

Introduction to LoRaWAN and Security Aspects

Johan Stokking
@johanstokking

CTO and Co-Founder, The Things Industries
Tech Lead and Co-Founder, The Things Network
Chair, Security Working Group, LoRa Alliance

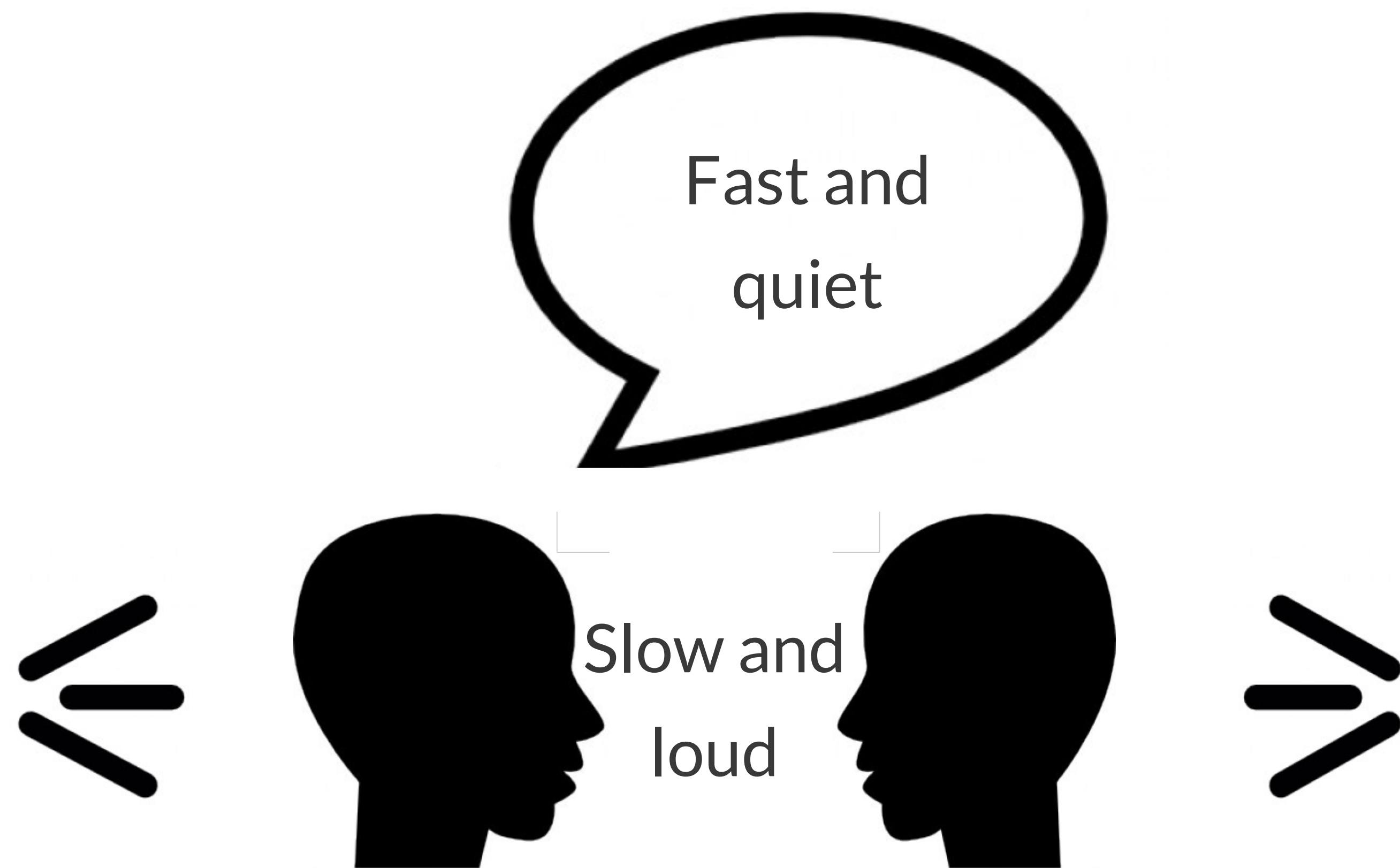


**Up to tens of thousands
devices per gateway**

Low power and small messages

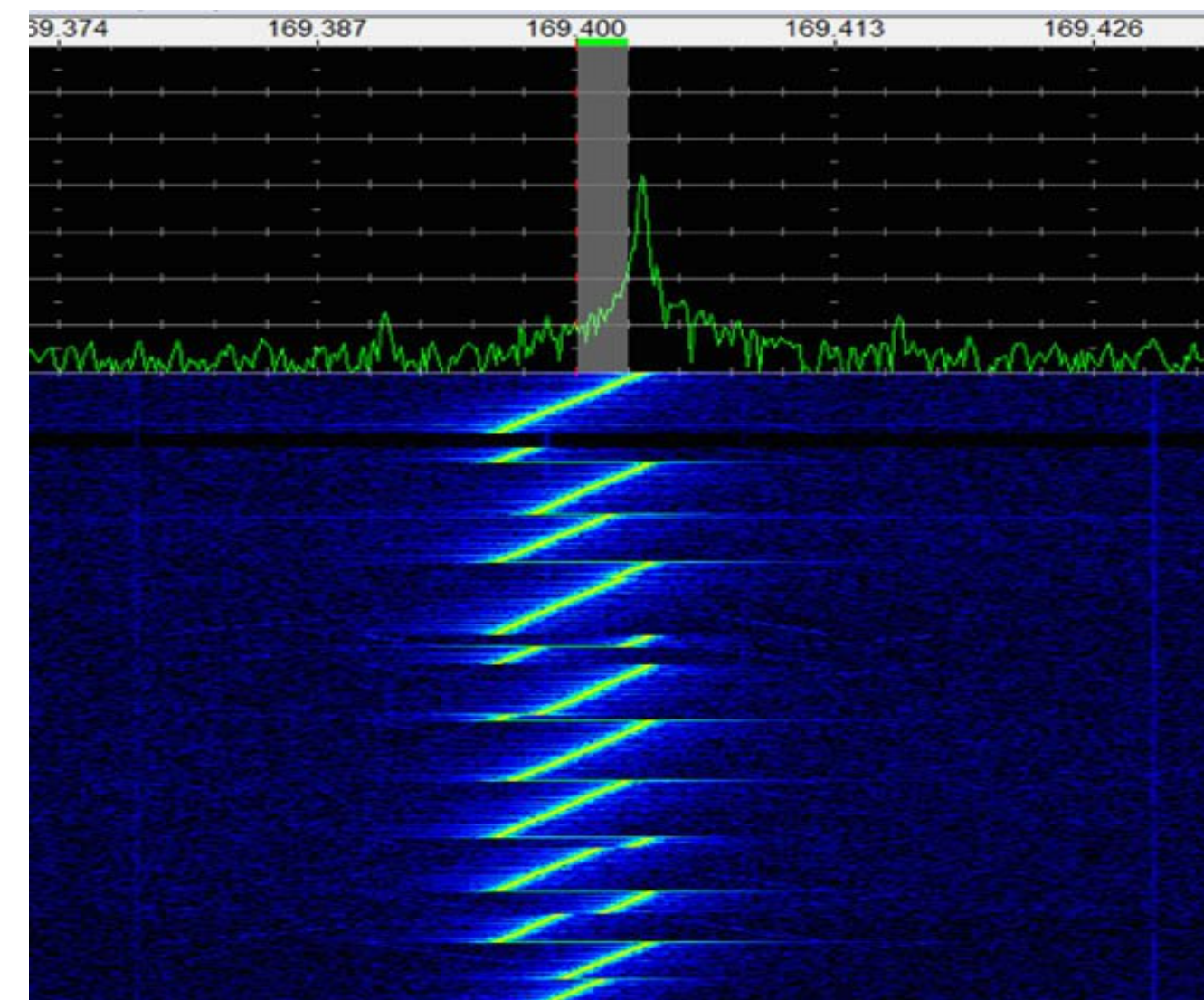
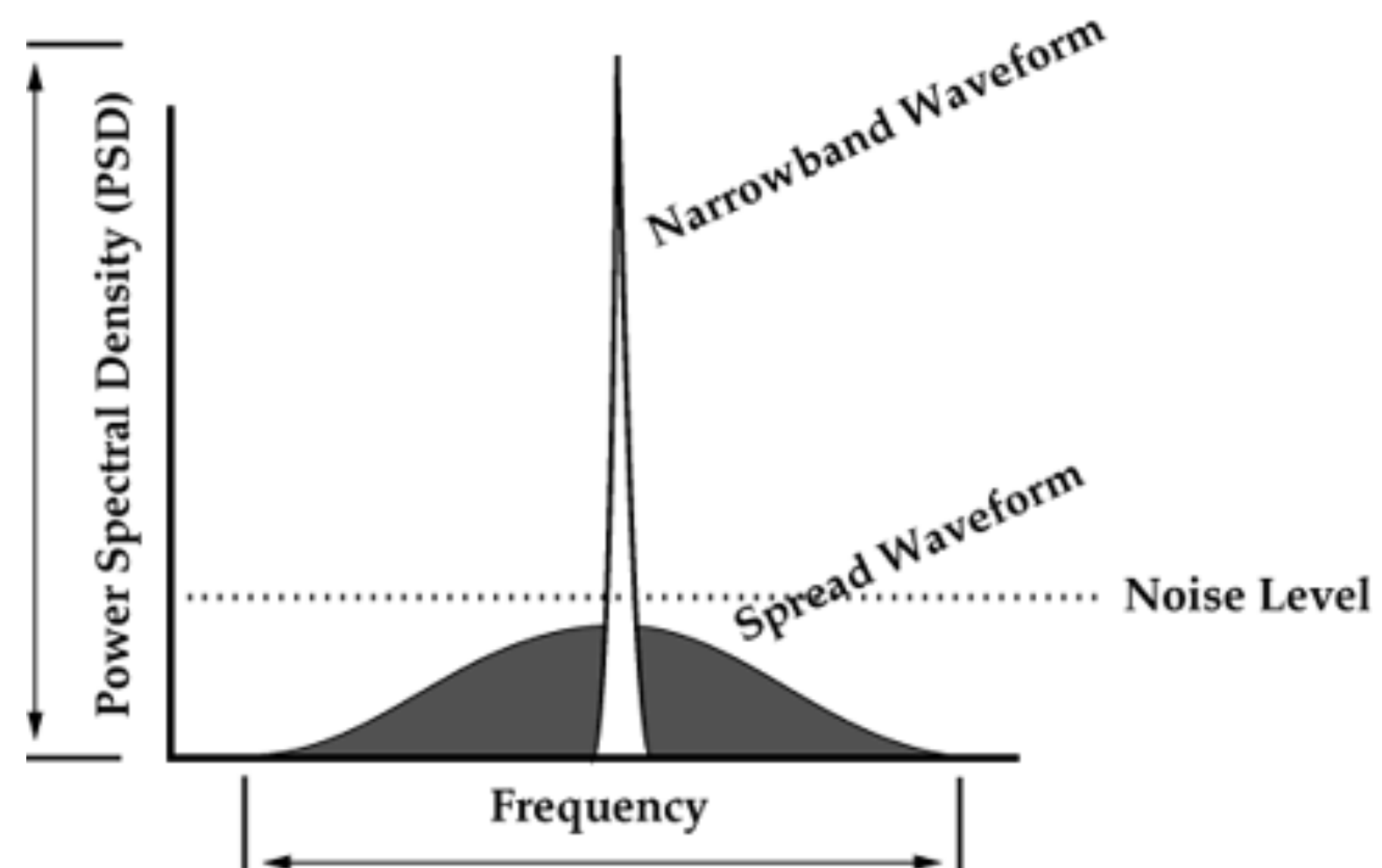


**so devices can run on solar panels
for months or years on batteries**



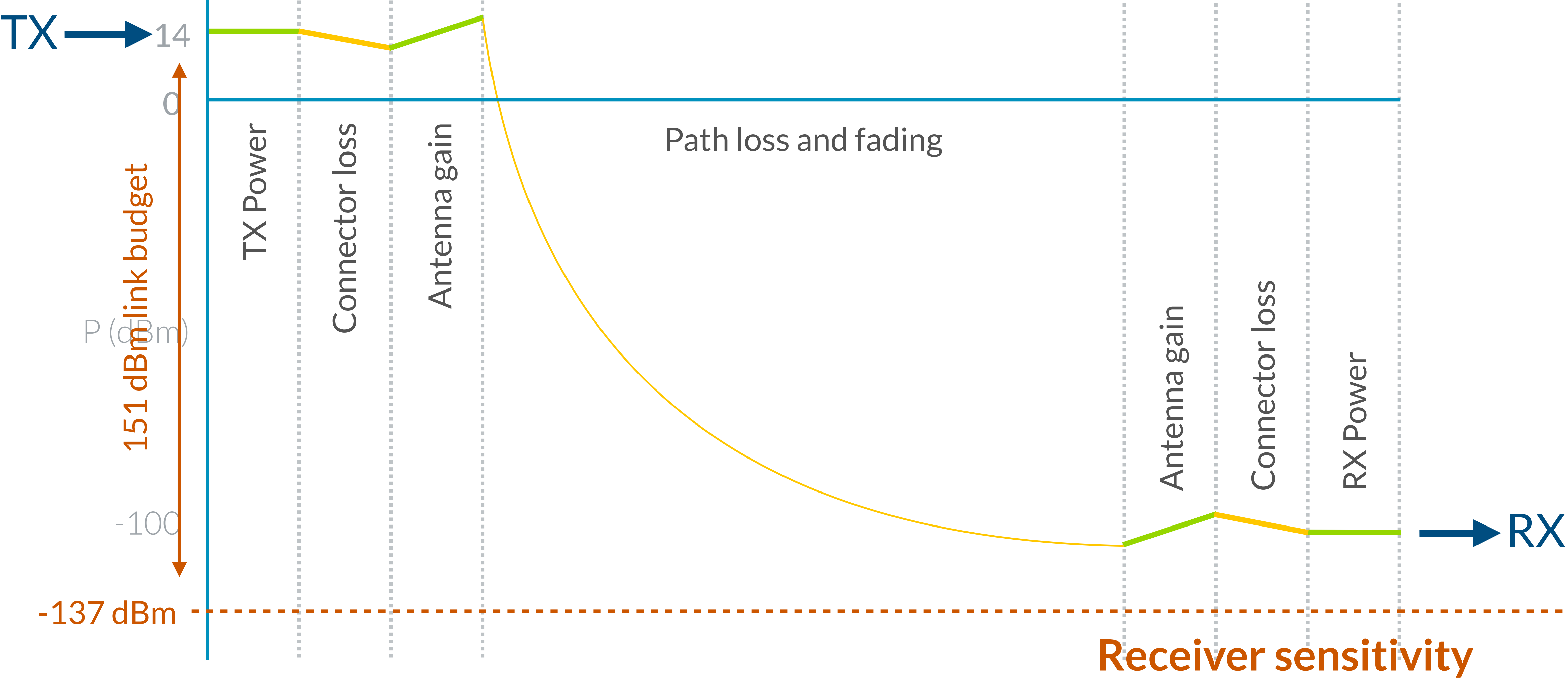
LoRa: modulation for wireless transmission

