Firmware update Group wise for NB-IoT devices

Architecture and technology proposal

NOKIA

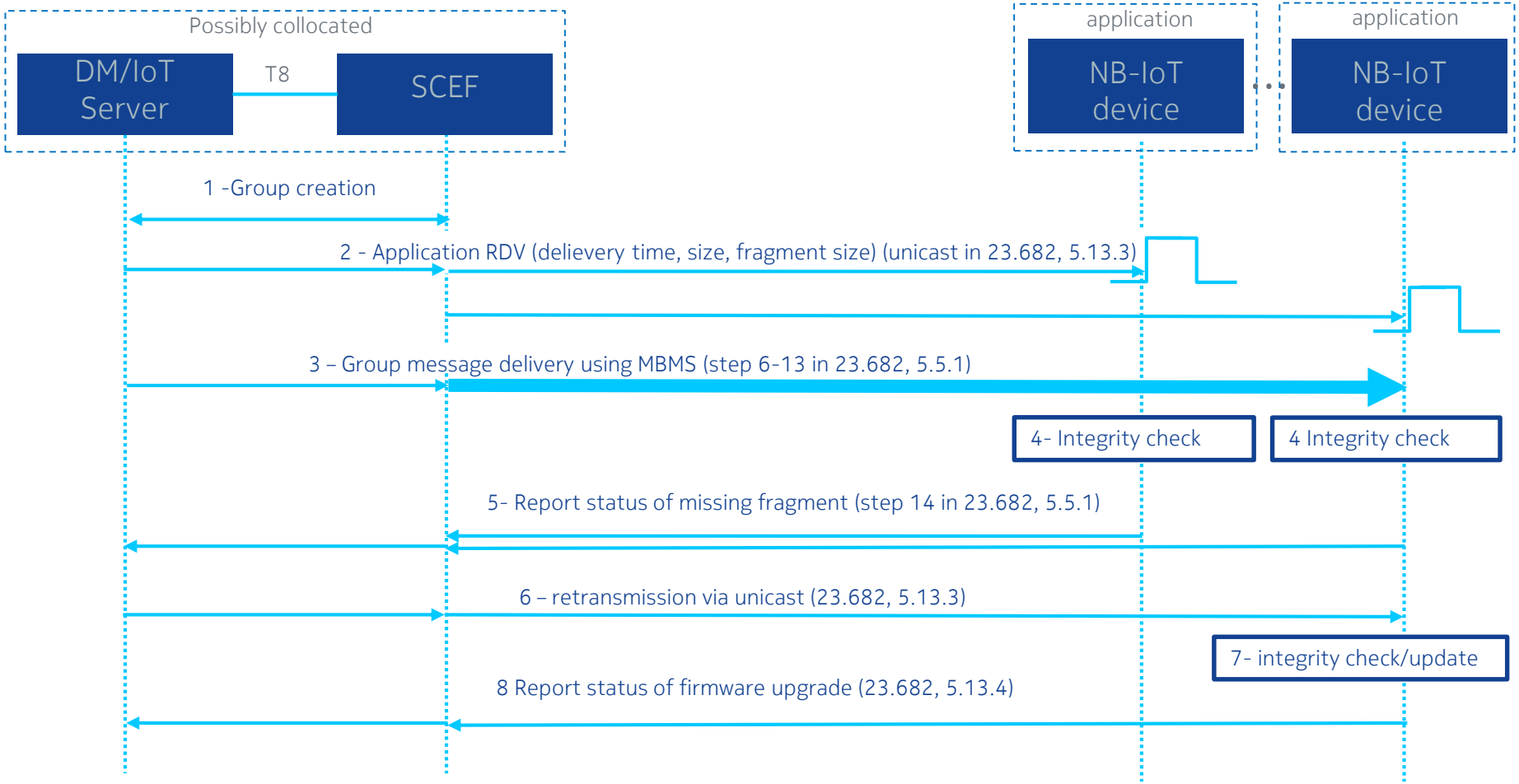
Motivation & Challenges

- Firmware upgrade of NB-IoT devices is important feature to manage the lifecycle of devices
- NB-IoT devices are expected to be deployed for many years (e.g. Smart Meters), firmware upgrade is a business imperative
- Constrained devices:
  - Low power,
  - Limited CPU,
  - Limited memory,
  - Battery operated (more than 10 years
- Non IP based network, while existing firmware update solution have been built for IP
- NB-IoT uses control plane elements

