Post-Quantum

Cryptography Conference

Post-Quantum Cryptography & Trust Services

Lizzy Polman

Inspector, Dutch Authority for Digital Infrastructure

Rijksinspectie Digitale Infrastructuur
*Ministerie van Economische Zaken
en Klimaat*

eIdentification (eID)
eProcurement
eInvoicing
eDelivery
Website authentication
eTime-stamp
Signing contract online
Online banking
eSignature
eSeal
eHealth
Tax online

PQC Conference, Meervaart Amsterdam

eIDAS realm & Post-Quantum Cryptography

Speaker: Lizzy Polman

Dutch Authority for Digital Infrastructure /

Ministry of Economical Affairs and Climate Policy

eIDAS realm & Post-Quantum Cryptography

What about eIDAS & Trust Services?

- Dutch Authority for Digital Infrastructure:
  Background and Introduction
- Legislative framework:
  eIDAS Regulation and Trust Services
  Near future: eIDAS2 & NIS2 Directive

What's going on?

- Current cryptography and the quantum threat
- Impact on eIDAS Regulation and Trust Services
  ETSI standardization, ENISA guidelines
- NIST & ETSI TC CYBER WG QSC

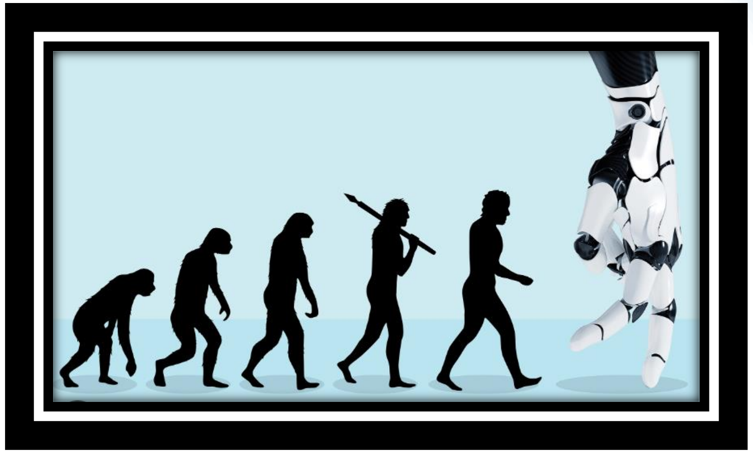
What's the course of action?

- What do we aim for?
- Initiatives & activities of the Authority

What about eIDAS & Trust Services?

Dutch Authority for Digital Infrastructure:

