USER & THING IDENTITY IN THE "ZERO TRUST" NETWORKING ERA

@TIMCAPPALLI

identiverse® 2020

Topics

Tunneled EAP

Wi-Fi Easy Connect

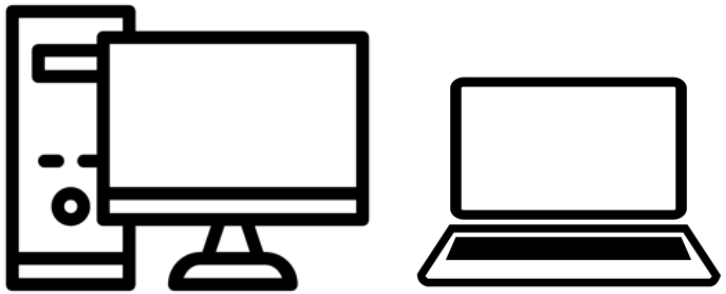
Device Provisioning Protocol (DPP)

Let's set the stage

identiverse® 2020

Device Classes

COMPUTERS
(desktop OS)

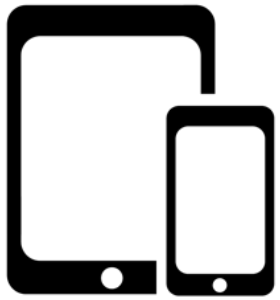


managed or unmanaged

flexible network supplicant

rich UI

SMART DEVICES
(mobile OS)



