ARTICLE:

WHEN THE EU QUALIFIED ELECTRONIC SIGNATURE BECOMES AN INFORMATION SERVICES PREVENTER

By **Paweł Krawczyk**

The practical failure of the qualified electronic signature across Europe is a good lesson on the factors that are critical for information security in public administration and business: the need for well defined objectives, the differentiation of security services, interoperability and a design approach based on risk management. The qualified electronic signature (QES)[1] and the global electronic services market have existed for some time now, but each seems to exist in parallel realities.

People buy goods and services over the internet all the time with other forms of electronic signature (such as the 'I accept' icon, by ticking a box, or typing a name into an e-mail[2]), but the market for QES only seems to serve itself, and there is little connection between sales of goods and services over the internet and the use of a QES. E-government is widely available in some countries, but not in those that took the QES approach. In this article, the author offers an opinion as to how this happened, based on a decade of experience in consulting on information security with a special focus on authentication and the digital signature (the digital signature is also called an 'advanced electronic signature' in the EU Directive), commenting and observing legislation and what actually happens in this field.

Interoperability issues with the qualified electronic signature

Directive 1999/93/EC is a good legal framework for the QES, but its high-level and abstract nature was one factor that largely attributed to its failure. This Directive resulted in a number of different laws by Member States that are incompatible at a technical and semantic level.

The first challenge was the selection of signature and document formats for qualified electronic signatures. At the time the directive was enacted, there were two well-established and standard signature formats available: PKCS#7 and CMS – now called CAdES (ETSI 101 733) and initial drafts of XAdES (ETSI 101 903).[3] When newly established certification authorities and software houses (often the same entity), encouraged by the new legislation, started to design their certification services, they had to make decisions on appropriate formats. But the problem was that in 2002 this sector seemed to have no idea what anyone would be going to use the QES for, except for a very general (and very optimistic) buzz of having a lot of e-everything in front of every word (e-government, e-business, e-banking, etc).

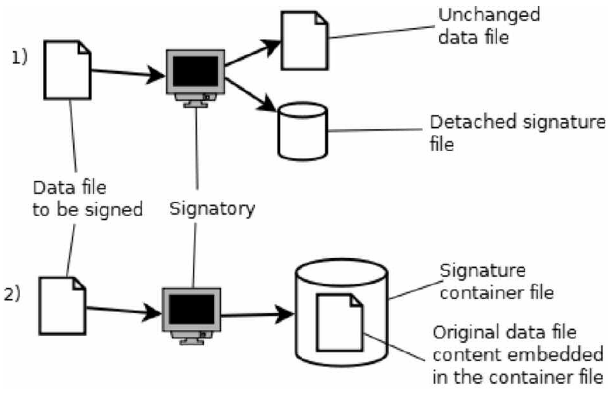
Technical products developed at that time – with no specific business problem that needed to be solved – and submitted greatly to the pan-European format mess that we are now enjoying. Having no specific objective, companies designed the most general solutions they could think of ('sign something'), and QES became an example of the common wisdom that something

[1] *The qualified electronic signature is a construct that merges from a combination of the application of Annex I, Annex II, Annex III and Annex IV of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 013, 19/01/2000 P. 0012 – 0020.*

[2] *For case law across the globe on these and other forms of electronic signature, see Stephen Mason, Electronic Signatures in Law (2nd edn, Tottel, 2007).*

[3] *For an exhaustive list of standards relating to digital signatures, see appendix 3 in Stephen Mason, Electronic Signatures in Law (2nd edn, Tottel, 2007).*

designed to do everything is not good at doing anything. For example, four Polish certification authorities that existed at that time all produced a generic 'sign-a-byte-stream' program[4] that allowed the user to create a detached signature (figure 1) or embed the file inside a signed container (figure 2).



Surprisingly, each of the companies chose a different signature format,[5] and this simple decision has prevented any possible intra-country interoperability for years. If the reader wonders how this happened with four companies and just three formats allowed by law, here is the solution: one of them used XAdES, one used CAdES and two used PKCS#7 for a signature, but in a different file container.

This is how the situation looked like in 2005. As hard to believe as it is, in 2008 there were already fourteen formats available on the Polish market, and each of the four initial formats evolved by changing minor details, plus a few new ones were added by small companies fortunate enough to win bids from the public administration. Out of the fourteen formats, only one pair was interoperable. For example, three products on the market used XAdES format to output signed files, but all used different file extensions (.sig, .xml, .xades),[6] although it might be correct to say that it was likely that each could open the other's files. To add even more confusion, the .sig extension seemed very popular – at the same time four products used it do name their output files, but they used different formats inside.[7] As a result of these two trends, virtually every application was enclosed in its own format and extension, even if some of them could have been interoperable.

From the functional point of view, it is not important to select the best format, because where a single format is agreed between all the parties, it will then be numerous enough to create a critical mass in a given sector.[8] Most specific business functions that might be required can be achieved using any of the available formats, even if it is considered 'old', such as PKCS#7, and does not have any 'modern' features. Looking back over the previous years, it seems as if there were endless technical academic discussions on minor and relatively unimportant aspects of the QES that caused different companies to choose different formats to do the same thing. As a result, useful facilities such as the ability to use minor security-enhancing features prevented people from tackling the much bigger issue of interoperability and usefulness. A rare example of such interoperability was where several countries chose the same signature format (PKCS#7) and the same extension (.p7m) as their basic container for digitally signed files. As result, it was, for example, possible to take a file created by an Italian application and open it in a German application – which is the purpose of interoperability.

[4] *A digital signature may be applied to data in a number of ways. The signature may be an integral part of the electronic document structure (format) and cover specific parts of the content. This is usually the case with document formats that are equipped with digital signature formats by design (e.g. PDF, ODF, OOXML). A more generic case is when a digital signature algorithm treats the input file as raw binary stream of data. The first technique is more flexible and it may, for instance, allow changes to some parts of the document (e.g. an electronic form where only the form layout is protected but the user is allowed to change fields). The latter would verify integrity of the file as a whole and not allow any changes.*

[5] *A signature format is a standardised order in which the technical details of a digital signature are stored in a file. Examples of signature format are PKCS#7, XAdES, CadES and OpenPGP. They differ in their technical details (e.g. XadES stores data as textual XML data, while all the others stores data as binary), and often by security features that are standardised in the format (the functional differences are often very subtle: usually these standards are built like catalogues of features that the developers can choose from, depending on what they need. For example, a developer that needs just a basic signed container for his data could use PKCS#7, which is the oldest available format. If he needed a long-term archival, he would prefer CAdES or XAdES, because these formats have this feature standardised. Or, he could implement this feature by himself using generic PKCS#7 features). The signature data in a chosen format may be stored in another file, separate from the signed data (a detached signature), or it may be stored together with the signed data in one file (an embedded signature). The outermost file format that is visible to the user is called a ' file container' . An example is the PDF format which may contain user data and an embedded digital signature in PKCS#7 format.*

