COMMUNICATIONS BETWEEN GOVERNMENT MINISTRIES

CONFIDENTIAL COMMUNICATIONS IN THE TOP ECHELONS OF GOVERNMENT

The efficiency of a modern state is based mainly on a performance-oriented flow of communication between governmental organisations, ministries and offices. Political actors and experts apply national strategies daily to help the top echelons of government form opinions. In terms of content, these efforts involve political agreements, arguments, analyses and research findings. They all have to be circulated with maximum secrecy so that, for example, they can be played as trump cards in negotiations at just the right moment.

By Urs Kürzi, Customer Segment Manager

In short, what is needed is the efficient networking of numerous governmental units with information and communication technology. At the same time, only a limited group of authorised users is granted access to classified information in the core network of the top echelons of government. How can this separation be reliably implemented?

The solution is to establish a cryptographically protected interministerial communication network. Depending on the form of government, it could include the president's residence, the ministry of the interior, other ministries and beyond to defence organisations. Ultra-secure encryption sets these participants apart as a high-security zone within ICT. A secure virtual network area of this kind is also known as logical topology. The advantage is that cryptographic connections between participants or cryptographic groups alone can be used to build self-contained, highly secure network areas without any change to the technical or physical structure of the network! In an interministerial network, information circulates at the highest level in encrypted form and is protected against all manner of attacks.

An interministerial communication network can be implemented in practically any common network technologies and protocols, for instance with Ethernet or IP. Access is made on-site using a network encryption unit from Crypto AG, typically via a fibre-optic connection.

Secure interfaces

In actual practice, further protected areas are needed in the ICT infrastructure of the government as a whole for it to be able to perform its duties. These zones have a lower level of security. Transitions into these zones with a lower classification are inevitable because government employees and indeed entire departments have to maintain direct contact with individuals and government offices across the hierarchical structure. These transitions into other zones are implemented using gateways, or data locks to be more precise. They work just like the locks in river navigation do. There is never an online connection from the source network to the target network. In the data lock, data first enters an interim storage area, which interrupts the physical connection with the source network and subsequently establishes the new physical connection into the target network. At no time is there a continuous connection between two networks (zones) with different classifications. As a result, the tough security requirements for warding off online attacks are met and the security policy for the corresponding zone is duly applied at the zone transition.

The three zones: high security, secure, trusted

In actual planning and projects at Crypto AG, an approach with three classes of security zones has proved effective. It strictly separates the data streams into sensitive and less sensitive information. The ministries of an e-government system are connected in a high-security zone. These data streams between various locations are encrypted using the Crypto AG process. This process entails the use of customer-specific algorithms that customers themselves can profile. The data is not visible to everyone, only to users and systems in the high-security zone.

High-security zone for ministries in the e-government system.

The next lower classified zone is the secure zone. The application servers with the business logic of the corresponding ministry are located at this level, along with the PCs of the clerks in charge. These PCs also warrant protection but to a much lesser degree than the actual core system for interministerial communications.

The third network zone – usually referred to as the trusted zone – is at the point of transition into a public

An encryption solution from Crypto AG guarantees that data within the interministerial communication network is exchanged confidentially and in a way that protects its integrity and authenticity. With cryptography, rules for cooperation and separation can also be put in place within networked government. In other words, a presidential office, the military secret service and the ministry of the interior can rely on the same communication platform without direct collaboration. Their data circulates with varying classifications and varying authorisations.

network. This zone can be accessed from the public network and from the secure zone but only with certain restrictions. Two security tools are employed to implement these restrictions. First, firewalls are used to filter the electronic traffic and ensure that only authorised services and users conforming to the security policy are granted access. Second, security gateways are installed in addition to the firewalls to handle incoming and outgoing data traffic. These precautions ensure that the appropriate security policy for zone transition is implemented for each application, for instance, for file transfer or for e-mail. IDP (Intrusion Detection and Prevention) also prevents attacks from non-trustworthy networks.

