asseco

DATA SYSTEMS

ASSECO DATA SYSTEMS

Post Quantum Cryptography and Trust services

Robert Poznański

Analyst

Warsaw, 06.06.2022

DATA SYSTEMS

Agenda

- What is Post Quantum Cryptography
- What challenges do we face
- Services and solutions will be affected
- What are the consequences
- How can we prepare
- Impact on business

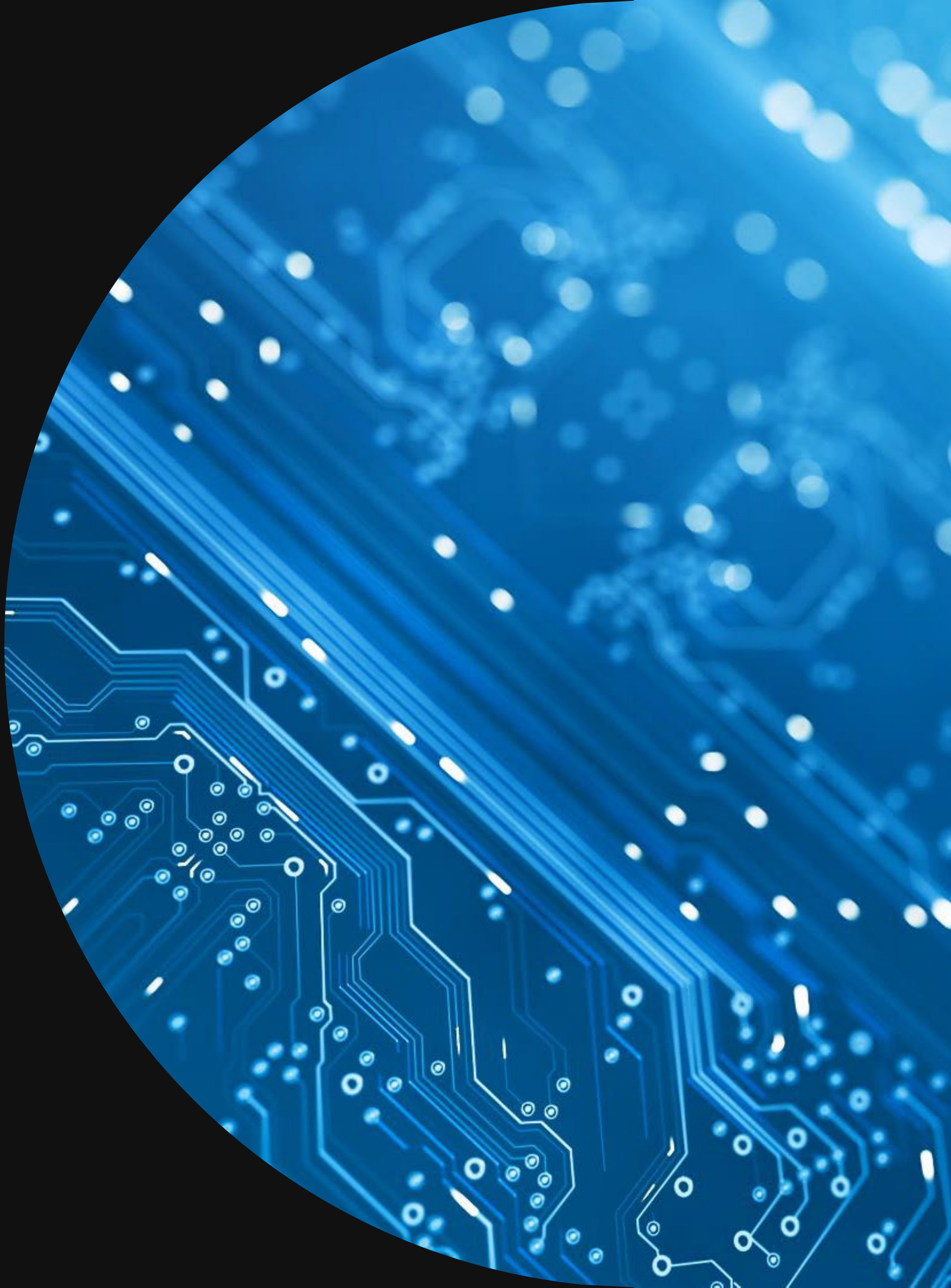
- Q&A

What is Post Quantum Cryptography?