Background and Introduction

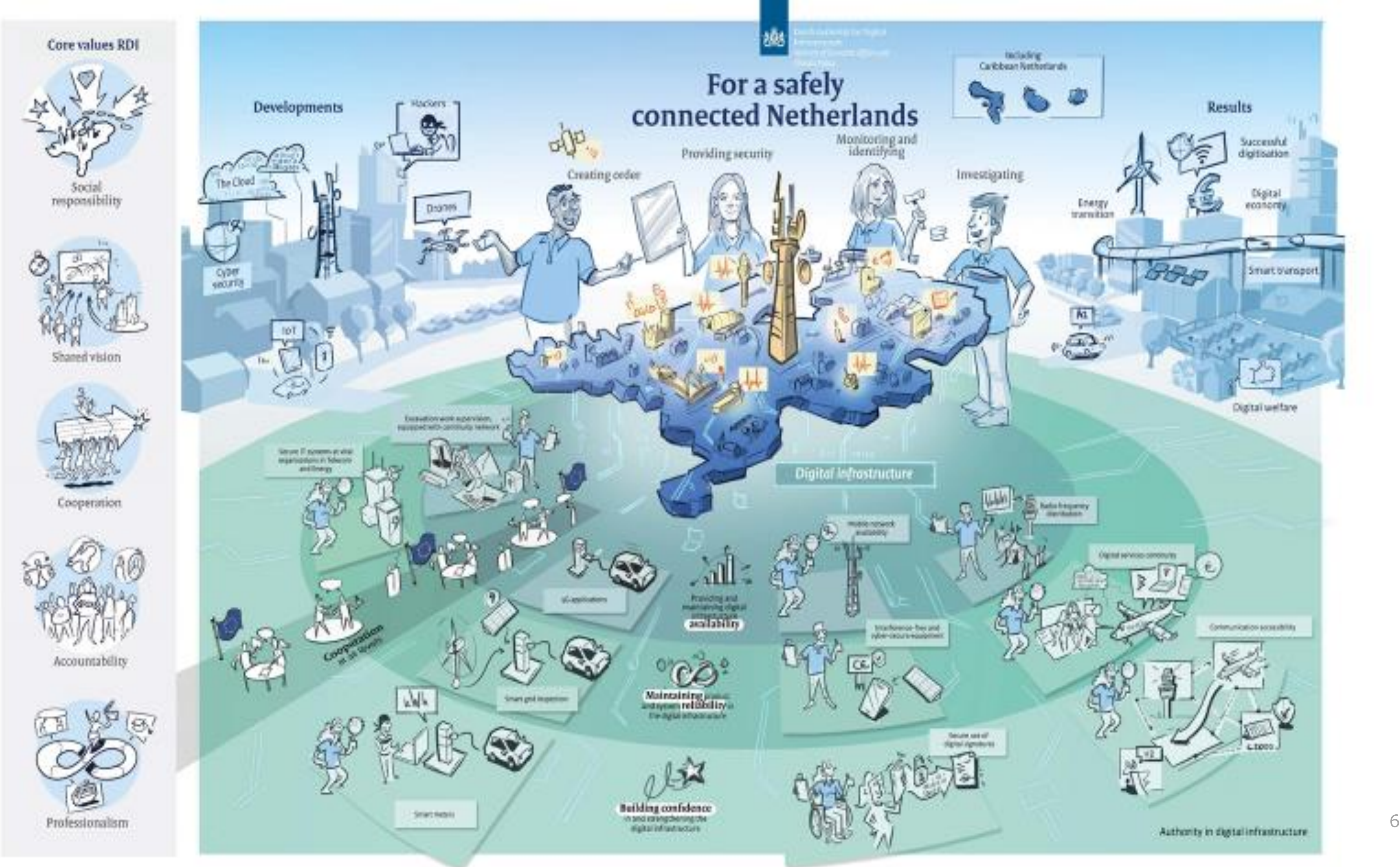


History goes back to 1929:
Radiocontroledienst van het Staatsbedrijf der PTT

Before January 2023: The Radiocommunications Agency (Agentschap Telecom)

Mission: For a safely connected Netherlands.
"*We strive to and hold an available and convidential IT- and communication network across the Netherlands.*"

Area's of activities: IoT, 5- and 6G, radiofrequency, WIBON,
NIS, CSA, AI, metrology, eIDAS, eID, Quantum, etc.


Core values RDI
Social responsibility
Shared vision
Cooperation
Accountability
Professionalism
For a safely connected Netherlands
Including Caribbean Netherlands
Developments
Hackers
The Cloud
Drones
Cyber security
IoT
Creating order
Providing security
Monitoring and identifying
Investigating
Results
Successful digitisation
Energy transition
Digital economy
Smart transport
Digital welfare
Excavation work supervision, equipped with continuity network
Secure IT systems at vital organisations in Telecom and Energy
5G applications
Smart grid inspection
Smart meters
Cooperation
Providing and maintaining digital infrastructure availability
Maintaining product and system reliability in the digital infrastructure
Building confidence in and strengthening the digital infrastructure
Digital infrastructure
Mobile network availability
Radio frequency distribution
Digital services continuity
Interference-free and cyber-secure equipment
Communication accessibility
Secure use of digital signatures
Authority in digital infrastructure

Legislative framework: eIDAS Regulation….

