



Stephen Lewis of AEP Networks discusses the aims of the new Unified Police Security Architecture (UPSA) guidelines for secure electronic information sharing and the company's own very relevant experience in this area.

Taking the Risk Out of Information Sharing

UPSA guidelines

The issue of enabling secure information sharing is the main driver behind the creation of the new Unified Police Security Architecture (UPSA), a set of guidelines introduced in June of this year by the National Policing Improvement Agency (NPIA).

Programmes such as the Cross Region Information Sharing Project (CRISP) and IMPACT (Intelligence Management, Prioritisation, Analysis, Co-ordination and Tasking) have identified an increased demand for making police information more widely available to organisations external to the owning force. The new UPSA framework addresses this need by setting out the required standards to facilitate the secure sharing of information electronically among UK police forces.

The vision statement for UPSA is defined by the Association of Chief Police Officers (ACPO) as follows: "The police service security architecture is to enable employees (and systems) to access the services, when needed, that they require under their basis of employment, whether access is via fixed, mobile or remote device, from either their 'home force', 'other force' systems or elsewhere, within security constraints."



A security framework

The new initiative is designed to allow users to access national police data services with a single digital identity. It consists of a security framework that provides identification, authentication and authorisation services for access to national police data services.

In effect the UPSA aims to deliver a service to ensure that information and intelligence is more widely available while at the same time helping to ensure it is being accessed securely and only by the right people. While it is initially aimed at providing services to all UK police forces, in time it may evolve to encompass partners and government agencies, such as the prison service, magistrates courts and the probation service.

Well positioned advisor

One organisation that is well positioned to advise UK police forces about the UPSA and the challenge of creating systems for secure electronic information sharing is AEP Networks. The company is a pioneer in the development of cyber security technologies for information sharing and has been providing security technology to government and commercial customers since its first SmartGate® product shipped to the US Government in 1995.

AEP SmartGate is an identity-based Virtual Private Network (VPN) solution which enables secure intra-enterprise access to information and applications over private IP Local Area Networks (LANs) and Wide Area Networks (WANs); inter-enterprise information and application access between disparate organisations; and extranet and remote access across the public Internet.

SmartGate's core capabilities include end-to-end encryption, strong user authentication and fine-grained access control. It is widely used in configurations where user authentication is critical such as remote access, extranets and intranets.

Scale is not an issue. The product is optimised for use with large scale, distributed architectures in public sector, financial and other organisations where audit and compliance are critical. Its largest currently deployed system has 5,000 servers and 130,000 users

A USA example

In the USA, as an example, SmartGate has been used as part of a secure information sharing network for law enforcement agencies and criminal justice officials. This is aimed at helping users to communicate critical and time sensitive information – for investigation, prosecution and training needs – that should not be disclosed in a public forum on the Internet.

The introduction of SmartGate into the network enabled users to take advantage of the high speeds and economies of Internet communications for secure Sensitive But Unclassified (SBU) information sharing among multiple jurisdictions and venues. Using SmartGate's VPN, authorised users are able to access the system securely from any Internet connection in the world.

The ability to create and administer groups, with precise and easily managed access controls, was critical to SmartGate's inclusion in the network. This enables Special Interest Groups (SIGs) to be set up for users with common interests and needs – whether they be narcotics, organised crime, gangs, etc. – and allows group members to control access to their own group's information.

Enhanced information sharing

This is just one of many implementations in which SmartGate and other AEP Networks technologies enhance information sharing within and between organisations while reducing risk. With UK police forces now facing just this sort of challenge, who better to turn to?

AEP Networks credentials

AEP has a proven history of securing Central Government and Criminal Justice networks in the UK, Europe and the USA. With design and development based in both the USA and the UK, and products in the company's portfolio assured to CAPS, CCTM and FIPS standards, AEP Networks is uniquely positioned to meet NPIA's exacting Information Assurance (IA) standards.

For more information on AEP Networks' security products:

Tel: +44 (0)1442 458 600
Email: info@aepnetworks.com

