|  |  |  |
| --- | --- | --- |
| itu_logo | World Telecommunication Standardization Assembly (WTSA-16)Hammamet, 25 October - 3 November 2016 | CCITT/ITU-T 60th Anniversary logo |
|  |  |
|  |  |
| PLENARY MEETING | Revision 1 toDocument 58-E |
|  | 27 October 2016 |
|  | Original: English |
|  |
| Director of TSB |
| Conclusions of the third Global Standards Symposium |
|  |
|  |

|  |  |
| --- | --- |
| **Abstract:** | This report summarizes the conclusions of the third Global Standards Symposium (GSS). Revision 1 of this document includes a summary of all GSS presentations in Appendix 1. |

Conclusions of the 3rd Global Standards Symposium

The 3rd Global Standards Symposium, Hammamet, Tunisia, 24 October 2016, brought together thought leaders in the standardization sphere to discuss how standards efforts could best integrate the consideration of security, privacy and trust.

# 1 Introduction

Global Standards Symposiums (GSS) are high-level standardization policy debates that explore the evolving dynamics of information and communication technology (ICT) and associated implications for technical standardization. GSS is held at the outset of ITU’s quadrennial World Telecommunication Standardization Assembly (WTSA). Previous editions were held in Johannesburg in 2008, and Dubai in 2012.

The theme of GSS-12 – *Standardization at the intersection of the ICT sector with other sectors such as health care, utilities, and transport* – proved very timely, and the conclusions of the symposium offered valuable guidance to the ITU standardization work carried out from 2013 to 2016. GSS-12 touched on security, privacy and trust in ICT infrastructure and services when discussing topics such as the wireless transmission of medical data, the storage of data on the movements of connected vehicles, and the collection of consumer data by online retailers. In such environments, standardized frameworks are necessary to provide the assurance that a service possesses trusted security attributes, and that users’ security and privacy needs are protected.

The 3rd Global Standards Symposium (GSS-16) discussed how interested stakeholders could work in collaboration to develop international frameworks for security, privacy and trust. The symposium brought together leading experts in the fields of security, privacy and trust, representing governments, regulators, standards bodies and industry. Participants exchanged views on what they perceive to be the key elements of such frameworks, as well as which of these elements should be assigned priority in related ITU standardization work to be undertaken from 2017 to 2020.

Welcome remarks were delivered by **H.E. Mohamed Anouar Maarouf**, Minister of Communication Technologies and Digital Economy, Republic of Tunisia. Opening remarks were given by ITU Secretary-General **Houlin Zhao**, and the Director of the ITU Telecommunication Standardization Bureau **Chaesub Lee**. The symposium was chaired by **Mongi Marzoug**, former Minister of ICT, Tunisia.

The opening session of GSS-16 was followed by three sessions approaching the symposium’s theme from the perspectives of regulation and policy, industry, and standardization. Followed by an examination of the theme of GSS-16 in the context of the United Nations (UN) system in Section 2 of this report, Section 3 summarizes the key findings and recommendations of each of the Symposium’s sessions. A detailed summary of all the discussions of GSS-16 is included in Appendix I.

The final programme, speaker biographies and presentations are available at:
<http://itu.int/en/ITU-T/wtsa16/gss/>.

In accordance with Resolution 122 (Rev. Guadelajara, 2010) and ITU Council Resolution 1272 (MOD), the conclusions of GSS-16 detailed by this report are transmitted for consideration by WTSA-16.

# 2 Security, privacy and trust in ICTs – the UN context

ICTs have enabled billions of people to exchange digital information on a global scale. The use of these technologies, which rely heavily on technical standards, has brought about a host of challenges with respect to the privacy and security of communications, and ultimately end-user confidence in ICTs.

ITU engages with this challenge both as a standards-developing organization that aims to develop privacy-friendly voluntary international ICT standards[[1]](#endnote-1) and as an intergovernmental organization mandated to build confidence and security in the use of ICTs.[[2]](#endnote-2) The World Summit on the Information Society conferred on ITU the responsibility to act as the facilitator of Action Line C.5, working among ITU Member States and other stakeholders towards *“strengthen[ing] the trust and security framework with complementary and mutually reinforcing initiatives in the fields of security in the use of ICTs, with initiatives or guidelines with respect to rights to privacy, data and consumer protection”*.

