Redefining Security

Use Case: Central Bank

Digital Trust Platform

Digital Money Generation for Central Bank

Customer: Central Bank

Industry: Banking / Logistics

Country: Confidential

Business need

Development of digital fiat currency for central bank, with secure architecture design & implementation and crypto customisation & agility

Solution

Digital bank note generation platform producing authenticated validated digital tokens with assigned monetary value

Results

Credibility of innovative solution based on Swiss trust and security

Business need

A central bank wanted to test the issuance and use of digital tokens of the country's currency via a digital money platform. This pilot process, the world first at an international level, consisted of a test with thousands of mobile phone users of the national telecommunications provider.

The platform allowed payment operations at merchants and mobile networks, as well as transfers from person to person among registered users. To use the platform, users must download the mobile application, access the digital wallet, register and make the first charge to create the digital wallet. The mechanism is available for both smartphones and non-smartphones.

To be a credible substitute to physical money, a fiat currency must have the same feature as its counterpart among its users: trust. This means that the digital tokens issued by the central bank must offer the same security. It is important to specify that this is not a new currency but a currency that has a digital support instead of a physical support.

In order to guarantee total security to end users, our customer needed outstanding randomness, key management and authentication capabilities.

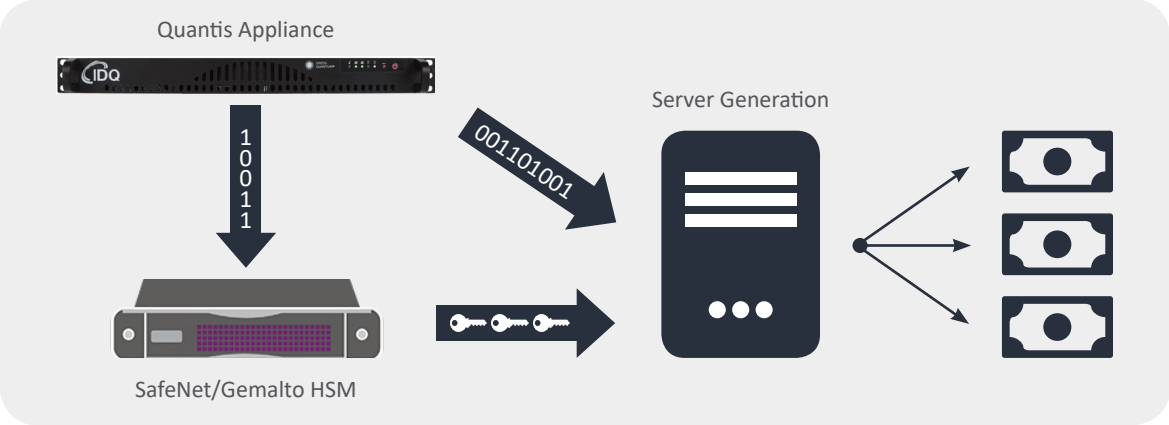
ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com

Solution

The customer mandated IDQ to develop the digital money generation platform for the solution. IDQ's Quantis Appliance served as a basis to securely generate and deliver high-quality random numbers, cryptographic keys and secure cryptographic signatures.

The Quantis Appliance issued unique IDs to the tokens holding monetary value. These monetary tokens were then signed by SafeNet/Gemalto HSM to validate that they were issued by the central bank. In order to strengthen digital signatures, IDQ and a leading academic partner co-studied and approved bespoke (non NIST) elliptic curves. IDQ then set up the elliptic curves on the HSM to use them into a private/public key signature scheme. Additionally, in order to provide higher security of token generation and signature, the Quantis QRNG Appliance fed extra entropy into the HSM. The whole secure cryptographic architecture and database were built by IDQ.

Finally, the digital tokens were passed to commercial banks which then made them available for users to perform transactions via the mobile operator.



Results

The Digital Trust Platform benefits from IDQ's Swiss trust and security based on its patented technologies.

In addition, digital money has multiple advantages over physical money. Central banks and regulatory authorities eliminated printing costs and cut into logistics expenses, such as distribution in the whole territory and security for transport, while simultaneously improving security and transparency. Traceability of payments is another advantage which makes it possible to effectively combat money laundering and different forms of fiscal and social fraud.

Finally, the Digital Trust Platform gives access to financial transactions in developing countries where much of the population lacks access to banking infrastructure.

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com