WorldSecure

A Technology Whitepaper

WorldSecure™

Business-Grade E-mail for the Enterprise

WorldSecure™
Business-Grade E-mail for the Enterprise

This paper introduces the WorldSecure™ product line from Worldtalk Corporation. WorldSecure allows organizations to completely secure their electronic mail networks. The paper describes features and functionality of the product line and discusses several deployment options. Finally, the paper also contains a brief technology backgrounder on technology heavily used by WorldSecure components.

The information contained in this document is subject to change without notice and should not be construed as a commitment by Worldtalk® Corporation. Worldtalk Corporation assumes no responsibility for any consequences resulting from errors that may appear in this document.

For publications, bulletins or later revisions of this guide, contact:

Worldtalk Corporation
5155 Old Ironsides Drive
Santa Clara, CA 95054
Tel: (408) 567-1500, Fax: (408) 567-1501
e-mail: info@worldtalk.com
http://www.worldtalk.com

Worldtalk Document Number G-PBMD-0927-A7-MKT

Worldtalk Corporation
5155 Old Ironsides Drive
Santa Clara, CA 95054
Tel: (408) 567-1500, Fax: (408) 567-1501
e-mail: info@worldtalk.com
http://www.worldtalk.com

1. Overview

Today's distributed computing environment offers the promise of enhanced business communications. E-mail and groupware systems transport many types of files or documents, including simple text, applications such as spreadsheets and complex multimedia information, sound, graphics and video. Organizations use these systems for the transfer of critical files such as purchase orders, expense reports, sales forecasts, financial information and contracts, both within the organization and increasingly with other organizations over the Internet. In this setting, these files are now tangible information assets that must be protected. A recent market survey of the Fortune 1000 ranked the top two threats to information security which resulted in financial losses to be computer viruses and inadvertent errors. Moreover, an estimated $24 billion was lost due to information security breaches in 1996 alone .

The good news is that many of the obvious holes within today's communications networks are being plugged with security countermeasures in existence. Traditional firewalls prevent network access by unauthorized users. Secure sockets (SSL) allow for data to be passed securely over the Worldwide WEB (WWW). Standards such as SET and IPSEC are also allowing for transactions to be secured over the Internet as well. Electronic mail however, still remains problematic for the enterprise. Most organizations simply pass e-mail through their conventional firewalls (SMTP, port 25) without any form of audit on the information being exchanged. This situation is growing increasingly unacceptable, since e-mail is still by far the most used application within organizations and over the Internet.

Introducing WorldSecure™: A Complete Secure E-mail Solution for the Enterprise

The WorldSecure product family is a complete set of tools for securing already-deployed enterprise e-mail and groupware applications. It is a security overlay; it does not require organizations to throw away existing investments in e-mail and groupware infrastructure, and eliminates the need for retraining end users on a new e-mail system. With it, organizations can:

- secure internal desktop to desktop e-mail,
- secure e-mail over the Internet for e-commerce applications,
- define and enforce bi-directional e-mail access controls and content policies for SPAM and nuisance mail filtering,
- screen e-mail for viruses before they multiply throughout the organization and,
- provide a detailed audit trail of e-mail activity for specific sets of users

Figure 1 shows how WorldSecure can be used to connect an organization with remote offices, trading partners, and remote clients to create a worldwide secure e-mail network. In this figure, ACME corporation deployed WorldSecure servers in its headquarters and at its remote office. This guarantees that all e-mail traffic between these two sites is completely encrypted. ACME also encrypts every e-mail message that goes to its trading partner who also employs a WorldSecure client to encrypt and decrypt all e-mail exchanged with ACME. Finally, ACME has left all e-mail traffic with its customers in clear text, as less sensitive information is being exchanged. Both WorldSecure Server and Client are explained in details later in the document.

