Article

The probative value of digital certificates: Information Assurance is critical to e-Identity Assurance

PATRICK MCKENNA

Abstract

It is widely acknowledged among all echelons of global organizations and governments alike, that the Internet is a critical global infrastructure to the information society. This critical global infrastructure offers much to the twenty-first century; however, it has already become synonymous with misuse, abuse and the emergence of a new vocabulary that includes cyber terrorism, cyber trust, cyber fraud and identity theft, to mention a few. Furthermore, these vulnerabilities of the information society (information infrastructure) have become more prevalent in recent times.

Whilst this is not a desirable state for the information society, it has focused attention on internet identities. In particular, there is a growing body of opinion that shares the view that it is the cloak of anonymity that fuels such undesirable and sometimes illegal use of our information infrastructure (internet).

In short, this all adds up to a general mistrust of the internet, especially where it concerns the exchange of sensitive or confidential information. If the internet is to mature into a trustworthy utility-like infrastructure and a medium in which both consumers and producers of information can have implicit faith, then we must look to other trusted utility infrastructures and services and the way they operate. In general, these same producers and consumers use electricity, water and gas, for example, and rarely question the integrity of those infrastructures that provide the life-support to economic and social activity. These critical services are regulated because of the potential risk to public safety, and the consumers and producers of such services are not anonymous.

In contrast, cyber trust is now considered by many observers to be a risk to public safety because of our increasing dependence on the internet. Yet we really cannot be sure about the genuineness of the identities that participate in information exchanges on the internet. In addition, we cannot be confident that a person claiming to be a doctor, lawyer or police officer, for example, is their genuine role at any given time. There is also general agreement emerging that some form of regulation is now required in order to restore confidence and trust in the internet as a safe environment in which we can exchange information. This leads us to many challenges, not least of which is, how can we regulate anonymity?

This article will offer a view that it is the registration business processes, employed to bind real-world personal and professional data to a digital certificate that is crucial. These registration business processes are critical because they have a direct bearing on the probative value of a digital certificate. These registration business processes will need to enable each information society individual to declare his or her (or the organizations') genuine digital identities (digital certificates) and contribute to a safer information infrastructure by removing the opportunity for identity theft and identity plagiarism that exists on the internet today.

Such registration business processes will need to consider carefully regulation and legislation, digital identity (certificate) lifecycle management and information assurance. The registration business processes will need to scale and be available to all real-world custodians of trust: those organizations and employees engaged in the exchange of sensitive medical, legal, scientific and commercial information over the internet. Control of registration would be done as part of a Certification Authorities policy or certification practice.

In the United Kingdom, tScheme is the industry-led, self-regulatory, not-for-profit organisation that was set up to create strict service criteria and to approve electronic trust services, including qualified certificate services. tScheme plays an important

In particular, there is a growing body of opinion that shares the view that it is the cloak of anonymity that fuels such undesirable and sometimes illegal use of our information infrastructure (internet) role by assuring that Trust Services meet rigorous quality standards so that we can have confidence in online identities.

The Public Key Infrastructure (PKI) landscape

There is no doubt that the future of PKI and digital signatures represents one of the more complex technology and legal debates. The spectrum of opinion ranges from a complex technology in search of a problem, to a panacea, to the challenge of establishing identity as we live in a digital society.

Whilst PKI is a mature technology and has been around for a number of years, it remains poorly understood. PKI represents a single technology solution to the problems surrounding confidentiality, authentication and non-repudiation; it is supported in most major technical security standards; it is integrated into applications such as Microsoft's Windows Server 2003, and it is one form of electronic signature that is acceptable within the legal framework of the European Union Directive on electronic signatures,[1] adopted by many of the Member State legislatures.

PKI provides us with an important security component for enterprise security and overlaps into other important areas such as secure login with smart cards, file and folder encryption (EFS), web services (SSL) and secure e-mail.

Microsoft, for example, considers PKI as a core technology for its future products, and their approach has been to embed PKI as a core infrastructure component. This Microsoft decision to embrace PKI as a core component means that it can be exploited transparently by many business applications. More importantly, this will reduce dramatically the costs of deployment and administration of PKI, which is well known for being an expensive technology. This is an important enabler to widespread adoption of PKI technology.

What concerns the Chief Information Officer?

There is an abundance of PKI technology offerings from many vendors; however there remains little appetite to adopt these PKI solutions beyond internal perimeter security i.e. a closed system. This is explained by the consensus expressed by many leading Chief Information Officers (CIOs). These CIOs hold responsible positions in large multinational companies and they are not complacent. It is their view that PKI is too expensive, difficult to implement and not user friendly. More importantly, even successful internal deployments of PKI, referred to as closed systems, have no return on investment.

