Regulating a European eID

A preliminary study on a regulatory framework for entity authentication and a pan European Electronic ID

for the Porvoo e-ID Group

31 January 2005

Thomas Myhr
thomas.myhr@nhd.dep.no

1 Short summary

This document shall be used as a starting point for a discussion within the Provoo Group on what necessary steps should be taken in order to pave way for a legal framework for a pan European eID. The document is not supposed to bring all the answers but is trying to shed some light on some crucial/important questions and present some possible alternatives.

The Directive on Electronic Signatures covers also entity authentication. However, entity authentication leads to special regulatory needs that are not met in the Directive on Electronic Signatures or in any other EEA relevant legal document.

A legal framework for a pan European electronic ID has to be drafted with the realization of the limitations given by the EC Treaty Article 18.

Given these facts the report makes the following suggestions and conclusions:

- Use and interpret the existing regulation in the Directive on Electronic Signatures as far as possible as a building block for the establishment of a legal framework for a pan European electronic ID.

- Take in use existing standards and promote the development of new standards for entity authentication to support the use of a pan European electronic ID.

- One should maybe accept pan European electronic IDs on different security levels. It might be easier to find a consensus among Member States on a lower level.

- Further evaluate the possibility to use existing national and European regulation for passports as another building block for the legal framework for a pan European electronic ID.

2 Introduction

2.1 Background and the request/questions by the Porvoo eID Group

The Porvoo eID Group is an informal international cooperative network with the goal to promote and realise the potential of trans-national interoperable electronic identities using PKI and smart cards in order to help ensure public and private sector electronic transactions in Europe.[1] The Group has highlighted the need for minimum requirements to be established so that eIDs can be used across national borders. The Group has adopted the following resolution:

"The Provoo e-ID Group is convinced that electronic identity is of major importance for the deployment of secure e-government, e-administration and e-commerce services and that interoperable e-ID systems can help bringing Europe together. The Porvoo e-ID Group recognizes that minimum requirements have to be established to ensure that electronic identity can be used across borders."[2]

The Porvoo-Group decided in the beginning of 2004 to continue that work and evaluate the legal needs, implications and limits when drafting a legal framework for entity authentication. Inter alia the following questions were defined[3]:

- Is there a need for a European eID?
- What legal amendments, to existing regulatory framework, are necessary for a European eID?
- Why do we not have a Directive on Authentication, when we have a Directive on Electronic Signature?[4]
- Why are there not any standards on European eID?

[1] More information about the Porvoo Group cf. http://www.electronic-identity.org/

[2] "Electronic Identity White Paper", v. 1.0, June 2003, page 4

[3] Personal received e-mail from Ulla Westermarck 26 March 2004.

[4] In connection to this one should also note that in E-AUTH N0029 (2004-02-17) page 30 Chapter 4 "Recommendations" (Recommendation no. 2) the following is stated:

"A legal system for cross border acceptance of e-Authentication/eID should be installed in the European domain.

For the usage of the Digital signature there is a European directive which establishes the legal acceptance and validity of such a signature between parties concerned. A similar solution is needed for eAuthentication, i.e. for the legal acceptance of the on-line verified personal identity. The Member States should support such an action and the EU should take the lead."

2.2 Limitations etc.

This report is focusing on issues related to obtaining a legal framework for entity authentication that can be used for the deployment a pan European eID. This means that other issue matters that may very well be of equal importance, such as economical and organisational needs, have been set aside in this report. The report is also drafted under the assumption that there is a need for a pan European eID.

The main focus of the report is to look at a regulatory framework for an eID for private persons, not legal persons. The reasons behind this limitation is the need to reduce the report's scope, but is also due to the fact that authentication of a legal entity asserting its privileges and rights are in many legal orders based on the notion that a natural person is granted a right to represent the legal entity and not that the company in its own capacity can be authenticated and asserted such rights and privileges. Even though the report uses the definition "entity authentication" that also covers authentication of a legal person, this definition is aiming at the authentication of a natural person unless the opposite is explicitly stated.

The technological methods and specifications used for authentication are often based on cryptographic techniques. The prevailing technique at the present technology situation is the use of public key infrastructure (PKI) and to some extent smart cards. Notwithstanding these facts, the report is drafted with the aim to be, at as far as possible, neutral in respect of choice of technology and also in respect of business models. This report is subsequently limited to issues specifically related to the fact that the ID is in electronic form. If an electronic ID is made part of a visual ID additional legal issues may emerge. However, with the need to limit the scope of the report these additional issues are not further addressed.

This document shall be used as a starting point for a discussion within the Provoo Group on what necessary steps should be taken in order to pave way for a legal framework for a pan European eID. The document is not supposed to bring all the answers but is trying to shed some light on some crucial/important questions and present some possible alternatives.

Opinions and conclusions presented in this report are my own and do not necessary coincide with my employer's views.

3 Abbreviations etc.

Entity authentication	Entity authentication refers to a process determining – with a degree of confidence - whether someone or something is, in fact, who or what it is declared to be. Even though this assertion does not necessarily have to relate to someones identity, the term will in this report be connect to the determining of a natural persons identity.[5]
Certification Service Provider (CSP)	An entity or a legal or natural person who issues certificates or provides other services related to electronic signatures, cf. the Directive on Electronic Signatures Article 2 no. 11
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CWA	Common Workshop Agreement
EEA	European Economic Area
eID	Electronic Identity; which in a PKI-environment is manifested by an electronic certificate
ETSI	European Telecommunication Standards Institute
Issuer	Cf. Certification Service Provider
PKI	Public Key Infrastructure – Data transmission infrastructure that considers inter alia authentication, integrity, non-repudiation and confidentiality aspects.
SSCD	Secure Signature Creation Device, cf. Directive on Electronic Signatures Annex III.
TS	Technical Standard

[5] This report distinguishes between entity authentication and data authentication. However, when it is clear from the context only the term authentication may be used when referring to entity authentication.

4 Electronic Identity

4.1 Authentication

Human identity is a delicate notion that requires consideration at the levels of philosophy and psychology. Human identification, on the other hand, is a practical matter. In a variety of contexts, each of us needs to identify other individuals, in order to conduct a conversation or transact business. Organisations also seek to identify the individuals with whom they deal, variously to provide better service to them, and to protect their own interests.[6]

In the context of information systems, the purpose of identification is more concrete: it is used to link a stream of data with a person. The purposes of the interchange of identification include to develop mutual confidence, and to reduce the scope for dishonesty and to enable a person or a system to associate transactions and information with the other person.

In a historic perspective up until not very long ago a person had no need for an identity card. He was operating and communicating within an environment where he was known on a person-to-person level. The persons to whom he needed to identify himself knew him personally, e.g. the local bank. The identification was made by personal appearance and the bank clerk's recognition of him. The introduction and the need of a visual ID on a more general scale came slowly, and where legal processes that normally are quite slow could keep up with the pace on the development of the need and use of visual IDs and thus provide a functional legal framework.

With the use of Internet new challenges and new needs have arisen very rapidly. Even though existing laws that regulates a paper-based environment and visual IDs to a large extent also can be applied to electronic communication and the use of eIDs, this rapid development has lead to the fact that necessary or appropriate regulating within this new fields is lacking. This applies not only on a national level but also on a European level for inter alia cross-border communication.

4.2 Signature vs. Authentication

There is a difference between the legal concept of signature and the concept of identification. These differences are also pertinent for electronic communication.

A formal requirement of a signature is normally a clear legal concept under national law and is met by writing your name on a (legal) document. On the other hand identification/authentication is a process. When the requirements of that process are fulfilled,

[6] More about human identity etc. cf; "Towards Understanding Identity – An examination of the fundamentals underlying the definitions and understanding of identity based on the assumption and experience known form the real-world in order to map them on to the requirements emerging form the digital world", produced by an EEMA Identity Technologies and Services Working Group, authors Bowden, Bramhall, Cameron, Cassassa-Mont, Colvill, Goodman, Hilton, Marhøfer, White, daft v0.35, 24 March 2004

it asserts privileges or rights (a legal position) of the person being authenticated. Authentication is a more complex concept compared to a signature. The requirements of authentication is usually linked to the area of law in which one is “navigating”. The need to identify someone differs and has different aims, when it is done by the immigration control, by the highway patrol, by the bartender, by the bank clerk etc. You may also have different means of fulfilling the authentication requirements, compared to a signature that is identical disregarding the value of or seriousness of the document. The signature is the same disregarding whether it is used to sign a will or a hotel register.[7] However, the consequences of the signature may vary. The differences between a signature and entity authentication and their legal implications are further discussed in this report.

