White Paper

Securing the IoT - OpenVPN and the Utimaco CryptoServer 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 IoT. As we will see here, letting them fall into the wrong hands can be a disaster. Let us explore why this is important for IoT and OpenVPN.

What is IoT?

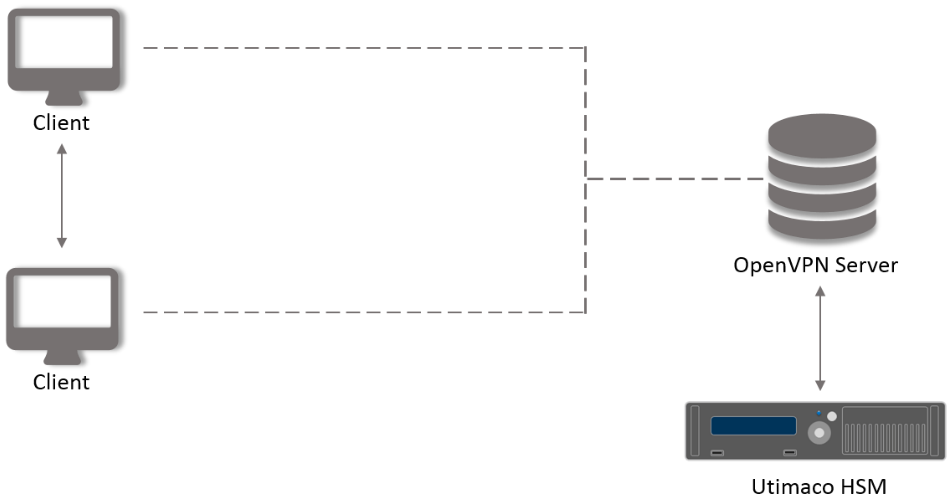
The IoT or the Internet of Things is a vast new frontier for the interconnectivity of a wide array of devices. These devices can be temperature sensors, motion and control elements in process control or a factory system. They can be ECUs in driverless cars on a roadway, Smart Meters in a nation's power grid or oil refining and distribution systems. These devices may ultimately be your home furnace, refrigerator and toaster in a Smart Home environment. These devices need to be secure. Anywhere where a device needs to have access to the internet to receive command and control data or deliver data back to a central location, needs to be secure. This command and control traffic requires signing in order to ensure that the command or response originated with the actual expected device. Each IoT device must be able to confirm the identity of the sender.

IoT devices commonly use Elliptic Curve operations with lower resource requirements than RSA; to not overwhelm the low power IoT devices supporting the security layer. In a networked environment where IoT devices communicate, an HSM is used to create a supply of certificates and keys to distribute to each IoT device. To improve security the HSM can periodically create new certs and keys to replace the previous set. Known as "rolling the keys" this improves security by invalidating old keys and issuing new ones. Most IoT devices exist in local private subnets. While they can communicate with their peer devices on that shared subnet, they need to interconnect over the public internet for monitoring and command control purposes. It is best that this traffic is not visible over the public network. This is where OpenVPN enters the picture. It will link multiple local private subnets over the public internet while concealing the contents of that traffic. It can secure that point-to-point and site-to-site link.

What is OpenVPN?

OpenVPN is an open source software application that implements a virtual private network or VPN creating secure point-to-point and site-to-site connections in a routed or bridged configuration. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable of traversing network address translations NAT and firewalls. OpenVPN allows peer devices to authenticate each other using a pre-shared secret key, certificates or user name and password. The OpenVPN server configuration provisions authentication certificates for every connecting client with signatures and certs provided by a Certificate Authority (CA). The CA can be a public one or one that the organization sets up and operates locally. These certs can be stored directly on the OpenVPN server machine. Since the certs are visible files they could become compromised. A superior solution is to store key material inside an Utimaco HSM. When using the Utimaco HSM; access to the certs is secure and accessible only inside the HSM via the PKCS#11 API. OpenVPN can then operate with no worries as your certs are safe.

OpenVPN has a Client-Server architecture. The Server operates a connection nexus for its assigned local networks. This is typically an internal corporate infrastructure. The Server holds a certificate which identifies its endpoint. The Client issues a certificate that it uses to identify itself to the Server. Using these certs they mutually identify and authenticate each other. Then a Tunnel is formed between them. The Server creates and manages routes and subnets to present to the Client. The Server would use an HSM to hold all of the know certs issued in its domain. The Client could use either a local file or Smart Card to hold its issued certificate. When the exchange completes successful, the Client connects to the Server side network. Traffic can now move safely from the Client local network over the OpenVPN tunnel to the Server side where it can be routed to other devices, some of which could be on other Client initiated Tunnels to other sites.



Utimaco CryptoServer

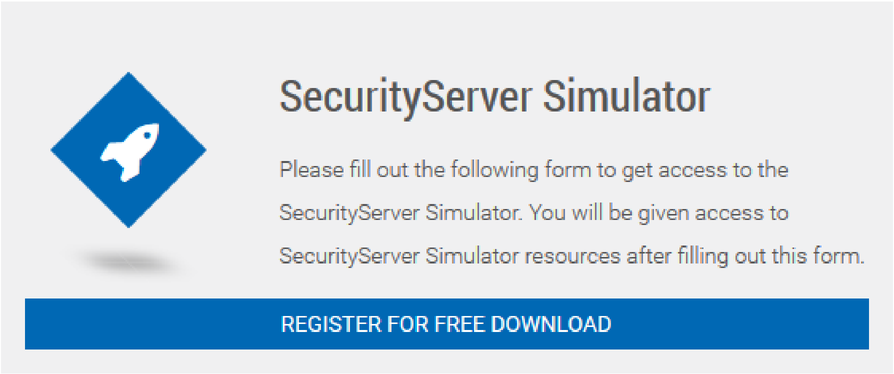
Utimaco provides the “root of trust” securely storing the connection certs of the OpenVPN server. That identity resides inside the Utimaco HSM. All signing operations are performed internal to the HSM so that the key material is not visible in the clear. The Utimaco HSM easily integrates with IoT devices and OpenVPN via an industry standard PKCS#11 or Microsoft CNG API. IoT certs and keys are generated derived keys from the master key inside the Utimaco HSM. These keys and certs get delivered to each IoT device for identity management and command signature validation using low resource Elliptic Curve mathematics. The OpenVPN certificates are also stored in the Utimaco HSM and accessed when needed using the Serialized ID associated with the client’s certificate. OpenVPN can safely issue and control client certificates without worry that they will get compromised. You now have safe VPN tunnels between your connected sites. Inside these VPN tunnels you have an added layer of security in that the IoT devices can identify and validate communication traffic using key material safely stored inside the Utimaco HSM.

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



SecurityServer Simulator

Please fill out the following form to get access to the SecurityServer Simulator. You will be given access to SecurityServer Simulator resources after filling out this form.

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.