



HOME BIOGRAPHY TOPICS RESOURCES NEWS CONTACT

E-TRUST – BACK TO THE FUTURE OF BANKING

The phenomenal growth of [e-commerce](#) presents banks with a number of business opportunities (see "financial futures" website). The most exciting of these – arguably the biggest banking opportunity of the decade – is the opportunity to create a trusted environment for bank customers to trade and communicate securely over the Internet. We refer to this opportunity as the emerging "**e-trust**" market, and to the services which banks will provide as "**e-trust**" services.

THE ISSUE

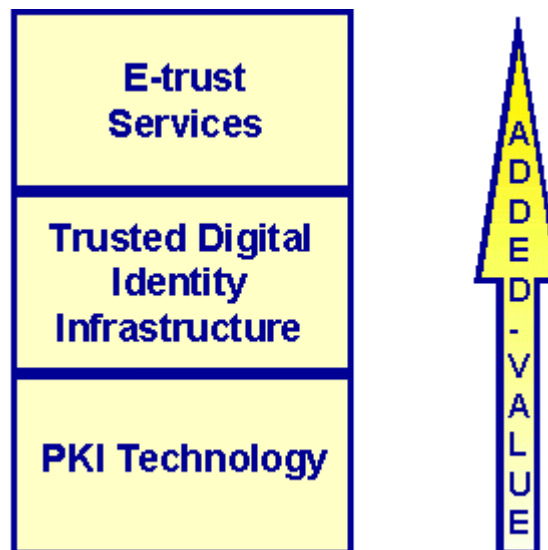
Conventional commerce takes place mainly between trading parties who already know and trust each other. E-commerce will change all that. Increasingly, we will find ourselves doing business with previously unknown counterparties who may be located thousands of miles away, in regions with foreign legal, commercial and regulatory jurisdictions. Before we trade, we will want satisfactory answers to questions such as:

- ⋮ "Is my trading partner who he says he is?"
- ⋮ "Is he trustworthy?"
- ⋮ "Can he pay, and if he doesn't, who will?"
- ⋮ "Will he deliver according to our agreed terms of trade, and if not, is there comeback?"
- ⋮ "Will I have recourse if things go wrong?"

Banks will soon be in a position to offer e-trust services which address all these issues and more. In doing so they will unlock the full potential of the new digital economy as a vast, highly efficient, global electronic marketplace. This represents enormous added value for bank customers and it follows that banks can expect to reap rich rewards from the e-trust market.

E-TRUST FRAMEWORK

For e-trust to work there needs to be a substantial technological and commercial infrastructure in place. This is best described in terms of a three layered framework as follows:



Each layer is now described in turn.

PKI TECHNOLOGY

The technology underlying e-trust is known as public key encryption or Public Key Infrastructure (PKI) and has been around for some time. Very briefly, PKI works by means of cryptographic keys issued in the form of digital certificates, which enable parties to communicate securely over an insecure network such as the Internet (see, for example, [RSA's website](#) for a detailed description). Specifically, digital certificates can be used to prove beyond reasonable doubt:

- ⋮ **Authentication** (someone is who they claim to be).
- ⋮ **Message integrity** (a message has not been tampered with in any way).
- ⋮ **Non-repudiation** (a message can be digitally signed to prove that it originated from a particular party, even if that party denies it).
- ⋮ **Confidentiality** (a message can be encrypted so that only the intended recipient can read it).

PKI technology vendors include companies such as [Baltimore](#) , [Entrust](#) and [Verisign](#) . Banks would be well advised to use such vendors rather than attempting to build their e-trust technology infrastructures from scratch.

