Trust Services: A Trust Infrastructure for E-Commerce

Adrian Baldwin, Yolanta Beres, Marco Casassa Mont, Simon Shiu
Trusted E-Services Laboratory
HP Laboratories Bristol
HPL-2001-198
August 15th , 2001*

E-mail: adrian_baldwin@hp.com, yolanta_beres@hp.com, marco_casassa-mont@hp.com, simon_shiu@hp.com

integrity, web services, B2B, trust, trust services, security, e-commerce, accountability, survivability, confidentiality

Trust Services are an emerging enabler for e-commerce. They deliver trust and confidence at various stages of business interaction, including: establishing and maintaining trust, negotiations, contract formation, fulfilment, collaboration, through to dispute resolution. However, there are significant technical and business problems to overcome. Trust service providers must be accountable for the service they provide and, because disputes can occur many years after a transaction, they must be around for the long term. Finally, to be successful, their services must make life simpler for e-commerce participants. This paper uses examples to elucidate the advantages and problems presented by trust services. The authors are working on some of the technology problems, which is a necessary first step to realising a full trust services infrastructure.

* Internal Accession Date Only Approved for External Publication

1 Introduction

There are many risks in trading on the Internet. Moreover, it is getting more difficult for companies to establish and enforce procedures for engaging safely in e-commerce. For example, how to establish the authenticity of electronic communications, how to ensure electronic signatures are fair and legally binding, and how to create an electronic audit trail that can be used for dispute resolution.

This complexity means that mistakes will be made thereby increasing the level of risk. Trust Services are an attempt to address this problem. The idea is to package the operations that must be performed (to protect participating companies), and offer them as simple to use (and understand) "trust services". The provider of a trust service will be an expert in managing risks associated with the particular service they offer.

In the physical world, a bank can be viewed as a trust service. People can choose to look after their own money, say by storing it under the mattress. One reason why people do not do this is that they would have to invest in significant security to avoid being robbed. It is much simpler to use a bank to store the money; they are specialists, and are accountable for the money they keep. Further, they understand the risks of losing money, and so can mitigate against this using appropriate investments in physical and computer security.

Taking this analogy further, banks have moved beyond "not losing" money, to offering various value added services such as credit cards, cash machines, and direct debits. It is imagined that trust services can extend to various value added notions. For example, a storage service could extend to monitor contracts, or enforce storage policy, a reliable messaging service could extend to offer message audits, and so on.

The notion of trust services is not new; there are various financial, insurance, and legal services available that make commercial activity simpler and less risky. However, many of them rely on well established, usually paper based, processes. For example, although web and e-mail is being used more and more to set up transactions, most deals will involve paper based contracts, invoices, and receipts, any of which could be used to support a claim with an insurance company, or in a court of law. The reliance on these processes enables businesses to engage in ordinary commerce.

There has been much talk of streamlining business processes and transactions to achieving cost savings using the promises of the internet. Digital signatures provide a mechanism to underpin the legality behind such digital business transactions and are supported by recent e-signature legislation [ESign99]. In spite of this, it seems clear that companies need more help to move away from paper and into a digital world. To achieve this trust services must fit seamlessly into the business processes of these companies.

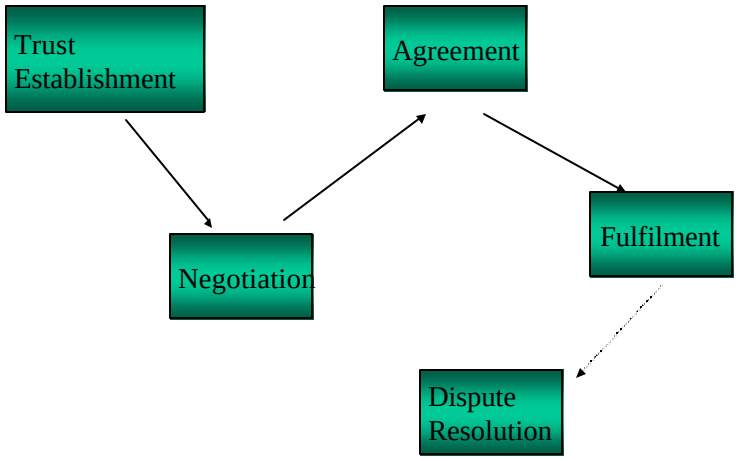

Figure 1.1
The lifecycle of a business transaction

For example, a typical lifecycle for a business transaction would be as shown in figure 1.1. Historically trust establishment has been performed in a variety of ways including face to face meetings, recommendations, letters of credit, background checks and so on. In e-commerce all the transactions are likely to be electronic, and perhaps automated. There are technologies available for identity and authorization; however, it is not at all easy for non-specialist companies to use them appropriately to establish trust. The trust services vision is to package these technologies and deliver services that would allow such companies to easily achieve the trust levels they desire.