The normative international basis for the protection of privacy is provided primarily by human rights treaties such as the UN Universal Declaration of Human Rights of 1948[[3]](#endnote-3) and the UN International Covenant on Civil and Political Rights of 1966[[4]](#endnote-4), both of which contain provisions on the right to privacy/private life (arts. 12 and 17, respectively). These conventions, however, do not refer explicitly to the digital processing of personal information, a concept which, in the context of the UN system, has been addressed only in the form of a non-binding guidance document, namely the 1990 UN Guidelines concerning Computerized Personal Data Files.[[5]](#endnote-5)

While a number of legally binding international conventions do contain a right to privacy – such as the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[[6]](#endnote-6), the European Convention of Human Rights and Fundamental Freedoms[[7]](#endnote-7) and the American Convention of Human Rights[[8]](#endnote-8) – these legal instruments have been developed and adopted on a regional rather than global basis. Many of these regional agreements are based on the same fundamental privacy principles, such as the concept of informed consent of the individual and the adequacy of the security measures put in place prior to processing personal information.[[9]](#endnote-9)

A variety of stakeholders have called for increased attention to be paid to the need for a common global understanding on the processing of personal information. For example, the International Conference of Data Protection and Privacy Commissioners has appealed to a) the United Nations, to prepare a legally binding *“universal convention for the protection of individuals with regard to the processing of personal data”*; b) international organizations, *“to commit themselves to complying with principles which are compatible with the principal international instruments dealing with data protection and privacy”*; and c) hardware and software manufacturers, *“to develop products and systems integrating privacy enhancing technologies”*.[[10]](#endnote-10)

The UN General Assembly heeded this call during its 68th Session (2013) by adopting a Resolution titled *“The right to privacy in the digital age”*, calling on all UN Member States to *“respect and protect the right to privacy, including in the context of digital communication”*[[11]](#endnote-11). Following this Resolution, the UN Human Rights Council appointed a Special Rapporteur with a mandate to, *inter alia*, report on alleged violations of the right to privacy, including in connection with the challenges arising from new technologies.

# 3 Main conclusions of GSS-16

## 3.1 Regulatory principles for security, privacy and trust

*Recalling that privacy and data protection constitute core values of individuals and societies, and that the Universal Declaration of Human Rights enshrine privacy as a fundamental right;*

*Noting that almost all areas of life now rely on ICT infrastructure and services, and would therefore be affected if trustworthiness cannot be maintained; and,*

*Recognizing the alarming trend in data breaches and security incidents, having an adverse impact on people’s trust,*

*GSS stressed:*

– Leverage **international frameworks** that contain basic principles of security, privacy and trust, and establish mechanisms of implementing these principles.

– Promote adherence to **privacy-by-design principles, privacy impact assessment and the development of privacy enhancing technologies** (PETs), technologies that, when integrated in ICT infrastructure and services, minimize the processing of personally identifiable information.

– Establish means for the **sharing of information between the public and private sectors** on threats to ICT infrastructure and services, best practices and mitigation strategies.

– Mobilize the international community and establish partnerships to **develop national capabilities** to protect from cyber-attacks, increasing countries’ capacity to detect security incidents and effect coordinated responses to such incidents.

– Create a balance between the need to protect the privacy of individuals and encourage the **innovative use of data** to drive the digital economy. When designed into new technologies and services, good privacy and security practices become attractive selling points to customers and make a contribution to the improvement of the whole network.

– Contribute to **international standards to address global issues**, recognizing that cyber-attacks do not respect national borders and that breaches of privacy and security undermine trust in ICT, and that security frameworks standardized at the international level are necessary to provide the assurance that a service’s security attributes can be trusted and that a user’s security and privacy needs are protected across borders.

– Promote the development of **standards for the ‘de-identification’ of personal data** and **data portability**, standards able to contribute to greater consumer protection and greater choice with respect to consumers’ ability to subscribe to and unsubscribe from ICT services.

## 3.2 How industry meets end-users’ expectations of security, privacy and trust

*Reaffirming the enormous potential of information and communication technologies and digitization to improve our lives and society;*

*Recognizing that security breaches, privacy violations and lack of trust in ICT infrastructure and services can pose serious threats to a company’s business and reputation; and,*

*Calling for implementable international standards,*

*GSS stressed:*

– Support and promote principles of **transparency** and **technological integrity.** Acknowledging that there can be no trust without transparency, users should have the ability to know how their data are being used and decide whether or not to accept such use. Technological integrity supports the need for strong security in ICT infrastructure and services, endorsing privacy measures and rejecting the prospect of hidden functionality, to prevent unauthorized modifications of information and establish trust in the accuracy, completeness and reliability of information.

