

The Challenge of Secure e-health

Developing innovative solutions in emerging e-health markets requires strong efforts which may be justified only in presence of particularly suitable boundary conditions. Among factors retained of primary importance for the development of secure and trustworthy e-health, a correct approach to a reliable identity management is unanimously considered fundamental. Four keywords in the management of identities appear particularly important: standardization, security, safety, and privacy. Standardization may contribute to increase the size and duration of the e-health market, while security, safety, and privacy encourage stakeholders to trust in a appropriate and safe management of all very sensitive personal data involved in e-health applications. The aim of research is analyzing security and safety issues in e-health from the particular prospective of the identity management and standardization highlighting, among others, the approach of the EU-funded "Bio-Health" project whose mission is an increased stakeholders' knowledge about existing and emerging standards in eHealth particularly for identity management.

The Conceptual Approach

Advanced concepts of e-health place citizens in the focus of a net-centric architecture in which the peripheral is represented by devices that bear medical data, improve accessibility to information on services and data, or serve for authentication. Since they enable high-level healthcare data and services access and provision, aspects like security, safety, privacy, ethics as well as underlying supporting technologies need to be addressed before establishing a technical solution.

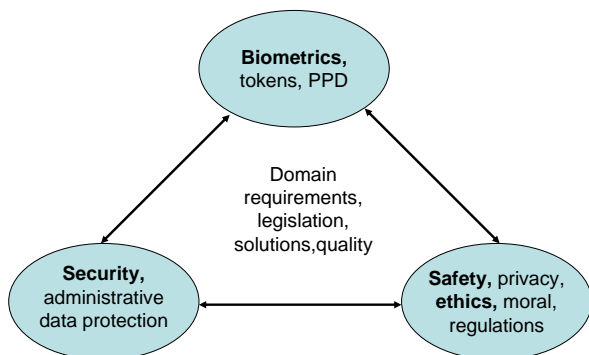
The preferred way to deal with future challenges of modern healthcare requirements shall be a well-balanced combination of mobile personalized security devices and advanced health networks for both information and services provision. Identity management for all principals (persons, systems, applications, devices, components, etc.) in this respect is the key for the provision of all security and safety services.

Thus, concepts of security, safety, privacy, quality, and ethics play an important role in the framework of advanced e-health services. The addressed technologies like biometrics, RFID and NFC are able to technically support the derived legal, political, and social requirements for such advanced and secure person-related healthcare and welfare service provision.

The Technical Approach

Realizing the importance of security, safety, and privacy aspects in modern e-health solutions, several specific R&D areas need to be addressed including:

- Basic security aspects;
- Information security aspects;
- Digital identity and authentication;
- Identity management;
- Data protection and privacy;
- Biometrics, and
- Applied bridging technologies (RFID, NFC, etc.).



As all of them depend on each other, the whole problem could be considered being the triangle of secure e-health service provision linking the various areas to each other mainly by means of applied technology.

Conclusions and Strategies

A reliable, secure, and trustworthy identification is the basis for all advanced security and safety concepts and services (authentication, authorization, integrity, confidentiality, etc.). This is particularly true for e-health information systems and respective applications requiring an empowerment of all parties (principals) involved. As all these parties rely on a secure and trustworthy way of communication and collaboration, they strongly depend on common acceptance which, in its turn, is strictly correlated to privacy and ethical issues.

Different technologies including biometrics, RFID, and NFC but also portable devices, sensors, actuators, and networks allow for guaranteeing standard-based high-level security, safety, and privacy services addressing proper identification of both human beings, services, components, and goods.

As the diffusion of standards in these fields is still away from a satisfactory level, various standardization initiatives, organizations, and projects such as BioHealth promote knowledge and dissemination of standards which will be extremely useful in supporting secure and trustworthy eHealth applications. Applied standardization and promotion of such standards allow developing innovative products for the future global markets of secure e-health solutions worldwide.

For further information please contact:

Asbjorn HOVSTO, *Portahead, Gjøvik, Norway*
Peter PHAROW, *eHealth Competence Center, Regensburg University Hospital, Regensburg, Germany*