# Identity and accountability in business-to-business e-commerce

Yolanta Beres, Adrian Baldwin, Marco Casassa Mont, Simon Shiu
Trusted E-Services Laboratory
HP Laboratories Bristol

HPL-2002-112
April 26th , 2002*

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

trust services,
accountability,
identity, B2B,
e-commerce

To be successful, e-commerce solutions need to properly address accountability issues. Accountability is fundamental to business, and identity is fundamental to accountability. This paper analyses the role identity services play in supporting business-to-business (B2B) e-commerce. There are many good reasons for outsourcing identity management, and current solutions address some of these such as convenience or access control at the time of a transaction. However, if identity services are to help reduce the risks and track liabilities, then they must also support long-term accountability. By analysing the long-term accountability needs of e-business this paper shows that a trusted identity service must address longevity, confidentiality, simplicity and trustworthiness. This in turn produces new challenges for the technology, architecture and business model of such services. Identity is only one piece needed for accountability. The trust services vision is that the other pieces will be resolved by using similar accountable third party services.

* Internal Accession Date Only

Approved for External Publication

# 1. INTRODUCTION

Presently one of the greatest challenges for B2B e-commerce is providing the means for tracing accountability and verifying what happened during online transactions. Many e-commerce players recognize that risks related to the difficulty of proving legal liabilities in case of disputes are as influential in e-commerce as client risk[1] and financial risk[2] combined [SY 00].

In the conventional world, the two social factors of reputation and law have grounded fair trade for centuries. Since the first days of commerce, buyers and sellers have known each other's identities, first through face-to-face contacts, and later through letters, phone conversations and trusted intermediaries. This knowledge allowed for research into the past histories of the trading partners and helped in solving disputes when deals went bad.

Since electronic transactions have the same legal significance as their traditional counterparts, they are just as susceptible to disputes about what happened during a particular transaction. Any B2B electronic commerce system should guarantee that in case of a dispute the parties are able to identify the responsible entity; thus requiring that trading parties are able to conclusively identify one another. Recently different solutions have been proposed for solving identity issues, ranging from MS Passport [Passport] to Identrus based PKI [Iden 01]. Each solution proposes to centralize identity management into one single trust authority. In delivering these solutions the emphasis is on ease of use issues, such as single sign on, or immediate online authentication.

However, one aspect that is often overlooked is the accountability framework that should underpin such a service. Since trading parties will use the service to conclusively identify one another they should be able to hold an identity service provider to account over the identifications it provides. In addition, any actions by the identity service such as registration of identities and identity authentication have to remain verifiable long after the event if the service is to be of any legal value.

In this paper, we argue that in order for businesses worldwide to develop trust and confidence in the ability of identity service providers to represent their identity, the infrastructure must provide adequate accountability. Requirements for delivering a *trusted* identity service present significant technical and business challenges. Section 2 describes the issues in identity management, indicating its complexities and outlining existing approaches. An e-business scenario is used to illustrate the role an identity service might be expected to play in determining and proving responsibility.

In section 3 we outline requirements that identity services will need to meet if they are to address accountability needs and discuss known and potential technologies that will help in meeting these requirements.

[1] Client risk reflects the uncertainty a buyer or seller may have about dealing with an anonymous customer through online process.

[2] Financial risk reflects the value of goods or money exchanged in a transaction that could be lost through the use of the Web as a channel of delivery.

We also believe that although identity is essential in delivering accountability, in many cases of e-commerce, identity and digital signatures alone are not sufficient to make a party accountable for their actions. Disputes may relate to the (non) occurrence of a particular action as well as to the time of the occurrence. Additional trust services are required to provide certification and counter-signatures, as well as mechanisms such as time stamping, notarisation, and long-term storage. In section 4 we describe how these services come together with the trusted identity service to create an indisputable account of actions performed for each participating party.

