ENLETS
Mobile

ENLETS Mobile 16th Meeting, 14/16 September 2016
Dublin, Ireland

MEETING REPORT

2 October 2016

Summary

This is the report of a meeting of ENLETS Mobile held in Dublin, kindly hosted by An Garda Síochána, the Irish Police. We are indebted to the Garda for making the meeting a great success and welcoming participants warmly for our visit to Dublin—thank you.

Highlights: further evidence that mobile solutions are gaining traction with more functionality, more programmes and more users; new examples of collaboration between countries. Important workshop on how to **start** a new mobile programme.

The meeting report covers:

- **Law enforcement**—**Garda transformation strategy** including technology and mobile components; Body Worn Video (**BWV**); **eu-LISA** and mobile solutions for refugee / migration hotspots; **Germany**: **Hamburg** Police; **Danish** Police; **Estonian** Police; **Finnish** police and border guard; National Police of the **Netherlands**: MEOS programme and SPLENDOR secure messaging app (FIOD); **Polish** Border Guard; **Slovenia**—update on ePOLICIST; **Swedish** police; **UK Home Office**—borders, immigration enforcement and national co-ordination with police; **Police Service Northern Ireland** (**PSNI**); **West Yorkshire** Police mobile programme (UK); and the SINUS mobile app used in **France** to report casualties in major incidents.
- **Industry**—presentations by **Ericsson**; **Accenture**; and **BPI Services** and **Motorola**.
- **Workshop**—a practitioner event centred on a case study of the National Police of the Netherlands MEOS to consider **how do you set up and gain support for a new mobile programme for law enforcement?** After discussion, the working group overwhelmingly **recommended** a **progressive** (iterative) approach.
- **Technology**—presentations on **critical communications**, cryptographic-based **authentication of data** (**PKI**), examples of **secure documents** in use and how they are authenticated (EUROSMART) and **biometric standards**.
- **Finally**—**participants, evaluation, reference papers** and **glossary**.

Frank Smith, Chair, ENLETS Mobile

Law Enforcement

Introductions and keynote address

Fintan Fanning, Assistant Commissioner of the Garda, warmly welcomed participants to the ENLETS Mobile meeting and to Dublin. The Garda faced many challenges shared with other law enforcement agencies taking part in the meeting, including policing and border security, and was keen to share experience with others. The Garda was keen to introduce mobile solutions to front line operations and saw the meeting in Dublin as a real opportunity to learn. He said that a further session would explain the Garda transformation strategy that had been launched recently and specifically asked if participants could tell the Garda about insights on body worn video (BWV), which the Garda were considering that week.

Frank Smith, Chair of **ENLETS Mobile**, thanked Fintan for the welcome and said he looked forward to a very useful meeting: he was sure that those taking part would see reports of further progress with these solutions. He explained that the working group had just been re-named from e-MOBIDIG because it was now a sub-group of the European Network of Law Enforcement Technology Services (ENLETS): the Chair of the Core Group of ENLETS was Pat Padding of the National Police of the Netherlands.

Garda transformation strategy

Denis Ferry described the transformation strategy launched recently for the Garda in Ireland. This was a holistic reform programme covering all aspects of police effectiveness including training, skills, operational practice and human resources, but technology in general and within that mobile solutions were seen as an important. BWV was of interest, too. The Garda saw building on the experience of European partners as a valuable part of the process. Overall, the transformation would be substantial, and the programme would require prioritisation and a phased approach over a number of years, but was crucial for the Garda.

Body Worn Video (BWV)

Frank referred to work co-ordinated by **Stephen Goodier** of Hampshire Police in the UK for the full ENLETS group. He said a critical factor in managing BWV effectively was to have a good **content management** system to receive and store material from the personal cameras. This had been emphasised by Motorola Solutions in their presentation on BWV to the previous e-MOBIDIG meeting in Finland. Privacy issues were important. Frank had sent the Garda some links to material on the internet including news of major UK purchases of BWV (Met and West Mids Police) and guidance from the UK College of Policing. Ian Williams said West Yorkshire has experience of BWV solutions. PSNI too (2,500 units). Heikki said the Finnish Police were testing a prototype with a wide-angle lens and were streaming voice and video.

Mobile solutions for migration hot spots

Ciarán Carolan of eu-LISA agreed that mobile solutions for law enforcement were at a tipping point. He suggested that they could be of real importance for registering refugees at migration hotspots—a real problem for Europe. Dealing with mass arrivals can be very difficult for the receiving country and an effective European response could include the possibility of joint resourcing between the border agencies of different Member States—but this required appropriate mobile (or at least portable) enrolment equipment able to connect directly or indirectly to EURODAC and the immigration systems of the receiving country, possibly from inhospitable locations. How to organise this was not clear. More work was needed to understand the requirements and trial a proof of concept.

