Deploying a Secure Cyberbazaar by adding Trust on Commercial Transactions

D. Spinellis,[a] K. Moulinos,[b] J. Iliadis,[c] D. Gritzalis,[b] S. Gritzalis,[cd] S. Katsikas[c]

[a] Department of Management Science and Technology
Athens University of Economics & Business (AUEB)
76 Patission St., Athens GR-10434, Greece, email: dds@aueb.gr

[b] Department of Informatics, Athens University of Economics & Business (AUEB)
76 Patission St., Athens GR-10434, Greece, email: {kdm, dgrit}@aueb.gr

[c] Department of Information & Communication Systems,University of the Aegean,
Samos, GR-83200, Greece, e-mail: {jiliad, sgritz, ska}@aegean.gr

[d] Department of Informatics, Technological Educational Institute (TEI) of Athens
Ag. Spiridonos St., Athens GR-12210, Greece, e-mail: sgritz@teiath.gr

Abstract

Traditional business practice depends on trust relations between the transacting parties. One of the most important aspects of this trust is the quality of the offered services or products. The Web currently constitutes an enabler for Electronic Commerce, providing a global transaction platform that does not require physical presence. However, transferring trust from the physical world to the electronic one is a process that requires a trust infrastructure to be provided by the electronic world. We believe that current infrastructure models based on Trusted Third Parties can be enhanced. We introduce the notion of Digital Seals and we provide a mechanism for transferring the trust placed by users to companies in the physical world, to the electronic one.

Keywords

Security, Electronic Commerce, Trusted Third Party (TTP), Public Key Infrastructure (PKI), Digital Seal.

Acknowledgments

This work has been partially funded by the European Commission's *Telematics for Administrations* Programme, *COSACC* (Co-ordination of Security Activities between Chambers of Commerce) AD 4001 project, 1999-2000.

1. Introduction

Electronic Commerce could be the dominant way of making business in the not so distant future. The advantages of e-commerce are numerous: it eliminates the need of intermediaries, minimizes the cost of the product delivery, provides customers with worldwide market access, provides a platform for new business models. The reasons for the current explosive growth of e-commerce are mainly two, namely the wide deployment of data network technologies, and the evolution of the World Wide Web (Web).

For the past fifty years, advances in telecommunications and computing largely occurred side by side. Nowadays, the rate of advances in these technologies is converging. Moreover, the Internet is becoming the first manifestation of a unified channel. Information Technology is becoming more and more tied to network-enabled applications and solutions. The Internet is becoming a major conduit for commerce [IMRG98], since it is used for communication between organizations or businesses, between individuals and organizations, between individuals, and for intercommunication within an organization.

The friendly interface of the Web and the fact that it enables users to interact using multimedia content, is attracting individuals and businesses altogether to enter into e-commerce. The security problems Web faces [GS97] do not seem to discourage these entities against using the Web for the time being. However, as the spectrum of e-commerce and e-business applications is widens, the user demand for a secure application framework they can trust will augment. Users have also not been discouraged by the current lack of an appropriate legal framework for the regulation of services over the Internet. This lack forces network-based technological applications to have specific features that allow them to operate in a loosely federated environment.

Traditional business practice depends on the trust between the involved parties. The cornerstone of this trust consists of:

1. The security of the transactions performed. This practically means that neither the user nor the service provider (or merchant) can act in a malicious or unpredicted manner.

2. The quality of the exchanged services or products. The consumer must be able verify that the service or product he wishes to receive originates from the provider he selects and trusts, and not from another provider who is claiming to be the former.

There are organizations that individuals typically trust, like Banks and Chambers of Commerce. These organisations often act like intermediaries between two or more parties of a transaction, protecting the interests of these parties. The role of these organisations is to deliver confidence and inspire trust in those transactions. A similar scheme applies to the distributed communication networks, that of Trusted Third Parties (TTPs). A TTP is an impartial organization delivering business confidence, through commercial and technical security features, to an electronic transaction [CEC94]. The most typical application areas of TTPs include the protection of confidentiality, integrity and authenticity in electronic transactions.

TTPs deliver confidence and trust, concerning the transactions themselves. What they do not deliver is confidence and trust regarding the service or product delivered through transactions at a loosely federated environment, like the Web. We introduce the notion of TTP-supported "digital seals", which can be used for that purpose. A digital seal is a token, which is put on the e-commerce company's electronic assets, like the company's Web pages, and validates certain characteristics of the company itself, the services or the products offered

by that company. These characteristics include the objective information towards the user, quality of a company, quality of a product, customer satisfaction etc.