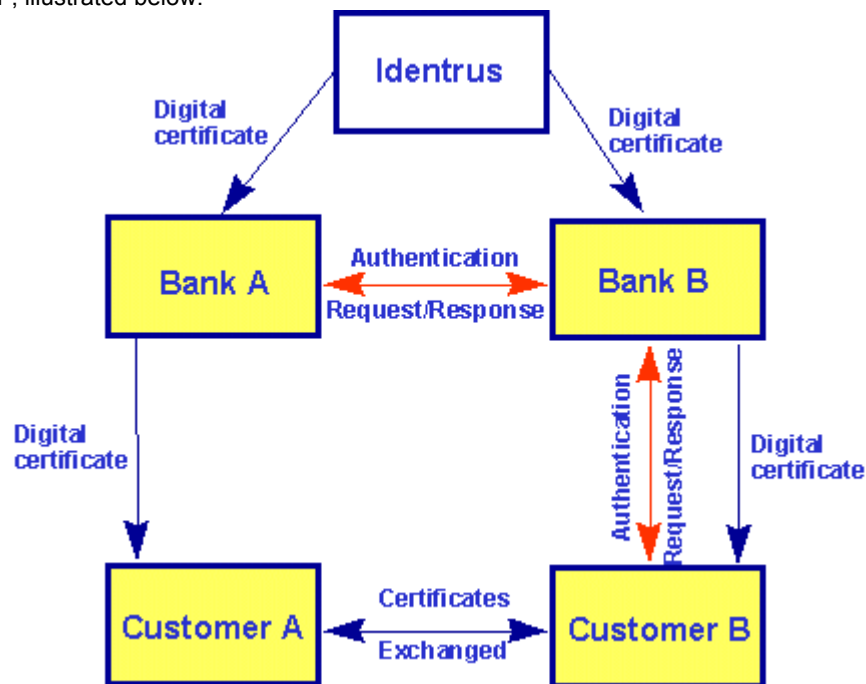
TRUSTED DIGITAL IDENTITY INFRASTRUCTURE

It is important to understand that a digital certificate can only be trusted insofar as the organisation which issued the certificate can itself be trusted. This represents a good opportunity for banks, which are highly trusted institutions, to set themselves up as Certificate Authorities (CAs), issuing digital certificates to customers on the basis of a stringent registration process. But it is also a good opportunity for similarly trusted non-banking institutions, such as [BT](#) and [Royal Mail](#) , both of which have launched digital identity services in the UK. However, such single-issuer services are limited in that both counterparties to a transaction must use digital certificates issued by the same CA. If two or more CAs are involved, then there needs to be a trusted relationship **between** the CAs as well as between each CA and its customers. In fact there needs to be a whole commercial and legal infrastructure or "scheme" with well defined rules governing roles,

responsibilities, risks and liabilities if digital certificates issued by one CA are to be interoperable with those issued by another.

This is where banks really come into their own, by virtue of belonging to an international banking community whose members trust each other and are used to participating in similar schemes (for payments for example).

Currently, the most important bank e-trust scheme is probably [Identrus](#) , a global trust authority backed by some of the biggest banks in the world. Identrus operates according to a "four box model", illustrated below:



Customer B, on receipt of Customer A's digital certificate, can validate that certificate with Bank A, which issued the certificate, by means of an authentication request/response routed via its own issuing bank, Bank B. Banks A and B validate each other by reference to a "root key" held by Identrus.

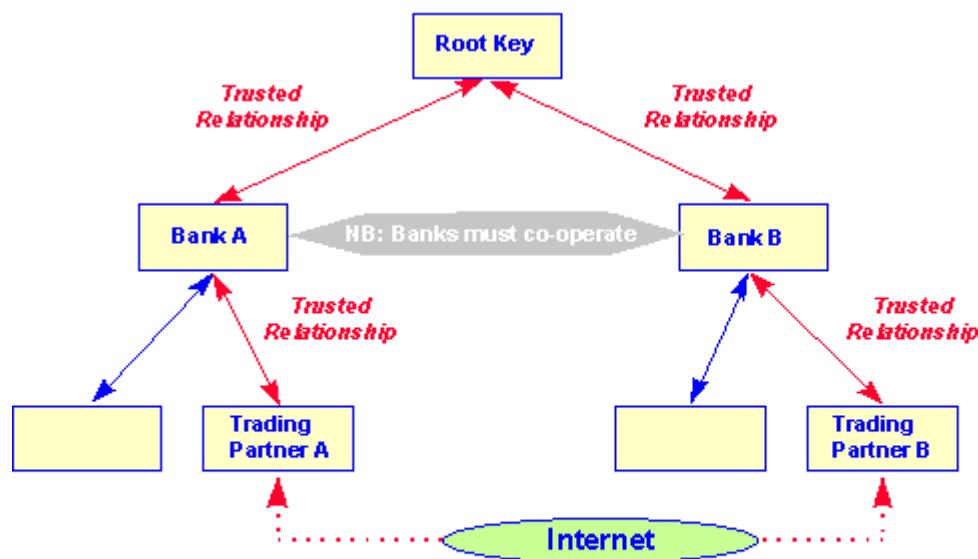
Provided Banks A and B issue interoperable certificates and adhere strictly to a set of well defined rules (governing, for example, registration criteria and service levels) then customers A and B, previously unknown to each other, can have a very high degree of trust in each others digital identities.