What is quantum computing?

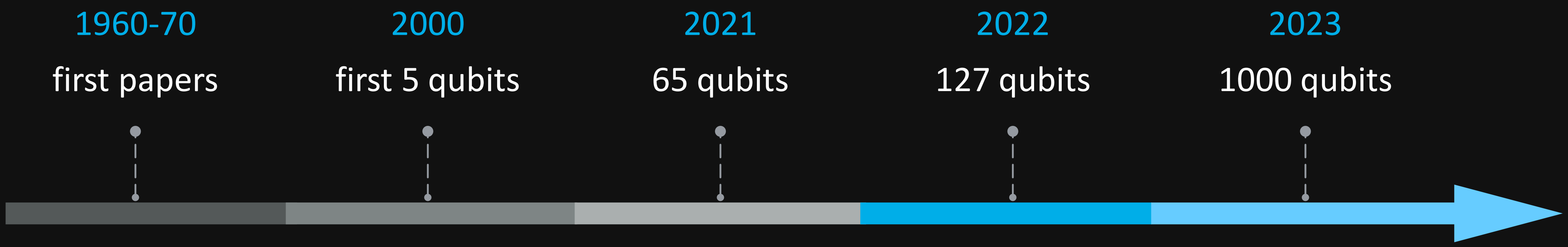
Computers that use quantum state of matter called superposition (and qubits) to conduct large scale calculations

- IBM
- Google
- Microsoft
- D-Wave
- Intel



What is quantum computing?

Idea of quantum computers is not new



1960-70 first papers

2000 first 5 qubits

2021 65 qubits

2022 127 qubits

2023 1000 qubits

Certain algorithms and mathematical equations are computed faster than on traditional computers

What is quantum computing?

What is the impact of QC?

Quantum computer will allow to perform almost instantly or greatly reduce computing time of certain algorithms necessary for cryptoanalysis of todays cryptography standards

Grover's algorithm
– symmetric ciphers
(like AES)

Shor's algorithm
– asymmetric ciphers
(like RSA, ECC)

What is quantum computing?

What is the impact of QC?

- There is another use for quantum computers

Physics

Chemistry

Medicine

AI

What challenges do we face?

What challenges do we face?

Security: confidentiality, integrity, proof of origin

- How long should data be confidential
  - → 3 years?
  - → 7 years?
  - → Maybe more?
- Proof of origin
- Proof of integrity

asseco
DATA SYSTEMS

Services and solutions will be affected?

asseco DATA SYSTEMS

Services and solutions will be affected

Who should be afraid?

- Everyone – every service and device using PKI
- Potential attacks may influence nearly every cryptographic implementation that uses RSA or ECC algorithms
- For symmetric algorithms longer keys should be enough to provide security
- Hash functions will not be affected

Services and solutions will be affected

Who should be afraid?

- TLS – Transport Layer Security
  - → Confidentiality of data exchange
  - → Traffic scanning and collecting for future decryption

