Technological choices of CCBE
in the electronic identification of EU lawyers

Report

CMS Cameron McKenna LLP
Ybl Palace
Károlyi Mihály utca 12.
1053 - Budapest
Hungary

T +36 1 4834800
F +36 1 4834801
v2.0

1st February, 2012
Reference Number: 132711.00001

By Peter Homoki, senior lawyer at CMS Cameron McKenna LLP, Budapest.

I am very much indebted to dr. Istvan Zsolt Berta in providing invaluable help to me regarding the more technical parts of this report. (Any inaccuracies or unfounded statements remaining in the report are however are only attributable to me.)

Table of Contents

1. Executive Summary 4
2. List of abbreviations used 6
3. Introduction 7
4. High level overview of technologies, solutions and trends concerned 9
4.1. Terminology: identification, authentication and authorization 9
4.2. The purpose of the report in relation to authentication technologies 10
4.2.1. A Brief Overview of Credentials 12
4.2.2. Something you know 13
4.2.3. Something you have/own 13
Possibilities for better interoperability and reuse of security devices 18
4.2.4. Something you are 19
4.2.5. Generic IT Trends Affecting the Future of Authentication Credentials 20
a) "Media Tablets and Beyond" and "Mobile-Centric Applications and Interface" 21
b) Contextual and Social User Experience 22
c) Internet of Things 22
d) Cloud Computing 22
4.2.6. The guidance e-CODEX and STORK gives in relation to authentication 23
e-CODEX 23
STORK 24
4.2.7. A menu like overview of possible authentication choices. 28
4.3. A high level overview of authorization (being a lawyer, having a client mandate etc.) 29
4.3.1. Cross-border authorization in the EU in e-government services 29
4.3.2. Authorization in e-CODEX 30
4.3.3. An attribute certificate as a basis for authorization 32
4.3.4. European Professional Card and the proposed amendments of 2005/36/EC Article 4a. 33
5. CCBE's possible choices in supporting authentication and authorization technologies 37
5.1. CCBE formulating technical requirements 38
5.2. Requirements related to e-government services provided by CCBE's members 40
5.3. Coordinated and focused communications with European regulators 40
6. Analysis of the responses from the questionnaire 42
6.1. Current practice in MSs for checking lawyers identity in electronic ways 42
6.2. Does your Government already provide e-Identity for citizens, or will it provide this in the future? (Q4) 43
6.3. Any well-used e-Government services in your country that already provide a reliable web service or other database interface for automatic querying frequently used business information, and which is free for the public? (Q5) 44
6.4. Lawyer's technical capabilities and what technologies are lawyers familiar with (Q7, Q8 and Q14-Q16) 44
6.5. Could the Bar provide CCBE with up-to-date lawyer’s licence? (Q9) 45
6.6. Does the Bar maintain a system where lawyers are identified by electronic means and what are the per lawyer costs in € of these systems? (Q10-Q13) 45
6.7. Advantages and disadvantages of current national electronic lawyer e-ID systems 45
6.8. Conclusions – Proposed Approach for CCBE 46
Annex 1: CCBE Questionnaire on Lawyer E-Identity 47
Annex 2: Responses to the questionnaire summarized in tables and charts **Error! Bookmark not defined.**

Table of Figures

Figure 1 Credentials and other technical levels of authentication 12
Figure 2 OTP example – scratch pad 15
Figure 3 A hardware OTP token (Vasco's Digipass) 16
Figure 4 A different hardware based OTP (Yubikey) 17
Figure 5 OTP example – ArrayShield 18
Figure 6 Expected Chart on Global Unit Shipments 21
Table 1 Required QAA levels 25
Table 2 QAA evaluation levels 25
Figure 7 Composition of QAA Evaluation Levels 25
Table 3 Overview of Authentication Technologies 28
Table 4 Responses in e-CODEX to Electronic Confirmation 30
Table 5 Responses in e-CODEX to Paper Based Confirmation 31
Figure 8 EPC in a paper / electronic form 34
Figure 9 EPC in plastic form 35
Figure 10 EPC Procedure (Temporary Mobility) 36
Table 6 The Annual Number of Electronic Payment Transactions 38
Table 7 Response to e-CODEX Questionnaire 43
Figure 11 Chart of Responses to Q4 51
Table 8 Table of Responses to Q6 51
Figure 12 Chart of Responses to Q6 51
Table 9 Table of Responses for Q7 52
Table 10 List of "other" Responses to Q7 52
Figure 13 Chart on responses to Q7 53
Table 11 Table of Responses to Q8 53
Table 12 Table of Responses to Q9 53
Figure 14 Chart of Responses to Q9 54
Table 13 Table of Responses to Q10 54
Figure 15 Chart of Responses to Q10 54
Table 14 Table of Responses to Q14 55
Figure 16 Chart of Responses to Q14 55
Table 15 Table of Responses to Q15 55
Figure 17 Chart of Responses to Q15 55
Table 16 Table of Responses to Q16 56

1. Executive Summary

This report was commissioned by the CCBE for the following reasons:

a) The growth in use of technology means that it is only a matter of time before lawyers will be able to, and in due course maybe obliged to, conduct cross-border electronic transactions – the CCBE needs to be ready with EU-wide solutions for this, since it is clear that it will be an EU-wide project (see b) below).

b) The EU has begun to contemplate electronic cross-border legal transactions, and has invested millions of euros in the e-CODEX project to investigate how this will happen. e-CODEX is a Member States' project, with the CCBE as an active project partner. The e-CODEX project has now reached the point where it is crucial that the CCBE comes up with solutions for how a lawyer will prove his or her identity electronically across borders for the purpose of a cross-border transaction.

c) The Member States and the CCBE's member bars have different approaches to, and have begun to come up with different solutions to, lawyers' e-identity. This report aims to investigate those different approaches, look at the conceptual basis for e-identity and the direction in which technology is heading, and come up with a solution which will be acceptable to CCBE members and to the e-CODEX project for the future.

d) If CCBE does not come up with a solution in the very short term, there is a danger that the e-CODEX project will move on without CCBE, either leaving out lawyers from the equation or making decisions for the lawyers.

e) CCBE is currently at a stage similar to the stage several decades ago in relation to the lawyers' directives regarding cross-border movement, except this time with the important dimension of electronic cross-border transactions.

The report's main conclusions are as follows:

a) Technology for e-identification is expected to change in the near future. For the time being, CCBE should continue its support for smartcards (including continuing the current level of support provided for CCBE identity card with optional chip capabilities) while taking into account that mobile devices (smartphones, tablets) are expected to be replacing desktop and laptop computers in several use scenarios. Any support provided by CCBE regarding certain technologies has to take this factor into account in the near future, and therefore it is important for CCBE to work towards enabling lawyers to identify themselves in a secure way using mobile devices as well.

b) The CCBE should not support the compulsory use of e-Signatures in all e-proceedings.

c) The CCBE should not support an increase in the requirements for using secure signature creation devices for the creation of signature.

d) The CCBE should in general support technologies that guarantee security (to minimise risk of fraud with lawyers' identity) at an appropriate cost (which includes the use of existing credentials when possible) and that are familiar to EU lawyers.

e) The CCBE should make proposals to EU legislators in order to ensure that lawyers always have to prove their identity (including having a valid license to act as a lawyer) when dealing with cross-border legal e-proceedings.

f) Identifying a person as a lawyer must always involve only data from the bars and law societies (this information is now being provided at EU level by bars and law societies which participate in Find-A-Lawyer, and it is hoped that the EU will soon finance the Find-A-Lawyer 2 project which will use the Find-A-Lawyer e-directory to prove a lawyer’s identity electronically in the future).

g) Based on the large scale project STORK, we have also analysed in more detail some of the security requirements of possible pilot procedures (European Arrest Warrant, European Payment Order and Small Claims Procedure) within the e-CODEX project. Although corresponding legal acts do not give sufficient detail for technical analysis and regulation, the framework provided by STORK (so-called "QAA levels") does so. It is reassuring that this framework is flexible enough to accommodate most of the technologies that we expect to be available for lawyers in the medium term, and the level of security recommended can also be decided based on the expected impact of relevant risks (e.g. a strong password could be enough for filing small claims, but this would not be sufficient in relation to arrest warrants, where more robust, hardware based security solutions should be required.)

2. List of abbreviations used

AC:	Attribute certificate.
ACL:	Access Control List as defined in X.800 3.3.2: "*A list of entities, together with their access rights, which are authorized to have access to a resource*".
Directive 1999/93/EC:	Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signature, OJ L 13, 19.1.2000, p 12-20.
Directive 2005/36/EC:	Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications, OJ L 255, 30.9.2005, p 22-142.
e-CODEX:	e-Justice Communication via Online Data Exchange (COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME, ICT Policy Support Programme,).
FAL:	Find-A-Lawyer, a project initiated by CCBE for finding lawyers in CCBE MSs through the use of a central search facility.
IAM:	Identity and Access Management.
IMI:	Internal Market Information System
LSP:	Large Scale Project
MS:	Member State. Based on the context, it could mean a member state of the European Union, European Economic Area or the home country of bars and law societies being member of CCBE.
NFC	Near Field Communication, a short range high frequency wireless communication technology which enables the exchange of data between devices over about a 10 centimeter (4 inches) distance.
OTP:	One Time Password (see the description in more detail in Section 4.2.3.)
PCI DSS:	Payment Card Industry Data Security Standard
PKC:	Public Key Certificate
PMI:	Privilege Management Infrastructure.
QAA	Quality of Authentication Assurance
STORK:	Secure idenTity acrOss boRders linKed" programme
UI:	User interface.
X.509:	ITU-T X.509 (11/2008) Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, http://www.itu.int/rec/T-REC-X.509-200811-I/en
X.800:	CCITT Recommendation X.800 (1991): Security Architecture for Open Systems Interconnection for CCITT

3. Introduction

CCBE's goal is to think more widely about the future needs of EU lawyers to identify themselves electronically either in another member state or before different forums of the EU. In order to deepen its understanding of the electronic identification of EU lawyers, CCBE has asked the Budapest Office of CMS Cameron McKenna to carry out an on-line survey and an analysis of the responses to this topic, and to summarize its findings and its recommendations in a report.

Identification of EU lawyers means three separate things: *identification* of a person in an electronic system (selecting a single entity from a possible set), *authentication* of the same by providing reliable proofs in ways that are usable an electronic systems, and provision of up to date information on whether the given entity is indeed a lawyer, also called *authorization*.

As long as we differentiate identification from authentication, identification is not necessarily a process that we should analyse from a technological point of view, so we go into more depth regarding first authentication and then authorization.

Regarding authentication, numerous comparative analysis of electronic authentication techniques have already been published based on funding from the EU. The main difference of this report is that we would like to take into account both the specific viewpoint of CCBE and the currently expected future trends in technology, and based on these findings, we would like to see where this future, specific viewpoint fits into the path already set by STORK Deliverable D2.3.

Trying to start from a regulatory perspective, we try to introduce a wide assortment of common authentication credentials, based on a classification of authentication and certain form factors (paper based credentials, software and hardware credentials etc.) We detail certain specific types of credentials in separate paragraphs, e.g. cryptographic chips in smartcards or other formats, and also go into more specifics about NFC and the changes it could cause in the longer term. By introducing the expected effects of strategic IT forces of the near future, we come to the following conclusions regarding the authentication technologies:

a) *Reuse of security devices* (using specific secure hardware for as many scenarios as possible) should be a top priority in the near future, requiring a separate smartcard involving readers for security uses is not desirous even in mid term.

b) The promise of *NFC* is the possibility to decrease the grip (the choke) of mobile operators, and card associations in securely identifying a user, and therefore could be a primary success factor in enabling the reuse of security devices (cf. the convergence in the use of mobile phones for payment purposes, where neither the mobile operator, nor the payment card association is in a unilateral position to decide on the terms of use of the secure element);

c) If it turns out that for some reasons mobile devices and/or payment cards still can't be used for purposes outside its primary domain, *eIDs issued by governments* with secure chip capabilities could still turn the tide toward multiple use eIDs.

d) The most ubiquitous personal computing device in the near future is neither the desktop computer, nor the notebook, it will be an even more mobile device: *a smartphone or tablet device*. This will also have an impact on how people use computers, and security solution using the smartphone platform will also spread. This will be further accelerated if in the future governments also accept identification by social networks.

We also try to put these conclusions into more direct use by showing how these technologies could be evaluated within the context of authentication for e-CODEX: it is possible to accept strong password solutions for Small Claims Procedures, on condition that the registration procedure itself becomes more robust. However, within the framework of STORK, European Arrest Warrant will certainly require qualified certificates included in a hardware security device. For authentication uses of the European Payment Order, there is currently no requirement that makes it necessary to use a hardware token by all means, so a software certificate would seem to be enough as well (but this doesn't mean that smartcards or OTP hardware tokens could not be used for this purpose.)

From the menu-like overview of authentication technologies, we have to stress that requiring hardware-based X.509 certificates for either authentication or signature would be both a very secure option and still with very good chances for later interoperability and later reuse (which could also decrease the corresponding costs.)

Following the overview of authentication technologies, we turn to the analysis of the authorization and of some of the infrastructural problems characterizing this area. It is hard to define a generic legal framework for cross-border authorization, because authorization heavily depends on the area of law affected in the cross-border service and of already existing solutions. There are two issues of authorization of utmost important for CCBE: licence of lawyers and mandates. With regard to the licence of lawyers, it seems that the majority of CCBE members responding to the questionnaire are willing and able to provide data to CCBE (some of the CCBE members are effectively already providing this information thanks to current Find-A-Lawyer database.) Providing a cross-border database for clients' mandate is a tougher problem – useful alternatives could be based on using trusted third parties serving as an interface for offline citizens to the e-government services, e.g. a notary public or even another lawyer who would certify that the mandate was given by that citizen identified therein. Regarding the technical infrastructure of authorizations, although Privilege Management Infrastructure as described by X.509 v4 is a technology that we have to keep an eye on, CCBE is not yet in a position to adapt this technology or to start using it for live purposes.

We do not expect European Professional Card to be used for cross-border e-government purposes, because it is not built with that purpose in mind, and issuance of such an electronic file usually requires previous request by the lawyer to upload his or her file to IMI.

Based on the analysis of the responses and of the previous analysis of technological trend, we conclude that

a) *currently*, CCBE should continue to support the use of *smartcards in identifying lawyers*, but also take into account that all requirements laid down in legislative acts and all conclusions in LSP e-CODEX should be *phrased in such a way that in the near future, lawyers should also be able to use the security elements in their mobile devices* and not only smartcards usable with special readers on a desktop or notebook computer;

b) Based on the expected technological trends, it is also an important conclusion that CCBE should not restrict its support to the use of electronic signature, because e-signatures might not be a good answer in all the electronic procedures affected, and CCBE take efforts to ensure that hardware based authentication technologies without signature capabilities are not excluded at the regulatory level without clear and very specific reasons.

c) We also recommend not to support any widening of the requirements for using secure signature creation devices for the creation of signatures. This could not only create significant and unjustified costs for lawyers, but also lead to unnecessarily increasing the number of devices and corresponding PINs that the lawyers should keep by themselves.

4. High level overview of technologies, solutions and trends concerned

4.1. Terminology: identification, authentication and authorization

In order to be able to delve into technical details, we first have to draft our scope of overview in a more precise manner, paying more attention to some of the underlying terminology.

Electronic identification of an EU lawyer is an electronic transaction in itself and also a part of an electronic service – we will mostly concentrate on electronic services provided by any kind of government, whether it is a local, a federal or a self-government body like a bar or a law society.

In order to securely identify an EU lawyer, we have to concentrate on two separate and very different security services:[1] (a) identification of an entity, which in this regard includes verification of the claimed identity; and (b) being identified as someone being an EU lawyer.

Identification is about providing a user identity to a security system (to the service provider behind the system), searching based on the information given to the system a single identity from the possible set of identities at the disposal of the system. Security professionals consider **authentication** a different phase after identification: the user must provide evidence to prove his claimed identity in the system based on some *credential*[2] or token. We will go into more details about usual and desirable credentials later.[3]

Although there are problems with cross-border identification of EU lawyers *per se* as differentiated from authenticating these lawyers only, these problems are of pure data protection, privacy or constitutional law origin: can we use any unique identifier for lawyers and other e-process participants, can anybody in the EU issue such unique identifiers for cross border identification purposes? Could these identifiers be listed in e.g. public X.509 certificates used within the authentication as well?[4] Should these unique, cross border identifiers be permanent or is it enough if they are transient?[5] From the point of view of this report, it is only the technology of electronic authentication that is important for analysing the choices of CCBE.

Please note that the abovementioned separate steps of the identification and authentication are quite often used together (cf. the term IAM for "identification and authentication management"), interchangeably or even as synonyms.

[1] See definition and enumeration of security services in Section 3.3.5.1 and Section 5 in X.800.

[2] See definition of authentication in Section 3.3.7 in X.800: "*See data origin authentication, and peer entity authentication. Note – In this Recommendation the term "authentication" is not used in connection with data integrity; the term "data integrity" is used instead*". Also see Section 3.3.40 in X.800: "*peer entity authentication: The corroboration that a peer entity in an association is the one claimed*."

[3] Todorov, Dobromir: Mechanics of User Identification and Authentication: Fundamentals of Identity Management, Auerbach Publications, Boca Raton, 2007, p. 5. and Section 3.3.17 in X.800: "***Credentials***: *Data that is transferred to establish the claimed identity of an entity.*"

[4] Please also see:

a) Large Scale Project STORK, "D2.2 Report on Legal Interoperability", https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=578, p. 41; and

b) Large Scale Project e-CODEX ("*e-Justice Communication via Online Data Exchange*") "D4.1 Identity inventory and requirements", WP4-REQ-F-003 "Resolving the EOPIC", WP4-REQ-NF-003 on pp. 30 and 31, and Section 6.1. on p. 48 ("*But only half of MS credentials which based on X.509V3 certificates include the EOPIC or have an option to include one within the certificate*"), http://www.e-codex.eu/index.php/downloads2/category/1-deliverables?download=3:d41

[5] Please compare the different conclusions in e-CODEX in section a) in footnote 4 with the conclusions on p. 36-37 of STORK D2.3 - Quality authenticator scheme https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577.