Ad Van der Meijden said use of mobile devices at migration hotspots would benefit from high resolution facial image capture to enable the possibility of facial recognition (FR) as well as high quality fingerprint capture.

Hamburg Police, Germany

Peter Ludwig said Hamburg police were investing in mobile technology but were anxious to secure maximum value for money with limited resources. They were collaborating with the National Police of the Netherlands on the use of MEOS. They currently used 900 Windows 10 smartphones but were changing to Android. They had also interfaced their solution to 22 Mercedes E class police patrol pars using the dashboard display to show information from the smartphone—something that could be developed for other vehicles. There was a drive to reduce the large number of paper forms (380) is use, when building the mobile application, and to make it possible to *complete* work on the mobile device instead of double-working (starting a task on the mobile then having to change to a desktop system to complete the task).

Peter believed that more ought to be done to build on the **common element across police work** and **not over-complicating the job** with complex processes. We are all trying to do very much the same thing in whatever city or country: surely extensive customisation should not be needed every time—we don't all need a new wheel. The collaboration with MEOS was showing how this could be made a reality. Keep the rules simple and robust, fit for 90% of process; use open industry standards; develop standard software components using Service Oriented Architecture (SOA)… ideas were taking shape in the current collaboration. Could this go wider to a European level? **Patrick Padding** endorsed these thoughts—more co-operation was needed, retaining flexibility where it was necessary. He felt a new legal entity might help to make such joint co-operation possible.

Danish Police

Robert Mortensen had demonstrated a burglary app at the previous meeting: this was being used by app police districts and had recorded over 6,000 cases. 8 apps were in development for Android including people search (national and international). Collaboration was being discussed with MEOS.

Estonian Police

Annika Sepp reported that the Estonian police mobile solution described at earlier meetings was now live with users and included document authentication and checking, geo-positioning and navigation with police overlays. Users can send online feedback to the programme team from the device with comments and suggestions—this is popular, and useful to the programme team.

Finnish Police

Heikki Riippa said the Finnish Police had selected an integration supplier for their police mobile strategy and for their IT environment. A debate was being had to make their approach agile enough but also to meet formal requirements of IT security. Heikki demonstrated the prototype of a Finnish Police video communications app.

Finnish Border Guard

Pasi Nokelainen and Jussi Kosunen had spoken about and demonstrated the new Finnish Border Guard mobile solution based on a 7" tablet at the previous meeting in Finland. Further development of the application is taking place.

National Police of the Netherlands

Edwin Delwel explained that following the success so far with MEOS, already over 30,000 users, the decision had been taken to increase further the number of MEOS units. Functionality was continuing to be developed and extended to cover crime scenes, traffic accidents, heavy transport, reporting, CID and surveillance. The MEOS programme was in discussion about joint collaboration with Hamburg, Sweden, Denmark and others. The programme had received visits from several other European police forces.

SPLENDOR: Netherlands iOS Secure Chat Application

Arnoud Goudbeek of the FIOD Criminal Information and Investigation Service, Netherlands explained that instant chat applications were popular with users of mobile devices and there was real interest in having a version of such a facility for investigators which had full end-to-end security—confidential to the two parties exchanging messages and not intelligible to **any** party who might be able to access the communication in between. There was a need to do this with parties in other organisations outside FIOD. After reviewing various potential solutions, the decision had been taken to develop their own solution, SPLENDOR, which was popular with its users. This allowed chat between pairs of iOS users, using TouchID and PIN access, and was under the Mobile Iron Mobile Device Management system.

Polish Border Guard

Celina Sliwa-Tomaszewska said that preparations were under way for the next release of Polish Border Guard mobile functionality. Some rationalisation was intended as functionality on mobile devices, currently 10” tablets, mirrored the solution for desktop PCs and could be optimised better to allow smaller format of tablets to be used. The Polish Police were also understood to be starting a mobile policing programme.

Swedish Police

Sarah Hjortsmarker of the Swedish Police said that development is continuing of the mobile police application described at earlier meetings. Development capability was being expanded to run two scrum (agile) teams in parallel. Camera functionality was being planned. Communications work was being expanded. The facility for officers to rate applications they use and give narrative feedback to the programme team was proving useful and was yielding positive (and sometimes very enthusiastic!) support, building rapport with users. Sarah also said that Swedish police programme was in discussion with the Netherlands (MEOS) about collaboration.

