POLICEBOX

The role of interoperability and APIs in achieving policing strategic aims

The lack of interoperability between police systems wastes taxpayers' money and reduces effectiveness. How can police ICT escape from the silos of legacy systems?

A white paper by Chris Eccles, CTO PoliceBox

Contents

Looking into the future

Police Vision 2025 and the National Digital Policing Strategy 2020-2030 set out a bold ambition for future policing. But getting there requires a new level of agility, flexibility, and cost effectiveness. How can this be achieved?

UK police forces are currently between a rock and a hard place. They have large investments in legacy systems and complex software integrations, yet they need to adapt to rapidly changing requirements, with limited human and financial resources.

Let's fast forward to a possible future. Imagine a world where a police force can procure a new software system online, in a store of pre-approved applications. The service is "stood up" the same day. Over the course of a few days the new system is configured, then integrated with the force's existing systems, using a separate integration platform product, requiring either no code or minimal code.

After a short period of optimisation, testing and familiarisation, the system goes live force wide, all with no on-site installation. Benefits are realised before even the first subscription payment is made, with real-time statistics showing an immediate improvement in some key performance indicators.

Meanwhile, another agency is carrying out an investigation that needs to find data spread across several other forces. A national catalogue of APIs is searched, and the relevant data sources are identified. Using a desktop tool, the investigator searches for the data. The relevant trust, identity and access permissions are automatically established through a national identity management system. In minutes, the data is found, which helps the agency complete its investigation successfully.

This may sound like a far-off nirvana, but the tools to do this securely exist today, and are in widespread use in the private sector and parts of the public sector. What is the secret sauce that makes this work? At the core are Application Programming Interfaces, or APIs for short. APIs provide a simple, yet powerful means of accessing and connecting data and services.

The state of police IT today; fragmented, siloed and expensive

Before looking forward, let's consider where we are.

Currently, police forces operate many software systems, some of which work together, some of which do not. Different forces use different products to do the same thing, some forces write their own software. This creates numerous data silos where joining up data – to gain operational insight - can be difficult. There are problems with varying data quality, and numerous different definitions of the same types of data. Different systems have different interfaces. There is no national repository to track where data is available.

Forces, at great pain and expense, have invested heavily in integrating these applications together, often using bespoke software, or by commissioning add-on integration features to dominant applications such as records management systems. In many cases, the result is a mass of point-to-point integrations, which are hard to implement, maintain and to see where the data is going.

The number of point-to-point connections needed grows roughly in proportion to the square of the number of interconnected applications, for 30 applications, this adds up to 435 connectors. Each connector must understand the interfaces exposed by the applications at each end. Clearly this does not scale well.

Such an approach stifles agility and innovation – replacing a legacy system with a newer, better product can be a daunting process, as existing integrations must be unpicked and new integrations with other products re developed, with attendant cost and risk. Sometimes it is just better to stick with the devil you know.

Replicate the "Apple® model" with APIs

As we move to ever-more complex and accelerating digital demands, the status quo is becoming untenable. But what is the alternative?

Before 2008, there were smart devices like Windows Mobile, Blackberries, Palm Pilots and so on. They came with some built-in apps like email and a web browser, but it wasn't very easy to add other apps. The world changed in 2008 when Apple decided to open their platform to outside developers who could publish their own applications on a regulated app store. A whole new market sprang up, now worth over $100 billion a year globally, which has transformed both the consumer and enterprise space. There is now an app to do just about anything. To find the app you want, you just search for it in an app store. To solve more complex problems, just use a set of apps and use them together.

If this works on mobile devices, why not adopt the same principles in the back office? Instead of mobile apps, the building blocks are APIs, which become the interfaces to back office systems.

An API is like a web browser app, using similar open standards, except instead of providing a visual interface in a web browser, an API provides an interface to data that applications can access directly over a network.