Similarly for negotiation, agreement formation and fulfilment there are established roles such as notarisation, record retention, underwriting, and business verification[1]. These roles will still be needed for e-commerce, but because of the differences of digital transactions new ones will also be needed. For example, to ensure appropriate processes for all the contexts in which digital signatures are produced, and preserved. There are technologies that solve some of these problems, for example timestamping, and document management systems, however again, it is not easy to do due diligence at each stage in the process.

To be of value, the trust service providers must be accountable for the service they perform. The risks will be passed to these specialist providers, which will have the expertise to understand the trade offs and handle the complexity. For example, a company should be able to hold an identity service to account over an identification it

[1] Third party business verification, i.e. checking and inspection of suppliers, customers, and individual fulfilments, is a service from the old economy. For example SGS founded 1878, has been providing such services for a long time.

provided; and a notarisation service should be available for verification many years after notarising a document. Many analysts are citing lack of accountability as a major stumbling block for wide scale adoption of e-marketplaces [Thomp01].

Thus there are three distinguishing features of trust services,

i. they are each components in a trust infrastructure that give e-commerce participants confidence to trade,

ii. they simplify life for their users,

iii. they are accountable, or can be used to vouch for the service that they provide.

It is not yet clear what the range of trust services will be. They can certainly be expected to include mechanisms to support trust establishment, negotiation, agreement and fulfilment. For Example:

- Identity services,
- Authorisation service,
- Anonymity services,
- Trust rating and recommendation services,
- Guaranteed message delivery,
- Auditable receipt generation,
- Storage,
- Notarisation

A guaranteed delivery service may offer storage and notarisation of documents transmitted thereby building one trust service using others. Moreover there would seem to be a role for a set of component trust services (i.e. services that would not make sense to the ordinary business customer, but which will be essential to deliver the above services), for example:

- Secret/Key storage services (as a confidential storage service will use cryptography and so keys),
- Archival services,
- Timestamping services.

The next section uses a generic example to paint a vision of what the world would be like if there were a trust service eco-system in place. It tries to remain technology neutral, but since some current solutions can be viewed as trust services, it is natural to describe

•

them. This leads to section 3, a discussion of the emergence of trust services in e-commerce today, and in the research literature. Some current technologies that can and in some cases are being used as trust services are discussed.

The problems in making the trust services infrastructure are more than just technical. Section 4 discusses in more depth the characteristics of trust services. This leads to a discussion of the broader challenges in delivering trust services. Finally section 5 draws conclusions and recommendations.

2 Scenario

In this section we consider a business scenario and look at what role trust services play in the different stages of it.

Take a classical example of using an external third party to help in finding and forming a business relationship between two companies. Lets say the player is a large drug manufacture that needs to find another company to perform tests on certain drugs. An external party, such as an online exchange, is employed during the initial stage in order to find a selection of potential partners.

The task of finding the right test laboratory and forming a business relationship is performed in stages as depicted in figure 2.1.

