Conference Report
eu-LISA Annual Conference

Going Digital for a Safe and Secure Europe

17-18 October 2017
Tallinn, Estonia - Hotel Hilton

eulisaconference.eu
eulisa.europa.eu
eu2017.ee

Printed by Ilotrükk in Estonia
Luxembourg: Publications Office of the European Union, 2017

Photo Credits: Sven Tupits

This report is based on audio/video recordings and notes taken during the Conference. It does not purport to reproduce in extenso all debates and intervention. The opinions expressed are those of the speaker(s) only and should not be considered as representative of eu-LISA's official position.

ISBN 978-92-95208-62-9
doi:10.2857/033024
Catalogue number: EL-06-17-127-EN-N

Conference Report
eu-LISA Annual Conference

Content

Day 1 (17 October):

Keynote Addresses:
Going Digital - IT solutions for a safe and secure Europe

Krum Garkov,
Executive Director of eu-LISA

In his opening address, Mr Garkov greeted all attendees and those watching online on the occasion of the Agency's 4th conference, noting that it took place as the 5-year anniversary of the Agency's establishment approached. He expressed his pride at bringing together participants from the private and public sectors across Europe, noting that the subjects of the conference were chosen in cooperation with the top experts and decision makers in the field and in a timely manner.

Mr Garkov began by recalling that a safe and secure Europe is a priority of the Estonian Presidency of the Council of the European Union, which is also why it was chosen as the main topic of the conference – it reflects shared European values. More specifically, he noted, the intention was to enable exploration of how going digital can strengthen European security and border management. He went on to explain that practitioners are especially interested in hands-on aspects of digital solutions that affect law enforcement, border control and migration management.

According to Mr Garkov, despite doubts and concerns about turning real life into bits and bytes, we are already well advanced in the digital revolution. We started this revolution voluntarily, realising that it presents opportunities for next generation public services and should have a positive impact on society. This belief is shared by two thirds of European citizens. In just 3 years, there will be more than 4 billion internet users in Europe and more than 26 billion connected devices.

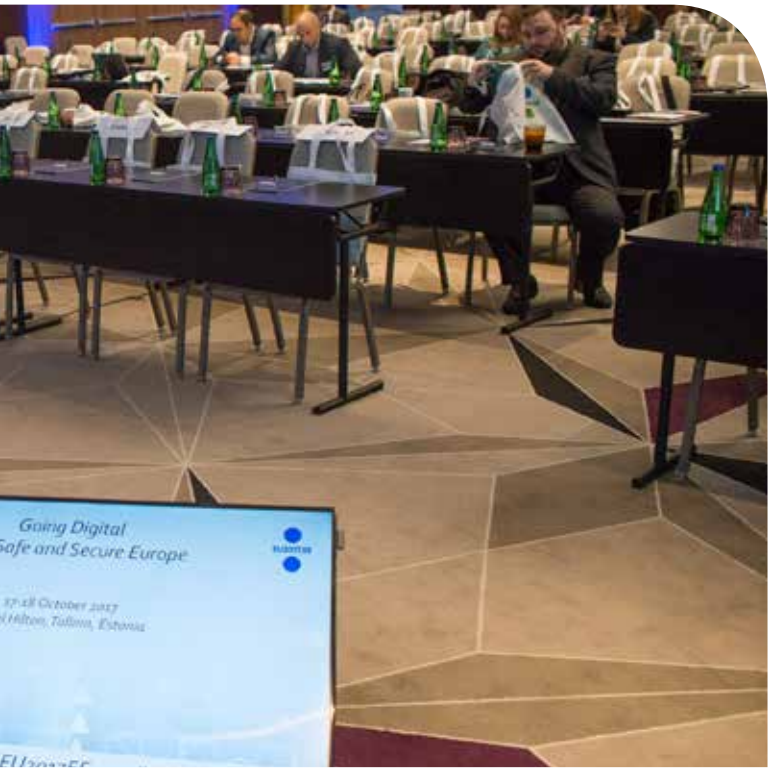
Digitalisation is a part of our daily life – exemplified by the everyday usage of digital solutions for ordering taxis, booking flights and purchasing products. Like all previous revolutions, there is an engine behind it. While for previous revolutions the engines were water, steam, electricity and electronics, when it comes to the digital revolution, the engine is data, which is the main fuel that creates value. Mr Garkov stated that how we use this data will be the measure of our success. We have to work even smarter, customise tools and services and use them best to serve the demands of society.

At the Digital Summit, Mr Garkov recalled, we were reminded that cross-border data flows were not invented yesterday, they have existed since at least 2005. Yet since then, the amount of data transferred across borders has increased 45 times, and in the coming 5 years is projected to grow some 10 times more. Novel solutions will fundamentally change jobs in many areas, including, for example, in the border management domain.

Mr Garkov went on to describe how he has been an IT enthusiast and early adopter from an early age,

as technology makes our life easier and helps to make work more efficient. He jokingly added that, of course, his son's relationship with his tablet is more passionate than his own could ever be. Sharing information is a crucial part of connectivity. However, privacy, data protection and security are critical to ensure sharing only occurs within our individual boundaries. We expect it from those who manage data. In Europe, data protection, privacy and security sometimes inhibit rapid exploration. Apparently, the digital revolution has a price that needs to be paid, and holding back digital potential seems to be that price.

However, as Mr Garkov explained, the digital revolution is not happening in a vacuum. Today, Europe faces a dual challenge. One the one hand, we aim to stay open as a part of the global world contending with increasing international mobility; more people are coming to Europe to study, for work and pleasure, and to seek asylum. The EU is faced with the consequences of instability in its close neighbourhood. On the other hand, we still need a life with adequate security, fully respectful of fundamental European values.



Technology has developed rapidly, and it affects everyone's daily life. However, it comes with a price – a dramatic increase in security challenges. Cybercrime cases are growing, terrorism remains a threat, utilising as it does new social platforms, and cross-border crime is continuously evolving. To address these challenges, the EU will have to consolidate successful policies.

At the same time, we face a very rapid transformation in the Justice and Home Affairs (JHA) area – fast convergence between border management, internal security and migration management. The digital revolution will continue to impact the EU policy domain, which is why we should already today explore technologies to make border management, internal security management and migration management stronger and smarter. Interoperability is an important way to achieve that, he argued, as would be discussed later in the conference.

Mr Garkov explained that in the context of the ongoing digital revolution, the Agency's role will be changing. The Agency will have to act as a significant contributor to JHA policies. But in doing so, it will face challenges. Foremost among them will be the fact that as well as focussing on its core tasks related to the operational management and development of large-scale IT systems 24/7, it will have to increase its contribution to Member States and the EU as a whole, capitalising on its knowledge and capabilities.

Reflecting on the conference that was to follow, Mr Garkov noted that all these mentioned topics would be discussed and the impacts of digital transformation will be analysed. The focus would also be on interoperability, which has become a key concept not only for practitioners but also for policy makers and EU policy as a whole. The conference would explore visions, but also practical examples such as the European Search Portal and the shared Biometric Matching Service.

He informed the participants that for the first time, the conference would also feature an innovation day, focused on topics including mobile devices, secure platforms and enhanced data processing. Mr Garkov assured the listeners that although such discussions might sound very technical, it would be clear that solutions are not about technology but about people – particularly about meeting the expectations of EU citizens who are concerned about security and their future. He expressed his belief that the ideas exchanged over the 2-day conference would empower eu-LISA to further develop as the EU's digital centre of excellence. He concluded by wishing everyone a successful conference.

Andres Anvelt,
Minister of the Interior of Estonia

Firstly, Mr Anvelt expressed his pleasure at opening the annual conference and having the chance to discuss opportunities and challenges in going digital for a safe and secure Europe. Before starting, he put forward his view that holding these conferences has become a very good tradition and expressed hope that they will continue.

He began by stating that it should not be a surprise that the key priorities of the Estonian Presidency include a focus on promoting a digital, safe and secure Europe. He was happy to see that the various dimensions of this topic were so comprehensively covered in the conference. Before attempting to be an oracle, looking towards the future, Mr Anvelt chose to briefly look back at the previous 5 years. In 2012, he noted, one of the coolest phones was a Samsung Galaxy S3; the average internet speed was 2MB/s; digital music accounted for only 35% of the global recorded music revenue; the sale of audio books was twice that of e-books. Before 2012, there was no eu-LISA, he recalled. Today, he stated, we have the Galaxy S8. We can browse social media at speeds of 1GB/s. Digital music now has 50% of global music markets. However, the sale of e-books dropped, and statistics show that people have returned to printed books. Some things don't change, he wryly noted.

eu-LISA has also changed in the time since 2012, he noted, taking up as it has the challenge of making sure that the Schengen area can function properly. Mr Anvelt recalled that in 2012 eu-LISA managed the same 3 systems that it does today, at least by name. Yet these systems were completely stand alone and located in separate places. The Eurodac we had then is not the one we have now, he argued. Today's system is a completely new system that asylum

authorities use intensively. The migration crisis two years ago put an unprecedented pressure on the EU in terms of the numbers of irregular entrants and asylum seekers. Mr Anvelt explained that the Estonian Presidency will seek to progress the reform of the Eurodac system in order to achieve a situation where those who are not authorised to stay could be returned to their countries of origin. However, in the interest of fully understanding the European asylum system, we have to upgrade Eurodac and turn it into a full-case management system like the Visa Information System (VIS).

Mr Anvelt went on to similarly look at the evolution of the VIS in the preceding 5-year period. In 2012, it was only usable in a few regions and was undisputedly not the same VIS that we are using today. In the past years, it has developed so as to allow around 40 million Schengen area visas to be issued annually to visitors from third countries. It is a vital tool enabling visa information to be exchanged swiftly, preventing visa shopping and helping to fight terrorism and serious crime.

The Schengen Information System, meanwhile, went operationally live as a fully new version in spring 2013, he noted. Since then, the number of inquiries to SIS has increased 4 times. The system is the most successful EU large-scale information system, allowing, for example, law enforcement authorities to exchange information about missing or wanted people.

However, he admitted that work is not finished and constant development is needed. This, he noted, was particularly true given his belief that the role that digital services can and will play in promoting security and trust is constantly increasing.

He stated that Estonia has emphasised use of IT systems for secure citizen-government and G2G communication, with a clear focus on innovation and safe exchange of information. He expressed his happiness in being able to see the same progress at the EU level, where a number of processes in justice and home affairs are undergoing a digital transformation. New systems are being set up, such as the EES, ETIAS, PNR, and European Criminal Records Information System for Third Country Nationals (ECRIS-TCN).

Mr Anvelt continued by showing a video of how Estonian IT systems for law enforcement function – a good example of interoperability at the national level, he suggested. One example that he highlighted from the video was the Estonian e-police system, recently updated such that all now patrols have tablets that speed up inquiries and enable information exchange on-the-go. Checks on missing persons, vehicles and ID document can all be done quickly with one device. With such a development, Mr Anvelt stated that the safety of the Estonian people has taken a step forward. He expressed his appreciation of the fact that interoperability is on the agenda for Europe and that it would be discussed in-depth at the conference.

He went on to voice a small, but important point – when developing a digital strategy, it must be considered that technology is only a tool, and every tool can have hiccups. Like skyscrapers have stairs, similar measures need to be in place for IT, he argued.

He expressed another concern, which falls under the domains of Commissioners Vera Jourova, Dimitris Avramopoulos and Julian King. To improve access to systems across borders in the EU, it is crucial that e-CODEX finds a competent operational manager. e-CODEX is the key for exchanging European Investigation Orders and for e-evidence, both so important in the Home Affairs area. The Council is ready to start discussing the proposal and Mr Anvelt called on the Commissioners to submit their proposal this year.

Next, Mr Anvelt took a peek into the future, to discuss possible needs in 2025. He stated a belief that it is important to start working towards those goals today, so that we don't look back on missed opportunities at a later stage. He put forward two main areas requiring special attention – user experience, and trust and transparency. When considering user experience, we should not forget that our customers are not only police officers and border guards, but citizens and visitors from third countries. We have to design IT systems with a focus on customers and interoperability is just the first step in the right direction, he argued. We have to measure user experience in real time and adapt systems swiftly. The digital transformation raises doubts and concerns in society that often related to trust and transparency, he noted. If we strive to be leaders on a global scale, it will require us to process more data than we do today. However, Mr Anvelt said that we have to send a clear message – that the data entrusted to us is safe and secure and that all manipulations are traceable. Blockchain will allow this, but we have to be smart enough to demand the use of all modern technologies at the political level. Mr Anvelt stated that we should support eu-LISA in developing into a centre of excellence that can advise us in these transformational times.

Mr Anvelt went on to emphasise that the Presidency priority is to put various IT systems and technologies at the service of the citizens in order to keep the EU more safe and secure. He stated that work will continue to make the exchanges of data between IT systems run smoothly by 2020. He stated that Estonia is a good example of how interoperability has strengthened our law enforcement to be more efficient and has decreased crime. The EU has to take the same road because its citizens deserve the highest levels of security possible.

He finished by reminding the participants that the EU information systems in the JHA domain are developed and managed by eu-LISA. Both the European Parliament and the Council are working on eu-LISA's new mandate. The increasing demands on the Agency will require more resources for the Agency to fulfil new assignments. Mr Anvelt expressed hope that he could count on the support of all Member States during the negotiations of the new mandate. He concluded expressing a hope that in 2018, the conference would be held in eu-LISA's new premises, which the government hopes to hand over to the Agency in June 2018.

Dimitris Avramopoulos,
Commissioner for Migration, Home Affairs and Citizenship

The Commissioner provided his input through a video message shown to attendees, having had to cancel his participation at short notice. He began by expressing his regret at not being able to attend in person, noting the relevance of the conference and the topics being discussed given that our lives are becoming increasingly digitalised and that all dots need to be connected in an increasingly digital world.

The importance of smooth information exchange between Member States, EU agencies, law enforcement and judicial authorities was well known to attendees, he suggested, and requires deployment of digital solutions to be undertaken effectively. Going digital in security is therefore a must to effectively target security threats, he argued, and eu-LISA is at the very heart of this. Commissioner Avramopoulos stated that we need

to build an environment of trust and Member States have to demonstrate trust. We have a range of instruments at the disposal of our law enforcement and security authorities and what matters now is to use these systems well, he suggested. The dots need to be connected both at national and EU levels. All parties need accurate information from information systems to make the right decisions at the right time. According to the Commissioner, eu-LISA will be a cornerstone for the EU's work on interoperability. It already plays a crucial role through its management of SIS, VIS and future systems such as the EES. That is why, he suggested, that the Commission submitted a proposal for a stronger mandate for the Agency in June. Once adopted, this mandate will reflect eu-LISA's role in properly connecting the dots. It will give the Agency the powers, tasks and resources needed to host our existing and future systems, to ensure data quality and security, to make sure they work like clockwork and in the end enhance the security of our citizens.

