QUANTUM SAFE
PKI TRANSITIONS

Quantum Valley Investments Headquarters

We offer quantum readiness assessments to help you identify your organization's quantum risks, develop an upgrade path, and deliver a plan to move forward.

We created the first commercially available security solution to offer quantum resistant algorithms that can replace the classical algorithms that are weak against quantum computing threats.

Agenda

Threat

The Authentication Challenge

Options

Conclusions and Recommendations

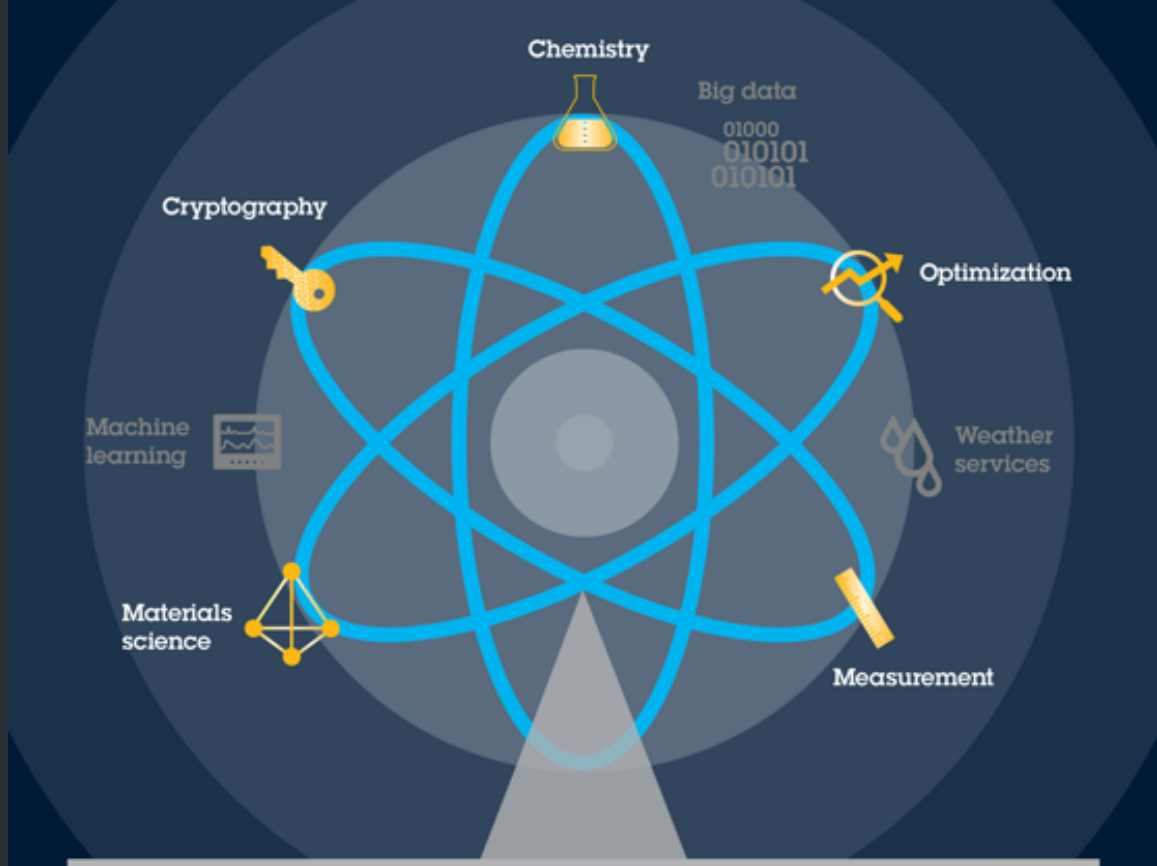
Quantum Computing

Threat

Why Quantum Computers?

Exploiting the power of quantum physics to create a new way of computing, with applications to:

- Drug design
- Unstructured search
- Materials science
- Code breaking
- Machine learning
- Chemistry and physics simulations



GOVERNMENT
e.g. Support deep cryptoanalysis of critical data

PHARMACEUTICAL
e.g. Develop new drugs and treatments

MANUFACTURING & INDUSTRIAL
e.g. Develop new materials and processes

TELECOMMUNICATIONS
e.g. Enable secure communications across networks

TRAVEL & TRANSPORTATION
e.g. Design new vehicles and transport systems

FINANCIAL SERVICES
e.g. Predict market trends and risks

IBM **Center for Applied Insights**
ibm.com/ibmcai | ibmcai.com/tag/quantum | #QuantumComputing

IBM

Source: IBM Center for Applied Insights, "A quantum of possibilities: The business advantages of taking the quantum leap" ibm.com/ibmcai/quantumcomputing

Cryptographic Challenges For A Post Quantum World

Today's security solutions rely on the complexity of the underlying mathematical problems that form the foundation for modern cryptographic systems.

The massive processing capabilities found in quantum computers will challenge our current beliefs around complexity.

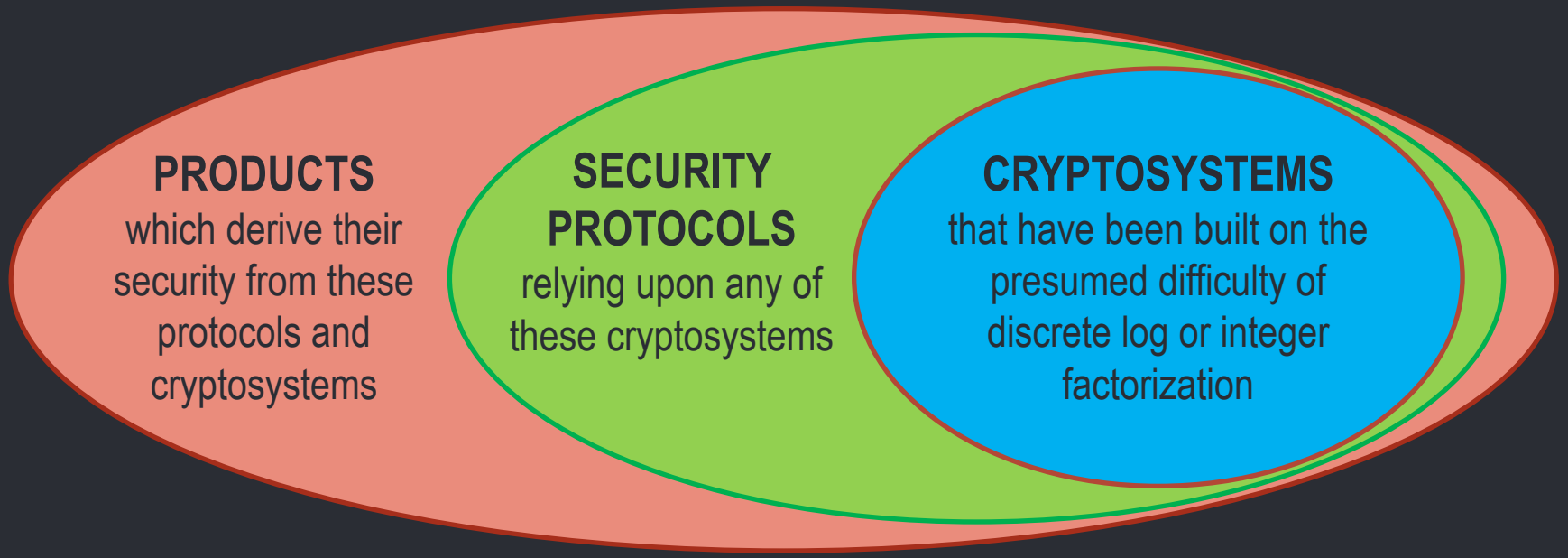
What needs to be protected today?

Any encrypted data where key establishment is communicated or stored along with it will not remain confidential beyond Y2Q.

Any digital documents signed today that must maintain their authenticity beyond Y2Q.

Any signed software that needs to remain authentic at crossover point.

So, What Is Vulnerable?



This is the case for anything that is encrypted after a large-scale quantum computer has been built, anything we encrypt today, and anything we encrypted in the past!

Quantum Computing
Authentication

Code Signing

Authenticity of software updates are essential to trust

Digital signatures are ubiquitous with software updates

Frequency of updates are much less than authentication requests at a web server, for example

Hash Based Signatures provide a safe option

Secure Email

Email continues to be the main communication medium for business

- Large amounts of sensitive information continues to be sent
- Mail server breaches can cause enormous brand/financial/trust damage