## 2. IDENTITY MANAGEMENT

Identity has proved to be problematic over the centuries, as commerce was expanding from small closed communities. The Internet has massively increased the scope of the communities where people and companies trade and interact both by widening the geographic scope and by forming more dynamic and changeable communities. This dynamic nature is magnified by the way people change jobs both within companies and between companies. Whilst two companies are engaged in business it is common for the individuals involved to change. To this extent we consider identities to include not only named individuals, within or outside a company context, but also roles, job titles and even software processes acting as agents. It is with this in mind that identity is better described as a reference to a responsible entity that can be held to account rather than an individual.

Three important aspects of identity within e-commerce are:

1. Ensuring that an action is correctly associated with an identity and that this identity is linked to the originating user or process.

2. Providing profile information associated with the identity.

3. Managing a set of identities to ensure that overall information is accurate.

The first aspect addresses the requirement for the identity system to ensure that any action can be linked with the originating identity and that the user is properly authenticated when taking on this identity. There has been a large volume of work carried out on authenticating users via a variety or combination of mechanisms such as passwords, biometrics and physical tokens. Although this paper is not concerned with the mechanisms, it is important to highlight two aspects: firstly, whether the level of authentication is appropriate for the type of identity and secondly, what proof of authentication is required within an audit trail [EGov 01]. Note that an identity system cannot be expected to have responsibility for users who exchange, or divulge secrets and tokens and hence allow fraudulent actions to occur.

There are a variety of mechanisms for linking actions to identities. They range from strong non-repudiation devices using PKI [pkcs#7] ensuring an action has been signed through to single sign on systems, such as those supported by NT and systems like Passport [Passport] where cookies and redirection are used to manage a single identity session across multiple web sites. Systems such as single sign on and even SSL sessions where both parties are authenticated only associate a login session with a user; further audit mechanisms are necessary to link the session to the actions undertaken.

Having an identifier that links a person to a name or identity may be sufficient in a few cases, however other profile information associated with the identifier is often of critical importance. Commonly access control would be based on identifiers whether an identifier points to a role or job title [SCFY 96]. Alternatively the profile information could be used in making an access control decision [BG 98] but only if an identity system can vouch for, or has performed sufficient checks on the attributes in the profile. In such cases credentials that typically are linked to the identity can be useful to individually vouch for these profile attributes [BGC 99, FH 01].

Much of the current debate surrounding privacy issues on the Internet relates to identity profiles held by individual web sites. Services such as *Microsoft Passport* [Passport] and potentially those developed by the *Liberty Alliance* [Lib] attempt to centralise the information currently held in the numerous profiles into one or a federated set of identity services. These solutions, however, can lead to an even greater privacy concern when insufficient control is enforced on access to this information. Within a corporate intranet such profile information may well be included within a LDAP directory and will probably be accessible to all – it is, perhaps, the management of such data that forms one of the biggest challenges for identity management.

### 2.1. Management Issues

For many years user management has been a perpetual problem for IT departments with a considerable portion of their time spent creating and removing user accounts, administering profile information and dealing with forgotten passwords [GHDL 96]. The introduction of PKI further complicates the situation where administrators have to manage certificate issuing and revocation processes [FA 99] as well as managing single sign on infrastructure. Removing user accounts and revoking certificates can prove particularly problematic, often leading to errors and security holes. A number of tools exist to try to simplify this process and perhaps the task could be further simplified by integrating them with HR processes. The problem, however, is worsened when companies collaborate, requiring some form of joint user administration. It could become even more challenging if companies were required to be liable to other participating parties for the actions of erroneous identities.

Tracking changes in users identities, roles and job titles will always be time consuming and some what problematic. The issue increases considerably if a company needs to manage identities for each collaborative application. It is here that identity services bring a significant advantage, not only do they take charge of some of the management processes and associated IT systems but they also simplify the trust relationships.

Take the example described in Identrus case studies [Iden 01] where a pension management company collaborates with HR departments dealing with employee pension policies. Initially they need separate trust relationships between each HR department and each side has to handle the trust issues associated with user management. The switch to using Identrus as an identity service considerably simplifies these relationships. Each involved party set ups a trust relationship with Identrus's identity assurance service such that now the pension management company needs not worry about verification of the HR departments' users – this is achieved by all parties having a trust relationship with the identity provider.

