Securing VoIP Networks

the importance of device security

A Certicom White Paper
January 2006

certicom™

Introduction

Securing a Voice over IP (VoIP) network is a complex issue that involves many factors, including elements unique to each specific network configuration. As with any IP based network, VoIP systems are potential targets of many types of attacks. In this paper, we will discuss some of these attacks, and present some mechanisms that the developer of a VoIP product can incorporate to make the device more secure.

The list of potential threats to a VoIP system (or any IP system) is extensive, and new issues may be uncovered on an on-going basis. Just as there is no exhaustive list of potential threats to a VoIP system, there is no definitive solution for preventing someone from finding and exploiting a specific vulnerability. From section 20 of the SIP RFC[1], the following statement should set the tone for the challenge of securing VoIP:

> SIP is not an easy protocol to secure. Its use of intermediaries, its multi-faceted trust relationships, its expected usage between elements with no trust at all, and its user-to-user operation make security far from trivial. Security solutions are needed that are deployable today, without extensive coordination, in a wide variety of environments and usages. In order to meet these diverse needs, several distinct mechanisms applicable to different aspects and usages of SIP will be required.

A VoIP system can be composed of many different products – voice terminals (VoIP Phones), desktop systems, servers, gateways, firewalls, etc. Many of the security solutions discussed in this paper are applicable to all of these products, some may be more applicable to only certain products. A signaling gateway, for example, does not deal with media streams directly, and as such is not concerned with how to secure the media stream.

This document is not intended to be a VoIP network planning guide. Such a discussion would fill volumes, and is outside the scope of this paper. Rather, this document discusses various techniques that the developer of a VoIP device can utilize to help secure that device. Achieving robust security is a key consideration when designing an end-to-end network security architecture with high reliability and quality of service requirements. OEMs can gain competitive advantage by ensuring their devices offer a wide range of security features that give their customers the flexibility they need to secure their unique VoIP network.

[1] Rosenberg, J., Schulzrinne, H., Ca,arillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and Schooler, E., "SIP: Session Initiation Protocol", *RFC 3261*, June 2002

certicom™

General VoIP Architecture

There are many different ways in which a VoIP network can be implemented. For example, in some instances the Media Gateway could be part of the corporate VoIP network, or in other instances it may only reside in the service provider network. For simplicity, this paper will assume the simplified VoIP network presented in Figure 1, however keep in mind that specific networks may vary. From the viewpoint of the developer building a VoIP product, the specific location of the device is not critical from a security perspective.

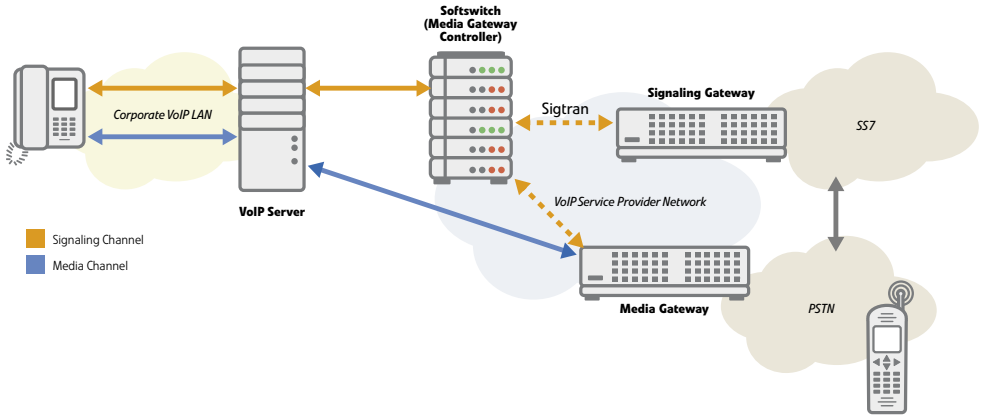

Figure 1: **Simplified VoIP Network**

Potential Threats

VoIP networks are certainly subject to the same long list of potential threats that any IP based network faces. These are well published and discussed elsewhere, and as such will only be touched upon briefly here. These threats reinforce the need for careful planning of a security strategy when developing a product for the VoIP market. Some of the threats that a VoIP network may face include:

