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

h_da darmstadt university of applied sciences

member of EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

Nouri Alnahawi
Hochschule Darmstadt

Post-Quantum Cryptography in eMRTDs

Mindshare 2025

acsd applied cyber security darmstadt

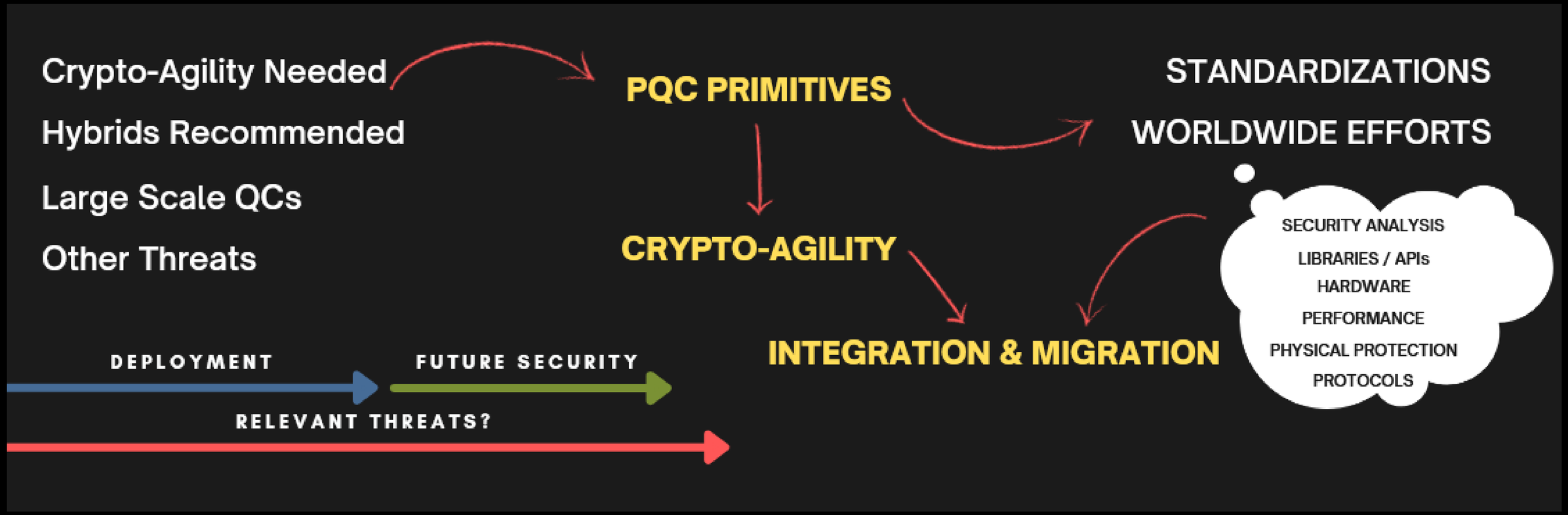
UR

MINDSHARE

h_da darmstadt university of applied sciences | member of EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

Motivation

Post-Quantum Cryptography



MINDSHARE

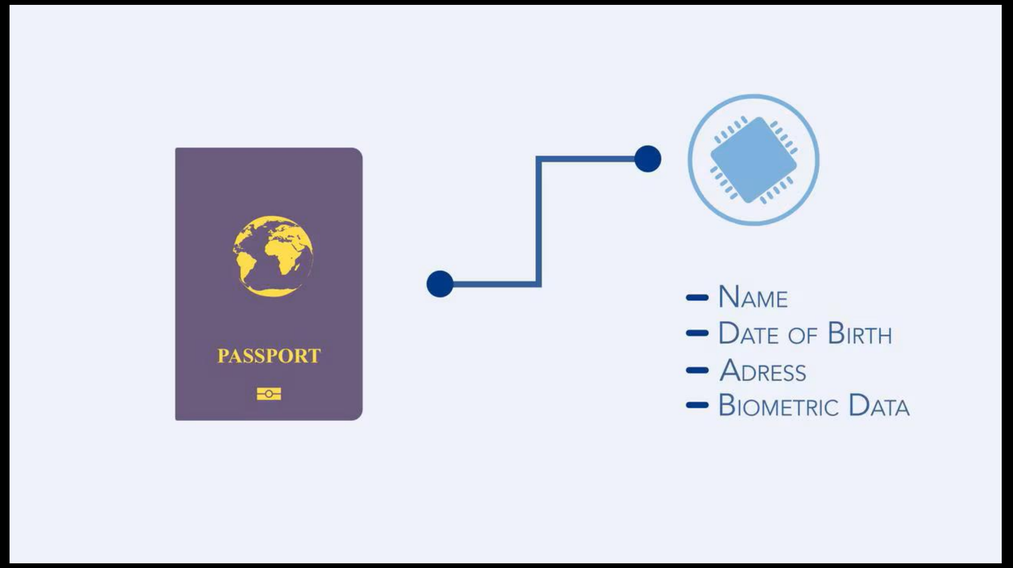
h_da darmstadt university of applied sciences