In more general terms as long as such trust relationships exist between trading parties and associated identity services much of the risk in collaborative identity management is mitigated. This will, however, only be the case where the identity services provide sufficient guarantees as to the nature of the identities for which they are vouching. In particular contexts (like blind auctions, negotiation phases, etc.), an outsourced identity service can also guarantee that the requirement of pseudo-anonymity is satisfied, without compromising the liability of the involved parties.

### 2.2. Current Approaches

In this section we consider two major approaches currently available in the market to third party provided identity services. Firstly, there are certification authorities (CAs) such as Identrus and VeriSign. Secondly, there is Microsoft's Passport service, aimed more specifically at consumers. Although it comes under the label of identity, as a service Passport provides little if any guarantees about identity; no initial verification and assessment is made about the correctness of the identity.  It's main function is to simplify the overall interaction among customers and merchants by managing user profiles and allowing merchants to access details instead of users filling out forms. Even with the profile management the involved information is not validated.

Certificate authorities, on the other hand, provide a range of guarantees, from a simple 'they seemed to have that e-mail address' to full vetting services. Often these guarantees consist of complex legal arguments; for example, VeriSign's Certificate Practice Statement (CPS) is about 104 pages long and there is little clarity concerning the CA's liabilities, especially to the lay reader. Having said this version 2 of VeriSign's CPS [Ver01] is considerably clearer suggesting that CAs are recognising these issues.

One of the other aspects that is often overlooked is longevity of the identities – firstly, there are no mechanisms for tying together a series of certificates representing the same identity particularly as names change; this makes managing continuity of identity problematic. Secondly, CAs often do not keep records for sufficiently long timescales, as required by various country jurisdictions[3]. For example, VeriSign keeps records associated with class 1 certificates for 5 years, while retention periods of class 2 certificates have been just recently increased from 5 to 10 years; it is only the class 3 certificates that have information retained for 30 years. Beside that CAs should also be available to validate past signatures and acts represented in session audit logs long after the action taken place. This means that certificates, revocation lists, certificate practice statements and policy information have to be publicly available for the long timescales.

[3] See [EESSI 00] for legal record preservation obligations in European countries.

## 2.3. Identity in a Tendering Process Scenario

In this section we describe an e-business scenario in order to highlight certain trust and identity issues. The scenario involves a Government Agency advertising an engineering job and asking for contractors to bid for the work. Many government organisations have strict guidelines [OGPA01] that must be followed during the tendering process, a simplified version of which is shown in figure 1.