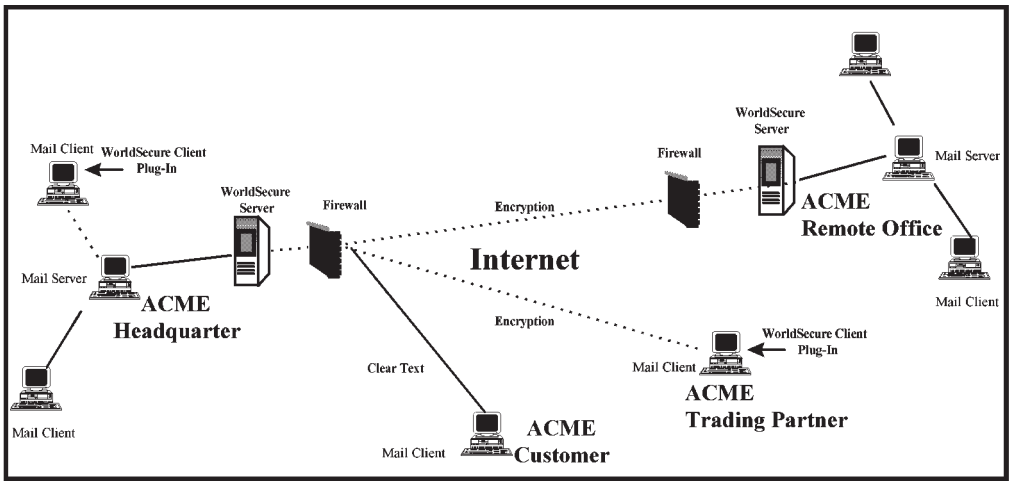


Figure 1: Securing e-mail across the Internet

The WorldSecure product family employs the S/MIME™ protocol to encrypt and digitally sign all e-mail that flows over the Internet or within your corporate intranet.

Why S/MIME?

The S/MIME™ protocol is an extension to the standard Internet mail protocol called MIME (Multipurpose Internet Mail Extensions). S/MIME™ provides encryption and digital signature capabilities to electronic mail, which solves three critical business problems that occur when sending e-mail: (i) the lack of message confidentiality, (ii) the lack of message integrity, and (iii) the inability to confirm message authenticity.

- Confidentiality: ensures that only authorized users may read an e-mail message after it has been sent.
- Integrity: ensures that a recipient of a message can confirm whether or not it was modified after it was sent.
- Authenticity: guarantees that a recipient of a message can confirm the originator's identity. This ability also provides for non-repudiation of the message, meaning the originator cannot deny that the message was sent.

A detailed description of the S/MIME standard and/or public/private key cryptography is beyond the scope of this paper.

2. Requirements of a Secure Electronic Mail Solution

Any secure electronic mail solution must be based upon a robust set of requirements that make it enforceable, manageable, easy-to-use for end-users, interoperable, reliable, and scaleable. The WorldSecure solution is based on these requirements:

Security policies must be enforceable

One of the most important aspects of the WorldSecure solution is that it allows administrators and policy-makers to both define and enforce corporate security policies for e-mail. This is totally unique to WorldSecure; other solutions certainly provide encryption and digital signature, however only WorldSecure allows administrators to mandate virus scanning, content control, access control, encryption, and digital signature policies from a central point of administration.

Solution must be ubiquitous

Security solutions are most effective when they apply to everyone in an organization. WorldSecure Server intercepts every piece of e-mail and enforces security policies on it. Further, WorldSecure Client and Server both support the S/MIME protocol for encryption and digital signature, making them interoperable with millions of other S/MIME-enabled applications (such as Netscape Communicator). For organizations that wish to secure home-grown workflow or other mail-enabled applications, Worldtalk has developed an S/MIME toolkit allowing organizations to leverage S/MIME throughout their organization for all security applications.

Solution must be easy to use for end users

WorldSecure is designed as a security overlay to existing e-mail products and technologies. The WorldSecure Client natively "plugs in" to existing desktop e-mail clients. With this approach, end users can continue to use the applications they are familiar with, while adding the benefits of secure e-mail. Even better, the WorldSecure Server is completely transparent to the end user altogether. Its job is to define and enforce e-mail policies, while providing reminders to e-mail users when they are in policy violation.

Solution must be thoroughly modular and interoperable

WorldSecure supports all major open standards for all elements of the solution, including S/MIME as the secure e-mail protocol, LDAP for the directory/certificate access protocol, and X.509 for digital identification. Additionally, it supports a wide variety of trust models – including the most flexible choice of certificate authorities available from a secure application suite. This allows organizations to combine their preferred e-mail solutions with their preferred certificate authority.

Solution must be easy to deploy and manage

WorldSecure has both client and server components that have a quick installation, with very few steps to perform before the products are up and running. Both client and server are native "win32" applications; the server runs as a native Windows NT service, and the client runs on both Windows 95 and Windows NT machines. WorldSecure fully takes advantage of Windows NT event logging, performance monitoring, and high performance I/O.

3. Elements of a Secure E-mail Solution

A complete secure e-mail solution for the enterprise consists of the following components: (i) a secure client, (ii) an e-mail firewall, (iii) a certificate server, (iv) a certificate authority, and (v) a toolkit for securing in-house developed applications.

WorldSecure provides items (i) the WorldSecure Client, (ii) the WorldSecure Server, and (iii) the WorldSecure Certificate Server, respectively, and integrates seamlessly with Certificate Authorities and S/MIME toolkits from other vendors.

