December 2024

Post Quantum Crypto for Secure Elements

Cybersecurity Vehicle Forum, Berlin

sebastian.hans@oracle.com

Why Post Quantum Crypto (PQC)

- Quantum computers are seen as the greatest threat to information security
- Once a sufficiently powerful machine emerges, the current public key cryptography will be obsolete
- This will affect ALL information system government, banking, mobile networks …
- It will happen in svereal steps with a migration from legacy (RSA/ECC) to first generation PQC and hybrid solutions followed by next steps to second or nth generation of PQC algorithm
- Development of Quantum Computing is an ongoing process in several companies with a steady progress but no technical breakthrough so far

IBM pushes qubit count over 400 with new processor

Alternate qubit design does error correction in hardware

Amazon, IBM, and traditional silicon makers are all working toward error correction.

Global Platform™

Why transition now to PQC

NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

- *„Store now, decrypt later“* is a real threat & considerable migration times are to be expected.
  → PQC-migration has to be initiated **now**!

BSI and partners from 17 other EU member states demand transition to Post-Quantum Cryptography

https://www.bsi.bund.de/EN/Service-Navi/Presse/Pressemitteilungen/Presse2024/241127_Post-Quantum_Cryptography.html

Migration to PQC Cryptography has already started

- New cryptographic primitives are now available from NIST FIPS 203, 204, 205 for Digital Signature and Key Encapsulation
- Different approaches for the transitions are poposed
  - Pure Post Quantum Crypto
  - Hybrid or Combined solutions, a combination of traditional algorithm and PQC algorithm
  - In the future a transition from PQC 1st generation to 2nd generation
- New algorithm are not just drop in for existing algorithm
- Protocol flows needs needs to be updated
  - Key Encapsulation (ML-KEM) instead of Key agreement into account
  - For Hybrid solutions as requested especially in European markets
- This protocol migration is ongoing in SDO’s and Specification group
  - IETF, ISO, ITU, 3GPP …
- For Secure Elements GlobalPlatform has started this process in 2023
  - With an inventory of all effected specifications

How does GlobalPlatform work

- Everything is contribution driven
- We have a core specification “GlobalPlatform Card Specification 2.X”
  - Where everything is optional
- We have Amendments that define additional optional features
  - e.g. at the moment PQC support is defined in draft Amendments
- Based on the core specification and the Amendments we define Configurations
  - Configurations are targeting a specific market
    - UICC/SIM configuration, Financial configurations
    - Configurations pick the features they need from the core spec and Amendments and make them mandatory
  - A test specification test the conformance of a Configurations

Transition and Adaptations

- During the process of transition to PQC algorithm we also want to proceed with the modernization of our protocols
- Delete or Deprecate obsolete and outdated algorithms and processes
- Adopt a more Agile approach for the protocol design by including a protocol negotiation phase
- We started with the adoption of X.509 certificates instead of Card Verifiable Certificates in our latest specs and plan to use X.509 certificates for PQC and Hybrid protocols only
- We are at the start of the deployment of PQC algorithm
  - We take into account that new algorithms need to be integrated with our protocol
    - New algorithms under development
    - Algorithms that need to be supported on a local level
  - We want to avoid that our protocol have to be redesigned every few years
- We plan to support all the features defined in ML-KEM and ML-DSA but may not use them
  - Pre-hashing for ML-DSA, optional context …

Dependencies

- SE with GlobalPlatform and Java Card are used in
  - Payment, Mobile Networks, Government ID, SE in embedded devices
  - These infrastructure come with different requirements
- Therefor our development depends on a range of external standards and rulations
  - We rely on NIST Post Quantum Crypto standards
  - IETF and ITU standrds for X.509 or PKI infrstructure in general
  - ETSI / 3GPP / GSMA for security standards related to mobile communication (SIM/UICC)
  - NIST, BSI, ANSSI for security regulation and especiall PQC transition
  - ETSI and IETF for combiner functions in Hybrid solutions
  - …

GlobalPlatform technical work

- GlobalPlatform main specification define how to establish a secure communication between an off-card entity and the SE to perform management operations:
  - Load new keys
  - Manage applications in the SE (load, install, personalize, update, delete)
  - Load software updates
  - Configuration updates
- Transition to PQC means integration of PQC Signatures and Hybrid Signatures with our existing Card content management operations
  - Signing the load files, load data and the management commands
- Creating a new Secure Channel Protocol (SCP)
  - Session key generation based on ML-KEM and ML-KEM / ECKA in the Hybrid mode
  - Defining a new process for confidential SE management

