Towards harmonising Identrus with the European signature legislation

Ignacio Alamillo[1] · Detlef Hühnlein[2]

[1]agencia certificación electrónica S.A.
alamillo@ace.es

[2]secunet Security Networks AG
detlef.huehnlein@secunet.com

Abstract

This work aims at assisting the harmonisation process between the Identrus scheme and the European signature legislation. For this purpose, we will provide a gap analysis between the Identrus operating rules and the European signature legislation, i.e. the Directive [1999/93] and the corresponding national implementations of it, and discuss potential path towards harmonising these two worlds.

1 Introduction

The Identrus scheme, which is currently supported by 50 major international banks whereof more than half of them have Europe-based headquarters, provides a PKI-based trust infrastructure for global B2B e-commerce transactions. While the sophisticated, private law based, operating rules and minimum operational requirements ensure, that the certificates issued within the Identrus system provide a very high level of trust, and hence are very well suited for valuable e-commerce-transactions, these certificates currently do *not* meet the requirements of "qualified certificates" according to the European signature legislation. This implies, that signatures based on Identrus certificates can not replace hand-written signatures in general, and hence can not be used in electronic business processes, where (an equivalent of) a hand-written signature or the utilisation of qualified certificates is required by public law. A recent consequence of this fact is the absurd situation, that the customers of German Identrus participants may use Identrus certificates for Electronic Bill Presentment and Payment (EBPP), but need to issue additional cumulative paper-based bills to obtain admissible bills for claiming VAT-reductions. Similar problems (will) arise in many e-Government transactions across Europe, for which qualified certificates are required by public law.

Therefore it is important to investigate means for harmonising Identrus with the European signature legislation, such that (future) Identrus certificates will be considered to be qualified certificates across Europe. For this purpose we will provide a gap analysis, which highlights the (legal, political and technical) differences between Identrus Certificates[1] (IC) and Qualified Certificates (QC), as defined in the various European signature laws. Furthermore we will sketch potential paths which could lead to "Qualified Identrus Certificates".

This work is organised as follows: In section 2 we will analyse the gap between Identrus Certificates and Qualified Certificates. This analysis will consist of two phases. First we will highlight the differences due to European rules, like the European Directive on electronic signatures [1999/93] or the standards defined within the European Signature Standardisation Initiative [EESSI]. In a second phase, we will highlight the differences due to national signature laws. In section 3 we will sketch potential paths towards the harmonisation of Identrus with the European signature legislation. In section 4 we will compile the most important aspects of this contribution and draw conclusions for future steps.

2 Analysing the gap between Identity Certificates and Qualified Certificates

In this section we will highlight the differences between Identrus Certificates and Qualified Certificates in the sense of [1999/93].

2.1 Differences due to European rules

In this section we will highlight the differences between Identrus' rules and the European regulations, like the directive [1999/93] and standards developed in [EESSI]. These differences will appear in all national implementations of [1999/93] and hence should be addressed in harmonisation initiatives with high priority. In section 2.2 we will see however that there are additional differences, due to national signature laws, which would also need to be addressed.

To avoid misinterpretations of the present contribution it seems to be important to highlight a few general observations concerning the Identrus rules in the light of the directive [1999/93].

- The Identrus rules are "conform to" [1999/93]

  As the European Directive [1999/93] explicitly states in reason (16) of the motivation, that "a regulatory framework is not needed for electronic signatures exclusively used within systems, which are based on voluntary agreements under private law", such as Identrus, and Art. 5 (2) of [1999/93] requires that the legal effect of a signature may not be denied only because it is not based on a qualified certificate, it is clear that the Identrus rules are in a general sense "conform to" the directive [1999/93].

However it must be stated that

- Identrus Certificates are not Qualified Certificates in the sense of [1999/93]

  Among other differences, explained below, this is due to the banal fact that the IC, as defined in [IT-PKI], does not contain "an indication that the certificate is issued as qualified certificate", as required by [1999/93] Annex I (a).

-

[1] It should be noted, that there are various types of certificates defined in [IT-PKI] and used within the Identrus scheme. However, as we are only interested in one type of certificate, i.e. the "End-Entity Identity (Personal Signing) Certificate", we will use the term "Identrus Certificate" or "IC" as abbreviation for "End-Entity Identity (Personal Signing) Certificate".

We will see in the following that a naive approach to replace the IC-profile in [IT-PKI] by a profile based on [TS101862], which in turn is based on [RFC3039], would be necessary, but not sufficient. We refer to Section 3 for potential path towards harmonising Identrus with the European signature laws.