Security Operations Centre

The Security Operations Centre (SOC) is the heart of the communication infrastructure. Trained personnel can operate the secure interministerial communication network from there with confidence, efficiency and reliability. They deal with issues and responsibilities such as encryption parameters, algorithms, service desk functions, and event and problem management. These sensitive duties are performed in rooms specially provided for that purpose.

The SOC is the practical implementation of the previously defined behavioural regulations (security policy) and precisely sets down which communication goals must be guaranteed in the various zones.

Interesting key figures on internal communications

A survey of organisations with 50 to 30,000 employees[1] yielded interesting findings. An employee receives an average of 28 relevant e-mails a day and requires a data rate of 328 gigabytes a month for the transfer of e-mails. According to the survey, an employee spends an average of one hour on the phone and conducts these calls over VoIP, generating an additional 900 megabytes of data a month. Services using video conferences also have a major impact on data volume. It can rise quickly by 10 gigabytes per employee each month. Annual growth in data volume is estimated to be 20 %. These types of findings on data volume and the associated classification are crucial for designing a networking approach. The more facts there are available, the better protected the networking and security investments are in the long term and the more effectively networking and security can be taken into account in the planning.

Encryption in the core network engenders trust and acceptance.

Two scenarios

A secure interministerial communication network can be implemented with one of two network technologies – Ethernet or IP VPN encryption – depending on the data volume transmitted, the network topology envisioned and the on-site communication services included in the provider's package. If powerful data transmission capabilities are provided at a low network level (OSI model layer 2) of between 20 megabits and 10 gigabits per second, the suitable choice is the Ethernet standard with point-to-point connections or for fully intermeshed structures with multipoint connections (backbone).

If the focus is more on networking and the interfacing of mobile terminals, an IP VPN encryption solution at a higher network level (OSI model layer 3) is recommended. A communication network via IP VPN encryption has the added advantage of end-to-end encryption.

Obligated to good governance: the team of strategic experts

A suitable management concept with a clear strategy for networking the government ministries is vital to the successful implementation of the solution. A set of national guidelines should clearly present the requirements set down by the national security services, the

benefits for the ministries and the type of technical implementation for the group of ICT experts.

A practical approach involving the formation of a team of strategic experts has proved effective. These experts should be authorised to act and be empowered to issue ICT standards in accordance with national laws and fundamental conditions. They apply the zone approach and define the scope and affiliations for all participating ministries. The experts also greatly help people to understand that effectiveness in performing complex administrative duties depends heavily on the use of new ICT solutions and on the security of these solutions. It is no longer enough today for a government to roll out new ICT solutions. It must actively shape and guide this change, the need for maximum security in the core network, and the implementation of networking and give grounds for these actions. Situations implementable just a few years ago with a firewall and antivirus software nowadays require an entire comprehensive ICT protection concept, covering technology, processes and employees.

Security, the foundation of networked government

Technical solutions can usually be implemented efficiently. Things become complex, though, when an ICT solution is politically legitimised and even more so when it is used in a group of all participating ministries. The chair of the team of experts should have both key qualifications, namely the ability to assess the technical aspects and a firm place in the political structure. He and his top-ranking team of strategically-thinking experts should draw up plans and act as coordinators between the ministries, define joint goals and ultimately be able to implement a secure core network for the ministries.

Information security is the first priority. After all, the protection coming from the encryption of information in the core network engenders trust and acceptance among users. That in turn opens the way for optimum and carefree use of networked government. An encryption solution from Crypto AG lays the foundation for secure electronic data traffic within a government and ensures autonomy. What is that wise saying? The highest towers are built on a solid foundation.

Source:
[1] Seminar paper on statistics and projections: Corporate needs for bandwidth in the future, Professor Dr. Norbert Pohlmann, University of Applied Sciences Gelsenkirchen – Department of Computer Science.