E-TRUST SERVICES

Once an infrastructure of **trusted digital identities** is in place, banks can develop, on top of it, all sorts of added value e-trust services for their customers, for example:

- ⌘ By combining identity validation with digital signing of electronic documents (and encryption, if necessary), together with an audit trail, banks can offer a **secure messaging** service.
- ⌘ By using information about the financial standing and credit history of their customers, banks can offer on-line credit reference services, effectively upgrading digital identity to "**digital status**".
- ⌘ By adding links to existing or new electronic payments systems, customers can be provided with a seamless **payments integration** service; further integration with back office accounting and order processing systems could result in automation of the entire trading process, with huge savings for most customers.
- ⌘ By standing behind the integrity of digital identities and their supporting systems, banks can reduce customers' trading risks through services such as **payments guarantees** and **performance bonds**. More generally, banks will be in a position to offer **recourse** and **comeback** when things go wrong.
- ⌘ By combining these elements into innovative applications based on the needs of particular customers, banks can develop a whole new range of products and services in areas such as **trade finance**, or **electronic auctions** electronic procurement.

The principle underlying all these services is that banks leverage their trusted relationships with their customers and with each other, as illustrated below. This "trusted intermediary" role for banks is of course centuries old, and it is in this sense that the emerging e-trust business is a "back to the future" opportunity for banks, updated for the new Internet age.



Previously unknown trading partners A and B have a virtual trusted relationship by virtue of the trusted relationships higher in the hierarchy

IMPLICATIONS FOR BANKS

Although the e-trust market will take years to evolve into its final form, the speed with which e-commerce is developing, and the intense competition from powerful non-banking players, means that banks cannot afford to be complacent. Each individual bank needs to consider carefully its strategic positioning in the

marketplace. Three principles, corresponding to the three layers in the framework above, are worth emphasising in this respect:

- ❖ **Infrastructure** . Banks wishing to offer e-trust services will need to build an appropriate technology and commercial infrastructure to enable it to act as a CA and issue digital certificates. This is technically quite straightforward but complex in terms of scale and scope. For example, most banks will wish to use the same infrastructure across all business units, to support not just e-trust services but also electronic delivery of its own financial products.
- ❖ **Interoperability** . E-trust services only work if there is interoperability between banks. Individual banks need to be quite sure that they adopt digital certificate standards and processes which enable interoperability on a global scale. Backing the wrong horse at this stage could be an expensive strategic mistake.
- ❖ **Cooperation** . More generally, banks need to cooperate if they are to dominate the e-trust market as an industry. Individual banks will, of course, compete vigorously with each other to offer superior services to their customers, but by definition, if two banks are required at either end of a transaction, then such competition must occur within a context of a cooperatively developed scheme. Some schemes will be national – most developed countries are in the process of building their own banking e-trust schemes (see, for example [Isabel](#) , or [Swisskey](#)). Others will be organised by market – most schemes are currently targeted mainly at business-to-business e-commerce, but others will emerge to address the needs of business-to-consumer or government-to-consumer e-commerce. Still others will be organised by product or financial sector. Each individual bank will need to think hard about how the market is likely to develop, and will then need to cooperate with one or more schemes on that basis.

Interested? Please contact Nick Collin on nick@ncollin.demon.co.uk or **+44 (0)207 833 8765** with comments or questions.

Designed by - Blue Nostromo © 200505