[6] *A file extension is merely a label, part of file name, that does not interfere with the contents of the file, but allows applications to quickly determine what file format they should expect inside the file and how to handle it. If the file extensions were changed manually in the scenario described, it is likely that they would start to open properly in other programs – obviously that is not something that can be expected from an end user. File extensions are not standardized, and a designer decides which extension to use because of tradition and personal preferences. For example, the .doc extension has been traditionally associated with Microsoft Word, but it is not exclusively assigned to the program.*

[7] *Paweł Krawczyk, ' Tabela kompatybilności formatów podpisu elektronicznego w Polsce' , 19 March 2008, a technical article published on IPSec.pl and available at http://ipsec.pl/firmy/ 2008/ kompatybilnosc-formatow-podpisu-elektronicznego-w-polsce-bliska-zeru.html.*

[8] *Deciding which format is the best to use depends on establishing the purpose. If this is not agreed, the dispute on the features to be given to a format can easily slip into pointless discussion using irrelevant arguments.*

All the generic ‘sign-a-byte-stream’ applications have yet another problem – they are all autonomous, single-function applications, and do not integrate with any other technology, and are barely usable. All a user can do is to run the application, open a file, click through several screens loaded with technical and legal information, and either click to ‘sign’ or ‘verify’ a file created in another application. This is how most applications of qualified electronic signatures sold by certification authorities for users in Europe work.

If the current model of QES is considered in relation to ergonomics and ease of use, it can be equated to early Windows as we remember it from the 1990s. Technical excellence (at least *theoretical* technical excellence[9]), compliance with the requirements of CWA 14355[10] and the general lack of any idea what the applications should be actually be signing, made them difficult to understand for anyone without a strong technical background (and having a legal background did not necessarily mean that a lawyer or judge understood the complexities of the QES).[11] This is a perfect example on how ignoring the human factor in the design of the system rendered a perfectly secure architecture (at least theoretically[12]) unusable. Potential users declined to consider using the QES, and used WinZip if they wanted a generic file archive, and possibly SecureZIP, if they wanted enhanced security features. In addition, if a user wanted to produce an electronic document with an embedded signature, then they would rather consider the digital signature features in MS Office, Open Office or Adobe Acrobat, although these are not suitable for a QES, for the reasons explained below. [13]

Parallel worlds, parallel applications

A great deal of paper was used and words expended on the meaning of the important sentence dealing with ‘sole control’ of the signatory in Directive 1999/93/EC.[14] The main consequence of these disputes was a set of very strict technical requirements for signature creation devices and applications that were subsequently refined in a series of CEN Workshop Agreement (CWA) and European Telecommunications Standards Institute (ETSI) technical standards. These requirements effectively prevented the use of such applications as MS Office, Open Office or Adobe that supported digital signatures, conveniently embedded in their electronic document formats, but not in the way required by the CWA or ETSI.[15] In addition, since the specific requirements are all slightly different in each of the Member States of the EU, it is virtually impossible to make a product that complies with all of them.[16] This converted the EU QES market into small national enclaves, with local companies guarding their local interpretations and regulatory secrets.

As for the general architecture of the QES, Estonia is a notable exception from the negative trend. In Estonia,

[9] *In Poland, the QES was marketed as a ‘secure signature’. In 2005 the antivirus vendor G DATA publicly demonstrated how to subvert a popular QES application to sign a false content so that different data was presented to the user and different data was sent to the card for signing. This resulted in a very nervous reaction of the vendor, that accused the company of spreading fear, uncertainty and doubt, and argued that a ‘secure signature’ is not secure in general but ‘secure in the legal sense’. [Editor’s comment: it would not be secure in the legal sense either].*

[10] *CEN Workshop Agreement (CWA) 14355, ‘Guidelines for implementation of Secure Signature-Creation Devices’, 2004, European committee for Standardisation.*

[11] *Editors note: most lawyers across the globe still do not understand the basic elements of electronic signatures yet.*

[12] *According to the Polish technical regulation of the QES (Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. z dnia 12 sierpnia 2002 r.) a ‘public’ signature creation software requires a ‘trusted channel’ (paragraph 4.4). That is, a security feature that can prevent the modification of data in transit as it is read from file and sent to the technical component (smart card) for signature (this was the basis of the G DATA attack in 2005). Unfortunately the ‘public software’ (paragraph 2.9) is defined in such way that it excludes virtually any software used at home or in the office (and nothing else is left). From a business point of view, the objective of this requirement is obvious – no general-purpose operating system (such as Windows or Linux or MacOS) can offer such a feature in the strict sense, so having it in force would prevent anyone from using QES on these systems. From an engineering point of view, however, this is a clear sign that the regulators had no idea what they were going to use the technology for and what they are trying to protect from.*

[13] *Note the discussion on this topic by Nicholas Bohm, ‘Watch what you sign!’, Digital Evidence and Electronic Signature Law Journal, 3 (2006) 45 – 49.*

[14] *Directive 1999/93/EC, Article 2, item 2c requires that an ‘advanced electronic signature’ is ‘created using means that the signatory can maintain under his sole control’. The technical interpretation of this phrase was discussed in CWA (14355, 14365), ETSI TS (102 042) and FESA (Forum of European Supervisory Authorities for Electronic Signatures) statements (2004, 2005). For an exposition on this point in legal terms, see Stephen Mason, Electronic Signatures in Law (2nd edn, Tottel, 2007) 4.6 and 4.9.*

[15] *More precisely, this was the case for those jurisdictions that required a qualified electronic signature with a qualified certificate and a secure signature creations device (SSCD in CWA 14169 terms) and where signature creation application (SCA) was regulated (a declaration of compliance, as required by the Polish electronic signature act from 2001). In Poland, the SSCD itself was defined as hardware (a smart card) plus software. The problem with this approach was that while it may be considered by some that the security inherent in a smart card is substantial (until it is lost or stolen), the added value of an SCA is much smaller. At the same time, the administrative and legal burden has increased significantly, because new, QES compliant programs must be created and the user cannot use those they previously used on a daily basis any more.*