This paper is organized as follows: In section 2 we present the threats against electronic trust, while in section 3 we provide an overview of the trust relationships in a loosely federated environment, like the global Public Key Infrastructure (PKI). In section 4 we outline the framework that is needed in order to meet the evolving requirements of e-commerce. In section 5 we propose a mechanism that contributes to providing secure e-commerce, by enabling another level of trust in electronic transactions. Finally, in section 6 we present our concluding remarks.

2. Threats against electronic trust

The usage of electronic messaging is becoming more widespread as Information and Communication Technology becomes more effective and cheaper. This results in more information being carried electronically, and becoming vulnerable to attacks such as eavesdropping, non-authorized modification and masquerading. A short overview of the threats against a communication channel follows [CGGG98, SKG99]:

1. *Monitoring of communication lines*: Electronic transaction information being transmitted in cleartext form renders an unauthorized third entity capable of monitoring it.

2. *Shared key guessing*: Digital envelopes are used in order to maintain the confidentiality of exchanged information, and at the same time reduce the computational overhead of public key encryption. If the symmetric keys used in digital envelopes, or the respective symmetric ciphers, are not cryptographically strong then the exchanged messages can be recovered

3. .*Shared key stealing*: Transporting a symmetric key to the other party must be done with a mechanism that protects its confidentiality. If this is omitted, it might be monitored.

4. *Unauthorized modification of information in transit*: An entity monitoring the messages exchanged throughout an electronic transaction may actively block them, modify them and forward the modified ones to the recipient without the latter being able to notice the modification. This kind of attack is known as the "man in the middle attack" [Garfi97].

5. *Forged Network Addresses*: The lack of security mechanisms in the DNS [DeViv98] renders the IP-based authentication vulnerable to attacks. An imposter may succeed in authenticating himself by forging his network address. Until DNS evolves in a secure naming system, IP-based authentication should be avoided or additional authentication measures should be used.

6. *Masquerade*: This threat refers to unscrupulous entities that pretend to be trusted ones. "Web spoofing" is a widely deployed attack of this kind. It is manifested either by exploiting DNS protocol vulnerabilities and misleading users to untrusted sites, or by properly modifying the DNS records of a name server and thus allowing an attacker to mislead a name server to wrong sites. In addition to that, Web spoofing is also manifested by unauthorized modifications of HTML pages. An attacker may alter the links of an HTML page and lead an unsuspected user to malicious programs or false information. [Garfi97]

7. *Password stealing*: Passwords gained their popularity due to their ease of use and implementation low cost. However, passwords transmitted in the clear and reusable passwords [Garfi96] should be avoided because they constitute a security threat.

8. *Unauthorized access*: An unauthorized user may gain access to local or network resources by masquerading, password stealing and exploiting bugs of the underline operating system. A sound access control policy is required, that meets the requirements of a well-defined security policy of the organization.

9. *Repudiation of origin*: An unscrupulous user may deny having digitally signed a document, claiming prior key compromise or loss.

10. *Private key stealing*: Should the private key be stolen, unauthorized entities will be able to act on the private key owner's behalf and recover confidential information.

11. *Private key compromise*: Should the private key be compromised, unauthorized entities will be able to act on the private key owner's behalf and recover confidential information. A TTP should take seriously under consideration the place where the private key generation has taken place, in order to avoid possible future accusations by keyholders, claiming that the TTP colluded in having their keys compromised, or did not take the necessary security measures during key generation and transport.

3. Trust Relationships

TTPs supply technically and legally reliable means for producing objective evidence concerning an electronic transaction. TTP services are provided and underwritten by technical, legal, financial and structural means [Caste93]. TTPs are connected through chains of trust (usually called certificate paths) in order to provide a web of trust forming the notion of a Public Key Infrastructure.

A PKI consists of more than one TTPs, hence the need for cross-certification of users registered with different TTPs. Fulfillment of this requirement presupposes the establishment of communication paths [Rensb97, Cliff98, AGGPS98] between the final users. There are four distinct implementation alternatives, depending on the level of intercommunication (see Figure 1) [Gritz98]:

1. *User-to-User*: Users must be capable of processing the entire certificate path that leads to the communicating party.

2. *User-TTP-User*: TTP acts as an inline intermediary. Users are expected to be registered with the same TTP, and the latter becomes a communication bottleneck.

3. *TTP-to-TTP*: Cross-certification is implemented on the TTP level. The communicating entities possess certificates from TTPs that corroborate. TTPs must have previously established a bilateral agreement.

