TDL | Trust in Digital Life

Trust in Digital Life Annual Report 2017

Contents

Chairman's Report

Amardeo Sarma
General Manager
Security and Networking Research Division, NEC Laboratories Europe

TDL's view on research and innovation priorities is driven by an observed erosion of trust, caused by both opportunistic and organized cybercrime with increasing impact and frequency, as well as privacy threats to citizens and society with numerous incidents and breaches of trust and privacy even by governments. This leads to an increased awareness of security and privacy topics, as re ected, for instance, in European initiatives for directives targeting security and privacy, while, paradoxically, the online behaviour of people is less risk-aware than the physical world. (From TDL's recommendations to the NIS platform)

Photo credit: Evelin Frerk

We are becoming increasingly dependent on the digital world. Today, every aspect of our personal, professional and civic lives is undergoing a digital transformation. It is a world of attractive and easy-to-use devices and services that many users - even in professional environments - do not fully understand. Unlike the service providers, curiosity hackers and cybercriminals who have the edge over the ordinary citizen at home or in the office.

The unforeseen and potentially grave consequences of a data or system breach also undermine confidence and enthusiasm for taking up opportunities in the online world and threatening the layers of business trust built up over centuries in the physical world. The situation demands action to establish – or restore – the trust and trustworthiness that are vital to fulfilling Europe's ambition for a digital society and a single digital market that protects the rights of its citizens.

In the meantime, new directives are coming into effect, of which GDPR and PSD2 are but two examples, providing both new challenges for existing businesses and citizens to adjust to, as well as a new range of opportunities.

Over the last year, we have entirely re-written and re-cast the Strategic Research Agenda as TDL's Work Programme. This new document represents the goals and ambitions of the association, and, based on its insights and experience, describes the drivers and motivations behind an ambitious research agenda for the coming two-three years.

Our work programme reflects the changes in the environment and addresses new developments in technology and regulation. We continue to evolve the working group on blockchain and leverage the high degree of multi-disciplinary interest in this technology. We have started two new working groups. One addresses personal data and looks at the impact of upcoming EU regulation for both businesses and consumers. The other addresses security issues in light of the proliferation of Internet-enabled objects large and small. We have re-launched our Sprint initiative by opening it up to non-members of TDL.

Our events demonstrate that, despite our intellectual aspirations, we are still human and that, at least in this generation, trust in the digital life goes hand in hand with establishing trust in the non-digital world.

As an association whose goal is to make the digital world more human, there is much work to be done: I am excited about the challenge and hope you are too..

TDL Work Programme 2017-18

The target audience for TDL's Work Programme includes anyone who wishes to better understand the association's objectives and motivations. This may include current and prospective TDL members as well as national and international government agencies and standards bodies, which may find that TDL's work resonates with their own efforts to improve trust in digital life for both society and business. This document offers guidance on TDL's direction of research and on when and how to deploy its research results.

This document lays out the roadmap for TDL for the foreseeable future in the context of the ongoing changes, trends, and developments occurring in information technology, business management, and legislation, primarily (but not exclusively) in Europe. TDL is committed to improving awareness of these developments from different perspectives and to creating building blocks based on open platforms and standards that others can leverage to promulgate trustworthy computing.

The TDL community's unifying principle is that trust and trustworthy services are essential for the success of the digital economy. As a community of industrialists, entrepreneurs, and academics, TDL's objective is to provide the tools and awareness to benefit the wider community in their daily digital lives. Therefore, TDL is committed to enabling a trustworthy ecosystem that both protects the rights of citizens – who deserve the best possible products and services – and creates opportunities for businesses to develop new and protective devices, applications, and services, provided at an affordable price. To this end, TDL researches, pilots, and incubates trustworthy ICT services and technologies in an innovative environment through collaborative activities. The research and business agenda of the European Union is also a major focus for TDL.

Trust has been an essential component of all successful societies throughout human history. However, our changing understanding of trust has not kept pace with our speed of movement into the digital world; the inherent lack of physical contact and added complexity create new impediments. From banking to healthcare, driverless cars to online shopping, every aspect of our twenty-first century digital world is dependent on varying degrees of trust between consumers and suppliers, governments and citizens. The continuing threat of cyber attacks is undermining the confidence we need to take full advantage of the opportunities available to grow the digital economy. A trusted ecosystem based on innovative and trustworthy ICT products and solutions will protect the data and assets of European citizens and enterprises.

The challenges for research and innovation

Trust is an essential component of digital life. Both consumers and businesses need to be able to trust that the technologies, products, and services they rely on are protected against purposeful or accidental misuse. New challenges are constantly being created by:

- the spread of new technologies such as cloud computing and blockchain
- BYOD (bring your own device), and crypto-currencies;
- the passage of new legislation such as eIDAS, PSD2, the cyber security directive, and data protection reform;
- the rising value of digital assets and the damage breaches can cause;
- the rising sophistication of cyber attacks.