Figure 2 shows how these items fit in the enterprise. In this figure, all WorldSecure components integrate with other applications in the enterprise. The WorldSecure Client integrates with most e-mail applications to provide desktop-level encryption. WorldSecure Server resides on the safe side of the firewall and encrypts all outbound traffic based on pre-configured rules. The WorldSecure Certificate Server stores all X.509 certificates required by WorldSecure Client and Server and works with any Certificate Authority on the network. Certificate requests from WorldSecure Clients and Servers are done using LDAP.

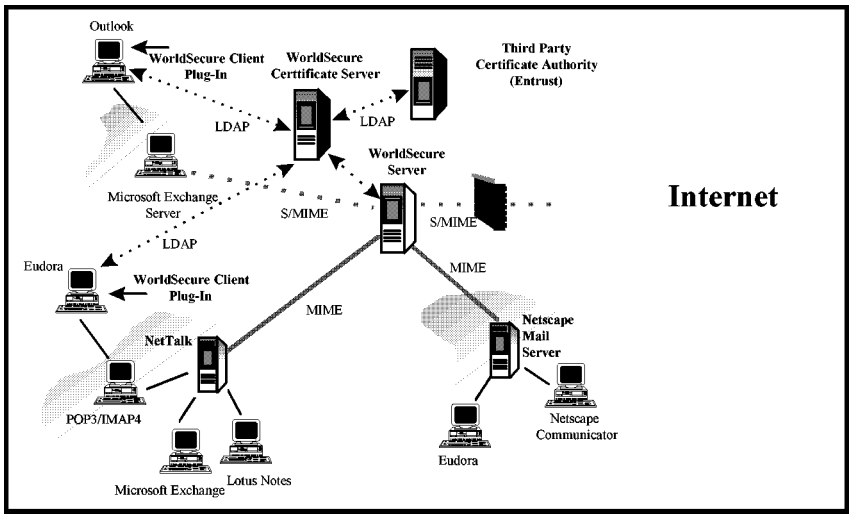


Figure 2: WorldSecure in the enterprise

WorldSecure Client: Desktop S/MIME "Add-On"

The WorldSecure Client (previously known as "Secure Messenger") is a desktop S/MIME product that can be used to build a complete desktop to desktop secure e-mail solution for the enterprise. With intuitive "add-ons" to existing e-mail clients, it is designed to "overlay" an existing e-mail infrastructure – not obsolete it.

The WorldSecure Client brings two major benefits which end up saving organizations lots of time and money:

- it eliminates the need for end-users to learn an entirely new e-mail package; instead, they can secure their e-mail while using the products they are already comfortable with
- it allows organizations to preserve their investment in existing e-mail infrastructure; there's no need to throw away an e-mail system that is already working

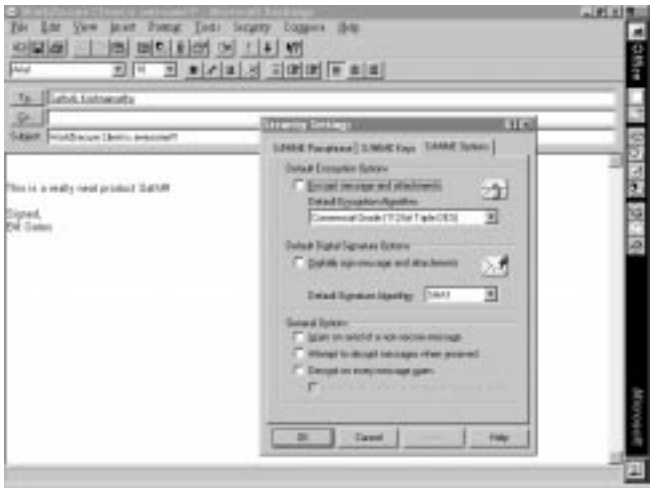


Figure 3: WorldSecure Client Add-On for Microsoft Exchange

Table 1 summarizes the major benefits of the WorldSecure Client:

Benefit	**Description**
Works In Any E-mail Environment	The WorldSecure Client's convenient and intuitive user interface allows S/MIME files to be dragged and dropped into any e-mail client on the desktop, giving users freedom of choice, while securing their electronic environment over the Internet or corporate Intranet. The WorldSecure Client also includes special security add-ons for a variety of e-mail clients that integrate S/MIME security seamlessly with the messaging application.
Convenient and Easy to Use	One of the typical barriers to adoption for encryption and digital signature software is their difficulty of usage. The WorldSecure Client has a convenient and intuitive user interface, and tightly integrates with today's popular e-mail packages for a positive user experience.
Strong Cryptography	No product available provides stronger security than WorldSecure™. The following grades of encryption are available: Security Grade — RSA Key Size — Symmetric Cipher Key Export Grade — 512 bits — 40 bits Low Grade — 768 bits — 56 bits Commercial Grade — 1024 bits — 128 bits Military Grade — 2048 bits — 255 bits
Open And Interoperable Security	The WorldSecure Client uses the industry standard Secure MIME (S/MIME) protocol, providing interoperability with other S/MIME compliant products. In addition to supporting a range of encryption grades, the WorldSecure Client also supports a wide variety of encryption and digital signature algorithms to provide the broadest interoperability available. • Encryption Algorithms: RC2, RC5, DES and Triple DES (EDE CBC) • Digital Signature Algorithms: MD5, SHA1

