EUROSMART

The Voice of the Smart Security Industry

Position Paper

How to extend e-EHIC to others e-topics?

July 2012

Contributors:

Bruno Rouchouze
Didier Chaudun
Ingo Liersch
Detlef Houdeau

1. Purpose of the Position Paper

Digital identity became a reality with electronic passports based on the international ICAO standard, electronic health cards, electronic national ID cards, electronic driving licences, and e-Government services cards. Up until now government focus was nationally oriented but digital identification could also be used for European citizens' requirements everywhere in Europe.

Eurosmart distinguishes identity from identification. According to the Eurosmart glossary[1]:

Identity	• Information that is unique within a security domain and which is recognized as denoting a particular entity within that domain. • Representation uniquely identifying entities (e.g. a user, a process or a disk) within the context of the TOE. An example of such a representation is a string. For a human user, the representation can be the full or abbreviated name or a (still unique) pseudonym.[CC]
Identification	• The process, generally employing unique machine-readable names, that enables recognition of users or resources as identical to those previously described to the computer system • The assignment of a name by which an entity can be referenced. The entity may be high level (such as a user) or low level (such as a process or communication channel) • In a biometric system, a task where the system searches a database for a reference matching a submitted sample, and if found, returns a corresponding identity.

In the e-ID context, one is used for border controls and identity verification while the other one is more focused on digital requirements in the internet world. Identity programs are under Member States definition at the national level for national ID cards and international for e-Passport (ICAO, BIG), Resident Permit (E.C., Article 6) and e-EHIC (E.C., CA.SS.TM) Identity falls under Member States' responsibilities for all the above needs when identification responsibility is managed by the specific entity which managed the connected program asking for identification to access to e-services. In such cases, the identification process could be delivered by an independent identification management system such as those proposed by some Member States.

This Position Paper gives Eurosmart's analysis as experts on the e-EHIC usage extensions based on Identification process in respect to European guidelines.

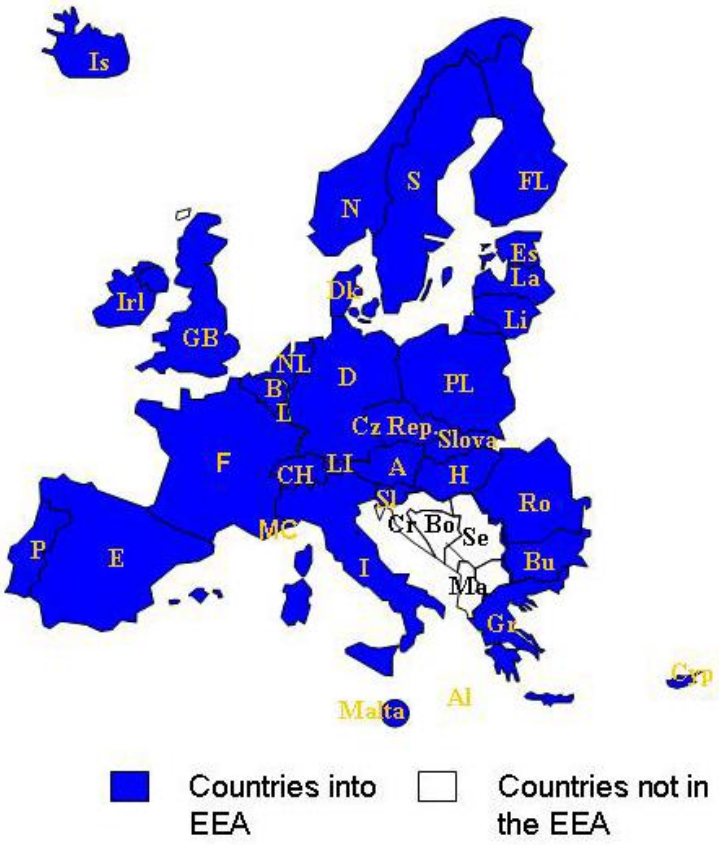
[1] http://www.eurosmart.com/index.php/glossary.html

