

E-health Use Case

1. Background

E-health is defined as a complete ICT-based eco-system involving the patients and all the stakeholders, delivering health services. E-health is a patient-centric environment, whereby ICT will support the implementation of policies for a better management of identities, health records and secure transactions inside a trusted group of actors.

The approach taken in this use case document is to start from a real e-health initiative (in Slovenia) and expand it with a vision of the next steps of foreseeable deployments; looking at the 2010-2015 horizon, through the eyes of a real citizen going through such visionary e-health services. A use case scenario is an efficient way to visualize such a technology roadmap. It is also a good way to establish if the vision meets the needs and expectations of real people along the way.

By observing the lessons learnt from current deployments of ICT-based e-health solutions, this document describes the two key aspects of such solutions and anticipates which technologies and policies will be needed to further implement them. Those two areas are:

- The e-health document itself: This is typically a microprocessor card, aiming at fraud reduction; simpler issuing mechanisms; and, more convenience and ease of use for all the stakeholders in the value chain, from the e-health Service Provider (ESP) to the Patient. This document will play three key roles: Managing identities; securing access to systems; and, (potentially) hosting some critical data of the public health record (PHR).
- The protection and management of the Patient's digital assets or PHR: Who has access to what data and when? What policies need to be in place to protect the Patients while still insuring the efficiency of the healthcare services? What new technologies are needed to implement such policies? Where is the data stored and what are the guarantees of protection?

PHR policies are the core definition of e-health programs. Technologies will support the implementation of management procedures for identities, assets and transactions, but it is actually the policies that will ensure Security, Privacy and Trust in the eco-system.

1- Defining the new perimeter, including all the e-health stakeholders

The e-health eco-system involves multiple stakeholders, from the ESP, the physicians, the hospitals and various care providers, the medical drugs industry and distributors and last but not least the Patients and the Governmental entity supervising the Healthcare network. In the past, the perceived level of Privacy and Trust was totally based on paper transactions and on the best known practices on how such documents should be handled. Moving forward, any ICT-based system will have to fully take into account the roles and liabilities of each of these

stakeholders. The Chain of Trust requires solutions in four areas (with the support of Policies to define the appropriate procedures):

- 1- Identities Management
- 2- Assets management (PHR access right and edits right)
- 3- Data Storage and Revisions Management
- 4- Secure Transactions over the Network

2- E-health Document issued to the Patient

In many aspects, the e-health card is very similar to e-ID documents. Key technologies and policies involve issuing mechanisms, service provisioning mechanisms, terminals and data encryption. Patients are familiar with the ease of use and convenience of smart cards in various domains such as payment, mass transit or mobile telephony. The practical use case in Slovenia will describe how, from the Patient's perspective, all of his/her needs – from registration to usage of services – are well met and optimized, compared to previous ESP systems.

3- Chain of Trust to manage the PHR

Going much further than just how the services are delivered, the strategy and policies dealing with data management are critical when implementing tangible trust and privacy. It involves both the card issued and the back-office systems and their processes. It has to be driven by clear policies defining all aspects of the PHR life cycle and especially its access rights.

The challenge remains to define sufficient levels of privacy and trust to address the concerns of Citizens. The previous reference for this matter was the paper-based transactions e-health eco-system. That baseline is a good start but is not enough to build a fair comparison since an ICT-based e-health deployment introduces far more functionalities (and therefore further issues to be addressed) than any other e-health strategy based on paper-trails.

In order to design a proper Chain of Trust, we should keep in mind some fundamental rules to be respected at all times: [1] The Patient owns his/her PHR. [2] His access rights may exclude editing rights but he owns the PHR. [3] Any query or transfer of all or part of his PHR should be done with the consent and awareness of the Patient. [4] Any exception to such fundamental rules should be thoroughly defined by related policies.

In addition to the Patient rights and duties, the Chain of Trust must also include a charter for each stakeholder in the e-health eco-system. That charter (implemented by technology) should cover in detail access rights, where the data is fetched from, where the data will be stored after consulting/editing, how long can the data be kept, who gets informed about the fact the data was accessed, etc.

The Chain of Trust needs also to be designed with heuristics to solve complex issues such as conflicting diagnostics, competition between ESPs, legal implications of health diagnostics, data disaster recovery techniques, etc.