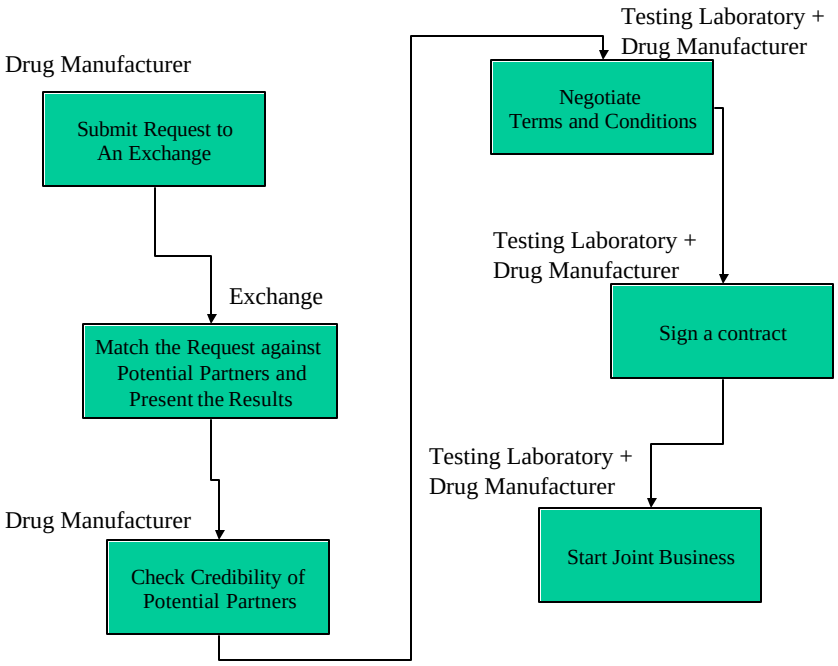

Figure 2.1
A sample process of a drug company engaging with a test laboratory

Each stage in this scenario consists of a separate business process involving either the drug manufacturer and exchange or the drug manufacturer and testing laboratory. The next sections proceed to look at what trust services should be in place to support these separate business processes in an online world.

2.1 Role of Trust Services in Business Processes

2.1.1 Process of Submitting a Request

The first transaction of submitting the request to an exchange seems to be quite straightforward, in an e-world it is necessary for an exchange to establish the authenticity of the request and also the eligibility by the party to participate in exchange. The exchange will incur unnecessary costs if it proceeds with bogus requests for which it will not be paid. The full process of submitting a request will consist of at least the following steps:

1. Drug manufacturer authenticates itself.
2. An authorised request is submitted.
3. The request is verified and logged.

The trust services that would be used in this process as shown in figure 2.2 are an authentication service to identify the manufacturer submitting a request; an authorisation service to validate the submitter's entitlement to make the request; and potentially an e-signature verification and request timestamping services.

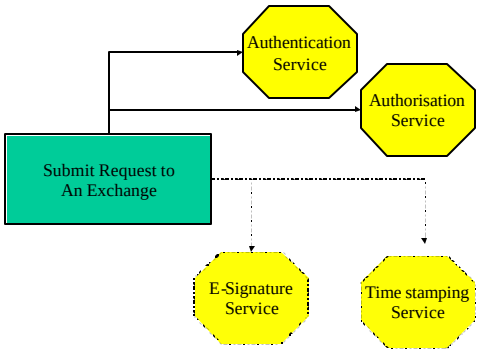

Figure 2.2
Trust services required in submitting a request to an exchange

The authentication service provided by a third party might potentially serve several exchanges in which the drug manufacture participates. The verification and time-stamping services in this case are optional since they would probably be used by an exchange only on certain (perhaps costly) transactions to provide additional assurance.

2.1.2 The Process of Finding Potential Partners

The second transaction from our scenario is performed by the exchange with the results being submitted back to the drug manufacturer. The exchange must identify companies who have the potential to fulfil the request. Typically, this would be done using catalogues held by the exchange although the exchange may also pass the request to other collaborating exchanges.

If a request is passed to other exchanges, certain security mechanisms have to be in place: the requester may need to be anonymised; however, the integrity and authenticity of requests still have to be assured. A special purpose messaging service is used in these cases.

The exchange can then check the credentials of chosen or potential partners to ensure that they are capable of meeting the requirements.

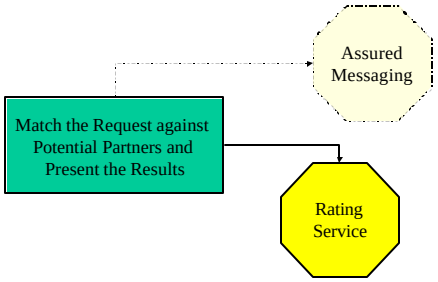

Figure 2.3
Trust services required in request matching

2.1.3 Credibility Establishment

Before engaging in business with one of the potential test laboratories the drug manufacturer either performs its own credibility verification, or uses an insurance company to underwrite the transaction. In this case, the insurer would probably check out the company with a credibility verification service. The insurer and the credibility verification service are both trust services.

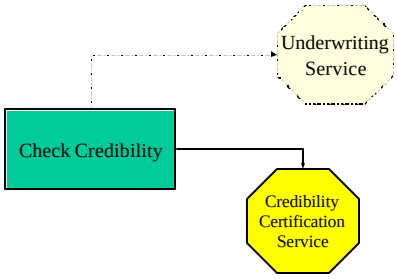

Figure 2.4
Trust services for credibility checks

2.1.4 Contract Negotiation

During negotiation phase an assured messaging service has to be used by both parties to not only ensure confidentiality of transactions but also to enhance accountability by

keeping the sequence of exchanged messages. This service will itself use time-stamping and secure storage.

