LG U+

GROWTH LEADING AX COMPANY

PQC Application

2024. 06.

Seri Park
seripark@lguplus.co.kr

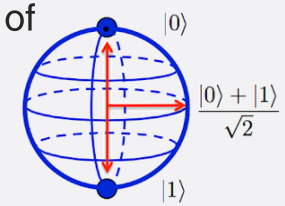
01 Quantum security Background

Quantum computers have ushered in an era of revolutionary high-speed computation for complex problems, yet they also pose new security concerns, such as the potential obsolescence of current encryption systems.

Quantum Computing

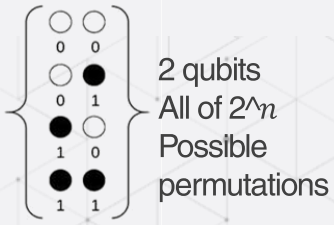
01 Physical properties of quantum

- Superposition, entanglement, uncertainty, impossibility of cloning



02 Quantum Computer

- Quantum computers process information at the qubit level, leveraging quantum properties, unlike traditional computers that use binary (0 or 1).



Quantum Algorithm

01 Shor's algorithm (by Peter Shor,1994)

- Quantum algorithm that factors integers in polynomial time.
- **Risk of compromising traditional public-key algorithms (RSA, DH).**

Time required for RSA attack using Shor's algorithm

Size in bits	1024	2048	4096
number of qubits	5124	10244	20484
number of gates	$3x10^9$	$2x10^{11}$	$2x10^{12}$
Factoring time	**4.5 min.**	**36 min.**	**4.8 hours**

2 Grover's algorithm (by Lov Grover,1996)

- Quantum algorithm for searching unsorted data in polynomial time.
- **There is a risk of decryption due to the ability to quickly search symmetric key encryption.**

02 Security Threats from Quantum Computing

The ultrafast computations with quantum computer **could** **threaten traditional cryptographic schemes.**

Quantum Computers

Faster computation
More optimized

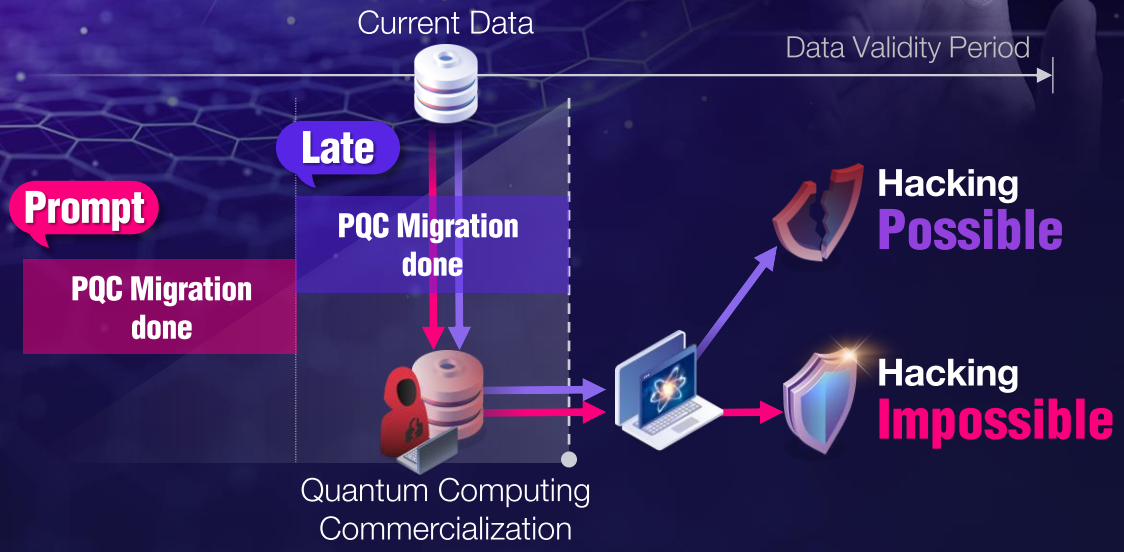
Side effects of advances in quantum computer

Vulnerable to modern cryptography

THREAT

The need for unbreakable next-gen Cryptography

Quantum Revolution: 'Harvest now, decrypt later'



03 Quantum cryptography technologies to counter quantum threats

QKD uses photons for data protection against **physical interception,**
while PQC prevents decryption by quantum computers using mathematical algorithms.

Physical methods QKD

Photon

“Integrity that disappears upon physical contact”

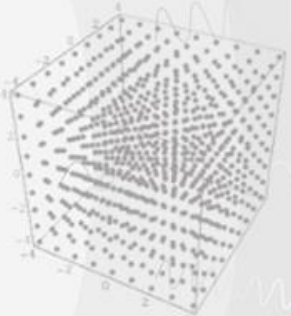
Noise
Absorption, scattering,
fog, dust, sun...

- ✓ Physically impossible to steal or alter keys due to quantum properties.
- ✓ Requires separate hardware for quantum transmission.
- ✓ Limited to key exchange functionality.
- ✓ Currently applicable to optical transmission equipment.

PQC Mathematical methods

Digital Packet

“ Hacking with a quantum computer would take thousands of years to crack the ultra-hard problems. ”



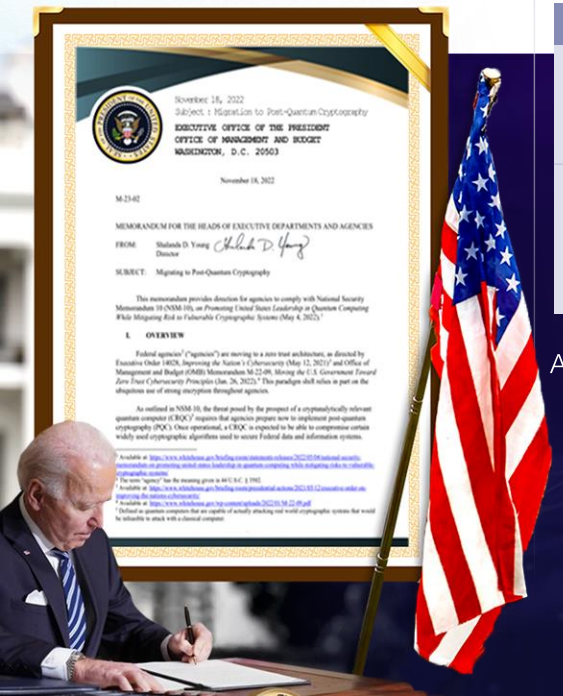
Lattice-based,
Code-based,
Multivariate-based
algorithms
...