- Denial of Service (DoS)
- Man-in-the-Middle attack
- Call Hijacking
- Call Termination
- Password Cracking (brute force and others)
- Server Impersonation
- Eavesdropping
- Exception Packet attacks
- Disturbance Call attacks against endpoints
- Call Leaflet attacks

To protect against these threats, any VoIP security solution needs to perform the following functions:

- **Authentication** – you must be able to authenticate the peer you are communicating with.
- **Data Protection** – You must be able to protect the data being exchanged from being viewed by others
- **Data Integrity** – You must be able to validate that the data received has not been tampered with (you actually received what the other person sent).
- **Non-Repudiation** – You must be able to prove that the message actually came from the other person. This is especially important if the signaling message is being used to generate billing information.

This paper will explore how achieving robust VoIP device security requires applying these security functions to:

- **Securing the signaling channel**
- **Securing the media channel**
- **Securing the device itself**

Securing the Signaling Channel

If you are building a VoIP server, gateway, telephone, or mobile device, the basic security issues are similar with regards to the signaling channel. The signaling protocol (e.g. SIP) traverses an IP network that may or may not be secure. If the underlying IP network is fully secure, one could argue that the signaling between the SIP terminals and the SIP server, for example, doesn't need to be secured. However, the developer of a VoIP terminal can't make such assumptions, and therefore needs to design in a security option. Any VoIP device , such as a VoIP gateway, that connects to an external network (such as the Internet) definitely needs to be considered a potential target for attack, and as such needs to provide security mechanisms.

The signaling channel can be secured relatively easily using a standard protocol such as IPSec[2] or TLS[3]. The choice of which protocol to use could be the subject of an entire paper in itself. To a large extent, this may be dependent on other system level architecture issues. IPSec, for example, is intended to secure a connection running over IP. TLS, on the other hand, is intended to secure a connection running over a reliable transport protocol, such as TCP or SCTP.

Both protocols give you a great deal of flexibility in what you implement and how you implement it. It is not uncommon in e-commerce applications, for example, for authentication to happen in one direction only. For signaling exchanges, in most cases you will want to authenticate in both directions. The user needs to know that the server is actually the server (not a rogue server) and the server needs to make sure that the user is really the user, not someone trying to make fraudulent calls masquerading as the user. Such implementation flexibility needs to be available in your product.

[2] Kent, S. and Seo, K., "Security Architecture for the Internet Protocol", *RFC 4301*, December 2005

[3] 3. Dierks, T. and Allen, C., "The TLS Protocol", Version 1.0, *RFC 2246*, January 1999

From the viewpoint of securing the Sigtran messages, the reader is referred to RFC 3788 [4] for a better understanding of the issues to be considered. Again, either TLS or IPSec can be used in this application, as discussed in RFC 3788.

There has been a great deal written regarding the advantages and disadvantages of IPSec vs. TLS for these applications. For our purposes, it is sufficient to say that either TLS or IPSec can be used, and the specific decisions as to which, needs to be carefully thought out based on the requirements of your product.

Signaling Points

As is illustrated in Figure 1, there are several signaling points in an IP network. These signaling points, including user to access point; access point to network; and network to network, affect how security should be implemented in a VoIP device.

User to Access Point

Users may enter a VoIP network at any one of several points. From the developers standpoint, securing the signaling channel is pretty much the same regardless of the access point. However, there are some factors to consider.