Slovenian Police

Igor Vučko of the Slovenian Police explained that further development was continuing on the ePolicist mobile police solution described at the Slovenian meeting in November 2015. The system was being extended and was now replacing a legacy system that was being decommissioned.

Home Office, UK

Dylan Langley explained that a major transformation of technology solutions was under way in the UK Home Office and associated law enforcement services including local police forces, Border Force and Immigration Enforcement. This included the Emergency Services Network (see Critical Communications, later); police data services (Police National Computer (PNC)—criminal records, and others); and biometrics (renewal of existing national police and immigration fingerprints systems in a more coherent long-term framework). As well as national systems, local police forces and the immigration services run by the Home Office depended on their own technology systems. There had been earlier mobile solutions in use in UK law enforcement as long ago as 2002 but significant updating was being actively considered and seen as important, for the same reasons that were familiar to participants in ENLETS Mobile. Forming a practitioner forum on similar lines to ENETS Mobile / e-MOBIDIG might be useful. He looked forward to updating the working group in the future.

Police Service Northern Ireland (PSNI)

PSNI officers described the continued development and rollout of the PUMA solution presented in the Rotterdam meeting (July 2015). The innovation then was integration so that a fingerprint search could retrieve criminal and other records known to the force (previous UK mobile solutions did not have this capability). The solution now included administration functions, and push alerts and warnings. Stop and search records and fixed penalties for driving offences were now all-electronic through the device. Volume and usage was increasing. Robust auditing of the use of the device was in place. A refresh of over 3,000 devices was planned soon. Multiple platforms were to be supported for different types of user and device including Android and iOS. Mobile Device Management was to be rationalised across all platforms. Sufficiency of network bandwidth was an issue (for smartphones and BWV, above).

West Yorkshire Police, UK

Ian Williams said the West Yorkshire project aimed to improve business process. They were building a portfolio of functions including officer notebook, links to command + control, crime investigation, penalty notices and more, with relevant integration to back-end local and national systems. The force had deployed over 5,500 smartphones and a few tablets. Challenges: *thorough* testing, better collaboration and exchange of ideas on mobiles between police forces, delivering security without blocking good ideas. The public sometimes assumed an officer using a smartphone in the street must be using social media for his or her own purposes instead of doing real police work—there is a need to change perceptions!

SINUS mobile application for major incidents, France

The Chair said he had seen a report in a French local newspaper in July describing a mobile system, SINUS, used by the French emergency services to gain earliest possible understanding of the scale of casualties in a major incident. It had been deployed after the Bataclan Theatre attack in Paris, November 2015; and the lorry attack in Nice on Bastille Day, 14 July 2016. First responder vehicles carry sets of numbered and barcoded wrist bands, coded: black (deceased), red (grave injury—top priority aid needed), amber (next priority), and green (lesser / minor injury). In the event of a major incident the armbands are put on each casualty according to their injury status. A mobile app is used immediately to scan the barcode and send it to a central incident point, registering each casualty in real time with geo-location, date and time reported. This informs the central incident command quickly of the number, location and severity of injuries, helping to direct emergency teams accurately and quickly to where they were required. The information is updated live e.g. as each casualty arrives at the hospital emergency department, or if their status changes. (With kind thanks to Mrs Ros Smith for drawing this newspaper article to the Chair's attention.)

Law Enforcement Discussion

Summary output from discussion groups by law enforcement participants:

- Many applications are developed—not all are appropriate for mobile. Too much duplication?
- Good user experience is critical.
- So is battery life of the equipment.
- Develop solutions with incremental improvement over time, not big bang.
- Different ways of implementing, e.g. by browser? HTML-5? SAML 2.0?
- Young front-line officers are ready adopters of mobile tech: start with them?
- Business benefits should always be the primary driver of what you build.
- Encourage good, rapid feedback to the project team form the users. Listen!
- Leadership from the top is very important for success.
- Join mobile solutions up with the rest of the organisation.
- Need to be able to read and authenticate Mobile ID on citizen smartphones.
- Difficult to collaborate when different counties have different laws and tech.
- Need access to good website to share good practice / knowledge.
- Please can we have a reference architecture, service catalogue, glossary?
- Plan cycles / dates of ENLETS Mobile meetings well ahead. (Q1 + Q3 2017)
- Great to see such fast progress e.g. Estonia moving from ideas to delivery.
- Believe this joint working group is helping to accelerate progress like that.
- Lots of autonomy (e.g. 43 forces in UK) -> collaboration / sharing is difficult.
- Handheld and vehicle integration needs to be tackled better.
- It is a challenge to decide how much information to show the mobile officer.
- Pace of change, especially of the underlying technology, is a challenge.
- Body Worn Video—may be different privacy / legal issues in different countries.
- Do we need a group to standardise police equipment across Europe? (ENLETS?)
- A European Research Centre? (note—Antonia Rana of the EU Joint Research Centre (JRC) Ispra was there: JRC originally founded e-MOBIDIG!)