[16] *A good example of the impossibility of making a globally available application that complies with all the relevant QES regulations is that of Adobe Acrobat, which introduced increased support for the functions required to enable the product to be compliant to QES in version 8. The product included an internal ‘library’ of options typically required by different EU Member States. This, it was hoped, would ensure compliance with local requirements. But this was not sufficient for the German regulations, which required a dedicated option to change between ‘shell’ or ‘chain’ validation models and special ISIS-MTT object identifiers (this can only be configured by an administrator by registry modifications, so the user does not see them).*

the government implemented a reasonably complete and consistent product (DigiDoc), which started from clearly defined objectives, an open technical specification, software packages and an internet portal. In addition, an attempt was made to invite others to consider interoperability by publishing an open implementation (OpenXAdES[17]). Another helpful move in right direction is PDF Advanced Electronic Signatures (PAdES) (ETSI TS 102 778). PAdES is interesting because it is a format that tries to solve a specific problem: secure delivery and long-term storage of electronic documents,[18] and it can also help with providing for technical interoperability.[19] Introduced ten years after Directive 1999/93/EC, implementing this standard would require the gradual reversal of all local inventions, which may take another decade to complete. At the time of the Directive, the technical nature of the concept of the digital signature was based on the X.509 security framework, and this model may no longer be interesting for anyone except for companies earning income from endless consulting and analysis of the Directive 1999/93/EC model.[20]

Hardware limitations

The requirement to use a secure signature creation device (SSCD), or a cryptographic card for a QES also seems to be a significant barrier for most users. This is the main method to satisfy the requirements of article 2(2) of Directive 1999/93/EC for the signature device to remain under the sole control of the signatory:

> 2. 'advanced electronic signature' means 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 pointed out by Mason, this is not a definition, but a number of characteristics relating to performance.[21] This is one of the basic assumptions of the QES security model, although in many cases it is not necessary for a QES to have a SSCD. The problem is, that requiring a QES to have a SSCD without fully understanding the consequences of complex hardware and software dependency is one of the factors that have made digital signatures and qualified electronic signatures exceedingly difficult to use.[22] However, there is a flaw in the characteristics relating to the advanced electronic signature, as pointed out by Brazell and Mason – that is, a digital signature cannot meet the requirements of the first characteristic, that of being 'uniquely linked to the signatory'.[23] This is because it can only be linked to the private key of the signatory, and no person is capable of memorising the private key. This means the private key must be retained on a computer, disk or smart card. This is what is meant by 'means that the signatory can maintain under his sole control'. The problem is, a person cannot control the private key. If the private key is on a smart card, the card can be lost, stolen or 'borrowed'.[24] If the private key is on a computer, a malicious third party can obtain access to it and, once they have obtained the password, us it as they wish. In electronic signature engineering, the 'link to the signatory' is explained as follows: theoretically, only one copy of the private key exists, and it is usually created by the certification authority and issued to the signatory for their use. It is usually stored on a smart card that prevents the creation of more copies, and its use is

[17] *http://www.openxades.org/.*

[18] *Although note the problems about the long-term archiving of digital signatures in Stefanie Fischer-Dieskau and Daniel Wilke, 'Electronically signed documents: legal requirements and measures for their long-term conservation', Digital Evidence and Electronic Signature Law Review, 3 (2006) 40 – 44.*

[19] *Technically, PAdES is a file format that is backwards compatible with the popular PDF. While the basic PDF standard (ISO 32000) defines the PKCS#7 format, the PAdES adds CAdES support to comply with QES requirements. The file format and file extension is identical. From the user's point of view, most PDF programs should open a PAdES file even if they cannot fully verify the QES signature.*

[20] *The story of QES largely resembles the Internet Protocol Security (IPSec) (this is a method for providing for the security of IP communications by authenticating and encrypting each IP packet of a data), that was introduced as complex but consistent architecture in the early 1990s with the intent of creating a universal standard for trust over the internet. Then everyone realised that the perfect and universal IPSec would not work with private IP addresses for a private network developed in accordance with RFC 1918 (Address Allocation for Private Internets). Before it was understood and became somewhat interoperable in countless bake-off meetings, the world had to use something that was not so perfect, such as Point-to-Point Tunneling Protocol (PPTP) (a Microsoft method used to implement a virtual private network, fatally flawed in the first versions), and when numerous extensions to IPSec started to be published, everyone was annoyed enough to move to SSL VPN (Secure Sockets Layer Virtual Private Network).*

[21] *Stephen Mason, Electronic Signatures in Law (2nd edn, Tottel, 2007) 4.6.*

[22] *See also Chapter 5 'Mechanical instruments: the presumption of being in order' in Stephen Mason, general editor, Electronic Evidence, (2nd edn, LexisNexis Butterworths, 2010) in which this discussion is considered in detail.*

[23] *Stephen Mason, Electronic Signatures in Law (2nd edn, Tottel, 2007) 4.7 – 4.8; Lorna Brazell, Electronic Signatures Law and Regulation, (Sweet & Maxwell, 2004) 5.045 – 5.046*

[24] *S. C. Rennie and J. R. Rudland, 'Differences in medical students' attitudes to academic misconduct and reported behaviour across the years—a questionnaire study', J Med Ethics 2003; 29:97-102, in which medical students admitted they would forge signatures on work submitted (Stephen Mason, Electronic Signatures in Law (2nd edn, Tottel, 2007) 4.9 footnote 1).*

protected by the password that only the person issued with the private key should know.[25] Under Polish law it is prohibited to use the card and password of another person under article 47 of Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym – Law of 09.18.2001 on electronic signature:

> Art. 47. Kto składa bezpieczny podpis elektroniczny za pomocą danych służących do składania podpisu elektronicznego, które zostały przyporządkowane do innej osoby, podlega grzywnie lub karze pozbawienia wolności do lat 3 albo obu tym karom łącznie.
>
> Article 47. Anyone who executes a secure electronic signature using the data for the execution of an electronic signature which were assigned to another person shall be liable to a fine or a penalty of deprivation of liberty for up to three years or both these penalties jointly.

Certification authorities also require the user to protect the card and password in the certification service contract, but in reality, users do not follow this, as described below in the ZUS case study.[26]

The hardware itself was significant problem in 2002, when most readers were connected over RS-232 (Recommended Standard 232) (this is by the Electronic Industries Association, and is a standard for data and control signals that connect between data terminal equipment and data circuit terminating equipment, and is commonly used in computer serial ports). At the time, even engineers found it really difficult to have all the components of a QES working. For instance, a smart card reader would not work until the user provided the operating system with the serial port parameters and installed an item of special software provided by the vendor – this was a significant usability problem. Most of the configuration is now automated; if the user connects the reader, it should work, although the user must still install the smart card driver software manually. However, cryptographic card drivers (a driver is an additional item of software that provides the interface between the device and the operating system – drivers are supplied by the vendor in most cases) remain a problem. This is because smart card drivers are not installed automatically when the user inserts the smart card into the reader; which means it will not work unless the user installs the driver software provided by the vendor. The intention may not be to compel the customer to use their particular technology, but it enables the personalisation of a large number of smart cards. This problem is exacerbated, because some vendors do not install PKCS#11 drivers that enable any user application to work with each other (PKCS#11 is a standard from RSA Security for cryptographic hardware drivers). Cryptographic API from Microsoft was the first, vendor specific way for applications to communicate to a smart card and, for instance, request the signing of data. Then PKCS#11 was developed, and now both standards seem to coexist. An increasing number of vendors now provide PKCS#11 drivers for their smart cards, but it is not universally true. PKCS#11 is, in general, more interoperable and not bound to an operating system. Matters are more complex for those handling qualified certificates for operating systems other than Windows. In addition to the standard PKCS#11 interface, they have a built-in JavaCard applet that provides additional protection; in reality, this means that it is necessary to have a matching driver from the vendor to use each card, which causes more problems of interoperability.