Industry Trends

Accelerating digital transformation is bringing wholesale changes in business and IT models to all enterprises, whether industrial, governmental, or academic. Key industry trends include the disappearing enterprise perimeter, the move to cloud computing, bring your own device (BYOD, now extending to identity/network/key), and new regulations on data protection and privacy.

Cloud computing has numerous financial, operational, and resource benefits, yet it moves, rather than removes, concerns about security, data loss, and breaches of confidentiality. BYOD creates issues with respect to controlling access to enterprise assets from non-IT managed resources, and raises questions about how to protect the privacy and security of the company data that is stored on or transits through such devices – or the personal data that can just as easily be compromised.

In an environment which is increasingly less tolerant of data breaches, the threats of reputational damage and the loss of customers' and partners' trust are as potent as that of regulatory action.

In order to build trust – and to mitigate its erosion over time – the providers of infrastructures, platforms, applications and services must consistently demonstrate their trustworthiness to both themselves and their customers.

Advancing Technology

New technologies are constantly becoming mainstream: big data, internet-enabled objects, sophisticated analytical tools, machine learning algorithms, and blockchain. All present new opportunities and new challenges. Distributed ledger technology in particular offers great potential to meet the business challenges of a range of vertical sectors while maintaining the technical criteria necessary for security, privacy, redundancy, and resilience. Interest in this technology, principally but not exclusively the blockchain, has taken the business world by storm, particularly the financial community. Despite valid concerns about performance and privacy and the inevitable hype, there are many signs that in the blockchain industry leaders have found a technology that they can agree presents a significant infrastructure building block for the future.

Legislation & Regulation

The EU legislation coming into force in the next two years covers diverse but interconnected areas such as identity, trust services, privacy, data protection, payment services, cybersecurity, and anti-money laundering. The new laws and regulations are already profoundly changing the way organisations in every sector are approaching the way they manage data and data assets.

The new regulations bring considerable benefits to consumers. GDPR requires most companies to undergo a cultural shift in order to maintain, or in many cases establish, consumer trust with respect to the way in which their personal is managed and stored. Besides creating a lot of additional work for enterprises both large and small, the new regulatory regime will impose a significant strain on the authorities, who are responsible for both creating awareness of these new responsibilities and monitoring and policing them once they have passed into national law in every EU Member State.

If you would like to review TDL's Work Programme in full, it can be downloaded from the association's website **trustindigitallife.eu/publications**

Working Group: Blockchain

A blockchain is a distributed database that maintains a continuously-growing list of data records hardened against tampering and revision. It consists of data structure blocks—which hold exclusively data in initial blockchain implementations, and both data and programs in some of the more recent implementations—with each block holding batches of individual transactions and the results of any blockchain executables. Each block contains a timestamp and information linking it to a previous block.

The emergence and success of Bitcoin propelled blockchain technologies into prominence. Since then, financial institutions have explored the potential of Bitcoin-like systems; the Open Source community has delved into the Open Source implementations, and the research community has worked on developing and optimizing associated cryptographic protocols, improving architectural solutions, and understanding the economics of systems like Bitcoin. Governments have started looking at the regulatory space for distributed financial systems and requirements for integrity; civil society organizations have looked into privacy support in blockchain systems, and law enforcement agencies have examined the new potential for financial crime. As work on exploring all the potential diverse uses of blockchain technology has expanded, applications for e-government, storage, document notarization, identity protection, real estate, and enterprise have emerged.

At the Paris working group meeting in September 2015, Intel took the initiative to lead a working group on blockchain with an initial focus on crypto-currencies but broadening out the discussion to be multi-disciplinary. Since then the group has expanded and attracted other TDL members as well as a number of high profile non-members as participants.

If you would like to get involved in TDL's Blockchain Working Group or start a new working group initiative within the scope of TDL's activities, contact **office@trustindigitallife.eu**

"

TDL provides a unique opportunity to, as a collective, work towards addressing the modern challenge of trust in the internet, not only for large corporate institutions, but increasingly critical for the SMEs and innovators that are powering the digital world we live in today.

—

James Varga, The ID Company

Blockchain: Perspective on Research, Technology, & Policy

Blockchain technology has captured the imagination of technologists, investors, and policy makers. Thrown into prominence by the success of Bitcoin, it has created interest in other applications that could be decentralized as well as new security models that have been discussed for decades, but mostly as theoretical possibilities. The number of research papers associated with Bitcoin and blockchain skyrocketed, and a number of startups, in the US and elsewhere, appeared. Open Source activities associated with blockchain approaches have become more prominent and now boast the participation of technology giants such as Cisco, IBM, and Intel.

Governments have conducted studies of crypto-currencies and blockchain applications. The UK, US and other nations published reports evaluating technology and regulatory issues in blockchain areas. The first regulation associated with crypto-currencies appeared. At the same time, the first non-financial services based on blockchain made their appearance, with the first implementations in Estonia and experiments in Gulf states.

We consider blockchain an important technology direction that requires extensive research. This paper will put this technology in perspective with regard to technical and regulatory priorities in a number of application areas, not limited to finance. We hope the paper when completed will be used by technology and regulatory communities as an instrument of building understanding and improving prioritization of topics.

