Learnings from SDO & FIDO Alliance IoT TWG Protocols

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Geoffrey Cooper
geoffrey.cooper@intel.com
FIDO IOT Technical Working Group

intel®

SDO/FIDO protocol

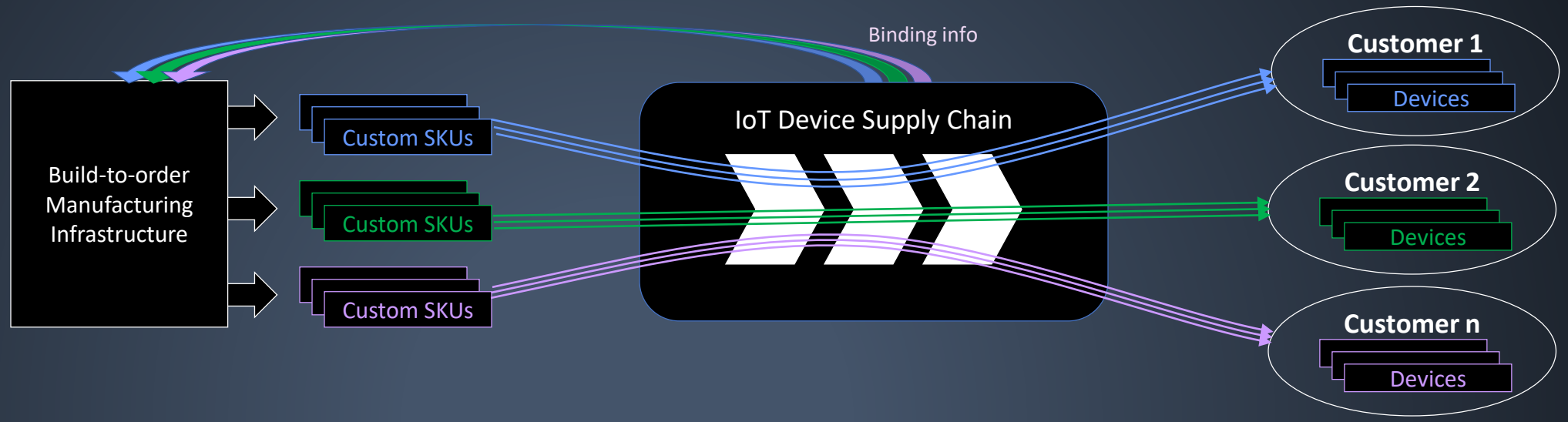
- Secure Device Onboard is a protocol from Intel, released to LF-Edge
- FIDO IOT Technical Working Group is using SDO as a base, Working Draft available
- Main features
  - Late binding – one device SKU for “any” IOT platform
  - Application keys are negotiated during onboarding
  - Flexible: as many credentials, data, updates as you need
  - Internet / Enterprise / Closed networks
  - FIDO IOT protocol will address trusted- and untrusted-installer
- Open solution
  - FIDO specification, working draft
    https://fidoalliance.org/specs/fidoiot/FIDO-IoT-spec-v1.0-wd-20200730.html
  - LF-Edge reference implementation (see SDO spec in docs section)
    https://www.lfedge.org/projects/securedeviceonboard/
- Plan for LF-Edge to migrate to FIDO spec when it is complete.
- FIDO draft implementation is already posted to LF-Edge github

Late Binding for Supply Chain Efficiency

Zero Touch <u>without</u> SDO

IoT device software and security customization happens during manufacturing

Result:
Complicated build-to-order manufacturing infrastructure, many SKUs, small lot sizes, long lead times, higher cost



