Technolution

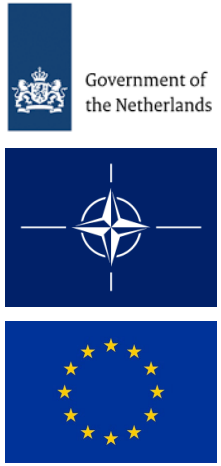
Why you should address post-quantum data safety in your product development right now?

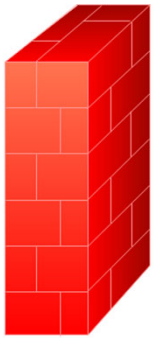
Redefining **solutions**

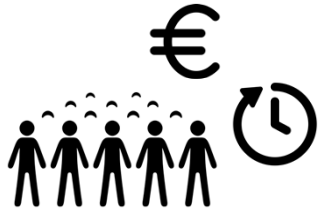
What is High Assurance?

Protecting data with high impact on confidentiality breach and with a high threat profile

Government of the Netherlands







Timeline

postponed attacks

"record now/exploit later"

Relevant for all products with long confidentiality requirements

confidentiality

2030

SPOILER ALERT

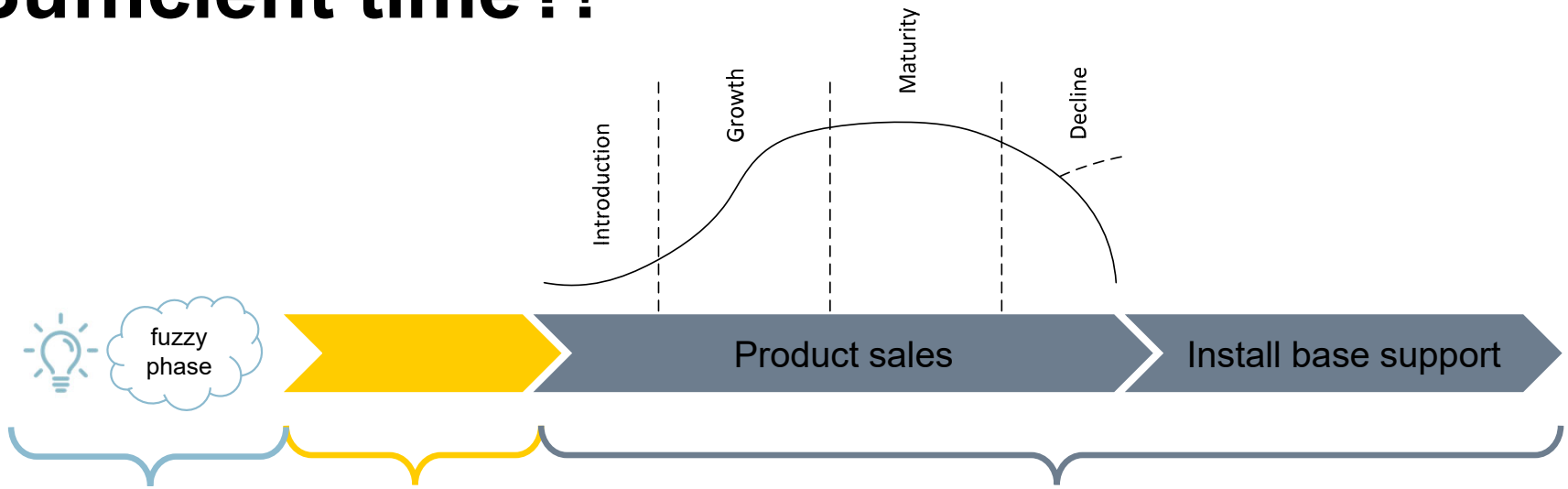
confidentiality & authenticity

Relevant for all products requiring security

direct attacks

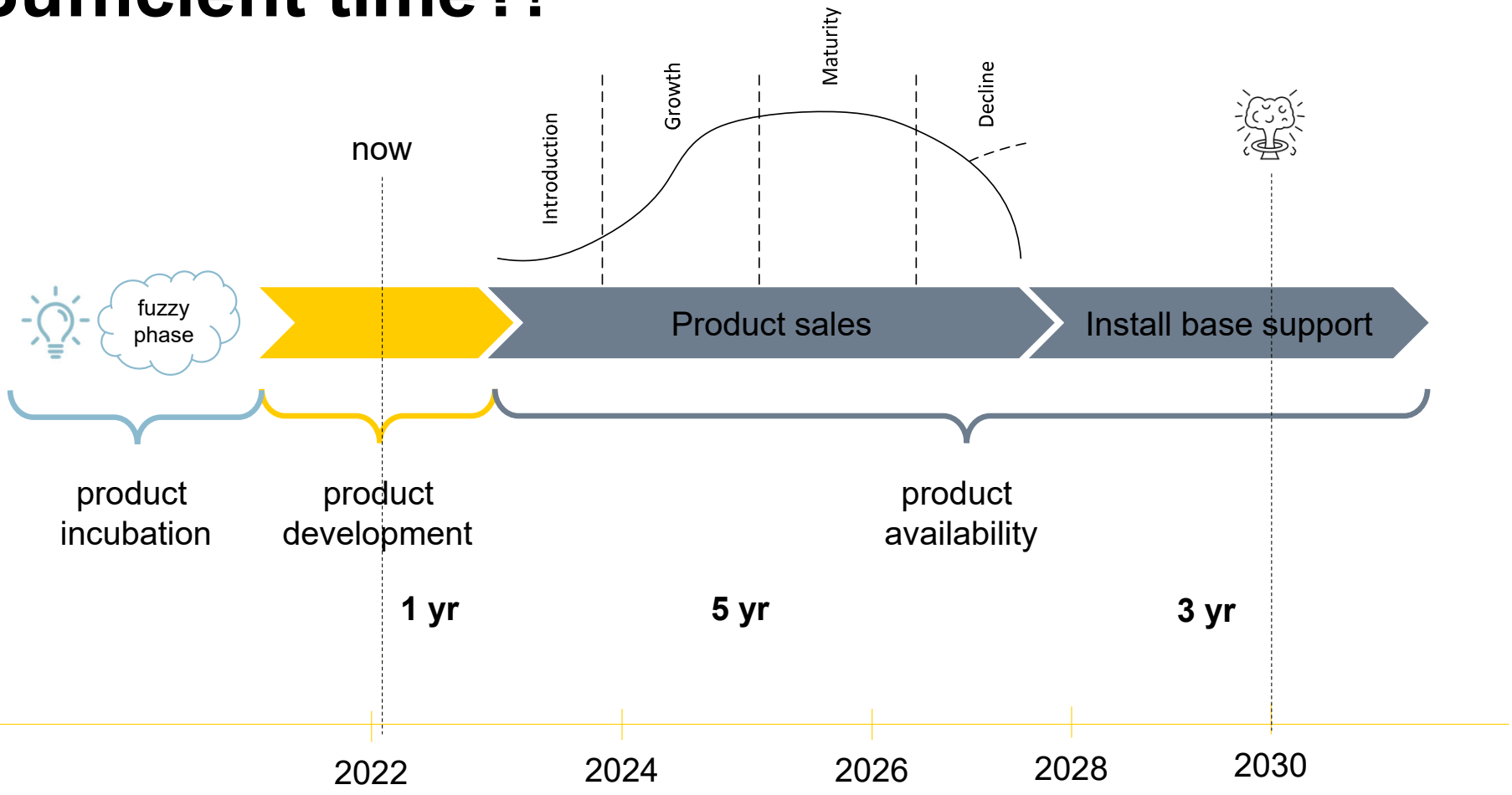
e.g. "man in the middle"

Sufficient time?!



product incubation	product development	product availability	
? yr	1-3 yr	5 -10 yr	3 - 5 yr

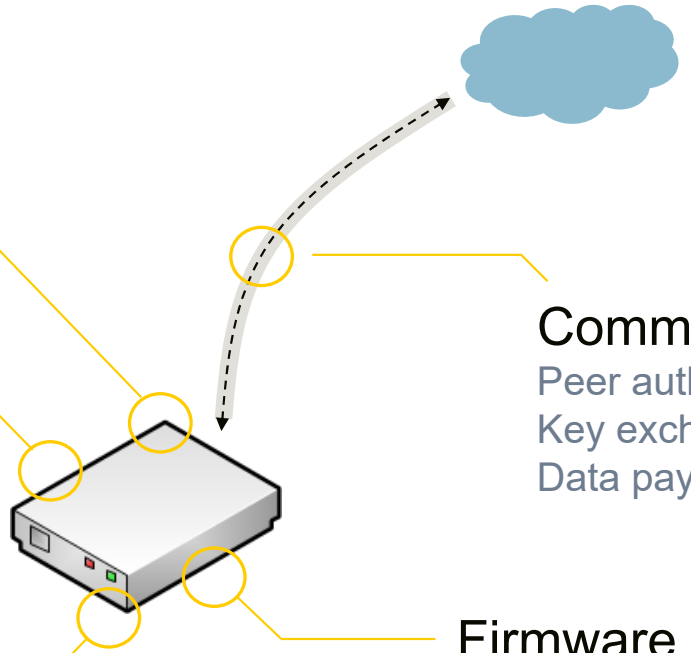
Sufficient time?!