4. *HighLevelTTP-to-HighLevelTTP*: Cross-certification is performed at a high level of the TTP certification hierarchy. Each communicating entity trusts its own high-level TTP, and since these are cross-certified, the communicating entities also trust each other’s high-level TTP and therefore the low-level TTP that issued each other’s certificates.

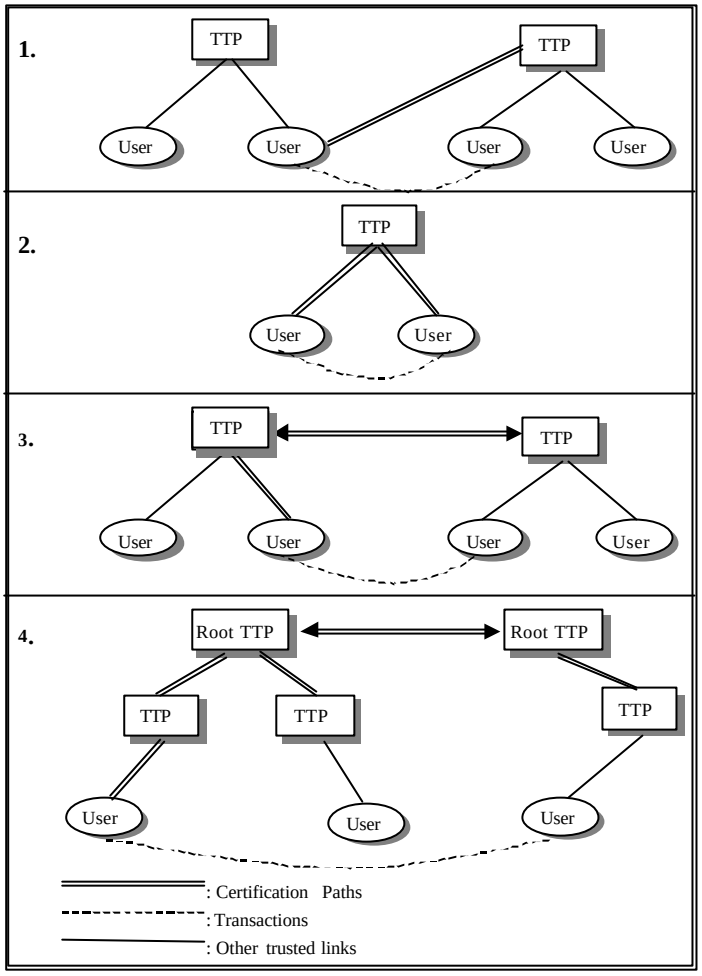

Figure 1: Cross Certification Alternatives

The first alternative is not efficient because it requires the end user to obtain all the existing certificates (e.g. the case of PGP). The second alternative, the case of Kerberos authentication scheme, is not suitable for large-scale networks, since the TTP becomes the bottleneck of the whole PKI. In the last two alternatives the creation of a trust relationship requires the digital signing of an entity's certificate by another entity (cross certification). In the case of network model (alternative 3) each TTP digitally signs the certificates of the other TTPs, while in the hierarchical model (alternative 4) the higher level TTP digitally signs the certificate of the subordinate TTP. Obstacles may emerge when these models are used on a wide scale. We identify three distinct categories of these obstacles:

1. *Technical.* TTPs of a specific geographical or business domain may develop infrastructures and Certification Policies that are not interoperable with those of TTPs of another domain.

2. *Legal.* Legal particularities, especially national-level ones, may hinder the interoperability of TTPs being subject to different or even contradicting legislature and regulatory frameworks. An instance of this problem is the case of Germany, where Federal Law prohibits national TTPs to be certified by foreign TTPs [GFMER98].

3. *Managerial/organizational.* Generating trust chains premises bilateral contractual agreements. These may impose restrictions on the management of a TTP, including additional, expensive protection mechanisms for the TTP itself, or minor adjustments in

the Certificate Policy of the TTP. These restrictions render the aforementioned bilateral agreements unattractive to TTPs.

We conclude that end-users are restricted to isolated electronic trust islands. Users trust the security of certain transactions, which are protected by a specific group of authorities they trust. Moreover, this trust model does not enable trust on the business side of electronic transactions, that is the quality of services or products offered by e-commerce providers. One of the reasons why this model is not capable of enabling this kind of trust is because it requires the intermediation of entities (i.e. Certificate Authorities or TTPs) that do not, and should not, belong or be involved in any way with the business sector.

The trust model we have presented needs enhancements. These could derive either from ongoing research on PKI, and from managerial solutions such as bilateral agreements between TTPs. However, we believe that another trust model is needed as well, complementary to the one we presented above. This model must enable trust on the quality of services or products offered by e-commerce. The rest of this paper investigates solutions for communicating this kind of trust in loosely federated environments.

