|  |  |  |
| --- | --- | --- |
| 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(Rev.1)-C** |
|  | | **2016年10月27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（GSS）的结论。本文件修订1的附录一包含GSS的所有发言摘要。 |

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。

**附录一**

**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）

第1节会议：欢迎辞和主旨发言

**Mohamed Anouar Maarouf**阁下（突尼斯共和国通信技术和数字经济部长）[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Maarouf)]向所有与会者表示热**烈**欢迎并感谢国际电联成员选择将突尼斯哈马马特作为全球标准专题研讨会（GSS）和世界电信标准化全会（WTSA）的会址。他强调有必要树立对ICT基础设施和服务的信心和信任，同时认识到GSS-16主题（标准化中的安全、隐私和信任）的重要性。

在开幕辞中，GSS-16主席**Mongi Marzoug**（突尼斯前ICT部长）[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Marzoug)]对所有与会者莅临突尼斯表示欢迎，并预祝他们在哈马马特生活愉快。他强调了突尼斯在建设信息社会中发挥的作用并阐述了信息通信技术（ICT）对当下的日常生活和未来的重要意义。他强调了开放、安全、可靠和可信的ICT业务对促进全球各行各业（例如医疗、金融、公用事业、物联网）发展的重要意义。他指出，在此方面，标准化可以发挥重要作用，以提高ICT的安全性、保护隐私和帮助公民、政府和企业树立对ICT业务的信任。他强调，第三次GSS旨在介绍和讨论三大利益攸关方（政府和监管机构、业界和标准化机构）在解决ICT基础设施和业务的安全性、隐私和信任问题方面发挥的作用，并就上述议题向WTSA-16提出结论和建议。

**赵厚麟先生**（国际电联秘书长）[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Zhao)]感谢GSS和WTSA东道国突尼斯共和国对国际电联工作的支持。在介绍之前历届GSS作出的积极贡献时，他阐述了GSS如何作为国际平台将公众和私营部门领导者云集一堂就标准化政策开展辩论，使技术标准顺应ICT行业的发展重心。GSS-08和GSS-12都为国际电联标准化工作计划的制定发挥了根本性作用。他亦指出，可信赖的ICT环境将使用户和企业在充分使用ICT中充满信心。国际电联标准化工作在国际电联履行其“树立使用ICT信心并提高安全性”的职责中发挥了重要作用。最后，他向所有发言人、主持人和与会者对GSS-16做出的贡献表示感谢。

国际电联电信标准化局主任**李在摄**[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Lee)]在欢迎辞中表示，未来网络需要支持大量ICT应用和极其广泛的业务。数十亿部联网设备、事物和对象将使系统得以在彼此之间进行通信和学习，并创造使行为适应效率需求的智能生态系统。下一代通信所涉及的应用将横跨话音、视频、工业机器人、智能交通、远程医疗手术和虚拟现实等领域。李博士指出，ICT的日益复杂及其史无前例的无处不在规模将要求网络基础设施和业务发生重大转变。随着社会方方面面的经济和社会活动几乎均将依赖于ICT，我们必须建设值得我们信任的ICT基础设施和业务。他突出了技术标准在防止不同行业出现数据“孤岛”中发挥重要作用并指出，参加国际电联标准化工作的专家正在努力支持打造一个共用和整合的数据生态系统。

第2节会议：安全、隐私和信任的监管原则

本节会议介绍了安全、隐私和信任的监管原则，会议主持人为国际电联电信标准化局研究组主任**Bilel Jamoussi**[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Jamoussi)]。

在其主旨发言中，**John Edwards**（新西兰隐私问题专员兼国际数据保护和隐私问题专员会议执行委员会主席）[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Edwards)]认识到以往相互分离的机构正在逐步快速走向协商一致。他们一致认为，隐私已成为这一时代的关键问题之一。Edwards强调指出，2013年联大第68届会议通过了一项题为“数字时代的隐私权”的决议，呼吁所有联合国成员国“尊重并保护隐私权，其中包括数字通信方面的隐私权”。他介绍了其所代表的组织国际数据保护和隐私权委员大会（ICDPPC）所开展的工作并就通过在电信行业实施隐私权原则以及制定标准增强信心和信任提出了一些想法：