The paper will also serve as the foundation for future work, highlighting areas that were identified as potential research and policy priorities in the course of the initial discussions at the formation of the TDL Blockchain Working Group.

A paper written and co-ordinated by members of the Blockchain Working Group and available from ***trustindigitallife.eu/publications****.*

Multiple Views on Blockchain: Technology, Use Cases, Economics, and Policies

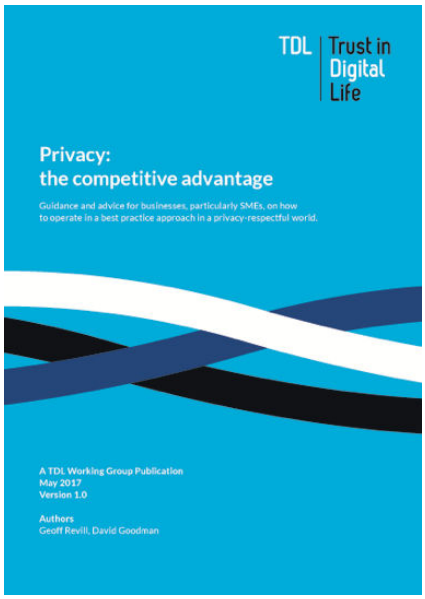
Besides the extensive, in depth report, the working group co-ordinated a one day conference, in partnership with The Hague Security Delta and the Institute for Financial Crime (IFFC), and sponsored by Intel, miiCard and NEC, on 17 June in The Hague. The objective was to bring together researchers, practitioners and regulators engaged in crypto-currency and blockchain activities in order to initiate a multi-disciplinary community of blockchain research and practice.

The high profile set of speakers included:

- **Marietje Schaake**, Member of the European Parliament
- **Professor Srdjan Capkun**, ETH Zürich
- **Jason Albert**, Assistant General Counsel, Microsoft
- **Robert Reinder Nederhoed**, CEO, Bitmymoney
- **Professor Michael Huth**, Imperial College London

> *TDL enables fruitful discussions with stakeholders from real life and industry partners interested in a wide area of trust and security services.*
>
> —
>
> **Prof. Dr. Kai Rannenberg,** Goethe University

Working Group: Personal Data



In recent years, the exploitation of personal data has prompted disruption, initiated digital transformations, increased competition, and raised unprecedented awareness of security, privacy, and identity issues. The market is changing quickly and the regulators are working hard to catch up. The responsibilities of companies and service providers are becoming more explicit. A more balanced approach to managing personal data is required, but providing it presents challenges. Assigning responsibility is a particular issue, especially given new and expanded EU legislation, including the General Data Protection Regulation (GDPR), the ePrivacy Regulation, the Electronic Identification and Trust Services regulation (eIDAS), Anti-Money Laundering 4 (AMLD4), and the Payment Services Directive 2 (PSD2).

The introduction of GDPR in May 2018 will have a significant impact on all companies, including many outside Europe that are involved in processing EU citizens' personal data. GDPR will harmonise data protection law across EU member states, strengthen the rights of citizens, require breach notification, and grant supervisory authorities more powers to impose substantial fines for non-compliance. NIS will close the gap between personal data breaches and other security incidents so that breaches must be reported to regulators even where personal data is not exposed.

If you would like to get involved in TDL's Personal Data Working Group or start a new working group initiative within the scope of TDL's activities, contact **office@trustindigitallife.eu**

Privacy: The Competitive Advantage

New obligations also present new opportunities for businesses, especially given new data sources and new ways to improve and re-invent the trustworthiness of technologies, systems, and processes. This is especially the case with financial technology (Fintech), PSD2, and improvements to data portability and mobility, self-sovereign identity, and access to global services. Similarly, eIDAS presents great opportunities to streamline identity verification and support the legally-binding use of e-Signatures.

These EU legislative changes have further heightened the need to focus on the management and protection of personal data, especially in traditionally regulated contexts but also beyond. These topics are inextricably linked and affect both consumers and businesses alike, as recent court cases hinging on the "right to be forgotten", data mobility, and privacy have shown.

Despite efforts to spread the word by lawyers, consultants, and journalists, as well as researchers, specialist vendors and service providers, remarkably few companies are taking steps to prepare, especially for GDPR. Most very large companies have access to the help they need from their own Chief Privacy Office or Data Protection Officer as well as external advisors. However, SMEs lack these advantages, and may remain unaware of the changes and their consequences until it is too late.

A paper written and co-ordinated by members of the Personal Data Working Group and available from ***trustindigitallife.eu/publications****.*

GDPR Compliance

The work in this area consists of three complementary analyses of how the GDPR interacts and co-exists with other identity- and privacy-related EC regulations:

- PSD2: there are contrasting ways of looking at the impact of implementing PSD2 and the potential challenges in the context of GDPR. On the one hand, it demands more transparency in financial transactions, whereas PSD2 is primarily about opening up authentication data, the value of which to consumers could be limited by GDPR.

