SIP Cross-ministerial Strategic Innovation Promotion Program

Overview of Quantum Communication Technology in SIP CAO, Japan

22 April 2022

Sub Program Director
Masahide Sasaki
(NICT)

Target

Develop a cyber physical system for smart manufacturing,
by using photonics and quantum technologies.

Main themes

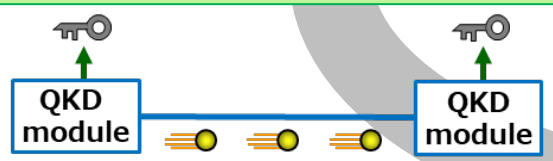
PD: N. Nishida (Toshiba)
SPDs: K. Yasui (Mitsubishi Electric)
M. Sasaki (NICT)

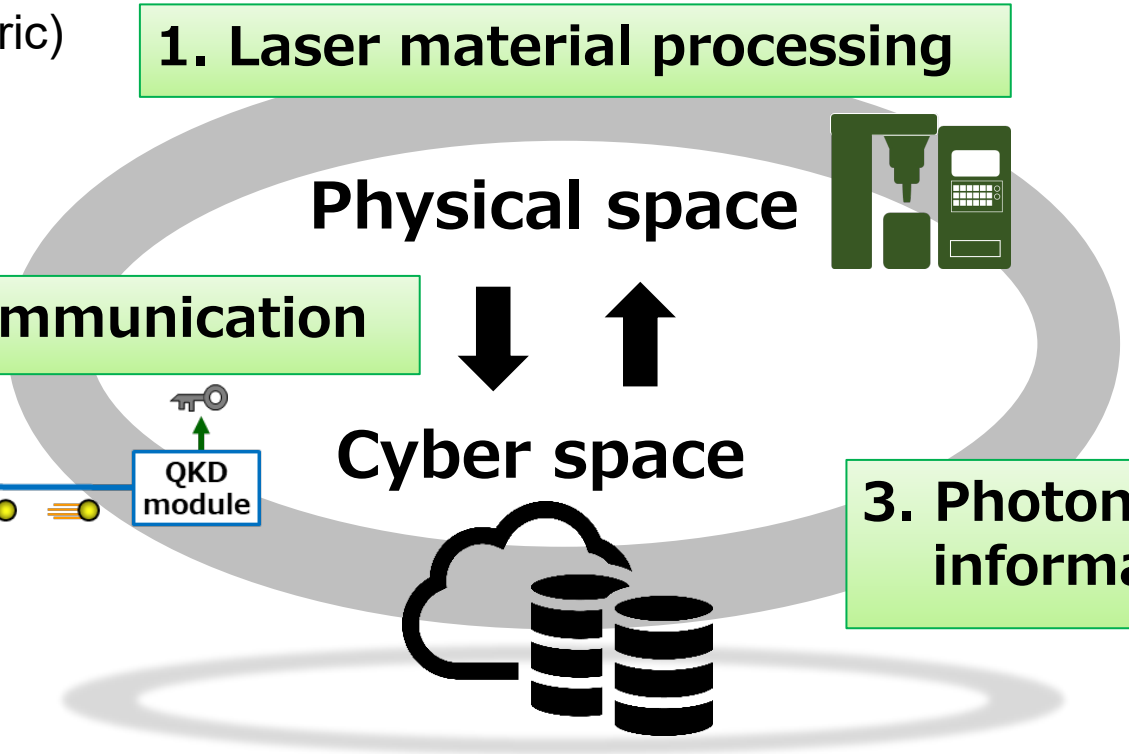
1. Laser material processing

U Tokyo
Hamamatsu Photonics
Kyoto U
Mitsubishi Electric
ROHM

2. Photonic quantum communication

NICT
NEC
Toshiba
Gakushuin U
Hokkaido U
U Tokyo
ZenmuTech





3. Photonic and electronic information processing

