CPME/AD/Brd/23112013/039_Final/EN

On 23 November 2013, the CPME Board adopted the CPME Policy "Ensuring the secure use of telemedicine and e-health applications in an integrated Europe - Towards a Common Policy Agreement on Electronic ID Systems for Physicians"

CPME Policy
"Ensuring the secure use of telemedicine and e-health applications in an integrated Europe – Towards a Common Policy Agreement on Electronic ID Systems for Physicians"

The Standing Committee of European Doctors (CPME) represents national medical associations across Europe. We are committed to contributing the medical profession's point of view to EU and European policy-making through pro-active cooperation on a wide range of health and healthcare related issues[1].

[1] CPME is registered in the Transparency Register with the ID number 9276943405-41.
More information about CPME's activities can be found under www.cpme.eu

Ensuring the secure use of telemedicine and e-health applications in an integrated Europe - Towards a Common Policy Agreement on Electronic ID Systems for Physicians

European integration and technological progress will, without doubt, lead to an increased cross-border use of telemedicine and e-health, both within the European Union and further afield. At present, the theoretical possibilities of the cross-border use of telemedicine are already evident. Both patients and physicians in Europe are increasingly mobile. Chronic diseases can be monitored using telemedicine when a patient is on holiday abroad. It is also possible to imagine a scenario in which, for example, a Belgian physician logs into a server at a Cypriot hospital in order to gain information about one of his patients in an e-health or telemedicine context.

Whereas there is currently an undeniable focus on eHealth, there remains a certain amount of legal uncertainty in this area, especially in a cross-border context. The European Union has, however, taken some first regulatory steps in this direction. Not only does the directive on cross-border healthcare include an article foreseeing the establishment of a European network bringing together, on a voluntary basis, the national authorities responsible for eHealth, the European Commission is currently also undertaking a revision of the framework Directive on Electronic Signatures. European actors, especially the European Commission have been constantly and actively promoting all aspects of eHealth.

electronic Identity for physicians: What do we mean?

The above mentioned scenario highlights the fact that a high level of security and reliability in electronic communication across borders is essential. Still, there is no European legislation on electronic identities for physicians. The suggested Common Policy Agreement on Electronic ID Systems for Physicians tries to close this regulatory gap. By electronic Identity (eID) for physicians we mean the electronic professional identity for physicians for use in e-health scenarios, and due to CPME's supranational nature especially in a cross-border setting.

To go back to our example of a Belgian physician wanting to access e.g. an electronic patient summary of a Cypriot patient, if for example this physician in a case of emergency wants to log into a server at a Cypriot hospital or wants to open the patient summary as suggested by the eHGI he needs

to have an eID to electronically prove his identity and professional authorisation in a secure and trustworthy way. Typically a username and password is used in comparable scenarios e.g. in eCommerce. But for accessing sensitive patient data a password is not secure enough because it is prone to identity theft, i.e. it can be stolen by viruses and other malicious software. An eID under the policy proposed here would use cryptography, i.e. in order to prove the identity of the physician instead of a password a secure private key is used which cannot be stolen. The corresponding electronic certificate (according to the X.509 standard[2]) attests the identity and the professional authorisation ("physician") of the eID (private key) holder.

Hence the eID for physicians suggested under this Policy is meant to facilitate the identification of physicians in these specific situations by setting up common security standards that would be accepted as appropriate in the Member States where the Policy is being recognised.

A common agreement on electronic ID systems for physicians?

While certain Member States have already introduced card systems at the national level, others are either currently in the process of introducing a system, or rely on different technology using, for example, USB sticks, smartphones, etc.. Regardless of the technology in use at the national level, cross-border use, which is favoured by the Commission, requires cross-border interoperability.