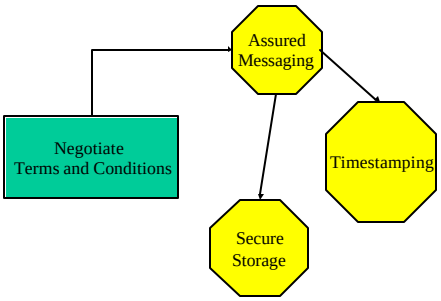

Figure 2.5
Trust services in negotiation of a contract.

2.1.5 Signing a Contract

After the contract has been finalised, it is digitally signed and time stamped, in which case both e-signature and time stamping services are used. To ensure long term preservation of the signed document the e-contract is passed to the secure storage service.

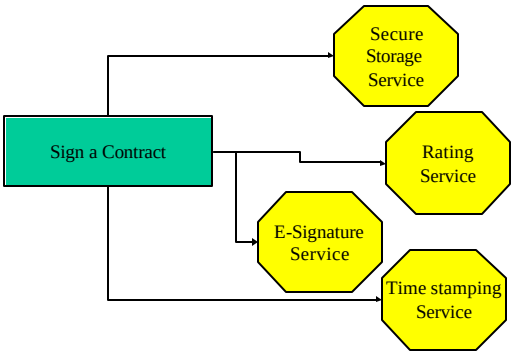

Figure 2.6
Trust services required for contract signing.

2.1.6 Stage of Joint Business

Once the contract has been signed, the drug manufacturer and test laboratory enter the stage of joint business. During this time the drug manufacture has to supply the drugs for

testing, whilst the laboratory carries out testing providing the results back to the manufacturer.

During this process, both parties have access to the shared confidential information, such as drug details and test progress. Both authentication and authorisation service are used to identify individuals and control the information that they can access.

In addition, the parties agree to use assured messaging service since information regarding drug testing is highly confidential and sensitive, and thus must be communicated in secure way.

Finally, the results of tests are stored by a secure storage service for long-term preservation.

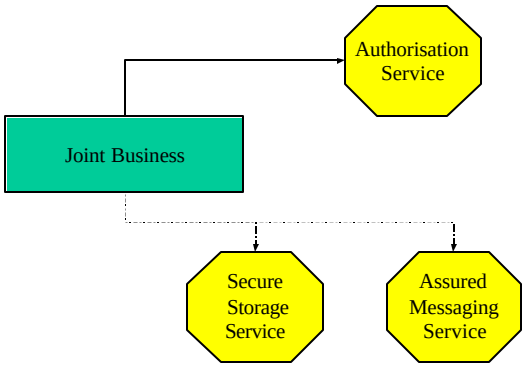

Figure 2.7
Trust services for continuing business

2.2 Summary

The scenario demonstrates that many of the trust services are used in various places during the business process. Table 2.1 summarises which services have been used at which stages. For example, the secure storage service is used in negotiating, contract signing, and joint business stages.

The final set of trust services used during business processes might be different depending on the scenario and applications. The examples list an essential set of trust services and demonstrate how they can be used although the list is definitely not exhaustive.

•

	Contacting Exchange	Finding Partners	Credibility Checking	Negotiating	Contract Signing	Joint Business
Authentication	☑					☑
Authorisation	☑					☑
Assured Messaging		☑		☑		☑
Secure Storage				☑	☑	☑
Underwriting			☑			
Time stamping	☑			☑	☑	
E-Signature	☑				☑	
Certification/Rating		☑	☑			☑

Table 2.1
Trust service usages throughout the business process

3 Emerging Trust Services

Researchers from NIST have presented a similar vision to trust services see [Stein97].

> *"Electronic Commerce will modify some of the traditional models for the conduct of business. However, it is important that many of the long-standing elements of commerce be replicated in the electronic world."*

The paper goes on to describe "*trust enhancers*" that will be needed to support these models and elements, and some of the technology needed to deliver them. These clearly align with trust services. There are many emerging technologies, and in some cases services that could play a part in a trust services infrastructure.