managed or unmanaged

flexible network supplicant

rich UI

IOT / HEADLESS

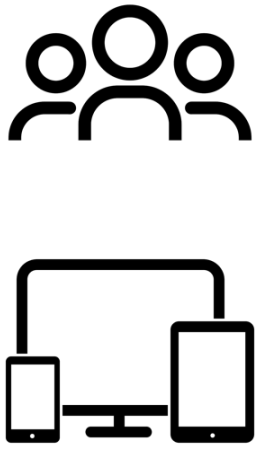
unmanaged*

basic network supplicant

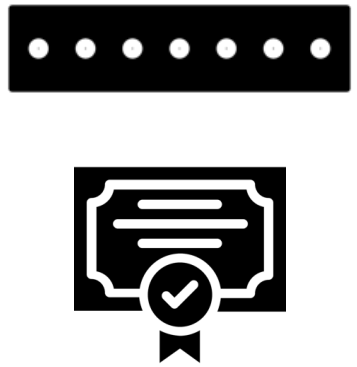
poor or no UI

Typical Enterprise Network

SUBJECTS



AUTHENTICATION METHODS



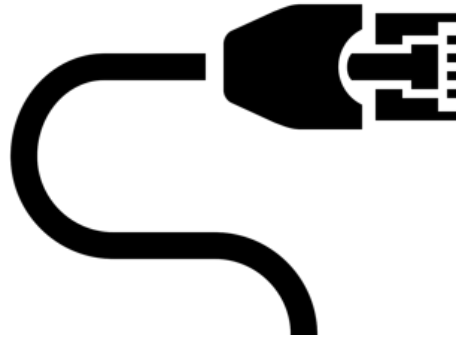
A1:B2:C3:98:12:34

ACCESS METHODS

"SecureNet"
802.1X

"DeviceNet"
PSK

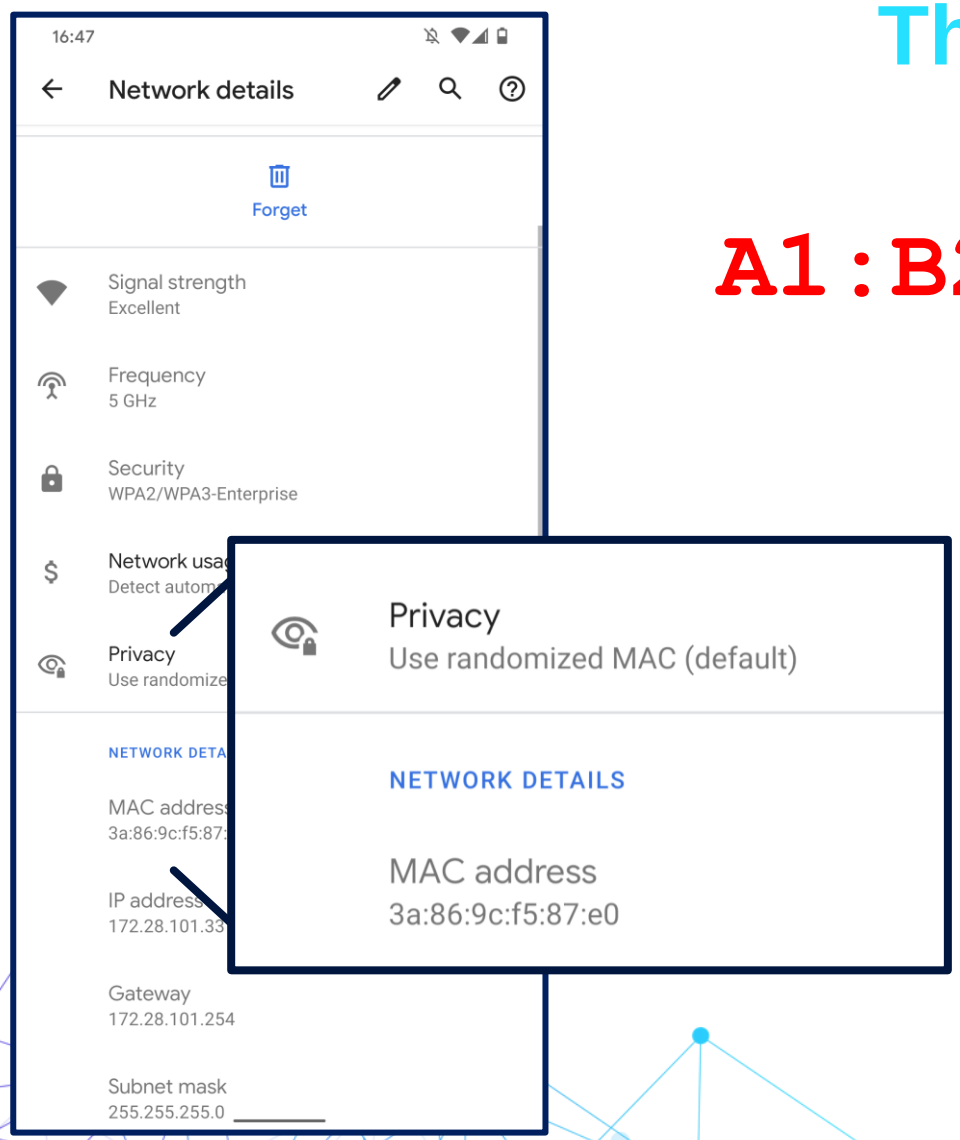
"GuestNet"
Open or PSK



ROLES & POLICIES

The MAC Address

A1:B2:C3:98:12:34



layer 2 address visible over the air

can be cloned or randomized

not always easy for end users to find

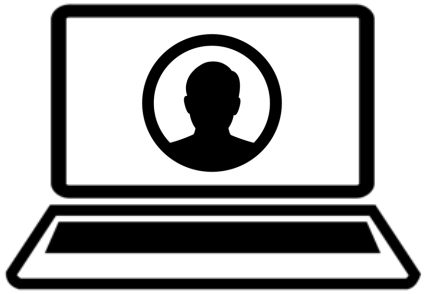
identiverse® 2020

User Only

device-specific cert* with the user as the subject

(*can also be a password)

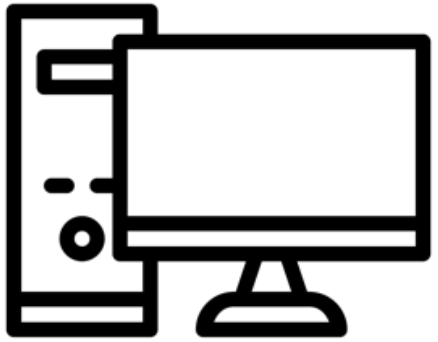
common with BYO devices



CN = `ethan.hunt@capptoso.com`
Issuer CN = `Capptoso Unmanaged Device CA`
serialNumber = `b87e239aa5a98b34dd67a3e4`
SubjectAltName:
msUPN = `ethan.hunt@capptoso.com`
deviceType = `Windows Laptop`