- eIDAS trust services: the risk with offline signatures is that the signatory is judge and party: it cannot validly certify the probative value of its dematerialized transaction to each counter-party. There is a lack of exhaustive traceability and impartiality in this kind of unilateral transaction whereas eIDAS opens up the market for multi-lateral eSignatures.

- PECR: The ePrivacy Directive formerly contained a complex blend of three approaches, service-, data- and value-centric in the context of electronic communication privacy rules whereas the current regulation is more tightly aligned with GDPR than ever before and it is questionable whether that is enough to avoid overlap or redundancy.

Working Group: Securing Internet-Connected Devices

Three issues need to be urgently addressed. One is making a new generation of devices inherently more secure against attacks even if they are physically accessible. Another is ensuring that, even if they are designed better, devices' properties may not be used for cyber attacks. The third is dealing with a potentially very large number of legacy devices - that is, implementing some form of access control to ensure that communicating and participating in larger actions cannot take place until the devices can be verified as trustworthy.

The number of devices connected to the Internet is expected to reach approximately 30 billion by 2020, creating a market worth $1.7 trillion globally. The consequence of having so many devices, most of which are designed with minimal protection, is already apparent. Attackers have used poorly secured devices like routers, baby monitors, and digital video recorders into botnets to attack the wider Internet, or have used vulnerabilities in such devices to permanently disable them. In other cases, connected devices provide the ingress for stealthy, long-term, persistent attacks. As industrial control systems, vehicles, and traffic control systems become connected, the risk of physical-world damage is a major concern.

The method of release-and-patch that worked with desktop software and, to a much lesser extent, mobile phones will not work with the Internet of Things. Consumers will be reluctant to risk patching large, expensive appliances that previously required little maintenance per decade, while patching very small devices will be too expensive for manufacturers to support. Accordingly, the design of the systems that manage these devices will be crucial; they will need to be able to isolate devices that pose a threat.

If you would like to get involved in TDL's Securing Internet-Connected Devices Working Group or start a new working group initiative within the scope of TDL's activities, contact **office@trustindigitallife.eu**

Demonstrator Platform

The objective of this task is to demonstrate the trustworthiness of IOT with a demo that includes testing, verification, certification as well as labelling. It can be broken down into:

(1) Conceptual architecture for levels of trust and monitoring trust to manage our overconfidence in devices
(2) Tools for designing a trustworthy system
(3) Metrics

Insights and recommendations for businesses, governments and citizens

The intention is to provide an overview of the state of play focussing on current cyber attack threats and to identify the items of research necessary to address the above, bearing in mind the direction outlined in the ECSO SRIA and the contents of the H2020 IOT-03-2017 call.

The scope of this activity is to take the perspective of specific use cases, such as 'Blockchain for IOT', not least given the synergy with the Blockchain Working Group, which may be narrowed down further to, for example, smart contracts, identity management or supply chain.

IOT device security: quantification and improvements

This activity consists of two different tasks being undertaken by Technical University Darmstadt:

(1) Security quantification for devices using methods based on computational trust. The task is to split mobile and domestic devices into components and performing a trust and reputation analysis to generate a set of qualitative ratings to demonstrate how good or secure a device is, based on an array of 'sensible' dimensions and criteria. Still to be determined are the most beneficial means of disseminating or utilising the results of the project.
(2) AlterEgo: making mobile devices more trustworthy and controllable representatives of their owners. This task is aimed at determining how to build something good or trustworthy and will seek to produce prototypes to that end.

Future Priorities

TDL uses a variety of enabling concepts and proven instruments to advance and disseminate its vision of trustworthy digital services and platforms, which include working groups, short collaborative projects (known as sprints), and Trust in the Digital World-branded conferences and events. As output from these activities, TDL provides strategic documents, recommendations, and practical demonstrators that are shared with partner organisations such as the European Commission, the European Union Agency for Network and Information Security (ENISA), and the European Cyber Security Organisation (ECSO), as well as the wider community.

In response to the challenges and their impact on business and society, TDL has chosen the following technical and business areas of focus as its work priorities over the coming three to five years.

Cloud Computing

The deployment of cloud services and data offers huge cost savings. The concept of cloud computing is essentially alien to human nature, and it still requires work to establish the next level of trust between the X-as-a-Service providers and their customers. Citizens and SMEs often have little bargaining power with respect to service contracts, and little insight into the security practices of cloud service providers. The real and perceived loss of control as well as the possibility of data breaches and loss of access are major deterrents to adoption. Everyone's own portion of the cloud – whether services, functions, or data – is not yet as secure and reliable as if it were local and isolated. Providing such assurance continues to be a major challenge, both technical and psychological, and may apply even more to businesses than to citizens.

TDL's primary research interest is in the technical aspects of achieving these properties of trustworthiness. As many of the underlying technologies are already available, TDL will firstly address how they are used. This approach will need to be complemented by educational and policy measures.