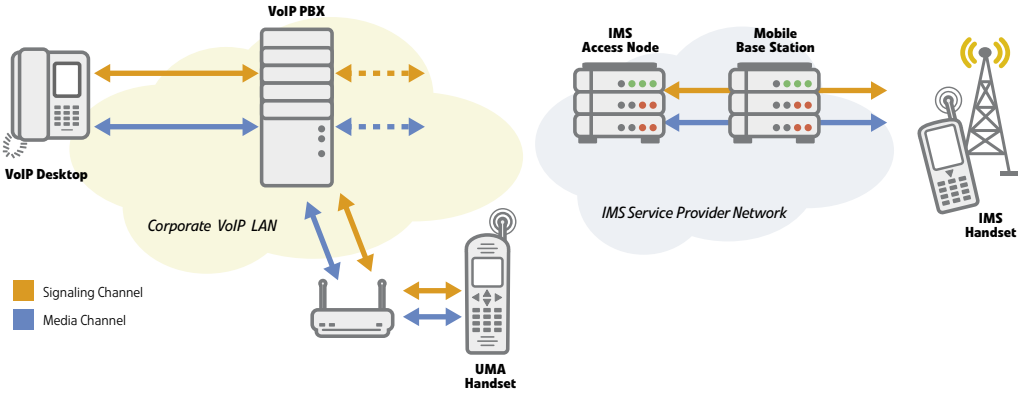

Figure 2: **User Access Points**

Figure 2 illustrates some of the potential user access points. As the developer of the user equipment, your primary concern is what security mechanisms are supported in the access point(s) that your device will support. If the VoIP PBX only supports TLS, then it is of no value to build an IPSec VPN client into your handset for the purpose of securing the signaling channel.

The IP Multimedia Subsystem (IMS) creates some additional challenges for the handset developer. IMS specifications[5] "encourage" the use of IPSec for securing the signaling channel, but acknowledge that TLS may be used, since the SIP specifications require that SIP Servers support the use of TLS. If you are targeting a specific network provider with your product, you need to know what they are using for servers. If you want to sell your product globally, you may find that you need a TLS and an IPSec version, or a dual mode device (ignoring the cost issues of such an implementation for now).

[4] Loughney, J., Tuexen, M., Pastor-Balbas, J., "Security Considerations for Signaling Transport (Sigtran) Protocols", *RFC 3788*, June 2004

[5] 3GPP2, "IMS Security Framework", *S.P0086-B*

Access Point to Network

Within an enterprise network or within a carrier network, there may be a hierarchy of devices handling various aspects of VoIP signaling. In the case of SIP, these may be proxy servers, registration servers, gateways, firewalls, etc. Regardless of the device, the basic requirements are the same – securing the signaling channel using one of the standard mechanisms discussed above.

Network to Network

It is likely that any VoIP network will need to interwork with other voice networks. An enterprise may use VoIP internally, but needs to access the PSTN for all external communications. A VoIP service provider needs to provide interworking with the PSTN to enable users to transparently communicate with non-VoIP users.

In the case of the enterprise example, the VoIP signaling stops at the Gateway between the VoIP network and the PSTN. The gateway will then convert the VoIP signaling into PSTN signaling (e.g. ISDN PRI), appearing to the PSTN as a traditional Private Branch Exchange (PBX). The signaling is only secured up to the gateway and the security does not extend into the PSTN. This is illustrated in Figure 3.

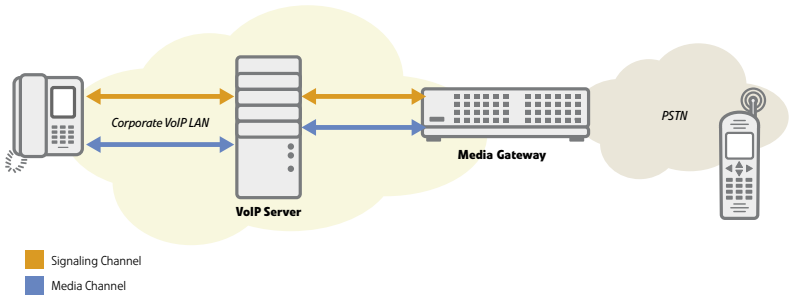

Figure 3: **Enterprise VoIP Network**

In the case of the VoIP Service provider Network, the security needs to be extended a bit further, as shown in Figure 4.