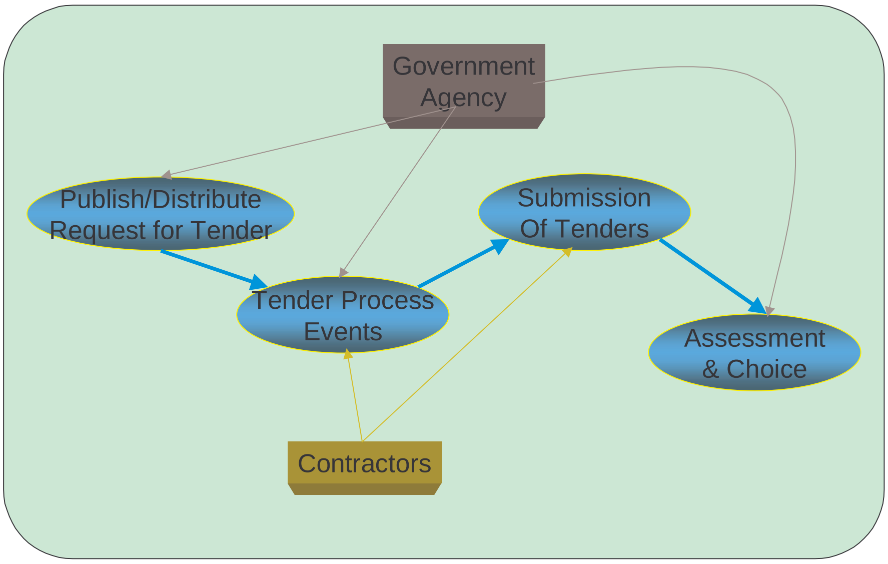

**Figure 1.** A generic tendering process.

Essentially the agency submits a request for tender, perhaps to a restricted list of contractors. They are free to ask questions. Questions are anonymous, and the answers (provided by the agency) are published to all parties to ensure fair play and to retain confidentiality concerns of the agency and their suppliers. Finally the contractors must submit their bids within an allotted time, and the agency chooses one supplier.

The main role of an identity service in this scenario is to authenticate representatives of the agency and the contractors every time they perform an action. Authorizations for different actions may require different information; for example when asking a question about the engineering job, it may be enough to prove it comes from a participating contractor, whereas when submitting a tender or an answer to a question it may be necessary to demonstrate that the source is a bona fide representative.

One clear advantage of using a generic identity service is that it saves users (or programs/services/agents) having to re-authenticate themselves, i.e. the users of the agency are authenticated only once when they log in, and this is then propagated to the portal of the tendering process.

An assumption in the above is that the identity service has a relationship with each of the corporations involved. For example, in order to verify that an appropriate authority within the organisation has submitted a contractor's submission, the identity service must have a trust relationship with that organisation.

Time is crucial to the participants in this scenario, and it would be severely undermined if events could not occur because the identity service is down; or if search results are unreliable due to partial failures. This raises the question of who is responsible when mistakes or delays occur.

In addition, confidentiality is of great importance in this scenario. The agency may not wish the contractors to know who is bidding for the job, and may also wish to avoid the possibility of collusion between contractors and the tender process providers. It is, therefore, imperative that the identity service authenticates and anonymises contractors when they ask questions. The service should have a clear model of how and when it releases information about entities, disclosing only necessary information in response to properly validated requests. It may be important to go further and ensure that even the administrators[4] of the identity service have no access to the confidential information of their customers.

In case of disputes, the identity service has to be able to recover enough evidence from its audit records to establish what actually occurred. Suppose there is a dispute about one of the answers given by the agency to a question. It is important to recover the answer given, and to establish precisely who submitted that answer. Verifying the authenticity and the authorization of the submission relies on the information recorded by the identity service. The service should sign its responses so that they can be audited, therefore vouching for any authentications and authorizations it has provided.

When a dispute occurs many years after the tendering process has taken place, the ability to prove the authenticity of old records becomes crucial. For example, the dispute could involve credentials presented by an engineering contractor to prove its identity at the time of the tendering process. Since a dispute in court may take place long after the tendering process has occurred, the credentials of the contractor in question may have been revoked, and the identity might have changed. It is important for the identity service provider to be able to prove that at the time of the tendering process both the identity and the credentials were valid and that they performed due diligence in checking them.

## 3. ACCOUNTABLE IDENTITY SERVICE

From the above discussion, it is clear that there are a number of issues associated with managing identity and its use. Even within a corporate intranet context the management

[4] In days of a competitive IT employment market contractors often fill roles of administrators and operators.

of identity can prove problematic and expensive. On moving to identities for business-to-business commerce identity management presents even bigger challenges with mis-management leading to greater liabilities. As the previous section has demonstrated, trusted identity providers, as third party services, can be of considerable value both in helping to manage these processes and in providing the technology to underpin the integrity and confidentiality of the identity and related profile information. However, such services must provide clear guarantees over the timescales on which the identities are relied upon and clearly state their management practices.

It is these clear guarantees that keep the identity services accountable. To take on accountability, along with the implied liabilities, they must have very tight computing systems along with professional operating procedures and good audit trails. They are not only accountable for the service they offer but their identity information helps underpin the whole accountability framework by allowing users to be properly linked to their actions – over considerable time periods. If that is not the case the relying parties would no longer trust the identity service, and trust may break down in the whole e-commerce application.