Such additional aspects, which demand harmonisation are as follows:

- Different sets for admissible certificate holders

  While a certificate, as defined in Art. 2 (9) of [1999/93] is linked to a person, Identrus (in Section 3, Paragraph 1 of [IL-OPRUL]) only permits to issue certificates to non-consumer entities, whereas the holder of the certificate can either be a natural person or an organisational entity, acting on behalf of a company for example.
- Identrus does not make certificate status information publicly available

  The status information within the Identrus scheme is communicated using the OCSP protocol. However this service is only available for “Relying Customers”, i.e. entities within the closed user group. In fact, requirement R13 in section 2.3 of [IT-DSMS] states that “all OCSP requests must be signed by the Relying Customer’s signing key”.

  On the other hand, section 7.3.5 of [TS100456] states that the certification service provider (CSP) shall ensure that certificates are made available as necessary to subscribers, subjects and relying parties. For certificates issued to the public2, this obviously implies that the certificate status information needs to be publicly available.
- Different points of emphasis for liability

  Art. 6 of [1999/93] states that the CSP shall at a minimum be liable for damage caused to any entity who reasonably relies on the certificate. As stated in Annex A (I. A.) of [TS100456], Art. 6 requires a CSP issuing qualified certificates to the public to ensure:

  - the accuracy of the information contained in the certificate at the time of issuance;
  - that the certificate contains all information required for a qualified certificate at the time of issuance;
  - that the signatory holds the signature-creation data corresponding to the signature-verification data identified in the certificate;
  - that the signature-creation data and signature-verification data work together where the CA generated both of them; and
  - that it registers any revocation of the certificate.

  On the other hand, section 3, par. 15 (4) of [IL-OPRUL] states that damages below US$ 5000 shall not be recovered at all and introduces a monetary limit (US$ 100 Million per calendar year) on the total liability for the participant3. The detailed liability of the par-

•

[2] While [1999/93] does not exclude the possibility that qualified certificates are not issued to the public, it seems that most national implementations of [1999/93] implicitly assume that qualified certificates are issued to the public. Thus for harmonising Identrus with these laws, one would need to introduce the concept of qualified signatures *not* issued to the public in these national signature laws; we will return to this point in section 3.1.

[3] There are similar rules for Identrus’ liability in section 4, par. 9 of [IL-OPRUL].

ticipant and the recourse of a relying party are regulated by suitable customer agreements, as governed by [IL-RTCARC].

Thus, while [1999/93] focuses on a minimum amount of liability for the CSP, [IL-OPRUL] in turn governs the maximum liability. The consequence is that systems which are compliant to current Identrus rules are not automatically satisfying the liability requirements of [1999/93], but it seems to be possible to design a system such that both requirements are met.

In a similar fashion there are many (minor) differences in the requirements of Identrus and the various European signature laws. However it seems that these differences do not represent insurmountable obstacles in the sense that it is possible to design systems, which both meet the requirements of Identrus *and* the respective signature law(s).

2.2 Differences due to national signature laws

In this section we will highlight the differences between Identrus and the national signature laws. While we will content ourselves to a treatment of the German legislation here, the full version of this paper will cover all countries in the European Community and other relevant countries, such as Switzerland for example. As these differences stem from the transposition of [1999/93] into national law, we will refer to [Dumo01] and [Keus02] for recent surveys on this topic.

The main differences in the rules stipulated by Identrus and the German signature legislation, mainly consisting of the law [Ger-SigG] and the corresponding signature decree [Ger-SigV], are as follows:

- Security concept

  According to §4 (2) [Ger-SigG] the CSP is required to present a comprehensive security concept to the appropriate authority, which shows that the security requirements laid down in [Ger-SigG] and [Ger-SigV] are met. The minimum content of this security concept is defined in §2 [Ger-SigV]. While [IL-OPRUL] and [IO-MOR] also contain some security related requirements, which must be fulfilled, most security specific regulations only appear as recommendations in [IO-CCAG].

- Liability / Coverage of at least DM 500 000 per incident

  §11 [Ger-SigG], which governs the liability of the CSP, exceeds the minimum requirements of [1999/93]. The CSP is also liable for damages, which are caused by malfunctions of the products for electronic signatures, which are used and supplied by the CSP. By §12 [Ger-SigG], the CSP needs to provide a minimum coverage of at least DM 500 000 per incident.

- Voluntary accreditation process is more stringent

  To obtain the voluntary accreditation, as defined in §15 (1) [Ger-SigG], the effectiveness and the implementation of the security measures, laid down in the security concept, will be comprehensively evaluated and certified. This process is by far more stringent than the WebTrust-like external system audit required by Identrus. For products for electronic signatures, there is a similar accreditation process covered by §15 (7), which consists of the product evaluation - according to ITSEC or CC - and the subsequent certification by the appropriate authority.