Identity

Public key infrastructure (PKI) based certificate authorities [Housl99] are commonly used to underpin digital identities. Companies such as Verisign, provide signed certificates vouching for the identity of the owner of the public key. In theory step 1. in the scenario the exchange need only check publicly available revocation lists, to get confirmation of the identity.

PKI infrastructures are hard to use and integrate with applications and services, especially for tasks concerning the verification of digital identities. Companies like ValiCert (www.valicert.com) offer mechanisms and services to outsource validation and verification controls, based on OCSP protocols and related technology [Myers99].

In practice, there are many standardisation issues to be resolved before PKI certificates can be accepted between companies, see [Casas00]. The current scheme lacks accountability with the certificate provider. Without this there is no pressure on the provider to do the necessary offline identity checks and therefore the certificate cannot be relied upon. A further problem is the short-term nature of the certificates; that is, the certificate is only valid for a limited period, typically twelve months. There are many cases, for example in dispute resolution, where there is a need to prove the identity of an author or signatory many years after the event. Extra identity tracking services would be needed to achieve these aims.

Digital Credentials

Emerging privilege management infrastructures (PMIs) address the very basic need of certifying attributes associated to users and enterprises. These attributes include credit card numbers, certified credit limits, ranking information, etc.

The two principal competing approaches based on X.509 [Housl99] and SPKI [Ellis99] technologies uses digital credentials to represent and certify digital attributes. These approaches suffer the same problems described in the identity section. In particular little

has been done to address the accountability of attribute authorities (credential issuers) and the management of long-term digital credentials.

Recommendation and Rating

Reputation is an important asset for people and enterprises and it is definitely a trust enabler. In our scenario, recommendation and rating services are used by the exchange as part of the trust establishment phase: digital credentials could be used to represent and certify enterprises' attributes.

On the business side, recommendation and rating services are emerging within electronic exchanges and e-marketplaces to vouch for market participants. Market makers (e-marketplace providers) are starting to run such recommendation services for participants in their closed communities. However, it is not just e-marketplaces and startup service providers that are taking business-to-business e-commerce trust seriously. Century-old insurers, banks and business services companies also have stepped to the fore to help e-businesses mitigate the risks of buying and selling on the Web [Hicks01].

Among others, the business information provider The Dun & Bradstreet Corp. and verification and testing provider SGS Société Générale de Surveillance SA, have recently launched e-trust service offerings.

In particular SGS launched a division and service called SGSonsite (www.sgsonsite.com). SGS's first online offering is a service that allows B2B suppliers to receive a seal of approval after SGS has assessed criteria such as production capacity, online trading capabilities, quality assurance and control systems, and even environmental stewardship.

Since last year, through a series of new products and joint ventures, companies are adding services to secure online B2B transactions, insure against risk in online trade, verify the readiness of suppliers and discover details of a potential trading partner's background. Online rating services, like credit rating services (www.clearlybusiness.com, www.mcphersons.co.uk, etc.) are already available on the internet providing a view on the financial reputation of enterprises.

Companies like TRUSTe (www.etrust.com) address the need for branded symbols of trust and privacy on the Internet. Web sites displaying the TRUSTe Privacy Seal are committed to abiding by a privacy policy that gives users notice, choice, access, and security with regard to their personal information; and in the event of failure giving users redress.

These kinds of recommendation and rating services need a high level of accountability to the accuracy of the information that they impart. They must provide a high degree of confidentiality on the information they have and ensure that the necessary checks have been made to the source of the information. For such services to be successful trusted companies and organisations must run them and they must maintain the quality of the information they provide to keep their reputation.

Anonymity

Anonymity services are becoming popular on the Internet to protect users privacy. This is true not only for consumers but also for businesses: the management of the privacy and security of corporate and customer information assets can determine the success or failure of critical e-business initiatives.

Companies like Zero-Knowledge Systems (www.zeroknowledge.com) offer an online anonymiser service based on strong encryption mechanisms and IP masking techniques.

Anonymity and privacy are also more and more important for auctions, exchanges and e-marketplaces where the identity and credentials of market participants need to be hidden for business and strategic reasons.

Messaging

Being able to exchange messages in a secure and guaranteed way, during business interactions, is a fundamental requirement.

From a low-level technology perspective, the S/MIME technology standard allows the exchange of messages by providing mechanisms to sign and (optionally) encrypt messages. S/MIME makes use of the sender's and receiver's digital certificates. S/MIME only defines a standard format for messages and does not guarantee delivery. Moreover, it suffers from the PKI problems described in the identity section.