In standard computer systems, after the authentication process is successful and the claimed identity is verified, the entity is provided access to the system, with previously defined rights that are assigned to his identity. But it is also possible that the system doesn't know the user in advance, these rights are not set a priori. In this case, besides identification and authorization, the system also has to check from a different directory, system or a separate certificate what this particular user is entitled to do in the system. This step of checking and assigning rights to a particular user is called **authorization**.[6]

So if we talk about "*identification of an EU lawyer*", we do not speak only about *identification and authentication* of a person, but also about this prior check of *authorization*, about checking whether that particular person identified by e.g. a common European personal identification number is in fact a lawyer at the time of access or not. However, this separate step of authorization could technically be very different from authentication. This authorization can be carried out in several different, non-related ways:

a) based on paper certificates (similar to checking of qualifications according to Directive 2005/36/EC[7]) and by manually entering the results into the target system by a verifying person;

b) based on reliable electronic messages from trusted parties, like public notaries or a department of a Member State who themselves have verified the information;

c) by an automated web service using an electronic authentic register, like land registers (similar to the web service response in Find-A-Lawyer given by bars to the central search engine);

d) directly by checking a special attribute in an X.509 qualified public key certificate identifying the lawyer; or

e) by using a special X.509 electronic certificate (called attribute certificate) issued and digitally signed by an attribute service provider, which is usually valid only for that electronic service session (e.g. for minutes only).

We also have to mention that e.g. in the Large Scale Project of e-CODEX, at least two different issues of authorization arise, that is, at least two attributes are to be certified in an electronic service:[8] one is whether the person identified is licensed as a lawyer, and the other is whether this lawyer has any effective mandate (power of attorney) from the client concerned. Some further attributes could also be checked in an electronic service, e.g. where a law firm is given a mandate, which lawyer is entitled to act on behalf of this law firm, or when a lawyer is to be substituted by another lawyer in front of the court etc.

Although the majority of the technical part of this report is about authentication technologies, and more closely, on the security devices issued to clients, we also go later into some detail about authorization techniques and whether CCBE could be in any position to support authorization techniques.

4.2. The purpose of the report in relation to authentication technologies

Numerous, wide-ranging and comparative analysis of electronic authentication techniques have already been published within the EU, and we have to specifically mention two papers

[6] See Section 3.3.10 in X.800: "*The granting of rights, which includes the granting of access based on access rights.*"

[7] Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications.

[8] Cf. e-CODEX Deliverable D7.1 Governance and Guidelines Definition, p. 40, Section 5.3.1.1.

funded by the EU, the IDABC proposal[9] and the more recent STORK Deliverable D2.3 Quality authenticator scheme.[10] Both reports can be seen as providing a menu-like alternatives for its readers as well.

So in order to create any possible value for CCBE, we do not want to repeat neither the approach, the methodology, nor the results of those papers, but if possible, still build upon them. Therefore, first will give a user friendly overview of possible authentication technologies (and try not to be too technical at the same time), then take a glimpse at the future of IT trends affecting the use of these technologies, and also take an inventory of how this all fits into the abovementioned STORK Deliverable D2.3 (which itself builds upon the IDABC proposal also mentioned). Finally, from the probable point of view of CCBE, we include the required "menu-like overview of the possible options".

Authentication is considered to be a security service and therefore is always part of a wider system. Thus, the technologies used for authentication and the security of authentication can't be analysed only by looking at the evidence that the user provides. We *should* also take into account where and how this evidence is issued, checked, how the authentication protocol works etc.

Nevertheless, we will restrict our scope of overview to credentials only for several reasons:

a) the chosen credential and the associated risks have a considerable impact on higher levels of the authentication architecture as well, i.e. a robust credential is a precondition for a robust authentication architecture;

b) analysis of higher level technology would require analysis of either certain market leader IAM software products, very generic IT architectures or very specific procurement requirements of CCBE;

c) the analysis of the quality of authentication in STORK deliverables also focused mainly on credentials and the registration process, with only a slight detour to the area of the security of the authentication protocol used;[11]

d) we do not consider the registration process carried out prior to issuing the credential as a technological process, so we exclude it from our review, even though a reliable registration process is a prerequisite for secure authentication;

e) the reason for drafting this report was not to provide a technical background for implementing some specific, secure authentication protocol on behalf of CCBE or the bars, but to help CCBE "*to think more widely about the future needs of EU lawyers to identify themselves electronically*", and currently the most expensive, most decisive factor in providing a secure computing environment for an indefinite number of pan-European e-government services lies on the client side, with the provision of credentials;

The following figure is from a STORK deliverable "D5.1 Evaluation and assessment of existing reference models and common specs"[12], and it illustrates how the level of credentials relate to other levels of the authentication service.

[9] eID Interoperability for PEGS – Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms, December 2007, http://ec.europa.eu/idabc/servlets/Docbf72.pdf?id=29622

[10] https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577

[11] Cf. section 2.4.2 of e-CODEX Deliverable D2.3 - Quality authenticator scheme, https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577

[12] p. 40, https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1440

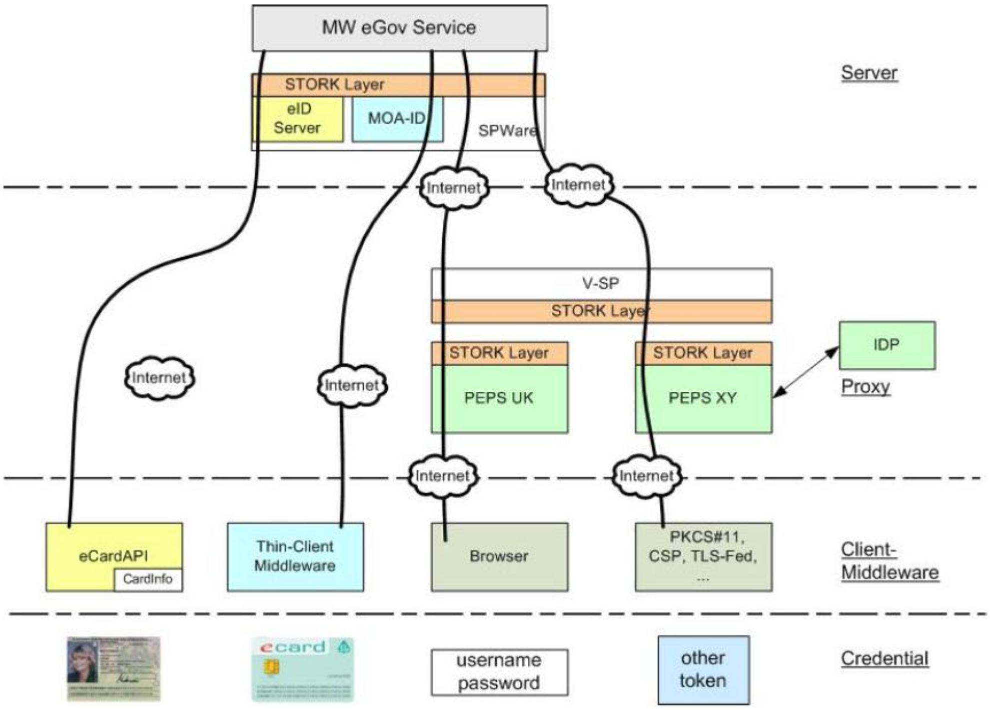


Figure 1 Credentials and other technical levels of authentication

4.2.1. A Brief Overview of Credentials

To more closely follow the viewpoint of a lawyer, it seems it would be useful to start the overview of credentials from a normative perspective. Unfortunately, there aren't any generic legal requirements of secure authentication at the EU level. Other than legal acts prescribing certain technologies and other than Directive 1999/93/EC itself (which is mostly specific to a given type of credential), there aren't any requirements of authentication in the legal acts of the EU.

The closest similar requirement within the secondary law of the EU is the generic requirement in Article 57 (1) a) of the payment services directive[13] of making sure "*the personalised security features of the payment instrument are not accessible to parties other than the payment service user entitled to use the payment instrument […]*". It is not part of the acquis communautaire, but some of the principles set by the Basel Committee for electronic banking (Risk Management Principles for Electronic Banking) also cover a similar requirement: "*Banks should take appropriate measures to authenticate the identity and authorization of customers with whom it conducts business over the Internet.*"[14])

But we can find a very good starting point for the presentation of credentials in a normative document applicable to US financial institutions:[15] "*The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties*. […]

[13] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L 319, 5.12.2007, p. 1-36.

[14] Principle 4 in Risk Management Principles for Electronic Banking, May 2001, p. 17., available at: http://www.bis.org/publ/bcbs82.pdf. See also the provision of the Basel II requirements (serving as a background for "MiFID directive" 2004/39/EC) naming identity theft as a Basel II event type: "External fraud for operational risk management" in Basel Committee on Banking Supervision: International Convergence of Capital Measurement and Capital Standards, Annex 7, available at: http://www.bis.org/publ/bcbs107.pdf.

[15] Federal Financial Institutions Examination Council: Authentication in an Internet Banking Environment, p. 3. http://www.ffiec.gov/pdf/authentication_guidance.pdf. Cf. also Dobromir, Todorov op. cit., p. 18-19.

Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods." and also "*single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks*."

So to give an overview of credentials, it is useful to start categorization by using these so called *factors* of authentications. The same document describes these factors as follows:

"*Existing authentication methodologies involve three basic "factors":*
- *Something the user knows (e.g., password, PIN);*
- *Something the user has (e.g., ATM card, smart card); and*
- *Something the user is (e.g., biometric characteristic, such as a fingerprint).*"[16]

It is important to note in advance that differentiation between these factors is in many cases subjective, not clear-cut, and they have no universally accepted definitions. Therefore, we start each factor with a short description of how we understood this definition. As credential is defined as "*data that is transferred to establish the claimed identity of an entity*",[17] a common characteristics of all credentials is that certain specific data has to be transmitted for authentication – the difference is how this data is protected from different security risks.

We will cover the most important credential types based on these categories, but we have to mention that the "something the user knows" factor is not really technology-dependent, and will not be affected by any future technology changes.

As we have seen from the requirements of the FFIEC, usually more than one of the abovementioned credentials are used during secure processes. (This is also the reason why we need to enter either PIN-codes or biometrics when accessing even secure hardware devices, like smart cards or OTP supplying tokens.)

4.2.2. Something you know

We consider an authentication factor "you know" if during the process of authentication, the natural person user has to input some data based on his or her memory (and not e.g. based on information the person reads from certain devices, which we discuss under "you own".) Here, the main assumption is that in order to be secure, the data to be directly used for authentication, should not be revealed to unauthorized persons.

Also known as the password, PIN-code and any similar information (gesture pattern on a multi-touch screen phone.) Evidently, there are no techniques involved in this authentication factor. We can differentiate between passwords only based on their *strength*, that is, how easy it is to guess or spy its content.

4.2.3. Something you have/own

We consider an authentication factor "you own" if during the process of authentication, the natural person has to provide an evidence in his or her possession based on some of the input capabilities of the computer system used. This is the most heterogeneous category of credentials, so in order to give an overview, it is indispensible to create further categories (features) of these credentials and show the most popular types by showing how they differ in these different features.

For this category of credentials, the data to be used for credential purposes is either protected by using unique physical characteristics other than biometrics (4.2.4) or certain physical or

[16] There are further factors not mentioned above, e.g. someone who knows you, somewhere you are etc. They would not be really useful in overviewing associated technologies, so we do not mention them.
[17] Cf. footnote 3 above.

non-physical devices provide help for a user in keeping the data secret (and thus, secure). Physical keys can be classified in the previous group, whenever they are used in an authentication process connected to a computer system (by way of e.g. an electronic lock or similar.)

Most of the "something you have/own" credentials belong to the latter group, so we have to further differentiate these credentials based on **how they protect the secret**, and how the **data** to be protected **is delivered** from the device to the authentication system.

Regarding "*how they protect the secret*", a simple method is when they trust *physical barriers* in the protection of the secret, e.g. using printed keys stored in a supposedly safe location, or even using a computer in a location with personal access control. In most cases that are relevant to us, mechanisms for data security are used for such protection of the secret, and these mechanisms can range from storing the secret in a secured storage area in an average computer to storing the secret in a separate secure device or set of devices, which could be anything from a special memory, a chip sized computer system (e.g. smartcard) or a separate secure computer environment composed of several physical computer servers etc.

The less access the user has to this secure device (the more his access is restricted to the necessary extent), the greater the security of the device could be, so it is common practice not to send the secret itself outside the device: they use the secure device to deliver such an answers for the authentication a) from which it is very hard to guess the original secret, still b) it is possible for the authentication system to decide whether the device providing the answer was indeed in possession of the secret.

This can be done by making use of data previously shared by the authentication system and the security device (including using the same cryptographic keys or other secret parameters) or by using public key cryptography.[18]

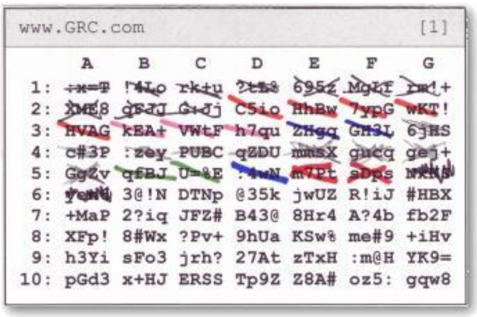
Means of *delivery of the data* to the authentication system are also manyfold and depend on the method of protecting the secret. Delivery works differently if the user receives the credential from a device and user interaction is required for entering the credential to the system (e.g. reading it from a paper or from a special computer and type it), and differently if the authentication system receives this credential in a fully automatic way, either from a radio interface for short distances or from an IP message through the Internet etc.

To give a good overview of all these possible methods of "something you have/own" credentials, we will now demonstrate certain credential types, show where they belong to the abovementioned categories, and then go into more detail for certain important technologies.

A rather unsophisticated "something you have/own" credential is a printed paper sent to the user, where the user enters the passcodes as one-time passwords, either in a given order or according to the position randomly required by the authentication server).19 This is usually called a passcode scratch pad or transaction authentication numbers. This credential is clearly protected by only the assumption of physical security of this paper, and there is no point in going to more details about the method of delivery used.

[18] We do not see it is necessary here to go into details regarding public key cryptography, but the generation of the public and private key is based on a common number and the possibility of finding out the unique connectivity of the two keys, which common number for key generation could also be seen as a "shared data" between the device holding the private key and the authenticating system holding the public key.

[19] Also called unique grid card, e.g. https://www.grc.com/ppp



www.GRC.com [1]

	A	B	C	D	E	F	G
1:	~~+x=T~~	~~!4Lo~~	~~rk+u~~	~~?t$8~~	~~695z~~	~~MgLf~~	~~rm!+~~
2:	~~XME8~~	~~qF2J~~	~~G+dj~~	~~C5io~~	~~HhBw~~	~~7ypG~~	~~wKT!~~
3:	~~HVAG~~	~~kEA+~~	~~VWtF~~	~~h7qu~~	~~ZHgq~~	~~GH3L~~	~~6jHS~~
4:	~~c#3P~~	~~:zey~~	~~PUBC~~	~~qZDU~~	~~mmsX~~	~~gucq~~	~~gej+~~
5:	~~GgZv~~	~~qfBJ~~	~~U=&E~~	~~:4wN~~	~~m7Pt~~	~~sDps~~	[illegible]
6:	[illegible]	3@!N	DTNp	@35k	jwUZ	R!iJ	#HBX
7:	+MaP	2?iq	JFZ#	B43@	8Hr4	A?4b	fb2F
8:	XFp!	8#Wx	?Pv+	9hUa	KSw%	me#9	+iHv
9:	h3Yi	sFo3	jrh?	27At	zTxH	:m@H	YK9=
10:	pGd3	x+HJ	ERSS	Tp9Z	Z8A#	oz5:	gqw8

Figure 2 OTP example – scratch pad

Even this has certain advantages over traditional strong passwords, called static passwords. The most serious drawback of every *static*, even very strong passwords is the possibility of a *replay*. If there is no separate protection in the protocol against replay, it is possible that someone eavesdropping on a non-encrypted channel (e.g. on the computer of the user or on the server or between them) has the possibility to reuse that information submitted for entering into the system (even if not the password itself, but only its hash was transmitted for that particular login.[20])

This risk of replay can be mitigated by solutions such as this, and they are called as "one time passwords" ("**OTP**") by using *dynamic* (changing) *passwords*. (The risk of replay can also be reduced by other parts of the authentication process could, e.g. uniqueness of the message to be signed by the private – secret – key is ensured by time data or a serial number-type of data called nonce.)

Another example for a non electronic device providing OTPs and considered also as "something you have/own" credential is a "unique grid" issued to the user. E.g. in the case of a solution called ArrayShield, users first have to register a pattern (e.g. they will first enter the first character in the lower left corner and then go through the three characters to the right and at the end, go one character up), and users also receive a specific card (a mask) where the empty fields will be translucent, and some remaining fields fixed. At login, they will see a randomly generated table of 5x5 fields, put the mask on this field on the monitor and enter the characters they see on the monitor in the order of their previously recorded pattern (as a one-time password).[21] In this case, the credential is protected by both the physical security of the mask and also by something the user knows (the order of entry of numbers), otherwise it is similar to the scratch pad. But in practice, unique grid based OTPs are not much used (as opposed to passcode scratch pad).

One-time passwords sent in **SMS to mobile phones** for human reading and typing are also a very frequently used method in this "something you have/own", where the dynamic password for entry is generated at a different system and sent to the user by the mobile phone. Thus, the secret for generating the OTP is protected in a reliable computer, and the assumption is that the delivery channel for the OTP to the user is through a reliable medium and the mobile phone is possessed by the right person. Here, the trade off for a much better protection of the secret is the cost of the delivery channel and the inconvenience of having to manually type the SMS into the authenticating system.

[20] The risk of replay is the reason why simply digitally signing a web entry form is not desirous in itself, and is not considered to be safe, because care has to be taken to include a one-off information in the form signed, e.g. exact date and time or similar, or better yet, to use X.509 keypair specifically for authentication and not for digital signature purposes. When using digital signature, we want to ensure the non-repudiation of that given document, and not the uniqueness of the result..

[21] http://www.arrayshield.com/products/howitworks/

Of course there are also credentials where there is no need for manual entry. There are authentication methods for smart mobile phones with internet or other data connectivity that are not using SMS, but specific mobile phone data communications methods, e.g. WAP between a mobile phone and a server etc. (in these cases usually, but necessarily the whole authentication communication is carried out using these mobile data channels.)

A very similar credential is when a specific (previously enrolled) PC or laptop has to be used in the authentication process (as a proof of possession), and certain characteristics of these computers are used for verification (e.g. a unique identifier of the operating system or the hardware or the network card, and a combination of these etc.) All three above methods are based on a unique identification of the devices and the assumption of the *physical possession* of these devices.

