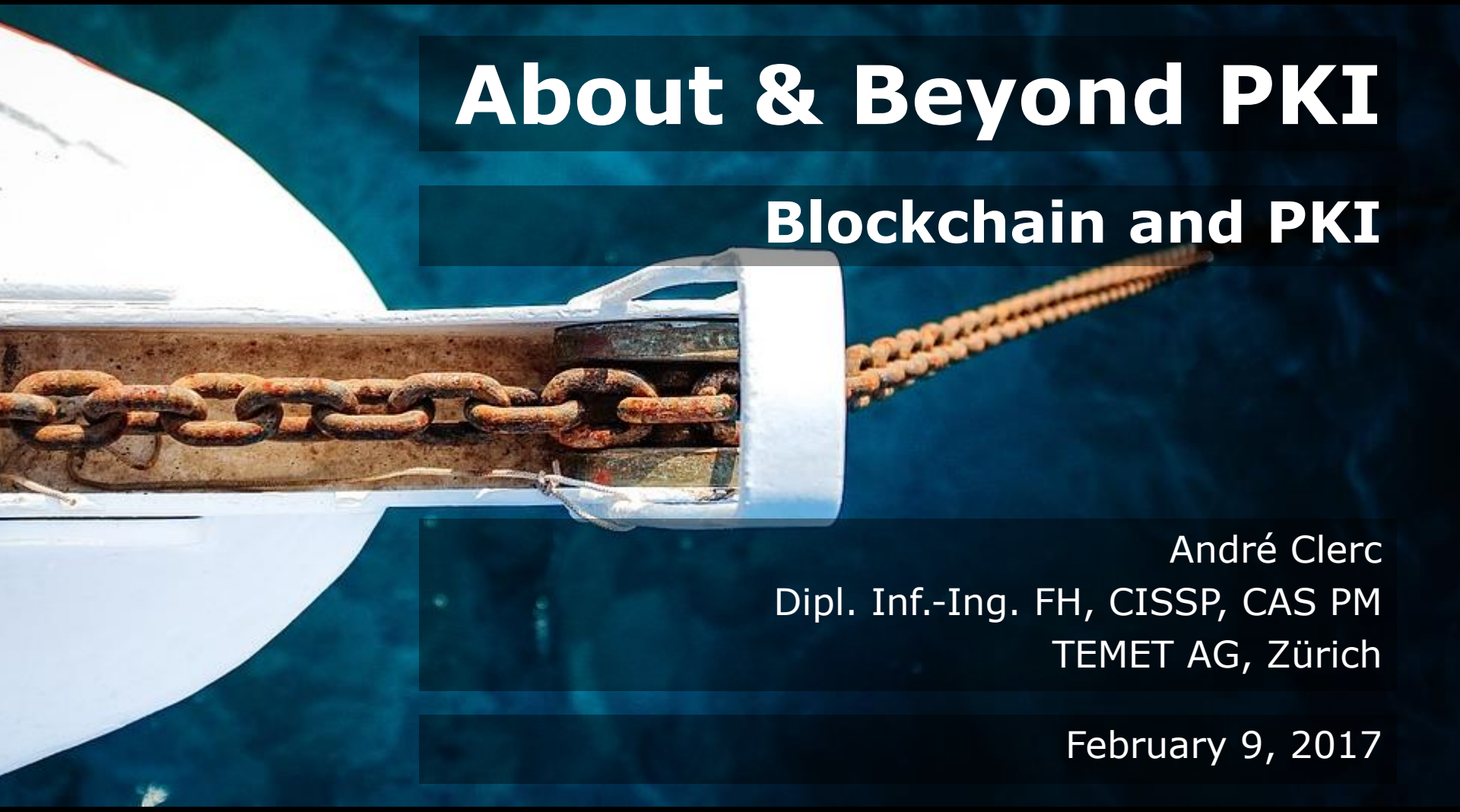


About & Beyond PKI

Blockchain and PKI

André Clerc
Dipl. Inf.-Ing. FH, CISSP, CAS PM
TEMET AG, Zürich

February 9, 2017

Agenda

- Does **blockchain** secure **PKIs** in the long-term?
  - Disadvantages of classic PKIs
  - Facts about blockchain
  - Implementation approaches
  - Advantages and disadvantages of blockchain
- What can we do if **post quantum cryptography** (PQC) is not available yet?
- What shall we do if **PQC** can be used?

