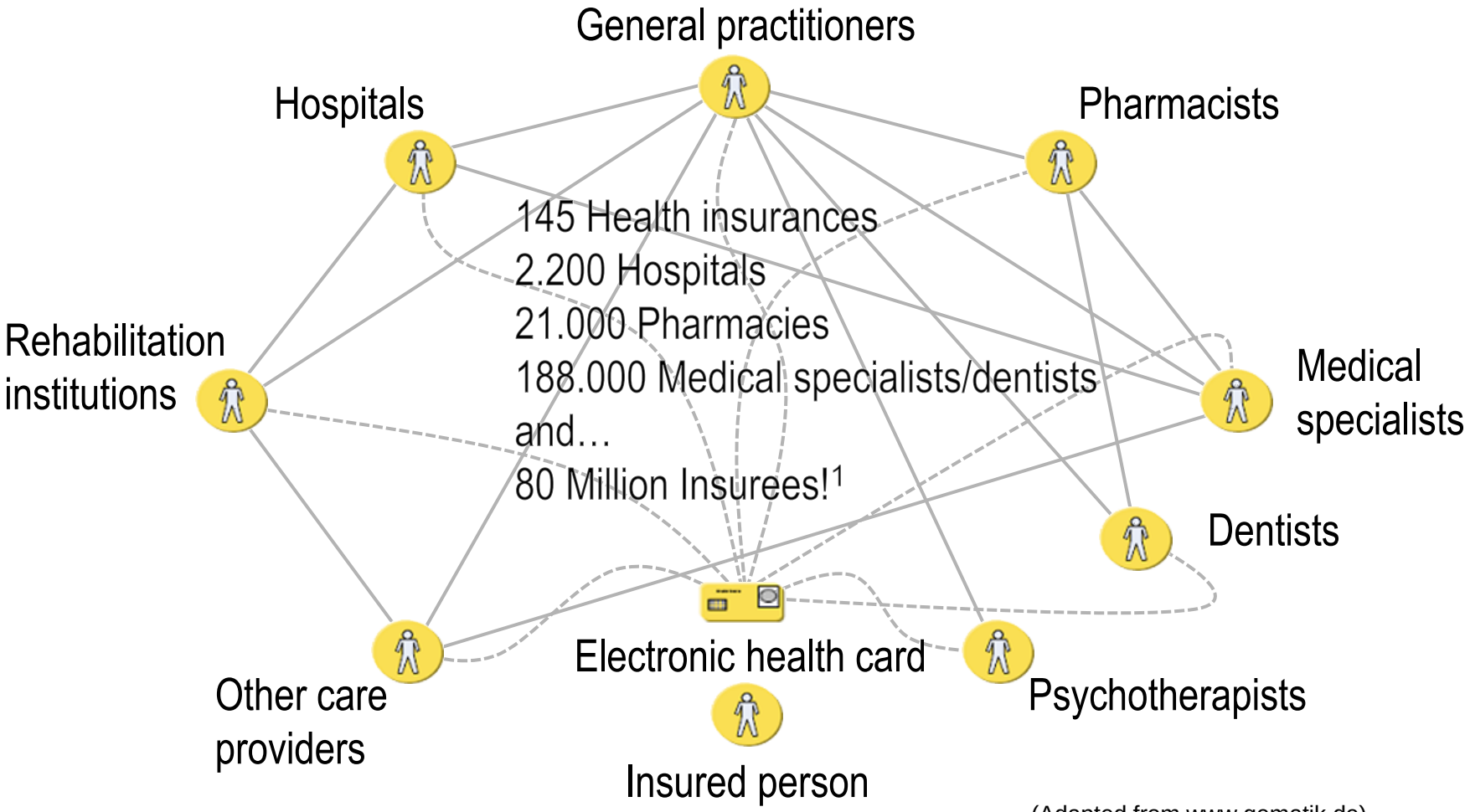
- **Challenges of Ensuring Information Security**
  - Large spectrum of possible points of attack
  - Requires specialised, up-to-date knowledge
  - Users need to deal with/trust in diverse approaches
  - Neglect of security issues until something goes wrong might be appealing

⇒ **Can common, certified, and widely-used security functionality serve as foundation for secure provision of patient-centered services?**

Background

- Germany is building a **nationwide telemedicine infrastructure** to centralize the storage of health data and harmonize interactions of all actors in the public health system.
- Misuse should be avoided by **mandatory encryption** of health data and **role based access** rules provided by SmartCard technology.
- Enforcement of **extended patient rights** through strong involvement in many medical processes.