It is the potential for increased efficiencies in complex supply chains and commercial exchanges with customers over the Internet (an open system), where returns on investment will lie. This represents a fundamental shift in the context of the problem to be solved. More precisely, the scope of this problem domain extends beyond that which PKI alone can solve.

This shift, from one of internal use of PKI technology and digital certificates to bolster perimeter and internal security, to using this technology with their supply chains and customers, introduces further challenges. This exposure places an increased emphasis on the significance of information assurance about those digital identities, which will later be relied upon.

It is now more commonplace for the CIO to be a member of the board of directors who share responsibility for corporate governance. Corporate governance needs control of, and assurance about, the information upon which it basis its decisions. The organization needs to know that information is from a genuine and trustworthy source. To know that the source of information is genuine is to know that identity of that source is genuine.

This can be summarised as follows: corporate governance requires information governance; information governance requires information assurance and information assurance requires identity assurance. Many CIOs highlight the limitations of a PKI technology alone, when it comes to linking a digital certificate to our personal, professional and corporate notion of identity, in order to prove we are who we say we are, and prove we are what we say we are, to the outside world. PKI and digital certificates are employed to secure websites and servers with little difficulty. However, binding a digital certificate with a person or an organization's identity is an entirely different challenge that raises many problems that are more business and legal, rather than a technology issue alone, and for which there is no appealing software solution.

Invariably, these challenges concern the information assurance aspects of the digital certificate content. Who controls the registration process? What control does the individual have over the content and accuracy of his or her digital certificate?

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ 19.1.2000 L13/12).

Many other end-user issues translate into: how safe is my personal data; collection of evidence of identity seems to be arbitrary; collection of evidence of identity is for the most part a manual process; it is difficult to understand why a digital certificate can be trusted; there is too little transparency. In short, it is too much trouble and too labour intensive, particularly for large organizations.

These are significant barriers to the widespread adoption of digital certificates for both individuals and organizations. An efficient, automated registration business process that is consistent, transparent and user-friendly, would go some way towards solving the problems. Such a registration business process would need to offer full lifecycle digital certificate management. Furthermore, if the registration business process were to implement the burden-of-compliance on behalf of the organization, this would be significant to overcoming these obstacles.

Registration

A robust registration business process, if supported by a software system, would serve to allay many of those genuine societal fears about identity management, whilst at the same time engaging their vital cooperation in declaring their digital identities. This is crucial to removing the cloak of anonymity that plagues the internet.

Fundamental to any registration business process solution is the International Telecommunication Union's ITU-T Recommendation X.509v3 (1997) | ISO/IEC 9594-8: *Information technology - Open Systems Interconnection - The directory: Public-key and attribute certificate frameworks* ('X.509v3'). This technical standard underpins any viable solution. However, on its own, this standard is not intended as the solution to the additional challenges of registering people and organizations for digital certificates.

The business of registering individuals and organizations for digital certificates involves processing personal, professional and other data that may be conferred on individuals in the context of employment or some other affiliation. The scope of any solution that binds real-world identity data to digital certificates now includes observing all the legal and regulatory requirements associated with processing such data.

What has become increasingly important, and the focus of attention of many CIOs, is the significance of a registration layer that is part of the underlying PKI technology; the registration business process. Like any legislation, the legal requirements are expressed in a technology-neutral fashion. It is also worth noting that the application of such legal requirements is not necessarily confined to the United Kingdom and Europe. In addition, as examples, there are specific sector requirements such as the European Health Informatics Standards (ISO Technical Committee 215 on Health Informatics) and the requirements of International Air Transport and Aerospace (IATA Standardising Digital Certifications in Global Air Transport - The Digital Certification Working Group (DCWG)).

In terms of European Health Informatics Standards, our personal medical information is regarded as the most sensitive information that is now exchanged over the internet. The healthcare industry is rigorous in its efforts to provide appropriate protection for that data conveyed across the internet in a practical, cost-effective way. It is no surprise to find that this standard (International Standards Organization Technical Committee 215 on Health Informatics three-part specification *Health Informatics - Public Key Infrastructure* 2001) is lengthy and rich in the detail of what is required of a registration business process.

