ISSN 1479-4195 online / ISSN 1479-4209 CDRom

# Trusted? Third? Parties

Gavin Jones

*To ensure certainty in e-Commerce, a Trusted Third Party can be used to issue certificates, which act as an electronic equivalent to a witness acknowledging and authenticating the identity of the contracting party. The trusted third party issues the certificate which correlates the contracting party to a unique public key, which in turn is used in creating the digital signature. However, the European legislation, in particular, Directive 1999/93/EC on a Community framework for electronic signatures fails to ensure that the certificate is issued by a third party. Therefore a party can act as both a contracting party and a certificate issuer. This causes a conflict of interest, should a dispute arise, as authentication has not been performed by a party independent to those contracting.*

To ensure certainty in commerce, a third party is often used as a witness to acknowledge and authenticate the transaction; for example, a Notary witnessing the signing of a document. In secure electronic commerce, the logically equivalent form of witnessing involves a trusted third party (TTP)[1] validating the transaction, often by the provision of a certificate for authenticating the contracting agent.[2] This certificate is issued by a certification service provider. However, Directive 1999/93/EC[3] fails to ensure that the certificate is issued by a third party. Therefore a contracting party can meet the requirements for a certification service provider and 'authenticate' the other contracting party. This, in itself, is fine unless the transaction is disputed. In the event that the transaction is disputed and the contracting party also authenticated the disputing party, there is no independent party to review the use of the certificate.

A certificate associates the certificate subject's public key with subject identifying information. It also contains the time validity of the certificate, and any specific aspects of the transaction that the certificate authorises.[4] Assuming that the certificate subject keeps their 'private key' private and that the subject identifying information held within the certificate uniquely identifies them, then the certificate can be used to authenticate the party; however, the certificate, itself, must also be able to be authenticated. This involves both verifying the certificate issuer's identity (this is contained in the issued certificate), and that the certificate has not been tampered with since it was issued. This verification is made possible by the certificate issuer signing the certificate.[5]

[1] An e-Commerce TTP definition is: 'an entity trusted by other entities with respect to security related services and activities'. See LICENSING OF TRUSTED THIRD PARTIES FOR THE PROVISION OF ENCRYPTION SERVICES Public Consultation Paper on Detailed Proposals for Legislation March 1997, DTI.

[2] The use of a certificate assures the recipient / contracting party that the public key associated with the digital signature really does belong to the signer (certificate subject). i.e. The certificate associates the public key with a particular certificate subject which may be a person / organisation or a particular hardware device.

[3] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[4] Such as limitations on the scope of use of value of transactions. See Directive 1999/93/EC Annex I (i) and (j).

[5] The X.509 Certificate format (the commonly used certificate standard) contains a field for the Signature Algorithm Identifier which is used for determining how to decrypt the Certification Issuer's Digital Signature, which once decrypted, authenticates that the certificate was issued by the Certification Issuer and that the certificate has not been tampered with.

Two important distinguishing methods of signature verification involving trusted third parties for non-repudiation of origin in an electronic transaction are:

a. Originator signed
b. Trusted third party signed

Originator signed involves the originator signing the transaction with the private key associated with their public key and the recipient verifying the public key associated with the certificate (which the originator may send in the transaction, or the recipient may verify from a publicly available certificate store). Upon receipt, the recipient must verify that the certificate has not been revoked.[6] This can be done by checking against the Certificate Revocation List (CRL) which is published at regular intervals (normally at least daily) by the Certification Service Provider.[7]

