A NEW APPROACH TO IMPROVING THE INTEROPERABILITY OF ELECTRONIC SIGNATURES IN CROSS-BORDER LEGAL TRANSACTIONS

Ugo Bechini[*]
Dominik Gassen[**]

I. Introduction

Electronic Signatures have become an integral part of many online legal procedures and electronic transactions that require more security than run-of-the-mill e-commerce. For example, many electronic legal

[*] Dr. Ugo Bechini (www.bechini.net) is a Civil Law Notary in Genoa, Italy, member of the Faculty of the Genoa State University Law School, President of the Comité Francoitalien du Notariat (Genoa/Marseilles) and author of essays on IT law, family law and contract law. He chairs the New Technology Committee of CNUE (Council of Notariats of the European Union, Brussels) and lectures on a regular basis on IT law topics.

[**] Dr. Dominik Gassen is a Civil Law Notary in Bonn, Germany. After completing a doctoral thesis about legal aspects of electronic signatures, he has worked for several years as an expert on e-government matters for the German chamber of notaries (Bundesnotarkammer), liaising with government entities and developing software solutions. He chairs the electronic signature interoperability project at CNUE, discussed in this article.

transactions, such court filings, have come to rely on this technology. With growing interest and increasingly higher stakes, new questions are emerging regarding the use of electronic signatures, particularly concerning the technical, practical, and legal obstacles to using signatures for cross-border transactions. This article provides an overview of existing problems and reports on a new solution that has been developed by civil law notaries (CLNs) in Europe.

II. Electronic Signatures Under the EU

The legal framework for electronic signatures in the European Union is based on Directive 93/1999.[1] The Directive defines electronic signatures as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication."[2] Article 2(2) of the Directive requires that an *advanced electronic signature* comply with the following requirements:

> – it is uniquely linked to the signatory;
>
> – it is capable of identifying the signatory;
>
> – it is created using means that the signatory can maintain under his sole control;
> and
>
> – it is linked to the data to which it relates in such a manner that any subsequent
> change of the data is detectable.[3]Article 5(1) requires that advanced electronic signatures, which are based on a qualified certificate and created by a secure signature-creation device:
>
> (a) satisfy the legal requirements of a signature in relation to data in electronic

[1] Council Directive 93/1999/EC of the European Parliament and of the Council on a Community Framework for Electronic Signatures, 1999 O.J. (L 13) 12–20. For a useful overview of the Directive, see Francisco Javier, Comercio y firma electrónicos 37 (2d. ed. 2004). European Union Directives are binding, as to the result to be achieved upon each Member State to whom they are addressed. National authorities are left the choice of the form and methods to achieve their objectives. Nevertheless, Council Directives are often quite detailed, as it is in our case.

[2] Council Directive 93/1999, *supra* note 1, art. 2.

[3] *Id.* art. 2(2).

> 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.

And Article 5(2) requires Member States to

> ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on grounds that it is:
>
> – in electronic form, or
>
> – not based upon a qualified certificate,[4] or
>
> – not based upon a qualified certificate issued by an accredited certification-service-provider,[5] or
>
> – not created by a secure signature-creation device.[6]

Basically, this means that any electronic signature generated within the EU, whatever its intrinsic reliability,[7] must be granted some degree of legal enforceability by each EU Member State.[8]

[4] *Id.* Annex I.

[5] *Id.* art. 2(13).

[6] *Id.* Annex III(1). Moreover, secure signature-creation devices "must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process." *Id.* Annex III(2).

[7] Even a cellphone text message (SMS) qualifies. STEPHEN MASON, ELECTRONIC SIGNATURES IN LAW 101 (2003). It is difficult to deny that such messages match the European Directive's definition: they are indeed "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication." EU Directive 93/1999, *supra* note 1, art. 2(1).

[8] Although each EU Member State is required to recognize digital signatures, the implementation of Directive 93/1999 has created a variety of national legal flavors.