[7] There is a Supreme Court decision from Denmark (U.1959.40/1H) where the court denied a signature legal effectiveness due to the fact that it was written with the use of a ballpoint pen, and not a fountain pen. The decision was based on the fact that that the ink in the ballpoint pen was not as good/permanent as required for long time storage. This might seem to be a little comic, but actually you make the same evaluation with an electronic signature. Is it stable enough, can it be altered/have it been altered, or can I trust the signature and give it the legal effectiveness as a valid signature? Cf. Bryde Andersen, M., Bilag B: Retlige problemstillinger, "Digitale dokumenters bevisværdi", IT-Sikkerhetsrådet, København, December, 1998, s. 51.

5 Does the Directive on Electronic Signatures cover entity authentication?

5.1 The Directive on electronic signatures

The main aim of the Directive on Electronic Signatures is to create a Community framework for the use of electronic signatures, allowing for the free cross-border flow of products and services provisions, together with a basic legal recognition of electronic signatures throughout the EU. The object was not to harmonize the requirements for the legal validity of a electronic signature, but instead to establish in every EEA-state an equivalence between the legal status of handwritten signatures in the paper-based environment and the legal status of electronic signatures in the electronic environment.

The relevant question here is whether the regulatory framework in the Directive on Electronic Signatures also covers entity authentication made in an electronic environment and thus can be used as a cornerstone in order to establish a legal framework for a pan European eID.

5.1.1 Article 5.1 – legal effects of a qualified electronic signature

Article 5 of the Directive, regulates the "Legal effects of electronic signatures" and paragraph 1 of this article states the following:

"Member States shall ensure that advanced electronic signatures[8] which are based on a qualified certificate[9] and which are created by a secure-signature-creation device[10]:

(a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and

(b) are admissible as evidence in legal proceedings"

This Article gives – under certain conditions – an electronic signature on a specific level (hereinafter called a "qualified electronic signature") the same legal effectiveness as a handwritten signature.[11] The signature shall also be given legal

---

[8] Pursuant to the Directive on Electronic Signatures (Article 3.2) an advanced electronic signature is defined as "an electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable." As of today only a PKI-based technology can fulfil these requirements.

[9] Requirements for a qualified certificate is given in Annex I to the Directive on Electronic Signatures.

[10] Requirements for a Secure Signature Creation Device is given in Annex III to the Directive on Electronic Signatures. The EU Commission has also published standards fulfilling these requirements. Cf. Commission Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council.

[11] Cf. recital 20 in the Directive on Electronic Signatures:
"Harmonised criteria relating to the legal effects of electronic signatures will preserve a coherent legal framework across the Community; national law lays down different requirements for the legal validity of hand-written signatures; whereas certificates can be used to confirm the identity of a person signing electronically; advanced electronic signatures based on qualified certificates aim at a higher level of security; advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-

admissibility as evidence. Pursuant to the Directive it is not possible for a Member State to set "higher requirements" when putting an electronic signature on par with a handwritten signature.[12]

Unfortunately, Article 5.1 is sometimes "over-interpreted", thus giving it a larger scope than what was intended. There are some important limitations in the article that often is forgotten or overlooked, inter alia:

1) The "automatic effect" of the legal effectiveness and admissibility as evidence only applies to qualified electronic signatures, and not any other type of electronic signature. Due to this fact a qualified electronic signature is sometimes referred to as an "electronic signature passport".[13] This is especially relevant to companies, conducting cross-border commerce within the EEA. They can always be sure that a qualified electronic signature will be "valid" when signing a contract etc.
2) It only applies to the formal requirements of a signature, and nothing else.
    a. Any other formal (mandatory) requirement that is not upheld can make the legal transaction null and void and/or inadmissible as evidence even if it has been signed with a qualified electronic signature, e.g. that the document does not contain certain information or is not signed by a notary public.
    b. Even if the signature is deemed to satisfy the legal requirements of a handwritten signature it can be contested on the same grounds as a handwritten signature; that it was done under duress, because deception, because lack of legal capacity etc.
3) This automatic fulfilment of legal requirements only applies when the law, directly or indirectly, permits that the legal transaction in question can be made electronically. It is possible for a Member State to "block" the sought effect of this Article by "forbidding" electronic communication within certain legal fields.[14]

The objective of Article 5.1 has never been to introduce a more or less unique European standardized secure electronic signature that can be used for various legal transactions. In order to remain stable and to avoid constant changes and updates, laws formulate rules but rarely describe how they shall be implemented. The law sets requirements on functions sought but the "how" is usually the object

---

creation device can be regarded as legally equivalent to hand-written signatures only if the requirements for hand-written signatures are fulfilled."

[12] There is one exception in Article 3.7 stating "Member States may make the use of electronic signatures in the public sector subject to possible additional requirements."

[13] Cf. Study for the European Commission – DG Information Society "The Legal and Market aspects of Electronic Signature – Legal and market aspects of the application of Directive 1999/93/EC and practical applications of electronic signatures in the Member States, the EEA, the Candidate and the Accession countries." Drafted by Jus Dumortier, Stefan Kelm, Hans Nilsson, Gerogira Skouma and Patrick Van Eecke. Service Contractract Nr. C 28.400, page 12.

[14] The Directive on Electronic Signatures does not regulate when an electronic signature can/shall be used. However, there are other legal documents that do. Cf. inter alia the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) Article 9 stating: *"Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means."*

of standards, which have, by definition a voluntary character. As long as people comply with the rule, they are free to decide how they shall do this. Sometimes legislation refers explicitly to standards, but only insofar that this is strictly necessary and the reference to a particular standard is mostly interpreted in a restrictive manner.[15]

What is of interest here is whether the definition of a qualified electronic signature can be interpreted to also cover entity authentication. I will come back to this question when looking into standard documents drafted under the auspices of ETSI, based on the Directive on Electronic Signatures.

5.1.2 Article 5.2 – legal effects of non-qualified electronic signatures

The second Paragraph of Article 5 states the following:

"*Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:*

- *in electronic form, or*
- *not based upon a qualified certificate, or*
- *not based upon a qualified certificate issued by an accredited certification-service-provider, or*
- *not created by a secure signature-creation device."*

This is an important Article, also when discussing the need for regulatory measures giving entity authentication a legal effect. The content of Article 5.2 is a regulation that is mainly directed to the Member States and its courts, stating that they may not disqualify an electronic signature solely on the grounds that it is e.g. in electronic form. One can of course deny an electronic signature legal effectiveness and admissibility as evidence on the ground that it is not "secure" enough, through explicit regulation in an act or in a case-to-case evaluation where the law sets functional requirements. It is as such permissible to require the use of a qualified electronic signature for a certain type of legal transactions, and thus deny an electronic signature legal effectiveness and legal admissibility as evidence at a "lower-level".

Also this Article is only applicable when it is possible as such to communicate electronically. The effect of this Paragraph is that also other signatures, other than qualified electronic signatures, can be given legal effectiveness and admissibility as evidence. But does this article also cover entity authentication? I will come back to this question later on. Before an answer can be given one have to look at the Directive on Electronic Signatures and its definition of inter alia electronic signature and qualified certificate.

5.1.3 Article 2.1 – "electronic signature"

[15] Dumoriter, J., "The European Regulatory Framework for Electronic Signatures", EU Electronic Commerce Law, ed. Nielsen, Jacobsen and Trzaskowski, Djølf publishing, Denmark, 2004 , page 90.

To be able to answer this question we have to look at the definition of "electronic signature" in the Directive on Electronic Signatures. In Article 2.1 electronic signature is defined as:

> *"data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication."*

How shall this definition be interpreted? To begin with one should note that the definition is not linked to the definition of a "signatory", which has to be a natural person.[16] This means that an electronic signature also can be used by inter alia a legal person or even a server. Which method of authentication is covered by the definition? Is it only data authentication or does it also cover entity authentication?

In the report to the EU Commission -"The Legal and Market aspects of Electronic Signature" which inter alia interprets the Directive on Electronic Signatures and also looks at all EEA Member States implementation of the Directive - it is stated that the definition of electronic signatures relates only to data authentication and not entity authentication.[17] As an example to describe what is covered by the Directive and what is not the report states that a PIN-code is not an electronic signature if it is used only to get access to an electronic bank account. On the other hand, when the same PIN-code is used in order to confirm a financial transaction it is used for data authentication and is deemed to be an electronic signature covered by the definition in the Directive on Electronic Signatures.

However, in a CEN/ISSS draft CWA on Evidential Value of Electronic Signatures,[18] the definition of electronic signature in the Directive is given a wider scope. The document states inter alia that:

"…it suffice for a given technology or method to enable authentication in order to fall within the directives scope of application… The potential of a certain method to serve authentication purposes is the only functional condition imposed by the directive's definition for this method to be qualified as 'electronic signature', irrespective of its intrinsic capabilities to generate or not the legal effects of a signature…electronic signatures as authentication tools in the light of Article 2 nr. 1 – which is the definition of an electronic signature - do not necessarily bear the functions of the signature as process to generate specific legal effects." [19]

---

[16] Directive on Electronic Signatures Article 2.3: signatory" means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents.