– Mitigate the risks posed by **IoT botnets** using security standards. Reported cases of the abuse of Internet of Things (IoT) devices in large-scale distributed denial-of-service (DDoS) attacks are on the rise. Such attacks can result in data breaches, and significant economic and reputational damage for organizations affected. It needs to be studied how advances in areas such as lightweight cryptography and standardized security methods could be leveraged to achieve high levels of security with only limited computing power.

– Assess the impact of **quantum computing** on security, privacy and trust, and study **quantum-safe technologies**. Although quantum computing may still be in its infancy, it is widely accepted that, once the use of this technology becomes practical, the conventional encryption methods that protect today’s online payments, banking transactions, and email and phone conversations could quickly be rendered inadequate. The time is ripe to assess the impact of quantum computing, and to research, test, standardize and prepare a transition to new security schemes that resist quantum attacks, well before our systems become vulnerable to such attacks.

## 3.3 Standards bodies’ approach to security, privacy and trust

*Recognizing the crucial role played by standards in ensuring security, protecting privacy and establishing trust in ICT infrastructure and services;*

*Highlighting that security, privacy and trust are established areas of work in many international standards bodies that address ICT and other technology areas; and*

*Calling for standardization to address challenges to security, privacy and trust,*

*GSS stressed:*

– Support a **privacy-by-design** mindset, paying due regard to privacy considerations throughout the standards-development process. Privacy-by-design can be promoted by standards that incorporate privacy and data protection features, and standards can also be effective in ensuring interoperability between privacy features.

– Understand the role of **open-source software** in addressing challenges to security, privacy and trust challenges. Open-source software and standards make complementary contributions to the growth and innovation of the ICT industry. Software has grown in complexity, and while open-source and standardization communities are collaborating in many areas, more effort should be made to facilitate the exchange of work between these communities and thereby ensure high-quality, high-security software implementations.

– **Strengthen collaboration** among standards bodies in the development of international frameworks for security, privacy and trust, recognizing their mandates and strengths and leveraging existing work. Standards bodies should adhere to due process, broad consensus, transparency, balance and openness in standards development; commitment to technical merit, interoperability, competition, innovation and benefit to all; availability of standards to all; and the voluntary adoption of standards. Standards bodies should also collaborate in their efforts to address the disparity between developing and developed countries in their ability to access and implement standards and frameworks addressing security, privacy and trust in ICT infrastructure and services, and participate in their development on an equal footing.

Appendix I
Detailed summary of GSS-16 discussions

(This appendix does not form an integral part of this Report)

Session 1: Welcome and keynotes

**H.E. Mohamed Anouar Maarouf**, Minister of Communication Technologies and Digital Economy, Republic of Tunisia [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Maarouf) ] extended a warm welcome to all participants and thanked the ITU membership for choosing Hammamet, Tunisia, as the venue for the Global Standards Symposium (GSS) and the World Telecommunication Standardization Assembly (WTSA). He highlighted the necessity to build condidence and trust in ICT infrastructure and services, recognizing the importance of the theme of GSS-16: *Security, Privacy and Trust in Standardization*.

In his opening remarks, GSS-16 Chairman **Mongi Marzoug** (Former ICT Minister, Tunisia) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Marzoug) ] welcomed all attendees to Tunisia and whished them an enjoyable stay in Hammamet. He highlighted Tunisia’s role in building the Information Society, and described the important role that information and communication technologies (ICTs) play in our daily lives today and will continue to play in the future. He stressed the importance of open, safe, secure and trustworthy ICT services for the world’s development, across all domains (e.g., healthcare, finance, utilities, Internet of things (IoT)). In this context, he noted that standardization has a key role to play to improve ICT security, protect privacy and build trust in ICT services for citizens, governments and companies. He highlighted that the aim of this third GSS was to present and discuss the contributions to security, privacy and trust in ICT infrastructure and services of three main stakeholders: government and regulators, industry, and standardization bodies, and to provide conclusions and recommendations on these topics to WTSA-16.