The variety of eID systems already existing in the member states, however, has prevented a cross-border interoperability, interoperability meaning that an eID working in one national system will function in the environment of another member states system without any technical adjustments Considering the existing variety cross-border eID will only work under the condition that technical specifications are matched precisely, hence interoperability will almost certainly lead to harmonisation. Technical interoperability is a challenge which will most probably not be solved by a full harmonisation of the technical specifications of all eIDs across Europe but rather by using mediating components and identity federation techniques, as already proposed in certain European projects[3]. In light of ongoing developments, and in order to be actively involved in the discussion, CPME proposes a common European framework (or a “policy” if we borrow the term in widespread use in the IT sector) on eIDs for physicians, thus taking an alternative approach. Efforts to introduce European technical standards for eIDs have so far failed, mainly because they were either technically too ambitious, or they were perceived as an attempt to replace existing national systems. As we

[2] An X.509 electronic certificate links a public cryptographic key with personal data - in our case with the identity and professional authorisation - of the holder of the corresponding private key which is securely stored in the eID carrier medium (usually a chipcard, a secure USB-token etc.). It must be technically separated from the "e-Certificate" in terms of the EU Professional Qualifications Directive. This e-Certificate cannot be used for authentication purposes as part of an eID because it is just a legal document in electronic form with no corresponding private key and its contents are not consistent with established cryptographic eID-standards.

[3] An example is the STORK-Project, https://www.eid-stork.eu

cannot set technical standards (and do not want to either), we intend to define minimum security standards and build mutual trust between the member states and their respective eID systems. Hence the policy is a voluntary, bottom-up approach intended to coordinate rather than harmonise national standards.

Minimum security standards for electronic IDs

Rather, the proposed policy needs to address the level of security and reliability of underlying eIDs. The aim is to coordinate certain standards of existing national eIDs for physicians. As the reliability and security level of an electronic identity for physicians is of fundamental importance to this approach, such considerations are at the centre of CPME's approach. It thereby aims to establish confidence in electronic identities for physicians across Europe by defining minimum organisational and technical standards. Picking up on the example of a Belgian physician described above, it is evident that the administrator of the Cypriot hospital server would expect an assurance that the Belgian professional eID used to log into the server is trustworthy. If the Belgian eID conforms to certain standards defined by the CPME policy agreement then the administrator knows that the electronic identity was issued according to certain minimum standards and can therefore be trusted.

What the suggested eID policy cannot offer

As there has been a certain ambiguity between the suggested eID and a professional card as foreseen in e.g. the Professional Qualifications Directive currently being modernised (Com(2011) 883 final) it seems necessary to highlight what is <u>not</u> suggested by the proposed eID policy:

- developing a common policy does not imply suggesting the introduction of a European card, or of national ID card systems for physicians. There will be no requirement for national medical associations to introduce any form of eID.

- The policy's aim is not to define a European professional card for physicians as defined by the Professional Qualifications Directive. Issuing the license to practice or processing the recognition of professional qualification would have been happened at an earlier stage, i.e. before the eID was issued. The electronic professional identity for physicians according to this policy does not replace the process of recognition of medical qualifications and does not entitle the holder to practice medicine in a Member State.

- The policy does not aim at harmonising existing systems of eID, but rather to define comprehensive minimum security standards which are suitable for building confidence in professional eIDs across Europe. The specific implementation of the security guidelines,

technical specifications, procedures, and the issuance and administration of eIDs for physicians remains within the jurisdiction of the national issuing authorities, for example the chambers of physicians.

The concept of conformity

This policy defines regulatory provisions for the issuance, administration and life cycle of an eID for physicians. The aim of these regulations is to define minimum standards for the quality and security of electronic identities for physicians. eIDs for physicians, may be carried on chip cards or other security tokens containing a cryptographic key and certificate[4] which are suitable, at the minimum, for the secure authentication of a physician when utilising electronic healthcare services.

The key concept of this policy is conformity. Conformity can be achieved if national issuing authorities adhere to the organisational and technical standards regarding the production and issuance of the eID and its carrier media set out in this policy. Conformity of eIDs to this policy should enable physicians, hospitals, patients and e-health services to be certain that they are dealing with an instrument and an infrastructure which they can trust.