The Commissioner concluded by stating that in an increasingly digital world, the safety of our citizens' matters and is one of our main priorities. He expressed a wish that all participants could engage in fruitful discussions and urged that we have to make the most of the opportunities that technology offers. Finally, he expressed his conviction that eu-LISA and its fantastic specialists will rise to the challenges that lie ahead.

Session 2:
The Digital Transformation - Looking forward

Moderator:
Stephan Brandes,
Head of Application Management and Maintenance Unit, eu-LISA

Panellists:
Filip Pynckels, Director-General IT, Federal Ministry of the Interior, Belgium
Richard Ares Baumgartner, Senior Strategic Advisor of Frontex
Luis de Eusebio Ramos, Deputy Executive Director of Europol
Lauri Lugna, Secretary General of the Ministry of the Interior of Estonia

Introduction by **Filip Pynckels,**
Director-General IT, Federal Ministry of the Interior, Belgium

Mr Pynckels provided some opening views on the topics to be discussed by the panel. Introducing himself as a mathematician and IT guy, he suggested that he had initially wondered how he could contribute best to discussions at the conference. However, he noted that given due consideration of the issues at hand, he felt that it would be helpful if he could elaborate upon some of the challenges presenting, especially given the apparent interest in what was to be discussed demonstrated by the large attendance. Some challenges in ensuring a safe and secure Europe could be related to the some 200 million border crossings undertaken annually at external borders and increasing conflicts in neighbouring regions. In the EU, law enforcement and border control effectiveness is strongly based on the fact that the chain is as strong as its weakest link. If one of the Member States has a problem, we all do. Mr Pynckels added that we see a deformation of the social fabric if there are too many irregular immigrants in particular areas and/or a perceived lack of control.

He posed a series of questions to kick off panel discussions. Specifically looking at digital transformation as a term on which panel discussions were to focus, he wondered whether it is just another buzzword to which everyone has their own definition Do we have uniform vision on what to achieve in such a transformation? he asked. And is there a coherent technical strategy? Indeed, is changing always better? What about budgets? And even if economic growth can be seen in the IT sector, how expensive will it be for

other sectors? What about legacy systems as such a transformation takes hold? What about the coherence between different frameworks? And is a digital transformation really digital, given that digital developments have to follow business processes?

He continued looking at specific operational challenges, wondering, for example, how to control many people in a border check/law enforcement context in a short time? He questioned what digital transformation might bring when it comes to business operations and procedures. And he specifically drew attention to the important topic of interoperability, questioning what impacts it might have for operations.

Finally, looking to future possibilities and developments in cutting edge technologies, he questioned whether European authorities should be early adopters or only use proven systems. Should we use AI? he asked. And given digitalisation and increasing digital dependencies, he wondered how business and IT continuity could be effectively ensured going forward.

Stephan Brandes stepped in and asked Mr Pynckels **whether, given his introductory remarks, he felt that the digital transformation is an IT topic or more of a business topic. He also wondered whether technology renewal is the main driver of the transformation or whether digitalisation is transforming business processes.**

Mr Pynckels answered that the digital transformation, in fact, has nothing to do with digital. For example, some time ago everyone was talking about virtualisation, which was the hot item. Yet, in the 1980s when IT was in the mainframe world, he worked with virtual machines. Clearly, the technology is not new. He expressed his opinion on this basis that in the digital transformation, we have to focus on certain technologies and their use, as fundamentally the basic technologies available stay the same. If networks become slower, we will be more local activity centred while if networks get faster, activities will be more central. The main problem is, he postulated, that business, legal and financial processes need to all be transformed to take advantage of digitalisation.

Mr Richard Ares Baumgartner presented some initial points from the Frontex viewpoint on how the digital transformation affects business in the border management domain. He concurred with Mr Pynckels that transformation was less about ICT and more about how an organisation works, its workflows and operations and how new technology can support them. He stated that digital transformation cannot be driven only by technology. From a border management perspective, it can facilitate simplification of operations. Such operations, he noted, deal with mobility, facilitation of travel, crossing of borders, but also the security of the Schengen space. These dual functions, he stated, are not mutually exclusive but are interdependent and technology can help to simultaneously improve operations in both related functions simultaneously.

He continued by talking about relevant challenges and opportunities. On the challenges side, the first topic mentioned was mobility. Mr Baumgartner drew attention to the recent open letter from airlines and IATA addressed to EU home affairs ministers that criticised the fact that due to the systematic checks of persons at the Schengen external borders, flights were being delayed. He suggested that such challenges present opportunities, in this case perhaps to review processes and see how to best use information. We could better use advanced information - API and PNR data - which will allow background checks to be carried out before people arrive at the border. Perhaps some of the border checking processes, including some risk assessment, can be done ahead of time to relieve pressure on the border guards.

New systems like the EES also pose challenges yet simultaneously present opportunities, he suggested. At Frontex, work has been ongoing on elaborating best practices for use of Automated Border Control gates for some time now, he noted. While their use at airports is prevalence, their use at land borders is challenging – very relevant in the context of EES since one third of the arrivals into the Schengen area come through land borders. Mr Baumgartner cited Frontex statistics that indicated that some 73% of refusals of entry in 2016 were at land borders. He proposed that there are opportunities to look at infrastructure, to change processes and perhaps to use mobile equipment to deal with people on busses, trains, cars, etc.

Appropriate sharing and usage of data can also be challenging, he noted. Frontline officers -border guards, immigration/asylum officers, police – all need relevant information. The difference that additional data makes to their decision-making

capabilities (for example, access to relevant INTERPOL databases) is evident. Access to this information has to be easy because the officers do not have much time. Therefore, proposals for new single search interface capabilities in the context of systems interoperability are welcome, he noted. Access must be seamless for the law enforcement officer.

A final challenge addressed was accurate person identification. It is a fundamental elements of every process undertaken by a border guard, he noted, indicating that if the guard incorrectly identifies the person, the decision made is likely flawed. Identification can be particularly difficult when it comes to TCNs. He argued that there is a definite need to work with biometric data so that the border guard can make the appropriate decision. Furthermore, as well as search capacity, accurate data entry capacities are required. False documents are a major challenge in the domain of identification, and capabilities for their detection need improvement given that there are more and more such documents being utilised and their quality is increasing.

Concluding with his main messages, Mr Baumgartner reiterated that for border guards, access to information is a must. Silos persist but we need to promote sharing of information, he argued. There is a cultural change aspect to this issue as well as a legislative one, he suggested. When it comes to interagency cooperation, Mr Baumgartner explained, the European Travel Authorisation System will be a challenge in the domain of large-scale systems development an operations given that 3 Agencies are involved, but an opportunity as well. Lastly, he mentioned P2B partnership as an important topic. When it comes to airports, seaports, and carriers, cooperation must be enhanced, especially with the individual traveller as well, he argued. Technology-enhanced processes must be easy for them, he suggested, while guaranteeing their rights.

Stephan Brandes briefly recalled that the topic of the first eu-LISA conference was how to balance security and efficiency in the border crossing process using technology, noting that some of the challenges brought forward then were raised by Mr Baumgartner as relevant to this day, although

others were already being addressed through technological innovation and process change. He passed the floor to Mr Luis de Eusebio Ramos to present some views from the Europol perspective.

Mr Luis de Eusebio Ramos began with a definition of digital transformation. From the Europol side, he noted, digital transformation is the possibility for collecting and handling information from thousands of third parties, to leverage that information and to provide back added value. So, for Europol, he explained that digital transformation is about challenging business based on IT and the added value of this information.

He went on to challenge the notion put forward by other panellists that the digital transformation is not about IT – he suggested, rather, that it is not only about IT. He argued that IT is the basis on which we build the digital transformation. The mission of Europol is to make Europe safer. Certainly, police officers and citizens are the final recipients of the services. IT is the core of the digital transformation, but it is clear that we are going much further, such that legislation, processes and economical aspects are also included. He said that we see many projects that focus on business hypotheses in their transformation but forget the value of IT.

Mr Ramos went on to talk about how Europol is observing a huge increase in the volume of information being received. The variety of sources is one reason for this – mobiles, social media, internet of things. Yet it increasingly begs the question of how to provide new value with this information, increasingly in real time given the demands of users. Europol considers that three pillars are essential: integration, interoperability and innovation. Mr Ramos reported that it was decided this year in Europol to launch a new plan to improve services based on the digital transformation along these 3 pillars.

Within the integration pillar, he noted that on 1 May 2017, there was a change in the Europol legal framework that has already helped to deal with previously-existing data and information silos. Now the focus is on different sources, enabling Europol to better deliver added value using the information. The change is not focused on the systems, but on the value that the information creates for users. Briefly considering interoperability, he highlighted the work of the high-level expert group on information systems and interoperability chaired by the European Commission and the follow-up work ongoing related to the concepts of a single-search portal, shared Biometric Matching Service and Common Identity Repository. Interoperability will undoubtedly change business, but also raise questions as to how to tackle 100TB of information and how to process and analyse all of this information at the pace and scale demanded. The third pillar of Europol's plan – innovation – is necessary in this context to provide business with new possibilities. When it comes to innovation, Europol is working along 6 lines of innovations and Mr Ramos touched on 3 of them –

- provision of new services to businesses based on smart capabilities, including artificial intelligence. Europol is currently trying to find business cases from the user side, teaching businesses about new opportunities, scouting the market for available technologies and running pilots using the information. When Europol is confident in the application, the pilots will be transformed into operational capabilities.

- utilisation of facial recognition, particularly to reduce identification times. Technologies based on neural networks are of high priority. Recalling that terrorists increasingly spread radicalisation messages through online media, video recognition and natural language processing are also promising in helping combat terrorism, Mr Ramos noted.
- development of new tools for protection of the internet space, required particularly as crime becomes more digital.

Mr Ramos also mentioned supercomputing capabilities as a core requirement as the digital transformation gathers increasing pace and more tools become available and relevant.

As a concluding point, he brought forward the need for dialogue. We need to leverage our relationship with the industry, the academia and all stakeholders, he argued. This needs to be more constructive. Europol's relationship with eu-LISA is full of promise in this regard, he noted, as one looks towards the future.

Stephan Brandes picked up on Mr Ramos' intervention on the topic of AI, noting that it presents opportunities, but at the same time it can be seen as a threat as well – for example, implementation of AI solutions could lead to job losses. He wondered how to manage and balance these opposing impacts?

Mr Ramos replied that AI sounds like science-fiction but indicated that it actually uses well-known technology. He recalled that even 15 years ago there were courses on AI and the algorithms used now are similar to those used back then. Challenges are presenting because of the increasing potential of these algorithms and solutions. The discussion about AI is similar to one about IT in general, he argued. Questions related to, inter alia, the limits in privacy and law enforcement usage limits. For Europol, emphasis is on using AI with strict application of standards and within the legal framework. He said that Europol has a data protection officer in-house and they have a good collaboration with him. He always advises Europol on how to improve business while maintaining data protection standards.

Lauri Lugna presented his opening views, starting by noting how glad everyone is that eu-LISA is in Tallinn. He recalled the active discussions that took place some 10 years previously regarding the location of the Agency and stated that it was very important for Estonia that the country could host the Agency. At that time, of course, nobody could foresee the priorities of the Presidency. Yet he expressed pleasure that eu-LISA could contribute to addressing some of these priorities.

Before talking about technology, Mr Lugna pointed out that Estonia is one of the most forested nations in the EU. For Estonians, he noted, nature has a lot of meaning and it is represented in the Presidency's slogan – 'balance through unity'. Balance, he suggested, is important when discussing technological issues as well.

Turning first to the term digital transformation, Mr Lugna reflected on how it is happening no matter what we do. At the end of the day, he suggested, it is the private sector at the wheel and the government has the option of taking part in the journey or watching from the side. Having said that, he noted that it is worth remembering what our clients, the citizens who pay taxes, expect. Creating trust in the system is the cornerstone, he argued. The citizens expect the governments to uphold trust in uncertain times. A second expectation is that the trust and processes and controls created are seamless, meaning that the citizens shouldn't even notice them. Mr Lugna noted that we are saving time for the citizens - at the border, in traffic control, in crime investigations – for citizens time is also a significant concern. In addressing these challenges, technology can be an addiction, he argued. We are eager to adopt new technologies and be on this journey, but at the same time, we should keep in mind that things break down. With this, he came to his main point – that with digital transformation, business continuity and building up redundancy is something that must be kept in mind. When skyscrapers were built they had elevators, but somehow everyone agreed that stairs should be there too, which he then paralleled with the previous thought. Mr Lugna said that whatever systems we build, it is worth considering and taking the time and money necessary to build redundancy into those systems. For example, Estonia is a digital society that has used all possibilities offered by technology in government. Yet in the months prior to the conference, he noted that it was realised that Estonian ID cards had theoretical vulnerabilities, meaning that the Estonian authorities needed to look at other approaches to offering services based on use of these ID cards.

Mr Lugna went on to reflect on what the digital transformation means for government. He noted that it typically means a lot of experimenting and prototyping but governments don't usually do this well. Similarly, we need room for failing as well, he suggested, meaning that there needs to be a shift in how we lead our people and organisations. Thomas Edison, before he invented the lightbulb, learned a 1000 ways in which not to make a lightbulb, he noted, stating that failures provide the experiences that allow us to see what our customers need. He gave another example from Estonia, where there is an agile way of bringing in new possibilities for law enforcement, and they have discovered that beta testing is OK.

When it comes to the digital transformation, Mr Lugna considered whether legislative transformation might also be necessary, moving towards a more agile approach. He indicated that

although we have been prototyping, legislative work means agreeing on rules, so agreement takes time and can still lead to outcomes that are contradictory with the outcomes of technological development and testing. In conclusion, he stated that pilot projects are the way to go forward, expressing his view that it is indeed a quick and agile way of moving forward.

Mr Ramos took up Mr Lugna's point on legislative transformation, indicating that he fully supported the sentiments put forward. It is clear that all the elements of the digital transformation have to happen at the same time, he noted. When it comes to the legal framework, Europol has a new one that allows it to provide new services for the law enforcement community. The afore-mentioned change in the Agency's regulation led to a huge change in how information is handled, he suggested. It focuses on how to leverage information to provide added value for the end user and has been a real game changer for Europol. He said that the legal unit of Europol is very much focused on the future and supported by all other parts of Europol. The new focus on the user side has led to a decision by Europol to break down silos and start work on a unique data repository. Mr Ramos concluded that this provides intelligence with a higher value than in the past.