– 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

– 确保国家机构对网络、系统、内容、通信和原数据的接入只能在必要的情况下，在适当范围内按照合法机构的规定进行。

– 加强个人数据在用于数据主题以外时的接入或使用透明度。

– 制定并推广适当的标准，保障个人数据“去除标识”，防止通过去除标识的数据集对个人进行重新标识。

– 为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。

– 确保公民和消费者继续掌握作为对其产生影响的自动化决策的基础的透明度。

**Victor Manuel Martinez Vanegas**（墨西哥联邦电信研究所国际政策主任）[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Vanegas)|[发言](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GSS_IFT_Draft_Presentation.pdf)]在发言时从全球角度探讨了GSS主题，并讨论了在区域层面采取的举措，同时介绍了旨在实现ICT安全、隐私和信任的国家框架。

他表示，ICT的发展和普及对经济和社会发展有着积极影响，但亦带来可能会危及上述利益的威胁和挑战。安全、隐私和信任已成为须以适当方式加以解决的关键问题。他在演讲中援引了相关出版物、宣言和协议中的内容，其中包括联合国大会、ITU-T和IEC的标准化活动以及联合国贸易和发展会议（UNCTAD）2015年信息经济报告，该报告断言：“安全和信任在为电子商务营造有利环境方面必不可少”。Martinez Vanegas先生指出，他所在的拉丁美洲和加勒比区域是世界上互联网用户增长最快的区域，解决ICT的安全、隐私和信任问题对该区域的经济和社会发展至关重要。他还强调，该区域的经验表明，任何国家仅靠一己之力均不能充分保障网络安全，因此，合作是必不可少的。

**Ilias Chantzos先生**（赛门铁克公司欧洲、中东和非洲政府事务高级主管兼全球CIP及隐私问题顾问）[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Chantzos)|[背景文件](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/InternationalCyberNorms_Ch10%20-%20Symantec.pdf)]介绍了政策和监管驱动因素与技术进步之间的相互影响方式，并援引了欧盟的一般数据保护法规，同时指出此类法规是上述相互影响关系的最直接例子之一。现有的隐私指令已实行逾20年，必须对其加以大幅度调整，以体现演进或革命、技术和其他因素（如社交媒体）。反之，当前在使用技术和社交媒体时必须遵守新的法规，而公共和私人组织将推动其数据治理（包括保护个人数据免受网络攻击）的方式发生根本性变化。Chantzos还介绍了技术完整性理念。该理念有助于满足对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。

坦桑尼亚通信管理局（TCRA）代理局长**James M. Kilaba先生**强调[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Kilaba)|[发言](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GSSWTSA2016-Kilaba.pdf)]强调了技术从仅有少数个人计算机连接上网到当今任何人、任何事物随时随处通信的变革中产生的安全和隐私挑战。他介绍了为保护隐私、安全数据和ICT基础设施在国家和区域层面采取的举措。这些举措包括建立国家计算机应急响应小组（TZ-CERT），以便向不同利益攸关方传播有关网络安全的知识、信息和技能；在域名注册系统中实施DNSSEC并在东非通信组织（EACO）中探讨网络安全问题。Kilaba呼吁以全面的视角应对这些挑战并突出了为支持发展中国家而统一国际标准的必要性。

**Chawki Gaddes先生**（突尼斯保护个人信息国家管理局主任）[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Gaddes)|[发言](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GSS-Gaddes.pdf)]介绍了突尼斯通过立宪在保护隐私和个人数据（2014年，第24条）、信息和通信网络接入（2004年，第32条）和政府文件的获取（将于2017年生效）方面发挥的领先作用。他强调，突尼斯高度重视营造公民、私营部门和政府之间的信任。

第3节会议：业界如何达到终端用户对安全、隐私和信任的预期？

**Ilias Chantzos先生**（美国赛门铁克公司欧洲、中东和非洲政府事务高级主管兼全球CIP及隐私问题顾问）主持了关于行业如何满足监管原则和终端用户对安全性、隐私和信任期望的双议题会议。

**Ammar Alkassar先生**（德国Rohde & Schwarz公司网络安全部首席执行官）[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Alkassar)|[发言](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/3-1201601024_ITU%20GSS16_ALKASSAR_2.pptx)]概括了将以可持续方式改变世界的ICT发展趋势。他阐述了网络安全如何在变革中作为关键驱动力并在未来发挥更加重要的作用。Alkassar指出，当今部署的安全手段与其所保护的经济价值相比相距甚远。他认为有必要根据IT安全局势的变化确定一套新的标准以便应对日益狡诈的威胁环境。根据Rohde & Schwarz的情况，这一格局的变化将包含以下要素：通过设计将安全落实到位，与其回应不如采取防范措施；加强信息流控制而不是接入控制；并在网络安全方面免除用户无法履行的责任。他指出，国际电联在此领域大有作为，尤其是通过其开展的标准化工作，将传统的电信业与新的ICT力量结合起来。