III. Civil Law Notaries and Electronic Signatures

Civil Law Notaries around Europe were among the early adopters of the new electronic signature technology. The reason is quite simple: CLNs are the one stop shop for real estate conveyances, estate planning, contract drafting, business transactions, and powers of attorney in most of Europe.[9] The buyer of a home, for example, typically signs the deed in the CLN's office, and it is up to the CLN to collect the taxes, have the sale registered, and to make sure that all mortgage payments are made when due. During this process, CLNs generate a huge amount of data that is later entered into variety of public registers, thereby building a foundation for transactions based on increased public trust, resulting in increased security, lower insurance costs, and less litigation. The electronic provision and transmission of this data is an option that is increasingly used and obviously advantageous for many reasons. In this context, electronic signatures have become an essential tool for the authentication of documents in these transactions.[10]

While massive data transfer is the primary advantage of CLNs adopting a digital notary system, digitally notarized documents have other benefits as well. For example, in France, deeds can be notarized in real time even if the parties are in two different cities, provided that videoconferencing is available and a CLN is present at both locations. Additionally, powers of attorney can be sent from one location to another in real time.[11] European CLNs also routinely

[9] *See* Consiglio Nazionale del Notario [Official Site of Italian Notaries], http://www.notariato.it/ portal/site/notariato (last visited Feb. 20, 2009) (providing a brief description of the job of Civil Law Notaries). About 55% of the world population lives in countries where Civil Law Notaries, instead of Notaries Public, operate. Pedro A. Malavet, *The Non-Adversarial, Extra-Judicial Search for Legality and Truth: Foreign Notarial Transactions as an Inexpensive and Reliable Model for a Market-Driven System of Informed Contracting and Fact-Determination*, 16 Wis. Int'l L.J. 1 (1997–1998).

[10] *See Generally* Ugo Bechini and Michele Nastri, Italian Nat'l Report to the 2004 Congress of the Unión Internazionale du Notariato [International Union of Notaries] in Mexico City: The Role of the Civil Law Notary in Electronic Contracts, abstract *available at* http://xoomer.virgilio.it/ubechini/demo/. *See also,* Sabrina Chibbaro, Presentation at the Third International Forum on Digital Evidence: Usage of Information and Communications Technology in Real Estate Conveyancing: Italian Experience (Los Angeles 2007), powerpoint presentation *available at* http://www.nationalnotary.org/intlforum/pdf/ Forum_3_Chibbaro.pdf.

[11] This is very interesting from an international perspective, and there is some irony in the present situation. Notarial deeds can be sent over the internet to local branches of state agencies that are sometimes located only a few hundred yards away, while paper forms are

certify the powers of company directors and executives. The benefit of using a CLN for these transactions is that electronic certifications can be made available in real time anywhere, and digital signatures can make them even more reliable than their paper equivalents.

Early on, CLNs caught on to the importance of using electronic signatures as a way to increase the trust in electronic communication to a level that approaches paper-based notarial deeds.[12] Investments were made in the necessary infrastructure, and soon smart cards were a familiar sight in notary offices all over Europe.[13] In line with professional traditions, notarial organizations around Europe chose the most advanced and secure technology: in Eurolegal jargon, *advanced electronic signatures based on a qualified certificate*.[14] The encryption technology that is used to generate and authenticate these electronic signatures is administered by entities known as Certification Authorities,[15] which are also responsible for issuing smart cards.[16]

The verification of electronic signatures is a well-established process. Using the relevant data provided online in real time by the Certification Authorities, the user of an electronic signature verification system can easily and reliably ascertain (a) who signed the document, and (b) that the document was not tampered with after the signature was performed—or at least this is the way it is supposed to work. In reality, however, there are some problems with the system that can diminish the reliability of electronic signatures. For example, electronic signatures do not really provide any evidence that the document was signed by John Doe. An electronic signature only proves that the data in question was signed using a device (usually a smart card) that was delivered to a person that had been previously

required for documents that will travel across oceans.

[12] *See* MARIO MICCOLI, DOCUMENTO E COMMERCIO TELEMATICO (1998).

[13] The National Reports to the 2004 World Congress of International Union of Notaries in Mexico City (on file with author) provide valuable information, especially those from France, Germany, Italy, Spain, and the Netherlands. *See also* Bernard Reynis & Ugo Bechini, *European Civil Law Notaries ready to launch international digital deeds*, 4 DIGITAL EVIDENCE J. 12, n. 1 (2007) (on file with author).

[14] Digital signature technology is based on asymetric cryptography and a Public Key Infrastructure (PKI). *See* WARWICK FORD & MICHAEL S. BAUM, SECURE ELECTRONIC COMMERCE 49, 101–14 (2001).

[15] Some of the functions performed by the Certification Authority can be sometimes carried out by a separate organization, called a Registration Authority. *Id*. at 191–92.

