Building Trust in the Global Electronic Marketplace: Auditing Trusted Third Parties

Roger Auinger, Pierre Brun, Henrik Czurda
Revisuisse Price Waterhouse
Stampfenbachstr. 109, P.O. Box 8035 Zürich, Switzerland

(V1.0: 12.5.1997)

Quality and Trust are the very foundations of the "Trusted Third Party"-infrastructures which are now emerging. In order to succeed, the proper rules of operation need to be built into the electronic trust-network right from the start. A clear set of operation rules need to be proposed and negotiated on an international level. The objective is to have the rules become a world wide trust standard for Electronic Commerce to enable a trustworthy relationship between Trusted Third Parties.

1. Introduction

Electronic Commerce (EC) [KW96, PWTC97] will allow internet users around the world to exchange their business transactions over the net in close to real time, including electronic payments, EDI [COLB95], and electronically signed contracts that will travel to their destinations almost without delay. However, while several forms of trade over the Internet are already widely practiced, Internet business still lacks several prerequisites before its full business potential will be unleashed. One of the most pressing issues that needs to be resolved is how to effectively and efficiently build trust between any two parties that are willing to conduct electronic business transactions.

A secure electronic channel can be established between two parties, even over such inherently insecure channels as the Internet, through the use of public key cryptography (PKC) [SCHN95]. This common type of Internet security encrypts and decrypts using two keys that work together: a private key and a public key. The private key is kept strictly confidential by each user. Anybody can gain access to the public key, which has to be certified by a Trusted Third Party (TTP). Implemented in either hardware or software, it offers the benefits of confidential transmissions and digital signatures [PW93, VEU95] in an open network environment in which parties do not know one another in advance, and without the need to share secret key information. However, the use of PKC engenders itself to

a whole new range of problems. The most obvious of them are key management and key certification. TTPs are being proposed to solve such problems[1].

"A TTP can be described as an entity trusted by other entities with respect to security related services and activities. A TTP would be used to offer value added services to users wishing to enhance the trust and business confidence in the services they receive, and to facilitate secure communications between business trading partners. TTPs need to offer value with regard to integrity or confidentiality and assurance of the services and information involved in the communications between business applications. The use of a TTP is dependent on the fundamental requirement that it is trusted by the entities it serves to perform certain functions" [DTI97].

TTPs will be operating within the legal and regulatory framework of existing governments and states. In order to facilitate global electronic trust, locally licensed TTPs will establish trust arrangements on an international level with other TTPs. This will allow a user to communicate securely with every user of another TTP which his TTP has an agreement.

2. The risk of losing trust due to improper operation

The international and networked character of the emerging TTP-infrastructure will require every local TTP to adhere to the same quality standards of operation. Compliance with local legislation, proper licensing, highest levels of availability, integrity and confidentiality are among the key requirements that the market will inevitably demand of trusted entities. Conversely, faulty or improper operation of even a single TTP in the trust-network will likely have a negative impact on the electronic trust infrastructure as a whole.

2.1 The role of a traditional audit company to build up trust for Trusted Third Parties

The Internet places certain trust demands on institutions operating on a global level. International TTPs can fulfill this requirement. National legal frameworks have only to declare digital signatures, digital time stamps [SCHN95], etc. as legally binding. Many countries have already identified the challenge and reacted with parliamentary propositions. Consequently, TTPs will be required to have a known reputation.

[1] As of today, some isolated instances of TTPs are already operational. VeriSign is a well known example. VeriSign issues Digital IDs to individuals for use with WWW client software, secure e-mail packages, and other end-user software.

One of the best ways to build up reputation for a company, is to let certify the proper running of the business by a third party. However, this organisation should not have own business interests and therefore it must be an independent institution.

Such independent corporations are the auditing firms. While TTPs are a new need to establish global electronic trust, auditing -in our case external auditing- is the traditional independent appraisal function to an organisation.