An eID for physicians may be considered to conform to this policy if the production and issuance of the eID medium fulfils all organisational and technical requirements and regulations set out in this policy. The following applies in this respect:

- All requirements or regulations which are denoted with either “MUST”, “MUST NOT” or “MAY NOT” must be fulfilled or prohibited respectively.
- Requirements or regulations which are denoted with “SHOULD” or “SHOULD NOT” must be fulfilled or prohibited respectively, unless there are reasonable and plausible grounds for not doing so.

The conformity of an issuing authority or of an eID already in existence to this policy can be indicated in one or more of the following ways:

- A declaration by the issuing authority (for example on its website)
- The incorporation of the object identifier (OID) of the policy document in the certificate(s)[5] of the eID

[4] The term ”certificate“ refers here to an electronic certificate which conforms to the X.509 standard for the purpose of electronic authentication, signature or encryption. It does NOT mean an eCertificate in terms of the EU Professional Qualifications Directive

[5] The term ”certificate“ refers here to an electronic certificate which conforms to the X.509 standard, for the purpose of electronic authentication, signature or encryption. It does NOT mean an eCertificate in terms of the EU Professional Qualifications Directive.

- The policy logo printed on the carrier medium, e.g. the card (if applicable)
- Entry into the corresponding list by CPME

Issuing authorities must declare to CPME that they fulfil all the regulations of this policy and request permission to use the OID and logo. If there is no obvious reason to doubt this declaration then CPME will grant this permission. CPME reserves the right to demand proof of compliance to the policy, e.g. a testimony from an organisation authorised to carry out security audits and certification according to international recognised standards like Common Criteria[6] or ISO 27001.

CPME maintains a list of those issuing authorities that have declared that they have adopted this policy for the issuance of eIDs for physicians. CPME does not guarantee that the organisations on this list actually comply with the policy. Whereas the issuing authority must engage to respect the standards set out in this policy in order to be granted the CPME European eID certification the use of the OID and the logo also does not represent a guarantee by CPME that the issuing authority complies with the policy. Conformity to the policy is based on the self-declaration of the issuing authority. The announcement of the declaration of conformity and the use of the OID and the logo by an issuing authority is, however, only allowed after permission has been granted by CPME. In the case of violations of the policy, CPME can revoke this permission and forbid the use of the logo and OID.

[6] Common Criteria for Information Technology Security Evaluation, see http://www.commoncriteriaportal.org

Technical part

Version and Policy OID, Authors, Policy Logo

This policy has the following characteristics:

Name: Ensuring the secure use of telemedicine and e-health applications in an integrated Europe - Towards a Common Policy Agreement on Electronic ID Systems for Physicians [working title]

Short Name: CPME European eID-Policy for Physicians

Reference: [CPME_eID-Policy]

Publisher: CPME

Authors: Dr. Georgios Raptis, Dr. Alexander Jäkel

Version: 1.0.0 of 23/11/2013

Object identifier: 1.3.6.1.4.1.42675.1.1

Logo: (a neutral logo will be provided at a later stage)

Responsible for creation, update and maintenance of the Policy

The responsible organisation for the creation, updating and maintenance of this policy is the publisher of the policy, currently CPME.

Liability Provisions

The issuing authority of the electronic ID under this policy is liable as specified by the respective national law.

Relation to other Policies, Security Level

An issuing authority is permitted to prescribe security requirements for its own electronic professional identities that are stricter, more secure or of a higher quality then the measures set out in this policy.

If other policies also apply to certain electronic professional identities alongside this policy, meaning that certain specific regulatory areas of this policy are also covered by other policies, then those measures apply which are stricter, more secure or of a higher quality.

Obligations of the Issuing Authority

Issuing authorities are obliged to remain in compliance with the regulations contained within this policy at all times. They may only charge certification authorities with the technical production of electronic professional identities for physicians if these also commit to abide by the regulations contained within this policy. The obligation to adhere to the policy persists at least until all electronic professional identities issued under this policy have been revoked or have expired.