Elements of the solution

- Collocating applications with SCEF in trust domain, management at application level
- **Group management**
  - Static groups
  - Group of devices within a geographical location for a given customer
- Application level **rendez-vous** communicated to targeted by DM
- **Fragmentation and reassembly** mechanism
- **Unicast retransmission** of missing fragments
- **Delta firmware upgrade** (transmit the delta between new and existing firmware)

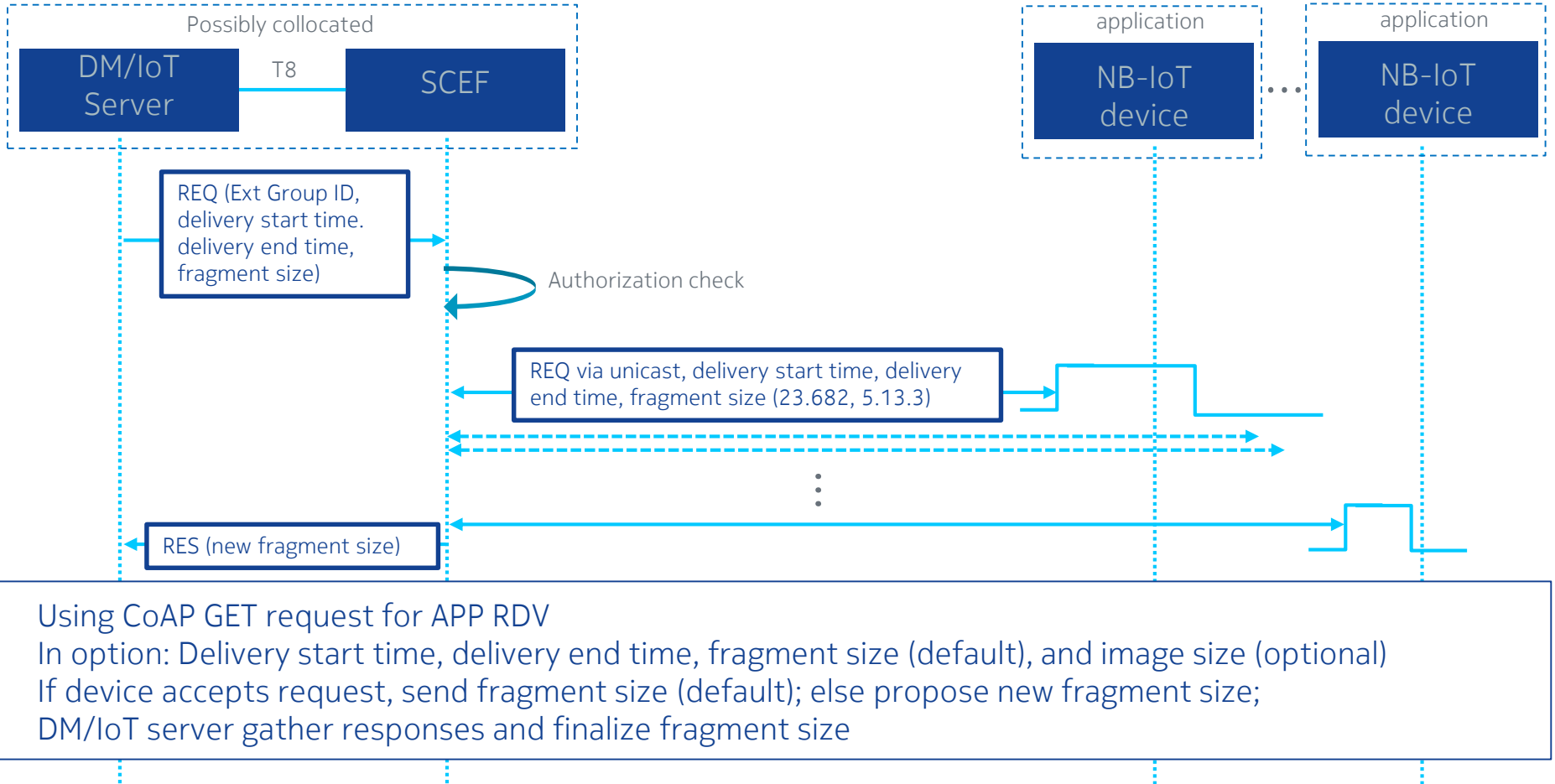
Message flow – pushing mode