Table 1: WorldSecure Client Benefits

WorldSecure Server: Electronic Mail Firewall

The WorldSecure Server is a new product category called an electronic mail firewall that plays an extremely important role in enforcing security policies for the enterprise. Typically deployed on a stand-alone machine on the safe-side of your firewall, the WorldSecure Server replaces (or complements) an existing Internet relay host with a high-performance, e-mail clearinghouse. The e-mail firewall is an essential component to any secure e-mail solution. Why? Because use of desktop e-mail encryption products are totally up to the discretion of end-users. Bad judgment, or inadvertent errors, by the end-user as to when messages should be encrypted and/or digitally signed, means information assets are at risk. This must be enforced centrally.

The following list exemplifies how the WorldSecure Server can be used:

- to protect information assets before they leave for the Internet by enforcing access control, content filter, virus scanning, encryption, and digital signature policies
- to enforce security policies between your organization and business partners using the S/MIME protocol for secure e-mail exchange
- to protect your organization's internal network from SPAMs, hate mail, and other nuisance mail with comprehensive content filtering
- to screen e-mail for viruses before they multiply throughout your organization
- to provide a detailed audit trail of e-mail activity for specific sets of users, for general purposes and/or suspicious activity monitoring

Table 2 summarizes the major benefits of the WorldSecure Server:

Benefit	**Description**
Enforceable Security Policies	The WorldSecure Server monitors all e-mail messages, both inbound and outbound, and enforces comprehensive security policies on a per-domain and/or per-user basis including: • virus scanning for attachments • encryption/digital signature • content management· access management
Virus-Free Electronic Mail	The WorldSecure Server protects the Intranet from infection without requiring desk top tools. Embedded within it is the Trend Micro virus scanning engine, which provides high-performance virus scanning, with easily accessible pattern updates over the Internet.
Easy to Deploy Encryption and Authentication	Server-based S/MIME capability allows your organization to exchange secure e-mail with the millions of S/MIME clients that will be appearing over the course of the year, while providing easy deployment of a single-box solution. In addition to supporting a range of encryption grades, the WorldSecure Server also supports a wide variety of encryption and digital signature algorithms to provide the broadest interoperability available. • Encryption Algorithms: RC2, RC5, DES and Triple DES (EDE CBC) • Digital Signature Algorithms: MD5, SHA1
Centralized Control of Access, Content Management	The WorldSecure Server allows flexible control over: (i) who is allowed to send/receive e-mail, (ii) what type of information they can (or cannot) send/receive, and (iii) when they can send/receive this information. The flexible rules engine allows your organization to define comprehensive keyword searches and take actions on specific filename extensions. Specific actions include quarantine, reject, drop, annotate, and defer delivery.

Table 2: WorldSecure Server Benefits

One of the most important aspects of the WorldSecure Server is that all of the aforementioned capabilities are integrated into a single product, in a modular fashion such that any organization can pick and choose which features to use and which ones to not use. For example, if an S/MIME message comes in from the Internet, the message can be decrypted, then scanned for viruses before being sent onward into the organization. But if the company already has desktop virus scanners, then the WorldSecure Server can easily be configured to disable that feature. Regardless of how the product is used however, the WorldSecure Server allows any organization to keep its existing e-mail infrastructure intact, while providing value-added security benefits, transparent to the end-user.

WorldSecure Certificate Server: Directory Services for Digital Certificates

The WorldSecure Certificate Server is a repository for digital certificates. At its core is a "meta-directory" service, which provides the ability for certificates to be published, revoked, distributed, and accessed by applications. What makes this product unique is its ability to replicate directory entries with e-mail name and address books. The same directory that holds an organization's digital certificates can be used to hold other important information about users including: e-mail addresses, which encryption algorithms they support, and key lengths that should be used for them. This approach simplifies administration and management.