member of EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

Motivation

eIDs & eMRTDs

- Electronic Identification
- Sensitive (Personal) Data
- Resource Constrained HW
- Built-in Security Mechanisms
- Built-in Cryptographic Support



Source: https://www.nxp.com/products/MOB10

eMRTDs

Hardware

Source: https://www.nxp.com/products/SMARTMX3-P71D321

Source: https://www.mouser.de/new/infineon/infineon-mid-range-sbc-family/

- RFID (NFC)
- PICC
- Micro-Controller Architecture
  - **NXP60 / TCOS / SLC52 etc.**
  - **8-12 KB RAM**
  - **12-32 Bit CPU**

eMRTDs

Specification of Some Certified Security Chips

Model	Date	ROM	EEPROM	Flash	RAM
NXP SmartMX2 P60	2010	586 KB*	144 KB*	—	11 KB*
NXP SmartMX3 P71	2017	150 KB*	—	344 KB*	12 KB
Infineon SLE78	—	444 KB*	—	628 KB*	18 KB*
Toshiba T6ND1	2010	64 KB	80 KB	—	6 KB
Toshiba T6NE1	2011	64 KB	80 KB	—	6 KB
ST Micro. ST31G480	2014	—	—	480 KB	12 KB

*Up to.

Adopted from [2]

MINDSHARE

h_da darmstadt university of applied sciences | member of EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

eMRTDs

Security Protocols

Protocol	Security Goal	Cryptographic Mechanism
Passive Authentication	Check Authenticity of Chip Data	DS (on chip data)
Active Authentication	Check Chip Genuineness	Challenge-Response (DS)
Basic Access Control	Initial comms. channel, prevent eavesdropping	Challenge-Response (SKE)
PACE	Initial comms. channel, prevent eavesdropping	PAKE (incl. ephemeral DH)
Chip Authentication	Check Chip Genuineness	Ephemeral-Static DH
Terminal Authentication	Check terminal authorized to read secondary biometrics	Challenge-Response (DS)
Payload Comms.	Confidentiality / Data Integrity	SKE, MAC

Adopted from [1]

MINDSHARE

h_da darmstadt university of applied sciences

member of EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

eMRTDs

Certificates & PKI

- Certificate Authorities per Country
- Signing and Verifying
  - CSCA => Root Cert. => Document Signer (DS) Cert.
  - DS Cert. => eMRTD Cert. (both on chip)
  - CVCA => Root Cert. => Document Verifier (DV) Cert.
  - DV Cert. => Terminal

eMRTDs

Cryptographic Primitives

Protocol	Cryptographic Mechanism	Algorithm	Recommended Key Length
PA	Hashing	SHA-2	384
	Digital Signatures	ECDSA	384
BAC	Encryption	3DES CBC-Mode	112
	Authentication	3DES Retail MAC	112
PACE	Key Agreement	ECKA	256
	Encryption	AES CBC-Mode	128
	Authentication	AES MAC	128
CA	Key Agreement	ECKA	256
	Encryption	AES CBC-Mode	128
	Authentication	AES MAC	128
TA	Hashing	SHA-2	256
	Digital Signatures	ECDSA	256
PKI	Hashing	SHA-2	512
	Digital Signatures	ECDSA	512

Key length measured in bits.

Adopted from [2]

eMRTDs

Authentication (Example)

Protocol Sequence for eMRTDs supporting EAC

eMRTD		**Terminal**
Cert.eMRTD		Cert.Term
	Scan MRZ ⟷	
	PAKE ⟷ (with MRZ as password)	
	Terminal Authentication ⟷ ← Cert.Term	
	Chip Authentication ⟷ Cert.eMRTD →	
	Secondary biometrics ⟶	

Adopted from [1]