The Digital Certification Working Group (DCWG) of IATA's Standardising Digital Certifications in Global Air Transport is a subcommittee of the Aerospace Focus group that was given a task in 1999 to come up with a standard methodology for the acceptance of X.509 Certificates and digital signatures. Since then, the committee has been informally adopted by the International Air Transport Association TICC-DART group, as well as IATA's E-Business Initiative. This international collaboration includes such names as Rolls Royce, British Airways, Boeing, Airbus and General Electric, who have worked together to agree common requirements for their sector. tScheme also provides many service approval profiles, one of which is the 'Profile for Registration Services' that defines the requirements for the verification and registration of identity and other attributes. A registration business process will be expected to meet these general and sector specific requirements.

The business of registration: United Kingdom

In the United Kingdom, the registration process will need to consider carefully new and emerging legislation. The following is not an exhaustive list, and registration will need to be transparent about observing such legal requirements: as the

What is important and helpful to recipients is to be able to see enough meaningful information in a digital certificate to support any judgement about the probative value of that certificate

Electronic Communications Act 2000; Electronic Signatures Regulations 2002; Data Protection Act 1998; Regulation of Investigatory Powers Act 2000 and *Freedom of Information Act 2000*.

Further to these legal requirements, the central sponsor for information assurance in the Cabinet Office of the United Kingdom government has developed and issued guidance documents on the government's requirements for the verification of identity.[2] These documents, which are detailed technical documents supporting the Registration and Authentication Framework, describe the minimum evidence that needs to be presented by an organization or an individual in order to be issued with a digital certificate: a digital certificate which, it can be said with degrees of confidence, is genuine.

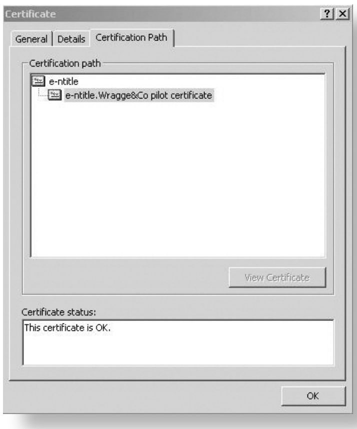
A registration business process can provide digital certificates that have a higher degree of probative value if the registration process is transparent, offers regulatory compliance, and information assurance about the genuineness of digital certificates to owners and recipients.

The probative value of a digital certificate is partly judged on the basis of the registration process. What is important and helpful to recipients is to be able to see enough meaningful information in a digital certificate to support any judgement about the probative value of that certificate. They also need to be assured about the accuracy of the information declared in the digital certificate. Furthermore, when a recipient is aware that the registration process has captured more information than that declared in the associated digital certificate, which can be made available to the recipient, this contributes further to the evidential or probative value and trust.

Recipients can decide whether to trust such a digital certificate because they trust and have confidence in a rigorous and transparent process of registration that the owner of the certificate went through before being issued a digital certificate. Moreover, when the registration process is controlled and operated by the employing organization, for instance, which has a vested interest in the good stewardship of all matters relating to their e-business, this too can be well received by recipients. This approach serves to build on the real-world relationships that already exist between the parties.

The evidential value of a digital certificate: an e-conveyancing lawyer

The legislation contained in the *Land Registration Act 2002* covers the groundwork for e-conveyancing, by giving equal status to electronic versions of the documents currently used in the conveyancing process. The following example illustrates what is meaningful to recipients such as solicitors, conveyancers, lenders and possibly Land Registry staff, when engaged in e-conveyancing transactions.



Certification path

e-ntitle

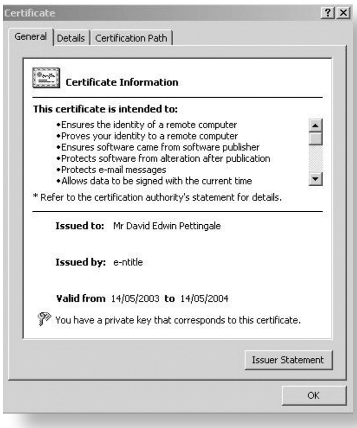
e-ntitle.Wragge&Co pilot certificate

Certificate status:

This certificate is OK.

Figure 1: The Wragge & Co LLP signing certificate is highlighted

Wragge & Co is a law firm and keen advocate of the emerging e-conveyancing market. Figure 1 illustrates their signing certificate that they use to sign employees' digital certificates requests during their registration process. David Pettingale is such a partner at Wragge & Co.



Certificate Information

This certificate is intended to:

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Ensures software came from software publisher
- Protects software from alteration after publication
- Protects e-mail messages
- Allows data to be signed with the current time

* Refer to the certification authority's statement for details.