Table 3 summarizes the major benefits of the WorldSecure Certificate Server:

Benefit	**Description**
Interoperability with	The WorldSecure Certificate Server has full support for the lightweight directory access protocol (LDAP), which is the defacto protocol used by popular certificate authorities to publish and revoke digital certificates from a directory server. Additionally, both the WorldSecure Client and Server both support LDAP, so certificates can be easily retrieved from the WorldSecure Certificate Server.
Full replication with	Yet another example of how WorldSecure leverages an organization's existing e-mail infrastructure, the WorldSecure Certificate Server has full directory replication capability with Microsoft Exchange, Lotus Notes, Lotus cc:Mail, Microsoft Mail/PC environments. This allows organizations to manage digital certificates in the context of e-mail users, and automatically keep them up-to-date.
Ubiquitous Access to Certificates	The WorldSecure Certificate Server can distribute digital certificates throughout an organization with server to server replication. Additionally, certificates can be accessed by business partners via LDAP over the Internet.

Table 3: WorldSecure Certificate Server Benefits

Certificate Authorities: Who do you Trust?

One of the most important decisions that an organization makes is determining the nature of its Public Key Infrastructure (PKI). There are several choices today ranging from hosting a complete infrastructure internally to outsourcing. Appendix C of this paper describes these options in detail and provides guidelines on which PKI to choose from.

WorldSecure is designed to work with any PKI an organization chooses to deploy. For organizations with little or no PKI, both the WorldSecure Client and Server have an embedded PKI option that allows such organizations and their business partners to bootstrap their public key roll-out. Certificate exchange in these environments is done via e-mail. Either way, WorldSecure delivers a consistent, secure e-mail solution for your organization.

For example, when using WorldSecure Client with Verisign, WorldSecure Client generates its own public/private key pair. It then submits a certificate request to Verisign. Verisign returns its certificates to the client via

e-mail, after which it can be published to any LDAP enabled directory, such as Worldtalk's NetTalkÔ, or distributed via e-mail to other WorldSecure clients. WorldSecure Clients embeds Verisign's root key, so any Verisign certificate can be automatically trusted.

Toolkits

Finally, the ability to S/MIME-enable both client and server-based applications in an organization requires an easy to use, high-level toolkit. RSA Data Security has available the "Secure Mail Toolkit", which is based upon technology acquired from Worldtalk. This toolkit allows organizations to quickly and easily integrate S/MIME into their applications, and leverage the infrastructure deployed by WorldSecure.

4. WorldSecure: Client, Server or Both?

WorldSecure Client and Server each solve unique problems and should be examined carefully before deciding on a secure e-mail strategy. Table 4 summarizes the capabilities to help organizations choose the right combination of products to solve their business needs.

Requirement	**WorldSecure Client**	**WorldSecure Server**
Protection of internal & external security threats	Internal as well external to organization. Security is extended to desktop with this product.	External to organization. Security is enforced at Internet boundary, and/or at divisional, or LAN level.
Scaleability	Good. Being a desktop product however, roll out of this product to the masses can be time consuming.	Best. Being a server product, this can be deployed immediately to protect information assets being sent over e-mail.
Central enforceability of	Fair. Configuration defaults can set prior to rolling out product, however decision to encrypt and/or digitally sign is up to enduser.	Best. All e-mail security policies can be centrally monitored and enforced.
Virus management	N/A	Full virus protection available for e-mail messages before they enter organization.
Access management	N/A	Centralized control over who can send/receive e-mail and to/from which organizations or users.
Content management	N/A	Centralized alerts & actions for file types, keywords,
S/MIME support	Full desktop S/MIME support.	Full server S/MIME support.
Works in any e-mail environment	Add-ons to existing e-mail clients. Check Worldtalk home page for latest availability.	Being a server product, WorldSecure Server can be introduced into any e-mail environment, as an Internet mail relay host.
Minimal learning curve for end-users	Good. With intuitive drag-down menus & toolbars extensions, client add-ons allow end users to continue to use e-mail products they are used to with minimal changes	Best. Being a server product, policies are enforced completely transparent to the end user.

Table 4: WorldSecure Capability Summary

Typically, both products are applicable; WorldSecure Server can be deployed immediately, and WorldSecure Client can be deployed for users that require desktop security (e.g. corporate executives, finance departments, etc.)

5. Summary

In summary, WorldSecure™ is a long lasting investment – with its wide range of certificate authority and public key infrastructure options, and its overlay approach to existing e-mail systems, WorldSecure gives organizations the flexibility to change their e-mail infrastructure and even their PKI, while maintaining a consistent approach for e-mail security. There is no other product family available that is as flexible, open-standards based, and efficient in empowering such organizations and allowing them to define and enforce corporate-wide security policies.

Appendix A: Public/Private Key Cryptography

WorldSecure adopts public key encryption technology from RSA Data Security to encrypt and digitally sign messages. Figures 4 and 5 describe how this technology works.