- ✓ **Security based on mathematical puzzles that cannot be solved by quantum computers**
- ✓ **Without the need for additional hardware**
- ✓ **Utilized for key exchange/signature methods in traditional public-key algorithms**
- ✓ **Applicable to all network devices, applications, and services**

04 PQC Global Trends(USA)

The States is undergoing a **migration of cryptosystem** in major government agencies to PQC.

’May 2022 — President Biden signed a National Security Memorandum



‘July 2022 — Announcement of Standard Algorithms

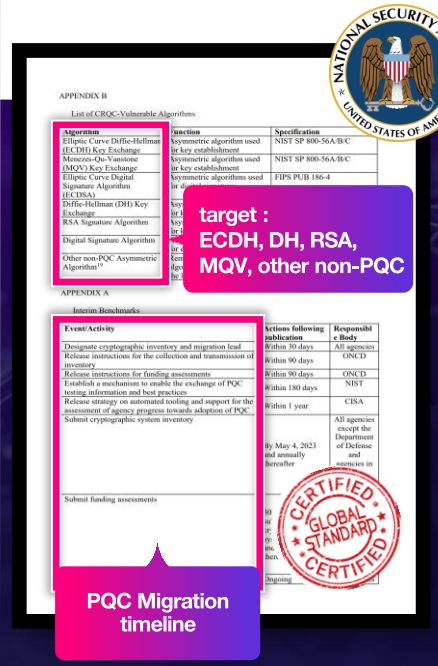
NIST National Institute of Standards and Technology

Category	Algorithms
KEM	CRYSTAL S-Kyber
DS	CRYSTAL S-Dilithium, FALCON, Sphincs+

Additional Selection of PQC Algorithms in Progress ▸▸

’Nov 2022 — Announcement of PQC Migration

Initiation of migration from Classical Cryptography to Post-Quantum Cryptography through Executive Order Implementation

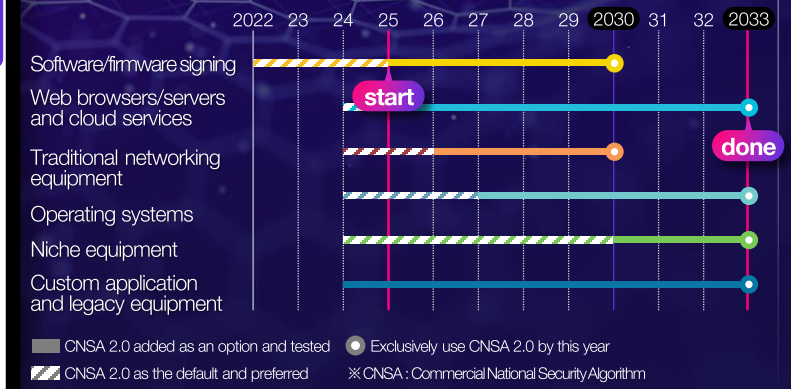


target : ECDH, DH, RSA, MQV, other non-PQC

PQC Migration timeline

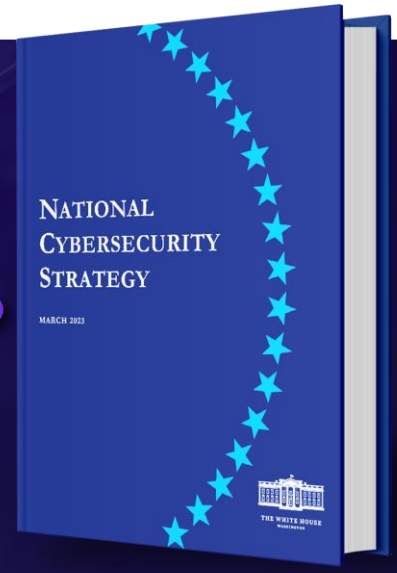
CNSA 2.0 Timeline

Recommendations for CRYSTALS-Kyber/ Dilithiumand 256-bit security parameters usage