According to this policy, issuing authorities are only permitted to issue electronic professional identities to physicians. They must verify on the basis of official documentary evidence whether, at the time of application, an applicant is entitled to practise the medical profession in the country of the issuing authority. If an issuing authority is made aware before the expiration of the electronic professional identity that the physician is no longer entitled to practise the profession then it must electronically revoke the electronic professional identity (as well as the e-certificate contained on the carrier medium).

The issuing authority must obtain a contractual obligation from the applicant to comply with those regulations contained within this policy which apply to him or her. It may also delegate this task to the certification authority.

The issuing authority should offer the identity holder the possibility of blocking his/her electronic professional identity medium which serves as a visual proof of identity in the case of loss or theft. The issuing authority must block the eID in case of revocation of medical credentials. Corresponding electronic services to verify the validity of visual identities should be brought into operation and made generally accessible.

Obligations of Applicants and eID holders

When applying for an electronic professional identity for physicians, applicants are obliged to ensure that they are legally entitled to work as a physician within the Member State of the issuing authority. They must report the issuing authority about any relevant change of their status, i.e. if their right to practice has been limited or revoked.

Furthermore they are obliged to ensure that the information they provide is accurate and complete. If the electronic professional identity contains a photo (printed onto the medium or in electronic form) then the applicant is obliged to provide an acceptable photograph.

Identity holders undertake to handle the eID medium with care, not to use it inappropriately and to maintain sole control over the use of the eID and prevent its use by third parties. Identity holders must ensure that the private key contained within the eID medium and the access information (PIN) are not misused. They may only use the electronic professional identity's electronic key and certificate for the purposes for which they were intended (e.g. authentication, encryption, decryption and signature).

eID holders may not use their electronic professional identities to gain unauthorised access to patient medical records, make these accessible to others, or manipulate them.

eID holders must ensure appropriate protection of the IT infrastructure for the purpose of preventing improper use by third parties.

If an electronic professional identity medium is lost or stolen, or if an eID holder suspects that the security of the eID has been compromised, he or she must take immediate action to block it electronically. eID holders whose entitlement to practise the medical profession has been revoked may not use their electronic professional identity any more.

Obligations of Users (relaying parties)

Users are obliged to verify the validity of the certificates of electronic professional identities in conformity with the validity model used by the certification authority. This includes online verification of the status of the certificate.

Users must take any restrictions recorded on the certificate into account. Users may only accept certificates if they are being used according to their intended purpose (e.g. signature, authentication, encryption).

Users must ensure appropriate protection of the IT infrastructure for the purpose of preventing the improper use of signature verification, authentication and the use of false encryption.

Obligations of the Certification Authority

Organisational Obligations

The certification authority is obliged to remain in compliance with the regulations contained within this policy at all times. The certification authority should indicate adherence to this policy by publishing a Certification Practice Statement (CPS).

An electronic professional identity may only be issued following reliable identification of the applicant through means of official documentation of identification. The surname and at least one given name shown on an official identification must be recorded on the electronic professional identity's certificate.

The certification authority may only produce and issue electronic professional identities after an applicant's professional status as a physician has been confirmed by the issuing authority, and revoke them if the issuing authority indicates that the eID holder has no more the right to practise medicine.

The certification authority must ensure that the eID carrier medium is securely delivered to the legitimate owner.

The certification authority must provide status information about issued certificates.

Technical Requirements

Adherence to Standards

Electronic professional identities should conform to current valid and accepted technical standards.

Cryptographic key management of the electronic professional identity

Electronic components must be built into eID carrier mediums which effectively protect the private cryptographic key for authentication, signature and decryption. Reading and copying the private key should be virtually impossible. Use of the Secure Signature Creation Devices, as cited in the EU Directive on Electronic Signatures (1999/93/EC), is recommended.

