TDL | Trust in Digital Life

Work Programme 2017–18

A TDL Publication
June 2017

Authors
Amardeo Sarma
David Goodman
Wendy M. Grossman

The editors wish to thank the following who have contributed to the discussion on TDL's research agenda and work programme, 2013–2017:

Pasic Aljosa, Harm Jan Arendshorst, Pascal Bisson, Ronny Bjones, Stefan Bumerl, Jacques Bus, Jörg Hladjk, Arthur Leitjens, Volkmar Lotz, Finn Myrstad, Kai Rannenberg, Peter Racsko, Jon Shamah, Neeraj Suri, James Varga, Claire Vishik

Executive Summary

This document outlines Trust in Digital Life's current and future research priorities for 2017–18. From the many developing trends in technology and the challenges they pose, TDL is addressing or planning to address seven areas of focus. Five are technically-oriented: blockchain, the Internet of Things, cloud computing, big data, and 5G whereas two are regulatory and more business-related: personal data and risk management.

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.

1 Introduction

This document lays out the roadmap for the Trust in Digital Life association (TDL) 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 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.

2
Trust In Digital Life: Purpose & Mission

2.1 Purpose & Mission

TDL is a not-for-profit membership association registered in Belgium. Its member organisations are leading companies and knowledge institutes. Via TDL, their representatives exchange knowledge and experience; share customer, technology, and market insights; and work to improve the trustworthiness of digital services and platforms through joint research, education, and development.

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.

2.2 Strategic Relationships

Ever since its founding in 2009, TDL has enjoyed a close and fruitful relationship with both the European Commission, particularly DG CONNECT, and the European Union Agency for Network and Information Security (ENISA). TDL has participated in several EC-funded work programmes, notably the ACTOR project (*see Appendix*), and the EC and ENISA have supported TDL's flagship conference, Trust in the Digital World (TDW). TDL also contributed recommendations to the EU's legislation for ensuring the security of network and information systems (the NIS directive).

In 2016, TDL became a member of the newly-established European Cyber Security Organisation (ECSO), a fully self-financed, not-for-profit organisation under Belgian law that is intended to be an industry-led contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO's objectives are to protect the European Digital Single Market from cyber threats, develop the cybersecurity market in Europe, and foster the growth and market position of a competitive cybersecurity and ICT industry. To achieve this, ECSO intends to develop and deploy cybersecurity solutions for the critical steps of trusted supply chains in sectoral applications where Europe is a leader.

Whereas ECSO's goal is to achieve broad consensus on a variety of issues, TDL's focus is more specific and short-term, aiming at quick returns. TDL's priority is to derive immediate benefits from research, recommendations, and targeted events on specific topics such as blockchain and data protection, and to quickly validate research results and spur product innovation via sprints.

3 Challenges

3.1 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.

De-perimeterisation effectively removes many of the barriers to greater transparency and flexibility for employees, partners, and customers. Cloud computing is being embraced by all large enterprises, whether public, private, or hybrid, accelerating the move to devolved and remote management and stimulating the market for a wide range of ISPs.

These trends have their downsides. Cloud computing has numerous financial, operational, and resource benefits, yet it moves, rather than removes, concerns about security, data loss, and breaches of confidentiality, especially when strategic or client information is involved. As the cloud seems to continue to be an essential part of the digital landscape, it's wise for companies and vendors to invest in ensuring that security issues do not undo its benefits. 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.

New regulations of significance that address such issues include the General Data Protection Regulation (GDPR), the ePrivacy Regulation, the Electronic Identification and Trust Services regulation (eIDAS), Anti-Money Laundering Directive 4 (AMLD4), Payment Services Directive 2 (PSD2), and the Directive on Security of Network and Information Systems (NIS).

These in turn affect organisations, particularly small-to-medium-sized enterprises (SMEs), who struggle to comply with new regulations in an environment in which the media and the public are increasingly less tolerant of data breaches. To a company's brand recognition, the threats of reputational damage and the loss of customers' and partners' trust are as potent as that of regulatory action.