Spread-spectrum; robust to interference, multi-path and fading



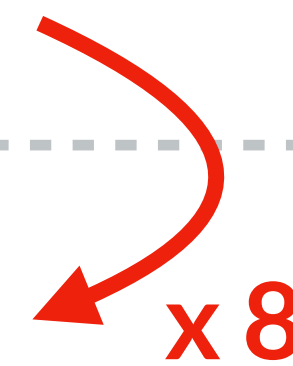
40 BBAA0126 80 D204 2A A50EDB DB2A5FFA

LoRa wireless performance



LoRa wireless performance

	TX Power	RX Sensitivity	Link budget
Wi-Fi	20.5 dBm	-75 dBm	95.5 dBm
LoRa	14 dBm	-137 dBm	151 dBm
NB-IoT	23 dBm	-129 dBm	152 dBm



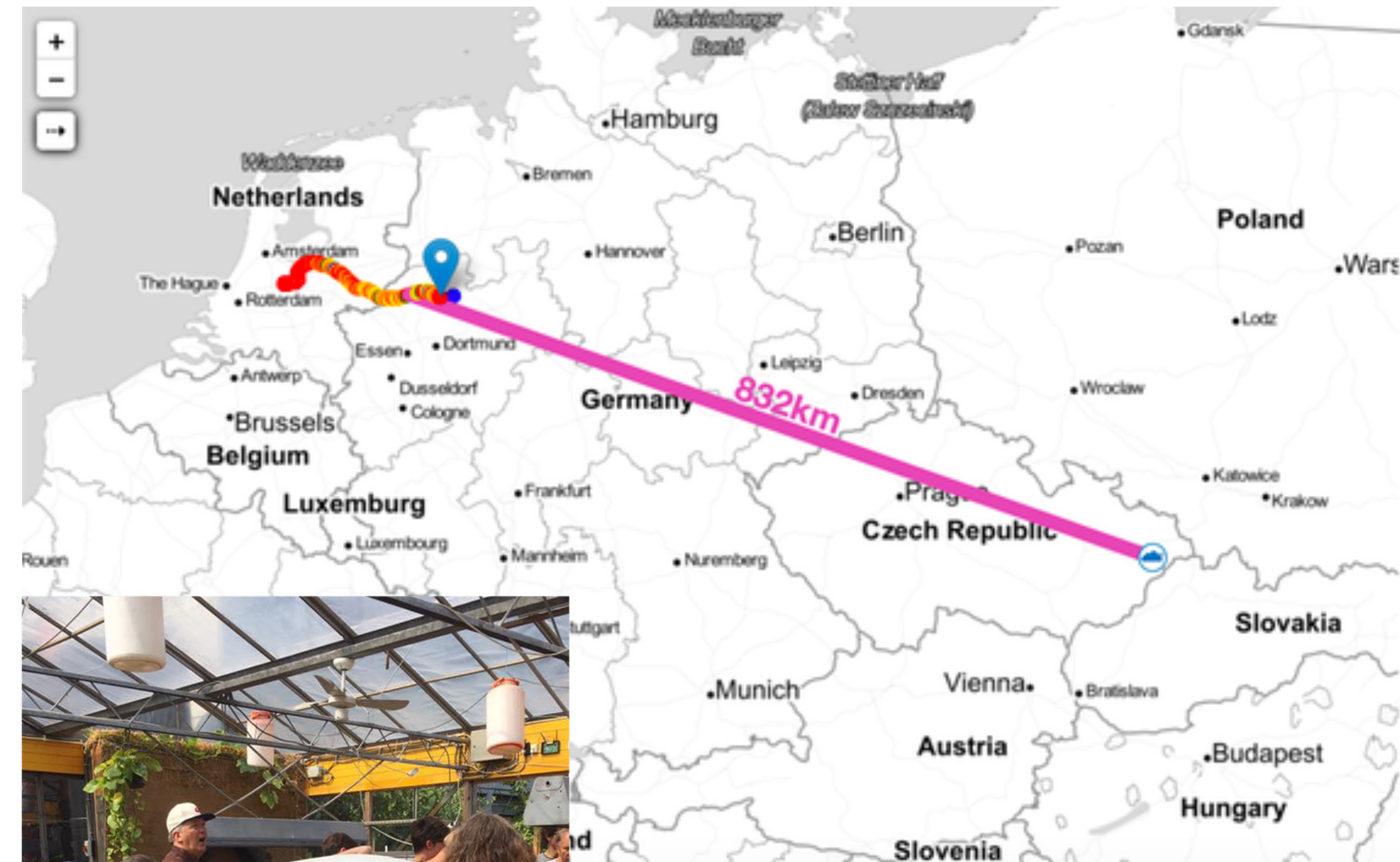
$$FSPL = 20 \log_{10}(d) + 20 \log_{10}(f) + 20 \log_{10}\left(\frac{4\pi}{c}\right) - G_t - G_r$$

LoRa wireless performance

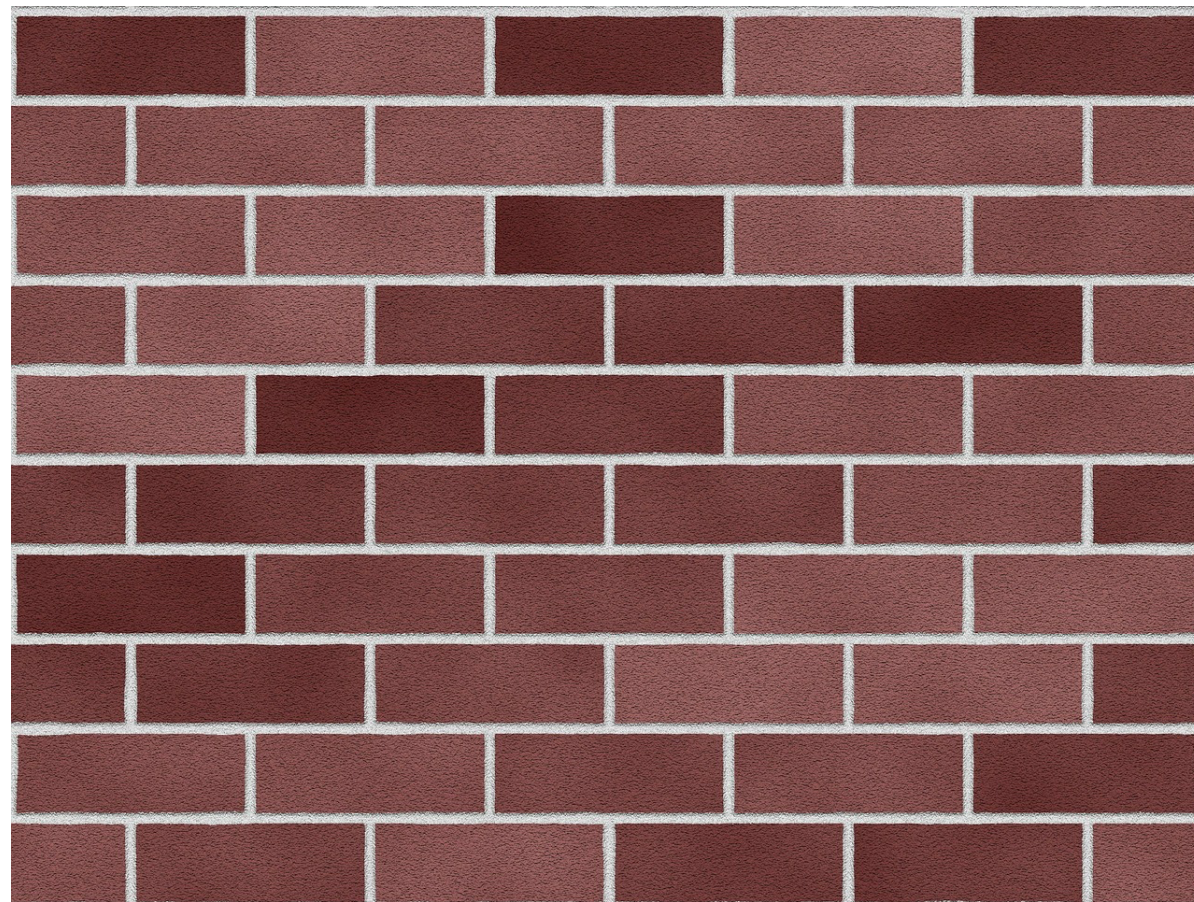
Theoretical maximum in free space is
850 km (US915 regulations)

Wi-Fi is only **550 meters**

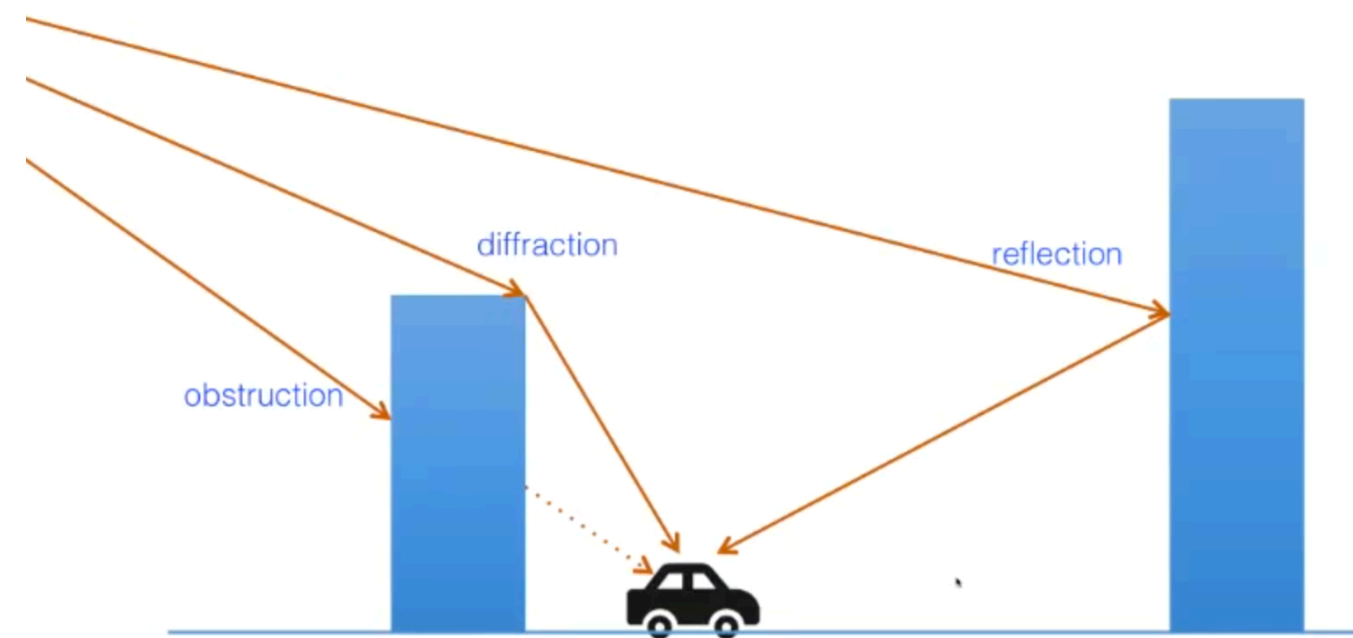
The Things Network
Community set the
world record: **832 km**
using a helium balloon



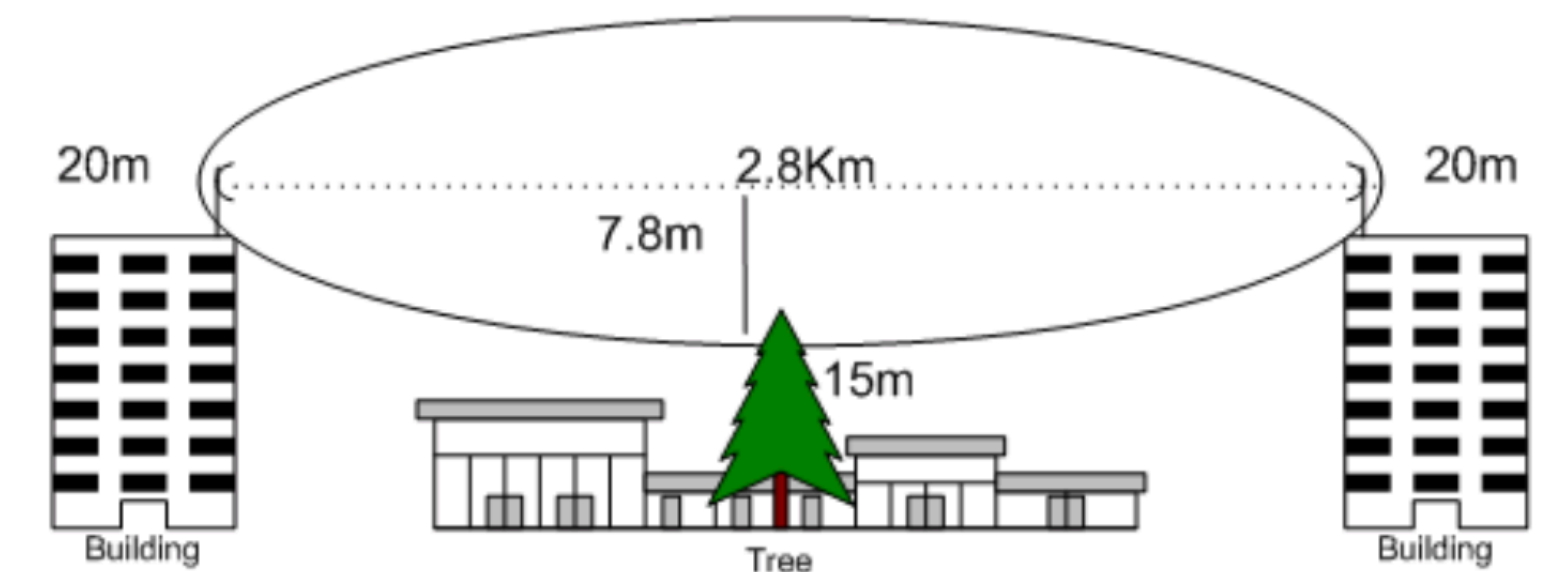
Free space is only in space



Attenuation



Reflection and diffraction



Fresnel zone



Complementary to:



Differentiators and benefits

Public and private deployment options

Firmware updates over the air

Geolocation

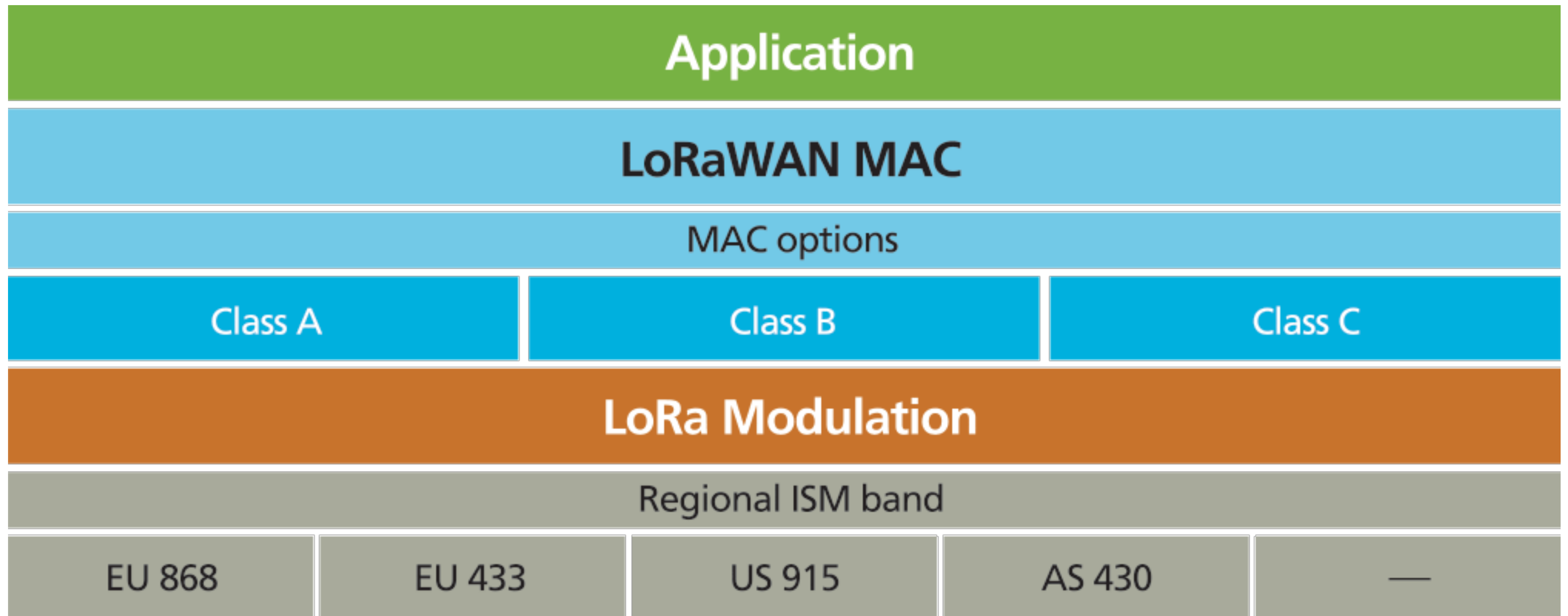
End-to-end security

Supports 10+ years battery lifetime

Long range

Deep indoor penetration

LoRa and LoRaWAN





Open, crowd sourced and decentralized community network

Largest global LoRaWAN network

142
Countries

**900
Cities**

11150 Gateways

106K Developers

11M
Packets/day



Empower with tools



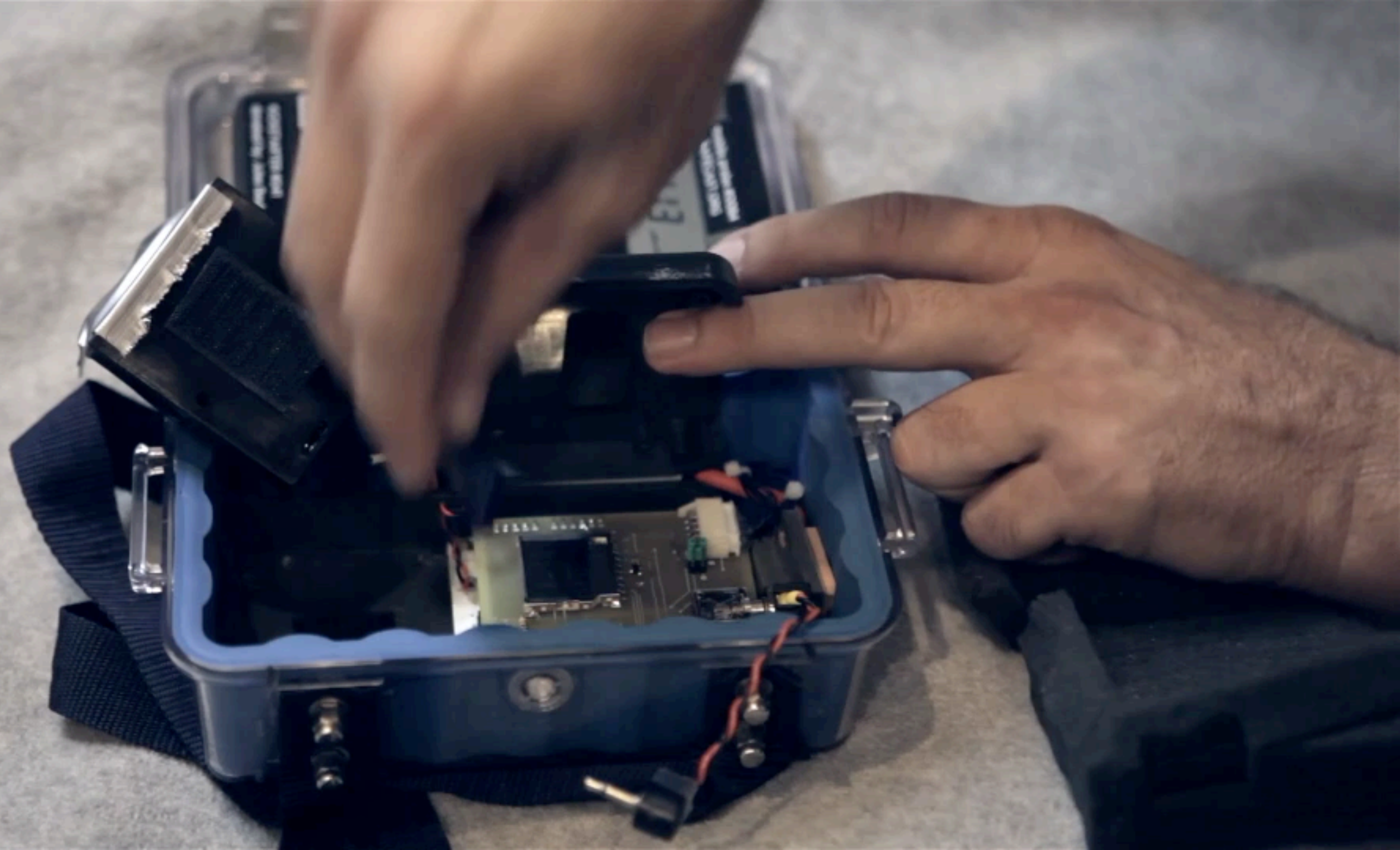


Rabobank

SODAQ









S5
Strausberg Nord
S9
S7
Schönefeld
Ahrensfelde
2 min
7 min

482 417-3



The Things Enterprise Stack

Best in class LoRaWAN Network Server

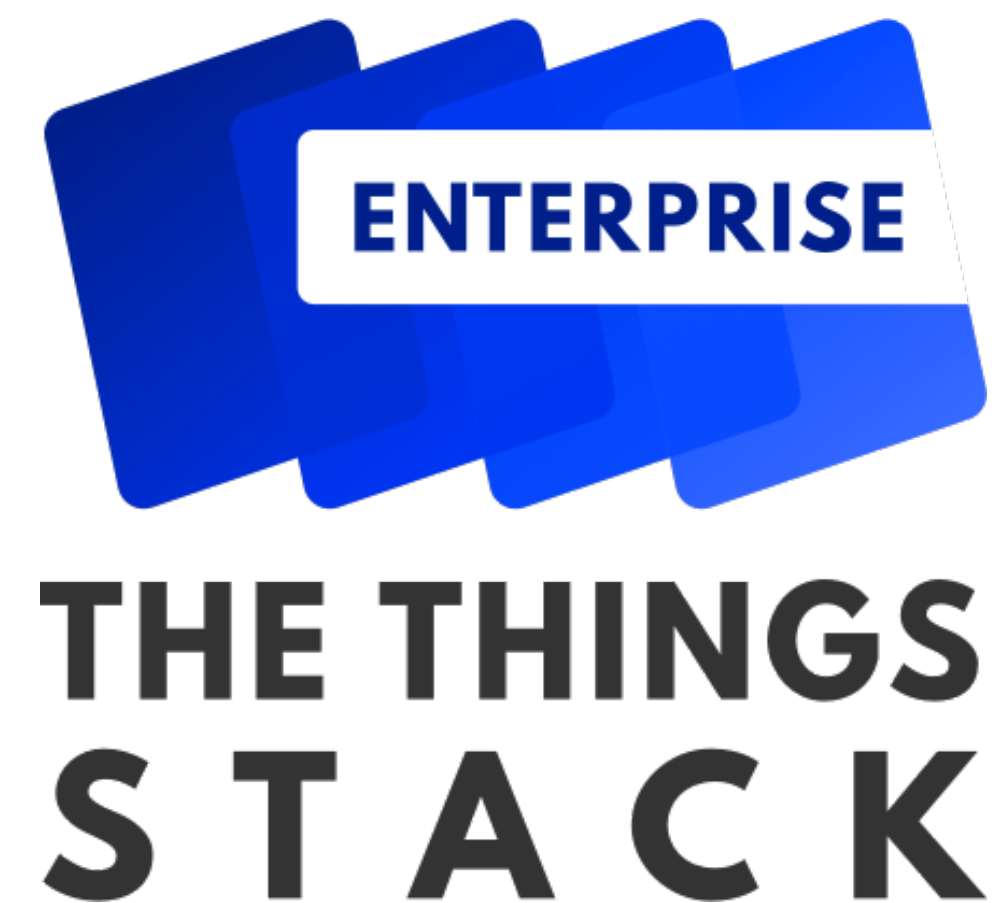
Built from scratch for scale, security, global distribution

API first design and loosely coupled components

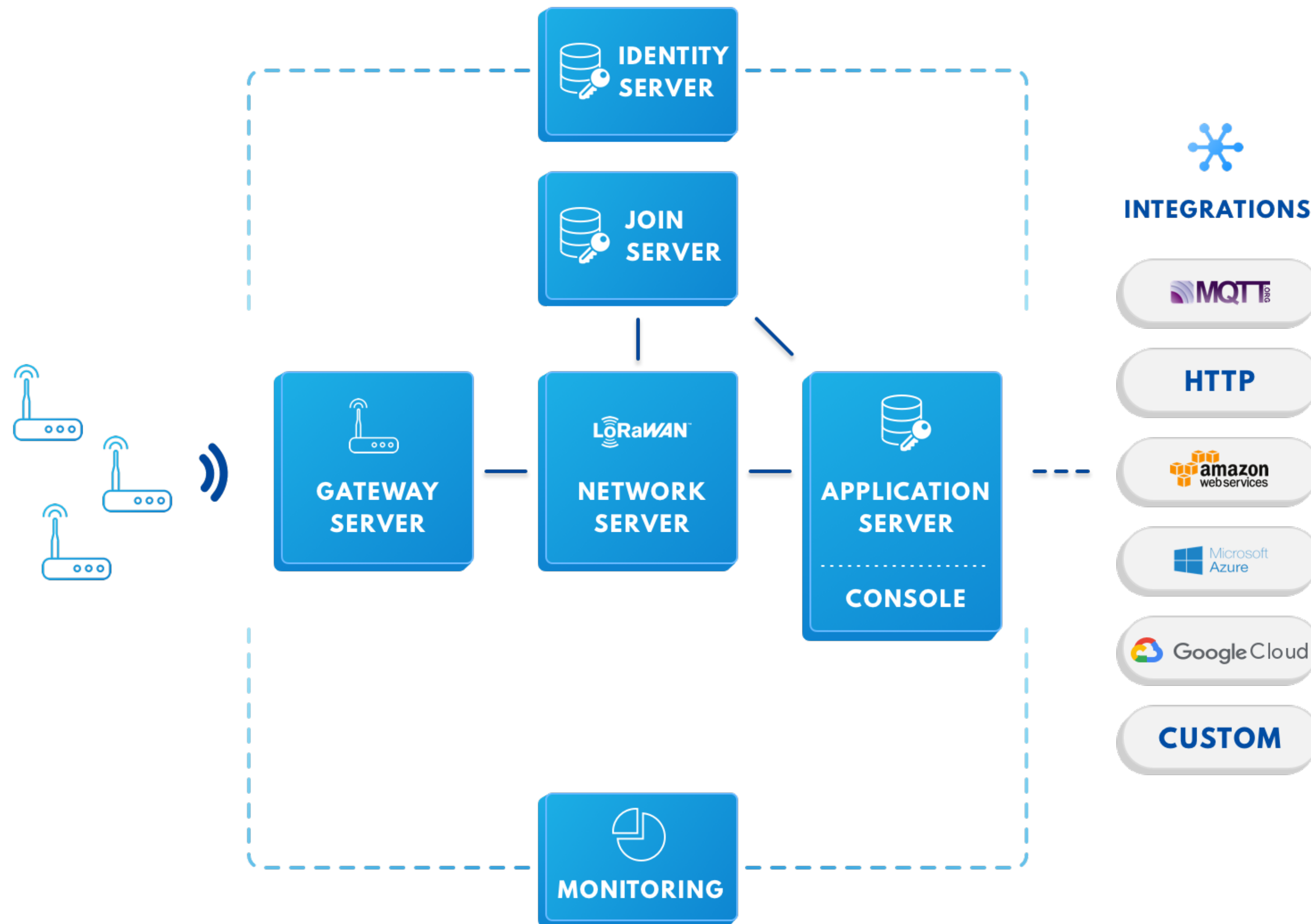
Powered by the open source The Things Stack