- No suspension in SigG

  While certificates in Identrus may be temporarily suspended, there is no such concept in the German signature legislation. Furthermore, §15 (3) [Ger-SigV] states that the technical components need to guarantee that "the revocation of a qualified certificate can not be undone without notice". By defining "suspension" as "temporary revocation", one might argue, that this statement implies that the suspension of a certificate would explicitly violate the requirements of [Ger-SigV].

- Different technical compliance requirements

  There are some differences concerning the compliance requirements for components used by the CSP, or the end-entity. In contrary to the Identrus requirements for HSMs, laid down in [IT-HSMCR], which allow an FIPS 140-1 (level 2 or level 3) evaluation and certification, appendix 1 of [Ger-SigV], which further specifies the requirements of §11 (3) and §15 (5) [Ger-SigV], only asks for ITSEC or CC evaluations.

  Another example, where the requirements slightly vary can be found in section 1.25.4 of [IO-MOR]. This section states that the used OCSP-responder "must meet, or is capable of meeting" ITSEC E24 … , while appendix 1 of [Ger-SigV] requires that this component must meet ITSEC E2 (with strength of mechanisms "high"), if the component is applied within a secure area, or even ITSEC E3 otherwise.

This (preliminary) analysis tends to indicate, that apart from the general differences between the Identrus rules and [1999/93] outlined above, the requirements formulated in the German signature act do not impose additional problems for the harmonisation of Identrus with [Ger-SigG]. Thus, if the problems listed in section 2.1 would be solved, it would be possible to design systems which satisfy *both* the requirements of Identrus and [Ger-SigG] and hence it would be possible to issue Qualified Identity Certificates in Germany.

3 Potential paths for closing the gap

In this section we will sketch different path for closing the gap between Identrus and the European signature legislation, in the sense that Identrus certificates can be applied for business processes, for which qualified certificates are required by law. In section 3.1 we will present four approaches for closing the gap between Identrus and the European signature laws.

3.1 Some approaches for closing the gap

In the following we will sketch four approaches for closing the gap between Identrus and the European signature legislation:

1. **Update all laws which require handwritten signatures or qualified certificates**

   Theoretically one could face the problem by attempting to change all national laws such that all requirements for handwritten signatures, and hence the application of qualified certificates, would disappear.

   While there are countries, like the United Kingdom or Scandinavian countries, with very few such requirements, this approach would certainly not be feasible for countries like

•

[4] or equivalent criteria, such as CC EAL3 or TCSEC C2

Germany, where there are hundreds of business processes which require the application of handwritten signatures or documents. Note that it is the latter requirement, which requires the application of Qualified Certificates for producing invoices in Germany – a conventional invoice does not need to be signed, but it is a document which needs to be made unique.

2. **Align signature legislation with Identrus rules**

   Another theoretical approach would be to use the review of the directive, as foreseen by Art. 12 of [1999/93], to align the signature legislation with the Identrus rules, as they are today. As above, this approach does not seem to be feasible at all.

3. **Accept Identrus Certificates as being equivalent to Qualified Certificates**

   One could aim at a general equivalence between Identrus Certificates, as they are specified today, and Qualified Certificates. This might be possible by applying Art. 7 of [1999/93], which governs international aspects of electronic signatures.

   However this approach is afflicted with general legal, technical and last but not least political challenges.

   The first point is that Art. 7 of [1999/93] seems to apply only for CSPs in third countries. This means that one could aim at putting through a general agreement that Identrus Certificates, which are produced by CSPs outside the European Community, are considered to be equivalent to Qualified Certificates. It is at least questionable, whether such an agreement could also cover Identrus Participants within Europe. Even if it would be possible to apply Art. 7 also for CSPs within Europe, by using the fact that Identrus LLC is based in the United States, one would need to make clear that the obvious differences in the technical and organisational requirements do not impact the general level of trust. An interesting approach could be to apply Art. 7 1. (b), where a CSP, which fulfils the requirements of the directive, guarantees for the Identrus Certificate. In some cases, the CSP which issues the Identrus certificate would be identical to the CSP which guarantees for it.

   In the opinion of the present author, it would be a major political task to put through such an agreement. It is highly questionable, whether such an approach could be successful.

4. **Align Identrus rules with signature legislation**

   Another approach would be to align the Identrus rules with the European signature legislation. This would not necessarily imply a major revision of the Identrus rules, but could be implemented by suitable extensions. Such an extension would at least need to cover the following aspects:

   - Specification of a certificate profile for “Qualified Identity Certificates”

     This profile should be compliant with [TS101862], such that the requirements of [1999/93] are covered and the interoperability with other systems using qualified certificates is guaranteed. It need to be investigated more thoroughly, whether it would be preferrable to replace the current IC-profile or to issue an additional certificate profile for Qualified Identity Certificates.