Mr Baumgartner continued in response, noting that Frontex is also in a process of change due to an extension of its mandate and mentioning briefly that similar changes will need to be handled by eu-LISA in the near future. He explained how the new mandate establishes the rights of the Agency and the multinational teams that are deployed at the external borders that include access to eu-LISA systems. An objective for Frontex is therefore to provide teams at the borders and at hot spots with mobile equipment for consultation of systems. While the teams always operate under the jurisdiction of the Member State, he argued that they need to equip the teams with the necessary ICT for the job. This will benefit Member States, he noted, because Frontex will be able to provide more operational support. He added that in terms of equipment, Frontex has to work with eu-LISA. There is an opportunity for capacity building, standardisation and best practices as well as for piloting equipment in operations and giving feedback to Member States. Mr Baumgartner also briefly alluded to the fact that Frontex's new mandate additionally requires it to work on guidelines for an IBM strategy and stated that experience in the field has to be incorporated into this strategy.

Stephan Brandes noted that there had not been a lot of talk about technology so far, which might be an answer to his initial question of whether digital transformation is an IT or a business-driven issue. He asked Mr Pynckels how national authorities keep up the pace of change.

Mr Pynckels replied, noting that realistically they don't keep up, although arguing additionally that one shouldn't necessarily try to, adding that in limiting one's options, one shows mastery. While we may bring forward all kinds of words, technologies

and innovative proposals, we should realise that in a few years IT solutions will be like electricity – we don't talk about them and nobody cares as long as they are there. The business should drive things.

Mr Pynckels suggested that we cope by limiting and shifting out buzzwords and by using real propositions. He brought forward the example of RFID technology, once a hot topic in itself but nowadays combined with other technologies to create useful products. The beauty of the technology is unimportant – it is the outcomes that support business value that are important.

Mr Lugna that silos at the business level are a challenge, often manifested between business, process and IT owners. He went on to explain that we don't talk about different possibilities and needs. When speaking solely about new buzzword technologies like driverless cars, AI and machine learning in a soiled manner, we are frequently missing important points. For example, 5 years ago we knew about drones and began to use them in the military. But organised crime also started to utilise them. A difficulty, Mr Lugna highlighted, is working out how to make sense of technology changes? Somehow, he argued, we need to bridge the gap between identifying what is actually developed and what will be in mass usage in 5-10 years. Additionally, he suggested that we need to better make sense of the technology for businesses, both from the perspective of what it offers but also what constraints it may introduce. Mr Lugna alluded to how his children started using drones years before his Ministry began thinking about it as an organisation. Thus, more understanding needs to be brought in, particularly through involvement of digital specialists.

Mr Ramos went on to stress the value of the user side and the need to take user perspectives on board. There are many successes in the private sphere. However, when it comes to deciding on the unit in a company that has to lead digital transformation, we see differences. Sometimes it is the IT department and other times the legal department. Yet in many cases digital transformation is driven by the marketing department because they know the expectations of the users and can provide the most suitable solution to those users. He added that Europol decided to pull down the silos to give the user the answers they wanted. Again, he stressed that the user is the key element in the digital transformation.

Stephan Brandes opened the floor to questions from the audience.

A representative from the EU counter terrorism coordinator in Brussels asked the panellists from Frontex and Europol about the necessity of their new regulations. What kind of encouraging message could there be from the institutions in terms of concerns around privacy by design, he wondered?

Mr Ramos explained that from the Europol side, they are thankful for the new legal framework. Europol is in the process of making the best of the new legislation to provide more services. So, he thanked the legislators for making it happen. He stressed the need for continuously looking towards EU institutions and aligning Europol actions with them.

Mr Baumgartner added that an important issue is having the information necessary. Having rule of law means that an officer has to implement such rules just as members of parliament need information for correct legislation. A border guard might not have another opportunity to apply the law after a single

meeting with a traveller and if the opportunity is missed because there is no access to information, may not have the chance to detect illicit activities as he or she should in accordance with rules. New technology and access to information allows for a more consolidated view of the traveller and to improve the experience for them. ABC gates and advance information is not only about security but also facilitation and comfort of travel. But users have to make the case and explain it well to the legislators, otherwise problems arise, he noted.

Mr Lugna talked in response about the legislative transformation that he brought forward earlier. Estonia has contributed to the debate on digital transformation by comparing systems, specifically digital systems against paper systems. He explained the fundamental differences observed – in a digital system, technology is applied and something is definitively logged. Whoever has access and looks at data can clearly be seen. However, paper systems do not log who has been looking at the data. So, in the debate on privacy by design, it needs to be clear that in digital systems, privacy is handled better than in paper systems. He also made a second point

regarding upholding trust towards the government and society. On the perception side, people perceive that there is a threat to privacy, however, it needs to be clear what the government can and cannot do.

Former MEP Miroslaw Wolski commented from the public that he dealt for 20 years with IT systems in health care. There has been a lot of discussion about electronic patient data records. If lives are in danger, everyone is happy to open their files, he noted. The situation is similar now. If we are discussing a safe and secure Europe in the European Parliament, everyone says we have to be careful and discuss it for 5 more years. However, if there is a feeling of personal danger, things move faster. He gave the futuristic example of using implanted chips and GPS to locate missing children. ETIAS was a welcome initiative, but the cost and duration were unreasonable. So, at the legislative level in the Parliament things move slowly, but we have to be much more flexible when it comes to present dangers, he suggested.

Mr Lugna broadly agreed, adding that he had similar conversations with colleagues in the health sector, who are also saving lives, and mentioning the e-health conference that was taking place in Tallinn on the same day looking at related topics. In fact, a colleague had already briefed him on debates there and they were similar. In Estonia, he noted that authorities have opened up data related to health and security for many years and everyone can see who has accessed their data. He explained that it hasn't made our lives worse, but better. It takes time to get there, but at the end of the day, demand drives in the business sector and the demand for data sharing is there.

Stephan Brandes asked the panellists for a final comment on how, having gone through the digital transformation, we can keep business running when the power is off.

Mr Pynckels replied that when there is failure, power is the least concern – there are batteries, diesel generators, etc. What's fundamental is legal and privacy aspects, he argued. We have to look into what is decided at what level in terms of business continuity and backups. He suggested that legislators shouldn't mess with things they often do not understand. He brought forward discussions on the new eu-LISA regulation related to active-active and active-passive approaches to high availability systems amongst many who didn't understand the concepts being discussed. The approach, he argued, should be that legislators say what they

want but not how they want it. He added that, with all due respect, on each level, what you want is not to have a law, but to describe what you want. When you mess with things you don't understand, you put in concrete terms things you don't want and tie the hands of technology specialists. Similarly, when dealing with privacy, he pushed for an approach in which legislators describe what they want and ensure that it is checked by audit specialists, rather than specifying specific technical solutions.

Mr Ramos added that business continuity is built into all levels of Europol. The mandate for the unit is to make sure that on the user side we can provide services either through IT or in other ways. Business continuity goes much further than IT, he noted.

Mr Lugna said that when it comes to internal security, we need to think more about the unthinkable. Compared to the military, law enforcement is in a daily battle. The military has more time to exercise and test. He said that we – the law enforcement community and its stakeholders - have to do more of this type of thinking, so that we can keep up our way of working in the future. Technology can be very addictive, he argued, and we get used to and attached to it. At some point, we will be looking at IT systems like electricity, but we have to build these systems so that they function in the same way as electricity currently does.

Mr Baumgartner wrapped up the discussion by saying that business continuity is based on dealing with crisis situations. At Frontex, they have done a lot of scenario building so that they wouldn't have to improvise. When it comes to IT, they don't have to deal with large IT systems but rather a border surveillance network. They have live data sent in by Member States and fortunately, have implemented an agreement with eu-LISA for backing that system up such that business continuity is inherently considered.


LISA

Session 3:
Interoperability for Internal Security - Breaking down the silos for improved efficiency

Moderator:
Ciaran Carolan,
Head of External Affairs and Capacity Building Sector, eu-LISA

Panellists:
Rob Rozenburg, Head of Information Systems for Borders and Security Unit, European Commission, DG Migration and Home Affairs
- Vision for interoperability in IT systems for internal security in Europe
Ana Maria Andrei, IT Specialist, Interoperability Team, eu-LISA
- Initiatives towards interoperability: European Search Portal, Biometric Matching Service
Johann Jergl, Senior Desk Officer, Police Information System Division, Federal Ministry of the Interior of Germany
- Enhancing interoperability in law enforcement
Klemen Oven, Policy Officer, Risk management and security, European Commission, DG Taxation and Customs Union
- Interoperability in the customs domain and synergies with home affairs

Introduction by **Rob Rozenburg,**
Head of Information Systems for Borders and Security Unit, European Commission, DG Migration and Home Affairs
- Vision for interoperability in IT systems for internal security in Europe

In his introduction to the panel, moderator Ciaran Carolan noted that interoperability has been something of a buzzword in discussions in the JHA domain in recent times, but is actually much more, and in fact is a paradigm shift that can bring positive change for system administrators, authorities and end users. He also noted that all panellists were acting as experts within the panel rather than as representatives of the entities from which they came. With that he opened the topic for discussion.

Rob Rozenburg started the panel by elaborating the vision of the Commission on the topic of interoperability. Firstly, he pointed out a problem – that the EC doesn't do visions because people don't seem to like it. He said that if there is any vision, it is simply that we need to make sure that border guards, customs, police, judicial authorities all have the information at their disposal that they need to do their jobs, in line with the legal constraints. He went on to explain that the existence of silos is one of the issues we have to take into account: silos between national and European, between police and border control, between police and counter terrorism or intelligence. These silos spring from national legislation, working methods and cultures. In his presentation, Mr Rozenburg focused on the central systems: current - SIS II, VIS and Eurodac; and future – the EES, the ETIAS, and the Criminal records system for TCN (ECRIS-TCN). In addition, he noted that Europol data is relevant to the end users of IT systems in the JHA domain. Mr Rozenburg explained that the EC has looked at all of these

systems and intends to address all of them in the interoperability proposal that should be completed by the end of this year.

According to Mr Rozenburg, silos exist for a reason. Each system is designed with a purpose, with safeguards and user access rights that are meant for that system. Silos have been built as an approach to ensuring the proportionality of system use. From the EC perspective, silos are not necessarily bad, but they should be overcome or circumvented to allow for things that need to be done without destroying the legitimate legal bases.

He went on to elaborate that the EC sees 4 big problems arising because of silos. Firstly, today's end users do not have easy and fast access to the information to which they have authorisation. This problem is already apparent with 3 information systems. The introduction of new systems will make it even more complex. Thus, at the EU level, there should be a tool developed for users to check the systems in a fast and systematic way. The tool has to be systematic because Member States have to be able to count on other Member States to act in the same way. He went on to add that a major issue is the lack of trust between Member States with regards to how correctly things are done. By making the checks faster, easier and more systematic, these issues can be overcome. The second problem he outlined was law enforcement access to the border management systems – the rules are, as reported by many Member States, too restrictive, albeit that they are there for a reason. The current cascading system of checks should be reviewed, he suggested. If you are a law enforcement authority, there is a cascading order of checks that needs to be followed. In reality, it creates problems due to the time requirements for such successive checks, while sometimes obstacles appear during the earlier phases of system checks so that the necessary information cannot be reached. Thus, law enforcement access procedures for Eurodac, VIS, EES and ETIAS need to be streamlined. The cascading logic needs to be replaced without compromising security. The High-Level Expert group identified a two-step solution that would use hit/no-hit flags highlighting the presence of information in the available systems as appropriate

without divulging the nature of that information, at least during the first cross-system query. The third problem he outlined related to identity checks, especially checks on Member State territories. Today, if a police officer wants to check the identity of a person without documents, the officer does not have many options. For instance, VIS could be a source of information but a street officer cannot access it unless it is in the strict context of migration management. In the EES, police officers similarly do not have access. Perhaps, therefore, it makes sense, he argued, to consider how to make it possible. This concerns simple checks, in traffic or during a demonstration, so that individuals who may or may not be involved in a crime could be identified. Finally, the fourth problem related to multiple identities - people in different systems under different names. The problem exists today, he noted, but with more systems, the problem will be bigger. Mostly, it is a question of spelling differences or errors - situations such as name changes arising through marriage. Mr. Rozenburg mentioned that these non-matching identities can cause a lot of problems for these individuals. Therefore, an objective is to identify and repair these inconsistencies. Of course, according to the same logic, if there is an issue of identity fraud, the system could detect it and mark it with a red flag instead of a green one.

After outlining the problems, Mr Rozenburg quickly outlined the solutions – the European Search Portal, the concept of a shared Biometric Matching System and the Common Identity Repository – which are part of the solution and could be used in combination.

High level consultations have taken place, he noted, with the Council Presidencies, the EDPS and FRA while there are also technical studies underway. By combining the outcomes at the technical, legal and political levels, the EC is still hoping to propose an interoperability package by the end of the year. Thus, work on solutions could start at the beginning of next year.

Ciaran Carolan followed up with an immediate question concerning comments being aired by many people stating that interoperability is *finally* on the agenda. In many ways, he suggested, the concept of interoperability seems sensible, leading to the question of why it is being examined only now as opposed to years ago?

Mr Rozenburg replied by saying that there are different ways of looking at it. Simply put, if there is only one system, interoperability is not a concern. So far, the SIS and VIS are most relevant

because Eurodac is very specific and doesn't contain biographic information – it only identifies the country of arrival for an asylum seeker or irregular migrant. The old Eurodac is not subject to interoperability. From that perspective, he stated that the debate is coming up because of more systems being developed. From the political perspective, there have been cases in recent years, especially concerning terrorism, where it was seen that the problem of multiple identities was at the root of the problem. For example, the Berlin case, where the perpetrator had 14 identities in German databases. The more these cases appear, the more urgent the sense is that something needs to be done with the way information is managed. It is no longer a choice to continue operating systems in the way we do so currently, he suggested.

Johann Jergl began by confirming that yes, interoperability is finally on the agenda. The work of the High Level Expert Group has been taken up by the Council and Mr Jergl expressed his pleasure at seeing it also on the agenda of the Estonian Presidency. However, everyone is talking about interoperability and it has become a buzzword, while at times the real goal is obscured, he argued. In Mr Jergl's opinion, interoperability is not a goal, but a tool to reach objectives - specifically to fundamentally improve the European information architecture and information sharing and to face challenges due to the current migration and security situations. In a globalised world, no nation can be effective alone, he noted. Organised crime, migration and travel have to be jointly managed. It is time to recognise that the challenges are all intertwined and must be dealt with accordingly. In the past, EU co-legislators created separate IT systems for each purpose but interconnections were not taken into account. The present system architecture with its silos cannot cope with challenges, especially when it comes to detecting multiple and false identities, he suggested. This leads to dangerous blind spots, such as the Berlin case in December 2016, but many more similar cases can be named in relation to terrorism and serious crime. This all, he argued, shows clearly how important it is to establish trusted identity.