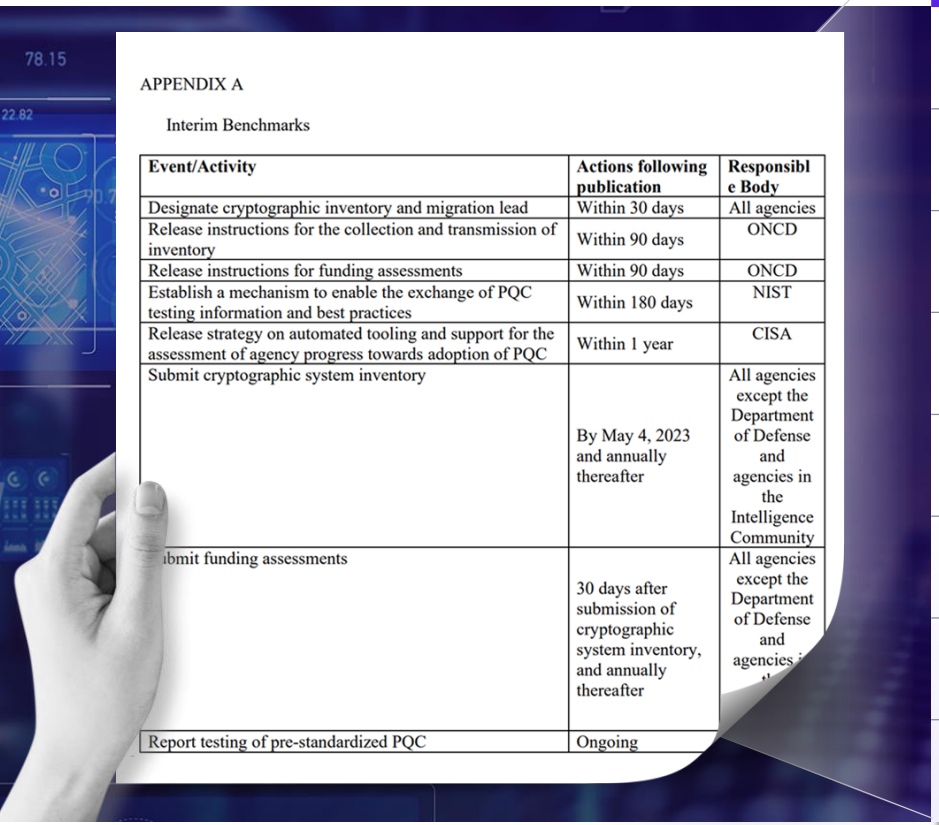
’April 2023 — National Cybersecurity Strategy

In preparation for the quantum era, prioritize the migration of vulnerable public networks and systems to post-quantum cryptography



05 PQC Migration Trends in development

Under the Migration Executive Order, detailed plans are rapidly being established by the responsible ministries, outlining timelines and activities needed for the national cryptographic transition.



APPENDIX A

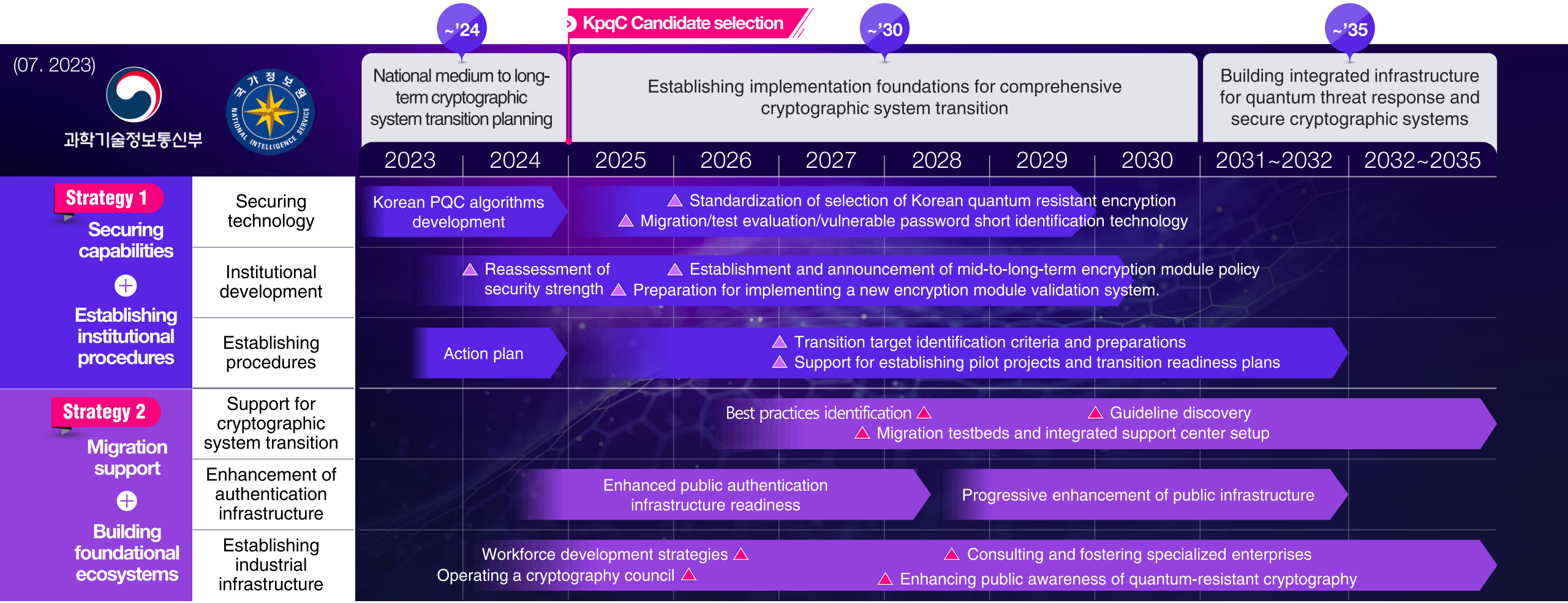
Interim Benchmarks

Event/Activity	Actions following publication	Responsible Body
Designate cryptographic inventory and migration lead	Within 30 days	All agencies
Release instructions for the collection and transmission of inventory	Within 90 days	ONCD
Release instructions for funding assessments	Within 90 days	ONCD
Establish a mechanism to enable the exchange of PQC testing information and best practices	Within 180 days	NIST
Release strategy on automated tooling and support for the assessment of agency progress towards adoption of PQC	Within 1 year	CISA
Submit cryptographic system inventory	By May 4, 2023 and annually thereafter	All agencies except the Department of Defense and agencies in the Intelligence Community
bmit funding assessments	30 days after submission of cryptographic system inventory, and annually thereafter	All agencies except the Department of Defense and agencies
Report testing of pre-standardized PQC	Ongoing	

Event/Activity	Actions following publication	Responsible Body
Designate cryptographic inventory and migration lead	Within 30 days	All agencies
Release instructions for the collection and transmission of inventory	Within 90 days	ONCD
Release instructions for funding assessments	Within 90 days	ONCD
Establish a mechanism to enable the exchange of PQC testing information and best practices	Within 180 days	NIST
Release strategy on automated tooling and support for the assessment of agency progress towards adoption of PQC	Within 1 year	CISA
Submit cryptographic system inventory	By May 4, 2023 and annually thereafter	All agencies except the Department of Defense and agencies in the Intelligence Community
Submit funding assessments	30 days after submission of cryptographic system inventory, and annually thereafter	All agencies except the Department of Defense and agencies in the Intelligence Community
Report testing of pre-standardized PQC	Ongoing	All agencies

06 Korean PQC Migration Master Plan

Efforts are underway to establish a multinational quantum-resistant cryptographic system, including promoting a Korean-specific algorithm for KPQC.