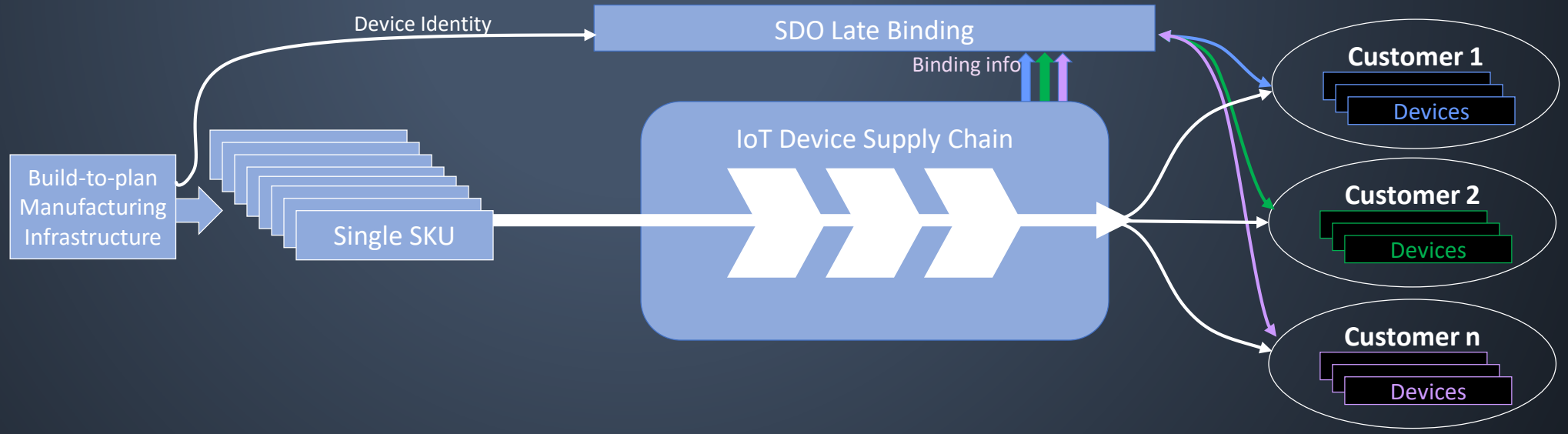
Zero Touch <u>with</u> SDO

IoT device software and security customization happens at the end of the supply chain

Benefits:

Simplified build-to-plan manufacturing infrastructure, fewer SKUs, large lot sizes, enable stocking distributors, low customization cost

Result: *Increased supply chain volume and velocity*



LATE BINDING REDUCES COSTS & COMPLEXITY IN SUPPLY CHAIN – A SINGLE DEVICE SKU FOR ALL CUSTOMERS

FIDO Alliance IOT WG Meeting

***FIDO IOT Charter**: "The IoT TWG has been established to develop use cases, …, **automated onboarding, and binding of applications and/or users to IoT devices**, …"*

First F2F meeting: July 2019
45 IoT Use Cases Presented

Attendees: 4 CSP's / 6 Chip companies

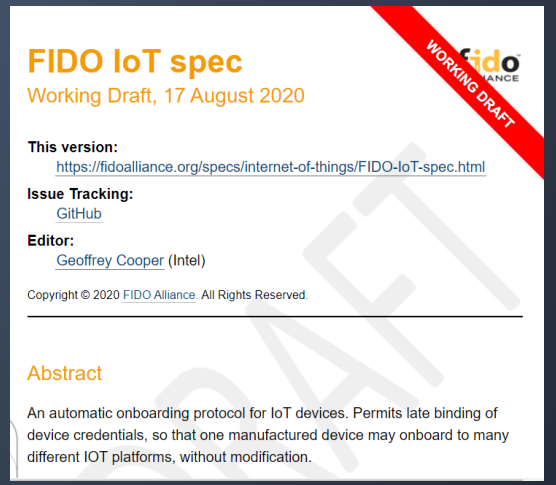
Google	Arm	Lenovo
Microsoft	Intel	NXP
RSA	AWS	eWBM
Qualcomm	Infineon	Device Authority
Alibaba	Phoenix Technologies	

Plenary, September 2019
Derived Requirements from Use Cases

R1	Open Solution
R2	Automatic Onboarding
R3	Authorization (to onboard) is end-to-end
R4	Communications Independence
R5	Late Binding
R6	Permits Supply Chain Flexibility
R7	Repurpose / Resale
R8	Limit Correlation Attacks (Breadcrumbs)
R9	Deferred Acceptance
R15	Trusted and Untrusted Installer
R16	Localized authentication
R17	Internet, Home, Enterprise & Closed networks
R18	IOT Owner need not be Network Owner
R19	Target device range (CPU/RAM/UI/OS etc.)

