



Encryption Technology Is Needed By Government for Sensitive Communications

By Stephen Lewis, VP of Business Development at AEP Networks

Mention the word cryptography and it immediately conjures up images of espionage and cold war code breakers. Most people recognise encryption as something that has long been used by militaries and governments to facilitate secret communication.

But the way in which government - both national and local - operates today, means there has never been a greater need for information to be protected using encryption to prevent it falling into the wrong hands.

Scrambling and unscrambling

In simple terms encryption is the process of scrambling and unscrambling information using secret codes or keys. The use of the codes means that any unauthorised person who is able to 'listen in' or intercept the communication can neither understand nor change the information.

In today's world encryption is primarily focused on protecting information which is stored and communicated digitally using computers - over the internet or other communications links. And there are very many situations throughout government and the public sector which call for the use of encryption technology.

Sharing resources

Large numbers of public sector workers increasingly find themselves having to share resources and sensitive information with other departments or are called on to work in collaboration with other organisations and agencies. This also includes staff stationed in temporary incident rooms at crime scenes, for example, or at outside meetings and conferences at locations which do not have secure communications.

Securing information in such scenarios is obviously of paramount importance and the growing number of departments involved in tackling terrorism and serious crime means the volume of information requiring protection is increasing.

Flexible working

An overall driver for encryption has been central government championing of policies that support flexible and home working. And rising concerns over the impact of pandemics is a related factor. As part of disaster management strategies, it is necessary for staff to be able to work from outside the office using remote access.

Public Key Cryptography

The most commonly used encryption methodology today is Public Key Cryptography, conceived by the genius of Cliff Cox in the early 1970s in GCHQ and developed around the world by mathematicians who have achieved fame for their work such as Schneier, Diffie, Hellman, and of course Rivest, Shamir and Adleman (RSA). Increasingly, commercially developed systems for encryption built to exacting Government standards are being used to protect information classified as Confidential and Restricted under UK government protective markings.

Impressive track record

AEP Networks is one organisation which has built an impressive track record of developing products that incorporate encryption to protect sensitive information for government agencies and critical infrastructure sectors. The company provides secure connectivity for a wide range of government users throughout Europe and the United States.

AEP Networks' products address the demands for secure networking solutions across the full spectrum of government requirements, including Law Enforcement and Homeland Security, Public Safety and Criminal Intelligence organisations. And in the UK the company supplies encryption based systems to almost every government department that needs to process Confidential data.

To support home working which has been fuelled by the demand for flexible working arrangements and the drive to make savings on office accommodation, AEP has developed its Net Remote product.

Portable encryption

Net Remote is a portable encryption device that home and mobile workers can connect directly from their PCs. It provides secure access to applications and data over a wide number of network access technologies including remote office Local Area Networks (LANs), broadband connections and Wi-Fi.

Like several of AEP's government products Net Remote by has been certified by the UK Communications Electronic Security Group (CESG) to protect remote communication to Enhanced Grade (Confidential) standard. And because it is approved for securing highly sensitive information, it incorporates sophisticated features to help prevent theft or duplication of the secret key information in the event of being lost or stolen. The system can be remotely disabled if required and its tamper reactive enclosure protects against sophisticated intrusion attacks.

Collaboration

The AEP SmartGate product is a large scale virtual private network product that uses encryption to support inter-departmental and inter-agency working. It enables each agency or department to collaborate by authorising members of other departments or agencies to share information resources. It might, for example, be used in a situation in which a field operative in a child services department may want to work in the centre, but may also need to collaborate with NHS Trusts, police forces and child protection and care charities. The system enables each entity to collaborate while enabling them to maintain independence.

Protecting the keys

Obviously, one of the issues at the heart of an encryption is protecting the secret key information. The keys are the electronic equivalent of padlock keys and enable the holder to unlock the data when they receive it. The AEP Keyper system is a hardware device which is designed

to protect and store the sensitive key information. It provides physical tamper protection and assures the safety and integrity of critical key material.

Encryption is now a mainstay

While it may have been perceived to be the preserve of the world's military, diplomatic and intelligence agencies, encryption is becoming a mainstay technology which is used for securing information throughout government. AEP Networks has been and continues to be a key technology partner for facilitating its implementation and use.

About AEP Networks

AEP Networks offers a comprehensive Policy Networking solution that provides complete security starting at the endpoints and working throughout a network - from the edge to the core. AEP's integrated portfolio of security products includes network admission control enforcement points, identity-based application security gateways, SSL VPNs, high assurance IPsec-based VPN encryptors, and hardware security modules for key management. Our products address the most demanding security requirements of public-sector organizations and commercial enterprises internationally. The company is headquartered in Somerset, New Jersey, USA, with offices worldwide.



For information on AEP Networks' government products email Stephen.Lewis@AEPNetworks.Com