07 LG U+ PQC dedicated-line service

LG U+ is leading PQC through NIA pilot projects, achieving the world's first launch and NIS certification in Korea.

STEP 01

Achieving technological maturity, customer validation, and securing reference cases.

Participation in the Digital New Deal Quantum Cryptography Communication Pilot Infrastructure Construction Project ('20-'22, 3 years).

STEP 02

National standard cryptographic module security/testing verification

"U+ PQC transmission equipment" KCMVP certification application completed

* Cryptographic Module Validation Program

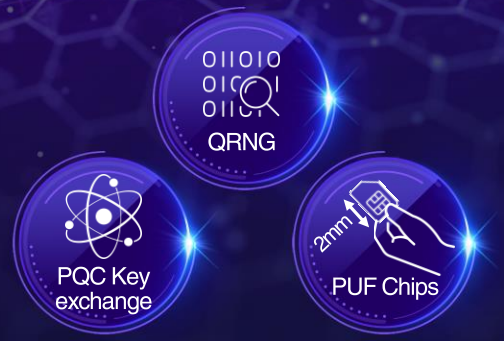
STEP 03

Terms of service declaration completed

Domestic leased line service terms updated as of April 19, 2022.

STEP 04

World's first PQC leased line service launch



STEP 05

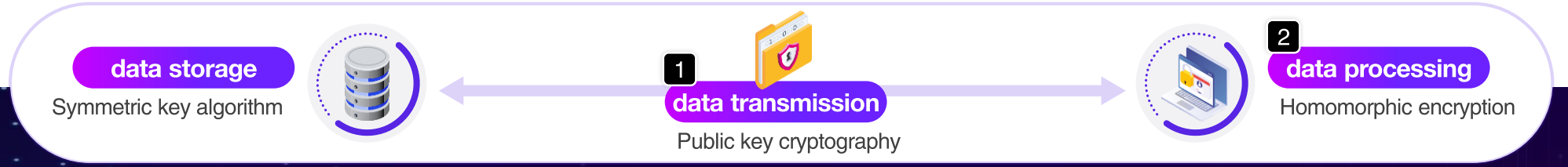
(National Intelligence Service)

Obtained the only NIS security functionality confirmation certificate in South Korea

LG U+

The PQC technology applied by LG U+

To maximize service security and reliability, the PQC algorithm will be applied for data transmission and processing.



data encryption and decryption

1 PQC Algorithm (public key)

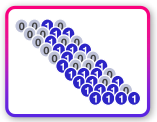
Securely exchanging symmetric keys (including authentication processes) to ensure safe data transmission between users.

generation process

1st-QRNG

Quantum-random number generation

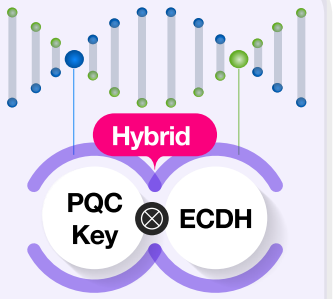
2nd-PQC



PQC key generation with quantum resistance

Selection
- Crystar Kyber (NIST)
- R.Lizard (TTA)
- SMAUG-T (KpqC)

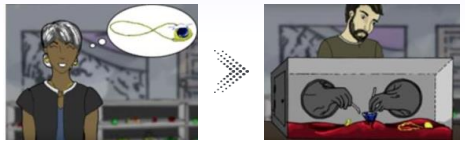
3rd-Hybrid processing



data processing

2 Homomorphic encryption (public key)

A cryptographic technique that incorporates the concept of homomorphism from algebra, enabling data analysis even in its encrypted state.

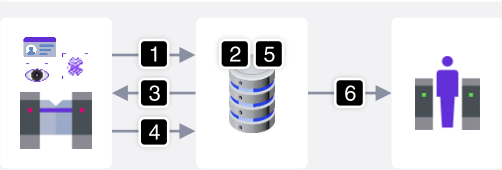


Standardization process stages

Domestic
- 2019, TTA Domestic standardization completed:
  – CKKS cipher scheme (Seoul National University)

Global
- 2024, ISO/IEC International standardization completion scheduled:
  – BGV/BFV, CKKS cipher scheme Homomorphic Encryption Standardization consortium formation.*

Example



1 Transmitting encrypted information
2 Computing while data is encrypted
3 Sending computation results
4 Transmitting decoded computation results
5 Verification of results
6 Request gate open

* Samsung SDS, Microsoft, Intel, IBM, google etc. / NIST, ITU, etc. / Seoul National University, MIT etc.

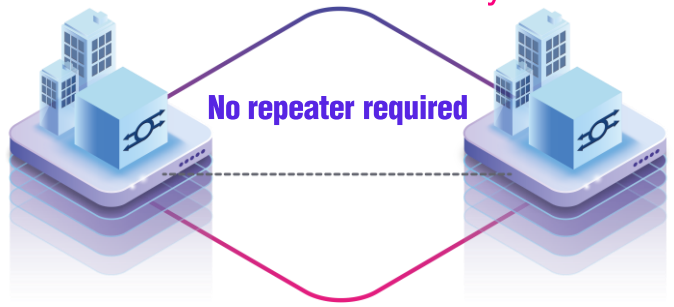
09 Advantage of PQC Technology

We views post-quantum cryptography as a more cost effective and easily maintained solution.