Where did we hear this before?

Y2K

Product dismantled



Product information
Device authentication ✗/✓

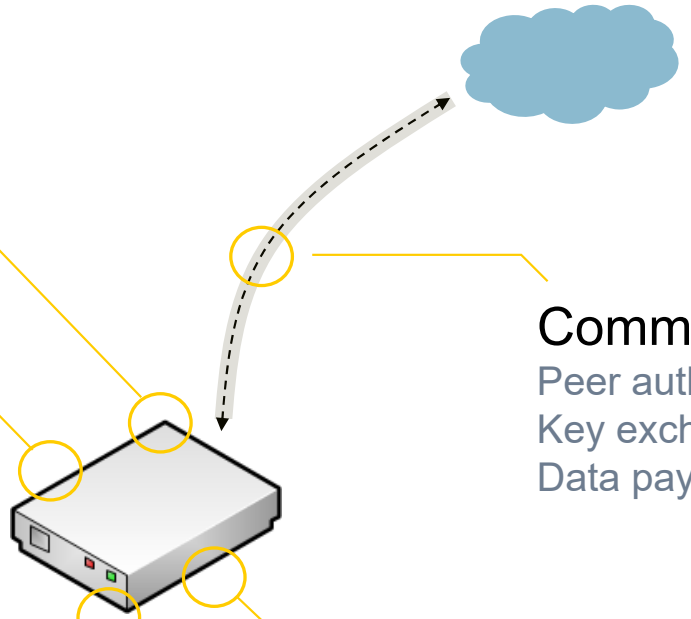
Application & user data storage
Stored data authentication ✓
Stored data encryption ✓

Communication
Peer authentication ✗
Key exchange ✗
Data payload encryption ✓

Firmware update
Firmware authentication ✗
Firmware encryption ✓

Secure boot
Firmware authentication ✗/✓
Firmware encryption ✓

Current PQ challenge



Product information
Device authentication ✘/✓

Application & user data storage
Stored data authentication ✓
Stored data encryption ✓

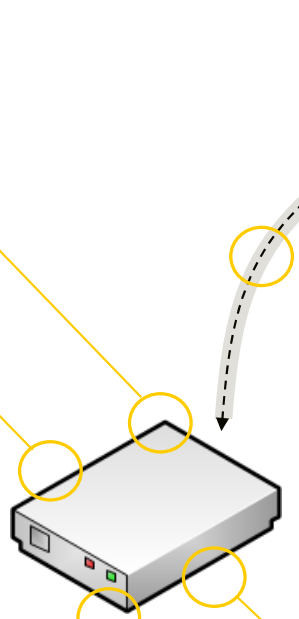
Likely not to be a problem if designed correctly

Secure boot
Firmware authentication ✘
Firmware encryption ✓

Communication
Peer authentication ✘
Key exchange ✘
Data payload encryption ✓

Firmware update
Firmware authentication ✘
Firmware encryption ✓

Current PQ challenge



Product information
Device authentication ✘/✓

Application & user data storage
Stored data authentication ✓
Stored data encryption ✓