Services and solutions will be affected

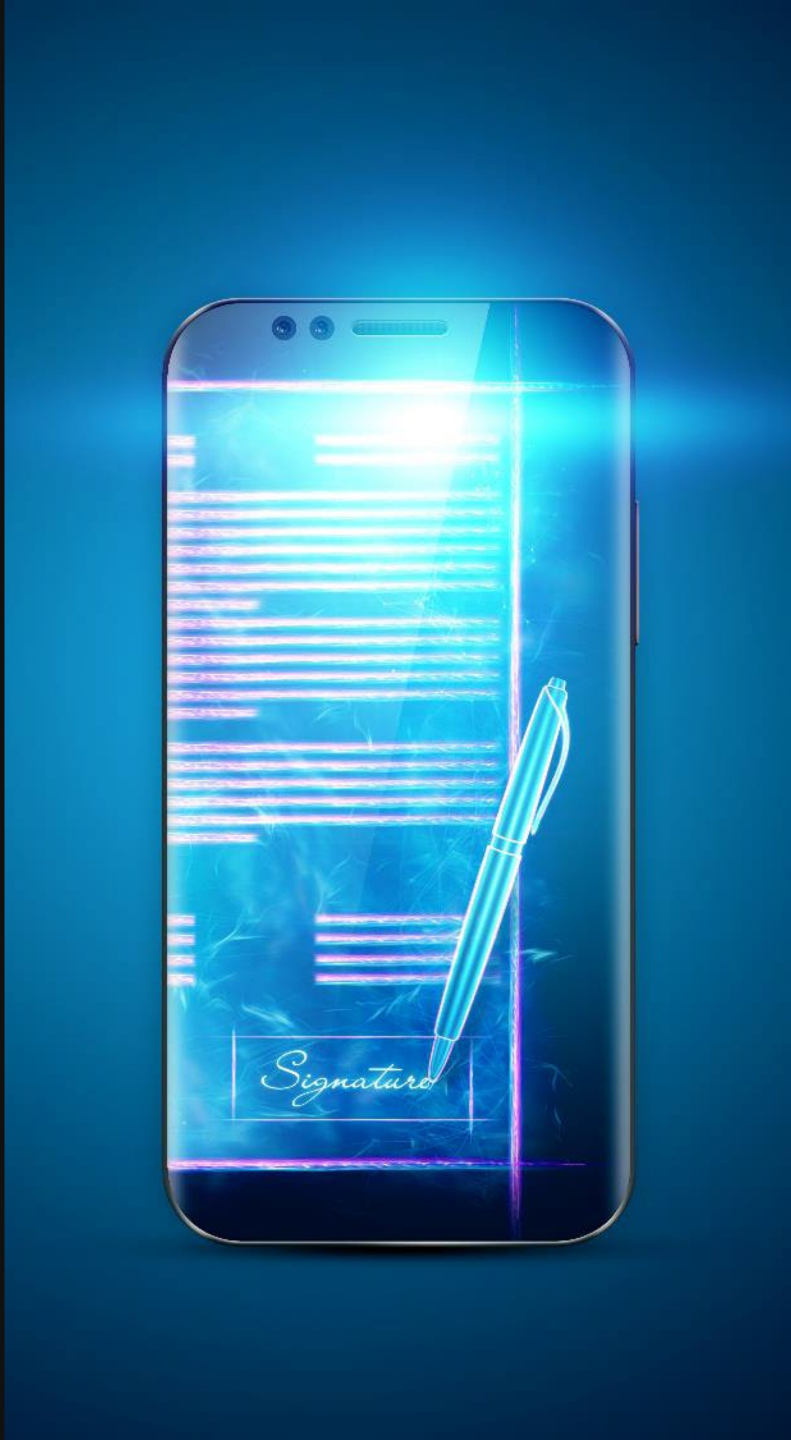
Who should be afraid?

Trust services providers:

- Long term certificates
- Documents archiving
- Signatures
- Other services

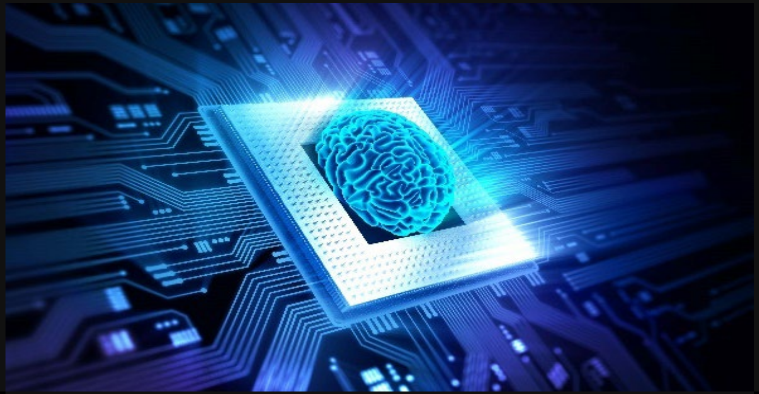
Consequences:

- Compromisation of signatures
- Loss of integrity
- Loss of proof of origin



Services and solutions will be affected

Who should be afraid?



