CAPITA

OPINION PIECE

Choosing a Digital Evidence Management Solution

A guide for UK police forces

Introduction

From video interviews in custody, body worn video (BWV), and managed and unmanaged CCTV, to forensic images and media from the public (including smartphone and dashcam footage); police forces are experiencing a huge increase in the amount of digital evidence.

Every police force recognises the pressing need to manage this evidence as effectively as possible. It's a significant business challenge that impacts their strategic roadmap for technology and IT infrastructure.

The need for effective digital evidence management

Whilst the need for digital evidence management (DEM) is clear, the definition of exactly what DEM solutions should include is less well defined.

Unfortunately, much of the current discussion around DEM is focused on video editing (clipping, redacting, etc.). Indeed, the temptation when stating requirements for a procurement tender is often to place an emphasis on this this.

However, much of the required functionality of a DEM solution lies beyond editing video files. This is in fact a relatively small part of the business process for end-to-end management of a huge range of digital evidence.

If a force fails to ensure the foundations of their DEM solution are complete, they will not deliver the full business benefit from the investment. More importantly, they will not source a solution capable of meeting changing business and policing needs in the years ahead.

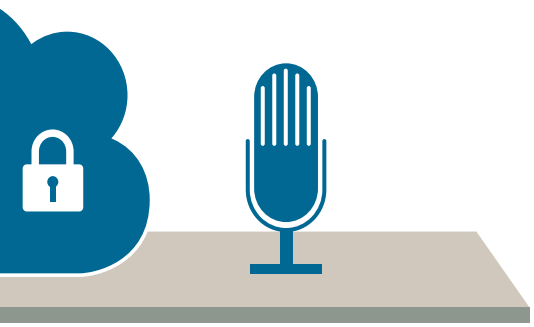
Sharing our experience

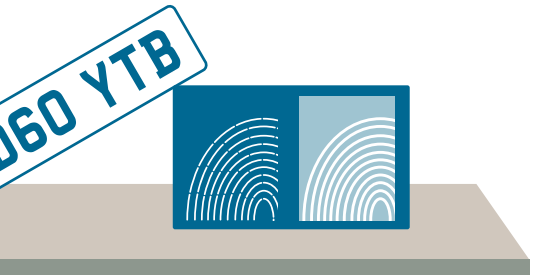
Capita believes that there is a clear need for enterprise scale (DEM) solutions, and that forces should set their sights on such systems, rather than limit their aspirations to integrating the management of just a few types of evidence.

Enterprise DEM solutions are necessary to manage media ingestion, guarantee evidential integrity, control access, support downstream sharing with the CPS (as will be required under the Digital First programme) and manage the ultimate disposal of the media.

We have developed a DEM solution as a new component of our EvidenceWorks® platform, which is used by 15 UK police forces. Our leading partner in this work is Avon and Somerset Constabulary, who began using the DEM functionality in 2015. Their feedback about what they require from the solution has been invaluable in helping Capita to evolve the solution and that work is ongoing.

As a result of our experience, we feel suitably-placed to offer guidance for police forces on the selection of DEM solutions. We hope that this paper furthers the discussion around the need for DEM, and the capability that such solutions should deliver.





Drivers for implementing a digital evidence management solution

The reasons for investing in a capable DEM solution are many. However, we would like to highlight three main drivers in order to set the scene for this paper.

Preparing for Digital First

The research and recommendations from the police-led Digital First programme will provide much needed-guidance for investing in digital evidence management. The programme is moving towards a situation where forces will share evidence electronically with each other, the CPS and, potentially, other organisations. Forces will struggle to do this efficiently unless they have a capable digital evidence solution in place.

Investing in this capability is one of the main drivers for Avon and Somerset, who are keen to be in a position where they can share data easily with the CPS. The force isn't waiting until the CPS establishes its requirement, but instead wants to be proactive rather than run the risk of having to play catch-up once the final details of Digital First become clear.