3.2 Advancing Technology

Myriad relatively young technologies are emerging into the mainstream: big data, Internet-enabled objects (that is, the Internet of Things), sophisticated analytical tools, machine learning algorithms, and the distributed database ledger known as the blockchain. All present new opportunities and new challenges.

The Internet of Things and the continuing growth in the use of mobile devices and applications for both social and commercial transactions dramatically increase the volume and velocity of data being generated on the Internet. It is increasingly beyond the capability of human beings to track or identify which data is valuable and how to process it. The result is to confer significant competitive advantages to businesses that adopt machine learning and data analytics in order to deliver a higher degree of personalisation, better user interfaces, and therefore improved services to consumers, although not without the risk that their profiles could be used for purposes that they had not given their consent to.

As is often heard at conferences today, "Every company is a data company". The downside to this progress is that many of the companies adding Internet connections to everyday objects from cars and washing machines to baby monitors and light bulbs have little experience with security, and as a result are creating opportunities and vulnerabilities for hackers, money launderers, terrorists, and other criminals to exploit. From a citizen's perspective, the situation presents the constant threat of compromised privacy and damaging financial or social consequences from devices that have been disabled or penetrated or from data loss or mishandling. Worse, the densely-written terms and conditions and privacy policies widely used to govern the use of the data these devices collect mimic those used by Internet services with little or no transparency for the majority of consumers. Meaningful consent is impossible in these circumstances, in which the balance of power rests entirely with the service providers, which take advantage to track, profile, and manipulate users.

Distributed ledger technology 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.

3.3 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.

A complex and poorly-understood studied issue is the interaction among these various pieces of legislation. For example, the technical standards for PSD2-compliant strong customer authentication and secure communication must also comply with eIDAS, while simultaneously feeding into the development of intelligence-based incident and identity management standards, especially in the areas of data protection and security. Technical standards for the Internet of Things must balance cybersecurity and privacy requirements as well as key management standards and solutions.

The new regulations bring considerable benefits to consumers. GDPR, in particular, requires most companies to undergo a culture shift in order to maintain, or in many cases establish, consumer trust with respect to the way in which their personal data is managed and stored. Of some concern are the considerable penalties that will accrue to non-compliance or negligence in reporting (for example, in case of a data breach). 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.

4 Impacts

4.1 Business Perspectives

The depth and breadth of the impact of the changes described above on all aspects of the enterprise can not be over-emphasised. Companies are increasingly realising the importance of ensuring they have made the right level of investment in cybersecurity to protect their assets as well as safeguard their brand and their chances of future survival. The near-ubiquitous use of mobile devices and the resulting greater online presence, awareness, and expectations are blurring the lines between employees, partners, and customers. On the other hand, the rapid change and scale of disruptions will also open a number of new business opportunities. Some companies may not be able to keep pace and will fail. This trend will undoubtedly continue to accelerate.

4.2 Personal & Societal Challenges

Over the last ten years, the EC has funnelled substantial investment into well-targeted legislation and research in order to develop and support the European Digital Single Market. However, individual citizens and society as a whole face market-driven challenges. Most people are willing to shop online, do their banking on their mobile device, find entertainment via the Internet, and interact with family and friends through social media. Too often, they only become concerned about the security of their systems or the entity that is handling their personal identity data after it is too late. According to Gemalto's 2016 Breach Level Index, 1.4 billion data records were compromised in 1,792 data breaches in 2015, an increase of 86% over the previous year. Much of this data was personally identifiable. In many cases, its disclosure risks distress, inconvenience, and/or financial loss. The Internet is fast becoming the social and commercial bedrock of our society and yet its trustworthiness is far from adequate for the purposes for which it is being used. If the situation does not improve, the loss of public confidence may lead some citizens to mistrust and show reluctance to fully engage in the digital world.

5
TDL's Work Programme

In response to the above challenges and their impact on business and society, TDL has chosen the following technical and business areas of focus for its research agenda over the coming three to five years, some of which are already being addressed.

5.1 Ongoing Research Activities

In 2017 TDL has three active Working Groups. A description of TDL's Working Groups can be found below.

