|  |  |  |
| --- | --- | --- |
| itu_logo | World Telecommunication Standardization Assembly (WTSA-16)Hammamet, 25 October - 3 November 2016 | CCITT/ITU-T 60th Anniversary logo |
|  |  |
|  |  |
| PLENARY MEETING | Document 58-E |
|  | 24 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. |

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 to:*

– 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 to:*

– 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 to:*

– 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)

A detailed summary of GSS-16 presentations will be included in Revision 1 of this document.

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)