Issued to: Mr David Edwin Pettingale

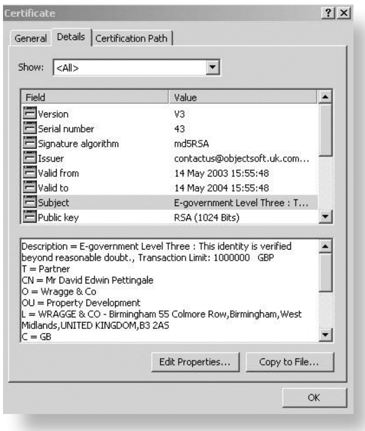
Issued by: e-ntitle

Valid from 14/05/2003 **to** 14/05/2004

You have a private key that corresponds to this certificate.

Figure 2: David Pettingale's digital certificate

[2] The reader is referred to http://www.cabinetoffice.gov.uk/csia/ for further detail. See also, at the time of writing, further detail is available at the following links: UK HMG's Registration & Authentication Framework v 3.0 http://www.knowledgenetwork.gov.uk/co/kimscsia.nsf/0/B372BF9C716556F980256EB60051ADD5/$FILE/Registration & Authentication V3.0 Sept 2002.pdf?openelement; UK HMG's minimum requirements for the verification of the identity of Individuals http://e-government.cabinetoffice.gov.uk/assetRoot/04/00/08/52/04000852.pdf; UK HMG's minimum requirements for the verification of the identity of organizations http://e-government.cabinetoffice.gov.uk/assetRoot/04/00/08/55/04000855.pdf.



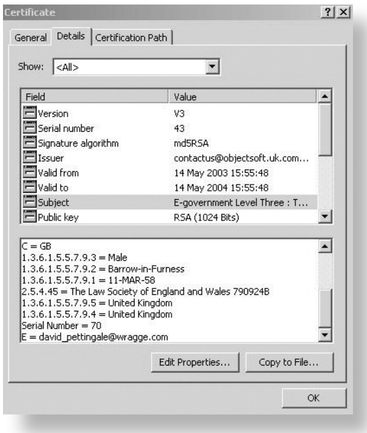
Show: <All>

Field	Value
Version	V3
Serial number	43
Signature algorithm	md5RSA
Issuer	contactus@objectsoft.uk.com...
Valid from	14 May 2003 15:55:48
Valid to	14 May 2004 15:55:48
Subject	E-government Level Three : T...
Public key	RSA (1024 Bits)

Description = E-government Level Three : This identity is verified beyond reasonable doubt., Transaction Limit: 1000000 GBP
T = Partner
CN = Mr David Edwin Pettingale
O = Wragge & Co
OU = Property Development
L = WRAGGE & CO - Birmingham 55 Colmore Row,Birmingham,West Midlands,UNITED KINGDOM,B3 2AS
C = GB

Figure 3: the registration process stores the additional registration data that corroborates the claim 'This identity is verified beyond reasonable doubt in accordance with government criteria' declared in David Pettingale's digital certificate

The subject of a digital certificate, highlighted in figure 3, declares that David Pettingale is a partner of the firm and is employed in Property Development. In this instance, a transaction limit and currency are also declared. This level of detail is helpful to recipients when making a judgement about the evidential value of David's digital certificate.