**Thomas Kremer博士**（德国电信负责数据隐私、法务和合规事务的管理董事会成员）[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Kremer)|[发言](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Deutsche%20Telekom%20-%20final.pptx)|[背景文件](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Getting%20out%20of%20the%20digital%20trust%20trap%20-%20deutsche%20telekom.pdf)]强调透明度是信任的先决条件。人们必须能够知道他们的数据如何被使用，并能够有意识地决定其是否接受这样的使用。不过，如企业希望履行其数字责任，仅有透明度通常是不够的。Kreme r博士呼吁在各类无需直接获取个人资料的情况下采用可以对数据进行稳妥匿名化处理的系统。他认为加密是建立客户信任的另一种手段，在诸如健康数据等敏感数据的情形下这一点尤其重要。德国电信认为，任何向政府官方提供“备用密钥”或“后门”以保护系统的建议最终均会产生适得其反的效果，并会给安全工作造成破坏，原因是上述“备用密钥”或“后门”将迅速成为对手进行网络攻击的软肋。Kremer博士呼吁在网络安全领域采用智能、可用和及时的解决方案。随着新技术（物联网、机器学习、量子计算等）的出现，攻击将变得更加复杂。因此，需要采用标准化的方法来检测和减轻风险与攻击。

**David Francis先生**（中国华为公司欧洲网络安全官）[简历|发言]从技术厂商角度解释了保护隐私和安全的原因所在。他讨论了诸如华为这样的公司在确保其产品的安全性和灵活性方面的政策和流程，而这将最终有助于保护终端用户的隐私和数据。以全局方式考虑的关键要素包括：安全设备：架构 – 网络是由多重复杂产品以及实施、管理、升级、修复和接入环境的人构成的。Francis先生阐述了全球供应链管理的必要性，原因是信息技术部门完全依赖于此类供应链来减轻各类安全风险；此外，他还阐述了透明度和全球标准的作用，并指出需要开展国际合作，以提高全球网络的安全性。

**Jaya Baloo女士**（荷兰KPN公司首席信息安全官）[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Baloo)|[发言](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/3-4ITU-GSS-Tunesia.pdf)]讨论了从量子计算到量子加密的量子技术竞赛问题。量子计算机的面世将对依赖于非对称加密（RSA、ECC）的国家和企业带来安全风险。必须做出的响应是分三个阶段的后量子解决方案。第一，增加目前加密算法的秘钥长度。第二，在网络的具体关键点使用量子秘钥分配。第三，创建并支持满足未来需求的后量子加密算法。全球信息安全界围绕量子技术创新取得了长足进步。然而，这种情况可能会带来新的数字安全鸿沟，使具有财务和学术资源的国家在拥有量子计算机保护自身通信的同时破解其它国家的加密，而另一些国家则既无攻击之力又无防范之功。

**James Snow先生**（美国谷歌公司安全与合规战略师）[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Snow)|[发言](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Google-final.pptx)|[背景文件](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GoogleExecSummary_2016.pdf)]指出，谷歌公司的优先要务之一是：在安全、可靠和合规的环境中处理数据，并以此来获得及保持客户的信任。安全性和隐私权对谷歌公司至关重要，因此该公司正在加大投资，以对客户数据加以保护。相关举措包括使用安全的专用服务器和网络基础设施以及对客户数据进行加密，而这与数据是存储在磁盘上、备份介质上、在互联网上移动还是在数据中心之间流转无关。

Snow先生表示，客户信任始于理解，而理解只能通过透明度来创造，例如提供详细的文档、审计报告和认证。谷歌公司认识到国际合作的重要性，并一直在利用若干国际安全和隐私标准，其中包括：

– ISO 27001：2013，信息技术 – 安全技术 – 信息安全管理系统 – 要求

– ISO 27017：2015，信息技术 – 安全技术 – 基于ISO/IEC 27002的云计算业务信息安全控制行为准则

– ISO 27018：2014，信息技术 – 安全技术 – 公共云中作为PII处理器的个人识别信息保护的行为准则 (PII) ；和

– SOC 2/SOC 3 – 包括安全性、可用性、处理完整性和保密性在内的非隐私原则的审核框架。

**杜跃进博士**（中国阿里巴巴集团安全部副总裁）[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Du)|[发言](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Yuejin-DU.pptx)]阐述了安全和隐私在阿里巴巴为客户提供的商用和数据技术基础设施中的重要意义。例如，阿里巴巴正在为伙伴提供信息安全产品并通过2016年创立来的电子商务生态系统联盟（EESA）推广标准。阿里巴巴及其伙伴利用EESA中已建立的风险检测模型来检查和识别威胁并通过实施已建立的联盟标准共同提高电子商务生态系统的安全性并为隐私提供保护。