Email can be protected by

- Server to server encryption
- Services such as S/MIME and PGP

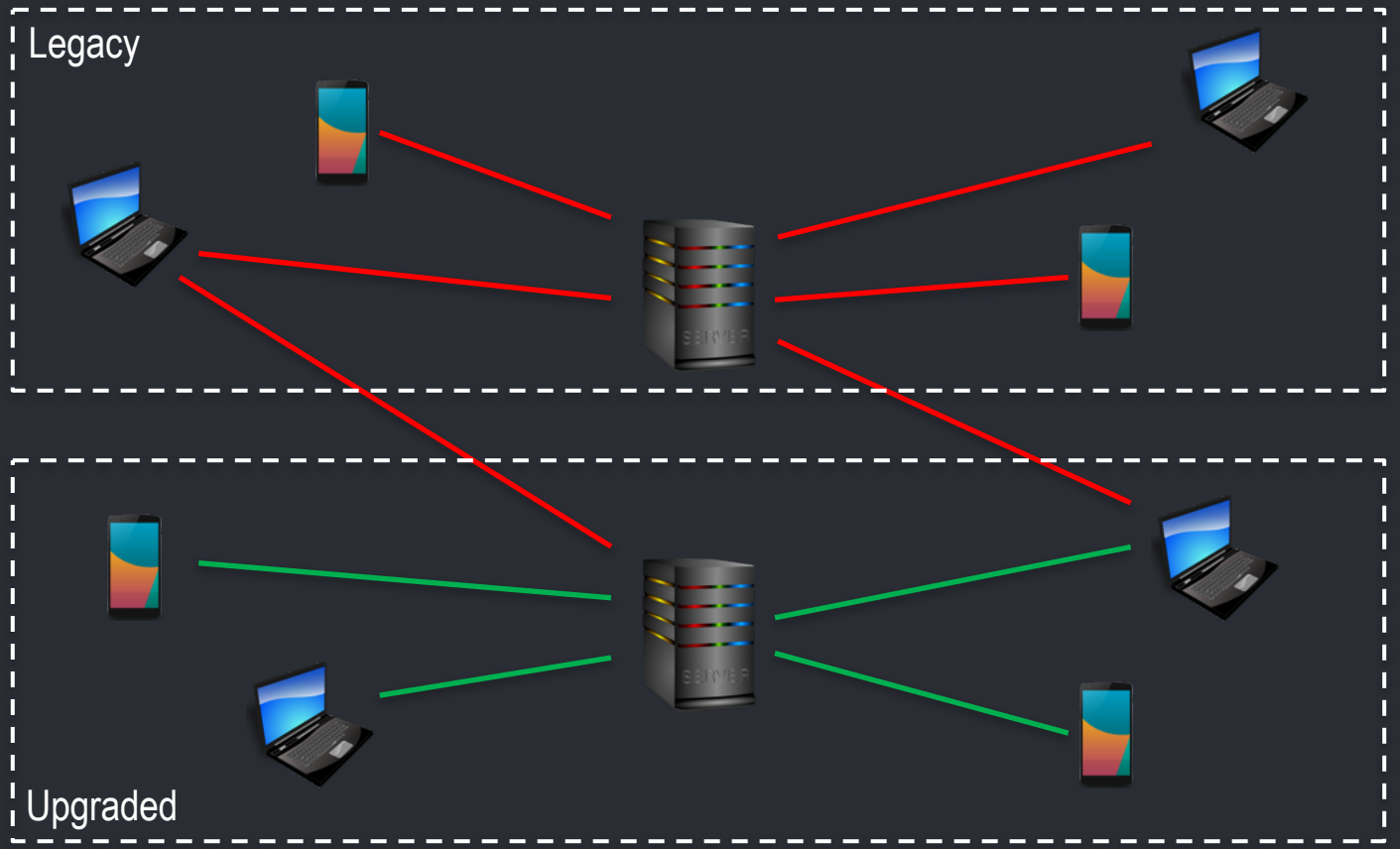
S/MIME and PGP differ on key management

- Imply need for PKI transition

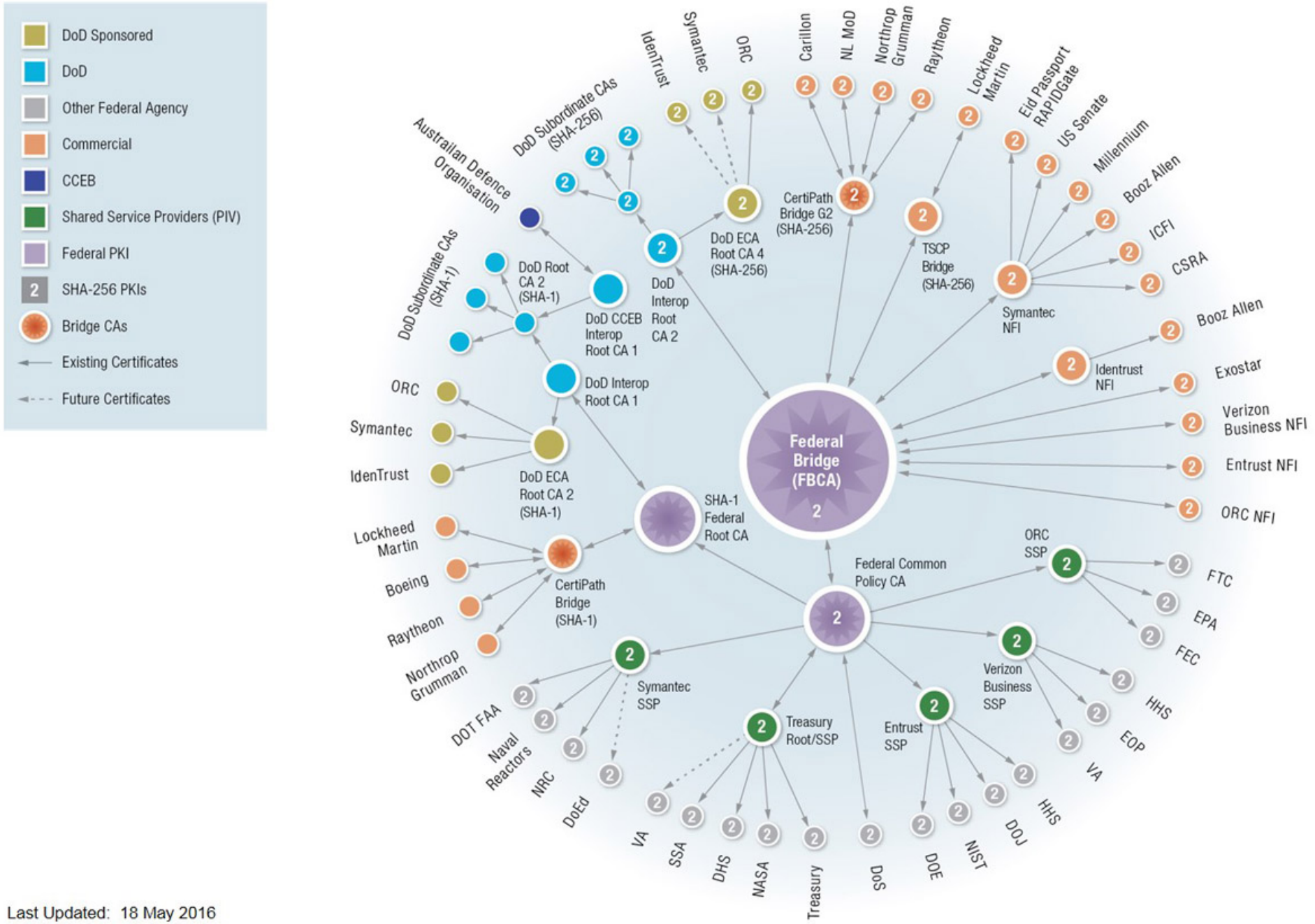
Quantum Safe Deployment Challenges

Moderate deployment effort with a phased deployment possible.

Timeline: Years.