Improving efficiency

Another significant driver for having all of a force's digital evidence in one place is the potential for quicker, more efficient investigation processes. With the right solution, officers or other users are able to access - in one place - all of the evidence related to a crime or other occurrence, from BWV footage to crime scene images.

Centralising digital evidence allows the force to decommission 'point' solutions in support of a cohesive security and access policy to evidence, and reduce officer training across multiple systems.

Reducing the time officers spend on what are essentially administrative tasks makes sense for every force. Freeing officers' time to perform more valuable tasks is something that the public and politicians alike would also welcome.

Coping with increases in evidence volume

Another driver for increasing digital evidence management capacity and capability is the sheer volume of evidence that will need to be addressed. The amount of data - from BWV and dashcam footage to CCTV and smartphone-captured video and images - will grow at an ever-faster rate and forces will find themselves at risk of having historic solutions and processes that cannot keep pace.

But it's not just about handling increasing quantities of digital evidence: it's about doing so effectively. Effective management of evidence is needed to avoid instances of defence lawyers successfully challenging the integrity of evidence. This is why robust security features such as digital signatures and audit trails are essential.

Device and data challenges

Every force must ensure that the DEM solution it chooses can operate free from major constraints around data formats. This is a significant challenge: eForensics Magazine reported in 2015 that there are 3,000+ video formats in the CCTV industry alone.

Although a force isn't likely to encounter anywhere near as many as 3,000, they will have to manage a great number of formats and codexes. The digital world is standardising and the number of formats will diminish over time, but the problem will take a long time to go away as legacy formats will remain in use for years to come.

Forces should therefore ensure that any DEM solution they choose should have the capability for playing a wide range of the most common formats they will encounter. There should also be capability to integrate with a suitable transcoding tool for less common formats.

The limitations of device-specific DEM solutions

Forces do of course have an alternative to sourcing a single DEM solution. They can instead use a number of data management solutions that are provided by device manufacturers, and somehow try to integrate these into a seamless system via a distributed indexing/search engine approach.

The Capita team has had first-hand experience of a number of such systems. Our observation is that they routinely fall short of the DEM solutions that are independent of devices. Even if a device provider's system looks great in terms of a user-friendly front end, the back end and overall functionality is much more limited than independent DEM solutions.

An enterprise system is about much more than the ingestion and storage of media. A full DEM solution must have the security and audit capabilities to ensure integrity, and be configured with the necessary workflow and rules for the review, retention and disposal of media in line with the MoPI guidelines.

Not all device-specific solutions provide this advanced level of management and this is also the case for distributed approaches operating across disparate data silos. It's also the case that not all suppliers have the experience and knowledge to implement such business rules, specifically in the policing arena.

In addition, device-specific solutions will inevitably lack the ability to manage a wide range of evidence from other devices and sources. They may be very good at managing data from the device itself, but can they also manage CCTV footage, interview audio and so on?

Another factor at play is that devices tend to have relatively short shelf lives - and that is perhaps truer of today's digital tools than their analogue predecessors.

For example, the 'best' BWV camera in use today may not be the best or the same BWV device in use in three years' time. When a force switches to another camera, its DEM solution must have the flexibility to support the previous camera's output, as well as the new device, which may be from a different vendor altogether.

To sum up, a force's DEM solution will no doubt outlive many or most of its hardware devices. The DEM roadmap should therefore focus on the needs of the force to effectively manage multiple media sources and business requirements. It shouldn't be tied-in to one or more devices that in any case won't be around for very long.

What should forces consider when assessing DEM solutions?

Now we move on to list and comment on some issues that should be considered when choosing a DEM solution. We don't claim that this list is truly comprehensive, but rather that it blends some of the more obvious requirements with some that we feel are often overlooked. We hope that this list will provide much assistance for anyone involved in DEM procurement.

Usability - from the perspective of multiple user groups

A DEM solution must be able to meet the needs of different users. For example, transcribers may need the solution to accommodate foot-pedals to pause and play audio as they type. Users in a specialist video unit will need all of the functionality they are used to. Officers may need a simpler interface so they can quickly upload evidence without having to spend more time than is necessary away from the front line. Across the force, the DEM solution will mean different things to different people.