4.Solution Framework

Let us assume the working example of an international trade firm. This firm maintains an e-commerce site, with a Web front-end, at its headquarters. Having all the customers communicate with the firm through this site would result in increased traffic around the site, and thus in lower availability of the electronic commerce services offered by the firm. Furthermore, a single point of trade would be an attractive target for availability attacks either by competitors or by unscrupulous entities that have no gain in performing such an attack.

The firm should provide a distributed system for providing its services and communicating with its customers. This is achieved by a network of local agents, which also operate an e-commerce site. Therefore customers will have the opportunity to contact the nearest local agent, this being beneficial both for the customers and for the firm itself.

However, customers who communicate with local agent sites would want to ensure that the agents (and the respective Web sites) they communicate with are indeed local agents, accredited by the firm. There is a clear need for transfer of the trust the customer's place on the firm, to the agents.

The firm should design a well-defined set of service quality criteria a potential local agent must meet in order to be accredited. A set of service quality criteria that would inspire trust to the customers, for the local agents. Designated representatives of the firm should audit the local agent's infrastructure and operation, and provide accreditation if the criteria are met.

Therefore, to provide a solution to the trust transfer problem it would be enough to find a way for customers to verify that a local agent meets those criteria. The firm could issue accreditation tokens to its agents, providing for the verification of compliance with the criteria, and enabling the trust transfer. We will be calling these accreditation tokens *seals*.

Seals provide customers with the capability to verify that a local agent is accredited by the firm, therefore they can trust the local agent as much as the firm itself, since the accreditation process includes compliance checks against quality criteria lay out by the firm. There is no point in providing different levels of accreditation, because that would cause confusion to the customers regarding the quality of services offered by the local agent. Moreover, the

customers will probably be willing to trust the local agent as much as the firm, only if the agent meets the full set of quality criteria set by the firm.

We provide a mechanism for customers to validate the seals they meet while visiting local agent sites. The accreditation and seal registration procedure encompasses five steps (Figure 2), if accreditation is successful, and three steps only if accreditation of the local agent is rejected. If the local agent is accredited, he receives a digital seal, which can be installed in its HTML pages, enabling the customers that visit the agent to confirm that it is a firm-accredited agent.

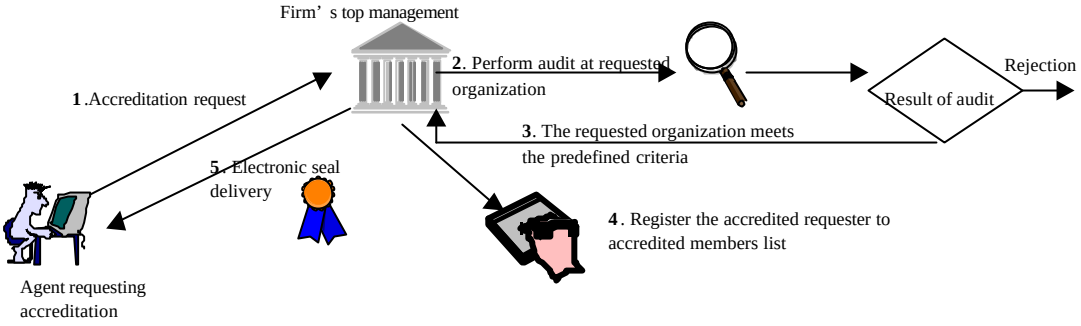

Figure 2: Accreditation and Seal Registration procedure

5. The proposed solution

5.1. Architectural Overview

We provide a mechanism for firms to register accredited agents of theirs, and for customers to verify online the validity of a digital seal. This mechanism includes the use of digital certificates, and requires from the agent to have obtained before requesting accreditation, a digital certificate from a Certification Authority.

A local agent applies for a digital seal to the firm. The firm audits the management of the services provided by the local agent and the services themselves and asserts whether they meet the predefined quality criteria. The audit procedures and the quality criteria themselves are of no interest to this mechanism. The firm is responsible for the design of those, according to the policy it wishes to follow regarding accreditation. Whatever policy the firm decides to adopt, it should make it readily available to its customers.

If the agent qualifies, the firm issues a digital seal and registers the agent in a database that contains all the local agents that have qualified for a digital seal. When a customer visits the site of the local agent, he will be able to verify the validity of the digital seal placed by the agent in its HTML pages.

Since the number of agents may be high, the communication lines used by the database of accredited agents could become a bottleneck in the seal verification process or a deterrent factor in the verification process, should the database fail to operate. This problem must be dealt with computing and network resources of the firm itself, such as replication of the database and fallback communication lines.