In terms of solutions, Mr Jergl focused on the identity issue. In Europe, a system is needed with

biographic and biometric data that would allow identification and detection of multiple identities without delay. How to do this? Mr. Jergl questioned. In immediate response, he outlined some proposed solutions. Firstly, he spoke about connections between existing databases arguing that such an architecture was preferable to cascading through systems to find relevant information. This also means, he noted, that entering data multiple times must be avoided. However, interoperability does not mean creating one European super-database - which would amount to a giant haystack where nobody can find a needle. Instead, individual systems can be maintained but the criteria for access have to be reassessed and practical. The European Search Portal will help end users swiftly access relevant data as needed on a case by case basis. The core data in the common identity repository, meanwhile, will be linked to information that will be kept in the core systems, taking into account the access rights and the purpose limitations. Compared to health information mentioned earlier in the conference, Mr Jergl argued that the level of sensitivity of identity information is generally quite low. As a principle, he stated that only the least sensitive information should be aggregated and the sensitive information left in separate databases, as it is today. Mr Jergl assumed that bundled systems will remain manageable and enable eu-LISA to use resources wisely in the interests of European citizens.

Mr Jergl pointed out that a lot is happening in the European information landscape at present. There are various changes being discussed in the legal bases for all systems, he noted. In this context, he described interoperability as an overarching issue in this landscape. A significant challenge will be to integrate the technical and legislative changes at the Member State level. Mr Jergl ended his intervention by praising all the initiative and commitment demonstrated by all stakeholders in the discussions on interoperability thus far.

Klemen Oven continued the session by offering perspectives from the customs community. He started by taking a look back to 2016, when the Commission issued its communication on interoperability and launched its comprehensive security plan, involving the contributions of all stakeholders. From his perspective, representing DG TAXUD and customs issues in the High-Level Working Group, it was difficult to understand the perspectives of the other communities. Mr Oven went on to explain why the customs side is represented and what their objectives are by showing a short video about the daily work of customs. In terms of facts, customs is omnipresent at the EU's external borders, contributing to EU internal security through security related seizures and customs supervision of goods flowing in and out of the EU. When it comes to seizures, he noted that after the horrific terrorist attacks, later analysis showed that the chemicals used for the explosives were smuggled in from third countries. Mr Oven took a global look at relevant seizure statistics: over 7000 pieces of firearms were seized by EU customs authorities in 2016, while more than 1000 shipments of chemicals or explosive precursors were seized; in addition, more than 300 tons of narcotics were seized, as well as enormous amounts of illicit cigarettes that are used by criminals for funding their activities, potentially also terrorism. Mr Oven also mentioned that a growing trend is the use of small consignment shipments for smuggling across external borders. Criminal organisations are using e-commerce to deliver illicit goods to the EU market.

Mr Oven took a brief look at how customs operate – specifically they look at supply chains. For the goods to move, there is always a contract that is made, in the form of an invoice, typically digital in the EU. These are given to the carriers, who get instructions for the transport of the goods. So altogether, he noted that there are more than 500 million such contracts crossing the EU external borders yearly, involving billions of actors. 16 shipments each second cross external borders. Mr Oven then asked how to detect risks? Answering immediately, he indicated his point of view that this could best be achieved by collecting all information from the trade. He further explained that customs currently collects advanced cargo information, although he noted that there are gaps in data coverage. Not all shipments are digitalised (for example, in the postal sector), and there are data quality gaps, as well as silos within the customs community, which are currently being addressed. Mr Oven explained that to break the silos, the advance cargo system is being reformed, and a new import control system is being developed. The data from the parties in the supply chain is being collected into a common repository that will have a harmonised interface, connecting the private sector to the public sector and providing relevant information for the customs checks. When it comes to silos outside the customs chain, Mr Oven stated that it would be logical to first agree that there is a strong link between goods and persons. In this regard, customs do not have all the knowledge about potentially criminal actors or persons of interest. Mr Oven concluded that more work is needed between disciplines in the future to understand how customs can contribute to detecting risks. In the future, there could be a link between alerts in the SIS and the customs systems. From the customs perspective, it would also be interesting to link up to national alerts systems, to Europol or to the European Search Portal, to compare alphanumerical information. This would allow the tracking of items that are connected to persons either known or suspected of terrorist activities. Concluding his presentation, Mr Oven noted that the legal aspects of potential future links need further exploration.

Ana Maria Andrei continued the panel by presenting eu-LISA perspectives on inter-operability. To address the current issues and gaps in EU information systems, she stated, and enable information to be shared, firstly eu-LISA will continue to provide centralised operational management of the current systems. eu-LISA will also continue to look at the current information gaps and try to look at architectural gaps to see where improvement can be made. In the future, eu-LISA will develop the main technical features of new IT systems and also approach the interoperability issue by tackling legal issues for the European Search Portal and the common identity repository. Work on data quality will also continue, with automated data quality control mechanisms being considered. Current project initiatives include the SIS II AFIS, which will be implemented in the first quarter of 2018; feasibility studies conducted in close cooperation with the EC on the European Search Portal and the identity repository; and a

shared biometric matching system study. eu-LISA acknowledges the need for high quality biometric data, particularly for undertaking identification, and Ms Andrei noted that all of these issues are taken into account in the feasibility studies. She also recalled that better data protection is a high priority and highlighted the fact that eu-LISA is in full compliance with EDPS and security requirements in all its studies.

According to Ms Andrei, eu-LISA conducted a technology strategy study and outlined 4 recommended dimensions based on the study that are also in focus in eu-LISA's general work: 1 – an intelligent infrastructure for the future, 2 – standardising monitoring solutions, 3 – a virtual operations centre, with continuous delivery through a process driven mainly by automation, and 4 – advanced security processes enhancement. Of course, all initiatives are in line with the EC communications and the recommendations of the last High-Level Expert group final report. eu-LISA is also consulting with Europol and Interpol to see what the European Search Portal could provide in terms of interconnectivity, specifically from the end-user point of view. Solid governance of the UMF standard is also a priority, she argued. In parallel, eu-LISA is still conducting a gap analysis on the existing systems, while a unified networks study that seeks to achieve interoperability at the network level is also underway.

Within this study, a legal assessment has also been started that is based on the three systems that eu-LISA currently operates. The second phase of this project will seek the consolidation of recommendations related to requirements and technologies. The third phase will involve testing, with the whole project set to be concluded by the end of 2018. Further work is still needed on a unified WAN perimeter, which will be considered as follow up to this work.

All of these studies are relevant in the context of the implementation of the European Search Portal, she noted.

Ms Andrei concluded by looking ahead to the significant future challenges that lie ahead. It will be crucial, she noted, that roadmaps and studies come together and that the considerable infrastructural changes necessary are planned in the right way. Facing this migration challenge wisely, with a focus on reusability, integration and future virtualisation, will be key. Also, privacy by design, which she noted was already mentioned by previous speakers, is a concern and she highlighted once more that eu-LISA needs to work in line with data protection and security regulations. In this regard, she described how the Agency is already thinking about future interoperability architectures and associated processes to ensure visibility and transparency where needed, as well as respect for the user's privacy.

Mr Carolan opened the floor to questions from the audience.

A representative of eu-LISA suggested that interoperability is not purely a matter of technology and proposed that we need to address interoperability in the way we work together on the European level. She asked the panellists for their comments on this sentiment.

Rob Rozenburg responded by pointing out that the four problems he outlined are not technical but operational. So, the challenge absolutely is not at the technology level, but at the user level and in the legal framework. It is a complex matter. He noted that the EC is currently considering only the 6 mentioned central systems with the intention of putting something in place to connect those systems and make it possible to match information (be it in the form of a search portal, an identity repository or a combination). Yet this interoperability is only the first step, he argued, and it will not be concluded once in place for these systems. He suggested, rather, that the work will be the basis for building further interoperability. Then, of course, the customs systems should be amongst the first that are plugged in, then Interpol, but also Prüm infrastructure, PNR, API, etc. When the systems are linked, the story just begins, he added.

Mr Jergl took the opportunity to speak about efficiency for the end user as something of great importance. He expressed his view that it is good to see that the technical ideas that can achieve such efficiency are supported by the EC, but noted nevertheless that the word interoperability means to work together across disciplines, e.g. border, migration, security, travel. Thus, interoperability must create a change in the mind-set, both at the central level and also at the Member State level. He noted that in Germany, authorities are discussing the border control procedure and how to bring together information from different systems across different domains. What the Commission is discussing is perhaps more complex, he suggested, as they wish to create a pan-European search engine. Information from decentralised systems, he felt, is especially a challenge when considering integration. Returning to the sentiment of the question posed, he indicated agreement – indeed, changing mind sets from formerly separate ways of working will be an important first step, he stated.

Haroona Franklin from Deloitte, queried how interoperability could result in a move away from building large systems that will need to be replaced at some point towards something more agile. Taking the example of border checks, she noted that the way a border was operated in 2012 is not the same as today. She wondered whether interoperable system designs could be adaptable to change, such as variation in threat levels.

Rob Rozenburg answered that we are in a way lucky that several systems being considered are currently being developed. It is already foreseen that the EES and ETIAS will have a shared identity repository, for instance, that can be the basis for the common identity repository, he noted. So, if you consider the 6 systems, there is a very important

basis to build on, he argued. The new elements will be part of the overall system development and will connect to existing systems over time. Looking at the pace of change in border check procedures, he noted that the rules of the Schengen area are essentially the same now as they were in 2012. The legislation is so detailed that there isn't much room for manoeuvring or using the systems in different ways. When we have the search engine in place, all information will immediately be available on the screen, he added.

Ciaran Carolan asked further, whether introducing a singular approach to system access, search and use could lead to some flexibility being lost. Noting that some speakers alluded to reasons why silos have appeared, he asked whether there is a danger of losing the possibility to utilise individual systems differently. How do we avoid that, he quizzed?

Ana Maria Andrei indicated that she is not sure if flexibility would be lost. Interoperability builds up an interface to the systems, but nothing at system level is lost, she argued. We are not changing existing systems, just preparing them for eventual interoperability. We build upon and improve them. Some of the standardisation is not mandatory, but it will help the administration level further on, she stated.

Johann Jergl added that he views eu-LISA's point of view positively, confirming once again that we are not building a super database that would remove flexibility from the landscape. Taking the example of the shared biometric system, he suggested that it will increase flexibility because eu-LISA no longer has to operate 3-5 biometric systems, but rather one towards which it can focus its resources. Perhaps one system is more complicated in terms of size, but it is still much easier to operate and thus more flexible than 3-5 different systems. So, interoperability will increase flexibility, he argued.

Peter Smallridge from Gemalto stated his feeling that the plans are good and noted that the agencies present seem to agree, meaning that interoperability is now just waiting for a legal basis. Will that come with the eu-LISA mandate, he asked? And will all biometric projects have to wait until the legislation is fully approved, he wondered?

Mr Rozenburg answered, stating that the European Search Portal and all its functionalities will have to have a legal basis and that is what the EC is preparing

now. It has been announced by Commissioner Avramopoulos that by the end of the year, it will go to the EP and Council. Thus, it will take time before entering into force. However, he suggested, this does not mean that eu-LISA cannot do its job because the development of the different systems to be later made interoperable is on a separate track. Work is ongoing on the EES and the SIS II AFIS, he noted as examples. Interoperability is part and parcel of eu-LISA work anyway, he argued, but this cross-cutting functionality will need additional legislation for further deepening functions.

Mr Carolan asked Klemen Oven whether the customs community had interest in all dimensions of interoperability being spoken about - the European Search Portal, the shared biometric matching system and the common identity repository. From the customs perspective, is there interest in the common identity portal in terms of analysis or is it really just the search portal, he asked?

Mr Oven responded by saying that while their target is more goods and the associated actors, it does not

mean that identity is not important in the customs domain. Customs is utilising information on persons in their risk analysis processes. A problem from the customs point of view is that the declarations can be presented in a false way, with names other than those of the receiving parties. So, this aspect of multiple identities is also important in customs work. However, there are constraints because customs data is alphanumeric, not biometric. Thus, the potential scope and advantages of interoperability must still be explored by the customs community, especially concerning risk analysis, he suggested.

Tonu Tammer from the Estonian Ministry of the Interior suggested that we have set up systems in silos because of privacy concerns, but challenged whether this approach was justified. He suggested that we have followed this setup intentionally, but rather out of ignorance. He asked the panellists whether they agree, and whether silos were a deliberate creation?

Mr Rozenburg indicated that he fully disagreed. Silos are there for a reason, he argued, mainly related to the purposes of the systems. Data

minimisation and proportionality have been applied, he argued. Law enforcement systems have been developed at different times and when rules were different. As an example, he noted that Eurodac rules are more stringent because the system pertains to more vulnerable people. European decision makers considered those things while developing the systems and this is the result, he stated. He put forward his perspective that it is good to have silos, but also proposed that there needs to be inter-system communication in a purpose related manner, which is why we need to look into interoperability. Smashing everything is not the thing to do and will not be acceptable, he clarified.

Mr Jergl agreed with Mr Rozenburg that purpose limitations are there intentionally. Yet we are discussing interoperability now as the EU information landscape is expanding and overlapping, he suggested, and that is why we need interoperability connections. Identity is one particular aspect where we have overlap, he suggested, particularly as the landscape expands, e.g., related to passenger information for flights and cruise ships. We discussed aspects of analytics in customs and the PNR sector for identifying risky travel patterns, he noted. As the EU landscape grows, interoperability is not black and white and has to be looked at case by case, focusing on the concrete operational needs. Creating smart networks and connections will be crucial, he stated.

Mr Carolan posed a final question about breaking down silos. It is clear that all parties present agree that for the systems in place right now, connecting them intelligently is the right way to move forward, he noted. However, looking forward, he wondered whether it will ever be sensible that new systems will be built as. And assuming that we don't want new silos, he asked how this could be achieved from legal and technical perspectives.

Mr Oven replied that customs runs IT systems in a very complex architectural setting, in which there are multiple IT systems (under the CCN network). As such, from the IT architecture point of view, there is no need to look into getting a common IT solution for all authorities at this point in time. When it comes to building different IT systems in silos, there could be a case for it, he suggested, since each customs authority has their own interests. However, in interoperability terms, it's not about breaking silos but rather smarter connections between systems are needed, he clarified. On the other hand, he added that customs have been working on the advanced cargo information system reform since 2014 and since have come to some

conclusions on how to build interconnections with customs and other authorities. However, in a cost-benefit analysis, the suitable approach was deemed very expensive. He added that connection with the European Search Engine might prove beneficial and is very interesting as a possible future approach for the community.

Mr Jergl agreed that the general concept of building systems as silos can be an underlying principle in systems development, while interoperability will always have to be proportionate and fulfils concrete operational needs. We need standards, such as the UMF, which is an important precondition, a common language between the silos, so that they can exchange information where needed and appropriate, he added.

Ms Andrei agreed that this is one way to go, but we do need a common language and there are elements of the infrastructure that will have to be considered, she added. We cannot build a system as a complete silo from now on, she argued. Some infrastructure will have to be interconnected. As we talk about, for example, the shared biometric matching service, she noted, the matchers will have to be different because different data means different technical parameters. Right now we still need some silos, she stated.