Another issue around usability is the type of device that people will use to access the DEM solution, and the type of deployment therefore appropriate for those users.

In most forces there will likely be a mix of users and deployment methods. 'heavyweight' users working from desktops may require a feature-rich thick client deployment. Web client deployment might be appropriate for 'light touch' users requiring less functionality working from mobile devices.

Access, security and the audit trail

It must be possible to model access to certain data and certain tools by role within a force. For example, the type of access available to officers may differ from the access suitable for transcribers. This should be possible regardless of the complexity of the organisational structure.

The solution should also allow for 'fine grain' management, with the ability to add further restrictions. This may include restricting access to specific items of data, permitting access to only those assigned the appropriate rights.

Whilst most evidence in a case might routinely be accessible to every officer, on occasions there is a need to flag specific data items as 'sensitive' to limit access. Examples include evidential interviews with a celebrity, or special designations to limit access to particular teams.

DEM solutions should also include sophisticated tools for auditing user access and behaviour. For example, the solution should capture the start-time and length of play for video files, and not simply the fact that a particular video was played.

Search capability

The ability to provide a sophisticated search engine across the evidential store is essential. If the DEM solution is to support efficient and streamlined business processes a single evidential store is essential. Federated searching across disparate data silos does not in itself improve business processes as the many source systems need to be upgraded which incurs cost and downtime and the federated search engine is dependent on source systems for search capability and compatibility.

Users in different roles should have access to suitable pre-configured searches to support efficient business practices.

Users should have the flexibility to use 'Google' style searching on all evidence metadata. They should be able to narrow down their search results to identify the single evidential file they wish to manage. Searching should also be limited within the context of user access rights within the solution.

Other functionality

We suggest that there are a number of other functionality must-haves for a DEM solution, including the following:

Support for efficient end-to-end business processes for all digital evidential material. In particular, it should be possible to tie evidence to the force's records management system and support an interface to that system. This should be combined with a capability to define new and flexible business process workflows for managing evidential material.

Control and management of evidence in a way that is relevant to the original evidence source. Not all data is the same, and not all data should be handled in the same way. For example, the process for managing BWV files and the associated meta-data will differ from that associated with an evidential interview. A DEM solution must therefore have capability for maintaining different sets of evidential metadata for each evidence source.

Architectural flexibility to share data securely. This should include a video streaming and file download mechanism to facilitate future support for the Digital First 'Digital Evidence Transfer Service' (DETS) service.

Comprehensive support for cascading the review, retention and disposal process from the force's case management system. The DEM solution should fully support core police systems, whilst providing the enterprise platform for sharing evidence within and outside the organisation. The solution should therefore have the architectural flexibility to share data securely across systems.

Flexible deployment models

Forces will each have their own requirements in terms of how the DEM solution is deployed: on-premise (thick client or thin client), cloud, or a mixture of approaches. It's likely that their requirements will change over time, with many forces expected to migrate to the cloud in the coming years.

A force's chosen DEM solution provider should therefore be able to work flexibly, for example by supporting on-premise deployment initially (where a force has good data infrastructure) followed by a strategic transition to the cloud over time.

Where cloud deployment is a force's chosen approach, it should look for transparency from the DEM provider in terms of deployment costs. Providers should ideally be prepared to work with a force's preferred cloud provider, and not insist that their own cloud service is taken up.

Collaboration between forces

This is a small section in the context of this document, but the issue is far from small. If a force senses an opportunity for shared deployment with a neighbouring force, or regional deployment, they should look for a provider who can accommodate this.

Another useful feature of a DEM solution would be to enable the expansion of collaboration. If two forces initially collaborate they should have a solution in place that can continue to work if more forces join the partnership.