- The eIDAS Regulation: ‘*Electronic Identification, Authentication and Trust Services*’.
- eIDAS oversees electronic identification and trust services for electronic transactions in the European Union's internal market.
- Chapter II: Electronic Identification
- *Chapter III: Trust Services*
- Established in: EU Regulation 910/2014 of 23 July 2014
- Applies from 1 July 2016

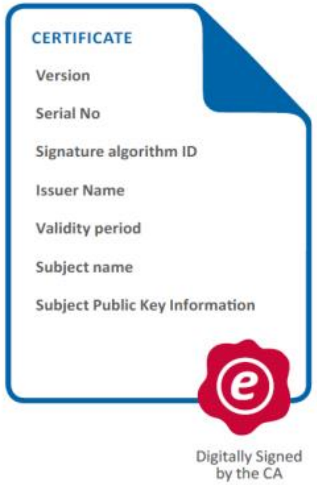
- eIDAS focus: Interoperability & Transparency
- eIDAS Supervisory Body in the Netherlands: Dutch Authority for Digital Infrastructure
- International fora: FESA / ECATS

… and Trust Services
eIDAS Regulation Chapter III

- (qualified certificate) Electronic signatures - section 4
- (qualified certificate) Electronic seals - section 5
- (qualified certificate) Electronic time stamps - section 6
- (qualified certificate) Electronic registered delivery services - section 7
- (qualified certificate) Website authentication - section 8

  - Ex Ante (qualified) vs Ex Post (non-qualified) supervision by the Authority
  - EC Trust Service List

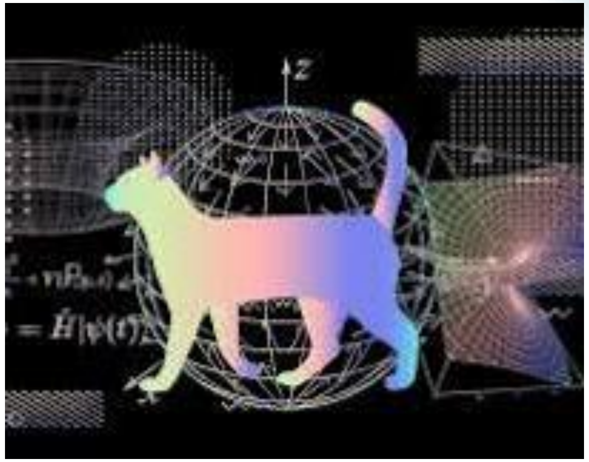
The EU trust mark for qualified trust services.



Near future: eIDAS2 & NIS2 Directive New dynamics?

What’s going on?

"Quantum computing only brings promises and will not be useful for the next 30-40 years" (A. Shamir, RSA conference April 2023)