This indicates that *trusted identity services* have to deliver on the following at least:

- The credibility and validity of the data it is going to certify has to be properly assessed: in some cases it needs to engage in close interactions with the entities whose identity needs to be certified.
- The service must be trustworthy in the way it manages potentially critical and confidential information.
- The service provider has to ensure business continuity: it must run the service and be able to justify decisions made after many years.
- Identities need to be managed over a long period of time, where certified "statements" could change or might need to be revoked.

These arguments suggest that any identity service delivery model must carefully consider the appropriate accountability framework and the underlying delivery technology. Since many business processes and other e-commerce services rely on the conclusively certified identity the implications of a failure in an identity service can be severe. In the following sections we outline the major requirements for an accountable service and discuss technical approaches.

### 3.1. Requirements

The search for a responsible party in a disputed e-commerce transaction often depends on the underlying ***liability framework.*** Therefore, it is essential to establish from the start the liabilities of the participating parties, which in our case are identity owners and identity service providers. Liabilities often depend on the specific agreement between the participating parties along with applicable measures and limits. Parties need to form contracts to allocate and mitigate liabilities, and then they must execute according to these agreements. It is necessary that all involved parties agree on the common terms regarding liability for representations and actions by identity services. Such a liability framework is usually based on three factors: the legal environment, the specific business policy, and the anticipated threats. In general the liability framework should be based on universal legal principles as widely recognized in international law as possible.

It is also important that standard ***dispute resolution*** mechanisms are specified, or failing this the jurisdiction under which the agreement is made, wherever possible to make enforcement practical and efficient. While a generic dispute resolution service can be designed for specific applications such as payment systems [AHS 98] using technology solutions, complete automated dispute resolution is not feasible or even desirable. A first step could be to specify dispute avoidance and resolution best practices, as has been done in the application service provider industry [ASP 00]. In any dispute, however, the final decision lies with a human player, called the verifier or arbiter.

Although it is realistic to state that disputes will happen, the overall goal should be to deliver such a service that chances for a dispute are minimal. This is motivated by at least the following two factors: (1) dispute resolution is one of the most expensive procedures to go through for any entity. Any mechanisms that will succeed in keeping the number of cases requiring an independent arbitration as low as possible will reduce cost considerably. (2) Parties in b2b e-commerce transactions need to be protected from possible abuses by authorities as well as fraud attempts by other parties.

The first challenge in achieving this goal is ***long-term survivability***, both in terms of technology to preserve the long-term integrity of the information held and of the related management processes, and to ensure service continuity under different threats: intrusions, viruses, environmental disasters, etc. The previous scenario has shown that timely service availability is essential for smooth execution of e-commerce transactions. The service should therefore be able to recover seamlessly from network and systems failures maintaining a consistent directory and state backup. Without survivability it is hard to see how much identity services can actually simplify lives for identity owners.

An example from the scenario, where a dispute occurs many years after the tendering process has taken place, emphasises the need for ***longevity*** of the identity information. The need to retain provable authenticity long after the action takes place implies that identity has to be traceable over periods of time. This is especially so within an enterprise context: the roles of people in the organisation change, together with people themselves. It is often important to know the people who occupied a role previously as well as the role history for a specific person. The identity service therefore has to keep information about expired identities and has to be able to specify relations between new identities/credentials and old ones. Such information would allow tracking down the responsible entity even years after its identity was first registered and verified.

Since identity services act as trusted parties in e-commerce transactions, their ***reliability and trustworthiness*** is crucial. The processes in the tendering scenario rely on both the security and honest actions of the identity service. Any dishonest actions or compromised service could drastically affect the final result. Keeping audit trails and accounting records should discourage fraud and malicious acts. Their purpose would be to ensure that failures due to omission or fraudulent behaviour are riskier and therefore less likely.