German Health Information Technology Infrastructure



(Adapted from www.gematik.de)

1: Tuffs (2010)

German Health Information Technology Infrastructure



Extensive Security Measures

- Certified components
- Patients and medical professionals are equipped with smart cards providing security functionality
- Public key infrastructures enable use of encryption and signatures
- …

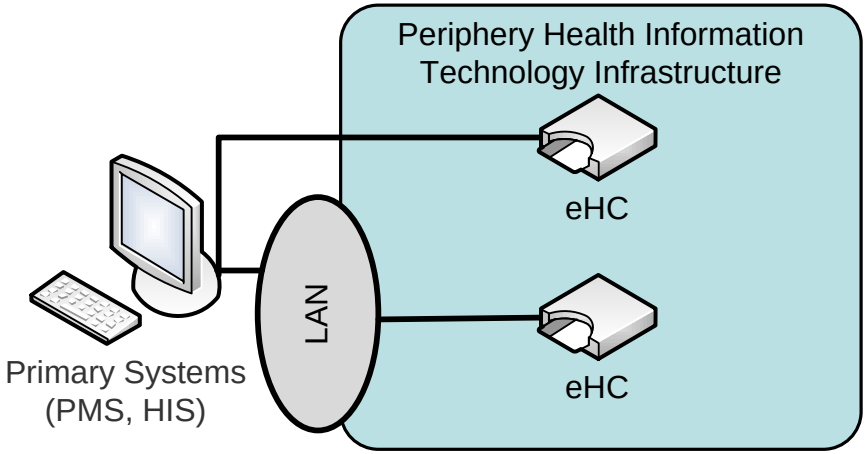
⇒Foundation for provision of patient services?

Overview of Smart Cards

Name	Deployment	Purpose
eHC	Issued to insurees	• Identify insuree (name, picture, insurance number, …) • Entitlement to retrieve care • Retrieve care in the EU (European Health Insurance Card) • Access security functionality (encryption, signatures, …) • Give consent for HTI services
HPC	Issued to medical professionals	• Identify medical professional • Access HTI services • Access security functionality (encryption, signatures, …)
SMC-B	Integrated into hardware	• Identify medical institution • Access HTI services
SMC-A	Issued to employees	• Access functionality delegated from a HPC or SMC-B • Relieve central authorities of card management for large institutions
SMC-K	Integrated into connectors	• Identify connector • Access security functionality (encryption, signatures, …)
SMC-KT	Integrated into card readers	• Identify card terminal • Access security functionality (card validation, encryption, …)

Base Rollout

- eHC distribution to insurees
- Equipment of medical professionals with eHC readers



Offline Management of Insuree Information

- Read information on eHCs
- Verfication of information stored on eHCs
- Update of information on eHCs

Online Rollout – Phase I

Establishment of Preliminary HTI:

- Design, specification, and establishment of necessary infrastructure to facilitate …
  - online verification of insuree information
  - utilsation of qualified electronic signatures

Online Management of Insuree Information:

- Connection of HTI periphery to central HTI services
- Online access, verification, and update of insuree information

Online Rollout – Phase 2 (I)

Secure Communication between Care Providers

- Encrypted, digital, and direct communication between care providers
- Avoidance of changes in media and secure exchange of sensitive medical information

Electronic Case Record:

- Cross-institutional documentation of a specific case

Patient Emergency Information:

- Storage of information that is relevant in case of an emergency on eHC
- Chronic diseases, allergies, et cetera

Online Rollout – Phase 2 (II)

Safety of Pharmacotherapy

- Document medication a patient is taking
- Track prescriptions
- List treatment options and undergone treatments

ABDA
Bundesvereinigung
Deutscher
Apothekerverbände

Establishment of Target HTI:

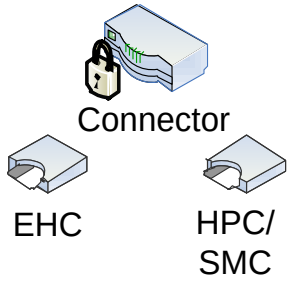
- Adaption and further development of the preliminary HTI
- Facilitate provision of functionality developed in the projects of second phase of the Online Rollout
- Provision of basic services that can be used by all other services

GKV Spitzenverband
KBV

HTI Components

Connectors

- Establish network connections (virtual private network connections)
- Security functionality (encrypted and signed communication)
- Authentication functionality
  - Hooked up to card readers for eHC and HPC/SMC
  - Verify access rights of medical professionals and patients
  - Enable patients to give consent
- Service application logic module
  - Provides interface to access HTI services for primary systems and card readers
  - Additional application logic can be loaded if necessary



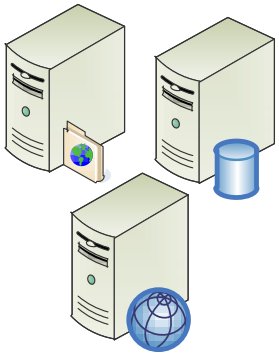
HTI Components

Security Gateways

- Link trusted networks
- Block not whitelisted traffic
- Employment of packet filters and application level gateways
- Further components can be added (e.g. malware or virus detection)



Security Gateway



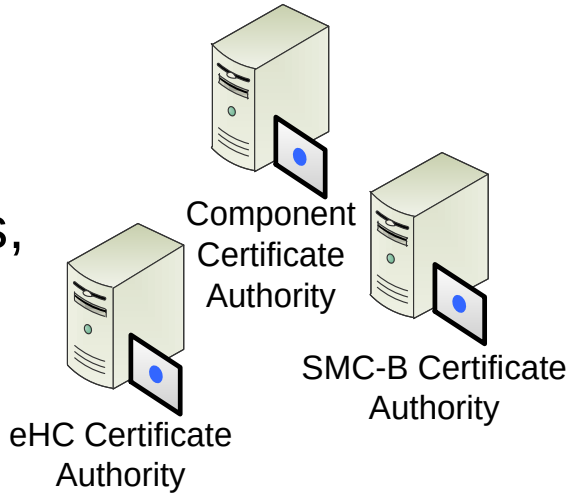
Professional Services

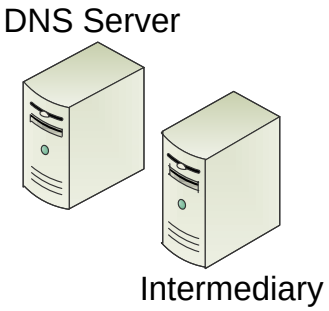
- Services provided by stakeholder organizations
  - Verification of insuree information
  - Management of medical documentation
  - Access to medical knowledge
  - …

HTI Components

Certificate Authorities

- Issue certificates for smart cards, components, and services
- Authenticate signatures

