Panel Statement - Achieving Global Trust in an e-World

Panel:

Chairman:	**Richard G. WILSHER**	(the Zygma partnership, GB)
Panelists:	**Michael S. BAUM**	(VeriSign inc., US)
	Caelen KING	(Baltimore Technologies plc., IE)
	Helmut KURTH	(atsec GmbH, DE)

Abstract:

The NISSC has a long and respected heritage as an important event in the field of information security. Its origins lie in the defence arena, which has naturally been subject to a very national perspective. However, in recent years the influence of 'infosec' has spread pervasively into the commercial domain; in that time its scope has also become fundamentally international. This panel has come about because its members believe that it is appropriate for the NISSC to adopt now a broader approach and to reach out to a much wider international audience. Perhaps the true start of the new millennium, the year 2001, could be the start of IISSC - the International ISSC?? In regard to this suggestion:

The panel will adopt the position that for businesses and individuals to truly benefit from e-commerce, technical inter-operability is neither the key issue nor a challenge. Rather, users need to know that trust in their service providers is justified, that they are subscribers to open services with no barriers to with whom they may communicate, and that they can rely upon the identity of their counter-parties throughout the trading chain.

The panelists will what ask what 'trust indicators' are really required to establish trust in an e-world. They will question the contribution that standards make and look to other means of assessing service providers, to give confidence to business and private users who. Reference will be made to activities on-going in Europe, the US and other parts of the world to address these issues, covering work done to identify real trust indicators, various international and regional rules governing the use of electronic signatures, a scheme being developed by European and global organisations to establish a world-wide trust infrastructure and efforts to establish standardised policies and conformance profiles.

This session will bring to a largely US audience some specific European perspectives and awareness of ongoing work. It is intended to be interactive, even provocative: members of the audience will be invited to respond and debate the issues in terms of the relevance of this work to the US business environment and exploring ways in which joint co-operation could be fostered.

Point of Contact:

Richard G. WILSHER, +44 12 45 40 15 24, RGW@Zygma.Co.UK

Richard WILSHER:

Bio: An independent specialist in the field of electronic signatures and trust(ed third party) services. He is closely involved with various European initiatives in this area as: an expert within the European Electronic Signature Standardisation Initiative; a specialist advisor to two projects establishing approval schemes (one in the UK specifically, *tScheme*, and another at the international level); a consultant to private clients establishing services or businesses based upon services in this field.

Thesis: Whilst large organisations can support the budgetary needs to operate or out-source their own (closed) PKIs, small enterprises (which constitute in excess of 90% of businesses in Europe, North America and Oceania) need publicly-offered and widely recognised electronic signature services.

This can only happen if the providers of supporting services can demonstrate their compliance to a standard of service provision which is widely recognised and which enables businesses to benefit from being able to carry out seam-free global e-commerce. Industry itself, in partnership with government, is best-placed to lead in the development of these concepts.

Europe is establishing a lead in how this can happen - North America and Oceania need to respond to these moves and would be welcome partners in developing the trust infrastructure required to allow businesses to prosper in an e-world. Until there is such a global move, e-commerce participants will be restricted in the way they can conduct their business.

Richard Wilsher will describe the work being undertaken within EESSI, the *tScheme* developments in the UK and broader efforts to make this more international within Europe and beyond. He will, at the end of the panellists' presentations, invite discussion as to what the major international issues are and how these could be addressed through co-operation, to develop fully solutions which can be adopted in the international arena.

Helmut KURTH:

Bio: Helmut Kurth has a career in the area of Information Security spanning almost 20 years. He developed the German Information Security Evaluation Criteria, which first separated functionality from assurance. This general principle was later adopted by the European Evaluation Criteria (the ITSEC) and the Common Criteria. He was active in the development of security products and the integration of security technology into large Information Systems. This also included the integration of public key cryptography into business processes from a technical as well as a management and organisational point of view. Helmut Kurth is now working for atsec information security GmbH as the Technical Director and Chief Scientist. He has been active in international standardisation of Information Security and has given numerous presentations on international conferences.