MOBIDIG, e-MOBIDIG and ENLETS Mobile

JRC's founding of **MOBIDIG**—the first meeting was in November 2008—was enlightened in recognising the potential of mobile solutions for law enforcement and the value of identification, interoperability and of working together to realise that potential. There was a slight change of name to **e-MOBIDIG**, and now, from the current (16th) meeting of the working group, to **ENLETS Mobile**. Work continues, as a sub-group of the European Network of Law Enforcement Technology Services (ENLETS). For the record here: a final opportunity to display the e-MOBIDIG logo, used for over 6 years.

Industry presentations

Ericsson

Gordon Scobbie (gordon.scobbie@ericsson.com) and **Martyn Jones** (Martyn.Jones@ericsson.com) gave a vision of public safety being transformed in the networked society, making use of capabilities in forthcoming mobile devices and networks. This would include challenges, for example balancing information access and privacy responsibly; and new behaviours, threats and challenges. Ericsson credentials include 140 years of involvement in telecoms; now active in 5G and as a subcontractor in UK ESN: it saw itself as a thought leader in mobility, including the digital citizen, responder and organisation; and was keen to engage with law enforcement organisations in this area.

Accenture

Agata Cooper (agata.cooper@accucentre.com) saw mobile solutions as essential to improve efficiency given cuts in public safety budgets. A good solution needs to be informed by what the client service has, needs, and what gap exists. Collaboration and user engagement are essential. The market is moving quickly—slow development risked delivering yesterday's solutions tomorrow. Danger signals—'red flags'—in a mobile project were statements such as "security is the most important thing" (not outcomes?); "the users will use what they are given" (even badly delivered?); "we just need to get the solution out" (design? Testing? Training?); "front-line officers won't be interested—it's an IT project" (business change is not important?); "it hasn't worked before" (why did it fail? Let's do it better?).

BPI Services

Jasper Peterse (j.peterse@bpiservices.eu) said BPI was able to develop and customise hardware and software to meet specialist needs with a good understanding of law enforcement mobile needs. This could include integration to cloud and network solutions, augmented reality and biometrics. Many developments were in the pipeline with higher resolution cameras and screens. Cross-platform compilers were available to write programs that could be loaded onto different IT platforms. BPI's new GridLer product attached an additional device magnetically to a smartphone, connecting to the host with Bluetooth Low Energy (LE).

Airwave (Motorola Solutions): PRONTO

Norman Dixon MBE (ndixon@KelvinConnect.com) of Airwave described experience with the PRONTO mobile policing solution used by 16 UK police forces. Much of police work is information management, for example around Parties, Objects, Locations and Events (POLE): digitised, mobile policing at the front end of the Criminal Justice system that can deliver better information and efficiencies for all parties. It can make information visible as never before, e.g. mobile pocket books accessible by others, to improve efficiency and accountability.

Suppliers presenting at the meeting welcomed follow-up contact from participants.

Workshop: Building Effective Mobile Solutions

MEOS Case Study—launching a mobile law enforcement project

Edwin Delwel of the National Police of the Netherlands presented a case study on how the MEOS mobile policing solution was established and delivered. The programme was set up to discover whether mobile technology could deliver radical improvements for operational policing. There was a hope that it could, but at the start, little clarity as to **how**. A conventional approach of specifying the complete system, writing a full business case, seeking authorisation, then building the solution as specified was not felt to be right. A **business change programme** was needed rather than a technical project, to build a generic mobile platform for operational policing. It would explore options, clarify what would work best for real users, discard ideas that were not good and progressively build and enhance the solution, reviewing and adapting the plan in the light of experience.

Purpose

Significant effort was invested at the start in clarifying the **purpose** of a mobile policing solution.