Big Data

From a TDL research perspective, bringing together big data on the one hand and adequate security, data protection, and privacy measures on the other to increase trust and confidence is a formidable task for the future. TDL's overall objective is to team or liaise with the Big Data Value PPP and focus on contributing specific research contribution which would be beneficial to the PPP. The twin goals of understanding and obscuring the data are diametrically opposed, and there is no simple answer. Encrypting the data, for example, will not be enough by itself. Reconciling these conflicting requirements presents a considerable challenge. This will also need to be addressed from the legal and regulatory point of view.

5G

5G brings new concepts and challenges to security, such as:

- Preventing unauthorized access to assets due to the heterogeneous nature of 5G with different ownership of different parts of the infrastructure
- Isolating the "slices" of the network assigned to different network operators and providers
- Accommodating different levels of security and encryption especially when combined with the Internet of Things as well as different requirements on security and privacy by different verticals, such as health and transportation
- Management of trust given the complexity of the infrastructure.
- Dealing with liability in a multi-tenant environment where the infrastructure may again be operated by different stakeholders.

TDL intends to address security-related research and deployment questions that will accompany the development and rollout of 5G. The target is to achieve a level of trustworthiness in line with the high expectations and dependencies associated with this new technology. To achieve this overarching goal, TDL plans to team or liaise with the 5G-PPP and more specifically 5G-PPP projects and/or working groups deeply active in 5G security.

Risk Management

When suppliers claim that products and services are trustworthy, they must be able to prove it in a way that users and consumers can see and understand for themselves, as evidenced, for example, in a certificate. Trustworthiness is not only about the security risks and the quality of programming, but also who controls and manipulates and ensures that systems are transparent, auditable and redress can be obtained.

The research challenge for TDL is to identify the strengths and weaknesses of each technique and the most meaningful combination for each given context (market, technology, application, users, regulations and others). In each case, the combination must be feasible to implement and meaningful to consumers.

Next Generation Sprints

One of TDL's key objectives is the operational implementation of an industry-driven ecosystem stimulating the development, promotion and acceptance of trustworthy ICT to validate technology, interoperability and trustworthiness proofs of concept.

Since its inception, TDL has proudly supported innovative integration technology projects – or sprints – from its SME and academic members in collaboration with industry partners to integrate with a reference platform. In 2017, it is intended to take the concept of trustworthy computing to the next level, bringing participation in the sprints beyond the association to a new audience.

TDL's sprints are short projects that run for one to three months. In the past, they have already shown how innovations can be built on and add value to existing reference platforms. Some were used in European projects, while others used the platform to connect their research output or product to a wider set of users.

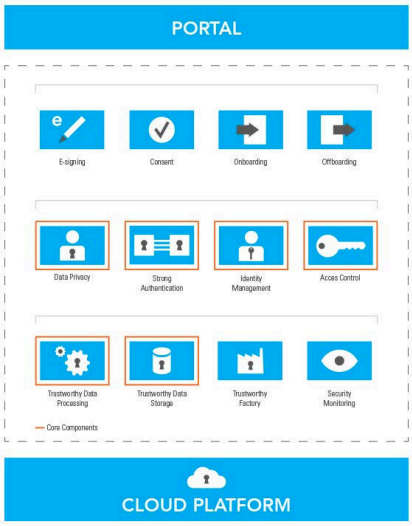
So far, the sprints have mostly used Microsoft's Azure and Azure Active Directory. The use of an agreed set of standard and quasi-standard interfaces and APIs make it possible to transfer the results of the sprints to any other platform. Hence, participants can use Microsoft's platform while at the same time ensuring that there is no vendor lock-in.

To date, TDL has restricted participation to its members. TDL now intends to extend the next generation of sprints to a community of platform enhancers, once the rules are defined, and alternative options that will include other platforms. These sprints will not be used to develop technology, such as in EC-funded projects, but to validate already developed technology in a broader context.

Next generation TDL sprints will engage two sets of actors: the producers of technology that plug into the platform and the consumers that benefit from the added value provided.

> *Such has been the success and interest in previous Sprints, we believe that now is the right time for us to welcome broader involvement, in order to give opportunity to some of the brightest and most innovative people and ideas*
>
> —
>
> **Amardeo Sarma,** NEC Labs

Evaluating Trustworthy Software



The TDL-developed Generic Trust Architecture (GTAC) defines a set of requirements and functionalities for a set of building blocks and core components, including mobile service and platform integrity, trusted stack and data life cycle management.

The GTAC was developed under the EC-funded 'Achieving the Trust Paradigm Shift' project (ATTPS).

The new download capability on the TDL website provides a service whereby software developers can offer, use and validate trustworthy software components. TDL members and approved authenticated users have the possibility to evaluate the technology that is offered and provide feedback to the element provider.

The overall intention is to deliver trustworthy software components and services available for experimentation. The TDL-developed Generic Trust Architecture defines a set of requirements and functionalities for a set of building blocks and core components, including mobile service and platform integrity, trusted stack and data life cycle management.

The requirements for element publishers to deploy trust elements for download are the provision of a standalone service element, first level support, and optional online questionnaires to be filled in by the users to gain insights. Each element is evaluated by a TDL committee for final deployment approval.