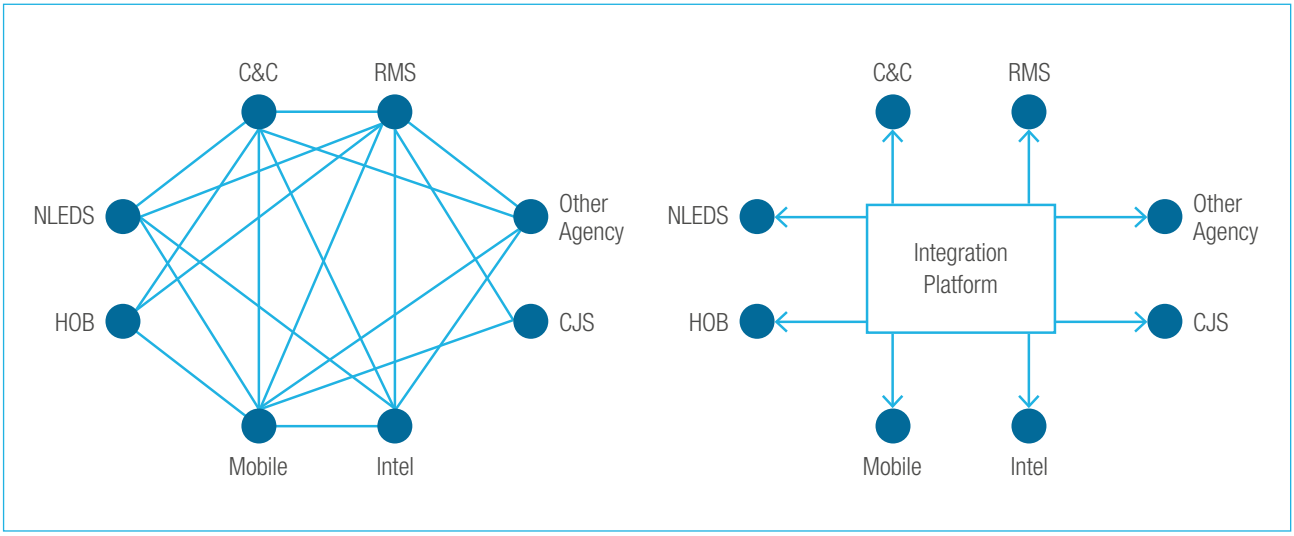
An API typically provides controlled read and write access to a set of data resources, subject to business rules. APIs can be secured, and their data restricted to those authorized to access them. By using a set of APIs, we can easily build complex functionality, and achieve interoperability across multiple applications, even across multiple agencies using different software systems.

One reason APIs are so powerful is that they can be self-describing. This means that an API can offer a machine-readable interface describing how to access it, what it can do and the data it exposes. As most APIs use standard protocols like HTTP, a new generation of integration platforms have sprung up. These platforms greatly simplify integration, as they understand what the APIs do and provide graphical user interfaces to join applications together.

APIs also provide an interface which is isolated from the underlying application, providing a stable point of connection, even if the application is updated.

To join the API club, legacy software vendors do not have to re-write their code, they just expose an API layer on top of their existing software. Clearly, this is oversimplifying things a bit, but the message here is that APIs can be introduced incrementally, and we do not need to replace all of our software.

So why bother going to the trouble?



Point-to-point vs Multipoint integration

With APIs offering a standardised way to access data, we can introduce a new type of software product, an Integration Platform, to join them together. This puts all of the integration logic in one place and, most importantly, only a single API connection is required to each application. So, 30 applications only require 30 APIs, not 435 connectors, and each only needs to know about the application it belongs to. This allows applications to evolve without affecting the others. Such platforms create a 'multipoint integration' environment, instead of a mass of point-to-point connections.

To add an application, we just add one extra connection and define the integration logic in our integration platform, and we are done. No other apps are affected, if they already provide the required functionality.

The integration platform can orchestrate the flow of information between all applications in the enterprise, including managing security, audit trails, and raising alerts when systems fail.

The best integration platforms are very good at what they do, providing sophisticated capabilities and graphical user interfaces, largely eliminating the pain, time and cost of integration. Integration Platforms can be provided as a service, known as iPaaS.

Integration Platforms can generate huge ROI, improve agility and help eliminate data silos, as well as simplifying the procurement and installation of new, innovative applications.

Why so few APIs in the police?

Clearly there are issues concerning security, data protection, data sovereignty and operational issues, but these have all been discussed elsewhere and are prime considerations in initiatives such as the National Enabling Programme. These are also central features of integration platforms.

Probably a major blocker is that there is an initial cost (and perceived risk) of transition, and no single business case can justify the initial investment.

For example, when asked about changing to a new system with a significant cost benefit, a force recently replied:

'We have looked into this and as I suspected, we consider the move away from xxxxxx to another platform to be too problematic and complex at this stage. The integration required to get our current solution up and running with other force systems was so time consuming and expensive that we would be extremely reluctant to change again - even if we knew that the replacement offered better value for money'

This is a pity, because taken together across a series of procurements, the ROI can be enormous, with both direct benefits (cost, risk, time saving) and indirect benefits (ability to do things that were previously impossible or impracticable).