Other services:

- IoT
- Cars
- Smartcard solutions
- Other devices
- eID systems

Consequences:

- Loss of device authentication mechanisms
- eID compromisation

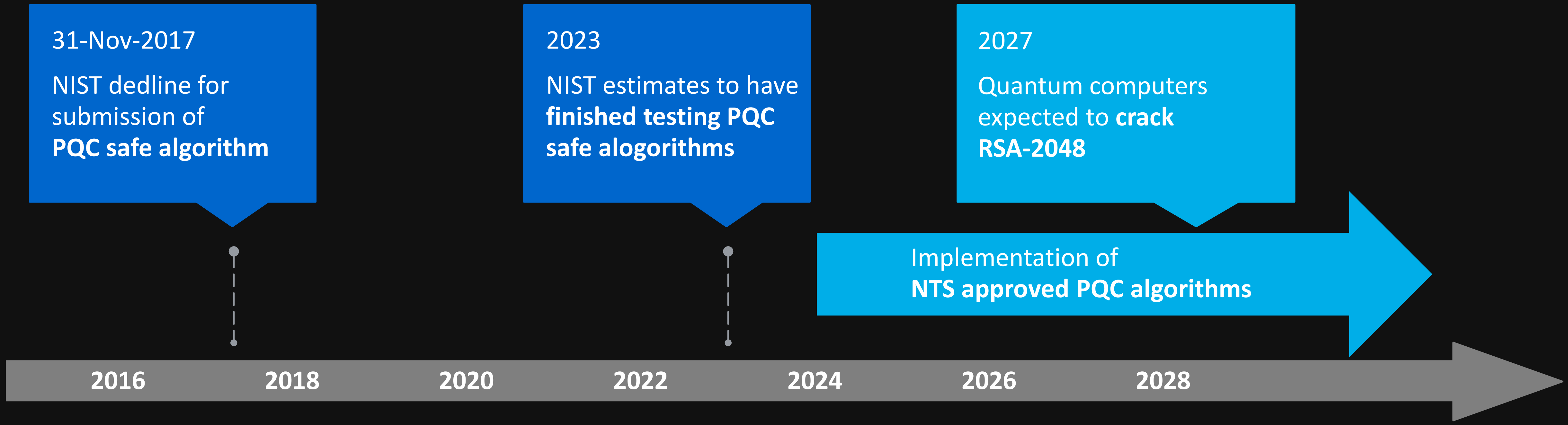
asseco DATA SYSTEMS

What are the consequences?

What are the consequences?

NIST

- Since 2016 NIST is working on standardization of new algorithms



31-Nov-2017

NIST dedline for submission of **PQC safe algorithm**

2023

NIST estimates to have **finished testing PQC safe alogorithms**

2027

Quantum computers expected to **crack RSA-2048**

Implementation of
NTS approved PQC algorithms

What are the consequences?

NIST

- New algorithms for data encryption:
  - → Classic McEliece
  - → CRYSTALS-KYBER
  - → NTRU
  - → SABER
- New algorithms for digital signatures:
  - → CRYSTALS-DILITHIUM
  - → FALCON
  - → Rainbow

asseco DATA SYSTEMS

What are the consequences?

ETSI, ENISA, BSI

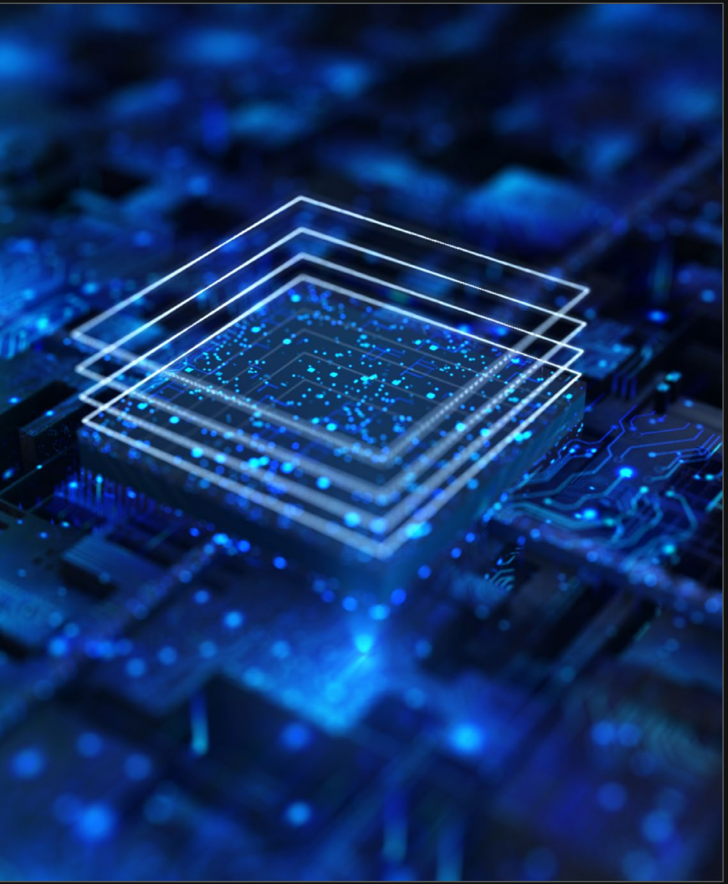
- Help in transition to new algorithms and implementations:
  - → ENISA: POST-QUANTUM CRYPTOGRAPHY Current state and quantum mitigation
  - → ETSI: CYBER Migration strategies and recommendations to Quantum Safe schemes
  - → BSI: Migration to Post Quantum Cryptography