[17] Study for the European Commission – DG Information Society "The Legal and Market aspects of Electronic Signature – Legal and market aspects of the application of Directive 1999/93/EC and practical applications of electronic signatures in the Member States, the EEA, the Candidate and the Accession countries." Drafted by Jus Dumortier, Stefan Kelm, Hans Nilsson, Gerogira Skouma and Patrick Van Eecke. Service Contractract Nr. C 28.400, page 29 where the report refers to recital (8) of the Directive on Electronic Signatures, stating that: "…rapid technology development and the global character of the Internet necessitate an approach which is open to various technologies and services capable of authenticating data electronically."

[18] Draft document CEN/ISSS WS/E-Sign WSES N 0383 (Turin 2003-12-16); Title CEN/ISSS WS/E-Sign Area AB "Evidential Value of Electronic Signatures" Version 0.07 November 2003. I have not been able to locate a final version of this document.

[19] A.a. page 12

The conclusions in this CEN/ISSS report are subsequently that the Directive and the definition of electronic signature also cover entity authentication.

5.1.4 Article 2.10 – "qualified certificate"

The Directive on Electronic Signatures contains a definition of a qualified certificate. Requirements on the content of such a certificate are mainly regulated in Annex I in the Directive.[20]

As far as I can see there is nothing in the Directive stating that a qualified certificate cannot be used for entity authentication, and entity authentication only. This is also in line with the above-mentioned conclusions from the CEN/ISSS report. Trying to confirm this position one can look at the ETSI Technical Standard for X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons, ETSI TS 102 280. In chapter 5.4.3 there is a table of five different profiles, named A to E.

"The following key usage settings are named in this profile as type A, B, C, D and E:

Type	Non-Repudiation [NR] (Bit 1)	Digital Signature [DS] (Bit 0)	Key Encipherment or Agreement [KEA] (Bit 2 or 4)
A	X		
B	X	X	
C		X	
D		X	X
E			X

In cases where a certificate is intended to be used to validate commitment to signed content, such as electronic signatures on agreements and/or transactions, then the key usage combination SHALL be limited to type A and B. This means that the non-repudiation bit (bit 1) SHALL be set. Of these alternatives it is RECOMMENDED to use the type A setting only…

…If the certificate is declared to be a Qualified Certificate according to TS 101 862 then the key usage setting SHALL be limited to type A, B and C."

The standard thus opens for that a qualified certificate can be used for non-repudiation only (profile A). Non-repudiation is here the equivalent to what also is referred to as a (electronic) signature. But what is interesting is that a qualified certificate also can be used for only digital signature (profile C). Digital signature in this context has the same functional meaning as the term entity authentication used in this report.

[20] Pursuant to the Directive Article 2.10 a Qualified Certificate "means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II".

Consequently, pursuant to this standard document a qualified certificate can have a key usage setting allowing the use of the certificate for entity authentication, and entity authentication only.

5.1.5 Conclusions

As has been shown above there are divergent opinions in the legal doctrine as to whether the Directive on Electronic Signatures covers entity authentication or not. However, it is clear that the standardisation work that has been done to support the legal framework laid down in the Directive is clear on the fact that a a qualified certificate, as defined in the Directive, also can be used for entity authentication and entity authentication only.

As to the question on the scope of the definition of a qualified electronic signature and Article 5.1 the following is stated in the CEN/ISSS draft CWA on Evidential Value on Electronic Signatures[21]:
"Article 5.1 does not include any requirement which would allow a signer to demonstrate an intention that on one occasion he wished to use his certificate and SSCD to create a qualified electronic signature for authentication purposes, and on another he wished to indicate a legal commitment.

Various solutions to this problem have been suggested; none are suitable throughout all Member States, and all are controversial to a greater or lesser extent. There is therefore, no accepted (and certainly no standardised) method by which a relying party can determine differences in the signer's intent.

Signatories should ensure that the meaning of their signatures is clear from the data or context in which they are signing: relying parties should ensure that the meaning of a signature is unambiguous before relying upon it. These are important matters to be taken into account when considering the legal validity and enforceability of electronic signatures under the Directive, particularly in relation to Art. 5.1 signatures."

The conclusions in this CEN/ISSS report are subsequently that the Directive also covers entity authentication, even Article 5.1 – putting a qualified electronic signature on par with a handwritten signature – covers the use of the signature for entity authentication and not only data authentication.

In addition I find it awkward to make such a distinction between entity authentication and data authentication as it is done in the above-mentioned report to the EU

[21] Draft document CEN/ISSS WS/E-Sign WSES N 0383 (Turin 2003-12-16); Title CEN/ISSS WS/E-Sign Area AB "Evidential Value of Electronic Signatures" Version 0.07 November 2003. I have not been able to locate a final version of this document, page 54.

Commission.[22] In my mind it is difficult to uphold such a distinction. It maybe true that this issue was not fully discussed or understood at the time the Directive on Electronic Signature was drafted, but I cannot see any good reasons to interpret the Directive on Electronic Signatures in such a way that it would disqualify entity authentication. Thus I agree as such with what is stated in the CEN/ISSS CWA on Evidential Value of Electronic Signatures. It might technical very well be that also a qualified electronic signature covers entity authentication, but since the automatic effect of a qualified electronic signature is only given in relation to a handwritten signature, Article 5.1 has a limited value for entity authentication.

Identification (entity authentication) is a more nuanced legal process than the legal requirement of a handwritten signature, cf. chapter 4.2. This relates both to the fact that identification can be achieved in so many different ways depending within which legal field one is navigating and what legal privileges and rights one wishes to obtain. Thus, it can be difficult to draft an article for the electronic equivalence to identification, akin to Article 5.1 for the electronic equivalence to a handwritten signature. Maybe the closest one can get is to ensure that the electronic equivalence to identification is not disqualified only due to the fact that it is in electronic form. Given the fact that Article 5.2 in the Directive on Electronic Signatures also covers entity authentication, this might already been obtained.

My conclusion is that Article 5.2 of the Directive on Electronic Signatures, which is a non discriminatory rule stating that also non-qualified electronic signatures can be given legal effectiveness and legal admissibility as evidence, also applies to entity authentication. This means that we already today have a regulation implemented by all Member States that is relevant to entity authentication.

[22] The presented dividing line between entity authentication and data authentication in the mentioned report is difficult to wholly understand. The consequence of what is stated in the report is that the directive does not cover a single-sign on procedure, even if the non-repudiation key is used. Whether that would be a probable solution or not is not the point here. By stating that the directive only covers non-repudiation and not digital signature / entity authentication, the watershed should be focusing on key usage settings and when in the process the electronic signature is used. (This is also the main objection presented in the CEN/ISSS draft CWA on Evidential Value of Electronic Signatures.) It is possible (but maybe not practical) to have a system that requires that the signatory have to verify every transaction with the key usage set for digital signature and not non-repudiation.

6 Key issues when drafting a Directive on Authentication

Even if the Directive on Electronic Signatures also covers, or at least partly covers, entity authentication, it is clear that its drafter primarily sought to find the electronic equivalence to a handwritten signature. As mentioned in chapter 4.2 and 5.1.5 there are differences between electronic signature and entity authentication. The Directive on Electronic Signatures does not address these differences and their consequences. This chapter will present issues that needs to be addressed, someway or another, to achieve a functioning legal framework for entity authentication and the use of a pan European eID.

Entity authentication is a process of confirming a person's identity. This can be achieved by the use of an electronic ID in a PKI environment. That means that an electronic certificate to which a public and a private key are attached will be the electronic ID.[23] It is in relation to this certificate there is a need for additional requirements when drafting a legal framework for entity authentication.

6.1 Issuance procedures of an eID etc.

It is of vital importance to ensure the link between the natural person holding an eID and the information in the eID. This link has to be ensured in order for a third party to be able to accept the eID as a valid ID. To ensure the link between the declared holder of the eID and the natural person identified in the eID, the issuer must maintain good and secure procedures where the person must prove his identity to the issuer.

This issue is regulated in the Directive on Electronic Signatures. Pursuant to Annex II of the Directive litra d a certification service provider issuing qualified certificates shall:
"... verify, by appropriate means, in accordance with national law, the identity .... of the person to which a qualified certificate is issued."

In addition the certification service provider shall pursuant to Article 6.1 litra b ensure:
"…that at the time of issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data [24] corresponding to the signature-verification data [25] given or identified in the certificate."

Article 6.1 states that if the information is incorrect at the time of issuance the issuer / certification service provider can be held liable for damages.