Commercially available in four distributions

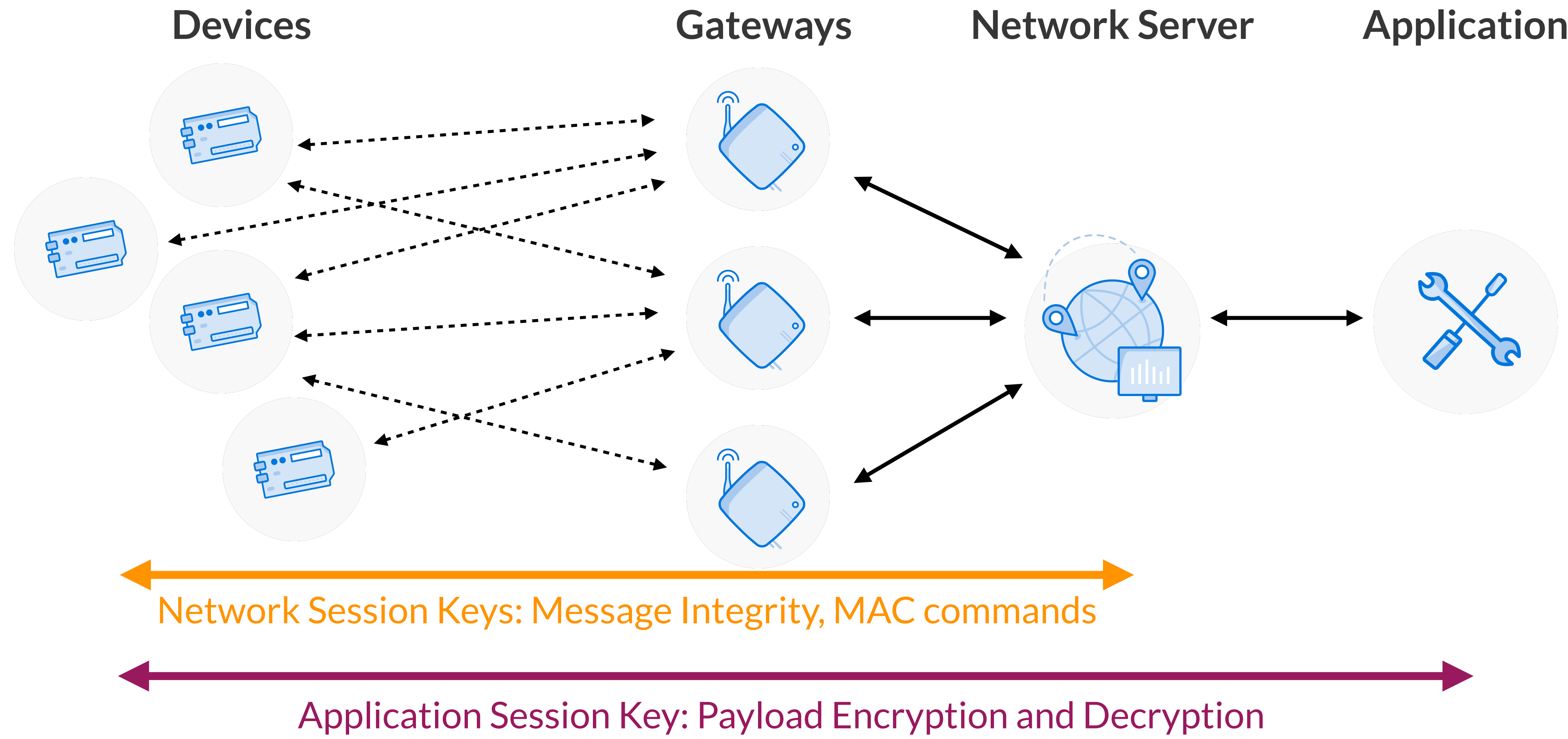
Supports peering across all deployment models



The Things Enterprise Stack



LoRaWAN network topology



Symmetric Cryptographic Security Primitives

Threats	Protecting Tools	Security primitives and procedures
Unauthorized access	Mutual end point authentication	Join procedure: AES128 – CMAC AES128 – ECB Electronic CodeBook
Modification	Integrity protection	MIC Message Integrity Check <ul style="list-style-type: none">AES128 – CMAC Cypher-based message authentication codeDevice address is part of MICFrame Counter is part of MIC
Spoofing	Data origin authentication	
	Replay protection	
Eavesdropping	Encryption	AES128 – CTR Counter Mode Encryption

Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

LoRaWAN session key derivation

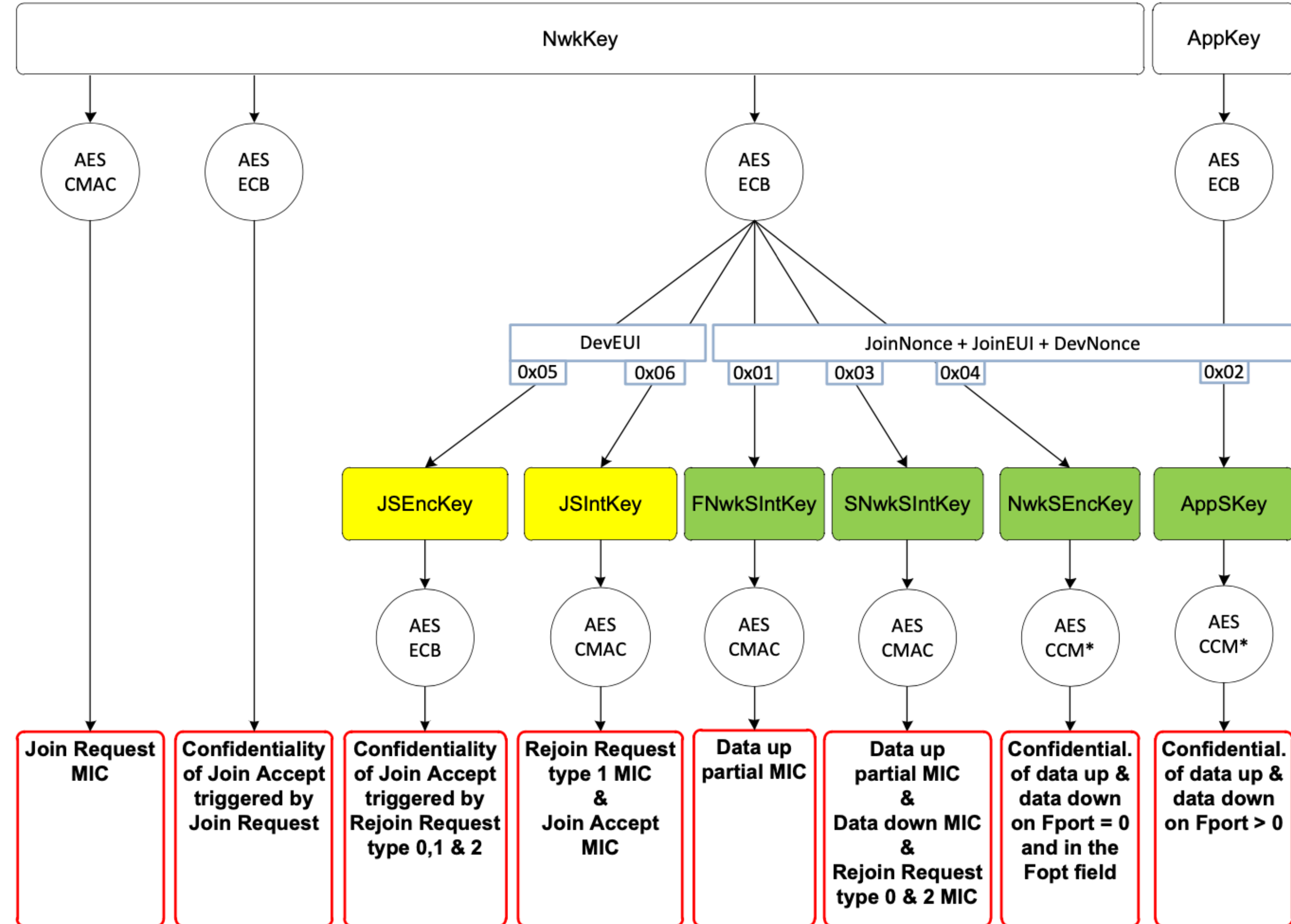
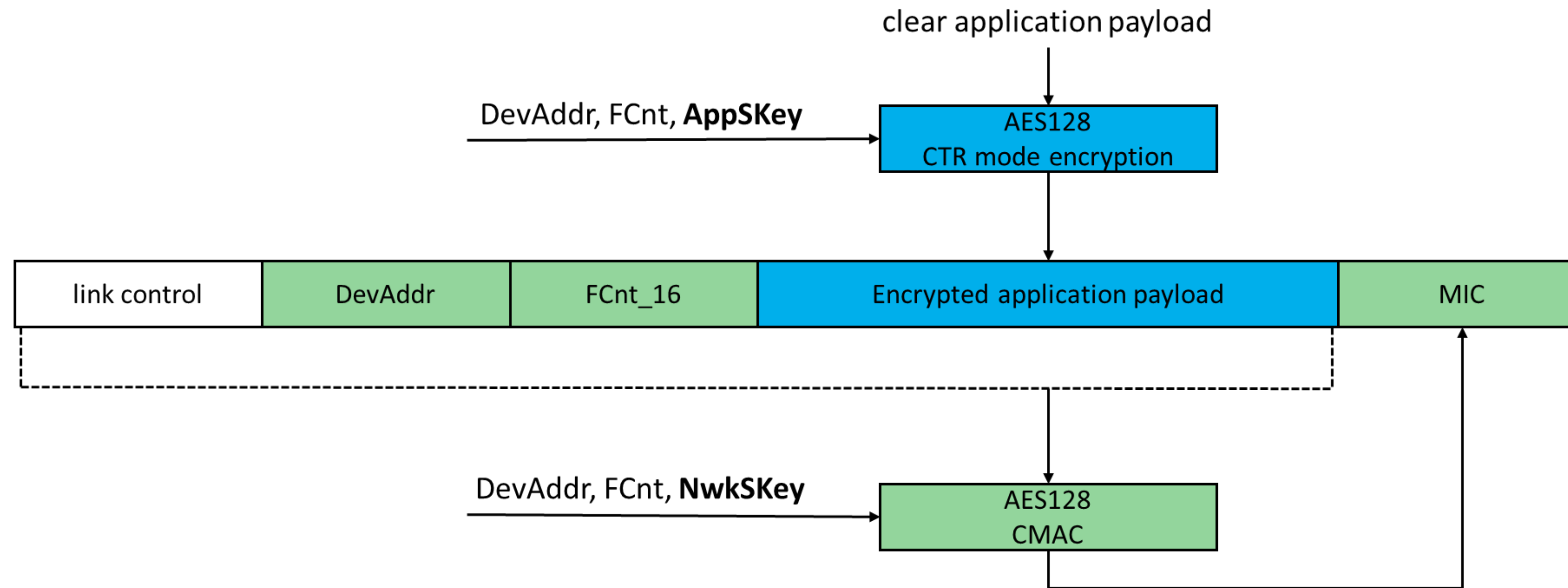


Figure 49 : LoRaWAN1.1 key derivation scheme

Frame Authentication and Encryption



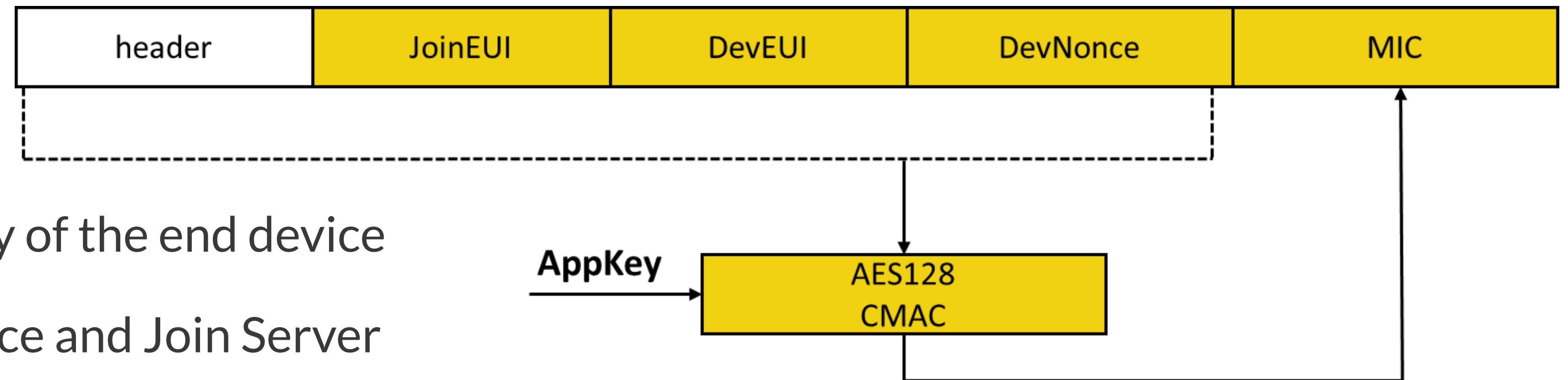
Message Integrity Check is 32 bits and can only be computed/verified with NwkSKey