CN = `ethan.hunt@capptoso.com`
Issuer CN = `Capptoso Unmanaged Device CA`
serialNumber = `13c50afcea343b773a55fa94`
SubjectAltName:
msUPN = `ethan.hunt@capptoso.com`
deviceType = `Android Smartphone`

Device Only

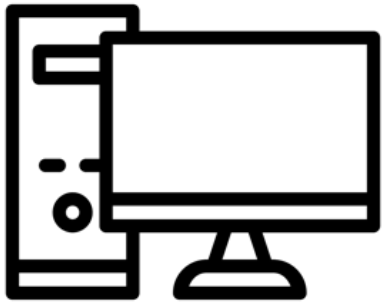


device-specific cert* with the device as the subject

(*can also be a password)

CN = `bos-kiosk-37.device.capptoso.com`
Issuer CN = `Capptoso Corporate Device CA`
serialNumber = `ed613a9329d59ad0ba5ace19`
SubjectAltName:
dNSName = `bos-kiosk-37.device.capptoso.com`
deviceType = `Windows Desktop`

User + Device



SUBJECT
bos-kiosk-37.device.capptoso.com

SUBJECT
ethan.hunt@capptoso.com

A1:B2:C3:[illegible]8:12:34

Tunneled EAP (TEAP)

RFC 7170

identiverse® 2020

Tunneled EAP (TEAP)

TLS SESSION

SUPPLICANT

AUTH SERVER

Hello! Please send me your machine credential

Here's my machine certificate with username host/bos-kiosk-37.device.capptoso.com

Credential 1 Success! Please send me the user credential

Here's my user certificate with username ethan.hunt@capptoso.com

Credential 2 Success! EAP Success! Connected!

SEQUENCES SHORTENED AND SUMMARIZED FOR PRESENTATION

identiverse® 2020

Potential Future Uses

STANDARDIZED BUT NOT IMPLEMENTED

Certificate enrollment

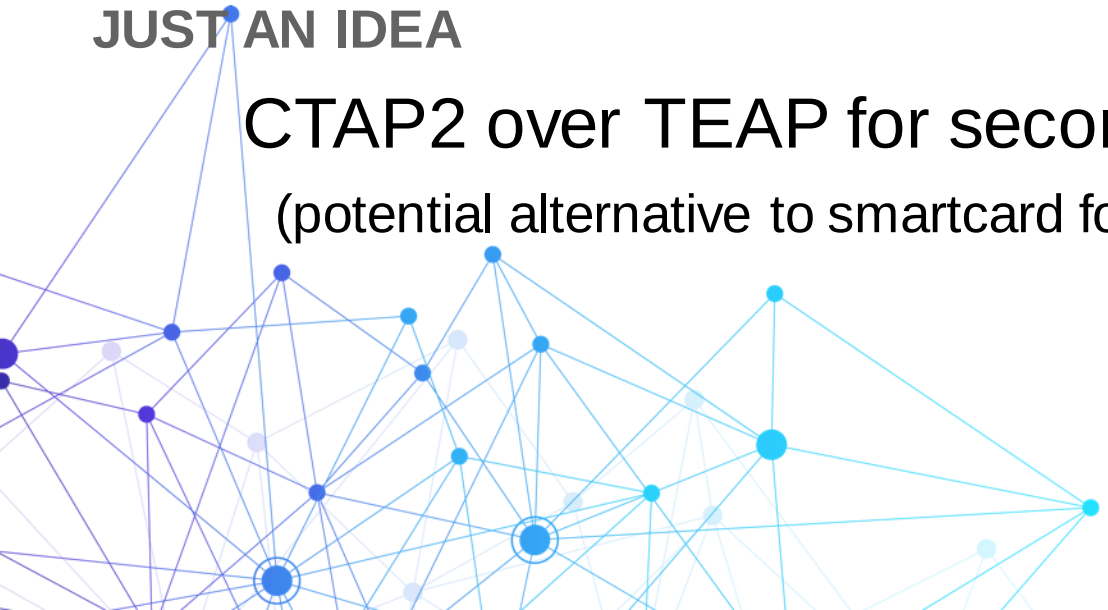
STANDARDS EFFORTS IN-PROGRESS

IoT / headless device enrollment via TEAP (IETF: draft-lear-eap-teap-brski-05)