Blockchain and PKI
Introduction

- It is assumed that all current PKIs are based on cryptographic procedures which will be broken in the future by quantum computers

- It's even **worse**:
  - *There are physicists who believe that the breaking of the asymmetric key is more efficient than its creation!*
- The **question** arise:
  - *Will new technologies (e.g. blockchain) help us to solve the above mentioned fact or do we have to look for new solutions?*

Blockchain and PKI
Disadvantages of classic PKIs

- The **identity verification** process may be insufficient
- An offered guarantees of **identity retention** may not be strong enough
- A certificate authority (CA) may issue **unauthorized certificates**
- The misbehavior of a CA may not be detected
  - Expect log-based PKIs

Blockchain and PKI
Disadvantages of classic PKIs

- **Responding** to CA misbehavior takes time and requires manual effort
- A CRL **check** can be based on a outdated list (inadequate update cycle)
- A CRL or OCSP check can been disabled
  - Revoked certificates will not be detected
- The **CRL distribution point** (CDP) may become a single point of failure

Blockchain and PKI
Disadvantages of classic PKIs

- All currently used algorithms for PKIs are **not safe** against quantum computers
  - RSA, DSA, ElGamal, ECC, DH Key Exchange
  - SHA-1, RIPEMD-160, SHA256
  - Symmetric keys < 128-bit
- The algorithms Shor and Grover were developed more than 20 years ago!
- *Why don't we use blockchain?*

Blockchain and PKI
Blockchain facts

- **Blockchain *is not* Bitcoin**; it enables it

- It is a distributed database that maintains an increasing list *(ledger)* of records *(blocks)*
- Each block in the ledger *(blockchain)* is *"linked"* to a previous block
  → *hash-tree or hash-calendar*
- In general the ledger is open and not centralized
  → *Distributed Open Ledger - DOL*

Blockchain and PKI
Blockchain facts

- Can built with hash-tree, merkle-hash-tree or hash-calendar
- Based on “proof-of-work (PoW)”, “proof-of-stake (PoS)” or proof-based KSI
- A 512-bit public key is built on a 256-bit private key by using ECDSA
- Hashes are built with SHA256 and RIPEM-160; SHA3-256
- We **can not say**, that these algorithms are quantum computer proof

Blockchain and PKI
Implementation approaches

- Instant Karma PKI (IKP) - Turning a PKI Around with Blockchains
  - *"Carnegie Mellon University and ETH Zurich, 2016"*
  - Based on Ethereum
  - Addresses the **problem of log-based PKI**, which do not offer sufficient incentives to logs and monitors, and do not offer any actions that domains can take in response to CA misbehavior
  - Describe a blockchain-based enhancement that offers **automatic responses to CA misbehavior** and incentives for those who help detect misbehavior.

Blockchain and PKI
Implementation approaches

- Decentralized Public Key Infrastructure (DPKI)
  - *"Respect Network, PricewaterhouseCoopers, Open Identity Exchange, and Alacrity Software, Dec. 2015"*
  - Based on Namecoin
  - Approach which **returns control** of online identities to the entities they belong to
  - It **enables bootstrapping of online identities** and provides to create stronger SSL certificates

Blockchain and PKI
Implementation approaches

- Backing Rich Credentials with a Blockchain PKI
  - *"Karen Lewison and Francisco Corella, Oct. 2016"*
  - Based on Ethereum
  - *Remote identity proofing*
  - ***Revocation checking*** *is performed on the verifier's* ***local copy*** *of the blockchain without requiring CRLs or OCSP*
  - *A* ***service that issues certificate revocation lists*** *(CRLs) or responds to online certificate status protocol (OCSP) is* ***not used***

Blockchain and PKI
Implementation approaches

- KSI Keyless Signature Infrastructure
  - *Based on hash trees*
  - *"Guardtime"*
  - *A globally distributed system for **providing timestamping** and server-supported **digital signature** services.*
  - *Global per-second hash trees are created and their root hash values published*
  - *Are not **vulnerable to key compromise** and thus provide a solution to the problem of long-term validity of digital signatures*
  - ***KSI** in intended to **protect integrity** of an asset while **PKI** is intended to **protect its confidentiality***
  - ***Is not usable for encryption***

Blockchain and PKI
Pros and Cons of Blockchain

Pros

- **Inherently resistant against unwanted modifications**

- High availability
- Operated by a decentralized authority
- Open for all participants so that they can verify all modifications
- Cloud contains data or even code (smart contracts - *Ethereum*)

Cons

- **Scalability** and throughput capacity
- If someone gets more than 50% mining power he **controls the ledger**
- The linking process could be **extremely wasteful** (as it is in Bitcoin)
  - Difficulty: 392,963,262,344
  - **Average 3.1 EH/s or 3.1E+18 (Trillion), require 200MW and more**
- *According to the current state of research,* ***all used algorithms are not quantum computer proof***