F2F meeting: Dec 2019
SDO moved to working draft

FIDO IOT TWG: Aug 2020
FIDO IOT protocol working draft released
https://fidoalliance.org/specs/fidoiot/FIDO-IoT-spec-v1.0-wd-20200730.html


FIDO IoT spec
Working Draft, 17 August 2020
WORKING DRAFT
This version:
https://fidoalliance.org/specs/internet-of-things/FIDO-IoT-spec.html
Issue Tracking:
GitHub
Editor:
Geoffrey Cooper (Intel)
Copyright © 2020 FIDO Alliance. All Rights Reserved.
Abstract
An automatic onboarding protocol for IoT devices. Permits late binding of device credentials, so that one manufactured device may onboard to many different IOT platforms, without modification.

SDO/FIDO protocol – interesting features

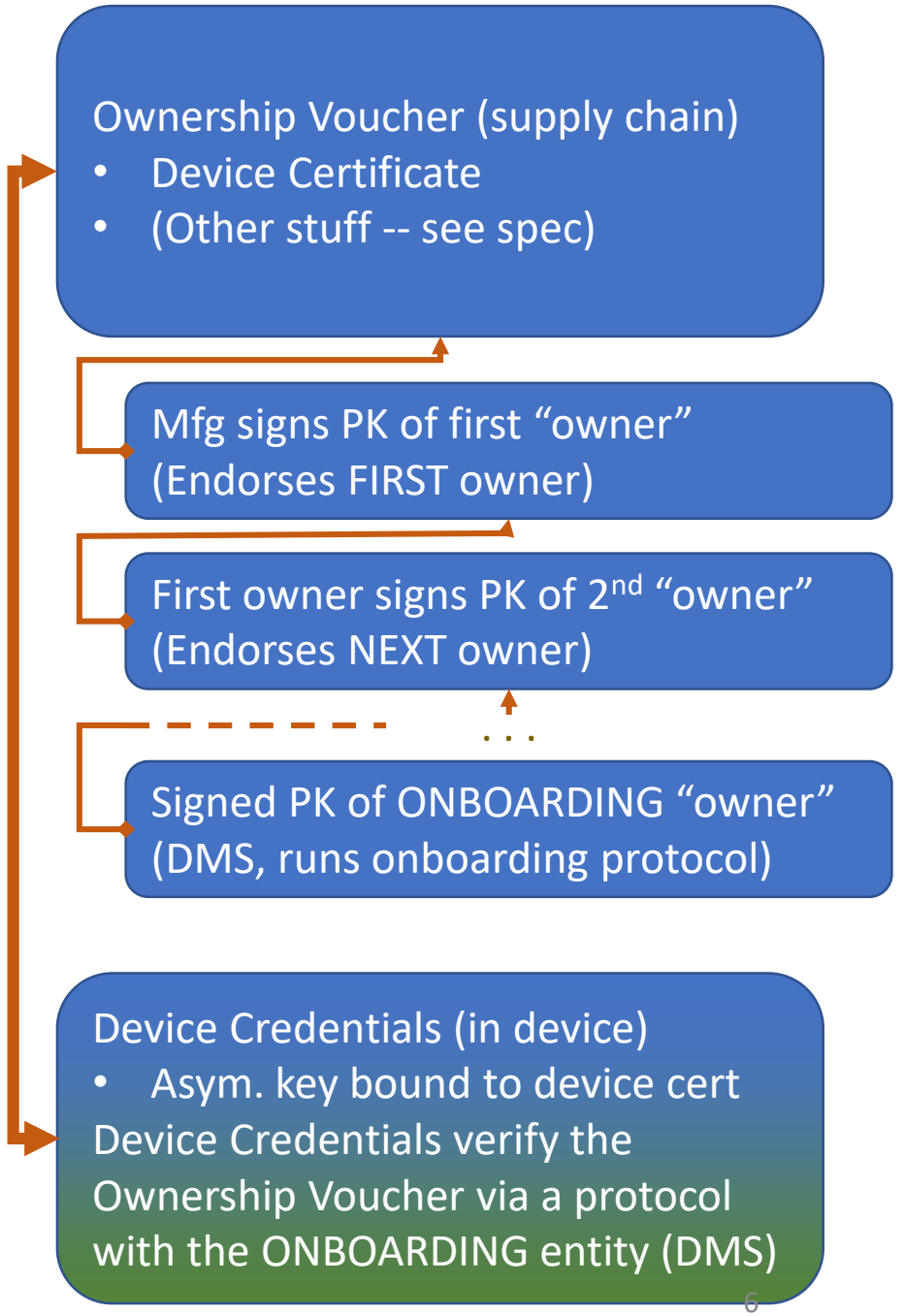
- Late binding – single device SKU can connect to “any” IOT platform
  - Ownership Voucher data structure builds ledger of changes in ownership during supply chain
- Network entry is out of scope, but a proxy can give temporary access
- SDO – untrusted installer only
- FIDO – also working on trusted installer
  - aka “trusted onboarder”
  - Specific definition of what trusted installer means

