techUK
FOR WHAT COMES NEXT

Demystifying Digital Interoperability in Policing

September 2024

Introduction

This paper has been developed by techUK's Interoperability in Policing Working Group (IPWG) which is an industry led initiative, formed in 2018, for industry and policing stakeholders to come together to accelerate the interoperability of police IT systems.

'Digital Interoperability' in this context refers to the ability of different IT systems and software used by police forces to work together seamlessly, allowing for more efficient data sharing and communication.

Historically policing applications have been developed in isolation, with the data held only being available to the application itself. However there is a now a recognition that this silo approach must change. To this end the first principle of the UK Police Industry Charter is that future systems should be interoperable by design. Interoperability is also a central concept of the NPCC Digital Strategy, the Policing Vision 2025 and the National Information Sharing Strategy (NISS) for Policing.

The purpose of this paper is to help those interested in digital interoperability in policing to understand digital interoperability and unpackage some key concepts and technology approaches. It concludes by setting out ongoing work and those recommended developments which are necessary if digital interoperability is to become routine and truly 'by design'.

Overview

Police officers and staff continue to raise their frustrations with the lack of interoperability of digital policing systems.

The inability of systems to share data and communicate results in the rekeying of data, multiple logins, searches, and interactions across policing systems to conduct day-to-day policing activity.

Data can often then reside in isolated 'silos', leading to duplication, inconsistencies, and inability to cross-reference and form a single view of all information available. This can lead to missed opportunities to respond and intervene effectively.

The experience of using silo systems, particularly for frontline staff, is often frustrating and demoralising. It impacts operational effectiveness and efficiency every day. As information is the lifeblood of policing, not having easy joined-up access to key information or the ability to complete business processes seamlessly across multiple systems is a fundamental blocker hindering service delivery and productivity.

Greater digital interoperability is necessary to support seamless access to local, regional, and national information and across multiple agencies. This would also improve operational effectiveness and efficiency at the frontline. Information sharing agreements and data governance arrangements must be key controls for wider information sharing, particularly between agencies.

This issue is now recognised at the highest-level withing UK Policing. Connected technology is seen as a key enabler in the National Policing Digital Strategy, stating that the service 'will put the power of data and information in the hands of officers and staff, when and where they need it'. Interoperability is also core to the 2024 Police Industry Charter's principles and purpose.

With a focus on digital interoperability in a UK policing context, this paper seeks to assist those interested in understanding this area. It starts by defining terms, then considers examples of the benefits and goes on to explore the differences between different approaches to delivering interoperable systems. The document concludes by suggesting areas for further consideration.

Definition of Terms

An online search of definitions of terms like interoperability can produce some quite technical descriptions which can stifle a general conversation on the subject.

Within this discussion document, in a policing context, we use the following plain-English terms:

Data sharing:
the exchange of information, between systems and/or organisations.

Digital interoperability:
the ability for digital systems to operate together seamlessly and effectively to support policing activity.

Native digital interoperability:
where systems communicate via common standards requiring no translation between them.

Integration:
the technical means by which interoperability is achieved.

Point-to-point integration:
a way of achieving interoperability by connecting applications directly to each other.

Integration platform:
an application which is designed specifically to integrate multiple applications together to achieve interoperability. Integration platforms are one method of implementing integration.

iPaaS:
an integration platform which is provided as a cloud-based service.

Interoperability Examples and Benefits

There are some fantastic examples of successful digital transformation through integration platforms across both public and private sectors, showcasing how these technologies have been effectively implemented to improve processes and user experiences. Learning from different sectors is crucial and it provides best practices that can drive innovation within policing. All of the following examples derive benefit from systems that are able to interoperate and share information.

Policing: Improved Victim Support

In UK policing, the online victim journey is a digital transformation initiative aimed at enhancing the experience and support for victims of crime. This journey begins when a victim first contacts the police, continuing through the response, investigation, and the criminal justice system. The use of technology, such as integration and CRM platforms, allows police forces to centralize information and provide automated updates throughout the crime or incident lifecycle, keeping victims informed and engaged. This approach not only improves efficiency but also ensures that victims feel heard and supported, fostering trust in law enforcement. A good example is the Digital Case File project that facilitates the fully digital exchange of case files between police forces and Crown Prosecution Service (CPS).

Seamless Banking, Finance and Insurance

In this sector many companies now offer almost instant decisions on loans, mortgages, and insurance applications. This is achieved through the interoperation of multiple services from different providers, including identity verification, credit rating checks, searches on court orders and the like. This is achieved via modern integration platforms, compressing processes that used to take days or weeks into minutes or seconds.