[16] A smart card is a special card used to create electronic signatures that is carried by notaries or others and that identifies the person and verifies he or she is registered with the Certification Authority.

identified by the Certification Authority as John Doe.[17] Therefore, electronic signature technology, despite its rock-solid mathematical and technical foundations, still remains heavily dependent on the human factor. If a smart card, for instance, is handed over to the wrong person,[18] or if the legitimate owner loses control of the card, voluntarily or as a consequence of violence or fraud, the verification process will still result in a technical confirmation of the authenticity of a document, even though it does not actually originate from the apparent signer.[19] For these reasons, electronically signed documents

[17] *See* Jane K. Winn, *The Emperor's New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce*, 37 Idaho L. Rev. 353, 366 (2001):

> There are several obvious problems posed by trying to tie the identity described in a digital signature certificate to an actual person with the intention of binding the party thus identified to the content of an electronic record. Among these are:
>
> – whether the token/smart card has been deliverd to the right person;
>
> – whether the authorized person has used the token with the private key when performing the signature;
>
> – and if a person other than the identified person has used the digital signature, how that person was able to gain access without authorization and who should bear responsibility for that unauthorized access.
>
> The breach in security may occur at the level of the end user's failure to take reasonable steps to safeguard access to a private key, or it may occur because the software and hardware used to store the private key have not been made reasonably secure. It may even stem from an uninformed attempt of the authorized user to delegate an inconvenient procedure. Before a digital signature can be presumed to be as valuable as a traditional handwritten signature, the behavior, attitudes and sophistication of individuals using the technology will have to be analyzed as well as the security characteristics of the entire system within which an individual digital signature is used.

[18] On Jan. 29 and 30, 2001, VeriSign, a Californian Certification Authority and worldwide leader in the industry, issued two digital certificates to an individual who fraudulently claimed to be a representative of Microsoft Corporation. According to Verisign's own website:

> [T]he certificates were VeriSign Class 3 Software Publisher certificates and could be used to sign executable content under the name "Microsoft Corporation." The risk associated with these certificates is that the fraudulent party could produce digitally signed code and appear to be Microsoft Corporation. In this scenario, it is possible that the fraudulent party could create a destructive program or ActiveX control, then sign it using either certificate and host it on a Web site or distribute it to other Web sites.

Jan. 2001 – Advisory from VeriSign, Inc., http://www.verisign.com/support/advisories/authenticode fraud.html.

[19] According to Stephen Mason, "no form of electronic signature is capable of linking the use of a signature to a particular person. Unless the sending party confirms they sent the message or document with the signature attached, the recipient cannot determine whether the sending party authorized the use of the signature." Mason, *supra* note 8, at 348.

coming from the general public are widely regarded as less reliable than documents notorized by a CLN.[20]

How do electronic documents that have been signed by notaries fit into this picture? Each CLN is required by the European Code of Notarial Professional Ethics to adopt specific measures in order to prevent any security breach.[21] While these requirements, in concert with the level of protection provided by electronic signature technology, help to ensure the reliability of the CLNs, they do not solve the question of reliability of the Certification Authority that has issued the notary's signature card. Moreover, even if the personal identity of the notary is securely established, can it be assumed that he is in fact a CLN currently in office? In other words, how can one be certain that a document received via e-mail (e.g., a power of attorney) really is a *notarized* document and can be used as such in a different jurisdiction?

Notarial organizations all over Europe use different approaches to address these issues. Italy was the first European country to create such an infrastructure, choosing a relatively simple system known as the Flat Certification Authority (FCA): a dedicated Certification Authority, owned by Italian notaries, which accepts as customers only CLNs that are currently in office.[22] Certificates issued to notaries by the FCA can be used for official business only. And if a CLN loses his or her license for any reason, the President of the local Notarial Chamber revokes his certificate immediately. In other countries, such as France, CLNs control their own Certification Authority as well, but the Certification Authority delivers certificates to both CLNs and other officers who are not CLNs.[23] Throughout the EU, strict

[20] "Digitally signed documents do not achieve the same assurances of genuineness that documents signed in the personal presence of a notary achieve, and should not be given the same legal status." Brad Biddle, *Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure*, 33 SAN DIEGO L. REV. 1143, 1182 (1996).

[21] Notaries must strictly ensure that they are the only ones who use their signature devices at any time, to immediately inform the agency or system if it is lost, and to inform the system of any event that may endanger the security of the system. Council of Notoriats of the European Union (CNUE), Code of Professional Ethics, ¶ 1.2.9, *available at* http://www.cnue-nouvelles.be/en/002/003.html (last visited March 4, 2009).

