信頼される安心を、社会へ。
SECOM

Quantum WG liaison (& ECDSA key usage at IETF) report

Tadahiko Ito

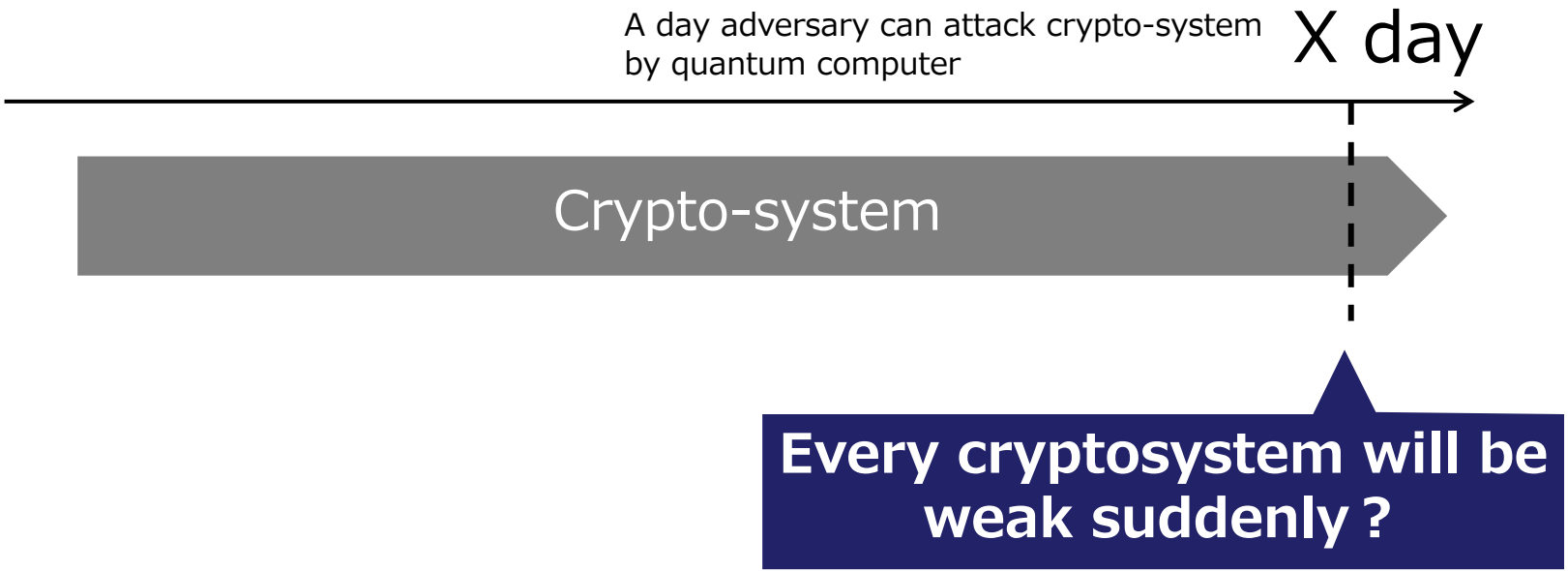
Feb. 2020

CRYPTREC (2020, 17th Feb)

