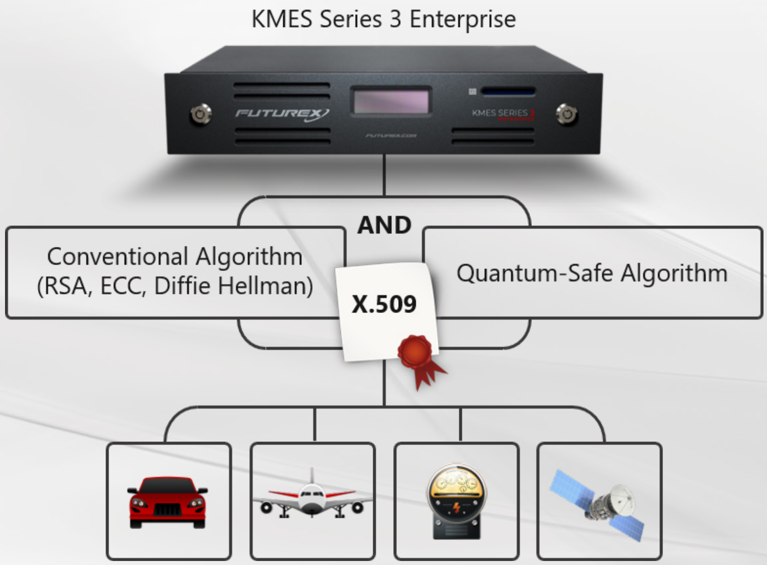
FUTUREX

Quantum-Safe Solutions

Futurex's Quantum-Safe Hybrid Certificate Authority Solution

An Original Solution to Counteract the Threat of Quantum Computers

With the rise of quantum computing on the horizon, society faces a threat that will break public key cryptography as we know it. Futurex has developed a quantum-safe hybrid certificate authority solution, delivered as a turnkey, HSM-integrated appliance or cloud service. With this technology, you can simultaneously issue certificates to IoT devices or any other digital object with both classical and quantum-safe algorithms. After integrating Futurex's KMES Series 3 with quantum-safe functionality into your cryptographic ecosystem, as soon as your organization is ready, you can make the post-quantum shift without issuing new certificates.



KMES Series 3 Enterprise

AND

Conventional Algorithm (RSA, ECC, Diffie Hellman)

X.509

Quantum-Safe Algorithm

A Hybrid Solution

Why create a hybrid solution instead of a new quantum-safe solution? Futurex wants to simplify the process for its customers. With a hybrid certificate authority solution that combines current cryptographic standards with quantum-safe technology powered by ISARA Corporation, customers won't need to issue any new certificates. Instead, the certificates can be converted to use quantum-safe algorithms, so when quantum computing becomes widespread and risks impacting public key algorithms like RSA, ECC, and Diffie-Hellman, you'll be ready.

The Future of Computing

In today's computing landscapes, we mainly have classical computers that process bits of information existing in binary. As technology evolves, we are beginning to see tech giants and even nation-states working to create super computers known as quantum computers.

Quantum computers differ from the current classical model through their ability to analyze data existing in more than one state at a time. Quantum computers use quantum bits, also known as qubits, enabling them to solve complex problems exponentially quicker than classical computers.

Due to their highly efficient processing capabilities, quantum computers will be powerful enough to render public key cryptographic algorithms useless. Although quantum computers are not yet widespread, it will only be a matter of years before organizations everywhere will be relying on quantum computing.

Partnering with ISARA Corporation

In order to implement this quantum-safe solution, Futurex is partnering with ISARA Corporation. ISARA is a security solutions provider that specializes in quantum-safe technology. They focus on helping organizations migrate from standard cryptographic systems to ones equipped to handle attacks from quantum computers.

Together with ISARA's expertise in quantum-safe cryptography, Futurex has developed a post-quantum hybrid certificate authority solution that will utilize both classical and quantum algorithms to take IoT manufacturers into the next generation of security.

ISARA + FUTUREX

How to Implement Your Quantum-Safe Solution

The implementation process for the post-quantum hybrid certificate authority solution is straightforward. Because this solution combines both standard cryptographic measures as well as the new quantum-safe method, hybrid certificates can be issued the same way as always, using X.509 format certificates. This is beneficial to your organization because the existing processes remain the same and migration to a new system is not necessary.

FUTUREX

Benefits of a Quantum-Safe Hybrid Solution

- ✓ No need to migrate from current certificate management system
- ✓ Mitigates risks presented by quantum computing
- ✓ Simultaneously sign with classical and quantum-safe algorithms
- ✓ Shift to quantum-safe cryptography at your own pace
- ✓ Partner with a trustworthy leading provider in quantum-safe solutions

Key Management

All cryptographic operations performed as part of Futurex's quantum-safe hybrid certificate authority solution take place within the secure, FIPS 140-2 Level 3 validated boundary of the Key Management Enterprise Server (KMES) Series 3. Quantum-safe functionality is offered as a license upgrade to the device and can be enabled for hardware already deployed in the field.

Time Frame

Industry experts predict that quantum computers will be widespread in the next five to ten years. However, prototypes of quantum computer have already been developed. This indicates it will only be a few years before we see significant strides in the industry. That is why it is better to be prepared ahead of time, before the inevitable threat strikes, especially for long-lifespan devices such as satellites and automobiles.