Thesis: Many organisations claim they need a PKI but only few of them have a well developed business case how to use this PKI. When developing such business cases one will recognise very often that the processes defined in current PKI technology does not match the business processes. PKI seems to be a technology that has been developed with no clear business application in mind and now faces the problem that the integration with e-commerce transactions is hard. One of the main reasons is that the PKI solutions offered today do not fit well into the existing trust relationships. As a result the acceptance of digital certificates for e-commerce is low.

Achieving global trust in an e-world sounds wonderful but this will probably not happen within the foreseeable future. A network of trust built upon sound contractual relationships is the way trust has been established between business partners since more than 2000 years and I don't believe that a new technology like public key cryptography will change this. This technology can assist in commerce but it will not change the way we do commerce! And especially public key certificates alone will not define any new trust relationship. My thesis is: Public key certificates will only used between business partners that have trust relationship established on a sound contractual and legal basis. Within such a relationship they can and will be used to authenticate the partners and authorise business transactions. But in those cases many architectural features of today's PKI systems and the way digital certificates are structured do not fit very well. Therefore I think we have to re-think the technical application of public key cryptography for e-commerce and not focus on technical solutions that have been developed without real business applications in mind.

A full paper accompanies this thesis.

Michael BAUM:

Bio: Michael S. Baum serves as Vice President of Practices and External Affairs, VeriSign, Inc. His responsibilities include developing and overseeing practices and controls under which VeriSign conducts its Digital ID and VeriSign Trust Network operations; and legislative oversight.

Mr. Baum serves as *Chairman*, Information Security Committee within the American Bar Association; a *Commissioner*, the Electronic Health Network Accreditation Commission; *Chairman,* International Chamber of Commerce (ICC) ETERMS Working Party, an *Observer Delegate* to the United Nations Commission on International Trade Law (UNCITRAL) on behalf of the ICC; *Member of the Board of Directors*, the PKI Forum, and a member of various digital signature legislative advisory committees.

Mr. Baum is *co-author* (with Warwick Ford) of Secure Electronic Commerce (Prentice Hall, 1997), *primary author* of VeriSign's Certification Practice Statement (1996), *author* of Federal Certification Authority Liability and Policy – Law and Policy of Certificate-Based Public Key and Digital Signatures (NIST, 1994), *co-author* of Electronic Contracting, Publishing and EDI Law (Wiley Law Publications, 1991), *contributing author* to EDI and the Law (Blenheim Online, 1989), and the *author* of diverse information security publications including the first American articles on EDI law. He served as *Guest Editor* for the Jurimetrics Journal *Symposium on PKI* (July 1998); honoured as an *EDI Pioneer* in 1993 (EDI Forum), and recipient of the National Notary Association's *Achievement Award*. He is a member of the Massachusetts Bar, an MBA graduate of the Wharton School, and a Certified Information Systems Security Professional (CISSP).

Thesis: See accompanying paper.

Caelen KING:

Bio: Product Marketing Manager at Baltimore Technologies, he is responsible for marketing Baltimore UniCERT Options™, a range of Public Key Infrastructure (PKI) products that are essential e-business enablers. Since joining Baltimore in 1997 Caelen has moved from Professional Services, were he worked on some of the world's first PKI deployments, to creating marketing campaigns and directing product direction.

Caelen is a regular speaker and lecturer in the field of e-security.

Thesis: There are three commonly perceived problems facing trust in the digital world: Technology, Policy and Human/cultural acceptance. Of the three, most emphasis has traditionally been placed on the technology and to a lesser extent policy issues. We are finally getting to a stage in Europe where there seems to be light at the end of the legislative tunnel; however, like technology, there will always be work to be done.

When analysing what is necessary in legislation to equate digital signature with hand-written signatures it is important to take note of the features of hand-written signatures. Traditional signatures have limitations and disputes commonly have to be settled in court. There is no standardisation on how a signature is formed, various different levels of authentication are possible and the context in which the signature is formed (duress, age etc.) has to be taken into account.

Germany and Italy both enacted their own legislation and this led to a fear that Europe would have to deal with 15 or more different set of legislation. This is something that the European Commission (EC) is actively trying to discourage. As a result the EC proposed to the Member States a Directive with the purpose of harmonising the rules and allowing for cross border legal trust to be established.

