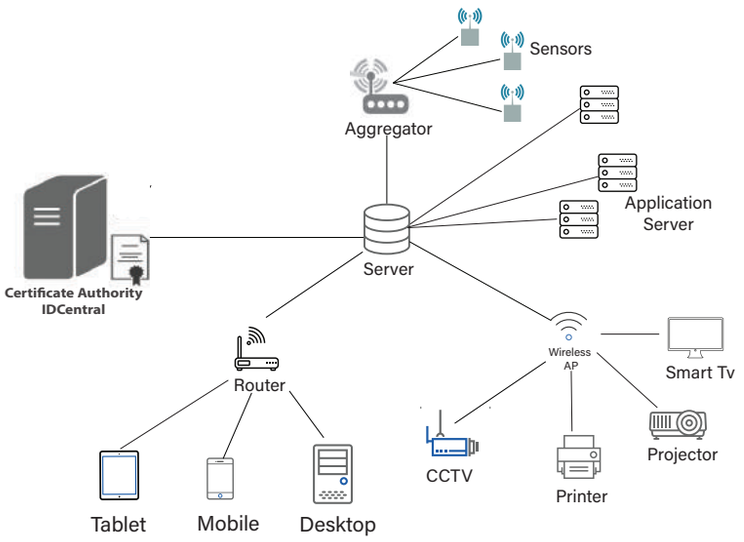
Application Note

IoT Security using Automated Certificate Management Platform



IoT and smart cities are no longer technologies of the future. Many cosmopolitan cities have become "Smart Cities" which is the application of IoT ("Internet of Things"). Many device manufacturers have simplified deployment by making IoT devices and platforms easier to manage. However, IoT security can still be a challenge in many large scale networks, since it is not an easy task to ensure different device manufacturers will follow recommended security standards. Implementing IoT security can be a difficult challenge.

Sixscape Communications provides a security platform called IDCentral which enables IoT devices and users to be issued with a digital identity (technically a "digital certificate" comes with a public key and a "private key").

IDCentral distributed PKI design allows million or billion of IoT devices distributed across in different domains (with each domain served by a domain IDCentral server), to be issued with client certificates, avoiding a traditional PKI scenario issuing all client certificates all from a centralized location with potential bottlenecks.

Once IoT devices and users have been assigned a unique digital identity, it can be used for authentication and enabling encryption on communications between other users and services.

This automated cert management is enabled by Sixscape new cert management protocol called Identity Registration Protocol (IRP), which the Internet Assigned Number Authority (IANA) has assigned port 4604 (much like SMTP, used in E-mail was assigned port 25 many years ago). IRP can automate certificate issuing and renewal without the need for human intervention to manually install the certs. In a growing large scale network like IoT, it is extremely difficult and time consuming to install a cert in each device manually or to renew one when the cert is due to expire. IRP hides the complexity of handling digital certs and make it simple to maintain a unique digital identity for all devices in the network. For example, a smart video camera could be issued a cert (tied to the camera's serial number) that could be used for authentication and even encryption when it connects to a central server.

IDWallet is an IRP client application which needs to be installed on each IoT device. In some cases, the IRP functionality could be added to a device's firmware. When a new device with IDWallet is installed in an IoT network, it will connect to IDCentral to obtain its unique digital identity, based on some unique identifier in the device (like a serial number). The device creates a matched public/private keypair and submits a request for a certificate including the public key. When this unique identifier is confirmed to be an authorized device, IDCentral will issue a digital cert including the public key and send it to the device. Once the device receives the digital cert, it will be used as digital identity for all communications and request from other devices in the network. Technically the digital cert (which is a public document) is sent instead of a username, and a cryptographic challenge verifies that the device has the corresponding private key (without revealing it).

When a network device such as video camera connects to a video server, the server will authenticate itself to the device using its server cert (normal SSL/TLS). The network device will then authenticate itself to the video server, using its own client cert. Once they are mutually authenticated, the network device can exchange information with the server. During the authentication handshake, a symmetric session key is securely exchanged which allows the network device and server to encrypt all information sent between them. If someone were to snoop on the traffic between the device and the server, all they would see is binary gibberish (ciphertext). If someone tried to substitute a different camera, the authentication would fail and the server would not accept any information from it – it could even alert the administrators of tampering with (or replacement of) the network device.

Traditional web based PKI systems are designed for humans that can interact with web pages using a browser. IRP makes it easy for devices to interact with our IDCentral Certification Authority in a highly secure, fully automated manner. This is critical for IoT applications, which might have a very large number of network devices. This was one of the most important goals in the design of IRP.

33 Ubi Avenue 3
#08-26 The Vertex Tower B
Tel: +65 6509 8070
www.sixscape.com
enquiries@sixscape.com