Turning to less tangible "something you have/own" credentials, a private and public key pair saved on the disk drive of the computer and protected by e.g. the operating system is an example of a **software based credential**. However, current everyday computer platforms are not inherently secure, and there is a considerable risk in such practice, e.g. illegal eavesdropping on keyboard use, on information displayed, on files stored etc. These risks can't be effectively mitigated in everyday software environments without restricting everyday computer use we are accustomed to.

Therefore for normal computing environments and for security sensitive applications, it is usually better to incorporate the elements that are really important from security purposes viewpoint into separate, hardened computing environments, specifically designed for such use. As the smaller these systems are, the most cost effective and convenient they can become, so we will take a closer look at the smaller end of the spectrum of these systems.

A very distinct group of these devices are what they call hardware OTP tokens. Some of these devices are similar to the mobile SMS or the scratch pad OTP in the way that they display a number the user has to type in to the authentication system (e.g. RSA's SecureID or Vasco's Digipass).

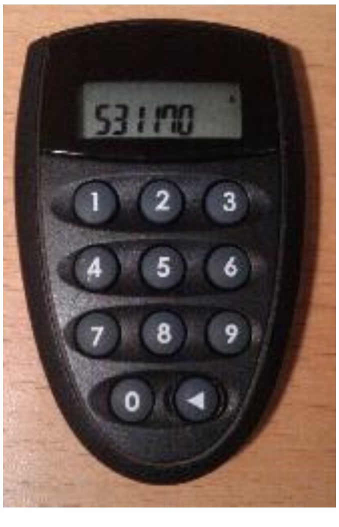


Figure 3 A hardware OTP token (Vasco's Digipass)

However, there are also hardware OTP tokens that just connect to a computer and automatically send a necessary OTP to the computer through the USB port whenever authentication is required.

Figure 4 A different hardware based OTP (Yubikey)

At the smallest end of the scale, there are systems on a chip or microcontrollers. If these microcontrollers are put on a card format, we call them **smartcards**[22] (when used in mobile phones for identification purposes defined in the GSM standards, smartcards are called SIM cards). It is of course of no importance whether the chip is embedded in a plastic card or not, and more such secure chips are being embedded directly into mobile devices like phones or tablets.[23] Even microSD cards inserted into standard memory slots of less advanced phones and tablets can provide these so called *secure elements*. The cryptographic chips in these secure elements (even in microSD cards[24]) are also capable of creating digital signature, so there really is no material difference between the chips of smart cards and these more mobile oriented devices.

No matter how secure these devices are, requiring **separate devices** for security purposes **increases costs and decreases adoption rate**. We also have to take into account that at present, most of these security elements are **single purpose devices only**. Thus, possession of one security device makes a user less likely to be willing to buy the next one (if he has any choice), and the less likely to carry that device with himself wherever he goes. The more costly and the bulkier these devices are, the more serious this issue becomes.

That's when connectivity and interoperability of credentials becomes very important, and this is a factor that CCBE should also very seriously take into account when deciding on the support of certain technologies.

We think is a top priority to choose reliable security elements that can also be used for as many purposes as possible, and that's why security elements within existing mobile devices are more a way forward than smartcards requiring special card readers.

[22] Sometimes chips that provide only passive memory are also called smartcards, but we do not consider these as smart, they are without computing capacity.

[23] TazTag Tazpad, http://www.taztag.com/index.php?option=com_content&view=article&id=104:tazpad&catid=38:slideshow

[24] Even though microSDs are originally a memory only device, the security chip inside them can be capable of doing so, e.g. http://www.oberthur.com/get_downloadsection_file.aspx%3Fid%3D355&sa=U&ei=mSoDT7jYKIXP4QSN3syNCA&ved=0CA8QFjAA&usg=AFQjCNGNLpNcC3vOtkkGxrQHbuYTpjDxcg

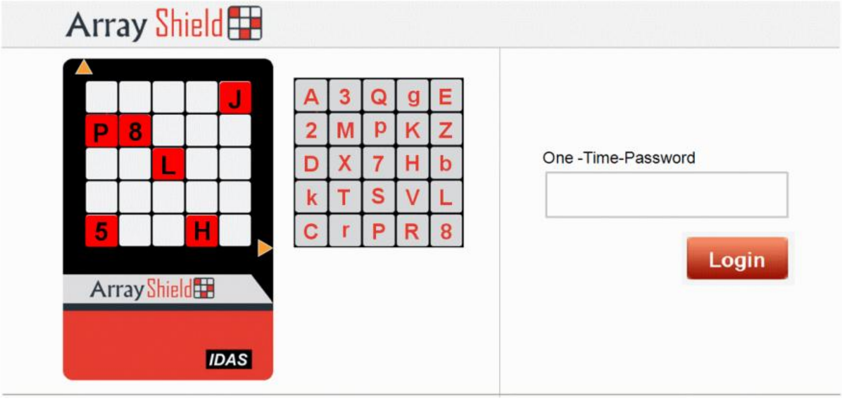


Figure 5 OTP example – ArrayShield

Possibilities for better interoperability and reuse of security devices

If we take a look at the raw numbers of issued secure chips per year, it seems that currently the number of SIM cards is the highest: 4 billion SIM have been shipped worldwide in 2010, 1 billion payment cards with microcontrollers were expected to have been shipped in 2011. In comparison: 190 million eID with microcontrollers were sold in Germany in 2010 only.[25] Taking into account the low percentage of payment cards in the US with microcontrollers and the requirements of VISA and Mastercard, the number of payment cards with microcontrollers will certainly significantly increase in the coming years.[26] (We do not see similar increase in the magnitude of eIDs issued in the coming years.)

Unfortunately, even if we have one or two secure chip already at our disposal, certain circumstances make it impossible to use this secure chip for purposes other than what they were originally intended for.

The *SIM cards* in our mobile phones are only accessible through the *mobile operator*, and identification by way of the SIM card always required their cooperation, and the mobile operators have always retained a strong hold on this infrastructure.[27]

Similarly, *payment cards with EMV capabilities* (debit cards, credit cards etc.) could only be used according to the terms and conditions defined by the card associations Visa and MasterCard (e.g. Brand Value Transaction in MasterCard Rules 6.3.[28]) Maybe this is necessary for ensuring the security of payments, but so far, nobody really had a choice.

This situation can also be seen as some bottlenecks plaguing mobile secure devices. These problems can be solved either by somehow making interoperability more desirous for current controllers of these bottlenecks, or by starting to use new, more open devices or devices under government control.

[25] Gemalto Annual Report 2010, Extending the boundaries of Digital Security, p. 15., available at: http://www.gemalto.com/investors/download/gemalto_ar2010_print.pdf

[26] Cf. resolution of the European Payments Council on SEPA Card Framework, which have introduced in 2006 a deadline that from 1st January, 2011, acquiring banks may – and in many EU countries, already do – decline non-EMV compatible products (payment cards not containing a secure microcontroller), http://www.europeanpaymentscouncil.eu/knowledge_bank_download.cfm?file=Cards SCF 006 09 v 2 1.pdf. The same is expected to happen in the US from 1st October, 2015 for VISA cards only. http://corporate.visa.com/media-center/press-releases/press1142.jsp

[27] This is what made it possible for operators to take 40%-50% of mobile payments where the user was identified by way of the SIM in Hungary.

[28] http://www.mastercard.com/us/merchant/pdf/BM-Entire_Manual_public.pdf&sa=U&ei=KZAZT-7zA8XQsgbp8ahI&ved=0CBAQFjAA&usg=AFQjCNHil7tf9jYFzCZrBhwvYwV2UGC2Rg

Newer mobile phones more frequently contain secure elements independent of the SIM-card. Mobile phone manufacturers are including such capabilities in their higher end models and certain operating system suppliers for smart phones are also starting to require such capabilities from their phones.

When using low-powered radio interfaces, interoperability of security devices is made simpler by making the physical format of the device containing the secure chip less important and transactions based on these devices are at the same time, made quicker (an example for such a solution is the near-field-communications can also show a way forward.[29]

NFC can be a possibility where neither mobile operators, nor card associations are in a position to control one bottleneck and by way of technical capabilities, are forced to cooperate on this level as well (if it is really possible without compromising the security of their devices) – if they do not cooperate, there are also NFC controllers capable of handling multiple secure chips, and making it possible to use the same mobile device for different purposes. (Cf. Mastercard PayPass built into "Google Wallet" capable phones, and VISA payWave in microSD.) However, NFC is not without a challenge, and can also itself turn to be a bottleneck in the future, e.g. by way of certain companies controlling key patents necessary for the use of this technology.

Even if the multi-purpose use of secure chips is somehow prevented by both mobile operators and card associations, *eIDs* with secure chip capabilities issued by certain MSs could (should) be used for lawyer's authentication as well. This could mean ID cards as issued in Austria, Belgium, Portugal, Germany, Estonia, and from 2012 on Lithuania, or e-Passports, electronic EU residence permits, electronic vehicle registration cards etc as well.

4.2.4. Something you are

Also known as biometrics. The only technical means involved in this factor is how the machine *reads* the required value of the user, and they are based on the assumption that some of the characteristics of certain person can be measured more precisely than how these characteristics can be forged at the given level of technology.

We have to stress that although some biometric techniques are capable of directly identifying (not only authenticating) persons, this approach would not be acceptable anywhere outside law enforcement, or forensics. Should anyone start to use biometrics for direct identification of persons, such data would be valid for almost the entire life of a person, without any possibility to revoke it, and there could be only a single such credential for any given biological person, which is culturally unacceptable in most countries.

However, biometrics can still be very effectively used for authentication purposes as long as a) it is only directly connected to non-biometrical identifiers of a person, and b) as long as theoretically it is possible to issue multiple, separate identities for a single biological person, and it is possible for a biological person to use different credentials for the same identity.

As we have already mentioned, it is not secure to base an authentication only on what the user owns, and without resort to biometrics, PIN-codes and passwords could never be retired. They would be the only way to ensure the required second factor of authentication, and we all

[29] NFC's advantages compared to wireless internet is mainly about the simplicity of communication. Communication over wireless internet requires a lot more energy and computing power, with plenty more layers of protocols and possible services to look out for, than what is necessary for two microcontrollers to communicate with each other through NFC. The low power of NFC communications also make it more secure in the meaning that the user can be sure that these communications between machines will only happen within a short distance.

know that the more PIN-codes and passwords we have, the more we tend to use the same or tend to forget the different codes.

There are serious drawbacks of biometrics:

a) Most of them need a special interface for humans (unlike PINs, passwords), which is a considerable barrier for their adoption.

b) Technologies used for biometrics vary greatly in their effectiveness (false accept rate and false reject rate), and the corresponding security they provide, how easily it is possible to fake one or another, how frequently certain characteristics change with time or with situation (medical conditions), how easily it is to collect it from other sources (fingerprints, high resolution photos of the iris and the face, we can't keep them secret). Regarding the effectiveness of certain technologies, it is very hard to reliably verify claims of supplier, and therefore there is a great risk that certain assumptions will turn out not be true in the longer run.

c) We have mentioned the impossibility to revoke biometrics, so if any of the assumptions fail as written above, it is possible that the whole biometrics infrastructure, including all the expensive readers have to be replaced.

d) It is also important that biometrics can be used without being aware of doing so, so it is not necessarily the same as giving a PIN, where we know that currently we are giving consent to being authenticated. E.g. iris recognition works the same way as a "near field" verification like NFC with hardware security devices, even from meters away (but this can theoretically be solved by requiring certain complementary biometrical requirements, e.g. gestures or words that can be considered as approvals.)

In summary, use of biometrics techniques is not yet fully mature. Even if there are very promising results with e.g. iris recognition, [30] and we already have a number of fingerprint readers at the end users, we can expect PINs and passwords to be used for the coming years.

But it is a clear trend the biometrics built into mobile devices could become a substitute for at least some of the PIN-codes that we use.[31]

4.2.5. Generic IT Trends Affecting the Future of Authentication Credentials

While providing an overview of currently available authentication technologies, we have also mentioned some of the expected changes, cf. description of NFC and the use of biometrics.

If we try to see the expected changes in this area of technology, it is not enough to view the future from the perspective of the given industry, we also have to take into account generic trends of the IT industry. Generic IT trends are decided by effects that most currently view as long term, strategic forces shaping the IT industry. E.g. if tablets are a strategic force because they dramatically change UI with the user and at a considerable adoption rate – but smartcards with special readers do not fit at all into this strategic direction, so when supporting smartcards, we have to take this into account that they may inhibit use of tablets by lawyers and of using a single security device by lawyers for multiple purposes.

[30] http://www.theregister.co.uk/2001/05/18/iris_recognition_is_best_biometric/

[31] Cf. Gemalto op.cit, Electronic passports, p. 32.; http://www.oberthur.com/press_page.aspx?id=383&otherid=112&menuId=182&divisionId=0, Oberthur Technologies and AuthenTec Team Up to Demonstrate Fingerprint-enabled Access to SIM-based NFC Services, available at: http://www.oberthur.com/press_page.aspx?id=383&otherid=112&menuId=182&divisionId=0

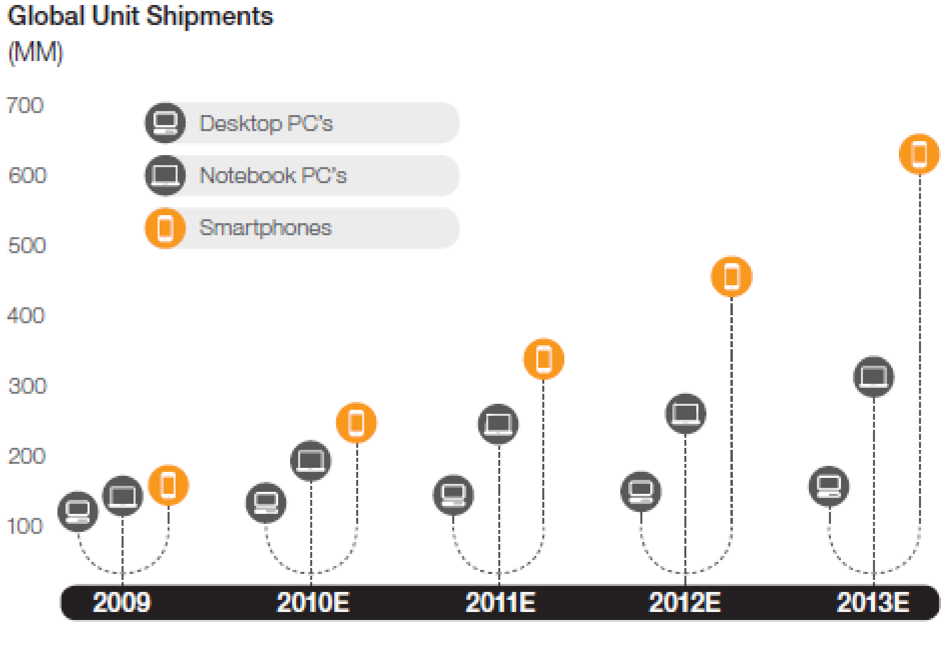
In order to identify strategic forces we have used the key observations of the Gartner 2012 strategic survey,[32] as well as annual reports of market leader suppliers of secure chips' market.[33]

Within the top 10 strategic technologies for 2012 by Gartner, five strategies could have considerable impact on authentication technologies and the use of credentials, "Media Tablets and Beyond", "Mobile-Centric Applications and Interface", "Contextual and Social User Experience", "Cloud Computing" and "Internet of Things". We take a closer look at each of these strategies below.

a) "Media Tablets and Beyond" and "Mobile-Centric Applications and Interface"

Regarding Media Tablets and Beyond, Gartner have highlighted that "Users can choose between various form factors when it comes to mobile computing", "should expect to manage a diverse environment with two to four intelligent clients through 2015", "employees bringing their own smartphones and tablet devices into the workplace". Regarding Mobile-Centric Applications and Interfaces, the key message important for CCBE is that "UIs with windows, icons, menus, and pointers will be replaced by mobile-centric interfaces".

We have to emphasize that not only the number of smartphones sold is expected to increase in the forthcoming years, but that their rate of increase will accelerate and also that it is neither the desktop, nor the notebook computer that is expected to be the most ubiquitous personal computing device in the near future.



Source: Morgan Stanley
E: estimate

Figure 6 Expected Chart on Global Unit Shipments[34]

[32] Gartner Identifies the Top 10 Strategic Tehnologies for 2012, http://www.google.hu/url?q=http://www.gartner.com/it/page.jsp%3Fid%3D1826214&sa=U&ei=dfUXT7LnNoTP4QSsx5TsDQ&ved=0CBcQFjAA&usg=AFQjCNGqctNH8hbBLq3Icg_MPQlhGup8Lw

[33] Gemalto op. cit.; Giesecke & Devrient Annual Report 2010, Questions//Answers Markets//Solutions, available at: http://www.gi-de.com/gd_media/media/en/documents/brochures/corporate/Annual-Report_2010.pdf; Oberthur Technologies Activity Report 2010, http://www.oberthur.com/UserFiles/File/Activity%20Report/OT_AR2010_Locked_UK.pdf

[34] Gemalto Annual Report 2010, Extending the boundaries of Digital Security, p 15.

This will also have an impact on how people will use computers at their workplaces as well, and with the spread of smartphones, security solution usable on the smartphone platform will spread as well. If that is true, users expectations are going to be the usability of mobile secure solutions in other computer platforms as well, e.g. identifying themselves for e-CODEX purposes as well. Users can be expected to prefer use of smartphone based security solutions to current smartcard solutions requiring separate readers.

b) Contextual and Social User Experience

As Gartner have said "A contextually aware system anticipates the user's needs and proactively serves up the most appropriate and customized content" based on the user's environment, connections etc.

A context aware system could make authentication simpler if e.g. the location of the user is taken into account as a secondary factor, or if in case of doubts, social context information is used for verification, the so-called social authentication. (E.g. if a user logs into from a new device not previously used, the user has to recognize certain of its assumed friends.[35]) Context-aware systems could also make issuing a credential easier or more secure. This strategic force could have more direct effect related to authorization, when authorization will build upon the same data sources that are used for context as well.

