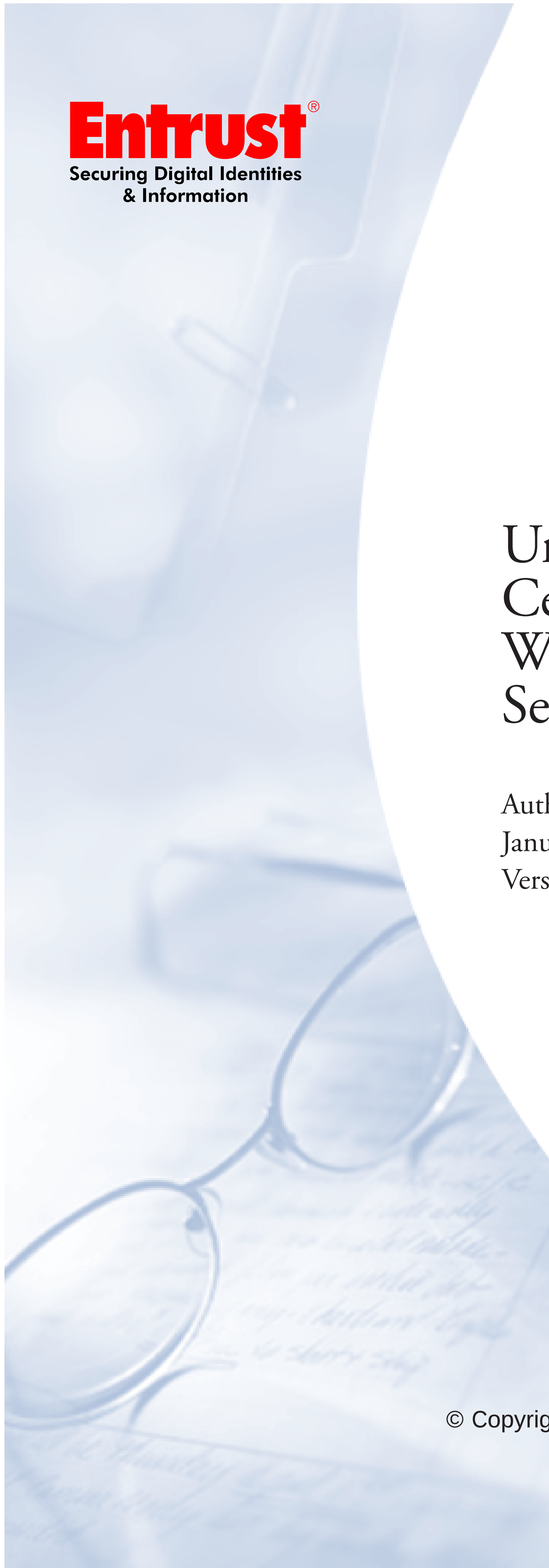


Entrust®

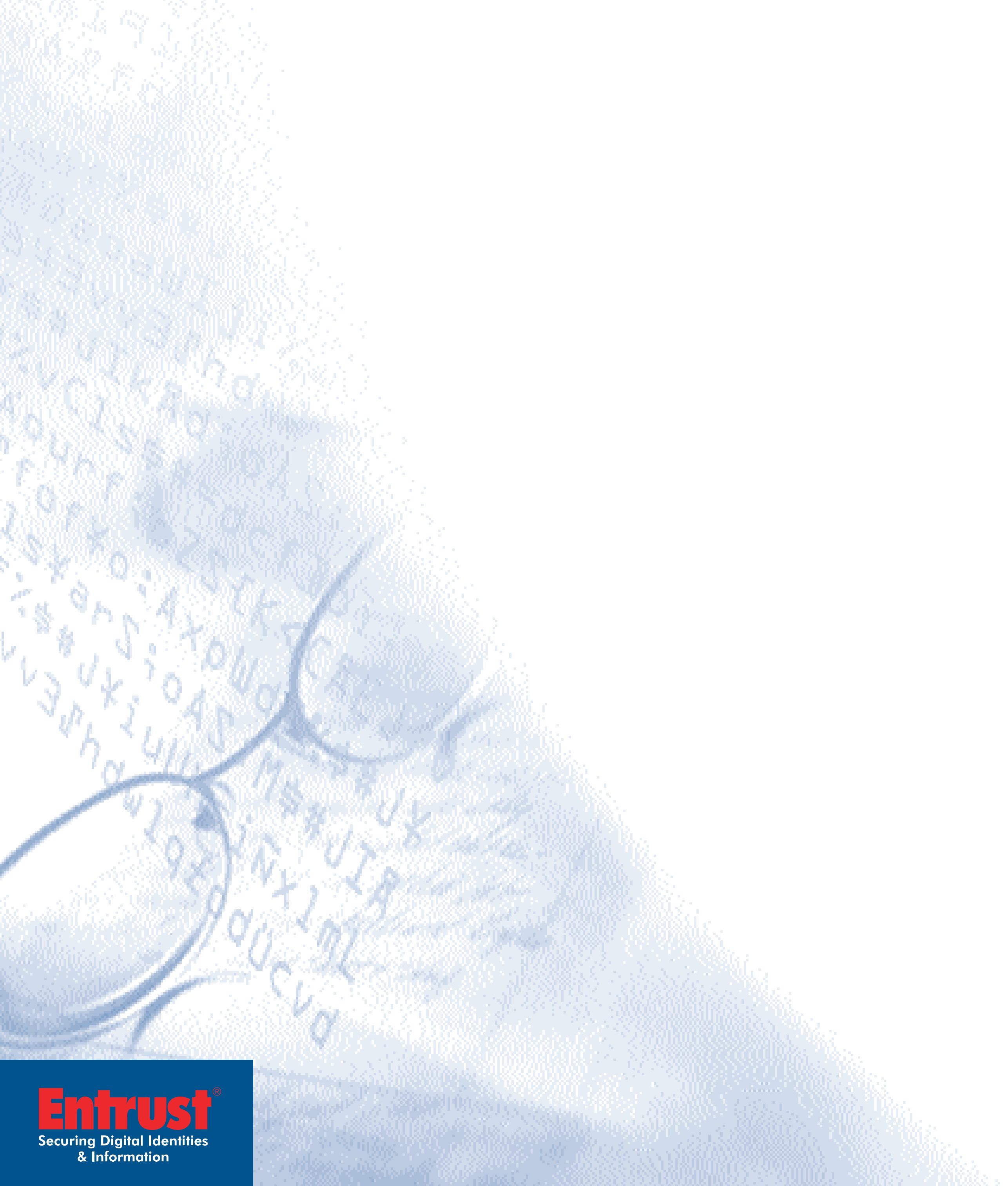
Securing Digital Identities
& Information

Understanding Digital Certificates and Wireless Transport Layer Security (WTLS)

Author: Allan Macphee

January 2001

Version 1.1



Entrust®
Securing Digital Identities
& Information

Digital Certificates

What are they?

Digital certificates are electronic files that are used to uniquely identify people and resources over networks such as the Internet. Digital certificates also enable secure, confidential communication between two parties.

When you travel to another country, your passport provides a universal way to establish your identity and gain entry. Digital certificates provide similar identification in the electronic world. Certificates are issued by a trusted third party called a Certification Authority (CA). Much like the role of the passport office, the role of the CA is to validate the certificate holders' identity and to "sign" the certificate so that it cannot be forged or tampered with. Once a CA has signed a certificate, the holder can present their certificate to people, Web sites, and network resources to prove their identity and establish encrypted, confidential communications.

For more information on trust, refer to the White Paper *The Concept of Trust in Network Security*, available at: http://www.entrust.com/resourcecenter/whitepapers.htm

A certificate typically includes a variety of information pertaining to its owner and to the CA that issued it, such as:

- The name of the holder and other identification information required to uniquely identify the holder, such as the URL of the Web server using the certificate, or an individual's e-mail address;
- The holder's public key (more on this below). The public key can be used to encrypt sensitive information for the certificate holder;
- The name of the Certification Authority that issued the certificate;
- A serial number;
- The validity period (or lifetime) of the certificate (a start and an end date).

In creating the certificate, this information is digitally signed by the issuing CA. The CA's signature on the certificate is like a tamper-detection seal on a bottle of pills – any tampering with the contents is easily detected.