5.1.1 Blockchain

The success of Bitcoin since its invention in 2008 has propelled the blockchain technologies on which it's based into public prominence. Yet the science of blockchain has lagged behind. In the last few years, financial institutions have begun exploring the potential of Bitcoin-like crypto-currencies; the open source community has experimented with a variety of implementations; and the research community has worked on developing and optimising the associated cryptographic protocols, improving architectural solutions, and understanding the sociology and economics of crypto-currency systems. Governments are considering how to regulate distributed financial systems and ensure integrity; civil society organisations are looking into privacy support in blockchain systems, and law enforcement agencies are studying the potential for new types of financial crime.

As work on exploring the diverse potential uses of blockchain technology has expanded, applications for e-government, storage, document notarisation, identity protection, real estate and enterprise have emerged.

TDL's Blockchain Working Group was set up in late 2015.

In June 2016, the Working Group held a highly successful, multi-disciplinary one-day event, *Multiple Views on Blockchain: Technology, Use Cases, Economics, and Policies*, in The Hague in collaboration with The Hague Security Delta and the Institute for Financial Crime. The event was divided into four panels covering research, application development, regulatory issues and innovation[1].

A follow-up workshop, *From Research To Innovation: The Blockchain Era*, will be held in June 2017 in Brussels in collaboration with *New Europe* and the Press Club Brussels.

1 The conference report as well as a list of the speakers and their presentations can be found at https://trustindigitallife.eu/events/past-events/multiple-views-on-blockchain-technology-use-cases-economics-and-policies/

In 2017 the Working Group completed and published its first collaborative paper, *Blockchain: Perspectives on Research, Technology & Policy*. The paper finds that blockchain has the potential to solve some security and privacy problems but warns of the risks of compromise at the point where humans interact with it. It argues that its use both protects privacy by allowing pseudonymous transactions and compromises privacy by making all transactions public. It also advocates the development of clear standards to ensure interoperability between varying blockchain systems and between blockchain and legacy applications. Further plans include:

(A) Specific papers:

(1) Successful applications of blockchain already deployed, also highlighting use cases which do not need to be on the blockchain, clarifying where blockchain is hype and where it is a game-changer.
(2) Blockchain and data protection legislation (EU and beyond). Advantages and challenges for a broader adoption of blockchain.

(B) A blockchain demo/prototype

The development of an open source prototype project.

5.1.2 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. The NIS Directive 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.

However, 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.

The Personal Data Working Group, set up in 2017, is focused on finding practical approaches to the new requirements and responsibilities arising from this rapidly changing legal landscape. The primary intention is to support SMEs and innovators who will be affected by these changes but are unaware or unprepared.

In May 2017, the Working Group published its first deliverable, *Privacy – The Competitive Advantage*, which highlights the positive benefits for companies, large and small, of embracing the guiding principles underlying the GDPR that will lead not only to compliance but also to a more trustworthy relationship with customers. Other work plans and deliverables for 2017-18 include:

(A) GDPR Compliance, comprising three documentary analyses:

- The potential challenges in implementing GDPR and PSD2
- The gaps between GDPR and eIDAS trust services
- The overlap and differences between GDPR and ePrivacy

(B) Practical implementation support

- An overall architecture with building blocks and what's missing
- A demonstration platform for electronic transactions leveraging an updated GTAC
- Interoperability of technology service providers

It is also planned to hold a one-day workshop with external stakeholders later in 2017. The latest information on the Personal Data Working Group can be found on our website[2].

5.1.3 The Internet of Things

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.

2 https://trustindigitallife.eu/what-we-do/working-groups/personal-data/

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.

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 *Securing Internet-Connected Devices Working Group* was formed in 2017 to address these and other issues.

(A) 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 confidence in devices
(2) Tools for designing a trustworthy system
(3) Metrics

(B) Insights and recommendations for businesses, governments and citizens

The original intention was 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 *Strategic Research and Innovation Agenda* (SRIA)[3] and the contents of the IoT calls, such as H2020 IOT-03-2017.

However, the scope of this activity was considered too broad and was revised to approach it from the perspective of specific use cases, such as 'Blockchain for IOT', not least given the synergy with the blockchain working group, which could be narrowed down further to, for example, smart contracts, identity management or supply chain.

3 https://ecs-org.eu/documents/ecs-cppp-sria.pdf

(C) IOT device security: quantification and improvements

This activity consists of two different tasks:

(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.