Mr Rozenburg agreed that silos will remain but there will be smart networks additionally, he suggested. There are hundreds of thousands of practitioners who don't care about silos, he argued. The users should not be concerned about it because it is a legal and technical issue. In the future, the border guard and police officer should not think about which system or systems to use, he proposed. Rather, a check will be made on a device and a response will come back depending on the access rights of the user. This principle is all that matters, he argued. What we are doing here is behind the screen and should not concern the end users. He suggested more focus on user-friendliness, operational needs and the people who need information for their everyday work.

Mr Carolan concluded the session by admitting that seamless integration, functional legislation and user-friendliness is a great goal to work towards. Finally, he expressed hope that the ideas from the panel have contributed towards reaching that goal.

Session 4:
Digitalisation and Interoperability in the Justice Domain

Moderator:
Stephan Brandes,
Head of Application Management and Maintenance Unit, eu-LISA

Panellists:
Dick Heimans, Deputy Head of the Criminal Law and Judicial Training Unit, European Commission, DG for Justice and Consumers
- Perspectives for interoperability in the justice domain
Ernst Steigenga, Project Manager, Digital Interaction, Ministry of Justice, the Netherland
- Future of e-CODEX
Vincent Cambier, Director of the Central Criminal Record, Ministry of Justice of Belgium
- ECRIS - creating synergies between justice and home affairs
Joanna Goodey, Head of Department, Freedoms and Justice, Fundamental Rights Agency
- Digitalisation, Interoperability and Fundamental Rights

Introduction by **Dick Heimans,**

Deputy Head of the Criminal Law and Judicial Training Unit, European Commission, DG for Justice and Consumers

- Perspectives for interoperability in the justice domain

Dick Heimans began by expressing his pleasure at being able to represent the justice community, noting that his presence as a representative of the third Commission directorate to participate on the day demonstrated that connections are being made. By way of introduction, Mr Heimans gave the public a brief taste of digitalisation in the justice domain. He informed that their unit is also working on creating the EU Public Prosecutor's office, with a historic agreement made at the most recent JHA Council on the final text of the regulation to establish this new organisation. In implementing the organisation, they are now looking at creating a case management system, which is an interesting challenge from an interoperability point of view. The organisation will work at both the Member State and EU level on combating financial fraud, and possibly later also terrorism and organised crime. It will be located in Luxembourg, with delegated prosecutors in each participating Member State. Mr Heimans said that he had the opportunity to meet Ms Lavly Perling and her team in Tallinn to benefit from the digitalisation experience of Estonia. She had a few interesting pieces of advice, including one tip to always involve practitioners from the start when designing IT systems, and additionally to always focus on the use cases. Make sure what is developed is needed and works, he stated bluntly. One obvious challenge is, of course, linguistic interoperability. Mr Heimans noted that all of those at the conference speak English but in the same way that not everyone has such skills and translations are sometimes needed, the EPPO will need to prepare cases to be presented before

national courts and thus in the language of the court. To outline further challenges, Mr Heimans also pointed out that they have to integrate case management with national law enforcement systems and prosecution authorities. The systems have to be able to talk to each other, he clarified. Also, in any EU project of this size, managing differences in legislation, operations, and systems usage are always challenges to overcome.

Mr Heimans continued by providing some brief political context. The topic of digitalisation in the justice domain is firmly on the EU agenda and cuts across sectors, he noted. It is linked to the Digital Single Market strategy, which references work on the e-Justice system, he noted. Mr Heimans then went on to touch on three of the most topical issues: e-Justice, e-Evidence, and interoperability. First, on the subject of e-Justice, he asked the audience who has visited the e-Justice portal. Increasing visitation still needs a lot of work, he added; however, it is already a useful resource. The portal recently received a message from Harvard University, he announced, as the lecturers there use the portal to teach European law to students. The portal has

different functionalities that he briefly summarised – a generic information page with information on EU instruments and national law as well as about individual rights is available. Notably, information is available in all EU languages. The cross-border digital services available were highlighted as being perhaps more interesting, particularly the ECLI (the case law identifier). These services are an interesting example of how harmonisation and legislation work with digitalisation, he argued. Firstly, an agreement was needed to see how case law is referenced in Member States. Subsequently, common reference numbers were needed, requiring an implementation that is quite sophisticated. For legal specialists, it is a real treasure trove, Mr Heimans explained. So, it is a nice innovation in the justice domain and a good example of interoperability. He went on to inform that the portal also features a 'find a lawyer and notary' tool, which is very useful! Searches can be very specific, for example, helping to find a lawyer specialised in criminal cases who speaks German. The same system works for finding notaries. He mentioned that for these two systems, the Commission worked

closely with associations of lawyers and notaries to ensure optimal development.

Mr. Heimans continued by describing the e-CODEX system for e-Justice. It allows the use of automated forms to send a European small claim or payment order to a court in another state. Other examples of interoperability include business registers, insolvency registers and land registers. There is a legal obligation of Member States to interconnect their systems. He also noted that concerning e-CODEX, there is a future possibility to transfer responsibility for maintaining the application to eu-LISA, and the EC is working on that currently. He foresaw publication of the legislative proposal within a month. Mr Heimans went on to explain that the Commission is working on a new e-Justice strategy that will give these developments further impetus.

He continued by stating that e-Evidence is a complex topic. By way of example, he asked the audience to consider what is acceptable in a court of law. Considerations on the quality of evidence start at the time of data collection, and may include points on how a computer is seized, how the information is copied and how it is stored. Things are even more complex if the case concerns EU level cooperation between Member States, he added. It is vital to consider approaches to work with service providers that hold the data too. He mentioned that the Commission is currently looking at how to better ensure the functionality of the EIO, the European Investigation Order, which is a relatively new instrument, so that everything that could help understanding between Member States is included. There should be a platform for digital EIO exchanges, he argued, which will ensure an increased speed of cooperation. He continued by mentioning the new legal framework that is in preparation to deal with orders and requests to service providers in other Member States. Law enforcement needs to be quick in this context to access information before it is deleted by service providers. Mr Heimans explained that all the ongoing work is geared at complementing existing agreements.

Mr Heimans went on to speak about the ECRIS-TCN system, stating the current ECRIS system does not work very well for TCN. As a result, the Commission proposed creation of a new central system to deal with TCN, to be developed and managed by eu-LISA. If there was one European criminal records system, he noted, we would not need the ECRIS-TCN, but from the point of view of policy and personal data protection, this is the best solution

possible currently, he argued. The central system will contain only identity and biometric information and thus is a reference database. Certain issues are being negotiated, with data protection as a central issue, he clarified. Other topics of discussion include possible inclusion of dual nationals – should those with both EU citizenship and third country citizenship be included, he asked, and retroactive inclusion of information – should all information that is already in Member States' criminal records be reflected in the central system, he wondered. Mr Heimans also mentioned that on the issue of implementation, they are working closely with eu-LISA who will be responsible for system operation.

Finally, on the subject of interoperability, Mr Heimans looked briefly towards the ETIAS system and suggested that should a TCN be convicted in the EU, relevant authorities should be able to know that. Yet operationalising this principle is challenging, he noted. Should one include all convictions or certain types only? he asked. And in follow up, if there is a database that only has references and no information on the seriousness of the crime, how can that work? he pondered. This indicates a need for a common EU policy to describe what is indicated in the system, he surmised. And on the topic of combating identity fraud, he asked what to do when a hit against ECRIS-TCN is notified in the ETIAS system? What does it tell a border guard about a previous conviction in the EU? It is key to ensure that there are clear instructions for people on the street or at the border, he stated, arguing that these issues around identity should be dealt with offline. In concluding his intervention, Mr Heimans mentioned the legal proposal on interoperability due in December and said that they are looking forward to discussions with the EP and Council going forward.

Stephan Brandes asked a question about the digital platform for EIOs – does it facilitate an exchange of orders or the results of investigations, he asked?

Mr Heimans answered that the easy part is exchanging the forms and requests for information. However, some answers to cases could take the form of terabytes of information, he noted. Of

course, there are technological solutions that can be used for exchange of such information too, he mentioned, comparable to Dropbox but with the appropriate security and data protection.

Vincent Cambier continued with the Belgian perspectives, particularly focussed on ECRIS. He first gave some background information about ECRIS, its operating principles and the four processes it handles (notifications of convictions sent abroad, received from abroad, requests about TCNs and requests about EU citizens). He then spoke of benefits and issues to face, as well as statistics.

First, on the topic of operating principles, Mr Cambier noted that ECRIS is not a huge database containing all convictions. It connects a Member State's criminal record system to those of other MS. A Member State centralises its convictions, and each Member State must have a central authority determined as an official point of contact with the other Member State. Another operating principle he pointed out is an obligation to exchange information. ECRIS exists since 2012, having replaced the network of judicial registers that was a forerunner of ECRIS and involved France, Germany, Belgium and the Netherlands. Another principle is that responses have to be sent when requests are received. ECRIS operates with codes for the majority of data, which allows for automatic translation and presents great added value. Before ECRIS, Mr Cambier explained, transmissions were received from abroad but sometimes document contents could not be understood or registered in the criminal records. The most important list of codes is about sanctions and offences, he added. It was elaborated based on the European Arrest Warrant, but this alone wasn't enough, which is why a list of the 100 most registered offences in each country was compiled as an elaborated list to enable data exchange. Another important note put forward is that ECRIS has a deadline for responses – 10 working days maximum. ECRIS is used for criminal purposes, which is obligatory, but also for administrative ones. He mentioned that each Member State is free to answer or not in administrative matters. Another important operating principle of ECRIS is that it allows exchange of fingerprints. Mr Cambier is sure that it can help to solve the problem of identification raised by other speakers previously. Nevertheless, he noted that in Belgium, fingerprints are not yet used for criminal records.

On the topic of the four processes, Mr Cambier noted that there are 2 kinds of requests and 2 types of notification. 'Notifications out' involve the sending of registered conviction information regarding a person from another Member State to that Member State. In Belgium, when a conviction is made of an EU national, it is automatically registered in a central Belgian registry and simultaneously sent to the other Member State through a central system for courts. The rapidity of transfer of information is of great value, with notifications reaching the other Member State the same day. The second process is 'Notifications in'. Requests in are received that relate to one's own national. According to Mr Cambier, the benefits of ECRIS and its added value are in the automatic translation of transmitted data. Another benefit is that Member States are now obliged to exchange information, which was not the case in the past. Also, the requests were not always answered or at least were not answered in a timely manner prior to system implementation, he noted.

Practically, Mr Cambier pointed out that the most important issue is the reliability of identity information which is not always correct in requests. For requests about one's own nationals, registers in Belgium can be checked and this sometimes brings forward information that reveals that the person in question is in fact not a national. Aliases are another concern, as is the mix up of data elements, such as the city of birth or the family name. Sometimes the data is incomplete, only including date of birth information, or the name is spelled incorrectly. Another problem he mentioned is that older files are not in the database, meaning that there is a delay in responses to requests. The last problem, although rare, is that some Member States use general codes for other offences that receivers do not understand. Mr Cambier remarked that in 2016, 2 million ECRIS messages were sent all over Europe. He said that ECRIS is a revolution.

In conclusion, he asked whether ECRIS can be a tool for other purposes and perhaps be considered in interoperability discussions as well. Having seen the benefits, his personal opinion is that ECRIS could be extended. It is an easy to use tool and could have other uses as long as there are strict rules in place - for example, border guards, if informed of convictions, must have rules to guide what to do next. Nearly everything is possible, he concluded, but political will is needed.

Stephan Brandes enquired further about identity management, which Mr Cambier had pointed to as one of the major challenges. Could the use of biometrics help, he wondered, and would a connection to a common biometric matching system or identity repository be beneficial for ECRIS?

Mr Cambier indicated that he is sure it would be beneficial. Even in Belgium, he pleads for the use of fingerprints, he noted. The use of biometric data has to be foreseen. He alluded to the fact that in the on-going Council discussions, use of facial images is also being debated. Noting that it typically takes a long time to reach a goal - for example, it took 8 years to implement ECRIS – he expressed hope that implementing other aspects such as biometrics will be speedier.

Ernst Steigenga spoke about e-CODEX and how it could help to deal with some of the issues in judicial data exchange. He began by saying that it is always special to get acquainted with a new community and expressed his view that the e-CODEX community will be now interacting with eu-LISA's community for some time to come. Generally, he mentioned that e-CODEX stakeholders are connecting the European e-Justice communities because there is such a wide range of legal information to exchange. The exchange platform for e-evidence will be e-CODEX and Mr Steigenga said that they would be starting with it very soon if the necessary grant is awarded by the European Parliament. There are 18 million people of multinational descent in Europe, he noted, and everything in life has a legal aspect - children, properties, inheritance. All of this needs care. If people are multinational, these issues are immediately cross-border, and hence,

he felt, the need to provide cross-border oriented support. Luckily Member States have been drafting the procedures to make it happen. Right now, filing claims across borders needs professionals, and even for them it is difficult, he noted. This is something that e-CODEX aims to improve by digital means. Specifically, what e-CODEX tries to do is overcome legal boundaries while increasing safety.

Mr Steigenga went on to explain that e-CODEX took account of the principle of subsidiarity from the start in order to respect the Member States' legal traditions and connect the systems without taking them over. Of course, different legal systems are involved, but e-CODEX created a system for mutual and equal interpretation of data. Instead of seeking to build a common system, they use a common interoperability language that is based on European legislation. Before a full roll-out, each process included is thoroughly analysed. Every time more people are added, the principles have to also be explained, which e-CODEX does. They also use reusable software modules to make it all happen rather quickly, he noted. He also demonstrated the process through visual materials. A lawyer in one state might not be as competent as their counterparts, so the competent persons have to be identified ahead of time for each process. The e-Justice portal is one of the great achievements of the European Union, he argued.

In conclusion, Mr Steigenga also stated that e-CODEX would like to be part of the eu-LISA portfolio. They are very happy about the EC announcement that there will be an impact assessment brought before the scrutiny board in early December and he expressed a desire that work on the regulation will start early in 2018. He mentioned that in that regulation, the e-CODEX community would like to see a paragraph about e-CODEX being a part of the eu-LISA portfolio. e-CODEX is also available on social media channels, where materials are available, he noted. Looking briefly to the future, he suggested that once forms become digital, analogue procedures should no longer be necessary. e-CODEX is building a simple interface that provides services similar to booking a flight or car, with guidance always available.

Stephan Brandes followed up with two short questions. He questioned what the envisaged timeframe for further development of e-CODEX is and wonder whether e-CODEX will be mandatory for use by Member States?

Mr Steigenga replied that the scrutiny board will convene on 6th December 2017. All going well, this could lead to tabling of the regulation during the Bulgarian Presidency with a view to achieving approval during the Austrian Presidency. At the same time, there are procedures inside the EC and

workloads need to be clearly considered. However, the sooner e-CODEX is part of the eu-LISA portfolio, the better, he suggested. The e-CODEX community understands that there is a lot of work to be done at eu-LISA as well, and thus he indicated that somewhere between all the activities, proper dates need to be found and agreed that respect eu-LISA's other important and on-going activities and provide the possibility to successfully overcome the differences between e-CODEX and the current eu-LISA portfolio.

