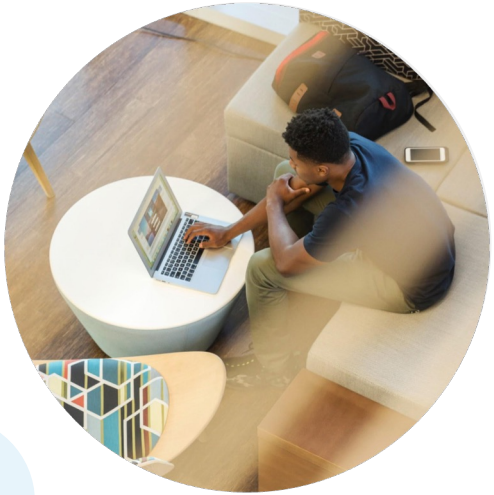
LPWAN 2019 - Paris

IETF standards for IoT device bootstrapping

Sandoche Balakrichenan

afnic



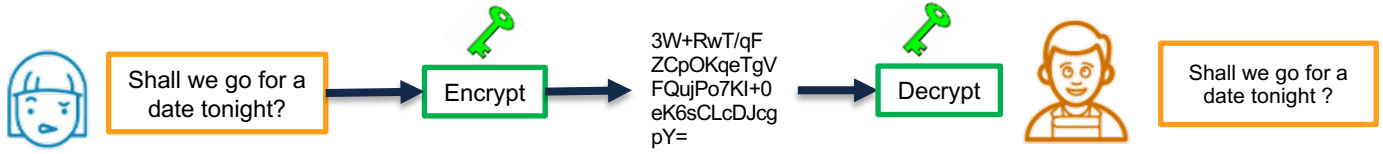
IoT Bootstrapping – Definition

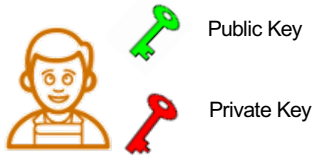
A process that is required
before the resource constrained IoT device can operate in a network

Introduction

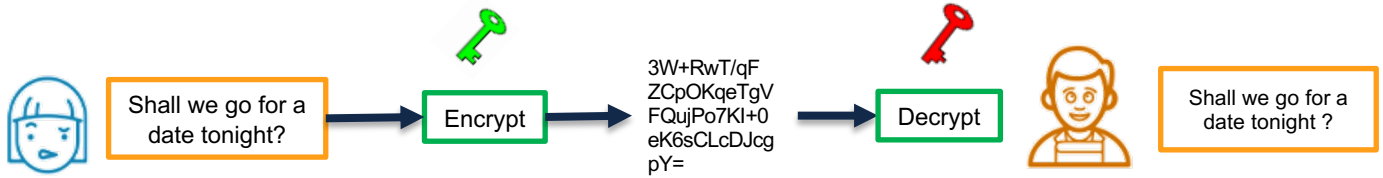
Symmetric and Asymmetric

Symmetric Keys





Asymmetric Keys



Device fabrication



The device contains the DevEUI

Generic Device





AppKey



NwkKey

The device contains the DevEUI, NwkKey, AppKey, JoinEUI

Information at the JS (before OTAA)



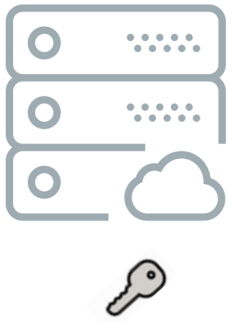
AppKey

NwkKey

The JS contains the DevEUI, NwkKey, AppKey

Information at the AS (before OTAA)