Ownership Voucher

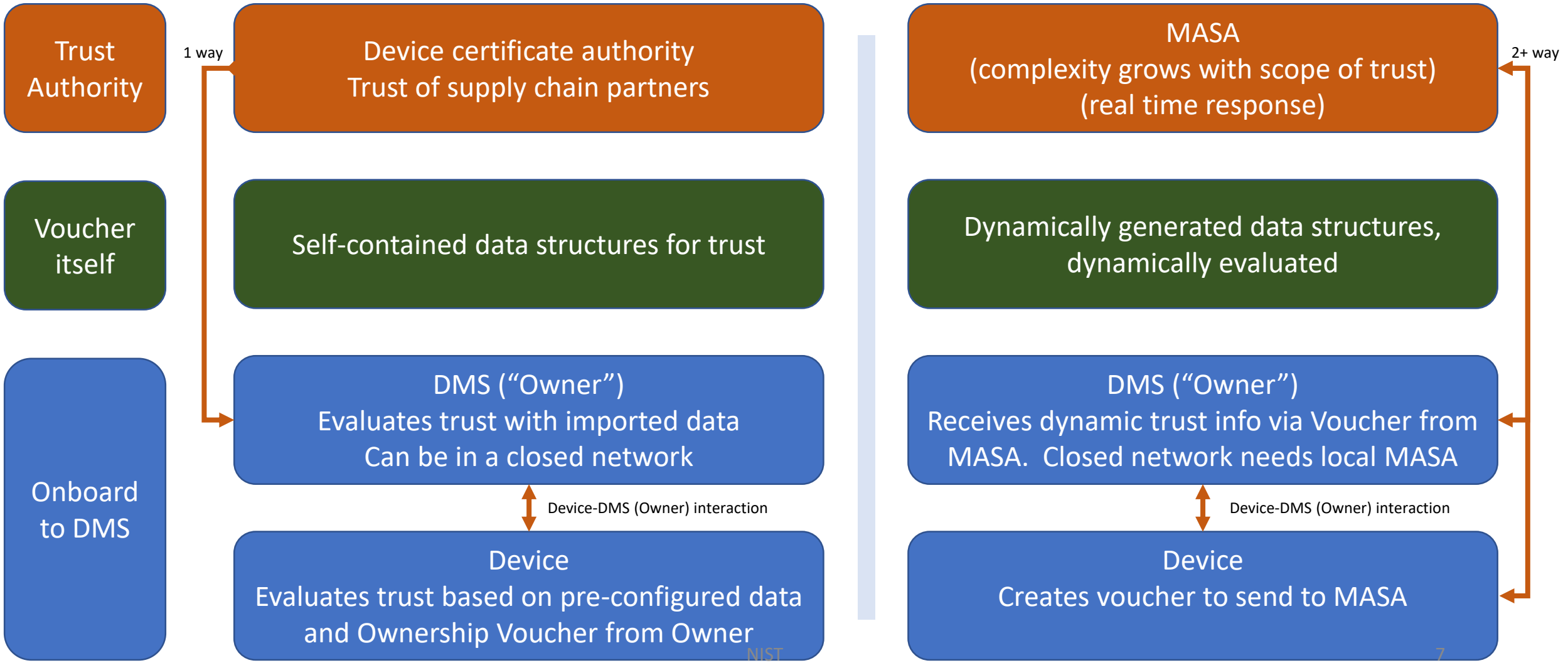
Created in Mfg

Mated during Onboarding Protocol

- Data structure secured by signatures
- Simplified, see specs for other ingredients
- Self contained & distributed mechanism
- Passed through supply chain
  - Allows late decisions of supply chain routing, onboarding owner
  - Distributed, some work at each routing step (toolkits)