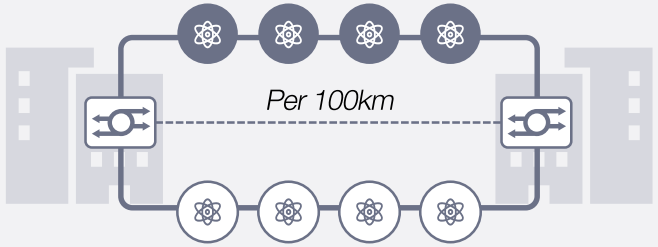
U+ PQC

Step 01
No limit of distance

End-to-End Security

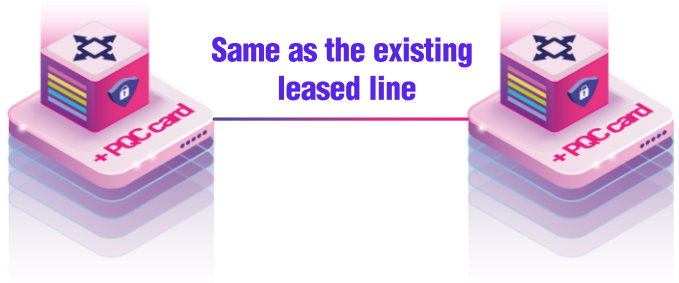


QKD **Multiple repeater required**

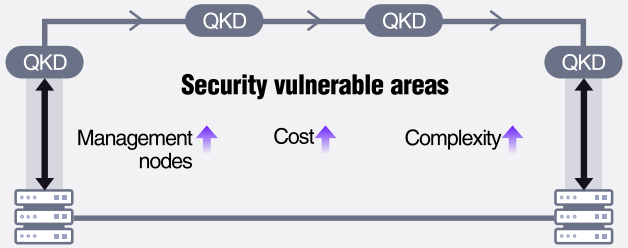


Step 02
No additional leased line or equipment

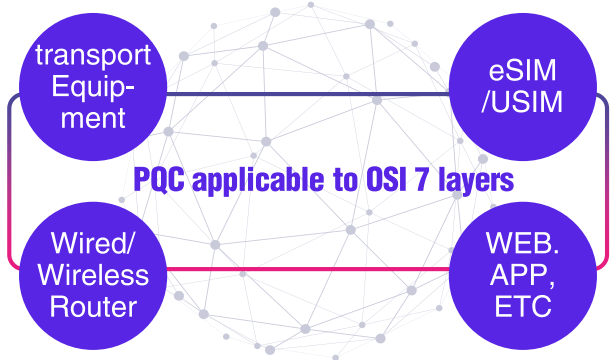
1-core, 1-path

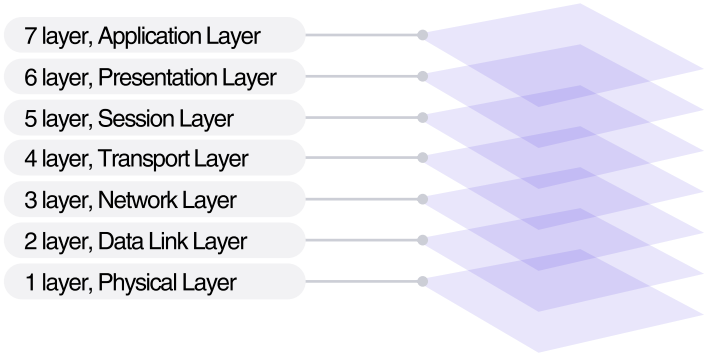


QKD **2-core, 2-path**
(data+quantum key networks)



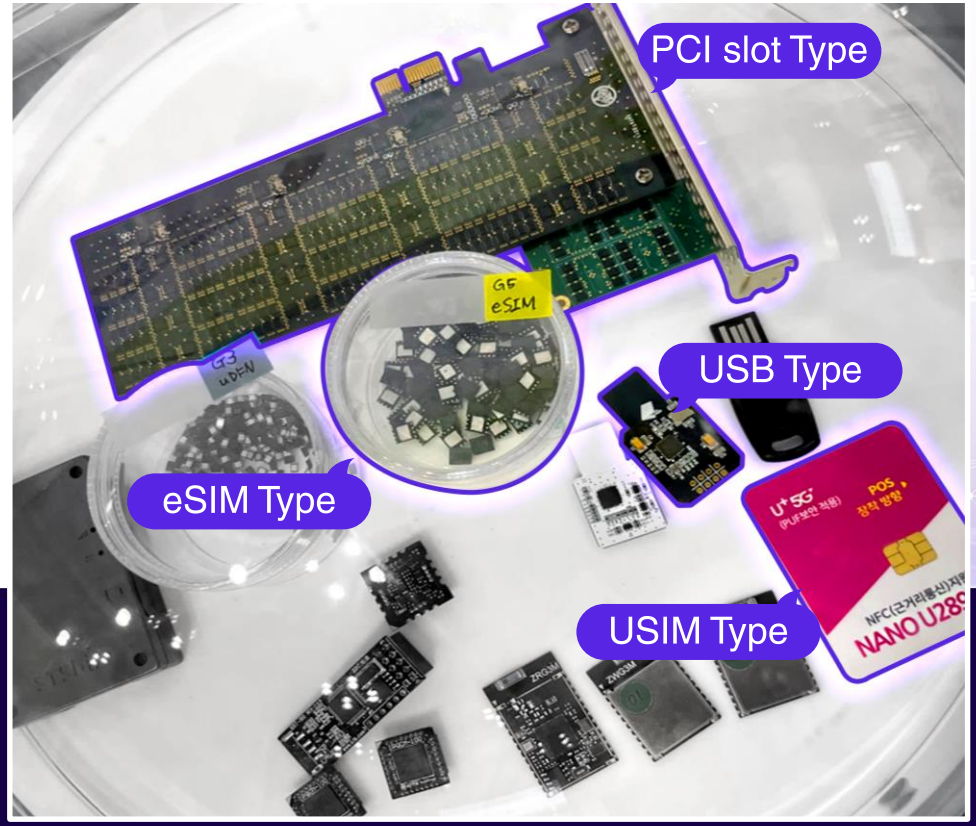
Step 03
Easily applied equipment





Miniaturization and Diversification

By applying PQC PUFs to **USIMs** and **ESIMs,** we enable secure communication **in a variety of small devices.**