**Houlin Zhao** (Secretary-General, ITU) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Zhao) ] thanked the host of GSS and WTSA, the Republic of Tunisia, for its support to the work of ITU. Describing the positive contribution of the previous editions of GSS, he described how GSS provides an international platform to debate standardization policy, bringing together leaders in the public and private sector to discuss how technical standardization should respond to the evolving priorities of the ICT sector. The conclusions and recommendations of GSS-08 and GSS-12 have all become essential to the work programme of ITU standardization. He also noted that a trusted ICT environment will give users and business the confidence to use ICTs to their full potential, and that ITU standardization plays an important role in fulfilling ITU’s mandate to “build confidence and security in the use of ICTs”. In concluding, he expressed his gratitude to all speakers, moderators and participants for their contribution to GSS-16.

In his welcome address, **Chaesub Lee** (Director of the ITU Telecommunication Standardization Bureau) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Lee) ] described how future networks would need to support a great volume of ICT applications and a very broad spectrum of services. Billions of networked devices, things and objects would enable systems to communicate and learn from one another, creating intelligent ecosystems that adapt their behavior in the interests of efficiency. The next generation of communications would see applications in areas spanning from voice and video to industrial robotics, intelligent transport, remote medical surgery, virtual reality and much more.Lee noted that this increasing sophistication of ICTs and unprecedented level of ICT ubiquity would demand significant transformations in network infrastructure and services. As societies are on course for a world in which nearly every aspect of economic and social activity would depend on ICTs, it becomes essential that we build ICT infrastructure and services deserving our trust. He highlighted the role of technical standards in preventing the emergence of data ‘silos’ in different sectors of our economies, and noted that experts participating in ITU standardization are working to support the development of a shared, integrated data ecosystem.

Session 2: Regulatory principles for security, privacy and trust

The session introduced regulatory principles for security, privacy and trust and was moderated by **Bilel Jamoussi** (Chief of Study Groups, ITU Telecommunication Standardization Bureau) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Jamoussi) ].

In his keynote address, **John Edwards** (Privacy Commissioner of New Zealand; and Chair, Executive Committee of the International Conference of Data Protection and Privacy Commissioners) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Edwards) ] recognized a gradual but an accelerating movement towards consensus among previously disparate organizations, and consensus that privacy is becoming one of the defining issues of our age. Edwards highlighted that the UN General Assembly during its 68th Session (2013) adopted a Resolution entitled *“The right to privacy in the digital age”*, calling on all UN Member States to *“respect and protect the right to privacy, including in the context of digital communication”*. He introduced the work of the organization he represents, the International Conference of Data Protection and Privacy Commissioners (ICDPPC), and proposed some ideas for increasingconfidence and trust by applying privacy principles and perhaps developing standards in the telecommunications sector, including:

– To promote adherence to privacy-by-design principles, privacy impact assessment and the development of privacy enhancing technologies.

– To ensure that access to networks, systems, content, communications and medata by agents of the State is undertaken only in accordance with lawful authority, and only in cases where that access is necessary, and proportionate.

– To promote transparency in relation to the access to or use of personal data for purposes other than those for which the data subject has provided their consent.

– To develop and promote appropriate standards and safeguards for the ‘de-identification’ of personal data, and for the prevention of reidentification of individuals from deidentified datasets.

– To develop standards for data portability, standards able to contribute to greater consumer protection and greater choice with respect to consumers’ability to subscribe to and unsubscribe from ICT services.

– To ensure that citizens and consumers continue to have transparency as to the basis on which the automated decisions affecting them have been made.

In his intervention, **Victor Manuel Martinez Vanegas** (Director of International Policy, Federal Telecommunications Institute, Mexico) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Vanegas) | [Presentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GSS_IFT_Draft_Presentation.pdf) ] approached the GSS topic from a global perspective, discussed initiatives taken at a regional level, and introduced a national context for security, privacy and trust in ICTs.

He described how the development and adoption of ICTs have a positive impact on economic and social growth, but that there also exist threats and challenges that can jeopardize these benefits. Security, privacy and trust have become key elements to be addressed in an appropriate manner. He cited from related publications, declarations and agreements, including the United Nations General Assembly, standardization activities in ITU-T and IEC, and UNCTAD’s Information Economy Report 2015, which identified that *“security and trust are essential to create an enabling environment for electronic commerce”*. Martinez Vanegas pointed out that his own region, Latin America and the Caribbean, has the fastest growing Internet population in the world, and that addressing security, privacy and trust in ICTs was imperative to economic and social development in the region. He also stressed that experience in the region has shown that no nation by itself can adequately secure its networks and that cooperation is essential.