Application Session Key (AppSKey) and Network Session Key (NwkSKey) are 128 bits

- They are specific to a device, which is identified by its address (DevAddr)
- They are renewed at each session, starting with device activation

Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

Joining a Network: Over The Air Activation (OTAA)



AppKey is the 128 bit root key of the end device

- Shared between end device and Join Server
- Unique, random, difficult to guess

DevEUI identifies the device

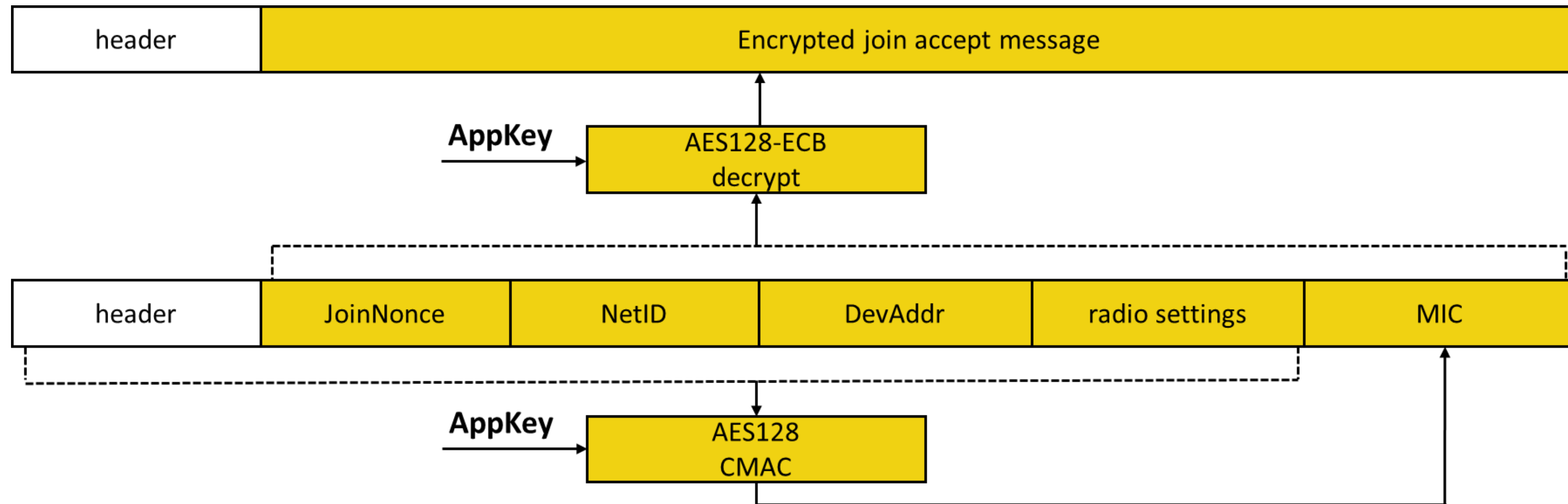
JoinEUI identifies the Join Server that knows (DevEUI, AppKey)

DevEUI and JoinEUI are EUI-64-based identifiers, allocated by IEEE

DevNonce is a counter to prevent replay attacks

Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

Joining a Network: Over The Air Activation (OTAA)



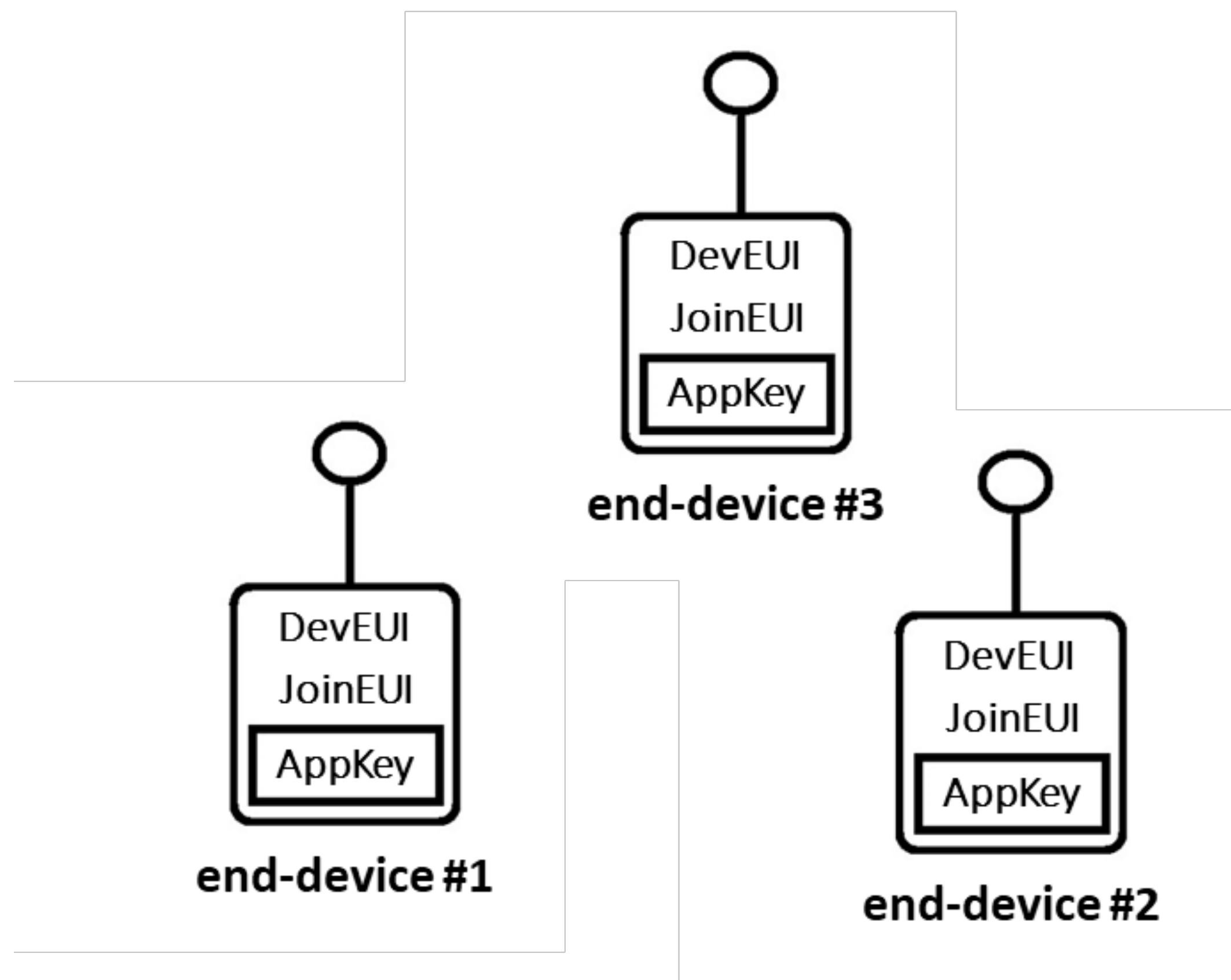
Only end device, which knows the AppKey, can decrypt the Join Accept frame and verify integrity

NwkSKey and AppSKey are derived using AES 128 encryption of AppKey, NetID, JoinNonce, DevNonce

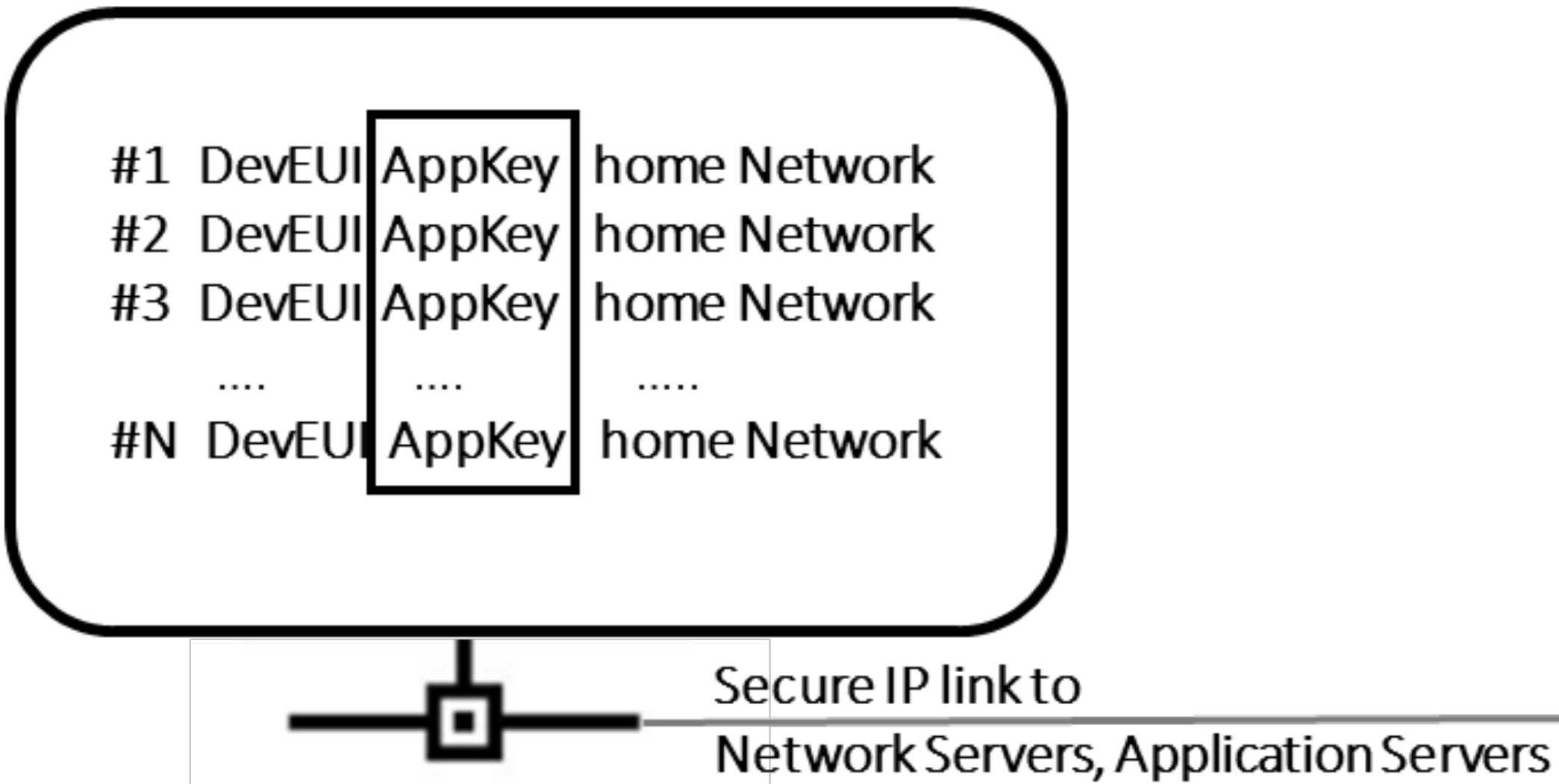
The first uplink that follows Join Accept frame confirms the new session keys

Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

Device Provisioning



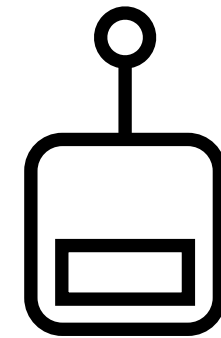
Join Server (JoinEUI)



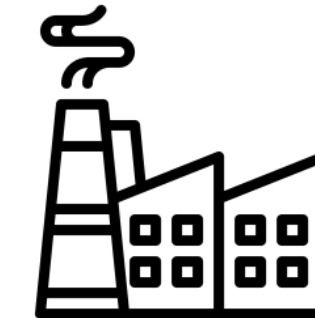
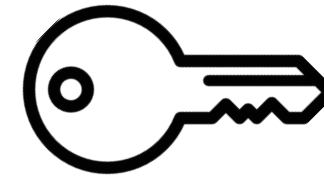
Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)



Implementation & Deployment Matters



End Device



Device Manufacturer

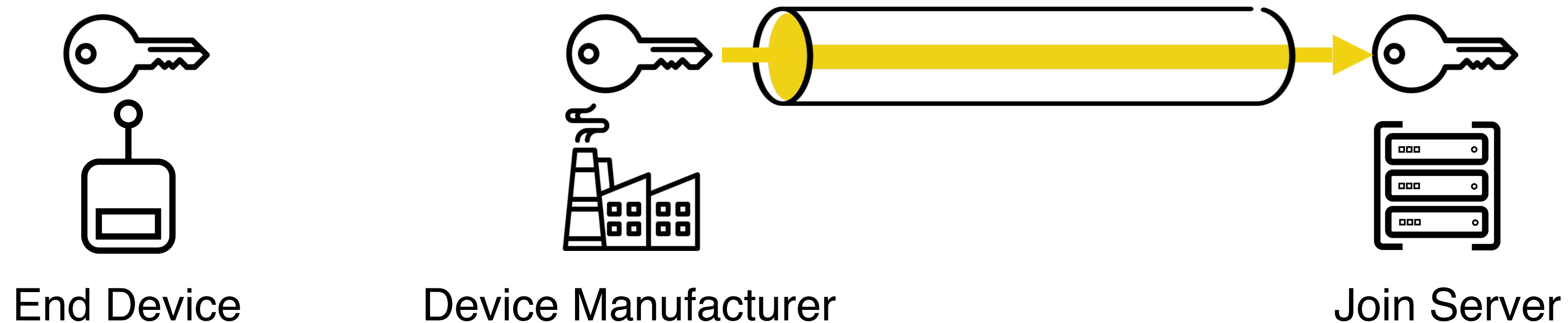
Root key (AppKey) generation

Unique per device

Strong (hard to guess)

Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

Implementation & Deployment Matters

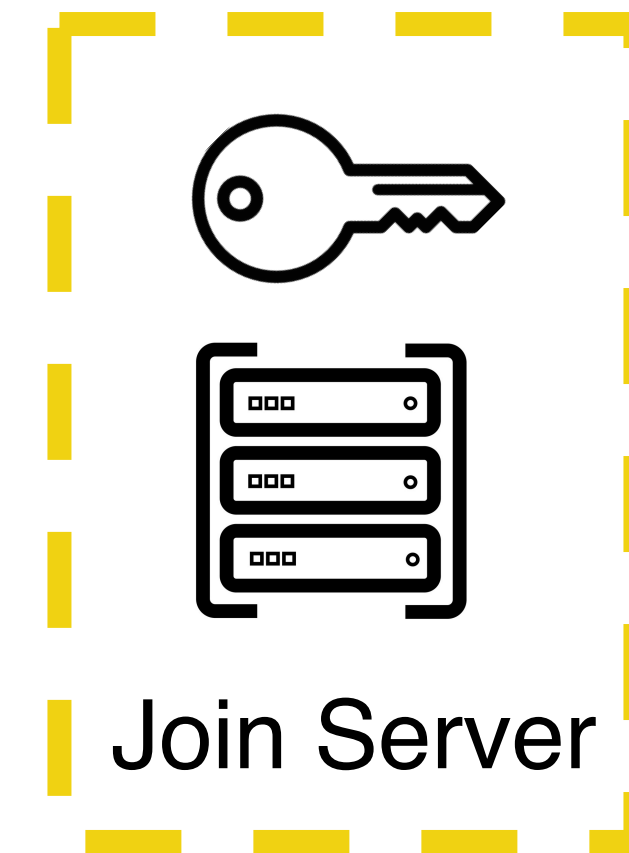
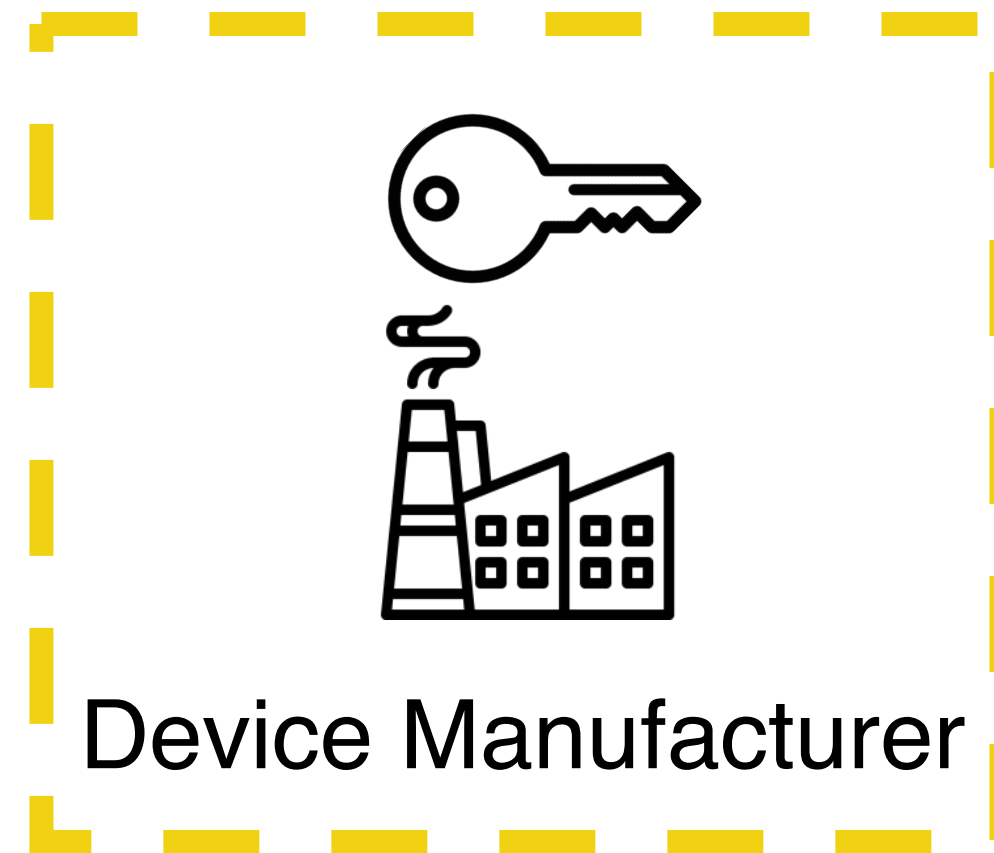
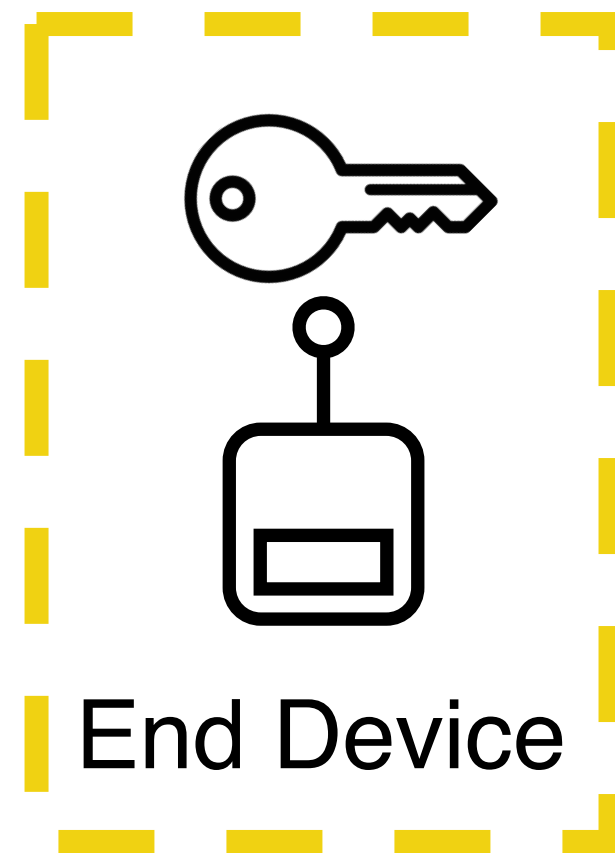


Root key delivery

End-to-end integrity protection and
privacy

Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

Implementation & Deployment Matters

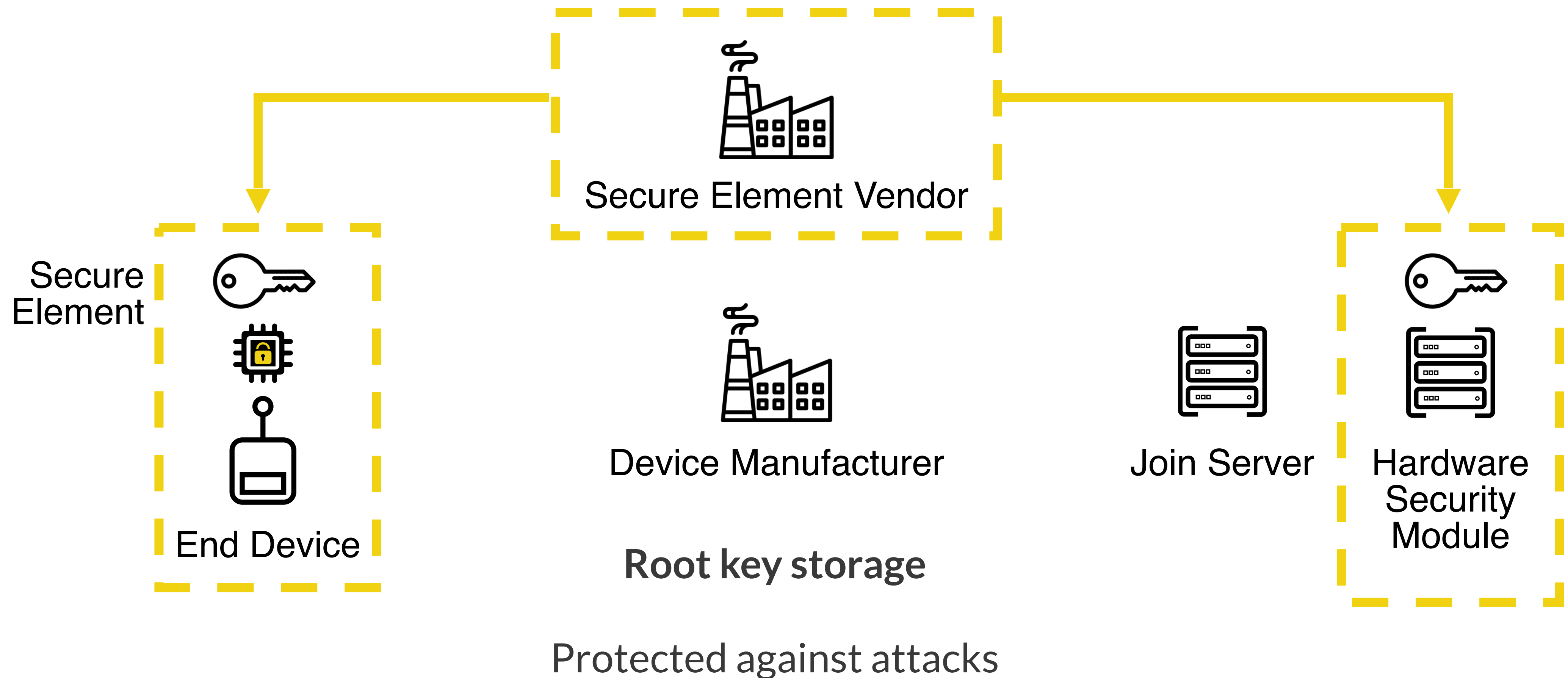


Root key storage

Protected against attacks

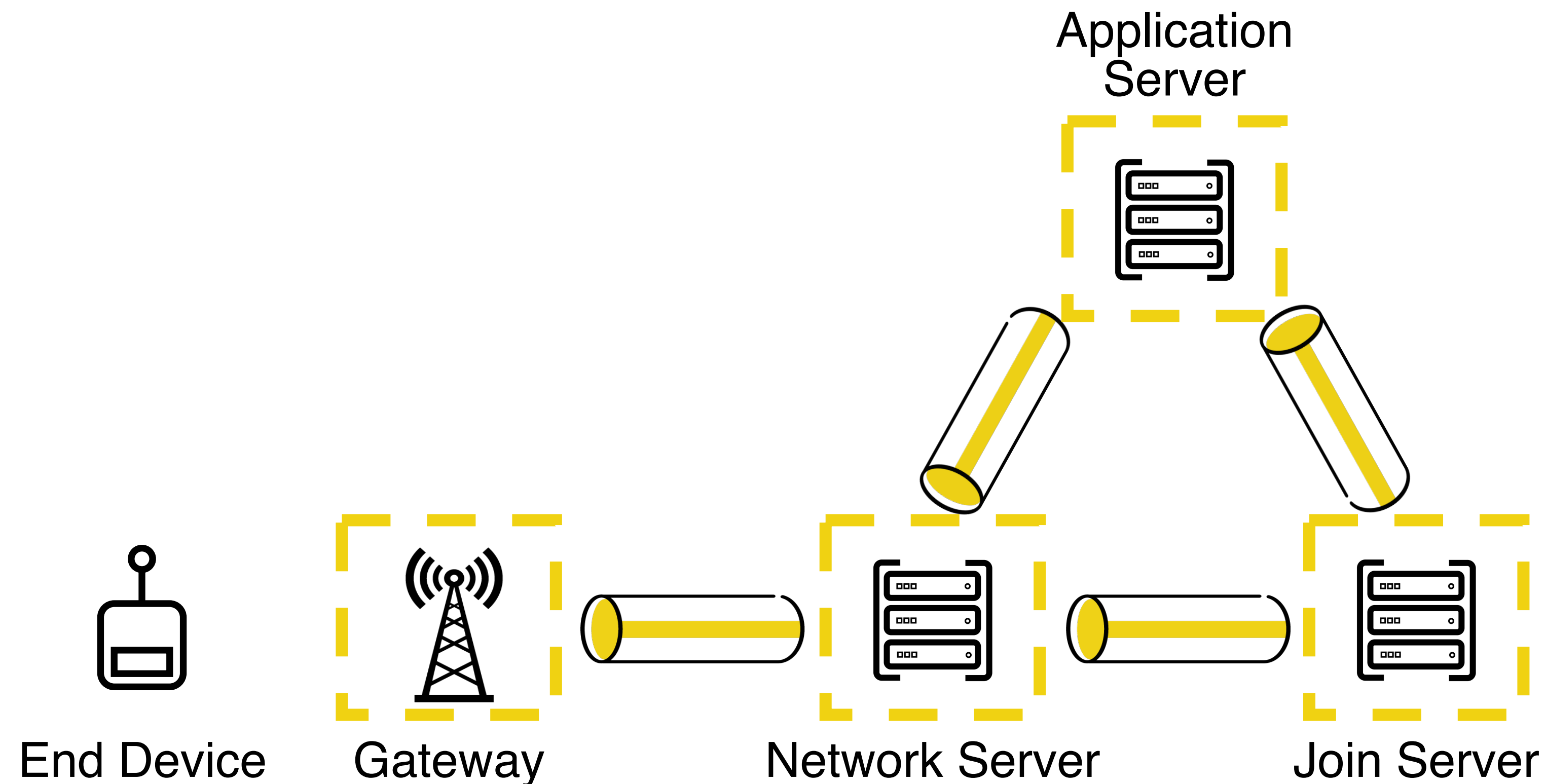
Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