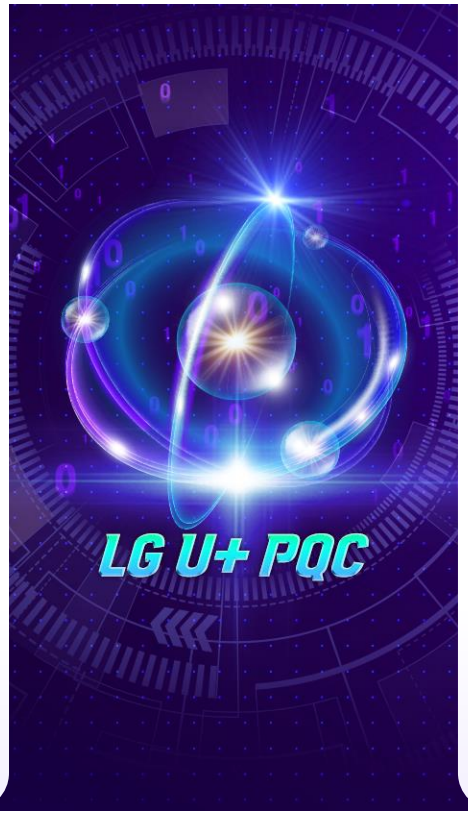


U+ PQC PUF chip roadmap

11 U+ PQC Applications

We are exploring specialized services enhanced with strengthened security using easily applicable PQC technologies across various sectors such as corporate, public, financial, and healthcare.

PQC devices	Applications	
• PQC Transmission equipment (10G) • PQC Video conferencing	VIP video conferencing solution	
• PQC Transmission equipment (10G) • PQC LTE router	Parking management solution	
• PQC Transmission equipment (10G) • PQC File transfer solution	Industrial data encryption and file transfer service	
• PQC Transmission equipment (10G) • PQC DB Encryption solution	Medical information encryption service	



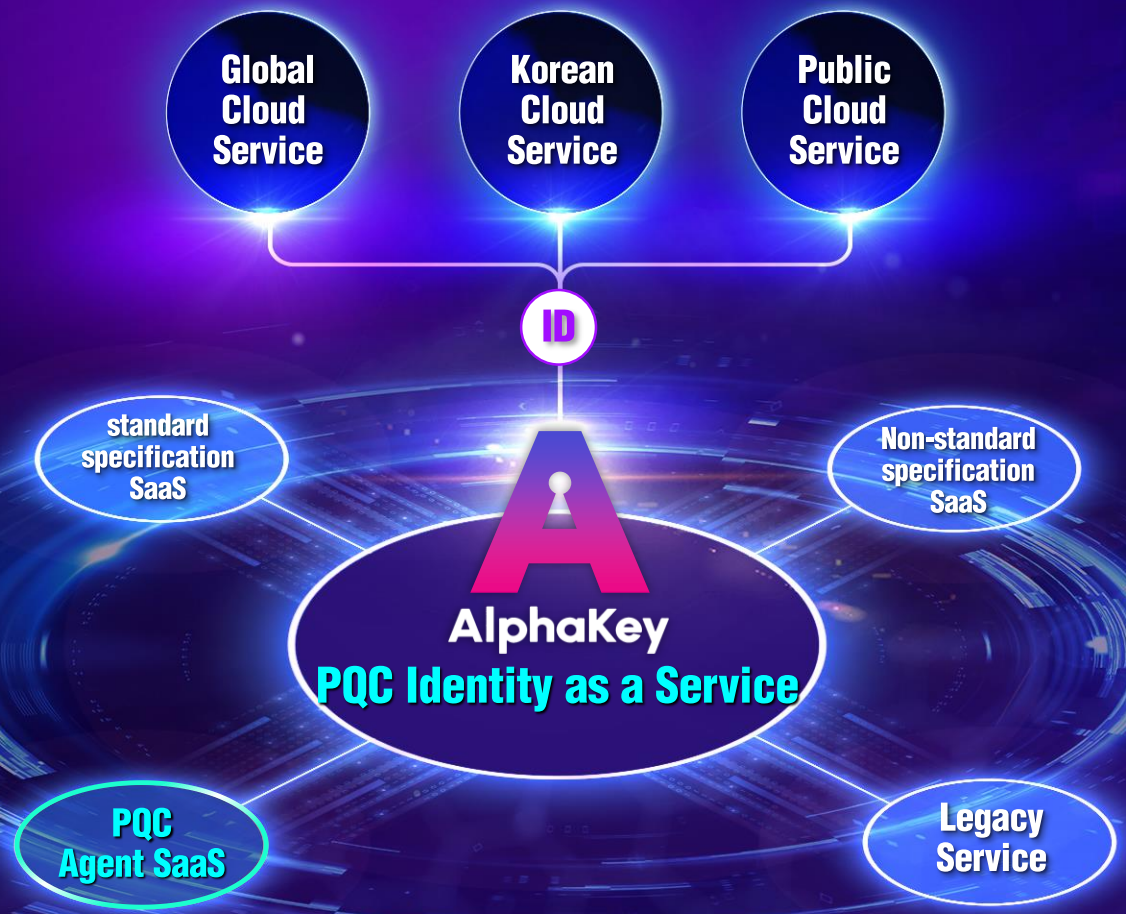
Applications	PQC devices	
Personal information database encryption service	• PQC Transmission equipment (10G) • PQC DB Encryption solution	
Ticket booking service	• PQC Transmission equipment (10G) • PQC Ticket booking solution	
Facial recognition access control system	• PQC Transmission equipment (10G) • PQC Facial recognition solution	