The internet users could require an auditing of a TTP exactly as the shareholders of most enterprises require an annual audit of the financial statements to be conducted by an independent certified public accountant [WELP96].

To make the auditing of TTPs a reality, an auditing firm such as Price Waterhouse (PW) should take the lead rather than by a government agency. One of the advantages would be that PW is a global firm with an established presence in every major market and the ability to deploy a consistent approach worldwide. PW could also set up this structure very quickly as our infrastructure is already in place. An equally important reason why this kind of auditing should not be performed by government, is that government would not be willing to accept liability for a TTP.

2.2 Assurance of proper operation

A number of audit and security frameworks exist for controlling the proper operation of complex infrastructures[2]. In general, all TTPs would need to implement an internal control system, which would have to be audited in regular intervals by external, independent auditors.

As of today, no such control system is in place. However, whatever its future shape, it will have to address the following minimal criteria (as defined by CobiT):

Confidentiality The protection of sensitive information from unauthorized disclosure.

Integrity The accuracy and completeness of information, as well as its validity in accordance with business values and expectations.

Availability Information being available when required by the business now and in the future. The safeguarding of necessary resources and associated capabilities.

Effectiveness Information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.

[2] e.g. CobiT (Control Objectives for Information and related technology) [ISAC96] ; Code of Practice for Information Security Management (BS 7799) [BRIT95].; and publications of the European Security Forum, to name just a few.

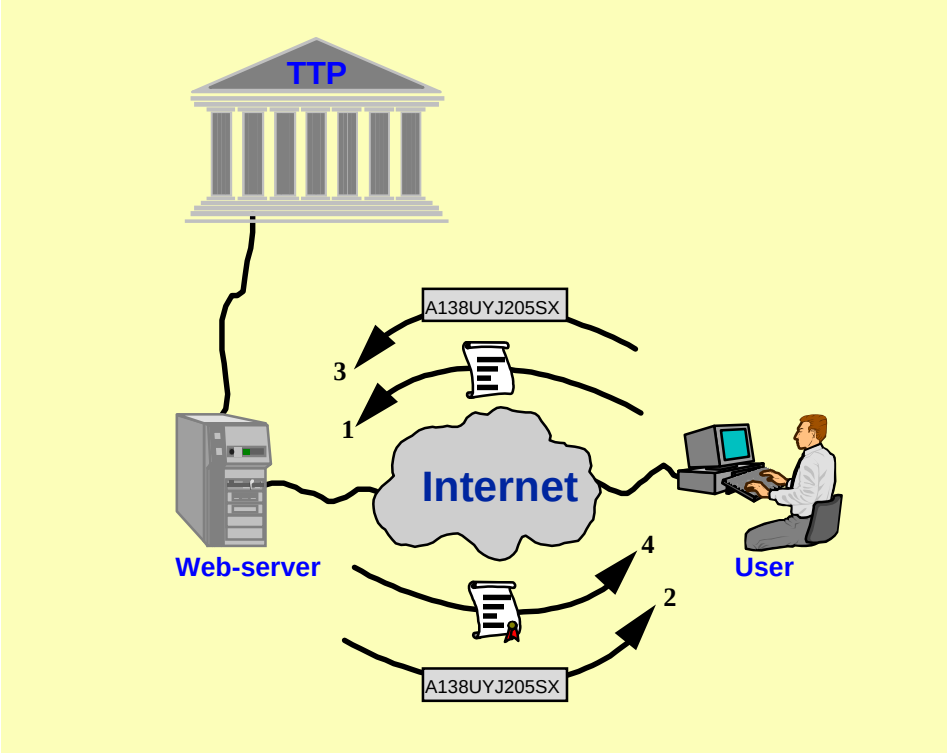
Efficiency	The provision of information through the optimal use of resources.
Compliance	Compliance with laws, regulations and contractual arrangements to which the business process is subject, i.e. externally imposed business criteria.
Reliability	The provision of appropriate information to operate the entity and for management to exercise its financial and compliance reporting responsibilities.