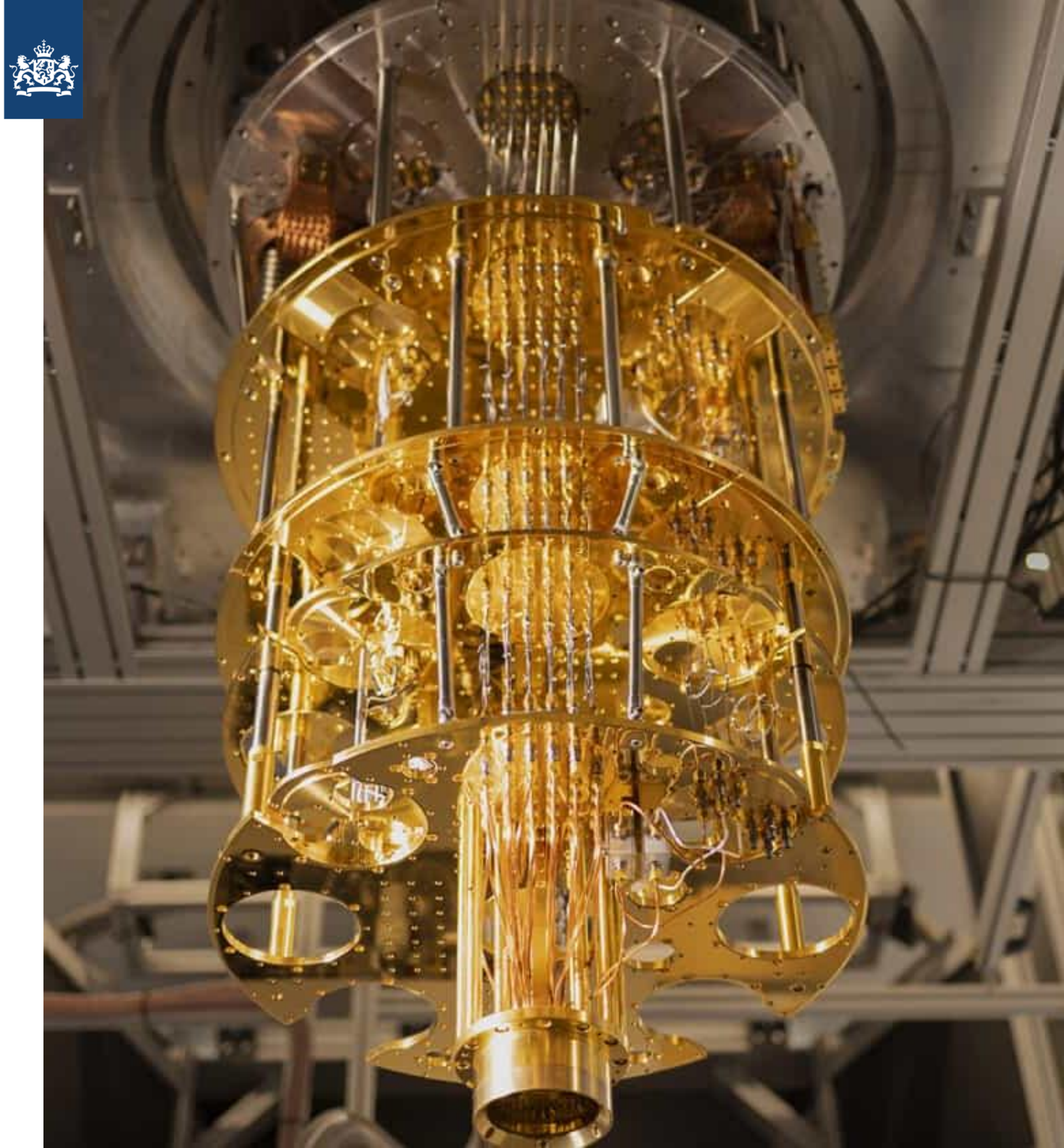
"Without preparation, sensitive data currently protected by encryption schemes will become accessible. The communication infrastructure will be disrupted, and our transactions and information will be vulnerable to criminals. This will affect countless organisations and millions of people." (The Hapkido project, Logius/TNO website)

"We don't have to wait for the perfect quantum computer to see the first applications" (Alain Aspect, Q2B conference May 2023)

Requirements for a physical implementation of a universal quantum computer:

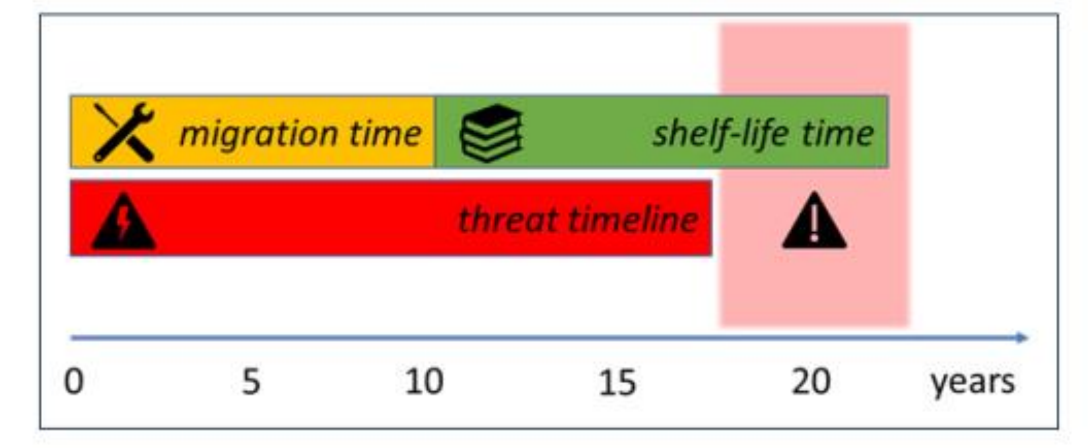
- stable (fault-tolerant) qubit power
- implementation of/ compatible with quantum algorithms: Shor / Grover
- long coherence times
- high gate fidelities
- large connectivity
- continued lab & production costs
- isolation near absolute zero (-273ºC))
- hardware/ materials (chips)/ experts….etc