Cryptographic algorithms and key lengths must be used which correspond with the most up to date status of science and technology[7]. The period of validity of the certificate should take into account the strength of the cryptographic algorithms and key lengths used. There may be no backup of the signature key and the authentication key.

Cryptographic key management by the Certification Authority (CA)

[7] A current overview and a yearly report is provided by the European Network of Excellence in Cryptology II, http://www.ecrypt.eu.org/

It should be virtually impossible for the cryptographic private root and CA key to be compromised (unauthorised use, disclosure or calculation).

The CA must utilise technical components and cryptographic keys which correspond to the most up to date status of science and technology.

Organisation of the CA, security management

CAs must employ reliable and appropriately trained personnel. They must be able to demonstrate an appropriate level of security, security management and quality assurance through means of generally acknowledged certification of their operations. CAs must take precautions against emergencies so that their operations and security are safeguarded in the event of unforeseen situations.

Revocation of electronic professional identities

The CA must provide for the cardholder to technically revoke an electronic professional identity's certificate in case of theft or loss. Likewise, the issuing authority must be able to technically revoke the eID if the professional title of the holder is no longer valid.

Publication of the status of the certificate

CAs must offer services which enable users to verify the status of an electronic professional identity's certificate. These services should correspond to established technical standards.

Processes for the Revision of the Document

This policy will be regularly updated to appropriately reflect scientific and technological advances. The creation of a new version could either be initiated by CPME itself, or by a member organisation of CPME with a specific requirement. Any new version must be approved by the Board of CPME. The new version will then be published on the CPME website and would generally come into force 6 months later. Variation of this procedure is possible if well justified, for example due to the adoption of legal regulations or advances in crypto analysis.

New versions of the policy must contain a clarification as to whether older versions remain valid, either on a long term basis or merely for the transitional period. New versions of the policy with major changes[8] receive a new Object Identifier (OID).

[8] Major changes are changes having all varieties of effects on the level of security of this policy, e.g. by creating, modifying or removing obligations for any party.

Definitions

Applicant

Applicant refers to an individual who has applied to an issuing authority for an electronic professional identity for physicians.

Certificate

A certificate, as defined by this policy, refers to an electronic certificate according to the X.509 standard. The certificate links a public cryptographic key with personal data about an individual. Thus, an electronic professional identity enables not only the mathematical verification of a signature or authentication; it also enables these to be attributed to a particular individual.

The certificate must at least contain the surname of the eID holder / physician, as well as the information that the eID holder is a physician. The issuing authority should be apparent from the certificate.

A certificate, as defined by this policy does not correspond to the "e-Certificate" in terms of the EU Professional Qualifications Directive.

Certification authority

The certification authority refers to a technical service provider that is contracted by the issuing authority to operate the technical infrastructure producing electronic professional identities for physicians, as well as the certificates contained on them.

(eID) holder

The eID holder is a physical person who applies for the electronic professional identity, receives this and exercises sole control over it. The eID holder must legally hold the title of "physician" and the valid license to practise in the Member State of the Issuing Authority.

Issuing authority

The term "issuing authority" refers to an organisation which is able to confirm that a certain individual is granted the license to practice as a physician. Hence the issuing body must be able to confirm that an individual is a physician and is entitled to and should receive an electronic professional identity.

The authority issues electronic professional identities for physicians according to the provisions laid out in this policy. It is not mandatory for issuing authorities to technically produce electronic professional identity media themselves. An issuing authority can also be a certification authority.

It is not mandatory for an issuing authority to be a member of CPME.

Publisher of the policy

The publisher of the policy refers to the organisation which defines the content of the policy and publishes the policy. The number of publishers of the policy may be increased in the future. The decision about whether to increase the number of publishers is made by the current publishers.

User (relaying party)

User (relaying party) refers to an individual who

- verifies authentications or signatures which were generated through the use of an electronic professional identity for physicians according to this policy
- encrypts information on an electronic professional identity's encryption certificate
- verifies an electronic professional identity as a visual form of identification (if applicable)