The extent of the technical difficulties that can prevent ordinary people from using a QES can be illustrated by the requirement to buy and install a $15 smart card reader. This was one of the proposed explanations as to why only 5.4 per cent (30,275) of Estonian citizens that were eligible voted over the internet in the 2007 elections[27] – and this was even where the majority of Estonian citizens have qualified certificates as part of their national identity cards, compared to less than 1 per cent in Poland. According to Ministerstwo Gospodarki (Ministry of Economics), the statistics for 2009 indicate that there are around 200,000 active certificates in Poland. With a population

[25] An advanced electronic signature must be protected by complex password that makes it more difficult to guess by an exhaustive search. Guessing the password will not work for smart cards where they are designed to have a fixed limit of attempts at entering the password (usually 3), after which the software will block the use of the card. Obviously, the strength of the QES still depends on the password in the sense that if the password is revealed (Post-It stickers, shoulder surfing, etc) and an attacker obtains access to the smart card, the link to the signatory is then lost.

[26] For cases where digital signatures have been used by criminals to transfer funds from company bank accounts, see Olga I. Kudryavtseva, ‘ The use of electronic digital signatures in banking relationships in the Russian Federation’ , Digital Evidence and Electronic Signature Law Review, 5 (2008) 51 – 57, and Olga I. Kudryavtseva, Case note: Resolution of the Federal Arbitration Court of Moscow Region of 5 November 2003 N КГ-А 40/8531-03-П, Digital Evidence and Electronic Signature Law Review, 5 (2008) 149 – 151.

[27] ‘ Internet voting in the March 2007 Parliamentary Elections in Estonia’ , a study directed by Prof. Alexander H. Trechsel and Robert Schuman in collaboration with Guido Schwerdt, Dr. Fabian Breuer, Prof. R. Michael Alvarez and Prof. Thad E. Hall, (Report for the Council of Europe, 31 July 2007) available at http://www.vvk.ee/public/dok/Coe_and_NEC_Report_E-voting_2007.pdf and http://www.vote.caltech.edu/drupal/node/140.

The popular explanation by technicians that security has its own special requirements has never been valid, especially when such an assertion is plainly not true.

of 38 million, this means the take-up is less than 0.5 per cent of the population. In Estonia, the coverage is over 77 per cent.[28]

In addition, the immensely complex legal and organisational requirements to create a qualified electronic signature caused vendors to design software and hardware in such a way to ensure the customer must always buy the same application or product in the future. For instance, it is practically impossible to install a qualified certificate on a smart card other than the one sold by a given certification authority (in Poland the qualified certification authority must be approved by the Ministerstwo Gospodarki (Ministry of Economics)), even if the smart card would satisfy such legal requirements[29] as Common Criteria certification[30] by SSCD profile at EAL4 (evaluation assurance level).[31]

The way Directive 1999/93/EC has been interpreted by regulation at the local level, together with the immaturity of the technology, has resulted in a situation where it is necessary to devise a separate project for each business purpose that required smart cards, which means that each employee is issued with a number of cards, each tied to different vendor. For example, if a customer has a compliant smart card from certification authority 1 (CA 1), and they go to CA 2, then CA 2 will require the customer to buy their card, rather than generate the private key on the card they already have in their possession. This can partially be explained by an attempt by the vendor to force the customer to buy a new smart card from them, and partially because of the incompatibilities described above.

Interoperability summary

All of the challenges mentioned above – lack of format compatibility, few generic and usable applications (by an 'application' is meant 'a computer program used by a user'), the requirement to install software drivers for both the reader and the card, plus additional difficulties requiring technical skills (such as those described below) – make the applications sector that produces qualified electronic signatures one of the worst in respect of ease of use. Taken together, these small annoyances that each separately looked 'easy' (engineers) or 'necessary' (lawyers) have made the QES difficult to use.

The popular explanation by technicians that security has its own special requirements has never been valid, especially when such an assertion is plainly not true. For instance, authors of one Polish application (Elektroniczna Skrzynka Podawcza by Zeto Białystok) required the user to run a special command line to change the settings of .NET security policies (this is a Microsoft programming library or framework that is used to code the program – the user should never be required to even touch this), and another one (e-Deklaracje by the Ministry of Finance) instructed users to manually change extensions of Adobe AIR programs (with the same problem as previously described, but with a different vendor) just to send an electronically signed file. Neither of these technical design attributes was caused by the need for security, but rather by the immaturity of the underlying technology. On the other hand, vendors did not consider such issues as of any relevance. For instance, the administration offices in Poland were required to buy or outsource the Internet document gateway (ESP) in a relatively short time; it was formal compliance with law that was a priority, not the ease of use, even if the average citizen could not use the software.[32]

[28] *Tarvi Martens, ' Evolution in cross-border interoperability of eSignatures and eID' , IDABC, http://ec.europa.eu/idabc/en/document/7339#martens; the current number of eID cards in Estonia can be found at http://www.sk.ee/pages.php/ 020304,1115.*

[29] *As required by Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. z dnia 12 sierpnia 2002 r.).*

[30] *http://www.commoncriteriaportal.org/.*

[31] *EAL4: Methodically Designed, Tested, and Reviewed – this standard enables a developer to provide a degree of assurance for their produce on the basis of positive security engineering based on good commercial development practices.*

[32] *Paweł Krawczyk, ' Ekscytująco prosta w użyciu skrzynka podawcza Zeto Białystok' , 21 February 2008, article published at IPSec.pl and available at http://ipsec.pl/podpis-elektroniczny/2008/ekscytujaco-prosta-w-uzyciu-skrzynka-podawcza.html.*

The conclusion is, that regardless of the optimistic visions of digital signatures that are presented to users, the technology will not work if the underlying technologies are not mature enough to provide stable products that can be used by lay people. Where the user has the choice of ugly, counter-intuitive but highly secure applications that only allowed them to produce a qualified electronic signature, or their popular office applications that were not considered approved for QES, the users simply voted with their feet. The failure for the QES to be taken up by users has nothing to do with lack of trust in the internet or old habits, because the same people use the internet to buy and sell (auctions, food, clothes, holidays, air travel, to name but a few) and use internet banking all the time.[33]

