MINDSHARE

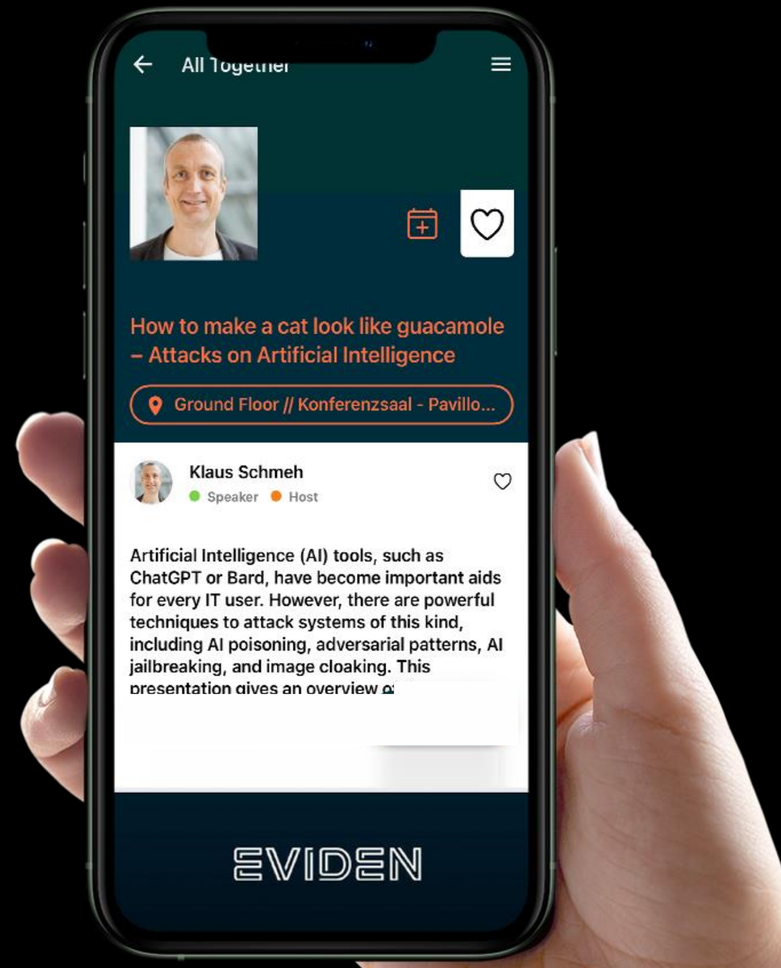
2025 10–11 SEP

CYBERSECURITY LEADERSHIP FORUM

Securing Identity for our Digital Future

MINDSHARE AGENDA

GET APP



MINDSHARE
2025 10–11 SEP
CYBERSECURITY LEADERSHIP FORUM
Securing Identity for our Digital Future

Mario Stoltz
NXP Semiconductors

Crypto agility for PQC credentials

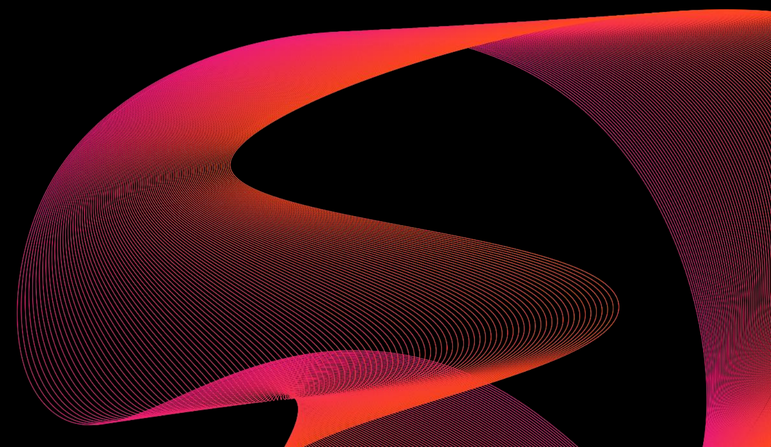
10 Sep 2025, 12:50…13:15

MINDSHARE

Agenda

how to upgrade eID documents and tokens to post quantum capability, and then: why and how to update them in the field?