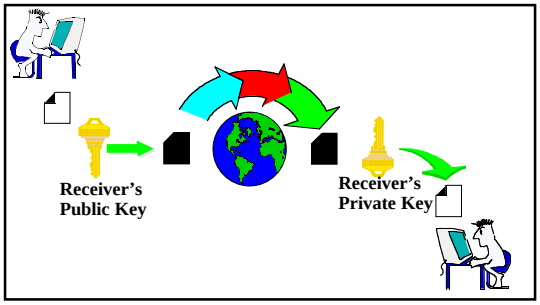


Figure 4: How public/private key cryptography protects e-mail confidentiality

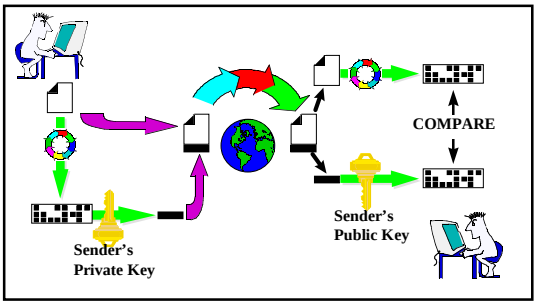


Figure 5: How public/private key cryptography protects e-mail integrity and confirms authenticity

In Figure 4, an e-mail message is encrypted using the recipient's public key. The encrypted message is sent over the Internet and can only be decrypted by the recipient who holds the corresponding private key. Using such strong cryptography, a message is only read by its destined recipient, independent of its path. This fully guarantees confidentiality of e-mail messages as they travel over the Internet or corporate intranets.

In Figure 5, e-mail is passed through a hashing algorithm to produce the message "digest", which is encrypted with the private key, creating an "RSA digital signature".

The receiver uses the same hashing algorithm to create another message "digest", and also decrypts the signature using the sender's public key. The two resulting digests are then compared. If they match the message was not altered and was indeed sent by the holder of the private key that corresponds to the sender's public key. This fully guarantees e-mail integrity and confirms the authenticity of the sender.

These two algorithms (or procedures) can be used together to provide ultimate e-mail security over the Internet and corporate intranets.

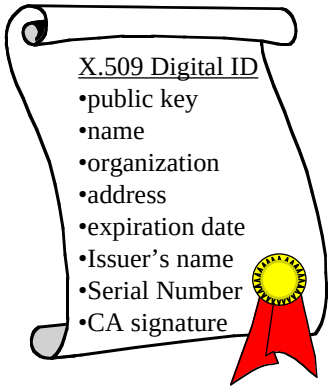
Appendix B: Digital Certificates

Digital certificates, also known as X.509 certificates or Digital ID's™ were created to solve an obvious problem that occurs when two users are trying to communicate securely using public key encryption. How does an originator get the public key of their recipient?

The problem is complex when dealing in the world of security threats and hackers. If someone were to send the originator their public key over an unsecured line, the key could be intercepted and replaced with someone else's key. This would lead the originator to unknowingly use the wrong key and encrypt their e-mail directly for the hacker.

This problem is solved by introducing a trusted third party – also known as a "certificate authority" (CA) – who validates the identity of users, stores each users' public keys in individual digital certificates, and signs the certificates.

A Digital ID typically contains the following: Owner's public key, Owner's name, organization, address, Expiration date of the public key, Name of the issuer (which is that of the Certificate Authority), Serial Number of the certificate, Digital signature of the Certificate Authority.



Security applications usually employ thorough procedures to bind a user (usually a recipient) to his or her Digital ID. Security applications perform four steps in order to retrieve the public key of a recipient:

1. Query certificate store for recipient's X.509 certificate
2. Verify that certificate is from a trusted CA, and that certificate has not been altered
3. If so, then originator is guaranteed that the public key within the certificate is that of the recipient
4. Verify that key is still valid - i.e. key lifetime has not expired, or key has not been added to "black-list". In X.509 terminology, this black-list is called a certificate revocation list ("CRL").

Appendix C: Certificate Authorities and Public Key Infrastructures

Operations involving Certificate Authorities

There are four major processes associated with someone's certificate and a Certificate Authority : CA bootstrap, CA management, directory access, and directory management. Some of these procedures, mainly CA bootstrap and CA management, can be outsourced to organizations such as Verisign or GTE Cybertrust.

The following is a detailed description of these procedures:

CA Bootstrap

The certificate authority bootstrap operations refer to the steps necessary to register a new user on to the system. Before these operations occur, users must first be "authenticated" by the organization, or by a designated third party. Generally, such organization will need to dedicate security personnel to act as local registration authorities (LRA) in order to carry out this user identification process. After each user is authenticated to the appropriate level, the processes that must occur include: public/private key generation, certificate requests, and certificate issuance. Note that no standards exist today for where public/private key pairs are generated (i.e. in the applications, or at the CA). There is a quasi-standard called "PKCS #10" which is defined by RSA Data Security that defines how applications can request a certificate from a CA, however this is not broadly adopted among all CA's. Certificate issuance is also non-standard: do CAs return the certificate to the application, or do they publish the certificate directly to the directory service, or both? The answers to these questions vary among CA solutions, making them proprietary in nature. Worldtalk is working with all of the CA vendors to further standardize these operations, and to support all of the variants in WorldSecure.