Waseda U
QunaSys
Fixters
Keio U

Quantum secure cloud

To provide secure cloud services in the quantum era

Enhanced computing services

- Quantum-classical hybrid solvers

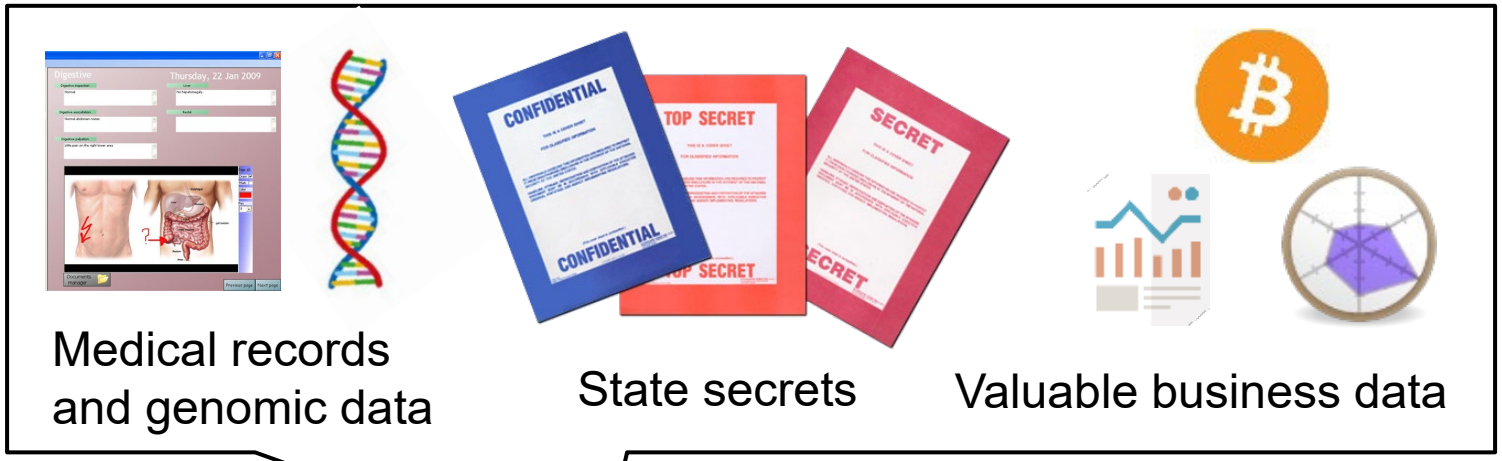
X

Long-term security protection

- Quantum cryptography
- Post-quantum cryptography
- Secret sharing

Long-term security protection

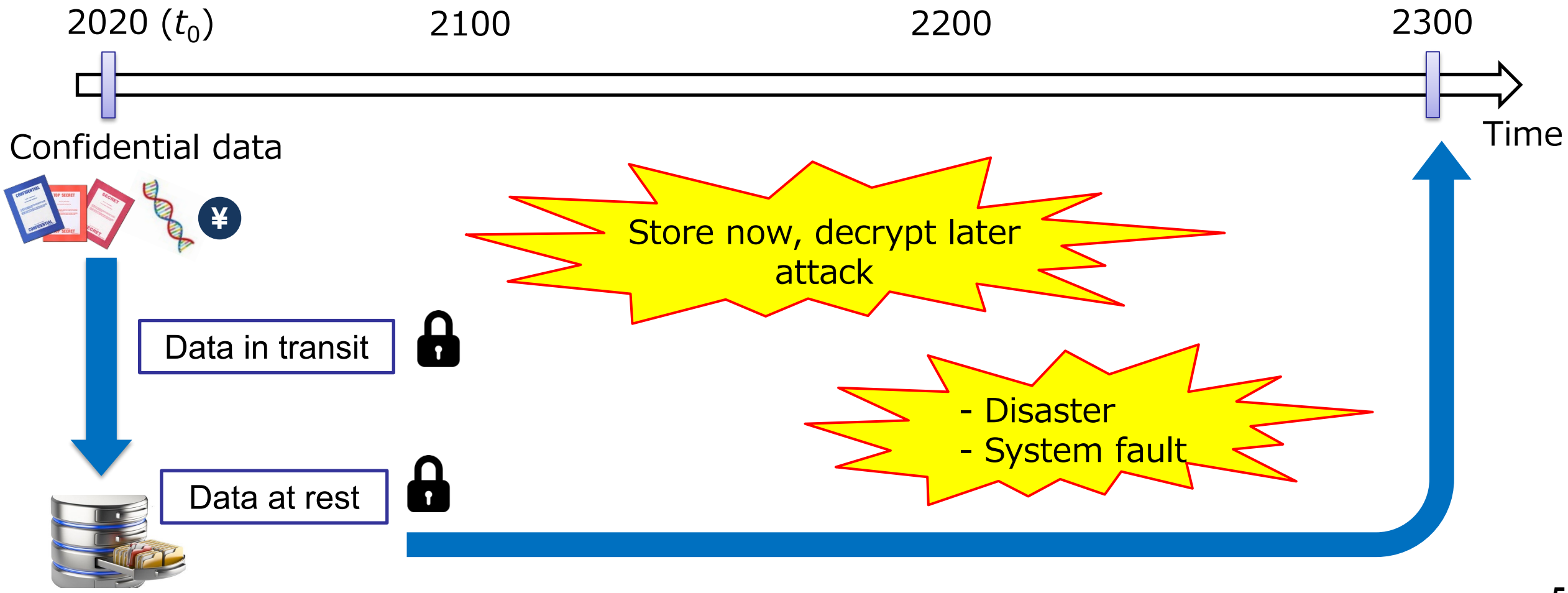
Today, various digital data on individuals, private and public organizations are produced in cloud services.



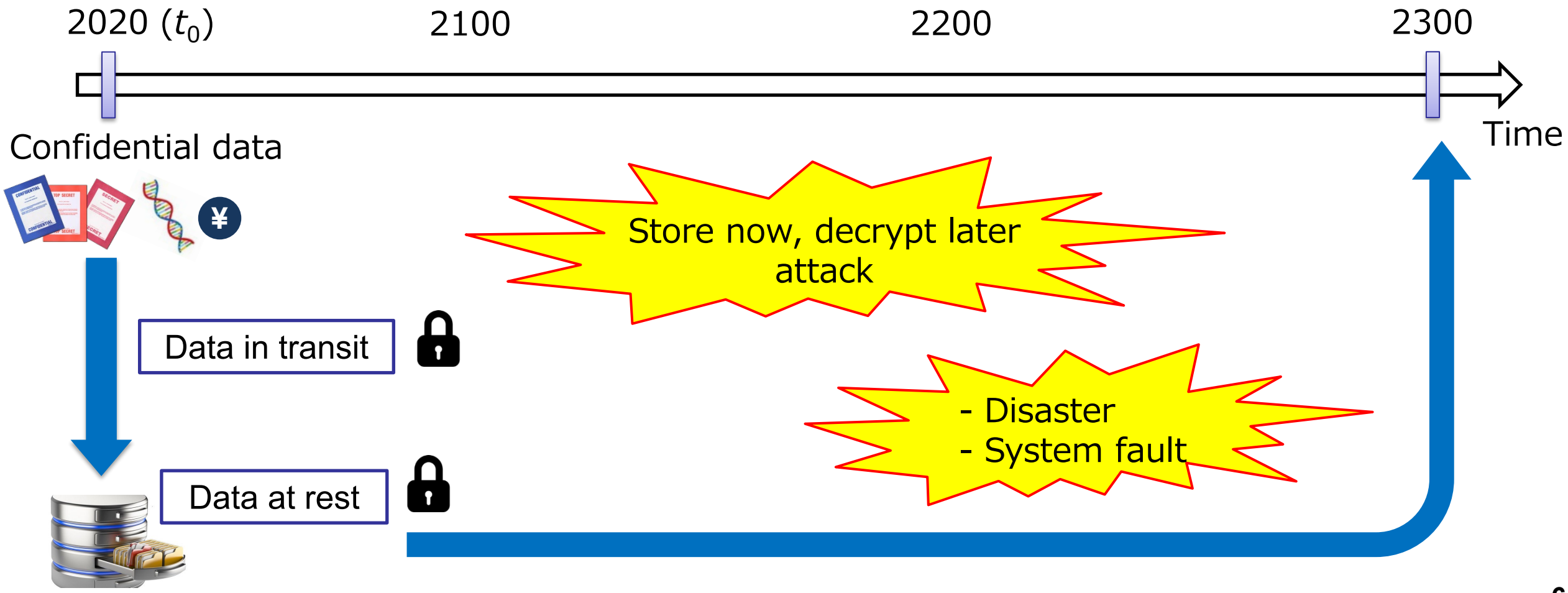
These data are preserved in data centers **forever**.

Long-term security protection

Critical data need to be transmitted, stored, and processed securely for a long time.