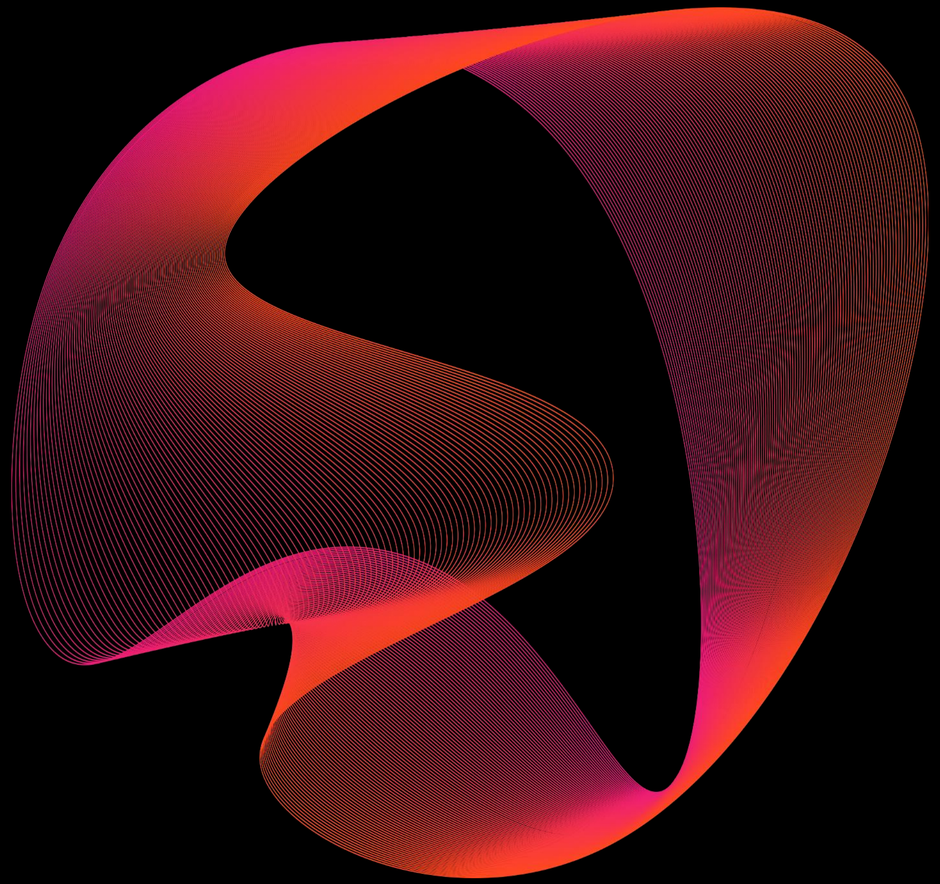
- Problem statement
- Migration / upgrade process from pre-PQC to fully PQC-enabled
- Why be ready to update?
- How to update an inventory of items in the field?
- Summary and takeaways



MINDSHARE

Problem statement

Crypto agility is a must have for the transition



- The keyword „crypto agility“ has been repeated for a few years now
  …for good reasons
- The industry knows from painful experience why this matters

Event	Reputation damage	Commercial damage	Cost of replacement
MIFARE hack, 2008	Limited	Medium	(indirect)
Tarnovsky attack, 2010	Limited	Medium	?
ROCA weakness, 2017	Medium	152 M€ lawsuit	>20M ID cards updated / replaced

- All of these were caused by vulnerability in the *implementation* of crypto functions

MINDSHARE

The migration to PQC

An unprecedented process in the 45-year history of secure microprocessors

Transition	New crypto algorithms(!) standardized	Supported by eSE HW acceleration / crypto libs	Progress / speed of transition
DES to AES	AES: 2000	2004	70%? in 22 years
RSA to ECC	ECDH, ECIES, ECDSA: pre-2000	by 2005	55%? in 20 years
RSA and ECC to ML-KEM, ML-DSA, SLH-DSA, LMS, XMSS, (FN-DSA, more…)	2020 (LMS, XMSS) 2024 (ML-KEM, ML-DSA, SLH-DSA) 2025…2030 (FN-DSA and others)	2025…2028	Authorities demand **100% within 5…10 years**