[22] CONSIGLIO NAZIONALE DEL NOTARIATO, QUALIFIED CERTIFICATION AUTHORITY CERTIFICATION PRACTICE STATEMENT, VERSION 1.0, § 3.3, at 34, *available at* http://ca.notariato.it/documentazione/CPSCNN.PDF.

[23] CONSEIL SUPÉRIEUR DU NOTARIAT, POLITIQUE DE CERTIFICATION POUR LES CERTIFICATS DE CLASS 0 ET 4 ÉMIS PAR L'AUTORITÉ DE CERTIFICATION NOTAIRES ¶ 2.3.5 (May 30, 2007), http://www.preuve-electronique.org (follow "Autorité de certification Notaires" hyperlink; then follow

procedures have been put in place in order to ensure that the smart card is safely delivered to the CLN.[24]

IV. Core Problems of Electronic Signature Verification

Every time an electronic signature is used in a transaction that has any legal relevance, the verification process, as outlined above, is a necessary component in establishing the reliability of the document. But without a technical examination of the document, the recipient of a digitally signed document cannot determine that the data has not been tampered with, and without controlling the signature certification process, the recipient cannot be certain of the identity of the signer. For this reason, electronically signed documents must be heavily scrutinized to ensure their reliability. German and Italian companies registers, for instance, automatically scrutinize any such documents as soon as they are received on the entry server.[25] If any part of the signature verification fails, the document is rejected.[26] This level of scrutiny means that the inexperienced user of electronic signature software will quickly run into problems.

A. Electronic Signature Verification Software

On a technical level, electronic signature verification software is regularly included as an annex feature to the program that is used to generate the signature. Early applications in the market mostly concentrated on verifying the application's own signatures. That part usually worked well enough. But if one tried to verify a signature that had been generated with another signature app, even when it was based on the same certificate, errors occurred quite regularly. Even

"Politique de Certification" hyperlink).

[24] For example, in Italy, this duty can only be performed by the President of the local Notarial Chamber, who personally knows each of the CLNs in his jurisdiction. Consiglio Nazionale del Notariato, *supra* note 22, § 4.4, at 37.

[25] Dominik Gassen & Stefan Wegerhoff, Elektronische Beglaubigung und elektronische Handelsregisteranmeldung in der Praxis, 228 (2007) (on file with author). Automatic verification procedures soon caused technical difficulties in Germany when for every signature verification, every certificate (whether originating from an individual user, a certification service provider, or from the governmental) had to be verified online. The result was an unexpected massive increase of traffic on the directory servers. *Id.*

[26] Under German law, electronic signatures rated below *qualified* are not admissible in legal proceedings. *See* Beurkundungsgesetz [BeurkG] [German Notorial Act], Aug. 28, 1969, BGBI. I at 1513, §§ 12–39.

seasoned users were often surprised by this. For a significant period of time, there had been numerous standards for various aspects of signature technology,[27] and software developers claimed to be adhering to them. Still, there seemed to be confusion of Babylonian proportions even among products in common national markets. This turned out to be a big obstacle limiting the use of electronic signature technology.[28] The root of the problem was that existing standards still allowed too much leeway for divergent technical interpretations that, lacking suitable supervisory bodies, produced negative results.

This situation improved somewhat with the second generation of electronic signature apps.[29] Common standards interpretations that were agreed upon by groups of software developers helped reduce variations that were causing the aforementioned problems.[30] Regrettably, there is still no standard that has achieved significant international recognition.[31] Thus, interoperability still remains a difficult problem among EU Member States.

B. Smart Cards

A lack of interoperability can also be found among the smart cards used to generate electronic signatures.[32] For example, many apps have problems displaying content in different languages. Character encoding may be faulty or lacking, and language-specific characters

[27] *See, e.g.*, BSI (German Federal Office for Information Security), Standards, http://www.bsi.de/esig/standards.htm (last visited Apr. 11, 2009). There are also Public Key Cryptography Standards (PKCS) that cover a large variety of aspects. *See, e.g.*, RSA Laboratories, http://www.rsa.com/rsalabs/node.asp?id=2124 (last visited Mar. 2, 2009).

[28] A good example for this is the situation in Germany and Italy after the first signature laws came into effect 1997. *See generally*, Stefek Zaba, *Digital Signature Legislation: The First 10 years*, 11 INFO. SECURITY TECHNICAL REP. 18 (2006).

