

# Wi-Fi Repeater Onboarding – full zero touch

This document describe the bootstrapping methods for Wi-Fi EasyConnect onboarding of Repeater devices to an EasyMesh Multi-AP network.

## Revision History

Revision	Last updated	Author	Description
1.0	17-Sep-2025	Anjan Chanda <anjan.chanda@genexis.eu>	First version. Defines vendor specific PA frames and how DPP-URI from an unconfigured Enrollee Repeater is passed on securely to the Gateway-AP for EasyConnect onboarding.
1.1	9-Oct-2025	Anjan Chanda <anjan.chanda@genexis.eu>	Describes another ('mobile app assisted') method for transferring DPP bootstrapping URI of Repeater securely by reading from legacy WiFi QR Code label.

# 1. Bootstrapping

When the bootstrapping methods defined in Wi-Fi Easy Connect Specification cannot be used, the Vendor-specific methods outlined in this document can be adopted to transfer Enrollee's Bootstrapping Public Key to a DPP Configurator.

This bootstrapping method achieves full zero-touch onboarding of a Wi-Fi Extender to the Multi-AP network.

Example-1 shows a DPP URI string with bootstrapping key from the secp256r1 (or P-256 or NIST-256) curve. The key data in the URI is base64 encoded SubjectPublicKeyInfo of Enrollee's public bootstrapping key.

*Example 1:*

`DPP:I:SN=4774LH2b4044;M:010203040506;V:2;K:MDkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDIgADURzxmttZoIRIPWGoQMV00XHWCAQIhXruVWOz0NjlkIA=;;`

The goal is to transfer such URI in a secured manner to the DPP Configurator.

