White Paper

BroadSAFE Enhanced IP Phone Networks

Secure VoIP Using the Broadcom BCM11xx IP Phone Technology

September 2005

Executive Summary

Voice over Internet Protocol (VoIP) enables telephone calls over a computer network. VoIP converts telephone voice signals into a digital signal that travels over the Internet. Industry trends confirm that VoIP usage is rapidly increasing, and this elevates the level of security concerns associated with the technology.

Deployment of IP-enabled devices on corporate and public networks has resulted in new challenges for network managers, particularly in the realm of security. Until recently, VoIP usage has primarily been enterprise-based where, in comparison to the public Internet, the number of users is small and the environment tightly controlled, therefore, security concerns have been limited.

With the marked growth and developmental progress of VoIP on the public Internet, there is a correlative increase in risk for data traffic sniffing and device spoofing attacks. Even in the enterprise, the overriding corporate concern is the unauthorized use of the network by both outsiders and employees.[1]

How do we keep the mailroom employee from accessing confidential voice mails belonging to the CEO? Unprotected networks are susceptible to audio capture (eavesdropping on phone calls), identity theft where a hacker may spoof SIP messages and IP addresses to emulate another client device, and Denial of Service (DoS) attacks such as packet/broadcast storms, worms, and viruses which render the network unusable. DoS attacks are especially problematic because the intrusion is characterized by an explicit attempt to prevent legitimate users of a service from using that service, and, depending on the nature of your enterprise, this can effectively disable your organization.

How can we secure the endpoints on the network so that:

- Devices will only receive packets from authorized or trusted sources?
- Only authenticated users may communicate in the network?
- Communications between endpoints or between a server and an endpoint are private and the data integrity is maintained?

The intent of this paper is to help the reader understand how the use of the BroadSAFE™ core embedded in the BCM1103 and BCM1104 IP phone chips provide the foundation for strong security in IP Phone networks.

Overview

BroadSAFE™ Technology Overview

BroadSAFE is a general term used to describe the security technology implemented across a wide variety of Broadcom products. There are currently five different BroadSAFE implementations available, with each providing distinct levels of security services. The BroadSAFE implementation used in both the BCM1103 and BCM1104 is named µHSM or micro Hardware Security Module. This paper is focused on the security capabilities of the µHSM and its application in the IP Phone Networking space.

Broadcom developed the µHSM to address the emergent requirement for hardware protection of private keys, and the need to manage keys in a construct that can scale to satisfy the demands of very large organizations. Certificates (keys) form the basis for any secure protocol by providing the credentials of a particular device on the network. When these credentials are stored in software, they can be copied, modified or spoofed by a rogue device on your network, exposing the network to attacks.

As secure protocols like certificate-based Extensible Authentication Protocol/ Transport Level Security (EAP-TLS) and TLS-based Session Initiation Protocol (SIP) messaging are adopted, IT managers can respond to the vulnerability associated with storing certificates in software, and the challenge of managing certificates across a large enterprise. Broadcom's µHSM addresses each of these requirements by providing a hardware key usage and storage environment as well as a secure endpoint that enables secure remote certificate management.

µHSM Core

Every µHSM core contains a 16-bit RISC processor, One Time Programmable (OTP) memory, ROM, public key (RSA, DSA, DH) engines, a 3DES engine, HMAC-SHA-1 engine and a random number generator. These components enable the µHSM core to establish a security boundary outside of which keys are never exposed in the clear. Keys are delivered to the µHSM in an encrypted form and decrypted inside the secure boundary of the µHSM, where they can be used and managed. For more details on the µHSM core, please refer to the micro Hardware Security Module Design Specification (HSM-TI-10x-R) stored in your docSAFE account.

Initialization

Each µHSM module includes a block of OTP memory used to store the values of two unique private keys that are examined when the µHSM is initialized:

- A 160-bit Digital Signature Algorithm (DSA) identity key
- A 256-bit DH device confidentiality key

These two keys are “hardened” into the device and establish the foundation for trusted client device and secure “no touch” network management. Storing these keys in hardware provides manifold advantages over storing them in software. Software is accessible and fluid. It can be changed, copied, debugged, and inspected, leaving keys susceptible to key-finding attacks. The private keys stored in the µHSM however, are never exposed outside of the µHSM core – not to Broadcom, not to the OEM, not to anyone. Only associated public keys can ever be dispatched from the µHSM core.

The OTP memory is programmed during final test at Broadcom. There is no need for in-field programming. Every BCM1103/BCM1104 is shipped with unique keys programmed and verified. These values are listed in Table 1.