All identification documents are dependent on a seed document, and the integrity of an identification scheme also depends on a provable relationship between the person and the document. In relation to the question whether there is a need to

[23] The Directive on Electronic Signatures regulates such a certificate – a qualified certificate – with requirements on the content of the certificate and on the issuer of it.
[24] In a PKI environment the signature-creation data is the private key.
[25] In a PKI environment the signature-verification data is the public key.

have additional regulation on identification and issuance procedures to those already given in the Directive on Electronic Signatures, one needs to inter alia evaluate the following issues:

- Is there a need to ensure a "stronger" connection between the holder and the certificate when it is used for entity authentication (as an eID) compared to when the certificate is used for signing only?

- Should the regulation specify what documents an applicant/holder needs to present to the certification service provider's registration authority. If so, what documents would that be?

- Should there be a procedure requirement in addition to that, e.g. a mandatory requirement of personal appearance?

- Should there be any other evidential requirements, to prove the identity of the holder?

- Should it be mandatory that the personal information details are derived from or checked against a national population register?

There are at the European level scarce with detailed legislation on issuance procedures.[26] The Directive on Electronic Signatures and the Directive on Money Laundry, and also in standards issued by ETSI there are to some extent some regulation on issuance procedures. These and similar requirements have been transposed into national law within the EEA, and they co-exist with requirements based on internal national needs and traditions in Member States.

The requirements in the Directive on Electronic Signatures have already been mentioned.

Article 3 of the Directive of 2001 amending the Directive on Money Laundry[27] has a similar non-specific wording, stipulating that:
"... institutions shall require identification of their customers by means of supporting evidence when entering into business relations."

The standard on Policy Requirements for Certification Authorities issuing Qualified Certificates - ETSI TS 101 456 – is more detailed concerning this issue and states that:

> *"the service provider shall verify by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes*

[26] The reason for that could be the limitations set by the EC Treaty Article 18, cf. chapter 7 below.
[27] Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering.

of the person to which a qualified certificate is issued. Evidence of the identity shall be checked against a physical person either directly or indirectly using means which provides equivalent assurance to physical presence. Submitted evidence may be in the form of either paper or electronic documentation."

The ETSIs standard TS 101 456 is not more precise on what documents the applicant shall produce, but only on procedures requiring, as a general principle, the applicant to appear in person. It is not uncommon to have a requirement of personal appearance. For example when applying for a Finnish national eID (FINEID) the applicant must appear personally.[28] When submitting the application the applicant must present an ID accepted as valid by the police authority, i.e. a visual ID-card, a driving license or a passport. In addition the applicant must in person come back to get his/hers FINEID. It is not stated how the applicant is to be identified this time, but it is probably by the same type of documents as when applying for the eID.

As mentioned above the ETSI standard TS 101 456 does not provide additional requirements on what documents that shall be presented. The reason for that could possible be that such requirements vary form state to state and it its difficult to find a specified regulation at a European level that could be accepted by all Member States. National legislation has usually very precise regulations on procedures and document requirements when issuing an ID. Today these requirements normally only apply to visual IDs since the spread and use of eIDs at the present time is quite limited. If an eID shall be given the same legal validity and be used in the same types of transactions as a national accepted visual ID, the requirements on the issuance of the eID has to be the same - mutates mutandis - as for the visual ID. If it were easier to obtain an eID, it would be detrimental to the trust we as of today give the use of IDs. It would facilitate a possible circumvention of existing rules and regulation that has built this trust over a long period of time.

To demonstrate the rigidity of national regulation I could mention a legal challenge in Norway. When drafting the new Act on Money Laundry a question related to the use of eID came up. In the proposed Act a client entering into a new business relationship with a bank, a lawyer etc. must produce a valid ID. A valid ID is pursuant to the act a "visual ID". The Norwegian Financial Surveillance Authority gives regulatory guidelines on which visual IDs are to be deemed as valid IDs. In the hearing of the draft act it was proposed that one should also accept a qualified certificate as defined in the Directive on Electronic Signatures as a valid ID. The Ministry of Finance was in favour of opening up for the use of eIDs in the act but opposed that a qualified certificate would suffice. The reason for that was that the Act on Electronic Signature (transposing the EU Directive on Electronic Signatures) does not explicitly state which documents need to be presented to the certification service provider before issuing a qualified certificate. The Ministry of Finance stated that without a more precise regulation on this matter it might be easier to get a qualified certificate (an eID) than a valid visual ID, and this would make it possible to circumvent existing requirements and build down existing trust.

[28] Cf. PKI Disclosure Statement – the Citizen Certificate of the Population Register Centre v. 1.4 (Chapter 2.2) and Certificat Policy for - the Citizen Certificate of the Population Register Centre v. 1.2 (Chapter 1.2).http://www.sahkoinenhenkilokortti.fi/default.asp?path=5%2CPublikationer&file=1%2CCertifieringspolitik%2Elink&template=

In order to have a success with a pan European eID, all issuers of eID will need to apply similar procedural rules/requirements when issuing the eID. Should that not be possible one ought to at least find a functional equivalence to what these procedures aim to ensure. This issue is further discussed in chapter 9.

6.2 The content of the eID and the verification of the eID.

This is to a greater or lesser extent a continuance of the question on issuance procedures. In respect to the issuance procedures one has to answer the question on how one shall make the link between the holder and the information in the eID clear to a third party relying on the eID. Here one has to answer the following questions: what information has to be in the eID/certificate, how is it going to be presented and how can a third party verify the information in the eID in order to be able to ascertain the connection between the natural person and the declared holder of the eID?

It is of vital importance to have a set of rules that ensures that not two persons can have an eID containing identical information. It is imperative that there is information in the eID distinguishing holders from each other. There are several ways to do that, and probably they are equally good, but if one wants to have a pan European eID we probably need to have to accept only one solution.[29] Disregarding what solution one decides to implement to separate holders from each other it must provide the following features:

- universality of coverage
    - every relevant person should have an identifier
- uniqueness
    - each relevant person should have only one identifier
    - no two people should have the same identifier
- permanence
    - the identifier should not change, nor be changeable
- exclusivity
    - no other form of identification should be necessary or used
- precision
    - every identifier should be sufficiently different from every other identifier that mistakes are unlikely

As mentioned above one of the relevant questions here is how one can ensure the unique link between the holder and the eID and how a third party can verify it. In e.g.

[29] Or would it be possible to accept several solutions side by side? Even if that would be possible it will most probably have a negative effect on the chances to obtain interoperability and on the possibility to pave way for automated processes.

the Nordic countries all natural persons are at birth given a unique "national identity number" composing of date of birth and an additional four to five digits. Other Member States have other types of national identity numbers, social security numbers etc. and then again other states may not provide unique national identity numbers at all for it's citizens. The question is then what shall be used as a unique link and how can it be verified by e.g. a foreign entity that is not used to handle those specific types of identifiers used in foreign eIDs.

The holder of an eID may also want to be able to control what information in the eID/certificate is presented to a third party. The type of information a third party needs differs based on the situation and/or the context where the eID is used, eg. if the third party is a hospital or a private company selling products over the Internet. A hospital needs to assert the identity with whom it is communicating, in the Nordic countries that means mapping the holder's national identity number (stated in the eID) against the hospital's database with medical record. When the third party is a company selling products over the Internet it might not even have a need to know with whom it is communicating (entering into a sales contract with), as long it is given assurance by the purchaser's bank that it will receive due payment for the delivered goods. For the purpose of delivery of tangible goods the seller will though still need a name and address, but that does not necessary have to be ascertained from information in the eID.

Pursuant to the Directive on Electronic Signatures Annex I litra c a qualified certificate must contain the name of the signatory, the signatory being a natural person. The directive also allows the use of pseudonym, under the condition that it can be identified as a pseudonym. Here you have a difference between the concept of signing and entity authentication. As already mentioned above it is not always relevant to really know with whom you e.g. have entered into a sales agreement with, provided that you get your rights under the agreement; payment and delivery. But for authentication purposes that is normally exactly what you want to assure. With whom am I communicating? There are, to my knowledge, no visual ID today issued with a pseudonym instead of a real name, at least not if it shall provide any certainty to a third party with whom he/she is communicating. An eID with a pseudonym would most probably have a limited legal and practical value. Subsequently, if one wants to build a legal framework for entity authentication on the Directive on Electronic Signatures and qualified certificates the "right/possibility" to use a pseudonym in the certificate must be addressed.

6.3 Archival/storage services

The Directive on Electronic Signatures does not contain regulation on storage of information in connection of the use of a qualified certificate. The reason for that is probably based on the mere fact that the Directive as such does not state anything about when an electronic signature / qualified certificate can be used. Regulation on storage will vary depending within which legal area the certificate is used. Here you may have a wide spectre between very precise regulation stating what information and documents are to be stored, in what manner how and for how long, to explicit regulation that information may not be stored at all due to data protection.