The provisions relating to the QES in Directive 1999/93/EC provide an imperfect attempt at providing for an almost totally secure method of electronic signature. But those responsible for producing the QES fail to understand that the practical issues for both people and business centre around weighting the cost and benefits of a specific technical product. The QES, which is very expensive and a burden to use, provides highly sophisticated protection against attacks that are not very relevant for most e-commerce use[34] – indeed, the QES level of security was often figuratively demonstrated by comparison with the notary services.[35]

The qualified electronic signature as an information services preventer

The qualified electronic signature provides a very high level of security: it offers authenticity, integrity and non-repudiation (non-repudiation means that it can be demonstrated that software communicated with software, not that the person whose private key it was, was the person responsible for using the key) – but its history in Europe is the ultimate proof that more security is not always better. This is because of cost, which is a direct function of the amount of security. The cost includes not only the direct cost of buying a certificate, but also the costs of running an organisation and the cost of using a QES. In the case of the QES, the assumed security strength levels make all these costs relatively high.

The QES was initially intended to make cross-border business and administration contacts easier and cheaper, but this objective was lost somewhere on the way. It is not possible to make things cheaper and easier with something that is disproportionately expensive and difficult to use in comparison to the purpose for which such signatures will be put. For instance, simple informative services usually require little or even no authentication of the requesting party (for instance, checking a VAT number, a business registration number or a certificate of residence). Where a user wishes to test the authenticity and integrity of a source of data, it is usually sufficient to rely on SSL server authentication or a Web Trust signature built into a PDF file.[36] Even the submission of annual or monthly tax declarations usually require authentication at a level not exceeding what is currently used by most internet banks (password and username), and such levels have worked for years in the USA[37] and UK,[38] and now in the new Polish e-Deklaracje system that no longer requires QES since 2009, as described below.

One security function that needs to be pointed out separately is non-repudiation. This is a function that QES provides at very high level, but it is very expensive. By non-repudiation, is meant the accumulation of evidence in respect to the use of the card, and the use of behaviour modification to force users into changing their behaviour, thus making it more difficult for a user to provide a trivial excuse to deny that they were responsible for initiating a transaction.

The security surrounding the QES provides a high level of assurance that a QES was affixed to a document and sent from one computer to another computer over the internet. Although the concept of single security mechanism such as the QES is tempting to use from the point of view of the organisation and in terms of

[33] *Number of e-banking users in Poland will probably reach 10 million in 2010, being roughly one quarter of the whole population: the 2008 prognoses is provided by Zwiàzek Banków Polskich (Association of Polish Banks).*

[34] *Who cares about strong non-repudiation and long-term signature validity when requesting a simple certificate of residence or issuing an invoice? For a discussion about non-repudiation in a legal context, see Stephen Mason, Electronic Signatures in Law (2nd edn, Tottel, 2007) 14.20.*

[35] *Piotr Kolodziejczyk, ‘ To prawo i brak chęci blokują rozwój e-administracji’ , Gazeta Wyborcza, 29 June 2008; the comparison was not actually a legal or technical equation of notary signature and QES, but rather a figurative demonstration of the levels of the strength of security; this argument was often used against proponents of QES for e-invoicing who claimed that security is the priority. Opponents argued that if security is a priority, all paper invoices should perhaps be signed before a notary.*

[36] *WebTrust are standard, commercial root certificates that are built-in to most operating systems such as Windows – for example VeriSign and Thawte; everything that is signed with them can by verified by an average user instantly, without the need to install any additional root certificates; for instance, the author's bank in Poland (MultiBank) sends a monthly credit card statement in PDF format with such a signature, and the Adobe Reader verifies the signature.*

[37] *For instance, courts in the USA have accepted documents electronically for many years by a number of providers, one of which is LexisNexis: http://www.lexisnexis.com/fileandserve/courts/ – users submit files to court using a password and username.*

[38] *For instance, HM Revenue and Customs have accepted electronic submissions for many years, using passwords and userid: http://www.hmrc.gov.uk/online/index.htm.*

interoperability, the problems and costs associated with the QES effectively prevents the development of electronic services, instead of helping to develop them. This is because each administration has large number of processes that vary in requirements for the level of security assurance associated with the QES. Defining a single security function covering all of the processes an organisation might want, means that the security level needs to be adjusted for the most demanding process. But the 'one size fits all' approach means that excess security is not for free. In particular, the costs of security for the end user are notoriously ignored. Some Member States in the EU understood this. E-government services were begun, such as revenue service declarations, without a QES. The government gateway in the United Kingdom started around 2001 with login and password, and new security features have been subsequently introduced for users to take up if they wish to.

On the other hand, a large number of trivial informative processes (such as the issuing of declarations and certificates) were effectively blocked in Poland by the strategic decision taken in 2001 that a QES was the only method that was permitted to establish trust between the citizen and the government. Buying a qualified certificate at a cost of US$100 to request or send a simple declaration made no economic sense for most citizens, but the administration was not permitted to use simpler methods, even if they were considered to be adequate for the purpose.[39] The inability to admit this simple fact resulted in the waste of public money on an unbelievable scale. By 2008, most public administration units in Poland were required to buy or outsource an Internet document gateway (ESP)[40] that only allowed communications with the use of a QES. The market for qualified certificates was such that only 0.01 per cent of the population acquired a qualified certificate, and there was little economic sense for citizens to buy any more, which meant that the administration spent millions of euros for systems that were virtually never used. An ESP gateway in Krakow (population of 750,000) reported in 2009 that around five electronically signed documents were being submitted annually since it was installed.[41]

It follows that official communications still had to occur, and they continued to be transacted on paper, not because people were afraid of the internet as some claimed,[42] but because the solution created with the QES was not easy to use and expensive.

The view that it was only possible to use a qualified electronic signature was supported by some certification authorities that acted in various ways to encourage their use, and requested the government to create incentives for citizens to use a QES. These efforts were partially successful. Attempts to liberalise the use of qualified electronic signatures were effectively prevented in 2004, when they were first mentioned, until 2010 when new draft law should be enacted (Projekt z dnia 23.03.2010 – Ustawa o podpisach elektronicznych). As result, in 2005 Poland implemented Directive 2001/115/EC[43] and subsequently enacted the e-invoicing legislation: Rozporzàdzenie Ministra Finansów z dnia 14 lipca 2005 r. w sprawie wystawiania oraz przesyłania faktur w formie elektronicznej, which only permitted the use of the QES and EDI as a means of authentication. This legislation effectively ensured e-invoicing did not occur in Poland for some time.