Its clients would consider a lot of the information handled by the identity service as highly confidential. Achieving a high level of ***privacy*** is therefore essential. The underlying privacy framework should be able to interoperate between various jurisdictions and trust domains. In addition, access control measures must be in place to control access to the confidential information both from inside and outside the service. The service must allow identity owners to control their information subject to legal requirements. Pseudo-anonymity must be available when required and allowed: identity owners should be able to decide when and where they want to disclose their identity. Whilst enforcing this, the identity service must associate pseudo-identities to the real ones and keep track of those associations over long periods of time. In cases where identity information is kept for longer terms by an identity service, the mechanisms should be present that allow control of the privacy terms even if the identity owners have changed.

The final note is on ***ease of use and integration***. It should be easy to integrate the identity service into existing e-commerce applications. The internal business processes of identity owners should be affected as little as possible when the identity service is introduced. This means that the service must use common protocols for asserting and authenticating identities, and support extensible mapping of its identities to other types of identifiers, including real-world names, domain names, roles within companies, email addresses, etc. As was mentioned in section 2, numerous existing solutions although simplifying certain aspects of identity management, also introduce complexity in integrating with existing business processes and in administration of various identities. Great care must be taken to ensure that business processes do not need re-engineering to fit in with the trust service solution. Otherwise, this would not only increase the cost of security management, but would also create administrative confusion and error leading to possible abuse, and thus increasing the likelihood of service failure and the possibility of disputes. Standardization efforts and related initiatives are a viable way to ease this burden.

### 3.2. Technical Approaches

Although some of the accountability challenges such as developing a liability framework and dispute resolution standards are outside the scope of technical issues, others can at least be partly solved with the help of technical approaches. Technical features then help in delivering the most reliable and survivable service.

Long-term survivability, for example, is a function of an overall system and should therefore be incorporated into the basic architecture of a service [EFLM 98, Neum 99]. Whilst traditional business continuity is concerned with the survival of businesses in the short term, a long-term survivability approach should aim to ensure that the correct functionality is achieved in the event of failures and attacks over long periods of time. For the identity service this means ensuring relying parties can find out about identities and that the information about these identities survives for the appropriate timescales. A number of mechanisms can be used to achieve levels of survivability with many drawing inspiration from biological and sociological models. Survivability should be considered whilst designing the system to ensure that there is a high level of adaptability. The use of the following mechanisms can help achieve a survivable design:

*Replication* – Commonly used to achieve high availability.

*Randomness*—Ensuring random data placement, for example, making it harder to attack all copies of a piece of data.

*Diversity*—A lack of diversity in the code base can lead to replicated systems that all fail due to the same bug [Ling 01].

*No single point of failure*—Obviously any single point of failure leads to vulnerabilities and should be carefully controlled.

*Compensation*—A survivable system should acknowledge component failures and adapt, for example using delayed updates.

*Devolved Control*—The use of local management decreases reliance on a central management system and can make it harder to use the management system as an attack channel.

*Adaptability*—A system that can monitor its performance and adapt in response to problems or large workloads will help ensure continuity. Moving services away form broken components could even be seen as a form of self-healing.

Signing identity and profile statements, along with messages involved in business transactions and ensuring they are time-stamped with keys of sufficient size to protect them for their expected lifetime can achieve information integrity. When digitally signed, messages serve as binding statements for which the signatory is accountable. The accountability can be proven if the association between the signature on the message and the signing party can be proven. Legal use of digital signatures, however, is impossible without using time stamps, because time plays a crucial role in the accountability assurance process. Digital time stamps are data items that, when added to signed statements, are capable of proving the date an identity was created, signed, or last modified [BRW 00].

Although security and confidentiality in web-based applications often refers to the ability to encrypt a link between a client and the service provider, stronger claims should be made about the way information is kept encrypted within the service itself. As mentioned previously, one of the most important issues is controlling access to the information; including residual information such as billing data. Many issues of access control are well understood and fine-grained access control has to be applied to the information within the identity service. Longevity, however, presents a challenge since identities change over time, and the identity that had access previously may have changed in later periods. Identity tracking and transitioning mechanisms are, therefore, essential.