JUST AN IDEA

CTAP2 over TEAP for second factor or passwordless

(potential alternative to smartcard for network access)

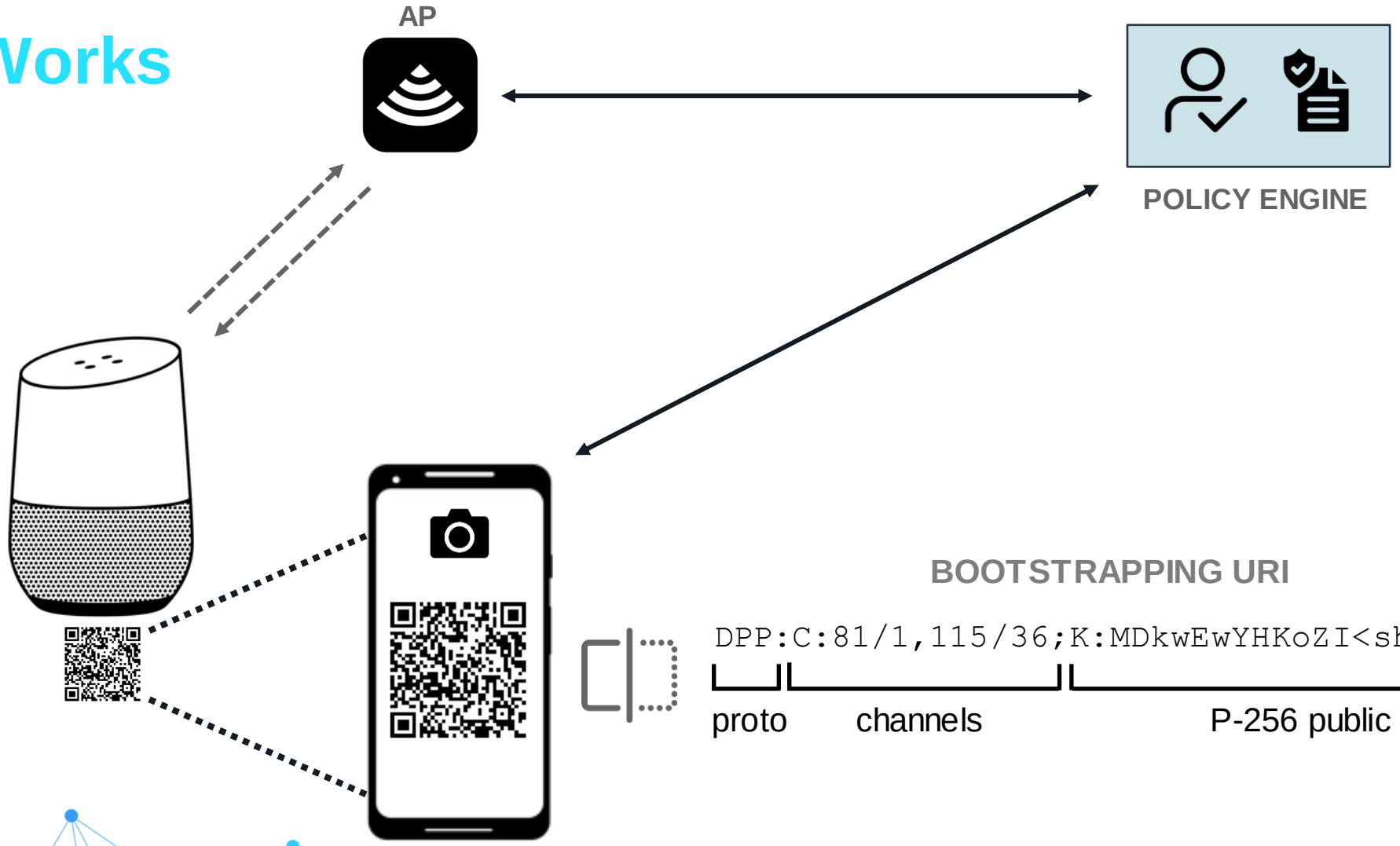


Wi-Fi Easy Connect

Device Provisioning Protocol (DPP)