Regarding social user experience, Gartner have mentioned that "*applications are taking on the characteristics of social networks*". We can also expect that in the longer run, more and more e-government services will be provided directly to users of social networks, i.e. where governments give up on managing the identity themselves in certain domains and accept assertions of social networks through the authentication mechanisms of the social network. However, this heavily depends on the security mechanisms the social networks use, and these are at the moment not as robust as most secure e-government services require.[36]

If governments will accept identification by social networks, and social networks continue to strengthen the authentication requirements and more widely accept e.g. secure elements in mobile phones as credentials, this will further accelerate the changes mentioned in relation to "Media Tablets and Beyond".

c) Internet of Things

The highlight of Gartner regarding Internet of Things is that "*more and more devices will be connected to each other through the common channel of the Internet, and [...] that these technologies will reach a critical mass and an economic tipping point over the next few years*". The techniques mentioned by Gartner are embedded sensors, NFC and image recognition.

With regard to authentication (and also authorization) technologies, embedded sensors and image recognition will play the same role as we have described in connection with context aware systems. Other expected effects of IoT has already been described in 4.2.3 and 4.2.4, that is, in relation to NFC and biometrics.

d) Cloud Computing

More widespread delivery of computing as a service rather than as a product also means a shift from "*border security*". In border security, some of the assurance of authentication was based on physical factors, such as you could only access a system from a specific room or

[35] http://www.facebook.com/blog.php?post=486790652130

[36] There is an SMS based two factor authentication for Facebook at the moment in certain countries, https://blog.facebook.com/blog.php?post=10150153272607131

from a specific computer, and entry to the latter was preceded by reliable access control mechanisms.

However, by using cloud computing, more diverse equipments and locations will be used for access to the same services and this also strengthens the requirements for "*identity based security*".

Thus, cloud computing also makes identification and authentication more frequent than it currently is, and reinforces the current problems with authentication: more dissatisfaction for having to use PINs and passwords, for requiring users to have different security devices to have access to different identities, and more risks from using the same passwords and PINs.

4.2.6. The guidance e-CODEX and STORK gives in relation to authentication

In this chapter, we review the results of the LSPs e-CODEX and STORK so far, and see how these instruments impact the choices of CCBE, and how we can take the results of the LSPs into account when providing an overview of technologies.

e-CODEX

While from CCBE's perspective, LSP e-CODEX seemed to have the greatest and most direct impact on the electronic procedures of lawyers throughout the EU, e-CODEX has only indirect significance regarding what authentication technology should CCBE support.

The reason for this is that at the current stage,[37] e-CODEX only refers back to STORK regarding the acceptable authentication techniques:[38] "*Due to the fact, that no existing national solution can be changed, there is currently only STORK providing a suitable solution for cross-border authentication.*" Therefore, the only contribution of e-CODEX at the present state, is the list of electronic procedures that we have to take into account in finding the proper authentication techniques, where lawyers will participate in an electronic way. From the list of applicable (expected pilot) electronic procedures of e-CODEX,[39] the following ones shall be of main interest to lawyers and thus, to CCBE:

a) Regulation (EC) 861/2007 of the European Parliament and of the Council of 11 July 2007 establishing a European Small Claims Procedure ("*Small Claims Procedure*")[40];

b) Regulation (EC) 1896/2006 of the European Parliament and of the Council of 12 December 2006 creating a European order for payment procedure ("*EPO*")[41];

c) Council Framework Decision 2002/584/JHA European Arrest Warrant ("*EAW*").

The required security of the authentication service depends on the *risks of unreliable identity* in the electronic procedure, and therefore the risk management method we use. STORK defines a risk evaluation method, so after introducing the results of STORK, we will return to analyse the requirements of these risk management procedures later.

[37] We have taken into account the latest deliverables received from CCBE regarding the e-CODEX, e.g. D10.2 Requirements Finalisation and Description of Test Scenarios, but in accordance to the email of Peter Homoki of 11/01/2012 17:43 to Alonso Hernández-Pinzón and the reply to it, the e-CODEX WP has not covered the issue of identification and eIDs yet, and therefore neither of authentication, only the use of electronic signature. Before the closing of this report, we have not received any further deliverables from e-CODEX on this issue.

[38] Section 5.1.2 of Deliverable D 4.1 e-Identity: Inventory and requirements documents, http://www.e-codex.eu/index.php/downloads2/category/1-deliverables?download=3:d41, p. 45. Also see Section 3.7.2. of Deliverable D7.1 Governance and Guidelines Definition, http://www.e-codex.eu/index.php/downloads2/category/1-deliverables?download=1:deliverable-71, p. 32.

[39] Appendix III of Deliverable D7.1., op. cit., p. 89.

[40] OJ L 199, 31.7.2007, p. 1-22.

[41] OJ L 399, 30.12.2006, p. 1-32.

However, we have to call the attention to the fact that we have also read somewhat disturbing communications from the e-CODEX group regarding how they currently imagine the working of identification. As long as identification of lawyers will be exclusively carried out by MSs only (and not according to the so called full STORK model),[42] there is also a considerable risk that lawyers, bars and law societies will not have much choice in the technology used, but to choose from the menu provided by their host MSs only, which will also limit cross-border interoperability.

STORK

The scope of STORK was limited to providing a cross-border framework for as many national authentication solutions, as possible. Thus, the results of STORK includes a description of necessary software, protocols and architectural framework, but it doesn't exclude low-security authentication processes, and *makes no recommendations as to avoiding certain kinds of credentials providing low assurance*.

In STORK, credentials were only analysed with a view of how the recommendations on protocol and framework affect the choice of credentials – and in this regard, STORK has demonstrated that the solutions provided by STORK are in line with these specifications related to credentials.

Therefore, STORK itself does not directly affect CCBE's choice in supporting certain types of credentials for lawyers.[43] However, STORK *does contain a "quality of authentication assurance model"*, that is, a model for assessing what kinds of technologies could be evaluated as safer than others. The authentication provisions within the *new regulation expected to replace directive 1999/93/EC* are also rumoured to be based on STORK, therefore this model in STORK will also affect CCBE's choices.

The authentication assurance model of STORK (Deliverable D2.3 - Quality authenticator scheme[44] defines a "*STORK QAA level*". In our opinion, this should have been called something like the "*required* level of assurance based on risks of the procedure" and a different level should have been phrased for the level that is the result of the evaluation processes. It is confusing that both the required and the final (actual) level is called STORK QAA. This could also be a reason for the fact that the guidelines for *risk impact assessment* in STORK are less detailed than that of the IDABC proposal[45], or that of the United States OMB M4-4.[46] From a lawyer's perspective, we have to admit that the OMB M4-4 is more usable than the IDABC proposal, because in STORK QAA and also in IDABC proposal, there is no detailed guideline as to in which procedure is "high assurance" required, whether any possible risk of personal injury caused by falsely asserting an identity is to be considered to require "high assurance" at all. (The IDABC proposal fails to give any guidance to the correlation between "Impact Severity Scaling" and different types of damages, and it is only

[42] Cf. MW and PEPS models in STORK, https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577.

[43] Cf. STORK Work Item 3.2.3 European Citizen Card, https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1396, STORK Work Item 3.2.2 Information Cards, https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1395, STORK Work Item 3.3.3 RFID & NFC https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1382.

[44] https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577

[45] eID Interoperability for PEGS – Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms, December 2007, http://ec.europa.eu/idabc/servlets/Docbf72.pdf?id=29622

[46] Cf. Table 1 in the Executive Office of the President, Office of Management and Budget: Memorandum to the Heads of all Departments and Agencies, December 16, 2003, M-04-04, E-Authentication Guidance for Federal Agencies, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf, p. 7.

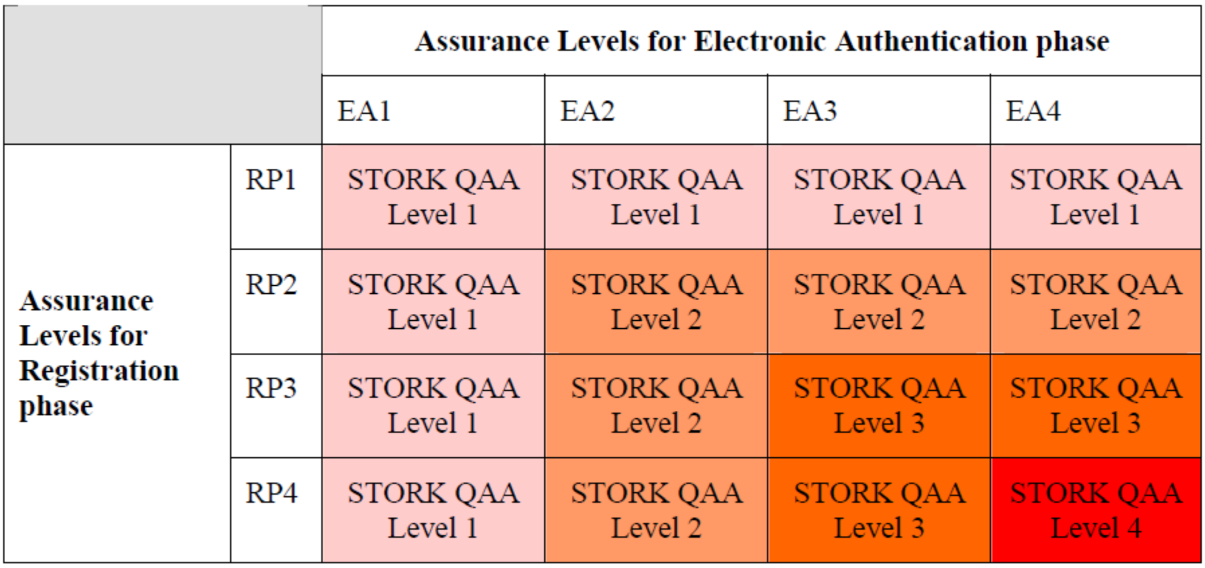
in the OMB M4-4 where specific guidance shows that risks e.g. to personal safety should be taken more seriously in impact ratings than that of e.g. confidentiality or financial loss.)

For illustration purposes and because we will use this QAA in later sections of this report, we cite two tables of STORK D2.3 below (table 1 and table 12 in STORK D2.3):

Risk based *required* level of assurance (STORK QAA levels)	Description
1	No/minimal assurance
2	Low assurance
3	Substantial assurance
4	High assurance

Table 1 Required QAA levels

Evaluation levels based on the results of the evaluation (what QAA levels is the given authentication process able to meet):



		Assurance Levels for Electronic Authentication phase			
		EA1	EA2	EA3	EA4
Assurance Levels for Registration phase	RP1	STORK QAA Level 1	STORK QAA Level 1	STORK QAA Level 1	STORK QAA Level 1
	RP2	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 2	STORK QAA Level 2
	RP3	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 3	STORK QAA Level 3
	RP4	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 3	STORK QAA Level 4

Table 2 QAA evaluation levels

The composition of the evaluation levels in STORK is the following (from figure 2 of STORK D2.3):

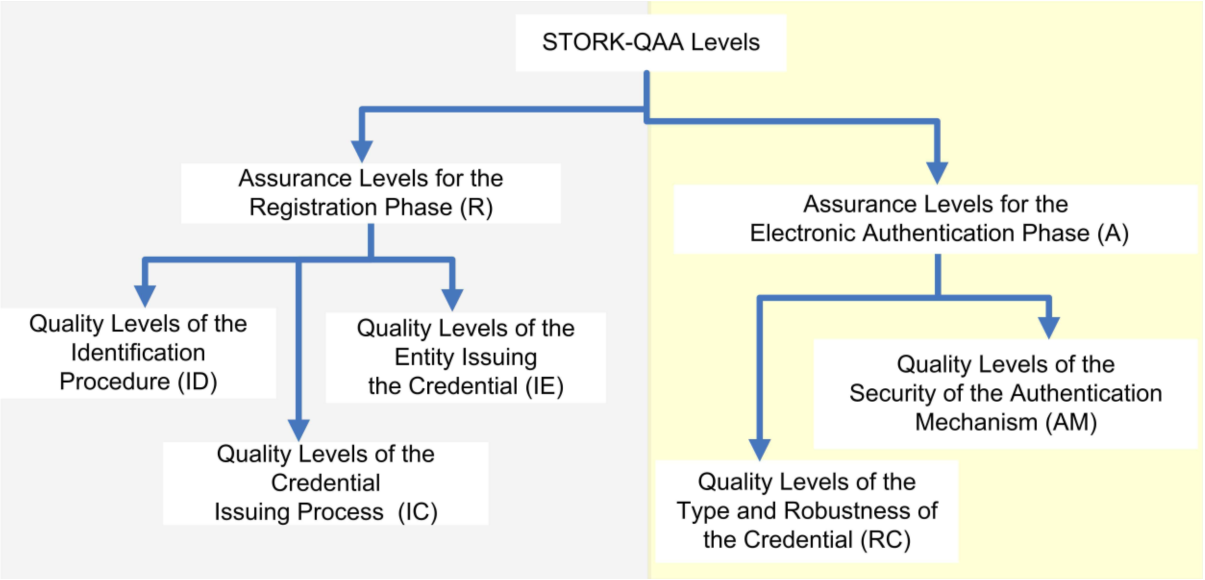

STORK-QAA Levels
Assurance Levels for the Registration Phase (R)
Assurance Levels for the Electronic Authentication Phase (A)
Quality Levels of the Identification Procedure (ID)
Quality Levels of the Entity Issuing the Credential (IE)
Quality Levels of the Credential Issuing Process (IC)
Quality Levels of the Security of the Authentication Mechanism (AM)
Quality Levels of the Type and Robustness of the Credential (RC)

Figure 7 Composition of QAA Evaluation Levels

To incorporate the results of STORK and e-CODEX in this report in providing an overview of technologies, we do not see it necessary to explain (repeat) the individual elements of the composite evaluation level.

We will therefore just analyse what QAA levels should the authentication for the given *e-CODEX procedures* (pilots) meet and *what technologies will meet these requirements*.

Taking into account the minimal definition of "no or minimal assurance" of STORK D2.3, it is clear that authentication of *QAA level 1* will not be suitable for the purposes of e-CODEX. Taking into account that in case of an eID theft, a person could also be unlawfully detained, it is also clear that a rather high level of assurance is required in the case of *EAW*, probably *QAA level 4*.

Thus the only question that remains is whether

a) *QAA level 3* is enough for *EPO* and *Small Claims Procedure*; and
b) should there be any *differentiation between EPO and Small Claims Procedure*, e.g. QAA level 3 of Small Claims Procedure (taking into account the cap of the value involved in this procedure) and level 4 for EPO, or level 2 for Small Claims Procedure and level 3 or 4 for EPO.

In light of the above, we explore what prescribing each QAA level would mean for a given authentication solution:

a) QAA level 4

To fulfil QAA level 4, the credential has to be a *qualified certificate* and *included in a hardware device* (but this hardware device is not necessarily a secure signature creation device, RC4). In order to provide this level, we also have to take a look at the authentication protocol (AM4, EAL4+ or higher of CC), but *this aspect is not affected by the credentials used*, only by looking at the whole authentication solution, end-to-end.

b) QAA level 3

This level is also fulfilled by *software certificates* (regardless of being qualified or not), non SSCD based hardware certificates and by *any kind of one-time password providing device* (RC3).

The entity issuing the credential should be subject to government accreditation or supervision (IE3).
There is a possibility to issue such a credential without the physical presence of the subject for verification. The precondition for such a non-physical presence is rather vaguely defined in the STORK D2.3, so that we do not recommend supporting this version. (Based on the online registration version of ID3, in this kind of online registration, the digital signature of *any kind of CSP* would be enough for validation, and regardless of any security mechanisms used or not used in the underlying digital signature[47]). Nevertheless, if a credential was issued based on a previously issued qualified certificate, then the issued new credential can be accepted at the corresponding level without separate registration.

After the credential is created, it could be either (a) sent by registered post to the official address of the entity (provided there is such an "official address" in the MS), or (b) to be made available for download by a password physically given previously to the claimant (IC3).

c) QAA level 2

[47] Op. cit. p. 20 (iii) (e).

At this level, even *a simple password is enough for authentication purposes*, provided that measures have been taken to ensure the strength of this password (e.g. minimum length and complexity.)

Registration without physical presence is also possible and not only based on a previous certificate, but also based on a simple cross-checking of certain identification data submitted (e.g. by sending a passport number and checking in an online database whether that passport number corresponds to other personal identification data submitted.) (ID2).

After the credential is created, it can be simply downloaded from a link sent to an email address recorded during the registration process (IC2).

Based on the above information, it seems that QAA level 2 in itself might not be enough even for the Small Claims Procedures, and would require further strengthening at least in relation to the registration process to be acceptable (ID3 and IC3 requirement, with strong password of RC2 level only). Similar reinforcements could also be required for the EPO if QAA level 3 is to be accepted (IC4 and/or ID4). There is no point in requiring stronger credentials as long as the registration process is not giving corresponding assurance.

Our conclusion in this regard is the following:

a) it is feasible to accept even strong password solutions in Small Claims Procedure (on condition that the registration procedure itself is stronger than basically requested for QAA level 2);

b) EAW will require qualified certificates included in a hardware security device, regardless of whether these devices are secure signature creation devices or not;

c) *either a software certificate or an OTP hardware token will have to be issued* for use with EPO, or this could be substituted by using any other stronger hardware based token already at the disposal of lawyers (whether based on a smartcard, a mobile phone or a tablet with secure active chip elements.)

4.2.7. A menu like overview of possible authentication choices.

CCBE clearly wanted to have a menu-like overview of the e-authentication techniques available. Please take into consideration that most of the rankings below are a result of only estimations, there have been no exact total cost of ownership calculations carried out.[48]

As already mentioned above, it is very hard to give any meaningful overview of e.g. all possible kinds of hardware based OTPs and all possible hardware based X.509 certificates. Therefore, with regard to certain techniques, we have to give two scores (1-2, 2-3, 3-4, 4-5).

Technique	TCO Ranking for Full Life of the Credential (lowest € = 5) (1-5)	Expected Lifetime Ranking (shortest = 1) (1-4)	Level of Security (lowest = 1) (1-5)	Ranking of Ease of Use, including how well EU lawyers are familiar with it (least familiar = 1) (1-3)	QAA level that can be met with this credential (1-4)	Comments
Strong password	4	1	1	3	2	Although very frequently used, strong passwords are not very user friendly (they are either strong or user friendly)
Unique Grid	2	2	2	1	2	e.g. ArrayField
Scratch Pad with One-Time Passcodes	5	2	1-2	2	2	
Tokens based on identification of computers	4	4	2	1	2	
Mobile phone SMS based OTP	3	4	3	3	2	The longer this solution is used, the more expensive it becomes.
Hardware based OTP	3	2-3	3	2	2	
Software only X.509 certificate	5	2	2-3	2	3	Security heavily depends on the certification service provider used and on its practice. The critical point in security is however the protection of the private key at the end user's device. If it is a trusted platform, security would almost be the same as for HW-based X.509 certificates.
HW-based X.509 certificate (for authentication or signature)	1-2	3	4-5	2	4	Good chances for interoperability in 5 years time: at this level of generality (e.g. not requiring e.g. smartcards), the definition of this credential seems to be the most future proof. If reuse of credentials will become possible, this could become a considerable cheaper solution.
Credential in 1999/93/EC SSCD	1	3	5	3	4	It is possible that future security chips used in NFC communications will not be certified as SSCDs and this could impair reuse of already existing credentials of lawyers. If chips used in NFC communications can be reused and certified as SSCD, then this could become a considerable cheaper solution.