As already mentioned the Directive on Electronic Signatures has focused mainly on the use of electronic signatures as a signature, for non-repudiation purposes. However, also in relation to

entity authentication it would be difficult to draft detailed principles on storage of information with a general validity. Any need to, or requirement not to, store information when using the eID will probably have to be solved pursuant to the regulatory regime to which the eID is used. In this area there are divergent regulatory needs reflected in relation to what purpose the electronic signature is used for, non-repudiation or digital signature. Thus, there is no need to, and it would probably also be quite futile, to try to draft general rules and requirements on a European level concerning storage of information.

6.4 Data protection

Any regulation on an eID must also address the issue on data protection and privacy. An issue related to data protection is inter alia the right for the holder to control the information a third party can access, cf. chapter 6.2 above.

There is a general directive on data protection, but it should be noted that the Directive on Electronic Signatures also regulates data protection.[30] The Directive on Electronic Signatures requires that qualified certificates must contain the name (pseudonym) of the signatory and contains a voluntary provision where a specific attribute of the signatory can be included if relevant, depending on the purpose for which the certificate is intended, eg. a insurance policy number if the certificate is mainly used in communication with an insurance company.

It should be noted that pursuant to the Directive Annex II litra l a qualified certificate should not be made public unless the signer/holder has given his approval. That seems to be an on or off "button", and it is not precise enough in this case where you want the certificate to be made public but that different information should be accessible in respect to whom you are communicating. This article in the Directive needs to be interpreted in a manner that complies with the specific needs arising from entity authentication. This can also be made more precise in standards drafted for the use of an eID.

Otherwise on this topic I would like to refer to the document "Electronic Identity – White Paper v. 1.0", Chapter 3.1 on "Legal issues in relation to the use of electronic identity" where these issues are addressed.[31] This document mentions inter alia:

- The directive 95/46/EC on data protection is thoroughly discussed in connection with an eID

- Confidentiality of personal data while processed and security of the processing it self are a must when protecting the personal data of a data subject

- In the report it is recommended to have one overall security component in this respect and the GIF model is mentioned as to

[30] Pursuant to Article 8 in the Directive on Electronic Signatures a certification service provider is more limited in how he can collect data concerning the holder/signatory. This Article applies to all certification service providers, not only those issuing qualified certificates.

[31] "Electronic Identity White Paper V 1.0", June 2003, eEurope Smart Cards/Trailblazer 1 "Public Identity", ed. Ringwald, A, "Part III: Aspects Related to e-ID Evolution and Implementation", pages 42 –45.

cover this issue

- Also the drawback of a single identification number in the eID is mentioned. Such an identification number would allow cumulating of personal data for various databases and eventually end in a personal profile

6.5 Liability

Who shall be liable for any false information in the eID (or any other "mishaps") in relation to the use of the eID?

As a starting point all participants in an identification and later an authentication process is responsible and accountable for security, in proportion to his or her role in that process. All participants have a responsibility to contribute to the mitigation of risk through sound security practices. However, infrastructure providers and those involved in authentication administration bear much of the burden of design and maintain systems based on policies and procedures that take into consideration relevant legislation, policy and industry standards.

The Directive on Electronic Signatures regulates the liability of certification service providers issuing qualified certificates. Since this is an area where technical expertise is necessary to prove any mishap in the use of electronic signatures, the burden of proof for the certification service provider is more onerous than in normal civil/tort cases. Pursuant to the Directive there is a reversed burden of proof for the certification service provider, i.e. he will be found liable for damages unless he can show that he has not acted negligently. The liability covers damage caused to any entity or legal or natural person who reasonably relied on that certificate, thus also including a third party that relied on the certificate.

The certification service provider can be liable for damages if he cannot ensure at the time of the issuance of the certificate:[32]

- that all information in the certificate was accurate and contained all details prescribed for a qualified certificate;
- that the signatory identified in the qualified certificate held the signature-creation data (private key) corresponding to the signature-verification data (public key) given or identified in the certificate;
- that the signature-creation data (private key) and the signature-verification data (public key) can be used in a complementary manner in cases where the certification service provider generates them both.

However, if the certificate contains limitation on the use or on the value of the transaction, the certification service provider will not be held liable for damages resulting from that these limits are exceeded.

[32] Cf. Directive on Electronic Signatures Article 6.1

Would it be possible to have the same type of liability regulation – with a reversed burden of proof for issuers of eID in all Member States? Are there differences between electronic signature and entity authentication that affects how liability shall be regulated? The liability rules in the Directive on Electronic Signatures are based on an assumption that paying pecuniary compensation (damages) can compensate for the consequences of a non-valid signature. If the contract is non-enforceable due to the fact that a party has used an electronic signature that is denied legal effectiveness or admissibility as evidence, the other party can normally be compensated by pecuniary means. Authentication procedures usually have a different purpose and legal connotation and can in some situations not be compensated by pecuniary means. There might not even be any money involved in the transaction as such. We can revert to my example from chapter 6.1 where banks etc. – pursuant to the Norwegian Act on Money Laundry - have to establish the identity of any new client by demanding the client to produce a valid ID. This is a requirement with the aim to ensure that the State – the police – shall be able to find out the identity of any person that uses the bank's services for money laundry, and thereby more easily locate the perpetrator to bring him before justice. Pecuniary compensation (damages/fines etc.) to the state would thus not be an adequate compensation in this case, but would only be a deterrent for that bank and other banks from breaking the law in the future.

Pursuant to the regulation in the Directive on Electronic Signatures anyone that reasonably has relied on a qualified certificate has a right to damages under certain conditions, cf. above. If a certificate is used in a criminal activity and the criminal activity is facilitated by the fact that the certificate contains wrong/false information, the liability of a certification service provider as an accomplice will be evaluated pursuant to national criminal law. The Directive does not cover this area and thus the situation would be the same disregarding whether the certificate is used for signing or entity authentication.

6.6 Revocation

The effect of "identity snatching" can be much greater when using someone else's eID, compared to a visual ID. The use of a visual ID usually requires personal appearance, which geographically limits the use of the visual ID. An eID accepted within the whole EEA can be used on the Internet for services etc. offered within the whole area disregarding where you are in the world, and almost for an unlimited amount of transactions in a short period of time.

However, if one takes the necessary precautionary actions, e.g. by having an effective system for the revocation of an eID, the security of an eID could be much higher than for any visual ID. It would be quite complex to have a revocation list for visual IDs, but it is normally a standard service rendered when offering an eID. The revocation must be made immediate once the holder has reported that his eID-card has been stolen, lost or compromised.[33] To facilitate an enhanced revocation service one could facilitate one European revocation point for the revocation of any pan

[33] Cf. the Directive on Electronic Signatures Annex II where a Certification Service Provider is required, pursuant to litra b, to "ensure the operation of a promt and secure directory and a secure and immediate revocation service" and pursuant to litra c to "ensure that the date and time when a certificate is issued and revoked can be determined precisely."

European eID. The European Commission has suggested something similar to this in the fight against money laundry and credit card frauds. The Commission has mentioned the possibility of setting up a single, easily-remembered, toll-free number at EU level for prompt notification of loss or theft of payments instruments (bank/credit cards).[34] [35]A similar feature has been discussed in the Council Proposal on passport and biometric, where it is stated that one could create a centralized biometric-based "EU passport register".[36] This would facilitate the "revocation" of a passport that has been lost or stolen.

Another question that relates to the issue of revocation is the question on whether it should be possible to use an eID as the only "seed document" to apply for a new eID from another issuer. This would mean that the new issuer would never meet the holder face to face, directly or indirectly through a local registration authority nor receive any additional documents supporting the process of identifying the applicant, but only an eID. There are many risks involved in relation to that, suggesting that one should have different policies on this issue when it comes to visual IDs and electronic IDs. What if the first eID contains false information due to mistakes by the first issuer? Would the second certification service provider be responsible for the false information in the second eID based on false information in the first eID? If a dishonest person succeeds in receiving a false ID he can immediately use that to establish many new eIDs. The major difference between a visual ID and an eID is that even "clear" mismatches between the user and the declared holder in the eID can not be detected since the eID is used without any personal contact. Thus, when the first certification service provider realises that it has issued an eID with information that is not accurate, the revocation of that ID would not solve very many problems. One would therefore need a system that links these eIDs together and that a revocation of one of the eIDs would automatically instigate a "chain-revocation" of the other eIDs, provided of course that the first revocation is done due to the fact that it contains non-accurate information etc. Given the fact that it would be difficult to establish such an "eID revocation-chain", and that it also may have unwanted effects on data protection, it would probably be advisable to disallow such use of a pan European eID, at least for the time being.[37] This does not mean that it shall not be possible to renew an eID from the same issuer using the eID.