We present our mechanism in the next section through an example of a transaction between Alice, a customer, and Bob, a local agent of a firm called Trend. We assume that Trend operates a Digital Seal Authority and has provided Bob with a Digital Seal. Alice

communicates with Bob in order to purchase services or products. Alice verifies the Digital Seal she sees at Bob's pages by communicating with Trend, and Trend communicates with Bob while verifying the validity of Bob's Digital Seal. Therefore, the communication channels are three:

1. Alice communicates with Bob

2. Alice communicates with Trend

3. Trend communicates with Bob

We assume that all communications occurring within the framework of our mechanism use HTTP over SSL, to protect the information being exchanged. Table **Error! Unknown switch argument.** contains a list with all the acronyms we use throughout our mechanism.

Table Error! Unknown switch argument. **: Acronyms**	
AP	Accreditation Validity Period. This is the validity period of a Digital Seal.
Cert-W	The digital certificate used by the Web server of the agent to enable SSL connections to it.
DAA	Database of Accredited Agents. This is the database that contains information on the agents that have been accredited and possess a Digital Seal.
DSA	Digital Seal Authority: the section of the firm which is responsible for the operation of the service we present.
H-Cert-W	The result of a predetermined hash function (e.g. MD5, SHA-1) on Cert-W
H-URL-W	The hash function result of a page WPC-W hosted by the agent's Web server.
URL-W	A URL to a page hosted by the agent's Web server, which will bare the Digital Seal. The agent may decide to place a Digital Seal to more than one pages hosted by his Web server.
WPC-W	The actual page (the data contained therein) hosted by the agent's Web server, and pointed at by URL-W.

5.1.1. Registration of the Local Agent

The agent requests accreditation from the firm. Our mechanism does not require any specific method for communicating this request. The request contains formatted information, as presented below. For this reason, we propose the use of a request collection mechanism that will allow automated filing and processing of the requests themselves.

The agent initiates the accreditation request by communicating the following information to the DSA, typically the firm:

1. Identification and contact information of the agent,

2. Cert-W,

3. the set of URL-Ws, and

4. the set WPC-Ws. These pages must contain the prospective Digital Seal itself, that is the image file that represents the Digital Seal and an underlying URL pointing to the DSA.

The DSA must then perform an extensive audit of the services provided by the agent, and decide whether to accredit the agent. The details of this audit are of no interest to this paper. The firm should establish a well-defined set of rules and controls to be used throughout the audit, and should also produce a publicly available document that states what is the agent being accredited for, if the audit is successful and it is issued a Digital Seal. If the firm decides to accredit the agent, it proceeds with signing the following information and storing it at the Database of Accredited Agents (DAA):

1. H-Cert-W (to be used as an index for Digital Seals at the DAA),
2. Cert-W,
3. the Accreditation Validity Period (AP),
4. the set of URL-W,
5. the respective set of H-URL-W.

The DSA then instructs the agent to install the set of pages WPC-W at his Web server. These pages differ only to the ones that were hosted by the server previously in that they include the graphic image of the Digital Seal and a respective link to the DSA verification script.

5.1.2. Verification of the Digital Seal

When a user visits the site of an agent, and specifically one of the pages included in the set of URL-W, the user can verify the validity of Digital Seals these pages bare, by clicking on the Digital Seal graphic images. The underlying link executes a script hosted by DSA, and the response of the DSA verification is returned to the user by the DSA Web server. Digital Seal verification is performed by the DSA, on behalf of the user.

Suppose that *Alice* (a user) wishes to communicate with *Bob* (an agent), and verify the Digital Seal found on Bob's page URL-W, which was issued by the Digital Seal Authority of the respective firm, *Trend*. The verification steps are the following:

1. Alice communicates with Bob using the HTTPS protocol (HTTP over SSL). When Alice views a page hosted by Bob's Web server, containing a Digital Seal graphic image, she can click on that image and the underlying URL will direct Alice to the Digital Seal verification script hosted by Trend's Web server. Alice must send to Trend at that time the hash of Bob's SSL certificate (H-Cert-W) and the URL of the page she was viewing at Bob's Web server (URL-W).

2. Trend locates Bob's Digital Seal record in his database, using as an index the H-Cert-W he received. If Trend does not locate any Digital Seal record with that index, Trend returns a page to Alice, informing her that the Web site she was visiting has not been accredited by the firm. If Trend locates the corresponding Digital Seal record, but Cert-W has expired, he informs Alice that the Digital Seal has expired as well. The Digital Seal record may also contain revocation information on Cert-W and respectively on the Digital Seal (see also next step of the verification phase). If Cert-W is revoked, then Trend informs Alice that the Digital Seal is revoked as well.