However, while legislation is undoubtedly important, is not absolutely necessary for digital trust to be established. For example, common usage of a driver license is proof of age; however, rarely either is a drivers license issued with such an intent or is there to legislation support that usage. The Australian Tax office is issuing ?electronic signature certificates for the purpose of tax returns. However, a secondary goal is for these certificates to have an accepted use of allowing B2B secure communication. Legislation is no panacea for trust.

Caelen will briefly discuss the initiatives taken by Germany, Italy and the European Commission. Allowing for successful acceptance of the Commission's guidelines, what will be the affect on e-business within Europe and world-wide? How will legislation affect cultural acceptance, if at all?

Target Audience:

The audience should be business-focused, or technical with a clear view of hoe technology supports and enables the business: Business Managers/Directors, Technical Managers/Directors, Risk Managers/Directors,. Those providing, and those building businesses based upon, trust services will be well-suited to participate, as will those having a legal or regulatory interest in this area. We are looking for genuine audience participation.

The Meaning of Trust on the Internet

Achieving trustworthy services for global e-business NISSC

Michael S. Baum, JD, MBA, CISSP
michael@verisign.com

Thesis: There are many perspectives on the underpinnings of trust on the Internet, perhaps the two most recognized perspectives can be characterized as the *pecuniary* and *security* views. Pundits espousing one or the other of these views have tended to discount the other. This presentation introduces and acknowledges the importance and limitations of each, and urges the inclusion of a third trust anchor*: assessment and accreditation* The presentation includes a relevant discussion of the PKI Assessment Guidelines (PAG) developed by the Information Security Committee, American Bar Association.

Trust is a highly subjective concept, just as love and humor. It is vexing to quantify, highly subjective depending on the particular circumstances and the parties involved, and yet essential. The challenge in defining trust may be akin to the highly celebrated challenge that the Supreme Court faced in defining pornography ("I know it when I see it."). Nonetheless, the importance of trust to the Internet demands that we focus attention on how to achieve and maintain it.

Perhaps the two most recognized viewpoints on trust can be summarized as follows:

- **The pecuniary view**: Trust is a function of the extent to which a promisor can "back up a promise", pay damages, and otherwise guarantee one's performance. Money talks! Nonetheless, the limitations on the effectiveness of the first view can be discerned from the following story about a brain surgeon.
- **The security view**: Trust is a function of the extent to which a promisor has deployed reliable security services and has responded effectively to the attendant risks.

As to the pecuniary view, there is no doubt that money talks! Nonetheless, without security there is no protection against becoming a victim. The pecuniary view may only provide some financial recovery following injury. The limitations to the pecuniary view can be discerned further from the following story.

> ***Who will you trust?*** Imagine that you require brain surgery and are given the choice of two surgeons: Dr. Pecuniary and Dr. Security. Dr. Pecuniary will not only fully guarantee the surgery, he will compensate any patient in an amount of 1000X (the $10,000 fee for the surgery). Dr. Security offers no guarantees. Oh yes, I forgot to mention that Dr. Pecuniary[1] graduated from medical school six months ago; and Dr. Security is board certified and chief-of-staff for Neurosurgery of the Johns Hopkins Medical Center.

The obvious conclusion is that the pecuniary view is not an effective substitute for security as a sound basis for trust – the synergy of both is a much more compelling proposition. However, there is a third dimension to the provision of effective trust over the Internet – a dimension that derives from the Reganesque sound bite: *trust but verify*. Such verification is a function of assessment and accreditation.

Assessment refers to a procedure for determining whether a system or sub-element (PKI for instance) satisfies a set of defined criteria. Generally, the goals of PKI assessment are ultimately intended to provide assurances of trustworthiness and quality. Meaningful and efficient PKI assessment is best facilitated if the number of assessment methodologies and programs are limited to no more than a few widely recognized models. The challenge is to ensure that the limited assessment models are responsive to the targets of such assessments. It is not surprising to observe a healthy competition among assessment models and programs. Indeed the race has begun to win the hearts and minds of the global PKI community.

***

[1] Oh, and I forgot to mention that Dr. Pecuniary is the defendant in two pending malpractice suits.