Table 3 Overview of Authentication Technologies

[48] These calculations would have been dependent on specific use scenarios and product offers, which was not possible within the time frame of one month for the analysis.

We will try to give further guidance regarding the suggested authentication technologies, but in these recommendations, we will also try to take into account both the possibilities of CCBE (Chapter 5) and the responses from member bars and law societies (Chapter 6).

4.3. A high level overview of authorization (being a lawyer, having a client mandate etc.)

After a terminological founding, we will be looking at the specific problems of cross border authorization related to e-government services, and then introduce certain possible approaches to the technical means of such authorization, namely Privilege Management Infrastructure (PMI) based on the standard X.509 and the European Professional Card.

As mentioned above, there are numerous methods how we can check in a computer system who is entitled to carry out which function.[49] Radically different methods are used for checking the access rights to certain files (data objects) than for checking access rights to web services for authenticated users, with very different time requirements, revocation mechanisms etc.

One frequently used approach for authorization is based on "*access control information bases*"[50], where the system checks the individual rights conferred to certain entities in access control lists or other access matrices. A different approach is based on the "*capabilities*" of an entity, which means that the authorization depends on the possession and presentation of certain tokens (similar to credentials used in authentication.)[51]

4.3.1. Cross-border authorization in the EU in e-government services

The eGovernment Unit of the European Commission Information Society and Media Directorate-General set out in its roadmap that MSs shall keep these authorization related complexities within its borders, and MSs themselves should provide all the online services required by these authorizations, including mandates etc.[52]

However, based on the deliverables in LSPs STORK, e-CODEX and DIM, it seems that this question is not solved by being referred back to MSs, it is simply avoided.

First, there is a problem of what do individual rights (A) conferred in MS No. 1 effectively mean in MS No. 2? This depends on how much the rights and roles are materially harmonized in the given MSs. Are those rights still the same under a different jurisdiction? Can we say that if public notaries have write access to the land register in MS No. 1 then public notaries from MS No. 2 shall have the same access? It is clear that they can't be the same, but we can consider them to be the same just for certain practical reasons, that is, within certain context and domain.

Can we solve this problem by saying that rights will be defined by the MS where the e-government service is provided, and that the principle of "national treatment" and "non-discrimination" of users from different MSs will solve remaining problems?

[49] Cf. Section 4.1.

[50] Cf. Section 5.3.3.2 in X.800.

[51] Section 3.3.12. in X.800: "***capability****: A token used as an identifier for a resource such that possession of the token confers access rights for the resource.*"

[52] A Roadmap for a pan-European eIDM Framework by 2010, p. 4. "Key principles for a pan-European eIDM system", Section 4-5: "4. With regard to mandate/representation authorisations, *each Member State should provide the means to manage the competences* of the identified users within its borders, insofar as these authorisations are not subject to approval by or on the authority of another Member State." "5. Each *Member State should support online validation mechanisms* of identities, *competences and mandates*, if it wishes to provide eIDM services".
http://ec.europa.eu/information_society/activities/ict_psp/documents/eidm_roadmap_paper.pdf

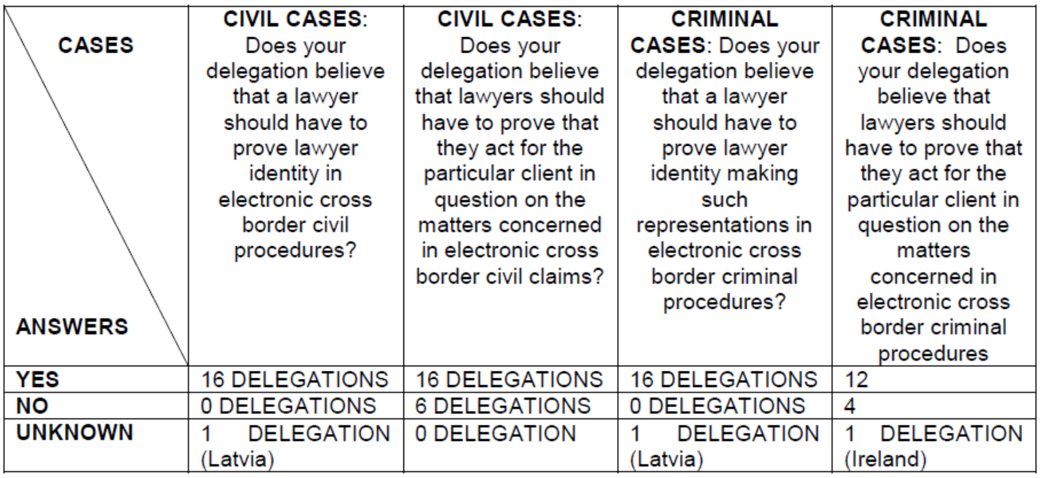
Nobody has expected that e.g. the principles of "free movement of goods, persons and services" within the Treaty establishing the European Economic Community of 1957 would in themselves solve all such problem. Therefore our view is that it would also be naive to think that we can give a clear cut and universal solution for *all* authorization problems in connection with e-government services.

This is not just a question of technology, this also heavily depends on the area of law affected in the cross-border service and of previous solutions. Therefore we can't expect any meaningful solution from LSP STORK, because STORK is independent of legal processes, it is meant to be a generic solution. STORK Deliverable D2.2 – "Report on Legal Interoperability"[53] has expressly confirmed this with regard to universal handling of delegations and mandates.[54]

What one can effectively aim at is to harmonize the technical background for certain specific authorizations, e.g. authorizations necessary in procedures covered by the LSP e-CODEX. If these authorizations are handled in the most flexible way, later on, this could also serve as a financial and regulatory basis for future authorization infrastructure.

4.3.2. Authorization in e-CODEX

Regarding e-CODEX, CCBE's position is that "lawyers e-Identity should be checked in cross-border e-Justice applications and proof of the client's mandate will depend on national requirements",[55] because that was what followed from the responses of member bars and law societies as illustrated in the following tables 4 and 5:[56]



CASES **ANSWERS**	**CIVIL CASES:** Does your delegation believe that a lawyer should have to prove lawyer identity in electronic cross border civil procedures?	**CIVIL CASES:** Does your delegation believe that lawyers should have to prove that they act for the particular client in question on the matters concerned in electronic cross border civil claims?	**CRIMINAL CASES:** Does your delegation believe that a lawyer should have to prove lawyer identity making such representations in electronic cross border criminal procedures?	**CRIMINAL CASES:** Does your delegation believe that lawyers should have to prove that they act for the particular client in question on the matters concerned in electronic cross border criminal procedures
YES	16 DELEGATIONS	16 DELEGATIONS	16 DELEGATIONS	12
NO	0 DELEGATIONS	6 DELEGATIONS	0 DELEGATIONS	4
UNKNOWN	1 DELEGATION (Latvia)	0 DELEGATION	1 DELEGATION (Latvia)	1 DELEGATION (Ireland)

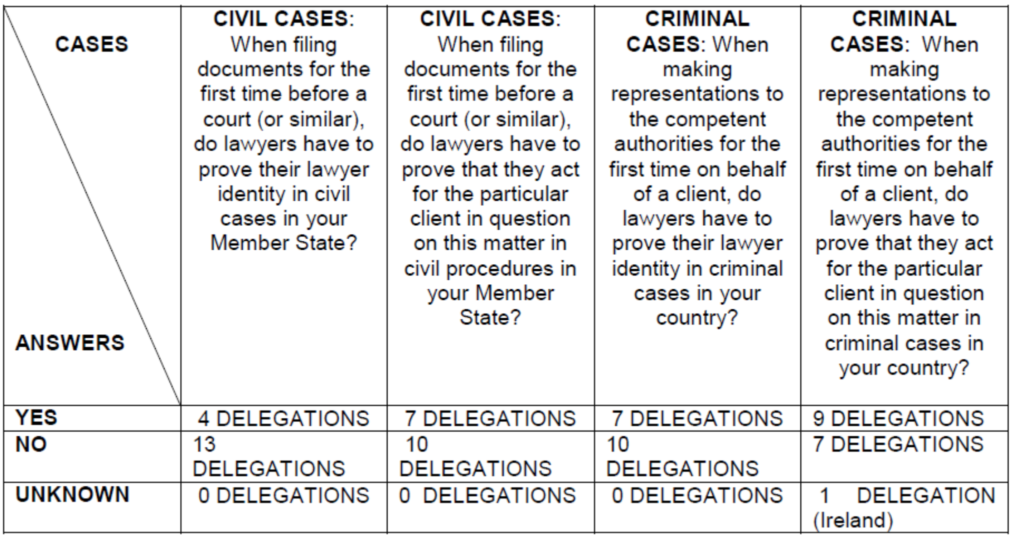
Table 4 Responses in e-CODEX to Electronic Confirmation

[53] https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=578

[54] : Cf. p. 37-38., 3.3.1.: Delegation, mandates and representation are to a large extent part of civil law which means that there may be significant differences between the EU member states. Also in the public sector we may expect significant differences in how representation is handled in the various member states. In some of the country reports submitted by the country reporters aspects of representation are addressed. Beyond this we can not draw hard conclusions regarding representation and delegation of eIDs

[55] ITEM 7 - SP/PS 25-26.11.2011, e-CODEX update by CCBE 10/11/2011, p.2.

[56] Op. cit.



CASES ANSWERS	**CIVIL CASES**: When filing documents for the first time before a court (or similar), do lawyers have to prove their lawyer identity in civil cases in your Member State?	**CIVIL CASES**: When filing documents for the first time before a court (or similar), do lawyers have to prove that they act for the particular client in question on this matter in civil procedures in your Member State?	**CRIMINAL CASES**: When making representations to the competent authorities for the first time on behalf of a client, do lawyers have to prove their lawyer identity in criminal cases in your country?	**CRIMINAL CASES**: When making representations to the competent authorities for the first time on behalf of a client, do lawyers have to prove that they act for the particular client in question on this matter in criminal cases in your country?
YES	4 DELEGATIONS	7 DELEGATIONS	7 DELEGATIONS	9 DELEGATIONS
NO	13 DELEGATIONS	10 DELEGATIONS	10 DELEGATIONS	7 DELEGATIONS
UNKNOWN	0 DELEGATIONS	0 DELEGATIONS	0 DELEGATIONS	1 DELEGATION (Ireland)

Table 5 Responses in e-CODEX to Paper Based Confirmation

This statement of CCBE currently contradicts with the currently published e-CODEX requirement, which says that "*these questions will be dealt with in a later phase of the project*."[57] Even this sentence in the e-CODEX deliverable was a result of CCBE's clear commitment only to the requirement of identifying lawyers as such in the electronic procedure (verifying their capability as lawyers).

Other than this sentence above, with regard to authorization, e-CODEX only refers to HardenedPERMIS as the possible technological basis for the foundations of authorization, see e-CODEX D4.1 p. 45. http://www.e-codex.eu/index.php/downloads2/category/1-deliverables?download=3:d41. We have to mention that this HardenedPERMIS builds upon the attribute certificates and attribute certificate service providers detailed in the next chapter.

However, HardenedPERMIS is not in itself a solution to all questions, and not giving any guidance to who and what the source of authority will be.

If the problematic approach of e-CODEX referred to in page 24 is used, where only MS provide information regarding the identity of lawyers, then there will not be any single source of authority for the information on the validity of lawyers licenses, but each MS has to supply this information (even if eventually based on the central register of the bars or law societies within that MS.)

But it seems more efficient to have a single source of authority. This source of authority will have to be appointed, and information will need to be regularly given to this source. One possible candidate is the European Commission's "Internal Market Information System" (IMI), even more so if the European Professional Card will be used widely.

But it is also possible that CCBE could be in the source of authority position. Identifying a person as being a lawyer requires data from the bars and law societies' of CCBE. Based the responses for the questionnaire attached to this report, a vast majority of CCBE's members are willing and able to provide this data to CCBE. Some of the CCBE members are already providing this information on an almost 7x24 basis to CCBE, thanks to the current availability of the Find-A-Lawyer database.

[57] e-CODEX D7.1 Governance and Guidelines Definition, 5. Organisational Interoperability- Legal Requirements, p. 40., 5.3.1.1, available on http://www.e-codex.eu/index.php/downloads2/category/1-deliverables?download=1:deliverable-71

Regarding the other attribute (authorization) of *mandates and representations*, some important building blocks are still missing here.

While lawyers' as such can easily be identified, in order to have an electronic proof of some mandate from a client, a way of identifying and authenticating the client himself would be required, with all the necessary related infrastructure of the possibility of quick revocation of the mandate. That is, to have a robust authorization for client's mandate, we will also need a robust identification of not only lawyers, but of all citizens as well.

In some of the countries, this could be done based on existing eIDs of citizens, but at this moment, we can't think of any EU-wide solution.

A useful alternative would be to have one or more trusted third parties who could serve as an interface for offline citizens to the e-government services: a notary public, a state-owned enterprise, or even another lawyer who would certify that the mandate was given by that citizen identified therein. But at the current moment, we most probably can't say anything more than what eGovernment Unit of the Commission said here: "*the MSs themselves have to provide a solutions for this*".[58]

4.3.3. An attribute certificate as a basis for authorization

In Chapter 4.1 we have listed two different methods for using the standard X.509 for authorization. One is a direct use of the X.509 *public key* certificate issued to a lawyer and by providing a special attribute saying that the person identified in the certificate is a lawyer. E.g. in the subject field, we could have: T = "lawyer", SERIALNUMBER = "Budapesti Ugyvedi Kamara, registration number:16411", E = peter.homoki@homoki.net, CN = Dr. Homoki Péter, where CN identifies the civil name of the subject, T and serialnumber and registration number identifies the subject as being a lawyer.

There are certain limits to such usage of a X.509 *public key* certificate. One limit is that the more information we put into a public key certificate, the harder it will be to create a unified certificate where all recorded information can be read by all interested countries. Another limit is that the more information we put into this public key certificate, the shorter it's expected validity will be. If any of the extra data changes within the certificate, the complete X.509 public key certificate has to be revoked and issued with new data, and this will be very costly on a pan-European basis. And if we do not revoke the certificate due to changes in certain information, the receiving parties will be less inclined to accept the *public key* certificate for certifying this extra information.

To address these problems, the standardization body of ITU (UN Special Agency) has accepted a new (v4) version for the X.509 standard back in 2001, where besides the previous Public Key Infrastructure (PKI) and public key certificates (PKC), a Privilege Management Infrastructure (PMI) and **attribute certificates** ("**AC**") are also regulated.

STORK D2.2 also confirms this approach: "In some cases, relying parties may want to obtain *more attributes from a claimant than present in the presented eID*, or they may want to *establish an attribute at a higher level of assurance than offered by the eID* (e.g., the address, and even name, present on a smart card may be outdated).[59]]

While PKC serves the purposes of authentication, AC serves the purpose of authorization. This AC is not signed and issued by certification authorities, but by attribute authorities.

[58] https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=578

[59] STORK D2.2 – Report on Legal Interoperability, 3.4.3, p. 42., https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=578

At this moment, *it is not yet known, how much technical knowledge and spending will someone need to be an attribute authorities*. Currently it seems that the regulation replacing Directive 1999/93/EC will not go into details regarding attribution authorities. From an infrastructural point of view, there is not much difference from the infrastructure of an attribute authority to that of a certification authority, which indicates that this *attribute authorities will also be a specialist companies*. They both "just" digitally sign a certificate, and maintain an up-to-date registry for suspension and revocation purposes, which would not necessarily require complex infrastructure, but in order to securely do so, lots of resources have to be invested (including quick response and the security of the signing process is.)

So currently, we do not think it practical that the actual authorities managing the authentic registers or providing a central access to such registers (such as e.g. CCBE for FAL 2.0) will be attribute authorities themselves, but will most probably serve as a source of authority for certain capabilities to be supported by the PMI.

So it seems more feasible to connect these attribute authorities of X.509 with the authentic registers already existing in many of the countries. Most of these authentic registers do not yet provide automatic information in an electronic way, and if they do, there is uniform solution for handling the validity of their assertions. Handling the validity of the authorizations will depend on the database that the verifying party uses, how they store the validity part of the response. However, X.509 based ACs are best issued with short term validity, e.g. for minutes, where there is no need for separate revocation infrastructure for ACs, and still, with long-term archival of the ACs as any other digitally signed document, we can easily demonstrate later that the AC was valid at the time of its issue, regardless of any backup of the database.

STORK D2.2 also refers to this possible future use of authorizations: "*In many of the member states studied, authentic registers exist that offer authorised entities access to authentic data pertaining to citizens. At least Austria, Belgium, France, Italy, Iceland, Luxembourg, Slovenia, the Netherlands and Sweden, offer extensive authentic registers that can be consulted to verify or obtain up to date attributes. The access regimes to these registries differ significantly between the member states. In some case the register is open to consultation by anyone, in other cases access is completely confined to authorised entities*."[60]

In summary, we think PMI is a technology that we have to keep an eye on and an early introduction of such could further speed up interconnection of e-government services, but at the moment, CCBE is not in a position to adapt this technology or to start using it for e-CODEX purposes.

4.3.4. European Professional Card and the proposed amendments of 2005/36/EC Article 4a.

In Directive 2005/36/EC,[61] the European Parliament and the Council encouraged professional associations and organizations to introduce European Professional Card ("**EPC**") to facilitate the mobility of professionals by speeding up the exchange of information between the host MS and the MS of origin.