**Ilias Chantzos** (Senior Director, Government Affairs, EMEA & APJ, Global CIP and Privacy Advisor, Symantec, United States) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Chantzos) | [Background Document](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/InternationalCyberNorms_Ch10%20-%20Symantec.pdf) ] described how policy and regulatory drivers influence, and are in turn influenced by, technological advancements. He cited the EU General Data Protection Regulation as one of the most evident examples of these dynamics. The existing Privacy Directive was more than 20 years old, and had to be significantly adapted to reflect the evolution, or revolution, technology and other factors like social media went through. In turn, the use of technology and social media will now have to comply with the new Regulation, with fundamental changes in the way public and private organizations will drive their data governance, including protecting personal data from cyberattacks. Chantzos also introduced the concept of technological integrity, which supports the need for strong security in ICT infrastructure and services, endorsing privacy measures and rejecting the prospect of hidden functionality, to prevent unauthorized modifications of information and establish trust in the accuracy, completeness and reliability of information.

**James M. Kilaba** (Director General, Tanzania Communications Regulatory Authority (TCRA)) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Kilaba) | [Presentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GSSWTSA2016-Kilaba.pdf) ] highlighted security and privacy challenges arising from the technological shift from a time when only few personal computers were connected to the Internet, to today’s communications by anyone, anything, anywhere, and anytime. He described initiatives taken at the national and regional levels to protect privacy, secure data and ICT infrastructures. These include: establishment of a National Computer Emergency Response Team (TZ-CERT), which is used for dissemination of cybersecurity knowledge, information and skills to various stakeholders; the implementation of DNSSEC in the Domain Name Registry System; and discussion about cybersecurity in the East African Communications Organization (EACO). Kilaba called for a holistic approach to address these challenges, highlighting the need to harmonize international standards to support developing countries.

**Chawki Gaddes** (President, National Authority for the Protection of Personal Information, Tunisia) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Gaddes) | [Presentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GSS-Gaddes.pdf) ] described Tunisia’s leading role in guaranteeing, through its Constitution, the protection of privacy and personal data (Article 24, 2014), access to information and communications networks (Article 32, 2004), and access to government documents (to enter into force in 2017). He highlighted how Tunisia is attaching great importance to creating a space of trust between its citizens, the private sector, and the government.

Session 3: How industry meets end-users’ expectations of security, privacy and trust

**Ilias Chantzos** (Senior Director, Government Affairs, EMEA & APJ, Global CIP and Privacy Advisor, Symantec, United States) moderated a double-session on how industry meets regulatory principles and end-users’ expectations of security, privacy and trust.

**Ammar Alkassar** (CEO, Rohde & Schwarz Cybersecurity, Germany) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Alkassar) | [Presentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/3-1201601024_ITU%20GSS16_ALKASSAR_2.pptx) ] outlined trends in ICTs that will change our world in a sustainable way. He described how cybersecurity will act as a key enabler of this change, and will become even more critical in the future. Alkassar pointed out that the security tools deployed today are far behind to be adequate, compared to the economical values to be protected. He described the need to define new sets of standards following a paradigm shift in IT security to cope with the increasingly smarter threat environment. According to Rohde & Schwarz, such paradigm shift would be comprised of the following elements: implementing security by design, and using preemptive rather than reactive measures; building on information flow control, rather than access control; and leveraging users from unfulfillable responsibilities when it comes to cybersecurity. He noted that the ITU community can provide significant contributions in this area, especially through its standardization activities, and in linking the traditional telecommunications community and new ICT players.

**Thomas Kremer** (Member of the Board of Management for Data Privacy, Legal Affairs and Compliance, Deutsche Telekom, Germany) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Kremer) | [Presentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Deutsche%20Telekom%20-%20final.pptx) | [Background Document](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Getting%20out%20of%20the%20digital%20trust%20trap%20-%20deutsche%20telekom.pdf) ] highlighted that transparency is a prerequisite to trust. People must be able to know how their data are being used, and they must be able to consciously decide whether or not to accept such use. However, transparency alone is not enough if companies want to live up to their digital responsibility. Kremer called for systems that can reliably anonymize data in all use cases not requiring direct personal reference. He identified encryption as another means to build customer trust, in particular in the context of sensitive data such as health data. According to Deutsche Telekom, any proposal to furnish authorities with “spare keys” or “backdoors” to secure systems would prove counterproductive and undermine efforts to enhance security, as these would quickly be exploited by adversaries. Kremer called for smart, usable and timely solutions in the area of cybersecurity. As new technologies emerge (IoT, machine learning, quantum computing, etc.), attacks would become more sophisticated. Standardized approaches to detect and mitigate risks and attacks are required.

