SafeNet HSMs for DNSSEC

SOLUTION BRIEF

Features and Benefits

- Two of the three biggest DNS providers trust SafeNet HSMs to protect and accelerate digital signatures for DNSSEC
- Combines strongest cryptographic security with highest performance and availability
- Broadest array of HSMs for any DNSSEC requirement
- Easy to integrate with well documented API's including PKCS#11, Java, MS CAPI
- Supports DNSSEC and OpenDNSSEC
- World-class Support and Documentation
- Most worldwide HSMs deployments for PKI

For root, top level domain and enterprise level DNS hierarchies, SafeNet HSMs combine the strongest cryptographic security with the highest performance, reliability and ease of integration for rapid and affordable DNSSEC implementation.

Security Issues with DNS

At the pinnacle of the Domain Name System (DNS) hierarchy server clusters carry the DNS root zone data. Web applications like eCommerce, SaaS, social networking, and even email rely on DNS. Unfortunately, the DNS contains unsecured and vulnerable cashing name servers that are easy targets for hackers to hijack Web traffic containing sensitive data. With cache poisoning an attacker inserts a fake address record into a DNS caching server. The caching server stores the fake record, thus "poisoning" the cache unbeknownst to users who think they are dealing with a legitimate site. This vulnerability has spawned an immediate need for security, as security researcher Dan Kaminsky brought to worldwide attention in the summer of 2008.

Why DNSSEC is the Answer

The solution recommended by the DNS developer community is Domain Name System Security Extensions (DNSSEC), which uses digital signatures and public-key cryptography to allow Web servers to verify their website domain names and corresponding IP addresses. DNS root zones are in urgent need of being digitally signed as delay is detrimental to the ongoing integrity of the Internet, eCommerce and Web applications. Signing the zones would in effect configure the caching name servers to become security aware. DNSSEC is viewed as the best way to bolster the DNS against vulnerabilities such as cache poisoning attacks. In fact, security researcher Dan Kaminsky recommends widespread deployment of DNSSEC. The world is paying attention and DNSSEC has been deployed on top-level domains operated by Sweden, Puerto Rico, Bulgaria, Brazil, Portugal, Thailand, Namibia, and the Czech Republic to name a few.

Key Management for DNSSEC

SafeNet hardware security modules (HSMs) meet the demanding requirements for robust security and availability required to ensure integrity of the domain name space. Like any other security model relying on public key cryptography, it is imperative that private DNSSEC signing keys are kept secure. By definition, the public key can be made widely available; it does not need to be secured. However, if the private key is compromised, a rogue DNS server can masquerade as the real authoritative server for a signed zone. This is where hardware security modules (HSMs) come into play.

HSMs are dedicated systems that physically and logically secure the cryptographic keys and cryptographic processing that are at the heart of digital signatures. HSMs secure the DNS server so the generation of keys, the storing of the private key, and the signing of zones is performed on a DNS server that physically secure and whose access is restricted to essential personnel only. HSMs also allow the secure storage of a backup private key copy in a centralized, hardened device.

SafeNet HSMs: A Case for Higher Expectations

SafeNet has been trusted for more than twenty years to protect more digital identities than any other hardware security module in the world. Following are several reasons why banks, retailers, large enterprises, government agencies and educational institutions are choosing SafeNet:

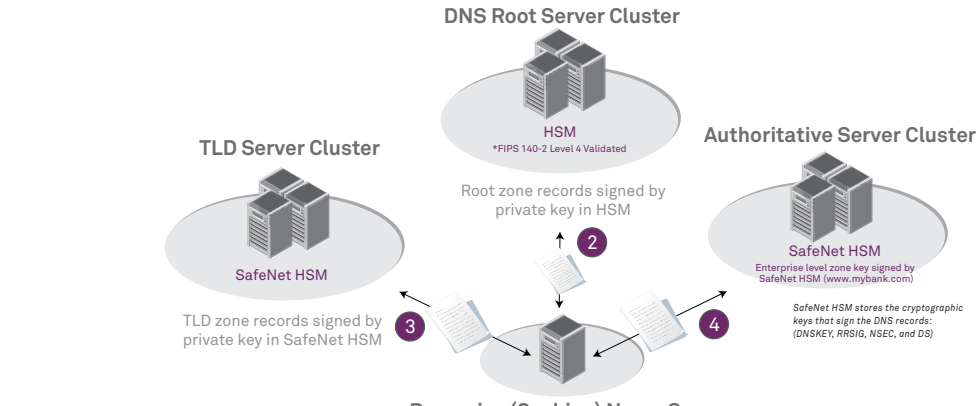
- SafeNet HSMs integrate with the leading DNS platforms, including OpenDNSSEC, BIND, FreeBSD and Linux;
- SafeNet HSMs provide trusted key security used to sign the DNS packets and create a secure DNS infrastructure with high-performance solutions, up to 7,000 operations per second, for both Zone Signing Key (ZSK) and Key Signing Key (KSK) scenarios;
- SafeNet HSMs feature local and remote key management control for flexibility and ECC key limit size constraints for reduced crypto footprint, allowing for a smaller impact on the DNS packet;
- SafeNet HSMs are easy to integrate into any security environment with well documented APIs such as PKCS#11, OpenSSL, Java, and MS CAPI, as well as central management consoles for easy and rapid setup;
- All digital signing and verification operations are performed within the HSM to deliver the highest levels of performance, availability and security to ensure business processes and systems are running efficiently;
- Stored on hardened and FIPS 140-2 Level 3 and Common Criteria EAL 4+ certified cryptographic modules, cryptographic keys never leave the confines of the HSM; and
- SafeNet HSMs are available in different form factors and performance classes to meet the unique design goals of any cryptographic key deployment - from PCI cards embedded in the server to highly scalable network-attached appliances that can be transparently shared by multiple servers.

In addition SafeNet HSMs support key rollover functions, since DNSSEC keys do not have a permanent lifetime. The chances a key will be compromised, whether through accident, espionage, or cryptanalysis, increase the longer the key is used. Key rollover is the process by which a key is replaced with a new key and associated signatures are updated.

Implementing DNSSEC with Scalability & Robust Processing

A phased approach is recommended when deploying DNSSEC in your organization. Depending on the complexity of your environment, you might want to limit the initial deployment to a small number of domains before you deploy DNSSEC broadly. When responding to queries, the DNS server will respond with additional DNSSEC resource records. This will increase the number of packets on the network and can decrease the maximum query throughput of the DNS server. A DNS server that is performing validation of DNSSEC data can experience an increase in CPU usage. Configuring an HSM to the DNS server ensures that the server has sufficient processing capabilities. SafeNet HSMs can scale to meet the phased approach, but also keep up with the large number of incoming requests for domain name resolution in large zones, and can scale to thousands of signing operations per second.

A Recursive Query Being Secured Using SafeNet HSMs for DNSSEC



1. Client initiates query for www.mybank.com
2. ISP Caching name server starts recursive search at root if no record found in cache.
3. Recursive search referred to applicable TLD by root. If record does not exist in TLD zone query referred to the Authoritative server. (Simplified example – additional zone searches may be required to identify Authoritative Name Server.)
4. Authoritative Server responds with signed DNS zone record
5. Recursive server returns verified IP address for "mybank.com" to DNS client

Contact Us: For all office locations and contact information, please visit **www.safenet-inc.com**
Follow Us: www.safenet-inc.com/connected