PQC cloud authentication service

By applying PQC algorithms for 'authentication,' **we can consolidate individual SaaS accounts into a unified authentication service for centralized management.**

PQC can be used for 'key exchange, encryption-decryption, authentication' using public key algorithms.

category	PQC	QKD
Key exchange	O	O
ENC/ DEC	O	-
Authentication	O	-



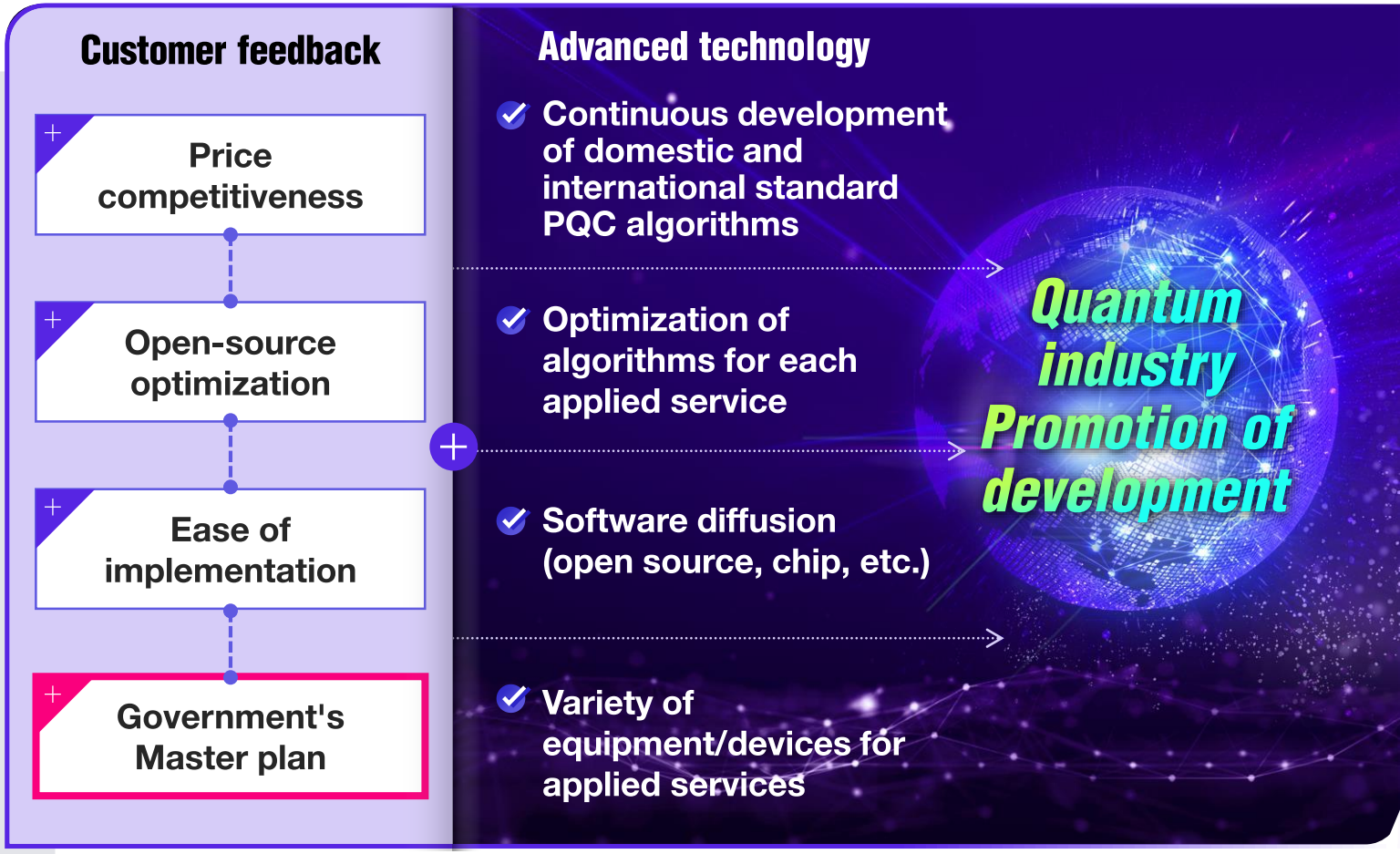
- AlphaKey is a service that integrates and manages employees' business service accounts based on integration with HR databases.
- Features : IAM, MFA, SSO, Context security, Workflow, audit, AI calculator
- AlphaKey provide enhanced user authentication with strengthened security through PQC

customer needs

IT security managers require sector-specific practical guides and testing support for the national transition to a cryptographic system, aiming to establish security guidelines and achieve cost savings

Customer feedback on PQC usage

- "Our mission is to achieve communication/network budget savings."
- "Even with technical support provided, it should be easy to operate."
- "Government guidelines are crucial."
- "We currently face a shortage of space in the server room, with nowhere to place additional equipment."
- "We need to prevent security incidents, but I'm unsure what steps to take."
- Will the quantum era really arrive? (Will it really break?)
- "It needs to be applied at the service level."



K-PQC Migration Platform Implementation plan

PQC Migration platform to assess vulnerabilities in current encryption and PQC implementations, **contributing to national cryptographic system transition plans.**

NIST PQC Migration scenario

Migration to PQC, NIST, ’21.06

A systematic approach to transitioning from vulnerable public-key algorithms to PQC for various types of assets.