Mr Steigenga said that in terms of mandatory or voluntary usage at MS level, it is not proposed that MS will be completely forbidden to use paper. However, if the MS is going digital, it will have to use e-CODEX because that is the common platform, he noted. Based on his own semantic interoperability background, Mr Steigenga said that incredible effort has gone into preserving the judicial traditions of Member States. Once started on interoperability, it is important to preserve national investments as well, he argued, and this is a definite goal.

Joanna Goodey from the EU Agency for Fundamental Rights gave the last presentation of the session. She started by explaining that fundamental rights seem to sometimes be viewed as an add-on or a hindrance to data exchange. She quoted Julian King, who spoke a week earlier at the European Parliament Special Committee on Terrorism and said that *"Fundamental rights protection does not hamper exchange of data, it is an element of the challenge of effective data management. But the reverse is also a problem, if you cannot prove that you do your work in full respect of fundamental rights, you risk undermining the credibility of your efforts."*

Ms Goodey spoke in some depth about digital information sharing and its positive fundamental rights implications. She drew on the mainstay of the work done at the Agency on migration, asylum and borders, but argued that the principles apply equally to the justice field. With respect to interoperability, if you have a system that is fully operational and in compliance with fundamental rights, it has huge benefits, she argued. Such a system could alert users to criminals, protect our citizens or ensure that missing children are found. It could provide for the robust and timely protection of those entering the EU seeking international protection, enabling confirmation that someone entering the EU has a genuine claim and ensuring they don't have to be detained and are not returned. Also, if mistakes are discovered through interactions between data systems, then the opportunity to identify and rectify the data will be of great benefit. Of course, in the justice field, there is the once only principle, which could have huge positive implications for the data subjects, such as victims of crime, she argued.

However, there are also negatives, she noted, before alluding to some of them in detail. The e-Justice portal builds bridges, as does e-CODEX and ECRIS-TCN. The Fundamental Rights Agency produced a legal opinion in 2015 on ECRIS-TCN, outlining obvious benefits to citizen safety. Ms Goodey referred to Article 8 of the European

Charter for Fundamental Rights while reminding the audience of the purpose limitation principle. Interoperability should not lead to collection of more data that is necessary, she clarified. She also underlined the issue of data accuracy, giving examples from the Agency's work on the ground. Authorities must develop standardised procedures to detect and correct inaccuracies. Ms Goodey went on to underline some potential risks. In relation to the protection of personal data, she mentioned that interoperable systems are increasingly attractive to those with criminal intentions, such as those involved in organised crime or hackers. Also, she said, we have to consider the potential of unlawful sharing of data or use by unauthorised third parties. Access limitations must be very strict and checks and balances must be in place for verification of information given by countries, for example, in cases where fleeing journalists in conflict with the regime might not get accurate verification of their documents. Also, flagged hits must be qualified so that the border guard officer can make the correct decision, she stated. Other considerations she mentioned included the use of biometrics in relation to children, where limits to using biometric data must be considered. For children, if there is a criminal record, it can have a disproportionate effect, she noted. Thus, limitations must be in place related to the retention period and use of such information. Data quality and accuracy were also issues alluded to. While the perception of biometrics is that they are highly credible, Ms. Goodey also noted that this implies that inaccurate information is hard to rebut. In this regard, she stated that people need to be made aware of their rights, such as the right to effective remedy. Drawing on that last point, Ms Goodey highlighted evidence from ongoing research undertaken by FRA that will be published at the beginning of 2018. This research, undertaken in embassies and consulates worldwide, looked at data collection and use in the context of the Visa Information System and Schengen Information System and showed that some 40-50% of those questioned had seen instances of incorrect matching or presence of inaccurate data in the systems. She underlined that this was a small survey, nevertheless. Also, looking at the main problems of SIS II in relation to identification of missing children, 62% of the problem cases that the research examined involved incorrect and 41% insufficient data. Not all Member States are issuing alerts concerning missing children, with 36% of

cases not being alerted, meanwhile. Ms Goodey went on to repeat the fact already noted that interoperability, when it functions correctly, could have huge positive implications for fundamental rights, addressing many of these points.

Finally, Ms Goodey mentioned some important considerations for the justice domain, especially relevant considering that there is a push towards sharing information more systematically on suspects, defendants, victims and perpetrators. Relevant fundamental rights principles always applicable given this push include purpose limitation, access rights, transparency for the data subject, data retention period limitation, and particularly the rights of the child, she stated. In the justice field, there are different ages of criminal responsibility, with the lowest being 9. She also underlined the particular considerations for victims of crime. Concluding, she said that lessons learned from interoperability in the home affairs domain have implications for the justice domain. She underlined that in addition to usability, ex-ante and ex-post assessments of fundamental rights impact assessments need to be built in to the systems.

Challenges are amplified in cross-border contexts, but correct function can benefit the data subject, the users and fundamental rights generally.

Stephan Brandes asked a final question concerning use of biometrics and the use of tools like the common identity repository and biometric matching system. Could these systems provide opportunities for the justice domain, he asked?

Mr Heiman answered that the Commission is striving towards interoperability in all domains with large scale IT systems. The question is not so much whether it will happen but how we will do it, he suggested, particular so that all issues outlined are considered. The benefits for security and combatting identity fraud are clear.

Ms Goodey replied that the use of biometrics should not be seen as a negative. The potential for inaccuracies concerns alphanumeric data,

which needs to be properly matched with quality biometric data. The important aspect is how the data is used, but there are definitely positives to consider, she indicated.

Mr Steigenga said that use of biometrics depends on the use cases for any associated system. In the e-CODEX context, if there is a reason to use the biometrics, the stakeholders would support it and it would be up to the competent authorities to decide on their use. He mentioned that e-CODEX has carried out an impact assessment on privacy that found that most of the responsibility for fundamental rights lies with the authorities that want to use the information. The responsibility of e-CODEX is to decide if the use of a certain instrument has a legal foundation, and if it is there, they will support it. In the end, if e-CODEX is used, it is user communities that decide on the instruments used and the information exchanged, he summarised.

Closing remarks for day one by eu-LISA Executive Director Krum Garkov

Mr Garkov concluded the day by telling a short story about two men who were chopping wood. The first one worked very hard from sunset to sundown, but each day the other man, who was taking longer breaks and resting more often, had a higher pile of wood chopped. So, when the first man asked the other about his secret, he replied that while he is resting, he is also sharpening his axe. He expressed his hopes that the exchanges of the day helped the participants sharpen their digital axes rendering them better prepared for the digital revolution. He thanked everyone for their excellent work and contributions.

Day 2 (18 October): **Innovation Day/Workshops**

Session 1: **Mobile Devices and Technologies – Driving efficiency of the operations on the ground**

Moderator:
Maria Bouligaraki,
Head of Asylum Systems Sector, eu-LISA

Panellists:
Frank Smith, Chair, ENLETS Mobile
- Trends and perspectives in mobile technologies
Sarah Hjortsmarker, Swedish Police
- Practical initiatives towards the use of mobile technologies in operational work
Axel Görlich, Senior Sales Engineer, Crossmatch
- Mobile technologies for operational efficiency
Joao Fernandes, Head of Information & Communication Technology Unit, EASO
- Enhancement of the use of mobile devices in hotspots

Introduction by **Frank Smith,**
Chair, ENLETS Mobile - *Trends and perspectives in mobile technologies*

Frank Smith began by introducing the ENLETS mobile group. It is a network focussed on mobile law enforcement technologies that meets twice a year to keep in touch with developments. He described some areas in which the group is active, in particular focussing on the use of smart phones in police work, at borders and in law enforcement generally. He noted that mobile technologies allow officers to efficiently resolve identity issues, helping to determine who is the person stopped and what is known about them. Having a hand-held machine that is highly portable and can give access to backend IT systems can help to avoid unnecessary arrests that cost time and inconvenience the citizens, while ensuring that perpetrators of crime do not get missed. More mundane applications include issuance of parking and speeding tickets. Hand-written slips easily contain errors and tickets get rejected. However, with smart phones, information can be directly transmitted to a central system, providing a one-stop-shop in which transactions are initiated and completed in one contact. Mr Smith noted that what is evident in the ENLETS group over the past 1,5 years is that there has been a lot of work building upon successful small-scale pilots. For the first time, the group is seeing police authorities that are so convinced of the usefulness of smart phones that they have rolled out to 100% of officers. This is significant, he added, because it maximises benefit and makes a statement that such devices are a standard part of police equipment. Four participants of ENLETS have rolled out smart phones to 100% of officers: Sweden, the Netherlands, Denmark and Norway.

Mr Smith went on to explain that getting development right from the beginning is important. The ENLETS mobile group acts as a forum for gaining consensus on and sharing best practices, taking input from those that have implemented mobile solutions already. Amongst the best practices already identified, he alluded to the realisation that the introduction of mobile technology requires re-examination of business processes. He added that truly engaging with

the users is also important. Piloting, testing, revising and agile development are all part of the active development process that is advisable. Mr Smith highlighted that one cannot write perfect specifications at the beginning that should be followed throughout; rather, with the perfect team, adjustments can be made as they arise. He informed that the next ENLETS meeting would be held in Tallinn a month after the conference, as part of the Presidency. One of the topics of the agenda is to look at where mobile is going. The past 5-10 years have been a period of very radical and disruptive change in mobile technologies. His conclusion in the paper that he will be presenting at the meeting is that change will continue to be disruptive and radical and projects will have to cope with this change and evolve continuously.

Sarah Hjortsmarker began by explaining that resolution of identities is one of the first challenges countries tackle when going mobile. As work in the streets is really important, Sweden began by enquiring what 35 police officers need in such work. They indicated that tools for identification of persons were needed first. Other priorities were set later according to the answers provided. According

to Ms Hjortsmarker, it took 2 months for the first delivery to be completed thereafter. All 35 police officers involved tried the new version and provided feedback for further functional additions through an on-board app. The interface for feedback is easy and well used and has been mimicked by other countries. Over the past 2,5 years, 1500 evaluations have been submitted by police. Sweden has rolled out 17 000 phones to officers, with 9000 more set to be rolled out in the next period.

The moderator Maria Bouligaraki followed up with two questions. She asked Mr Smith to further explain his statement about how we can use mobile technology to enhance information availability. She also questioned how difficult a change in approach from a specification-focussed approach to something more agile typically is.

Mr Smith explained that while a smart phone may look rather insignificant as part of a police officer's tool kit, the solutions are typically connected to a lot of different systems; in Sweden 18 different databases are connected, he added, meaning that a lot of things are brought together on the device.

Ms Hjortsmarker indicated that sometimes police officers give feedback and ask for things that can't be done of course and reminded that one always needs to stay within the legislative framework. But often, the requested features are adapted from desktop to mobile. They try to undertake such development in a minimalistic way and then add on features in the course of in-house development.

Mr Smith recalled that the Netherlands were considering provision of alerts as discrete vibrations – an officer, without looking and while speaking to a suspect or victim, could be alerted regarding former convictions of assault, e.g. against police, so that the officer knows to be careful. After discussions, the feature was built and tested and is now part of the Swedish system. Building specifications is interesting in contract terms, Mr Smith said, but sometimes developers come to a boss and say that it should be built in a manner different to that specified after contracts have been signed. In this manner, building of something different is penalised and this can be frustrating. Authorities need to consider how to contract better, he argued, in order to keep things flexible.

Ms Hjortsmarker added that in Sweden, they decided to build their own capacity with internal teams as one approach to provide such flexibility.

Joao Fernandes noted from the outset his point of view that mobile devices could improve efficiency at migration hot spots. EASO has been working at hotspots for two years, he noted, implying that they have a lot of experience in the field. In hotspots, the conditions are sometimes very complicated for work, he explained. The Moria hotspot on Lesbos island in Greece, for example, is surrounded by a chain linked fence because rocks have previously been thrown into the compound by frustrated persons outside. There are efficiency problems that arise, inter alia due to unreliable systems and infrastructure often present in remote places. Amongst problems often apparent, he enumerated frequent interruption in connections, a chaotic working environment, high staff turnover and rioting. Furthermore, processes are often cumbersome and involve many actors, and thus are often inefficient.

Mr Fernandes suggested that mobile could be part of the solution. Such a solution would need to be highly portable and flexible in its applications, offer a greater reach than current solutions and in an asymmetrical fashion. A good example of how mobile is already demonstrating potential, according to Mr Fernandes, is the EU Relocation Programme App. It provides a reference for understanding rights and obligations of applicants.

Mr Fernandes went on to explain the asylum procedure as typically managed at hotspots, explaining that after arrival, a migrant is registered as a TCN by Member State officials and Frontex, who are the first contact officials. The migrant is then asked whether they will apply for international protection, after which the logging of the application takes place involving the collection of personal data, such as age, country of origin, marital status, etc. The flow of asylum procedure continues into the Dublin procedure, which potentially leads to a transfer and the initiation of activities related to relocation.

Looking towards opportunities for use of mobile devices in the context of the elaborated processes, Mr Fernandes noted that EASO has developed a series of practical guides to consolidate terminology, solidify processes, structure checklists and support easy reference. One such guide, used during registration, details matters related to access to asylum for first contact officials. Border guards and Frontex official don't carry books or computers, so a mobile guide could significantly help gain efficiency. Another guide relates to reception standards that should be communicated properly to the migrant and could be similarly accessed on a mobile device. The third tool he mentioned concerns the identification of people with special needs. It includes a decision tree designed to address signs of distress and another to help assess if the person has been a victim of physical or sexual violence; such processes could be supported with mobile apps. On the admissibility process, he also suggested that there is room for improving processes with mobile applications. Last, on eligibility, he mentioned the reference guide for methodology, which is useful for interviews.

Additional practical suggestions put forward included apps for interview scheduling (currently an information board is utilised, a rather inefficient solution), translation (dictation and transcription post-interview currently takes 5-6h), queueing and ticketing for migrant access to information and health, provisioning of information on relocation, rights and obligations, identification of dialects, biometric identification and reception management (dispensing of food, clothing, bed allocation, etc.)

In conclusion, he reminded the audience that EASO seeks harmonisation of efficient hotspot processes and expressed his view that mobile technology is the way to go to achieve such efficiency.

Ms Bouligaraki noted that simple and solutions for many of the matters raised exist and therefore wondered why they have not been deployed yet? What prevents us, she asked?

Mr Fernandes replied that some solutions can be implemented without difficulty. It is not about regulations, but going through procurement and engaging vendors. This needs to be done more efficiently, he suggested. Thus, problems arose through bureaucracy rather than technology or vendor constraints.