Reflections on Trusting Third Parties

or why it is hard to sell a certificate

Helmut Kurth
atsec information security GmbH

Summary

We have been told for many years now that digital certificates issued by a "Trusted Third Party" are essential for doing electronic business. As a consequence many "Certification Authorities" (CA) have established themselves as such „Trusted Third Parties" to issue (X.509) certificates for public keys. Many of them claim to have the goal to establish the basis for e-commerce and hope to issue a large number of certificates to almost everybody in the world.

But there are some simple questions that almost nobody seems to ask. We nevertheless now want to ask those questions to get away from the myth that digital certificates solve the world's problem with e-commerce. Just to avoid a misunderstanding: There is no doubt that public key cryptography will play its role in electronic business, but probably in a way different to that proposed in the past.

Other people have addressed similar concerns. Carl Ellison and Bruce Schneier have addressed some problems in [1] dealing especially with the problem of trust in a CA and the technical components used to issue and manage certificates and private keys. We will address an even more fundamental question: Do we need X.509 certificates at all for electronic commerce? How useful are they? Do we need something else in addition to our current models, or are they just a good solution to a problem that nobody has?

This paper will try to contribute in a constructive way on the use of public key cryptography for electronic business but will also raise considerable concern on the usefulness of the model of X.509 certificates within the context of e-commerce.

A few Questions

Let us start with the simple question: What are we using digital certificates for and how important are those issues for e-commerce?

As everybody knows digital certificates are used to "bind" a public key to a person, allowing the person to authenticate himself to other parties by proving the possession of the associated private key. This sounds good, but we should ask ourselves:

Question 1: How important is authentication of persons for today's commerce?

To analyse this, let us look on the way "commerce" is done today (oh yes, there was "commerce" before "e-commerce"!). How important was authentication in the past and how important is it today? To clarify this issue, let us try to answer the following questions:

- How often do you show your passport to authenticate yourself to a business partner?
- How often has your passport been checked in detail by your business partner (performing an in depth analysis that it is not a forged one)?
- How often does he call the issuing agency to check that it has not been revoked?
- Do you know how to distinguish a forged passport from Belgium, Barbados or Bhutan from an original one?

The answer to all those questions is: We almost never use our passport (or any other authentication media) in normal business. How can we do commerce in such an insecure world?

Actually as everybody knows, the answer to this question is "Very easily"! Why? Because we don't rely on personal authentication. Furthermore, in most cases we don't even care about personal authentication of our trade partners! Why? Because authentication to business partners does not solve a single problem we have when doing commerce! Authentication is required only in a few cases.

Before discussing those issues further, let us look into another application area for digital certificates: digital signatures. We have been told that digital signatures are important for e-commerce. And now we come to ….

Question 2: How important are manual signatures for today's commerce?

So, now let us try to answer the following questions:

- How often do you check a signature you receive against a reference signature certified by a notary (or similar trusted party)?
- How often do you check in detail that a signature you receive has not been forged?
- Or even more simple: How often do you check that the signature you receive has any similarity with the person's name?

I don't want to continue these questions, because you know the answer: you almost never verify a signature. How can we do commerce in such an insecure world?

As everybody knows, the answer to this question is "Very easily"! Why? Because we don't rely very much on the manual signatures of our trading partner (there are exceptions, of course when it comes to really important contracts). But have you ever tried to sign as "Donald Duck". If you did so, did anybody care? Did anybody ask you if were really Donald Duck? Of course signatures play their role in commerce, but only in specific transactions.

But why is personal authentication and manual signing of so low importance in today's commerce? The answer is rather simple: It does not solve the problems we have with commerce. So, there remains the fundamental ….

Question 3: What is the main problem we have to solve when doing commerce?

The answer is very simple: The merchant's problem is. Whenever I deliver goods or services I want to be sure to be paid. The customer's problem is: Whenever I pay with my money, I want to be sure to get the goods or services I ordered. It's so simple! And so complicated! As one easily sees, authentication of business partners and digital signatures can assist in solving the problem, but they are not a solution in themselves! It doesn't help you to know the name of the person at the other end of the world that betrayed you! It doesn't even help that you are able to prove that he did it! This won't bring your money back! And now you probably understand that a digital certificate alone, issued by a "Trusted Third Party" does not solve any problem we have with e-commerce.

But how can we solve the merchant's and customer's problem in e-commerce? Let us look at how we do this today!

