A CONCEPT TO PRESERVE DATA PRIVACY IN INTEGRATED NATIONAL HEALTH CARE INFORMATION SYSTEMS AND INFRASTRUCTURES

Thomas Grechenig, Philipp Tomsich, Anna Wujciow, Barbara Tappeiner

Vienna University of Technology, Institute of Automation
Research Group for Industrial Software (INSO), {firstname.lastname}@inso.tuwien.ac.at

Abstract: Establishing a nationwide electronic health care infrastructure promises an increase in transparency, efficiency and patient care. The transformation of health records into a modern form of processing must be suitable for storage and analysis, online queries of the patient's health insurance status and integration of hitherto distributed health records into national health care information systems. Since the processed data is highly sensitive, the protection of data privacy plays a crucial role: technical and architectural measures need to comply with, and moreover, excel the procedural safeguards already in place. The challenge (secure yet transparent) is further increased by the difficulties directly resulting from the *scattered nature* of any appropriate system. In contrast, for a traditional *distributed system,* access to health-related data origins from diverse locations belonging to different organisational hierarchies.

The major data privacy measures of national health care information systems fall into three categories:

- **Medical data** encompassing diagnoses, prescriptions, medical records and emergency data. Access may be provided only with the patient's consent to authorised health care professionals, except for life-threatening medical emergencies when the necessity to access the data can override the patient's right to data privacy.
- **Administrative data** characterising information such as roles, access permissions, identities or audit trails. This class of information may be revealed on a need-to-know basis only, e.g. a requester may need to reveal his identity to a central application to establish access permissions.
- **Other personal data** and highly sensitive information also needs to be processed in the context of health care, e.g. the inference of the social situation of an individual can be derived from his insurance history and current insurance coverage. Access to this class of information generally requires the consent of the patient, but may occur in a time-deferred manner.

Furthermore, a large amount of sensitive, mainly medical, data is stored in de-central systems, such as at health care facilities. These *primary systems* now contribute data – such as prescriptions or diagnoses – into an integrated national health care information system, but also act as consumers to said data. It may be assumed, that these *primary systems* are a secure sink for information and that existing mechanisms sufficiently safeguard the privacy of data entering those systems. Yet the implementation of an integrated national health care information infrastructure may not compromise the safety of the existing *primary systems*, raising specific demands on the networking infrastructure connecting individual health care providers. In contrast, central infrastructure components and services need to be protected from malicious or erroneous (flawed!) queries from *primary systems*.

A flexible and security-centred architecture needs to be chosen to satisfy these multifaceted requirements:

- A mobile, tamper-proof key and data-store is provided to all participants in the system, including patients and health care professionals for unambiguous identification.
- A "connector" – i.e., a specific kind of security-certified consumer premises equipment providing limited application logic – completely uncouples the *primary systems* from the infrastructure. Under no circumstances a primary system will communicate directly with a central service or vice versa.
- Authentication, authorisation and information flow-control occur at multiple layers and both centrally and de-centrally.

In greater detail, seven layers of security are provided that complement each other to guarantee data privacy and minimise the potential for abuse:

1. A **smart card** acts as a mobile, tamper-proof key- and data-store both for patients and for health care professionals.
2. Customer premises equipment consists of a **"connector" and smart card-terminals**, providing a trusted computing platform. The "connector" is a security-certified trusted system that defines the outer edge of the health care infrastructure.
3. Each connector contains a **cryptographic identity** and requires a pluggable security access module.
4. Access is limited at the network level to a **closed user group**. Authentication, access for individual security access modules can be revoked at any time.
5. System participants may not communicate freely among each other. Predefined **rules are enforced at each coupling** of two autonomous systems.
6. **Central applications are certified** for operation within the infrastructure; only after passing compliance tests, a certificate is issued for each such accredited application.
7. **Application-level authentication, authorisation and encryption** can be added where permitted.

ISSN: 1727-1983 © 2005 IFMBE