Challenges for Secure Elements

- Secure Element are small constrained devices in every aspect
  - computing power, memory, I/O capabilities
- The biggest problem for us is that all PQC crypto is (to) big
- Not every PQC algorithm under discussion can be implemented on a Secure Element
  - Size and computing resources restrict our choices
  - Our focus is on ML-KEM and ML-DSA specified by NIST in FIPS 203 and 204
    - ML-KEM and ML-DSA keys are already much larger then existing keys
    - and ML-DSA needs more computing power and has even longer keys then ML-KEM
    - ML-KEM and ML-DSA are not the same algorithm
  - Hash based Signatures are under observation, but the issue is that their signatures are mindboggling big

Size and Performance overview

Operation	Sec Level 1	Sec Level 2	Sec Level 3	Compared with ECC
ML-KEM end certificate (signed with ML-DSA of the same category)	3566	4839	6542	
ML-DSA certificate (self signed certificate with ML-DSA of the same strength)	3958	5511	7469	
ML-DSA signature	2420	3309	4627	10-14
ML-KEM ciphertext	768	1088	1568	
ML-KEM decapsulation key (secret)	1632	2400	3168	2,3-5,5
ML-KEM encapsulation key (public)	800	1184	1568	2,3-5,3
ML-DSA key (private)	2528	4000	4864	
ML-DSA key (public)	1312	1952	2592	