Improved NHS Processing of Prescriptions

When getting a prescription, a pharmacy can check within a few seconds whether a patient is entitled to a free prescription. The processing behind this is orchestrated by an integration platform, which interrogates data sources from multiple government departments and applies rules to determine eligibility. Learn from Patient Safety Events Service is a great example of interoperability in the health sector.

Different Approaches to System Integration

How can interoperability via data sharing be achieved? As this document is intended to be as non-technical as possible it is useful here to consider an analogy.[1]

Imagine that you are visiting an international conference with people from across the globe. Many different languages are spoken. The point of a conference is to work together and share data in one form or another.

So, how do you communicate with everybody? There are four basic options:

1. Everyone learns every language spoken

All attendees must be multi-lingual. This is equivalent to using point-to-point integration – each software system must learn how to speak to each of the other software systems it shares data with, typically by some kind of custom 'connector'. The approach can work if there are very few systems, but rapidly becomes impracticable as numbers increase.

For example, if a delegate from a new country wanted to attend the conference, everyone would have to learn their language (or simply refuse permission for them to attend). Similarly, a new or updated software product would require other applications to adapt to communicate with it, increasing the cost and time to adapt to new requirements.

2. Hire a translator for every language

This allows everyone to speak their own language, and not have to learn any others – that is taken care of by using an official language and a small group of translators provided by the conference. In fact, presenters at the conference do not speak to the delegates directly – the delegates hear the translations instead in their own language.

This is equivalent to using an integration platform, to convert between the interfaces exposed by each software system, like a central team of translators. Software products do not need direct knowledge of other products' interfaces. This scales much better.

For example, if a new delegate presented at the conference in a new language, one extra translator would be needed but everyone else would be unaffected. Similarly, if a new application were added, one new integration would need to be added to the platform, but no changes to other apps would be needed.

3. Everyone learns one common language

For example, all the delegates could speak English. A new delegate would need to speak English and everyone else would be unaffected. However, a conference held in another country may choose French instead, so this may not be the best solution for delegates who travel internationally to conferences. In software terms, a global vendor may not like this approach unless the same standards are agreed internationally.

This is the equivalent to native interoperability – all applications must expose interfaces that conform to common standards shared and understood by all applications.

4. Read the published materials after the event

After the event has finished, the conference organisers publish selected information in a library for people to read. This may be in one language or perhaps translated into several standard languages.

This is equivalent to exporting the information to a common data store which everyone can access, subject to appropriate access permissions. The data may be stored in several formats. This approach is more suited to sharing information of record, rather than on-going processing.

1 With thanks to caredove.com for the analogy: https://about.caredove.com/blog/integration-vs-interoperability

Applying Interoperability at Different Organisational Levels

At the local level, a police force is in full control of their own systems and data and is free to deploy software using its own proprietary data standards.

This approach works, as long as there is an efficient way to interconnect the local systems without creating ambiguities in the data. However, this means that many forces develop tactical (short term) point-to-point connections between applications, which, as we saw earlier in the conference analogy, is not efficient at scale and tends to block new products and updates from being adopted.

As the need for data sharing with other organisations increases, the need for standards-driven full native interoperability also increases. However, once the data is no longer under the direct control of the originating force or agency, there needs to be formal agreement between parties over data meaning, formats, governance, and regulations. This implies the use of a common standard to which all parties comply. Standards ensure the data is correctly understood by third parties and is correctly handled, with audit trails.

We do indeed see that national services tend to adopt well defined standards (e.g. Police National Computer (PNC), Law Enforcement Data Service (LEDS)) whereas local systems may adopt more proprietary standards.

In policing, we could define four hierarchical levels of interoperability:

1. Local Level Interoperability

Local interoperability supports the ability for software systems to work together within a single force, and to ensure that officers do not need to manually log in to multiple systems to complete a task. This includes, for example, processes that span command and control, records management, mobile operation, and outreach to the public.

As a single force is in control of the data, standards-based native interoperability is not necessarily required. Native interoperability at this level could even stifle innovation as little could be changed without having to change agreed standards.

However, integration needs to be efficient and agile. Many legacy systems still use point-to-point integration, which can be slow and expensive to update.

2. Inter-force Interoperability

This supports the ability to share data between forces to support mutually agreed processes according to agreed rules. Agreed standards are needed to ensure the data is used and interpreted correctly. There needs to be buy-in to the use cases for inter-force data sharing.

3. Inter-agency Interoperability

This supports the ability to share data across agency boundaries to support mutually agreed processes according to agreed rules. Agreed standards are needed to ensure the data is used and interpreted correctly. This includes the use of national services by forces, such as PNC, LEDS etc. Again, there needs to be buy-in to the use cases for inter-agency data sharing.