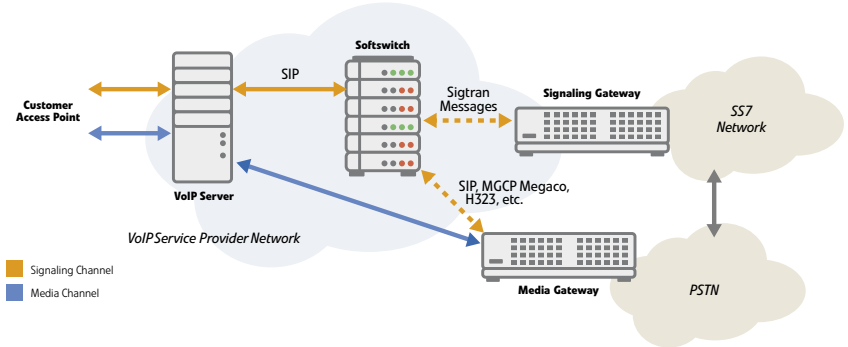

Figure 4: **Service Provider VoIP Network**

In this case, when the call is destined for a user on the PSTN, for example, the Softswitch in the carrier network may need to access the SS7 network to determine proper call routing. In this case, SS7 messages are passed using the SIGTRAN protocol suite,[6] which is essentially a mechanism for passing traditional SS7 messages over an IP

[6] Ong, L., Rytina, I., Garcia, M., Schwarzbauer, H., Coene, L., Lin, H., Juhasz, I., Holdrege, M., Sharp, C., "Framework Architecture for Signalling Transport", RFC2719, October 1999

network. These Sigtran messages also need to be secured, as they form the basis for the ultimate call setup and billing.

Securing the Media Channel

VoIP devices normally use the Real-time Transport Protocol (RTP) [7] to handle the media streams. RTP does not provide any mechanism for securing the media stream. Traditional security protocols such as IPSec could be used, but in most cases the required QoS may be difficult to achieve (see Performance Considerations below). Due to the tight requirements on performance of media streams, a small, efficient protocol is needed to handle the security. The Secure Real-time Transport Protocol (SRTP)[8] has been developed to specifically address the needs of VoIP media stream security.

SRTP provides confidentiality, message authentication, and replay protection to the RTP traffic and to the control traffic for RTP, the Real-time Transport Control Protocol (RTCP).

SRTP is designed to be efficient, adding minimal overhead to the RTP and RTCP packets. It also uses minimal memory for keying and replay lists, and can be implemented in a relatively small code space. For these reasons, SRTP seems to be the preferred mechanism for securing the media channel. Please refer to the SRTP RFC[8] for more details on the features, functions and issues associated with SRTP.

Aside from the traditional security choices of symmetric (private) vs. asymmetric (public) cryptography, crypto algorithm selections, etc, the developer also needs to make decisions regarding issues associated with keying. In the case of IPSec, for example, UMA (and IMS) make use of IKEv2 for key exchange.

For securing the media channel, several keying mechanisms are possible, but the currently popular implementation is to use the Session Description Protocol[9] with the proposed extensions for security descriptions.[10] This enables keys to be exchanged, but those keys must be protected, and the mechanisms in the proposed extensions do not provide that protection, and rely on the use of a secure protocol such as IPSec or TLS to protect the SDP messages containing the keys.

Securing the Device

We have looked at securing the signaling channel and securing the media channel. However, many vendors are finding it increasingly necessary to provide additional layers of security. As more and more connected devices are deployed, it is becoming increasingly important to be able to remotely provision those devices, and remotely update the code base, either with new versions of existing software or with software that adds new applications and services. This is true in the VoIP market, especially as we move towards IMS (IP Multimedia Services).

[7] Schulzrinne, H., Casner, S., Frederick, R., "RTP: A Transport Protocol for Real-time Applications", *RFC 3550*, July 2004

[8] Baugher, M., McGrew, D., Naslund, M., Carrara, E., Norrman K., "The Secure Real-time Transport Protocol", *RFC 3711*, March 2004

[9] M. Handley, V. Jacobson, "SDP: Session Description Protocol", *RFC 2327*, April 1998.

[10] Andreasen, F., Baugher, M., and Wing, D., "Session Description Protocol Security Descriptions for Media Streams", draft-ietf-mmusic-sdecriptions-12.txt, September 2005

As users subscribe to new services, it is often necessary to download client software to enable the use of that service. It is a vital part of the overall security process to ensure that the software being downloaded is valid. Likewise, you want to verify at boot time that the image you are loading is the same as the verified image you originally installed (ensuring that it wasn't maliciously altered). The same scenario applies when updating software or provisioning the device.

To this end, three processes are available and becoming more widely used: code signing, trusted boot and secure provisioning.