Where the qualified electronic signature does not work

E-invoicing was introduced to reduce the cost of traditional invoicing – printing, paper, human work, postal services etc – and it makes sense only if the cost is indeed smaller. The QES was introduced to provide

[39] *The requirement to use a QES was one of the factors that prevented most citizens interacting with the otherwise highly useful SEKAP portal in the Silesia district.*

[40] *Elektroniczna Skrzynka Podawcza (ESP), literally 'electronic lodgement of documents office'. This was introduced by Rozporządzenie Prezesa Rady Ministrów z dnia 29 września 2005 w sprawie warunków organizacyjno-technicznych doręczania dokumentów elektronicznych podmiotom publicznym.*

[41] *Katarzyna Ponikowska, 'Podpiszesz bez długopisu', 30 November 2009, Echo Miasta Krakowa, and Paweł Krawczyk, 'Raport na temat masowego wykorzystania elektronicznych skrzynek podawczych', 21 June 2010, at IPSec.pl. Estimating the cost of such an ESP at around 15-25 thousand euros, the return on investment would produce a large, negative figure. Another way of assessing the economic efficiency would be by dividing cost of the ESP by the number of documents processed. Both estimates suggest that the example cannot be seen other than as a shocking waste of public money as result of the implementation of flawed legislation.*

[42] *The 'Poles are afraid of Internet' excuse was offered for a number of times by various representatives of the public administration when asked about the low usage of QES services. But according to the 2010 Reader's Digest study 'European Trusted Brands', over 70 per cent of Poles trusted the internet, with a European average of 49 per cent (a copy is available from http://www.rdtrustedbrands.com/).*

[43] *Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax, OJ L15, 17.1.2002, p. 24–28.*

high levels of security, including non-repudiation – which is arguably irrelevant in the case of e-invoicing.[44] E-invoicing is about fast, automated generation and provision of VAT tax and deduction information. The objectives of a QES are the opposite – it is necessary to view the document, unblock the smart card, view the legal notices (which are substantial) and sign – it is not possible to make it a fast and automated process.[45]

The e-invoicing security model centres around the authenticity of the company of origin, and the integrity[46] of the content – and that is all that is required (as explicitly stated in Directive 2001/115/EC[47]). The QES provides for a reasonably strong link to an individual person and technical non-repudiation. The latter aspect increases the cost and makes it unsuitable for e-invoicing. This means the security requirements of e-invoicing and the features provided by a QES are largely contrary to what is required.

As mentioned above, Directive 2001/115/EC requires 'authenticity and integrity' of an e-invoice, but it does not require a QES (it merely allows the use of a qualified electronic signature along with other methods). However, Polish legislation has chosen the QES-only approach, also allowing EDI. Supporters of QES-only e-invoices raised three main types of arguments: the highest level security is required for customers to trust e-invoices; any other integrity protection other than QES will confuse customers, and e-invoices should promote QES (a circular argument).[48]

Polish statistics from 2007[49] indicated that only 5 per cent of companies were exposed to e-invoicing, and out of that, most were supermarkets using EDI, and not the QES. The QES based e-invoicing exchange between small and medium companies is still practically non-existent, in that the 5 per cent use is based on the statistics from the Central Statistical Office – especially if compared to other countries such as Denmark, where it is over 60 per cent.[50]

Instead of the promised savings and increase in the take-up of electronic invoicing, a number of pathological business practices started to appear to work around the flawed legislation.

From 2009, several companies with a large end-user base, such as Telekomunikacja Polska S.A., started to issue e-invoices using a QES, because they presumably saw it as a way to reduce the costs while preserving the legal requirement to provide the invoice to consumers. But the increased value of security was questionable because of how it was implemented. Consumers received an unsigned PDF with the invoice in one file and a detached QES signature in another file. The signature could be verified only by using a special program from the vendor, which meant the users merely looked at the unsigned PDF and ignored the signature file. This is a perfect example of how the implementation of security can be perfectly legal and perfectly useless in reality. Other companies on the other hand, especially small and medium size companies, resolved the problem of the restrictive e-invoice regulations by exchanging plain, unsigned PDF files by e-mail, which the recipient printed and dealt with as if they received the invoice as a paper invoice

[44] There can be a significant requirement for non-repudiation (that is, proof that data was sent to and from computers). For example, there are a number of corporate banks and investment funds in Poland (e.g. Nordea, Fortis) which seem to make their clients use a digital signature (not necessarily a QES) intentionally, to reduce the risk of a claim by the customer that they were not responsible for sending the communication in the event of a failed investment or late payment (but see the Russian cases: Olga I. Kudryavtseva, ' The use of electronic digital signatures in banking relationships in the Russian Federation' , Digital Evidence and Electronic Signature Law Review, 5 (2008) 51 – 57; Olga I. Kudryavtseva, Case note: Resolution of the Federal Arbitration Court of Moscow Region of 5 November 2003 N КГ-А 40/8531-03-П, Digital Evidence and Electronic Signature Law Review, 5 (2008) 149 – 151.) For a short time there was lobbying to enforce this at consumer banks, but it stopped very quickly when the banks realised it would effectively stop all consumer internet banking in Poland. In 2008 a number of experts, including representatives of Nordea bank and PIIT (Polska Izba Informatyki i Telekomunikacji – a telecom chamber) praised this solution in the public media: ' Banki przesądzą o e-podpisie' , 15 May 2008, Gazeta Wyborcza.

[45] Most QES applications require at least six steps to place a digital signature; longer for communications with a smart card. A number of invoices may be signed with one operation, but this would only work for companies who issue them once a month, for instance. In addition, some experts raised a need to use time stamping, because the certificate is only valid for two years, and the minimum life time of an invoice in Poland is five years. Each time stamp costs money, and takes a few seconds to complete, especially if a third party service is used.

[46] The simplest means of making an e-invoice authentic and integral is making it available for download from an SSL web site, either as printable text (as Google Europe does) or a PDF file (as cable operator UPC does). In the long-term (at least in e-invoicing terms), authentication and integrity can be provided by digitally signing the PDF with a commercial certificate, that can be generated automatically – many banks sending credit card statements already use this technique (although note the comments in Stefanie Fischer-Dieskau and Daniel Wilke, ' Electronically signed documents: legal requirements and measures for their long-term conservation' , Digital Evidence and Electronic Signature Law Review, 3 (2006) 40 – 44).

[47] Directive 2001/115/EC requires protection for the authenticity and integrity of the data, and presents a relatively open catalogue of technical means to achieve this, including advanced signature, QES and EDI.

[48] Zbigniew Domaszewicz, Rafał Zasuń, Leszek Baj ' Konflikt o elektroniczne faktury' , 17 June 2005, Gazeta Wyborcza; Zbigniew Domaszewicz, Rafał Zasuń ' E-faktury tylko na papierze' , 29 June 2005, Gazeta Wyborcza; Zbigniew Domaszewicz, ' Minister nauki podpisał rozporządzenie o e-fakturach' , 14 July 2005, Gazeta Wyborcza.