The provision of this facility is for software developers and providers to test and experiment modules, services and concepts on four different dimensions that interact with each other:

- **Technology:** parties invited to deploy their applications in a regulated and trusted environment receive feedback on different aspects of functionality.
- **Legal:** developers identify bottlenecks hampering adoption in a generic fashion in order improve their usability in trustworthy ICT solutions.
- **Business:** developers receive more insights to support their investment decisions and receiving valuable feedback on user requirements,
- **Standards:** validation of the overall technology, concepts and generic architecture to provide input for standardisation bodies on a European level

Further information about how to submit and download trustworthy components will be available on the TDL website from September 2017.

Multiple Views on Blockchain: Technology, Use Cases, Economics, and Policies

In partnership with **The Hague Security Delta** and the **Institute for Financial Crime (IFFC)**, and sponsored by **Intel**, **miiCard** and **NEC**

—

17 June 2016, The Hague

The Blockchain Working Group co-ordinated a one-day conference, in partnership with The Hague Security Delta and the Institute for Financial Crime (IFFC), with sponsorship from Intel, miiCard and NEC,

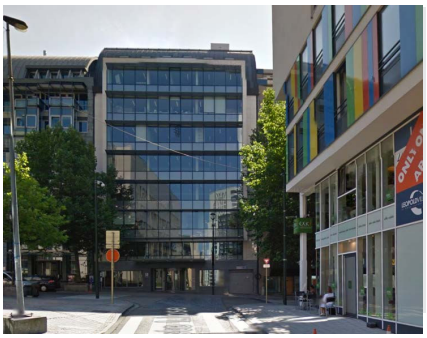
The goal of the event was to examine the opportunities and challenges associated with blockchain from different perspectives in order to create a multi-faceted picture of the field. By taking multiple views on blockchain, the event aimed at providing a forum to discuss technology, use cases, economics and policies bringing together researchers, practitioners and regulators engaged in blockchain and crypto-currency activities. Hence, the longer term objective is to create a multi-disciplinary community focussed on blockchain research and practice.

The high profile set of speakers included:

- **Marietje Schaake**, Member of the European Parliament
- **Srdjan Capkun**, Professor, ETH Zürich
- **Jason Albert**, Assistant General Counsel, Microsoft
- **Robert Reinder Nederhoed**, CEO, Bitmymoney
- **Michael Huth**, Professor, Imperial College London

*A conference report and speaker presentations are available from **trustindigitallife.eu/past-events**.*

The Blockchain Era - From Research to Innovation



Hosted by **Press Club Brussels** and in collaboration with **New Europe**

—

6 June 2017, Brussels

The second annual Blockchain Working Group event was co-ordinated with New Europe and hosted at the Press Club Brussels with support from the Association of European Journalists.

Featuring speakers from government, industry and academia, this one-day workshop in collaboration with New Europe explored how all parties are working together towards a common aim. While researchers investigate the technology itself, entrepreneurs are exploring the opportunities to develop new applications.

Among the key speakers were:

- **Bart Preneel,** Professor, KU Leuven
- **Eva Kaili**, Member of the European Parliament
- **Daichi Iwata,** Head of Fintech, NEC Corporation
- **Jean-Jacques Quisqater,** Professor, UC Louvain
- **Hervé De Halleux,** Associate Partner EU Institutions, GBS, IBM
- **Joshua Kroeker,** Senior Product Manager, HSBC Global Trade and Receivables Finance
- **Benoît Abeloos,** Policy Officer – Startups and Innovation, DG CONNECT
- **Lenard Koschwitz,** Director Public Affairs, Allied for Startups

The day was structured into four distinct but interconnected areas:

Assessing the Viability of Blockchain Applications	Financial applications generated the early excitement around blockchain which has now spread to many other sectors
Priorities for Research	Although research has been ongoing for years, areas such as scalability and security still require rigorous scrutiny by the research community
Supporting Public Policy Priorities	Policy makers are striving to support innovation while at the same time seeking to use blockchain to meet civic priorities such as efficiency, transparency, accountability, privacy and security
New Ideas, New Scenarios	As entrepreneurs understand the diverse scenarios that blockchain can adapt to, new and unusual business ideas are emerging.

Whose Data Is It Anyway?

In collaboration with The ID Co. and the School of Informatics University of Edinburgh, and sponsored by Head Resourcing.