2. e-EHIC smartcard & Identity controls

EHIC means European Health Insurance Card. It concerns anyone who is insured by or covered by a statutory social security scheme of the European Economic Area (EEA) or Switzerland. In line with E.U. rules, it replaces several paper forms:

- E110 for international road hauliers
- E11 for tourists
- E119 for unemployed/job seekers
- E128 for students and workers in another Member State

According to regulation 1408/71, the EHIC grants the European holder the right to any treatment that becomes medically necessary during a temporary visit in other EEA countries or Switzerland. The EHIC covers treatment provided by the state healthcare scheme in the country you are visiting. It does not cover repatriation costs. The intention of the scheme is to allow people to continue their stay in a country without having to return home for medical care.



The EHIC was phased in from June 2004 and throughout 2005, becoming the sole healthcare entitlement document on 1st January 2006, and is now provided free to all citizens of participating countries.

This plastic card has been designed as a first step towards a full-blown electronic system where patients, healthcare professionals and social security institutions can communicate without paper in cross-border situations, in the same way as they would within countries.

e-EHIC is the electronic European Health Insurance Card and falls under the European Commission's responsibility (CA.SS.TM). The main features of an electronic EHIC are that it:

- Carries the same dataset in electronic form that is defined by the data printed on the outside of the EHIC.
- Is readable by healthcare providers[2] equipped with appropriate technology from the ecosystem e-EHIC (card reader, middleware on the PC or on the server, workstation with e-EHIC computer program).
- Is verified on-line under conditions (validity, entitlement of the card holder)

The standard endorsed for the e-EHIC is the European Citizen Card even if the e-EHIC is currently viewed as a data set container.

The proposed approach by the E.C. is flexible and progressive, taking into account the diversity of national systems in Europe. It will replace the EHIC in the coming years in some EU countries and retain on its electronic chip the same personal data. The non-electronic EHIC already in the field will therefore be allowed to remain in full use all over Europe even when the e-EHIC is already introduced.

Today, EU-MS can choose from four possibilities for the EHIC document:

- Printed EHIC-Card, ID1-format (smart card); EHIC-doc.
- Printed EHIC-Data Set on the backside of a national patient card; EHIC-doc
- Electronic, stored in a microcontroller, e.g. as part of a national patient card; e-EHIC-doc.
- Electronic, stored in a microcontroller and printed on the backside of a national patient card; EHIC-/e-EHIC-doc

[2] Healthcare providers are general practitioners, pharmacists, hospitals, dentists and other health related practitioners

3. European opportunities through e-EHIC challenges

e-ID opportunity

Health systems are a fundamental part of Europe's social infrastructure. The health sector is a prime growth sector of our economies and widely supported by the European Union Lisbon Strategy and the i2010 initiative. E-Health, the beneficial application of ICT-enabled solutions to health and healthcare has been recognised as a key factor to better cope with the European Digital Agenda and to benefit all citizens. Such health solutions are probably the magic bullet "e-ID" application for all European Member States.

Regarding e-ID, even if governments and smart card industries have developed the European Citizen Card (ECC) standard at CEN, there are always opportunities for Member States to select other standards. The freedom given to them for selecting their own national solutions without any recommendations at the E.U. level, and the lack of widely-used standards mean that standards often conflict and interoperability problems often occur in Europe.

This flexibility is a barrier to generic and useful interoperable solutions and paves the way for complex and expensive bridges between national e-Government solutions.

As the connection standard to the e-EHIC is based on the European Citizen Standard (CEN14480), that means basic functionalities such as identification, authentication and digital signature are available into all future e-EHICs. These standardized Identification Authentication & digital Signature (IAS) capacities should be widely used for others e-topics.

There is a strong opportunity for Europe to develop common basic tools responding to government and private digital requirements, and responding to the needs of the mobile European Citizen who must keep connected everywhere in Europe. In this way, the E.U. should manage Identification when Identity falls under Member States' responsibilities.

Such digital connection will reuse existing infrastructure as do the European ICT consortium STORK[3], epSOS or the NETC@RDS[4] project which already manages the (e)-EHIC and other national healthcare cards in Europe.