In fact, the potential benefits to the police are massive. The burden on IT departments is greatly reduced, whilst preserving data integrity and security, as they can re-focus on managing APIs to become the gatekeepers of data. Any applications sitting on top of these services are inherently protected. This opens up the force to rapid innovation, both by using APIs in new ways, and also by enabling new innovative products to be introduced without a massive integration burden. Real-time situational awareness, the analysis of big data to draw new insights, as well as closer oversight and governance of processes and data becomes more feasible.

Finally, APIs that meet appropriate standards can be listed in a national catalogue to enable re-use. With a national identity management system, users across multiple forces and agencies can discover the availability of the data, and use it, subject to the establishment of appropriate data protection measures and trust relationships, which can be established within the NEP's national identity framework.

APIs, data quality and standardisation

There are multiple dimensions to data quality, but one is the need to have a common set of names and definitions, so that applications can effectively interoperate accurately. There have been several attempts over the years to arrive at a common set of data definitions for software across police forces and the broader criminal justice system. These national initiatives, despite good intentions, have mostly not been broadly adopted and seem doomed to fail. This is probably due to the diverse range of legacy systems which each have their own definitions of data – it is just not feasible to bring them all into line.

This is an area where APIs and integration platforms can achieve rapid results. Instead of standardising data, we can map those systems against a common master lexicon. Integration platforms can transform data as required to be understandable by all the participating software applications, whilst being traceable back to a master reference.

As national standards emerge, the APIs can map application data on to those standards without having to re-write the underlying applications. Like a mobile app store policed by Apple or Google, a national searchable API catalogue can provide a central repository to find sources of data that conform to certain minimal standards, standards which can be steadily raised over time.

The rise of iPaaS

Before the cloud came to prominence, an Enterprise Service Bus (ESB) was a popular, if expensive, way of achieving multipoint integration. With cloud technology and lightweight web services, Integration Platforms as a Service (iPaaS) are coming to the fore. Several large cloud technology companies like Microsoft and AWS have iPaaS offerings of some kind. There are also iPaaS specialist companies such as MuleSoft who already have established solutions in the public sector. iPaaS solutions tend to be much simpler to implement than ESB solutions, because they leverage the simplicity and power of APIs.

Integration Platforms are already in widespread use in the private sector such as banking and finance, and in parts of the public sector. Every time the pharmacist checks to see if you are entitled to a free prescription, a set of APIs in the DWP and NHS are being orchestrated using iPaaS to verify your details and check the complex rules from multiple sources, getting the answer back to you in milliseconds. Designed correctly, those same APIs can be re used in future (i.e. unchanged) to contribute to other services as they are rolled out.

As organisations introduce APIs, they discover new ways of using and gaining insight into data that were not possible previously. What were previously “data silos” are opened up, and whole new capabilities can be created. The advantages to policing become clear. Over time, IT thinking becomes centred around the provision and management of APIs as primary services of value. IT departments can lock down the access to data via APIs, allowing more innovative applications that consume them to be developed outside of the IT department without compromising security. In the private sector, APIs can become products in their own right, and the IT department becomes a generator of revenue rather than being seen as a cost centre responsible for ‘keeping the lights on’.

The iPaaS market is predicted to be worth $2.7 billion by 2025. This is not a new technology, but with the rapidly advancing adoption of cloud technology, the advantages are becoming compelling.

Delivering APIs today: A checklist for policing

This vision all fits in with the objectives of NEP and the National Digital Policing Strategy 2020-2030.

So, the question is, how do we get there? Policing needs a way to get this off the ground today. In order to deliver the sort of connected policing that Vision 2025 and the National Digital Policing Strategy 2020-2030 aspire to, there are a number of steps that police forces need to take:

Stimulus funding

Some kind of stimulus funding would go a long way to help catalyse the transition, to offset the initial cost of investment in iPaaS systems.

Take the first step (no need for a "Big Bang")

The transition to an API-led architecture does not have to be a Big Bang; once the initial building blocks are invested in, the new approach could be introduced one process at a time.

Mandate API interfaces in all new procurements

If police forces mandate that all vendors that wish to work with them have an API for their applications, you can be assured they will build them, and will do so quickly. This will ensure that, over time, a force can migrate to a fully interoperable set of application services, extending not just across the force, but to other agencies. APIs also offer great benefits to vendors too, as they offer potential new revenue streams, without the need to significantly modify their existing products.