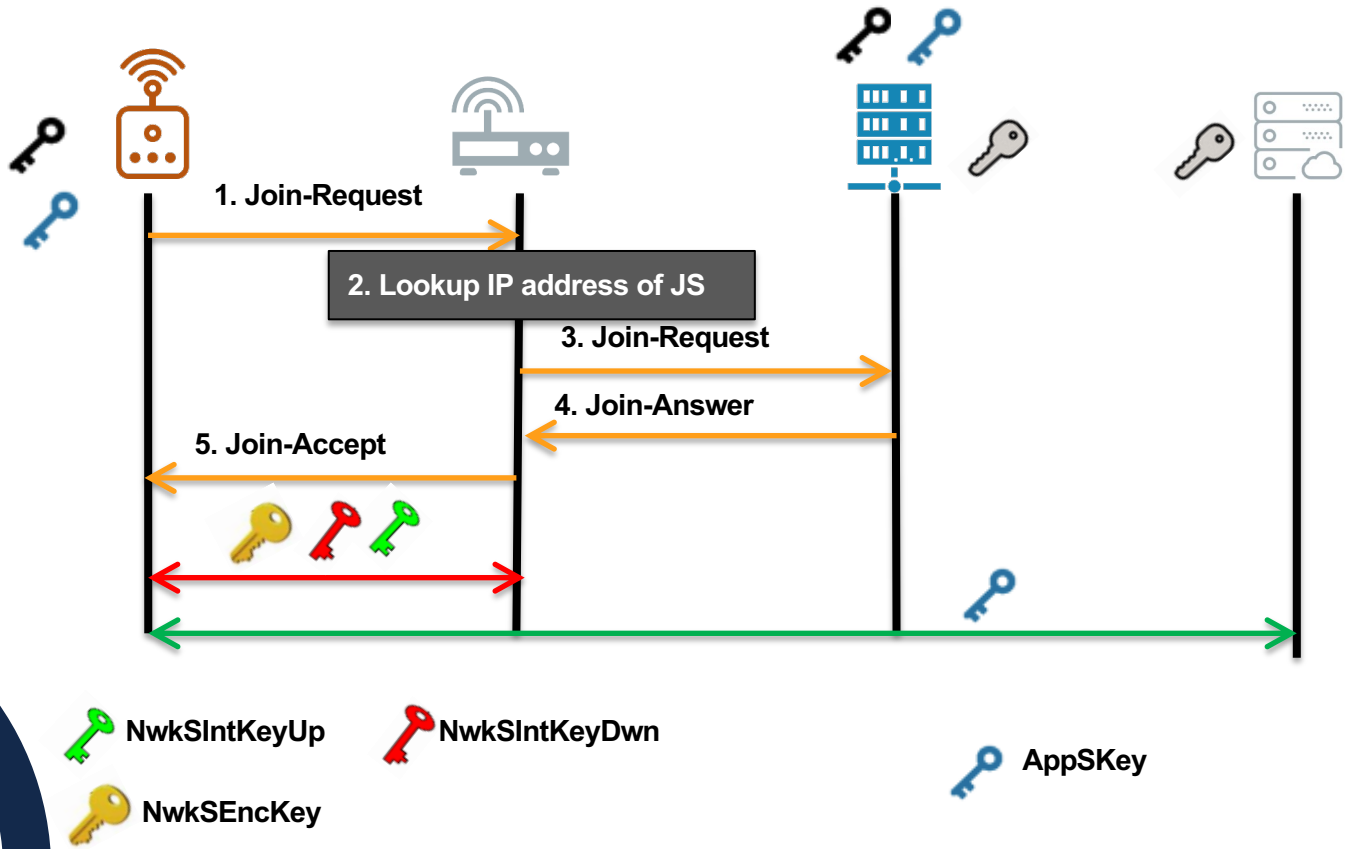






Secret Key shared between JS and AS

A simple bootstrapping view of LoRaWAN end-to-end communication



Issues



Bootstrapping terminologies

Onboarding

Initial establishment of keys and configuration information

Bootstrapping

Provisioning of keys and configuration information

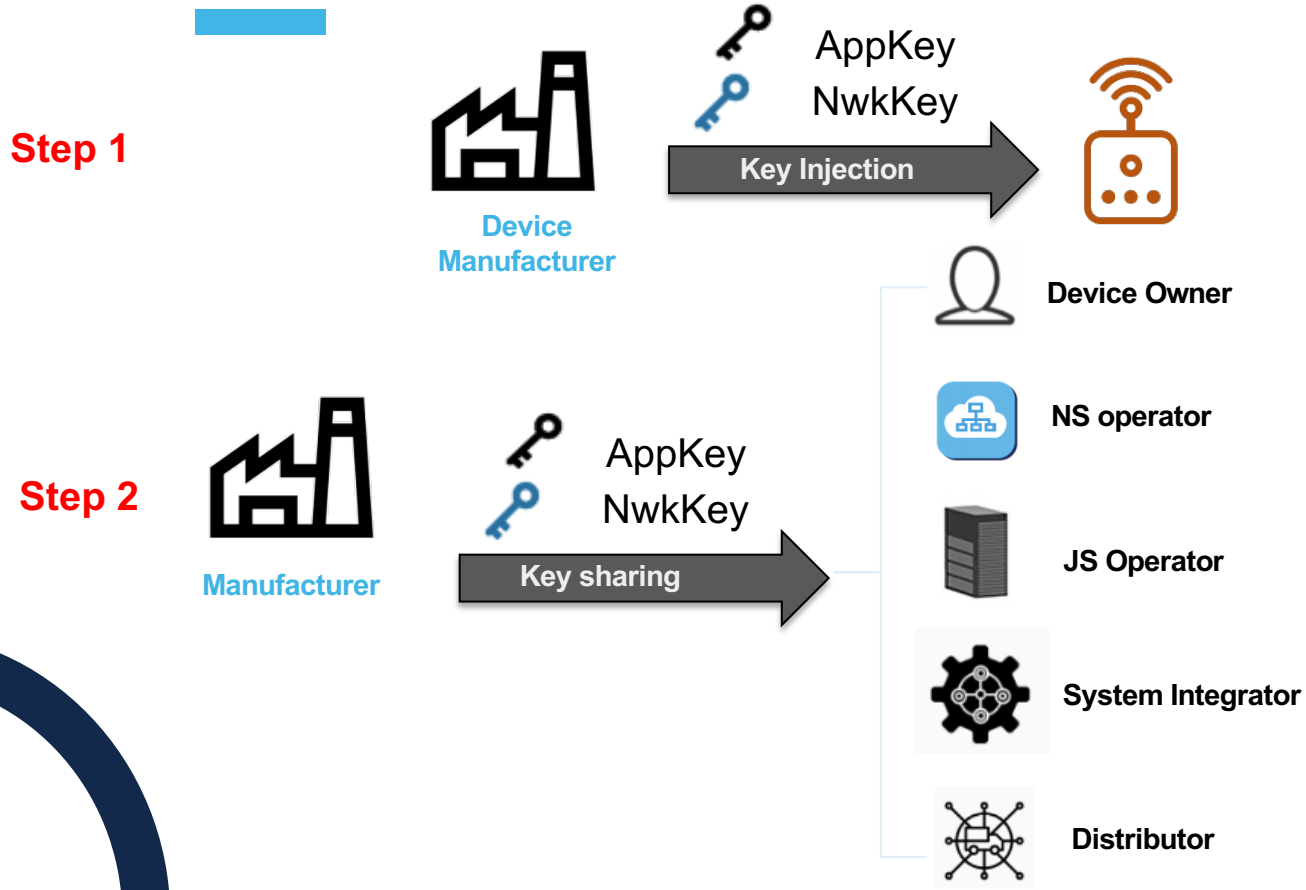
Secure Bootstrapping

The security material that will be used to participate in the network should be delivered in a secure manner

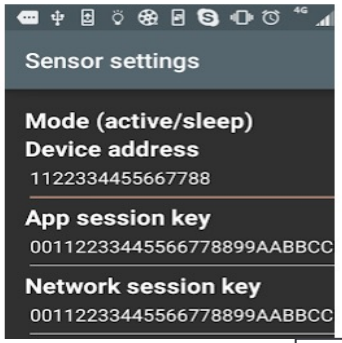
➔ **How ?**

Asymmetric cryptography, secure key exchange protocols or out-of-band bootstrapping procedure

The Key sharing challenge (LoRaWAN use case)



How the Keys are shared between different entities?



Accessible via NFC
on mobile phones



Printed behind the device



Sent via mail

Change of network



Solution



Using Secure Element (1/3)

