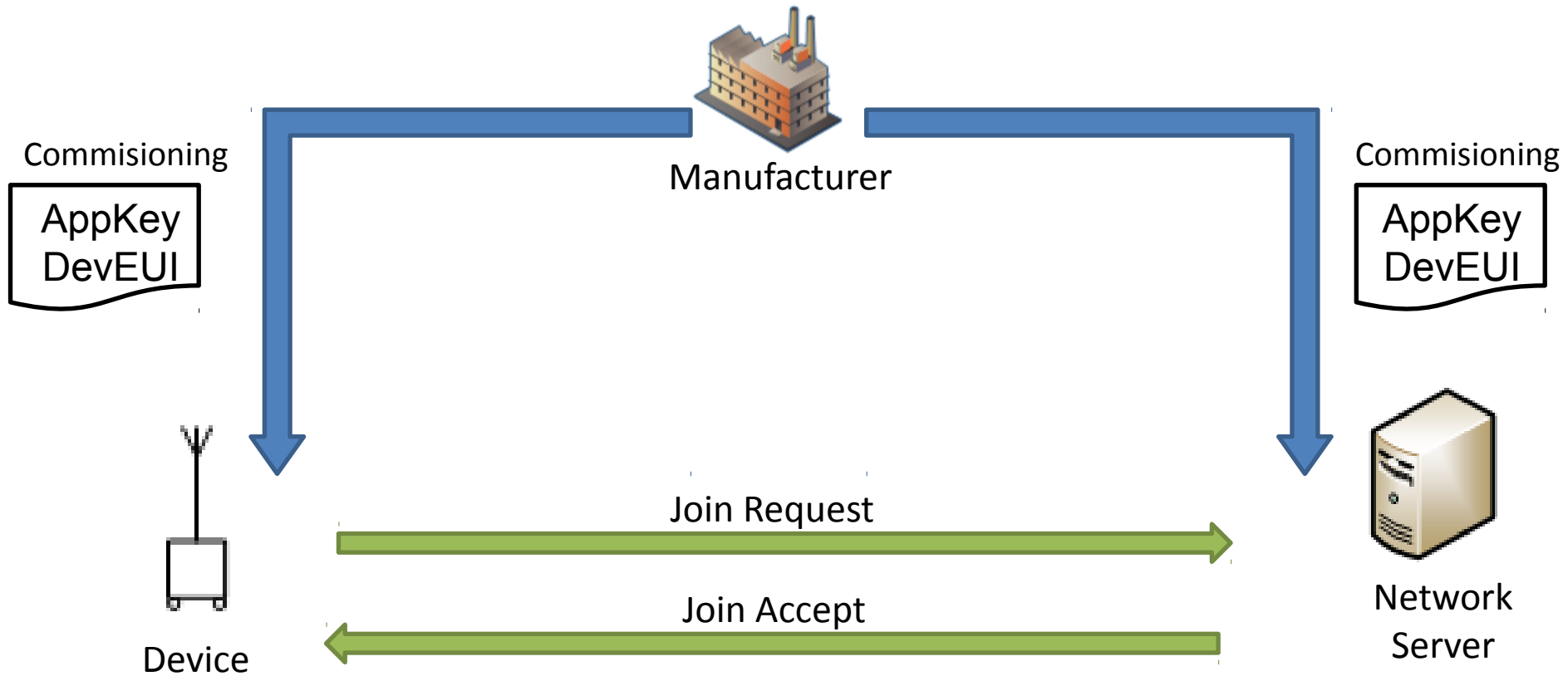# LoRaWAN Authentication with RADIUS

Dan Garcia-Carrillo (University of Murcia)
Rafael Marin-Lopez (University of Murcia)
Arunprabhu Kandasamy (Acklio)
Alexander Pelov   (Acklio)

LoRaWAN Authentication -
LoRaWAN 1.0 Join procedure

1. **Commissioning**
2. **Over the Air Activation (Join Procedure)**

Manufacturer

Commisioning

AppKey
DevEUI

Commisioning

AppKey
DevEUI

Join Request

Join Accept

Device

Network
Server

LoRaWAN Authentication - Message Definition

- ## The request (join-request)

Size(bytes)	8	8	2
Join Request	AppEUI	DevEUI	DevNonce

- ## The Response (join-accept)

Size(bytes)	3	3	4	1	1	16(opt)
Join Accept	AppNonce	NetID	DevAddr	DLSettings	RxDelay	CFList

LoRaWAN Authentication with RADIUS

1. **Commissioning**
2. **Over the Air Activation (Join Procedure)**
3. **RADIUS Extension**

Commisioning

AppKey
DevEUI

Join Server
(RADIUS server)

Commisioning

AppKey
DevEUI

Manufacturer

Access Accept
(Join Accept,
 AppSKey **,
 NwkSKey)

Access Request
(Join Request,
Join Accept*)

