White Paper

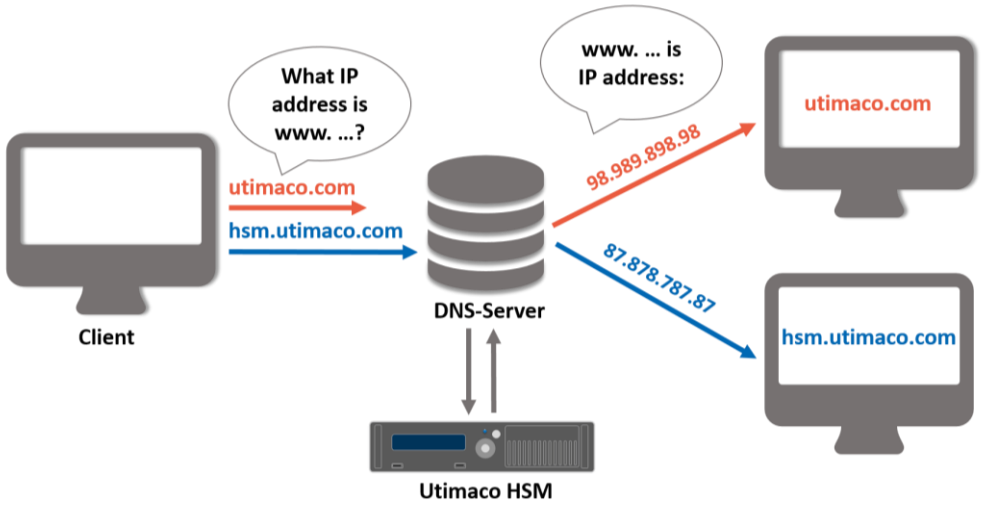
The Importance of Securing DNSSEC with the Utimaco HSM

Introduction

Utimaco is a major provider of a unique device called a Hardware Security Module or HSM. This HSM is a purpose built computing device that generates, secures, stores and manages cryptographic materials, such as certificates and keys. This critical crypto material is stored inside the HSM, protecting it from theft and compromise. Your certificates and keys are your verified and validated unique identity. They represent you on the Internet. As we will see here, letting them fall into the wrong hands can be a disaster. Let us explore why this is important for DNSSEC.

What is DNS or Domain Name Service?

The mechanism used for taking a URL or website name and converting it to an IP address is DNS or Domain Name Service. One common implementation is the Linux Bind server. This service allows a user to request the URL www.google.com and have the internet magically convert that into an IP address and direct your browser to that website. Your computer has configuration information you get when you connect to your local area network or WiFi network that tells your browser and computer which server on the network is your local DNS server. That DNS server IP address is then known to your browser. When your browser received your URL request it passes that request to this DNS server. The DNS server looks at the list of know URL and returns the required IP address and your browser then accesses that website for you. If that URL is not currently known then your DNS server will ask other DNS servers if they know that URL and can provide your DNS server with the required information. This checking and requesting may move through 2 or more DNS servers until the authoritative DNS server – the one that holds the authoritative record of the URL you want – returns the IP address. This normally happens very quickly as the system will cache common URL to IP address relationships and return them to you.



When you access an ecommerce website, the page access is normally done using SSL/TLS and the https://www.url.com with the HTTPS securing the web page communication. However the DNS information exchange is typically done in the clear with no signature or validation. Each DNS server trusts the other DNS servers. In a perfect world this would be fine. But what if someone configured a DNS server to mascaraed as another DNS server. In that case this fake DNS server would respond with a DNS record then return the wrong IP address. Your browser could then connect to the wrong server. The answer to this problem is DNSSEC or DNS Security which can be added to the DNS server and ensure that only valid records from legitimate DNS servers are passed on to you.

What is DNSSEC?