The DoD PKI External Interoperability Landscape



Last Updated: 18 May 2016

Quantum Computing

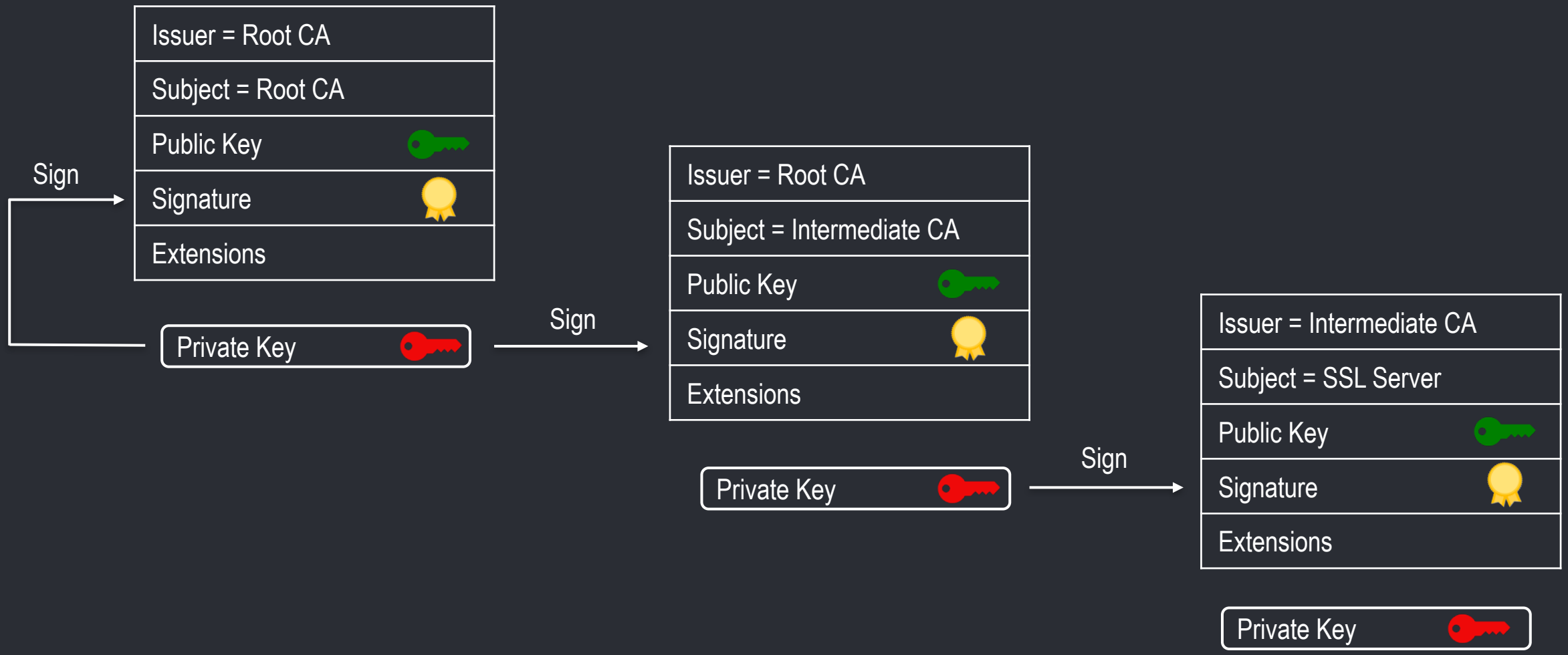
PKI

Quantum Resistant PKI

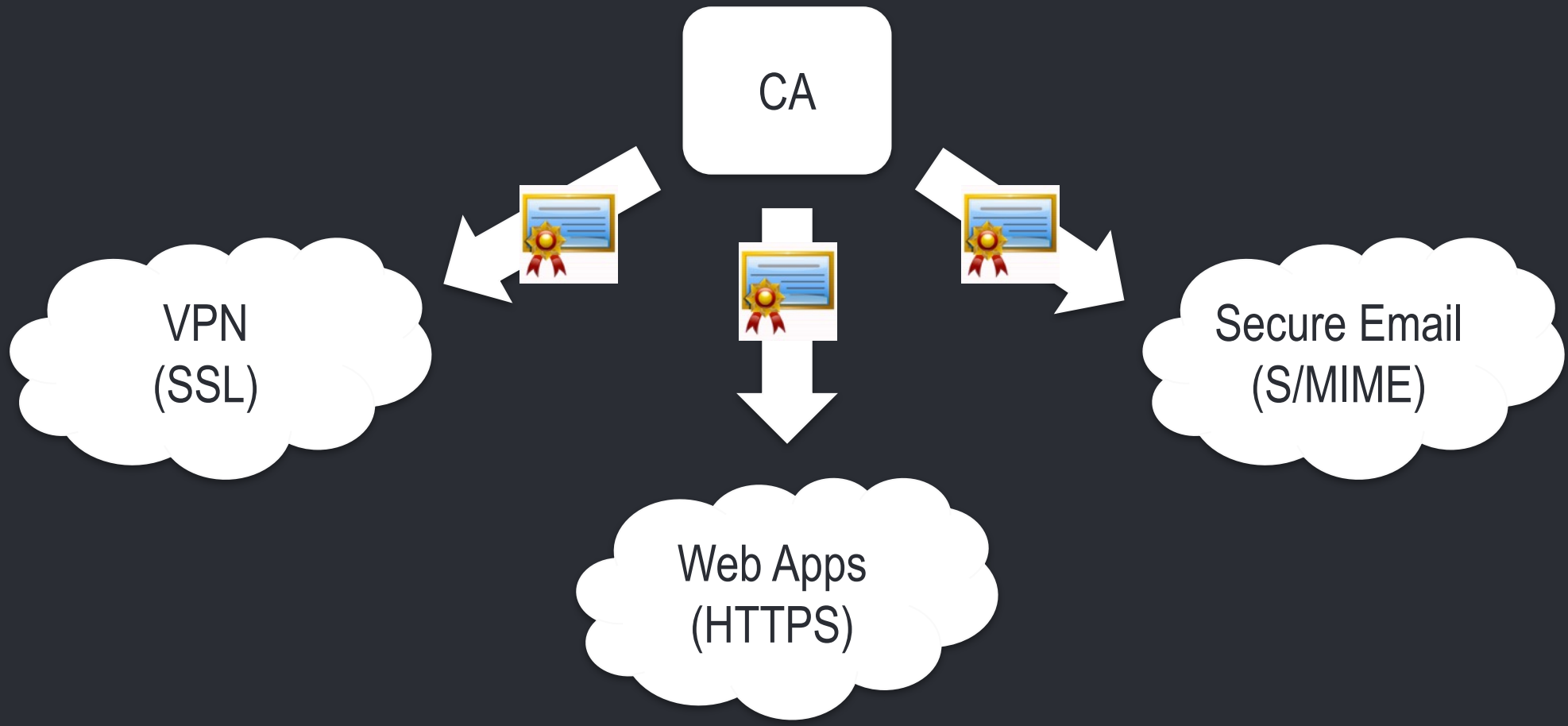
Enterprise PKI supporting remote VPN can be quite large and cannot be updated overnight.

To avoid service stoppage a sophisticated strategy, clever mechanism, and systematic method are needed to gradually migrate the monolithic PKI system to new algorithms that allow mixture of algorithms, including interim choices of algorithms.

X509 Certificate Chain



Enterprise Infrastructure



Upgrade Approaches

Forklift upgrade

- Expensive!
- Requires you to wait until all systems are made Quantum Safe
- Many failure points tested all at once
- Infrastructure risk through waiting

Upgrade Approaches

Running a Parallel Infrastructure

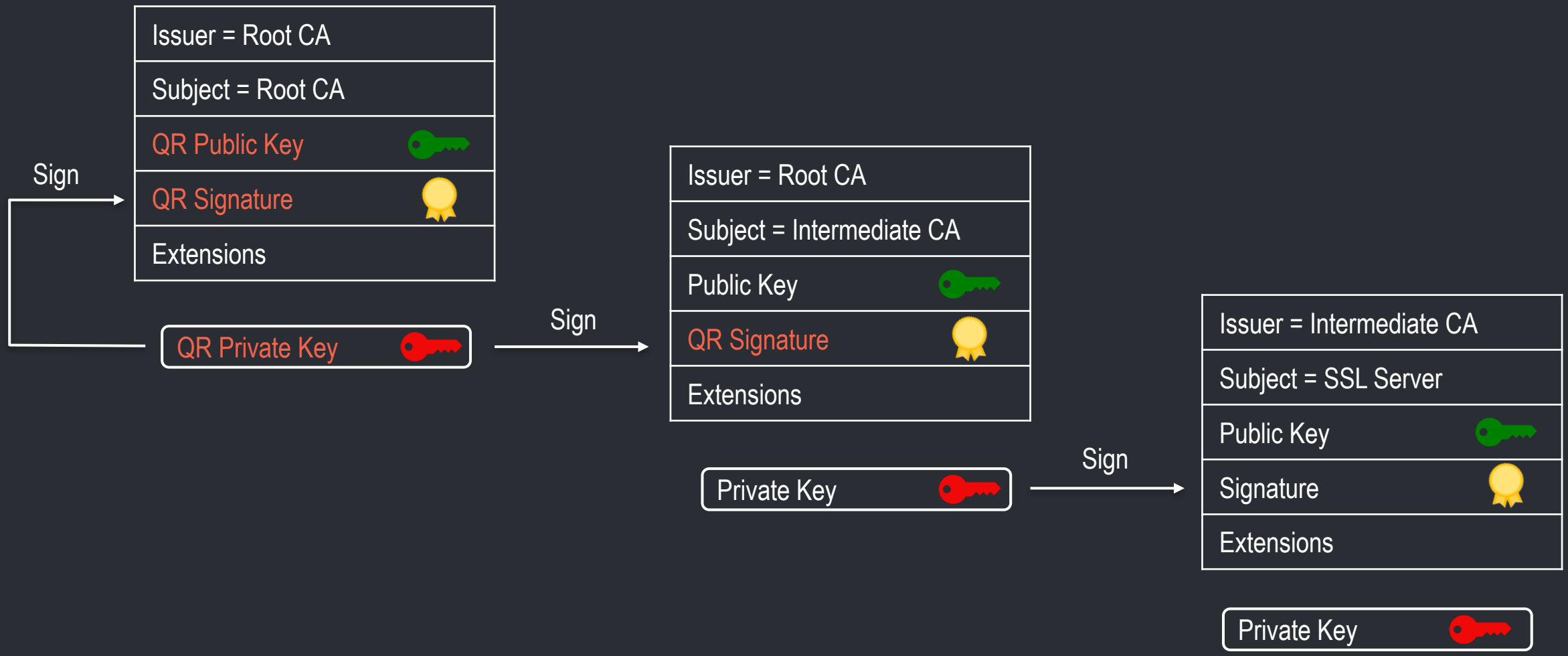
- Multiple user credentials to individually manage
  - Two smart cards?
- User training on which system to use at which particular moment
- Cost of running two instances of your systems

Applying Hybrid Ideas to Authentication

Using Hash Based Signatures for Root Certificates

- Subordinate CAs signed with LMS/XMSS
  - Public Key is RSA/ECC
- End-entity certificates signed with quantum vulnerable scheme
- Upgrade subordinate CAs, and end entities, as stateless options are finalized
- Root certificates finalized early
  - Migration across browsers is slow