1. Scenario for transitioning to FIPS-140 certified HW/SW modules
2. Crypto libraries containing vulnerable public-key encryption
3. Encryption app and encryption support app
4. Transitioning from vulnerable encryption on computing platforms
5. **Transitioning communication protocols using vulnerable encryption algorithms**

PQC Migration Platform

Providing user vulnerability analysis reports and verification guidelines

- ✓ Providing guidance on methods for transitioning to PQC.
- ✓ Analyzing minimum requirements for applying PQC on low-spec devices like IoT devices (e.g., CPU performance, memory size).
- ✓ Analyzing and providing guidance on PQC types suitable for different environments (e.g., IoT, cloud, enterprise).

Vulnerability assessment of algorithms

Provided functionalities

- Providing integrated API for NIST PQC 4 types
- Providing API for NIST PQC 4 types security protocols
- Providing user API(PQC/Crypto) software verification results
- Providing user API(PQC/Crypto) vulnerability detection results

K-PQC Migration plan

KpqC 알고리즘 선정

	~’24	~’30	~’35
과학기술정보통신부	국가 중장기 암호체계 전환 추진 방향 수립	체계적·입체적 암호체계 전환을 위한 이행기반 마련	양자 위협대응 통합인프라구축 및 안전한 암호체계 구현
국가정보원			

’23 ’24 ’25 ’26 ’27 ’28 ’29 ’30 ’32 ’35

전략 1 역량 확보 + 제도 정비

- 기술 확보: 한국형 양자내성암호 개발 → △한국형 양자내성암호선정·표준화 △전환/시범평가/취약암호탐지식별기술
- 제도 정비: △보안강도재정립 △암호모듈중장기정책수립·공지 △암호모듈검증제도시행준비

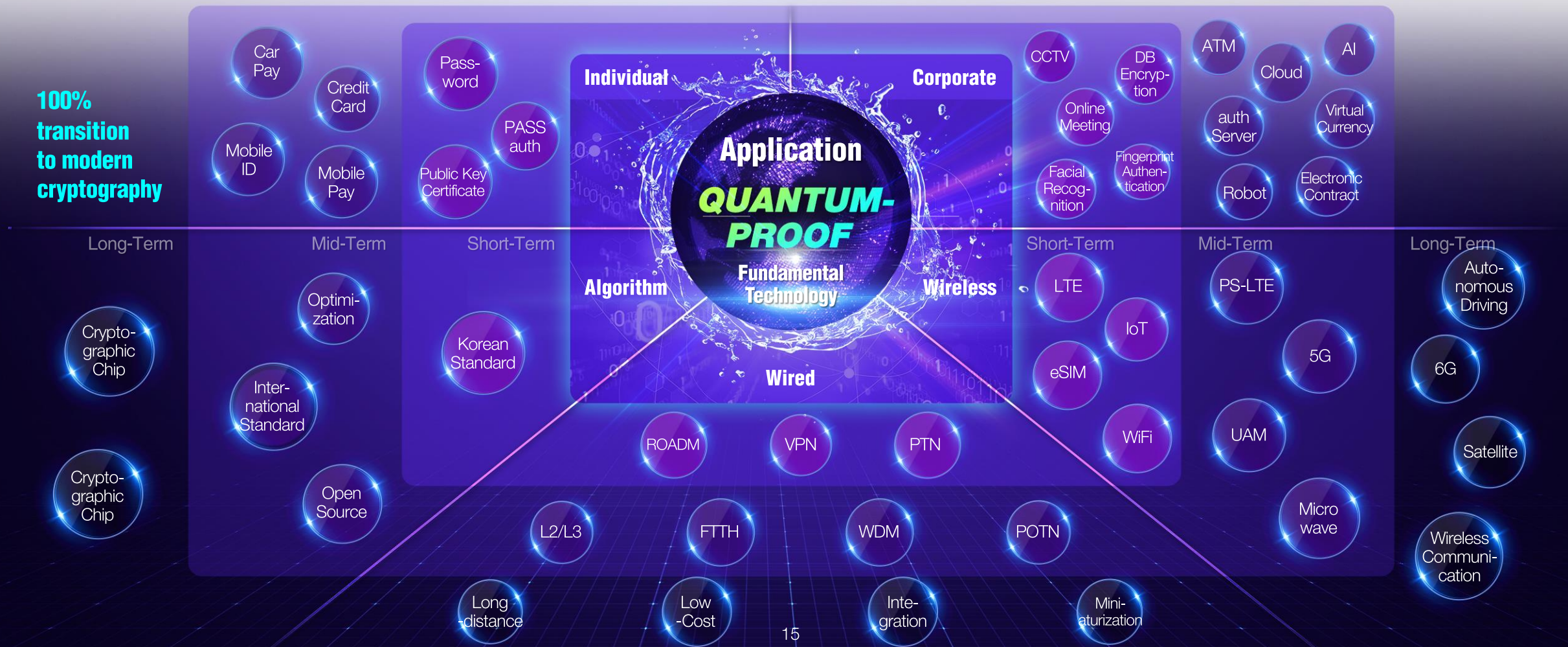
Accelerating cryptographic system transition led by global pioneers

전략 2 전환 지원 + 기반 생태계 조성

- 암호체계 전환지원: △모범사례 발굴 △가이드라인 발굴 △전환 테스트베드 및 통합 지원센터 구축·운영
- 인증 인프라 고도화: 공공 인증인프라 고도화 준비 (호환성 및 최소중단 전이체계 등 마련) → 공공 인프라의 단계별 고도화
- 산업 기반 구축: △인력양성방안마련 △컨설팅·전문기업 육성 △암호협의회 운영 △양자내성암호 전환 국민 인식 제고

PQC Technology Roadmap

For quantum security, Wired, wireless networks, and even applications **should be developed based on the PQC algorithm.**



LG U+

Thank you

GROWTH LEADING AX COMPANY