Likely not to be a problem if designed correctly

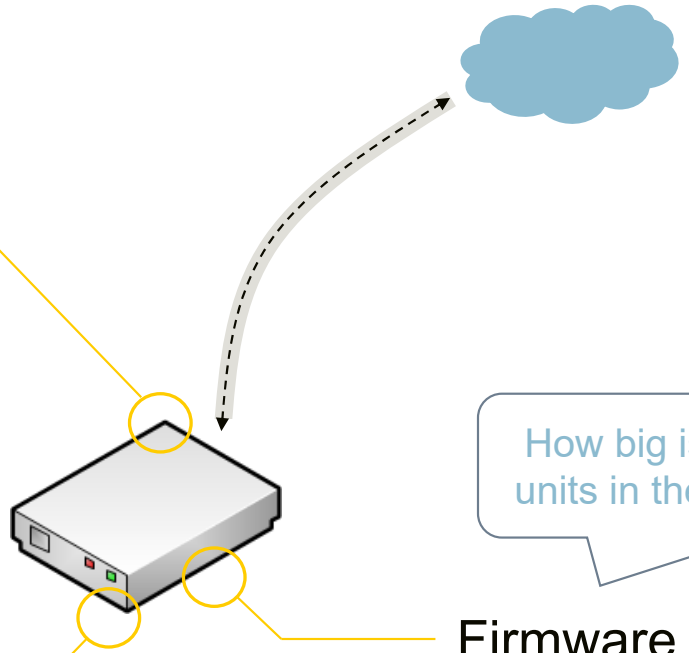
Secure boot
Firmware authentication ✘
Firmware encryption ✓

Solve with firmware update if "record now/exploit later" is not a threat

Communication
Peer authentication ✘
Key exchange ✘
Data payload encryption ✓

Firmware update
Firmware authentication ✘
Firmware encryption ✓

Current PQ challenge



Product information

Device authentication ✘/✓

Can you mitigate for non genuine products?

Do you store secrets inside the device?
Is reverse engineering your firmware an issue?
What is the impact of an adversary imitate a genuine device?

Secure boot

Firmware authentication ✘

Firmware encryption ✓

How big is the risk of unpatched units in the field being breached?

Firmware update

Firmware authentication ✘

Firmware encryption ✓

Secure boot vs. Secure update

Difference depends on the application and implementation…..

Firmware update

Part of the application firmware itself, mechanism and keys can be updated….

Accessible from the outside by an user

Would require the user to access the internals of your product

Secure boot

Builds initial root of trust of the device
Initial stage part of hardware → can not be updated

The PQ headache for product developers

Difference is depended on the application and implementation…..

Firmware update

Part of the application firmware itself,
mechanism and keys can be updated….

Trust chain can be broken….

Fix your update before the PQ-computer is available!

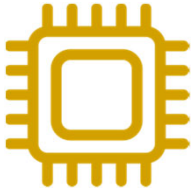
Secure boot

Builds initial root of trust of the device

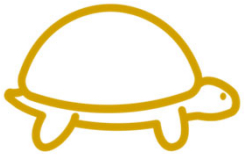
Initial stage part of hardware → can not be updated

Hardware limitations

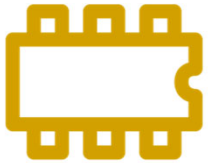
Most embedded microcontrollers are not PQ ready…..!!



no PQ-resilient boot



no hardware PQ crypto accelerators



no sufficient memory

no PQ crypto power optimization

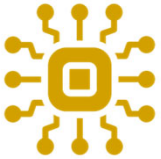
What can you do?

symmetric encapsulation

reduce impact of compromise

smart key scheme

Combine traditional & PQC



Choose the right hardware

Other….

Product developers; Act now!

- Determine your desired product lifespan
- Determine and apply your PQ resilient roadmap
- Regular check with reality and update your plan!

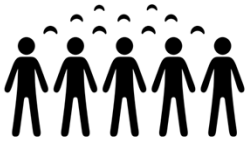
Redefining **solutions**

Technolution

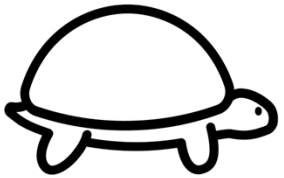
Attributions

Images used from the The Noun Project

Created by Viral faisalovers from the Noun Project

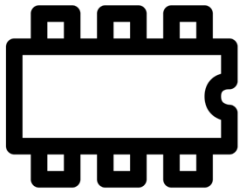


Created by Shane Holley from the Noun Project



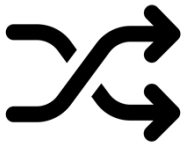
Created by IronSV from the Noun Project

Created by ClickHan

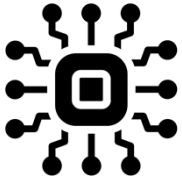


Created by Julie Zoe from the Noun Project

Created by Sophie Spiridonoff from the Noun Project



Created by Adrien Coquet from the Noun Project



Created by Adrien Coquet from the Noun Project

Created by Gregor Cresnar from the Noun Project

Created by Vector Portal