Last but not least, the Chain of Trust needs to define its control authority, as well as the Controller of the controllers. Beyond policies, it involves several critical technology hinges such as, for example, the choice of a trusted entity for certificates management for PKI.

To conclude this introduction, it is fair to say that a successful Chain of Trust for an ICT-based system will be the combination of detailed policies (a truth table to handle every possible scenario) and four technology pillars: [1] Identity management; [2] Assets management; [3] Data storage; and. [4] Secure transactions over networks.

2. Vision

Practical example to document the case

This use case will be developed using the example of the Slovenia deployment of the first European Java Card solution with a PKI infrastructure to secure a full Web Services Health system, with digital signature for health professionals.

This deployment is state-of-the-art for both the Card and the back-office. It is a good example of an ICT-based solution with the benefits of PKI. At this point in time, it does not expand into additional layers of Privacy and Trust such as minimal disclosure of credentials technologies. This document will attempt to position such possible enhancements to the PHR life cycle management as a logical next step to what is already deployed in the field

Abstract / Intro

Of all the Smart Cards solutions deployed today in the digital world, e-health cards and secure online health services are the most self-explanatory to citizens about the advantages, in terms of security, privacy, speed and ease of use, that those technologies can bring. PHR is one of the most intimate types of information for each of us. Going paperless is the first tangible benefit in such programs for citizens, because it simplifies procedures for the Patient. In some countries like France where e-health cards are deployed, it also removes the constraints of advance payments from the Patient to the Physicians, which is a major help for Patients with limited sources of income. In addition to the cost and time savings, and fraud reduction for Patients, there are additional major gains for the Authorities who manage such programs.

Slovenia is at the leading edge in terms of technology among all the e-health programs under deployment in the world (about 25 as of today). Slovenia was an early adopter of Microprocessor Cards solutions for Healthcare; as early as 2000 for its two millions citizens. The second phase under deployment since 2008 involves state-of-the-art technologies from card issuance all the way to on-line services for citizens and health professionals.

Moving forward, Slovenia plans to merge its *Identity Card* and its *Health Insurance Card* (HIC) into one single card. Such a card will enable the cardholder to install his own Digital Certificates to use the card for other online services beyond e-health (for example: e-mail, secure login or secure on-line storage access). Slovenia also plans to leave the choice to its citizens between three different options of e-ID and e-health credentials configurations. Security, Privacy and respect of the citizen choice to combine his e-ID with his HIC card: That is why we believe Slovenia is an excellent use case to study: it is currently (2009) the most advanced known implementation. Moreover, the intended expansion indicated by the e-health authority in Slovenia validates many of the hypotheses taken when defining the elements of the Chain of Trust at the Horizon 2015 when expanding the ICT-based system.

Today, deploying a PKI is, by itself, a very strong achievement given the diversity of platforms and devices used by physicians and ESP. Slovenia is both strong in the execution of its e-health plan today and visionary about the next steps to be deployed.

Horizon 2015 scenario

E-health + E-ID Combo Card

Jorge is a young student in Ljubljana and is very committed to a clean planet; “going paperless” whenever possible is an attractive proposition to him. He also likes the simplicity of on-line services and is inclined to forget to organize bill payments or properly manage his schedule, especially when it comes to health check-ups. When the time comes to renew his ID card, he decides to select **Option Four** (an e-ID card with his HIC profile on it, as well as the Digital Certificate). **Option One** was simply an ID card without a chip on it. Jorge likes the fact he had a choice and finally he goes for the big one because, after all, we are in the 21st century!

From home, Jorge makes his appointment on-line and later goes to the nearest National Health Care Administration office. In a matter of minutes, by providing his old ID card and the reference number of his on-line reservation, he gets his brand new Smart Card e-ID issued. No weeks and weeks of waiting time to get a new ID card; no long queues; and, no paperwork to fill out. Jorge thinks that since he has his new card, it may be time to visit the dentist - a task he has avoided for the last two years. Thanks to the portfolio of Java Applets loaded in the microprocessor of the card, Jorge simply inserts his card in the built-in card reader on his Personal Computer and, via the web browser, selects a nearby Dentist and books the appointment on-line. In addition to booking the appointment, all his dental records are securely uploaded from the flash memory which is resident on his e-health card to the dentist's computer. This will save the dentist the cost of redoing a complete set of X-Ray; as dentists used to do for all new patients, before the on-line services used to be available.