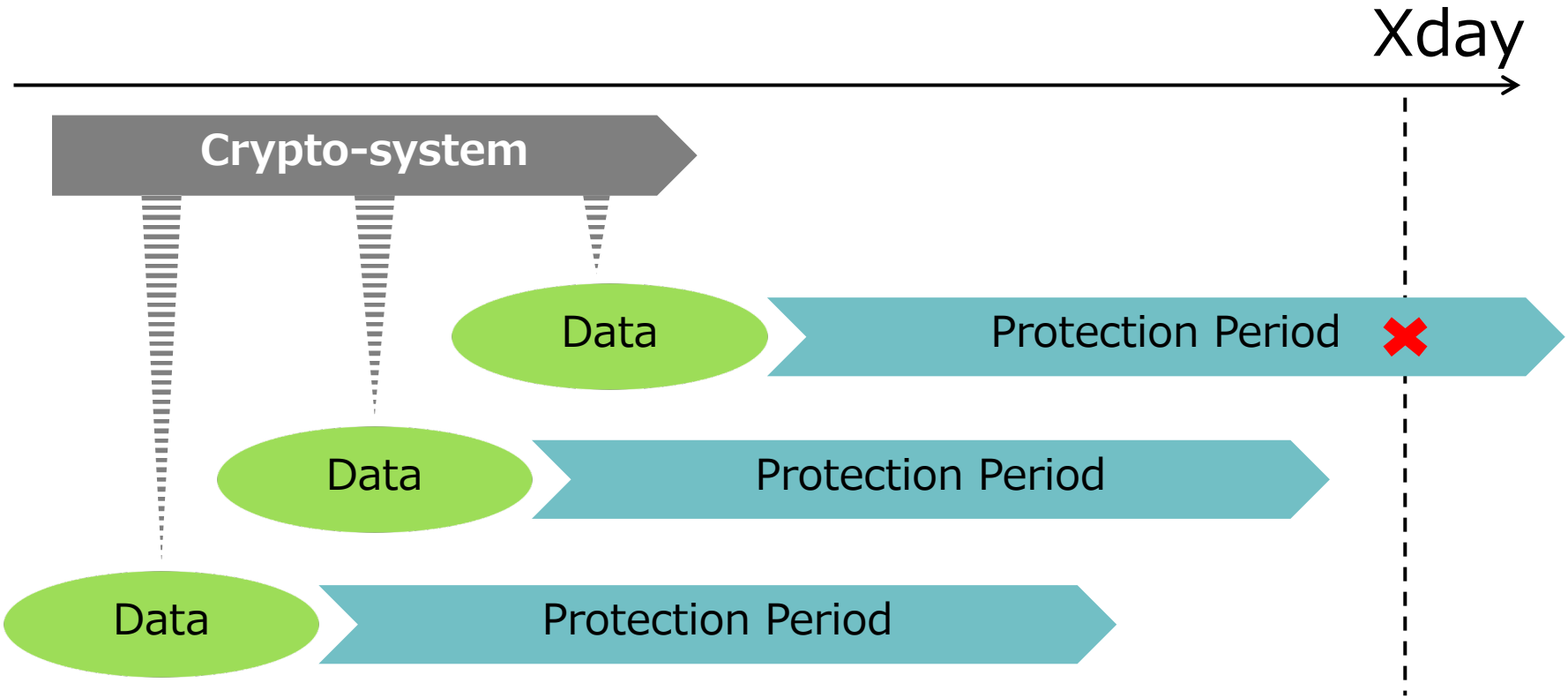
信頼される安心を、社会へ。
SECOM

It will not likely happen **near future** that
current cryptographies were decrypted by quantum computer