CA Management

Ongoing management that occurs at the certificate authority includes the ability to recover individual users' private keys out of "escrow" and to revoke certificates if their security has been compromised. These are absolutely necessary features for organizations to control in any large scale PKI. Again, these operations are all done in a proprietary manner among CAs. How do private keys get centrally stored? Who has access to them? No standards exist yet for this. Likewise, certificate revocation can typically be done centrally from the CA by an administrator, but what standard mechanisms exist for end-users to revoke their certificates? None at the moment. And finally, the "root keys" that are embedded within applications, must be changed periodically, or in the case of a disaster. The mechanism by which applications automatically recognize such a "root key rollover" is totally proprietary at the moment.

Directory Access

Fortunately, the industry has standardized on the lightweight directory access protocol (LDAP) as the means by which applications can retrieve information (including digital certificates) from a directory service. WorldSecure applications fully support LDAP to retrieve certificates for remote users.

Directory Management

LDAP plays an important role for CAs and/or applications to publish digital certificates as well. The WorldSecure Certificate Server has a full LDAP server which allows leading CAs, such as Entrust to publish their certificates in a central location. It is up to the Certificate Server to then distribute these certificates to all other locations in your organization so that they are available to any application that may need them.

Types of Certificate Authorities

There are also four basic types of Certificate Authorities that define and influence a Public Key Infrastructure (PKI):

- Embedded Certificate Authority
- Workgroup Certificate Authority
- Enterprise Certificate Authority
- Inter-Enterprise Certificate Authority

An Embedded CA is one that is embedded in the security application. These CAs are tailored to individual applications and are not designed to work with any other security applications. They are ideal for organizations looking at a complete security solution for a specific application or protocol.

A Workgroup CA, such as Netscape Certificate Server™, is designed to support specific applications suites. Workgroup CAs generally lack the ability to cross certify with other CAs, and lack interoperability with other applications.

An Enterprise CA, like Entrust™, is designed to work throughout the enterprise and with all security applications. It really eliminates the need for workgroup CAs, but generally requires a rather significant investment and cooperation from all departments within the organization.

Inter-Enterprise CAs, like Verisign or GTE Cybertrust, are designed to allow organizations to outsource a major section of CA operations. They provide the highest level of interoperability, especially for applications securing traffic between organizations.

Table 5 shows how these CAs rank relative to important issues such as scaleability and interoperability.

Please note that WorldSecure is designed to work with any PKI an organization chooses to deploy. For organizations with little or no PKI, both the WorldSecure Client and Server have an embedded PKI option that allows such organizations and their business partners to automatically perform the "CA bootstrap" processes described above. Certificate exchange in these environments is done via e-mail. Either way, WorldSecure delivers a consistent, secure e-mail solution for your organization.

Criteria	Embedded CA	Workgroup CA	Enterprise CA	Inter-Enterprise CA
Scaleability	In general, fair. With WorldSecure ™ this option is appropriate for small numbers of users.	Good	Best	Good for small numbers only. User authentication processes do not scale well.
Insource vs. Outsource	Can outsource CA Bootstrap and Management	Can outsource CA Booststrap and Management	Insource only	Can outsource CA Bootstrap and Management
Protocol Interoperability	In general, poor. WorldSecure™ however, has full S/MIME protocol interoperabitlity, with root key import, and direct trust capabillity	Future. Requires cross-certification standards (e.g.) PKIX for use beyond enterprise.	Future. Requires cross-certification standards (e.g. PKIX) for use beyond enterprise.	Good. By sitting at the top of the trust hierarchy, Verisign and GTE CyberTrust can extend protocol interoperability to all parties
PKI Interoperabiltity	N/A	In general, only supported by single vendor application suite (fair). WorldSecure™ is designed for full PKI interoperability with all leading workgroup CA's.	In general, supported by multiple vendors (good). WorldSecure™ is designed for full PKI interoperabiltiy with all leading enterprise CA's.	In general, supported by multiple vendors (best). WorldSecure™ is designed for full PKI interoperability with all leading inter-enterprise CA's.
Completeness of Solution	In general, good. WorldSecure™ has full support for: • CA Bootstrap • CA Management • Directory Access • Directory Management	Good. CA Bootstrap CA Management Directory Access Directory Management	Best. CA Bootstrap CA Management Directory Access Directory Management	Fair. Inter-enterprise solutions only handle CA Bootstrap, CA Management. Directory Access and Management must be handled within your organization. WorldSecure™ Certificate Server can be used for this.

