On behalf of the EEMA team I thank our many members and supporters, throughout Europe and beyond, for making 2019 a milestone year. Whether you have worked with us to advance the FutureTrust and LIGHTest projects, kick-off our the new LOCARD and DE4A initiatives, attended or presented at our Annual Conference and ISSE, or joined the debate at one of our High Level Fireside Briefings, every contribution has been greatly appreciated.

We look forward to supporting your work and collaborating with you in 2020.

Self-sovereign identity

Do we know the destination? Do we know the journey to take? And, do we all want to get there? EEMA’s final High Level Fireside Briefing of 2019 proved that there is still a fierce debate as to whether giving citizens the ability to administer and manage their own identities (self-sovereign) is a prudent idea. Posing the initial question ‘Can we every migrate easily?’ the focus soon shifted from the technological implications to more philosophical and societal concerns.

“It is evident that if consensus is to be reached, more discussion and debate between the influencers and enablers who joined EEMA in London in November is required. We will continue to provide an open forum for these important high level conversations to continue.”
Privacy is becoming an upfront consumer proposition

In a new vlog recorded at ISSE 2019 in Brussels, the renowned author, advisor and commentator on digital financial services, and member of the EEMA Board of Management, Dave Birch, shared his view on the most exciting developments in the world of identity right now. You can watch the video at: https://www.youtube.com/watch?v=TKdtrNytQoE

Your predictions for the coming year

**Personal data enforcement and breaches**

In 2020, personal data enforcement actions will become more common and no organisation will be out of scope of such action: the bigs and the smalls must ensure compliance with data protection laws.

Personal data breaches will represent a very important risk for all organisation, each should be ready to prevent, detect and react to such breaches; this means that in addition to information security measures, processes and procedures must be in place and tested to ensure that breaches are properly identified, assessed and reported when necessary.

Finally, the ePrivacy Regulation, replacing the directive, should be voted, so compliance work and budget will need to be foreseen.

Laurie-Anne Bourdain, Risk Officer at Isabel Group

**Even bigger data breaches**

Pretty much every organisation breached to date has been a soft target by virtue of fragile management. So my top prediction is that we’re in for even bigger data breaches with more far reaching consequences, and that with luck the back blast of these might at last cause us to rethink the dominant emphasis on ‘anti-hacking’ in favour of resilience grounded in better process and systems management, particularly at nation state level.

Michael D. Barwise, Managing Director, Business Information Risk Management Consulting

**Privacy coming to the fore**

My prediction is that, largely driven by Apple, privacy will become part of the upfront customer proposition for services in a way that it has not been in the past.

David G.W. Birch, Author, advisor and commentator on digital financial services

**Crypto currency regulation**

After the initial virtual currency hype, central banks will get their act together and finally start regulating such currencies. Hopefully before it’s too late. They will need a solid plan to stop FB’s Libra. Such a plan would require global coordination, hence unfortunately it’s unlikely that will happen.

Understanding of cryptology and how to apply it will become a standard part in the quest for ICT talent in most large corporations and the public sector alike.
Trustworthiness of ICT solutions will continue to be shaken by examples of how systems fail.
Marc Sel, Director, Trust Warp

Sharing digital evidence
Police services across the globe are seeing an exponential rise in the volume and variety of digital evidence, due to the availability of smartphones and other technologies. This presents both challenges and opportunities. Law enforcement agencies will develop capabilities to collect, analyse and share digital evidence at scale.
Investigators will have the ability to automate investigations, for example by extracting relevant video footage of a crime from high volumes of material. They will also be able to share digital evidence securely and electronically with prosecutors and other judicial partners.
Paul Kennedy, Strategic – Law Enforcement & Security Presenter

Age verification in the UK
I predict that the UK government will finally introduce Age Verification in 2020, after delaying it several times during 2019. I also predict that W3C Verifiable Credentials will be a major component of one of the BBFC certified solutions.
David Chadwick, Managing Director, Verifiable Credentials Ltd

Cyber security insurance
1. Cyber security* insurances will emerge in the near future.
2. A large scale physical disaster happens due to badly secured IOT access or hacked process controls.
3. SSI is becoming a preferred solution but it will take years to become mainstream.
Jacoba Sieders, Head of IAM, European Investment Bank (EIB)

Increasing electronic identities on mobile devices
In 2020, a further increase of electronic identities, especially on mobile devices is expected. Driven by several standardization efforts (i.e. the eIDAS regulation in Europe, ISO mobile driver license) more and more use cases in the area of eGovernment and eHealth will be introduced to the public.
Furthermore, big players for mobile handset operating systems, like Apple and Google, opened up their ecosystems for various identity solutions. Therefore, in the near future, a rise in commercial identity solutions is expected.
Tim Ohlendorf, Security Researcher & PhD candidate, Fraunhofer AISEC

Crypto agility
Organisations are in the process of migrating workloads to diverse cloud platforms. They are increasingly concerned with the security of their sensitive data assets. Data at rest encryption is provided natively by cloud service providers. However, the major challenge will be to make organisations understand that managing today’s and tomorrow’s crypto (crypto agility) will require governance and processes on top of technology to manage data risk and prepare for the future.
Christiane Peters, Senior Security Architect, Global Lead Cryptography Services, IBM
Security of IoT

The digitalization of the environment that we live in day to day is going faster and faster. Not only in the way that we communicate with our banks, government and other kind of companies but also with our car, coffee machine, the Internet of Things (IOT). Most of the IOT is designed and build for our convenience, not to keep us secure. And because the early adaptors of the digitalization are becoming more and more secure and harder to break, criminals will aim their arrows on the IOT. So we need to put a lot of effort in the security of IOT, starting in the next year.

Peter Cozijnsen, Business/Security Consultant, CGI

Increasing need for security focus

- Increasing need for, and focus on, investment in OT / Industrial Control System security.
- Increased exploitation of IoT devices, which need to be better protected and managed.
- Continuing need for, and focus on, cloud security and a distributed network perimeter.
- Industry alliances evolving and increased co-operation against common threats from cyber attack

Dr Andrew Hutchison, CyberSecurity Specialist, T-Systems Schweiz AG

2019 a year in pictures
2019 a year in pictures