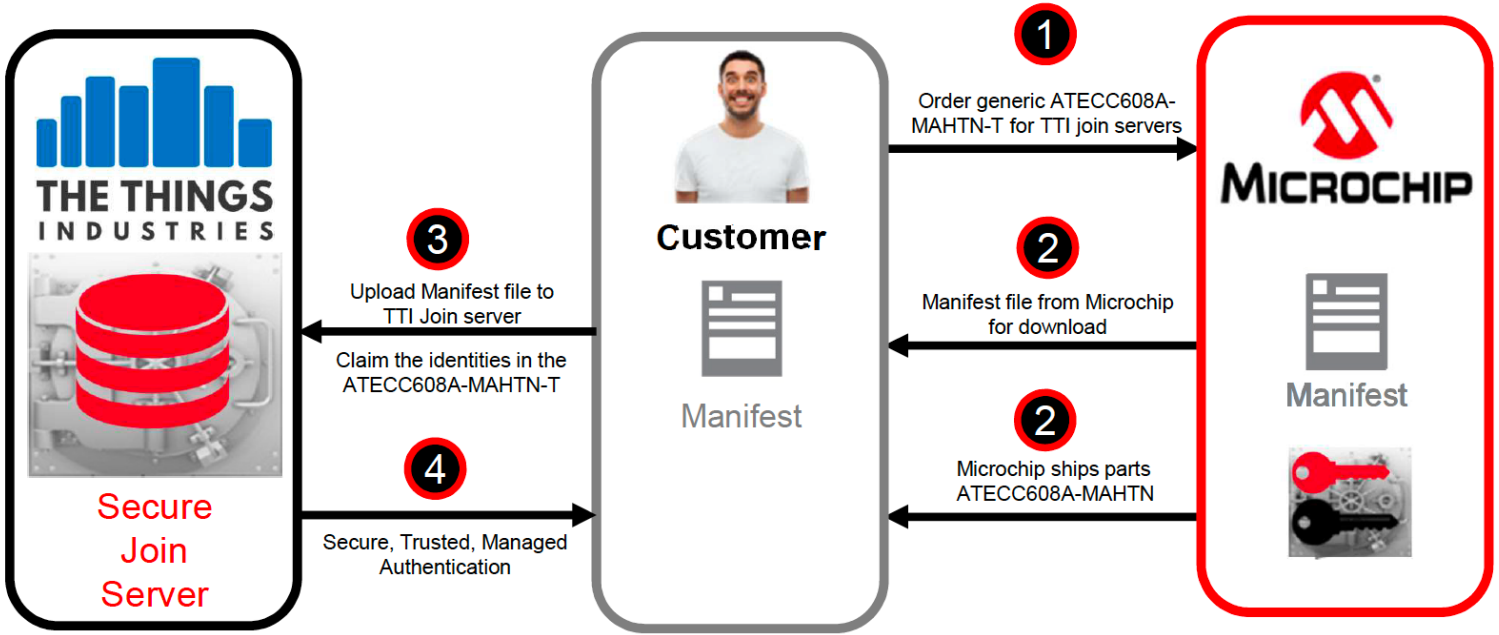


Image Courtesy : Microchip

Using Secure Element (SE) (2/3)

Step:1

THE THINGS INDUSTRIES

Root Key for Provisioning

Root Key for Re-keying

Step:2

MICROCHIP

Step:3



Orders LoRa Devices with Secure elements from Microchip

Using Secure Element (SE) (3/3)