Axel Görlich took the floor expressing an intention to look at the past, present and future of mobile devices and also assess the challenges that the industry is facing in dealing with new requirements related to mobile. Presently, he noted, we see a proliferation of mobile devices that is staggering. Technology is a key driver in the mass market and there are so many new things on the hardware and software sides. Experience has shown that use cases are also different, changing from location to location. However, end user demands are generally quite consistent. In mobile, he said, people want solutions that are smaller, lighter, more efficient, more powerful and consume less energy. Currently, looking at the history of mobile devices, it has evolved into several sectors. At the beginning, one saw a lot of biometric enrolment devices, yet then the requirements of border management developed alongside those of enterprise, retail, and the military. The challenges the industry is facing is to make sure and figure out what is now needed. Clearly, he assessed, having a monolithic set of specifications does not help. We see a variety of use cases for all-in-one products, often a smart phone with peripherals. Other challenges concern data privacy and interoperability, which, he considered, is where regulations come in. Of course, he added, price pressure is another issue. Special use cases also present a challenge for industry, as they entail small volumes and offer less ROI.

Mr Görlich explained that smart devices, especially those from the commercial sector, present a challenge as well. There used to be a requirement in tenders for maintenance of a minimum of 5 years. However, smart phone lifecycles might not be as long. For the police, he noted that devices were used in a closed environment up until now, yet mobile devices bring the systems out into real life. Data encryption is an issue, particularly when using open networks and new architectures need to be designed with that in mind.

Coming to the topic of evolution, Mr Görlich explained that as soon as devices became smaller, they made enrolment simpler. All-in-one devices provide a unique experience. In evolving enrolment and verification systems, existing information needs to be included while leveraging innovation. The variety of use cases has also led to the development of a lot of portable solutions. On the identification side, authentication is becoming key, particularly due to cybercrime considerations.

Mr Görlich added that interoperability is critical and compliance with industry standards is a must. The compatibility of data (formats) is crucial in today's multi-application environment. Cross-border operations require a common set of interfaces. Also, relay stations are needed to store, forward,

translate, convert and re-direct information. Another important aspect is multipurpose usage: leveraging a device for application A on one day and B on the next day.

Mr Görlich concluded by saying that in actuality, mobile is nothing new. Mobile is the future but also the present, he commented. Technology opens doors for further improvement, but capabilities of any device also require changes in associated processes if to be properly leveraged. Industry, meanwhile, will have to consider approaches to positively impacting efficiencies and cost savings.

Ms Bouligaraki started the discussion by asking about market perspectives. Is this an interesting and profitable market, considering the low ROI and price pressures mentioned, she wondered?

Mr Görlich remarked that industry has changed and has to continue changing. 10-15 years ago, he noted, it was easy to have a high-quality enrolment device rolled out. Yet now companies can't deal with all requirements, he suggested. They need to work with cloud based features, for example, which

inevitably leads to a different company strategy and architecture. Overall, he assessed nevertheless that there is certainly still some business.

Ms Bouligaraki opened the floor to questions.

Q – The first question from the audience concerned whether there was one solution for the mobile datasets used in several member states, and if so, who is responsible for the authorisation and the so-called back end?

Mr Smith replied that officers have access to the large-scale systems such as the SIS II, all of which are subject to the appropriate laws on privacy.

Mr Görlich added that making the life of the policeman easier has little to do with interoperability. It is about getting the information you already have, not only in police systems, but in other sources, even on websites. At the moment, there might be no mobile view and no login capabilities to access such information. Officers need to better use what already exists, he argued. Interoperability here doesn't mean there is a conflict of different formats; rather there is a need for interoperable language, making things easy to exchange. Then, it is simply a matter of making mobile versions available, he stated.

Q – A representative of industry in the audience suggested that her company, like others, is ready to propose solutions. One significant issue, she stated, was how to deal with EU procedures, typically built around exhaustive specifications, long procurement and bureaucracy

Mr Fernandes agreed that it's always the bureaucracy that stands in the way. Of course, it is necessary, because it is public money, but there must be an easier way to drive efficiency in cooperation with the private sector, he suggested. He could offer no solution other than following the necessary bureaucracy, however.

Q – The next comment and question came from Krum Garkov. He said it is clear that EU entities have to follow rules, of which they are

not masters. Thus, he suggested that it was incumbent on industry to adapt and be as flexible as possible. Rules are rules, but on the other hand, to make the best match between what we want and what the policy dictates, we need standards, he assessed. We have technology standards for mobile solutions, he noted, but he suggested that there is something missing beyond technical standards. Do we need to think that standards should go beyond technology, to define a standard reference architecture, for example, in hotspots, he asked?

Mr Smith answered that we've seen the usefulness of having some standards set out. He noted that his group set out a simple reference model in early 2011 with a structure in which multiple mobile devices could use a communication hub and a broker so that it becomes easier to plug in an extra system or device without having to rebuild everything. The pace of mobile development is high, so such a structure needs to be built into the front end, he suggested. It was a simple principle, but it has lasted 6 years and seems to be sustainable.

Mr Fernandes added that he is more in favour of a stepping stone/ staged approach, rather than a toolkit approach. He mentioned the spaghetti approach to architecture.

Q - Ms Bouligaraki added that from the EU agency side, they have seen that every Member State can have their own system on the ground. However, if we want to talk about European capabilities, we need standardisation and reference architecture, she suggested. This does not decrease flexibility but rather achieves quite the opposite. She wondered therefore, what prevents more numerous participation in the ENLETS mobile group that could be a forum for working towards such cross-European standardisation?

Mr Smith added that all Member States are welcome to participate. At the moment, there is more contact with some states than others, he noted. Of the 12 regular members, 4 now use mobile devices as standard equipment. That number will grow and the change is very tangible, he claimed. There is some industry participation in the network as well, he noted, which in 2011, for example, was instrumental for the network's developments. However, due to competitive issues, they are not always involved. No Member States would be turned down from participation, he reminded, and while there are some practical issues in terms of size, no rejections of membership have been made to date.

Q – Sebastian Muir from GoSwift in Tallinn asked the panel for their views on opportunities to include citizens' or travellers' smart phones in the context of systematic checks involving, for example, biometrics at the border. Is it realistic and what could be the implications?

Mr Smith noted that he was previously a member of the Article 6 committee on passport chip security and is, as a result, familiar with the complex cryptography and standards associated with e-passport verification. He suggested that he could envisage in the future a mobile phone becoming an identity carrier or a passport but added that it would take a lot more than is currently available. Interesting things are happening, he said, and although maybe the border wouldn't be the place to start, over time things must be moving in that direction. The police will surely see more engagement with citizens through electronic communication.

Mr Fernandes expressed the opinion, meanwhile, that consumer devices are not ready for law enforcement yet.

Mr Görlich expressed appreciation of the idea of using a smart phone to replace a passport or to prove an identity, noting that ID cards are already combined with credit cards, demonstrating the benefit of merging documents into one. However, he noted that to date, law enforcement and border security have always had transactional approaches. At a border, for example, we have an individual and enrol biometric data as a transaction. Yet he suggested that we no longer should look at individuals thus, but should combine information that we could get from open sources like Twitter. This will be possible and use of smart phones will be part of the solution, he assessed, yet looking at the bureaucracy to be overcome, suggested maybe in 10 years.

Q – A representative of SITA wondered if is there an increase in the challenges for physical, mobile, and access security given the proliferation of mobile?

Mr Görlich replied that over the last years, there have been lots of breaches related to credit card companies, healthcare systems and even law enforcement data, and agreed that we also need to secure devices themselves. Since mobile devices offers a door into our protected information, protection is critical, he suggested. Multifactor authentication technologies are there and should be used on mobile devices, he added.

Mr Smith added that security on devices has advanced and it is common for high end smart phones to have a secure chip. That is an important stage, as without that, both the device and the on-board data can't be trusted, he noted. However, looking at the developments in touch ID, banking, fingerprint access – a lot of the elements are there and there is great potential for development. The question is how to measure whether something is right for an application, he suggested.

Mr Görlich added that nowadays most operating systems are online systems and we cannot prevent designers from opening some backdoors. We have to rely on regulation and policy for prevention of such aspects, he stated.

Ms Bouligaraki added that physical access is easy in hotspots, we cannot safeguard all the devices and sometimes public networks are used, which makes security even more important.

She asked the panellists for their final thoughts.

Mr Smith concluded that we are living in a very exciting time. Previously, there were a lot of meetings and talk of pilots, but now we have reached a point where we see operation at scale. These operations are good examples and more will arise as a result.

Ms Hjortsmarker summed up by saying that the countries that have joined the mobile initiative have built capacities. Experience has demonstrated that having agile capabilities on the ground is critical, while it is vital that the end user is involved as part of the development process.

Mr Görlich's final comment was that from the industry point of view, end users must be consulted in definition of requirements and industry regarding capabilities before procurements are initiated.

Mr Fernandes' key message was that mobile can definitely drive efficiency. Also, he advised to not forget that some migrants do not have basic things - smart phones do exist in hotspots, he clarified, but not everyone has them.

Session 2:
Delivering Security through Enhanced Interoperability and Analytics

Moderator:
Tõnu Tammer,
Counsellor of IT systems in Home Affairs, Ministry of the Interior of Estonia

Panellists:
Andres Kütt, Former Architect of Estonian Information System, Information System Authority of Estonia (RIA)
- X-Road, Estonian experience and vision in building secure platforms enabling interoperability
Brandon Murdoch, Partner Software Engineer, Identity Division, Microsoft
- Global trends and innovation by the industry in developing solutions for interoperability for secure Europe
Sergio Fernandez, Regional Director for Airport, Passenger and Security in Europe, IATA
- Enhancing data processing through new interoperable technologies
Martin Ruubel, President, Guardtime
- Blockchain-based solutions for enhanced interoperability

Introduction by **Andres Kütt,**

Former Architect of Estonian Information System, Information System Authority of Estonia (RIA)

- X-Road, Estonian experience and vision in building secure platforms enabling interoperability

Andres Kütt began by indicating his pleasure at attending the conference and having the opportunity to hear about real experiences from the field. To begin, he outlined two problems with interoperability. The first was inception – how to get going. Making integration hubs is easy – one can simply pile up technology, but it doesn't mean it actually does something. Second, adaption – governments can't keep up with rapidly changing technology. He said that luckily, nature has shown us how to cope with these problems, in the form of demonstrating how ecosystems work. They get started fast - for example, one may bring species to an island and they will breed rapidly until an equilibrium is reached. With x-road, he compared its development to the chicken and egg problem. It makes no sense in joining any community if there is nobody in that community and vice versa. Like the first person with a fax machine, little happened for most of the time while he developed the service. Subsequently, in Estonia, the use of x-road was made compulsory, which kick started the ecosystem and it led to a flood of services joining. Most services were useless and were implemented for the sake of compliance, yet the more services joined, positive feedback loops were created along with exponential growth, he noted. So, the key message Mr Kütt wanted to pass on is that if we want to build something secure and interoperable, spanning the entire community, we must look for ways to ignite those ecosystems. Legal action and/or investments are critical to secure fast adoption and adaptable response. As technology changes, the members of the ecosystem should react automatically, he added.

Q – Moderator Tõnu Tammer asked two questions in follow up. Why did Estonia decide that we need to implement interoperability, he wondered? And how did Estonians overcome privacy concerns?

Mr Kütt said that the first decision was easy – it's amazing what you can do with very little money and a lack of resources, he asserted. As for privacy, he argued that sharing information actually greatly

enhances privacy. Let's assume, he said, that there is a society that doesn't share information. In such a situation, all agencies need to collect information, which means the data lives in 50 or 500 places. What are the chances of information leaking from 500 places, he quizzed rhetorically? Keeping data in one place actually enhances digital privacy because those leaks do not happen.

Tõnu Tammer introduced the next speaker by indicating that he watched 5 different YouTube videos to understand blockchain, however, he still wasn't sure if he fully understood all concepts. At the same time, he compared the situation to flying in a plane – you don't have to know how it works to get from point A to point B.

Martin Ruubel continued the discussion by suggesting that that the plane analogy was not entirely appropriate. While blockchain sometimes looks like magic, nobody wants to fly in a plane that runs on magic, he joked. On a more serious note, he said that blockchain is a technology concept, asserting that while bitcoin is a blockchain, the reverse is not true. There are a number of different interpretations out there, but his general recommendation would be to look at the problem

that might be solvable with a blockchain. He explained that blockchain is a database that is exceedingly hard to manipulate by any one party because that database is in many places at once and is continuously updated. If anyone wants to tamper with their instance of their database, everyone else would see that and reject the change. In this way, he argued that sharing is not actually the opposite of privacy, but the more witnesses there are, the more secure data is. Despite this inherently opposite nature and the need for privacy and confidentiality, the two can exist together in a way that advances interoperability and transparency for society without sacrificing the European core value of right to privacy.

Mr Ruubel went on to explain what can be done with blockchain. One option is building a global cryptocurrency with no need for central governance, and that was widely embraced by a number of sections of society. Of course, it has been the go-to currency for illegal activities, which has made it impossible for governments to use. Yet right now, he noted, cryptocurrency is worth 171bn dollars, with over 70% being bitcoin. With blockchain it is possible to track any digital assets such as insurance

contracts, claims and land records. He mentioned smart contracts as something that has received a lot of attention. The term smart contract is 2-3 years old and came about when blockchain did. He suggested that all such functionality is enabled by its ability to immutably assure the integrity of information stored on the blockchain. For the first time in history, it is possible to verify the integrity of data without any authorities confirming it. You just need trust in mathematics, Mr Ruubel added. So, the formal proof is the number one requirement for using blockchain, because it allows one to know under what conditions a cryptographic construct is valid and when it will break. If there is no understanding of where the limits are, it will cause problems. Mr Ruubel confirmed that there are blockchains with this type of formal proof, which is an academic activity that is time consuming and rather uninteresting, albeit important nevertheless.

Mr Ruubel summarised that blockchain is a technological concept and reiterated his point that one should not confuse it with bitcoin, etherium, any other blockchains. Blockchain can and is used to ensure traceability and data integrity across databases under the control of different parties without the need to sacrifice privacy and security. It is possible today, he clarified. Estonia has been testing one blockchain technology since 2007, specifically to enable integrity verification for its registries, and it has been in use since 2012. So, for any advice for blockchain usage in governments, there is no better place than Estonia, Mr Ruubel confirmed. There is no need to reinvent the wheel because there are many problems that can be and are solved using blockchain technology.

The moderator asked about policymakers talking about and demanding the use of new technology. Is it important for legislators to understand the technology in order to ask for it, he wondered?

Mr Ruubel suggested that it depends on who one talks to. The recent EU cyber security strategy outlined one or two technologies, he noted, explicitly mentioning blockchain. He thinks it is important for the executive branch to be aware of the stage of technology development, especially the ones that have a potential to increase interoperability. Blockchain really can be used to enhance cooperation quite extensively. At the political level, talking with parliament members, understanding is at a completely different level, he clarified, which is inevitable. He also said that it is beneficial to use simple examples and highlight simple use cases, because at the end it is the political bodies who finally sign off on any initiatives. Summing up, he said that blockchain understanding is already there, but it needs to grow.