- **Identification** was seen as a fundamental to operational policing. Edwin said police officers everywhere need to answer two key questions: who are you? What do we already know about you?
- Answering these questions in front-line policing could be **problematic**: it was hard for the officer to distinguish people who were genuine and honest from those who were unco-operative, concealing who they were, had false, or no, ID, or where the officer made mistakes typing in ID details.
- **Mobile technology** was seen as having great potential to resolve such problems by giving the officer real-time access on the street to systems otherwise only available in the police station, for example checking names and addresses; driving license, fingerprints or other records; and, when a true identity was revealed, the information known about that person.
- **Officer safety** could be improved by alerting the officer discretely if someone they were questioning on the street had convictions for assaulting police, or where other relevant information existed.
- **Data errors** and delays in completing penalty tickets or recording details for other processes manually on the street and later reviewing and entering the data in the police station can mean that many tickets cannot be enforced—real-time entry by a mobile device direct to the central system of data that is **verified online** can eliminate most of these errors and speed up the process. (The law was changed to allow tickets to be issued electronically without having to print an individualised ticket, making this more efficient.)
- Some **fundamental principles** were established early on:
    - **Keep it simple**, not cluttered: quick / easy real-time information.
    - **Streetsmart**—robust solutions that work in the real world of operational policing out on the street.

- The **user interface** is as simple as possible but allows enquiries to be interrupted if something urgent arises; but previous enquiries and results can be returned to and re-used. The results of a search that has identified a driver can be used to issue a penalty ticket without having to re-enter the person's details.
- **Verify data input** at the start—has benefits all down the line.
- Design the system so that it can be made to work on **all platforms**.
- Support **frequent updates** so that new functionality can be added regularly and incrementally, using agile development.
- **Re-design business processes** to exploit mobile technology—don't simply automate the existing (pre-mobile) manual processes.
- Re-use **generic functions** as widely as possible for 90% of cases rather than customise processes for the 10% of special cases.
- Define **common data entities** such as date/time, location (GPS), vehicle, statement, goods, etc. and re-use them across the system.
- Make the platform **secure enough** for its intended use. Excessive security it expensive and complicate the solution. The system can record extensive log files to create an **audit trail** of how it is used.

People

People issues—the stakeholders for the programme—are crucial to the success of the MEOS programme, in several ways.

- **Front-line, operational users** are central to the design and development of the solution. Experienced officers join the development team working closely with technical experts: solutions are developed jointly. Nothing is released for use unless real users agree. Users feel—rightly—that they **own** MEOS.
- **Experimentation** is a clear part of the programme mandate. That means ideas can be tried to discover what works: authority is not needed at every step and avoids provoking resistance from people discussing an idea without seeing how it might work. Ideas that don't work can be dropped privately; successful ideas can be shown to stakeholders and to gain approval. **Piloting** with selected operational users tests that new ideas really work before full rollout. Over time a track record of achievement is established that strengthens **trust and confidence** in the programme, which is important.
- **Financial approval** with a phased programme is in manageable stages—overall MEOS is still a substantial cost, but the commitment for each phase is reduced compared to a single proposition and there is confidence in the results from previous stages. A strong focus on **benefits** is important for stakeholders. In the early part of the programme careful analysis was undertaken of the early projected benefits: even for an initial set of functions, given a large base of operational users the overall results were impressive. Because the programme was new, external researchers reviewed the benefits and confirmed the estimates (in that first example, expected to exceed 500,000 hours of officer time per year). Small benefits per further transaction have built substantially on that initial base.

- **Leadership is essential**. That means steering the programme content successfully, developing future plans, but given the importance of the **way** of working described here, maintaining that approach through multiple tasks and people is important. Maintaining motivation and conviction that the outcome will be successful—as the evidence has shown.
- **Co-operation is not guaranteed**—Pasi Nokelainen had said in a previous meeting programmes need to deliver good mobile solutions because mobile devices are harder to supervise and users will find excuses not to use them if they don't like them. The Swedish system allows satisfaction ratings and comments by users. Edwin said users felt they understood mobiles and used them widely e.g. for WhatsApp, internet etc. They will expect excellent service and be critical if they don't—or use their own solutions even if not allowed.

Integration and infrastructure

- Integration is needed between the front end of the system (the mobile devices and their immediate services such as Enterprise Mobile Management), and the back end connections to all the systems users need to communicate with. For example, a name search in MEOS may access 21 back end systems; other transactions need to access driving licence, passport, fingerprint and penalty management systems, and others. Many of these back end systems are legacy systems and may be old, not built to work efficiently with a large mobile population of users—all of this increased complexity. The effort required to build the front end of MEOS and the bridge layer to legacy systems MEOS connects to are of comparable scale and effort.
- Developing, running and where necessary extending all this infrastructure is a significant task and requires a strong architecture function.