Step:4



Step:5



The Manifest contains the Device IDs

Step:6

TTI JS claims the ownership of the device ID via the Manifest



Fixing Key-sharing issues via SE

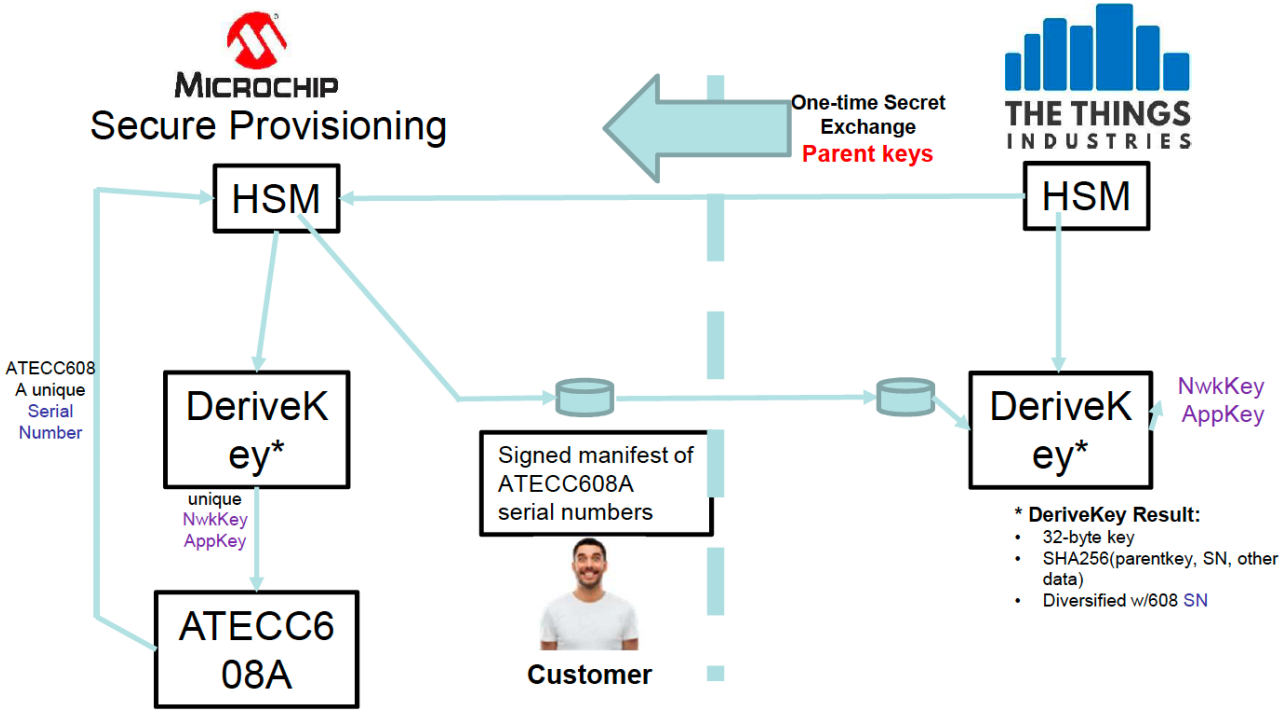


Image Courtesy : Microchip

Re-keying using SE

Step:1



Plans to move to a New JS



New JS

Step:2

THE THINGS INDUSTRIES



Root Key for Re-keying

New Root Key for the New JS



Step:3

THE THINGS INDUSTRIES





New JS



The problem of « many » in IoT


STANDARDS

Autonomic Networking Integrated Model and Approach (ANIMA) - IETF WG

The goal of this working group shall be to develop one or more protocol specifications (or extensions to existing protocols) to address the following problem areas. These were selected to according to the analyzed technical gaps
in draft-irtf-nmrg-an-gap-analysis:
o Discovery for autonomic nodes
o Negotiation for autonomic nodes
Starting point: draft-carpenter-anima-gdn-protocol
o Bootstrapping a trust infrastructure
Starting point: draft-pritikin-anima-bootstrapping-keyinfra
o Separated Autonomic Control Plane
Starting point: draft-behringer-anima-autonomic-control-plane

Device fabrication using Bootstrapping Remote Secure Key Infrastructure (BRSKI)