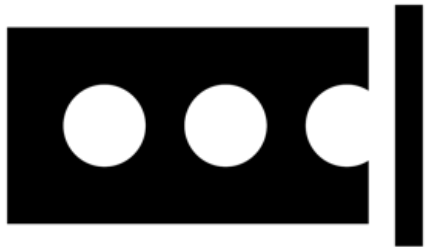
identiverse® 2020

How It Works



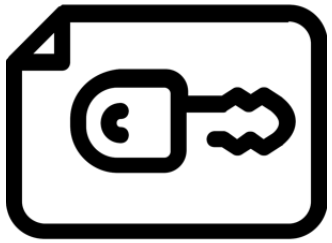
identiverse® 2020

Credential Options



Traditional Pre-Shared Key

Identity Binding ✗
Unique Per Device ✗
Strong Credential ✗



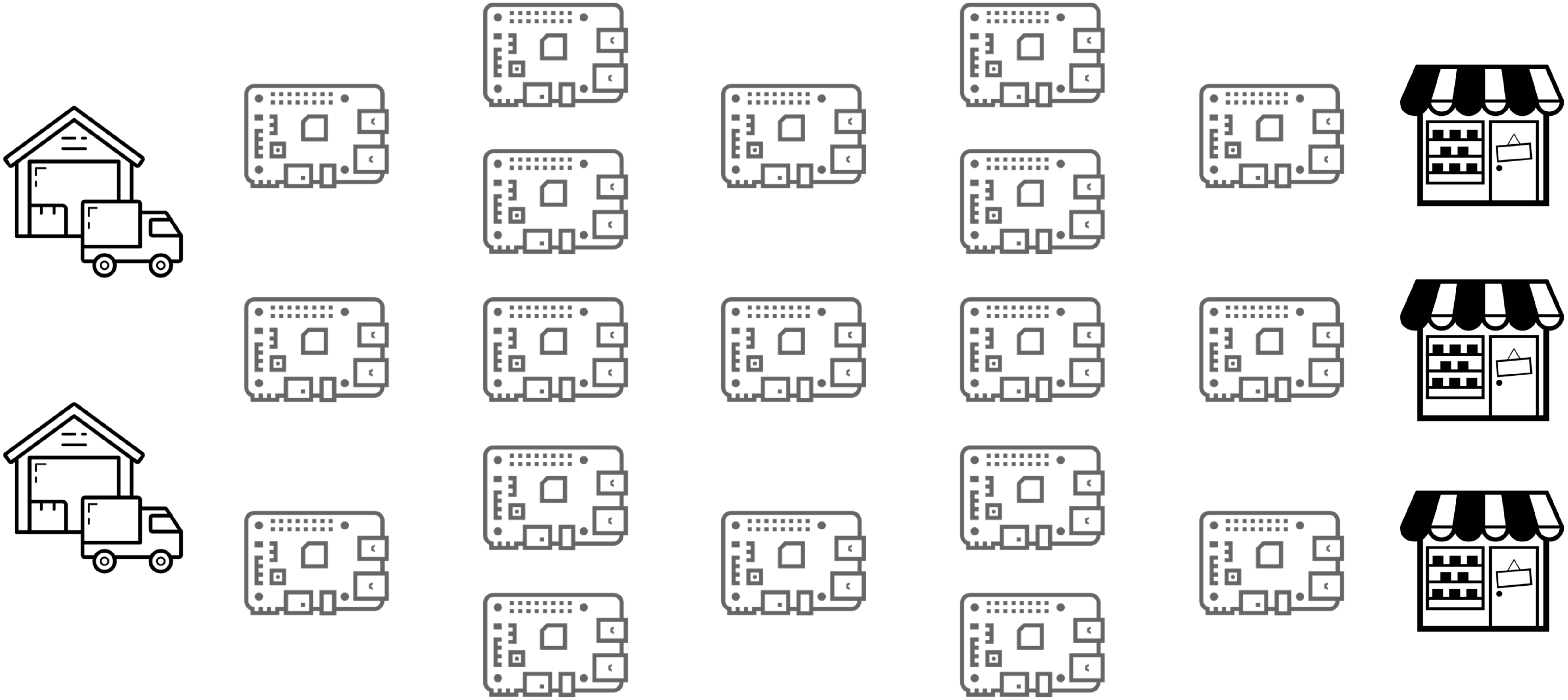
DPP Connector

Identity Binding ✓
Unique Per Device ✓
Strong Credential ✓

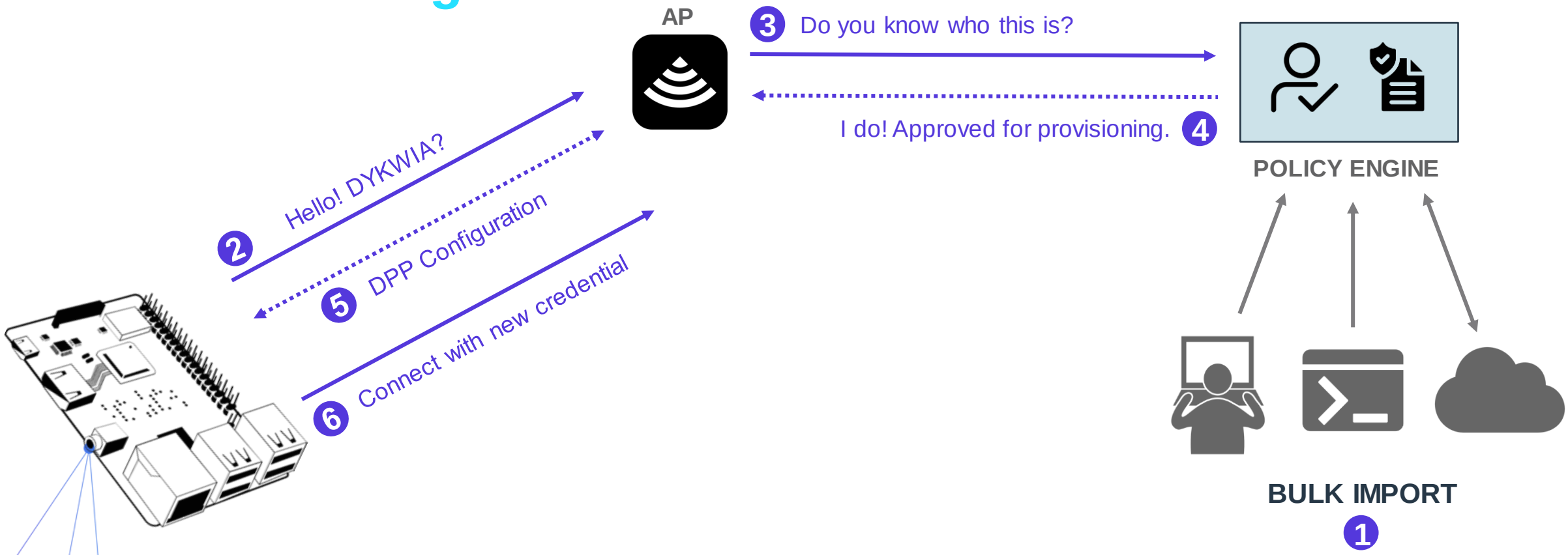
DPP Enterprise

Identity Binding ✓
Unique Per Device ✓
Strong Credential ✓

identiverse® 2020



Bulk Provisioning



identiverse® 2020

Summary

Tunneled EAP

Flexible authentication methods

Strong user + device identity binding

Lots of future potential

Wi-Fi Easy Connect

Strong device identity

Simple user experience

Bulk provisioning

identiverse® 2020


identiverse®
2020