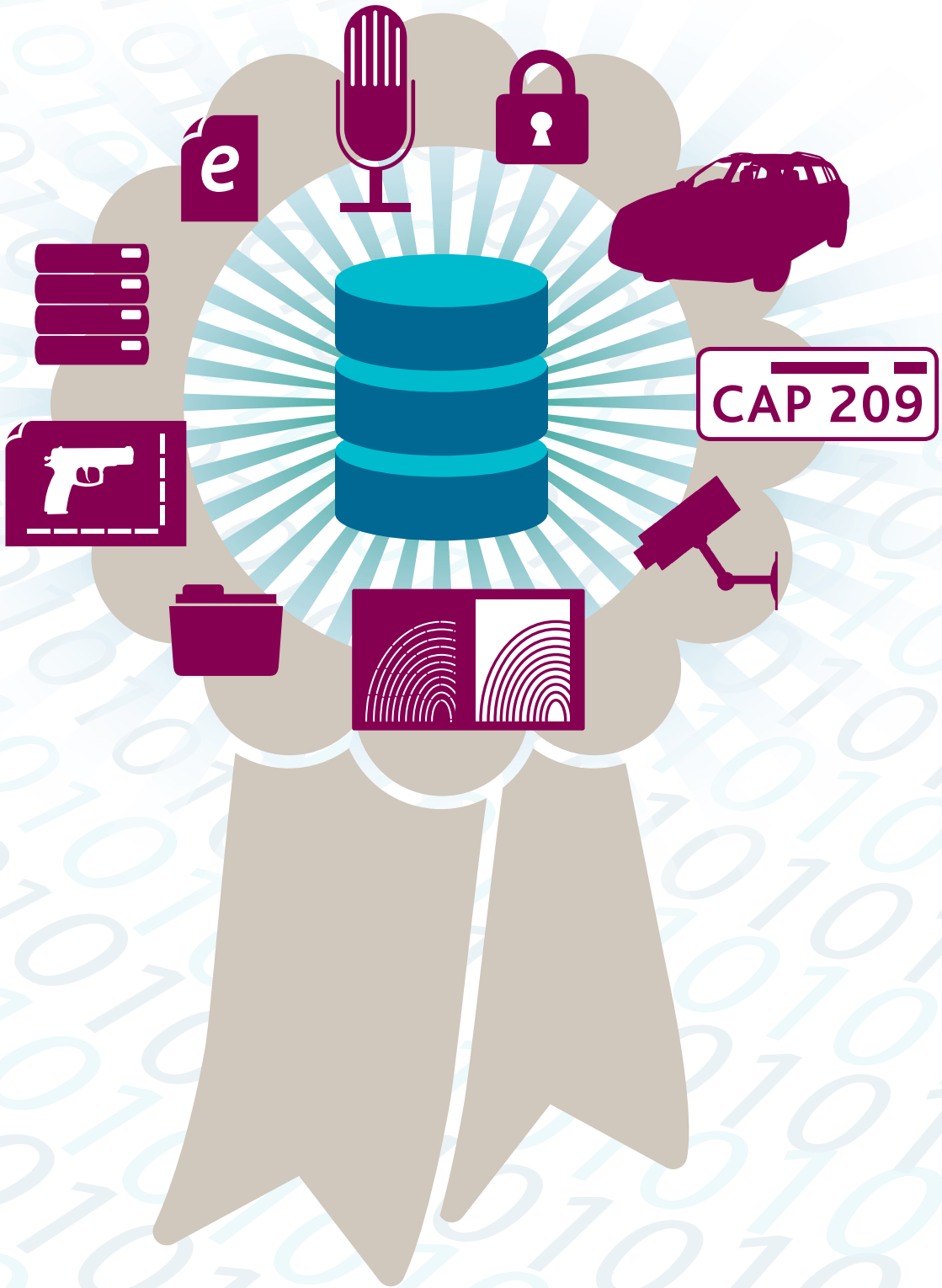
CAPITA

OPINION PIECE

Managing critical processes with a single Digital Evidence Management platform



As policies develop across the sector it is becoming an imperative to maintain a single evidence repository

Over the last few years there has been a concerted move in criminal justice systems across the world to remove paperwork and move towards a digital case file. In many cases significant funding streams have been put in place to support these initiatives.

This is bringing about technology challenges for the police, prosecutors, the courts and other stakeholders. The police are at the sharp end of managing digital information; responsible for identifying potential evidence from the vast volumes of data available, securing it, building it into cases and sharing it with those who need to see it.