—

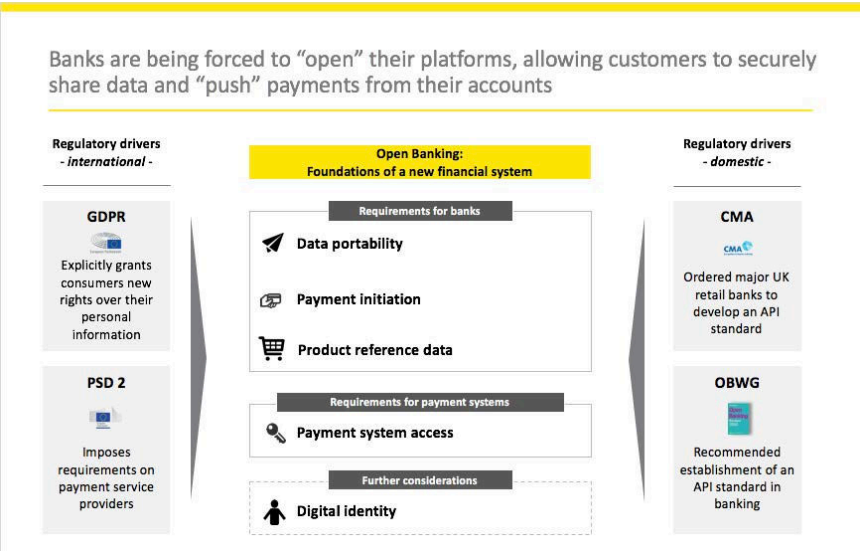
14 December 2017, Edinburgh

The Personal Data Working Group co-ordinated a one-day conference, in partnership with The ID Co. and the School of Informatics University of Edinburgh with sponsorship from Head Resourcing.

In keeping with other TDL events, the conference took a multi-disciplinary approach to the phenomenon that data protection and privacy has become in a very short time. GDPR and Open Banking, aligned with PSD2, are about to radically challenge the way that financial services operate. The objective of the one-day event was to achieve a better understanding of what the world might look like three to five years after the new regulations have been in force from the perspectives of all stakeholders.

The high profile set of speakers included:

- **Stuart Lang,** Financial Services Partner, EY
- **Gavin Littlejohn,** Fintech Stakeholder Group Convenor, UK Open Banking
- **Jörg Hladjk,** Of Counsel, Cybersecurity, Privacy and Data Protection, Jones Day
- **Robin Wilton,** Technical Outreach Director, Internet Society
- **Giles Watkins,** UK Country Leader, International Association of Privacy Professionals
- **David Alexander,** CEO & Platform Architect, Mydex CIC



A conference report and speaker presentations are available from trustindigitallife.eu/past-events.

Working Group Meetings

The highlight of every TDL meeting is the opportunity that it offers to sample the gastronomic delights of the local city or region, which it is the responsibility (and honour) of the host to choose. From Zunfthaus zur Haue in Zurich to the Kulturbrauerei in Heidelberg, this has been another good year for the TDL gourmand.

TDL Working Group meetings are important for members and observers to discuss the content and plans of working groups face-to-face. The objective of the meetings is to define next steps and action points so that content creation can proceed in a structured manner. Each working group is responsible for a number of deliverables and milestones due on certain dates. The working group leaders coordinate the meetings and are responsible for the agenda, charter, plenary presentations and progress reports. All members of the TDL community are invited to working group meetings where they can interact, network, share ideas and visions with the leading organisations in the field of security and trust on ICT, mobile communication and modern technologies. It is customary to invite presentations from keynote speakers who are specialists in research of security and future plans of the core elements of TDL.

IBM Zürich, Rüschlikon

22 September 2016

TDL invited **Dr David Goodman** to give the opening keynote. He is a Principal Consulting Analyst for TechVision Research and has written extensively about the raft of upcoming European regulations. He gave a lively presentation on **New European Privacy and Data Protection Regulations – Compliance or Consequences** and suggested the setting up of a Personal Data working group. Later there was a presentation and review of KU Leuven's sprint project on n-Auth as well as an introduction to the contractual Public-Private Partnership (cPPP) on cybersecurity.

Verizon Enterprise Solutions, Amsterdam

2 Amsterdam 2017

Unusually there were no guest speakers at this meeting which was entirely focused on reviewing the direction being taken by the Blockchain Working Group and to consolidate their plans for the coming year, which included the completion of the document, **Blockchain - Perspectives on Research, Technology & Policy**, as well as planning for another one-day event in June.

It also provided the opportunity to kick off two new working groups - Personal Data and Securing Internet Connected Devices and to discuss at length workplans for both for the coming year.

NEC Laboratories Europe, Heidelberg

23-24 May 2017

There were several guest speakers in Heidelberg. **Dr Huma Shah** from Coventry University introduced a proposal to the Horizon 2020 programme, entitled **Ethical Dimensions in IT**, with an invitation to TDL to participate. **Kumar Sharad** from NEC Europe similarly proposed engagement with another project on **Privacy Friendly, Cloud-Based Security Intelligence**.

Later in the day, **Mathias Kohler** from SAP gave a keynote presentation on **Security and Privacy in the Cloud**. Mathias joined SAP's security research team in 2006 and received his PhD in 2011 from TU Darmstadt. He worked since as a postdoctoral researcher at SAP and is now leading a team of nine security researcher at SAP's security research department in Karlsruhe. His main research topics include applied cryptography as well as anonymisation.

A half-day workshop was held the following day to launch the next generation of sprints, that will open up TDL's initiative to non-members and diversify the supported platforms. Presentations were given by Microsoft, Flightmap and Microsoft describing previous experiences and lessons learnt, as well as a joint sprint proposal by IBM Zürich and Alexandra Institute on an easy deployment model for Privacy-preserving Attribute-Based Authentication as a Service.

