

<"UK USA Kyberpass Baltimore Security Police">

Kyberpass and Scotland Yard

[[Inside Today's Issue](#)] [[News](#)] [[Special Reports](#)] [[Columns](#)] [[Backgrounders](#)] [[Editorials](#)] [[Appointments](#)] [[Wharton Reports](#)]



May 29, 2001

Scotland Yard Goes Digital

Written by [James Cain](#)



Scotland Yard is building a crime fighting net. [Kyberpass Corporation](#), in conjunction with [Baltimore Technologies](#), will provide infrastructure to authenticate police force users for the United Kingdom's Metropolitan Police (Scotland Yard). This will enable the police force to protect confidential police information, such as their database of informants and payments made to those sources.

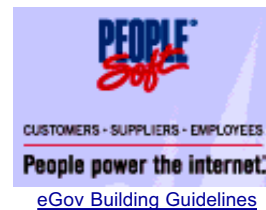
"Digital certificates give our members the confidence and security which is necessary to enable secure access to vital information," says Royston Barker, Infrastructure Program at the Metropolitan Police Service. "They help ensure that transaction information remains secure and confidential and that only authorized parties can access specific databases. The combination of Baltimore UniCERT and Kyberpass eBusiness TrustPlatform builds a strong chain of trust that is essential to the members of the Metropolitan Police Force."

The London Metropolitan Police Force wished to secure their Police Informants Management System (PIMS), which is an oracle based application that details contact information for police informers plus manages various payments and expenses. The system is in constant use by police employees throughout London.

The police environment is a unique one, where the bulk of the users for this application access the system from shared or common workstations, and their network servers are generally not physically secure (i.e. found in the kitchen of some of the smaller police stations).

To secure this unique environment, it was important that whatever security system they selected would have to:

- Be centrally administered
- Require no user set-up or configuration
- Easy for the end users to use
- Require no special training
- Place no additional hardware or elements on the network servers
- Require no modification to the PIMS application.



CONTENT PARTNERS:
[Computerworld](#)
[Wharton School \(UPenn\)](#)
[Russell Reynolds Assoc.](#)
[Bridge Financial](#)

FREE Business Credit Ratings
BusinessCreditUSA

At the same time the security system must provide strong authentication, access control, privacy and integrity over open networks as well as be easily integrated into the corporate infrastructure. There was also a requirement to use digital signatures at some future date. As they wanted to minimize their overhead costs it was decided early on that they would use this initial application as the template for their future security architecture, so the system had to be flexible for future needs as well as the specific requirement on the PIMS application.

The Metropolitan Police decided on Public Key Infrastructure as their starting point and selected the Baltimore UniCERT Public Key Infrastructure (PKI) system. This would provide them with the ability to issue electronic passports providing themselves with crypto management (for privacy and integrity), an electronic identity for authentication, and a digital signature for future non-repudiation requirements.

The Baltimore UniCERT PKI system issues and manages digital certificates, which use encryption technology to validate the electronic identity of people, devices, trusted communications, transactions and information. UniCERT is certified to ITSEC E3 level.

However, a PKI is not an application and they needed to find a way to link their PIMS (and future) applications to the PKI, provide themselves with a centralised point of management for their security policies, while at the same time meeting their unique security requirements.

This led them to Kyberpass, a member of the Baltimore TrustedWorld partner program, who's fifth-generation PKI-middleware accelerates the integration of enterprise applications with PKI systems.

"Our software is essentially PKI-middleware that dramatically accelerates the integration of PKI with new and existing software applications," says Robert Lendvai, Vice President of Marketing for Kyberpass. "As an example, Kyberpass can PKI-enable an entire organization in less than a week. That same process could take anywhere from 12 to 24 months using software toolkits provided by the PKI vendors."

In the Kyberpass and Baltimore Technologies application for Metropolitan Police:

- The client is completely generic, requiring no user configuration and is completely non-intrusive, allowing the shared workstation to be used normally in a non-secure manner.
- Transparent and intuitive user experience, with one single log on screen providing Single Sign-On capability for PIMS and future applications.
- No modification to the infrastructure or application was necessary to completely secure the application.
- The system provides support for the Metropolitan Police's unique infrastructure comprised of Windows NT, the oracle application, the Compaq smart card reader, the ActivCrad smart cards and the Baltimore PKI.
- All security is controlled from a central point – even securing communications that flow through physically unsecured servers.

The initial application is being rolled out to 3,000 users and future applications such as secure email and other database applications will be rolled out to the approximately 50,000 officers throughout the entire police force.

Baltimore Technologies develops and markets security products and services to enable companies to develop secure systems for e-business, the Internet and mobile commerce. Its products include a wide range of Public Key Infrastructure (PKI) products and services, wireless e-security solutions, cryptographic tool-kits, access control & authorization, content security (MIMESweeper products), security applications and hardware cryptographic devices. Baltimore Technologies employs more than 1200 people worldwide and operates from over 38 cities, with headquarters in Dublin, Ireland; London, UK; Boston, USA and Sydney, Australia.

Kyberpass delivers e-security TrustPlatforms for B2B exchanges, Identrus and e-business applications. The company works with all major PKI vendors including Entrust, Verisign, Microsoft and obviously Baltimore.

[Top of Page](#)