Estimation: 2030+



Threat timeline

‘Harvest attack’ or ‘Store now decrypt later’



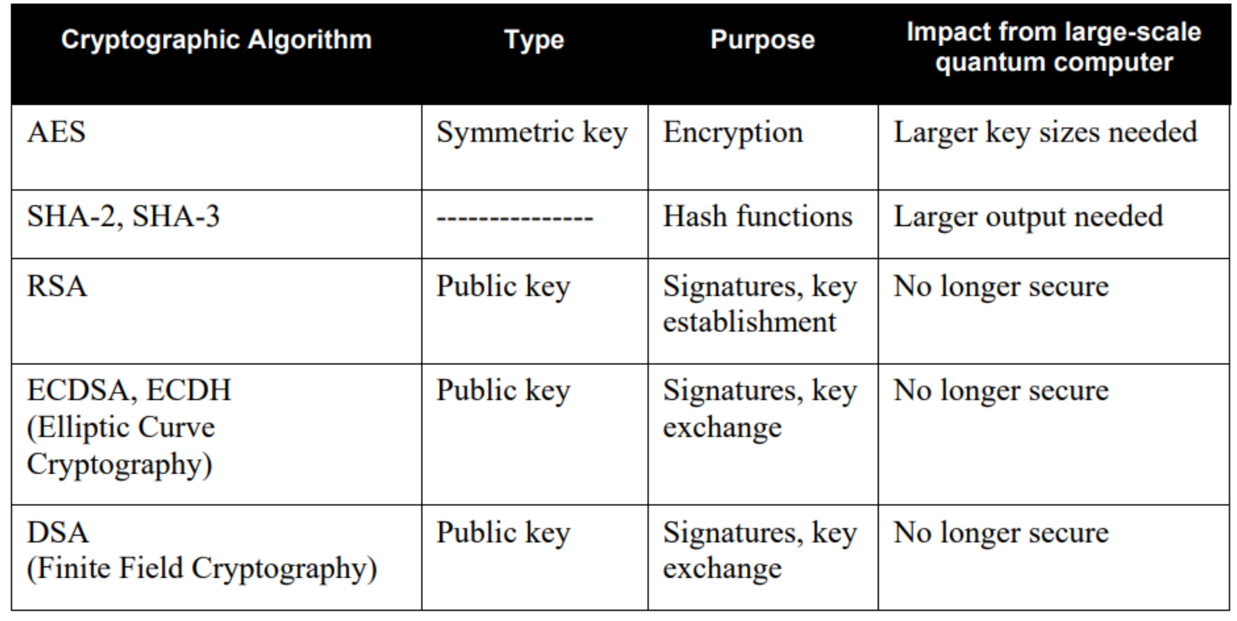
Mosca’s inequality

3 Parameters:

- the shelf-life time: n years the data must be protected by the cyber-system
- the migration time: n years to migrate the system to a quantum-safe solution, and
- the threat timeline: n years before the relevant threat actors will be able to break the quantum-vulnerable systems.