**David Francis** (European Cyber Security Officer, Huawei Technologies, China) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Francis) | [Presentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Huawei%20-%20final.pptx) ] explained what protecting privacy and security entails from a technology vendor’s point of view. He discussed the policies and processes in place in a company like Huawei Technologies to ensure the security and resilience of its products which would ultimately help protect the privacy and data of the end user. Key elements to be considered in a holistic approach include: secure devices; architecture – a network is constructed from multiple complex products; and people, who implement, manage, upgrade, fix and assess the environment.

Francis addressed the need for management of the global supply chain on which the IT sector fully relies to mitigate any security risks, the role of transparency and global standards, as well as the need for international cooperation to improve cybersecurity around the globe.

**Jaya Baloo** (Chief Information Security Officer, KPN, Netherlands) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Baloo) | [Presentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/3-4ITU-GSS-Tunesia.pdf) ] discussed the race for quantum technologies, from quantum computing to quantum cryptography. The availability of a quantum computer will pose a security risk to countries and companies reliant on asymmetric cryptography (RSA, ECC). The necessary response called for are post quantum solutions, which can occur in three stages. Firstly, by increasing the key length of the current crypto algorithms. Secondly, by using quantum key distribution for specific critical points in networks. Thirdly, by creating and supporting future proof post quantum cryptographic algorithms. The global information security community is making strides in innovation around quantum technologies. However, there is a danger that this will present a new digital security divide cleaving those countries that have the financial and academic resources to possess a quantum computer to break other countries' cryptography while protecting their own communications, and those who can neither attack nor defend themselves.

**James Snow** (Security & Compliance Strategist, Google, United States) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Snow) | [Presentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Google-final.pptx) | [Background Document](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GoogleExecSummary_2016.pdf) ] noted that it is a key priority for Google to earn and maintain its customers’ trust by processing data in a secure, reliable, and compliant environment. Security and privacy are critically important to Google, which is why the company is investing deeply to protect customer data. This includes the use of secure purpose-built servers and network infrastructure, and encryption of customer data whether it is on a disk, stored on backup media, moving over the Internet, or travelling between data centres.

Snow described how customer trust begins with understanding, and that understanding can only be created through transparency, e.g., by making available detailed documentation, auditing reports, and certifications. Google recognizes the importance of international cooperation, and leverages several international standards for security and privacy including:

– ISO 27001:2013, Information technology – Security techniques – Information security management systems – Requirements;

– ISO 27017:2015, Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services;

– ISO 27018:2014, Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors; and

– SOC 2/SOC 3 — Audit framework for non-privacy principles that include security, availability, processing integrity, and confidentiality.

**Yuejin Du** (Vice President of Security, Alibaba Group, China) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Du) | [Presentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Yuejin-DU.pptx) ] elaborated on the importance of security and privacy in the infrastructure Alibaba provides to its customers for commerce and data technology. For instance, Alibaba is providing information security products to partners and promoting standards through the E-commerce Ecosystem Security Alliance (EESA), which was initiated by Alibaba in July 2016. In EESA, Alibaba and its partners can leverage established risk detection models to examine and identify threats, and work together to improve security and protect privacy in the e-commerce ecosystem by implementing the established alliance standards.

**Bernard** **Benoit** (General Manager, WhiteNoise/Kudelski Security, Switzerland) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Benoit) | [Presentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Kudelski%20-%20final.pdf) ] described the possibly conflicting interests of users, service providers and governments, and how existing telecommunications networks are security-flaw ridden and hence were not able to guarantee the security and privacy of communications. To reinforce security and privacy over untrusted networks, he promoted a scalable hardware security component based over-the-top approach, which would operate independently from the underlying networks and protocols. Benoit reminded the audience of the need for platform-independent solutions, with standardized interfaces compatible to meet the applicable lawful intercept requirements, without jeopardizing technological integrity through backdoors, spare keys, etc.

Session 4: Standards bodies’ approach to security, privacy and trust

A review of the approaches taken by various standards development organizations (SDOs) with respect to security, privacy and trust took place in Session 4. The session was moderated by **Toni Eid** (Editor in Chief, Telecom Review) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Eid) ].