Step 1: Group creation

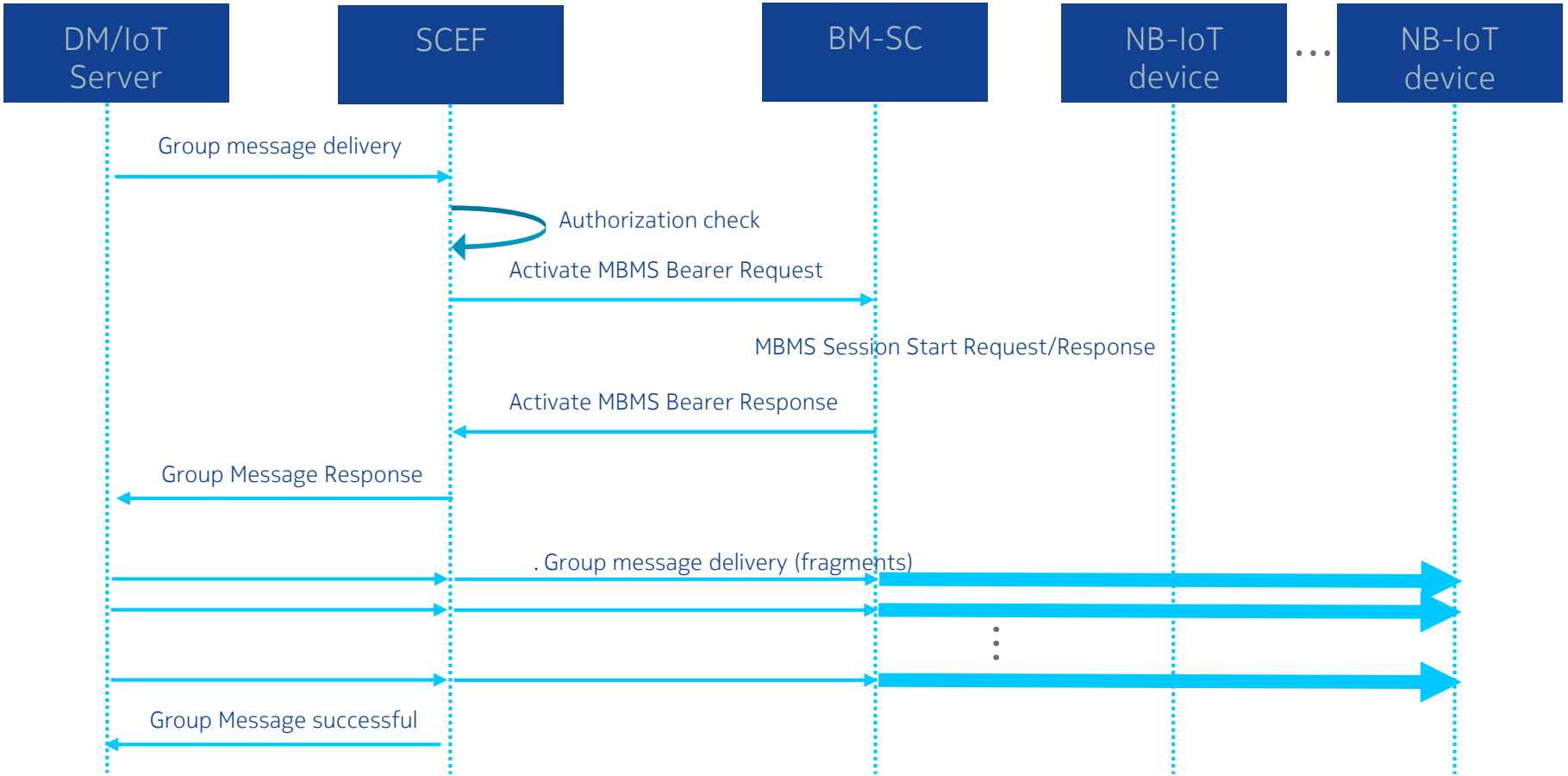
- **Group management**
  - Static groups
  - Using T8 interface for group creation
  - As SCEF is always within the trust domain, applications located on SCEF can belong to the trust domain for collecting parameters and capabilities of devices, e.g., active timer and periodic timer of PSM
  - It assumes that the application provider is the owner of devices, for instance, it has the authority to manage devices including collect parameters and capabilities of devices

