|  |  |  |
| --- | --- | --- |
| itu_logo | **世界电信标准化全会****（WTSA-16）2016年10月25日-11月3日，哈马马特** | Title: CCITT/ITU-T 60th Anniversary logo |
|  |  |
|  |  |
| **全体会议** | **文件 58-C** |
|  | **2016年10月24日** |
|  | **原文：英文** |
|  |
| 电信标准化局主任 |
| 第三届全球标准专题研讨会的结论 |
|  |
|  |

|  |  |
| --- | --- |
| **摘要：** | 本报告总结了第三届全球标准专题研讨会的结论 |

第三届全球标准专题研讨会的结论

2016年10月24日在突尼斯哈马马特举行了第三届全球标准专题研讨会，标准化领域的思想领袖会聚一堂，就如何在标准工作中最好地考虑到安全性、隐私和信任问题展开了讨论。

# 1 引言

全球标准专题研讨会（GSS）是高级别标准化政策辩论，探讨信息通信技术（ICT）的发展动态以及技术标准化的相关影响。GSS在国际电联四年一度的世界电信标准化全会（WTSA）拉开帷幕后举行。前两次会议于2008年在约翰内斯堡和2012年在迪拜举行。

实践证明，GSS-12的主题恰当其时，即：ICT行业与医疗、公用事业和运输等其他行业的交叉领域的标准化，该研讨会的结论为国际电联2013年至2016年开展的标准化工作提供了宝贵的指导意见。GSS-12讨论了诸如医疗数据的无线传输、联网车辆移动数据的存储以及网上零售商对消费者数据的收集等议题，并同时探讨了ICT基础设施和业务的安全性、隐私和信任问题。在此类环境中，需要标准化的框架来确保业务具有可信的安全属性，同时亦对用户的安全和隐私需求加以保护。

第三次全球标准专题研讨会（GSS-16）讨论了对此感兴趣的利益攸关方如何开展合作，以开发有关安全、隐私和信任的国际框架问题。该研讨会汇集了安全、隐私和信任领域的专家翘楚，他们分别代表了政府、监管机构、标准机构和业界。与会者就以下问题交换了意见：上述框架的关键要素；国际电联在2017年至2020年期间开展的相关标准化工作中应优先考虑上述哪些要素。

突尼斯共和国通信技术和数字经济部部长**H.E.Mohamed Anouar Maarouf**阁下致欢迎辞。国际电联秘书长**赵厚麟**和国际电联电信标准化局主任**李在摄**分别致开幕辞。研讨会由突尼斯前ICT部长**Mongi Marzoug**主持。

紧随开幕式之后的三节会议从监管与政策、行业和标准化的角度对研讨会的主题进行了探讨。本报告第2节在联合国系统框架下对GSS-16的主题进行了审议，第3节则总结了研讨会各节会议的主要结论和建议。GSS-16所有讨论的详细摘要见附录一。

活动安排、演讲人简介、演讲内容和网播可查阅GSS的网站：
<http://itu.int/en/ITU-T/wtsa16/gss/>。

根据第122号决议（2010年，瓜达拉哈拉）和国际电联理事会第1272 (MOD)号决议，将本报告详述的GSS-16的有关结论转呈WTSA‑16审议。

# 2 ICT中的安全、隐私和信任 – 联合国框架

ICT令数十亿人得以在全球范围内交换数字信息。对此类技术的使用严重依赖于技术标准，这在通信的隐私和安全以及终端用户对ICT的信心方面带来了一系列挑战。

作为一家致力于制定隐私友好的自愿国际ICT标准[[1]](#endnote-1)的标准制定组织以及政府间组织，国际电联致力于在ICT使用方面树立信心和提高安全性[[2]](#endnote-2)。信息社会世界峰会赋予国际电联作为有关国际电联成员国和其他利益攸关方之间合作的C.5行动方面的推进方的责任，以“利用ICT使用安全领域内的互补和相互强化举措以及针对隐私、数据和消费者权益保护的举措或指导方针，进一步加强信任和安全框架”。