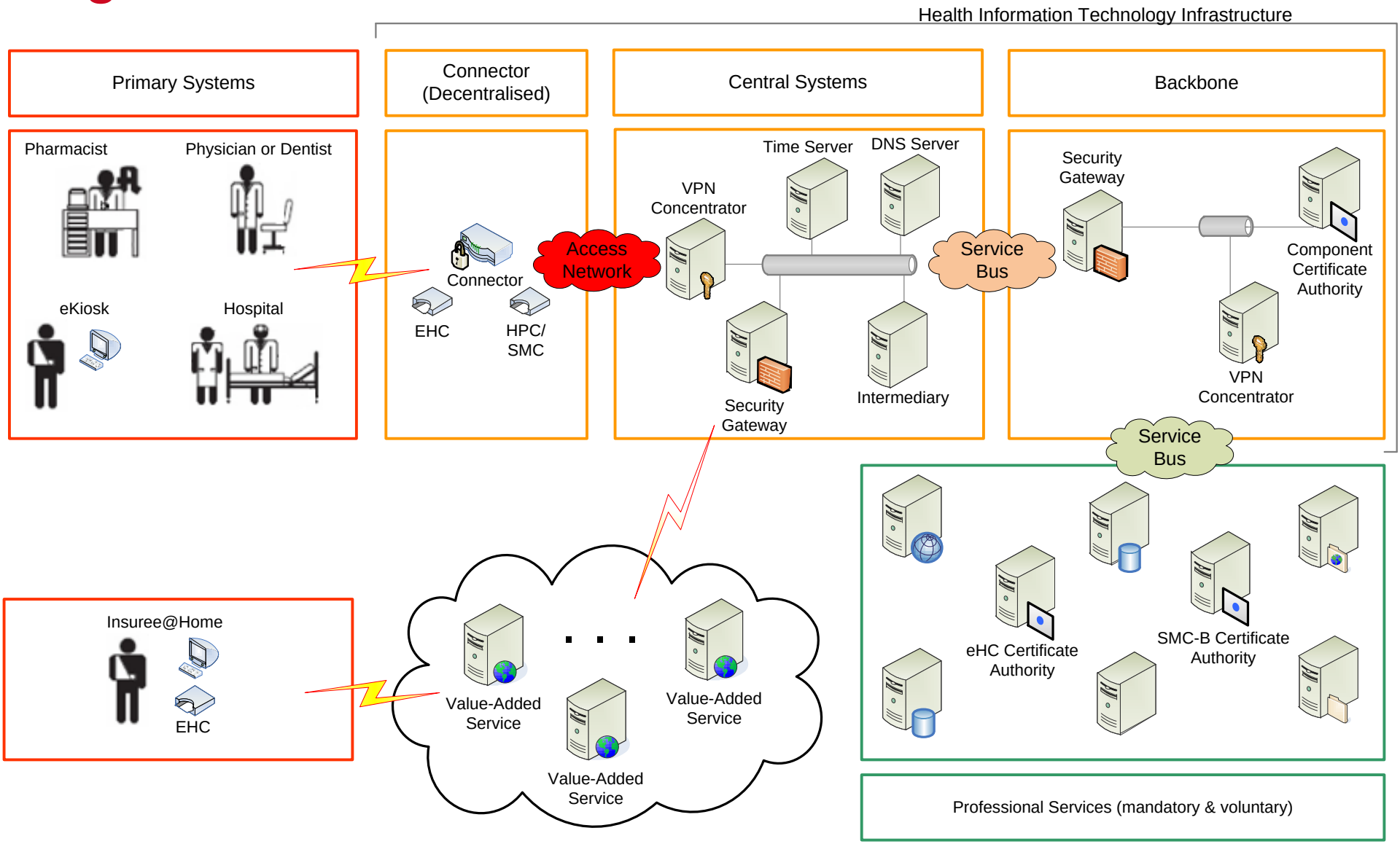




Intermediaries

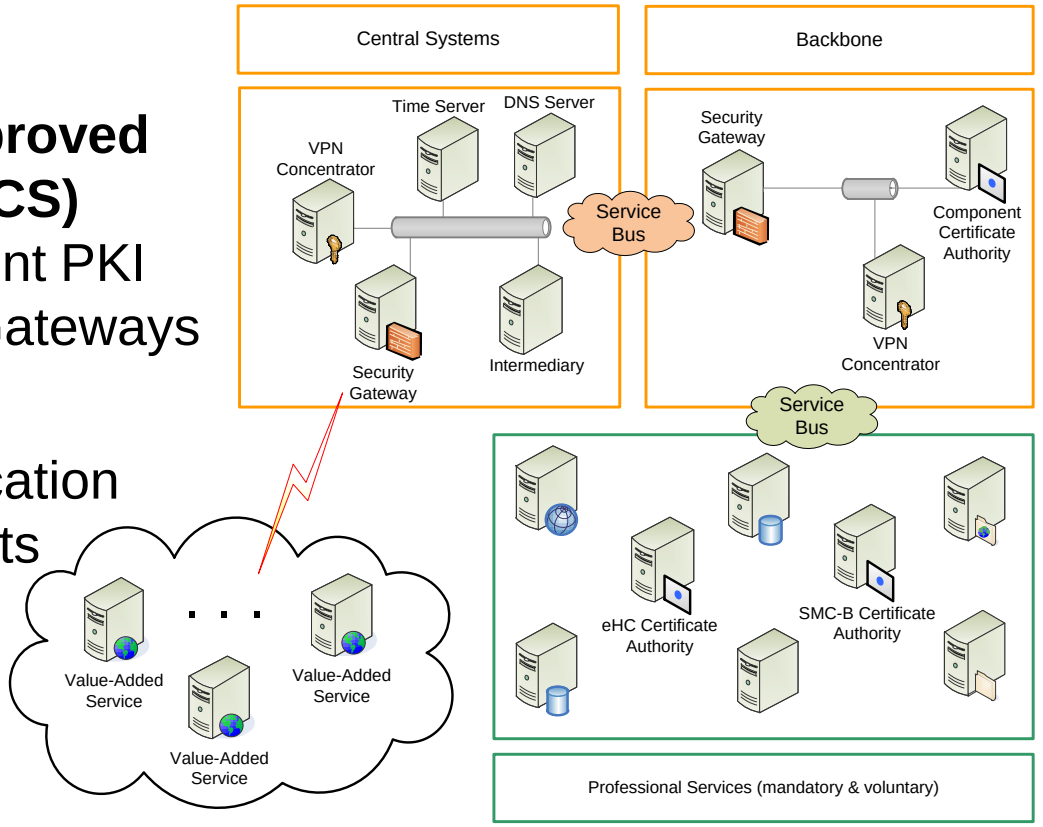
- Handle communication between connectors and professional services
- Locate services via DNS and pass packets without modification to professional services
- Concentrate many point-to-point connections in services buses to relieve other central components and professional services