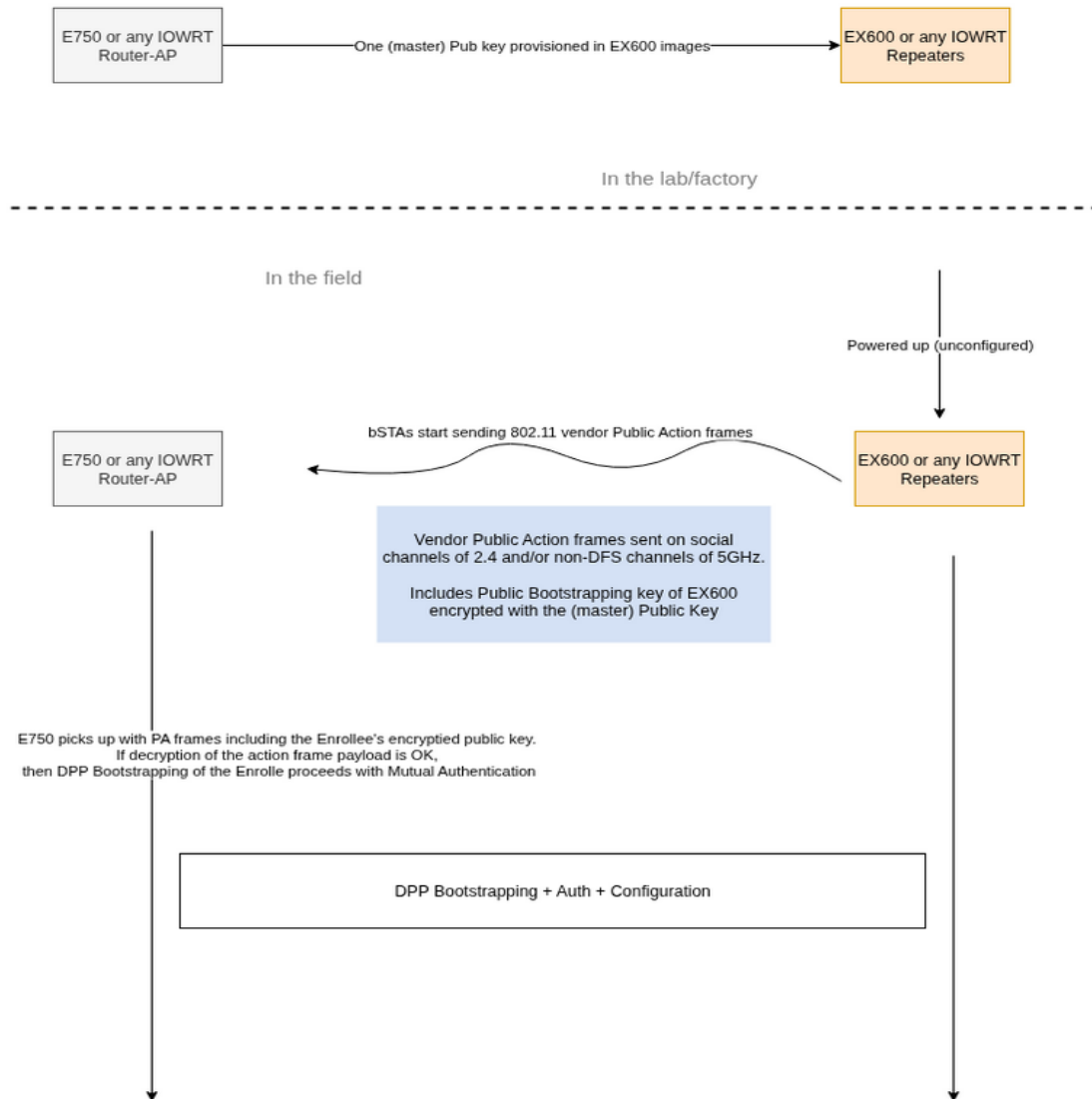
## 1.1 Vendor-specific Public Action

After power up, an un-provisioned Repeater will send 802.11 Public Action (PA) frames on the 2.4GHz social channels (1, 6 and 11). The format of PA frame is given in Table-1.

*Table 1: Table-1: Public Action frame for Full-Zero-Touch Bootstrap URI transfer*

Field	Field size (in bytes)	Value	Description
Category	1	4	Public action
Action	1	9	Vendor specific type
OUI	3	B4-56-FA	IOPSYS OUI
OUI Type	1	10	Vendor specific
Payload	variable	variable	Encoded DPP bootstrapping URI

Section 2 describes the encoding and decoding process of the DPP bootstrapping URI.  
 Section 3 describes the format of the Encoded DPP bootstrapping URI payload.  
 Section 4 describes how the received PA frame is Tunneled from a proxy-Agent/AP to the Controller.



Full Zero Touch provisioning of Extenders - DPP bootstrapping using in-band transfer of the Enrollee's bootstrapping key

Figure 1: Full zero touch onboarding flow.

## 2. DPP bootstrap URI encode and decode

1. The Enrollee (Repeater) generates an **ephemeral P-256 keypair** (epk, esk).
2. Enrollee (Repeater) has Configurator's (or AP's) static **P-256 public key B**.
  - This is pre-programmed in Repeater's firmware image, and/or available in it's production data.
3. Repeater computes **ECDH**:  $Z = \text{ECDH}(\text{esk}, B)$
4. Repeater runs Z through a **KDF** (e.g. HKDF-SHA256) to derive symmetric keys:
  - **K\_enc** for encryption (e.g. AES-SIV)
  - optionally **K\_mac** for authentication.
5. Repeater encrypts the plaintext **M** (e.g. DPP URI) with **K\_enc** producing ciphertext **C** and auth tag **T**.
6. Repeater sends to the Configurator AP: **(epk, C, [T])**
7. **Configurator AP** receives it and computes  $Z' = \text{ECDH}(\text{bsk}, \text{epk})$ . Runs the same KDF and gets same **K\_enc**. It then decrypts and validates the encrypted payload to get M. If decryption and the auth tag verification happens successfully, the Configurator AP accepts M as **authentic and confidential**.

