Invention Title:	Automated Internet of Things Certificate Installation Process
Invention Summary:	Defines an automated process for installing PKI certificates on retail purchased IoT devices allowing the MSOs to extend the privacy and security supplied by their HSD service to the emerging IoT ecosystem.
Invention Description:	see below
Invention Commercial Value/Customers:	Provides a common automated process for IoT appliance, sensor, gateway and consumer electronics manufactures to support certificate based security to the products they sell to consumers.
Invention Differences:	Retains privacy and security for consumers in automated process. Reduces power consumption of IoT devices until their purchase and installation, extending battery-life. Leverages existing PKI infrastructure. Extends security to the home network. Requires proximity to gateway or hub to onboard new devices, minimizing the likelihood of infiltration of bogus devices.

Automated Internet of Things Certificate Installation Process

Defining an automated process for installing certificates on to retail Internet of Things (IoT) devices is crucial to maintaining a consumer's privacy and retaining a secure private network. Cable operators have created a reliable secure network for consumers and businesses to communicate and exchange information using their certificate based Public Key Infrastructure (PKI). This secure network extends beyond the physical facilities of the operators to the customer's premise by ensuring the cable modems (CMs), set-top-boxes (STBs) and gateways (GWs), collectively referred to as customer premise equipment (CPE) in this document, are manufactured with certificates in a controlled and secure manner thus establishing a safe demarcation for private networks. Companies and individuals depend on the privacy and security this network provides to form the foundation to conduct numerous internet transactions on a daily basis. This document defines a process for automatically creating a PKI, communicating the newly created PKI and transferring the certificate to a new retail IoT device being added to a consumer's private network.

Upon the introduction of a new retail IoT device into connectivity range of the CPE, the two devices discover one another and establish a temporary secure link-layer network connection using whatever common communication protocol both devices support, e.g. ZigBee, Bluetooth LE, Wi-Fi, etc., that is outside the scope of this document. It is recommended that retail IoT devices should operate a reduced transmit power until a certificate has been installed. This has two advantages, one conserves battery life until device is sold in marketplace and secondly it forces proximity requirements between the new IoT device and the CPE to allow discovery to occur.

Next the CPE notifies all network administrators that a new device has been discovered and requests confirmation to add the device to the network, see Figure 1. This request for confirmation from the CPE

to the individual administrators may be presented in many forms across a variety of user interfaces such as television, tablets, PCs, smart phones, and web portals. After the CPE receives confirmation from the administrator to continue the process of adding the new IoT device, the CPE requests the Provisioning Server add it to the network and to create a new certificate using the secure connection established during the provisioning of the CPE. Upon successful creation of the new certificate, the Certificate Server returns it to the Provisioning Server for transference to the CPE. The CPE translates the certificate file or binary information and transmits the data to the IoT device using the standard communication supported by the device. The IoT device is required to store the certificate in non-volatile memory, in case communication is lost between the IoT and CPE at some future time. The IoT device is then required to begin communicating using the secure connection for all subsequent correspondence with the CPE.

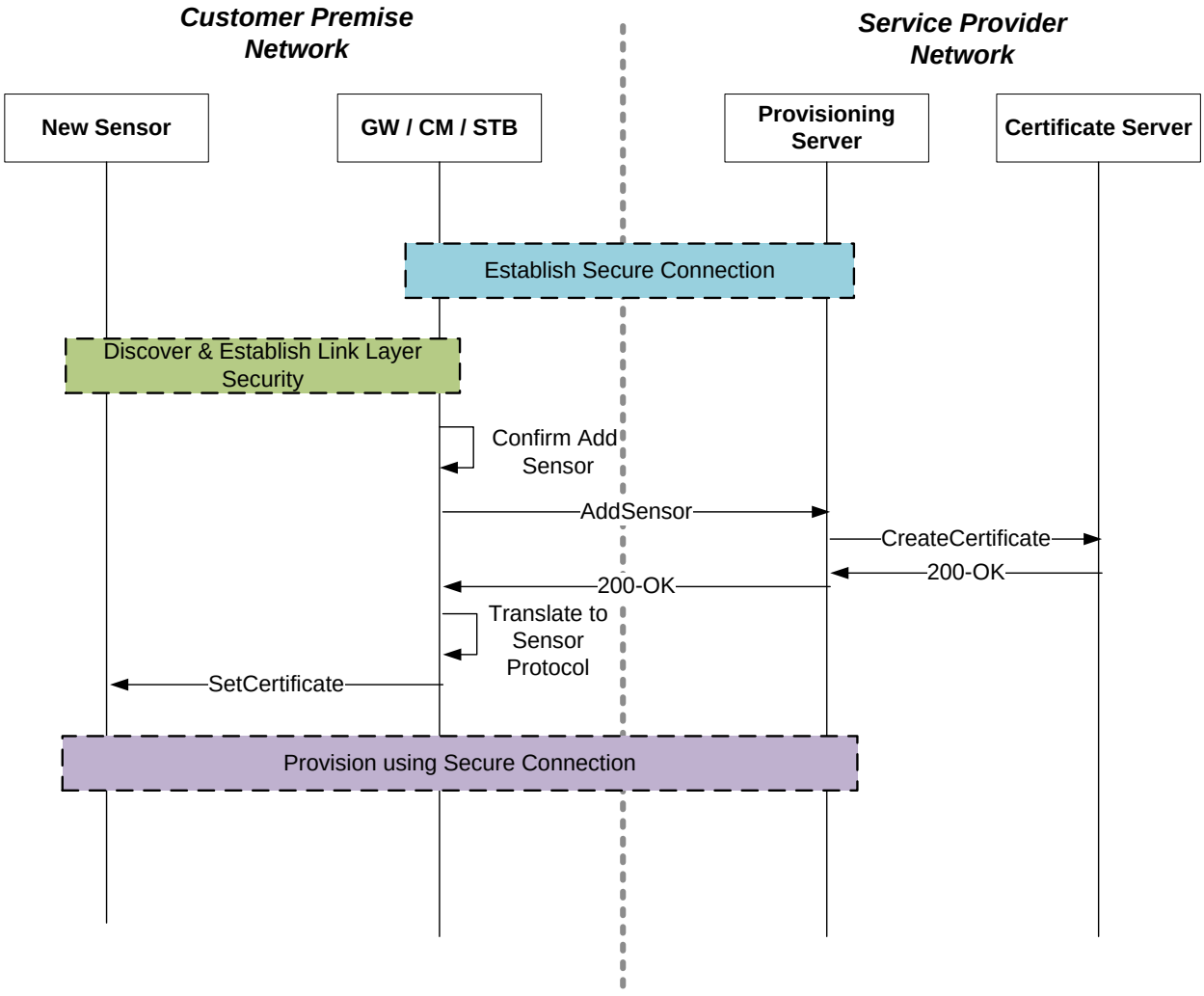

Figure 1 – Automated Certificate Installation Sequence Diagram

IoT devices must allow for the possibility revocation of a certificate and the need for a new certificate to be installed on the device. In this situation, the IoT device should return to factory settings and attempt to discover a network to establish an initial connection, which is outside the scope of this definition. This operation also supports the potential transfer of IoT devices between entities in an after or secondary market transaction.