DATA SYSTEMS

How can we prepare?

How can we prepare?

Are there any solutions for us?



✓

Get ready for new standards in cryptography

- Build knowledge
- Involve in standardization

✓

HSMs providers

- Pressure in implementing new algorithms
- Certification of devices will take time after new algorithms are recommended

How can we prepare?

What can we do?

- Implement Crypto agility
  - → Investigate new approaches
  - → Prepare infrastructure and applications
  - → Talk with vendors and pressure on new solutions
  - → Will allow easier change of todays and future algorithms
- Implement hybrid solutions
  - → We can use „classic" and post quantum algorithms for signatures
  - → Lack of standards to implement and recognize PQ algorithms today
  - → No PQ algorithm validation services

How can we prepare?

What can we do?

- ENISA guidelines
  - → TR 103 616 Quantum-Safe Signatures
  - → TR 103 619 Migration strategies and recommendations to Quantum Safe schemes
- Flexibility will allow to implement future changes easier and more reliable;
  - → Crypto agility
  - → Implement hybrid solutions
  - → Due to attack potential, focus on changing long term solutions and services like archive, conservation, and other using 3-5+ years valid certificates

Impact on the business?

asseco
DATA SYSTEMS

Impact on the business

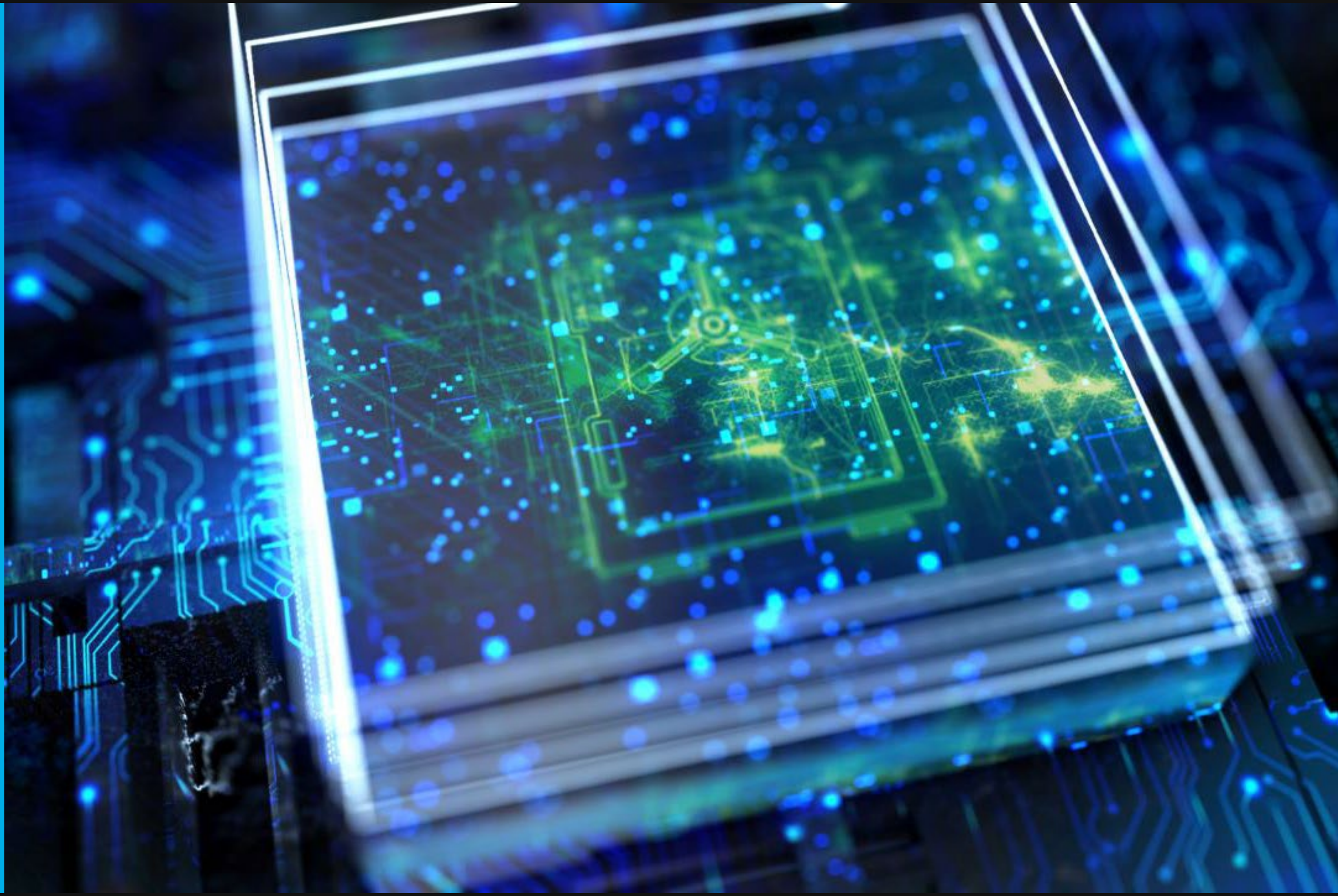
How Asseco is preparing?