X509 Certificate Chain

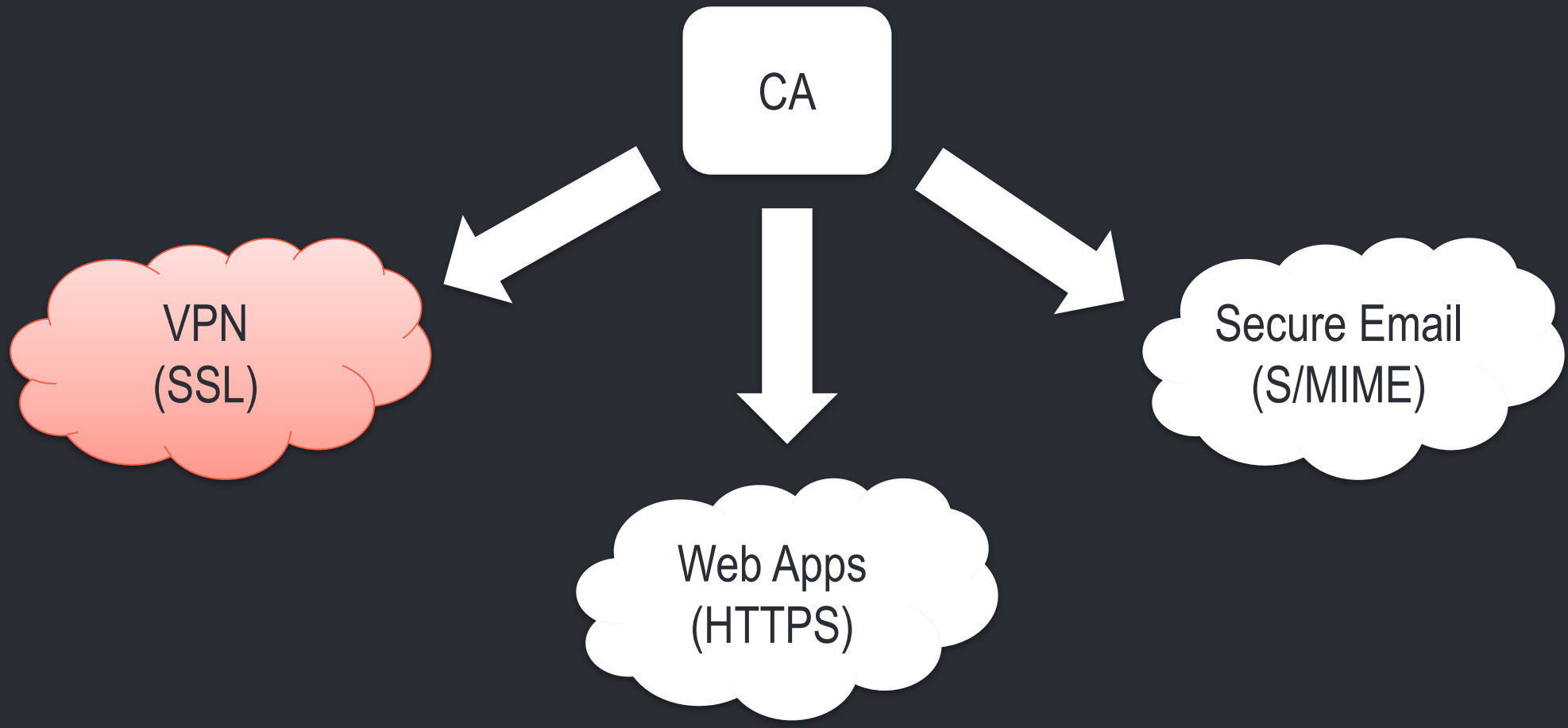


Applying Hybrid Ideas to Authentication

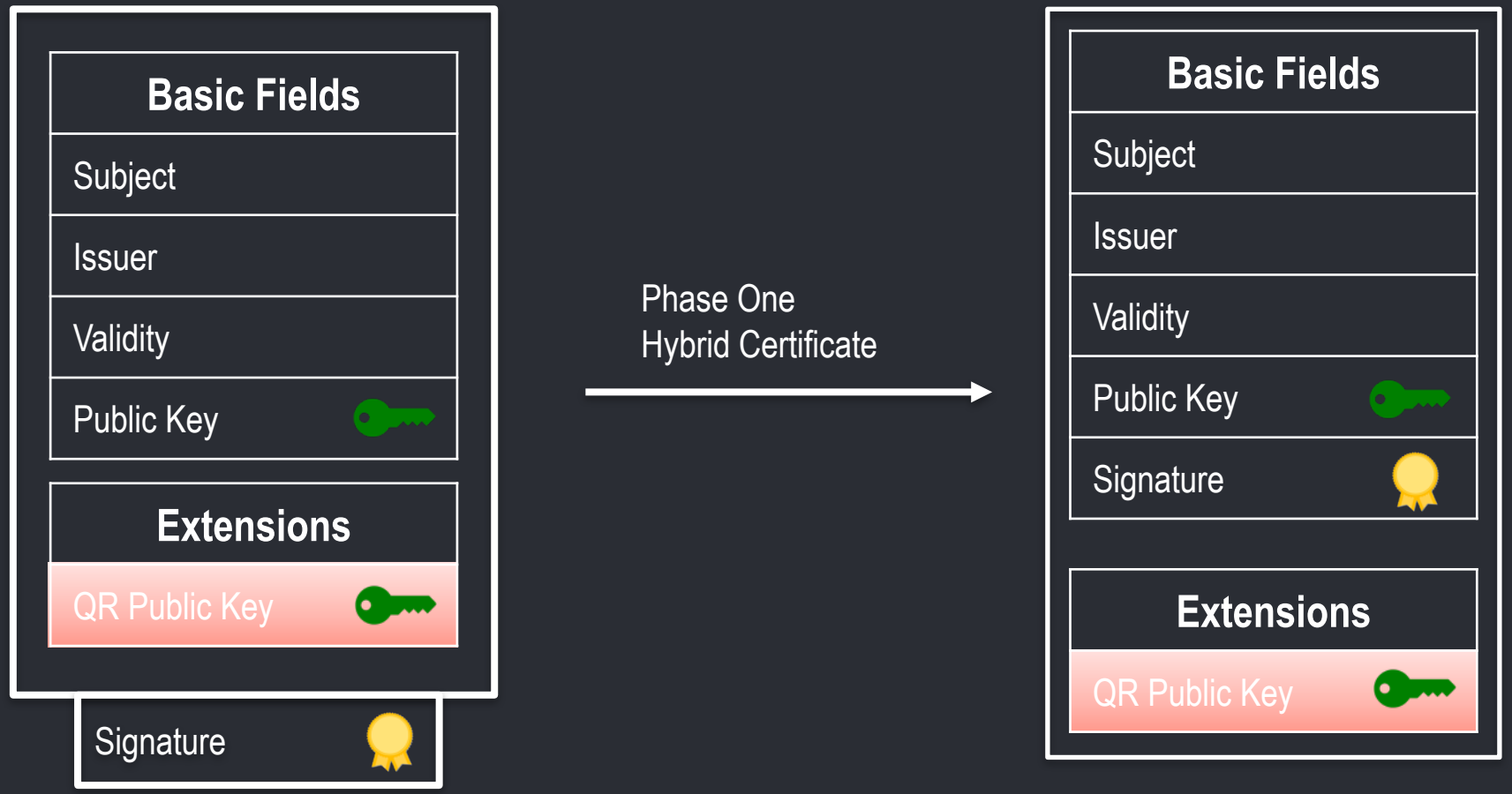
Creating Hybrid Certificates

- Utilize aspects of X.509 to include both quantum vulnerable and resistant keys
- Allow for an in-place migration of PKI credentials and applications
  - Upgrade systems use quantum resistant credentials
  - Legacy systems continue to quantum vulnerable keys/signatures