3. Trend communicates with the CA that issued the SSL certificate for Bob's Web server and verifies the validity of this SSL certificate. If Bob's Web server SSL certificate has been revoked Trend informs Alice that the Digital Seal is revoked as well, because of the respective SSL certificate revocation. Trend also stores the revocation information in the respective Digital Seal record at DAA. If other verification requests occur before Bob obtains a new SSL certificate and Digital Seal, the verification will not need to proceed any further than step 2.

4. Trend checks whether URL-W Alice was viewing is contained in the retrieved Digital Seal record. If it is not, Trend informs Alice that the contents of that page, and the respective services provided through that page, could have been accredited but Bob had not requested accreditation for them.

5. Trend retrieves the address of Bob (fully qualified hostname of Web server) from Bob's certificate, which is contained in the Digital Seal record retrieved in step 2. Trend proceeds with connecting to Bob using the HTTPS protocol.

6. Trend retrieves page URL-W from Bob's Web server, computes H-URL-W and verifies that this hash is one of the hashes in the set of URL-W contained in the Digital Seal record retrieved in step 2. If the computed H-URL-W is not contained in the aforementioned set, Trend informs Alice that although Bob's page had been certified, there have been changes in that page for which Trend was not notified and thus the Digital Seal the page bares should not be considered valid.

7. If all the previous steps are completed successfully, Trend returns to Alice a status page stating that the Digital Seal is valid. The status page contains the following information:

    - identification information of DSA,
    - identification information of Bob, as it is contained in Cert-W,
    - the digitally sealed page of Bob's Web server Alice has verified, URL-W,
    - the date and time of the accreditation of URL-W,
    - the validity period of the presented Digital Seal.

5.2. Implementation Issues

In step 1 of the Digital Seal verification phase, Alice has to send H-Cert-W and URL-W to Trend. This information is used in order to identify Bob to Trend, and inform Trend of the URL he has to visit later in the verification phase. One of the most practical ways to do that is to include both H-Cert-W and URL-W as parameters to the link referenced by the Digital Seal graphic. Thus, a link under a Digital Seal graphic could look like:

https://dsa.firm.org/verify?hCertW=B7CA3F5F75FBD3C57A36B21E1161AF4C
&UrlW=https://www.FirmAgent.com/pageX.html

The Digital Seal Policy, designed by the DSA should clearly state that Alice must verify the correctness of information contained in the aforementioned link in Bob's digitally sealed pages before clicking on it. It is Bob himself that includes this identification information, therefore he could provide false information.

There is at least one alternative for having Bob identify himself to Trend, relieving Alice from the responsibility of verifying the identification information before them being communicated to Trend. Trend could use the HTTP Referrer request-header field to retrieve this information, without any intervention either from Alice or Bob. In this case, Trend should also retrieve Cert-W in step 6 of the verification phase, compute H-Cert-W and compare it with the one stored in the Digital Seal record. However, the Referrer request-header field is not a trusted source of information. One of the vulnerabilities such a method presents is that the Referrer fields are sometimes blocked at the firewalls.

Other mechanisms can be found to implement step 1 of the Digital Seal verification phase as well. Another implementation mechanism could be investigated, providing a secure channel for communicating to Trend identification information concerning Bob without requiring any manual intervention from Alice or Bob. Such a mechanism could also be used in order to communicate to Trend the actual contents of URL-W, thus reducing the steps of the verification phase by two, since steps five and six would become redundant.

The Digital Seal verification mechanism could be more lax, and possibly efficient, if it did not check for any changes in WPC-W (based on comparing their hashes). In this case, the customers would have to trust that the —accredited— agents of the firm would not tamper with the digitally sealed WPC-Ws of theirs. However, we consider that protecting the integrity of WPC-Ws is essential because:

1. minor changes in the WPC-Ws could result in major fluctuations in the quality of services offered, and

2. changes in the WPC-Ws could be performed by malicious, authorised personnel of the firm's agent, witthout being traced.

Therefore, it could become more difficult for firms to monitor and audit their agents, thus guaranteeing for the services they provide and being able to accredit them. As a consequence, it could also become more difficult for customers to begin trusting agents of a firm they trust, simply because they trust the firm. However, integrity protection of WPC-Ws is also an efficiency issue. The agents of a firm will be restricted as to how often they can perform changes in their services, because they will have to re-apply for a Digital Seal every time they perform even the slightest change in their WPC-Ws. Protecting the integrity of WPC-Ws or not is, therefore, an issue to be decided by each firm. Whatever the decision of the firm is, it must be published in the policy document concerning Digital Seals, and that information be made readily available to customers.