Brandon Murdoch spoke of how Microsoft sees these developments from the standpoint of an industry leader. He first noted that he sees identity as the thread that runs through all conversations around interoperability, relevant to both those using the systems and those operating the systems. Mr Murdoch spoke of the lessons Microsoft has learned as it has made the shift from the old world to a cloud based world, and when seeing identity evolve from a network based issue to identity as a control plane. He first said that there have been major shifts in the enterprise IT landscape over the last years, with a move from centralised on-site solutions to de-centralised nodes, whether in cloud or outside the enterprise boundaries. This has created 'perimeterless' enterprise and government, a change from platform to standards-based integration, and this has led to a situation where identity is a transposable asset and moveable across enterprise boundaries. For a long time, Microsoft was not a positive advocate for open standards, he noted, but the organisation has made significant changes. Especially when it comes to identity and security, a wealth of standards is coming up, such as SAML2, Open ID connect, Token binding and SCIM2.0 (a cross-domain ID management protocol). All of these things are starting to gather pace, he asserted. According to Mr Murdoch, Microsoft is very involved with them and cooperates with other industry leaders such as Google and Amazon to drive standard development and evolution. As a company, he said that they have benefitted from standards in the area of identity. There is a wealth of cloud identity providers, and interoperability has been driven by standards and customer demand. Microsoft is fully aware that solving the identity issue requires collaboration and open standards drive that goal. He mentioned that SCIM is a relatively new protocol, used for integrating, managing and provisioning identities across systems. The benefit for Microsoft has been agility in meeting huge demand. Adopting standards has helped integrate with the likes of Facebook and other large entities in a secure, reliable and scalable manner in less than 6 weeks. He said that people are moving now to the Microsoft platform.

Mr Murdoch continued by saying that we talk about how identity needs to be secure, strong and without friction. There are new technologies coming out, for example, FIDO and the initiatives surrounding it, and there is a lot of adoption in government and large business. This kind of work needs collaboration with industry leaders, but also smaller innovative practices, creating an identity ecosystem. He said that the ambition of Microsoft is to have 1 billion identities, all without passwords.

He said that one of the advantages of building cloud capabilities has been the intelligence it brings, the adaptive learning and the real-time mitigation around identities. In terms of intelligent security growth, being able to see how identities are used and flow across various systems allows determination of how to deal with identity. For example, instead of blocking in some instances, creating additional hurdles is useful and allows the user to continue working. In terms of figures, he pointed out that they have 14 billion authentications per day. They also work globally around the world with law enforcement and security researchers. Microsoft is also very involved with learning lessons from the dark web regarding how to understand when identities are changing. Machine learning is now being used to drive this protection and to understand how identities are being compromised, leveraged and pivoted. Conditional access controls allow for adaptability so that the process does not get in the way of business.

Mr Murdoch went on to say that although there is a technological aspect to interoperability, for Microsoft it was a cultural change. He said that an open mind set to continually learn and embrace change is crucial, noting that change comes anyway. According to Mr Murdoch, Microsoft has designed for change and looks forward to it. This requires thought on perimeterless enterprise and heterogeneous environments. Across the organisation there are different conversations being had, frequently not about technology but about outcomes and change that the government or company wants to achieve. There are architectural imperatives, and all industry leaders are thinking in those terms. In summary, he clarified, interoperability is more about mind-set than technology.

The moderator asked whether in Mr Murdoch's opinion it would make sense to integrate private and public IT management? Would it work technically and politically?

Mr Murdoch replied that technically it can work and noted that it has been done already. There are political winds of change blowing in this direction, he suggested. No sector alone can solve identity problem; it takes collaboration. But beyond collaboration, adaptability is even more important as new technologies are developed and built, he asserted. The private sector is a bit more agile and it can lead, but it needs to work with the government.

Sergio Fernandez opened his intervention by outlining that he would present the passenger view of relevant data and its exchange. Firstly, however, he provided an overview of IATA in numbers: the organisation has over 260 members and it represents more than 84% of global air traffic. He went on to say that one of the questions when talking about interoperability and security in this domain was why? For IATA, the answer is clear, since there are more than 28 000 flights on a daily basis and 941mln passengers flying to, from or within Europe. Furthermore, this figure is going to double in the next 20 years. Yet governments are

currently not using digitalisation opportunities to process passengers in a smooth and secure way. Mr Fernandez warned that if we don't do anything, there will be longer queues and more risk. Airports need to control a lot of people in a short time. He said that IATA's vision is to provide passengers with an end to end experience that is secure, seamless and efficient, which is why we need to win the digitalisation war. Interoperability is key in this regard, he asserted. Mr Fernandez went on to explain that the current process examined by IATA has three focal parts. First, the pre-travel stage, where some travellers need a visa or some other authorization and fill out information to allow airlines to check with authorities. This often requires manual intervention but that implies error. Research by IATA on the validity of API information showed that more than 60% of information was unintentionally wrong. What passengers want is to move through the process faster in an airport, and particularly to do things pre-travel, which is why we need interoperability and the digital world. One of biggest frustrations is the security check point, he added. The process is the same for everyone, which does not increase security. Advance information means having advance risk profiles and differentiation, and it can ensure that the right resources focus on the right people. Mr Fernandez referred to an IATA letter submitted to the EU Council that also outlined that we need to balance security with efficiency.

According to Mr Fernandez, work moving forward has to be comprehensive and holistically driven. In his opinion, silos are not good because they lead to redundancy and duplication. Interoperability is a must, and it has to be implemented in a cost-efficient manner, he argued, that leads to safe and seamless procedures for passengers and authorities. He further mentioned that interoperability has to be based on collaboration and information sharing, and thus, that agencies must talk to one another. Mr Fernandez explained that key success factors for improved passenger experience include reducing repetitive identity checks, limiting manual interventions and avoiding repetitive data transmission to different parties.

Mr Fernandez said that IATA has tried to collect all these aspects into three key initiatives. Firstly, he said that we need a passenger information single window - now we have PNR, API, EES and ETIAS, we have four datasets all about the same passenger. This data can and should be assessed in advance, he suggested, to make processes secure and smooth at airports. Secondly, the concept of one identity should be promoted. Thirdly, he referred to IATA's Smart security initiative, which deals with how to improve security check points. There is a need for the security check points to recognise passengers and apply the appropriate security measures to ensure that more time and complex attention goes to the 'bad guys', not the frequent travellers.

Mr Tammer wondered whether passengers support and appreciate the efforts of governments to improve checks?

Mr Fernandez replied that in his opinion, passengers don't really understand. They think that

the government has more information than they actually do. A survey conducted by IATA among 70 thousand passengers showed that more than 85% would be willing to share more information if it made the process smoother. When passengers are stuck for over 10 minutes, it's already a mess, he argued. The passengers just want the airlines and authorities to do their jobs while making sure that everything runs smoothly and securely.

The moderator then opened the panel to questions from the floor.

A Council secretariat representative asked Mr Fernandez whether it would be conceivable to have an expedited procedure for the 85% that are willing to share more information?

Mr Fernandez asserted that there is no intention to decrease the level of security. Current systems can already check information ahead of time, meaning that the remaining 15% could also benefit from the expedited passage of the rest. There are talks ongoing to determine how this could be achieved, he stated. The technology is already out there to make it happen, but it just needs to be put in practice, he noted.

A representative of Accenture asked about the concept of one identity and wondered how trust can be established with the entity providing the service when a person might have 3 different identities in 3 countries or organisations?

Mr Fernandez replied that this is something that demonstrates the need for collaboration. Unfortunately, he said, most of the pilots for this concept are in different states, they are state driven, and nothing connects the dots at the moment. That is why IATA has encouraged the European Commission to also move towards one identity concepts. They suggest that authorities store in one rather than several different instances.

Mr Ruubel also reflected on the idea and stated that it would be useful to have one instance issue one identity, be the central point that shares the information to authorised users and carries out verification.

Mr Kütt added that there is also the question of data ownership, which means that having 3 identities in separate instances should not exist. Rather a person should have 1 identity and decide who has access to it, he suggested. There are interesting proof of concept solutions and something should be available soon, he suggested.

Mr Ruubel commented by saying that the example of three identities is an excellent one for demonstrating how a lack of interoperability actually endangers privacy, because all of a sudden, 3 organisations have access and store personal data, instead of just one.

Axel Görlich asked the panellists to consider a more holistic approach, noting that airlines collect significant information. He wondered whether it could be shared with other parties involved in activities at borders?

Mr Fernandez noted that when one travels by car across borders, no information is requested. A similar situation can be achieved with air travel, he argued, if redundancies and silos are removed. He suggested that one could complete checks seamlessly by using and sharing all of the information available, such that there would be no need for stopping. Mr Fernandez added that no physical stops are needed for risk assessment. Mr Kütt added that drug detection works in that way. He said that it is plausible that every passenger at the airport or at the border is identified without them knowing about it. However, then the question is how the information is used and how the citizen is made aware of it. Mr Ruubel also confirmed that the EI, the interoperable European Identity, is there. He suggested that one could use it to log in and buy a ticket before going to the airport, where he/she could insert the card in a kiosk and enter a pin. This is more secure than somebody checking the ID card as current procedures request, he noted. Mr Fernandez added that some suppliers are working on identifying passengers on the move by using technology. Mr Kütt said that a person is getting identified at many different points without understanding the reasons for this. On this basis, he suggested that simplification is definitely possible as long as it is done in a transparent way. Mr Ruubel added that he supports the notion that technology is in place for future developments already and that right now we can streamline the entire process considerably. When the blockchain layer is added on top of it, independent mathematic transparency can also be added to how the data is used and information on users will also be available, he noted. Mr Kütt referred to the General Data Protection Regulation (GDPR) that enters into force in a few months,

noting that there is a requirement that states a data subject must be notified of data misuse in 72 hours. However, the breach discovery average is 7 months.

Mr Carolan from eu-LISA posed a question related to governance. Noting that the data being spoken about was owned by various authorities and came from different sources, both private and public, he wondered who should drive work towards information sharing in the manners being considered and who would implement the standards and framework necessary to make sure that data is shared and accessible?

Mr Kütt said that he believes it is the government that should take this role. He also wondered about the data being owned by different parties, arguing that the data is still owned by the subject. From the private sector point of view, Mr Murdoch confirmed that the government needs to be involved, but it should be led by the private sector. The government should provide oversight and regulation. There are initiatives around shared signalling and this is where blockchain can be implemented. Mr Kütt agreed that it is a good base for cooperation.

Mr Ruubel suggested that in the global context, it is hard to imagine that there will be one government that will lead so that everyone else will rally around. Mr Kütt added that every government can take a lead role and set out their conditions for authorisation and usage independently. Generally concurring, Mr Ruubel felt that it was nevertheless also important to have an interoperability framework for those governments that have decided to take this route.

Mr Murdoch added that the general public has to understand the concept of consent. For example, in the case of Facebook, most people do not realise that they are the products. So, he thinks that we need more conversation on those types of topic. Mr Ruubel interjected that it comes down to the issue of trust and the perception of the general public, which is very difficult to change. Mr Murdoch agreed that it is amazing what people are willing to give up, while simultaneously demanding privacy.

Mr Fernandez replied that he would love the government to drive it, but noted that their pace is different from that of the private sector. Management costs are always high, so airlines would be very happy to see governments be the

divers, as they are in the case of those governments who have taken a driving role, although even they do not see the urgency that the private sector experiences.

In response to the previous assertion of Mr. Kütt regarding data ownership, a representative of Accenture pointed out that a citizen does not own their criminal records or risk assessments. In this regard, the countries define risk and that is why there is API and PNR.

Mr Fernandez agreed, stating that the citizen provides information and the risk assessment is done utilising this information, but he argued that validation does not have to take place at the airport. Information should be sent once and all entities should do their own risk assessments as necessary in order to decide whether a traveller can fly. Mr Ruubel added that in an ideal world, he would not have to share information. However, he suggested that when information is shared, he would like to have access not to the risk assessment but to the information about who accessed his information. Mr Fernandez said that if the responsibility for entering information would be placed more on the passengers, it would help eliminate errors from careless data entry by intermediaries, and it would also allow the citizen to directly know what information they have shared with the state. Mr Murdoch added that we do need to build trust in the systems in order to build understanding of what will be done to rectify the situation when systems go wrong. He stated that both the industry and other stakeholders have a lot of work to do in that regard.

A representative of Deloitte asked about the single identity token, noting that it requires registration. She indicated that processes and the infrastructure vary from airport to airport and suggested that the lack of standardisation and security rules needs to be addressed.

Mr Fernandez indicated that someone needs to verify identity and thus enrolment is always needed. While security rules may differ, he noted – by way of example, the US issued an emergency amendment that applies to all airports sending passengers their way recently – he pointed out the fact that the information that airlines collect is the same independently of where a passenger flies and thus harmonisation of passenger processes is possible. He noted that the single token pilot is being carried out in 4-5 airports currently.

Closing remarks by: **Stephan Brandes**

Mr Brandes took the floor on behalf of Krum Garkov. He expressed his hope that participants enjoyed the two days and would take home as much as he would. He concluded by saying that on the previous day, participants learned that business should be the driver for change although it has to adapt to changing environments. On the second day, he said, we learned that there is a lot of technology available for future projects, and that there are many cases where the industry and the government are not aligned, such that there is still a lot of room for further conferences. He closed the conference by wishing everyone safe travel and expressing a hope that he would see everyone at the next conference. He also thanked the panellists, the organisers and the participants.

The 2017 eu-LISA annual conference was the fourth of its kind and our largest to date. Over the course of two days, close to 180 participants took part in the event. Having the support of the Estonian Presidency of the Council of the EU made this event special and, since both strive for "a safe and secure Europe", it generated valuable outcome.

This gathering was an important forum in which responses to challenges such as irregular migration, cross-border crime and terrorism were addressed and approaches to advancement considered. Examining IT-based solutions that can enhance Europe's internal security is paramount more than ever.

Keynote speeches outlined thoughts on how IT solutions contribute to a safe and secure Europe and panel debates explored future perspectives on the digital transformation of the work of law enforcement, border and migration authorities.

Discussions on interoperability in both justice and internal security fields were particularly timely and significant, especially those based on the outcomes of the European Commission's High Level Expert Group on Information Systems and Interoperability. Interactive exchanges on day 2 drew upon audience expertise to bring innovative thinking to plans for advancement in the use of mobile devices and the possible application of analytics in an interoperable systems environment.

Enjoy this report, enjoy "Going Digital for a Safe and Secure Europe"!

Publications Office

Catalogue number: EL-06-17-127-EN-N
ISBN 978-92-95208-62-9

@EU2017EE
@EULISA_agency

/EU2017EE
/agencyeulisa