**Bernard Benoit**先生（瑞士WhiteNoise/Kudelski安全技术公司总经理）[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Benoit)|[发言](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Kudelski%20-%20final.pdf)]指出，用户、业务提供商和政府之间可能存在利益冲突，而现有的电信网络则安全漏洞百出，因此通信的安全和隐私便无法得到保证。为在不可信网络上提高安全性并加强隐私保护，他提出了一种可扩展的基于OTT方法的硬件安全组件，该组件可独立于底层网络和协议运行。Benoit先生亦向听众阐明了采用与平台无关的解决方案的必要性，指出此类解决方案需要配备标准化接口，以满足适用的合法拦截要求，且不会通过后门和备用密钥等来危害技术的完整性。

第4节会议：标准组织解决安全、隐私和信任问题的方法

第4节会议审议了不同标准制定组织（SDO）在安全、隐私和信任方面所采取的方法。本节会议由**Toni EID先生**（《电信评论》主编）主持[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Eid)]。

**Sophie Clivio女士**（国际标准化组织（ISO）标准化和技术政策主任）[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Clivio)|[发言](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/ISO%20-%20final.PPTX)]介绍了ISO在安全、隐私和信任方面采取的广泛和多部门联动方法。她着重介绍了ISO委员会有关安全性和灵活性的工作；风险管理；区块链和电子分布式账本技术；以及在信息技术联合委员会（ISO/IEC JTC 1）中有关信息安全和隐私的联合ISO/IEC活动。JTC 1涵盖的主要领域包括信息安全管理、加密和安全管理、身份管理和隐私技术；生物识别；卡片和个人身份证；信息技术治理；用于云计算、大数据和物联网的安全、隐私和信任机制。Clivio女士指出，ISO及其标准在医疗、运输（例如航空、智能交通系统和海洋技术）、能源、建筑、制造（包括增材制造）等经济部门得到了普遍采用，该组织还与其他组织签署了合作协议，以应对上述部门的某些特殊需求。

**Frans Vreeswijk先生**（国际电工委员会（IEC）总干事兼首席执行官）[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Vreeswijk)|[发言](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/IEC%20-%20final.pptx)]介绍了IEC如何将电子技术领域利益攸关各方团结起来以便通过使用IEC的国际标准和IEC一致性评定系统建立对安全和高校产品和系统的信任。IEC已发表了200多项网络安全标准，尤其重视保护诸如发电和配电、水和废物管理、医院和医疗、制造和数据中心等关键基础设施免受网络攻击的标准。IEC还为所有电子和电器硬件的安全提供根本的保护方式，以确保数据收集或接入和控制协议行之有效，例如，传感器、医疗设备、可佩带智慧设备以及计算和数据存储技术。IEC的国际标准成为改进复原力、风险管理和提供效率的关键驱动要素。

IEC与ISO通过信息技术联合委员会（ISO/IEC JTC1）在诸如信息安全管理、身份管理、加密和安全识别、隐私技术、生物特征卡和个人识别、云计算、大数据等领域密切合作。IEC与国际电联以及ISO在世界标准合作组织中长期保持友好关系。

MVreeswijk呼吁所有标准机构扩大合作以应对安全、隐私和信任问题。总之，单枪匹马无法提供该领域需要的所有标准。

**Karen McCabe女士**（IEEE标准协会（IEEE-SA）技术政策和国际事务高级总监）[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#McCabe)|[发言](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/IEEE-final.pptx)]强调，标准在帮助确保安全和隐私以及实现对ICT的信任方面可发挥关键作用。为发挥上述作用，最佳做法是按照一系列原则来开展工作，以便为有关各方和利益攸关方之间的自愿合作提供全球性社区，同时实现技术卓越、全球互操作性和创新。此类原则包括：直接参与；正当程序；广泛共识；平衡；透明度；普遍开放；相干性；发展维度。

她指出，从安全角度来看，开放流程是很好的做法，原因是由多个专家进行审查有助于发现潜在的缺陷及对开发中的标准加以完善。开放标准制定过程的透明度可促进对基于和遵守此类标准的平台、服务和产品的信任。此外，开放标准亦令隐私和安全增强技术得以广泛采用，原因是此类技术可提高互操作性。她的结论是，开放标准将推动创新，而创新则可推动能够应对安全性、隐私和信任方面挑战的解决方案的出台。