It is also important, that both the underlying operating system and hardware platform used in service delivery is secure and trusted. A trusted computer platform performs in accordance with its documented specification and will prevent any unauthorised activity. Specifically, a trusted computing system can be relied upon to enforce a documented security policy. The role of trusted systems 30 years ago was primarily for protection in military applications [BePa 76]. In more recent years, certain approaches such as TCPA [TCPA 01] are receiving wide acceptance in commercial applications. The fundamental requirements of a trustworthy computer system resonate with some of the requirements of an accountable service:

- Audit information must be selectively kept and protected so that actions affecting the security can be traced to the responsible entity;
- Individual subjects must be identified and access control measures associated with each object;
- Computer systems must contain hardware and software mechanisms that can be independently evaluated to provide sufficient assurance that the system enforces stated requirements;
- The trust mechanisms enforcing the basic requirements must be continuously protected against tampering and unauthorised changes.

## 4. BEYOND IDENTITY – TRUST SERVICES

In many cases of business conduct, identity alone is not sufficient to make someone accountable for their actions or data. Companies still need to consider how to make the transactions legally binding, so they'll stand up in the court of law. Having identity and authentication services properly set up is the essential starting point. However, disputes may relate to the (non) occurrence of a particular action as well as to the time of the occurrence. For example, in the tendering scenario there was a submission deadline for bids by contractors. The evidence about the time of submitting the bid is critical – particularly the time when the tendering service receives late bids.

In general, disagreements relate to whether a particular event occurred, when it occurred, what parties were involved in the event, and what information was associated with the event. The parties involved in the disputes should be able to obtain evidence for establishing what actually occurred. To minimise risks of possible disputes, the B2B e-commerce transactions should generate enough evidence for parties to be able to convince third parties of the misbehaviour. Accountability policies should specify rules to be applied during business transactions with regard to what evidence has to be kept for establishing and verifying accountability in case of disputes and misunderstandings.

Transactional evidence involves generating verifiable information that includes sequencing and time stamping, cross-certification, data integrity, and finally assurance of long-term authenticity for important transactions. Our vision [BBCS 01] is that each of these can be delivered as a series of trust services. Besides an identity service, other services are necessary such as recommendation and credential services for vetting the contractors, and an audit service (probably consisting of both a time stamping and a long-term document storage service) for post event non-repudiation. By acting together they create a trust services eco-system: services seamlessly interacting to deliver accountability assurance in B2B e-commerce.

## 5. CONCLUSIONS

It is widely recognized that identity plays major part in the establishment of accountability in e-commerce transactions. Identity management, however, is difficult both within company's internal systems and between companies participating in collaborative applications. To simplify the management process, third party identity services are being introduced. In this paper, we argued that in order for businesses, worldwide, to develop trust and confidence in the ability of identity service providers to represent their identity, the infrastructure must provide adequate accountability.

To support accountability, identity services have to address requirements ranging from longevity, survivability, reliability and trustworthiness to privacy and ease of use. This is likely to require more robust and secure approaches such as trusted computer platforms, highly tolerant distributed replication mechanisms, and fine-grained access control.

It is also essential for the legal industry to develop the underlying liability framework that helps establish the liabilities of both the identity service providers and the relying parties. Without such a framework it could prove difficult if not impossible to find the responsible entity when disputes or failures happen.

Finally having identity and authentication services properly set up is just the essential starting point. Additional trust services are necessary in helping to establish what actually occurred during e-commerce transaction. This means that the whole set of trust services might need to available for supporting accountability in B2B e-commerce.

## REFERENCES

[AHS 98] N. Asokan, E. van Herreweghen, and M. Steiner. Towards a Framework for Handling Disputes in Payment Systems. In *Proceedings of the 3rd USENIX Workshop on Electronic Commerce*, September 1998.