Training

Some classroom training is provided for MEOS users, but it is limited. Other provision:

- A practice copy of the solution is available containing test data.
- A training app is provided with slides, videos, information to read.
- U-turn forum is provided online for self-help questions / tips between users and a help/service desk.
- Helpdesk is available for telephone callers
- Video news bulletin is sent monthly to users—new things, tips, updates

Timeline

- Early 2010—the MEOS programme was mandated to begin.
- July 2015—Edwin Delwel described in the Rotterdam e-MOBIDIG meeting that the MEOS solution was being piloted with 1,500 users.
- November 2015—Slovenian meeting: MEOS now in use for >20,000 users.
- September 2016—Dublin: >30,000 current users; decision made to increase further the number in use.

Discussion

- Workshop participants discussed whether the approach described by Edwin and the MEOS team was essential when delivering a law enforcement mobile solution. The presentation has been very informative and participants were persuaded this approach should be **recommended** by **ENLETS Mobile**, rather than a more traditional 'sequential' approach of specifying, justifying, building and rolling out the whole solution as one unit.
- There was some debate over the use of **package solutions** for law enforcement mobiles systems. A 'package' approach is possible in many contexts in business computing: possible **advantages** can include lower cost from sharing software used successfully by others; the **disadvantages** can be less scope to develop the software exactly to any one user's preferences. During the meeting we had heard about solutions built by a police force for their own use; a collaboration for other forces to use such a system elsewhere; and a commercial package bought by multiple forces. Whatever approach is used the solution must be an acceptable fit to each customer's needs. Use of a solution developed elsewhere did not mean the organisation could miss out key activities thought important by ENLETS Mobile participants, including clear leadership by the law enforcement agency who will use the system; excellent user engagement; piloting; interfacing to all the right local IT systems; and the capability to respond in an agile way to new requirements and priorities. This may be a topic to discuss further to at future meetings.
- Frank Smith had discussed the **procurement of mobile solutions** shortly before the meeting with a supplier who had attended previous e-MOBIDIG meetings. He volunteered the insight that suppliers could find difficulties where a customer insisted on specifying the solution in detail before the contract was let. If different requirements became apparent as the solution was developed, the contract might well make it difficult to change the design in that way. This thinking corroborates the MEOS programme approach, from a supplier's perspective.

Inventory

Pat Padding had requested that an inventory of mobile programmes to be made to show expected progress over the next two years, and what ENLETS Mobile might be expected to be doing over that time.

Job started with the updates already recorded in the Law Enforcement section, above. More to be done to consider what further work would be profitable to do.

Technology briefing

Critical Communications

Frank Smith reported on his attendance at the Critical Communications World (CCW) conference in Amsterdam in June 2016, attended by a wide range of experts (see separate paper). Critical communications networks are used by emergency services such as police and ambulance. Over more than 20 years the specialist needs of these users have been met by special networks using TETRA and TETRAPOL standards which are specialised for critical voice requirements, but are not so good for mobile data, increasingly demanded by emergency services, as it is by business and society generally.

In the long-term critical communications will move away from TETRA and TETRAPOL to networks based on the Long Term Evolution (LTE) protocol for 4G and expected to be the basis for future 5G networks. This is good for data but requires voice to be sent digitally using the Voice over LTE (VoLTE) protocol. LTE is being enhanced to support more use cases for the future, particularly 5G and including critical communications features such as Push to Talk. Some at the CCW conference questioned how mature LTE is for critical communications. The UK will be an early adopter of LTE in its Emergency Services Network (ESN) to roll out in 2018 and 2019, based on the commercial UK mobile network by EE, enhanced for better connectivity and resilience.

Few participants in the ENLETS Mobile meeting used TETRA or TETRAPOL for their mobile solutions. Frank highlighted that as mobile law enforcement solutions grew rapidly and became used for more critical functions such as Command and Control, the use of critical communications networks would increase.

Heikki Riippa, Finnish Police, reported on some recent developments in Finland: a small LTE base station that could be carried and operated from a rucksack; and the same equipment suspended from a tethered balloon, to extend coverage—a temporary deployment to cover a network failure or a high-demand special event. Heikki is involved in the EU **Broadmap** project to develop requirements for the next generation of LTE critical communications networks: he urged national mobile programmes to make contact with their lead representative for this work.

Secure Authentication and Digital signatures (PKI)

Jeen de Swart, Dutch Ministry of Justice, gave a briefing on the security technology used to authenticate data read from the chip of a passport or messages sent over a network. The technology is known as Public Key Infrastructure (**PKI**), named because of the type of encryption used. This can deliver **trust**, **proving** that data protected and authenticated in this way comes from the expected originator, and has not been amended from the version digitally 'signed' using public key encryption by the originator.

PKI has several important applications for mobile devices such as authenticating data read from passport and card chips; authenticating data a mobile device receives over the air; and authenticating that the device is genuine when it connects to another system.