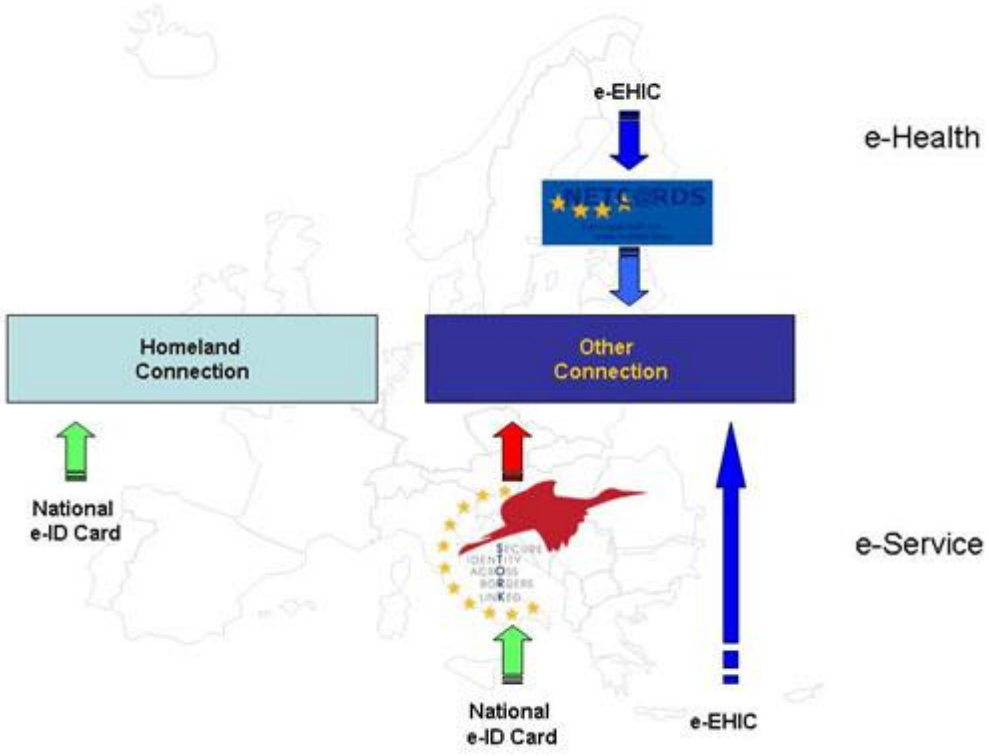
STORK

The aim of the STORK project is to establish a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID. Cross-border user authentication for such e-relations will be applied and tested by the project by means of five pilot projects that will use existing government services in EU Member States. In time however, additional service providers will also become connected to the platform thereby increasing the number of cross-border services available to European users. The role of the STORK platform is to identify a user who is in a session with a service provider, and to send his data to this service. Whilst the service provider may request various data items, the user always controls the data to be sent. The explicit consent of the owner of the data, the user, is always required before his data can be sent to the service provider. The platform will not store any personal data, so no data can be lost. This user centric approach was not taken to satisfy some philosophical preferences, but in line with the legislative requirements of all the various countries involved that require concrete measures to be taken to guarantee that a citizen's fundamental rights, such as his privacy, are respected.

[3] https://www.eid-stork.eu/
[4] http://netcards-project.com/web/frontpage

NETC@RDS

The current phase of the NETC@RDS for the e-EHIC ID project aims to achieve initial deployment of an on-line service for the “electronification” of the European Health Insurance Card (e-EHIC) in 16 EFTA/EU countries. The initial deployment project phase now extends implementations to enable healthcare access for European citizens who provide evidence of entitlement in any of the upcoming 260 Service Units (SU) and around 500 Service Points (SP) across the 16 participating countries (AT, BG, CZ, DE, FI, FR, GR, HU, IT, LI, NL, NO, PL, RO, SL, SK) at the end of the project. The service can be provided via an eye-readable EHIC or a national health insurance electronic card, or via certain national e-ID chip card issued by the relevant government authorities of the participating partners. An on-line verification provides assurance to support acceptance procedures for both health insurance and health care providers. The NETC@RDS application is thus expected to improve administrative healthcare services across member states and mobile access of European citizens to the national healthcare system.



e-Health opportunity

The EU has recognized that eGovernment offers European citizens important opportunities for improved access to better governmental services. When implemented and used correctly, eGovernment offers national governmental systems substantial productivity gains and helps them to cope with increasing demand for high-quality governmental services.