Blockchain and PKI

Blockchain and PKI

But there’s still a lot of work to do…

Blockchain and PKI
Steps/Processes before PQC

- Verify if you know **all critical applications** that use certificates
- Verify if your **inventory** contains all applications and communication channels where asymmetric cryptography is used
- Verify if you have a process to update your **cryptography policy**
  - Are there new standards which must be used?
- Verify if your current PKI **strategy** is up to date

Blockchain and PKI
Steps/Processes before PQC

- Verify if your key or certificate management is **in line** with your business
- Clean up all unnecessary keys (certificates)
- Verify if the current **key life cycle** process is up to date
  - Verify if your initial identity validation is performed according to your policies
  - Verify if your process to create, replace and revoke asymmetric keys works according to the policies
  - *If you have an automatic enrollment process in place ensure that you have also an **automatic withdrawal***
- Verify if your **certificate validation** process is up to date

Blockchain and PKI
Steps/Processes before PQC

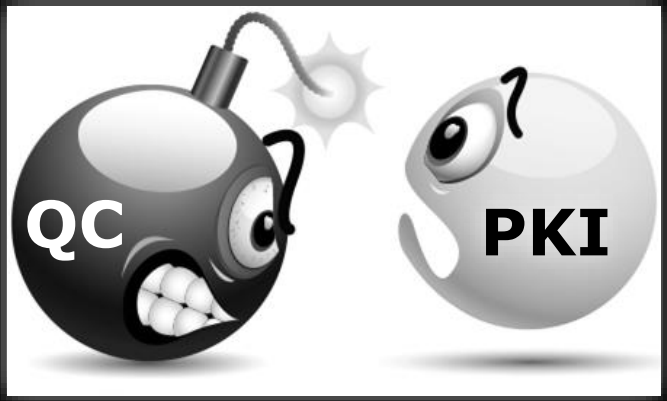
- Can you answer these questions for your organization:
  - Do I use adequate algorithms and key size?
  - Do I have a cryptography policy and who defines it *(Algorithms, key generation, length, storage, archiving and restoration, etc.)?*
  - Which instance (entity) uses which keys (certificates)?
  - Who is responsible for which keys and who should update or renew them?
  - When do public keys reach their expiration date?
  - Do I know all communication channels?

Blockchain and PKI
Steps/Processes before PQC

- Further questions for your organization:
  - Who creates the key material and the correlating certificate signing request (CSR)?
  - Which CA (internal / external) is responsible for issuing a certificate?
  - Do I know the life cycle of the current PKI regarding hardware (Server and HSM) and software?
  - Do I know how a CA renewal will influence the organization and what steps are involved?
  - ***Do I know the current (industrial/RFC) standards regarding quantum proofed algorithms?***

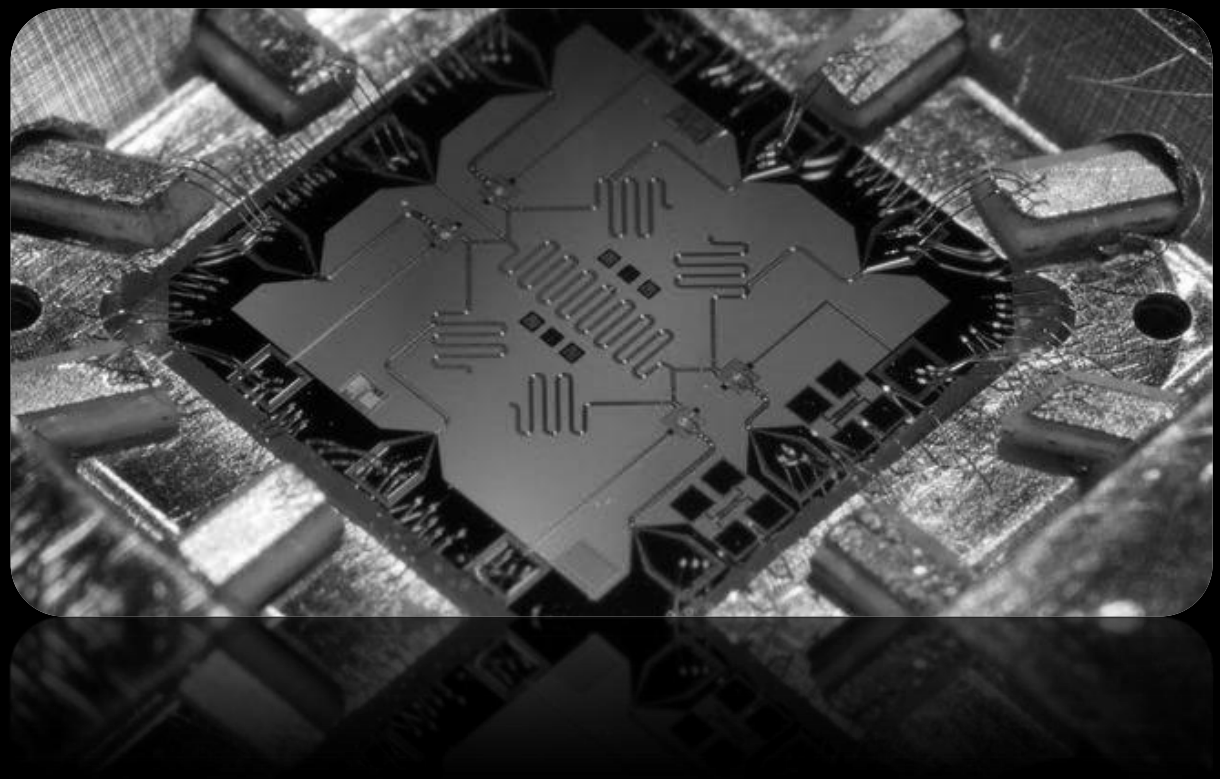
Blockchain and PKI
Steps/Processes before PQC

