On behalf of EEMA I would like to thank everyone who participated in our series of seven Annual Conference webinars. Recordings of the sessions including updates on the GLASS and LOCARD projects are available now on our Vimeo channel.

The team is now busy looking ahead to ISSE 2021 in November, as well as planning our programme of popular High-Level Fireside briefings. If you have a topic that you would like to debate with our world-class experts, whether it is the proposed digital wallets (more on that in this Communique from Mark King), the progress of eIDAS 2.0, or more discussion around issues relating to self-sovereign identity, then we want to hear from you: info@eema.org

Early on in the pandemic governments and businesses began to have conversations about the how technology such as Covid-19 passports, certificates and credentials, could be used to get the world moving again when the time was right. During this time the narrative was concentrated on returning to 'normal'. However, now there appears to be a shift focus to how freedoms can be returned and privacy protected (to a greater or lesser extent depending on the country), whilst recognising Covid-19 isn't necessarily going away for the foreseeable future and the need to keep people safe.

Professor Bart Preenel of KU Leuven and a member of the EEMA Board of Management, pointed to technology such as contact tracing that has been successful during the pandemic, in helping to reduce the spread of infection, whilst also protecting peoples privacy. Noting that some countries...
Signicat has acquired Spanish Electronic IDentification (eID), a digital identity pioneer that brought to the market asynchronous video identification.

were less concerned about privacy. Bart also highlighted the EU’s rapid progress on vaccination ‘green’ certificates with preparations beginning in December 2020 and the system going live at the start of July 2021.

Andy Tobin from Evernym, talked about how self-sovereign identity is being embraced by aviation industry to support the resumption of international air travel. He explained how the IATA Travel Pass has been developed to enable passengers to demonstrate that they meet the entry requirements (including Covid-19 related details) of their intended destination. Building on the work done by the EU, IATA will be able scan the new ‘green’ certificates and convert them into digital credentials, after matching it with passport data. In doing so this will allow some of the real benefits of digital credentials to be used for ‘green’ certificates. These include selective disclosure, strong identity binding with a passport, the ability to share elements and combine data/attributes from different providers in different ways, but always verified for authenticity.

Viky Manaila of Intesi Group argued that digital health passes could help restore a path for domestic and international travel, highlighting that the airline industry has lost $118.5 billion USD and 61.6 million jobs lost in the travel and tourism sector as a result of the pandemic. Viky introduced the Good Health Pass, which was launched earlier this year, as an initiative to bring together the technology, health and travel sectors, in order to create a blueprint for digital interoperable health passes.

Viky also referred to the game changing importance of the creation of a pan-European digital identity framework and eIDAS 2.0 proposal of an EU eID wallet capable of integrating credentials (which could include vaccination status) from public and private providers, to enable greater freedoms without the loss of privacy.
European Commission Digital Identity Wallets

Last month the EEMA Communique featured a story about the European Commission proposal for a digital identity wallet. We invited EEMA members to share their views and Speaker Panel member, Mark King has offered his insight.

The EU proposal cover note is a remarkably candid summary of the failure of eIDAS to deliver what was expected. The eIDAS regulation was based on the idea that the earlier Directive had not worked, and the answer was more European integration. Both had been presented as technology neutral, inventing new words and phrases to avoid the impression that it was excluding anything. Ironically, both technology and the services moved on.

There is, however, a real danger of trying to do the right things for the wrong reasons (or at least wrong open justifications): the 1990’s worry about whether anyone would trust a new open internet have been replaced with rampant fraud as a result of too much trust, yet the old canard that assurance will increase trust is trotted out, despite the evidence being strongly for the importance of branding. Likewise, the enthusiasm for fine-grain user control continues unabated, despite it being completely unused for the telephone preference service and spawning the barrage of cookie-warnings that are irritating and pointless, if the data protection principles are observed. The focus on the users completely ignores the fact that it is almost always not the users who want to provide the information but the relying parties who are obliged to check it.

The absence of the UK clearly simplifies the imposition of having a population register upon which to build, as well as a reminder that interoperability with foreigners who might be visitors, customers, or investors must be considered. There is, at least, a proposal for European Commission determinations, but the Schrems saga should raise a flag about that. At the simplest level, how do those of us not born (or not educated) in EU countries get our previous documentation incorporated?

There seems to be divergent images of what a wallet would be and a simplistic model for the liability issues for private sector provision in open systems, notably where the transactions are governed by statute rather than contract law. There are similarities with cash: the governments print it, but it’s held in a wallet of the person’s choice. Sometimes it’s handled by third parties, e.g. banks, as they can use it to get a return. What is the business model for the brokers, data-bankers, or orchestrators beyond plugging the current gaps in state provision?

There are also differences, since data can be copied, not just moved. It would be sufficient for the government to concentrate on what they need to do, namely provide authoritative source data and repair mechanisms for mistakes. Very low-tech solutions (such as printed master lists) will often suffice for validation. Any suggestion that relying parties (including courts) should be part of any framework is absurd: anyone can read a printed document and choose to take note of the content; there is no reason to add complexity.

There has been some recent robust academic scrutiny of decentralised digital identity by the Oxford Internet Institute.

DIARY DATE: Information Security Solutions Europe (ISSE) 2021 Conference - 16th – 18th November 2021