Code Signing

Code signing is the process of digitally signing files so that their authenticity can later be verified. The process of signing a file is generally straightforward. Signing a file consists of verifying the signing certificate, calculating a message digest on the file using a hashing algorithm, calculating the signature using an asymmetric key algorithm, and then writing the resulting data into a standard file format.[11]

Figure 5: **Code Signed Data Content**

Trusted Boot

The implementation of a trusted boot process is designed to secure devices against unauthorized usage, malicious code and unverified software updates.
It typically uses digital signatures and cryptographic hashing to validate the origin and integrity of the software image that is loaded during boot. If the image cannot be validated, the boot process can be modified according to a policy appropriate for the device.

The first code to run on a device at power-up must be trusted, or known to be intact and authentic. Normally this is done by placing the early boot code into either locked flash or ROM, such that once programmed, the memory cannot be modified. This establishes the Root of Trust (ROT).[12] The combination of small, efficient cryptographic primitives and hardware to ensure that the early boot firmware is immutable is all that is required to create a platform that boots securely.

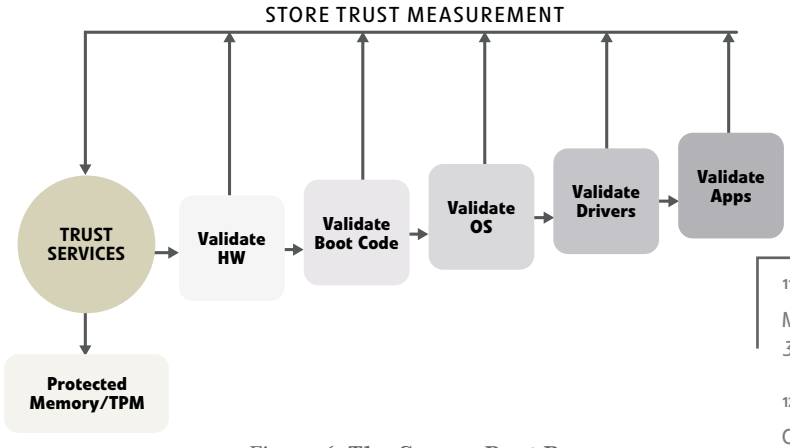

Figure 6: **The Secure Boot Process**

[11] Housley, R., "Cryptographic Message Syntax (CMS)", *RFC 3853*, July 2004

[12] Trusted Computing Group, *https://www.trustedcomputinggroup.org*

Once the ROT has been established, the hardware can be validated. The hardware can then be used to establish the fact that the boot code is valid, which can be used to verify the operating system code, which can be used to validate the system drivers, and then applications can be validated by building against the established trust of all the other components. Oftentimes trust may be established in a single step, with pre-boot code (the ROT) measuring the entire system image, an image that contains operating system code, drivers, file systems, and application code.

Assuming that the image has been signed, the process for verifying the image is straight forward. First, the public key in the CMS data block is verified using the secured hash of the public key located in the initial root of trust.

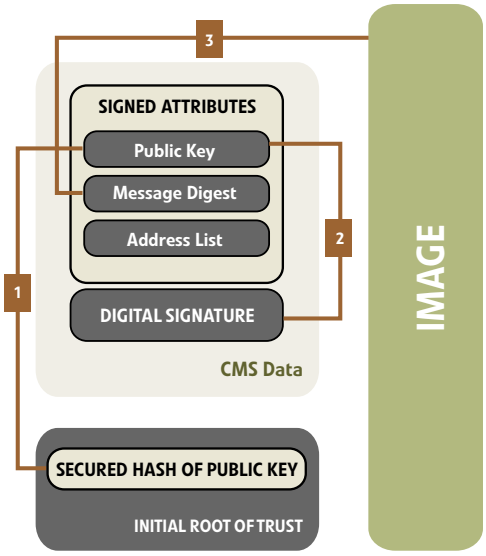

Figure 7: **Verifying the Image**

The digital signature is then verified using the verified public key. At this point, the signed attributes in the CMS can be trusted.

The final step is to verify the image, using the address information and the message digest from the CMS.

Secure Provisioning

Secure provisioning in another important piece of the security puzzle – one that is critical to protecting service provider revenue. The methodology used is similar to secure boot in that configuration files should be cryptographically validated with a certificate based signing scheme. Moreover, to prevent potential theft of service, prudent service providers should insist on locking configuration images to the hardware via a MAC address or some unique hardware attribute via an encryption scheme.