Interoperability is a basic requirement for systems and applications. The European eGovernment world is rather scattered and uncoordinated at the moment and requires some effort to consolidate it. National eID smart tokens could meet national needs as well as nationally specific e-services when the future e-EHIC could manage European cross border e-services

There are some e-health opportunities for e-EHIC by enlarging its scope to e-services due to the on-board standardized IAS capacities. The identification, authentication and digital signature functions could be reused for accessing medical data such as emergency data.

Such data could be stored on the smartcard itself or on a server. The key benefits will be for the patient himself, for the providers, and for the healthcare delivery organisations as described in the table below:

Patient	- Against fraud and misuse of personal data from health care providers - Patient security – enabling quick decision making based on correct facts - Link between the data and the patient
Provider	- Instant patient identification - Rapid accessibility of patient medical history - Elimination of duplicate and overlapping records - Accurate link between patients and institutional medical records - Faster care delivery in emergency care settings - Potential reduction in adverse events and medical errors due to lack of patient information - Reduction in claims denials - Integration with legacy systems with nominal IT costs - Audit trail through a course of treatment that crosses multiple organizations - Reduction in unnecessary/duplicate diagnostic tests or procedures by showing results from other medical providers
Healthcare delivery organisations	- Reduction or elimination of mismanaged, lost or stolen electronic records - Fraud Reduction via accurate patient identity - Data Integrity -- Reduced medical record maintenance costs (duplicate/overlapping) -- - Reduction of calls to Help Desk for password resets - Streamlined administrative processing

Due to the mobility of European citizens, such European e-Service should be managed under the E.U. responsibility and health data should be under the citizen's control. In such a way, citizens will keep connected with their own health data when travelling in Europe. Security, privacy and interoperability will be under control with the smartcard technology and the European Citizen Card standard used for e-EHIC.

In addition to the benefits already pointed out above, the eEHIC may serve some specific use cases of eHealth, telemedicine and social aids as described in appendix 1.

e-EHIC as unique solution in the face of eID challenges

Standards: Challenge n° 1

Even if governments and smart card industries have developed ECC standards at CEN, there are always opportunities to select other standards. The lack of widely-used standards implies that standards often conflict and interoperability problems often occur. Many of the conflicting standards are software based. There may also be differences involving flawed implementations of the same standard that are not interoperable. In some cases, even different versions of the same standard may conflict. This is due to the freedom given to all European member states to select their own national solutions without any current key recommendations at the European level for facilitating interoperability. This flexibility is a barrier to generic and useful interoperable solutions and paves the way for complex and expensive bridges between national eGovernment solutions. Are European citizens prepared to pay for such complex solutions when simpler ones already exist? Probably not.

Business analysts suggest the market for eService information systems in Europe is huge and largely untapped. However, interoperability problems may be one reason for governments and other eService providers to hold off from investing in information and communication technology (ICT). Consequently, growth in companies supplying ICT for the eServices sector is lower than it could be. Furthermore, economic growth related to standardization may accrue predominantly in the country or part of the European continent where a particular standard has been developed. Other economic implications of a lack of commonly-used eService standards are lost opportunities for cost reduction and compromised quality of eServices. In terms of cost, given the lack of commonly used standards, opportunities for streamlining governmental and private eService processes and for delivering activity data go unexploited. And as regards the quality of eServices, a lack of integrated information systems could introduce failures in a Europe-wide system of interoperability whereby European citizens – the final user – will be the victims.

There is now a powerful process in place to harmonize existing standards. The unique standard for e-EHIC could facilitate the common, cheap European approach when cross-border e-services are needed.

Security level requirements: Challenge n° 2

The security levels of deployed solutions may differ from one member state to another, creating conflicts for interoperable eServices. Given that cyber criminals and terrorists will always attack the weakest link in the European defence chain, pan-European security is only achievable if all eID projects are equally strong, but this is not the case for the more popular secure smart card-based approach and the purely software-based approaches used in some national infrastructures.