Implementation & Deployment Matters



Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

Implementation & Deployment Matters



Backend infrastructure and communication security

Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

Implementation & Deployment Matters

01_basic_transmission.bin	02_basic_transmission.bin	01_basic_transmission.hex
Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	
0001A940	50 EF E2 D6 E4 1A 4B 44 92 D5 4D 06 CF F0 80 44	PiãÖä.KD'ÖM.İ&ED
0001A950	F6 4A E1 C7 02 2D B5 44 B4 9D D9 79 43 78 EA 44	öJ&Ç.-µD'.ÛyCx&D
0001A960	05 00 00 00 19 00 00 00 7D 00 00 00 43 00 00 00}....C...
0001A970	50 4F 53 49 58 00 00 00 2E 00 00 00 00 20 20 20	POSIX.....
0001A980	20 20 20 20 20 20 28 28 28 28 28 20 20 20 20 20	(((((
0001A990	20 20 20 20 20 20 20 20 20 20 20 20 20 88 10 10	^..
0001A9A0	10 10 10 10 10 10 10 10 10 10 10 10 10 04 04 04
0001A9B0	04 04 04 04 04 04 04 10 10 10 10 10 10 10 41 41AA
0001A9C0	41 41 41 41 01 01 01 01 01 01 01 01 01 01 01 01	AAAA.....
0001A9D0	01 01 01 01 01 01 01 01 10 10 10 10 10 10 42 42BB
0001A9E0	42 42 42 42 02 02 02 02 02 02 02 02 02 02 02 02	BBBB.....
0001A9F0	02 02 02 02 02 02 02 02 10 10 10 10 20 00 00 00
0001AA00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AA10	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AA20	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AA30	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AA40	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AA50	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AA60	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AA70	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AA80	F8 B5 C0 46 F8 BC 08 BC 9E 46 70 47 59 5F 01 00	əuÀFø4.4zFpGY...
0001AA90	DD 00 00 00 F8 B5 C0 46 F8 BC 08 BC 9E 46 70 47	Ý...əuÀFø4.4zFpG
0001AAA0	B5 00 00 00 F8 6B FF 7F 01 00 00 00 40 1F 00 00	µ...əky.....@...
0001AAB0	08 00 00 00 01 00 00 00 51 D2 00 00 FF 0F 00 00QÖ..ÿ...
0001AAC0	70 B3 D5 7E D0 01 85 85 11 11 11 11 11 11 11 11	p*Ö~Ð.....
0001AAD0	11 11 11 11 11 11 11 11 E5 45 65 5A D8 B8 33 66äEeZØ,3f
0001AAE0	19 27 A1 56 E5 A5 AD 0F 22 13 01 26 00 04 25 19	..';V&Ÿ..."&...&.
0001AAF0	18 01 A7 87 39 1C 5B 9C 63 3A 1C A9 57 61 5D A4	..\$+9.[æc:..@Wa]#
0001AB00	3A 44 24 68 01 00 00 00 60 00 00 20 00 00 00 00	:D\$h.....`... ..
0001AB10	4C 03 00 20 B4 03 00 20 1C 04 00 20 00 00 00 00	L.. '... ..
0001AB20	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AB30	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AB40	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AB50	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AB60	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AB70	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AB80	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AB90	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001ABA0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

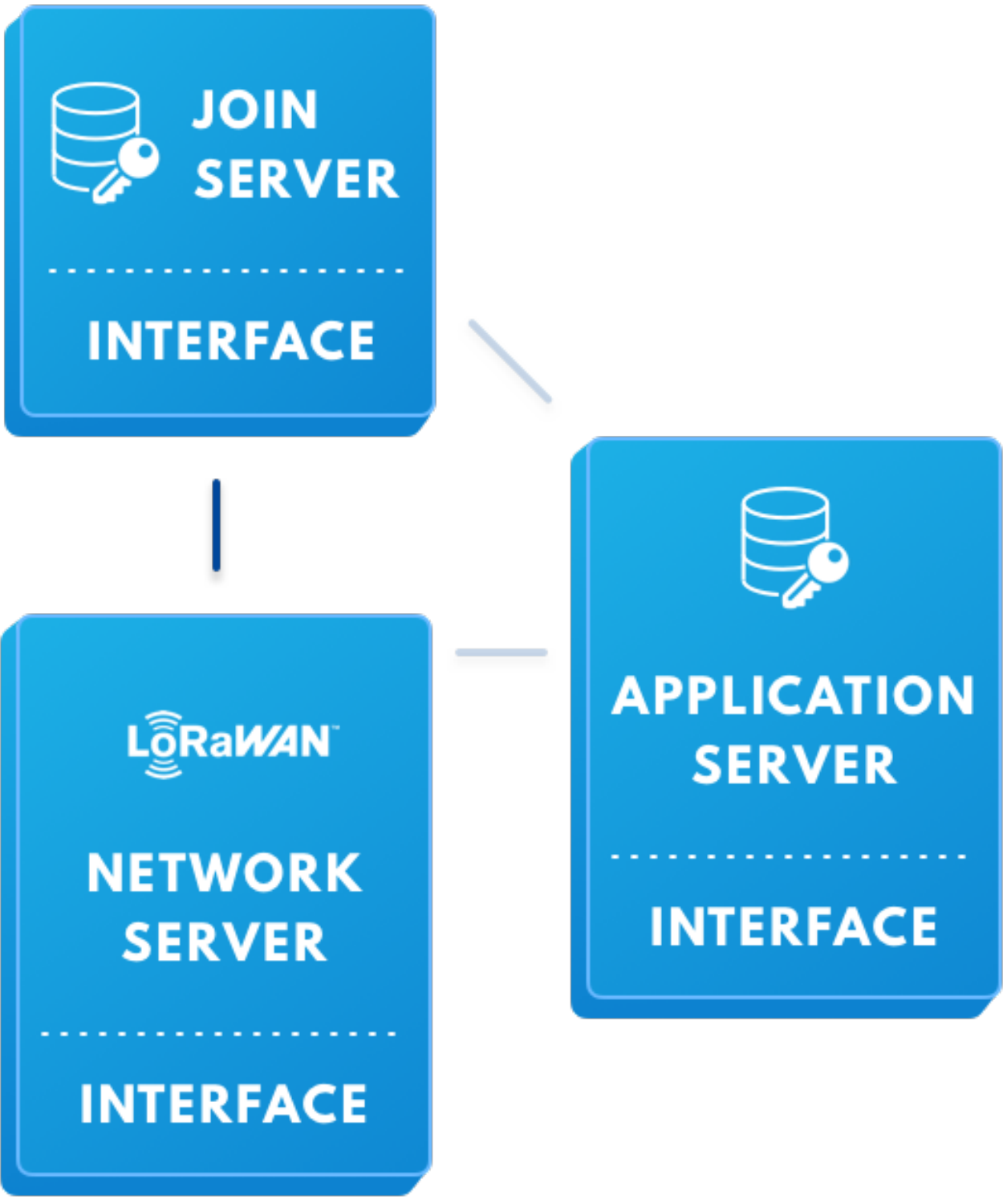
01_basic_transmission.bin	02_basic_transmission.bin	01_basic_transmission.hex
Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	
0001A970	50 4F 53 49 58 00 00 00 2E 00 00 00 00 20 20 20	POSIX.....
0001A980	20 20 20 20 20 20 28 28 28 28 28 20 20 20 20 20	(((((
0001A990	20 20 20 20 20 20 20 20 20 20 20 20 20 88 10 10	^..
0001A9A0	10 10 10 10 10 10 10 10 10 10 10 10 10 04 04 04
0001A9B0	04 04 04 04 04 04 04 10 10 10 10 10 10 10 41 41AA
0001A9C0	41 41 41 41 01 01 01 01 01 01 01 01 01 01 01 01	AAAA.....
0001A9D0	01 01 01 01 01 01 01 01 10 10 10 10 10 10 42 42BB
0001A9E0	42 42 42 42 02 02 02 02 02 02 02 02 02 02 02 02	BBBB.....
0001A9F0	02 02 02 02 02 02 02 02 10 10 10 10 20 00 00 00
0001AA00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AA10	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AA20	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AA30	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AA40	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AA50	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AA60	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AA70	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AA80	F8 B5 C0 46 F8 BC 08 BC 9E 46 70 47 59 5F 01 00	əuÀFø4.4zFpGY...
0001AA90	DD 00 00 00 F8 B5 C0 46 F8 BC 08 BC 9E 46 70 47	Ý...əuÀFø4.4zFpG
0001AAA0	B5 00 00 00 F8 6B FF 7F 01 00 00 00 40 1F 00 00	µ...əky.....@...
0001AAB0	08 00 00 00 01 00 00 00 51 D2 00 00 FF 0F 00 00QÖ..ÿ...
0001AAC0	70 B3 D5 7E D0 01 85 85 22 22 22 22 22 22 22 22	p*Ö~Ð.....
0001AAD0	22 22 22 22 22 22 22 22 E5 45 65 5A D8 B8 33 66äEeZØ,3f
0001AAE0	19 27 A1 56 E5 A5 AD 0F 22 13 01 26 00 04 25 19	..';V&Ÿ..."&...&.
0001AAF0	18 01 A7 87 39 1C 5B 9C 63 3A 1C A9 57 61 5D A4	..\$+9.[æc:..@Wa]#
0001AB00	3A 44 24 68 01 00 00 00 60 00 00 20 00 00 00 00	:D\$h.....`... ..
0001AB10	4C 03 00 20 B4 03 00 20 1C 04 00 20 00 00 00 00	L.. '... ..
0001AB20	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AB30	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AB40	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AB50	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AB60	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AB70	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AB80	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001AB90	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0001ABA0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Implementation & Deployment Matters



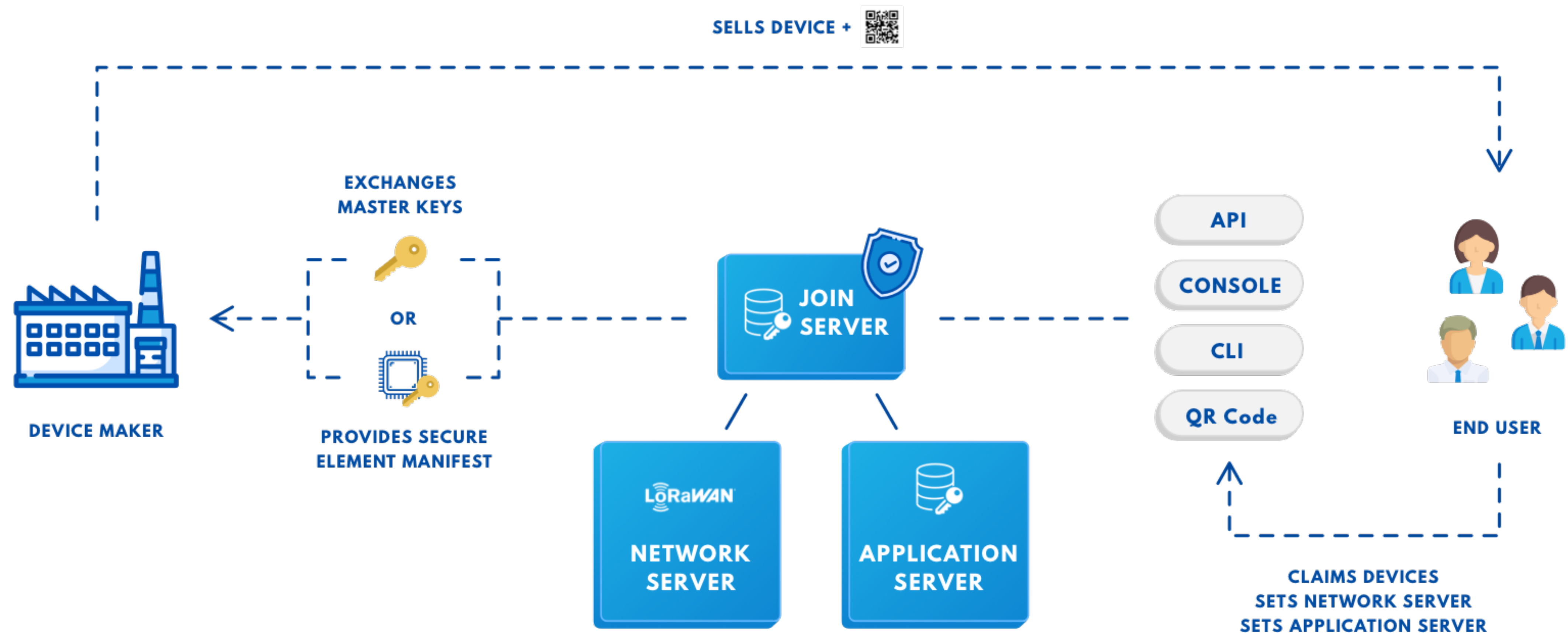
JoinEUI	DevEUI	NwkKey
70B3D57ED0029856	70B3D57ED0ff9205	f3c3ed4ea5a019e1fc00a0227aa66177
70B3D57ED0029856	70B3D57ED0fa3055	6ab1a7c8eea8b294d8d37e6d8c8d7e25
70B3D57ED0029856	70B3D57ED06f3880	cdf770dceba809fedb604c72db72a435
70B3D57ED0029856	70B3D57ED0deb1e	6ad9857305ca0224beb4c8f373b5c572
70B3D57ED0029856	70B3D57ED0f93bea	cbd8bcb042a8e3ecd8040f6c97870596
70B3D57ED0029856	70B3D57ED0a964a2	5cc8e452bb921c7a0f90c17e425617fe
70B3D57ED0029856	70B3D57ED08b7df7	601305a27d2150e9f95a70202c60b5e2
70B3D57ED0029856	70B3D57ED06ea74d	2455c85b8cf55d20d30c8ccd37f4bceb
70B3D57ED0029856	70B3D57ED063001a	640c2714ab4b26f5a9f53058ca7117caf
70B3D57ED0029856	70B3D57ED0edced5	6e21e64f6ae68a5b2999c2b2b514f2
70B3D57ED0029856	70B3D57ED06f90	46d90319b703b7258fea3a15244
70B3D57ED0029856	70B3D57ED0	bbff326417575aa88111h
70B3D57ED0029856	70B3D57ED023170	bfca1c690f79f
70B3D57ED0029856	70B3D57ED0366f5b	005f2e
70B3D57ED0029856	70B3D57ED0170b41	bf5c3
70B3D57ED0029856	70B3D57ED0f39d74	69c9aa55
70B3D57ED0029856	70B3D57ED0e486a7	824be
70B3D57ED0029856	70B3D57ED09d1e81	2e
70B3D57ED0029856	70B3D57ED0114ad	097e58a9c64
70B3D57ED0029856	70B3D57ED0	70981579f7e7a5441f
70B3D57ED0029856	70B3D57ED0c88	60cc938023136c5c1835d20bb4
70B3D57ED0029856	70B3D57ED023b4fc	ad0c0abd1fad7d9b2da3fbc
70B3D57ED0029856	70B3D57ED002b28a	fe11715c
70B3D57ED0029856	70B3D57ED0153939	79d2c12550dc132bc385d191c25f9aaf
70B3D57ED0029856	70B3D57ED070f5c2	d67ba61d94ad289614fb4278c2c56fbd
70B3D57ED0029856	70B3D57ED01a7744	203e86d8edfb4055fe0ac9b95e062f14
70B3D57ED0029856	70B3D57ED0ab5a57	ddb6c574c35d73c1e4d23fa7f2ca0730
70B3D57ED0029856	70B3D57ED006c348	d520fc94ffcbd4bd1ff931348b065469
70B3D57ED0029856	70B3D57ED05b716d	92fba89ac04aa3f7344ebc1cbc3b88bc
70B3D57ED0029856	70B3D57ED0f4fac8	25b75fa8e8f1ad4d9ce9d61eaa1977ef
70B3D57ED0029856	70B3D57ED03526b9	088ce39b2d0fca3ba278cd1359b64b4d
70B3D57ED0029856	70B3D57ED0552e3f	89a50a09b31a0939c4bd777666d727de
70B3D57ED0029856	70B3D57ED004ffe5	c3f3d4a1386028fdded2b857021e8827
70B3D57ED0029856	70B3D57ED05d4dbb	2964
70B3D57ED0029856	70B3D57ED059f096	465b8b5708
70B3D57ED0029856	70B3D57ED0650c51	6e2c51
70B3D57ED0029856	70B3D57ED0f6dcb6	ae2d0dddb442