5.2 Proposed Research Activities

5.2.1 Cloud Computing

Cloud computing allows everyone – large corporates, SMEs, not-for-profit organisations, and citizens – to store data and applications in a shared, low-cost, high-capacity, energy-efficient storage and processing resource that is scalable, flexible, and optimally available. The concept is not new – "time-sharing" prototyped it in 1970 - but this time the facility and its associated services are clearly here to stay. The benefits are considerable, but there are challenges which are only gradually being addressed. Among these are questions of ownership, security, liability, and responsibility. A strong element of trust is involved in committing valuable data assets to a service that is remote, unseen, and effectively anonymous. 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. This is especially true for citizens and SMEs, who often have little bargaining power with respect to service contracts, and little insight into the security practices of cloud service providers.

The deployment of cloud services and data offers huge cost savings. At the same time, the real and perceived loss of control as well as the possibility of data breaches and loss of access are major deterrents to adoption. We are still far from a situation where everyone's own portion of the cloud – whether services, functions, or data – is as secure and reliable as if it were local and isolated. Security and reliability on this level needs to both exist and be perceived to exist. 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.

5.2.2 Big Data

Just as twenty years ago all companies were rapidly becoming Internet companies, today all companies are increasingly becoming data companies. The wealth of data available to most organisations has increased exponentially over the last five to ten years, a trend that is set to accelerate with the avalanche of data that will be unleashed by the Internet of Things. Today, the value of much of that data is incalculable; in some cases it should - and maybe one day will - be entered in business accounts as a quantified asset. Irrespective of sector or specialty, most organisations are amassing more business-relevant data than they know what to do with, in real time and near-real time, from multiple sources, and generated both internally and externally by both people and machines. Making use of this data requires advanced analytics or machine learning algorithms to extract value.

The privacy concerns raised by this level of data collection are equally extensive. Using advanced machine-learning and data analysis techniques, big data uncovers attributes and behaviour that the concerned would most likely not reveal directly. Rather than just asking what data may be directly collected for business, the question is rather how to prevent attaining properties that users do not want to disclose by any means. Of especial importance is personally identifiable information, which may include data sets that seem at first glance not to be personal but can be easily re-identified when matched against each other. Big data takes these issues to an unprecedented scale, and the need to address them is pressing. Not least, this requires there to be appropriate regulatory controls in place.

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.

5.2.3 5G

Most analysts believe that the implementation of the fifth-generation mobile standard, 5G, due in 2020, presents an opportunity for a step change in the evolution of mobile connectivity. The 5G infrastructure will be far more heterogeneous and opens the door to multi-tenancy, i.e. allowing the infrastructure to be shared by several network operators. Another major shift is the softwarisation and virtualization of functions in the network. A whole range of new services in different domains are envisaged above such a 5G network.

Today's mobile standards, 3G and 4G, support a set of services and applications that are by and large the domain of personal devices. When it arrives, 5G is expected to make possible more advanced applications and services. However, industry debate continues about whether 5G should be optimised for lower latency, high reliability/availability, or high speed; trade-offs must be made in answering this question. While the realities of physics mean that wired broadband will always outpace wireless for speed and reliability, within five to ten years we may well see 5G or even 6G broadband connectivity prevail over fibre for many applications.

Besides the tremendous spur 5G networks are expected to provide to business communication, and therefore the global economy, 5G will also significantly boost the Internet of Things through the excellence of the network. The added power available to connected mobile devices will enable a wide range of innovative applications. Once the new technology is ready for deployment, the increased efficiencies in bandwidth, reliability, and security will give businesses and citizens the confidence to proceed with deploying autonomous and connected cars, automated factory processes, and a range of healthcare applications.

5G brings new concepts and thus new challenges to security[4], 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 so 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 operator 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[5].