For example, the European Digital Signature Directive has concrete requirements. But some pure software approaches cannot be used for strong secure signatures because they do not meet protection profile requirements for a level EAL4 augmented signature. What would happen if a document from Country A was signed in Country B with a login-password combination and then delivered for eServices by Country C but was hacked when Countries A or B requested a strong authentication mechanism for digital signature?

No European country would want to weaken national security and compromise their economic efforts further to unsecured foreign choices that could introduce a major risk into their global interoperable system. Member states must therefore evaluate and compare security levels of all national implementations.

European mobility necessitates total interoperability everywhere in Europe but harmonization is not really applied to security level requirements for concrete functions such as identification, authentication digital signature, data memory protection or privacy management. Even if technical solutions already exist, there is no consensus on such crucial and fundamental elements of complete and applied interoperability. The method for measuring security levels already exists with Common Criteria, which is an ISO standard and widely adopted in Europe. It would be highly satisfactory to harmonize security level requests by using common protection profiles for common security targets where security objectives, threats and security function requirements are strongly defined.

The e-EHIC based on the same security requirements could simplify the complex security issue at the European level for cross-border e-services.

Today, e-EHIC is linked to the European standard CEN TC 215, which is the mirror of ISO 251. This standard describes the data set of e-EHIC, which is exactly the same as the printed data set of EHIC. There is no optical and/or electronic security defined, neither on EHIC nor on e-EHIC. EHIC is a simple printed card, in the colour blue, combined with text field in white and the text, printed in black. The current standard on e-EHIC has no definition of a communication protocol between card and card-reader, there is no access condition defined to have access to the electronic data on the e-EHIC-document.

EHIC and e-EHIC have no binding information to the card holder, meaning no photo of the holder and no biometrics. For the identity check of the patient the health professional needs another document, like a driving license, national ID-card or Passport.

Semantics: Challenge n° 3

The interoperability of ICT systems is indispensable for efficient business processes. However, such interoperability for eServices is a big challenge. Those who provide eServices use ICT from different manufacturers from different technology generations and in Europe, from countries with different eService systems, languages and semantics. This means that eService information systems are often unable to exchange data in a meaningful way.

The eServices deployed in different European countries serve similar needs, being used for tax declarations, healthcare services, police declarations, secure private or public transactions, etc. However, the implementation of such eServices differs from one country to the next, and different semantics determine that different input data is required for similar fundamental eServices in different countries. This generates conflict in terms of interoperability.

Specific semantics could be established and deployed with the e-EHIC.

Legislation: Challenge n° 4

Legislation covers national requirements but legislation on a European level for electronic services is still being drafted. Certain definitions of failed responsibility could mean complex responsibility analysis in the case of eService fraud.

A first example is privacy. Privacy is defined as the right of an individual to keep his life and personal affairs out of public view, and to control the flow of his personal information. As a substrate of anonymity, privacy is sometimes related to anonymity and could be seen as an aspect of security. An invasion of privacy is a legal term essentially defined as a violation of the right to be left alone. There are different types of privacy, including bodily privacy, political privacy, medical privacy and privacy from corporations or from government interfaces but for our purposes, we will talk about ePrivacy. This is defined as a person’s right to keep their

electronic life and business out of public view, and to control the flow of their personal electronic information. In order to protect our ePrivacy, the necessary functionality must be part of our digital experience: eIdentification, eAuthentication, electronic signature and data eStorage.

Article 12 of the *Universal Declaration of Human Rights* is clear: "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*" In some countries, privacy is explicitly protected by a constitution. For example, France's Declaration of the Rights of Man and the Citizen and the right to freedom of speech granted in the first amendment of the US Constitution have limited the effects of lawsuits for breach of privacy. Other countries without constitutional privacy protection have laws protecting privacy such as the United Kingdom's Data Protection Act of 1998 or Australia's Privacy Act of 1988. In many countries, if an individual's privacy is breached, the individual may bring a lawsuit asking for monetary damages.