The positive contribution that new and better forms of evidence can have on detection and conviction is very welcome of course. However, it also brings a significant challenge: the potential to create a mountain of new data every day that has to be downloaded, stored, catalogued, shared and analysed.

A single, managed point of access to all digital media, whether evidential or not, will:

- ↑ improve security
- ↑ improve reliability
- ↓ reduce cost
- ↓ reduce the complexity of implementing guidelines on data retention or deletion

Managing critical processes

With improved management, security and integration of data will come the ability to more effectively manage Disclosure and Subject Access Requests; two critical processes in any successful criminal justice system.

Disclosure, the provision of all necessary evidence in a prosecution, can also be far easier to manage with a single, integrated repository. The pressures of large case workloads and disparate IT systems can make items easy to miss. A single repository that uses metadata to effectively manage data, integrated to the force's Records Management System, will make the identification and packaging of every piece of data in a case much more straightforward thus avoiding accidental errors that can prove crucial in prosecutions.

Subject Access Requests, typically a request from an individual for a copy of all information held about them by an organisation, need to be treated in a private and sensitive manner. In the world of ever-increasing volumes of digital media a single, an integrated repository of data will help the organisation retrieve this data much more effectively and thoroughly than if held in numerous different systems. As such requests are focussed on an individual it is imperative that the system provides tools for redaction in order to protect other identities.

A variety of models for Digital Evidence Management (DEM) are evolving and are summarised here:

MODEL 1

Police-centric DEM with defined sharing protocols

In a national jurisdiction with a single prosecuting agency that consumes digital data from a number of individual police forces the capture, storage and management of evidential multimedia collected as part of an investigation will remain the responsibility of the force with defined protocols and interfaces to share case-specific material as required.

By way of example: The Home Office Digital 1st programme is developing a Digital Evidential Transfer Service (DETS) for forces in England and Wales.

DETS will provide a national capability to securely share evidential multimedia (video, audio, still imagery and PDF evidential documentation) between the police (providers) and Crown Prosecution Service - CPS (primary consumers).

DETS will only host copies of evidential material with the originals maintained by the force under current procedures. The material will only be held within DETS for the duration of the prosecution activities, including appeal periods, or up to the point where the CPS decides the material is no longer relevant.

MODEL 2

Police-centric DEM with data sharing portal

In a local jurisdiction where there is no requirement for a national protocol the single police DEM could be augmented with a data publishing portal that is specifically designed to publish evidence for sharing with known and authorised 3rd party organisations such as prosecution, defence lawyers and other partner agencies.

Authorised DEM users would be permitted to select evidence for publication and, when evidence is marked for publication to a recipient selected from approved third parties, an email sent with a link to the portal for them to access the evidence. Access to the published evidence could be time-limited and the nature of access controlled as follows:

- accessible by an approved nominated individual, or
- accessed by an approved group of individuals, such as prosecuting team or defence lawyers in large complex cases.