[29] The second generation of electronic signature apps relied primarily on Public Key

[30] One example is the specification Common-PKI (formerly ISIS/MTT) that has been developed in Germany and resulted in a markedly improved interoperability among German Certification Service Providers (CSPs). *See* Common-PKI Specification 2.0, http://www.common-pki.org/index.php?id=567&L=1 (last visited Apr. 11, 2009).

[31] Even Microsoft failed to achieve a moderating influence on this market. Usually the sheer market share of its products would foster the establishment of the standards used therein. But with electronic signatures, Microsoft chose to focus solely on the U.S. market. European CSPs found that their smart card based products—while completely compliant with EU and EU Member State legislation—could not be recognized by Windows signature and verification procedures.

[32] Smart cards vary significantly in their technical specifications and security performance. *See* Smart Card Alliance, http://www.smartcardalliance.org/member (last visited Apr. 12, 2009).

may not be displayed correctly. This is common with German umlauts as well as special characters widely used in eastern european languages. Users may become confused when characters are translated into an incomprehensible textual mess.

Additionally, there may be uncertainty as to the reliability of the certification service—specifically concerning the process used to ascertain the identity of the person applying for a smart card. Methods range from the simple—Certification Service Provider (CSP) regards identification as valid if payment is made by credit card which has been issued to a person with a corresponding name—to highly secure—CSP will only issue certificates if the applicant's signature has been notarized, and the smart card bearing the certificate will only be delivered to the applicant in person. Information regarding the certification process the CSP employs is vital in determining the degree to which a recipient can and will trust the signer's identity.

Finally, electronic legal proceedings frequently require additional information apart from the signer's identity: the signer's role in the transaction, his professional position, and his professional qualifications may also be significant. Sometimes a person's personal identity is secondary to that person's professional identity and his role in regards to the transaction. This is quite obvious, for example, with any person who holds public office or represents a government agency. The special qualities that are attributed to a civil law notary's public documents stem from his position as bearer of a public office, not from his personal identity. Even outside of public transactions, a person's position can be important, e.g., a person holding power of attorney. Certificates that contain this type of information can provide an added level of security to electronic transactions.

There are several technical methods for conveying additional personal information in a certificate. It can be integrated into the personal certificate or reproduced in a separate *attribute* certificate. Some CSPs will offer special certificates only to a specific group of applicants.

Regrettably, standards for this specialized type of certificate are incredibly fragmented. As with standards for electronic signature formats, it is common that there are variations even among the CSPs in one country, and especially in larger countries where the market for certification services is more developed. Cross-border comparisons of standards are even more fragmented. Different languages and legal traditions create even more uncertainties as similar-sounding professional descriptions and official designations do not necessarily imply comparable functions or competencies.

C. Timestamps

One area of signature technology that might be the hardest to understand for the average user is *timestamping*. Signatures contain data on the time and date that they were performed.[33] This information can be easily tampered with because time and date are taken from the generating computer's internal system clock. Because of this, there is a security gap that can be used to generate seemingly valid signatures with compromised, expired, or revoked certificates. There are various approaches to address this situation. Some jurisdictions (e.g., Italy) reject out of hand any signature that is based on a certificate that has expired or been revoked at the time of verification because it is deemed untrustworthy.[34] Other jurisdictions (e.g., Germany) assume a slow loss of security over time, but generally assume signatures are valid.[35]

A third solution is to affix an additional secure time stamp to the signature information. This replaces the insecure system date with the time information of a trusted internet time server. Again, the lack of common standards and the various technical solutions available in the market complicate the verification of timestamped signatures.

D. Summary

For inexperienced end users, as well as more experienced users, the existing technical and legal situation is obscure, approaching impenetrable. For this reason, the use of electronic signatures in cross-border transactions is severely limited. If the recipient of the

[33] Timestamps can be integrated into signature files or constructed as separate files.

[34] RAIMONDO ZAGAMI, FIRMA DIGITALE E SICUREZZA GIURIDICA 214 (2000).

[35] Alexander Roßnagel et al., *Erneuerung elektronischer Signaturen—Grundfragen der Archivierung elektronischer Dokumente*, 15 COMPUTER UND RECHT, 301–06 (2003) (on file with author); Ulrich Pordesch & Christian Frye, *Sicherheitseignung von Algorithmen qualifizierter Signaturen*, 27(2) DATENSCHUTZ UND DATENSICHERHEIT 73 (2003) (on file with author).

electronic signature does not trust the authenticity of the electronic signature, the value and utility of the signature is severely reduced. Thus, the current system needs reform.