The assured and guaranteed messaging infrastructure (that we envisage in our scenario) needs to be provided at a higher level of abstraction, by an e-trust service that can be held to account.

Traditionally EDI messaging and business interaction infrastructures provide reliable and trusted infrastructures underpinning interactions within close business communities. Trusted third party, like GEIS (www.geis.com), supply these infrastructures by means of Value Added Networks (VANs). VANS use dedicated communication resource and the provider is accountable for their security trustworthiness.

EDI solutions are generally quite expensive and accessible only to large enterprises and businesses. The rise of the web has recently made these solutions evolve to include web based messaging facilities (webEDI).

Notarisation

Notarisation is an essential trust service that provides evidence of the existence of documents and messages at particular points in time. Notarisation services are emerging on the Internet as e–trust services. These services provide notarisation records of digital documents including undeniable timestamps of the content of these documents. A proof

of the notarisation act is usually returned to the owner of the digital document by means of a receipt.

For example, Surety (www.surety.com) is a provider of digital record notarisation service. Surety's Digital Notary Service enables enterprises and people to notarise electronic files and records before they are distributed or publicised, guaranteeing file content and enabling the owner to verify their content for years to come.

Timestamp.com (www.timestamp.com) provides a time-stamping service to digitally timestamp digital documents. The hash value of a document is digitally signed and time stamped and the result returned to the requester.

Storage

The storage of critical digital documents is extremely important, especially for long period of time, as it is the foundation of accountability. In the physical world enterprises and people are asked by law to store and keep paper-based documents for long periods such that they can be used as evidence of past events or actions. Because of the trend towards digital documents, enterprises and people are likely to be asked to store digital documents for similar long periods. These digital documents can be of any type, including e-mail conversations, e-contracts, receipts, etc.

As a pure storage play, many technologies have been developed so far, at the infrastructure, system and at the application level.

Infrastructure technologies like Storage Area Networks (SAN) and Network Attached Storage (NAS) provide high availability, replication and survivability of stored documents. Companies like Documentum (www.documentum.com) provide solutions to store, index and manage huge set of documents within enterprises.

Little has been done so far to deal with the longevity issues associated to the long-term storage of critical digital documents. Long-term storage services need to be provided by trusted storage services that support the renewal of document formats and signatures, the management of long term access control, the management of long term encryption and deal with long term survivability of the stored data.

Trusted collaboration

Trusted collaborative environments like Internet business communities are emerging on the Internet as safe-havens where enterprises can cooperate on common goals. These business communities include extended extranets, exchanges, supply chain communities, virtual conferences rooms, etc. Currently most of these services are either run by a dominant entity, such as with supply chain communities or trusted third parties, like in the case of exchanges.

One of the emerging problems to be addressed is the fine-grained management of the access to information, resources and services shared by the participants. Little has been done to address this problem so far. Support for the delegation and control of fine-grained

access control has to be provided at the data, resource and service levels. Flexible and trusted authorisation services need to be deployed to simplify the management within these environments.

4 Research Problems in Trust Services

Trust services underpin business processes and therefore the businesses place a high reliance on the trust services. The implications of a failure in a trust service can therefore be severe and as such, the trust service provider needs to minimise the risk of failure and therefore their liabilities. The whole focus behind the trust service industry is to take many of the trust tasks that companies find hard to manage and push them into specialist providers. Both these arguments suggest that trust service providers should be experts in the service they provide and the relevant technologies used to provide it. They must carefully consider the design of both their business processes and the underlying delivery technology.

4.1 Technology Issues

The range of trust services makes it hard to develop generic trust service technologies; however, there are some key issues that need to be addressed by many trust service providers. Four main technology issues are discussed below with many of the points being related to the long timescales over which the trust services make guarantees. This change from the short timescales often associated with computers to the much longer business timescales provides some considerable challenges.

Ease of use

Ease of use is important for all systems including trust services which will be integrated into many different companies business systems; and reintegrated into new systems as updates occur. Each company will have their own sets of policies concerning the way they wish to use trust services and the guarantees they expect from the trust services. As such, flexible agreements allowing differing policies must be supported.

Some trust services, for example a storage service, will require that the users maintain a relationship with the service for long periods. This task must be simplified across the whole set of services to reduce management overheads. For example, the complexity of informing and managing the removal of a user; or a change in their rights as a member of staff leaves or changes their job can be painful if each trust service must be updated.