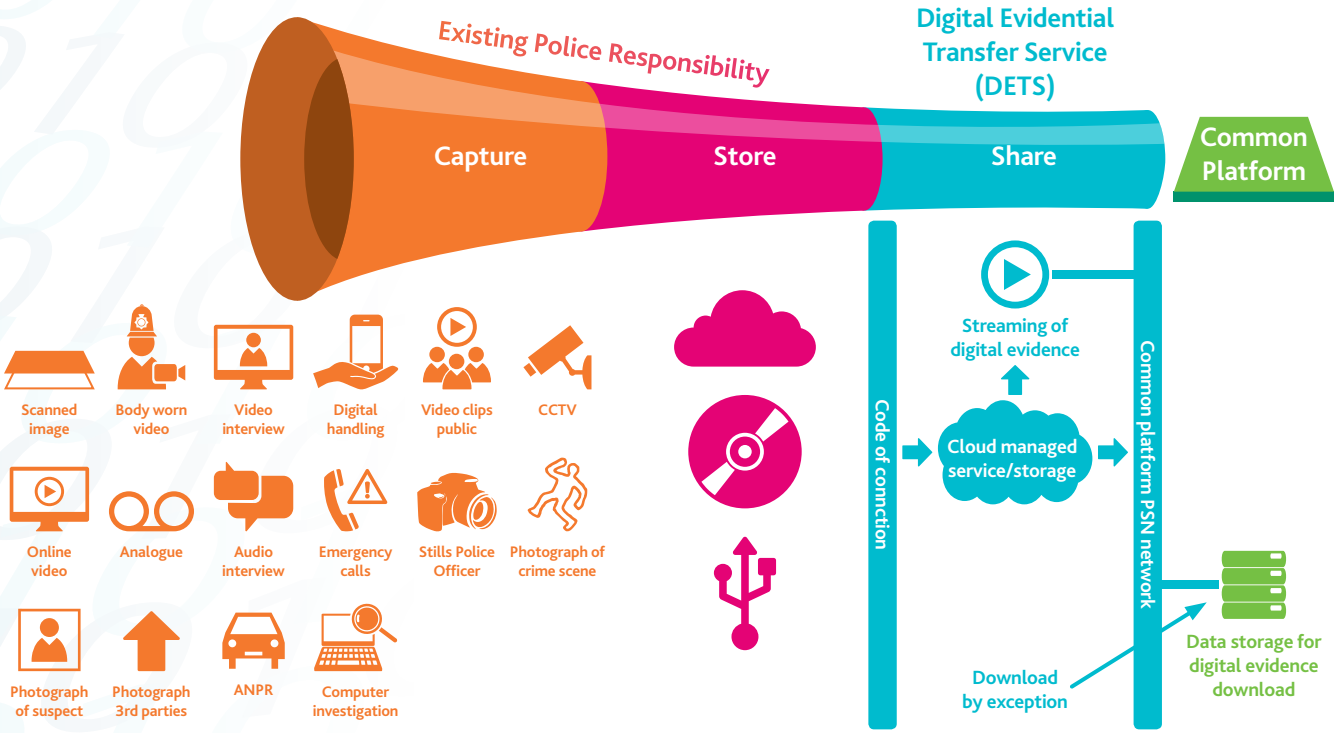
The portal should be logically separate from the police DEM to ensure that the police network remains secure and cannot be maliciously accessed by a rogue authorised 3rd party.

MODEL 3

Shared Criminal Justice DEM

Some countries and regions are modelling a combined evidential store where both the Police and Prosecuting agencies share the same DEM solution. In this scenario the DEM would be designed to allow multiple agencies to share a single digital evidence repository with an enterprise scale role based security access model that will ensure that each agency does not have access to evidence & potential evidence they are not permitted to view. This model requires the segregation of audit records such that one agency cannot see what use another agency has been making of the evidence files.

The federated access model can be complex and become cumbersome to manage with a shared criminal justice DEM solution but the technology exists to support this model today.



How Evidence*Works*® supports the models of deployment

From inception, **Evidence***Works*® has been designed and developed to provide a single, secure, scalable repository that is capable of delivering the requirements for an enterprise DEM for police forces and prosecuting agencies around the world.

Working closely with our users and with a clearly defined and funded development roadmap **Evidence***Works*® will continue to deliver an enterprise scale DEM solution with secure data sharing capabilities to support different deployment models.

Capable of being deployed both on premise, in the cloud on Azure, or supporting a variety of hybrid models **Evidence***Works*® provides a secure platform in which to collectively manage the huge array of digital evidence consistently across different teams reducing the need for training as users transfer between teams and adopt new roles. The process of sharing digital evidence with third parties remains consistent from an end-users perspective, whether responding to a disclosure request or un-solicited publication to an authorised third party. Users do not need to learn multiple siloed systems to share data between organisations regardless of the source of the originating data – BWV, Interviews, CCTV, Forensics etc.

Evidence*Works*® is "DETS ready" with a publication portal that uses the same approach as the Digital 1st programme to share digital evidence between the Police and CPS, i.e. a request and publication process for digital evidence to a separate portal to the force DEM.

Where partner organisations or agencies want to share a single DEM, the fine grained role based security model in **Evidence***Works*® can segregate access such that digital evidence is not exposed to one organisation or the other without prior knowledge and consent. **Evidence***Works*® has supported this efficient deployment model for more than three years with a consortium of four forces in the UK.

Proven and in live use across the UK and North America, **Evidence***Works*® is a natural choice for organisations wishing to consistently, securely and efficiently manage and share their digital evidence with partner organisations.

POINT OF CONTACT

Tom Edmonds

Product Manager - **Evidence***Works*®
Capita Secure Solutions and Services

07702 513267
tom.edmonds@capita.co.uk

Capita Secure Solutions and Services

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

sss.info@capita.co.uk www.capita-sss.com

@CapitaSSS Capita Secure Solutions and Services

Capita Secure Solutions and Services

WP-DEM-PLATFORM 06.18 WMM