

# Quantum Entropy-as-a-Service (QEaaS)



## The problem

In an increasingly connected world, tens of billions of IoT devices will soon be part of our daily lives, offering immense convenience. However, with each new connection comes a potential security risk, as these devices often lack the computational power necessary for secure cryptography. This opens the door to data leaks and potential breaches of our critical infrastructure systems.

This problem led to the idea of offloading tasks like the generation of randomness for cryptographic keys, giving rise to the concept of Entropy-as-a-Service, where a trusted source produces and distributes randomness to all devices that need it. At Quantum Dice, inspired by the original Entropy-as-a-Service framework developed by NIST, we have upgraded this concept by leveraging our proprietary DISC™-protected Quantum Random Number Generators (QRNGs) to create Quantum Entropy-as-a-Service (QEaaS).

## Introducing Quantum Dice's QEaaS

QEaaS provides a network-connected, high-quality source of randomness essential for cryptographic applications, such as the generation of secure encryption keys, certificates and digital signatures. By distributing entropy across remote servers, our solution ensures that even the most resource-limited devices and cloud instances receive the secure, certified randomness they need to implement all their cryptographic functions.

## Commercial benefits



**Enhanced security:** Our QEaaS solution improves security by providing high-quality random numbers for cryptographic operations, making it harder for adversaries to compromise communication channels and gain unauthorised access to sensitive data.



**Quantum-resistant security:** As quantum computing threatens traditional encryption, QEaaS provides reliably high-quality entropy for stronger encryption keys, future-proofing the security of IoT devices and cloud systems.



**Certifiable entropy:** At the core of our QEaaS solution is our patented source-device independent self-certification (DISC™) protocol, enabling real-time quantification of entropy quality and enhancing the audit trail recommended by NIST.



**Scalability:** QEaaS allows for efficient distribution of high-quality entropy to large numbers of devices, making it a scalable solution for the ever-growing IoT and cloud ecosystems.



**Easy integration:** Thanks to an easy-to-use API and SDK, QEaaS can be easily integrated into existing IoT and cloud infrastructure, enabling seamless adoption and deployment without the need for significant changes to the existing systems.



**Cost effectiveness:** The efficient distribution of entropy can help reduce the cost of implementing individual entropy generation solutions for each device or cloud instance.

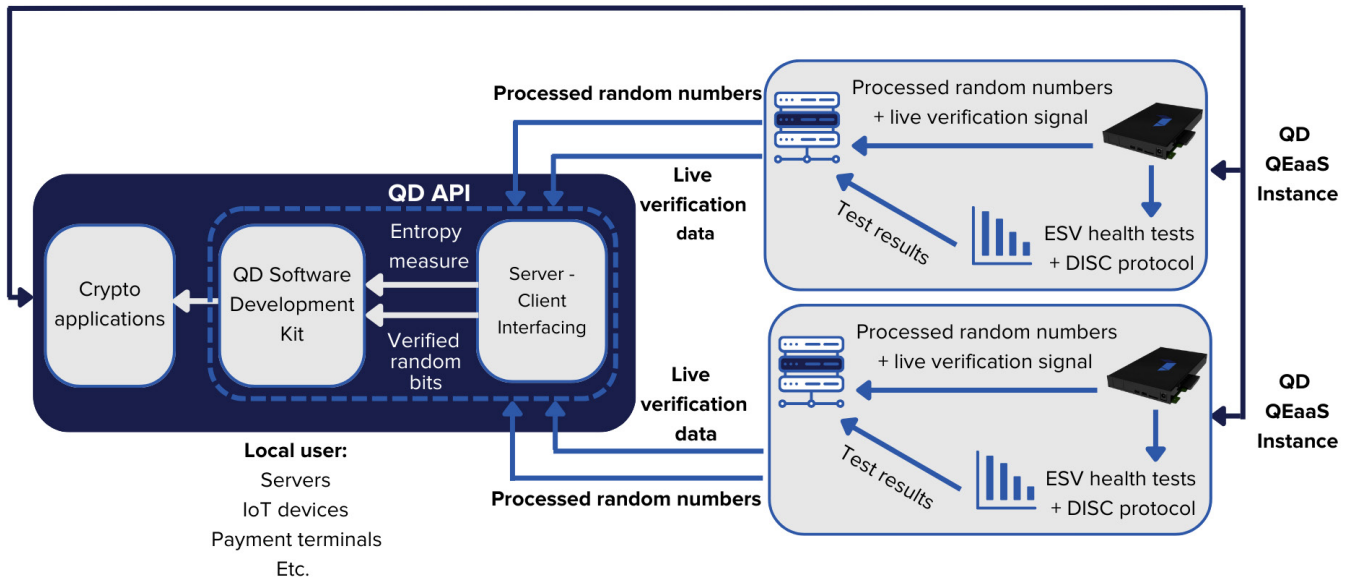
## Examples of use cases

QEaaS can enhance security in a wide range of cryptographic applications, including:

<b>Encryption and key management</b>	<ul style="list-style-type: none"><li>• Encryption key generation: Provides stronger encryption keys for secure communications.</li><li>• Certificate generation: Ensures the integrity and authenticity of digital certificates.</li></ul>
<b>Network security</b>	<ul style="list-style-type: none"><li>• Virtual Private Networks (VPNs): Strengthens the encryption used to secure VPN connections.</li><li>• Software-Defined Wide Area Networks (SD-WAN): Safeguards network traffic with secure, high-quality entropy for encryption.</li></ul>
<b>App development</b>	<ul style="list-style-type: none"><li>• Secure app development: Supports the development of cryptographically secure mobile and web applications.</li></ul>

## How QEaaS works

Inspired by the original concept developed by NIST, our QEaaS implementation uses QD's QRNG devices to generate certified, fully processed random numbers with continuous monitoring of quantum entropy levels.



QEaaS can be integrated into various programming environments, allowing developers to easily access high-quality randomness for cryptographic functions. By connecting to the QEaaS server, you can use Quantum Dice's randomness in Python, C, and C++ applications, as well as with libraries like NumPy. Additionally, QEaaS can be directly integrated into the Linux OS randomness pool.

## Try QEaaS for free!

Sign up to a four-week free trial to see how QEaaS can enhance your cryptographic applications.

[info@quantum-dice.com](mailto:info@quantum-dice.com) | [www.quantum-dice.com](http://www.quantum-dice.com)