Implications for current cryptography

“The threat of quantum computing to asymmetric cryptography […] has been recognized as an existential threat to the many business sectors that rely on asymmetric cryptography for their day-to-day existence.” (ETSI, ETSI website)



Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	---------------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Source Figure:NISTIR 8105

- ➢ Public key infrastructure/ asymmetric: RSA-2048 cryptosystem -> 4,000,000 qubits needed
- ➢ Estimation: y2035

- ➢ Private key infrastructure / symmetric: AES-128 -> AES-256

- ➢ Hash functions: increase output lengths of hash functions to at least 336 bits

Impact on eIDAS Regulation and Trust Services

eIDAS Regulation ‘current situation’

Article 19 *Security requirements applicable to trust service providers*

1. Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.

eIDAS Regulation ‘revision’

(36d)

~~Qualified~~ Trust service providers should reflect best current practices and should use proven cryptographic algorithms ~~use, when issuing a qualified certificate, state-of-theart cypher suites~~ and trusted implementations of these algorithms in order to ensure the security of their trust services and their reliability ~~sufficient time period resistance thereof.]~~

Article 24 1.e

use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them, including using suitable cryptographic algorithms, key lengths and hash functions in the systems, products and in the processes supported by them;

….and ETSI Standardization
ETSI 319 401/411

e.g. 7.5 Cryptographic controls REQ-7.5-01: Appropriate security controls shall be in place for the management of any cryptographic keys and any cryptographic devices throughout their lifecycle.

and recommendation ITU-T X.509

To allow smooth migration of a PKI or a PMI from a legacy use of one set of cryptographic algorithms to an assumingly stronger set of cryptographic algorithms, this Specification includes provisions for an alternative set of cryptographic algorithms. This allows some entities to move to a safer set of algorithms while at the same time legacy entities may keep using the old set of cryptographic algorithms during the migration period.

ENISA guidelines

- Recommendations for the implementation of trust services
- Guidelines on Initiation of Qualified Trust Services
- Guidelines on Supervision of Qualified Trust Services
- Guidelines on Termination of Qualified Trust Services
- Recommendations for QTSPs based on Standards
- Conformity Assessment of Trust Service Providers
- Security Framework for Trust Service Providers

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

NIST & ETSI TC CYBER WG QSC

NIST Selected Candidates Algorithms (per status update October 2023)

Public-key Encryption and Key-establishment Algorithms
CRYSTALS-KYBER

Digital Signature Algorithms
CRYSTALS-DILITHIUM
FALCON
SPHINCS+

-> NIST call for additional post-quantum signatures

4 additional Candidate Key-Establishment Mechanisms (KEMs)
BIKE
Classic McEliece
HQC
SIKE

ETSI TC CYBER WG QSC

- 2013 1st ETSI-IQC Quantum Safe Cryptography Workshop
- Meetings are coordinated with CYBER, meet 5 times a year in Sophia-Antipolis, France
- 30-40 registered participants from universities/ governments/ businesses

Finished TR/TS:

- QSC Migration; ITS and C-ITS migration study, ETSI TR 103 949 (2023-05)
- State Management for Stateful Authentication Mechanisms, ETSI TR 103 692 (2021-11)
- Quantum-safe Hybrid Key Exchanges, ETSI TS 103 744 V1.1.1 (2020-12)
- Migration strategies for Quantum Safe schemes, ETSI TR 103 619 V1.1.1 (2020-07)
- Quantum-Safe Identity-Based Encryption, ETSI TR 103 618 V1.1.1 (2019-12)
- Quantum-Safe Virtual Private Networks, ETSI TR 103 617 V1.1.1 (2018-09)

Current work items

- Quantum-Safe Hybrid Key Exchanges, RTS/CYBER-QSC-0019 (TS 103 744)
- Impact of Quantum Computing on Cryptographic Security Proofs, DTR/CYBER/QSC-0020
- Deployment Considerations for Hybrid Schemes, DTR/CYBER-QSC-0021
- Impact of Quantum Computing on Symmetric Cryptography, DTR/CYBER-QSC/0022