Table 1: BCM1103/BCM1104-Unique Keys

Key Name	Description
Identity Key (Kdi)	The 160-bit private key of a DSA Key. The key pair is generated on-chip and the secret is burned into the OTP. The public value is discarded, but can be regenerated on request.
Confidentiality Key (Kdc)	The 256-bit private key of a 2048-bit Diffie-Hellman Key. The key pair is generated on-chip. The private key is burned into the OTP. The public value is discarded, but can be regenerated on request.
Device Configuration (Dcfg)	Register bits can be mapped to blocks on the host chip to enable/disable features on the chip, and to configure µHSM behavior. The BCM1103/BCM1104 does not have the option of enabling/disabling features using this register.
Device Authorization (Dauth)	This value contains a hash of the public key of an entity that can change the device configuration bits. Since the device configuration bits are programmed in OTP, the bits aren't physically changed, but the value written by an authorized entity will override the Dcfg bits (This value is not used in either the BCM1103 or BCM1104).

Accessing the µHSM

All µHSM features are accessible through the BroadSAFE µHSM API provided by Broadcom. This API is included with the BCM1103/BCM1104 SDK. Included applications can replace existing software implementations of cryptographic functions with calls to the µHSM API. BroadSAFE µHSM API documentation is available using your docSAFE account.

µHSM Security Features

Designing a secure IP phone network using the BCM1103/BCM1104 device with embedded µHSM provides four distinct advantages:

- Public key engines inside the µHSM core can be accessed to offload public key operations by applications running on the host processor. This frees up the host processor for additional tasks, and may help eliminate any critical timing paths related to call setup.
- Two unique private keys programmed in OTP memory securely authenticate network devices. These keys are burned into each µHSM core during final testing. One key establishes identity and the other encrypts data that only the µHSM can decrypt. Device identity is established using one of these keys and the DSA. This identity key can be used with the client verification message in a TLS initialization session to sign a hash of all previous messages.
- The µHSM core provides a secure key storage and usage environment for private key operations.
- Designing around a µHSM enables secure, centralized key management.

In addition to hardware key protection, the µHSM also contains logic to enforce key expiration, revocation, usage and other key-based policy decisions. As keys expire, or are revoked, new keys must be distributed to end devices in a secure manner. The µHSM provides a trusted end point where the management server, housing a complete Hardware Security Module, handles key generation, backup, key-based policy setting, and secure key distribution. All of these advantages are distinct and independent, and can be implemented using a phased approach.

Cryptographic offload

One of the easiest techniques that can be used to take advantage of BCM1103/BCM1104 µHSM functionality is to offload public key operations to the public key engine contained in the µHSM. These engines can be used by any application to offload computationally expensive operations from software. The µHSM block was designed to be a small footprint, low-gate-count design, so performance from these engines is not comparable to traditional hardware cryptographic accelerators.

The ability to offload these operations to hardware frees up the host processor for other tasks. The public key engine can perform about 10 public key operations per second, and supports RSA, RSA-CRT, Diffie-Hellman, and DSA. µHSM offload capabilities can be accessed using the Broadcom µHSM software reference library.

In addition to the crypto engines contained inside the µHSM block, the BCM1103/BCM1104 also houses integrated AES and SHA-1 engines capable of 10Mbps sustained throughput. The AES engine supports 128-, 192- and 256-bit encryption in CTR, CBC and ECB cipher modes. The SHA-1 engine supports both pure SHA-1 hash as well as HMAC-SHA-1. These blocks operate independently of the µHSM block and are used primarily for encrypting and authenticating real-time media streams.

Robust Hardware-Based Authentication

Device identification lies at the heart of any security architecture. Once the identity of a device on the network has been compromised, a hacker can exploit that identity to access corporate networks and conduct transactions while posing as a valid network entity. If device credentials are duplicated on a corporate network, which is the fundamental problem with storing certificates in software, it would be easy to access sensitive information contained in voice mails or call logs. The µHSM enables you to store device credentials using dedicated hardware protection, thus ensuring that devices on your network "are who they say they are".

Using BroadSAFE With EAP-TLS

One method to ensure that only authenticated devices exist on the network is by using the EAP-TLS protocol. The µHSM secures X.509 certificates used in EAP-TLS by storing the certificate on an IP phone, encrypted with a key that can only be decrypted inside the µHSM.

During the manufacturing process, the µHSM is queried for a confidentiality key (Kdc). A manufacturer-provided certificate server generates a device certificate, formats the private key as part of a Discrete Logarithm Integrated Encryption Scheme (DLIES) message according to IEEE1363bis, and encrypts the message with Kdc. The certificate, along with the encrypted private key, is then installed in flash memory on the phone in a non-EAP network environment.

When the phone is installed on the network, software transports the encrypted private key of the certificate into the µHSM. Once the key is decrypted and resident in the µHSM, that certificate now resides in a hardware-protected boundary and can be used for network access in EAP-TLS or other similar protocol (see Figure 1). Additional certificates enabling different features can then be installed on the phone once network access is authorized.