3. Audit Requirements based on a practical example

The strongest type of Internet security encrypts and decrypts using two keys that work together: a private key, known only to its owner, and a public key. The private key is kept strictly confidential by each user. Anybody can gain access to the public key, which has to be certified by a TTP. Security require a TTP which would act as a clearinghouse which guarantees the authentity and confidentiality of digital information flowing between communication partners.

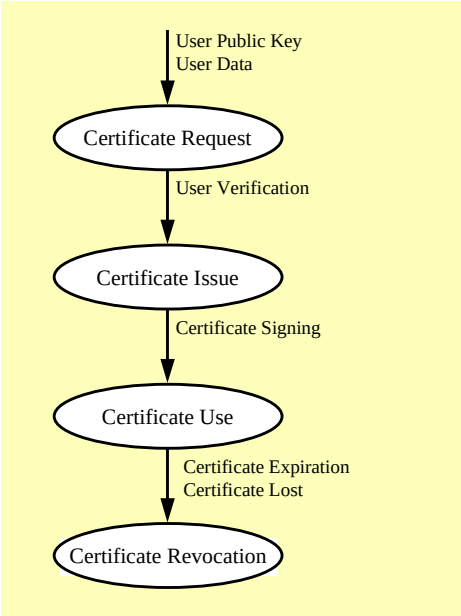
3.1 Technical description of the certification process (example)

Let's look at a typical process around certification: The TTP presents its services on a Web-interface. The communication between the TTP and the user who requests some services from the TTP, will be through Common Gateway Interface (CGI) scripts. CGI allows users on the WWW to access programs of all types on remote systems as if they were actually using the remote computer themselves. In this case the CGI is needed for transmitting the userdata to the TTP. The userdata will be stored in a database. The following process shows which security- and encryption-mechanisms are used throughout the system. A user possesses his own certificate getting with his browser to the Web-site of the TTP. For this the user has to verify that the Web-server is certified by a credible TTP. That could be a root TTP or the TTP about which will be mentioned. After this verification the user will get a secure connection to the Web-server. Afterwards the public key of the TTP should be downloaded. Now, the user is ready to request his own certified public key and to accept some regulations. A private and a public key are generated. The public key is sent through a CGI to the TTP (nr. **1** in the following picture). The TTP is then going to authenticate and verify the user. If the verification was successful, the TTP will sign the public key of the user. After this the user will receive a Personal Identification Number PIN (nr. **2** in the following picture). How this PIN is got will be mentioned later. With the PIN (nr. **3** in the following picture) the user is now able to download his signed public key (nr. **4** in the following picture). Through the Web-interface the user could have a view of any piece of information which the TTP presents on the net.



3.2 Structured Proceedings

From the perspective of auditing TTPs, we believe the following actions require protects on:



Listed at the right border are the CobiT-criterias for an audit.

3.3 Certificate-issue

It has to be tested whether a TTP can issue a certificate. This certificate should be a well known and commonly used by most of the clients. The type of this certificate must be used by other TTPs and should, if it is possible be defined in a standard by an international organization. ***compliance***

3.3.1 Certificate-issue for a Client

The certificate which has to be requested by a client must be installed automatically into the clients browser. For the certificate request, special regulations must be implemented. Special cases could occur, if a client requests a certificate and during this process the connection breaks. The client must have the possibility to request a certificate once again. After a successful certificate issue, the TTP has to update the list on which every client with his particulars is listed. ***effectiveness***

3.3.2 Certificate-issue for a Server

The administrator of a server should be able to send his Certificate Signing Request (CSR) [KW96] by email to the TTP. If this mechanism is not implemented he has to copy the servers CSR and paste it in a corresponding field in the Web-interface. Both of these actions must start an automated signing of the certificate. ***availability***