Learning from the Past

For many centuries we have done business, even on an international basis, without the ability to authenticate people or to verify their signatures. We authenticate **things** not persons. We verify the authenticity of a bank note or a cheque or a credit card. This is where authentication comes into the game. And as you see, there are only few organisations issuing bank notes, checks or credit cards. A trust relationship is established to those organisations in the sense that they will take the liability for transactions that use the tokens they have issued. The most important aspect for e-commerce is the fact that those organisations also provide the necessary assurance to the merchant to get his money if he has delivered the goods or services and to the customer to get his money back if he doesn't get the goods or services he ordered. This brings us to our ….

Statement 1: For e-commerce a Trusted Third Party has to provide the necessary assurance for electronic transactions and take a large amount of liability. Otherwise it is useless.

Now, to be able to provide this assurance and liability the Trusted Third Party will need to authenticate its customer and approve the transaction performed by their customer. But this requires a business relationship between the Trusted Third Party and the certificate holder. Actually in "old fashioned" commerce a Trusted Third Party like a bank will provide the required assurance for business transactions for their customers based on existing business contracts that establish a close relationship between the bank and its customer. This brings us to our ….

Statement 2: (Useful) Trusted Third Parties can only be built upon additional business and trust relationships.

This has of course significant consequences for the wide range of Certification Authorities that just try to sell certificates without being part of the business transactions. This is just like selling unforgeable, non-transferable tickets hoping that nobody asks what this ticket is good for. If you sell a ticket you have to associate a good or a service with this ticket, otherwise you will have a hard time to sell it (oh, before I forget to mention it: there is a market for those kind of tickets! You just have to market them as collector's items! Maybe this is a (the) business model of many commercial CAs).

With such a business relationship established we can start to do commerce. Now, how do we establish the trust chain between business partners that have not met and had no business relationship before? This is where the Trusted Third Party comes into the game. But unlike the X.509 model the TTP does not just assist the business partners in authenticating themselves enabling them to check their signatures. The TTP comes in to provide assurance to the business partners and the transactions they perform. The bank will set up a chain of trust, based on a sound contractual basis. This chain of trust starts with the contractual relationship between one of the business partners and his bank, continues with the contractual relationship between banks and end with another banks contractual relationship to the other business partner. Based on this chain of trust we do commerce. (Banks are just one example. Other examples are trade organisations and their contractual relationships).

But setting up new business and trust relationships is not very easy. It takes time, it requires agreements and contracts to be set up, it requires the definition of responsibilities and liabilities etc. Certificates make sense when they are used within such a framework and issued by an authority with defined responsibilities and liabilities for the business transaction where the certificates are used. Current „Certificate Practice Statements" are nice, but useless with this respect because they are related to the handling of certificates only and not related to the business processes where the certificates are used for! So we come to ….

Statement 3: Whenever a certificate is issued it should be clear for which business process it can be used, what the responsibilities of the business partners are (not just those of the CA and its customer) and how liability for the business transaction is regulated (not just for the handling and use of certificates.

But this requires that whenever you distribute a certificate to someone it has to be based upon a contract defining the business relationship. The certificate then is just a mechanism within this relationship to assist in authentication between the partners within the boundaries defined by the contract and to secure transaction between the contracting parties. Certificates are just a mechanism within the contractual relationship and not a basis to set up new relationships. So we come to our ….

Statement 4: Certificates have no use in themselves. They are only useful within defined business processes operating within an established framework covering business transactions, trust and liability issues.

In o-commerce (i.e. commerce conducted in the "old fashioned" commerce world) we have just a few trust relationships. We are relying on a network of such relationships but don't care about the structure of this network and how it works in detail. As an example nobody is really interested to know in detail the trust network that exists within the banking community. We just tell our bank to perform a money transfer to another bank and it is up to the bank how to do this securely. We don't care as long as our bank takes the liability. Transferring this to the electronic world we come to our ….

Statement 5: There are only a few public keys that have to be known to the wide public. And for the distribution and management of those keys a PKI might be an overkill.

And this is the reason why it is hard to sell just a certificate.

What now?