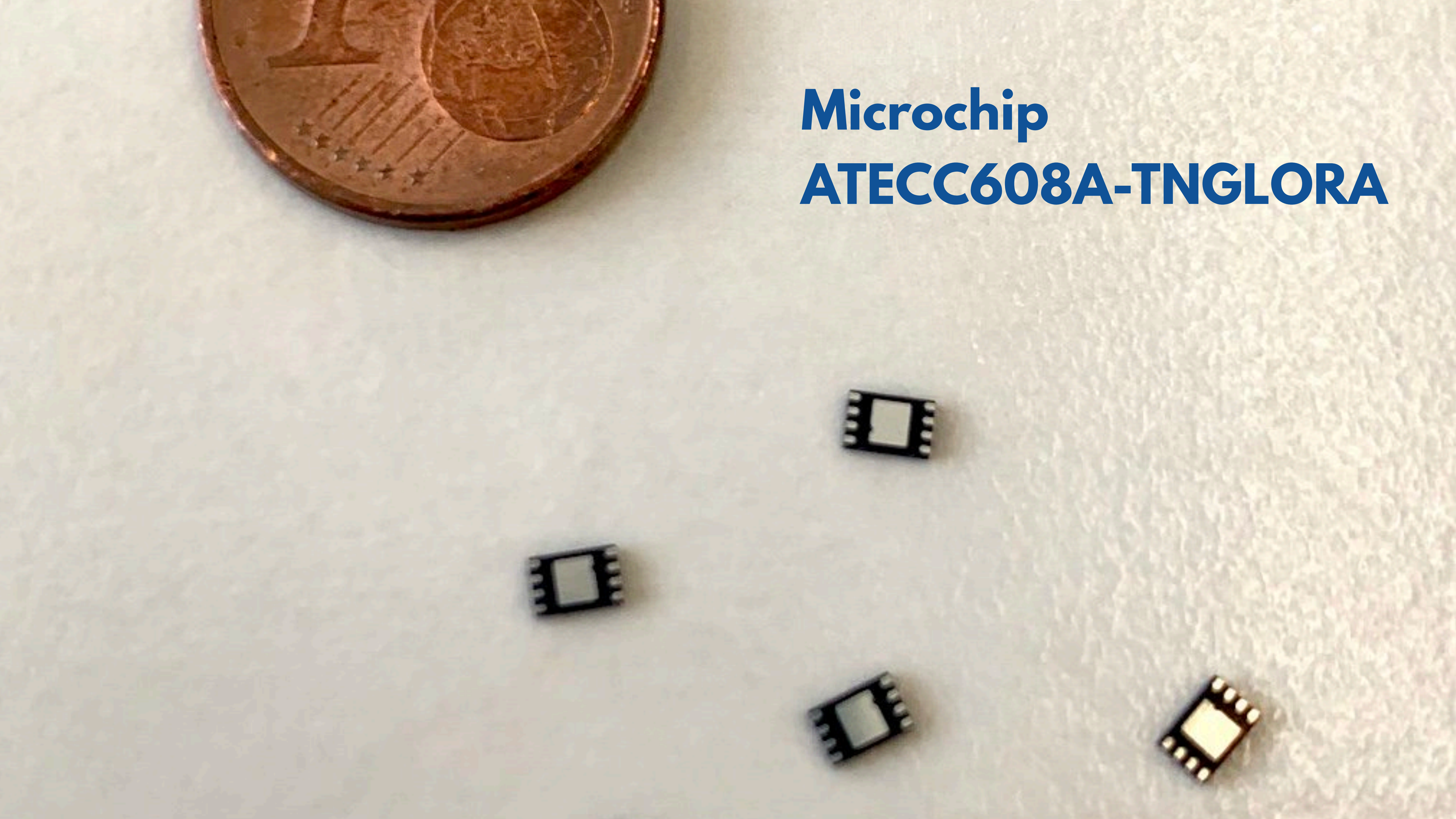
csv



Implementation & Deployment Matters

The Things Industries developed the first LoRaWAN security solution using hardware secure elements. These secure elements are pre-provisioned by Microchip.





Microchip

ATECC608A-TNGLORA

Firmware Updates over the Air (FUOTA)

Security for FUOTA

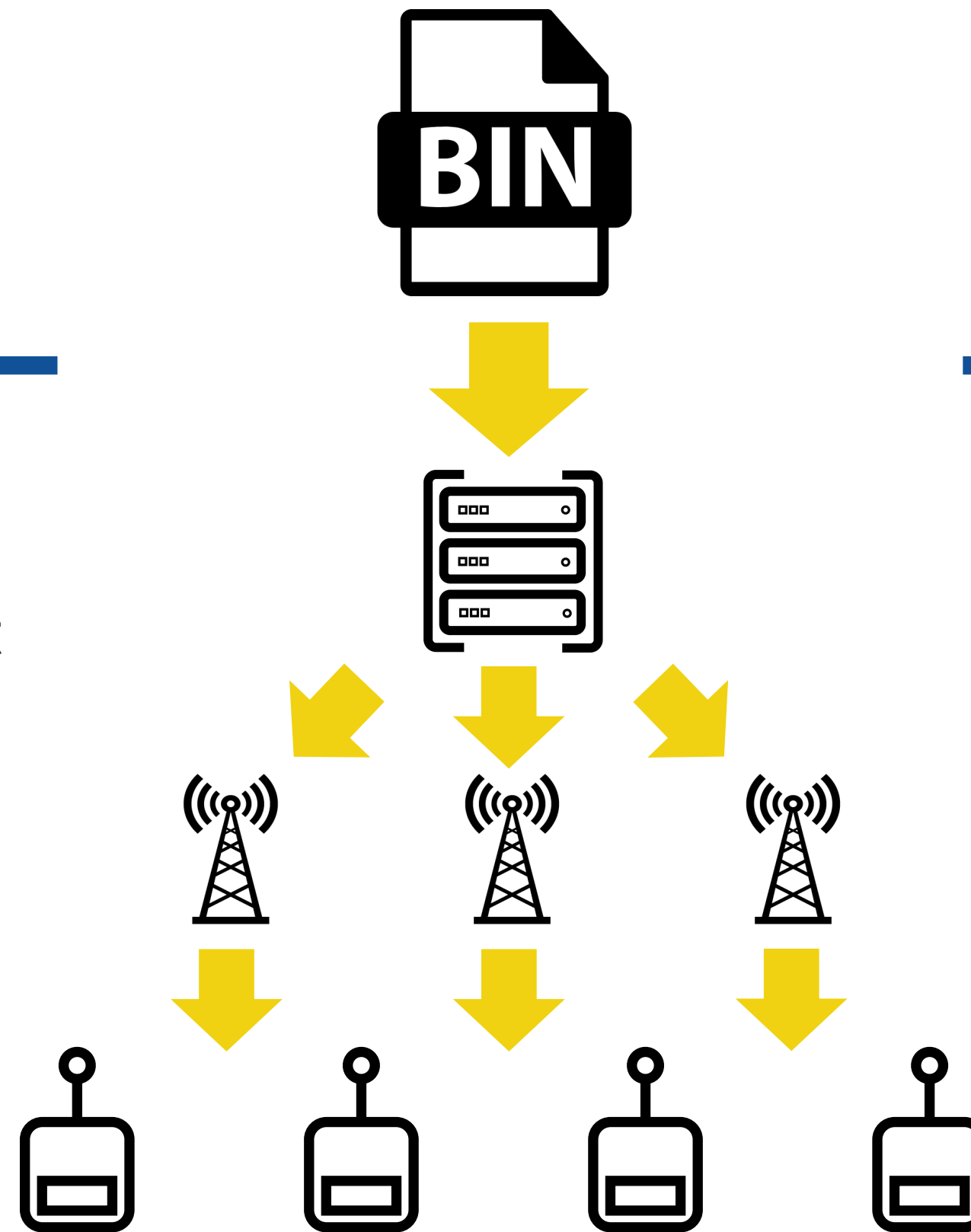
Signed firmware

Integrity-protected multicast
delivery (using group key)

Integrity-protected unicast
commands (using device key)

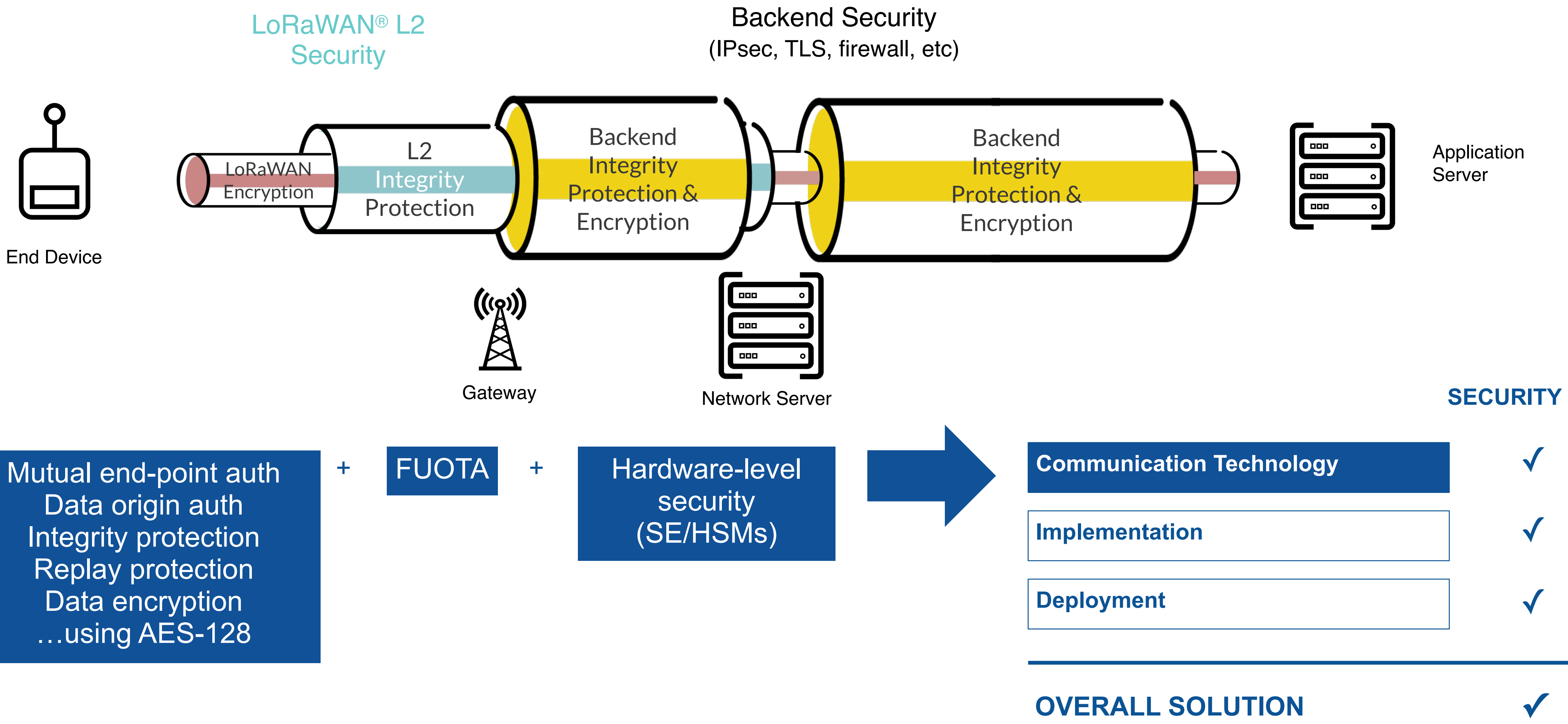
FUOTA for Security

Update device with software/
firmware (security) patches in
the field



Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)

Key Takeaways



Source: LoRaWAN; Providing Secure and Reliable Connectivity. Webinar hosted by Semtech, Actility and The Things Network (25-3-2020)





The Things Industries

Together with a team of professional developers we create the future of LoRaWAN.

Pushing open standards and tools that help the LoRaWAN ecosystem build IoT applications.

<https://join.thethingsindustries.com>





Thank you