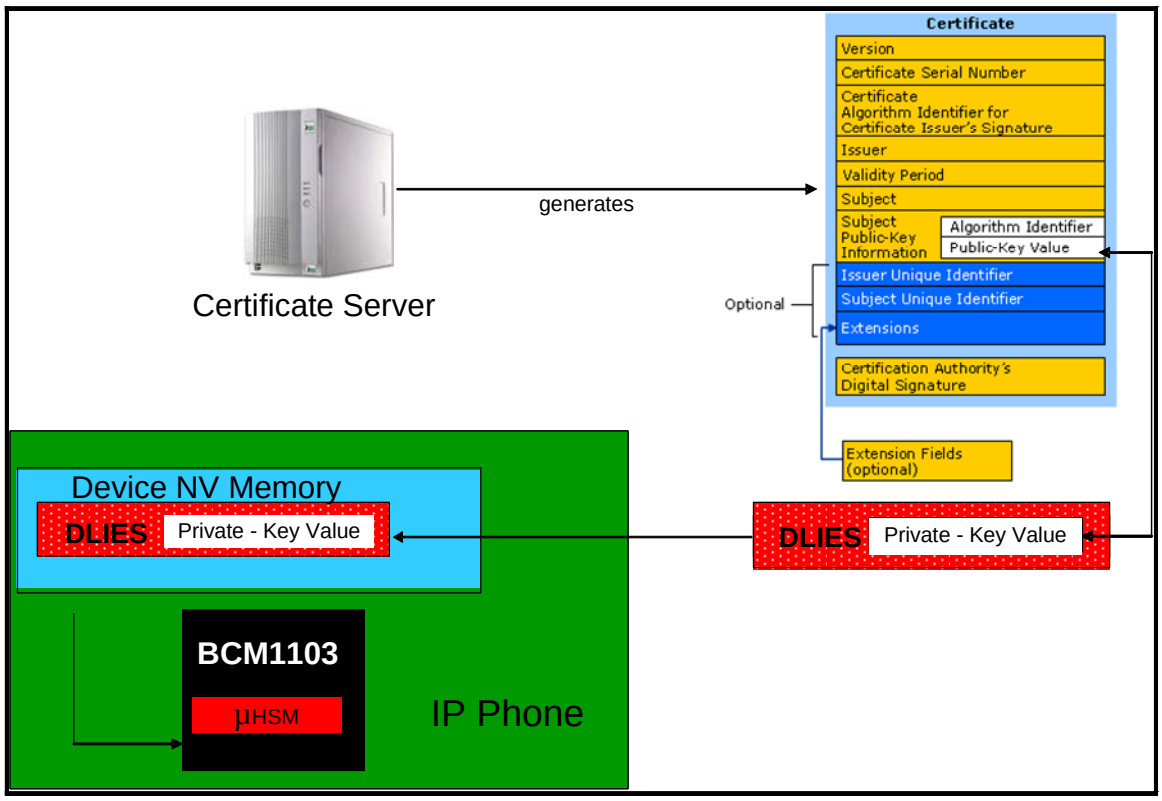

Figure 1: Certificate Server Key Generation and Delivery

Alternate Authentication Strategies

It is possible to create an authentication strategy using the µHSM's capability to sign challenge data from an authentication server. This is an option for applications where system cost is at a premium and client software must be minimized to reduce memory costs. Instead of implementing the TLS protocol on the client, an alternative authentication strategy can be employed (see Figure 2).