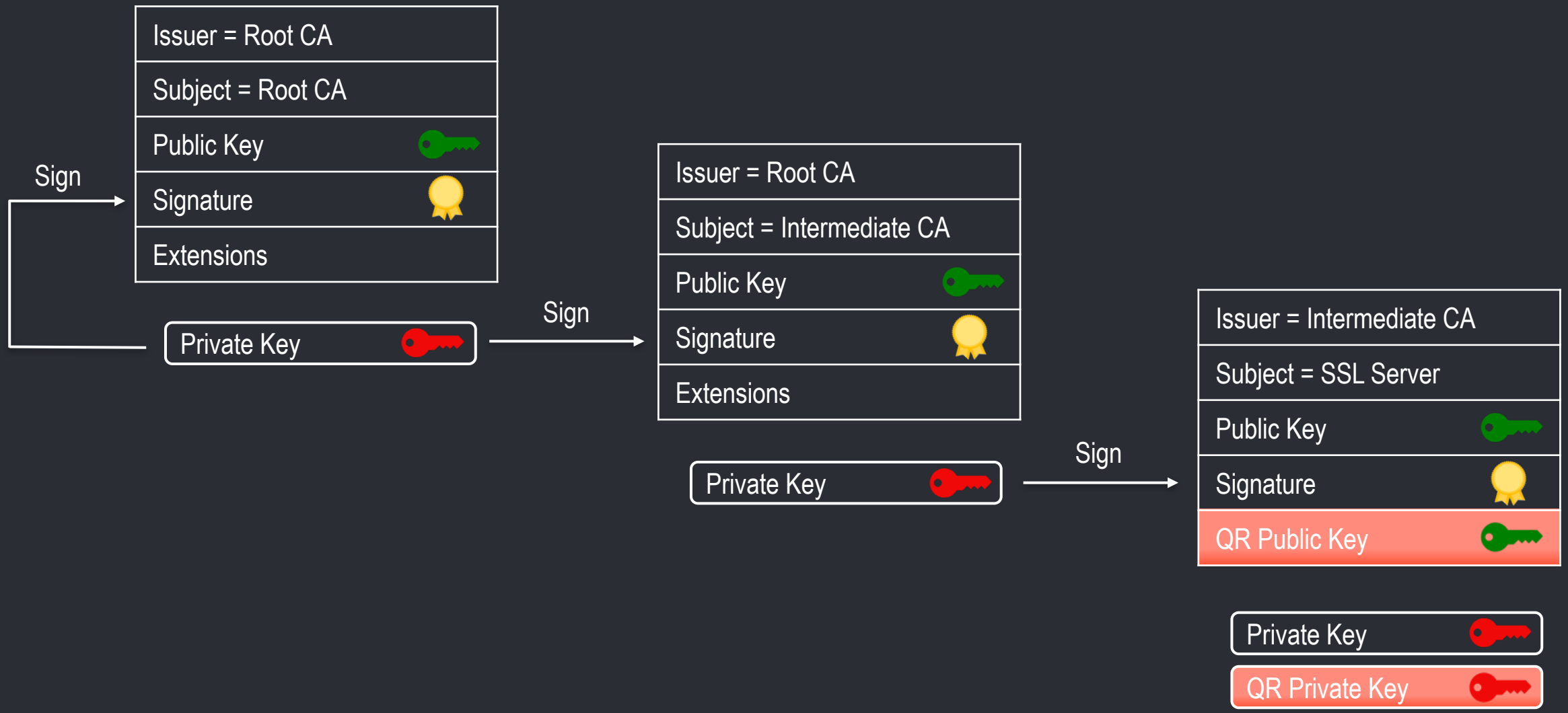
Phase One Enterprise Infrastructure



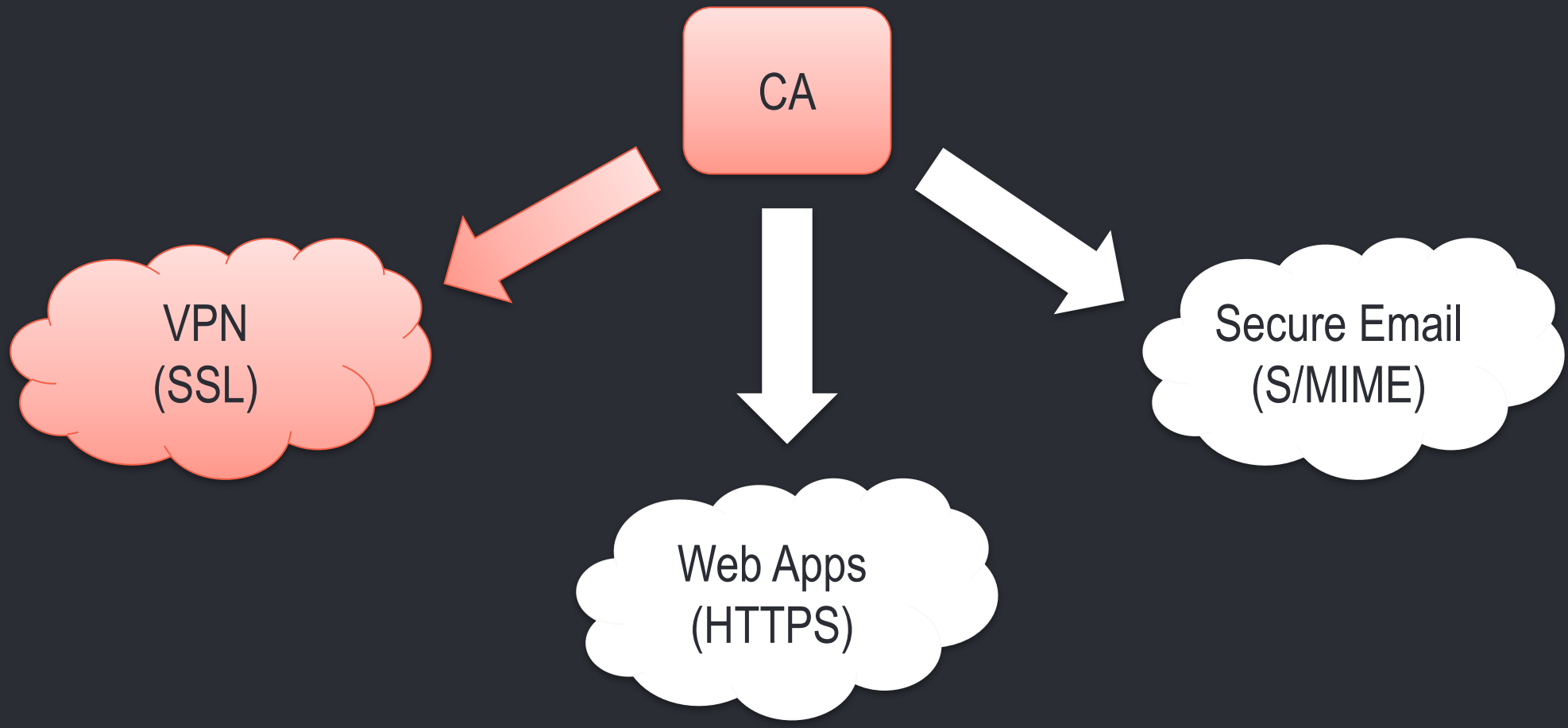
Phase One Certificate



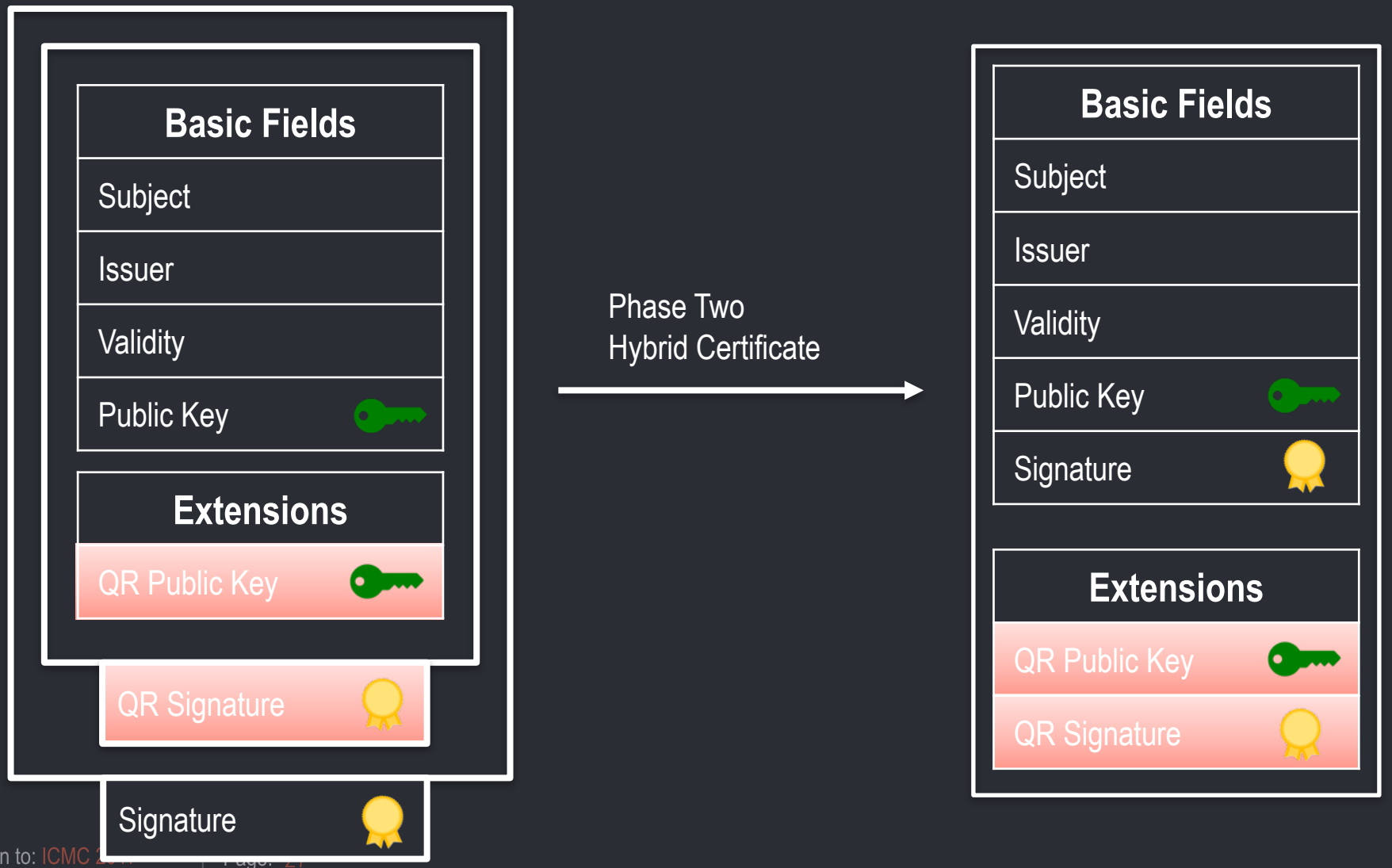
Phase One X509 Certificate Chain



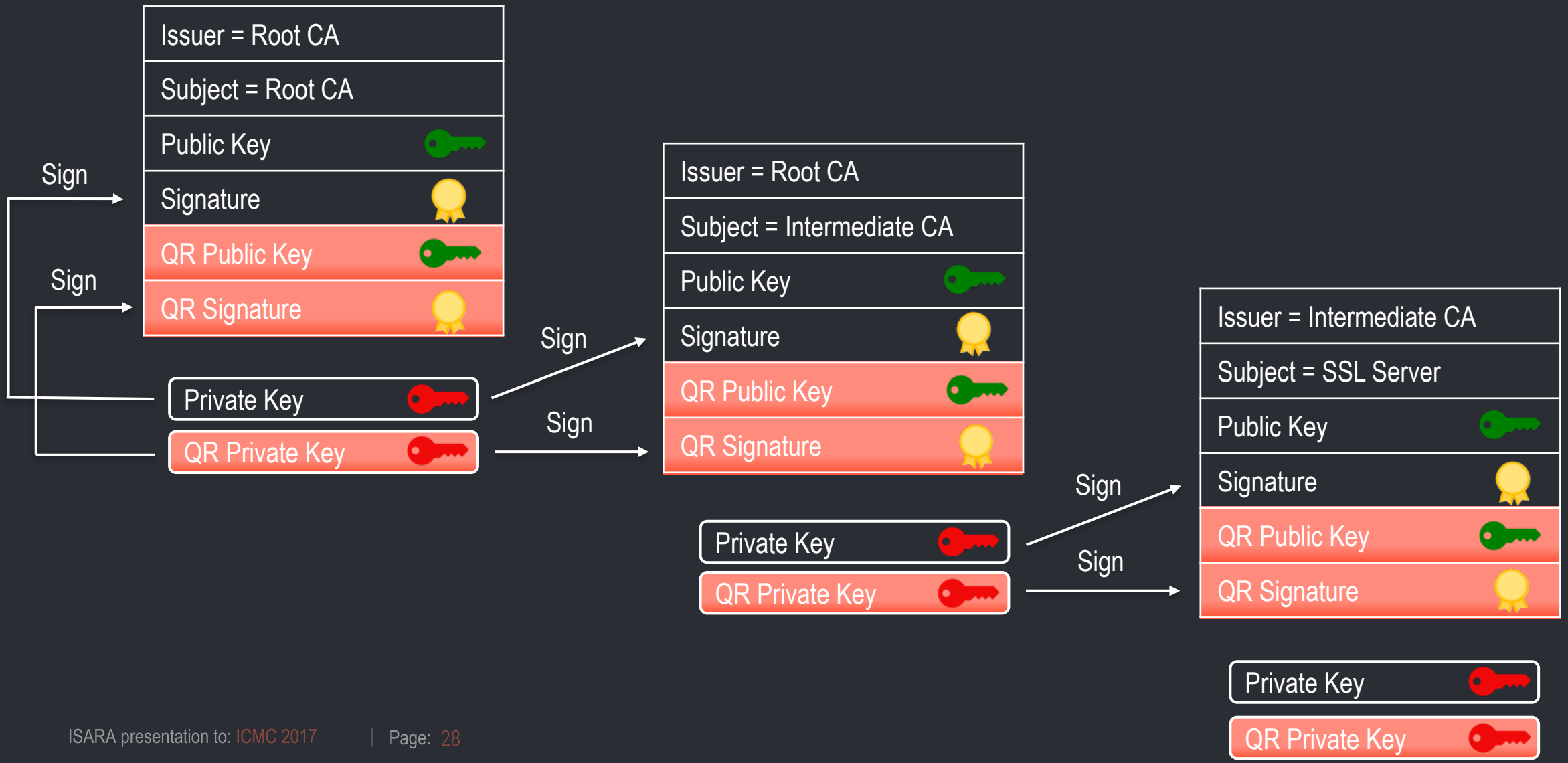
Phase Two Enterprise Infrastructure



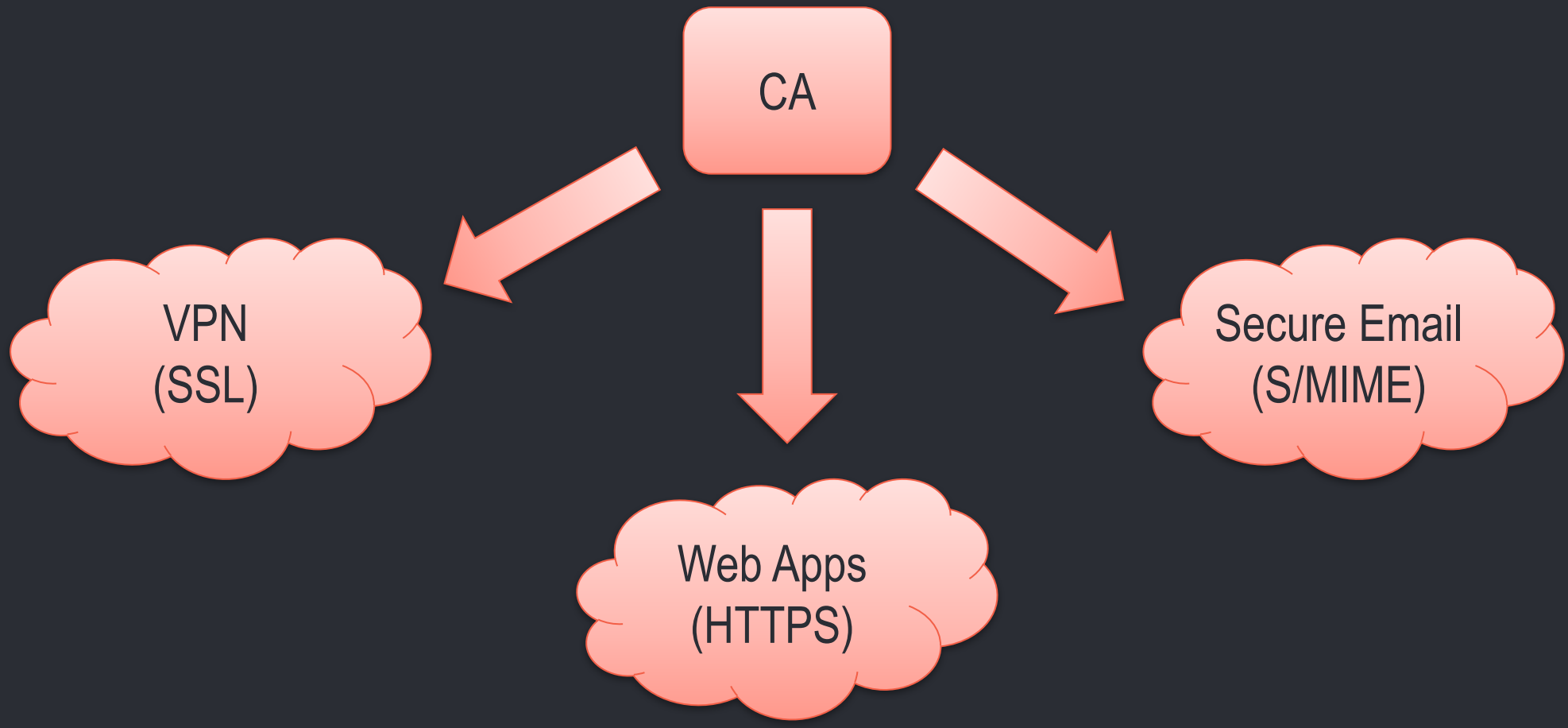
Phase Two Certificate



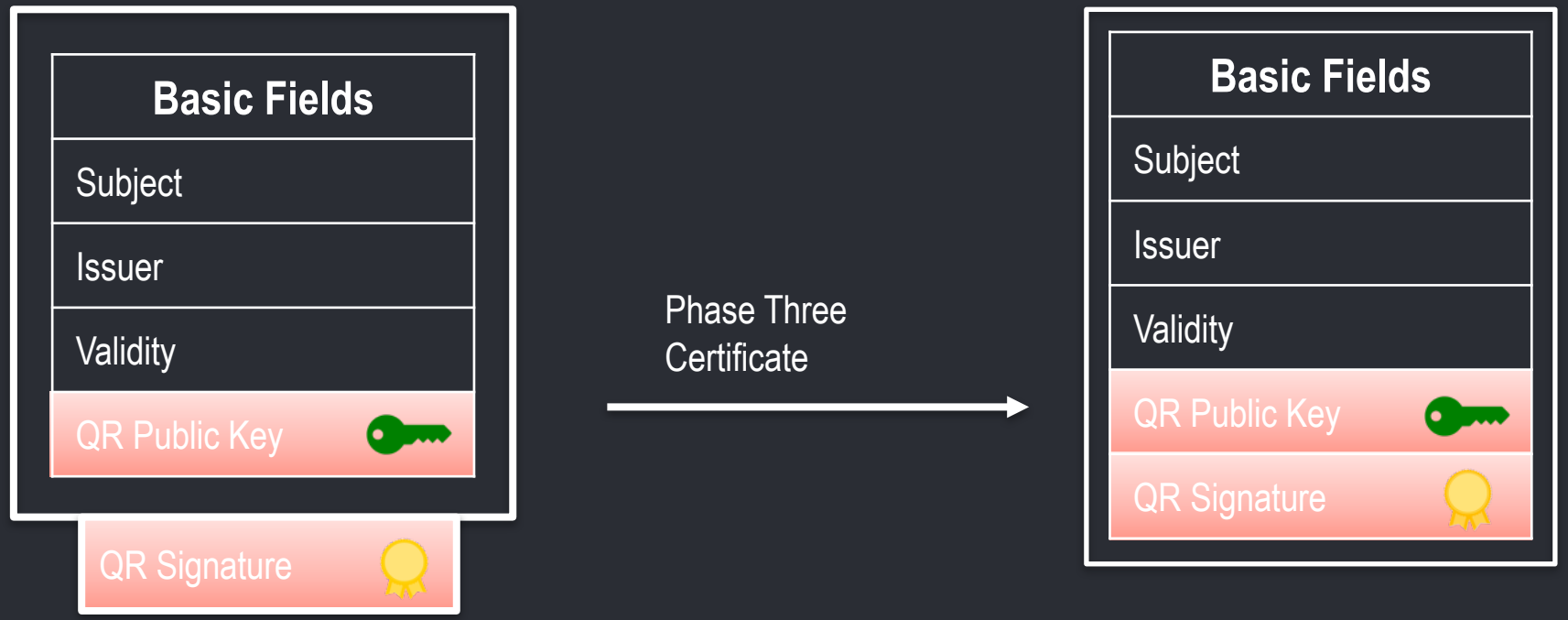
Phase Two X509 Certificate Chain



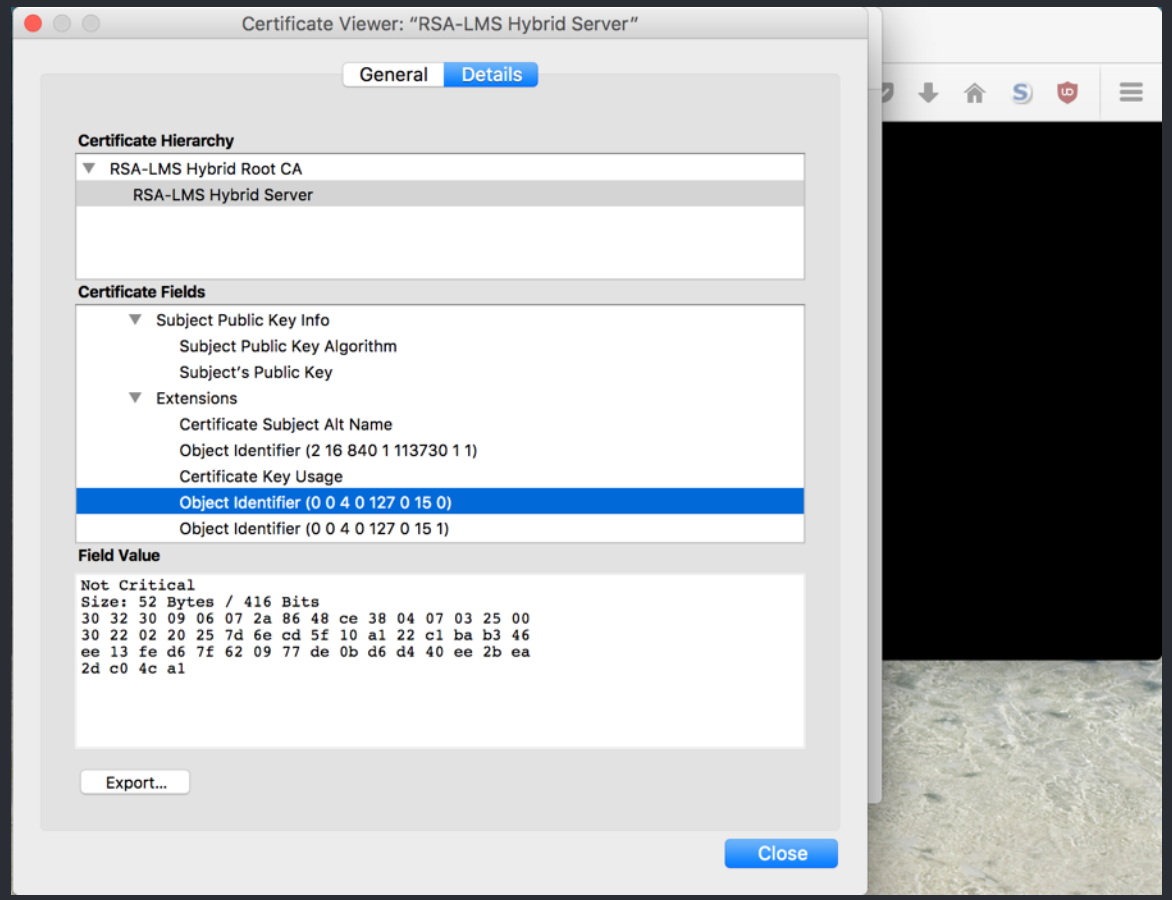
Phase Three Enterprise Infrastructure

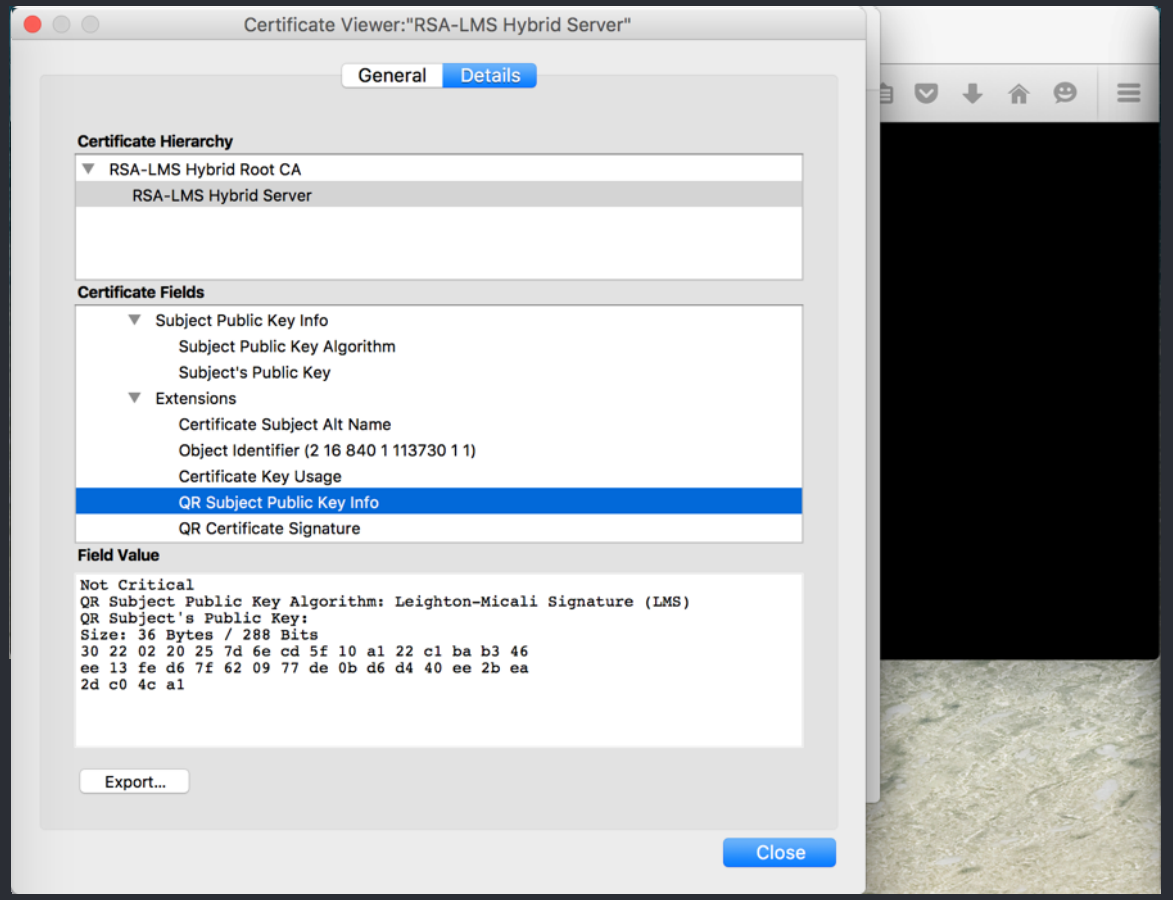


Phase Three Certificate



Example


Certificate Viewer: "RSA-LMS Hybrid Server"
General
Details
Certificate Hierarchy
RSA-LMS Hybrid Root CA
RSA-LMS Hybrid Server
Certificate Fields
Subject Public Key Info
Subject Public Key Algorithm
Subject's Public Key
Extensions
Certificate Subject Alt Name
Object Identifier (2 16 840 1 113730 1 1)
Certificate Key Usage
Object Identifier (0 0 4 0 127 0 15 0)
Object Identifier (0 0 4 0 127 0 15 1)
Field Value
Not Critical
Size: 52 Bytes / 416 Bits
30 32 30 09 06 07 2a 86 48 ce 38 04 07 03 25 00
30 22 02 20 25 7d 6e cd 5f 10 a1 22 c1 ba b3 46
ee 13 fe d6 7f 62 09 77 de 0b d6 d4 40 ee 2b ea
2d c0 4c a1
Export...
Close