Performance Considerations

In general, the performance of a secure connection on the signaling channel should not pose too many problems, especially for the client side of the connection. After all, the signaling messages are relatively short, and do not occur very often. Assuming that the entire security channel does not need to be established every time the user makes a call (this is a design consideration, but should be fairly obvious in all but the most extreme cases), performance should not be an issue.

However, as NIST points out in Special Publication 800-56,[13] this may not be the case for the media channel. User experience over many years with the PSTN has set our

[13] Kuhn, D. Richard, Walsh, Thomas J., and Fries, Steffen, "Security Considerations for Voice Over IP Systems", *National Institute of Standards and Technology, Special Publication* 800-58

expectation that any VoIP communications should have equal or better performance. In section 3.1 of the NIST document, there is an excellent discussion of one important element of the VoIP system – Jitter. Jitter is the amount of time it takes for the voice to reach the other party. In the PSTN, this is about 150ms (for domestic calls). Adding in all the various elements needed to digitize, transmit, and decode the voice packet, we are left with less than 50ms for security overhead and packet queuing.

This highlights the need for highly efficient crypto algorithms. At the same time, crypto strength needs to be carefully monitored. As processor power increases rapidly (Moore's Law), the strength of the crypto needs to keep pace. The National Security Agency (NSA) recently published their "Suite B" requirements for crypto algorithms (see *http://www.nsa.gov/ia/industry/crypto_suite_b.cfm*), to be used in all non-classified government applications.

Selecting more efficient crypto algorithms can yield significant benefits in performance and security. Key size is directly related to level of security, but inversely related to performance. Using 256 bit Elliptic Curve keys yields the same level of security as 3,072 bit RSA keys, but with much stronger performance (see the NSA web site at *http://www.nsa.gov/ia/industry/crypto_elliptic_curve.cfm* for more details.) All of the protocols discussed in this paper, including IPSec and SSL, can be implemented using Elliptic Curve Cryptography (ECC) to gain performance benefits over traditional RSA.

Another option is to utilize hardware based crypto capabilities. Hardware based encryption can be considerably faster than software based implementations, but this may also yield potentially higher product cost. The developer needs to ensure that the security architecture being employed can easily and cleanly support the integration of hardware crypto capabilities.

A clean low-level abstraction layer is very important when integrating higher-level security protocols and functions because it paves the way for code re-use. Porting security from one chip to another should be easy – and not require weeks of re-working platform specific application code.

Certicom Security for VoIP

To provide a strong foundation on which to achieve robust VoIP security, Certicom Security for VoIP provides developers with the tools they need to quickly and cost-effectively add strong security to their VoIP devices. The solution includes the Certicom Security Architecture and Certicom CodeSign, with the following components:

- SSL and IPSec protocol modules
- Embedded Trust Services (ETS) for secure key storage and management, as well as for implementing Trusted Boot and Secure Provisioning
- A code signing application for secure software and firmware updates

- A common API that sits between the security services or applications and the cryptographic providers maximizing portability and code re-use in products with different chipsets.
- Board support packages (BSPs) to expose hardware cryptographic providers in leading processors

