Certicom Security for Enterprise Instant Messaging

secure instant messaging for desktops, servers, embedded and wireless platforms

THE PROBLEM

Informal IM use within enterprises is widespread – the value is compelling. It's easy to deploy and facilitates collaboration among a wide variety of users and locations. And between wireless devices, it's also very convenient. But without authentication, message integrity, and confidentiality, it also jeopardizes enterprise security. Employees messaging in real time over wireless devices may inadvertently expose sensitive information or trade secrets to unauthorized users.

Corporate security policies are good in theory but difficult to enforce in practice. Many do not yet explicitly address the new risks of IM via wireless devices. Rather than benefiting from real-time messaging, enterprises tend to deny employee access to IM rather than risk the spread of viruses or unauthorized network access.

Any vendor hoping to successfully market an instant messaging application or device must integrate security.

Vendors who have integrated security within their desktop IM products are discovering the wireless frontier presents different challenges: less bandwidth, constrained processors and limited battery life. The wireless IM security challenge has also grown to include the need to secure a wide variety of platforms. Vendors who implement a single solution for multiple platforms enable enterprises to extend secure IM to employees, customers and trading partners.

The industry also contends with the issue of standardization common to any emerging technology. XMPP or SIMPLE: which are the right protocols for interoperability? AES and ECC: how can the strongest security be guaranteed?

THE SOLUTION

The value of instant messaging is the spontaneous collaboration allowed by real time performance and convenience. The security solution must be strong and reliable, without negatively impacting these requirements. The pace of change in the IM industry demands that security be integrated quickly without limiting your market to only a few platforms or verticals.

An ideal security package for instant messaging must address these questions:

- **How does it affect communications overhead?**
- **Is it FIPS 140-2 Validated for the burgeoning government market?**
- **Does it use industry standards for security and interoperability across multiple platforms, networks and operating systems?**

- **Can it offer strong security for continued use today and tomorrow?**
- **Will it work with evolving multimedia uses of IM such as audio and video file sharing?**

Typically, the need for security must be balanced against the impact that processor-intensive cryptography has on available resources such as computing power and bandwidth. These considerations are even more important in a wireless environment where these resources are in short supply. Instant messaging will not tolerate any communications lag.

Certicom has years of experience developing standards-based cryptography toolkits that are already optimized for wireless use. Certicom's cryptographic toolkits allow you to:

- **integrate client and server authenticated security with a footprint up to 80% smaller than open source alternatives.**
- **depend on a FIPS 140-2 Validated cryptographic module**
- **benefit from efficient ECC algorithms**
- **count on ECMQV key agreement that is both faster and stronger than Diffie-Hellman and RSA**
- **use FIPS-Validated algorithms and create your own FIPS-Validated applications or devices for government**
- **employ a single API to add security for more than 30 platforms**
- **rely on the speed and strength of modern AES security**
- **improve processor efficiency and speed with ARM/OMAP optimization**

THE IMPLEMENTATION

For your instant messaging application or device to communicate securely it requires three fundamental attributes to assure trust:

1. **authentication**
2. **message integrity**
3. **confidentiality**

Using Certicom's Security Builder® toolkits, your instant messaging application or device connects to another IM application, device or server and challenges it to guarantee its identity. Identity can be authenticated a variety of ways:

- **PINS**
- **passwords**
- **tokens**
- **digital certificates**

If you've already established an authentication procedure for a desktop IM application, the same method can be used for your wireless scenario. With authentication complete, Security Builder toolkits can enable applications to:

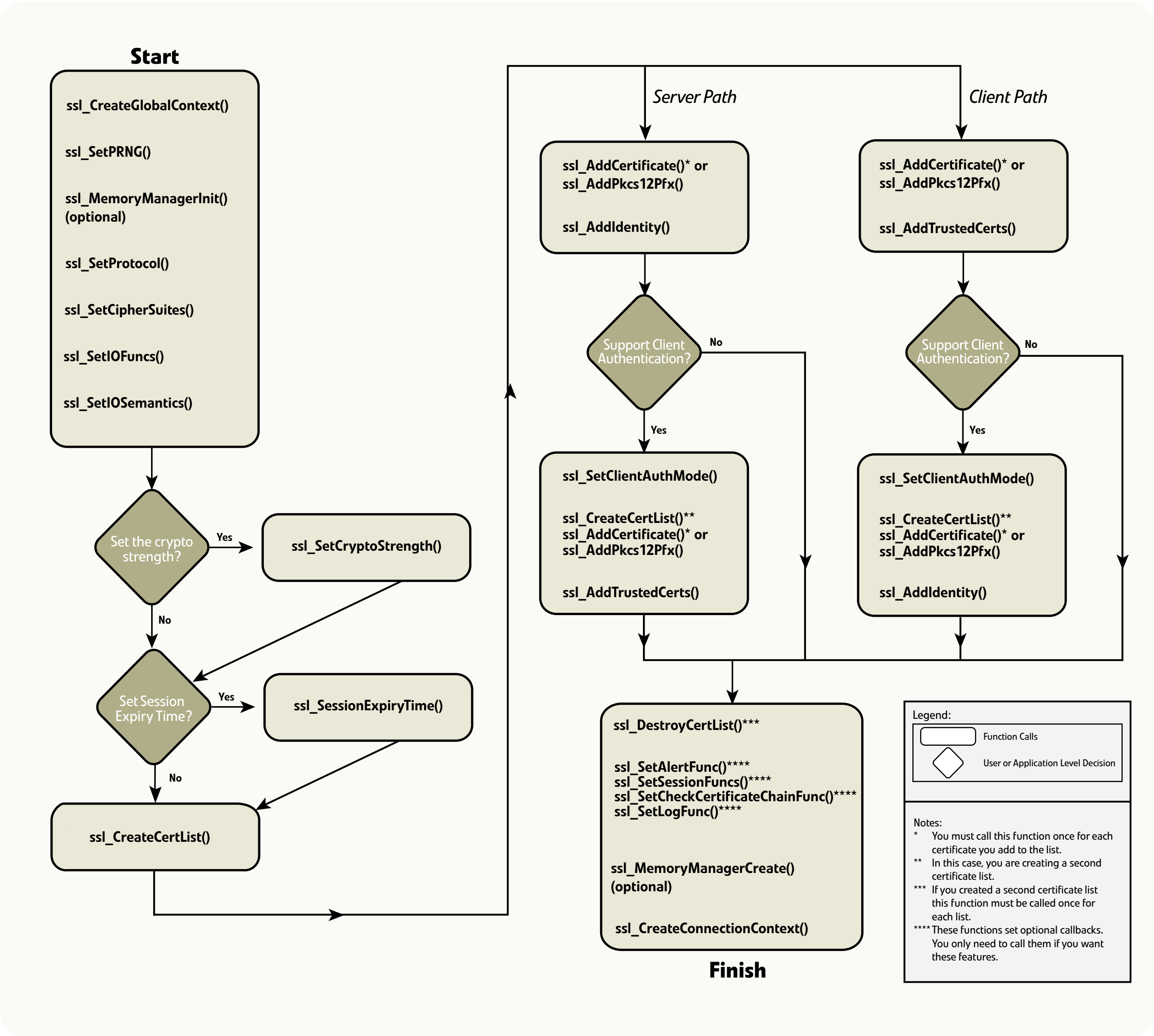
- **generate a shared secret key**
- **look up the publicly available public key of the other party**
- **use the shared secret and public key as a key pair to encrypt transport the shared secret between parties**

Generating, encrypting and exchanging shared secrets is processor-intensive. To reduce processing, the validity period of shared secrets is variable so they can be reused to facilitate faster communication. In high security environments, the shared secret can be created, encrypted and exchanged anew for every session.

For the highest security and efficiency in your application, Certicom uses and recommends:

- **AES or advanced encryption standard for the fastest and strongest symmetric encryption to maintain confidentiality**
- **SHA-1 hash algorithm for fast and strong message integrity**
- **ECMQV (Elliptic Curve Menezes-Qu-Vanstone) for the fastest and strongest key exchange protocol for authentication**

Security Builder SSL API Application Setup Flowchart



This flowchart illustrates how to set up a simple client or server application using the Security Builder SSL-C API.

Older algorithms such as RSA and Diffie-Hellman can be used but require additional network and processor overhead that may hinder wireless communications.

Standard SSL security is best suited to most IM applications and Security Builder® SSL Plus™ integrates with your code base in a matter of hours.

Alternatively, if your IM application or device requires FIPS-Validation for government use, or if your situation requires a unique implementation of SSL or another protocol, Security Builder GSE™, a FIPS 140-2 Validated cryptographic module, is ideal. FIPS-Validated platforms include Palm OS 3.5/4.x, Windows CE 3.0/4.0 and Windows 32 operating systems.

RESULTS

Certicom's Security Builder Crypto™, Security Builder GSE and Security Builder SSL toolkits integrate quickly to secure instant messaging applications on wireless devices using efficient and strong security that is ideal for desktop, server, embedded and wireless environments.

With security, instant messaging vendors expand their markets by 30% to include enterprises which currently deny access to instant messaging for security reasons. They also gain a significant competitive advantage over vendors that do no offer security.

Secure instant messaging products built on a FIPS-validated cryptographic module may also access the lucrative government, legal and financial services markets.

about certicom

Certicom is a leading provider of wireless security solutions, enabling developers, governments and enterprises to add strong security to their devices, networks and applications. Designed for constrained devices, Certicom's patented technologies are unsurpassed in delivering the strongest cryptography with the smallest impact on performance and usability.