**Sophie Clivio** (Director, Standardization and Technical Policy, International Organization for Standardization (ISO)) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Clivio) | [Presentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/ISO%20-%20final.PPTX) ] introduced ISO’s broad and multi-sectoral approach to security, privacy and trust. She emphasized the work of ISO committees on security and resilience; risk management; blockchain and electronic distributed ledger technologies; and the joint ISO/IEC activities on information security and privacy in the Joint Committee on Information Technology (ISO/IEC JTC 1). Key areas covered by JTC 1 include information security management, cryptographic and security management, identity management and privacy technologies; biometrics; cards and personal identification; IT governance; security, privacy and trust mechanisms for cloud computing, big data and IoT. Clivio noted that ISO and its standards are present across economic sectors including healthcare, transport (e.g., aviation, intelligent transport systems, marine technology), energy, construction, manufacturing (including additive manufacturing), and that cooperation agreements have been established with organizations addressing the needs and particularities of these sectors.

**Frans Vreeswijk** (General Secretary & CEO, International Electrotechnical Commission (IEC)) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Vreeswijk) | [Presentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/IEC%20-%20final.pptx) ] described how the IEC brings together all stakeholders in electrotechnology in an effort to build trust in safe and efficient products and systems through the use of IEC International Standards and the IEC Conformity Assessment Systems. IEC has published over 200 cybersecurity standards with a particular focus on protecting essential infrastructures such as electricity generation and distribution, water and waste management, hospitals and healthcare, manufacturing and data centres from cyber-vulnerabilities and attacks. IEC also contributes in an essential way to the safety and security of all electric and electronic hardware which enables data collection or access and control protocols. This includes, for example, sensors, medical devices, wearable smart devices as well as computing and data storage technologies. IEC International Standards are key enablers in the quest for resilience, risk management and efficiency improvements.

IEC closely collaborates with ISO in the Joint Committee on Information Technology (ISO/IEC JTC1) in areas such as information security management, identity management, cryptography and security identification, privacy technologies, biometrics, cards and personal identification, cloud computing, big data and much more. IEC has an ongoing relationship with ITU, together with ISO in the World Standards Cooperation.

Vreeswijk called for broad cooperation between all standards organizations to address topics of security, privacy and trust. In essence, no single organization will be able to deliver all the standards that are needed in this space.

**Karen McCabe** (Senior Director, Technology Policy and International Affairs, IEEE Standards Association (IEEE-SA)) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#McCabe) | [Presentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/IEEE-final.pptx) ] highlighted that standards have a critical role to play in helping to ensure security and privacy, and enabling trust in ICTs. To enable this role, a best practice is to work within a set of principles that provide a worldwide community for voluntary cooperation among interested parties and stakeholders, and enable technical excellence, global interoperability and innovation. These principles include: direct participation; due process; broad consensus; balance; transparency; universal openness; coherence; development dimension.

She noted that open processes are a good practice from a security perspective as the review of multiple experts can discover potential flaws and improve the standards in development. The transparency of open standards development promotes trust in platforms, services and products built upon and adhering to these standards. In addition, open standards enable privacy- and security-enhancing technologies to gain widespread adoption as they promote interoperability. She concluded that open standards fuel innovation that can advance solutions to the challenges of security, privacy and trust.

IEEE has a wide range of standards in its portfolio, starting from security, privacy and trust considerations for the IEEE 802 series of network standards, to cryptography in the IEEE 1363 series (with a focus on public key infrastructure (PKI) based algorithms), in the IEEE 1619 series, and many others. IEEE’s Industry Connections Security Group (ICSG) is a group of computer security entities that have come together to pool experiences and resources in combating the systematic and rapid rise in computer security threats. In another recent effort, the IEEE Internet Initiative was established to raise the organization’s influence and profile in global technology policy in the areas of Internet governance, cybersecurity and privacy policy development by providing a consensus of sound technical and scientific knowledge and guidance to the process. The IEEE Global Initiative for Ethical Considerations in the Design of Autonomous Systems and its Ethics, Society & Technology Ad Hoc Committee are exploring new standards and solutions, certifications and codes of conduct, and consensus building for ethical implementation of intelligent technologies, including artificial intelligence and autonomous systems.

Moving forward, McCabe called for the inclusion of a new generation of privacy, security and ethics professionals from across disciplines in the standards development processes, and for building privacy, security and ethics into the open standards themselves, in order to contribute to trust in ICTs.