The form of the original card envisaged was not set in the directive, but it was apparent that certain information would be included on its surface, e.g. university or institution attended, qualifications obtained, experience, etc.[62]

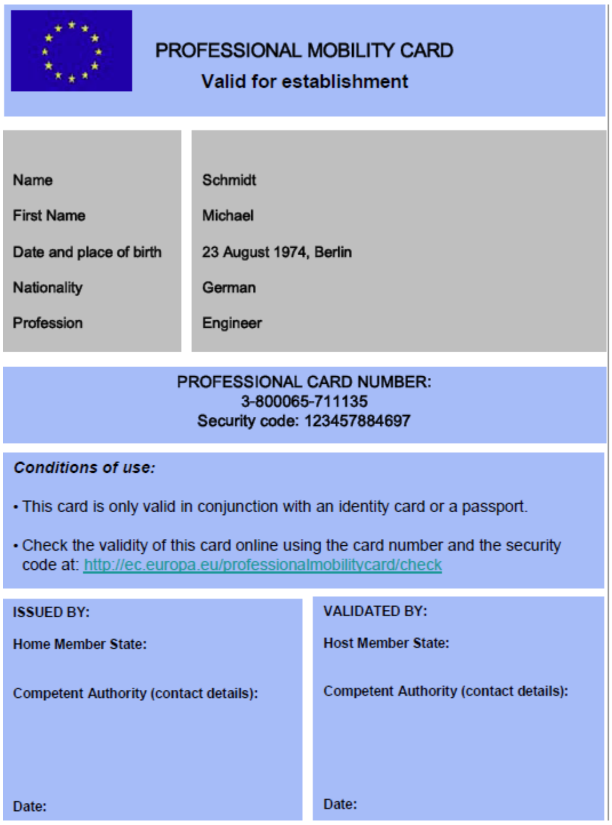
[60] STORK D2.2 – Report on Legal Interoperability, 3.4.3, p. 42., https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=578

[61] Preamble 32 of Directive 2005/36/EC.

[62] Op. cit.

The European Commission made further efforts by drafting a proposal on amending directive 2005/36/EC, [63] and by carrying out case studies on the possible future uses of these EPCs.

Both the proposed amendments and the case studies carried out so far[64] still leave some questions unanswered, but it seems that the EPC will be first and foremost an electronic certificate only in the meaning that upon request from the professional, the competent national authority checks whether it is entitled to carry out that profession and if the authority is affirmative, uploads a file to the IMI system of the European Commission. Later, there will be a public interface for both the professional, for possible employers and consumers with the IMI database serving as a background. Using this interface, the professional can print a paper based card (certificate, see Figure 8) or request print of a plastic card (see Figure 9), and both consumers and employers will check the validity of the professional mobility card on this website.



PROFESSIONAL MOBILITY CARD

Valid for establishment

Name	Schmidt
First Name	Michael
Date and place of birth	23 August 1974, Berlin
Nationality	German
Profession	Engineer

PROFESSIONAL CARD NUMBER:
3-800065-711135
Security code: 123457884697

Conditions of use:

- This card is only valid in conjunction with an identity card or a passport.
- Check the validity of this card online using the card number and the security code at: http://ec.europa.eu/professionalmobilitycard/check

ISSUED BY:

Home Member State:

Competent Authority (contact details):

Date:

VALIDATED BY:

Host Member State:

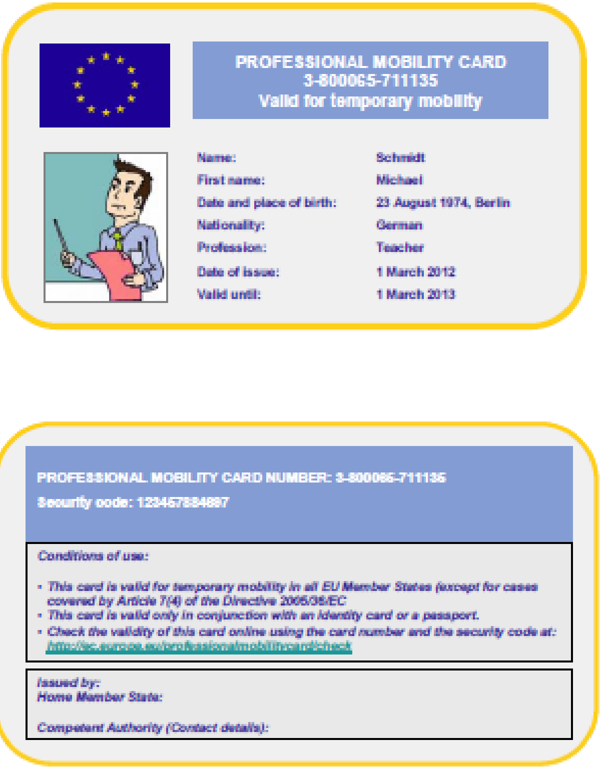
Competent Authority (contact details):

Date:

Figure 8 EPC in a paper / electronic form

[63] Proposal for a Directive of the European Parliament and of the Council amending 2005/36/EC on the recognition of professional qualifications and Regulation […] on administrative cooperation through the Internal Market Information System

[64] The most useful information on this subject was available in the report of the Steering Group on EPC, see the latest report at http://ec.europa.eu/internal_market/qualifications/docs/professional_cards/steering_group_13092011_meeting_report_en.pdf



PROFESSIONAL MOBILITY CARD
3-800065-711135
Valid for temporary mobility

Name:	Schmidt
First name:	Michael
Date and place of birth:	23 August 1974, Berlin
Nationality:	German
Profession:	Teacher
Date of issue:	1 March 2012
Valid until:	1 March 2013

PROFESSIONAL MOBILITY CARD NUMBER: 3-800065-711135

Security code: 123457884897

Conditions of use:

- *This card is valid for temporary mobility in all EU Member States (except for cases covered by Article 7(4) of the Directive 2005/36/EC*
- *This card is valid only in conjunction with an identity card or a passport.*
- *Check the validity of this card online using the card number and the security code at: http://ec.europa.eu/professionalmobilitycard/check*

Issued by:
Home Member State:

Competent Authority (Contact details):

Figure 9 EPC in plastic form

It is important that the public interface for the general public will not contain information other than the validity of the EPC, and if an authority revokes the licence of a professional, the EPC itself should be revoked as well. However, using the EPC is not mandatory, and it will be available only for those professions that wish to have such a card, and only for those lawyers who want to have an EPC. Therefore, publication of the validity of a lawyer's licence is not automatic and thus, if a lawyer has to use an e-government service of a different country, e.g. by way of e-CODEX, it is possible that the IMI database will not contain any information about the lawyer, even though the lawyer is licensed. For this reason, we do not expect the EPC to be used for cross-border e-government purposes.

It is also apparent that even though this EPC will be an electronic certificate only, this will clearly not be a PMI attribute certificate. Article 4c paragraph 4 of the proposal requires that the EPC "*shall be valid for as long as its holder maintains the right to practice in the home Member State*", which also contradicts with standard X.509 saying "*attribute certificates are inherently short term (sometimes in minutes, but definitely shorter than the validity of the holder's public key certificate, which may not be longer)*"[65] Therefore, this electronic certificate will be more like an authentic register, and it is also clear this card will not be an eID in itself.

A detailed description of the EPC procedure without any establishment in a different MS is below:[66]

[65] ITU-T X.509 (11/2008) Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, http://www.itu.int/rec/T-REC-X.509-200811-I/en

[66] All figures are copied from the report of the Steering Group on EPC, op. cit.

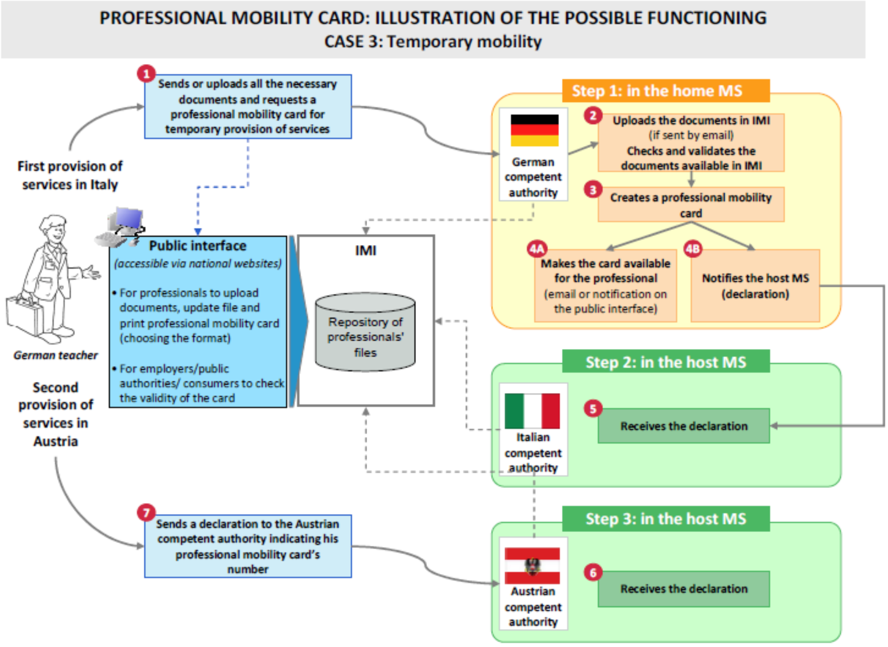

PROFESSIONAL MOBILITY CARD: ILLUSTRATION OF THE POSSIBLE FUNCTIONING
CASE 3: Temporary mobility
1
Sends or uploads all the necessary documents and requests a professional mobility card for temporary provision of services
First provision of services in Italy
German teacher
Second provision of services in Austria
Public interface
(accessible via national websites)
• For professionals to upload documents, update file and print professional mobility card (choosing the format)
• For employers/public authorities/ consumers to check the validity of the card
IMI
Repository of professionals' files
Step 1: in the home MS
German competent authority
2
Uploads the documents in IMI (if sent by email)
Checks and validates the documents available in IMI
3
Creates a professional mobility card
4A
Makes the card available for the professional (email or notification on the public interface)
4B
Notifies the host MS (declaration)
Step 2: in the host MS
Italian competent authority
5
Receives the declaration
Step 3: in the host MS
Austrian competent authority
6
Receives the declaration
7
Sends a declaration to the Austrian competent authority indicating his professional mobility card's number

Figure 10 EPC Procedure (Temporary Mobility)

5. CCBE's possible choices in supporting authentication and authorization technologies

Based on the previous overview of technical means, in this chapter, we would like to further narrow down the choices of CCBE based on its role and the means and measures at its disposal.

CCBE is a representative organisation of EU lawyers through its members, the national bars and law societies of Europe, being a non-profit making association. Therefore, the theoretically possible means at its disposal to support certain technologies are in our view, the following:

a) making proposals to the EU legislature (e.g. European Commission,[67] and LSP participants like that of e-CODEX);

b) influencing the practice of EU lawyers through its member bars and law societies, by issuing recommendations, position papers, declarations or by the Code of Conduct for European lawyers etc.;[68]

c) providing a non-mandatory service for member bars and law societies (e.g. Find-A-Lawyer previous to being taken over by the European Commission);

d) theoretically, it would also be possible to act like a non-mandatory group purchasing organisation for its members (although there had been no precedents for this, and most probably it is not desirous.)

CCBE is clearly not in a position to have an effect on the practice of governments providing e-government services or any independent market players, e.g. device producers, software developers, standardization organizations (other than market players who specialize in the provision of services to lawyers and law firms.)

Our conclusion is that CCBE could support certain authentication technologies in the following ways:

a) by issuing a recommendation to EU lawyers or member bars and law societies through formulating **technical requirements** of authentications (including suggested technologies used for credentials);

b) issuing a recommendation to national bars and law societies regarding the **e-government services** they provide to their members;

c) by coordinated and **focused communications** with the European Commission and other international decision makers where the opinion of CCBE is sought;

d) by **providing a central authentication** or **authorization service** for member bars, law societies or even interested third parties, like national governments or the European Commission;

[67] E.g. "CCBE Position on electronic identification, authentication and signatures", http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/EN_02052011_CCBE_Pos1_1304344346.pdf.

[68] Charter of core principles of the European legal profession and Code of Conduct for European lawyers, http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/EN_Code_of_conductp1_1306748215.pdf, The Declaration of Perugia, http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/perugia_enpdf1_1182334218.pdf, CCBE Guidelines on Legal Outsourcing, http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/EN_Guidelines_on_leg1_1277906265.pdf etc.

e) by **buying** certain technological capabilities for its members or for EU lawyers, using expected greater volumes that can be achieved at EU-wide level.

We explore possible choices a)-c) only in more depth. Both provision of a central authentication or authorization service (e.g. FAL 2.0) and a central buying could be an effective tool in supporting certain technologies, but any aspects to be taken into account while using these means of regulation are already explained in the other three approaches, and practicability of these latter two approaches really depend upon the financial resources bestowed upon CCBE (either by its the members or external parties like the European Commission.)

5.1. CCBE formulating technical requirements

Our starting-point is that to carry out any transactions, including electronic transactions, one has to take into consideration how cooperation of the parties and how security risks are handled. We should take a look at the amount of requirements defined for the cooperation and security of electronic transactions where these security risks are currently of the greatest concern.

Taking into account the number of such electronic transactions and the possible impact of risks, the most risk affected electronic transactions currently are electronic payment and electronic banking services transactions.

Company	Payments Volume (billions)	Total Volume (billions)	Total Transactions (billions)	Cards (millions)
Visa Inc.	$ 3,273	$ 5,191	70.8	1,897
MasterCard	2,047	2,727	34.8	975
American Express	702	713	4.8	91
Discover	107	114	1.8	56
JCB	87	93	0.9	64
Diners Club	26	27	0.2	6

Table 6 The Annual Number of Electronic Payment Transactions[69]

Security regulations in the electronic payment field are very detailed, essentially cover all parts of the transaction from endpoint to endpoint, and amount to thousands of pages.[70] But even with such considerable detail, card fraud and internet banking fraud is an accepted part of our life, e.g. the Annual Report of UK's Payment Council in 2010 showed that the amount of card fraud were £ 440,1 million for all type of fraud, £ 266,4 million for phone, internet and mail fraud.[71]

If we assume that electronic transactions other than the abovementioned electronic payment transactions have similar risks, it seems obvious that security regulations must be no less than that strict and detailed for those transactions. Statistics show that fraud, identity theft and similar criminal offences are also very serious danger to other electronic transactions. E.g. in a US survey, by far the most common form of identity theft was to use a legitimate taxpayer's

[69] Cf. VISA INC. (V) 10-K filed 11/18/2011.

[70] e.g. MasterCard Incorporated, MasterCard Rules 7 December 2011, available on http://www.mastercard.com/us/merchant/pdf/BM-Entire_Manual_public.pdf; MasterCard Incorporated, Maestro Global Rules 11 November 2011, http://www.mastercard.com/us/merchant/pdf/ORME-Entire_Manual.pdf etc.

[71] http://www.paymentscouncil.org.uk/files/payments_council/new_website/annual_fraud_review.pdf, or similar Hungarian data for first half of 2011 http://www.mnb.hu/Root/Dokumentumtar/MNB/Statisztika/mnbhu_statisztikai_idosorok/mnbhu_penzadatok/mnbhu_bkkartyavisszaeles_2011/visszaelesek_a_bankkartya_uzletagban_2011_I_felev.pdf.

identity to fraudulently file a tax return and claim a refund, being more frequent than bank or credit card frauds.[72]

In conclusion, we know that prescribing security requirement is only meaningful if we can take into consideration the whole process of electronic transaction (from endpoint-to-endpoint), and if we regulate only a few critical points generally seen as requirements of a safe transaction, we could miss mitigating very important security risks while at the same time creating some technical barriers.

If there is no technical expertise at a body to achieve a clear overview of the technical issues concerned, then *regulation should not take the form of technical regulations* (either of a prescriptive or recommendatory nature), but resort to softer approaches of regulation.

That is a reason why we do not consider it meaningful for CCBE to formulate certain requirements as to qualified electronic certificates issued to lawyers, e.g. Framework for Establishing a European Electronic ID-Cards System ("**CCBE Framework**").[73] This approach could have been seen as viable in 2007, but currently we think that even if a national bar is able to certify that certain policies of certification fulfil the standards of CCBE, if interoperability of eIDs will be realized, this will be more likely done through the approach recommended by STORK, that is, through the use of either national gateways or through middleware that will be provided by technical service providers. We do not want to insinuate that bars or their affiliate companies could not serve as such technical service providers, only that based on the responses to our questionnaire, this is not an option at the majority of the national bars and law societies.

Let's try to shed some light on the viability of this option from a different approach as well. CCBE's ultimate goal could be to have the lawyers be identified electronically and in a reliable way in the whole of the European Union, because this would both help the work of the lawyers and raise the prestige of the entire profession. This ultimate goal could be reached by specifying certain technical solutions with sufficient detail: there aren't enough such details for technical interoperability in neither Directive 1999/93/EC, nor in CCBE Framework either.

But enough such details would be available when prescribing the use of e.g. PenalNet cards, and a PenalNet card would also be considered as a qualified electronic signature in member states with a reference to an attribute of being lawyer as well. But a PenalNet card can't in itself ensure that this card will be usable for purposes *outside PenalNet*, and possibly outside other member bars, as neither CCBE, nor its members have no authority to do so. *CCBE has no effect on most of the providers of e-government services*, so any such technical solutions recommended by CCBE will be probably limited within our profession.

Therefore, mere regulation of the client security devices is not enough. We have to take into consideration that CCBE could not reach the goal of interoperability even by specifying a middleware like that of STORK. STORK has not solved cross-border cooperation of authentications by merely specifying a common protocol and publishing a toolkit for the middleware: every member state wishing to accept STORK-compliant credentials also have to do some developments. So if we want e-government service providers outside bars and law societies to accept any solution prescribed by CCBE, these service providers would need to

[72] http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf also see Taxpayer Guide to Identity Theft at http://www.irs.gov/newsroom/article/0,,id=251501,00.html

[73] http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/en_guidelines_framew1_1192450932.pdf, and the corresponding technical standards at http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/en_annex_technical_s1_1192451405.pdf

invest some time and money into it. Standardization of electronic transactions is not advanced far enough to make this a viable option at this moment.

So in our opinion, no matter what technical requirements CCBE formulates, it is simply not in a position to ensure usage of its own solution by e-government service providers outside its members.

5.2. Requirements related to e-government services provided by CCBE's members

Based on the responses, 44% of members (8 out of 18 bars) provide services themselves to lawyers where lawyers have to be identified in an electronic way.

Although it is possible for CCBE to influence the identification technologies used here, we do not yet see any reason for doing so, other then the reasons already examined in 5.1. However, this could change if considerable demand is generated by EU lawyers to access the bar of a different country (for establishment purposes and corresponding use of EPC cards etc.)

Currently it would be premature for CCBE to influence technologies used by bars for providing access to their own services.