If you got the impression that I view public key certificates within e-commerce as useless, you are wrong. They provide a technology that can be quite useful but probably in a different way than the vendors have in the past proposed . We need to rethink the use of public key technology in the view of business processes not just as a technology in itself that can be used as a general-purpose solution for authentication and digital signatures. Rethinking public key technology in the view of business process may result in some interesting new application fields and some surprises.

For example there are interesting application areas for public key technology that don't need a PKI! As an example just have a look at the paper I presented a few years ago at this conference [2]. The technology presented operates with just a few public/private key pairs but is able to provide useful services to millions of people! The business case of this example is very simple: Providing access service to a distributed database with information needing high integrity and proof of authentication. A lot of databases from public authorities exist (at least in Europe) where information has to be distributed in an officially signed way to a large number of people. The example presented in the paper was the European Business Register, but the technology used there can easily be used for any other database of this kind.

Other applications exist, where public key certificates are just used by the issuer. So there is no need to distribute them. An example is a bank that creates certificates for its customers. Customers then use these other certificates to authenticate themselves to the bank and to sign transactions to the bank. Why should anybody else than the bank have access to the public key of the customer? If just the bank needs access, why should they use X.509? Why shouldn't they use a format much more suited to the need of the business application? You may argue that other banks need to have access to the certificate and understand this. I argue: this is not true! Other banks are not interested in this certificate because they have no business relationship to this customer. They have a business relationship to the customer's bank and will only accept transactions signed by them.

Many papers about PKI talk about certificate chains and cross certification. But from a business point of view this does not make much sense. Why should anybody be interested to authenticate somebody he has no business relationship with? What is required in business processes is the authentication of business partners and their signature on transactions.

Coming back to the bank's customer who has a certificate from his bank and now wants to pay for a service provided by a business partner. The business process is as follows: The customer talks to his bank and sends a signed money transfer order to his bank to transfer the money to his business partner's account (usually at another bank). The customer's bank will set up their own signed transaction to perform the money transfer to the business partner's bank. This bank will then send a signed receipt to the business partner telling him that the money has been transferred.

This sounds complicated but actually is very simple. Now look at the transaction flow described in [2]. It is very similar to the one in this example. And actually in the prototype system described in [2] this all was done within milliseconds.

Who needs which certificates for the scenario described above? The customer needs a certificate issued by his bank that he uses to authenticate to his bank and to sign the transaction.

The bank needs a certificate to authenticate itself to another bank and to sign transactions. Those certificates could be issued by a banking organisation or perhaps each bank just issues certificates for all other banks with which they have a business relationship.

The business partner just needs the public key of his bank to verify the receipt.

So everybody just has the certificate of those counterparts with whom he has a contractual relationship and verifies the identity and signature of this partner. At the end we have a chain of secured transactions (each based on one certificate) and no chain of certificates. And there is no "cross-certification" within this model.

The most important aspect of this model is the fact that there is no need for interoperability. Banks may use their own certificate formats in the relationship with their customers. They may be completely different from bank to bank. In addition they may use a totally different certificate format in the relationship with other banks. Management of certificates may be done also in a completely different way. But nevertheless the transactions will work and will be based on a sound contractual basis defining the responsibilities and liabilities of each party.

Conclusion

As a result of this paper let me summarise the most important aspects:

1. Public key cryptography will play a major role within e-commerce, but in many cases there is no necessity for a complex PKI.

2. For e-commerce the certificate format of X.509 as well as the concept of TTP cross-certification or TTP hierarchy is not well suited.
3. Certificates will in most cases be used as a mechanism within existing business relationships between the certificate issuer and the certificate recipient (or subject). A certificate issued by a party not directly involved in the business transaction is useless.
4. Simpler models of certificate structure and management than those used within current PKI systems may suit the requirements of e-commerce better than those defined in X.509

I strongly believe we have re-think the application and management of public key cryptography. We should start from the business needs rather than from a technical model. We are too much focused on specific technical implementations and forget that public key technology is just a supporting factor and not a means in itself.

I am sure that the security of e-commerce can be enhanced significantly when we open our mind to new models to apply and use public key cryptography.

References

[1] Carl Ellison and Bruce Schneier: Ten Risks of PKI, Computer Security Journal, V16, No. 1

[2] Helmut Kurth: Integration of Digital Signatures into the European Business Register, Proceedings of the 1997 NISSC