The records of expired or revoked Digital Seals should be archived. These archives could prove to be useful in the future, supporting cases of DSA arbitration on matters of repudiation or other disputes.

The recommended expiration date of a Digital Seal is the date of expiration of the respective Cert-W. There is no point in the former being posterior to the latter, because a Digital Seal expires automatically at the time of expiration of Cert-W. Moreover, it is not efficient for the former to be prior to the latter, because thus it is inevitable that more than one Digital Seals would have to be obtained by an agent, in the lifetime of its Cert-W.

It is also recommended that the DSA specify a set of Certificate Authorities it approves, for agents to receive their certificates from. The sole criteria for including a CA in that set should be the kind of mechanisms used by that CA in order to distribute certificate status information. The DSA must be able to check the status of agent certificates promptly (step 3

of the Digital Seal verification phase), thus certain certificate status information mechanisms may suit a DSA more than others.

5.3. Addressing Threats

In this section we introduce another entity in our mechanism, Mallory. Mallory is a malicious entity trying to subvert the communication protocols or the services provided. The threats in the aforementioned communications and the respective mechanisms that face these threats are analyzed in this section. We follow the threat model presented in section 2.

1. *Monitoring of communication lines*. Protection of the confidentiality in the communications mentioned above is achieved through SSL.

2. *Shared key guessing*. Random symmetric keys are produced by SSL and distributed to the communicating parties, for each communication session. Their randomness, and the fact that they are not reused over different communication sessions, makes them hard to guess.

3. *Shared key stealing*. Random symmetric encryption SSL keys are distributed using an asymmetric distribution protocol, based on the use of the asymmetric keys of Alice, Bob and Trend which are contained in their respective certificates. These keys cannot be stolen in transit, however all three entities should protect their keys at a local level.

4. *Unauthorized modification of information in transit.* Protection of the integrity of communicated data is achieved through SSL.

5. *Forged Network addresses and Masquerading.* Mallory could not pretend to be Trend or Bob, since they both possess SSL certificates issued by a CA. To increase the possibility of Alice trusting the Certificate Authorities which issue certificates to Trend and Bob, Trend should have a certificate from a well-established CA which lies high in the global PKI hierarchy and Bob should have a certificate either from a CA which belongs to a trust chain where the aforementioned CA belongs also, or from a CA that is known to be widely trusted locally, at Bob's location. If Mallory possesses a valid certificate, but tries to masquerade its Web site into looking like Bob's Web site, the Digital Seal (or the lack of) provides Alice with a way to verify whether Mallory is indeed a local agent of the firm or not.
   Alice should verify the validity of the SSL certificates of Bob and Trend, before trusting information derived from them. However, since Trend has to verify anyway the validity of Bob's SSL certificate (step 3 of Digital Seal verification), technically there is no need for Alice to verify the SSL certificate of Bob herself. This delegation of certificate status verification makes the process more transparent for Alice. However, we should mention that Alice might want to verify the validity of Bob's SSL certificate herself because she, besides Trend, is also taking a risk by trusting Bob's SSL certificate [Rive98].

6. *Password stealing.* Our Digital Seals mechanism does not require the use of passwords. However, if the services provided by Bob require the use of passwords, then these will be encrypted by SSL. Even if Mallory captures the encrypted passwords, she will not be able to replay them, because SSL protects against replay attacks [OFrei96].

7. *Unauthorized Access.* Although our mechanism does not feature any access control functions, it provides a countermeasure against the impact of a potential unauthorized access to Bob's resources. If the pages hosted by the Web server of Bob are modified,

the respective Digital Seals will be rendered invalid, thus Alice will know that the respective services are not the ones Bob intended to offer, and Trend had accredited.

8. *Repudiation of Origin.* Trend and Bob cannot repudiate their actions because Mallory can neither replay SSL sessions, nor initiate an SSL session with Alice, pretending to be Trend or Bob. If Bob wishes to ensure that Alice will not be repudiating her actions as well, he could require from Alice to authenticate herself using a certificate obtained from a CA that belongs to one of the certification chains that Bob trusts.

9. *Private key stealing or compromise.* Private keys should be protected with adequate mechanisms, in general. The most valuable private key in the Digital Seals mechanism and the operation of the infrastructure we present is probably the private key used to sign the Digital Seals themselves. This key is only used offline by DSA and should be protected against disclosure or modification by adequate, technical protection mechanisms. However, since the data signed with this key (the actual Digital Seal) is not used directly by anyone except Trend, a potential compromise of this private key can be recovered relatively easily if the DAA is not compromised at the same time as well.