Join Request

Join Accept

Device

Network Server
(RADIUS client)
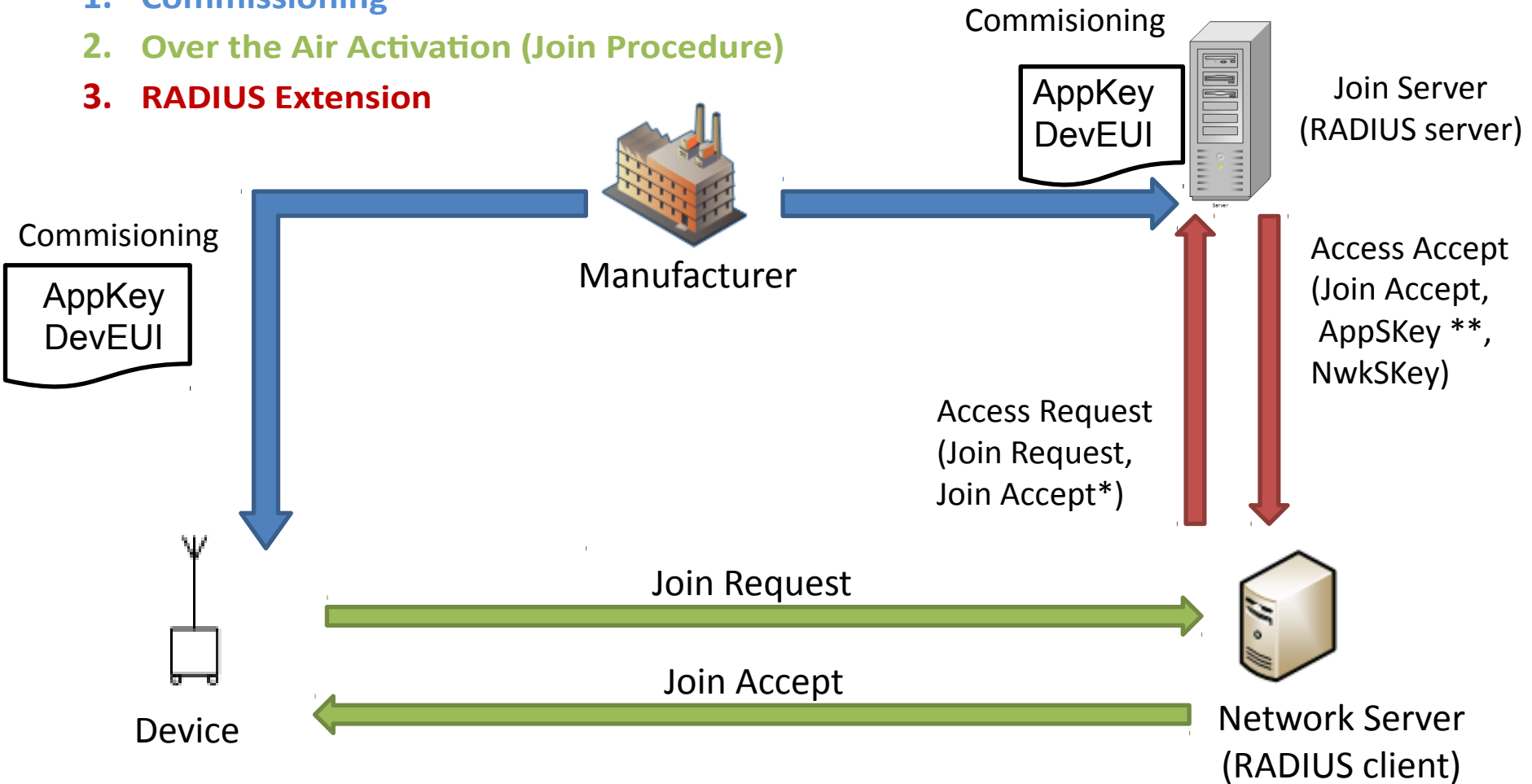
* MIC field empty. To be calculated by the RADIUS server.
** Optional field.

LoRaWAN Authentication with RADIUS

- New RADIUS Attributes
  - JoinRequest (containing the join-request)
  - JoinAnswer (containing the join-accept)
  - Nwkskey (containing the NwkSKey)
  - Appskey (containing the AppSKey, optional)

LoRaWAN Authentication with RADIUS

- Open Issues
  - The Join Request has AppEUI indicating the Organization, but to route JR and JA* through the AAA infrastructure we need to specify a realm (e.g. um.es).

00 11 22 33 44 55 66 77 88 99 AA ⟷ um.es

  - A mechanism for matching the AppEUI to the domain name of the organization is needed.
  - Possible solution a similar approach as in [RFC7043] using DNS.

LoRaWAN Authentication with RADIUS

- ## Proof of concept Implementation

- End Device (Nemeus)
   - usb key with Java app

- Base station (ExpEmB)
   - Intel Atom, 2GB RAM

- Lora Network server(Acklio)
   - implemented in golang

- RADIUS(bronze1man)
   -implemented in golang

Next: Implementation in
FreeRADIUS

- [Lora Base station] www.expemb.com/en/product/multi-connectivity-service-gateway-sgwmc-x86lr-12132/
- [LoRa Network Server] www.ackl.io
- [End-device] www.nemeus.fr/en/mk002-usb-key
- [Radius] github.com/bronze1man/radius

LoRaWAN Authentication with RADIUS