Manufacturer certificate + Private Key

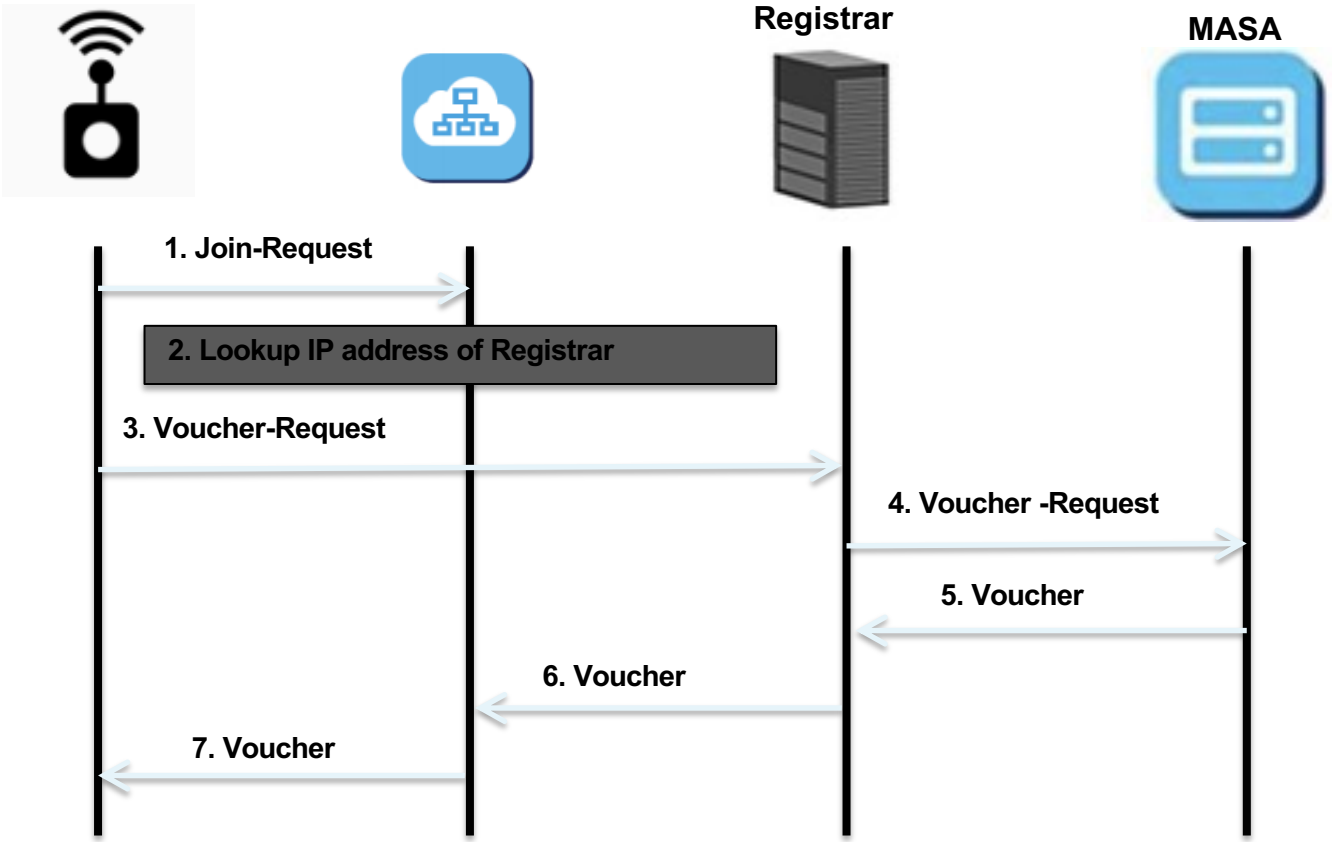
Registrar



MASA



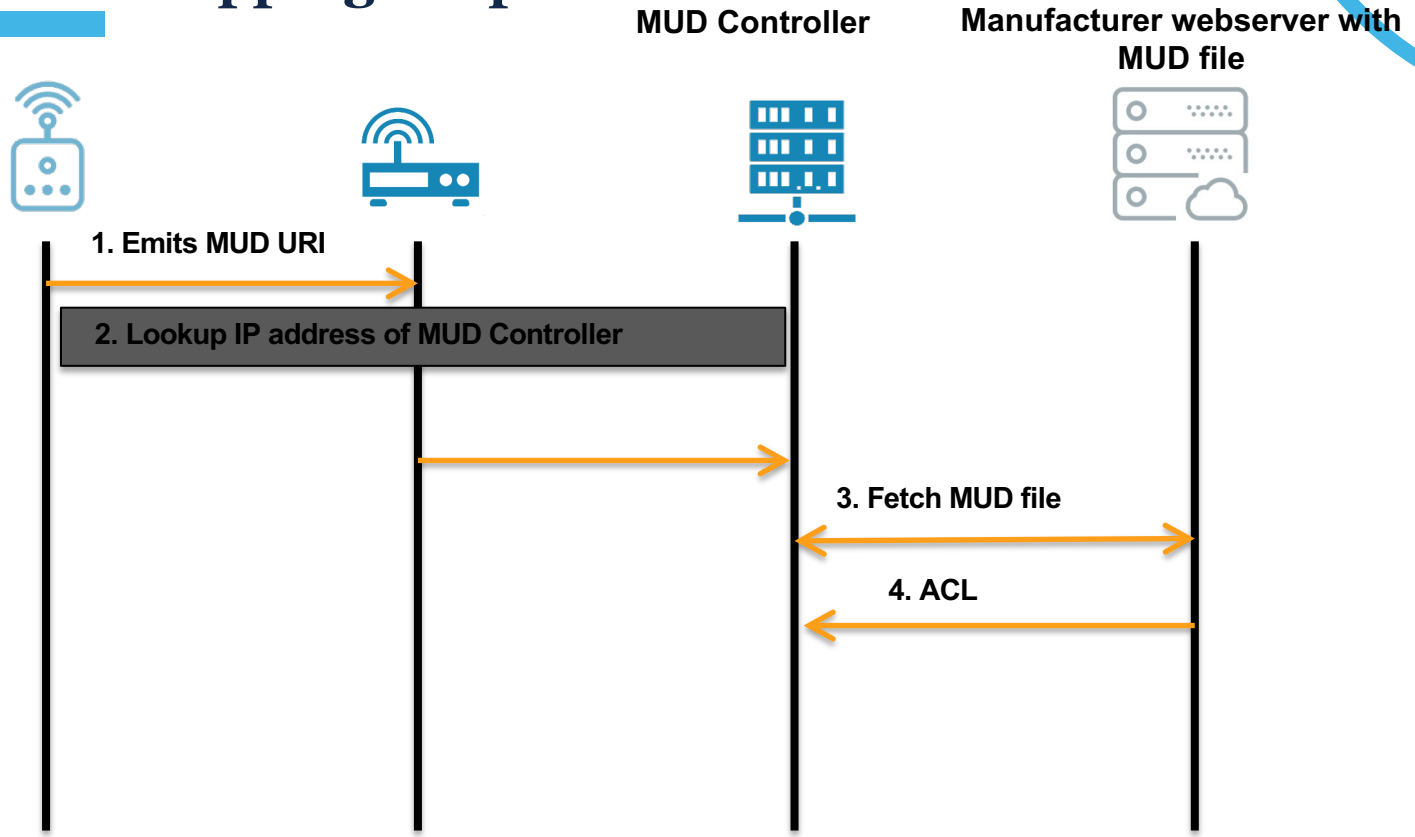
BRSKI Bootstrapping simplistic flow



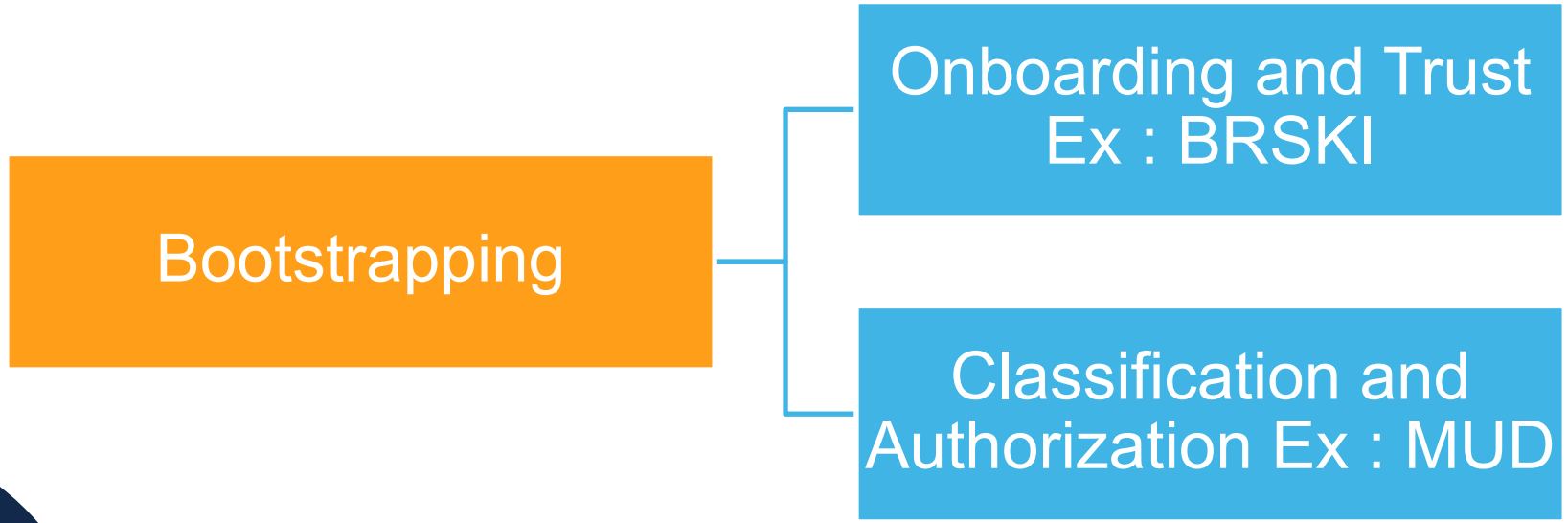
Operational and Management Are (OPSAWG) - IETF WG

The focus of the work will be on topics that govern the behavior or WGs in the O&M area (e.g., manageability requirements) and on small, highly focused projects that don't merit a WG of their own or belong to WGs that have already concluded (e.g. advancement of documents on the standards track, application statements, extensions of MIB modules).