MINDSHARE

The train has left the station

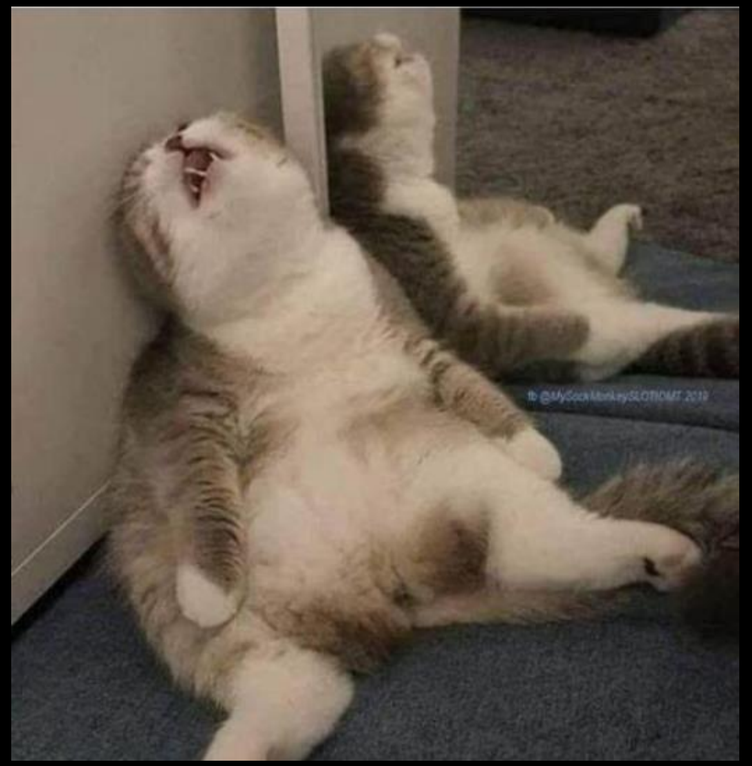
Where and when do we get on board, and what then?

Image: Tony Hisgett
via Wikimedia Commons

MINDSHARE

“…but do I really have to?”

well… lots of good information on this is available elsewhere. Let’s not discuss this now, but assume “yes” just as an experiment of thought, during this presentation

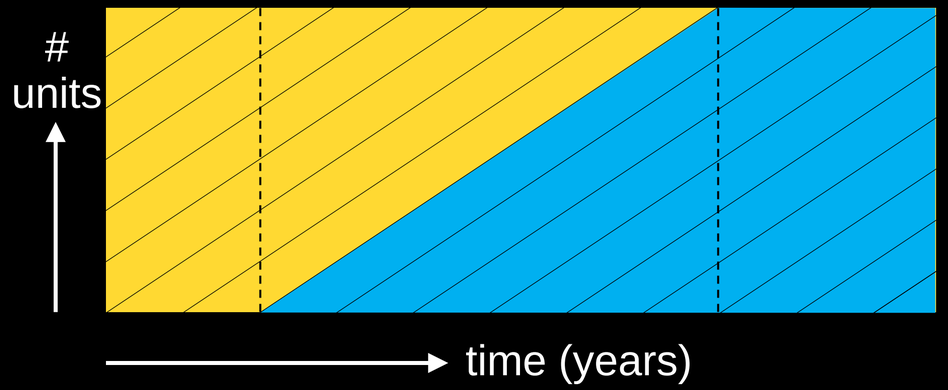


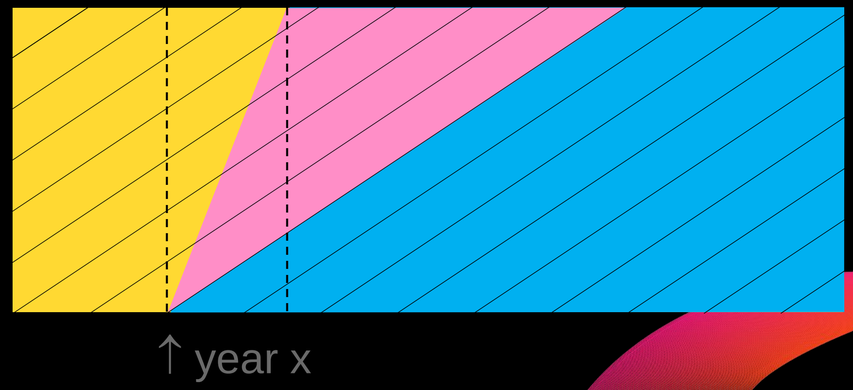
MINDSHARE

Upgrading a card/token inventory

From classical crypto eSE to PQC-enabled eSE

- Requirements, consultation, commercial tender, decision
- Upgrade by replacement (left) or by campaign (right)





classical crypto material

PQC-enabled material

double issuance / campaign cost

Upgrading: when?

