|  |  |  |
| --- | --- | --- |
| itu_logo | **国 际 电 信 联 盟****电信标准化局** |  |
|  |  |

 2016年4月4日，日内瓦

|  |  |  |
| --- | --- | --- |
| 文号：电话：传真： | **电信标准化局第214号通函**SG17/MEU+41 22 730 5866+41 22 730 5853 | – 致国际电联各成员国主管部门 |
| 电子邮件： | tsbsg17@itu.int | **抄送：**– ITU-T部门成员；– ITU-T部门准成员；– 国际电联学术成员；– ITU-T第17研究组正副主席；– 电信发展局主任；– 无线电通信局主任 |

|  |  |
| --- | --- |
| 事由： | **第17研究组会议按照世界电信标准化全会（2012年，迪拜）第1号决议第9节的规定批准X.1258 (ex X.eaaa)、X.1542 (ex X.simef)和X.1641 (ex X.CSCDataSec)建议书草案，2016年9月7日，日内瓦** |

尊敬的先生/女士：

1 应第ITU-T17研究组（安全）主席的请求，我荣幸地告知您，该研究组将于2016年8月29至9月7日召开会议，并将采用世界电信标准化全会（2012年，迪拜）第1号决议第9节规定的程序来批准上述建议书草案。

2 建议批准的ITU-T建议书草案的标题、摘要及其出处见**附件1**。

3 所有了解自己或他人持有的专利可能整体或部分地涉及建议批准的建议书草案内容的国际电联成员国、部门成员、部门准成员或学术机构，均需按照ITU-T/ITU-R/国际标准化组织（ISO）/国际电工委员会（IEC）的共同专利政策，向电信标准化局披露此类信息。

可通过ITU-T网站（[www.itu.int/ipr/](http://www.itu.int/ipr/)）在网上获取已公布的专利信息。

4 考虑到第1号决议第9节的规定，请您在2016年8月17日协调世界时24时之前告知我，贵主管部门是否同意授权ITU-T第17研究组在该研究组会议上审议并批准上述建议书草案。

如有成员国认为不应进入审议批准程序，应阐明其反对原因并提出可能的修改意见，以推动对相关建议书草案的进一步审议，以便批准。

5 如果70%以上的成员国在回复中支持在该研究组会议上审议批准上述建议书草案，则将于2016年9月7日召开一次全体会议，实施该批准程序。

为此，我邀请贵主管部门派出一名代表参加会议。**请国际电联成员国的主管部门提供其代表团团长的姓名。如果贵主管部门希望由一家经认可的运营机构、一个科学或工业组织或处理电信问题的另一实体作为代表参加会议，则应按照国际电联《公约》第19条第239款的规定，将有关情况适时向主任通报。**

6 有关第17研究组会议的议程和所有相关信息将在ITU-T第8/17号集体函中提供。

7 会后，电信标准化局主任将以通函的形式通报就这份建议书做出的决定。此信息还将在《国际电联操作公报》中公布。

顺致敬意!

电信标准化局主任
李在摄

**附件：1件**

**附件1
（附于电信标准化局第214号通函）**

案文摘要和出处

# 1 ITU-T X.1258 (ex X.eaaa)新建议书草案([R 64](http://www.itu.int/md/T13-SG17-R-0064))

**基于聚合属性的增强型实体验证**

摘要

可能确有必要利用多属性机构提供的聚合属性，提升依赖方对其它方身份的信任度。聚合可视作必须处理一系列适用于全局的唯一标识符，这在所有属性机构之间十分常见。实践过程中，各实体并无全局统一的标识，而是拥有不同的实体标识和其它各种实体业务提供商（IdSP）分配的属性。为解决此方案中的属性聚合问题，本文使用了身份联盟的概念。例如，若某网上书店计划向老年人出售产品，则该商店必须由IdSP分配一套聚合属性（信用卡和年龄段），但各IdSP之间相互并不了解对方的参与情况。在标准的联盟身份管理中，某实体只能提供来自一个身份的属性，但此交易要求两个实体均提供属性。目前存在多种身份联盟方法，例如安全断言标识语言 (SAML)、Shibboleth [b-Shibboleth]、公开身份（OpenID）和公开鉴权（OAuth）等。ITU-T X.1258 (X.eaaa)建议书引入了属性聚合概念，使实体能够聚合来自多个IdSP的属性。属性聚合是一种收集某实体从多个身份服务提供商那里检索到的属性的机制。属性聚合可用于按需动态汇聚各种属性。当某实体希望获得服务时，IdSP可实现聚合请求。此外，以实体为中心的属性聚合机制亦可用于缓解隐私泄露的鉴权。

# 2 ITU-T X.1542 (ex X.simef)新建议书草案([R 61](http://www.itu.int/md/T13-SG17-R-0061))

**会话信息的消息交换格式**

摘要

在当今的网络环境下，计算机网络可能同时会受到来自组织内外的威胁。防火墙系统负责记录选定的出入向传输控制协议/互联网协议(TCP/IP)连接的会话信息。但是，目前提供的这些系统通常无法实现互操作，因为各系统均有自身独特的功能、控制机制和会话日志格式。大多数安全管理员现今面临的需求是，在不同防火墙系统甚至是不同基础设施之间保持一致的会话信息交换格式。ITU-T X.1542 (X.simef)建议书阐述了会话信息的消息交换格式（SIMEF）的信息模型，并提供了使用扩展标识语言(XML)方案描述的相关数据模型。SIMEF为分享有关集中式网络安全管理和安全信息交换系统的传输层会话日志信息，定义了一种数据模型表达方法。所有传输协议的规范均不属于本建议书的讨论范围。

# 3 ITU-T X.1641 (ex X.CSCDataSec)新建议书草案([R 63](http://www.itu.int/md/T13-SG17-R-0063))

**云业务客户数据安全性导则**

摘要

ITU-T X.1641 (X.CSCdataSec)建议书为云计算的云业务客户（CSC）数据安全性制定了通用导则。导则分析了CSC数据安全性的生命周期并对数据生命周期内的各个阶段提出了安全要求。此外，建议书就何时应将各种控制应用于最佳安全实践，提出了指导原则。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_