Add greater emphasis on APIs/interoperability to the National Digital Policing Strategy 2020-2030 and Policing Vision 2025

Forces are actively working towards these strategies already (e.g. NEP). If they specifically called out the need for, and highlighted the benefits of, APIs/interoperability within these strategies, this will directly contribute to achieving interoperability objectives faster.

Solve the data quality problem by allowing integration platforms to develop organically

For applications to be able to talk to each other effectively without errors, a common set of names and definitions is required. Since national attempts to do this have largely failed, this is where APIs and the power of integration platforms will achieve rapid results. Forces' disparate systems can then communicate with each other without having to update their applications to meet a common lexicon. As has already happened in other industries where APIs have been opened up, a common integration platform will emerge naturally because it is in the common interest of those vendors that create the APIs and the forces that use them to do so.

Leverage the NEP's existing National Identity Framework as the default national identity management system

To deliver on the vision of agile police services that are able to share data securely across force borders, other agencies and central government, we need a way to verify a user's identity. This is where a national identity management system is necessary. Thankfully, with many police forces already working with the National Enabling Programme (NEP) to digitally transform how they work, such an identity management system already exists. To save reinventing the wheel, it will be relatively straightforward to utilise the NEP's existing national identity framework as the National (UK Public Sector wide) identity management system necessary to establish the data protection measures required to facilitate the safe interoperability of systems.

Deliver interoperability within the broader digital transformation of the police

There is little point delivering interoperability via APIs if there isn't a broader strategy among policing to digitally transform how it operates. Apart from the pure functionality of APIs and iPaaS to physically enable interoperability, there are issues of data governance, regulatory compliance, trust relationships, data quality, organisational culture and more that will need to be worked through. Digital transformation of policing won't be achieved by a handful of vendors offering APIs by themselves.

Policing as a whole needs to be behind the digital vision by instilling the necessary culture across everyone involved, from the frontline to senior management, procurement, operations, central government etc. – and suppliers.

Why use APIs to deliver interoperability? A quick recap

By way of a quick summary, it is important to remember why APIs are the best route forward for digital policing:

- APIs enable the use of integration platforms (iPaaS) to integrate multiple applications together significantly more efficiently than using point-to-point integration
- They simplify integration and data sharing between multiple applications
- APIs help improve organisational agility to response to change (change one system only, not everything its connected to as well!)
- Lock-in to individual applications is reduced, providing greater flexibility in procurement
- It's easier to track the flow of data between applications and to detect failures and security issues
- APIs reduce inter-dependencies between software vendors' products
- Less specialist programming skills are needed
- Significant opportunities to reduce costs, time and risk

Ultimately, a new solution should not be considered as fit for purpose if it does not have a suitable API. Existing solutions should be urged to publish APIs. Without an API, a software product will likely create a data silo, have limited utility, with high costs of integration, further increasing future cost and risk when procuring other applications which need to interoperate.

Taking the right steps now will set us on the path to that future world where procuring new systems is closer to the experience we already have when adding apps to our smart phones, with enterprise performance levels and agility that Policing can only dream of today.

Amazon's famous memo. A "Prime" example of the power of data sharing via APIs

In 2001, Amazon's market capitalisation was $2.25Bn. In 2002 CEO and founder Jeff Bezos sent out the following memo to all staff which has become legendary in IT circles:

" 1. All teams will henceforth expose their data and functionality through service interfaces.
2. Teams must communicate with each other through these interfaces.
3. There will be no other form of interprocess communication allowed: no direct linking, no direct reads of another team's data store, no shared-memory model, no back-doors whatsoever. The only communication allowed is via service interface calls over the network.
4. It doesn't matter what technology they use. HTTP, Corba, Pubsub, custom protocols — doesn't matter.
5. All service interfaces, without exception, must be designed from the ground up to be externalizable. That is to say, the team must plan and design to be able to expose the interface to developers in the outside world. No exceptions.
6. Anyone who doesn't do this will be fired.
7. Thank you; have a nice day! "

Amazon has grown 400 times in value since then, now offering a vast range of services, from retail to cloud computing. The market value in 2020 hit a trillion dollars. Draw your own conclusions, but it is hard to see how Amazon could have achieved this without the broad adoption of API technology.

POLICEBOX
Boho 5
Bridge Street East
Middlesbrough
TS2 1NY
0800 8498811

www.policebox.com

Coeus Software Ltd (trading as PoliceBox)
Registered in England & Wales: 058 305 05

WP01_0720