V. Proposed Solutions

A. Further Standardization of Systems

First, there is a need for clearer, stricter standards that reduce variations in electronic signature verification systems. While there have been various technical standards for electronic signature formats for quite some time, nobody has succeeded in condensing these into a single, widely accepted set of standards that would allow programmers to create universally accepted signature applications. There is little hope that help will come from the EU. EU lawmakers have been very reluctant to fix a single technical standard, trying instead to be as technologically open as possible to avoid artificially limiting development.[36] Thus, no significant change should be expected to come from a re-evaluation of the existing EU Directive on electronic signatures.

On the national level, however, some progress has been made. For example, the Common-PKI standard has improved the situation in Germany significantly.[37] With Common-PKI, the key to success was: (a) an official mechanism that application programmers could use to reliably validate the compatibility of their products with the specification, and (b) a compliance certificate that was issued to the Certification Service Provider (CSP) by the government administrative body.[38]

Unfortunately, Common-PKI and other similar initiatives have thus far not taken off internationally. The international market contains a large number of service providers interested in their product

[36] *See* Dominik Gassen, Digitale Signaturen in der Praxis 148 (2002) (on file with author). The wisdom of this decision might be questioned in retrospect. Signature technology today is fundamentally the same as it was upon its introduction in the mid-nineties. The legislative's self-limitation has furthered the fragmentation of standard variants rather than fostering new technologies. In contrast, the EU's approach to regulating the mobile telephone arena was much more successful. The mandatory GSM standard guaranteed total interoperability, and this ended up producing more competition in Europe.

[37] *See* Common-PKI Specification 2.0, *supra* note 30.

[38] *See id*.

becoming the accepted market standard in a market that is of limited size. In this situation, it is unlikely that a single service provider will come to dominate the market. Additionally, continuing technical differences between signature applications from American and European markets further decrease that chance.[39]

In order to facilitate international recognition and validation of certificates, there are currently several projects, such as European Bridge CA (EBCA), that are working to improve international acceptance of electronic signatures by connecting CSPs and improving access to certificate directories.[40] The connected service providers are able to mutually trust one another's certificates based on certain standards that every participant is obliged to comply with upon joining. Unfortunately, not enough service providers have agreed to join, and as a result, the programs have met with only limited success.[41]

B. Mass-Market Applications

There is a large degree of doubt as to whether local signature applications, which currently comprise a large share of the market, can provide a suitable long-term structure for flexible signature verification, both from a micro- and macro-economic point of view. Developers of electronic signature applications have traditionally been medium-sized enterprises or similarly sized subsidiaries of larger companies. Until recently, these applications have not been mass-market products. For a small or medium-sized business, the task of keeping up with the variety of different signature formats and certificates from different national and technical contexts is daunting to say the least. Most do not command the resources necessary for the development and maintenance of the large number of variations necessary to achieve universal acceptance. Furthermore, the technical

[39] Application development in the American market is influenced by the proprietary product interests of only a few software companies. The major American players are (a) Microsoft with their signature integration in Windows and Outlook product lines; and (b) Adobe with their Acrobat product that has integrated signatures into closed extensions of the pdf file format. Microsoft has been closely linked to Verisign as its CSP.

[40] *See* TeleTrust, Welcome to European Bridge-CA, http://www.bridge-ca.org/html/eb-ca.html (last visited Apr. 12, 2009).

[41] *See* TeleTrust, European Bridge-CA Participants, http://www.bridge-ca.org/html/members.html (last visited Apr. 12, 2009).

parameters of CSPs' programs and encryption technology are constantly changing. Certification authority certificates and algorithms are constantly being exchanged, discarded, or upgraded, and verification programs must be kept up to date. The extreme effort needed, especially in the international context, is simply not economically feasible for smaller companies. Additionally, it does not make economic sense for every software developer to invest in building parallel structures and know-how.

C. Online Electronic Signature Verification Platform

Notarial organizations have long been on the forefront of the implementation of new electronic signature technology. Since the mid-nineties, electronic signatures have been discussed in connection with the transfer of notarial functions to electronic medium. Notaries have often been the first professional group to embrace electronic signature technology in large numbers and to develop their own Certification Authorities to issue certificates to notaries.[42] With increased use of electronic signatures, there has also been an increase in the exchange of knowledge and experiences between the national notarial organizations within Europe through the Council of Notariats of the European Union (CNUE).[43]

Inside the CNUE, working groups have been promoting the adoption of new technologies, discussing national developments, and thinking about how these national experiments can be applied internationally. Electronic signatures have quickly come to occupy center stage at CNUE conferences. The cross-border circulation of notarized documents—in particular, powers of attorney—has always