Whenever a solution is shared it is of course also important that sovereignty of data is maintained. No matter how many forces are working together on the same deployment, each force must have strict ownership of its data, and of decisions about rules on how the data is managed.

Implementation and beyond

Now that we have looked at the features of DEM solutions, we turn to three issues about implementing and managing the solutions that should be considered right from the start of any decision-making process.

Phased or 'big bang' implementation?

Our belief is that a phased approach will be suitable for most forces. A 'big bang' implementation will be logistically very difficult, whereas having a roadmap for a piece-by-piece implementation will make more sense. This will be especially true when a force has made recent investments in separate pieces of technology.

A modular approach to implementation reduces risk and incrementally delivers business benefits. It will often be advisable to tackle priority areas of digital evidence at the outset, for example focusing on the highest volume areas such as evidential interviews, CCTV and BWV.

A capable DEM solution should be able to manage those initial priorities, with the flexibility and scalability to extend to many other types of evidence.

In fact, the implementation will likely be an ongoing process, since new sources of evidence will continue to emerge. We couldn't have predicted that motorists would one day have access to dashcam devices, and new devices and technologies will appear in the coming years, each of which will need to be brought into the digital evidence world.

An implication of a phased approach over the medium or long term is that the DEM solution, and the solution provider, must keep pace with changes in the policing world. Vendors specialising in the management of digital evidence for police forces should be more proactive in this regard than with less specialist solutions.

Police-focused providers will for example keep a close watch on Digital First and other relevant matters, and shape their solutions accordingly. Providers whose solutions specialise in other sectors, or cover multiple sectors, may not be able to achieve this.

Change management

Avon and Somerset Constabulary has given great thought to the change management side of their DEM implementation. The focus has been on demonstrating to officers and staff that the programme is being implemented to benefit them, by making their jobs simpler and more efficient.

User acceptance testing and liaison with staff representatives play an important role in this. Officers and PCSOs also attend suitable training so that they can get the most from the solution.

But change management shouldn't be left to the police force. The DEM solution provider should be an active player in this process, willing to engage with management, officers and staff in whatever ways are appropriate given each force's situation and culture.

Long term support

A DEM solution should be underwritten by a comprehensive support agreement. Access to 9-5 helpdesk support may be suitable initially, but as data volumes and the number of devices grows, the solution will become increasingly business critical, so 24/7 support might be essential.

We would suggest also that forces have access to in-country supplier support from appropriately vetted IT staff, in order to comply with certain levels of security-clearance. The provider's support staff have access to sensitive data, and frequently foreign nationals will struggle to obtain clearance.

Summary: a critical solution deserves careful decision making

We finish with a question: is it realistic to aim towards having all of a force's digital evidence in one place? As far as Avon and Somerset are concerned, the answer is definitely 'yes'. From forensic images to CCTV footage submitted by local businesses, the force's aim is to put everything at the fingertips of officers and other users.

This should be the aspiration of every police force, but it will only be possible when a force has a capable DEM solution in place. Naturally, we believe that our DEM solution within our EvidenceWorks® product, achieves this and we welcome opportunities to present its capabilities to police forces.

But whether a force chooses to partner with Capita or not, it is true that an enterprise DEM solution will be one of the critical IT systems for a force, along with the likes of records, case and contact management solutions.

This is why making the right decision about a solution is so important. We hope that this paper will help forces to better understand their needs and carry out robust supplier engagement processes when sourcing a DEM solution.

In the interests of brevity and avoiding information overload we have perhaps skimmed the surface of this topic. Our team has much more expertise in this area than we could cover in the paper, so please do get in touch if you have any questions or would like to discuss things further.

Point of contact

Neil Chivers

Business Development Director
Capita Secure Solutions and Services

07736 490278

neil.chivers@capita.co.uk

Capita
Methuen Park
Bath Road
Chippenham
Wiltshire
SN14 0TW
United Kingdom

E sds.info@capita.co.uk

W www.capitasecuredigitalsolutions.co.uk

WP-CHOOSING-A-DEM 08.15 WMM