



Nick Chorley weighs up the pros and cons of the proposed Central Services Gateway, which aims to support forces on a day-to-day basis by improving access to the Police National Computer

Portal power

The National Police Improvement Agency (NPIA) has a series of declared objectives that include 'delivering and developing critical essential services and infrastructure to support policing day-in and day-out...providing accessible, responsive and joined-up solutions, enabling the police services to put more time into frontline police work'.

Arguably, both objectives are embodied in the NPIA's latest initiative, the Central Services Gateway (CSG), which is being developed to provide a scalable gateway from police forces into the Police National Computer (PNC) and, in the words of the NPIA, 'other centrally hosted systems'.

The issues

The CSG will replace the STIF Replacement Gateway (SRG), which was, in theory, a

major move that affected tens of thousands of police users nationwide. It was intended to provide a standard gateway for access to the PNC, superseding both Directly Connected Terminal (DCT) and STIF (Standard Interface) methods of connecting computers to the PNC.

The advent of the SRG certainly accelerated a move towards browser-based access to the PNC for police employees. But how radical has it been in practice? Is the CSG what the SRG should have been?

It could be said that the STIF Replacement Gateway was something of a 'fudge' as it simply attached a user-friendly XML-emulating 'wrapper' to a rather unfriendly IBM 3270 mainframe environment, which still required unsatisfactory screen-scraping. This is the transfer of information into formats more readily adapted to

application specific requirements, for example, mobile data, command and control and automated searches.

'Putting an old engine in a new car then calling the vehicle new,' is how one expert has described the SRG.

The Central Services Gateway has been conceived to tackle these issues by:

- providing more flexible access for mobile officers and control rooms alike
- in NPIA's words, 'enabling progressive migration' from an IBM 3270 to a service-based, true XML architecture
- moving from proprietary to open standard interfaces, including those required for web services
- extending the SRG environment to manage a greater range of communication, not just PNC transactions

GUIDE TO ACRONYMS

SRG = STIF Replacement Gateway
STIF = Standard Interface
DCT = Directly Connected Terminal

TACKLING POLICE NATIONAL COMPUTER ACCESS

While the Central Services Gateway (CSG) will have a much wider declared set of objectives than the current STIF Replacement Gateway (SRG), providing PNC access will continue to be central to its role. This role has become increasingly demanding. The PNC holds details of people, vehicles, crimes and property that can be electronically accessed by the police and other criminal justice agencies. It allows for the sharing of information through a secure network, 24/7. Until 1995 the PNC was largely a data storage warehouse, but with later advances in technology it has become an on-line aid to investigations. The PNC began in 1974 with the stolen vehicles database and has grown to include many other information sources, such as wanted or missing people and missing property. It is continually being upgraded and more recent developments have included the National Firearms Register and mobile data checking.

During 2007 some 170 million transactions took place on the PNC, including a record monthly total of 15,375,162. Transaction totals on PNC are growing by some 10 per cent a year.

Source: National Policing Improvement Agency

Providing an open specification is also designed to allow any supplier to compete in the CSG market, with accreditation expected in 2009.

The timing of the introduction of the new gateway as a whole is less clear. Given there are hundreds of transaction codes in the current environment to contend with (representing hundreds of years of original development), it is hardly surprising the introduction date of the CSG is being presented as open-ended.

In practice

Accepting that the CSG is big, and certainly ambitious, what will the new environment mean for day-to-day policing? Or, as some forces are already asking, what difference will it make?

'If everything goes to plan there will be some short and medium term wins'

If everything goes according to plan there will be some short and medium term policing 'wins'. The authentication and identification process, which for many PNC applications is centralised, will increasingly be localised on each force's system – handled directly by the Central Services Gateway itself or through integration with each police force's Identification and Authentication Management (IAM) log-on system when it is introduced.

This means that local administration (and control) is likely to become the norm, as will

– importantly – local audit.

The link between IAM and the CSG will be popular with mobile data and other users as single sign-on web access can be done using employee authorisation card and PIN, with no need to remember multiple passwords. The Central Services Gateway's proposed higher security level requirement for machine-generated passwords that change every few days (already a bone of contention) will be made more manageable using IAM, without compromising the CSG security protocols.

The new gateway will support higher Government security (GPMS) ratings than the SRG – up to 'Confidential' and possibly beyond – allowing it to manage information that the lower-security STIF Replacement Gateway can not.

This is a good example of the way in which the CSG is a more suitable solution than the SRG's 'half-way house'. The Central Services Gateway will provide the foundation to offer connections to a wider variety of police applications in the long term (for example the Violent and Sex Offenders Register, Crimelink and the National Firearms License Management System) whether hosted by Police National Computer Services (PNCS) or not.

Initially, it will integrate access to existing and future PNCS web applications, including the general terminal access provided today. All existing applications that access the Police National Computer through the SRG will in the future go through the Central Services Gateway, which will act as a standardised service point for users, who will be able to access a wider PNC and non-PNC range of applications from their web browser via the new gateway.

Also, thanks to the CSG, all supplier application offerings will manage data in a standardised way, regardless of their 'look and feel'.

Forces to date have given the Central Services Gateway a mixed reception. This is not surprising, as the initiative (at this stage) appears to demand more than it delivers – a common challenge for major migration projects. Technology suppliers therefore have a key role to play in providing forces with better policing solutions that leverage the CSG without requiring major investment in new infrastructure. ■

Nick Chorley is a consultant for public safety and security technology company Intergraph.

WHY CSG?

The Central Services Gateway (CSG) is being developed to:

- Provide a scalable gateway from forces into the Police National Computer (PNC) and other centrally-hosted systems
- Enable the removal of screen-scraping
- Facilitate the transition from 3270 to a service-based architecture
- Move from proprietary to open

standard interfaces

- Extend the STIF Replacement Gateway (SRG) to manage all types of communication
- Local Force user authentication and authorisation
- Enable Web Services interfaces
- Provide an open specification for any supplier to compete in this market

Source: National Policing Improvement Agency