"TDL members bring diverse digital security knowledge and experiences and act as one voice to recommend recipes and best practices to deliver the promises of a digital world.

—

Xavier Larduinat, Gemalto

School of Informatics University of Edinburgh

24 October 2017

The meeting discussed the proposals submitted to the EU involving TDL, Science Outside the Classroom for Citizen Education and Recreation (SOCCER) and EU BLockchain OBServatory & Forum: Setting–up and running a European expertise hub on blockchain and distributed ledger technologies (BLOBS). It went on to report on the progress of the deliverables associated with the three working groups as well as to review preparations for the one-day event, Whose Data Is It Anyway?

The meeting heard about the MyData Declaration and the PANORAMIX EU project, introduced by Professor Aggelos Kiayias from the School of Informatics.

There was also an update on the progress of the expansion of the TDL website to incorporate the trustworthy software catalogue from the old GTAC site and the new showcase for Sprints.

The aftenoon saw news on the setting up of TDL Japan and a discussion on strategic plans for 2018 which included a comprehensive redefinition of what TDL does today.

Association Members

Members of the TDL community sign the articles of association and, having accepted its policies and procedures, are expected to participate in working group sessions and have the possibility to apply for a position on the Board of Directors.

Observers are representatives of an organisation who have been invited to participate in working groups and are interested in experiencing the value of the association before deciding whether to join as full members.

European Cybersecurity Organisation (ECSO)

In 2016, TDL joined the newly-formed European Cybersecurity Organisation (ECSO) which will engage with the EC and Member States to achieve the objectives stated as the industry part of the contractual Public-Private Partnership (cPPP) on cybersecurity established y the European Commission to strengthen EU's cybersecurity industry, as envisaged in the Digital Single Market Strategy.

The PPP is intended to stimulate European cybersecurity industry by:

- bringing together industrial and public resources to improve Europe's industrial policy on cybersecurity, focusing on innovation and following a jointly-agreed strategic research and innovation roadmap
- helping build trust among Member States and industrial actors by fostering bottom-up cooperation on research and innovation
- helping stimulate cybersecurity industry by aligning the demand and supply for cybersecurity products and services, and allowing industry to efficiently elicit future requirements from end-users
- leveraging funding from Horizon2020 and maximizing the impact of available industry funds through better coordination and better focus on a few technical priorities
- providing visibility to European research and innovation excellence in cybersecurity and digital privacy

ECSO's objective is to support initiatives and projects that aim to develop, promote and encourage European cybersecurity, as well as to:

- Foster and protect the growth of the Digital Single Market from cyber threats;
- Develop the cybersecurity market in Europe and the growth of a competitive cybersecurity and ICT industry, with an increased market position;
- Develop and implement cybersecurity solutions for the critical steps of trusted supply chains, in sectoral applications where Europe is a leader.

Board of Directors

The Board of Directors is responsible for the overall management of TDL activities and ensures the implementation of the association's objectives and the strategy. Directors are appointed at the General Assembly for a two-year term, for a maximum of two terms (four years), and are assigned well specified duties within the overall scope of the work of the Board of Directors.

The elected TDL Board of Directors for 2016–18 are:

Amardeo Sarma
General Manager, Security and Networking Research Division,
NEC Laboratories Europe

Ronny Bjones
Director, Cloud Identity & Privacy Services, Microsoft

Claire Vishik
Security and Privacy Standards and Policy Manager, Intel

Jan Camenisch
Principal Research Staff Member, IBM Research Zurich

Dr Svetla Nikova
Research Expert, COSIC research group,
Department of Electrical Engineering, KU Leuven

Professor Dr Kai Rannenberg
Deutsche Telekom Chair (formerly T-Mobile Chair) for Mobile
Business and Multilateral Security, Goethe University, Frankfurt

James Varga
Founder and CEO, The ID Co.

Rob Kroneman
Director Identity & Access Management, Verizon Enterprise Solutions

TDL's vision is that trust must become an intrinsic property of any online transaction involving personal information, incorporating legal, business, and technical advances, supporting cyber security policies, and integrating societal considerations so that citizens and end users will recognize trustworthy services, transactions, and data, and be prepared to pay for them. Trustworthy ICT will increase confidence and trust in modern society, bring new and attractive ways of living and working, and further strengthen Europe's democratic and social values.

The association's mission is to provide its members with a European business development platform in order to stimulate development and user acceptance of innovative but practical trustworthy ICT. Guided by its strategic research agenda, TDL acts as an incubator for a portfolio of sprint projects intended to validate new and innovative technology concepts, promotes cross-sector collaboration, and aggregates the results into industry recommendations for policy makers and the European Commission.

trustindigitallife.eu

trustindigitallife.eu

Trust In Digital Life Association
Maurice Dekeyserlaan 11 / avenue Maurice Dekeyser 11
1090 Jette, Brussels
Belgium

office@trustindigitallife.eu
+44 141 588 0892

TDL | Trust in Digital Life