保护隐私的规范性国际依据主要以人权条约为准，例如1948年的联合国《世界人权宣言》[[3]](#endnote-3)和1966年的《联合国公民权利和政治权利国际公约》[[4]](#endnote-4)，这两项条约均包含了有关隐私权/私人生活的条款（分别为第12条和第17条）。不过，上述公约并未明确提及个人信息的数字处理问题，此概念在联合国系统框架下仅以一种不具约束力的指导文件形式加以处理，即1990年的联合国《电脑个人数据档案的管理准则》[[5]](#endnote-5)。

尽管一些具有法律约束力的国际公约确实包含了有关隐私权的条款，如欧洲委员会《关于个人数据自动处理的个人保护公约》[[6]](#endnote-6)、《欧洲人权和基本自由公约》[[7]](#endnote-7)以及《美洲人权公约》[[8]](#endnote-8)，但此类法律文书均是在区域而非全球基础上制定和通过的。许多此类区域性协议以相同的基本隐私原则为基础，例如个人的知情同意概念以及在处理个人信息之前所采取的安全措施的充分性[[9]](#endnote-9)。

不同利益攸关方已开始呼吁对个人信息处理方面形成全球共识的必要性给予更多关注。例如，国际数据保护和隐私委员会会议呼吁a) 联合国编制一份具有法律约束力的“在处理个人数据方面保护个人的全球公约”；b) 国际组织“承诺遵守与有关数据保护和隐私的主要国际文书相一致的原则”；及c) 硬件和软件制造商，“开发集成了隐私增强技术的产品和系统”[[10]](#endnote-10)。

联合国大会第68届会议（2013年）通过了一项题为“数字时代的隐私权”的决议，决议呼吁所有联合国会员国“尊重并保护隐私权，其中包括数字通信方面的隐私权”[[11]](#endnote-11)。根据该决议，联合国人权理事会任命了一名特别报告员，其任务是，除其他外，对涉嫌侵犯隐私权的行为进行报告，其中包括与新技术带来的挑战有关的侵犯行为。

# 3 GSS-16的主要结论

## 3.1 安全、隐私和信任的监管原则

忆及隐私和数据保护是个人和社会的核心价值，《世界人权宣言》将隐私作为一项基本权利；

注意到当前生活的方方面面几乎均依赖于ICT基础设施和业务，因此，若不能维持此类基础设施和业务的可信性，则我们的生活便会受到影响；及，

认识到数据泄露和安全事件的发展呈惊人态势，这对人们的信任产生了不利影响，

GSS强调：

• 利用包含安全、隐私和信任基本原则的**国际框架**，并建立实施此类原则的机制。

• 促进遵守**隐私设计的原则、开展隐私影响评估并发展隐私增强技术（PET）**的采用，将此类技术集成到ICT基础设施和业务中将尽可能减少对个人身份信息的处理。

• 确立**公共和私营部门之间**就ICT基础设施和业务面临的威胁、最佳做法和减轻战略**共享信息**的手段。

• 动员国际社会并建立伙伴关系，以在为防止网络攻击方面**建设国家能力**，以提高各国检测安全事件的能力，并对此类事件做出协调一致的反应。

• 在保护个人隐私的需要和鼓励**以创新方式使用数据**来促进数字经济发展之间建立平衡。一旦将其融入新技术和业务，良好的隐私与安全做法将成为吸引客户的卖点，并为改进整个网络做出贡献。

• 为制定**旨在解决全球性问题的国际标准**贡献力量，并认识到网络攻击是无视国家边界的行为，对隐私和安全的侵犯将破坏用户对ICT的信任，故而有必要在国际层面建立标准化的安全框架，以确保业务的安全属性确凿可信，同时有必要对用户的安全和隐私进行跨境保护。