Europeans are acutely familiar with the dangers associated with the uncontrolled use of personal information from their experiences in World War II, with fascist governments and with post-war Communist regimes. In general, they are highly suspicious and fearful of the unchecked use of personal information. The right to privacy is a highly-developed area of law in Europe. The European Commission understands that diverging data protection legislation in EU member states would impede the free flow of data within the EU zone and all member states have also validated the *European Convention on Human Rights*, in which Article 8 provides a right to respect for an individual's "private and family life, their home and their correspondence". It is completed with the harmonization of data protection regulation with the *Directive on the Protection of Personal Data*. The EU Directive 95/46/EC limits and regulates the collection of personal information on individuals, including workers.

Even if the European Union requires all member states to legislate to ensure that citizens have a right to privacy through means such as Directives 95/46, national data privacy laws still vary greatly across Europe. This means privacy concerns are often viewed as a barrier, and there is a complex landscape of privacy within Europe which could have a very negative impact upon European interoperability. Even if privacy issues are seen as generally more difficult to tackle than technical issues, it is nonetheless critical to focus on them. There is currently no clear procedure governing the response to the loss of privacy in one country by a citizen from another country using eServices from a third. It is critical that Europe-wide legislation is completed.

Digital signatures can also pose similar problems. The potential security issues outlined in the conflict of security level requirements section is still pending in terms of European legislation. It is not clear how to manage such security issues in terms of legal and engaged responsibilities between member states, ICT eServices providers, companies supplying ICT for eServices sector and European citizens themselves.

Both examples show that national and European legislation is not sufficiently clear to satisfy the requirements of future cross-border interoperable eServices. In addition to educating citizens about eServices, it is crucial that we focus on such international legal aspects if member states wish to avoid confusing and complex situations linked to the future use of cross-border eServices.

A common European view thanks to the e-EHIC usage could offer a response to the legacy issues and drastically simplify the global approach whereby national eID solutions would be legally limited at national level usages.

4. Eurosmart recommendations

Referring to existing projects that have been deployed in mass production within Europe such as electronic Passports, National ID cards and Driving license and the above technical analysis of a comparison between data-base and Smart secure devices, Eurosmart recommend the use of e-EHIC in order to benefit from its portability, high security and performance. The Smart secure device represents an ideal storage support for personal data in accordance and respect of EU recommendation and privacy protection.

EUROSMART´s recommendations on these programs are as follow:

1. A common European security policy is needed for (e)-EHIC even if each country is responsible for its own security policy.
2. The EHIC data set may be electronically signed by e-EHIC issuers for proof of origin and of authenticity. It must use existing infrastructures.
3. Extend e-EHIC functionalities to identification & authentication for European public & private electronic services.
4. Have European and national e-government e-services able to use the e-EHIC for identification, authentication and digital signature
5. Integrate e-EHIC into STORK, epSOS and NETC@ARDS programs
6. eEHIC could be the right carrier for any social services in the 27 EU MS along with the European EESSI-Program, if the standard also entails security aspects, like level 1,2 and 3 through the optical method and card authentication, secure communication protocol and secure access to the data group through the electronic method.

The e-EHIC usage extension to the internet world should:

- Offer a better e-service to European citizens
- Simplify the mobility throughout Europe for all citizens
- Reduce cost of ownership
- Offer adequate protection of citizens' personal data
- Promote standardisation and interoperability for all Europe
- Keep an open door for differentiation for country specific needs through national e-ID programs under Member States responsibility
- Develop specific e-Health service for citizen travellers.

This is the way to duplicate GSM's success story within the European Digital Agenda and satisfy all European citizens.

Appendix I - eEHIC possible use cases

The ultimate aim of eEHIC is to strengthen the protection of the social security rights of citizens who are mobile by fully computerising application of the EC law on social security. It would simplify procedures:

- Registering a person and verifying entitlement/status;
- Declaring an event (work accident, unemployment, simultaneous activities);
- Requesting a decision (i.e. authorisation, benefit, exception);
- Requesting information.

This will in turn facilitate and speed up the decision-making process for the actual calculation and payment of social security benefits to citizens who move around Europe.
To make the e-EHIC the right token for gaining huge productivity savings, it should be used for more pragmatic use cases in, but not strictly limited to healthcare, and focused on mobility.