In the above situation the Chain of Trust validated that the Dentist had credentials to access the Patient dental records, that his intervention was not conflicting with previous care processes rendered to that Patient and that the Patient authorized a new transaction on his PHR. It also performed the pre-authorization for such care from the insurance point of view. In such a case, it is envisaged that all or part of the PHR would be securely stored on the card itself. Some e-health systems will use the Card for secure PHR storage with off-line access;

other solutions may involve a central database managed by the ESP with secure on-line access. One of the drivers of choice for smartcard-based solutions is to optimize the use of locally/securely stored data to benefit from a two-factor authentication mechanism when accessing the data “off-line” (i.e. locally) between the card and a terminal. This also empowers the Patient to have full control and ownership of his PHR on the central database at the ESP, because the data is only accessed via his card.

When Jorge goes to the dentist and gets his bad tooth fixed, the dentist inserts Jorge’s card in his card reader on his computer and at no stage is a paper form required nor a cash, check or banking card payment. Operations such as ‘Track Records Updates’, ‘Prescriptions’ and ‘Next Appointment Setup’ are all managed on-line and will be available later to all the authorized stakeholders. Everything is secure, confidential to those who have the right credentials and signed digitally by the health professional. Jorge remains in full control of both his PHR and his relationship with the various stakeholders in the e-health eco-system. Jorge can still select new physicians, stop seeing physicians he did not like and prevent them from further accessing his PHR. Jorge can also decide to block access to some critical data such as his genetic code. Jorge is the leading entity of the Chain of Trust involving a PHR and any situation where this ownership would have to be overwritten will have to be clearly defined by Policies.

Jorge has nothing more to do besides going to pick-up the prescribed drugs at the drugstore where his card will be the only way to execute the transaction.

By 2015, the e-health network will be able to deliver a more Patient-centric set of services and flags: Issues like conflicting prescriptions or cross-diagnostics over several independent elements of the PHR will be computed in real time and made available to the Patient and to the Physicians, with the authorization of the Patient.

3. Roadmap

Visionary aspects – Three key challenges that need to be addressed

Both the citizens’ and the Administrations’ gains are very compelling and described in the scenario above: A paperless, simple, fast solution for citizens and a secure, fraud-free and costs-reducing solution for the Health Care Administration.

To fully unleash the promises of e-health solutions, three key issues need to be further addressed by both the technology providers and the policies makers:

1) Independent Trusted Entity

Because of the need for PKI and digital signatures to validate point-to-point transactions, digital certificates have to be issued and provisioned on the cards either at the initial issuance or later on during the card life cycle. Government authorities will rely on Trusted Providers to manage those certificates. More than just a technology challenge, there is also a process challenge to qualify who/where/for-what services, when selecting a Trusted Entity to create and deliver such certificates. As yet, Europe, (unlike the USA) does not have such an established and proven independent Trusted Entity.

2) PHR ownership

The Patient needs to remain at the centre of the system and own his/her PHR data. But unlike any ICT-based solutions, where a root or administration system owner not only has access to

but can also modify the data, the Patient ownership of the data needs to be limited to his/her ability to consult the data and know who accesses the data, but not to edit the data. Any access to his PHR should be done with the consent and awareness of the Patient. Beside a few exceptions that are related to the legal implications of health diagnostics for the Patients, his consent is mandatory for any action with his PHR. An e-health ICT-based system is unique, but there is no single point of “root admin”. This means policies need to be in place to resolve complex issues in the event, for example, of disaster recovery (who makes the decision about the right baseline of the data to be used after disaster recovery?). Policies will be needed to define PHR ownership and accountabilities. New technologies such as ‘Document Revisions Management’ will have to be implemented on all content inside a PHR database, allowing traceability to observe who contributed to any given record and when. In the event of a conflict between two parties about a given record, policies will have to define who can overwrite or modify such a record. Policies need to go beyond file access permissions and files revisions management. New concepts such as shared administration or “multiple electronic signatures required” will be needed.