4. International and National Level Interoperability

This supports the ability to share data across national boundaries adhering to national and international regulatory frameworks. Agreed standards are needed to ensure the data is used and interpreted correctly.

The methods by which these objectives can be achieved are the subject of further discussion and will be documented separately. from the experiences of other jurisdictions, taking into account both successes and shortcomings in order to craft a framework that is effective and feasible for the unique challenges faced by the data centre industry.

Introduction to Interoperability Techniques

Various methods are available to achieve digital interoperability, each with their own advantages and disadvantages. Below is an explanation of those more commonly used.

Point-to-Point Integration

Point-to-point integration connects applications directly together, so each application needs to implement a means of communicating with and understanding the other applications' data structures, interfaces and protocols. This places an overhead on application vendors to support connections to other applications, as well as supporting their own software.

Complexity rises roughly with the square of the number of applications involved, so although the approach can be cost effective in simple situations, this approach does not scale well.

The complexity can be reduced somewhat if one dominant application, such as a Record Management Service (RMS) system, acts as a 'hub' for point-to-point connections. This however places a burden on the software provider to support new applications, which they may be reluctant to do, particularly if the other application is perceived as a competitor. This also implies that the RMS system is doing two very different jobs.

Being proprietary, point to point integration does not typically involve significant standards work, but the approach is slow and expensive. It is costly to replace software systems or add new ones. It is also difficult to manage processes that span multiple systems. A single process may encompass multiple technologies and protocols, requiring highly skilled people.

Platform-Based Integration

Platform-based integration treats the integration function as a separate application in its own right – an integration platform. Applications do not talk to each other directly; instead, the platform handles the transfer and translation of information, orchestrating processes that span multiple software systems, like the conductor of an orchestra. Implementing interoperability as an extra application has the potential to provide greater oversight and control over where data is going and who can see it.

Such an approach, initially known as an 'Enterprise Service Bus' (ESB), has been available for some time. These ESB platforms required specialist technical knowledge to implement. More recently, Integration Platforms provide sophisticated built in tools to make integration simpler.

However, care needs to be taken to ensure that translations between data models are correctly performed without ambiguity.

As well as communicating with other software systems, Integration Platforms can expose interfaces of their own. This provides a straightforward way to expose standards-based external interfaces even though individual applications do not.

A platform-based approach therefore offers the potential to scale well at reasonable cost.

Full Native Interoperability

By conforming to detailed standards, systems can communicate without translation, although something is still needed to orchestrate information flow between systems to support business processes.

This approach requires detailed standards to be developed, requiring participation of all stakeholders and implementation by vendors, but the integrator's job is made simpler as data translation is no longer needed, and the risk of mistranslation is eliminated.

Full interoperability, whereby systems talk to each other without translation, is a desirable outcome, but the cost to get there is significant:

- Standards need to be agreed and developed which work for all stakeholders, including each affected software vendor.
- Each software vendor then needs to implement the standards.
- Existing integrations need to be updated.
- A vendor may need to meet multiple standards if targeting an international market.
- Adding a new capability may require negotiation of an updated standard.

Standards are therefore expensive, and time consuming to define, implement and update.

For these reasons, full native interoperability may not be the best approach at individual application level but can be more suited to interoperability across organisational boundaries, where standards need to be defined.

Using a Common Data Repository

A different approach is to export selected data to a common repository that can be accessed by multiple systems or organisations (subject to appropriate access permissions etc).

This can scale well at reasonable cost as there are many hyperscale data storage solutions available. The approach may be most suited to historical records rather than as a way of coordinating ongoing business process transactions that span multiple systems.

Systems like PNC can be thought of as common data repositories, allowing forces to access national information generated from multiple sources. However, there is scope to introduce more flexible solutions encompassing a broader range of data, using newer technologies.

Necessary Developments

The techUK Interoperability working group has made significant progress in leading discussions on interoperability within the law enforcement sector, increasing awareness of its importance and fostering collaboration. Significant progress and dialogues have been established with law enforcement bodies and police forces, leading to tangible improvements and successful collaborations. The working group is effectively collaborating with the Police Digital Service, Police Chief Scientific Advisors Office, National Police Chiefs Council, Home Office (supporting the Police Information Strategy) and other law enforcement agencies, showcasing how cross-sector collaboration can drive meaningful advancements.

Whilst progress is being made in policing, moving forward there are several areas that require further research and discussion, particularly regarding interoperability and integration. More work needs to be done in learning from the private sector and how other agencies can offer new perspectives on effective strategies for achieving interoperability.