Step 2: Application RDV



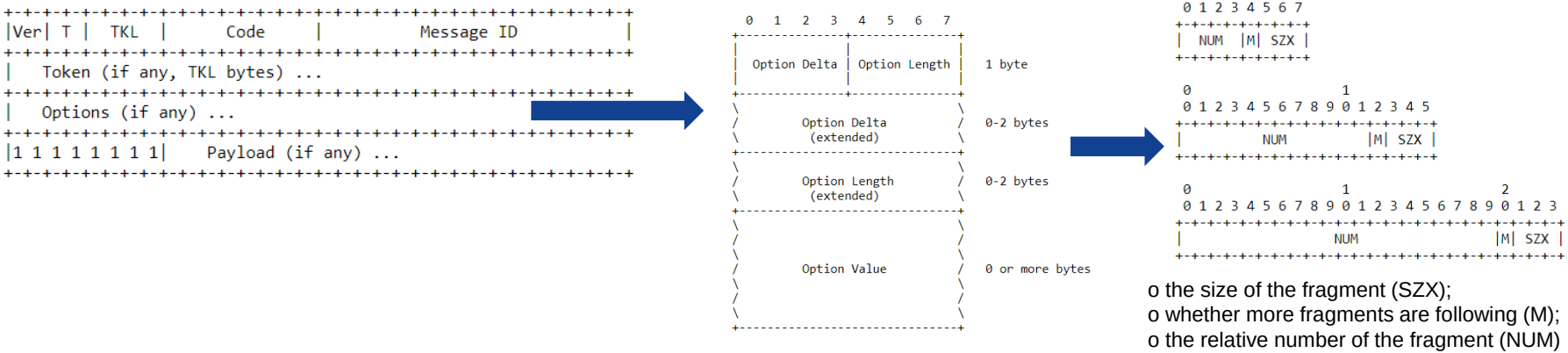
- Using CoAP GET request for APP RDV
- In option: Delivery start time, delivery end time, fragment size (default), and image size (optional)
- If device accepts request, send fragment size (default); else propose new fragment size;
- DM/IoT server gather responses and finalize fragment size

Step 3: Group message delivery (step 6-13 in 23.682, 5.5.1)



Step 3 (continue): message fragment

- Using Non-confirmable CoAP POST to NB IoT device (no application layer ack)
- Using CoAP option area to address fragment size, M flag, and the number of fragment;



o the size of the fragment (SZX);
o whether more fragments are following (M);
o the relative number of the fragment (NUM)

- Device: If M = = 0, device will start integrity check – step 4; or start integrity check after [delivery end time]

Summary

- Integrate this Group solution for SCEF method of firmware upgrade.
- Note for single device upgrades already LwM2M v1.1 solution would be sufficient.