3.4 Revocation

The TTP has to protect itself with special regulations against embarrassing situations. There are two different methods to implement an efficient revocation. One possibility is the user will receive a revocation key during the certificate process. This key he should keep on a disk in a secure place. The other possibility is the user could perform a revocation with his PIN. ***effectiveness***

3.4.1 Revocation List

Each user who has revoked his certificate and consequently his key pair has to be put on a list. According to this Certificate Revocation List (CRL) [NETS97] every other user could check whether the certificate of the future communication partner is still valid. This CRL has to be attainable through the revocation URL by every user. A special point is that the CRL always has to be up to date. To prevent any kind of embarrassment the system time of the TTP has to be the reference time for any process. To support this point a time stamp mechanism would be necessary. This means, if a user is looking up the CRL he will get a time stamp. With this stamp, the user could prove that on the time a transaction is performed, the certificate of the communication partner was valid. ***availability*** ***effectiveness***

3.5 User Verification

User verification requires different security levels. According to the level on which the user was certified, the level should be listed in the certificate. There has to be a distinction as for example the following.

compliance

3.5.1 User Verification through the same channel

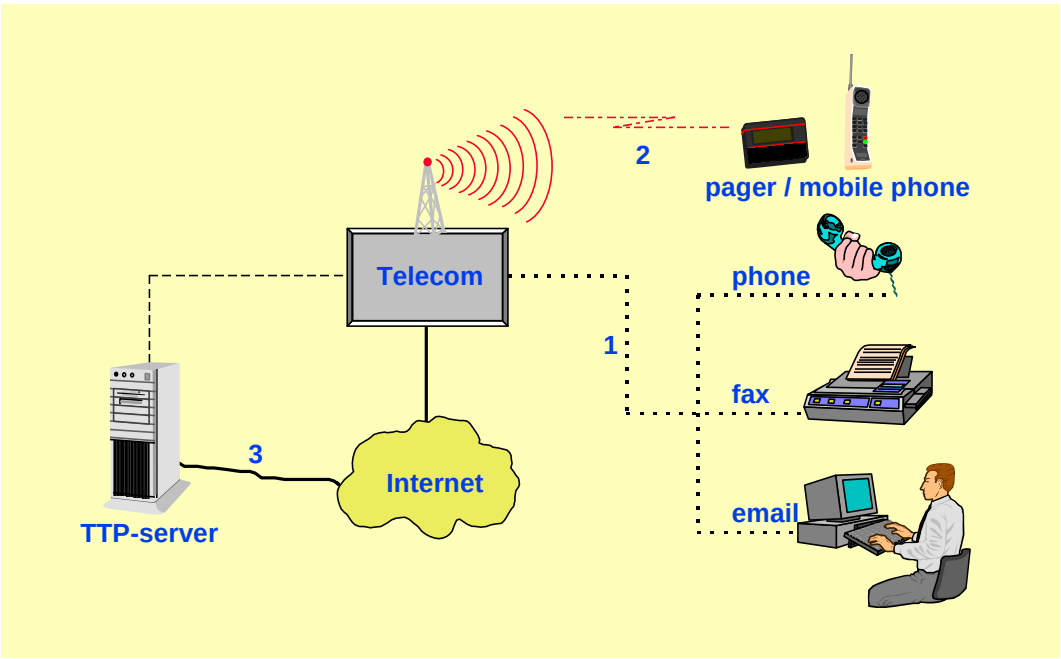
If the PIN goes to the user through the same channel over which the user initiated his request, the verification take place on the lowest level. An example for this kind of verification is email. To catch a PIN which goes to the user by a fax message or by a phone call the need for better equipment is obvious. For better verification, a check should be made, whether the name of the user and the given phone number are matched. In this case, it is important that such a check is performed through a secure medium and not through a telnet-connection over the Internet to a special host. The weakpoint of all these methods is the phone line from the home of the user to the phone company (nr. **1** in the following picture).

confidentiality integrity

3.5.2 User Verification through an other channel

If the PIN is sent by a pager message or by phone call from a mobile phone, it would be troublesome to catch the PIN. Because the attacker has to survey two channels (nr. **1** and **2** in the following picture).

confidentiality integrity



3.6 Segregation of systems

3.6.1 General

There has to be a clear separation between the Database and the Web-interface necessitating a secure connection between these two parties (nr. **3** in the picture above).