IEEE的产品组合包括了广泛的标准，其中包括IEEE 802系列网络标准中的安全性、隐私和信任技术；IEEE 1363系列标准、IEEE 1619系列标准和许多其他标准中的加密技术（重点是基于公钥基础设施（PKI）的算法）。IEEE的工业连接安全组（ICSG）包括多家计算机安全实体，这些实体通过协作来汇集经验和资源，以应对系统性和高发性的计算机安全威胁。近期的另一项工作为IEEE的互联网倡议，其目的是在互联网治理、网络安全和隐私政策制定领域提高该组织在全球技术政策方面的影响力和形象，为此，该组织将为有关工作提供已达成共识的可靠技术和科学知识及指导意见。IEEE有关自主系统设计中的伦理因素全球倡议及其伦理、社会和技术特设委员会正在对新的标准和解决方案、认证和行为准则以及在伦理层面实现智能技术（其中包括人工智能和自主系统）的共识达成问题进行研究。

随后，McCabe女士呼吁在标准制定过程中纳入跨学科的新一代隐私、安全和道德专业人员，并将隐私、安全和道德建设纳入开放标准，以增进对ICT的信任。

**Ashok Ganesh先生**（CEN-CENELEC创新总监）[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Ganesh)|[发言](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/CEN-CENELEC-final.pptx)]强调，所有行业部门均在经历转型，原因是采用数字技术和方法（例如物联网、云计算、机器人和传感器技术）从根本上改变了上述部门的流程、系统乃至商业模式。此类传统意义上的垂直行业（例如制造业、能源、运输）在过去并非ICT和数字技术的重要用户，但它们目前却希望为其转型提供支持和标准化解决方案。Ganesh先生指出，ISO、IEC、CEN和CENELEC等标准制定组织在欧洲的上述垂直行业中留下了明显的“足印”，并希望为此开发特定的方法来满足此类ICT/数字相关需求。此类技术的采用涉及工业厂房和制造流程系统的使用以及大量数据的产生、处理、共享和存储。Ganesh先生指出，标准化组织面临的挑战是多方面的：既要保持传统利益攸关方的参与，吸引ICT/数字利益攸关方，又要能够修正自身的方法，以能在日益复杂且迅速发展的领域直接或间接提供标准化解决方案。标准制定组织应优先关注垂直需求和应用，其中包括处理网络安全和功能安全、产品可靠性、数据安全性和隐私之间的联系。

**Reinhard Scholl博士**（国际电联电信标准化局主任代表）[[简历](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Scholl)|[发言](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Reinhard-final.pptx)]提醒所有与会者，在巴西弗洛里亚诺波利斯WTSA-04曾举办了有关网络安全的专题研讨会。此项活动传递了11条关键信息，这些信息多数依然有效，如，“安全必须内置而不能滞后”，或“利益攸关方应分享信息”以及“标准化是全球网络安全工作的重要组成部分”。

为显示当今状况，他提供了有关国际电联网络基础设施已知安全事件数量信息。他指出，在他看来，安全和隐私彼此并不排斥。他还表示，国际电联还在继续加强有关建立使用ICT的信心和提高安全性的工作，以促进实现更安全的网络基础设施、业务和应用。他介绍了国际电联近期在安全和信任领域开展的工作，其中包括一份强调在ICT背景下信任的重要性和必要性的报告，并介绍了信任的相关概念和主要特征。报告中讨论的一项议题为“信任指数”。该数值将多项信任相关指标结合为一个基准措施。信任指标可以用来在利益攸关方创建新的信任关系或信任价值链时比较相互之间的信任。

Scholl博士指出，国际电联成员已启动相关工作，以研究信任配置方面的需求、能力和服务方案；可信电信网络的架构框架；信任配置方面的技术解决方案；大数据分析中的信任配置；云间信任管理；并在ITU-T建议书中纳入上述问题。其他相关的ITU-T标准化工作涉及的领域包括：网络安全；安全管理；安全架构和框架；打击垃圾信息；身份管理；保护个人身份信息等。Scholl还建议研究开放源界可对解决ICT基础设施和服务安全、隐私和信任问题的标准做出的贡献。他表示，应进一步努力为开放源和标准界之间的交流提供便利，由此确保高品质的标准和软件实施。

**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)