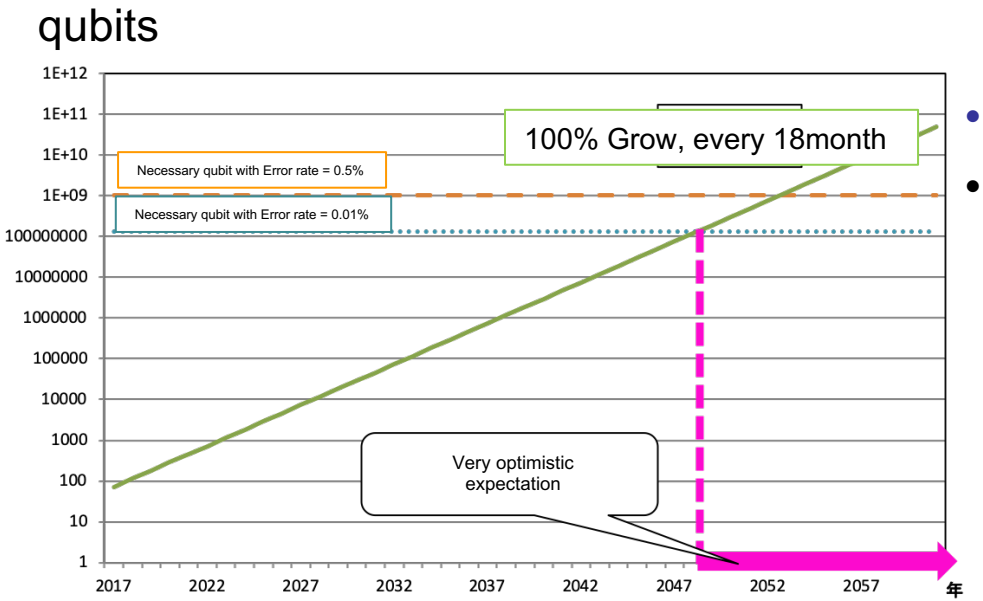
What is the Risk of Quantum computer for Crypto-system (August 2019, Liaison Work with Bank of Japan)



What is the Risk?



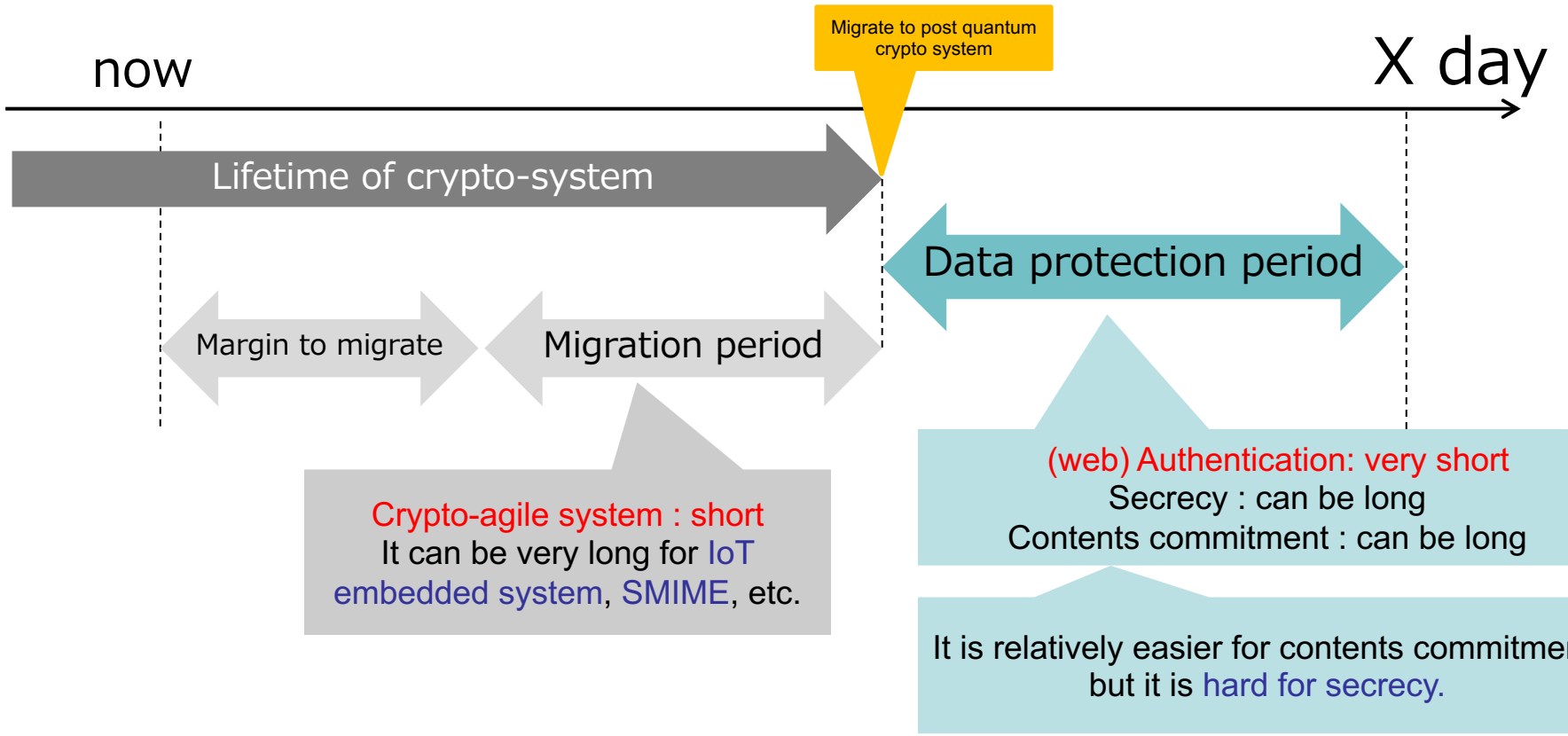
When is X day?? (with very optimisitic expectation)