• 促进为**个人数据‘去除标识’**和**数据便携性**制定**标准**，以便为更好地保护消费者并为提升消费者签约或取消ICT服务的能力做出贡献。

## 3.2 业界如何达到终端用户对安全、隐私和信任的预期？

重申ICT及数字化在改善我们的生活和社会方面的巨大潜力；

认识到安全漏洞、侵犯隐私权和对ICT基础设施和业务缺乏信任可能会对企业的业务和声誉构成严重威胁；及，

呼吁采用具有可实施性的国际标准，

GSS强调：

• 支持并促进**透明度**和**技术完整性**原则。与会者承认没有透明度就不可能有信任，用户应有能力了解其数据如何被使用，并就其是否接受此类使用做出决定。技术完整性有助于满足对ICT基础设施和业务的强大安全性的需求，提倡采取隐私措施，并拒绝接受隐藏性的功能设计，以杜绝未经授权的信息修改，同时建立对信息的准确性、完整性和可靠性的信任。

• 使用安全标准来减轻**物联网僵尸网络**带来的风险。在大规模分布式拒绝服务（DDoS）攻击中，滥用物联网（IoT）设备的报案数正在与日俱增。此类攻击可能会导致数据泄露，并给受影响的机构造成重大经济和声誉损失。因此，需要对轻量级加密和标准化安全方法等领域的技术进步加以研究并对其善加利用，以便在有限的计算能力下实现高水平的安全性。

• 评估**量子计算**对安全性、隐私和信任的影响，并对**量子安全技术**加以研究。尽管量子计算仍处于起步阶段，但人们普遍认为，一旦此类技术的实用性得到提高，则当下旨在保护在线支付、银行交易及电子邮件和电话呼叫的传统加密方法很快便会显得力不从心。在我们的系统被此类攻击抓到漏洞之前，便应及早着手对量子计算的影响加以评估，并对抵抗量子攻击的新安全方案进行研究、测试、推进标准化及制定相关过渡方案。

## 3.3 标准组织解决安全、隐私和信任问题的方法

认识到标准在确保安全、保护隐私和建立对ICT基础设施和业务的信任方面发挥的关键作用；

强调安全、隐私和信任是许多处理ICT和其他技术领域的国际标准组织的既定工作领域；及

呼吁实现标准化，以应对安全、隐私和信任方面的挑战，

GSS强调：

• 支持**隐私设计**的思维方式，并在整个标准制定过程中适当考虑隐私因素。隐私设计可以通过包含隐私和数据保护特征的标准来促进，而标准亦可有效确保隐私特征之间的互操作性。

• 了解**开源软件**在应对安全、隐私和信任挑战方面的作用。开源软件和标准对ICT行业的增长和创新起到了锦上添花的作用。软件正变得日益复杂，开源和标准化社区正在许多领域进行合作，应进一步促进此类社区之间的工作交流，从而确保高质量和高安全的软件部署。

• 在标准机构之间就制定国际安全、隐私和信任框架**加强合作**，并认识到其任务和优势，同时充分利用既已开展的工作。标准机构应遵循标准制定的正当程序、广泛共识、透明度、平衡度和开放性；致力于技术优势、互操作性、竞争、创新和惠及全民；让所有人都能用上标准；以及自愿采用标准。标准机构还应携手努力解决发展中国家和发达国家在获得和实施处理ICT基础设施和业务的安全、隐私和信任的标准和框架方面的差距，并平等参与其发展。

**附录I
GSS-16讨论内容的详细摘要**

（本附录并非本报告不可分割的组成部分）

GSS-16发言稿的详细摘要将纳入本文件的修订1

**尾注**

1. 例如，参见ITU-T X.1171建议书“在采用基于标签识别的应用中对保护个人可识别信息的威胁和要求” [↑](#endnote-ref-1)
2. 例如，参见全权代表大会第130号决议（2014年，釜山，修订版）– 加强国际电联在树立使用信息通信技术（ICT）的信心和提高安全性方面的作用； [↑](#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. 例如，参见APEC隐私框架和欧盟的隐私监管框架，这些框架在一定程度上受到OECD《保护个人数据跨境传送隐私权导则》的启发<http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> [↑](#endnote-ref-9)
10. 蒙特勒国际数据保护和隐私委员会会议的宣言，[https://icdppc.org/wp-content/uploads/2015/02/ Montreux-Declaration.pdf](https://icdppc.org/wp-content/uploads/2015/02/%20Montreux-Declaration.pdf) [↑](#endnote-ref-10)
11. 联合国大会第68/167号决议，<http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167>

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [↑](#endnote-ref-11)