### Encoding parameters:

- Curve: **NIST P-256** (secp256r1)
- KDF: **HKDF-SHA256**
- Symmetric cipher: **AES-SIV** (Authenticated encryption with associated data)
- Ephemeral key: generated per message which provides forward secrecy

For the DPP URI from *Example-1*, the encoded URI payload using above approach is following -

**B -**

04e46b0a35235325fb4a5d9a005993f33f2f92561c8556a8eb0899a8914230af7f4b92fc24318779e06  
2c51b89014f74363fee8baa9323c8023d5d6900b7299fde

**epk -**

04d8b4f5093c8c4df884eff2308305edcff36e62a94c88fa532bf5f4a34245b761c16ecd55185b1ab09e2  
5e8993a229f08ae44c57774049c117bb53b5140469366

**C -**

d02825b9955401e8c30b42a663836f3da36fc68c288dcb99d266356dff2b14f687374ca1ae3f2c260aa  
06f38b487e183e3643e1b4c786fdd6d7b8d73b6ff2596b05f0df1b454a2f5b53cae9d4bad06a6900abad  
04768aefd6a6b2970f7c5a6a32ee82df9e2864367f90f354a8fe61d242dda81882d4322ab825607fa4b

**M -**

DPP:I:SN=4774LH2b4044;M:010203040506;V:2;K:MDkwEwYHKoZlZj0CAQYIKoZlZj0DAQc  
DIgADURzxmttZoIRIPWGoQMV00XHWCAQIhXruVWOz0NjlkIA=;;

### 3. Action frame payload structure

Table 2: Format of encoded DPP URI payload in Public Action frames

Field	Field size (in bytes)	Description
epk_len	2	Length of DER encoded SubjectPublicKeyInfo of Enrollee's ephemeral public key in little-endian format
epk	variable	Hex-string of DER encoded SubjectPublicKeyInfo of Enrollee' ephemeral public key
c_len	2	Length of AES-SIV wrapped DPP URI wrapped data in little-endian format.
c	variable	AES-SIV encoded DPP URI cipher-text

### 4. Transfer of PA from Agent/AP to Controller

After the Agent/AP picks up the vendor-spec PA frame containing the encoded DPP URI payload, it tunnels the frame to the Controller via the EasyMesh **Tunneled message CMDU (0x8026)**.

*NOTE: Although DPP Bootstrapping URI Notification message CMDU (0x8031) may appear to be more appropriate for transferring the received URI from the Agent/AP to Controller, the same cannot be used. This is because the DPP URI payload is encrypted and only the Controller can decode it.*

The **STA\_MAC** field in **Source Info TLV** of the Tunneled message should contain the macaddress of the bSTA interface of the sending Repeater device.

A new 'Type' **0x0a** is defined for **Tunnel Message Type TLV** to denote the Vendor-specific Public Action frame containing the encoded DPP URI payload.

## 5. Mobile ‘app’ assisted transfer of DPP URI

The method outlined here leverages the legacy non DPP compatible Wi-Fi QR code printed on a Repeater device’s label.

The legacy Wi-Fi QR code holds the factory default Wi-Fi ssid and key. An app running on a mobile device, which is connected to the main/Gateway-AP, can read this QR code label. The app transfers this Wi-Fi key to the Gateway-AP (or DPP Configurator) securely. How the app transfers this Wi-Fi key to the main/Gateway-AP is implementation specific.

After the Controller receives the Wi-Fi key, it stores the key in a secured store (f.e. file) and also use it to decrypt the encoded PA frames received subsequently from the Repeater device.

The Repeater upon power up, starts sending vendor specific PA frames (OUI Type = **0x0b**), which has the format described in Table-3 below.

Table 3: Table-1: Public Action frame type 0x0b

Field	Field size (in bytes)	Value	Description
Category	1	4	Public action
Action	1	9	Vendor specific type
OUI	3	B4-56-FA	IOPSYS OUI
OUI Type	1	11	Vendor specific
c_len	2		Length of AES-SIV wrapped DPP URI wrapped data in little-endian format.
c	variable		AES-SIV encoded DPP URI cipher-text

The payload ‘c’ is AES-SIV encrypted using a key, which is derived from the same Wi-Fi key printed on the QR code label.

In this method, no a-priori AP side public key is needed in the Repeater.