6.7 Interoperability

[34] Communication from the Commission to the Council, the European Parliament, the European Central Bank, the Economic and Social Committee and Europol – "Preventing fraud and counterfeiting of non-cash means of payment", 9 February 2001 (COM (2001) 11 final)

[35] Cf. also the Common Position No. 12/2004 of 18 December 2003 concerning IDABC stating in Annex II litra A a stating that one of several horizontal measures is to establish "a single point of access to e.g. legal online information services in Member States." This access point could also be used as a recipient of revocation messages of pan European eIDs.

[36] Proposal for a Council Regulation on standards for security features and biometric in EU citizen's passports, 18.2. 2004 (COM(2004) 116 final) 2004/0039

[37] It should be noted that in relation CEN TC224 WG15 on European Citizen Card (ECC) Common Requirements it is assumed that a subscriber shall only be given one ECC.

In order to accomplish a wide spread use of a pan European eID one has to ensure interoperability, on inter alia a technical and organizational level. Interoperability is the ability of a system or a product to work with other systems or products without special effort on the part of the customer. In this report interoperability means that eg. a tax-authority in a Member State can receive and validate an eID issued from any certification service provider within the EEA issuing "valid" pan European eIDs. Interoperability shall thus make it possible – as a general aim – for an EEA citizen to use the same eID in communication within the whole EEA, especially with any public authority within the EEA.

An important prerequisite to be able to achieve interoperability, or at least to facilitate it, is by giving market actors incentives to take open industry standards into use.[38] This view is also supported by the report submitted to the EU Commission on the implementation of the Directive on Electronic Signatures etc.[39] The question is who is going to ensure that we will obtain interoperability. In many other areas this has been mainly achieved through agreements between the market actors. Neither EU nor the Member States can force the market actors to apply a standard unless the market actors deem it beneficial from a commercial point of view.

Interoperability reaches over different areas and can be implemented through various schemes. The need for interoperability for entity authentication is probably mainly eminent in electronic communication between citizens and public authorities. This can be solved in various ways:

1) The authority enters into agreement with all certification service providers issuing the eID that can be used.
2) The authority has an agreement with one certification service provider issuing pan European eIDs. In return all providers of pan European eIDs have agreements with each others enabling them to verify each other's eIDs.
3) The authority has an agreement with one trusted intermediary party. The intermediary in its turn has agreements with all certification service providers issuing pan European eIDs. In this scenario the intermediary would be akin to a trusted third party (without issuing any certificates itself) and the link between the authority and EEA-citizens using pan European eIDs issued by different certification service providers.

Solution #1 is time consuming, costly and probably not possible to carry out. It will be very difficult for all authorities to have an agreement with all relevant certification service providers at all time.

In theory solution #2 could work, but that would lead to a situation where all relevant certification service providers would have to have an agreement with

[38] Cf. "European Interoperability framework for pan-European eGovernmet Services" by IDABC/ETF – European Commission, v. 1.0, 2004, page 9 (Recommendation 2).

[39] "The Legal and Market aspects of Electronic Signature – Legal and market aspects of the application of Directive 1999/93/EC and practical applications of electronic signatures in the Member States, the EEA, the Candidate and the Accession countries." Drafted by Jus Dumortier, Stefan Kelm, Hans Nilsson, Gerogira Skouma and Patrick Van Eecke. Service Contractract Nr. C 28.400.

each other. It has been done in limited projects, but it has been a very time and resource consuming negotiation to obtain a unity on legal, financial and technical issues. In order to achieve such a solution the involved certification service providers need to have trust in each other, and maybe the market at this point is to immature that such a trust is at hand, especially cross-border.

Maybe solution #3 is one of the more interesting ways of achieving interoperability. The reason for that could also be that one will probably not obtain a pan European eID before the Member States have rolled out their own national eID and showed to their citizens the advantage of its use, the trust they can have in it and also that the Member States have opened up for electronic communication with e.g. public authorities on both a legal and factual level. Maybe we should have to accept that authentication requirements can be obtained differently within the EEA, based on functional requirements, and that interoperability must be achieved under these circumstances. The intermediary can be certified in accordance of a standard drafted by ETSI and approved and published by the EU Commission after a recommendation by the Electronic Committee (sometimes called the "Article 9 Committee") established pursuant to Article 9 in the Directive on Electronic Signatures. These very few intermediaries could thus act as "clearing houses" for e.g. public authorities accepting the use of a pan European eID. For these authorities the problems of a non-perfected interoperability between the issuers and different solutions are pushed over to and solved by these intermediaries. The level of complexity laying behind the validation etc. is also hidden for the holders of the eIDs.

Interoperability is a general sought function. The EU Commission mentions inter alia in the newly drafted amendment to the Directive on Public Procurement[40] that one will need interoperability for advanced electronic signatures (i.e. digital signatures). One of the main goals of developing eProcurement within the EEA is to support the development of the Internal Market in ensuring interoperability. It is a fact that such interoperability does not exist today. It is already difficult to achieve interoperability within one state, let alone within the whole EEA. The problem of the non-existing interoperability is thus a problem for all sectors using electronic communication and if interoperability is achieved many would benefit from that. The Porvoo Group is not alone addressing this issue, and any work to achieve interoperability should be made through a joint European effort to ensure the right input and that a generally accepted interoperability is achieved.

The eEurope Action Plan, adopted by the EU Commission in 2002 sets very ambitious goals. One goal that is mentioned is that on-line public services should be available to businesses and citizens by 2005. In addition the Action Plan specifically states that Member States should carry out a significant part of public procurement and that the EU Commission shall issue an agreed interoperable framework in support thereof.

[40] Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts

On the issue on interoperability one also needs to follow and support the IDABC-programme.[41] One of the programs aims is to "achieve interoperability, both within and across different policy areas and, where appropriate with businesses and citizens, notably on the basis of a European Interoperability Framework." [42]

6.8 Biometric

This report has already mentioned several differences between a visual and an electronic ID. One difference that has only been touched upon is related to the use of them. A visual ID usually requires personal appearance by the holder and makes it possible to establish who is using the visual ID. With the use of a visual ID where the holder is present you can at least control that eg. the there is match between the person's age and the alleged age in the ID and compare the person's appearance with the picture in the ID (if that exists) and you can also normally confirm such a basic thing as holder's sex. None of these simple screening processes are possible when using an eID. Since the "user" is not personally present the eID can be used by anybody, with or without the consent of the holder, and the third party cannot tell the difference.

One way to better ensure that the declared holder of the eID also is the user of it could be done by adding **biometric**[43] (instead of or together with a PIN-kode) to access and use the private key associated to the eID. However, on the scale between cost, easy functionality, risk and trust it can be argued that it would not be feasible to use biometric to get access to the eID, not at the present state. Maybe that will lead to a limitation of use of the eID within certain fields, e.g. e-voting from your home computer.

[41] A EU programme for Interoperable delivery of pan-European eGovernment services to European public administrations, common institutions and other entities and to European businesses and citizens.

[42] Common Position No. 12/2004 of 18 December 2003, Article 2 litra d

[43] The term 'biometrics' is used to refer to any and all of a variety of identification techniques which are based on some physical and difficult-to-alienate characteristic. They are sometimes referred to as 'positive identification', because they are claimed to provide greater confidence that the identification is accurate.

7 EC Treaty Article 18

Article 18 of the EC Treaty states the following[44]:

"1. Every citizen of the Union shall have the right to move and reside freely within the territory of the Member States, subject to the limitations and conditions laid down in this Treaty and by the measures adopted to give it effect.
2. If action by the Community should prove necessary to attain this objective and this Treaty has not provided the necessary powers, the Council may adopt provisions with a view to facilitating the exercise of the rights referred to in paragraph 1. The Council shall act in accordance with the procedure referred to in Article 251.
3. Paragraph 2 shall not apply to provisions on passports, identity cards, residence permits or any other such document or to provisions on social security or social protection."

This means that the Council to some extent is prevented from drafting regulation on inter alia identity cards. It is clear that this article sets up some legal parameters that have to be observed when drafting a legal framework for a pan European eID. There is a core of legal regulation on "identity cards" that is safeguarded the Member States. Exactly where these boundaries goes as to what is allowed to co-ordinate on a European level and what shall be reserved to each of the Member States in not easy to establish. One can, however, establish that the EU has shown an interest to co-ordinate a regulation on eIDs, such as e.g.:

- The Directive on Electronic Signatures that also covers entity authentication.

- On the EU Commission's web site concerning eGovernment[45] it is stated that: *"There is a plethora of open research issues in eGovernment. R&D needs to address networked technology that complements the diversity of organisations and cultural practices. An example is in managing the identity of citizens and companies across administrations and countries."*

- EU's work on regulation for passports shall also be mentioned. Since it has been possible to draft a regulation in this area it is probably possible to draft regulation within the area of a pan European eID. It should be noted that the EU regulation on passports and biometric e.g. explicitly states that the identification process is a national matter.