Certificate Viewer:"RSA-LMS Hybrid Server"
General
Details
Certificate Hierarchy
RSA-LMS Hybrid Root CA
RSA-LMS Hybrid Server
Certificate Fields
Subject Public Key Info
Subject Public Key Algorithm
Subject's Public Key
Extensions
Certificate Subject Alt Name
Object Identifier (2 16 840 1 113730 1 1)
Certificate Key Usage
QR Subject Public Key Info
QR Certificate Signature
Field Value
Not Critical
QR Subject Public Key Algorithm: Leighton-Micali Signature (LMS)
QR Subject's Public Key:
Size: 36 Bytes / 288 Bits
30 22 02 20 25 7d 6e cd 5f 10 a1 22 c1 ba b3 46
ee 13 fe d6 7f 62 09 77 de 0b d6 d4 40 ee 2b ea
2d c0 4c a1
Export...
Close

Quantum Safe Cryptography

Options for PKI

Hash-Based Signatures

Well studied and trusted

Fast operations and compact public key

But…

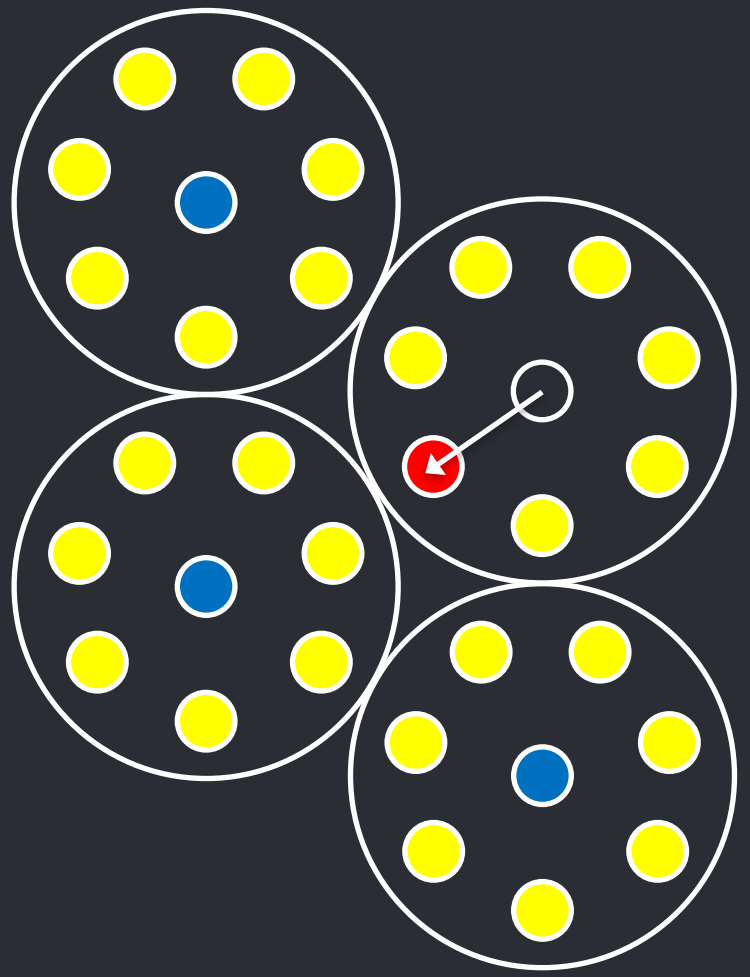
- State management
- Private key sizes

Code-Based Crypto

McEliece key transport with Goppa codes still well trusted

But…

- Focus on key transport, not signature schemes
- Key sizes!
- Constructions do exist focused on Niederreiter variant

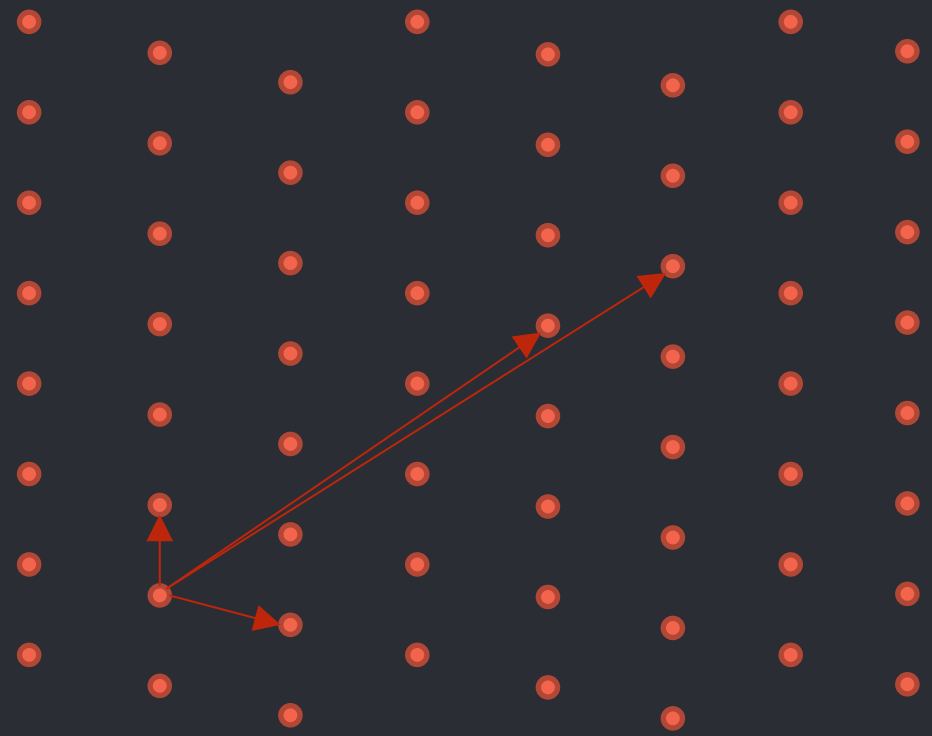


Lattice Cryptography

Lattice based cryptography offers very fast quantum resistant schemes with excellent key sizes, in the Ring variants

But…

- Signature space is much less mature
- BLISS and pqNTRUsign
- TESLA

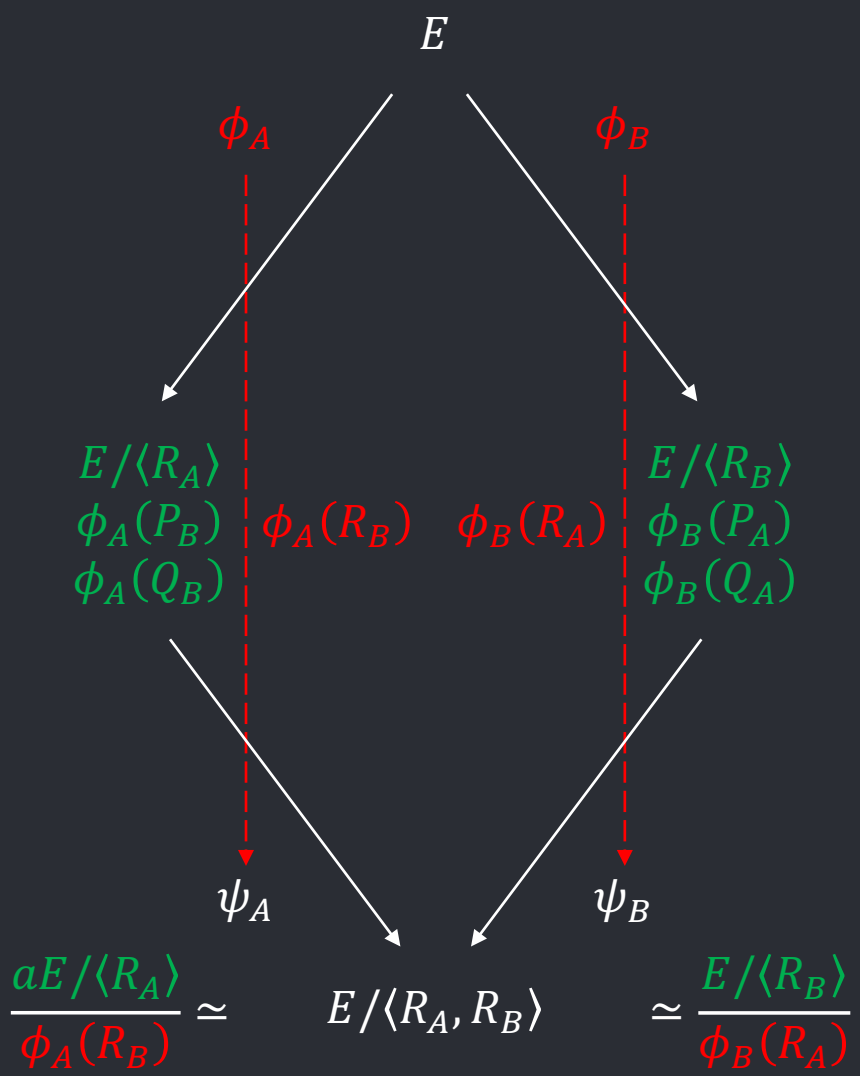


Isogeny-Based Cryptography

Offers crypto based off different hard problems

But…

- No efficient signature schemes available
- Still based off modified Zero Knowledge proof constructions
- Quite slow