**Ashok Ganesh** (Director Innovation, CEN-CENELEC) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Ganesh) | [Presentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/CEN-CENELEC-final.pptx) ] highlighted that all industry sectors are undergoing a transformation as they take up digital technologies and approaches (e.g., Internet of things, cloud computing, robotics, sensor technologies) that radically change their processes, systems and even their business models. These traditional, vertical industry sectors (e.g., manufacturing, energy, transport), who previously were not significant users of ICT and digital technologies, seek support and standardization solutions for this transformation. Ganesh noted that SDOs such as ISO, IEC, and CEN and CENELEC in Europe have a significant ‘footprint’ in these vertical sectors and wish to develop their approaches to fulfil these ICT/digital-related needs. The take-up of these technologies involves the employment of systems for industrial plant and manufacturing processes as well as the generation, processing, sharing and storage of masses of data. Ganesh pointed out that the challenge for standardization organizations is multi-stranded: to keep the engagement of traditional stakeholders, attract ICT/digital stakeholders and modify their own approaches to be in a position to provide directly and indirectly standardization solutions in an increasingly complex and fast moving area. A priority for SDOs is to focus on the vertical needs and applications including addressing the link between cybersecurity and functional safety, product reliability, data security and privacy.

**Reinhard Scholl** (Deputy to the Director of the ITU Telecommunication Standardization Bureau) [ [Biography](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Scholl) | [Presentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Reinhard-final.pptx) ] reminded all participants of a cybersecurity symposium held as side event of WTSA-04 in Florianopolis, Brazil. The event had concluded in 11 key messages, most of which are still valid today, e.g., “Security must be built-in, not bolt-on”, or “Stakeholders need to share information”, and “Standardization needs to be a vital part of the global cybersecurity effort.”

To illustrate today’s situation, he provided some figures about the number of known cyber-incidents in ITU’s network infrastructure. He stated that in his view security and privacy are not mutually exclusive. He also explained that ITU work to build confidence and security in the use of ICTs continued to intensify in a bid to facilitate more secure network infrastructure, services and applications. He introduced recent ITU work in the areas of security and trust, including a report which stresses the importance and necessity of trust in the ICT context, and introduces related concepts and key features of trust. One of the ideas discussed in the report is a “trust index”, a number that combines multiple trust related indicators into one benchmark measure. A trust index could be used to compare trust among stakeholders when they create a new trust relationship or a trust value chain.

Scholl noted that work was initiated by the membership to explore, *inter alia*, requirements, capabilities and service scenarios for trust provisioning; the architectural framework for trustworthy telecommunication networks; technical solutions for trust provisioning; trust provisioning in big data analytics; and inter-cloud trust management. Related ITU-T standardization efforts cover areas such as cybersecurity; security management; security architectures and frameworks; countering spam; identity management; and protection of personally identifiable information.

Scholl also recommended to study the contribution the open source community can make to standards addressing security, privacy and trust in ICT infrastructure and services. He said that more efforts should be undertaken to facilitate the exchange of work between open-source and standardization communities, and thereby ensuring high-quality standards and software implementations.

Endnotes

1. See for example, Recommendation ITU-T X.1171 “Threats and requirements for protection of personally identifiable information in applications using tag-based identification” [↑](#endnote-ref-1)
2. See for example, Resolution 130 (Rev. Busan 2014), on strengthening the role of the ITU in building confidence and security in the use of information and communication technologies. [↑](#endnote-ref-2)
3. <http://www.un.org/en/universal-declaration-human-rights/> [↑](#endnote-ref-3)
4. <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> [↑](#endnote-ref-4)
5. <http://www.un.org/documents/ga/res/45/a45r095.htm>; UN Doc E/CN.4/1990/72 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G90/107/08/PDF/G9010708.pdf?OpenElement> [↑](#endnote-ref-5)
6. <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37> [↑](#endnote-ref-6)
7. <http://www.echr.coe.int/Documents/Convention_ENG.pdf> [↑](#endnote-ref-7)
8. <https://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.htm> [↑](#endnote-ref-8)
9. See for example the APEC Privacy Framework and the EU regulatory framework on privacy, which have been inspired to a certain extent by the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> [↑](#endnote-ref-9)
10. Montreux Declaration of the International Conference of Data Protection and Privacy Commissioners, <https://icdppc.org/wp-content/uploads/2015/02/Montreux-Declaration.pdf> [↑](#endnote-ref-10)
11. UNGA Resolution 68/167, <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167> [↑](#endnote-ref-11)