- The work under the auspices of IDABC is of immense interest. One of its goals is to establish and develop pan European eGovernment Services and trans European networks. The realization that Article 18 can limit part of such an acheivment can to some extent be detected within this project. In the IDABC Common position it is

[44] Treaty establishing the European Community (Nice consolidated version) - Official Journal C 325, 24/12/2002 P. 0033 - 0184
[45] http://europa.eu.int/information_society/programmes/egov_rd/about_us/index_en.htm

> stated that "it is relevant to ensure close co-operation between the Member States and the Community and, where relevant, the Community institutions and stakeholders."[46]

Depending on how a legal framework for an eID shall be drafted one has to look further into the limitations set by the above-mentioned article in the EC Treaty. I will not here go any further into this issue, but only point out its existence and importance when drafting a legal framework for a pan European eID. It shall be noted that Paragraph 3 of Article 18 uses the word "document", that possibly relates to paper/visual documents. Thus, maybe the limitations in Article 18 is more pertinent should one work for a combined visual and eID than if one would draft a legal framework only applicable to electronic IDs.

[46] Common Position (EC) No 12/2004 of 18 December 2003 adopted by the Council, acting in accordance with the procedure referred to in Article 251 of the Treaty establishing the European Community, with a view to adopting a decision of the European Parliament and to the Council on interoperable delivery of pan-European eGovernment services to public administrations businesses and citizens (IDABC), preamble 19.

8 Should we have one or two levels of eIDs?

It should be noted that the pan European eID that has been described in this report with necessary regulation is a "high-end" certificate for entity authentication. It can be assumed that entity authentication will be mainly used in communication between natural and legal persons, on the one hand, and public authorities, on the other. However, communication with public authorities does not always require a high level of authentication. Even if you do not need a high level of assertion of the identity of a person you may still need to ensure that the electronic message (data) can only be accessed by the designated receiver or by authorised personnel. This issue will not be further addressed here.[47] When I say that you do not need a high level of authentication, I manly focus on the procedures on issuance of a certificate etc, and not the technical solution as such.[48] There is normally no immediate danger that someone else submits an enrolment application to a University or applies for a job in someone else name, or that you would submit an application to the Municipality's kindergarten for any other children than your own. Maybe one could take into use a pan European eID on a lower level to get people started in using electronic communication.[49] The next realisation could then be that the applicant/the EU Citizen is unable to receive a reply from the public authority with the use of the same eID. One of many solutions could be that the public authority makes its decisions etc. available on a closed server, where only authorized persons have access. Access can be given with the use of an eID. But since the published documents could contain personal/sensitive data, you will need a higher degree of assertion that it is the right person accessing and downloading these documents compared to when e.g. submitting the application in the first place. This dissymmetry of the use of eIDs might seem peculiar at first, but is actually very logic and to some extent copies the paper based environment. The public, which now have started to communicate electronically, will demand an eID that gives them the possibility to access databases, retrieve decisions/judgments etc. from public authorities, even when they contain sensitive personal date.

Taking this into consideration it would be relevant to discuss whether we should have two levels of a pan European eID. Many of the requirements mentioned in the report can then be disregarded or at least minimised on the lower level. The question on whether one should have more than one level is more a technical (interoperability) and financial issue than a legal. It is clear though, that one can not have to many different eIDs since it will be to costly, ineffective and contra productive.

Electronic documents can be "worn-out", and that also applies to an eID. A user of a "high-level" eID might be reluctant to take it into use unless it is absolute necessary, since the use of

[47] The assurance of secrecy can be achieve by the use of other technical means that the use of an electronic signature and PKI.

[48] To my knowledge it is also these "physical" requirements that affects the price the most. Requirements of physical appearance, sending documents as registered mail is very costly and every step to make these requirements less strict will lower the price of the signature. This does not apply to the same extent for technical solutions. However, the level of issuance procedures and the level of technical solutions assuring the authentication to the declared holder, once the eID is taken into use, should probably go pari-passu. There is no point in having a high-tech solution that is very costly, should you apply a less strict issuance procedure, and vice-versa.

[49] Cf. "European Interoperability Framework for pan European eGovernment Services", chapter 2.2.3 outlining four different levels of eGovernment.

the same eID in all situation leaves trails which could be used to set up a profile of your whereabouts on the net. By providing two levels of eIDs one will thus escape some of the worries presented in the above-mentioned Porvoo Group's White Paper "Legal issues in relation to the use of electronic identity", cf. chapter 6.4 above.

9 Conclusions and suggestions

This report does not aim at providing an overall solution on how to establish a legal framework for a pan European eID. The aim is to address relevant legal issues and discuss possible solutions with the Directive on Electronic Signatures as a central building block. The report is drafted with the aim at being used as a starting point for a discussion in the Porvoo Group on how to proceed in the work on the deployment of a functioning pan European eID. One should also be clear over the fact that that does not only lead to legal challenges, but also organizational, technical and economical challenges. However, other challenges than legal challenges have not been addressed in this report, but they do need to be addressed by the Porvoo Group in order to be able to present a complete plan on how to obtain the sought goal drafting a legal framework for a pan European eID.

My conclusions, reflections and suggestions can so far be summarized in the following way [50]:

1. As shown in this report entity authentication is to some extent covered by the regulation in the Directive on Electronic Signatures. In my opinion it is inter alia clear that a qualified certificate, as defined in the Directive, can be used for entity authentication only. In addition Article 5.2 in the Directive, ensuring that electronic signatures can not be denied legal effectiveness or denied as evidence, covers entity authentication.

2. Even if the Directive on Electronic Signatures covers entity authentication there are issues specific for entity authentication that are not regulated at all, or at least not sufficiently, in the Directive or in any other EEA relevant legal document. Some of these issues are addressed in Chapter 6 in this report.

3. Taking into account that many of the issues addressed in Chapter 6 probably are regulated in national law in all Member State for the handling of a visual ID, relevant also for an eID, and maybe explicitly for the handling of eIDs and that the EC Treaty Article 18.3 to some extent limits a coordinated legal framework for a pan European eID, it might be difficult to find a common understanding on requirements on a pan European eID.

4. We have a base to stand on through the Directive on Electronic Signatures. We should not “open up” the Directive for renegotiations, and make amendments specific for authentication. Trying to renegotiate the Directive could lead to a situation where “functioning” rules and regulation in the Directive will be amended or deleted. That is probably contra-productive for the Porvoo Group trying to achieve a coherent legal framework for a pan European eID. On top of that a re-negotiation of the Directive would take a long time, which would only slow down the process to achieve the Provoo Group’s goal.

[50] Opinions and conclusions in this report are my own and do not necessarily coincide with those of my employer’s.

Taking the above-mentioned statements into account my conclusions are the following:

A. Use the regulation in the Directive on Electronic Signatures as far as possible.

   The Directive on Electronic Signatures guarantees, within given limitations, an eID (an electronic signature used for entity authentication) legal effectiveness and legal admissibility. But is the regulation in Article 5.2 sufficient or do we also need a similar regulation as stated for handwritten signatures in Article 5.1? As a starting point the Porvoo Group should probably be satisfied with what can be interpreted pursuant to the Directive.

B. Take into use existing standards and promote the development of new standards for entity authentication, to support the use of eID.[51]

   Standards can provide a platform for eIDs within the EEA and facilitate the establishment of a policy on how to achieve interoperability. One should start with standards, take them into use, evaluate the result and then assess whether the standards should be used explicitly in a legal framework. By doing it in this order one would not get into the same predicaments as the Directive on Electronic Signatures has given us by trying to regulate an "immature" market.

   With the use of standards one is also more adapted to make necessary changes when new technologies emerges. An additional advantage of focusing on standards is that the use of standards is voluntary and thus it would probably not be in violation with the limitations set in Article 18 of the EC Treaty.

   Certification service providers (that can be a public or private entity) must have an incentive to start using these standards. In addition the standards must as far as possible comply with products already in use on the market (shelf products) so that they can be implemented swiftly and at a relatively low cost. The Electronic Signature Committee ("Article 9 Committee") should endorse relevant standards and have the EU Commission to approve and publish them.

C. Further evaluate the feasibility to use existing regulation for passport even if they at the present stage are founded on a paper-based document. This regulation might, mutatis mutandis, be a good

[51] Common Position (EC) No 12/2004 of 18 December 2003 adopted by the Council (IDABC), preambule no. 17 stating "it is essential to maximise the use of standards or public available specifications or open specifications for information exchange and service integration to ensure seamless interoperability and thereby increasing the benefits of pan-European eGovernment services and the underlying trans-European telematic networks."

building block for achieving a legal framework for a pan European eID.

The vision document from CEN/ISSS mentions that it is difficult to achieve a pan European eID given the fact that it involves 25 (+3) states and 450 million people. We do not have a pan European visual ID but the closest we get is the passport. Maybe we could use the passport, with its standing and the regulation around it, as a vehicle for a pan European eID. This is under the assumption that national passports from all Member States are accepted as valid IDs within the whole EEA.