4 5G-PPP *Security Group: Phase 1 Security Landscape, Final Version 2.01*, May 2017

5 For example, the 5G-ENSURE project for Phase 1; the 5G-PPP security working group, and others

5.2.4 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 ensuring that systems are transparent, auditable and redress can be obtained. The approach with the greatest potential for providing assurance at an acceptable cost is designing in security and privacy from the beginning. Privacy by design and security by design should be applied to all methods, techniques, and tools intended to enforce and guarantee security and privacy properties at the software and system level. Empirical research to back up this principle with hard data is of key importance in establishing "by design" methodologies, as are approaches that enable the smooth migration of legacy systems.

To build and maintain trust, the providers of the infrastructures, platforms, applications and services that together make up the foundation of the digital economy must repeatedly demonstrate the security and privacy-friendliness of their offerings to both their customers and partners. Providers who want to distinguish themselves from the competition need to provide assurance.

Academic researchers and industry have proposed numerous techniques for assurance, including static code analysis and verification, dynamic security testing, penetration testing, formal models and proofs, certification schemes, vetting processes, disclosure of security policies, and security metrics. No single one of these techniques outperforms all others and qualifies as the reference technique. Instead, the objectives, properties, scope, target artefacts, rigour and costs of these techniques are complementary.

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.

5.3 Next Generation of 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 there are 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.

It is proposed that these new sprints not conclude with the proof of concept. Rather, their output will be maintained long enough for consumers to avail themselves of the results. The use of the enhanced services will be subject to some level of service level agreement.

The emphasis on the interaction between producers and users in an extended validation phase with a wider audience is a significant change of direction for the next generation of sprints. The intention is to provide a sustainable environment for technology innovators and interested users to interact from TDL members and beyond. Sprints will also be used to ensure that the results of EU projects will be made available to the broader community through, for example, TDL's GTAC.

6
Outcomes & Conclusions

Present and near-future products, services, and business models for computer networking technology are generating new and unsettling challenges to secure and trustworthy operations. If these problems are not addressed properly, they will undermine the basis of the digital economy. Industry leaders have to not only embrace the whole lifecycle of trustworthy systems, software and services but also equip it with user-friendly tools and techniques, ensuring that they are conformant with applicable legislation and regulations. This is the only way to generate the necessary trust and confidence for not only citizens but also organisations to seize, if not create, new societal and business opportunities enabled by the major trends we observe today.

Hence, in TDL's opinion, any effective strategy for re-establishing and preserving trust in the digital experience has to be approached holistically, taking a multi-disciplinary approach and by incorporating technical, social, and economic factors. TDL will annually review its strategy and update the most important issues at the centre of its work.

Glossary

cPPP	Contractual Public Private Partnership
DG CONNECT	Directorate General for Communications Networks, Content & Technology
EC	European Commission
ECSO	European Cyber Security Organisation
eIDAS	Electronic Identification and Trust Services for Electronic Transactions
ENISA	EU Agency for Network and Information Security
EU	European Union
GDPR	General Data Protection Regulation
GTAC	Generic Trust Architecture Centre
ICT	Information and Communication Technology
IoT	Internet of Things
ISP	Internet Service Provider
PSD2	Payment Services Directive 2
SME	Small to Medium-size Enterprise
SRIA	Strategic Research and Impact Agenda
TDL	Trust in Digital Life

Annex A
Tools & Deliverables

TDL has created several vehicles to enable members to exchange ideas about leading edge technology, methodologies, and services. These activities help foster new bilateral business contacts and provide opportunities for new insights and innovation to arise.

A.1
Working Groups

TDL's working groups are at the heart of the association's activities. These provide a vibrant and engaging meeting place for members to exchange ideas, prioritise new research and innovation topics, generate new insights through collaboration and general networking, and demonstrate thought leadership. Any member is entitled to propose and lead a new working group providing the area of interest meets with the objectives of the association and is approved by the membership.

Each working group is responsible for a set of deliverables and specified milestones. Working group leaders coordinate their own meetings and are responsible for their agendas. Minutes of these meetings are made available to all TDL members and observers.

Working groups meet regularly to discuss technical issues and to monitor and track their technical progress. All TDL members and guests are welcome to attend these meetings, where they may:

- Interact, network, and share ideas with leading organisations in the field of security and trust in ICT, mobile communication, and modern technologies;
- Join in conversation about and the development of research content on use cases, law and technology, requirements, and technology;
- Follow presentations from keynote speakers who are researchers in security and core elements of ICT trustworthiness;
- Participate actively to influence the decisions of European policies concerning trust;
- Gain EU recognition for the results of the research.