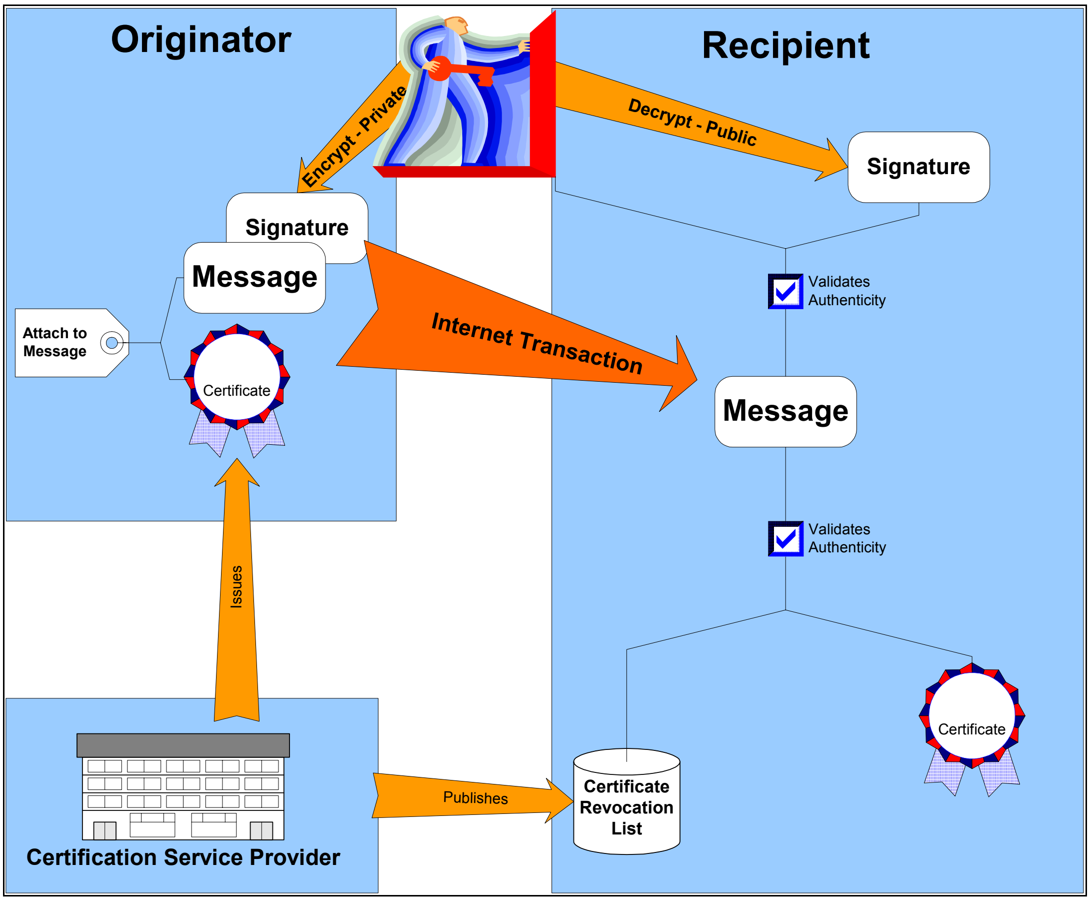

*Figure 1 – Originator Signed Transaction*

Trusted third party signed involves the originator forwarding the transaction to the trusted third party who signs the transaction upon authenticating the originator. This signed transaction is then forwarded by the originator to the recipient. The recipient uses the public key of the trusted third party to verify the authenticity and data integrity of the transaction.

[6] The precise determination of revocation time is important in ensuring validity of the transaction (and any subsequent liability associated with the failure to reject a transaction signed using a public key of a revoked certificate). This is included in Directive 1999/93/EC in Annex II (c).

[7] See Directive 1999/93/EC Annex IV (d) for correlating validity in signature verification.

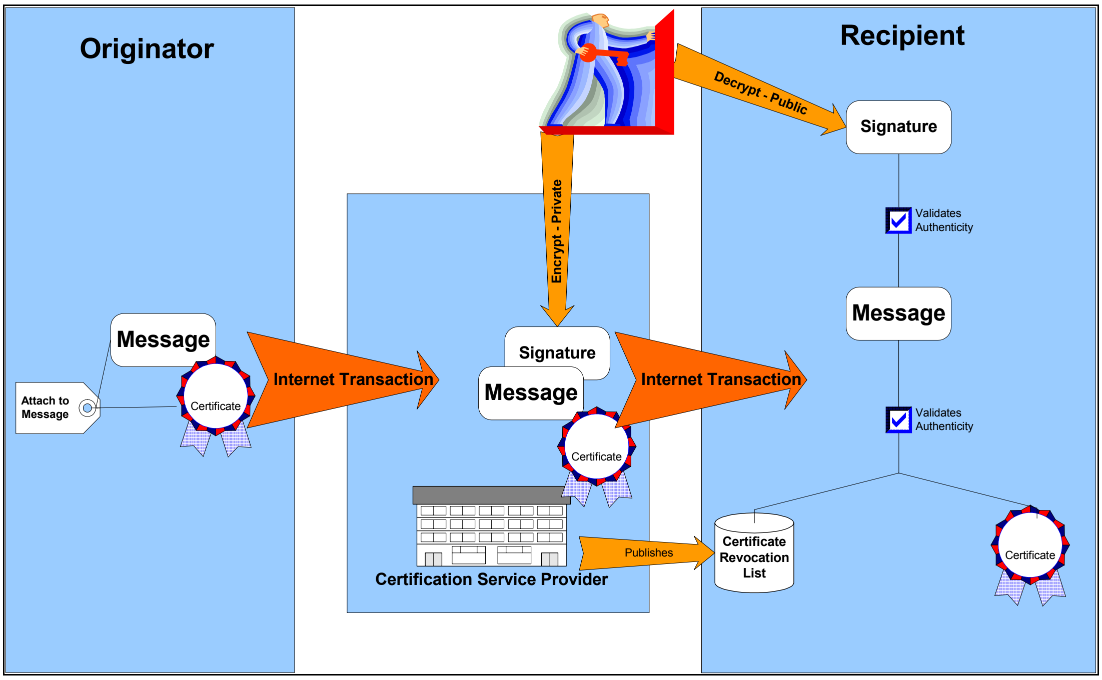

*Figure 2 – Trusted Third Party Signed*

The third party is responsible for ensuring the data integrity and the authenticity of the transaction and transaction source. This may be done via encryption / signing or by secure communication links.

When certificates are issued, they require authentication of the individual. This normally involves one of the following:

1. Verification of some privately known information, such as, a telephone banking PIN when applying for Internet access to a bank account
2. Visual / biometric identification of the person / personal attribute, such as, verification of a handwritten signature
3. Verification of the person against identity documents, such as, passport or photo driver's license.