The advantage of using existing regulation for passports, as a vehicle, is that many issues can be solved quite easily.

- Issuance – The regulation of issuance policies is probably covered by the limitations pursuant to Article 18 of the EC Treaty. This has inter alia been confirmed in the connection of drafting European common requirements on the use of biometrics in passports.[52] As far as I know every Member State have detailed procedures on how a passport shall be issued. These rules and regulations normally require personal appearance of the applicant and state what documents the applicant shall produce to prove his/hers identity. Thus accepting on a European level all Member States national regulation on issuance procedures for passports would solve this problem at the same time as it goes clear of the limitations in Article 18 of the EC Treaty. However, there is at least one problem with this solution and that is that even if the same national rules and regulations are applicable the trust given to the eID might not be on a par with a passport only due to the fact that it is a private and not a public entity that has applied these rules and regulations. Thus, the consequences of this solution could be that only public authorities can issue pan European eIDs.

  This is a consequence, which might not be unique for the requirements of issuance procedures, but might also apply to other issues in this list below where Member States passport regulations could be applied. Whether this is a consequence that can be accepted can be discussed. It would hamper the emerge of a market driven solution and could have negative effects on the situation in states where the most widely used visual ID is not issued by the state but by private entities. However, if we should accept several different levels of a pan-European eID, the lower level does not have to apply passport issuance procedures and policies but can very well accept “lower” requirements, and thus allowing private entities to at least offer such an eID on the

[52] Proposal for a Council Regulation on standards for security features and biometric in EU citizen’s passports, 18.2. 2004 (COM(2004) 116 final) 2004/0039.

market.

- Content – Also in relation to this issue there are detailed national (and international) regulation on what information shall be given in the passport and it is normally deemed enough to identify a person. However, there are no regulations that enable the holder to withhold some of the information when it is not relevant for the receiver or add additional requirements when that would be preferable.

- Data protection – This is probably an area where a solution can be found in standards and in agreements with the holder, based on the fact that this is already regulated in the Data Protection Directive and in the Directive on Electronic Signatures. The regulation in the Directive on Electronic Signatures on data protection applies to all types of certificates, not only qualified certificates.

- Liability – It is not sure that one needs additional liability rules on top of those given in the Directive on Electronic Signatures and existing tort laws etc. in all Member States. However, as mentioned above pecuniary compensation might not suffice in relation to the use of an eID, but that does not really make a difference whether the ID is visual or in electronic form.

- Revocation – The EU Commission has discussed the possibility of creating a centralised European register for issued passport.[53] The same or a similar register could also be used for a pan European eID.

- Interoperability – This is not dealt with in the world of passport, since they are not on a large scale in electronic form. There are ongoing processes on taking machine-readable passports into use, and those efforts could be a starting point for obtaining interoperability for eIDs. In addition it will be imperative to follow and participate in the work on interoperability being done by IDABC.

It should be noted that there are many areas related to the use of an electronic signature that are not regulated on a European level. In this report storage of information and criminal liability have been given as example of that. Another example that has not been mentioned in the report is the requirement of time

[53] Proposal for a Council Regulation on standards for security features and biometric in EU citizen's passports, 18.2. 2004 (COM(2004) 116 final) 2004/0039, Chapter 8 : "This register should then only include the fingerprint and the number of the travel document and no further personal data as its use should be limited to border controls in order to establish whether the travel document has been issued to the person present at the border in the first place. It goes without saying that such a development need to be further evaluated in order to assess the technical and legal implication …to examine the impact … on the fundamental rights of European citizens, and in particular the right to data protection."

stamping. Within these areas Member State's national laws will apply together with industry standards. This also means that from a legal point of view the situation will be the same disregarding whether the certificate / the electronic signature is used for signing (non-repudiation) or entity authentication (digital signature). One should bear this in mind when discussing the drafting of a regulatory framework for entity authentication. One should not, in an attempt to regulate this area, over regulate it.

10 Literature and references

Bryde Andersen, M., "Digitale dokumenters bevisværdi", IT-Sikkerhetsrådet, København, December, 1998.

Clarke, R., "Human Identification in Information Systems:
Management Challenges and Public Policy Issues", Published in Information Technology & People 7,4 (December 1994) 6-37.
http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html

Dumoriter, J., "The European Regulatory Framework for Electronic Signatures", EU Electronic Commerce Law, ed. Nielsen, Jacobsen and Trzaskowski, Djølf publishing, Denmark, 2004

EEMA Conference in Paris "Who are you who am I" (24 – 25 March 2004)

- Cameron, K. (Microsoft), "The Identity System"
- Hallis, R, "Identity Theft"

"Electronic Identity White Paper", v 1.0, June 2003, eEurope Smart Cards/Trailblazer 1 "Public Identity", ed. Ringwald, A..

"European Interoperability Framework for pan-European eGovernment Services", IDABC-EIF, European Commission, version 1.0 (http://europa.eu.int/idabc)

Kirchenberg, C et Olano, J.R., "Issues of Security and Interoperability in Electronic Public Procurement", Scandinavian Studies in Law, vol. 47 – IT Law, 2004, ed. Wahlgren, P Stockholm, Sweden, page 76

"The Legal and Market aspects of Electronic Signature – Legal and market aspects of the application of Directive 1999/93/EC and practical applications of electronic signatures in the Member States, the EEA, the Candidate and the Accession countries." Drafted by Jus Dumortier, Stefan Kelm, Hans Nilsson, Gerogira Skouma and Patrick Van Eecke. Service Contractract Nr. C 28.400

"Meeting on Electronic Identity Management for eGovernment – Meeting Report" - Meeting held at EC-DG INFSO-C6, Brussels, 27 January 2004
(http://europa.eu.int/information_society/programmes/egov_rd/doc/im_report.doc)

"Overall Roadmap 'Privacy and Identity Management", Final Report, Deliverable RD 3.0, IST-2001-38310, Ed. Huizenga, J. 21 August 2003
(http://europa.eu.int/information_society/programmes/egov_rd/doc/rapid_roadmap.doc)

"Principles for Electronic Authentication", Industry Canada, Cat. No. lu64-16/2004
http://strategis.ic.gc.ca/authen

"Technical contribution to the joint CEN TC224 WG15 – Porvoo Group e-Authentication Workshop – European Citizen Card Common Requirements", by Axalto to AFNOR July 6th 2004.

"Towards Understanding Identity – An examination of the fundamentals underlying the definitions and understanding of identity based on the assumption and experience known form the real-world in order to map them on to the requirements emerging form the digital world", produced by an EEMA Identity Technologies and Services Working Group, authors Bowden, Bramhall, Cameron, Cassassa-Mont, Colvill, Goodman, Hilton, Marhøfer, White, daft v0.35, 24 March 2004

CEN/ISSS – E-AUTH

- E-AUTH N0029 (2004-02-17) "Vision document on a common approach to Electronic ID for the European Citizen"
- E-AUTH N0010 (2003-10-21) "Revised Business Plan Draft V 1.4 October 2003"
- E-AUTH N0033 (2004-03-04) "CWA Part 2B: Best Practice Manual for card scheme operators exploiting mulit-application cards scheme incorporating an interoperable public eID"

CEN/ISS WS/eAuthenticaion Vision Document - "Towards an electronic ID for the European Citizen a strategic vision", Brussels, October 3, 2004

CEN/ISSS WS/E-Sign Area AB "Evidential Value of Electronic Signatures" Version 0.07 November 2003.

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering

Commission Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council

Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts

Communication from the Commission to the Council, the European Parliament, the European Central Bank, the Economic and Social Committee and Europol – "Preventing

fraud and counterfeiting of non-cash means of payment", 9 February 2001 (COM (2001) 11 final)

Proposal for a Council Regulation on standards for security features and biometric in EU citizen's passports, 18.2. 2004 (COM(2004) 116 final) 2004/0039

Common Position (EC) No 12/2004 of 18 December 2003 adopted by the Council, acting in accordance with the procedure referred to in Article 251 of the Treaty establishing the European Community, with a view to adopting a decision of the European Parliament and to the Council on interoperable delivery of pan-European eGovernment services to public administrations businesses and citizens (IDABC)

ETSI TS 101 456 – Policy requirements for certification authorities issuing qualified certificates (v.1.2.1 2002-04)

ETSI TS 101 733 – Electronic Signatures and Infrastructures (ESI); Electronic Signatures Formats (v. 1.4.0 2002-09)

ETSI TS 101 862 – Qualified Certificate Policy (v. 1.3.1 2004-03)

ETSI TS 102 042 – Policy requirements for certification authorities issuing public key certificates (v. 1.1.1 2002-04)

ETSI TS 102 280 – X.509 V. 3 Certificate Profile for Certificates Issued to Natural Persons (v.1.1.1 2004-03)