A passport includes important physical security features in the design. In addition, the title page includes 2 lines of formatted text, the Machine Readable Zone (**MRZ**) designed to be optically scanned. The MRZ is protected by some checksum information though this is not secure enough to protect against all errors or forgery.

ICAO e-Passport symbol

Information from the MRZ is used to open the **chip**. Since 2006 most new passports have included a secure chip containing a copy of the MRZ and a facial image of the holder. EU Schengen documents also contain two fingerprint images of the holder. The chip is opened and read using Basic Access Control (**BAC**) or by Password Authenticated Connection Establishment (**PACE**), but neither authenticates that data on the chip is genuine.

Cryptographic tests must be performed to authenticate the data after it is read, using secure encryption built into digital signatures of the data as 'signed' by the originator. Passive Authentication (**PA**) authenticates the data. Chip Authentication (**CA**) or Active Authentication (**AA**) authenticates that the chip is genuine and has not been copied (cloned). Further security is used to control access to fingerprint images on Schengen passport / card chips, under Extended Access Control (**EAC**).

Secure documents

EUROSMART
The Voice of the Smart Security Industry

Detlef Houdeau of the EUROSMART trade association (and Infineon) gave a comprehensive round-up of the different types of secure documents that might be encountered by an officer using a law enforcement mobile device. Each contains secure chips and digital signatures, as described by Jeen, above. Discussion following the presentation highlighted that although the different types of document have many conceptual similarities, different security and technology solutions are needed to be read and authenticated each type. The examples Detlef described were:

- **Passports and ID cards**—passports and residence permits including ICAO 9303 chips (1st generation); with Schengen EAC fingerprints (2nd generation); and the same with PACE added (3rd generation). EU ID cards accepted for travel do not have to follow the same standards as passports—various approaches are taken.
- **Electronic Driving Licence (eDL)** documents—EU regulation 383/2012 (not fully consistent with ISO/IEC 18013); can use contact or contactless access.
- **Tachograph cards**, 1st generation (required by May 2006) and 2nd generation (rolling out 2016 to 2020). Separate cards and readers are needed for the driver, the transport operator, garage mechanics, and traffic authorities.
- **Electronic Identity (eID) cards**—eIDAS scheme (EU regulation 910/2014) for electronic identification and trust services for electronic transactions in the European internal market. It provides for the interoperability of national eID schemes based on the eIDAS standards.

Biometric Standards

Geoff Whitaker gave an update on biometric standards (see slides).

PARTICIPANTS

- **Frank Smith**—Chair, ENLETS Mobile (formerly, e-MOBIDIG)
- **Fintan Fanning**—Assistant Commissioner, An Garda Síochána (Irish Police)
- **Supt. Pat Ryan**, Garda, IT Operations—meeting host
- **Pat Padding**, Dutch National Police, Core Group Co-ordinator, ENLETS

- **Arjen Baan**, BPI Services, Netherlands—Director
- **Fintan Brady**, Garda—IT
- **Ciarán Carolan**, eu-LISA—biometrics, mobiles and border security
- **Agata Cooper**, Accenture—mobile specialist
- **Cor de Jonge**, Dutch Ministry of Justice—PKI programme manager
- **Edwin Delwel**, Dutch National Police—mobile programme manager (MEOS)
- **Jeen de Swart**, Dutch Ministry of Justice—senior information architect PKI
- **Norman Dixon MBE**, Airwave (Motorola Solutions)—Business Consultant
- **Kieran Downey**, Garda—IT
- **Bill Egan**, Garda—IT, meeting support / mobile solutions
- **Supt. Denis Ferry**, Garda—Reform Programme
- **Michael Fischer**, Austrian Criminal Intelligence Service—Deputy Director
- **John Flahive**, UK Home Office—police systems architect, incl. mobile
- **Anoud Goudbeek**, Dutch financial investigation service (FIOD)—security officer
- **Daniel Heeb**, Swiss Customs—head of applications and data
- **Sarah Hjortsmarker**, Swedish Police—mobile programme lead
- **Szabolcs Horvath**, FRONTEX—co-ordinating officer
- **Dr. Detlef Houdeau**, EUROSMART trade association, and Infineon
- **Tapio Inkeröinen**, Finnish Police
- **Martyn Jones**, Ericsson—Engagement Manager, Public Safety + Security
- **David Kelly**, Garda—IT
- **Jussi Kosunen**, Finnish Border Guard—mobile project
- **Liina Lakur**, Estonian Ministry of the Interior—mobile IT
- **Gerhard Lang**, Austrian Crim. Intel. Service—head, crime strategies / innovation
- **Dylan Langley**, UK Home Office (BAE Systems)—law enforcement mobiles
- **Peter Ludwig**, Hamburg Police, Germany—lead project manager, MobiPol
- **Mike Lyne**, UK Border Force—mobile technology
- **Stefan Maxwell**, UK Home Office—programme manager, biometrics
- **Robert Mortensen**, Danish National Police—mobile project
- **Pasi Nokelainen**, Finnish Border Guard—mobile border application lead
- **Jasper Peterse**, BPI Services, Netherlands—sales manager
- **Kalle Putk**, Estonian Ministry of the Interior—mobile IT