Given the trusted third party vouches for the identity of a contracting party, there should be no conflict of interest in certificate issuance. The TTP should be independent of the contracting parties to ensure that there can be no conflict of interest in the event of a dispute between the contracting parties. Ideally they should exist solely as certificate issuing bodies, not only to ensure independence, but also to ensure that best practice security models are observed and that there is no security compromise for commercial reasons. Certainly the liability requirements within Article 6 of the Directive will ensure an obligation on independent certificate issuing bodies to implement robust security models.[8]

In the event that the 'trusted third party' is an agent of the recipient contracting party, the independence of the security model can be compromised, as certificate issuance is likely to be to the economic advantage of the issuer in stimulating their primary business. In the event of a transaction being disputed, the certificate subject is at a disadvantage as the certificate issuer is not independent to the disputing parties. This would not be a concern if the Directive was more prescriptive / specific with respect to the requirements for identifying the certificate subject.

[8] 1999/93/EC Article 6.

Interestingly, the Luxembourg implementation of the Directive is prescriptive and requires that the certification service provider verifies the identity of the certificate subject by means of their identity documents.[9] This provides a greater assurance than that of the UK implementation which clones Annex 2 of the Directive, requiring UK Certification Service Providers to:

> "verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificated is issued".[10]

For consumers to have confidence in the certificates issued by Certification Service Providers, the regulations need to go further towards ensuring that certificate issuance is a secure, trustworthy process. Voluntary accreditation, as proposed in Preamble 11 and Article 3(2) is insufficient. Contracting parties need to feel assured that the certificates issued are trustworthy and that identity information has been properly handled. Annex II of the Directive may provide lip service to this, but without an enforcement process such as accreditation or audit, the ability to dispute a defence of "not act[ing] negligently"[11] will be restricted. Financial Institutions have set up their own not-for-profit body, Identrus,[12] to handle authentication in business-to-business transactions. Participating financial institutions then act as Certification Authorities (Certificate Issuers) to businesses performing commerce over the Internet.

Outside of the EU, there have been some more restrictive implementations of electronic signature regulations, such as the Missouri State's 1998 Digital Signatures Act.[13] This Act grants legal recognition to documents signed using digital signatures that have been created using a certificate provided by a licensed private sector company. Unfortunately, Missouri does not appear to have licensed any company's to provide certificates, which suggests that digital signatures remain legally invalid in the state.[14] Although it seems prudent to regulate certificate issuers, restricting the recognition of digital signatures to only those associated with a certificate issued by a regulated issuer will have problems if issuers do not sign up to be licensed.

In an ideal implementation, Certification Service Providers would be independent bodies with no incentives to be biased in dispute resolution. The voluntary accreditation schemes referred to in Preamble (11) and Article 3(2) of the Directive, should be compulsory, or, at minimum an audit body should be set up to review the adherence of Certification Service Providers to Annex II of the Directive[15] as a next best alternative. This would go some way to assuring "trust" in Trusted Third Parties.

[9] Grand-Ducal Regulation of 1 June 2001 relating to electronic signatures, electronic payment and to the creation of the 'electronic commerce' committee Art 3(1) (4).

[10] The Electronic Signatures Regulations 2002, SI 2002 No. 318 Sch. 2.

[11] Directive 1999/93/EC Art 6(1)(c).

[12] See: www.identrus.com

[13] See: http://www.senate.state.mo.us/98info/pdf-bill/intro/SB708.pdf

[14] See: http://www.mobar.org/journal/2003/janfeb/niemoeller.htm

[15] Directive 1999/93/EC.

## References

M. S. Baum and W. Ford, *Secure Electronic Commerce*, 2nd ed, (Prentice Hall PTR, New Jersey, 2001).

UNCITRAL Model Law on Electronic Signatures (2001) Art 8(2).

M. A. Broderick, V. R. Gibson and P. Tarasewich, *Electronic Signatures: They're Legal, Now What*, (online), http://www.ccs.neu.edu/home/tarase/BrodGibTaraseESig.pdf
[Accessed on 07th September 2003].

DTI, *Licencing of Trusted Third Parties for the Provision of Encryption Services*, (online), http://www.cl.cam.ac.uk/users/rja14/dti.html#sec5
[Accessed on 06th September 2003].

A Gutzman, *Legalizing Ink: The New Electronic Signature Law,* http://ecommerce.internet.com/news/insights/ectech/article/0,,9561_413551,00.html
[Accessed on 30th March 2003].

Identrus, *website*, (online), www.identrus.com [Accessed on 21st March 2004].

Missouri Senate Bill No. 708, *Missouri Digital Signatures Act*, (online), http://www.senate.state.mo.us/98info/pdf-bill/intro/SB708.pdf [Accessed on 21st May 2004]

J. A. Niemoeller, *Electronic Transactions in Missouri*, (online), http://www.mobar.org/journal/2003/janfeb/niemoeller.htm
Accessed on 07th September 2003.

C. Spyrelli, *Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication,* Journal of Law Information and Technology (2002 Issue 2), http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html [Accessed on 21st March 2004]