Table 5: Selecting the right Public Key Infrastructure

Appendix D: Interoperability

There are two types of interoperability that are equally important: "protocol" and "PKI." Whether or not an organization needs one, or both depends on business requirements. The only situation where an organization would not require either type of interoperability would be if that organization has a single e-mail system, with a secure e-mail implementation, and has no requirement to exchange secure e-mail with the outside world.

Protocol Interoperability

"Protocol" interoperability means that e-mail messages from one vendor's S/MIME implementation can be successfully exchanged with and interpreted by all other vendor implementations. For any two S/MIME applications to achieve protocol interoperability, they must: (i) implement the S/MIME specification correctly, (ii) have physical access to the digital certificates of each other, and (iii) trust a common certificate authority, or have provisions for directly trusting each other. WorldSecure solves all three of these items in an open, standards-based fashion.

S/MIME Implementation

Worldtalk, along with RSA, is one of the co-authors of the S/MIME specification that has been submitted to the Internet Engineering Task Force (IETF) as an RFC and co-chairs the working group. This leadership has allowed Worldtalk to be one of the first vendors to have a commercially available S/MIME implementation, called "Secure Messenger." This product, now known as the WorldSecure Client, has been successfully tested against every vendor implementation available, including those from Netscape, Microsoft, Entrust, Connectsoft, Frontier Technologies, and OpenSoft. Indeed, RSA Data Security maintains an "S/MIME Compatibility Matrix," which contains the list of implementations that Worldtalk has success fully interoperated with.

Digital Certificate Access

The WorldSecure Client and Server have two flexible means to provide physical access to digital certificates: via e-mail, and the lightweight directory access protocol (LDAP). The e-mail certificate exchange wizards allow for two entities to automatically exchange certificates quickly and easily. Additionally, the WorldSecure Server has a certificate "auto-responder" that automatically e-mails its certificate to a requester. This mechanism is appropriate for small groups of secure e-mail users.

For larger deployments, the WorldSecure Certificate Server can be used to centrally manage and publish digital certificates. Any application that supports LDAP (including the WorldSecure Client and Server) can then gain access to the certificate of their intended recipients.

Trusting the Sender

WorldSecure can be configured to trust any certificate authority and the certificates that come from it, quickly and easily. A "root key" refers to the public key of a CA, which is nec essary to trust certificates that come from it. Both WorldSecure Client and Server have the ability to import new root keys. This enables organizations to centrally configure the CA's they trust, whether they be customers, clients, trading partners, other departments, or even well-known public CA's such as Verisign or GTE CyberTrust. For maximum flexibility, when untrusted certificates are received from a sender, both WorldSecure Client and Server have the provision to override any trust relationships in place, and "direct trust" or "direct distrust" a certificate.

PKI Interoperability

Even with open standards such as S/MIME, LDAP, and X.509, there are still proprietary aspects to a secure e-mail solution. In particular, every CA has proprietary mechanisms for public/private key generation, key recovery/escrow, and certificate requests/responses/revocations. "PKI Interoperability" refers to the ability for S/MIME applications to choose the CA which will generate and maintain their own digital certificates. As previously discussed, WorldSecure works with all PKI options.

Appendix E: WorldSecure and Traditional Firewalls

The traditional firewall is perhaps one of the most basic building blocks for securing corporate networks from outside intrusion. It implements native Internet protocol suite security with packet filtering, application proxy, and advanced "stateful inspection" techniques. Firewalls are more recently adopting packet-level encryption/authentication technology to build "virtual private networks" (VPN's) using public-key encryption standards such as S/WAN from RSA. This technique secures the "session" between two computers, such that all data that passes between them is secure.

Firewalls still do not provide for any form of message confidentiality, integrity, authenticity, or non-repudiation after the message is received by the destination machine. The store-and-forward nature of e-mail requires application-level encryption/authentication in order to ensure that information will be secure along every hop from sender to receiver. The S/MIME protocol used within WorldSecure solves this problem.

Many firewalls also tend to keep a "hands-off" approach to actual e-mail content, with support for the Internet e-mail delivery protocol "SMTP," but not the content protocols such as RFC-822 and MIME. As such, organizations are typically limited to controlling who can access e-mail, and which IP addresses can be reached.

In short, WorldSecure Server is totally complementary to existing network firewalls. It typically sits on the safe side or in the demilitarized zone (DMZ), and intercepts e-mail traffic while enforcing security policies. It can also be deployed within a corporate intranet, alongside POP3/IMAP4 e-mail servers or even next to SMTP e-mail gateways.