   - Update crucial aspects of the Identrus rules (for this type of certificate)

Here one would need to face the crucial differences between the Identrus rules and the signature legislation, as discussed in section 2.1. This would potentially include a removal of the liability caps, an update of the set of admissible certificate subjects and changes to the Identrus rules, which reflect the fact that certificates are not only used within a closed user group, but issued to the public.

It should be noted that the directive and the standards developed by EESSI do not exclude the possibility that one issues certificates not to the public, but for the use within a closed user group. However it seems that this concept has not been developed any further than the mere references in [1999/93] and [TS100456].

To avoid changes to the liability rules and the certificate and certificate status dissemination strategy in Identrus, one would need to develop a special qualified certificate policy for this case and introduce this possibility in all national signature laws. While the definition of a respective certificate policy is easy, it would be a major political task to put through such changes in all European signature laws. Thus this approach would be easier to implement, if Identrus decides to issue these Qualified Certificates to the public.

- Provide a reference to the requirements stipulated by the respective signature laws

  Finally one would need to provide additional references in the Identrus rules to the applicable requirements from the national signature laws. As the preliminary gap analysis with respect to the German signature legislation in section **Fehler! Verweisquelle konnte nicht gefunden werden.** tends to indicate, it seems to be possible to design systems which fulfil both the requirements by Identrus and the European signature laws.

3.2 Preliminary assessment of the approaches

As the brief discussion in section 3.1 indicates, there seem to be two promising approaches for closing the gap between Identrus and the signature laws. The first, highly political, approach would be to figure out, whether Identrus certificates could be accepted as qualified certificates across Europe. If this is not possible for legal or political reasons, one would need to introduce some changes to Identrus operating rules, as sketched above. In the opinion of the present author it seems to be most promising to investigate the latter approach more closely.

4 Conclusion

In this paper we provided a preliminary[5] gap analysis between Identrus and the European signature legislation and sketched potential paths towards a harmonisation. The preliminary results tend to indicate, that apart from some general differences (certificate profile, liability, certificate (status) dissemination) which would demand changes in the Identrus rules, it seems to be possible to design systems which meet both the requirements by Identrus and the signature laws.

•

[5] After analysing the other European signature laws in the full paper, our conclusion will be based on more solid ground.

Thus it seems that a harmonisation would be possible with moderate changes and without lengthy political interventions. Now it is up to Identrus to take this chance to create "Qualified Identity Certificates" – qualified certificates with global acceptance. This could be a major step towards a truly widespread global trust infrastructure.

Literature

[EESSI] *ESSI - The European Electronic Signature Standardization Initiative – homepage*, at http://www.ict.etsi.org/eessi/EESSI-homepage.htm

[Dumo01] Dumortier, J.: *Overview of the European Electronic Signatures Directive and its transposition in the Member States*, talk at EEMA workshop "The Legal Impact of the Electronic Signatures Directive on Business", November 29th – 30th, 2001

[TS100456] ETSI: *Policy requirements for certification authorities issuing qualified certificates*, TS 100 456, (draft of) version 1.1.2, via [EESSI]

[TS101862] ETSI: *Qualified certificate profile*, TS 101 862 V1.2.1 (2001-06), via [EESSI]

[1999/93] European Parliament and Council: *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*, OJL, 19.1.2000, p.12, e.g. via [EESSI]

[Ger-SigG] Germany: *German Signature Law* (*"Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften")*, enacted on May 22nd , 2001, via http://www.regtp.de

[Ger-SigV] Germany: *German Signature Decree* (*"Verordnung zur elektronischen Signatur"*, enacted on November 22nd, 2001, via http://www.regtp.de

[IL-OPRUL] Identrus LLC: *Identrus Operating Rules*, Version 1.7 of February 27th, 2001

[IL-RTCARC] Identrus LLC: *Identrus Required Terms for Customer Agreements (Relying Customer)*, Version 1.7 of January 24th, 2000

[IO-CCAG] Identrus LLC: *Identrus Compliance and Controls Assessment Guidelines for Level One Participants*, Version 1.7 of March 1st, 2001

[IO-MOR] Identrus LLC: *Identrus Minimum Operational Requirements*, Version 1.7 of February 28th, 2001

[IT-DSMS] Identrus LLC: *Identrus Digital Signature Messaging System Specifications*, Version 2.0a of November 6th, 2000

[IT-HSMCR] Identrus LLC: *Identrus Hardware Security Module Compliance Requirements*, Version 4.7b of November 30th, 2000

[IT-PKI] Identrus LLC: *Identrus Public Key Infrastructure and Certificate Profiles*, Version 4.7 of March, 27th, 2001

[Keus02] Keus, K.: *The transposition of the EU-Directive for electronic signatures in the European countries – an analysis and first assessment*, (in German), to appear, 2002

[RFC3039] RFC 3039: *Internet X.509 Public Key Infrastructure - Qualified Certificates Profile*, via http://www.ietf.org