High-Level HTI Architecture



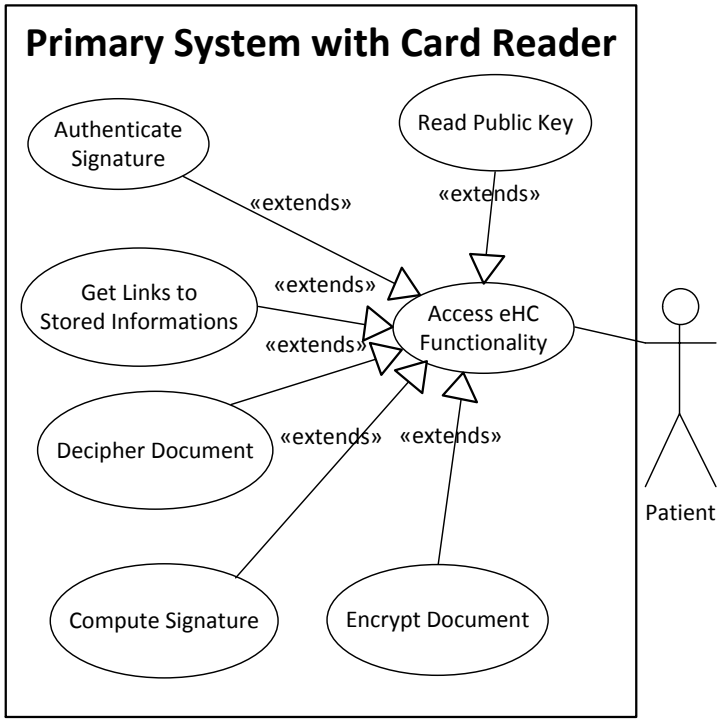
Access to HTI Security Features

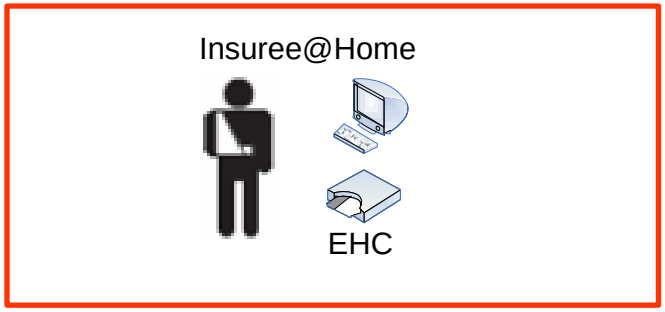
- **Approval**:
  - Demonstration that implementation corresponds to specification
  - Employment of sufficient measures to ensure information security
  - No endangerment of HTI services
- **HTI components can load configurations for newly approved patient-centered services (PCS)**
  ⇒Register PCS with component PKI
  ⇒Authorise PCS in Security Gateways
- **Accessible functionality:**
  - Creation of secure communication channels with HTI components
  - Authentication of signatures, signing/encryption of documents