3) PHR life cycle management and access rights

The Patient’s data are very sensitive and multiple stakeholders will have to access, consult or update such PHRs. It is fundamental to implement a technology of “minimal disclosure of credentials” to limit the level of access for the various actors in the Chain of Trust to what is strictly needed by them to accomplish their tasks. In that domain, the Patient remains the centre of the system and can control the setup of minimal disclosure heuristics. In some cases, like a Police investigation for example, involving a health diagnostic of a suspect, policies need to be clearly translated to define in which cases the Patient is not the owner of the minimal disclosure of credentials setup.

Privacy today is materialized in the world of paper transactions by the physical limitations of paper handling and paper viewing. We calibrate our standards of perception to concepts such as tangible assets, where the physical location of objects is a key contributor to the perceived level of Privacy. Even though many breaches of Privacy can occur in the world of paper transactions, we rely on best known practices based on the way we handle documents, edit their content and limit access to them. An ICT-based system would dematerialise content, so the concept of trustable partial access is far more complex. Technologies are now available to build “paper-like” perceived privacy, or even “far-superior-than-paper-like” privacy.

At this stage of the program, Slovenia is just a state-of-the-art PKI deployment, relying on a strict discipline with certificates issuance to offer the best possible security. The level of privacy and trust that can be achieved at that stage relies more on the concept of alarms and access tracking mechanisms.

PKI functionality, combined with logs and alarms whenever a transaction occurs, is already addressing a large part of this. The digital world being dematerialised, it is very disruptive for humans who only rely on their five senses and a brain to compute the information and make judgments calls on issues like privacy. We need to engineer new e-Senses to complement the ones we already have. We need to go beyond basic sensors and data computation like “I can see it and I can touch it therefore I trust it.”

Appendix A: Slovenia's Solution and its potential further evolutions

The deployment involves:

- Java Card 2.2.1
- GlobalPlatform 2.1.1
- PP SSCD & EAL4+ Certification
- Java Card applets are pre-loaded during the issuance process to deliver a portfolio of on-line services. That portfolio can continuously evolve by post-issuing new applets on cards already in the field
- Complete solution of instant issuance of the cards, including picture acquisitions and multiple security features for the card body

For use with the PKI infrastructure, the card includes two certificates from the Health Care Administration:

- One digital certificate to access the entry point with HPC (Health Providers Companies)
- One digital certificate to access the personal entry point
- RSA keys, SHA-1 & SHA-256 (API)
- 2048bits for non-qualified digital certificates

The card holder can add his own certificates and use the same card with the PKI infrastructure for secure authentication and secure transactions on additional services beyond the scope of e-health. The project also includes Terminals for self-services and the back-office for the hosting of online services

In the future and as a continuous evolution of the program (as seen in the scenario above), the Health Care Administration plans to:

- Allow the exchange of data sets for on-line authorization of expensive medical procedures (above a set limit, that requires an go/no-go decision)
- Enable access for physicians to analytical data (the dental track record of Jorge in the scenario above)
- Pilot a solution for e-prescriptions
- National vaccination records
- Tracking mechanism for appearance of contagious diseases
- Electronic archive management

Conclusion

Slovenia is a very good example of a successful e-health card deployment with a best-practise PKI deployment. In order to further improve the perception of privacy and trust for citizens, new policies will need to be in place to define PHR life cycle management and access rights. At this point in time, three technologies are expected as enablers for such policies: The first one is the ability to set up minimal disclosure of credentials, to enforce tangible privacy by

not giving access to all or part of the PHR to parties who do not absolutely need it. The second is the implementation of 'Document Revision Management' to implement some level of traceability of the data, especially from critical tasks such as IT system disaster recovery. The third one is the implementation of shared admin rights to co-own all or part of PHR with the authority to overwrite the data when needed.

The Slovenia use case is thus a very good example of a successful launch of an e-health plan. Its major benefits can be summarized by a check-list as followed:

- Benefits for Citizens: Yes: Speed, ease of use, less delays (cash) to use the HPC services
- Benefits for the Health Care Administration? Yes: Costs control, fraud reduction, time savings and multi application
- Security? Yes: State-of-the-art technology
- Privacy? Yes: Given today's knowledge of technologies to engineer privacy, but clearly there is room for improvement whenever additional technologies will emerge.