[42] *See* BNotK, German Civil Law Notaries and How They are Organised, http://www.bnotk.de/__English/info.english.html (last visited Apr. 12, 2009); Press Kit, Conseil Supérieur du Notariat [Higher Council of French Notaries], Signature of the First Electronic Notarised Deed (Oct. 28, 2008); Consiglio Nazionale del Notariato [National Council of the Notary's Office], http://www.notariato.it/portal/site/notariato (last visited Apr. 12, 2009) (representing Italy's attempt to embrace signature technology among its notaries and control their own CSPs); Agencia Notorial de Certificacion (ANCERT), http:// www.ancert.com/ (last visited Apr. 12, 2009) (representing Spain's attempt to embrace electronic authentication among its notaries and control their own CSPs).

[43] "The Council of the Notariats of the European Union (CNUE) is an official organism representing the notarial profession at the European institutions. Speaking for the profession, it handles negotiation and decision-making for all civil law notaries in the European Union." CNUE, http://www.cnue-nouvelles.be/en/001/ (last visited Mar. 2, 2009).

been a regular part of notarial practice. To address the use of electronic signatures, the CNUE formed a Working Group on Electronic Signatures (Working Group) in 2006,[44] which quickly determined that the transfer of these duties to electronic media posed unexpected technical obstacles, rather than facilitating these transactions as had been expected. Thus, for the average notary, it remains extremely difficult to verify the authenticity of electronically signed data received from another country because of the limits of the respective signature applications in use.

The first solution proposed by the Working Group was the development of a common verification app. This was quickly rejected because of the extraordinary effort that would be needed to develop, distribute, maintain, and support such an application for the many thousands of notary offices across Europe. Additionally, it would be difficult to find a common platform because the technical structure of the existing platforms (especially in regards to Operating Systems) is not homogeneous.

A sensible alternative was then proposed. Instead of developing an electronic signature application that would be installed on the notaries computers', the Working Group would establish an online service for signature verification, eliminating the need for the installation of any special software. This type of system would simply work through the computer's existing internet browser. Additionally, Italy had already implemented this type of system on a national level with positive results.[45] At the 2005 CNUE Conference, some of the core countries of the CNUE had already proposed this direction of development, committing themselves to the idea of development of a European Platform for the Validation of Notarial Electronic Signatures.

The Working Group agreed on four conditions beforehand that would be crucial to the success of the project. First, the electronic signature verification service would be limited to signatures

[44] Both authors have been and currently are members of the CNUE New Technologies Committee and have specifically on the matters discussed in this article. Co-Author Dominik Gassen has been CEO of the German Notaries' organisation's IT subsidy, NotarNet GmbH (www.notarnet.de) and Director of the German Notaries' CSP, with more that 15.000,- issued signature cards one of the biggest CSPs in the country.

[45] Ugo Bechini & Michele Nastri, Presentation at the First Congress of the Notariats of the European Union in Rome: Integrated System for the Processing of Computerised Notarial Documents, at 3 (Nov. 11, 2005), transcript *available at* http://www.cnue-nouvelles.be/fr/congres-2005-en/rapports-discours/2-integrated-system-for-the-processing-of-computerised-en.doc.

originating from European civil law notaries. This would reduce the technical and organizational complexity to a manageable level. Second, all technical work would be handled by CSPs that were members of the participating notarial organizations. As an initial condition this would be excellent because all of the service providers would have extensive experience in electronic signatures and be knowledgeable as to the specific signatures and certificates used by the notaries in their countries. Third, the local notarial organizations would provide the legal background on their local legal regimes for the use of electronic signatures. And finally, the participating notarial organizations would not provide *certification services* in the narrow sense (i.e., as described in EU Directive 93/1999)[46] because they would not be establishing a separate database and certificate register for the service. Instead, every validation request would be put to the certificate register of the respective CSP, thereby reducing the risk of liability for the notarial organization due to an incorrect certification.

The Working Group also set the following goals for the project. First, the verification platform should be able to analyze submitted data intelligently, independently recognize supported signature variations, set up fitting verification methods, and determine where and how to request certificate information. Thus, the system should be user-friendly, and the user should only have to provide the a limited amount of data. Second, detailed verification results should be made available to the user immediately and presented in a manner that is geared toward the average user, enabling him to assess at a glance if he is dealing with a trustworthy signature. Third, the user interface and presentation of verification results should be provided in the user's own language for best comprehensibility, and additional information on the specific legal rules for electronic signatures in the user's country of origin should also be made available in multiple languages. Fourth, in addition to providing information on the signer's identity, the service should also explicitly state if the signer was a civil law notary at the time the signature was performed. And finally, the project page should furnish links to legal resources on electronic signatures that are available online (e.g., texts of signature laws and electronic notarial acts).