Digital certificates are based on public-key cryptography, which uses a pair of keys for encryption and decryption. With public-key cryptography, keys work in pairs of matched "public" and "private" keys. In cryptographic systems, the term key refers to a numerical value used by an algorithm to alter information, making that information secure and visible only to individuals who have the corresponding key to recover the information.

For more information on public-key cryptography, refer to the White Paper *An Introduction to Cryptography,* available at: http://www.entrust.com/resourcecenter/whitepapers.htm

The public key can be freely distributed without compromising the private key, which must be kept secret by its owner. Since these keys only work as a pair, an operation (for example encryption) done with the public key can only be undone (decrypted) with the corresponding private key, and vice-versa.

A digital certificate securely binds your identity, as verified by a trusted third party (a CA), with your public key.

WAP Server WTLS certificates

A WAP server WTLS certificate is a certificate that authenticates the identity of a WAP site to visiting micro-browsers found in many mobile phones on the market. When a micro-browser user wants to send confidential information to a WAP server, the micro-browser will access the server's digital certificate. The certificate, which contains the WAP server's public key, will be used by the micro-browser to:

- Authenticate the identity of the WAP server and
- Encrypt information for the server using the Wireless Transport Layer Security (WTLS) protocol (more on WTLS below).

Since the WAP server is the only one with access to its private key, only the server can decrypt the information. This is how the information remains confidential and tamper-proof while in transit across the Internet.

CA certificates

A CA certificate is a certificate that identifies a Certification Authority. CA certificates are just like other digital certificates except that they are self-signed. CA certificates are used to determine whether to trust certificates issued by the CA.

In the case of a passport, a passport control officer will verify the validity and authenticity of your passport and determine whether to permit you entry. Similarly, the CA certificate is used to authenticate and validate the WAP server certificate. When a WAP server certificate is presented to a micro-browser, the micro-browser uses the CA certificate to determine whether to trust the WAP server's certificate. If the server certificate is valid, the WTLS session proceeds. If the server certificate is not valid, the server certificate is rejected and the WTLS session is stopped.

Wireless Transport Layer Security (WTLS)

What is WTLS?

Wireless Transport Layer Security (WTLS) technology is a security protocol. It is designed for securing communications and transactions over wireless networks. WTLS is being implemented in all the major micro-browsers and WAP servers, and as such will play a major role in e-business activities.

The WTLS protocol uses digital certificates to create a secure, confidential communications "pipe" between two entities, typically a mobile phone and a WAP Server. Data transmitted over a WTLS connection can not be tampered with or forged without the two parties becoming immediately aware of the tampering.

How WAP Server certificates are used in a WTLS transaction?

Suppose Alice wants to connect to a secure WAP site, with her mobile phone, to buy something online:

- When Alice visits a WAP site secured with WTLS her micro-browser sends a "Client Hello" message to the WAP server indicating that a secure session (WTLS) is requested.

- The WAP server responds by sending Alice it's server certificate (which includes it's public key).

- Alice's micro-browser will verify that the server's certificate is valid and has been signed by a CA whose certificate is in the micro-browser's database (and who Alice trusts).

- If the certificates are all valid, Alice's micro-browser will generate a one-time, unique "session" key and encrypt it with the server's public key. Her micro-browser will then send the encrypted session key to the server so that they will both have a copy.

  The server will decrypt the message using its private key and recover the session key. At this point Alice can be assured of two things:

- The WAP site she is communicating with is really the one it claims to be (its identity has been verified), and

- Only Alice's micro-browser and the WAP server have a copy of the session key.

The WTLS "handshake" - the process of identifying the two parties that want to establish a WTLS connection - is complete and a secure communications "pipe" has been established. Alice's micro-browser and the WAP server can now use the session key to send encrypted information back and forth, knowing that their communications are confidential and tamper-proof.

What’s Next?

The introduction of mobile phones with the capacity to support user certificates will permit for "mutual authentication" and digital signature processing enabling a wide range of opportunities for the introduction of new e-business applications and services. Entrusts' full range of products and services permit the creation of end-to-end trusted e-business transactions. Visit the Entrust Web site for the latest information http://www.entrust.com