6.Conclusions

Electronic trust concerns both the security of electronic transactions and the quality of services or products offered through them. PKI is being used to enable trust on the security of e-commerce transactions. We introduced the notion of Digital Seals, and a respective mechanism that enables trust on the quality of services or products offered by e-commerce infrastructures.

Our mechanism does not add to the complexity of trust relationships in PKI. On the contrary, certain features of our mechanism facilitate the use of PKI technologies; Alice can transparently delegate the verification of Bob's SSL certificate to Trend.

We analyzed an example of an e-commerce infrastructure, involving a firm comprising several agents around the globe. We have demonstrated that our Digital Seals mechanism, along with typical PKI services, can be used to enable trust on behalf of the e-commerce customers enhancing both the security of electronic markets, and the quality of the services or products offered through them.

7.References

[FGGGIK00] Forret P., Gatziani M., Gritzalis S., Grufferty S., Iliadis J., Kyrloglou N., Landrock P., Moulinos K., Polemi D., Spinellis D., Varvitsiotis A., *The C.O.S.A.C.C. Solution for the Secure Interconnection of Chambers of Commerce*, European Commission, EUROMED-ETS Project, March 2000.

[Rive98] Rivest L., “Can we eliminate certificate revocation lists?”, *Proceedings of the Second International Conference on Financial Cryptography*, Anguilla, British West Indies, February 1998, Springer Verlag

[IMRG98] IMRG Limited, "Electronic Commerce in Europe, An action plan for the marketplace", White Paper, July 1998

[AGGPS98] Amditis A., Gritzalis D., Gritzalis S., Polemi D., Spinellis D., Varvitsiotis A., Velentzas S., *Review of existing results of TTPs for Healthcare Systems*, European Commission, EUROMED-ETS Project, February 1998.

[Caste93] Castell S., *Code of Practice and Management Guidelines for Trusted Third Party Services*, European Commission, INFOSEC S-2101 project, report no. 2, 1993.

[CEC94] Commission of the European Community, DGXIII/B, Green Paper on the Security of Information Systems, ver.4.2.1, 1994

[CGGG98] Crijns M., Gatziani M., Gritzalis S., Grufferty S., Iliadis J., Kyrloglou N., Landrock P., Moulinos K., Mueller O., Passa P., Polemi D., Spinellis D., Varvitsiotis A., *Issues facing the secure link of Chambers of Commerce*, European Commission, COSACC (AD4001) project, Del. 3, December 1998.

[Cliff98] Clifford M., Lavine C., Bishop M., "The Solar Trust Model: Authentication without Limitation" , Proc. Of the 14th Annual Computer Security Applications Conference, IEEE Computer Society Press, pp 300-307, 1998.

[DeViv98] De Vivo M., De Vivo G., Isern G., *"Internet Security Attacks at the Basic Levels*" , Operating Systems Review, ACM Press, Vol. 32 No 2, April 1998.

[Garfi96] Garfinkel S., Spafford G., *Practical Unix and Internet Security*, O' Reilly & Associates, 1996.

[Garfi97] Garfinkel S., Spafford G., *Web Security and Commerce*, O' Reilly & Associates, 1997.

[GFMER98] German Federal Ministry of Education and Reasearch, *Digital Signature Ordinance*, 1998 (http://www.iid.de/contents.html).

[GS97] Gritzalis S., Spinellis D., "Addressing Threats and Security Issues in World Wide Web Technology", in *Proceedings of the CMS '97 3rd IFIP TC6/TC11 International joint working Conference on Communications and Multimedia Security*, pp.33-46, September 1997, Chapman & Hall

[Gritz98] Gritzalis S., Moulinos K., Lekkas D., Polidorou E., *European Cross Domain PKI Architecture: Functional Specifications*, European Commission, KEYSTONE (23187) project, November 1998.

[OFrei96] Freier A., Karlton P., Kocher P., *The SSL Protocol Version 3.0*, Netscape Communications, November 1996 (http://home.netscape.com/eng/ssl3/ draft302.txt).

[Rensb97] Rensburg A., Solms B., "A comparison of schemes for CAs" ,*in Proc. of the IFIP International Information Security Conference*, Chapman & Hall, pp. 222-240, 1997.

[SKG99] Diomidis Spinellis, Spyros Kokolakis, and Stephanos Gritzalis. Security requirements, risks, and recommendations for small enterprise and home-office environments. *Information Management and Computer Security*, 7(3):121-128, 1999