- Logical qubit = ideal qubit
- Real qubits（physical qubits）is not ideal
  - Need mechanism to reduce error
  - Need mechanism to make fault tolerant
  - Cohrence time

https://www.imes.boj.or.jp/research/papers/japanese/19-J-15.pdf

Who will have more problem



Conclusion (for banks)

- Post Quantum Cryptography
  - Early stage
  - Some question on cost efficiency
  - May need to watch trends for particular technology field.
- Data classification
  - In term of lifetime of data
  - Lifecycle management of data,
- More Crypto-aglity for IoT, long-term contents commitment, etc..
- Efficient use of timestamp for long term contents comittment
  - E.g) Evidence Record Syntax

May have side effect to increase security.

Mozilla Policy say.

5.1 Algorithms

Root certificates in our root program, and any certificate which chains up to them, MUST use only algorithms and key sizes from the following set:

•RSA keys whose modulus size in bits is divisible by 8, and is at least 2048.

•ECDSA keys using one of the following curves:

- P-256
- P-384

We do not have “id for ECDSA key”
Technically, ECDSA key can be use for any ECC

SubjectPublicKeyInfo	.algorithm	Meta data
Unrestricted (ECDSA, etc..)	id-ecPublicKey	Secp-256r1, etc…
ECDH [RFC5480]	(MAY) id-ecDH	id-ecPublicKey, etc..
ECMQV [RFC5480]	(MAY) id-ecMQV	id-ecPublicKey, etc..
EDDSA [RFC8410]	(only define) id-Ed25519	Absent
Other (like ECIES??)	Let them use that	(do not care)

Key usage problem

- We know ECDSA is signature algorithm
  - So we can not use that for key encipherment or data encipherment.
- However, if certs with encipherment bit exist, does that violate any standard / requirements??
  - Linting tools did not alert such certs
  - We had published such certs
  - We had problem of describe “reason” to revoke such certs.

- RFC5480 say…

For ECDSA ,(static)ECDH, and (possibly, other algorithm).

If the keyUsage extension is present in an End Entity (EE) certificate that indicates id-ecPublicKey in SubjectPublicKeyInfo, then any combination of the following values MAY be present: digitalSignature; nonRepudiation; and keyAgreement.

ECDSA, etc..

For (static)ECDH, ECMQV

ECDSA, etc..

Does not have any description for key encipherment or data encipherment

(Current) proposal at IETF

If the keyUsage extension is present in a certificate that indicates id-ecPublicKey as algorithm of AlgorithmIdentifier [RFC2986] in SubjectPublicKeyInfo, then following values MUST NOT be present: keyEncipherment; and dataEncipherment.

https://tools.ietf.org/html/draft-ietf-lamps-5480-ku-clarifications

Unrestricted cert :
https://tools.ietf.org/html/rfc5480#section-2.1

Key usage bit
https://tools.ietf.org/html/rfc5480#section-3