EAC: Extended Access Control consisting of Terminal and Chip Autentication

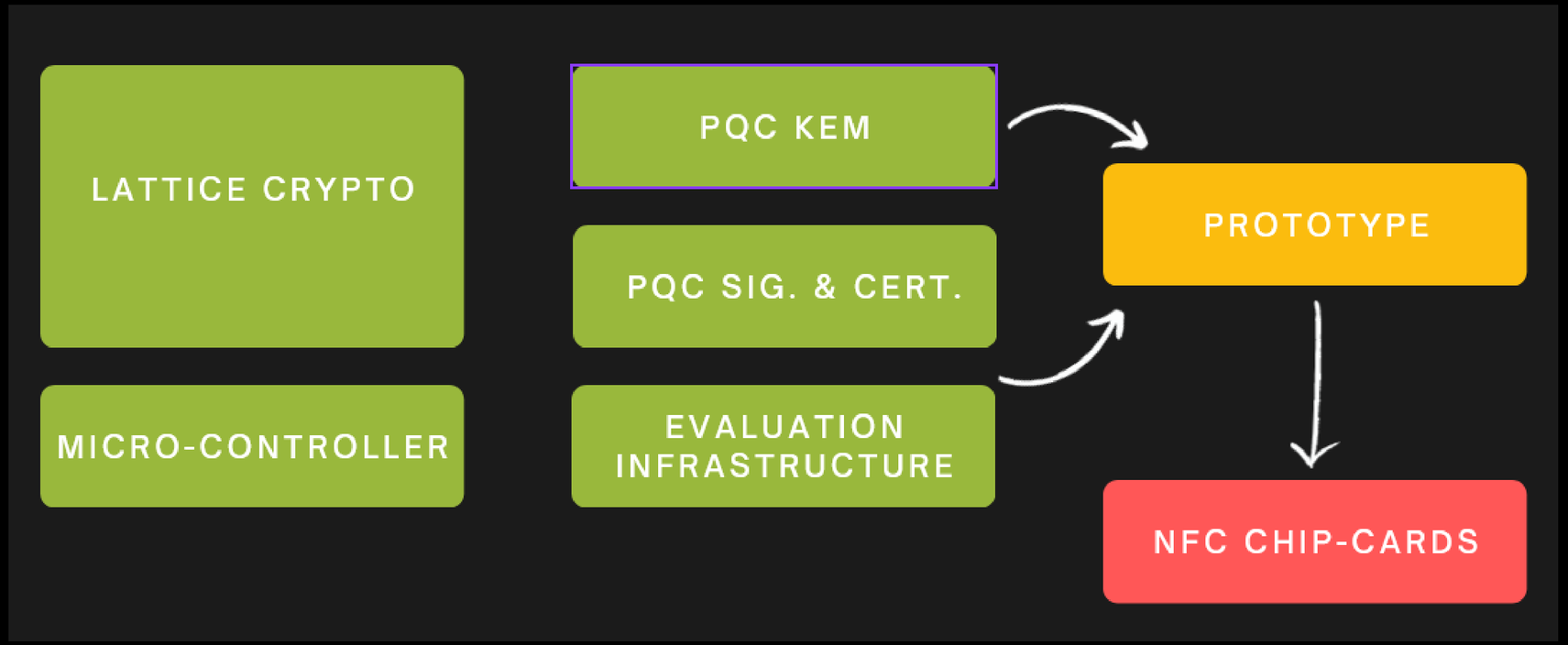
MINDSHARE

h_da darmstadt university of applied sciences

member of EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