[ASP 00] Application Service Provider Industry Consortium. Dispute Avoidance and Resolution Best Practices in the ASP Industry. ASP Industry Consortium White Paper, 2000, http://www.allaboutasp.org/.

[BBCS 01] A. Baldwin, Y. Beres, M. Casassa-Mont, and S. Shiu. Trust Services: A Trust Infrastructure for E-Commerce. In *HP Laboratories Technical Report*, August 2001.

[BePa 76] D.E. Bell and L.J. La Padula. Secure Computer System: Unified Exposition and Multics Interpretation. ESD-TR-75-306 (March), Mitre Corporation, 1976.

[BG 98] A. Baldwin and C. Goh. Towards a more complete model of role. In *Proceedings of the Third ACM Workshop on Role-Based Access Control*, October 1998.

[BGC 99] A. Baldwin, C. Goh, M. Casassa-Mont. Role of Policies in a Distributed Trust Framework. In *HP Laboratories Technical Report*, HPL-1999-104, 1999.

[BRW 00] A. Buldas, M. Roos, J. Willemson. Optimally efficient accountable time stamping. In *Public-key Cryptography PKC'2000*.

[EESSI 00] European Electronic Signature Standardization Initiative. Trusted Archival Services. Phase #3, Final Report, August 2000.

[EFLM 98] R. J. Ellison, D. A. Fisher, R. C. Linger, H. F. Lipson, T. A. Longstaff, and N. R. Mead, Survivability Protecting Your Critical Systems. In *Proceedings of the International Conference on Requirements Engineering*, 1998.

[EGov 01] E-Government Strategy Framework Policy and Guidelines: Registration and Authentication v2.1, 2nd Nov 2001, http://www.govtalk.gov.uk.

[FA 99] S Farrell, C Adams. Internet X.509 Public Key Infrastructure Certificate Management Protocols. IETF RFC 2510, http://www.ietf.org/rfc/rfc2510.txt.

[FH 01] S Farrell, R Housley. An Internet Attribute Certificate Profile for Authorization. IETF Draft, http://www.ietf.org/internet-drafts/draft-ietf-pkix-ac509prof-09.txt, 2001.

[GHDL 96] V.D. Gligor, A. Hummel, K. Deinhart, S. Lorenz. Role-Based Security Administration. In *Journal of Sicherheit in Informationssystemen*, 1996.

[Iden 01] Identrus Case Studies. http://www.identrus.com/products/allianz.xml.

[Lib] Liberty Alliance Project. http://www.projectliberty.org.

[Ling 01] R. C. Linger. Systematic Generation of Stochastic Diversity as an Intrusion Barrier. In *Technical Report*, CMU, Software Engineering Institute, CERT Coordination Centre, http://www.cert.org/archive/html/stochastic-divers.html.

[Neum 99] P. G. Neumann. Practical Architectures for Survivable Systems and Networks. SRI International, Final Report for the Army Research Lab, http://www.csl.sri.com/papers/arl-one/, Jan 1999.

[OGPA01] Overview of the Government Procurement Agreement, http://www.bipcontracts.com/Briefings/Briefings2001/Brief01_01.html.

[Passport] Microsoft .Net Passport, Business Services, http://www.passport.com/Business/Default.asp?lc=2057.

[pkcs#7] PKCS #7 Cryptographic Message Syntax Standard. *RSA Laboratories Technical Note*, ftp://ftp.rsasecurity.com/pub/pkcs/doc/pkcs-7.doc.

[SCFY 96] R. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman. Role-based Access Control Models. In *IEEE Computer*, 29(2), February 1996.

[SY 00] D Schoder, Pai-Ling Yin. Building Firm Trust Online. In *Communications of the ACM*, Vol 43 No 12, December 2000.

[TCPA 01] Trusted Computing Platform Alliance. Main Specification, Version 1.1a, November 2001, http://www.trustedpc.org/home/pdf/main v1_1a2.pdf.

[Ver 01] VeriSign Certification Practice Statement (CPS) version 2.0 (2001), https://www.verisign.com/repository/CPS/.