- GOOD NEWS:
  - There is still time
  - We have the chance to further verify possible disadvantages and find answers to our most important questions



- *What if PQC is available?*

Blockchain and PKI
If PQC is available…

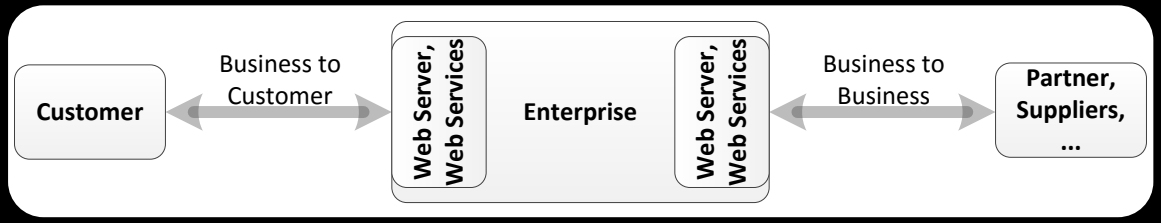


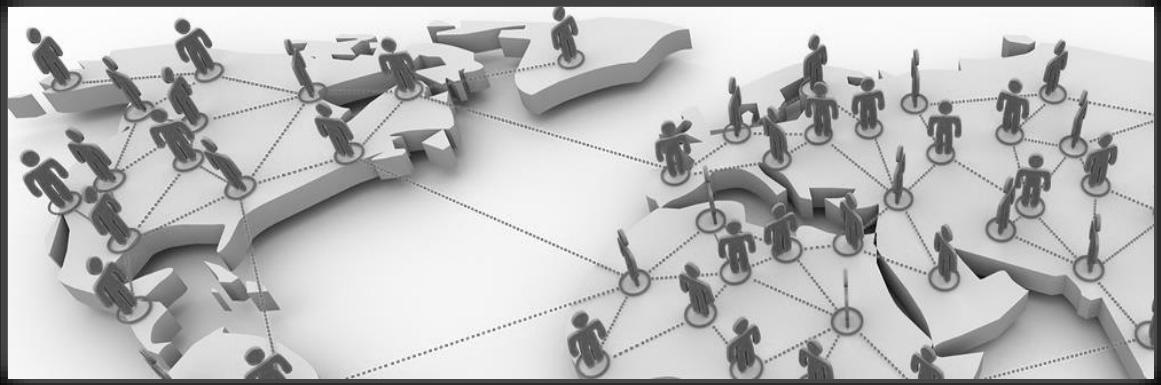
Blockchain and PKI
Steps/Processes with PQC

- Establish a process to verify the **maturity** of the PQC algorithm
  - Is the algorithm in development, draft or standardized (ETSI, ISO/IEC, ISA/ICE, ISF/SoGP, NIST, etc.)?
  - Is the algorithm commodity or does it only have a military purpose?
  - What degree of integration does the algorithm have by leading companies like Apple, Microsoft, IBM, Intel, etc.?
  - Is an early adoption necessary (because of long term data archiving) or not?
  - Are the algorithm and its implementations resistant regarding other attacks (side channels, etc.)?
  - Are there any legal or regulatory requirements such as FINMA, Swiss government, etc.?