Multivariate Public Key Cryptography

Offers a variety of digital signature options such as Rainbow, UOV, HFEv-

Work has been done on getting it to work on smart cards

But…

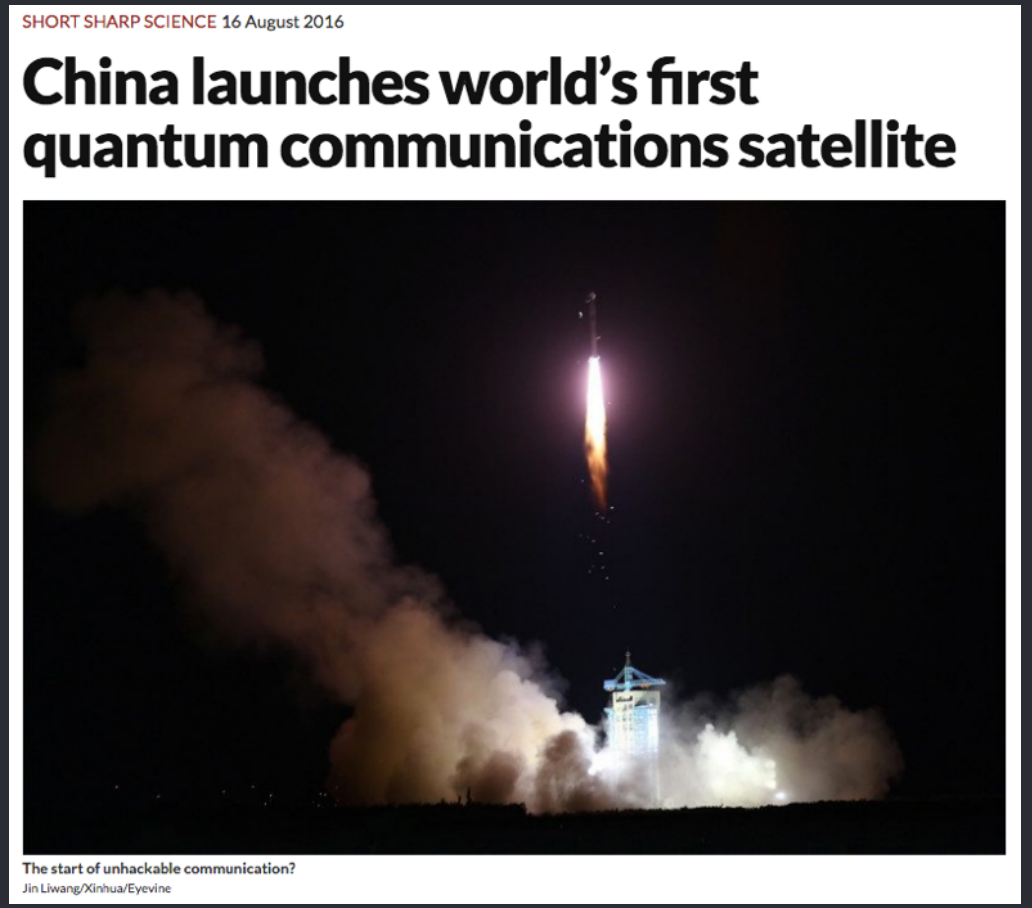
- Popularity more geographically centred
- Public key size not as competitive as Hash Based
- Fewer academic publications

Quantum Key Distribution

Promises a physics based approach to Quantum Security

But…

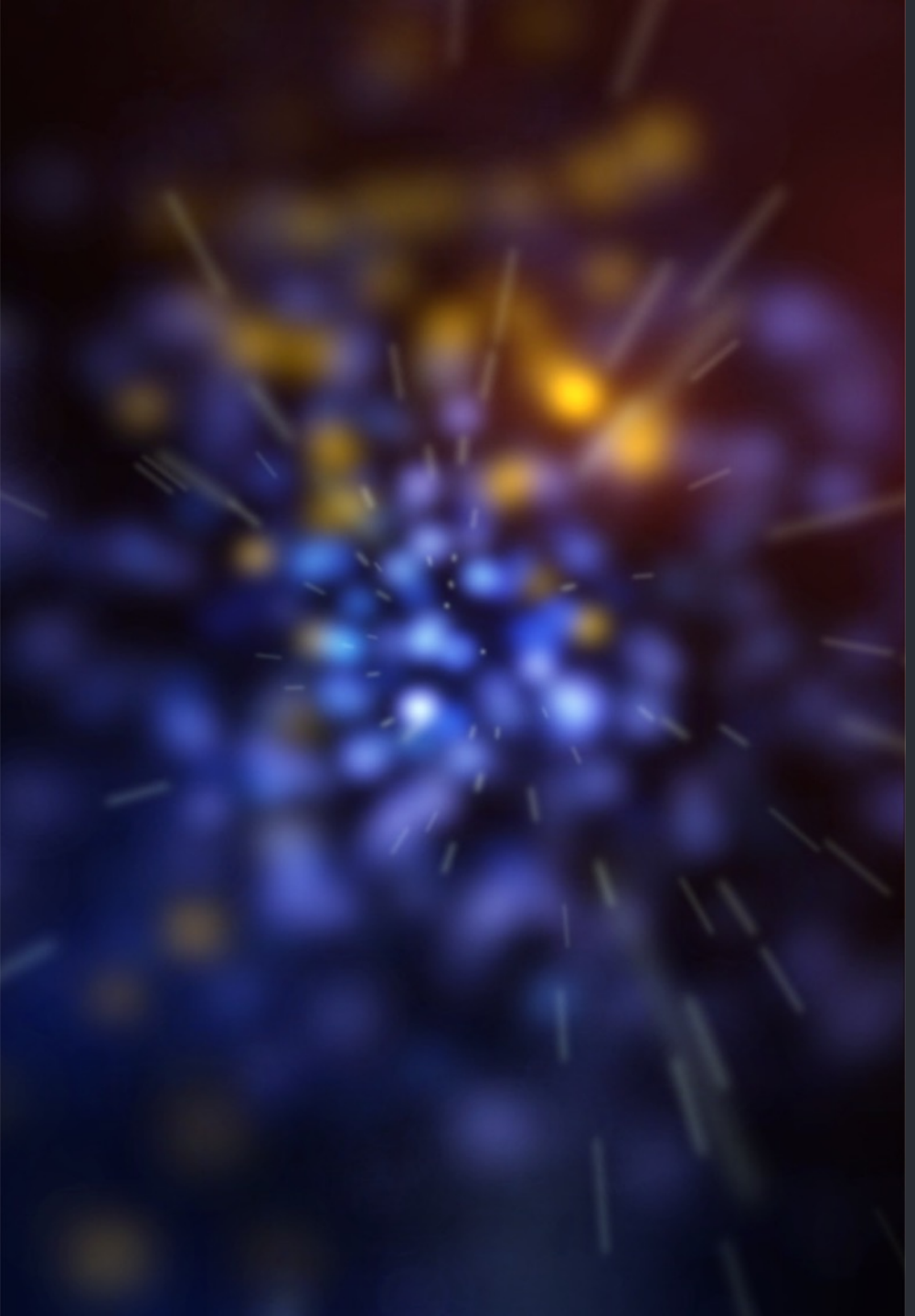
- Focus is key distribution
- Requires a Quantum Resistant algorithm, from the previous slides, to authenticate the exchange
- Physical limitations



SHORT SHARP SCIENCE 16 August 2016

China launches world's first quantum communications satellite

The start of unhackable communication?
Jin Liwang/Xinhua/Eyevine



Quantum Computing

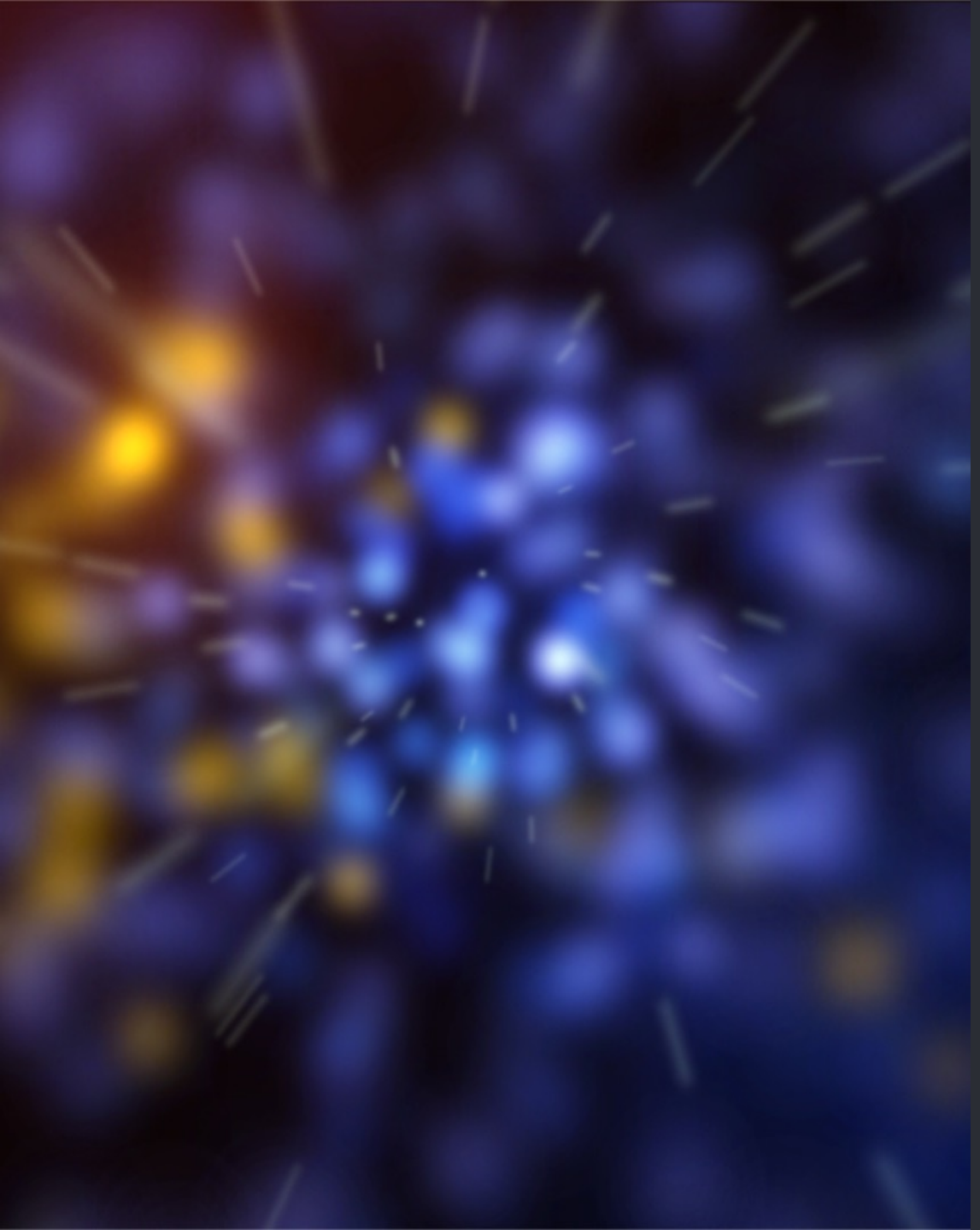
Conclusions and Recommendations

When Does The Clock Run Out?

While this seems enormous, its like drinking the ocean…

We do have viable solutions today and more are coming.

Start planning your transition today!



Thank you!

www.isara.com

mike@isara.com