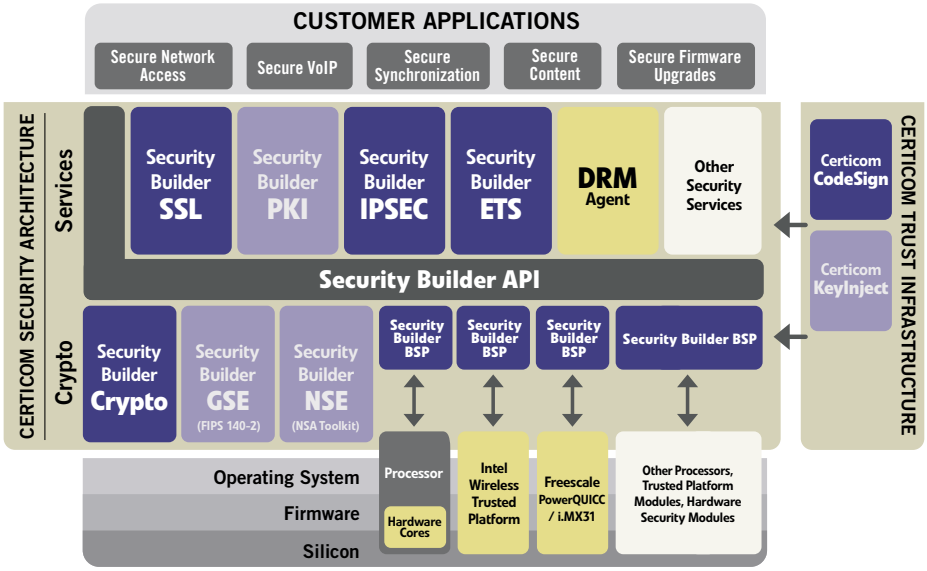

Figure 8 : Certicom Security for VoIP

Conclusion

Securing a VoIP device is a multi-level process, with several options and implementations possible. From the viewpoint of a developer, the selection of a security architecture needs to take into account the real likelihood that the security solution will migrate over time, as new requirements and applications are introduced. A flexible, extensible solution, such as Certicom Security for VoIP is required to ensure the ease of adapting to ever changing requirements.

certicom™

Certicom White Papers

To read other Certicom white papers, visit www.certicom.com/whitepapers.

The Inside Story

Many Happy Returns: The ROI of Embedded Security

Wireless Security Inside Out (authored by Texas Instruments and Certicom)

Welcome to the Real World: Embedded Security in Action

Sum Total: Determining the True Cost of Security

The Elliptic Curve Cryptosystem for Smart Cards

Elliptic Curve DSA (ECDSA): An Enhanced DSA

Formal Security Proofs for a Signature Scheme with Partial Message Recovery

Postal Revenue Collection in the Digital Age

An Elliptic Curve Cryptography Primer

ECC in Action: Real World Applications of Elliptic Curve Cryptography

Using ECC for Enhanced Embedded Security: Financial Advantages of ECC over RSA or Diffie-Hellman

Good Things Come in Small Packages: Certicom Security Architecture for Mobility

Using Digital Signatures to Cut Down on Bank Fraud Loss

Preparing for Unlicensed Mobile Access

Building Trust for Embedded Systems

Making the Grade - meeting government security requirements – Suite B

Current Public Key Cryptographic Systems

Injecting Trust to Protect Revenue and Reputation

certicom™

About Certicom

Certicom protects the value of your content, software and devices with government-approved security. Adopted by the National Security Agency (NSA) for classified and sensitive but unclassified government communications, Elliptic Curve Cryptography (ECC) provides the most security per bit of any known public-key scheme. As the undisputed leader in ECC, Certicom security offerings are currently licensed to more than 300 customers including General Dynamics, Motorola, Oracle, Research In Motion and Unisys. Founded in 1985, Certicom's corporate offices are in Mississauga, ON, Canada with worldwide sales headquarters in Reston, VA and offices in the US, Canada and Europe. Visit www.certicom.com

Contact Certicom

Corporate Headquarters

5520 Explorer Drive, 4th Floor
Mississauga, Ontario
L4W 5L1
Tel: +1-905-507-4220
Fax: +1-905-507-4230
E-mail: info@certicom.com

Sales Offices

Worldwide Sales Headquarters
1800 Alexander Bell Dr., Suite 400
Reston, Virginia 20190
Tel: 703-234-2357
Fax: 703-234-2356
E-mail: sales@certicom.com

Europe
Golden Cross House
8 Duncannon Street
London WC2N 4JF UK
Tel: +44 20 7484 5025
Fax: +44 (0)870 7606778

Ottawa
84 Hines Road, Suite 210
Ottawa, Ontario
K2K 3G3
Tel: 613-254-9270
Fax: 613-254-9275

Engelska Huset
Trappv 9
13242 Saltsjo-Boo
SWEDEN
Tel: +46 8 747 17 41
Mobile: +46 70 712 41 61
Fax: +46 708 74 41 61

U.S. Western Regional Office
393 Vintage Park Drive, Suite 260
Foster City, CA 94404
Tel: 650-655-3950
Fax: 650-655-3951
E-mail: sales@certicom.com

www.certicom.com