

Finance for the Future

a report by

Henk Tobias

Chairman, EEMA (The European Forum for Electronic Business)

Since humans first began trading, four main barriers have impeded collaboration in commerce – time, distance, common value/currency and trust. Unless the traders were in the same place at the same time, communicating in roughly the same language and with a modicum of trust, no exchange could occur. Centuries later, with global business-to-business (B2B) e-commerce, the same principals apply. Technology has conquered the impediments of distance and time, and common currencies such as the dollar and the euro have overcome currency problems. Trust, however, remains the final barrier, and one that is the major bottleneck in the electronic supply chain.

The Need for Trust

Today's supply chain is about creating seamless electronic relationships with customers and suppliers to smooth the flow of goods and cash, and to create hitherto untold efficiencies for all involved. The concept of partnering and sharing is at its heart. Clearly, within this new model, trust is of paramount importance. When trading partners are putting millions of pounds, Deutschmarks, francs or euros through an electronic exchange mechanism, it is not enough to be reasonably sure that the e-mail was received from the ostensible sender. From a purchasing point of view, neither is it enough to believe that a website is genuine. If a customer is about to order US\$1 million worth of goods or materials, they need to be able to minimise all possible risk, and have a bullet-proof audit trail.

There are a number of well-defined technologies and services that are gaining recognition as a suitable way forward to secure a transaction and create trust:

- Virtual authentication – digital certificates and digital signatures are two technologies already proven and in operation across the globe. Digital certificates are being hailed as the Internet's equivalent to a signature or passport.
- Guaranteeing integrity – today, virtually everybody wants electronic certificates and signatures to be made recognisable in law.

However, to guarantee their integrity requires a secure mode of transport to carry these certificates along with any correspondence to their destination without the threat of interception.

- Public key infrastructure (PKI) is acclaimed by some of the world's leading information technology (IT) vendors as the most flexible method of securing electronic transactions. PKI-based solutions act as a carrier for digital certificates, enabling secure online identification by adding cryptography and encryption technologies.
- The need for a trusted third party – the technology is available, but before industry can reap the benefits of e-commerce, users also require a high level of trust in the organisations that issue the digital certificates. Digital certificates are therefore created, issued and managed by a trusted third party.

Case Study – Identrus

While technology can secure a transaction, creating trust and forging buyer-seller relationships offline, conducting business via the Internet is still costly and time-consuming, especially given the need for cross certification. Conversely, if it were possible to bridge the trust gap, enormous efficiencies could be made. There has clearly been a need for third parties to enter the framework as 'networked' trust providers. In October 1999, such a group was formed when eight global financial institutions came together to tackle the problem. Known as Identrus, its nine early members included ABN AMRO, Bank of America, Barclays, Citigroup Inc., HypoVereinsbank, J.P. Morgan Chase & Co., Deutsche Bank AG, HSBC Holdings plc and The Royal Bank of Scotland.

Facilitating Business Worldwide

As the name suggests, Identrus' aim was to relieve companies of the costly and complex process of identifying multiple trading partners, and developing separate trust relationships with them. Instead, companies could form a single trust relationship with their financial institution. Through that financial



Henk Tobias is Chairman, EEMA (The European Forum for Electronic Business), and is closely involved in steering the organisation and introducing new projects and interest groups. He has served on the EEMA Board of Directors for eight years and was previously chairman of the EEMA User Interest Group. He has vast experience in electronic messaging – including his position as Technology Manager in the Global Infrastructure Organisation, (GIO), Unilever.

institution's relationship with Identrus, the trading partners could rely on common rules and policies to engage safely in e-commerce on a global scale. Trading partners could be confident that their communications remained private, unaltered and irrefutable. The partners also set out to provide dispute resolution and recourse mechanisms for participants and, through Identrus' electronic identities, trading partners would be instantly recognisable as authenticated participants in the e-marketplace. They could automatically identify themselves to any other trading partner through a common set of rules, and securely settle payments via their financial institution. Thus the aim was to create a seamless environment for global e-business collaboration – with trust.

Through its network of financial institutions, trading partners that are Identrus members can immediately assume the following things about each other:

- the trading partner has entered a contract with its financial institution to abide by Identrus' policies;
- the sponsor financial institution has undertaken due diligence about the trading partner to ensure their identity;
- identity is valid at the time of the transaction;
- a warranty is available to enable the relying party to manage his/her remaining risk with a clearly defined dispute resolution process; and
- the transaction has arrived from the sender unaltered.