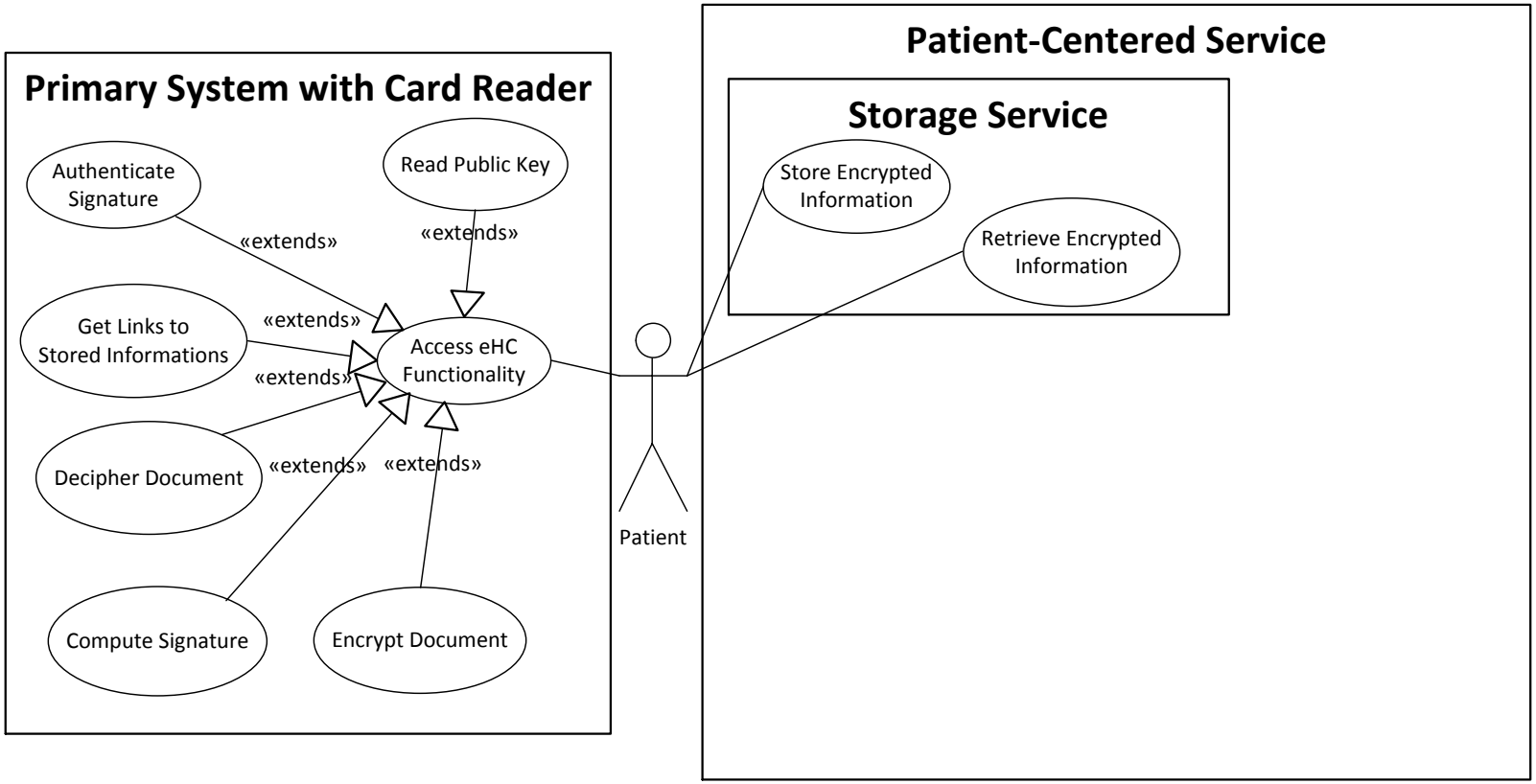
Access to eHC Functionality



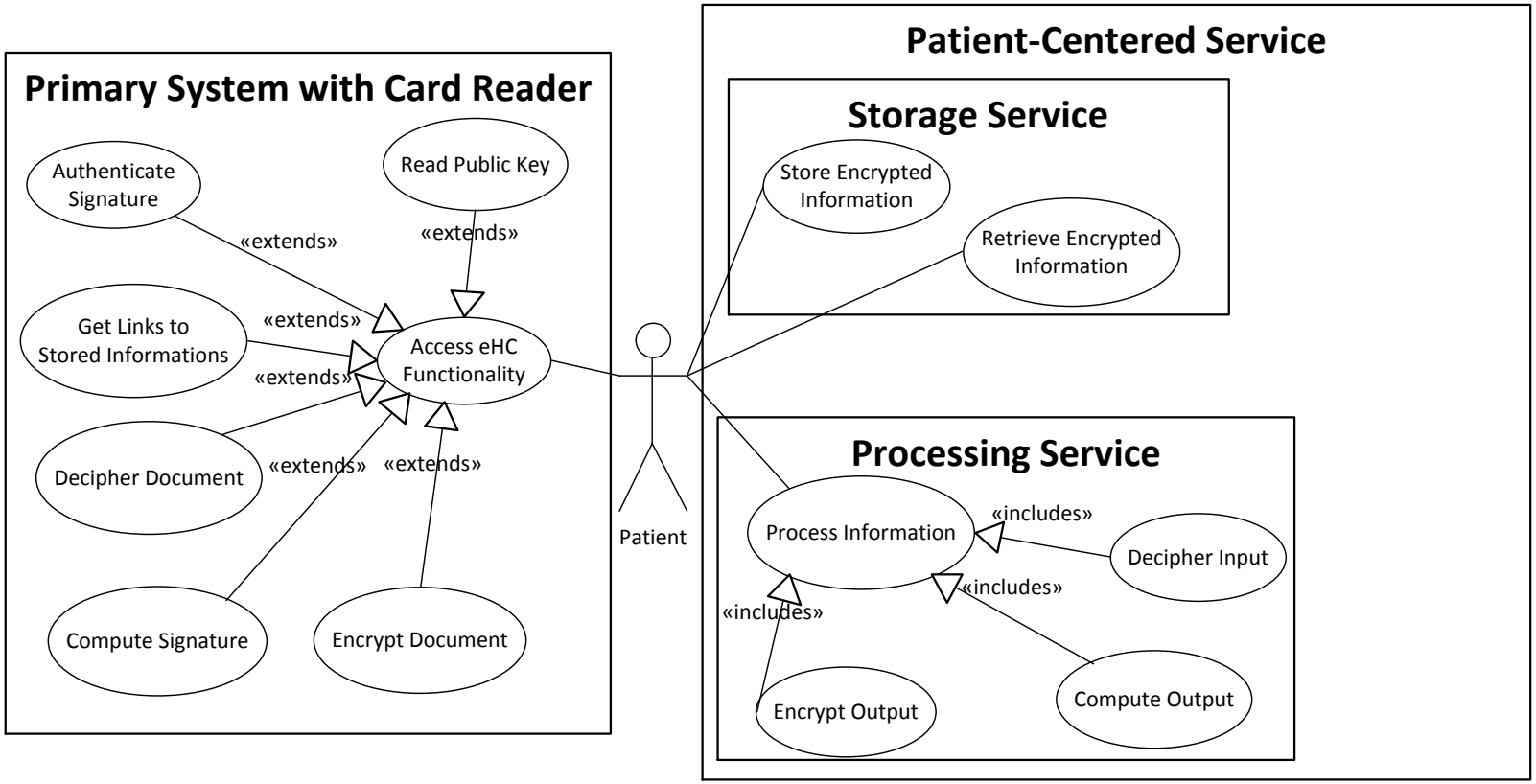




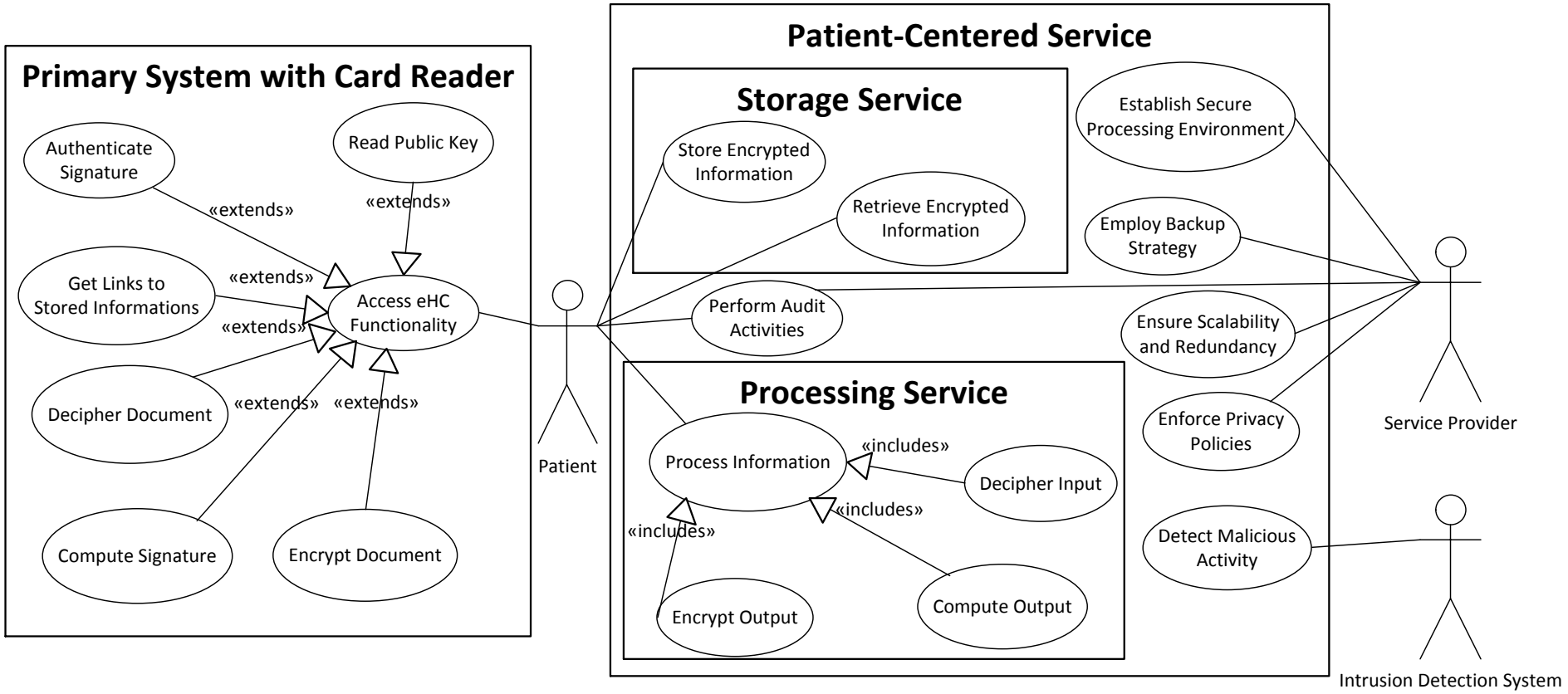
Storage Service



Processing Service



Responsibilities of PCS Provider



Conclusion

- HTI can serve as suitable foundation for secure provision of patient-centred services
- Providers of patient-centred services need to supplement the HTI security features with additional security measures
- Patient-centred services should either store or process information
- Security measures should be supplemented with functionality ensuring anonymous access to patient-centered services

Assistant Professor Dr. Ali Sunyaev
Information Systems and Information Systems Quality
University of Cologne

Information Security of Patient-Centred Services Utilising the German Nationwide Health Information Technology Infrastructure

Ali Sunyaev

HealthSec '12
3rd USENIX Workshop on Health Security and Privacy
Bellevue, WA
August 7th, 2012

Assistant Professor Dr. Ali Sunyaev
Information Systems and Information Systems Quality
University of Cologne

References

European Commission (2004) “e-Health: Making Healthcare Better for European Citizens: An Action Plan for a European e-Health Area,” COM (2004) 356 final.

Tuffs, A. (2010). Germany puts universal health e-card on hold. British Medical Journal, 340.

Waegemann C.P. 1999. "Current status of EPR developments in the US," Toward an Electronic Health Record '99, Medical Records Institute, pp. 116-118.