Some trust services such as a recommendation service or a timestamp service will make a statement that must be supported for long periods; others such as storage services will keep data that must be recoverable after long periods. Standards for the form of information must be developed to ease integration and the ability to interpret information after long periods. Equally, where information is retained, it should be easy to search for the required document stored some time ago.

Survivability

Trust services can be thought of as part of a critical business infrastructure and therefore, every effort should be taken to make the system resilient to failures and attacks – that is survivable. Properties of a survivable system include a mix of high availability and a

security allowing the system to have integrity of data and service continuity in the presence of attacks and failures.

In designing a trust service, it is a good assumption that failure (or successful attack) will occur within parts of the underlying system; but a level of service continuity needs to be maintained. Given some of the issues surrounding the times over which guarantees are made by trust services it is likely that all systems originally used to provide the service will have been replaced. For example, the original systems used in providing a timestamp service may have been scrapped but the timestamp service must be capable of verifying their original timestamps. When a user requests a timestamp some servers may be down but the service provider should ensure sufficient resources remain to meet the users needs.

Survivability is a function of an overall system and should therefore be incorporated into the basic architecture of a trust service. Trust services will often rely on other trust services; these linkages, and the strengths of the chains of trust, form part of the survivability considerations. A number of mechanisms can be used to obtain a degree of survivability and are discussed in [PASt01].

Confidentiality and Privacy

Trust services will see considerable amounts of data concerning their clients business. For example, a recommendation service will see tasks that a business is looking for people to carry out; a credential service will see on whom a business is checking and storage services may be storing, and therefore seeing, all a companies' important documentation. It is essential that consideration is given as to how a high level of confidentiality can be gained ensuring, for example, that a trust service provider does not leak clients' information – protecting it from even to its own operators.

Confidentiality often refers to the ability to encrypt a link between a client and the service provider. Whilst necessary for trust services, stronger claims should be made, for example, about the way information is kept encrypted within the trust services' computer systems. In cases, such as a trusted storage service, information is maintained for long periods of time there will be issues of long-term key management and the strength of the encryption algorithms over the lifetime of the data.

Confidentiality is not solely about encryption; one of the most important issues is the access control on information; including residual information such as billing data. Many issues of access control are well understood and applied in a variety of ways to computer systems and services. The longevity of some trust services brings further issues where the users and owners of each piece of information may change over time due, say to, job or organisational changes. Even tracing a single user's identity over time can prove problematic as keys, certificates and even user names change. It is probably necessary for the trust service industry to have generic solutions such as identity and role tracking services to simplify the access management tasks.

Integrity

Many trust services are acting as information providers and clients will be concerned with the integrity of the information and ensuring that it is correctly attributable to the trust service. Equally, the trust service will be keen that others cannot make statements on their behalf and that during the lifetime over which the statement will be used that they cannot be changed. Typically, this will be done by signing the statements and ensuring they are time-stamped with keys of sufficient size to protect them for their expected lifetime. Trust services should be concerned with the way their systems are run to ensure that rogue employees cannot form unintended trust statements.

To an extent the publication of trust statements, or receipts for say storage, will make it hard for a trust service to back down on claims. Trust services may be required make further demonstration of their claims; such as to justify that they correctly vouched for someone on the basis of the information available to them at that point in time. This means that trust services should be able to demonstrate the integrity of all their records and the functioning of their systems – a more challenging task.

4.2 Business Issues

The Trust Services vision involves much more than technology and in particular cannot be solely realised by a technology provider. It is likely to require collaboration and cooperation from many parties. This section outlines some of the non-technical issues and mentions some of the other stakeholders that have interests, opportunities or knowledge in this area.

Enterprises and consumers will be heavily reliant on individual trust services, which will in turn be reliant on the whole infrastructure. For this reason all providers will have an interest in preserving the reputation of the eco-system. It is believed that providers need to "look after" each other and share good practice, in much the same way that the banking industry operates. The reliance is very much long term and the technology brands are unlikely to be ones that enterprises will readily turn to for such services. The more likely brands would seem to be those involved in the current trust infrastructure, i.e. banks, insurance, audit, and perhaps government organisations.

Longevity also poses challenges for revenue models, for example, how would an enterprise expect to pay for the storage related to a transaction that must be kept for many years. It may be that the banks can readily understand the business models that are likely to emerge, but it may be that lateral business thinking will be required.