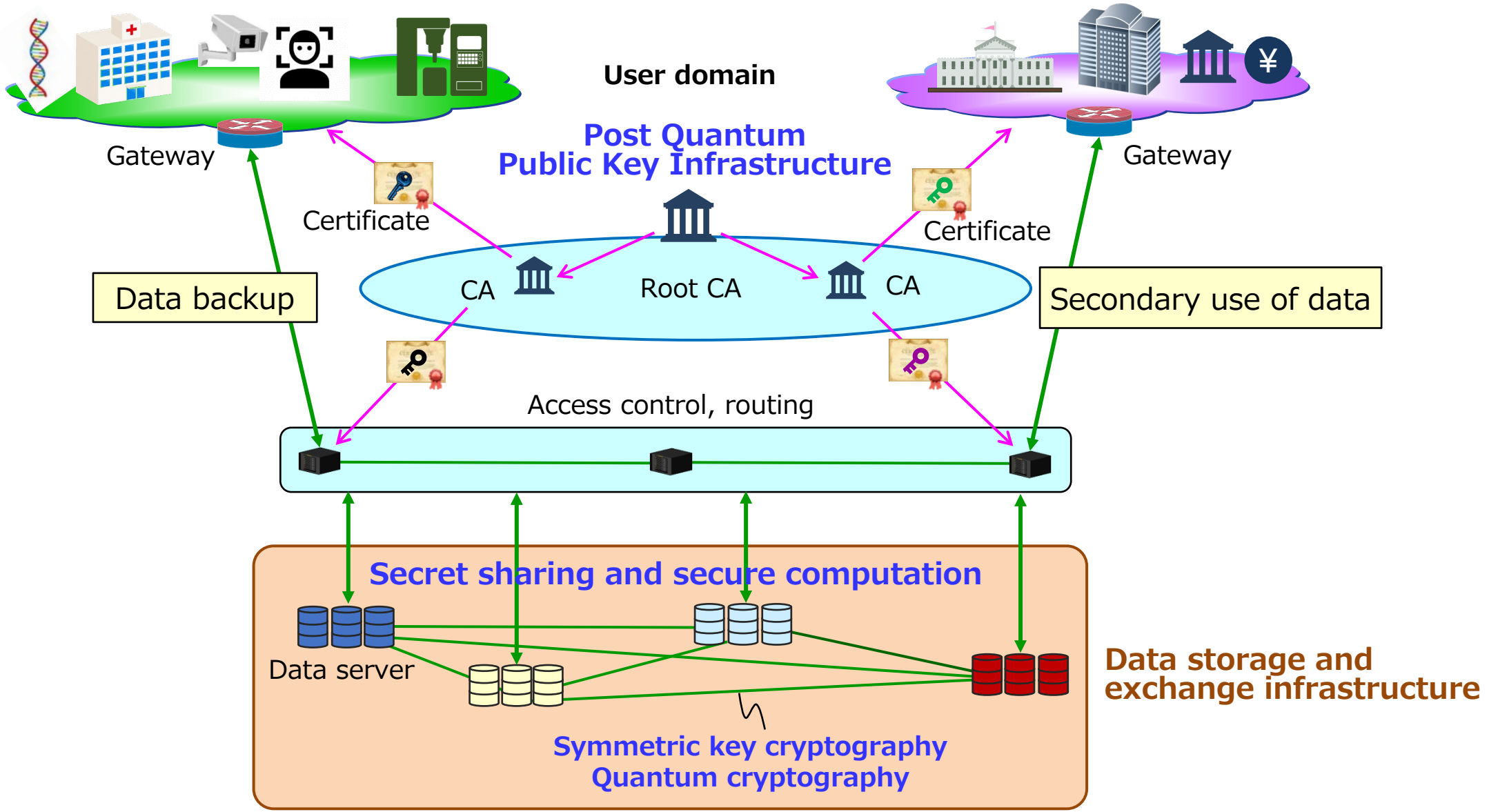
- No information leak of the data in transit and at rest.
- The data existed at time t_0 and has not been changed since.
- The data should not be lost.



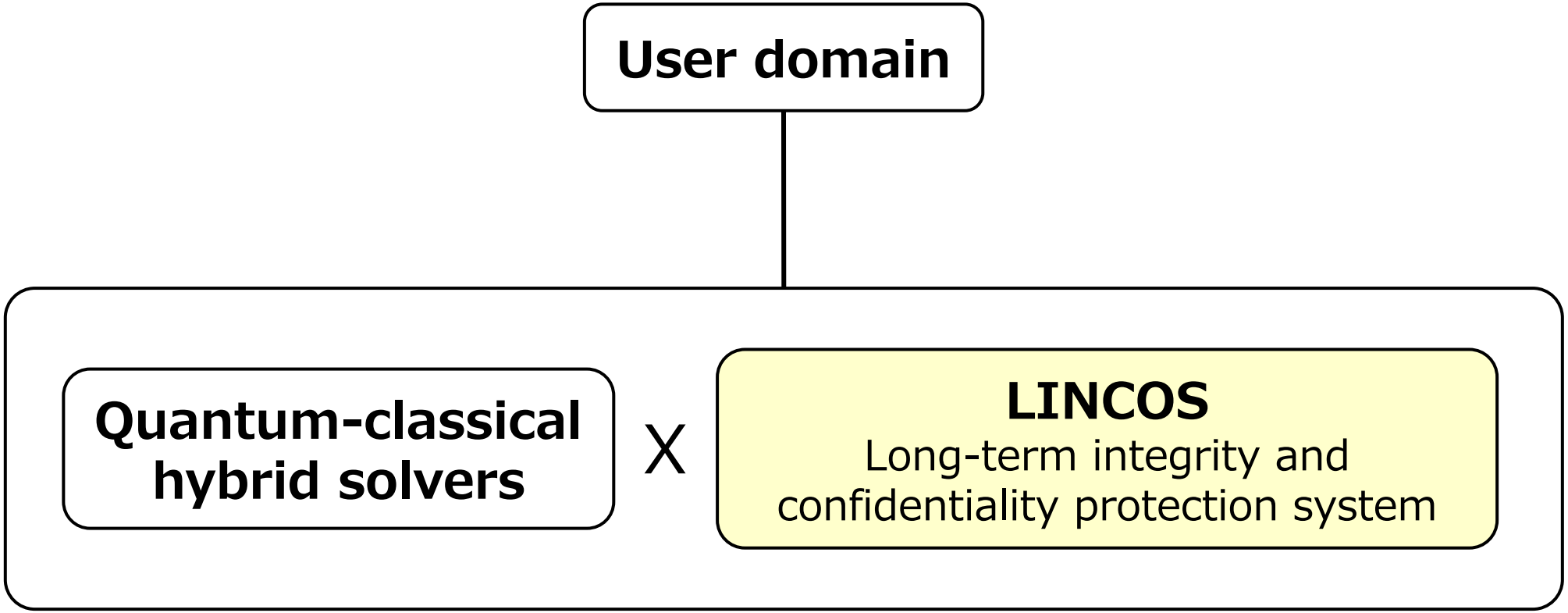
Four important technologies in the quantum era

Confidentiality	- **Symmetric key cryptography** (Computational security) - **Quantum cryptography** (Information theoretic security)
Integrity	Authentication and key exchange by **Post quantum public key cryptography**
Availability	Data backup by **secret sharing**

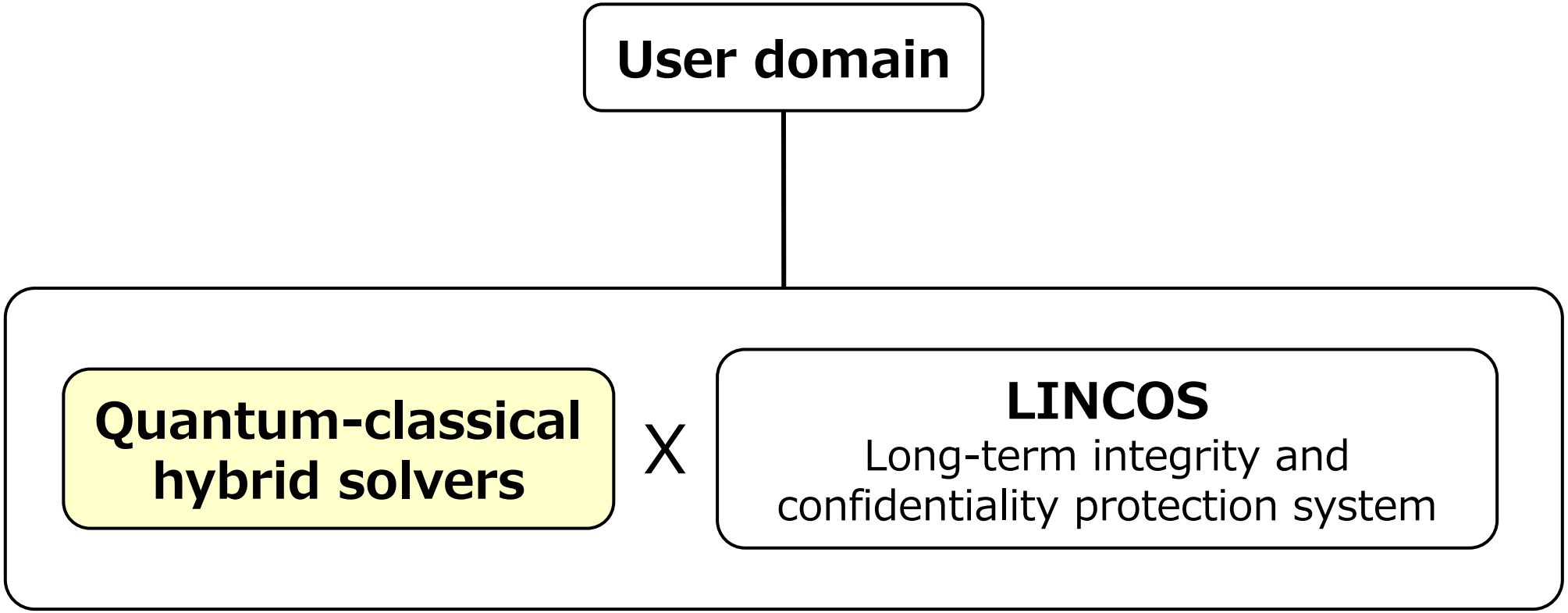
Long-term integrity and confidentiality protection system "LINCOS"