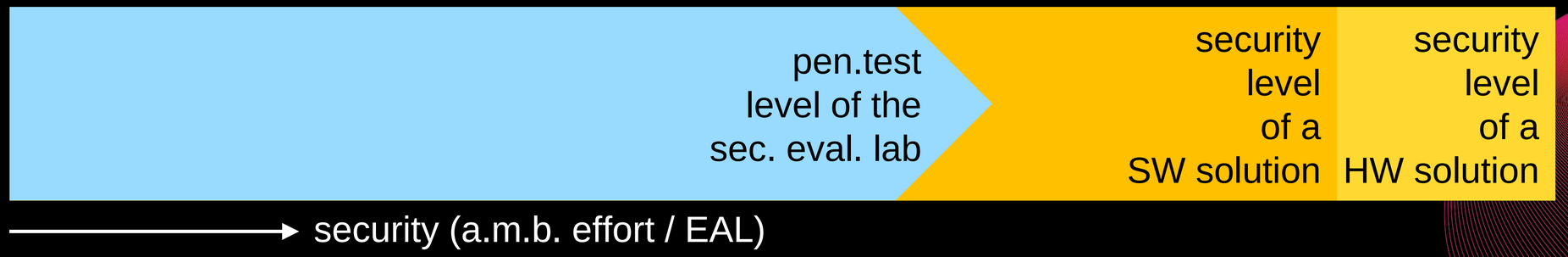
Answer: how standardized do you want to be?

- Early solutions that support PQC *may* later be found to be in line with what becomes an application standard *…or not*
- In some application areas, standardization may not be a concern
- In most application environments, there is a regulating body / (inter)national standard / industry association that issues technical specifications – including for cryptography – where compliance is mandatory
- Credential issuers typically require their suppliers to provide a certified security product – until regulations such as CC PPs are updated to reflect PQC, certification is not fully comparable
- ⇒ **when?** – for most: as soon as your application's certification scheme is ready

Why be ready to update?

Going from stable *status quo* to an emerging situation

- Academic and private institute security researchers, security labs are shifting their attention to PQC algorithms and implementations
- Expect 2025-2035 to be a decade of progress in security analysis and security hardening for PQC implementations
- The *point of good enough* will shift during this time, and solutions may have to be updated depending on their field life and risk profile

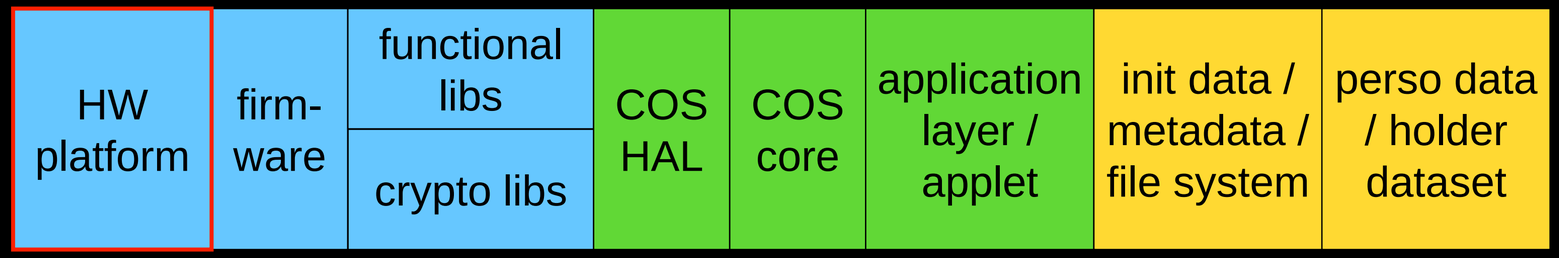


MINDSHARE

Prerequisites for updates

What needs to be done in advance?