- We are implementing Crypto agility
- Preparing issuing hybrid RSA/ECC + PQC certificates
- Testing PQ algorithms accepted to Round 3 NIST evaluation process

Impact on the business

How Asseco is preparing?

- We talk with
  - → IBM
  - → Entrust
  - → Microsoft
- We are preparing to test HSM devices
- We are testing our components with PQ
- We want to involve in standardization work of ETSI, ENISA
- Still looking for potential partners



Impact on the business

How can we all prepare?

- We need more involvement in standardization work from ETSI and ENISA
- We need more guidelines, standards, best practices
- We need updated ETSI ALGO paper
- We need data structures for hybrid solutions
- We need data structures for two signatures on one document (RSA and PQ)

Q&A

Thank you.

Robert Poznański

Analyst

e-mail: robert.poznanski@assecods.pl

tel.: +48 785 504 292

asseco
DATA SYSTEMS

The power of creation.

Asseco Group

www.asseco.com

@asseco_group

linkedin.com/company/asseco-group

Asseco Data Systems

www.assecods.pl

@assecods

linkedin.com/company/assecods

fb.me/assecods

Legal disclaimer

The content of the presentation is subject to copyright and is protected by law. Texts, graphics, photographs, sound, animations and videos, as well as their arrangement in presentation are subject to protection under the provisions in force, including in particular the Copyright and Related Rights Act and the Industrial Property Law Act. Any unauthorized use of any of the contents of this presentation may violate the rights of Asseco Data Systems S.A. (proprietary copyrights, protection rights to trademarks or other rights) or rights vested in Asseco Poland S.A. to the extent to which Asseco Data Systems S.A. makes use of the content to which Asseco Poland S.A. has the right under the concluded contracts and agreements. The content available in the presentation cannot be modified, reproduced, publicly presented, performed, distributed or used for other public or commercial purposes, unless Asseco Data Systems S.A. has explicitly expressed their consent in writing. Copyingfor commercial purposes, distribution, modification or transfer of the contents of this presentation (in whole or in part) by third parties is forbidden. Asseco Data Systems S.A. stipulates that the presentation may contain content referring to offers and services provided by third parties. The terms of use of the offers and services of third parties are specified by the said parties.

Asseco Data Systems S.A. shall bear no liability for the terms and effects of use of offers and services of the said third parties. The data and information contained in the presentation is general informational in nature.

The name and logo of Asseco Data Systems S.A. and Asseco Poland S.A. are registered trademarks. Using those trademarks requires an explicit consent of the above mentioned entities.