Quantum secure cloud



Quantum secure cloud



Enhanced computing services

Drug design | Material design | Finance | Factory | Energy | Mobility | ....

Quantum-classical hybrid solvers

Codesign platform of quantum and classical computers

to deliver best solver services for each use case by
- optimal allocation of computing resources
- optimization of input and output formats, algorithms, and APIs

CPUs and GPUs

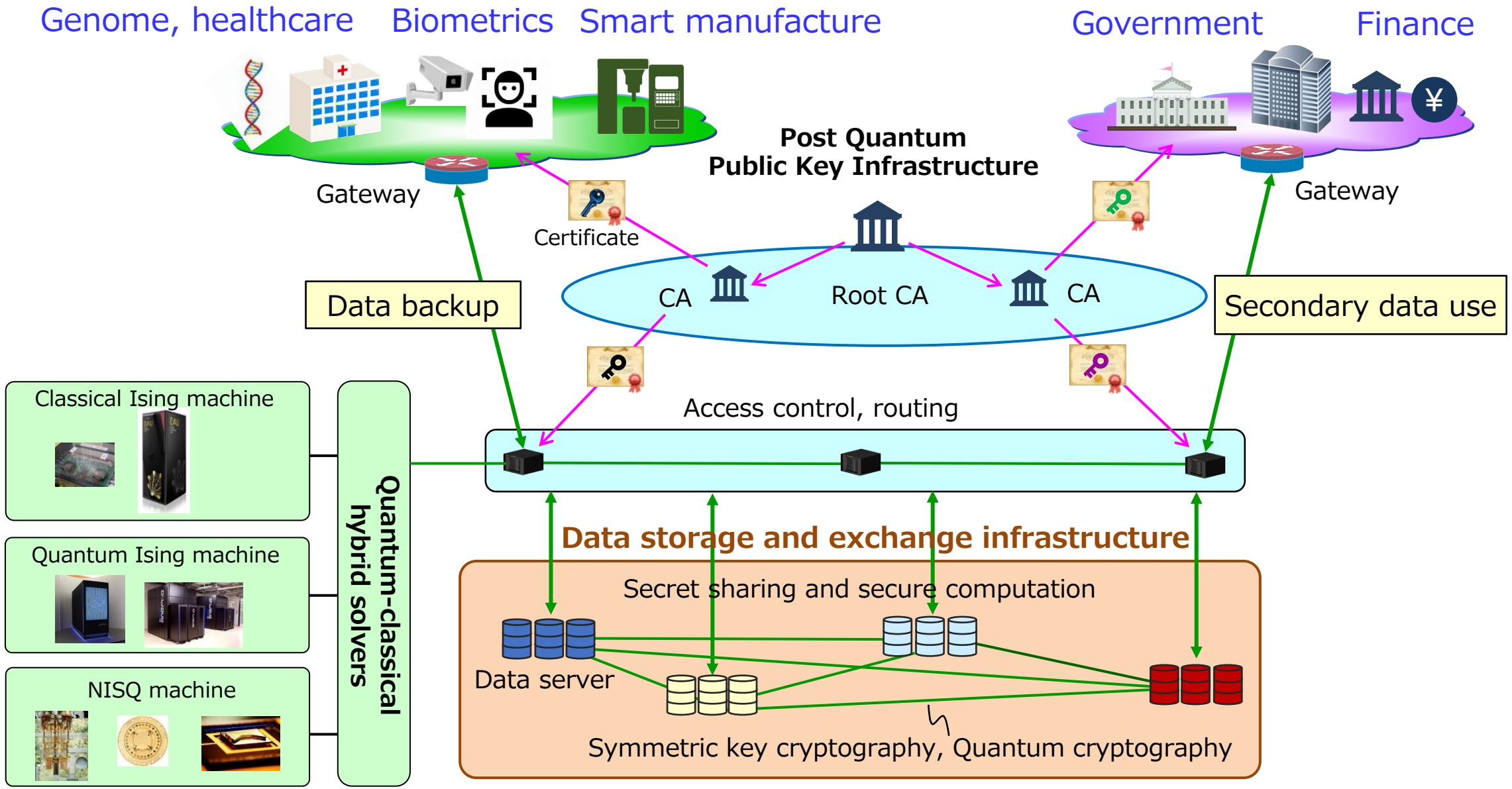
Classical Ising machines

Quantum Ising machines

NISQ machines

Quantum secure cloud

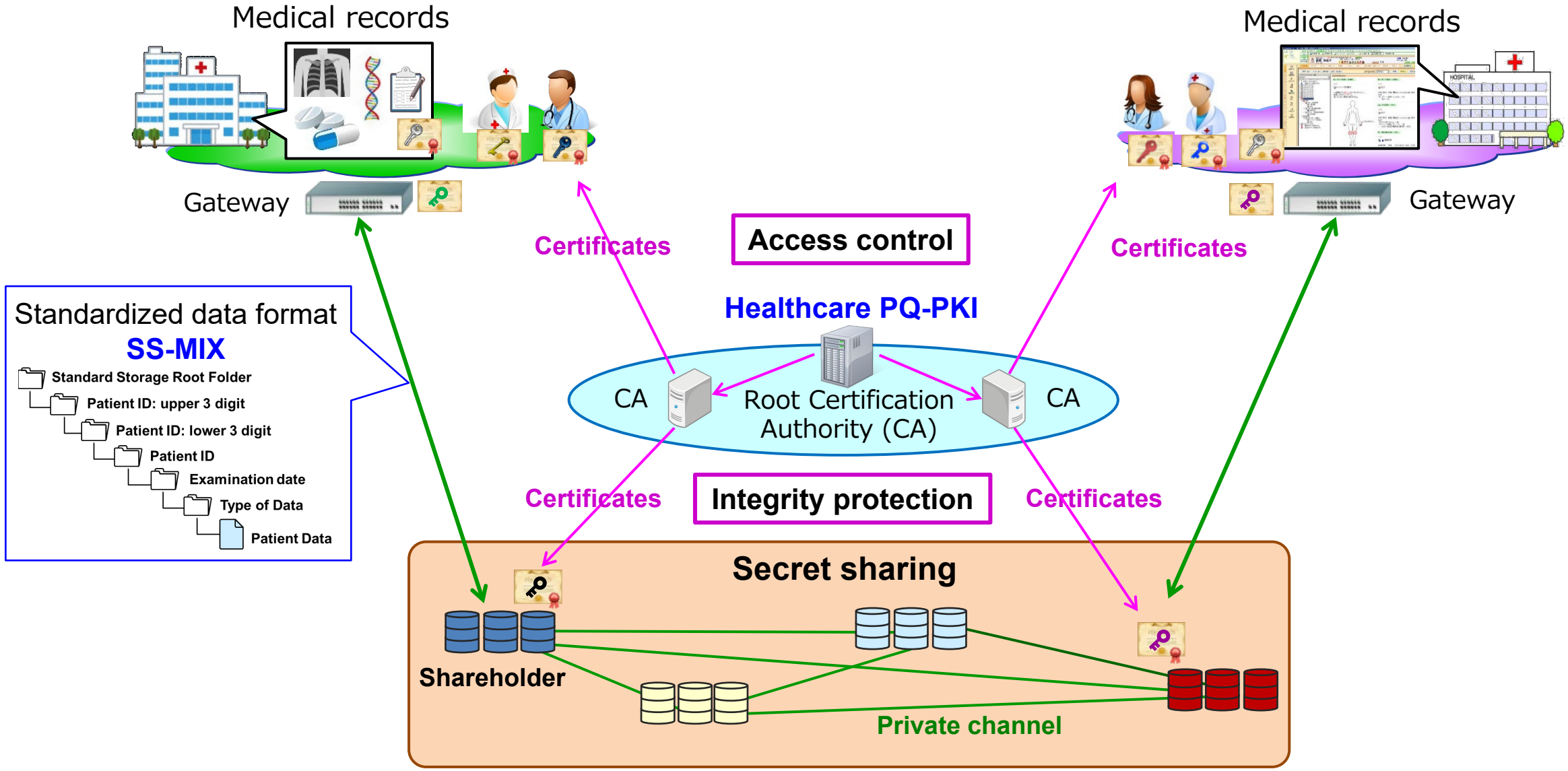
deployed for social implementations in SIP



Use cases of quantum secure cloud

Healthcare LINCOS

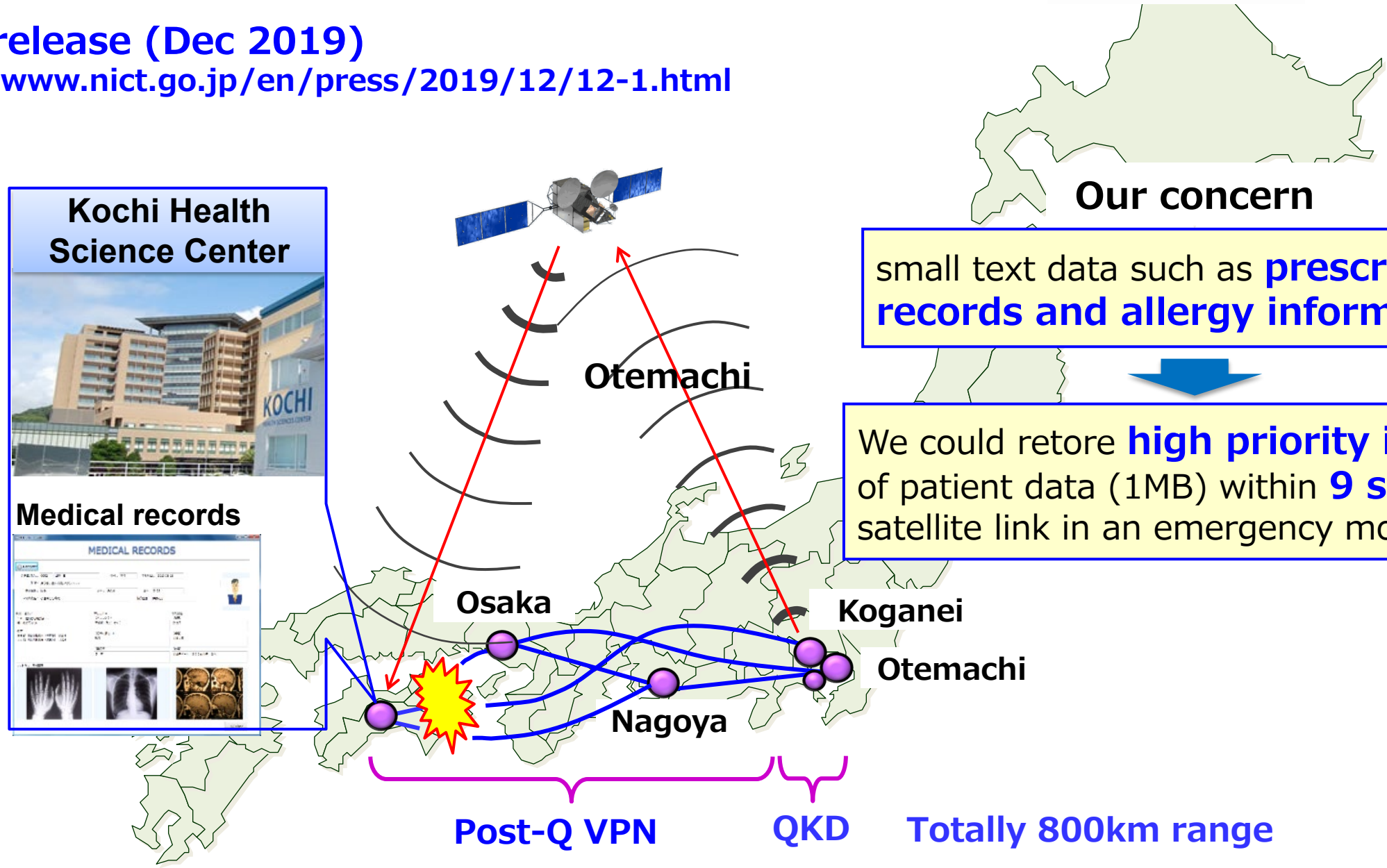
to store and exchange electrical medical records



Distributed storage of medical records

(90GB data of 10,000 patients)