Next Generation eMRTDs

Using PQC Primitives



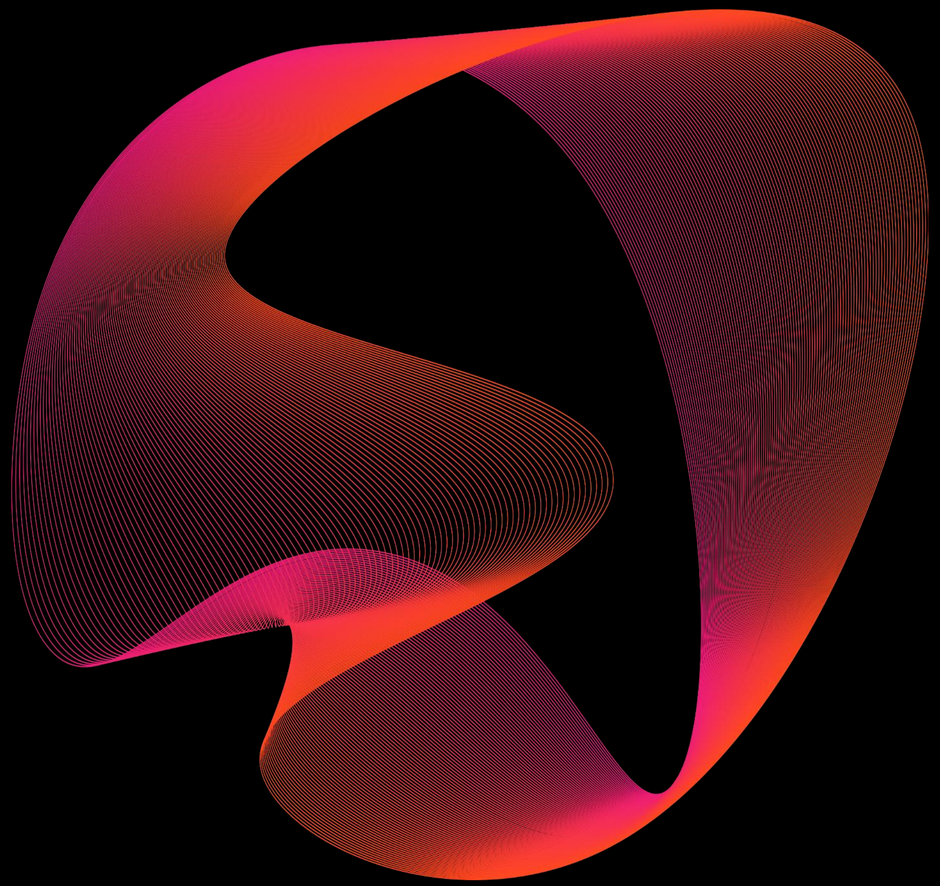
MINDSHARE

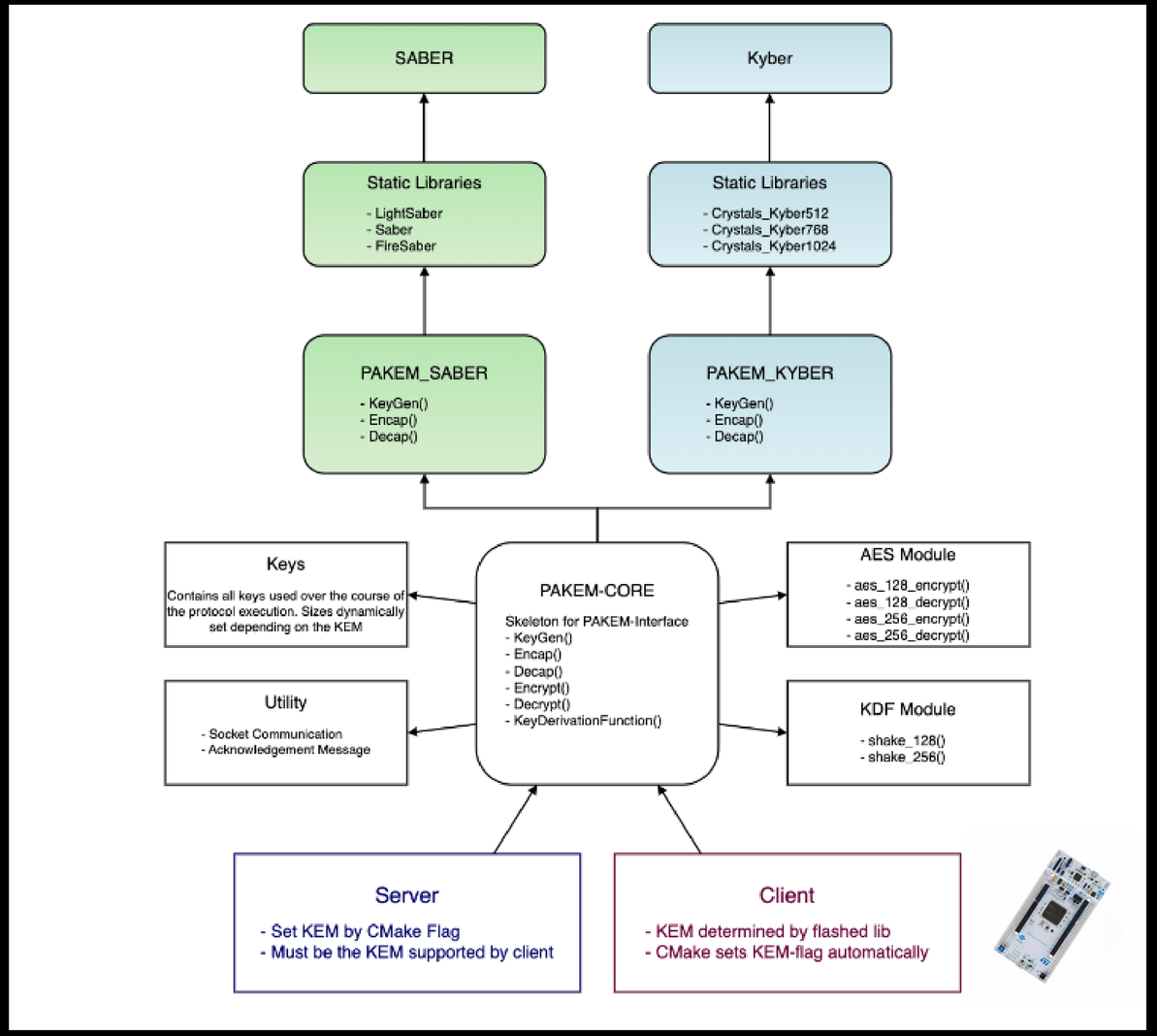
h_da darmstadt university of applied sciences