- **Antonia Rana**, European Commission—Joint Research Centre (JRC)
- **Heikki Riippa**, Finnish Police—critical communications / EU Broadmap
- **Marcel Romer**, Dutch National Police—MEOS architect
- **Pawel Sadownik**, FRONTEX—ICT unit
- **Dr. Evangelos Sakkopoulos**, Greece— Interior Ministry, immigration systems
- **Morten Olsen Sandnes**, Norwegian Police
- **Gordon Scobbie**, Ericsson—Head of Public Safety + Security, W + Cent. Europe
- **Annika Sepp**, Estonian Ministry of the Interior—ePOLICE mobile solution
- **Wim Setz**, Dutch National Police—mobile solution
- **Celina Sliwa-Tomaszewska**, Polish Border Guard—IT expert / developer
- **Brendan Smith**, Garda—IT procurement and Infrastructure
- **Donald Smith**, Immigration Enforcement, UK Home Office—mobile solutions
- **Heather Smith**, West Yorkshire Police, UK—IT project manager
- **Magnus Thorp**, UK Home Office (BAE Systems)—law enforcement mobiles
- **Ad Van der Meijden**, National Police of the Netherlands
- **Igor Vučko**, Slovenian Police—ePOLICIST mobile strategy / programme
- **Stefan Wendt**, German Border Guards
- **Geoff Whittaker**, UK Home Office, Centre for Applied Science and Technology
- **Ian Williams**, West Yorkshire Police, UK—lead for digital mobile
- **Eldrid Williksen**, Norwegian Police
- **Margaret-Mary Wilmot**, UK Home Office—mobile programme manager
- **Police Service Northern Ireland (PSNI)**—3 mobile solution specialists

Apologies—not able to attend

- **Ian Bell**, Cambridgeshire Constabulary, UK—Chief Technology Officer (CTO)
- **David Driezen**, UK Emergency Services Network (ESN) programme
- **Marco Facchini**, Italian State Police

Evaluation

Of the participants rating the meeting, **92%** scored the event as **good or very good**. The **average score was 4.5**, on the scale of very good = 5 and very poor = 1.

In more detail: of 53 participants in the meeting, 36 (68%) completed an evaluation sheet. Of these, 19 (53%) rated the meeting as very good; 14 (39%) as good; 2 (5%) as OK; 1 (3%) as poor and none as very poor. The evaluation was conducted at the end of day 2, attended by most people.

Useful narrative comments were also made which we will take into account… many thanks to all who attended.

Reference papers

Reports and presentations to go onto a new ENLETS Mobile website soon.

Presentations—open access

- (1) West Yorkshire Police—Ian Williams
- (2) Hamburg Police—Peter Ludwig
- (3) Ericsson—Gordon Scobie and Martyn Jones
- (4) BPI Services, Netherlands—Jasper Peterse
- (5) Airwave PRONTO—Norman Dixon MBE
- (6) Chip technology for mobile devices (PKI)—Jeen de Swart
- (7) Biometric Standards Update—Geoff Whitaker
- (8) EU eDocument standards and mobiles—Dr Detlef Houdeau, EUROSMART

Presentations—government access only

- (9) Mobile solutions for Migration Hotspots—Ciarán Carolan, eu-LISA

Papers—open access

- (10) Biometrics and mobiles: BTT article—Frank Smith
- (11) Critical Communications World report—Frank Smith

Glossary

BWV	Body Worn Video used here, or **BWC**—Body Worn Camera
EES	EU Entry Exit System (proposed—see previous meeting report)
ENLETS	European Network of Law Enforcement Technology Services
eu-LISA	EU agency running SIS II, VIS, EURODAC and sTESTA… and EES?
FIOD	Dutch financial investigation service
LEWP	Law Enforcement Working Party—parent body for ENLETS
LTE	Long Term Evolution
MDM	Mobile Device Management (**EMDM**: Enterprise MDM)
MEOS	Dutch Police mobile solution
PKI	Public key Infrastructure
PSNI	Police Service Northern Ireland