Press release (Dec 2019)
https://www.nict.go.jp/en/press/2019/12/12-1.html



Our concern

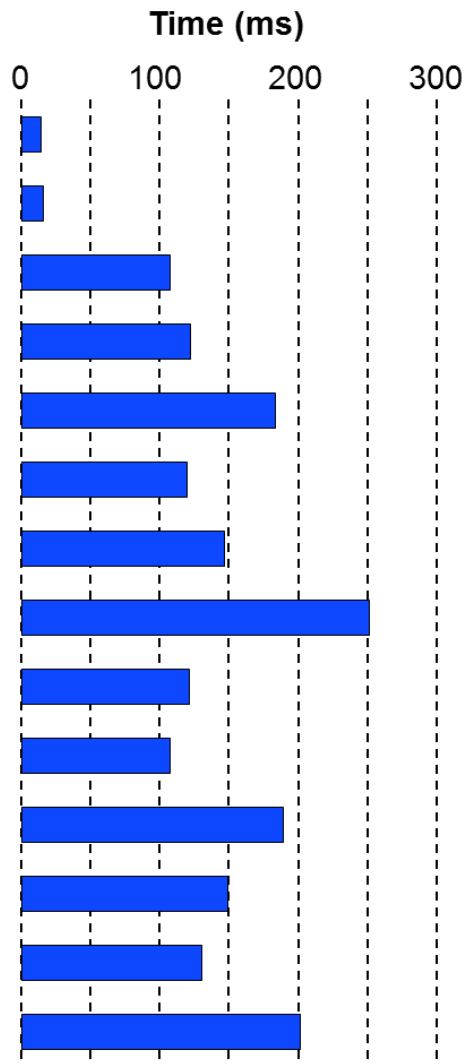
small text data such as **prescription records and allergy information**

We could retore **high priority items** of patient data (1MB) within **9 sec** via a satellite link in an emergency mode.

Access control by Healthcare PQ-PKI

- ✓ 7 PQC schemes
- ✓ 12 cipher suites in TLS

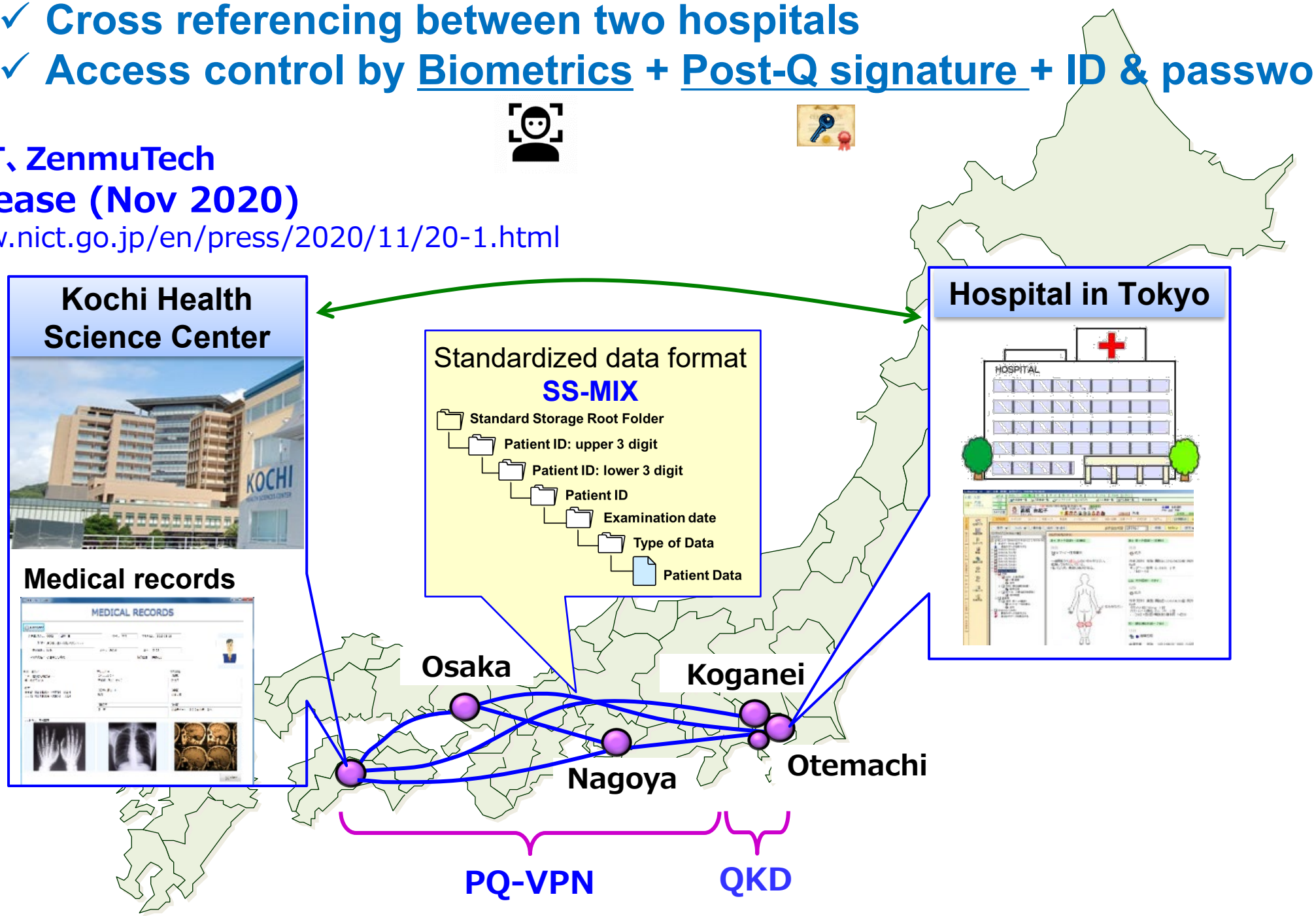
	Root certificate	Key exchange	Signature	Time (ms)
TLS	RSA	ECDHE	SHA384	14.4
		RSA	SHA384	15.8
Post Quantum TLS	LMS (Hash)	NewHope (Lattice)	Dilithum (Lattice)	107.2
			q-TESLA (Lattice)	122.2
			Rainbow (Multivariate)	183.9
		SIDH (Isogeny)	Dilithum (Lattice)	120.2
			q-TESLA (Lattice)	146.4
			Rainbow (Multivariate)	251.7
	XMSS (Hash)	NewHope (Lattice)	Dilithum (Lattice)	121.7
			q-TESLA (Lattice)	107.7
			Rainbow (Multivariate)	189.6
		SIDH (Isogeny)	Dilithum (Lattice)	149.2
			q-TESLA (Lattice)	130.0
			Rainbow (Multivariate)	201.9

