aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

Securely Connect IoT Devices To In-Building IT Networks

INTRODUCTION

Building owners and tenants are rapidly transforming workplaces into energy efficient smart spaces, and that process has aggravated a vexing problem that long faced the building controls market: how to on-board IP-based IoT controllers, displays, and protocol convertors to a building's secure IT network. A rash of high-profile security breaches that originated in IoT devices has put Chief Information Security Officers on high alert, and it's increasingly forbidden to add an IoT device to an IT network without first passing a cybersecurity review.

Even if a device passes a cybersecurity review getting it onto the IT network can be tedious. If a device's user interface wasn't designed with IT networks in mind then configuration options might be missing. And security certificate management can become a Catch-22: a device has to be on the network to receive a security credential, but the device can't be on the network without an installed credential. Some companies solve the latter problem by sending secret credentials over an unprotected open network, but that obviously poses its own risk.

DEVICE PROVISIONING PROTOCOL

Device Provisioning Protocol (DPP), certified under the Wi-Fi Alliance as "Easy Connect," is a standard that allows devices to be easily provisioned onto a secure network using simple, modern techniques such QR code scanning. The solution replaces Wireless Provisioning Service (WPS), a hugely popular onboarding solution that unfortunately had significant security gaps due, in part, to its reliance on immature Wi-Fi encryption services such as Wireless Protected Access (WPA).

DPP addresses this gap by leveraging WPA3 to enhance certificate handling and provide robust, secure, and scalable provisioning of IoT devices in any commercial, industrial, government, or consumer application. DPP also supports legacy WPA2 connections.

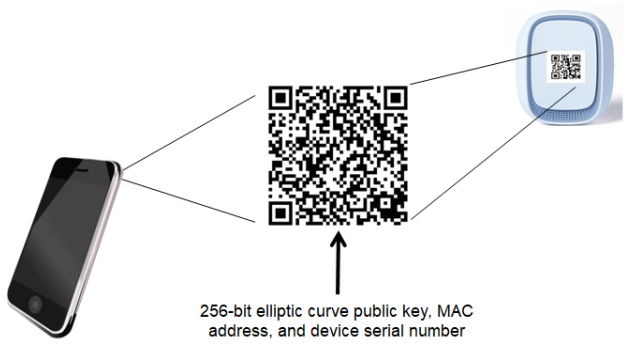

Figure 1. On-boarding Can Be As Simple As A QR Code

Designed to accommodate devices with or without a user interface, each DPP-enabled device is manufactured with an elliptic curve public/private key pair. The device can be brought onto a network via many paths, but the most common is by scanning a QR code on the device using a smartphone. The QR code contains an elliptic curve public key, and optionally the device's MAC address and serial number. Other bootstrapping methods are also available, including using near field communication (NFC) proximity to secure public key exchange and directly exchanging bootstrapping information with a cloud service.

Cybersecurity attacks are forcing IoT devices to use ever larger cryptography key sizes, which requires more expensive memory and processing power. DPP leverages WPA3 elliptic curve cryptography to achieve better cryptographic strength with smaller keys and less processing power than previously possible. That, in turn, lowers the device cost.

There are four steps to on-board an IoT device onto an IT network using DPP, and the total process can be completed in seconds:

- *Bootstrapping:* the device shares a public key that is bound to a unique private key;
- *Discovery:* unprovisioned devices are identified by the DPP-enabled network infrastructure;
- *Authentication and configuration:* a request-response process authenticates the device and the configuration service, following which a security role and group are assigned to the device;
- Network access: an Aruba Wi-Fi access point or wired controller advertises the availability of a DPP network. The device and the network exchange keys, and separately derive an authenticated Pairwise Master Key (PMK). If each side generates the same PMK then the device is allowed on the network.

PROBLEM SOLVED

DPP can run over Wi-Fi and Ethernet, addressing the vast majority of smart building applications. Cellular-enabled devices can obtain Wi-Fi credentials via DPP, too, so mobile devices can move between cellular and Wi-Fi networks.

QR code scanning is hard to get wrong. Just point the smartphone camera and hit "enter." In contrast, manually entering a pre-shared key is both time consuming and error-prone. If you make a mistake the process starts anew.

DPP QR codes can be scanned individually or batched. Individual scanning is ideal for smaller sites and when a device is being replaced. Batched scanning is perfect for a large upgrade and when commissioning a new site.

When coupled with a cloud-based device manufacturing service, DPP can obtain credentials for legitimate devices from the cloud and provide a secure, zero-touch onboarding experience where deployment involves just turning on a device and walking away.

Finally, DPP eliminates the need to configure security credentials over an open network, closing a significant security gap. By eliminating manual steps the installation can proceed faster and without IT-skilled labor.

SUMMARY

If you need to deploy IP-based IoT controllers, displays, or protocol convertors on a secure IT network then DPP is the answer. DPP speeds installation time, closes security gaps of earlier provisioning systems, and thru the use of WPA3 and other security mechanisms it meets the high standards sets by CISOs. Product developers interested in using DPP and accessing Aruba's DPP API should complete the contact form available at https://www.arubanetworks.com/partners/technology-partners/contact-form/.

aruba
a Hewlett Packard Enterprise company

SO_DeviceProvisioningProtocol_RVK_062222 a00124977enw

Contact us at www.arubanetworks.com/contact