member of EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

Next Generation eMRTDs

PAKE pqm4 Impl.





MINDSHARE

h_da darmstadt university of applied sciences

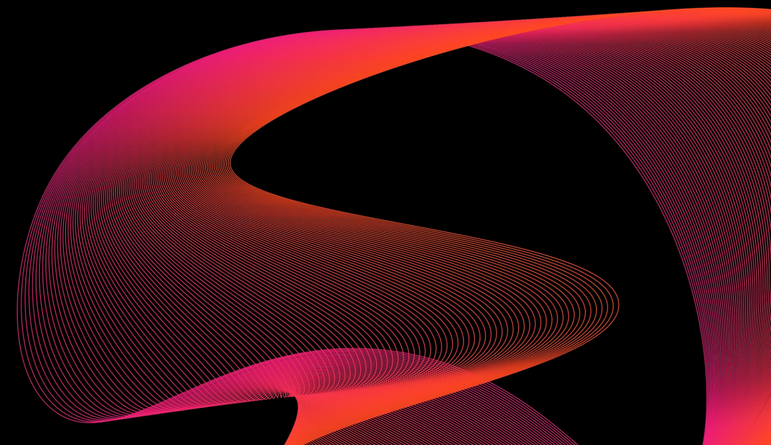
member of EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

Next Generation eMRTDs

Benchamrks on STM32 at 20 MHz

Protocol	Security Level	Runtime (ms)
OCAKE: Card as Initiator	ML-KEM-512 (m4fspeed)	980
	ML-KEM-768 (m4fspeed)	1.390
	ML-KEM-1024 (m4fspeed)	1.924
OCAKE: Card as Initiator	ML-KEM-512 (m4fstack)	986
	ML-KEM-768 (m4fstack)	1.400
	ML-KEM-1024 (m4fstack)	1.918

Adopted from [4]



MINDSHARE

h_da darmstadt university of applied sciences

member of EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

Next Generation eMRTDs

Benchamrks on NXP SmartMX3 P71D600

CPU clock at roughly 12 to 13 MHz

Protocol	Security Level	Runtime (ms)
PACE-BrainpoolP256r1		217
OCAKE: Card as Responder	ML-KEM-512	652
	ML-KEM-768	995
	ML-KEM-1024	1406
OCAKE: Card as Initiator	ML-KEM-512	917
	ML-KEM-768	1500
	ML-KEM-1024	2257

Adopted from [1]

Next Generation eMRTDs

Certificates & PKI (Analysis)

scheme choice	CSCA/CVCA	ML-DSA-65	LMS-h20-192-w8	LMS-h20-256-w8
	DS	ML-DSA-65		
	C	ML-KEM-768		
pk_{CVCA}		1 952	56	64
$Cert_{DS}$	pk_{DS}	1 952	1952	1952
	Signature by CSCA	3 293	1 140	1 772
$Cert_{C}$	pk_{C}	1 184	1 184	1 184
	Signature by DS	3 293	3 293	3 293
sk_{C}		2 400	2 400	2 400
Total (Bytes)		14 074	10 025	10 665

Adopted from [1]