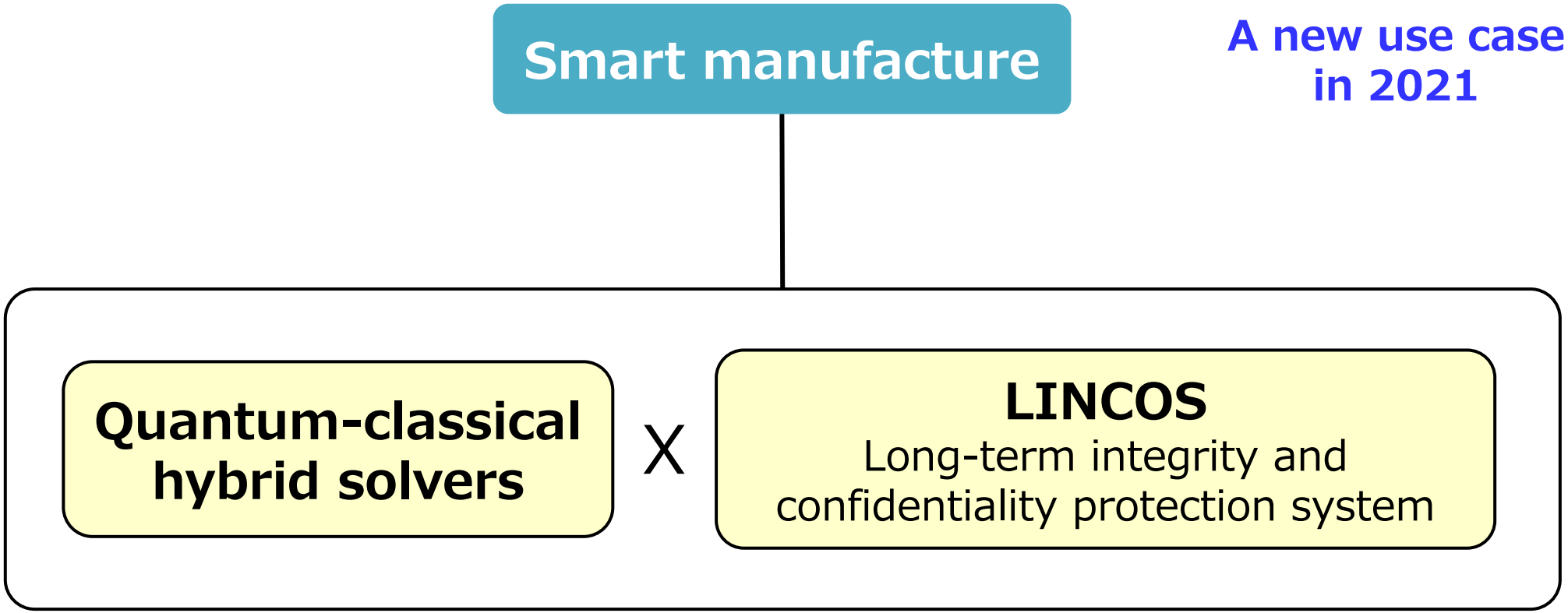


- ✓ 10 times longer than conventional TLS
- ✓ All suites worked well

✓ Cross referencing between two hospitals
✓ Access control by Biometrics + Post-Q signature + ID & password

NEC、NICT、ZenmuTech
Press release (Nov 2020)
https://www.nict.go.jp/en/press/2020/11/20-1.html




Smart manufacture
A new use case
in 2021
Quantum-classical
hybrid solvers
X
LINCOS
Long-term integrity and
confidentiality protection system

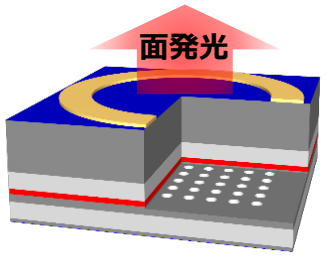
Smart design of photonic crystal laser

Since Nov. 2021

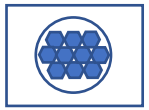
Dramatic speedup of finding optimal design parameters on photonic crystal laser by using the quantum-classical hybrid solvers (a month → a day).

Kyoto U

Optimal design of photonic crystal laser



Photos

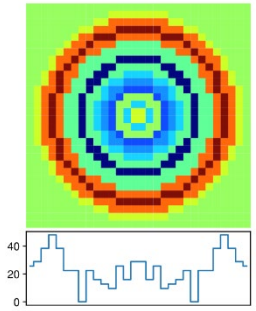


Device parameters

$[C_{ij}]$

Symmetric key cipher
(NEC's COMCIPHER)

Optimal solution



A new findings on optimal mode distributions

NICT

Routing & secret sharing

Quantum-classical hybrid solvers

Waseda U, Keio U, & Fixters

Quantum cryptography
(Toshiba, NEC)

Share

Share

Share

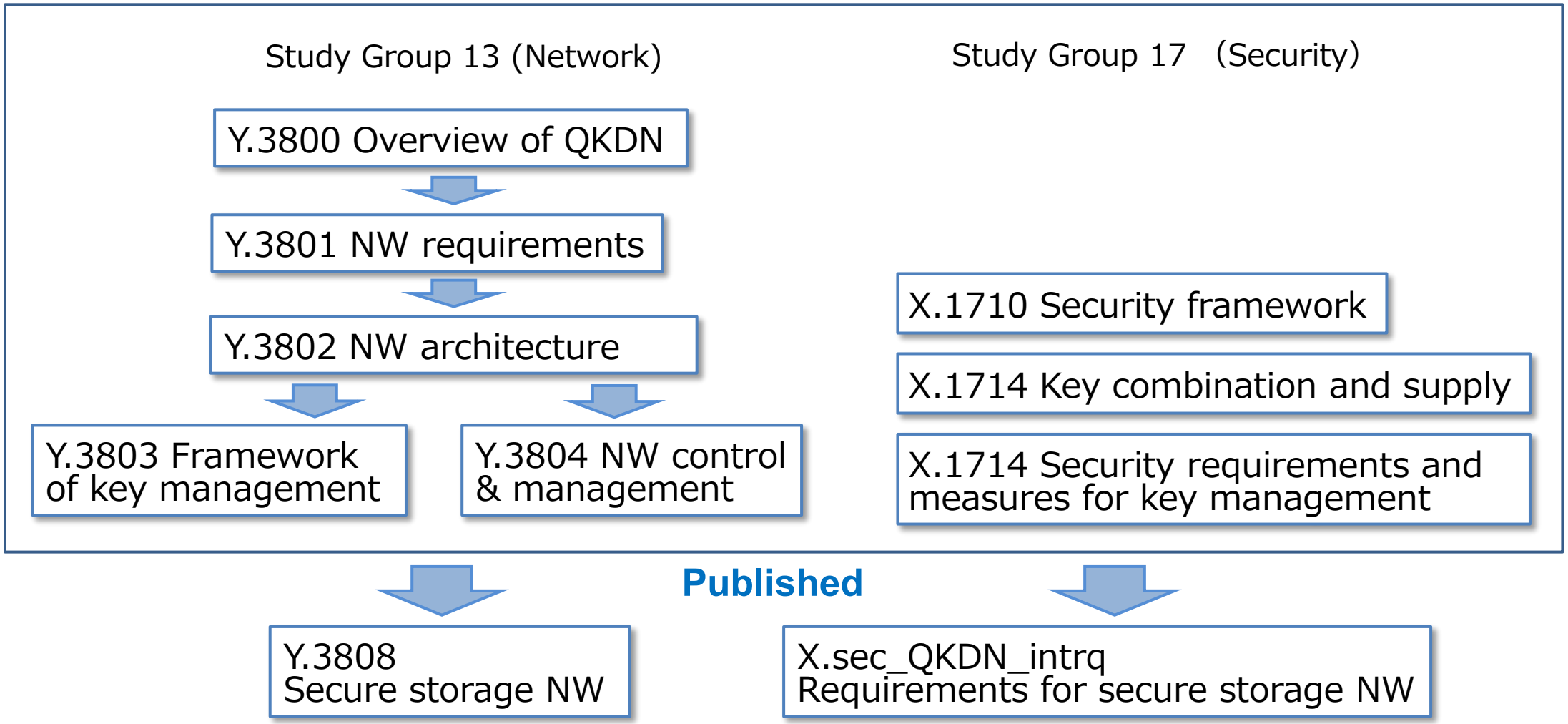
Optimal design parameters & device data

Protected by **LINCOS**

Standardization

Standardization (QKD network)

Examples of published recommendations and on-going drafts on QKD networks.