Potential Future Considerations:

- Identifying specific use cases and stakeholders for driving the interoperability agenda
- Improving data quality and leveraging existing standards
- Prioritising development efforts using the Pareto Principle (the 80:20 rule) - this states that for many outcomes, roughly 80% of consequences come from 20% of causes. So, identifying those enabling areas that deliver most benefits and prioritising these.
- Identifying funding strategies

In addition, in order to advance interoperability, there will be the need to address questions around data ownership, liability, and (crucially) withdrawal rights, together with promoting a competitive marketplace for integration providers and selecting optimal technical approaches.

There are also non-digital factors to be considered such as governance, agile approaches, data management, delivery management, technical strategy, standards, data pipeline operations, access control, business change management, and continuous improvement - these must also be considered to support these technical solutions.

To address the challenges outlined, there are some essential steps that need to be considered. The IPWG has identified several key areas in which it is recommended that work is undertaken to improve capabilities, these are:

1. **Interoperability Strategy:**
   Create a strategy to reduce application dependencies and vendor lock-in, aligning with a national framework.
2. **Skills and Knowledge:**
   Invest in training and external expertise to manage technology effectively and improve operational efficiency.
3. **Open APIs:**
   Prefer solutions with open APIs to ease integration and enhance data sharing, using common data standards.
4. **Technology Evaluation:**
   Regularly review technology performance to refine strategies and maximize investment.
5. **Collaboration:**
   Engage with techUK for insights and solutions through market sessions to improve data sharing and technology practices.

By progressing these recommendations, improving digital maturity and enhancing collaboration, we are confident that policing can significantly improve the extent and performance of digital interoperability.

Conclusion

In conclusion, the techUK Interoperability in Policing Working Group (IPWG) has made significant steps in addressing the long-standing challenge of digital interoperability in UK policing.

This document has been written to help those interested understand digital interoperability and unpackage some key concepts and technology approaches. It has also hopefully highlighted the critical need for seamless data sharing and the benefits demonstrated by successful implementations in both public and private sectors.

Whilst some positive examples of progress exist, there is no national strategy, framework or specific investment to facilitate interoperability and realise the dependent operational outcomes.

This paper highlights several key areas requiring further exploration and development, including identifying specific use cases, improving data quality, leveraging existing standards, and prioritising efforts through strategic frameworks like the Pareto Principle. Additionally, non-digital factors such as governance, education, and continuous improvement are essential to support the technical advancements in interoperability.

Moving forward, continued engagement between industry and policing stakeholders, along with learning from best practices in other sectors, will be crucial.

By focusing on these areas, the IPWG can work with policing stakeholders to drive meaningful advancements in digital interoperability, ultimately enhancing the effectiveness and efficiency of policing operations and improving the overall experience for both officers and the public they serve.

While achieving interoperability depends on the adoption of systems able to communicate with each other and on data, a cultural shift within police forces is also necessary.

Further information

About techUK

techUK is a membership organisation launched in 2013 to champion the technology sector and prepare and empower the UK for what comes next, delivering a better future for people, society, the economy and the planet.

It is the UK's leading technology membership organisation, with more than 1,000 members spread across the UK. We are a network that enables our members to learn from each other and grow in a way which contributes to the country both socially and economically.

By working collaboratively with government and others, we provide expert guidance and insight for our members and stakeholders about how to prepare for the future, anticipate change and realise the positive potential of technology in a fast-moving world.

Justice and Emergency Services Programme (JES)

The JES programme provides a forum for Justice and public safety stakeholders from national policing bodies, local forces, fire and rescue and Justice partners, to collaborate with members.

The programme creates a platform to understand the latest innovations, problem-solve and develop networks, championing the role technology plays in supporting the delivery of public safety services. The programme has a number of established workings groups, enabling the public and private sector to come together regularly.

Groups include Digital Justice, Driving Interoperability in Policing, Public Safety and Security SME Forum, Fire Innovation Forum, VAWG and RASSO Tech Working Group.

Interoperability in Policing Working Group (IPWG)

The working group is an industry led initiative, formed in 2018 by techUK, in order for industry and policing stakeholders to come together to accelerate the interoperability of police IT systems.

There is a strong consensus within the IPWG that further engagement between industry and senior policing stakeholders could ensure the benefits of interoperability are realised.

This could increase the scope of the group beyond technical standards to include wider force engagement, skills and awareness and procurement, and working closely with policing stakeholders such as PDS, NPCC and Home Office, to establish a process by which industry and policing can work together to enhance interoperability.

techUK
FOR WHAT COMES NEXT

linkedin.com/company/techuk

@techUK

youtube.com/user/techUKViews

info@techuk.org

Image credits | iStock by Getty Images

LeoPatrizi | monkeybusinessimages | SolStock | Larysa Tsyvinska | gorodenkoff | Wirestock