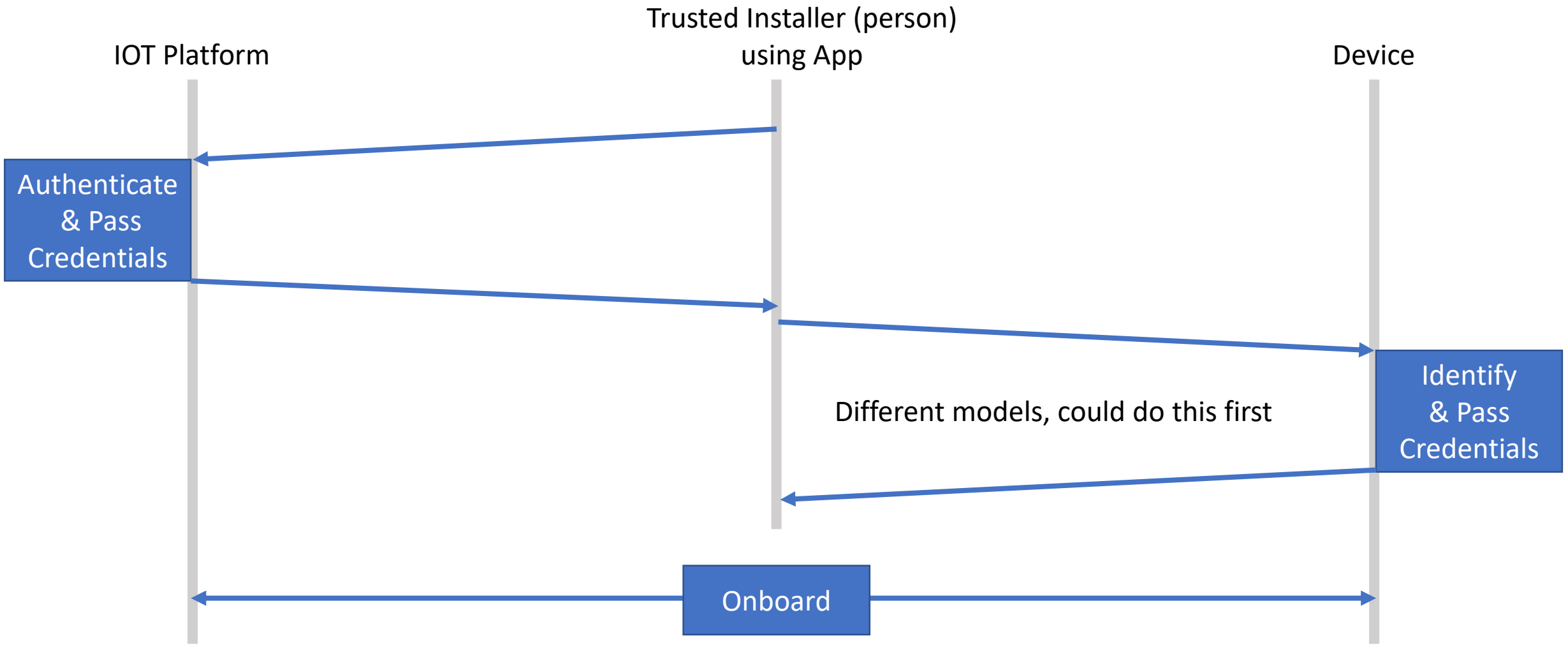
“Ownership Voucher” vs RFC8366 “voucher”



FIDO Alliance & Trusted Installer

- NIST white paper: “Trusted Onboarder”, but further constrained.
- Protocols under development at FIDO, give Key Message only
- Trusted Installer (person):
  - Uses App to interact with Device
  - Chooses the IOT platform on which to onboard
    - The “cloud”
    - The “account”
    - The “manager” / “DMS” – might be local to the network
- Trusted installer does not login to device
- Trusted installer does not control device
- Device has no residual trust in the installer, except choice of IOT platform
- Advantage: Trusted installer replaces trust in Network or Supply Chain
  - Big savings – If you trust the installer. Be careful that you really do!

Trusted Installer Basic Concept



Trusted Installer Onboards with new credentials, no subsequent trust in Installer person

Thanks for listening

geoffrey.cooper@intel.com
FIDO IOT Technical Working Group