- Select products that technically support an update process
  - Chose wisely: this selection process will constrain what you can and cannot do, and how you can do it
- “update” may be possible for different layers in the software stack, integrated, separately and with different degrees of flexibility

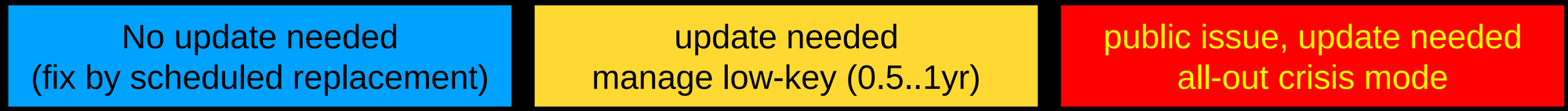


Note: only eSE aspect shown – on the host / system side, PQC also requires adaptation

MINDSHARE

How to update an inventory?

1) build a plan and perform fire drills

- Stakeholders should cooperate to develop example action scenarios
  - tools like FMEA (failure mode and effect analysis) may be helpful
  - 

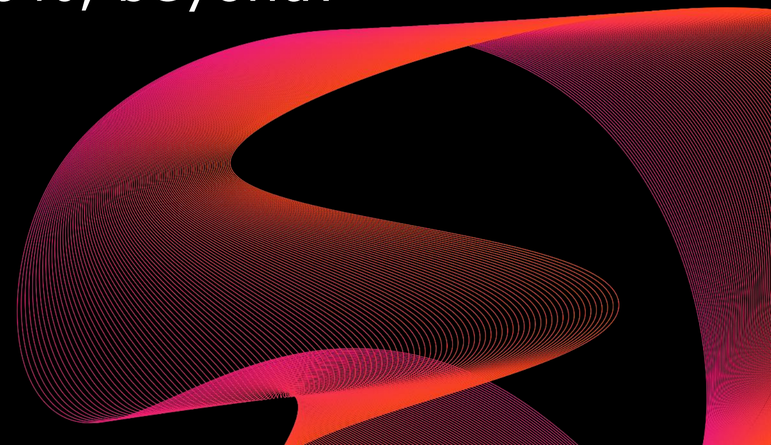
  - This is not primarily / not only an engineering topic, publicity and policy aspects may be just as important
- Difficult discussions about IT security with regulating authorities and public authorities may be required – but avoiding these may prove even more painful in the long run

MINDSHARE

Evaluate the situation

2) Develop metrics and stick to them

- Updating without a success metric is not healthy
  - “100% updated” is neither measurable nor realistic for a broader installation
  - Not all end points / credentials may be available with acceptable effort
    - e.g. IoT devices still in a warehouse at a reseller
    - e.g. never-activated ID cards somewhere in citizen households
    - activated ID cards in the hands of citizens that do not trust the government
  - How many resources spent for mobilization until 50%, 80%, beyond?
  - Business rule differences for updated vs. non-updated credentials?

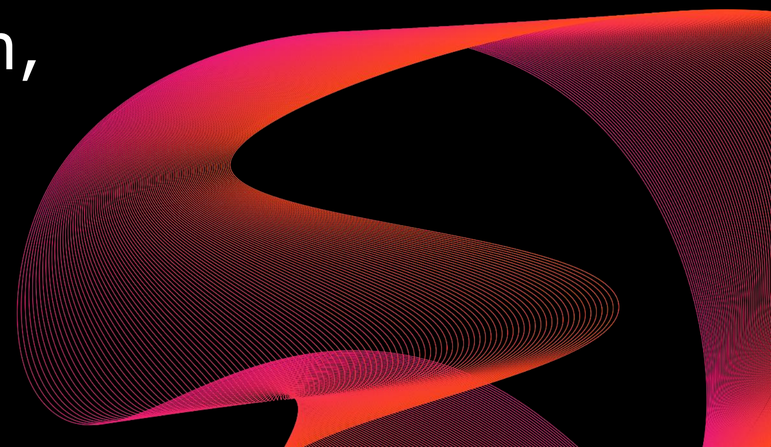


MINDSHARE

Evidence-based update

3) Use the available resources for the biggest impact

- Set realistic expectations with the issuing authority
  - An update (regardless how high-profile) is an IT project = resource constrained
  - The updated code or data must be developed, validated and probably security certified before it can be rolled out
  - Great if this can be done quickly, but it may as well take months or quarters
- Try to match measurable risk assumptions for the specific project with a realistic effort assumption for the update project
- Build a realistic resource perspective into the plan, and communicate it to key stakeholders from the beginning (see above)