- **Health insurance:**

Registering, verifying entitlement/status, issuing an electronic claim:

This use case gives the following results:

- Verification of insurance rights, preventing fraud. This is an immediate benefit for the health insurance company. In the context of European mobility, only automation makes it possible to have an efficient check.
- Practitioner gets reliable access to emergency data that helps for a sound prescription.
- Medical record preparation or update
- Electronic prescription that can be used by the pharmacist or laboratory, preventing misunderstanding of the prescription and allowing him to have a better automation of his own process
- Electronic claim issuance. The number of electronic claims is so huge, that automation provides savings that by themselves justify the cost of issuing healthcare cards.

- **Prevention of mistakes in the management of medical records**

There is the very important need to prevent mistakes in management medical record. The right Identification of the patient must be absolutely sure in some cases, for instance radiotherapy.

The radiotherapy parameters are strictly defined for a patient who cannot be the knowledgeable person.

Today EHIC and e-EHIC is not able to store medical records, as defined in the standard for the document and the international standard for the electronic data group. To achieve the this, a background system for the data management is needed, like a national data bank system on the net. This background system must be installed on a national scale, to allow access from all family doctors as well as from any hospital. In case the service is outside the state of issuing the EHIC/e-EHIC-document, the background system must be workable cross-border.

- **Access to medical personal information**

Huge savings may be obtained by avoiding superfluous examinations . This is the purpose of medical personal information databases. Of course, access to this information must be

controlled, and in many cases with the patient's consent. The Healthcare card is the right tool for this, and at European level e-EHIC would provide interoperability. To avoid fraud and malpractice, the e-EHIC should have electronic security architecture. This should entail three elements

- Card authentication to the card-reader
- Secure communication between card and card-reader
- Secure access condition to read the data group

- **Identification of patients with cognitive disease**

Such patients may have lost the knowledge of their own identity. Their identification by their healthcare card may provide many benefits:

- Identification when they have become lost. In some pathology cases patients may run away out of the control of their carers.
- Accurate identification in healthcare processes.

- Drug supply in anonymity

In this case it is both important to get a right identification of the person, in order to prevent fraud or supply mistakes, and to protect his/her anonymity. The smart card technology makes it possible to provide this service.

- **Telemedecine:**

Telemedecine is a promising service, for huge medical savings, for a better access to healthcare for patients that are in an area without medical services, and for the harmonization of healthcare access across Europe. But the whole process is done long-distance. In this case, identification of the patient, authentication, and maybe electronic signature are useful. Access to his emergency data are crucial. Electronic claims and electronic prescription become necessary.

The chip specifications could be reused for other purposes, such as:

- **Pensions and other social services**

In some countries such services are provided by the same organizers as Healthcare. So it makes sense to use the same personal device.

- **Tax declaration**

This procedure will be performed with security and privacy protection features. Identification, Authentication and electronic Signature embedded in the ECC standard referred by eEHIC.

- **Students/Erasmus program (social links);**

Student mobility is encouraged in the European Union. This population, in addition to the potential need for healthcare, also uses social services.

Eurosmart is an international non-profit association located in Brussels and representing the Smart Security Industry for multi-sector applications. Founded in 1995, the association is committed to expanding the world's Smart Secure Devices market, promoting Smart Security standards and continuously improving quality security applications and services.

Eurosmart members are suppliers and manufacturers of smart cards, semiconductors, terminals, equipment and technology for Smart Secure Devices, system integrators, application developers, issuers, associations, laboratories and independent experts. They work in dedicated working groups (communication, marketing, security, electronic identity, new form factors, and prospect emerging markets).

Eurosmart is acknowledged as representing "the Voice of the Smart Security Industry" and is largely involved in political and technical initiatives as well as research and development projects at the European and international levels.

For more information, please visit www.eurosmart.com

EUROSMART
Rue du Luxembourg 19-21 – B-1000 Brussels
Tel. (+32) 2 506 88 38/ Fax. (+32) 2 506 88 25
Email: eurosmart@eurosmart.com