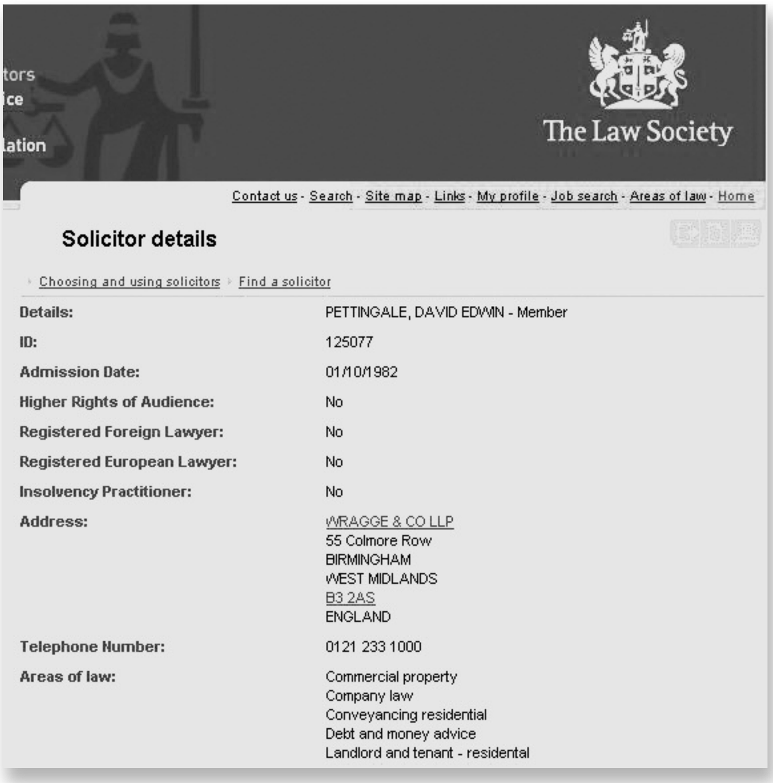


Show: <All>

Field	Value
Version	V3
Serial number	43
Signature algorithm	md5RSA
Issuer	contactus@objectsoft.uk.com...
Valid from	14 May 2003 15:55:48
Valid to	14 May 2004 15:55:48
Subject	E-government Level Three : T...
Public key	RSA (1024 Bits)

C = GB
1.3.6.1.5.5.7.9.3 = Male
1.3.6.1.5.5.7.9.2 = Barrow-in-Furness
1.3.6.1.5.5.7.9.1 = 11-MAR-58
2.5.4.45 = The Law Society of England and Wales 790924B
1.3.6.1.5.5.7.9.5 = United Kingdom
1.3.6.1.5.5.7.9.4 = United Kingdom
Serial Number = 70
E = david_pettingale@wragge.com

Figure 4: David Pettingale's Law Society number, place of birth, date of birth, country of citizenship and country of residence are declared


tors
ice
lation
The Law Society
Contact us - Search - Site map - Links - My profile - Job search - Areas of law - Home
Choosing and using solicitors
Find a solicitor

Solicitor details

Details:	PETTINGALE, DAVID EDWIN - Member
ID:	125077
Admission Date:	01/10/1982
Higher Rights of Audience:	No
Registered Foreign Lawyer:	No
Registered European Lawyer:	No
Insolvency Practitioner:	No
Address:	WRAGGE & CO LLP 55 Colmore Row BIRMINGHAM WEST MIDLANDS B3 2AS ENGLAND
Telephone Number:	0121 233 1000
Areas of law:	Commercial property Company law Conveyancing residential Debt and money advice Landlord and tenant - residental

Figure 5: The results of a search on the Law Society's website

Figure 5 illustrates that David Pettingale is a current member of the Law Society of England and Wales. However, the ultimate source of authority on his current role and responsibilities is the employing organization, Wragge & Co. who registered, processed and issued his digital certificate.

Federated identity management

Trust belongs to people and organizations, rather than technology. The significance of a registration process is that it is a socio-technical solution that fosters 'Federated Identity Management for the Information Society'. It is an answer that is owned and operated by organizations in their role as custodians of their digital identities. However, the challenge to the software and technology community is to provide such a socio-technology (not merely a technology) so that organizations and people have the autonomy to manage and control it.

It is the absence of a formal, consistent, transparent, efficient and auditable system of registration that utilises standard cryptography and PKI that deters many organizations from adopting PKI on a large-scale. It is important to organizations that a system of registration is capable of dealing with greater volumes of transactions so that they can accrue the many benefits that PKI can offer them.

There are both common and variant complexities involved in binding genuine real-world identities with digital certificates. In addition to technical standards such as ITU-T X509, it is the new and emerging legislation that a registration process needs to consider carefully.

The vulnerabilities of the information society (information infrastructure) can largely be attributed to a cloak of anonymity that discourages many of us from exchanging sensitive information using the internet. We, as an information society (individuals, information workers, organizations and decision makers), can help remove the cloak of anonymity by registering and claiming our own digital identities. This is a small effort by each individual that collectively can have an effect on the information society. It reduces the opportunity for identity theft.

Information is the life-support to decision-making; we usually trust information because we know and trust the identity of the source of that information. We need to claim and protect our own digital identities so that we can continue to be trusted as the genuine identity (genuine source of information) when using the internet. ■

■ Acknowledgments

Thanks to Mr David Pettingale for his permission to include his digital certificate in this article; also to Wragge & Co LLP, and the Law Society of England and Wales who have kindly given their explicit consent to use the references in this article.

Patrick McKenna is a software architect and the founder of Objectsoft®. He graduated from Dundalk Institute of Technology (Ireland) followed by postgraduate studies in Information Engineering and Computer Studies at Sheffield Hallam University. His 20 years IT experience include lead architect on large-scale, high-risk projects such as the successful de-regulation of the United Kingdom Gas Industry that provided for domestic competition.

patrick.mckenna@objectsoft.uk.com
http://www.objectsoft.uk.com