Redefining Security

Use Case: Government

Securing Data Transfer for Elections

Ethernet Encryption with Quantum Key Distribution

Customer Name: Republic and State of Geneva

Industry: Government

Country: Switzerland

REPUBLIC AND STATE OF GENEVA

POST TENEBRAS LUX

Business need

Ensure maximum security to protect the data authenticity and integrity as well as guarantee the axiom of One Citizen One Vote.

Solution

Layer 2 encryption combined with Quantum Key Distribution (QKD).

Results

Successful use of IDQ's Cerberis solution in every federal and cantonal election since 2007

Business need

Switzerland epitomised the concept of direct democracy. Citizens of Geneva are called on to vote multiple times every year, on anything from elections for the national and cantonal parliaments to local referendums.

The challenge for the Geneva government was to ensure maximum security to protect the data authenticity and integrity, while at the same time managing the process efficiently. They also had to guarantee the axiom of One Citizen One Vote.

Solution

On 21st October 2007 the Geneva government implemented for the first time IDQ's hybrid encryption solution, using state of the art Layer 2 encryption combined with Quantum Key Distribution (QKD). The Cerberis solution secures a point-to-point Gigabit Ethernet link used to send ballot information for the federal and cantonal elections from the central ballot counting station to the Geneva government data center.

Typically sealed ballot boxes are brought from the polling stations to the central counting station where they are opened and counted alongside the already delivered mail votes. Counting is done manually according to strict procedural norms. Geneva law dictates that any citizen can attend the ballot counting procedure to ensure the authenticity of the results. However in the modern world this principle has been reinterpreted- the Electoral Commission carries out close

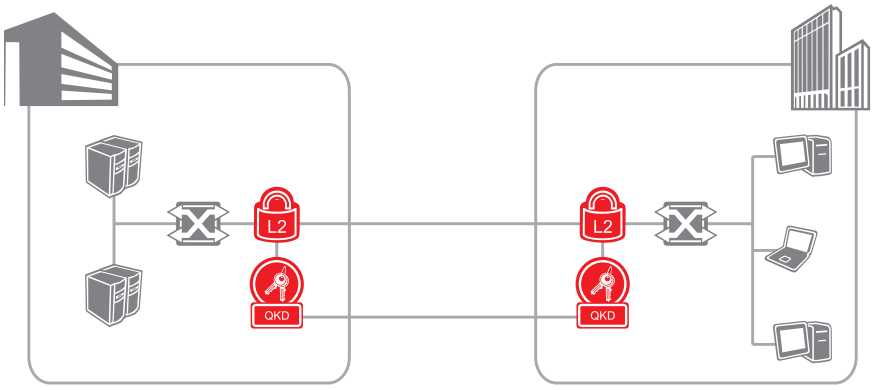
ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com

surveillance of the counting and the data entry, and the authenticity and integrity of any subsequent data transfer is then guaranteed by the highest level of encryption.

IDQ's Cerberis solution combines leading Layer 2 encryption techniques, based on 256-bit AES cipher (Advanced Encryption Standard), with the extra protection of Quantum Key Distribution. QKD derives its security from the proven principles of quantum physics- namely, that the generation of the quantum key is truly random, and that any interruption or eavesdropping of the data will perturb the system and can thus be detected.

Unlike "conventional" encryption based on mathematical algorithms, QKD will not be compromised by the continual increase in computing power or mathematical progress. It thus ensures true future-proofed security of key distribution.

Additionally, thanks to IDQ's Dual-Key agreement where the encryption key used by the AES encryptor is combined with the quantum key and changed up to 60 times per hour in both directions, two-fold key security is provided and renewed in real-time.



Results

The Geneva government has successfully used IDQ's Cerberis solution in every federal and cantonal election since 2007, as a key element in the integrity and security of the voting in the Canton of Geneva.

> *"We have to provide optimal security conditions for the counting of ballots... Quantum cryptography has the ability to verify that the data has not been corrupted in transit between entry & storage."*
>
> Robert Hensler,
> Ex State Chancellor
> Geneva

> *"IDQ's hybrid encryption solution using Quantum Key Distribution has been working reliably and faultlessly for many years to protect data integrity in Geneva elections. The system was easy to install and is very easy to manage."*
>
> David Crisinel,
> Head of Network Infrastructure
> Geneva

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