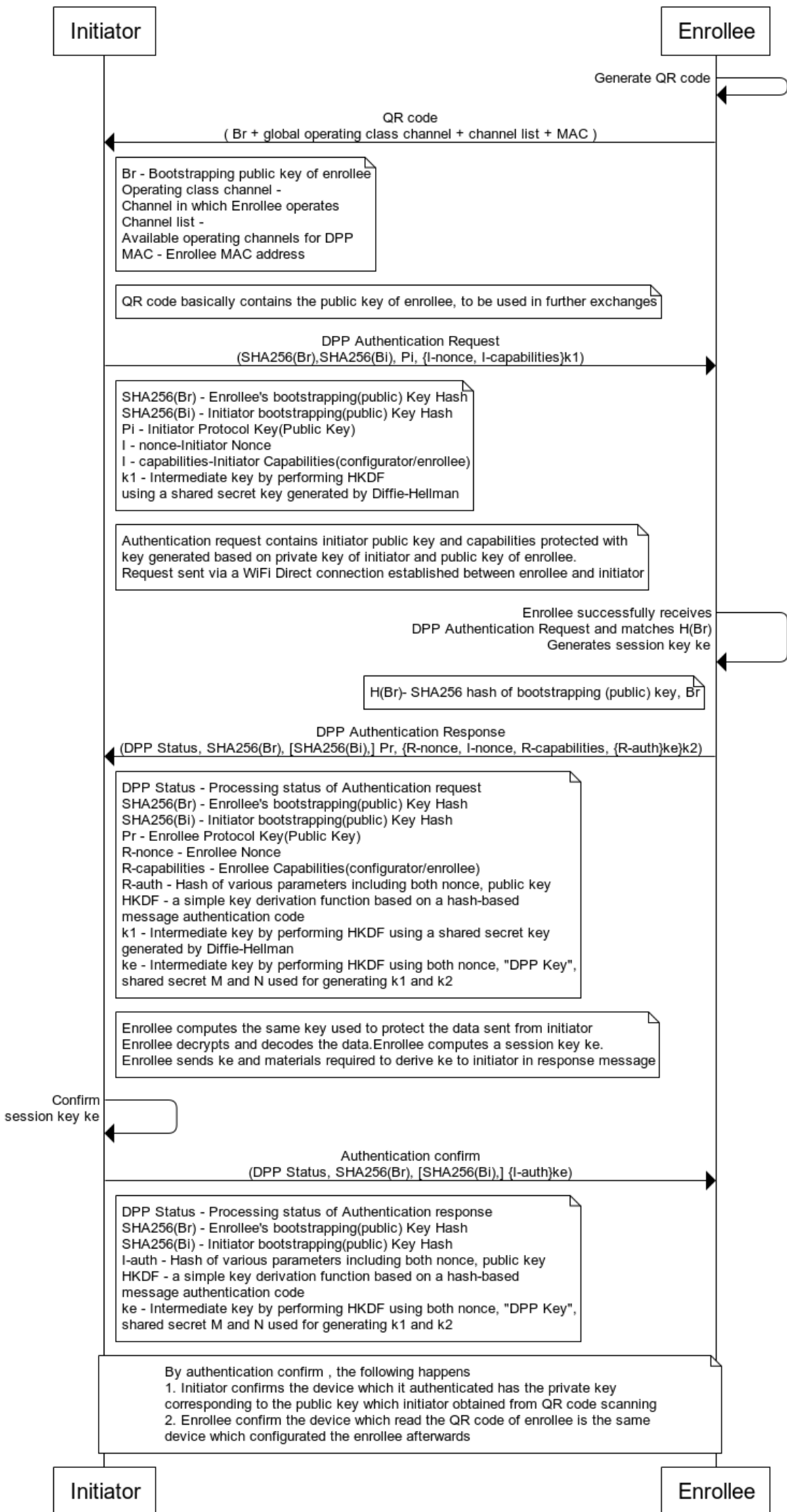


Authentication Sequence



DPP Configuration Sequence

Configurator

Enrollee

DPP Configuration request
(E-nonce, configuration attributes)ke)

E-nonce - Enrollee nonce
configuration attributes - JSON encoded data structure with details of Device Name, Wi-Fi Technology, Network Role(sta/ap)
ke - Key generated during DPP authentication

Enrollee notifies the configurator about the device name and role it will take(station or ap) in an encrypted format(using key ke)

DPP Configuration response
(DPP Status, {E-nonce, configuration object}ke)

DPP Status - Status of processing configuration request
E-nonce - Enrollee nonce
ke - Key generated during DPP authentication
configuration object - JSON encoded data structure with below details
-Wi-Fi Technology
-SSID
-WPA2 Passphrase and/or SAE password
-Authentication and key management type(psk, dpp, sae, psk+sae),
-Pre-shared key
-C-sign-key - public signing key of configurator
-DPP Connector - Json web signature with the following parameters
---groups - An array of groups(groups of devices)
---groupId - A string denoting one of the groups. The owner of the connector can connect to devices in that group only
---netRole - Role assigned to owner of this connector in group(ap/sta)
---netAccessKey - public analog of the enrollee protocol key
---expiry - life of the netAccessKey

The configurator creates a confirmation message with the details of SSID and security parameters and sends it to enrollee after encrypting

Parse DPP Configuration response
Obtain provisioning details

By configuration response , Configurator provides the below details to enrollee(used based on Authentication and key management type(akm))
1. The SSID to which the enrollee needs to be connected
2. Passphrase(WPA2 and/or SAE) needed to connect to SSID
3. Pre-shared-key in case of akm-psk
4. C-Sign key for akm=dpp
5. Net Access Key which is the public key in enrollee key pair

In case the akm is dpp, the csign and netaccesskey are used for security and connector contents are used for details of connection

Configurator

Enrollee

DPP Network Introduction