[49] Survey ' Wykorzystanie technologii informacyjno telekomunikacyjnych w przedsiębiorstwach' , (Glowny Urzad Statystyczny, 2007) (' Use of ICT-in companies' , Central Statistical Office), available at http://www.stat.gov.pl/gus/5840_wykorzystanie_ict_PLK_HTML.htm?action=show_archive; and by 2010 this number has risen only to 11 per cent, as shown in Itella Information survey (' Tylko 11% polskich firm wysyła elektroniczne faktury' , 16 June 2010, Gazeta Wyborcza).

[50] Sylwia Śmigiel, Piotr Poznański, ' E-faktura szansą dla firm' , 1 April 2009, article in Gazeta Wyborcza.

through the postal service. If they did not do this, it would not be possible to deduct the VAT – and it was virtually impossible for the tax inspector to prove that the document had not arrived by post.[51]

A positive example was Denmark where, from 1 February 2005, after creating a usable framework called OCES, it was made compulsory for both public entities and their suppliers to use e-invoices.[52] Since then, many countries have followed with flexible and purpose-oriented e-invoicing legal frameworks (Sweden, Finland, Italy, as mentioned in the European E-Invoicing Final Report). As result, more than 60 per cent of all invoices in use were electronic ones in Denmark as of 2007, including all invoices exchanged with the public administration.[53] The same applies for Swedish administration (Svefaktura), where invoicing savings are estimated at around 365 million euro over 5 years.[54]

Another case where Polish regulators insisted on the 'only a QES' approach, is when they tried to describe standard requirements for the electronic governmental gateway (ESP) that issued an electronic confirmation of reception: 'Urzędowe Poświadczenie Odbioru' (UPO) literally 'official reception confirmation'. The UPO should be automatically generated by the system, time-stamped and signed.[55] The problem was how to sign it. A QES cannot be used without human intervention, and all previous purpose-driven proposals to establish some less restrictive forms of signature were rejected based on the 'only a QES will be satisfactory' approach. Eventually, the regulator was forced to create a separate class of signatures, not tied to any certification tree, that are dedicated to signing the UPO.

On the other hand, an example on how giving up a qualified electronic signature has enabled electronic services, is the Polish revenue reporting service e-Deklaracje. When based on QES, its use was marginal (306 declarations were sent in 2007[56]). In 2009, for the first time, citizens could send declarations without a QES[57] – the simple sender authentication was based on the knowledge of the amount of tax paid the previous year. Even though this was only made available two weeks before the closing of the annual revenue reporting period (the end of April), over 90,000 citizens used it – this was probably by an order of magnitude more than the sum of any electronic documents sent by individuals to the administration over the past decade. In 2010, the number of tax declarations sent this way was 355,000.[58] The number of fraudulent submissions, jokes and other forms of misbehaviour predicted by the critics was zero in both years.

ZUS, an example of QES misunderstanding

ZUS, the Polish social insurance operator, introduced the digital signature in 1999, because it built a system that allowed companies to submit employee declarations electronically. It was initially based on X.509 certificates issued by an external Certification Authority on behalf of ZUS. The certificate was assigned to a company as a whole, it was software based (no smart card) and issued to companies for free. No design documents were ever published, but it seemed to work and to be close to an optimal compromise between security and usability.

In 2005, for reasons that have never been precisely explained, the government decided that ZUS would change over to using qualified electronic signatures. Obviously, the 200,000 companies that used to send their declarations to ZUS for free would have to pay for the certificate. In 2007, just before the conversion, there

[51] *In June 2009, a decision of the NSA (Naczelny Sąd Administracyjny) finally ruled that it is legal to send invoice contents in a PDF by way of e-mail, print it and treat as a paper invoice – without using technical means required for fully electronic invoicing (case I FSK 1444/09). This is, however, just one ruling in favour of one specific company and did not reduce the confusion for the others, as the tax authorities may, but are not forced to use this ruling in other cases.*

[52] *http://www.epractice.eu/cases/EID.*

[53] *In Denmark, the 'Act pertaining to public payments' was passed in December 2003. For more on e-invoice regulation, see 'European E-Invoicing Final Report', (European Commission Informal Task Force on e-Invoicing, 2007, Version 3.2 Final) http://ec.europa.eu/internal_market/payments/einvoicing/index_en.htm. Among other observations, the authors noted at page 22 that 'Given this penchant for overkill in signature requirements for electronic invoices, it should come as little surprise that EDI-based solutions tend to dominate in the market, since it is more flexible from a legal point of view.' In addition, the authors also remarked (page 22) that 'From a cross-border perspective, it should be noted that the necessity of an invoice being legally valid in both the sender's and the recipient's countries means that the strictest legal regime will determine the requirements to be met. Thus, a European e-Invoicing service provider under these conditions would be confronted with the arduous task of offering a solution that meets the most rigid European requirements (at least when the solution relies on electronic signatures), as any other solution would risk being invalid in stricter countries.'*

[54] *Ittela Information AB press release, February 2010; http://ipsec.pl/faktura-elektroniczna-e-faktura/2010/szwecja-finlandia-przeszly-juz-z-papierowych-na-elektroniczne-faktury.html*

[55] *'Rozporządzenie Prezesa Rady Ministrów z dnia 29 września 2005 w sprawie warunków organizacyjno-technicznych doręczania dokumentów elektronicznych podmiotom publicznym.*

[56] *Piotr Skwirowski, 'Już ponad 10 tys. PIT-ów złożonych przez internet!', 15 April 2009, article in Gazeta Wyborcza.*

[57] *It was possible only because the Ministry of Finance is not covered by the general regulation (Kodeks Postępowania Administracyjnego, KPA) that only allows QES for citizen to government communications.*

[58] *See the article 'Z e-PIT skorzystało ponad 355 tys. osób', Gazeta Prawna, 5 May 2010. The e-Deklaracje system is not perfect and has many deficiencies that limited the total number of people who were able to use it. For the first time, it used a modern approach based on availability, rational risk management and an open specification for the application programming interface. This approach seems to follow the attitude expressed in European Commission Decision 2009/767/EC, which also recommends usage of QES only where 'high level of security is needed' and after performing 'risk analysis'.*

were less than 10,000 active qualified certificates sold by Polish certification centres, most of which were bought by the public administration or organisations that were required to use QES by law in some part of their activities (for example, notaries and banks).