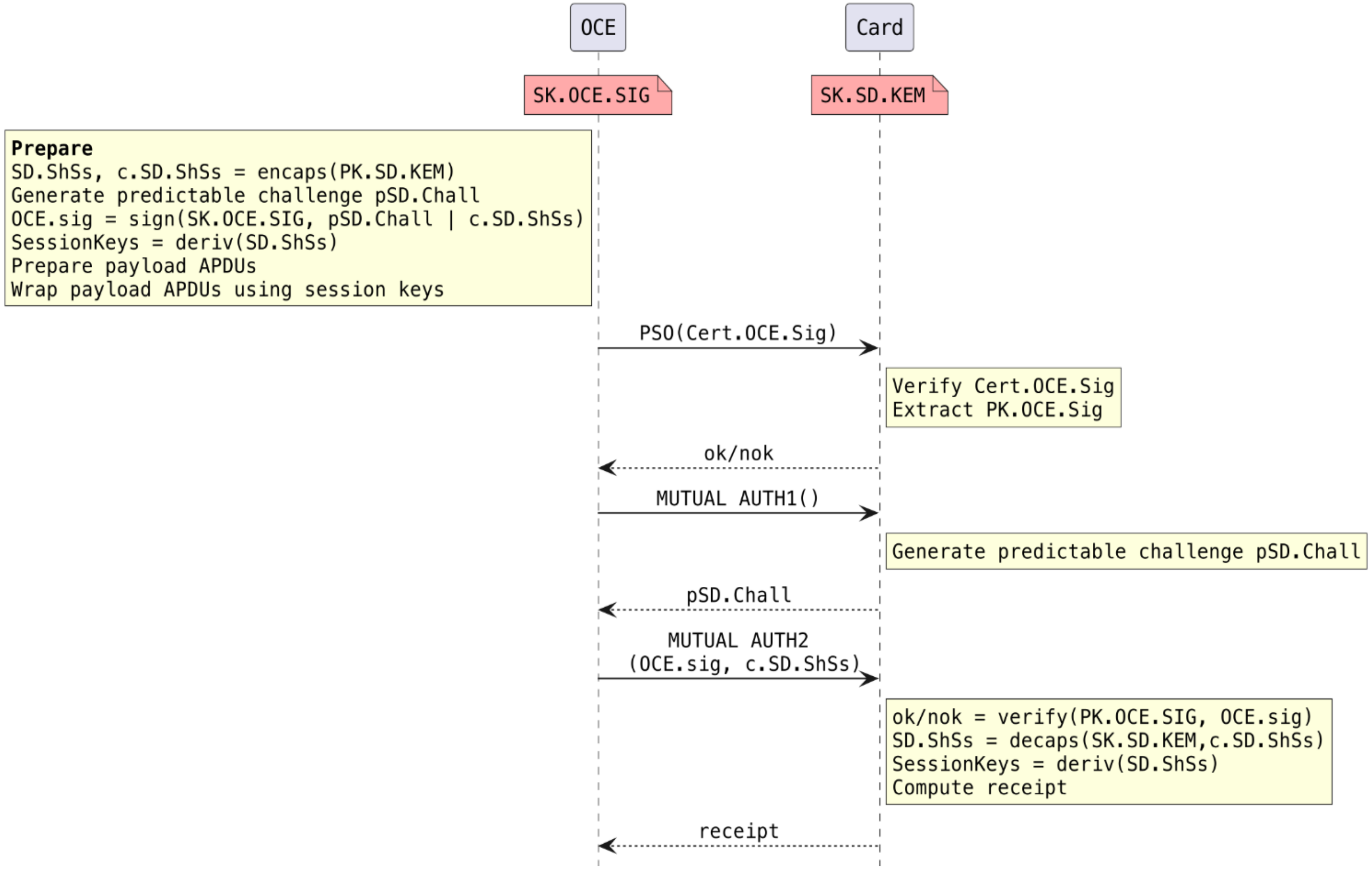
Global Platform™

Optimization of the Protocol flow

- We are currently analyzing different protocol flows
  - The goal is to optimize them in terms of data exchange and round trips needed to authenticate and perform session key agreement
  - Under discussion is to avoid if possible the use of Signatures for authentication and only use authenticated KEM
  - The most costly operation is a ML-DSA signature
    - If possible signature generation should be done outside of the SE, the SE is only verifying the signature
  - Certificate exchange has to be minimized if possible
  - We also work on formally proving the security of our drafts (ProVerif)

Scripted Secure Channel Mode

- For SE we need a scripted mode of an SCP
  - Commands are scripted and wrapped with a session key
  - Mutual authentication between OCE and Card
  - SE is ensured the script comes from an authorized source
  - OCE is ensured only an authorized card can decrypt the script



Global Platform™

Our Members

Full

- ANALOG DEVICES – AHEAD OF WHAT'S POSSIBLE™
- Apple
- arm
- Bundesamt für Sicherheit in der Informationstechnik
- BCTC 银行卡检测中心 BANK CARD TEST CENTER
- T · · ·
- FeliCa Networks
- fime
- galitt – a Sopra Steria company
- G+D Mobile Security
- Google
- HID
- HUAWEI
- IDEMIA – augmented identity
- infineon
- mastercard
- NTT
- NXP
- ORACLE
- Qualcomm
- SAMSUNG
- ST – life.augmented
- THALES
- T Mobile
- TRUSTONIC
- VISA
- winbond

Participant

- Applus+
- OPL Lab
- COMPRION – Test it. Prove it. Move it.
- DNP
- DEKRA
- HONOR
- riscure – Challenge your security
- SERMA – SAFETY & SECURITY
- SGS brightsight
- orange
- Quarkslab
- TRUSTCB – TRUST AND VERIFY
- UL
- VALID

Observer, Public Entity and Consultants

- AM EX
- AT&T
- CARIAD
- cea leti
- CB
- cisco
- 楚天龙 CHUTIAN DRAGON 龙行天下 昌赢未来
- Department of Defense – United States of America
- DISCOVER
- 东信和平 EASTCOMPEACE
- FEITIAN – WE BUILD SECURITY
- 財團法人資訊工業策進會 INSTITUTE FOR INFORMATION INDUSTRY
- JCB
- kaspersky
- Kigen
- KONA I
- MASKTECH
- MK smart – Smart Digital Security
- PQ SHIELD
- Rambus
- SAMSUNG
- SAMSUNG SDS
- 上海复旦微电子集团股份有限公司 Shanghai Fudan Microelectronics Group Company Limited
- SK
- synapse mobile networks
- SPREADTRUM
- TTL
- TOSHIBA
- UBIVELOX
- UNISOC
- xardpay
- XCURE CORP.
- mi
- BACTECH
- Digital Cubes
- INTERNET OF TRUST
- MoneTECH
- NEXTENDIS
- SAFEPAY
- zwipe

Global Platform™

The standard for secure digital services and devices

→globalplatform.org