3.6.2 Database

The Database has to stand alone, so that it is not possible to get any kind of external access to the Database-server. ***confidentiality***

3.6.3 Web-interface

The Web-interface has to be clear and self explanatory for clients. Before a client will get his certificate into his browser, he has to accept some regulations. These regulations protect the TTP. ***efficiency availability***

4. Conclusion

Our understanding is that the legal foundation for these TTPs or CAs are largely unspecified provoking the following questions:

- Which critical processes have to be audited?
- Is it possible or necessary to establish a real time auditing?
- Can auditors act as global trust builders?
- Could be established world wide accepted regulations?
- Is it possible to verify a certificate within a reasonable time?
- Is the processing power enough to do all the necessary calculations?

Therefore, questions such as “How can a user tell if a digital certificate is valid”? and “how can the user be sure that the certificate issuer is reliable”? or “what happens when one part of a chain of certificates is compromised or fraudulent” remain open.

References

[BRIT95] British Standards Institution (1995): Code of Practice for Information Security Management; BS 7799: 1995. British Standards Institution; BSI, 389 Chiswick High Road, London, W4 4AL, England.

[COLB95] Colberg, Th. P. (1995): *The Price Waterhouse EDI handbook*. New York: John Wiley & Sons Inc.

[DH96] Deep J. and P. Holfelder (1996): *Developing CGI Applications with Perl.* New York: John Wiley & Sons Inc.

[DTI97] British Ministry for Science and Technology (1997): *Licensing Of Trusted Third Parties, For The Provision Of Encryption Services,* Public Consultation Paper on Detailed Proposals for Legislation, `http://dtiinfo1.dti.gov.uk/pubs/`

[ISAC96] ISACA (1996): *Control Objectives (COBIT).* Information Systems Audit and Control Association (ISACA).

[KW96] Kalakota, R. and A. B. Whinston. (1996): *Frontiers of Electronic Commerce*. Menlo Park, California. Addison-Wesley Publishing Co.

[NETS97] http://home.netscape.com/eng/security/certs.html

[OECD97a] OECD (1997): *OECD Cryptography Policy Recommendation of the Council.* http://www.oecd.org/dsti/iccp/crypto_e.html

[OECD97b] OECD (1997): *OECD Cryptography Policy Recommendation of the Council.* http://www.oecd.org/news_and_events/release/nw97-24a.htm

[PW93] Pohl H. and G. Weck. (1993): *Internationale Sicherheitskriterien*. Oldenbourg-Verlag.

[PWTC97] Price Waterhouse Technology Centre. (1997): *Technoloy Forecast 1997*, PWTC-01-07, Menlo Park, California 94025 U.S.A.

[SCHN95] Schneier, B. (1995): *Applied cryptography: protocols, algorithms, and source code in C*, 2nd Edition. New York: John Wiley & Sons Inc.

[VEU95] VEU (1995): Verordnung über die elektronischen Unterschrift - VEU; Verordnung über die Annerkennung von Verfahren zur elektronischen Unterschrift nach Art. 126 a Abs. 2 BGB. - Vorentwurf des Bundesministeriums, Stand 30.08.1995. http://greenie.muc.de/freenet/pinnwand/euv300895.html

[WELP96] Warren, J. D., Lynn W. E. and X. Ley Parker (1996): *Handbook of IT Auditing*. Coopers & Lybrand L.L.P., Warren, Gorham & Lamont.