After the conversion, which is a perfect example of a market created by the government, the rush for qualified certificates started in 2008 and reached around 200,000 certificates, where it is now.[59] Contrary to what the people that advocated the use of qualified electronic signatures predicted, this enforced 'stimulus' did not cause an increase in interest among individuals, even if the ESP gateways mentioned above already existed (neither did it cause a predicted decline in the prices of qualified certificates). The estimated cost of the conversion for the private sector – ignored by most people speaking on this subject – was between 15 and 24 million euro, with an additional cost of 10 million euro annually. The cost of the conversion for ZUS is unknown.

The decision caused an avalanche of problems, apparently never predicted by whoever made the decision. First, the QES is associated with an individual person. For business continuity purposes, companies were advised to buy not one, but several certificates to ensure the declarations can be still sent if someone is not available because they are on leave, sick or otherwise not available. Large companies had to buy several certificates, to the amusement of companies selling certificates. Small companies did the opposite. To save money, they had one certificate, and everyone knew the password, making the whole QES model look like an amusing spectacle for laughter.

Second, a QES is issued to a named individual, so there is an assumption that when the QES is used, it was the person whose QES it is, who caused the signature to be affixed to the data. Now, ZUS knew with the highest confidence assured by a QES that Jan Kowalski purportedly sent a declaration for Acme, but ZUS did not know what relation Jan Kowalski was to Acme.[60] Jan Kowalski could be the company's accountant, the external accountant or a complete stranger, and ZUS had no way of knowing this.[61]

When this was first raised as an opportunity for forgery, ZUS correctly explained that it does not create any reasonable risk of forgery. Shortly after that, ZUS apparently decided that this gap, however, created a risk for the internal integrity of the data, and in 2009 introduced the idea that companies start buying attribute certificates[62] to confirm the relation between a physical person and a legal entity. In the meantime, the Ministry of Internal Affairs and Administration (MSWiA) announced that ZUS could potentially use a new, non-QES technique for authentication called a 'trusted profile',[63] that should go into production by the end of 2010. If this works, the QES 'silver bullet'[64] for ZUS would make a full circle to the point where it came from – back on a very bumpy and very expensive road indeed.

Conclusions

The QES does not solve all the issues between the administration, citizens and business regarding the trust to be given to its use. The qualified electronic signature is a high security and expensive technique suitable for relatively small set of business processes, probably slightly below the notary signature in the paper world. Large reports such as CROBIES[65] have a lot of exciting legal and technical discussions, but no solutions for the simple needs of citizens that have nothing to do with information technology. With the endless theoretical and legal discussions, it is possible that some EU Member States will continue to discuss a second or even a third wave of e-signaturism.[66]

If, after twenty years of X.509 and ten years of advanced electronic signatures, all the items set out in the CROBIES diagram entitled 'Key success factors of eSignatures' are red and marked as 'insufficient' or 'inappropriate',[67] then it means that the concept ought to be reconsidered, and it cannot be resolved by slightly changing interpretations of Directive 1999/93/EC. Perhaps it is time to rethink the whole concept of the

[59] *Unizeto, 'Kalendarium e-podpisu w Polsce', 2009.*

[60] *The company name is optional in the Polish qualified certificate profile.*

[61] *Qualified certificates sold in Poland can contain company name but they are not guaranteed, even if the company sponsors the certificate. At some point, some certification authorities started to discourage certificates with a company name because this would potentially create issues when a certificate is used for personal purposes.*

[62] *RFC 3281 – An Internet Attribute Certificate Profile for Authorization http://www.ietf.org/rfc/rfc3281.txt. While a X.509 certificate binds an identity to a cryptographic key in a certified manner, the attribute certificates are third-party certified confirmation of something that the person is allowed to do.*

[63] *'Zaufany profil' ('trusted profile') – a new single sign-on like technique for identity federation in the public administration services. Little details are known about this at the time of writing, but it will be most probably based on non-qualified digital signature and SAML (Security Assertions Markup Language).*

[64] *The term 'silver bullet' is a colloquial term that is often used to express the view that the invention will solve all the problems.*

[65] *CROBIES - Study on Cross-Border Interoperability of eSignatures: http://www.sealed.be/reports.htm.*

[66] *Editor's note: much of the legal discussion in the reports issued by the EU only concentrate on digital signatures (also known as advanced electronic signatures), and significantly fail to mention any of the relevant case law relating to all the forms of electronic signature that are reported in this journal and set out in Stephen Mason, Electronic Signatures in Law (2nd edn, Tottel, 2007).*

[67] *Study on Cross-Border Interoperability of eSignatures (CROBIES), Head Document, Figure 2, page 10 (version 1.0 29.3.10).*

Directive.

The present legal framework has approached electronic signatures by attempting to build a 'universal theory of everything' and too little discussion has been given to the forms of electronic signatures that are actually used every day, and to technical products that act to help provide for security. Even if the 'what authors of Annex III really meant' type casuistry is finished with a consensus by the experts (whoever they may be) at around 2020, no one will be interested in the solution. The world will have move forward, new problems will appear, and by that time any potential savings to be obtained from simpler solutions that could have been provided quickly will have failed to be made.

This article sets out a number of reasons why the qualified electronic signature alone is never going to work. The various products based on the model of Directive 1999/93/EC – advanced signature, advanced signature with qualified certificate and the latter with SSCD – can all be considered options, depending on how much security is required by a given process. Processes should be designed in respect of the purpose, not the other way around. Risk analysis and cost-benefit analysis should be used to select adequate techniques and then they should be amended by how easy they are to use and common sense.

There are some good examples in the Commission activities relating to electronic authentication. The first was the Commission Decision 2009/767/EC mentioned above. Another is the IDABC Authentication Policy, a document that was published in 2004 as part of IDABC,[68] and the aim of the document is to demonstrate the purpose of authentication and how it can be used for useful services. In the Policy, the European Commission produced reasonable guidelines to establish controls that are proportional for generic public administration processes that can be used as a template for the design of the establishment of trust for public or private systems.[69] The European Interoperability Framework[70] is another good set of guidelines that can be used to form usable services and – eventually – to start making individual lives easier.

Paweł Krawczyk is an information security consultant based in Krakow, Poland; he has experience in the design and assessment of information security systems; he is holder of the CISSP certificate.

http://ipsec.pl/

pawel.krawczyk@hush.com

[68] *IDABC (Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens); ' European Interoperability Framework for Pan-European eGoverment Services' , version 1.0 which apaers to be the ' final' version http://ec.europa.eu/idabc/en/document/3473/58*

[69] *The document contains a consistent sequence of organisational and technical controls, starting from registration of users up to their authentication as they use the system. All typical techniques are taken into account – passwords, one time passwords, software signature and hardware signature. All are assigned relative security strengths. A list of business processes is produced and assigned relative security requirements. At the end, these two lists are matched.*

[70] *European Interoperability Framework 2.0 (draft) http://ec.europa.eu/idabc/en/document/7728.*