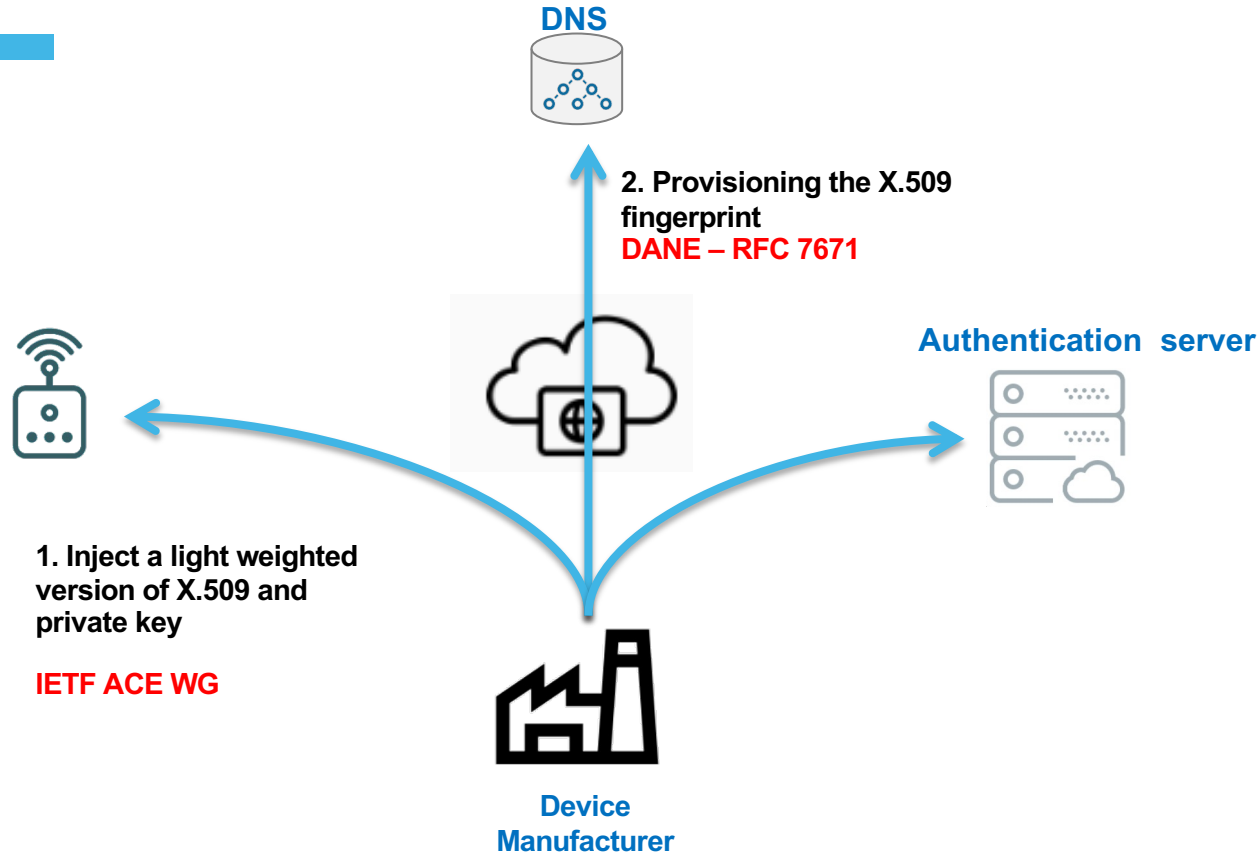
Manufacturer Usage Description (MUD) Bootstrapping simplistic flow



Device fabrication using Bootstrapping Remote Secure Key Infrastructure (BRSKI)



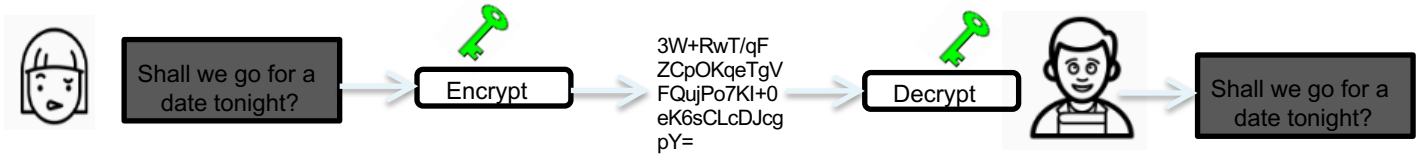
Bootstrapping using DNS infrastructure as the PKI



Merci !
Questions ?

Types of Encryption

Symmetric Keys



Asymmetric Keys

1. **Alice & Bob agree on two +ve integers : 17 and 3 (generator)**
2. **Alice chooses a random number '15' and does the computation (3^{15}Mod17 = 6) and sends the result as Public Key to Bob.**
3. **Similarly Bob chooses a random number '13' and does the computation (3^{13}Mod17 = 12) and sends the result as Public Key to Alice**
4. **Alice takes bob's public result and does the computation to create the shared key (12^{15}Mod17 = 10)**
5. **Similarly Bob takes Alice's public result and create the shared key (6^{13}Mod17 = 10)**