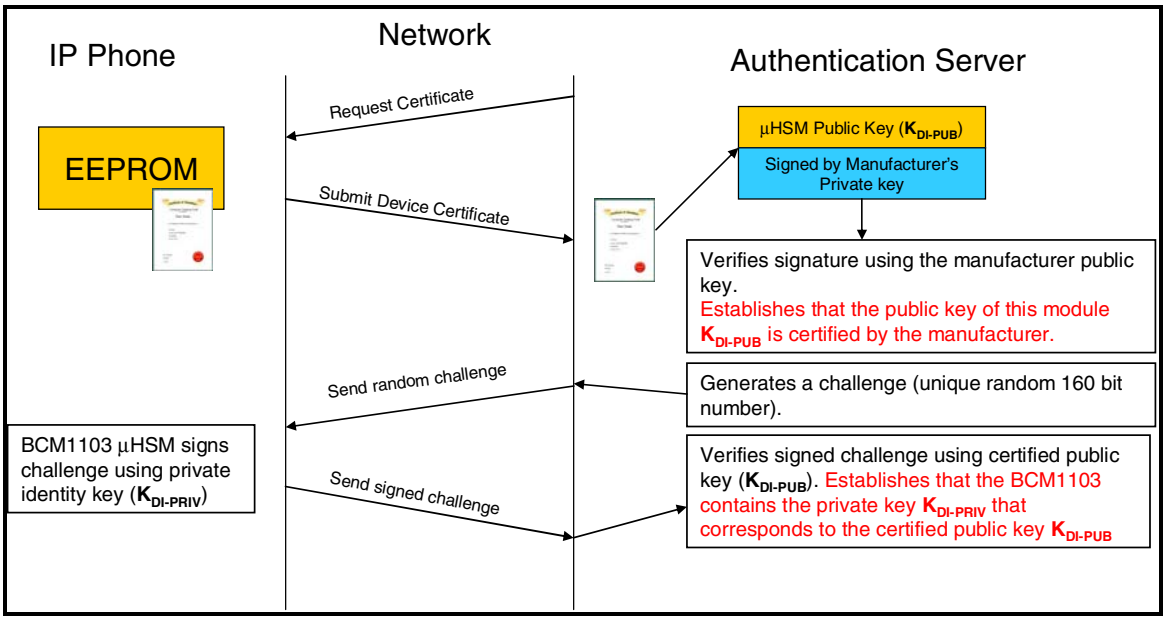

Figure 2: Alternate Authentication Strategy

Using this approach, a certificate, signed by the OEM, is installed on the IP phone. During authentication, the phone is queried for the certificate that the authentication server uses to verify the OEM signature. The server then authenticates the phone by sending it a random challenge that is signed by the µHSM. The signature is verified using the public key in the certificate. There is a minimal amount of code required on the client end for this type of authentication.

User Authentication

In addition to hardware-based device authentication, the BCM1103/BCM1104 µHSM provides the capability to authorize a network user. A user can enter a PIN via the keypad or supply credentials via the smartcard. These entries are input directly to the µHSM on GPIO lines. The µHSM hashes the input data and signs it with an identity key. This information can then be sent to a remote access server for authentication.

Key Management and Usage

Once a network device is securely identified, it must be configured and managed. An initial configuration typically involves installation of a device certificate and enrollment of the device on the network. If the device certificate has no expiration, then an enforceable method for updating the device certificate, and any subsequent certificates, must be in place.

These certificates authorize access to company databases, grant toll privileges and restrictions, or indicate the status of security patches and virus definitions. It is critical that these certificates securely transfer to the VoIP phone, without burdening IT with having to physically visit each device in order to install updated certificates. µHSM enables hardware-based secure communications using a certificate server to install certificates across the enterprise from remote locations.

Broadcom employs a light-weight, proprietary but open protocol for communications between a Key Management Server (KMS) and µHSM called Key Delivery Protocol (KDP). This is a simple client-server based protocol that wraps key material according to DLIES.

A KMS contains a hardware security module. The HSM provides secure key management to generate the cryptographic keys used in certificates, set the capabilities and security limits of keys, implement key backup and recovery, prepare keys for storage, and perform key revocation and destruction. Once keys are generated inside the protected HSM boundary, the KMS can establish a secure link between itself and a particular µHSM client, and install the keys or certificates on the client device.

KMS products from nCipher ship with support for the KDP protocol. For more information, please visit http://www.ncipher.com.

Secure Device Authentication at the Call Manager

It is possible to transfer the authentication function into the call manager by adding a key management and cryptographic offload module. Broadcom provides a FIPS-140-2 level 3 certifiable solution using the BCM5862 Security Processor with an embedded µHSM paired with a BCM5890 Secure Application Processor.

Keys can be generated and managed inside the secure boundary of the BCM5890. For example, the BCM5890 can generate session keys and distribute them securely to client devices using KDP once call setup has completed. Cryptographic operations can be offloaded to the high-performance BCM5862, with keys moving in and out of the BCM5862 through a secure serial channel to the BCM5890. For more information, contact your Broadcom representative.

Conclusion

The µHSM core embedded in the BCM1103/BCM1104 is a very flexible, hardware-based policy engine that uses advanced security features not available in competing devices. These features can be accessed using a variety of methods:

- Cryptographic offload
- Hardware-based authentication
- User authentication
- Certificate management

The secure authentication enabled by µHSM allows you to safeguard network assets, prevent potentially malicious devices from accessing your network, and enables "touch-free" management of µHSM secured endpoint devices.

Since the majority of VoIP security concerns surface after VoIP has been deployed, designing with the BCM1103/BCM1104 µHSM core gives you a hardware-based security platform, in addition to best-of-class VOIP features, allowing you to provide advanced security solutions now and in the future.

References

1 *Trends and Spending Plans for Security Appliances: Are We Ready for VoIP? (Instat Report by Reed Electronics Group, August 2005)*

Phone: 949-450-8700
Fax: 949-450-8710
E-mail: info@broadcom.com
Web: www.broadcom.com

BROADCOM CORPORATION
16215 Alton Parkway, P.O. Box 57013
Irvine, California 92619-7013

BroadSAFE-WP100-R 09/23/05