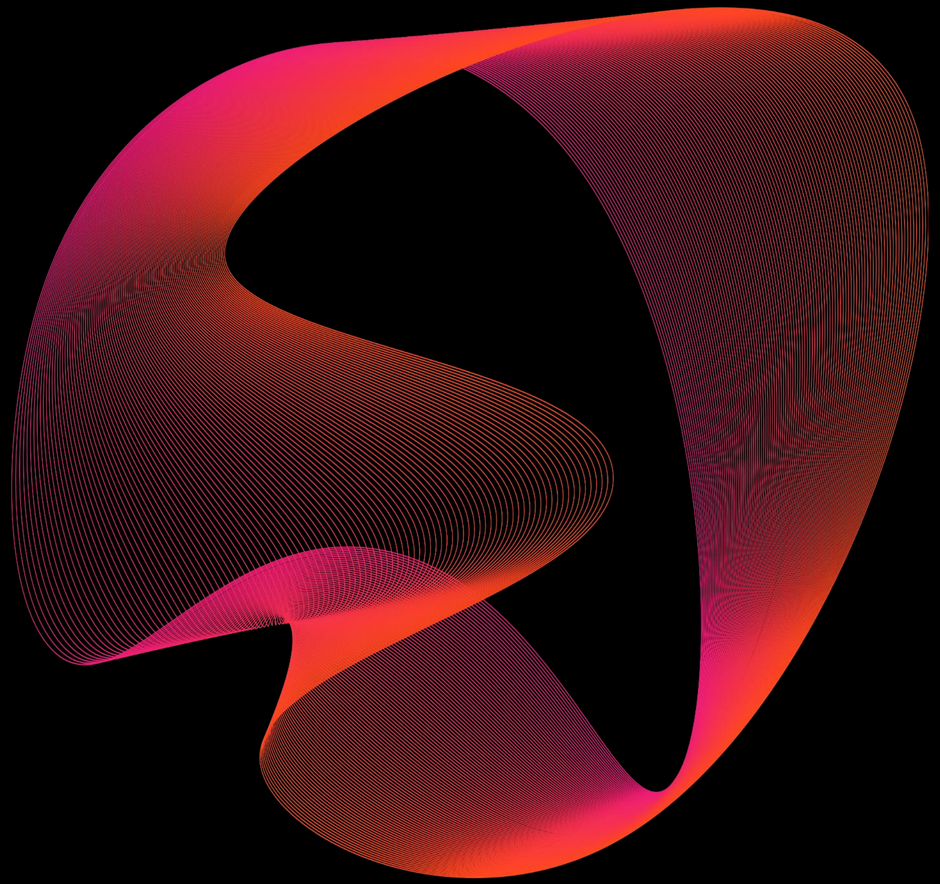
MINDSHARE

h_da darmstadt university of applied sciences

member of EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

Next Generation eMRTDs

Conclusion



- PQC feasible on current HW
- Performance penalties!
- ML-KEM & ML-DAS for eMRTD
- LMS for CA
- Optimized HW?
- SCA & FI?

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

h_da darmstadt university of applied sciences

member of EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

Questions

Nouri Alnahawi
Hochschule Darmstadt
nouri.alnahawi@h-da.de

acsd applied cyber security darmstadt

UR

MINDSHARE

h_da darmstadt university of applied sciences | member of EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

References

- [1] Alnahawi, Nouri, Melissa Azouaoui, Joppe W. Bos, Gareth T. Davies, SeoJeong Moon, Christine van Vredendaal, and Alexander Wiesmaier. "Post-Quantum Cryptography in eMRTDs: Evaluating PAKE and PKI for Travel Documents." *Cryptology ePrint Archive* (2025).

- [2] Alnahawi, Nouri, Nicolai Schmitt, Alexander Wiesmaier, and Chiara-Marie Zok. "Toward next generation quantum-safe eids and emrtds: A survey." *ACM Transactions on Embedded Computing Systems* 23, no. 2 (2024): 1-28.

- [3] Fischlin, Marc, Jonas von der Heyden, Marian Margraf, Frank Morgner, Andreas Wallner, and Holger Bock. "Post-quantum Security for the Extended Access Control Protocol." In *International Conference on Research in Security Standardisation*, pp. 22-52. Cham: Springer Nature Switzerland, 2023.

- [4] Alnahawi, Nouri, Kathrin Hövelmanns, Andreas Hülsing, and Silvia Ritsch. "Towards post-quantum secure PAKE-A tight security proof for OCAKE in the BPR model." In *International Conference on Cryptology and Network Security*, pp. 191-212. Singapore: Springer Nature Singapore, 2024.

- [5] Pradel, Gaëtan, and Chris J. Mitchell. "Post-quantum certificates for electronic travel documents." In *European Symposium on Research in Computer Security*, pp. 56-73. Cham: Springer International Publishing, 2020.