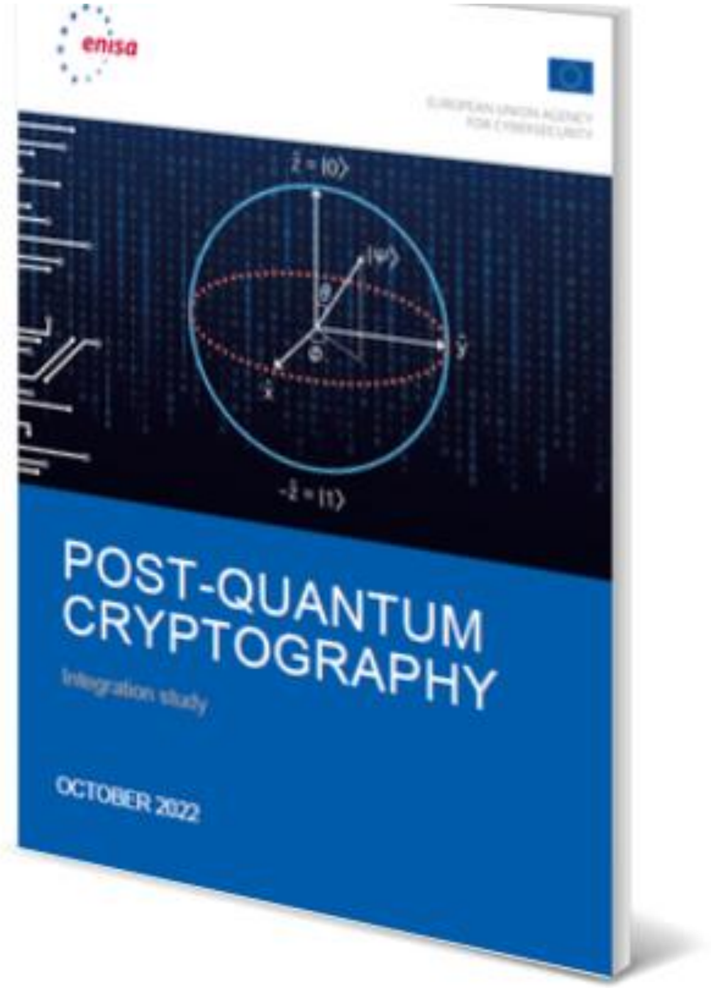
New work items

- Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies, DTR/CYBER-QSC-0023
- A Repeatable Framework for Quantum-Safe Migrations, DTR/CYBER-QSC-0024
- QSC Protocol Inventory, DTR/CYBER-QSC-0025

What’s the course of action?

ENISA – PQC initiatives

- Post-Quantum Cryptography: Current state and quantum mitigation — ENISA (europa.eu)



enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

POST-QUANTUM CRYPTOGRAPHY

Integration study

OCTOBER 2022

Initiatives & activities of the Dutch Authority for Digital Infrastructure

Quantum Program highlights:

- Assessing quantum impact on our workfield(s), e.g. eIDAS
- Quantumveilige Crypto Rijk / Quantum-safe Crypto Government of the Netherlands
- EQTA - Quantum Technology Impact Assessment (QuantumDelta NL) - Research paper on Quantum sensors
- Sharing knowledge with stakeholders
- Quantum Radar and Trend Rader

Useful websites

- eIDAS Regulation | Shaping Europe's digital future (europa.eu)
- Carriages preview | Legislative Train Schedule (europa.eu)
- Dutch Authority for Digital Infrastructure | Rijksinspectie Digitale Infrastructuur (RDI)
- eIDAS Dashboard (europa.eu)
- Onderzoek toepassing kwantumsensoren in radiotechnologie | Rapport | Rijksinspectie Digitale Infrastructuur (RDI)
- Quantum Technology Impact Assessment | Futurium (europa.eu)

Questions?

Lizzy Polman MA MSc CISM
Lizzy.Polman@rdi.nl

Post-Quantum Cryptography Conference

PKI Consortium

ENTRUST

HID

PQ SHIELD

Fortanix

KEYFACTOR

NOREG

QRL

THALES

d-trust.

01 COMMUNIQUE

amsterdam convention bureau

ascertia

亞洲誠信 TRUSTAsia