Blockchain and PKI
Steps/Processes with PQC

- **Integrate** a PQC algorithm
  - Which communication channel is relevant





Blockchain and PKI
Steps/Processes with PQC

- **Integrate** a PQC algorithm
  - Define which applications or topics are affected
    - S/MIME, SSL/TLS, SSH, VPN, LONG TERM ARCHIVE, WIRELESS COMMUNICATION, STRONG AUTHENTICATION, DATA ENCRYPTION/SIGNATURES, SMARTCARDS, ACCESS TOKENS, EXTERNAL/INTERNAL PKI

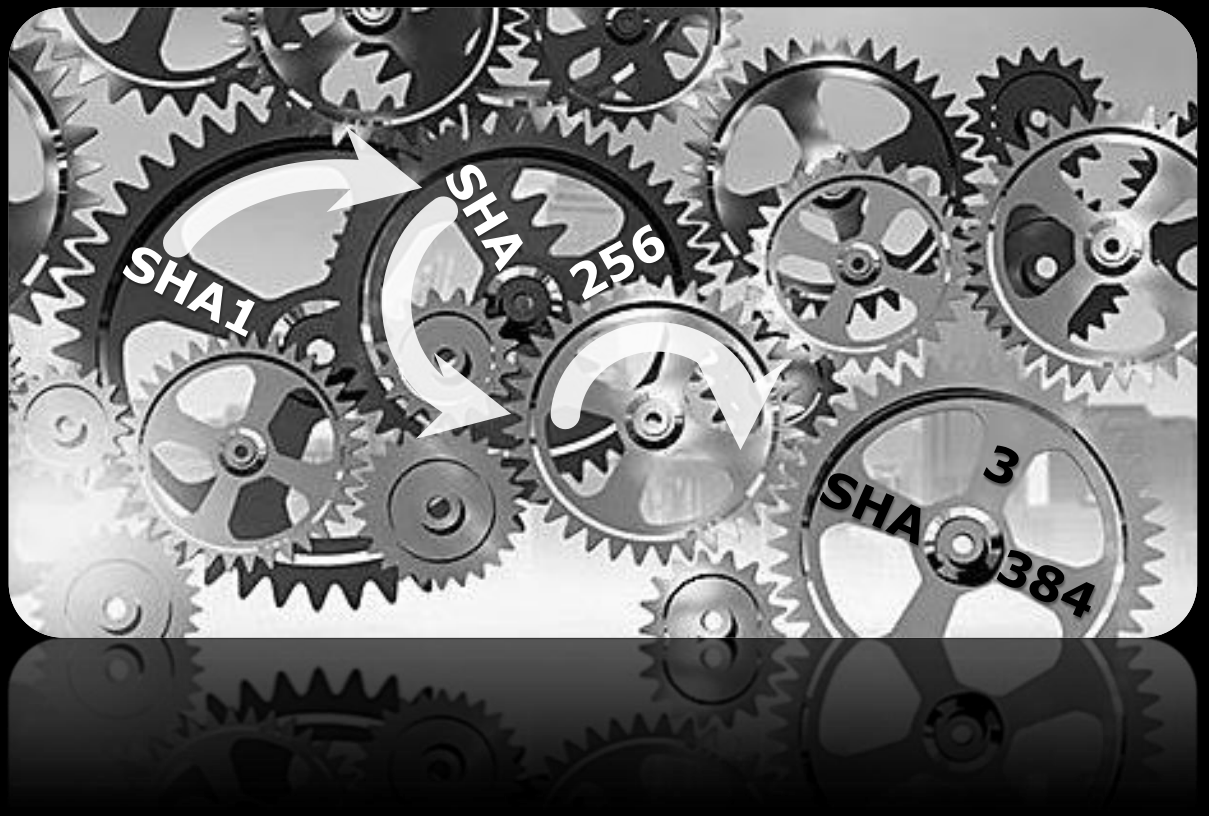
  - Define which keys or certificates have to be renewed within which time

Blockchain and PKI
Steps/Processes with PQC

- **Integrate** a PQC algorithm
  - Define a strategy to eliminate legacy applications
  - Define where new keys or certificates have to be distributed (e.g. AD, AIA, CDP, etc.)
  - Update your configuration management system (CM)
  - Involve your change management

Blockchain and PKI
Steps/Porcesses with PQC

- Conclusions
  - You might have already done things like that…



THANK YOU FOR YOUR ATTENTION