In the introduction, it was argued that providers are best placed to be accountable because they will understand the risks. It is worth noting that not all the risk is in the technology, and even if it were, there would still be a need or actuarial expertise when deciding what technology to deploy. Other factors that will need to be well understood, and perhaps influenced, are the constraints of the legal system, common practices within industries, auditors and government organisations. Standardization is a vital component. Some standardization efforts are already appearing (see [PRO00]), but there is a lot of work needed before the technology and processes are well enough understood for common

standardisation. Nevertheless, such forums are clearly important to encourage the collaboration between interested parties.

Another distinguishing and vital ingredient of trust services mentioned in the introduction was that they simplify things for their users. To do this they must integrate seamlessly with their business processes. Web services can help with this since using external services with standardised interfaces is easier than integrating a new system into an enterprises existing IT infrastructure. However, this explanation hides a lot of detail, and it would be extremely unwise to proceed without using the knowledge of customers, and perhaps the software providers that assist current business processes.

In summary, there is a large and eclectic community of stakeholders with different opportunities, influence, and knowledge to contribute to the vision. Establishing the necessary collaboration will be extremely challenging. It is worth noting that the vision can be reached incrementally. For example, technology providers with sufficient technology can partner with, say banks to offer any of the services described, and they should add value. The hope would be that the value would be such that using the service becomes standard and ends up influencing industry practice, which in turn may influence, say legal precedents.

5 Conclusion

This paper has described a trust services infrastructure consisting of e-trust services. Such an infrastructure will create a much needed step change in ensuring good practice and confidence in the context of e-commerce.

Five key ingredients that trust service providers must offer:

- Accountability: At a minimum this must mean assurance that their processes will stand up to scrutiny in disputes, but better still will mean they assume liability for the service they offer.

- Survivability/Longevity: Each service and the industry as a whole must produce technology and businesses that will be available to resolve disputes decades after events.

- Confidentiality: The customer will be giving their highly sensitive data to the trust services and the trust services must ensure confidentiality even within their own organisation.

- Integrity: Linked with accountability and longevity, but worth distinguishing. Because digital data is so easily created and forged, providers must be able to demonstrate the integrity of their information or the information they keep.

- Simplicity: Complexity and legacy are major stumbling blocks for e-commerce. To be successful, trust services must make life simpler for e-traders, and they must take account of existing infrastructure.

Understanding how to do all these things is not just about technology and a technology provider acting alone cannot resolve them. Realising the full vision will require collaboration amongst many of the likely stakeholders, for example governments, industry regulators, banks, insurers and lawyers.

There is a broad and deep set of technology problems that need to be addressed. The trust services team are working on some of the technology problems. At the same time, the team is engaging with customers from various industries to develop and validate models for trust services. It is worth noting that there are likely to be significant opportunities in many parts of the overall vision, and so it is worth researching this space in an incremental fashion, with one eye being kept on the big picture.

6 References

[Casas00] M. Casassa Mont – PASTELS project: Trust Management, Monitoring and Policy-driven Authorization Framework for E-Services in an Internet based B2B environment, 2000 [HP Restricted]

[Ellis99] C. Ellison – SPKI Requirements, RFC 2692, IETF – 1999

[Esign99] "Electronic Signatures in Global and National Commerce Act", 1999 House Bill 1714 (Bliley).

[Hicks01] M. Hicks, The old guard takes on trust issues, eWEEK –2001 http://www.zdnet.com/eweek/stories/general/0,11011,2699025,00.html

[Housl99] R Housley, W. Ford, W. Polk, D. Solo - RFC2459: Internet X.509 Public Key Infrastructure Certificate and CRL profile, IETF – 1999

[Myers99] M. Myers, R. Ankney, A. Malpani ,S. Galperin C. – RFC2560 - Adams X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, 1999

[PASt01] A. Baldwin, M.Casassa Mont, S.Shiu, A.Norman. – PAST Service: Permanent Active Storage Service: Survivability. HP Technical Report [HP Restricted]

[PRO00] UK Public Record Office - E-Records Management http://www.pro.gov.uk/recordsmanagement/

[Stein97] D.D. Steinauer, S.A. Wakid, S. Rasberry, - "Trust and Tracability in Electronic Commerce", http://nii.nist.gov/pubs/trust-1.html.

[Thomp01] J. Thompson - "A Matter of Trust", Infoconomy: Business Briefing No 16. pp B27-B29, Business Briefings 2001.