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
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

- General practitioners
- Hospitals
- Pharmacists
- Rehabilitation institutions
- Other care providers
- Electronic health card
- Insured person
- Medical specialists
- Dentists
- Psychotherapists

145 Health insurances
2,200 Hospitals
21,000 Pharmacies
188,000 Medical specialists/dentists
and...
80 Million Insurees!1

1: Tuffs (2010)

(Adapted from www.gematik.de)
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

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

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

Offline Management of Insuree Information
- Read information on eHCs
- Verification 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
  • utilisation 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

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
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)

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

Health Information Technology Infrastructure

Primary Systems

- Pharmacist
- Physician or Dentist
- eKiosk
- Hospital

Connector (Decentralised)

- Access Network
- EHC
- HPC/SMC

Central Systems

- Time Server
- DNS Server
- Intermediary
- Security Gateway

Backbone

- Security Gateway
- Component Certificate Authority
- VPN Concentrator

Service Bus

- Value-Added Service
- Professional Services (mandatory & voluntary)

Professional Services

- eHC Certificate Authority
- SMC-B Certificate Authority

Insuree@Home

- EHC
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

**Primary System with Card Reader**

- **Authenticate Signature**
- **Read Public Key**
- **Get Links to Stored Informations**
- **Decipher Document**
- **Compute Signature**
- **Encrypt Document**

**Patient**

**Insuree@Home**

**EHC**

Storage Service

Primary System with Card Reader

- Authenticate Signature
- Get Links to Stored Informations
- Decipher Document
- Compute Signature
- encrypt Document
- Access eHC Functionality

Patient-Centered Service

- Store Encrypted Information
- Retrieve Encrypted Information

Patient

«extends»

Storage Service

«extends»

«extends»

«extends»

«extends»

«extends»

«extends»
Processing Service

Primary System with Card Reader

- Authenticate Signature
- Get Links to Stored Informations
- Decipher Document
- Compute Signature
- Read Public Key
- Access eHC Functionality
- Encrypt Document

«extends»

Patient-Centered Service

Storage Service

- Store Encrypted Information
- Retrieve Encrypted Information

«extends»

Processing Service

- Process Information
- Decipher Input
- Encrypt Output
- Compute Output
- Retrieve Encrypted Information

«includes»

Patient

Access eHC Functionality

«extends»
Responsibilities of PCS Provider

Primary System with Card Reader

- Authenticate Signature
- Get Links to Stored Informations
- Decipher Document
- Compute Signature
- Encrypt Document
- Read Public Key

Processing Service

- Process Information
  - «includes» Decipher Input
  - «includes» Encrypt Output
  - «includes» Compute Output
- «includes» Encrypt Output

Storage Service

- Store Encrypted Information
- Retrieve Encrypted Information
- Perform Audit Activities
- «includes» Detect Malicious Activity
- «includes» Ensure Scalability and Redundancy
- «includes» Enforce Privacy Policies
- «includes» Employ Backup Strategy
- «includes» Establish Secure Processing Environment

Patient-Centered Service

- Patient
- «extends» Service Provider
- «extends» Intrusion Detection System

Access eHC Functionality

- «extends» Patient
- «extends» Get Links to Stored Informations
- «extends» Decipher Document
- «extends» Compute Signature
- «extends» Encrypt Document
- «extends» Read Public Key
**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
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