The use of digital signatures and certificates provides identity and certainty.

The banking industry has been one of the forerunners in e-business, in terms of implementing state-of-the-art technologies to deliver benefits to its

customers. The Identrus model describes how a partnership approach has delivered a truly international solution for the financial sector.

The Identrus initiative represents a significant advance, endorsing the use of the Internet, digital signatures, digital certificates and PKIs for conducting business.

Today, almost 50 financial institutions have joined the network, representing 133 countries and millions of business relationships. As Identrus Certificate Authorities, these financial institutions are tapping an explosive B2B e-commerce market, whose sales will expand to US\$7.29 trillion worldwide by 2004.¹

Society for Worldwide Interbank Financial Telecommunication (SWIFT)

In September 2000, Identrus and the Society for Worldwide Interbank Financial Telecommunication (SWIFT) joined forces to deepen this trust foundation. SWIFT is a bank-owned co-operative, supplying secure messaging services and interface software to 7,000 financial institutions in 190 countries. The emerging Identrus/SWIFT 'joint solution' aligns the Identrus trust model with SWIFT's new Internet-based messaging service, TrustAct, enabling banks to provide secure delivery and receipt of messages that financial institutions' corporate customers exchange on the Internet.

The Foundation for Global Trade

Through developing an infrastructure that is interoperable, global, simple to operate and with a high level of trust, Identrus has put together a powerful engine for the banking sector both within Europe, and for those who trade with Europe. It bodes well for prosperity in Europe and the world. Its trading partners can now rest assured that whenever they do business with each other, that transaction is

Box 1: Elements of Security

In order to create trusted relationships, our communications with partners should include the following elements:

- Confidentiality – the ability to keep things secret from prying eyes.
- Integrity – the ability to protect information from unauthorised changes, or to be able to detect if such changes occur.
- Accountability – the identities of all parties are assured and are made responsible for their actions.
- Non-repudiation – neither the sender nor the receiver can deny communication, or other action regarding specific information or resources, and at a specific time.
- Copy protection – ensuring protection from unauthorised copying of intellectual property.
- Availability – ensuring that access to information or services are available as and when required.

1. Gartner Group (<http://www.gartnergroup.com>)

secure and reliable. They have eliminated considerable transaction costs and off-loaded the complexity of forming traditional business trust relationships.²

PKI Challenge

A critical component of Identrus' network is PKI, and one of the cornerstones of its success is interoperability. Without it the initiative could not have been extended throughout Europe.

The implementation of PKI is not, however, as simple as it seems. There is a baffling array of products and services on the market, and they are not necessarily interoperable.

For this reason, EEMA (The European Forum for Electronic Business) has launched the PKI Challenge, a European Commission-funded initiative designed to test and demonstrate interoperability between the myriad PKI products and services available. So far, some 33 PKI/public key application vendors and certification service providers have expressed an interest in becoming an active participant and have submitted details of the products they wish to put

forward for consideration.³

The interoperability testing criteria will include the following:

- the ability for applications to exchange and operate with each other's certificates;
- in multiple PKI scenarios, the use of cross-certification;
- the use of certificate revocation solutions;
- the use of supporting trust services for non-repudiation, such as time stamping and timed audit logs;
- the use of cryptographic techniques for digital signatures and confidentiality;
- the use of qualified certificates in support of qualified signatures;
- the possible use of attribute certificates; and
- the use of smart card technologies. ■

2. Further information about Identrus is available from <http://www.identrus.com>

3. Further information about the PKI Challenge is available from <http://www.eema.org/pki-challenge>



Connectivity made simple.

For further information and to request your free copy of the independent research report 'A study of integration in and beyond the enterprise' register online at www.mercator.com/research.

"Electronic business to business (B2B) communication can present some bewildering problems. How do you marry the older EDI technologies or SWIFT messages with the New World of XML? How can you quickly adapt your business to take advantage of Net Markets that seemingly spring up by the day?

How can you manage the business relationships between your business areas, your partners and your clients via SWIFT, Thomson, FXAll, the Internet, proprietary connections- the extended enterprise?

And finally, how can you adapt your systems at Internet speed to meet the demands of new initiatives such as GSTPA and new Net Markets?

With Mercator – problem solved – we connect disparate systems both enterprise-wide and those connecting to your counterparties, non-invasively, without writing code."