The Domain Name System Security Extensions (DNSSEC) is a worldwide initiative to develop a set of add-on specifications to ensure that the information we transmit through the Internet remains safe and private. DNSSEC technology prevents fraudulent domains, or websites, by creating a unique signature for every domain name. By matching the requesting user with the correct website using this unique signature, we can prevent fake websites from intercepting and exploiting sensitive user data. This feature is especially important when users are redirected to a third-party website to process payment details for an online purchase.

The new gatekeepers of the Internet are the enablers of DNSSEC Signing. Groups of servers all over the Internet store information about domain names in readable open text to be able to direct user traffic. After applying DNSSEC Signing, the DNS data remains readable; but a unique signature proceeds the DNS data transfer to the requesting DNSSEC server. The server then authenticates or rejects the transfer request based on the confirmed identity of the sending DNSSEC server.

DNS and DNSSEC working together can securely resolve an IP address to a fully qualified Domain Name. It also can take a Domain Name and resolve it to the correct IP address. When your network is set up, each of the devices on that network is assigned an IP address. The DNS database has assigned each element a valid name. The DNS server exchanges this information in a domain transfer to other remote DNS servers requesting the information. In the case of DNSSEC mode; the transfer is signed by the authoritative DNS server before it is passed on to the requesting DNS server. The requestor knows that it came from a known good source, because it can verify with the Public Key Infrastructure (PKI) of the originating DNS server.

Utimaco CryptoServer

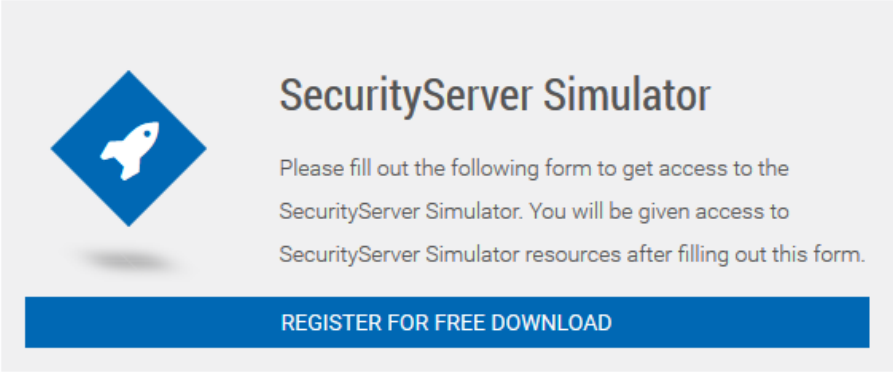
Utimaco provides the “Root of Trust” securely storing the identity of the DNSSEC server. That identity resides inside the Utimaco HSM. All signing operations are performed internal to the HSM so that the key material is not visible in the clear. The Utimaco HSM easily integrates with network devices and DNSSEC via industry standard PKCS#11 or Microsoft CNG APIs.

About Utimaco

Utimaco is a leading manufacturer of hardware security modules (HSMs) that provide the Root of Trust to the IoT. We keep cryptographic keys and digital identities safe to protect critical digital infrastructures and high value data assets. Our products enable innovations and support the creation of new business by helping to secure critical business data and transactions. Founded in 1983, Utimaco HSMs today are deployed across more than 80 countries in more than 1,000 installations. Utimaco employs a total of 170 people, with sales offices in Germany, the US, the UK and Singapore. For more information, visit hsm.utimaco.com

Download the Utimaco Software HSM Simulator to get started immediately learning about HSM devices. It is a FREE fully functioning Software version of the Hardware HSM. The download package includes documentation on our product. Here is the link to register for the download.

https://support.hsm.utimaco.com/hsm-simulator



The Simulator download includes tools for creating user accounts, sample code and libraries for PKCS#11 Microsoft CNG, Java JCE and the Utimaco CXI API to link and test your code. The Simulator will run on a Windows or Linux platform. This is your opportunity to try out the Utimaco HSM technology easily and without initial cost.