

Protecting governmental communications is mission critical, especially when those communications cross borders and traverse a range of networking technologies. The Romanian Ministry of Foreign Affairs (MoFA) turned to Certes Networks' CryptoFlow solutions for a flexible, scalable data communications security solution to protect essential networked applications.

## Customer Situation

As part of the preparation for Romania's integration into the Schengen Area by funding from the Schengen Facility program and the External Borders Fund, the Romanian Ministry of Foreign Affairs had been installing a complex set of systems and secured data network communications for delivering smooth operations for the Romanian consulates network, as per European regulations. These systems are classified into two main categories:

1. National Visa Information System (SNIV), whereby visas are issued to all consular offices;
2. Communication systems to ensure protection for consular offices and consular staff (alarm, video surveillance).

Security systems are designed for highly scalable, efficient and secure consular activity, which includes also the process of issuing visas. Security management systems were installed inside the Romanian MoFA central operational sites. This was necessary in order to support the overall Romanian MoFA security administration, a task that can only be performed by skilled personnel accredited by the MoFA for access to classified information.

### CASE STUDY

# The Romanian

Ministry of Foreign Affairs protects essential networked applications with Certes Networks' CryptoFlow solutions.



ROMÂNIA  
Ministerul Afacerilor Externe

## Solution Requirements

The RFP issued by the Romanian MoFA was mandating a turnkey security solution that could be customized by the MoFA technical specialists as required for securing end-to-end data in transit within the MoFA network, including the national Layer 2 core network infrastructure and the external Layer 3 consular network. They also required a flexible data communications protection solution that could adjust to future changes in the network infrastructure.

The RFP was also enforcing the implementation of a centralized system for managing the entire life-cycle of both cryptographic keys and network-based policy enforcers, capable of real-time monitoring and troubleshooting. Along with the ability to generate, a report for auditors to prove their inter-consular data is secured, thus ensuring the necessary conditions for solving real-time operational issues and to comply with audit requirements.

The communications security solution offered needed to avoid disruptive architecture changes in the network infrastructure, support AES 256-bit encryption at OSI Layers 2, 3, 4 and maintain the performance of high availability applications running on the network. Most importantly, data security administration tools needed to be easy to use and completely de-coupled from the networking administration tools, allowing the separation of duties enforcement across their networking and security teams.

During the RFP stage, most vendors could meet only a few of the requirements. Certes Networks offered a single platform with the ability to adjust to future changes being considered for the MoFA network infrastructure, customization and de-coupled management. Certes Networks' CryptoFlow Net solution offered all of the capabilities and flexibility required for this deployment. With its transparent nature and capability of being deployed into either Layer 2 or Layer 3 networks, it was a natural fit.

## Deployment

Communications and security systems have been fully operational in all 100+ consular offices since 2010, the same year as the RFP was initiated and the project was awarded.

The turnkey data communications security solution from Certes was designed for flexible and phased deployment. It allowed redundant encrypted communication lines per each consular office plus complete central management of keys and security policies, while different teams were managing the roll-out of new networking gear and new hardware encryption appliances.

## Results

Five years after the first successful deployment, the Romanian MoFA requested another RFP recommending new Certes Networks security solutions, to support network scaling and increased throughput needs.

MoFA now has almost 400 active Certes CryptoFlow Enforcement Points running in its network, providing throughput needs up to 10 Gbps. Certes Networks'

CryptoFlow Creator management systems equipped with HSM cards and Custom Base Key Encryption features allow MoFA to have a robust and customized encryption setup, providing a significantly higher level of confidence that encryption keys cannot be compromised and data communications are fully protected in all instances. MoFA has also started the deployment of the new CryptoFlow App solution provided by Certes, to meet its new requirements for mobile endpoint security. CryptoFlow App is based on the exact same core value propositions as the successfully deployed CryptoFlow Net solution, augmented with the ability to provide application-aware and user-aware segmentation of applications on virtual and physical networks. CryptoFlow App delivers end-to-end protection based on role-based access controls, enabling MoFA to use its Identity and Access Management services in conjunction with per-user and per-application policy enforcement for each mobile endpoint.



*When activating encryption services, MoFA had no hit on its network applications performance. Layer 4 encryption permitted real-time troubleshooting of its traffic data flows across the network whenever it had a networking issue or a new site roll-out.*



## About Certes Networks

Certes Networks is leading the Software-Defined Security revolution. The company's award-winning CryptoFlow® Solutions enable enterprise applications to be securely extended to any user on any device in any network, Cloud or virtual environment. Companies in 84 countries around the world rely on security solutions from Certes to protect access, accelerate application deployment, simplify network projects, reduce IT costs, contain breach threats, and shrink the enterprise attack surface. For more information, visit [certesnetworks.com](http://certesnetworks.com). For more information visit [CertesNetworks.com](http://CertesNetworks.com)

### Contact Certes Networks

300 Corporate Center Drive, Suite 140  
Pittsburgh, PA 15108 USA  
Tel: +1 (888) 833-1142  
Fax: +1 (412) 262-2574  
[CertesNetworks.com](http://CertesNetworks.com)

### North America Sales

[sales@certesnetworks.com](mailto:sales@certesnetworks.com)

### Government Sales

[sales@certesnetworks.com](mailto:sales@certesnetworks.com)

### Asia-Pacific Sales

[apac@certesnetworks.com](mailto:apac@certesnetworks.com)

### Central & Latin America Sales

[sales@certesnetworks.com](mailto:sales@certesnetworks.com)

### Europe, Middle East

and Africa Sales  
[emea@certesnetworks.com](mailto:emea@certesnetworks.com)