It was the hope of the Working Group that the European Platform for the Validation of Notarial Electronic Signatures would become a

[46] *See* Directive 93/1999, *supra* note 1. In other words, the CSPs would be providing the actual certification.

reference project for user-friendly online electronic signature verification services. In 2006, the Working Group was comprised of notarial organizations from France, Italy, Spain, and Germany. The Austrian Chamber of Notaries also took part as an observer. In the first half of 2006, several surveys were performed among interested notarial organizations to obtain a sufficiently detailed view of existing technical approaches. Basic feasibility was agreed upon in mid-2006, and the second half of the year was dedicated to the initial programming and establishment of necessary infrastructure.

It seems remarkable that a venture this complex could be successfully handled as a shared project by four organizations from different countries. The respective teams closely coordinated their work using electronic media. Project leaders conferred via videoconference in short intervals, effectively tackling problems as they appeared and distributing pressing tasks. Interestingly, the mix of engineers and technically inclined notaries was extremely useful in the Platform's development. It made it possible to address all levels of the project and solve problems.

Early 2007 witnessed the first internal presentations of a working prototype of the Platform containing all the features of the later production version. The service was available to everyone via internet and worked independently from operating system and browser platforms. The verification component was able to check user-supplied signed documents from notaries in France, Italy, Spain, and Germany. The user was offered two options. He could upload the data in question to the service and have the results displayed on the web page. Or, if this method was not viable because of the amount of data or privacy concerns, he could download a small java applet to perform parts of the verification process locally and avoid uploading sensitive data. Signature certificates were then validated by direct access to the certificate register of the issuing CSP.

During 2007, the platform prototype was presented at several conferences, primarily in the EU, to positive resonance and pronounced interest.[47] The Working Group's initiative has introduced an alternative to the proprietary solutions offered by major international software providers. The Working Group continues to refine the service and has started working on the integration of more signature variants. CNUE is currently deciding on the manner in

[47] *See, e.g.*, Work on E-Justice, Draft Conference Agenda, version Jan. 31, 2007, http://www.bmj.bund.de/files/-/1826/Draft%20Conference%20on%20E-Justice.pdf.

which the service can be provided to notaries, courts, and other public authorities worldwide.

VI. Conclusions and Outlook

Will the European Platform for the Validation of Notarial Electronic Signatures make European CLNs interchangeable? Will a Parisian CLN be able to perform the sale of real estate in Vienna and execute all the subsequent filings via the internet? The answer remains a definite no. The CLN's foremost task is not the mere identification of the parties. He is also responsible, and liable, for a huge array of different issues related to the contract.[48] These tasks are performed not only in the interest of the parties, but in the general public interest, as it keeps litigation in Europe at comparatively low levels.

Such a role can be played only by a qualified professional who is an officer of the State, familiar with local laws, able to work in cooperation with the authorities and agencies of the jurisdiction. Thus, only a CLN can perform these tasks. If the legal systems of the EU Member States are one day integrated to such a degree that national differences are hardly noticeable, the birth of a paneuropean notarial profession will be an obvious consequence. Until then, the EU will continue to operate with a system based on national notarial bodies, each of them in charge of their own country's legal affairs.

Therefore, the European Platform for the Validation of Notarial Electronic Signatures, at least in the first stage of its life, is expected to handle mainly electronic powers of attorney. Local CLNs will be in charge of the deeds, while CLNs in other countries will notarize powers in the interest of the parties who are unable to travel in order to attend in person. The deed will be prepared by the local CLN, who will be solely responsible for its lawfulness and effectiveness, and electronically executed by one party before the same CLN, and by the other party before a CLN in another jurisdiction.

[48] For example, if the seller is not the legitimate owner of the estate, the CLN is required to refund the buyer. The same is true if the CLN fails to properly execute the mortgages. The CLN must ensure that the results of the agreement are in accordance with applicable law and explain to the parties the value, legal effects, and consequences of the transaction. In most European countries, the CLN must also collect taxes and pay the Tax Administration out of his own pocket if the job is not properly done. In some jurisdictions, a CLN is even liable upon failing to inform the parties about an available tax deduction.