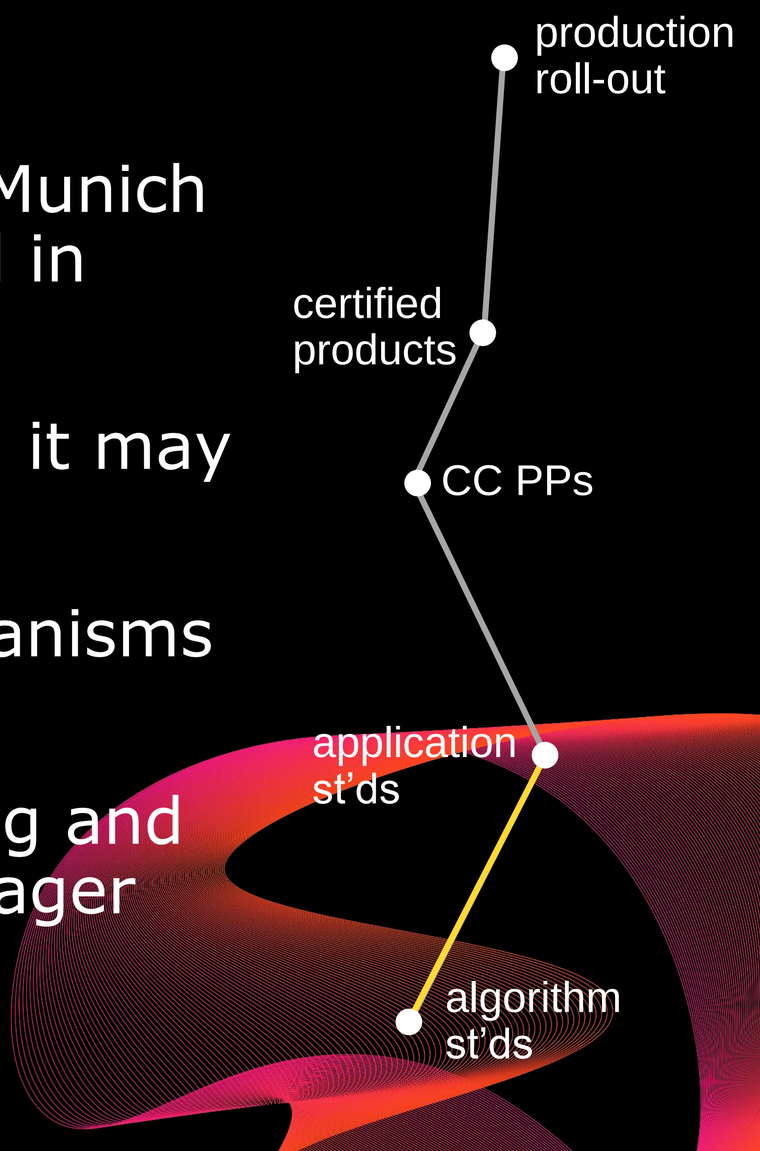
MINDSHARE

Summary and takeaways

The PQC train has left the station…

…but the good news is: if the PQC train went from Munich to Hamburg, most of you only need to get on board in Kassel-Wilhelmshöhe or even Hannover*

- Once first generation PQC solutions are deployed, it may be necessary to update their security in the field
- This requires appropriate, security certified mechanisms from the HW, OS and IT infrastructure supplier
- This also requires role definition, scenario planning and preparedness from the credential issuer and manager



*) but until then, you want to pack your bags, plan how and when to get to the station, pack some snacks – and you certainly want to continue monitoring the online status **regularly**

MINDSHARE
2025 10–11 SEP
CYBERSECURITY LEADERSHIP FORUM
Securing Identity for our Digital Future

Questions

Mario Stoltz
Product Manager SecID
Secure Connected Edge
NXP Semiconductors, Hamburg
mario.stoltz@nxp.com

NXP on PQC

Mario is a product manager at NXP Semiconductors. For more than 15 years, he has been responsible for secure microprocessor platforms for identity applications, at the hardware, at the operating system solution and at the application level.
He is an electrical engineer / MSEE graduated from TU Hamburg and has spent a total of 28 years in the semiconductor industry.


Thank you!
nxp.com

MINDSHARE

2025 10–11 SEP

CYBERSECURITY LEADERSHIP FORUM

Securing Identity for our Digital Future

TAKE A MINUTE AND GIVE US FEEDBACK