5.3. Coordinated and focused communications with European regulators

CCBE can communicate its interest to the legislature on European level, both by its responses to the regulation to be replacing Directive 1999/93/EC, and by expressing its opinion during EU-funded projects like e-CODEX.

STORK currently does not regulate such technology, certificate or content, it regulates only the framework for cooperation. Although e-CODEX does not yet contain such technical requirements, it will do so once completed. Therefore the final technology can still change. In e-CODEX processes, lawyers have outstanding roles, the whole project is currently under planning and resources are budgeted for changing and developing requirements communicated during the consultations with CCBE, therefore recommendations are probably more welcome than in existing e-government services.

Furthermore, as e-CODEX is one of the first cross-border e-government services of its kind, the outcome of this project can also serve as a basis for (a) cross-border implementation of new electronic procedures or (b) a basis for access to EU-wide databases where the capacity of a lawyer as such will be more strictly verified in the future (e.g. European Network of Registers of Wills Association[74]).

What aspects should CCBE take into account when providing opinions to European regulators and EU-funded projects? When expressing its opinion, we think CCBE should take the following generic elements into account:

(i) suggested solutions should be **secure** enough to minimise risk of frauds with lawyer's identity, taking into account the possible impacts of any identity theft;

(ii) authentication and identification should remain at appropriate **cost** for EU lawyers (which includes that lawyers should not be obliged to purchase a new device because this enables the faster implementation of the e-CODEX project);

(iii) techniques used should already be **familiar** to EU lawyers;

[74] http://www.europa-nu.nl/id/vi7jgt803jzl/list_of_existing_projects_in_the_field, http://www.ccbe.org/fileadmin/user_upload/NTCdocument/Study_EJustice_2_De1_1246866101.pdf

(iv) extra care should be taken to make it possible for lawyers to **use existing credentials** where possible;

(v) should introduction of a new credential be necessary, it would be desirous to use a solution that lawyers will be able to use for other purposes as well, and to use a future proof solution (e.g. not to support requirements excluding the use of mobile secure elements as credentials.)

6. Analysis of the responses from the questionnaire

The on-line questionnaire submitted to bars and law societies of CCBE is copied in Annex 1. We have inserted all the answers for the survey in Annex 2, in one table for quick comparison and overview and in multiple tables and charts for visual comparison. We also provide CCBE with the complete database of the answers in a text file (comma-separated value, CSV) format for any further use.

In order to increase legibility, in this chapter, we only give a wider overview of the answers, and we *do not copy all the charts and tables to this chapter* of the analysis. This also means that a considerable part of the analysis is included in Annex 2 only. We refer to questions based on their numbers in the survey and in Annex 1, the abbreviation Q3 shall mean question 3 etc. There were 19 questions, but Q1 and Q2 was about the name (identity) and the bar of the person giving a response, Q19 was only for quality management purposes and for providing any further comments. We have received eighteen responses, but two of the responders represented Germany, so wherever we were looking at differences in MSs, we have counted those two answers as one answer.

6.1. Current practice in MSs for checking lawyers identity in electronic ways

The purposes of Q3 and Q6 was to get to know better the general experience of lawyers in a given MS with regard to e-government services and when being identified in a MS as a lawyer. Q3 was a generic question to see how widespread is the checking of lawyers identity in each MS is, Q6 was about the actual method it is carried out, and is not necessarily restricted to checking of lawyer ID in electronic ways.

Of 17 MSs, in six MS there is *no electronic procedure* in place where the lawyer's identity is checked in an electronic way (35%). The majority (53%) of respondents have public key certificates in place containing an attribute with reference to the certificate subject being a lawyer. This data is not completely in line with the responses received from MSs earlier in 2011, in relation to an e-CODEX questionnaire (see Table 7 below), where out of 33 respondents, only 7 affirmed that there are such PKCs.

COUNTRY	HAVE THE LAWYERS IN THIS COUNTRY DIGITAL CERTIFICATES WHICH SHOW THEIR CONDITION AS LAWYERS?	IF YES, WHO IS ISSUING SUCH DIGITAL CERTIFICATES?
Austria	Yes	Local bars
Belgium (Wallonia and Brussels)	No	---------------------------------
Belgium (Flanders)		
Bulgaria		
Cyprus	No	---------------------------------
Czech Republic	Yes	Czech Bar Association
Denmark	No	---------------------------------
Estonia	No	---------------------------------
Finland	No	---------------------------------
France	Yes	French Bar Association
Germany		
Greece		
Hungary	Yes	Certification service providers after the Bar certifies lawyer's condition
Iceland	No	---------------------------------
Ireland	No	---------------------------------
Italy	Yes	Companies licensed in cooperation with National and local bars
Latvia		
Liechtenstein	No	---------------------------------
Lithuania		
Luxembourg	No	---------------------------------
Malta	No	---------------------------------
Norway		
Poland	No	---------------------------------
Portugal		
Romania		
Slovak Republic	No	---------------------------------
Slovenia	No	---------------------------------
Spain	Yes	Local bars
Sweden	No	---------------------------------
Switzerland	Yes	Issued by a company licensed by the Swiss Bar Association
The Netherlands		
United Kingdom	No	---------------------------------
UK (Scotland)	No, but working on that	The Law Society of Scotland

Table 7 Response to e-CODEX Questionnaire

Answers to this question also confirm the viability of an EU-wide online capability to check the license of lawyers, but this question was dealt with at more depth regarding Q9 (feasibility of providing CCBE with an up to date validity information), although this will clearly not work with all members of CCBE.

6.2. Does your Government already provide e-Identity for citizens, or will it provide this in the future? (Q4)

The purpose of this question was to evaluate general MS experiences in e-government services related to identification, and if necessary to verify from a lawyers point of view information already contained in e-CODEX and STORK surveys.

Three respondents answered that there is no e-government identity in their MSs at all (and neither be introduced in the close future, like in Latvia), but based on information in e-CODEX D4.1 and of different other sources, 3 of the respondents seem to have either misunderstood the question, or despite presence of eIDs in these countries, these eIDs are neither used frequently, nor well-known. It is also worth noting that based on 10 responses, there are smartcard based eIDs.

6.3. Any well-used e-Government services in your country that already provide a reliable web service or other database interface for automatic querying frequently used business information, and which is free for the public? (Q5)

Our purpose with this question was to get to know the general MS experiences in relation to *authorizations* used in e-government services, and whether there are already any national solutions in place that could serve as a viable basis for automatically checking certain attributes in an electronic way (by an authentic registers providing automated responses or attribute certificates etc.). We have to admit that this question was rather hard to understand, and numerous answers were given that were not able to support the abovementioned purpose, but this was a necessary consequence of *authorizations* not being present as a different concept in public administration.

According to the vast majority of responses, there were no such systems in place yet (of course, there were numerous company registers etc., but as long as you can't query those in an automatic way, they will not be of much help to possible future uses of authorizations.) Notable difference is Latvia, Poland, Portugal (Citius) and perhaps Spain (legal Aid).

In Latvia, there is a public web service for registers of authorizations (powers of attorneys) and for invalid documents, both of which could serve as a very strong basis for automatic query of authorizations. Lack of a central register for powers of attorneys is one of the major issues in e-CODEX, so experiences of Latvia in this regard could be invaluable. It is also important that in electronic orders for payment proceedings in Poland, a lawyer’s proxy (power of attorney) is checked in an electronic way.

The Spanish example of Legal Aid could be useful as an example of wide-ranging and automatic cooperation of different, standalone public registries when deciding whether to provide legal aid to a citizen or not.

6.4. Lawyer's technical capabilities and what technologies are lawyers familiar with (Q7, Q8 and Q14-Q16)

Q7 and Q8 was related to current technological capabilities of lawyers, one regarding the use of eIDs as lawyers, the other regarding use of eIDs as normal citizens in their everyday life.

In Q7, one respondent could designate more than one technology (so in Figure 13, % means what % of all the 18 respondents answered that they use this technology as a lawyer.) The majority of respondents indicated that they do use electronic signatures when working as a lawyer (50%).

The second largest number of responses was to the "other category", which both shows that categorization was not clear cut enough. Of the "Other" answers, it is worth mentioning that software certificates had no separate box, and therefore two respondents had to include their answer in the "Other" category. (The reply of the Czech Republic regarding data boxes should in our opinion be considered based on the actual method of authentication when the lawyer requests access to the "data box", e.g. by a password issued to the lawyer.)

It is important to note that the majority of respondents (83% of all respondents) have indicated that they are using some kind of hardware token (smartcards, OTP tokens etc.) when identifying themselves as lawyers, and it seems that only a small minority of respondents use either single factor authentication or with the basic means of identifying themselves using their normal email addresses (4 such responses in total.)

In Q8, lawyers were asked to rank the technologies that they use in their everyday life (not necessarily as lawyers), and all rankings gave certain scores to the given technologies (weighted according to their rank), and the sum of the scores decides the overall ranking of the technologies. Based on the answers, smart cards used for electronic signatures are the relative winners, but if we take smart cards together in one category (and do not differentiate between smartcards for authentication and for signature purposes), its ranking is even stronger.

Lawyers are also much used to using smart phones and tablet devices in their everyday life, but maybe the ranking is a little bit misleading, as it is not very probable that these devices are used in identification procedures yet (they are used for communications and work purposes, but most probably not as credentials.)

Q14-Q16 were used as a support for our technological trend analysis, and to check whether any technological suggestions related to future credentials are in line with current expectations of lawyers or not, and to see whether lawyers are ready to accept generic trends in computing.

Regarding the future use, smartcards are in the lead again: 13/18 responders consider it *at least* likely that in 3 years' time, lawyers will be using this technology for e-procedures, and the majority (7) of these 13 answers supporting smartcards already confirm that lawyers are using it even now.

It seems that 8 of 18 respondents expect tablets and mobile phones with secure elements to be used for access to online services, and there is greater uncertainty in this regard than with smartcards.

6.5. Could the Bar provide CCBE with up-to-date lawyer’s licence? (Q9)

With this question, we wanted to check the viability of CCBE authorization of lawyers being served by Bars and Law Societies of CCBE (also the rolling out of FAL and the creation of FAL 2.0). With the exception of Italy, all other responses (94%) were positive. The reason for Italy's inability to do so lies in the fact that they have no central database yet other then for the purposes of the national electronic civil proceedings system. (Based on this information, it seems that this is only a matter of development and national data protection issues than of some underlying strict policies.)

6.6. Does the Bar maintain a system where lawyers are identified by electronic means and what are the per lawyer costs in € of these systems? (Q10-Q13)

Of the 18 responses, only 8 bars (44%) maintain a system themselves where lawyer's identity is checked.

There is considerable deviation in the per lawyers costs of the systems, from 1 € to 60 € per lawyer set up fees, from effectively zero maintenance costs (per lawyer) to 100 € / per lawyer per year, and some of these annual costs are charged on lawyers. It is very hard to draw any meaningful conclusions from this data other than this would justify further, very detailed analysis of the systems provided by bars to their members. (It was CCBE's request to ask Q11-Q13.)

6.7. Advantages and disadvantages of current national electronic lawyer e-ID systems

We could not come to any conclusions that affect this report based on the answers to Q17-Q18 (which answers were asked by CCBE to be included in the questionnaire), other than multiple bars indicating their eagerness in helping other MSs in providing identification or authorization services.

6.8. Conclusions – Proposed Approach for CCBE

Based on conclusions of Sections 4.2.5-4.2.7, 4.3, and 5, and based on the analysis of the responses, we think that *currently*, CCBE should first and foremost support the use of *smartcards in identifying lawyers*, but also take into account that all requirements laid down in legislative acts and all conclusions in LSP e-CODEX should be *phrased in such a way that in the near future, lawyers should also be able to use the security elements in their mobile devices* and not only smartcards usable with special readers on a desktop or notebook computer.

Based on the expected technological trends, it is also an important conclusion that supporting the use of *electronic signature* and mainly digital signature (QES or AES) might not be a good answer in all the electronic procedures, and CCBE should always take efforts to ensure that other hardware token based authentication technologies without signature capabilities are not to be excluded at the regulatory level without clear and very good reasons.

At a different level of this same problem, we also recommend not to support any widening of requirements for using secure signature creation devices (SSCD) for the creation of signatures. This could not only create significant and unjustified costs for lawyers, but also contribute to the "*PIN, password and hardware token fatigue*" that we can expect to be a major headache for lawyers in the coming years. It is possible that SSCDs will remain in a special niche for special uses, and not be available for the wider audience: so as long as lawyers will have to use one, this will cause extra costs for them, and could require maintaining a separate desktop computing environment etc.

Annex 1: CCBE Questionnaire on Lawyer E-Identity

[A copy of the questionnaire]

Description of the Questionnaire

The CCBE is currently participating in a large-scale European project called e-CODEX, the aim of which is to provide access to justice systems across Europe.

Participation in this project has prompted the CCBE to think more widely about the future needs of EU lawyers to identify themselves electronically across borders in other member States and, more specifically, what kind of technological and contextual approach would be best suited to the bars and law societies.

In order to obtain a well-founded overview of the technical background of how lawyers identify themselves as such in each Member States, we would like to ask for your participation in this e-questionnaire.

The total number of questions is 19. For each set of questions, after you have reviewed your answers to assure accuracy, click on "NEXT" at the bottom of the web page to proceed to the next set of questions. If you have completed everything on that page correctly, you will proceed to the next page.

If you have filled in a block incorrectly or if you have failed to fill in a required block, red text will highlight the problem and provide guidance on how to correct the error. After correcting the problem, click on "NEXT" again to move to the next page. After completing the last question, click on "SUBMIT" to send your completed questionnaire to us.

Important notice: please take into consideration that, depending on the browser you use, answering these questions over more than two hours might cause some technical problems, and so – if this is likely to apply to you - you should be careful to avoid this.

General Questions

1) Please provide us with the name of the Bar or Law Society on behalf of whom you fill out this survey.

____

2) Please provide us with your name and your email address.

____

Questions relating to developments in your Member State

3) Could you please name the most important judicial procedures in your country where the lawyer's identity and his or her capacity to act as a lawyer is checked in an electronic way?

Please name no more than five procedures. If there is a public online link to the procedure or to the service, please provide us with the link as well.

4) Does your Government already provide e-Identity for citizens, or will it provide this in the future? If so, what kind of technology is being/will be used?

5) Are there any well-used e-Government services in your country that already provide a reliable web service or other database interface for automatic querying frequently used business information, and which is free for the public? We would like to identify possible national approaches and precedents (history) to role verifications. E.g. is there already a

public database on authorizations (delegations) to act on behalf of someone else? Or is there any well-used e-Government search engine where you can centrally search for different kinds of licenses, e.g. a central search engine for different kinds of licensed professional service providers (not only lawyers, but also auditor, accountants etc.)? If yes, please describe the type of information provided.

6) If you know, please describe how the validity of the lawyer's capacity to act ("licence") is checked in an electronic way in a judicial procedure in your Member State. What is the role of your Bar / Law Society in providing the information on the validity of the lawyer's licence?

E.g. your Bar supplies the validity information to the service provider of the electronic procedure every week, or provides a 7x24 web service for answering questions on the validity in almost real time. Or your Bar itself issues the e-signature certificate of the lawyer for that procedure, and your Bar withdraws the certificate if the lawyer no longer practices.

7) Please indicate which kind of electronic technologies are effectively used in your country when lawyers identify themselves as such in judicial procedures.

[ ] Electronic signature by using smartcards or other hardware token (qualified or advanced)
[ ] Identification using smartphone or tablet device specific applications
[ ] Electronic ID (authentication) by using any hardware token other than smartcards, smartphones or tablet devices
[ ] Other multi-factor authentication without smartcard (username and password or PIN code etc. together with one-time password or hardware token etc.)
[ ] Simple user name and password or PIN-code (without any hardware token, i.e. single factor authentication)
[ ] Email without any secure identification of the lawyer (normal email address and/or signature)
[ ] Other:
[ ] None

8) Please order the following items according to how much these kinds of techniques are used by lawyers in their everyday life in your country, how they are accustomed currently to their use.

Your answer to this question is important for us in order to better estimate the possible future scenario faced by CCBE in three years time (where things are now and where should we expect them later to be.)

_______Smart cards used for electronic signature
_______Smart cards for electronic authentication (for accessing online services)
_______Smart phones or tablet devices
_______Hardware based tokens (security devices)providing one-time password
_______Mobile phone providing one-time password
_______Other hardware based tokens enabling multi-factor authentication, not listed above

---

Questions relating to developments within your Bar / Law Society

9) Based on your current technical capabilities, would it be feasible that your Bar / Law Society provides the CCBE with up to date validity information in an electronic way regarding the licence of a lawyer registered with your Bar/Law Society?

E.g. do you and/or the local bars have a complete and reliable database on all lawyers in your Member State in an electronic form? Are all local bars capable of providing such access now or in the near future?

10) Does your Bar or Law Society itself maintain a system where lawyers are identified by electronic means (as opposed to it being run, for instance, by the government or some other authority)?

[ ] Yes (please answer questions 11-13 as well)
[ ] No (please proceed to question 14)

11) What was the estimated cost per lawyer (in euros) of setting up this system?

Please fill this out only if answer to the previous question was yes.

____

12) What is the estimated annual cost per lawyer (in euros) of running this system?

Please fill this out only if answer to question 10 was yes.

____

13) Is there a fee (per year, month, etc.) that the lawyer has to pay for using such system?

Please fill this out only if answer to question 10 was yes.

____

Questions relating to future developments

14) How likely do you think that in 3 years' time, lawyers in your country will be able to use smart cards in electronic procedures? (Either for signature or for identification only.)

By "being able to use", we mean that most lawyers will not generally see such technical requirements as inequitable, unfair or unreasonable for accessing the electronic service.

( ) Already using
( ) Very likely
( ) Likely
( ) Not likely, unsure
( ) Not applicable, don't know

15) How likely do you think that in 3 years' time, lawyers in your country will be able to use an electronic procedure where a smartphone or a tablet device is required for access to the online services?

( ) Already using
( ) Very likely
( ) Likely
( ) Not likely, unsure
( ) Not applicable, don't know

16) Can you think of any other specific hardware based tokens in your country that lawyers will be familiar with in 3 years' time and that enables multi-factor authentication? If yes, please specify.

Conclusions

17) What are the advantages of your current national electronic lawyer e-ID system (if you have such a system)?

18) What are the disadvantages of your current national electronic lawyer e-ID system (if you have such a system)?

19) If you have any further comments related to the above questions or to the technical background on the cross-border identification of lawyers, please share this information with us. (Optional.)