A.2 Generic Trust Architecture Centre (GTAC)

The Generic Trust Architecture was developed by TDL members as part of the EC-funded ATTPS project (*see below*). It defines the requirements, functionalities, building blocks, and core components for delivering the main targeted functionalities for trustworthy services, including mobile service and platform integrity, trusted stack, and data life cycle management.

GTAC enables members to share research results and make available outputs such as software components and services to both members and non-members for experimentation. Members sampling these new technologies benefit from early access; those offering the technologies gain from their feedback.

GTAC is accessible to the wider European research and innovation community so they may both offer their own components for testing and access those of others.

A.3 Collaborative Projects

TDL through its members and other partners have participated in several EC-funded research and development projects including ATTPS, AU2EU and ACTOR.

A.3.1 ACTOR (Accelerate Trust in Digital Life Organisation and Relations)

ACTOR was a two-year Coordination and Support Action funded by the European Commission that ran from 2010 to 2012 with the objective of establishing TDL's multidisciplinary research community and technological development policy for trustworthy ICT products and services.

ACTOR played a key role in helping expand TDL's membership, build its external relations, and develop its strategic activities with respect to developing and implementing trustworthy products and services. ACTOR focused on establishing an open research and innovation community with critical mass and helped position TDL as an initiative geared toward concrete aims in the near term and a lasting mindset going forward. The aims of ACTOR were to help TDL:

- Establish a multidisciplinary research and innovation community consisting of at least 50-60 leading edge partners
- Build broad support for TDL's research roadmaps for long-term research in the field of trustworthy ICT
- Bundle and coordinate TDL partners' efforts to develop a promising and ambitious strategic research agenda and work plan for TDL.
- Identify a balanced portfolio with project ideas covering the relevant dimensions for developing and implementing trustworthy products and services.

A.3.2 ATTPS
(Achieving The Trust Paradigm Shift)

ATTPS was a 40-month project that ran from June 2012 to October 2015. Initiated by TDL and co-funded by the European Commission, ATTPS was a twelve-partner consortium, the majority of which were TDL member organisations.

Through ATTPS, TDL addressed the tradeoffs that must be made among the business, legal, social, and technical aspects of building a public trust platform through practical work developing and testing generic trust architectures. ATTPS implemented and supported TDL's 2012 *Strategic Research Agenda* and actively contributed to raising awareness of the need for trustworthy ICT solutions. The project prioritised stimulating multi-disciplinary research communities; promoting standards, certification, and best practices; and coordinating national research and technical development activities.

A.3.3 AU2EU
(Authentication and Authorisation for Entrusted Unions)

TDL initiated and supported the objectives of AU2EU, a two-year EC-funded research and development collaboration between leading industry and research organisations from Europe and Australia, some of them current or former TDL members, that were determined to increase trust, security, and privacy. The project's aim was to foster the adoption of security-by-design and privacy-by-design in European and global markets; to contribute to increased trust, security and privacy; to foster the increased adoption of (cloud-based) critical infrastructures; and to facilitate the collaborative delivery of services dealing with sensitive data. Central to the AU2EU project was implementing and demonstrating, in a real-life environment, an integrated eAuthentication and eAuthorisation framework. Two pilot projects demonstrated the feasibility of TDL's approach. The first was secure information sharing for agencies involved in bio-security incident response in Australia; the second tested provisioning of trusted, dynamic, collaborative services for Ambient Assisted Living (AAL), a European eHealth project. AU2EU concluded in November 2015.

trustindigitallife.eu

Trust In Digital life Association
Aarlenstraat 22 / Rue d'Arlon 22
1050 Elsene, Brussels
Belgium

office@trustindigitallife.eu
+44 1738 583 533

TDL | Trust in Digital Life

TDL's vision is that trust must become an intrinsicproperty 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

Trust In Digital life Association
Aarlenstraat 22 / Rue d'Arlon 22
1050 Elsene, Brussels
Belgium

office@trustindigitallife.eu
T +44 1738 583 533

TDL | Trust in Digital Life