IDQ
FROM VISION TO TECHNOLOGY

USER CASE

REPUBLIC AND STATE OF GENEVA

POST TENEBRAS LUX

REDEFINING SECURITY

Geneva Government

Secure Data Transfer for Elections

Gigabit Ethernet Encryption with Quantum Key Distribution

"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 over 3 years to protect data integrity in Geneva elections "

David Crisinel, Head of Network Infrastructure, Geneva

The Challenge

Switzerland epitomises 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 is to ensure maximum security to protect the data authenticity and integrity, while at the same time managing the process efficiently. They also have to guarantee the axiom of One Citizen One Vote.

The 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.

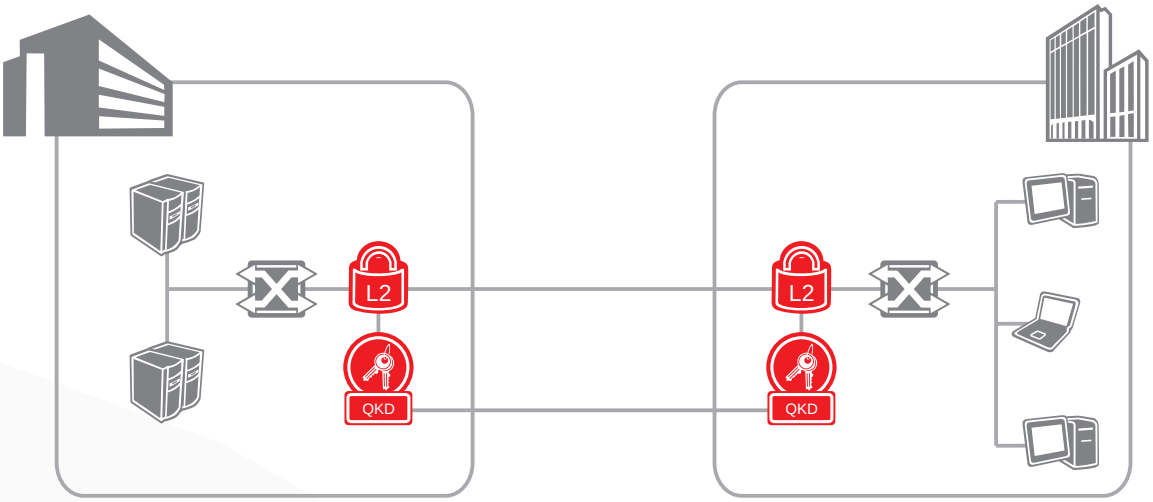
Typically sealed ballot boxes are brought from the polling stations to the central counting station where they are opened and counted alongside the already delivered mail votes. Counting is done manually according to strict procedural norms. Geneva law dictates that any citizen can attend the ballot 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 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.

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

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.



The Results

The Geneva government has successfully used IDQ's Cerberis solution in every federal and cantonal election since 2007. According to David Crisinel, responsible for the canton's network infrastructure, “IDQ's hybrid encryption solution using Quantum Key Distribution has been working reliably and faultlessly for over three years to protect data integrity in Geneva elections. The system was easy to install and is very easy to manage. ”

The Quantum Roll-Out

In addition to federal or cantonal parliamentary elections, Geneva citizens are also called on to vote in local initiatives, or referendums, between 4-6 times every year. In order to encourage maximum voter participation in today's busy global environment, the government introduced internet voting for the referendums in 2003 (although it is not yet used for parliament elections).

In order to e-vote, each citizen receives a voting card by post. This card bears a PIN code which allows the validation of the internet ballot. For the system to be secure, it is essential that the PIN is unique, and cannot be reproduced fraudulently.

Thanks to the ongoing success of the original Cerberis installation, the Geneva government once again turned to quantum physics and IDQ to secure their internet voting. In 2009 they implemented IDQ's true random number generator, Quantis, to produce the unique PIN for each citizen, ensuring that the PINS are unique, authentic and anonymous. In addition, the encryption keys for each internet voting session are generated by Quantis on the basis of the user's unique PIN.

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