Annex 2: Responses to the questionnaire summarized in tables and charts

Presence of government provided e-Id for citizens (Q4)	Count	Percentage %
Yes	14	82%
No	3	18%

Taking into account the imminent rollout of eIDs in Latvia, we have counted their answer as yes.

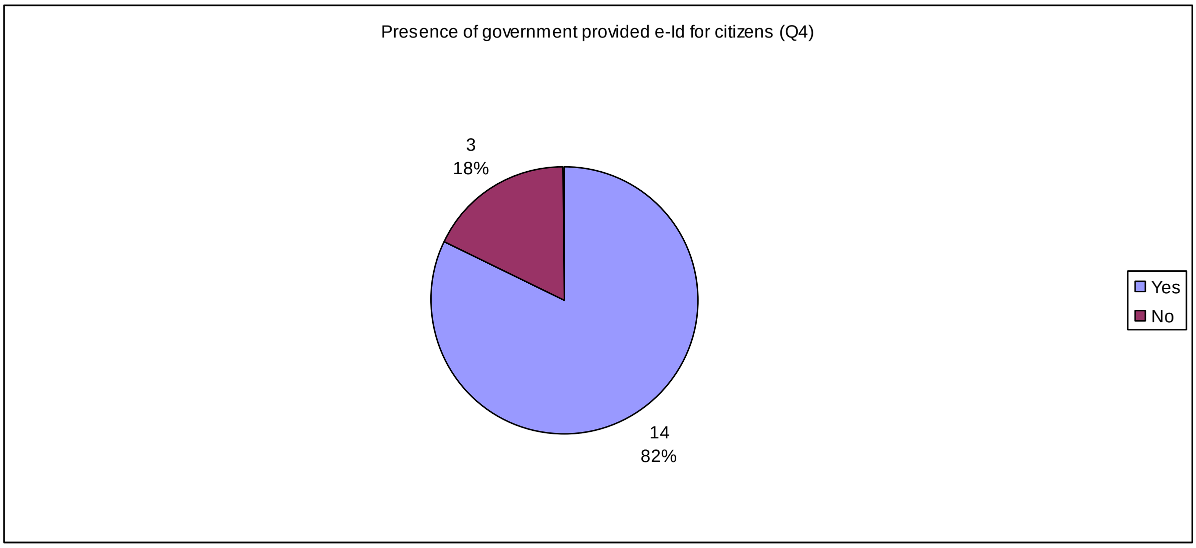


Figure 11 Chart of Responses to Q4

How the validity of the lawyer's licence is checked? (Q6)	Count	Percentage %
The public key certificate of the lawyer (used for identifying it) contains this information.	9	53%
Can be checked from the Bar's website only.	3	18%
Other automatic way by the courts	2	12%
Only offline solutions or solutions that are not complete	3	18%

Table 8 Table of Responses to Q6

Answers from the two bars/law societies from Germany counted as one.

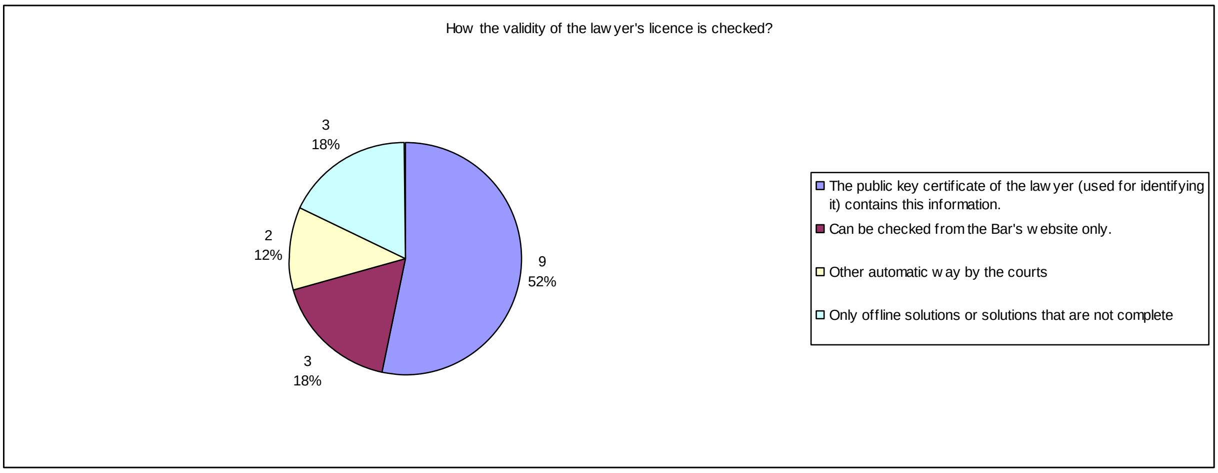


Figure 12 Chart of Responses to Q6

Technologies used for identifying lawyers in a MS (Q7)	Count	% share of all responses

Electronic signature by using smartcards or other hardware token (qualified or advanced)	9	50%
Identification using smartphone or tablet device specific applications	1	5.6%
Electronic ID (authentication) by using any hardware token other than smartcards, smartphones or tablet devices	2	11.1%
Other multi-factor authentication without smartcard (username and password or PIN code etc. together with one-time password or hardware token etc.)	3	16.7%
Simple user name and password or PIN-code (without any hardware token, i.e. single factor authentication)	2	11.1%
Email without any secure identification of the lawyer (normal email address and/or signature)	2	11.1%
Other	7	38.9%
None	4	22.2%

Table 9 Table of Responses for Q7

List of "other" responses for Q7:
(See answer on question No. 6 above)
Data boxes
ERV: software certificates
See question 6
We issue the CCBE ID card but am not aware of it being used for national judicial procedures
The procedure before the e-court requires username, general password and a special digital certificate, which is individual, protected by a separate password and could be downloaded from the court’s website after creating an account of a lawyer and after verifying his or her identity
For question 8, none of the items listed are used. Since one alternative answer must be given, this is done event though it is not correct.

Table 10 List of "other" Responses to Q7

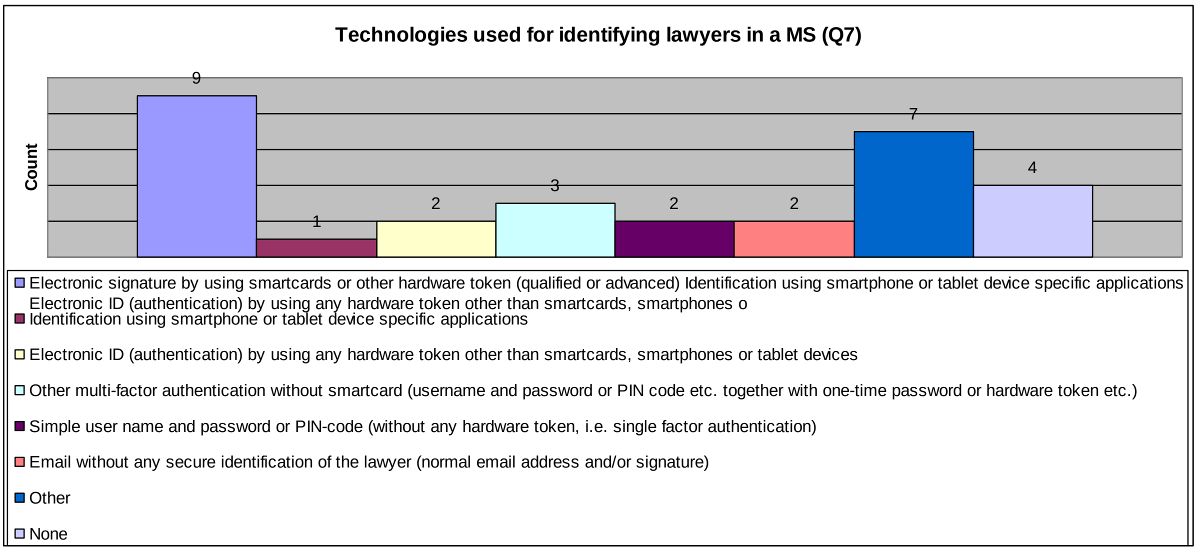


Figure 13 Chart on responses to Q7

Rank of technologies used in everyday life by lawyers (Q8)	Total score	Rank
Smart cards used for electronic signature	64	1
Smart cards for electronic authentication (for accessing online services)	48	2
Smart phones or tablet devices	48	2
Hardware based tokens (security devices) providing one-time password	36	3
Mobile phone providing one-time password	36	3
Other hardware based tokens enabling multi-factor authentication, not listed above	36	3

Table 11 Table of Responses to Q8

Feasibility of Bar / Law Society providing the CCBE with up to date validity information in an electronic way regarding the licence of a lawyer? (Q9)	Count	Percentage %
Yes	16	94%
No	1	6%

Table 12 Table of Responses to Q9

Answers from the two bars/law societies from Germany counted as one. Answers where "this solution will be provided from 2012 only" were counted as yes. Answers from Spanish delegate was counted as yes.

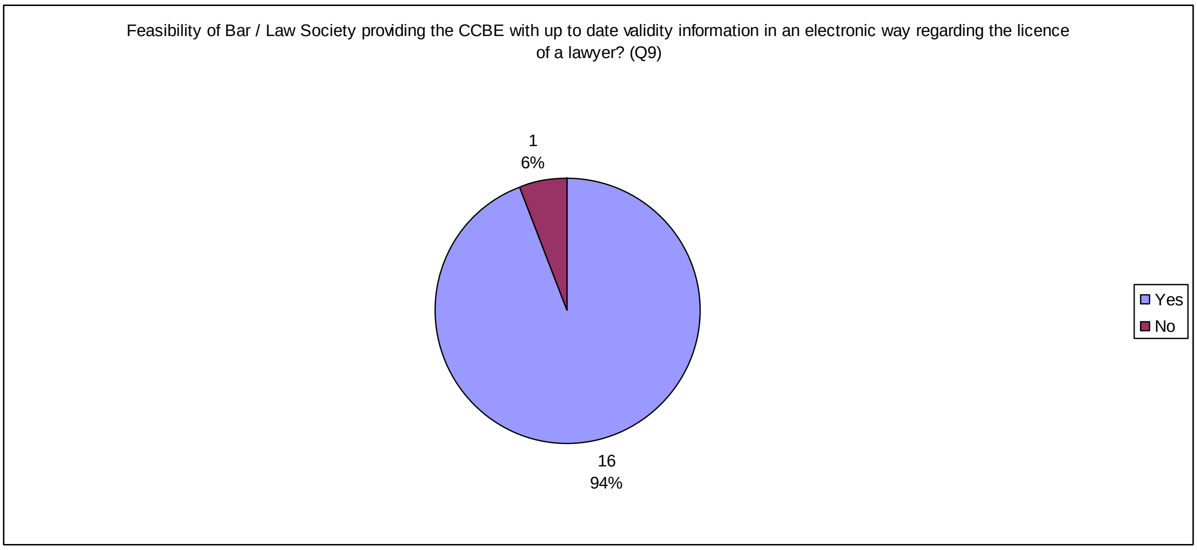


Figure 14 Chart of Responses to Q9

Bar or Law Society maintaining a system where lawyers are identified by electronic means (Q10)	Count	Percentage %
Yes	8	44.4%
No	10	55.6%

Table 13 Table of Responses to Q10

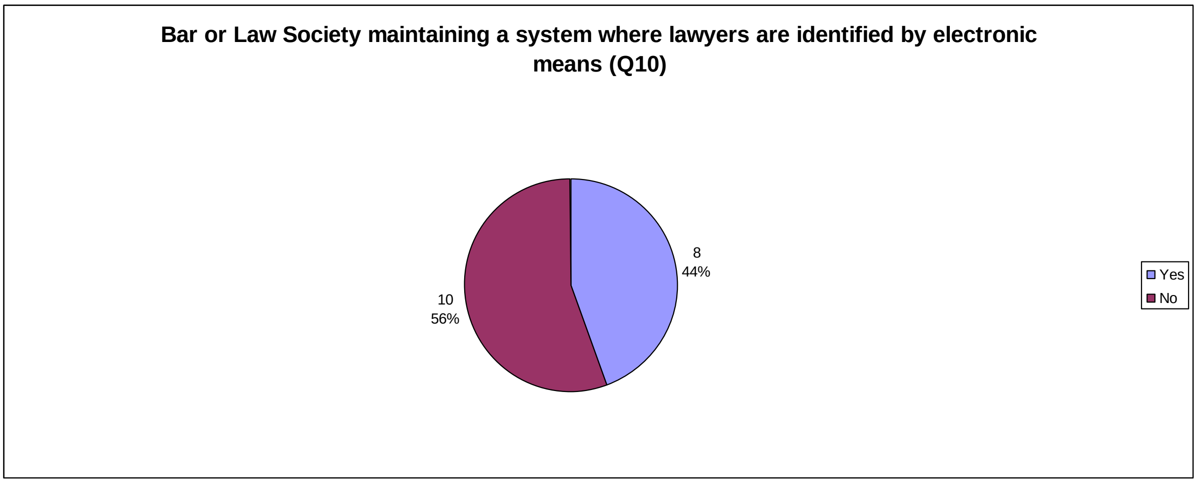


Figure 15 Chart of Responses to Q10

Likelihood of lawyers in your country using smart cards in electronic procedures in 3 years (Q14)	Count	Percentage %
Already using	7	38.9%
Very likely	3	16.7%
Likely	3	16.7%
Not likely, unsure	3	16.7%
Not applicable, don't know	2	11.1%

Table 14 Table of Responses to Q14

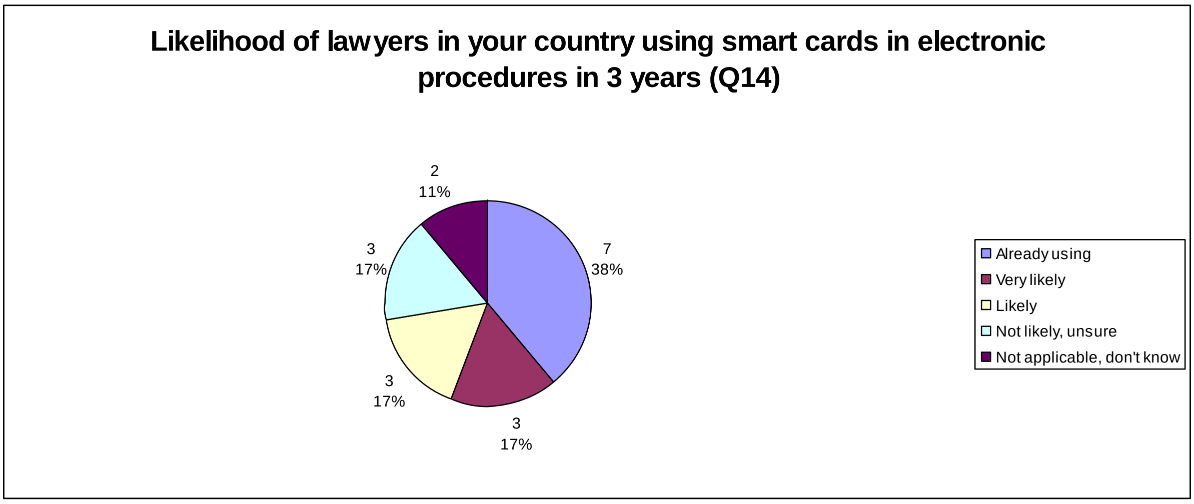


Figure 16 Chart of Responses to Q14

Likelihood of lawyers in your country using tablets or smartphones in electronic procedures in 3 years (Q15)	Count	Percentage %
Already using	1	5.6%
Very likely	4	22.2%
Likely	3	16.7%
Not likely, unsure	6	33.3%
Not applicable, don't know	4	22.2%

Table 15 Table of Responses to Q15

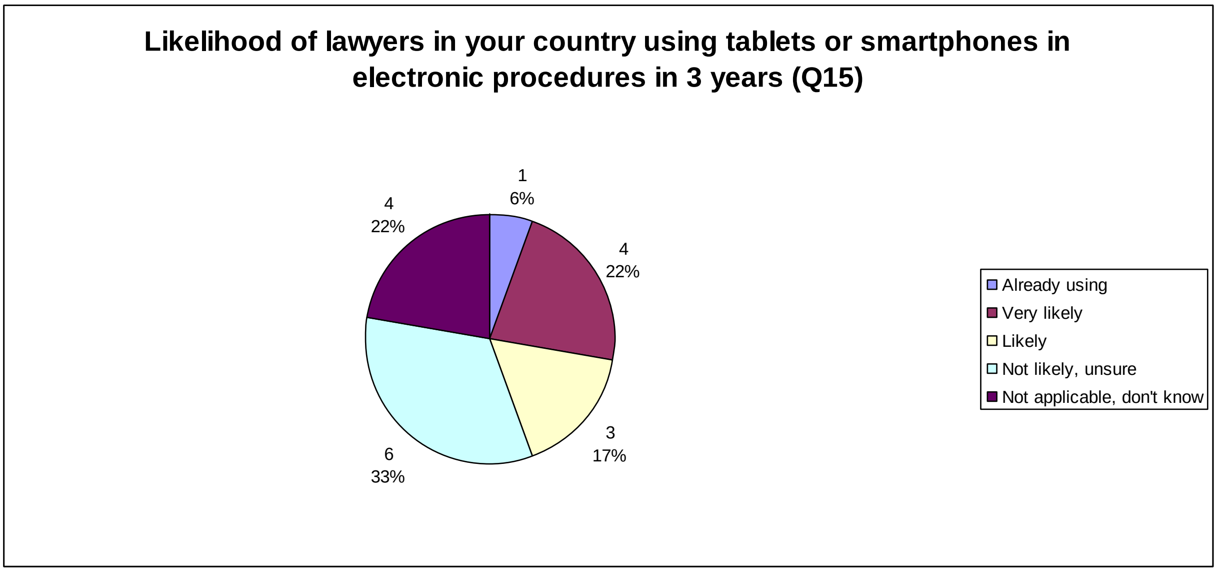


Figure 17 Chart of Responses to Q15

Any other hardware based tokens in your country that lawyers will be familiar with in 3 years' time (Q16)	Count
OTP tokens	1
A smartcard combined with a OTP-token	1
Security of mobile devices	1

Table 16 Table of Responses to Q16

Presence of government provided e-ID for citizens	Count	Percentage %
Yes	15	53%
No	2	18%

Answers from the two bars/law societies from Germany counted as one. Answers like "this solution will be provided from 2012 only" were counted as yes.