SG13 Y.3808

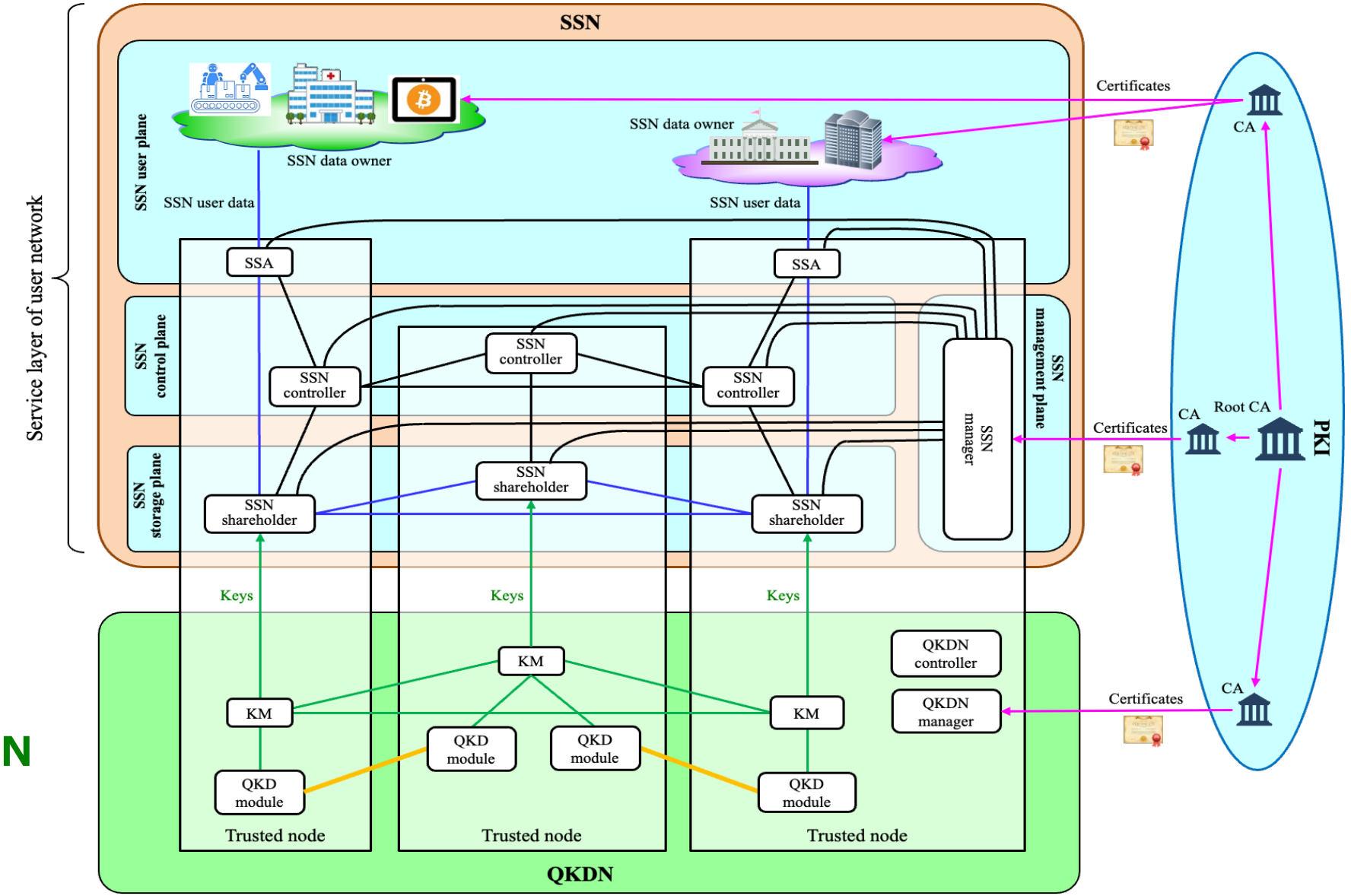
Published Dec. 2021

Framework for integration of QKDN and secure storage network

Secret sharing

QKDN

PKI



Toshiba participates in EU project “Open QKD”

18 OpenQKD Testbed Sites

OPEN QKD

Large geographic reach-out

Madrid ES
Telecom

Berlin DE
Telecom

Posnan PL
Governement

Vienna AT
Government

Delft NL
MDI QKD

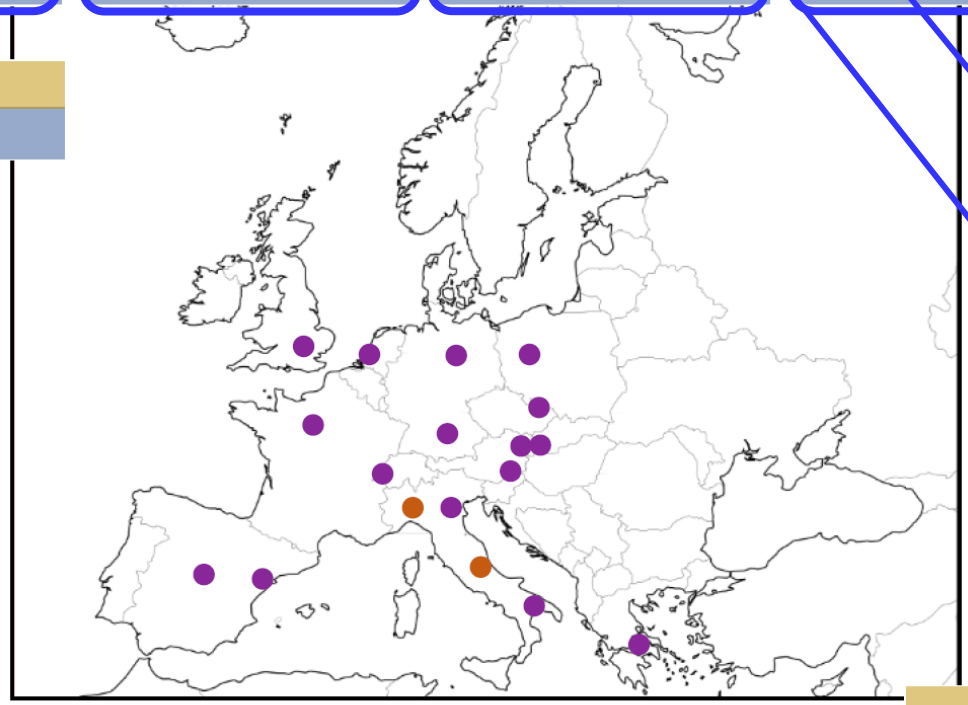
Cambridge UK
Data Centers

Paris FR
Academic network

Oberpfaffenhofen DE
Satellite QKD

Geneva CH
Smart Grid

Barcelona ES
Video Com



Torino IT
Telecom 5G

L’Aquila IT
Telecom multi-core

Ostrava CZ
High Perf. Comp.

Bratislava CZ
Government

Graz AT
Healthcare

Padua IT
Free-space QKD

Matera IT
Satellite QKD

Athens GR
Data Com

Thank you for your attention