|  |  |  |
| --- | --- | --- |
| The International Teleocmmunication Union - Connecting the World. | **国 际 电 信 联 盟****电信标准化局** |  |
|  | 2021年10月11日，日内瓦 |
| **文号：** | **电信标准化局第349号通函**TSB Events/DA | **致：**- 国际电联各成员国主管部门；- ITU-T部门成员；- ITU-T部门准成员；- 国际电联学术成员 |
| **联系人：** | **Denis ANDREEV** |
| **电话：** | +41 22 730 5780 |
| **传真：** | +41 22 730 5853 |
| **电子邮件：** | tsbevents@itu.int | **抄送：**- ITU-T各研究组正副主席；- 电信发展局主任；- 无线电通信局主任 |
| **事由：** | **国际电联“提升信令协议的安全性”讲习班（完全虚拟式会议，2021年11月29日）** |

尊敬的先生/女士：

1 我高兴地邀请您参加将于2021年11月29日（中欧时间/日内瓦时间）13时-17时以虚拟方式举办的国际电联“提升信令协议的安全性”讲习班。此活动之后将召开[ITU-T第11](https://www.itu.int/en/ITU-T/about/groups/Pages/sg11.aspx)研究组，该虚拟会议将于2021年12月1 — 10日举办。

2 在过去十年中，互联网在全球经济的各个部门得到广泛推广，从而加强了传统电信网络及其基础设施与不同行业之间的联系。

3 由于现有ICT基础设施在设计时没有考虑到互联网的潜在影响，面临着预料不到的攻击。

4 对于不同利益攸关方而言，这些攻击已成为主要优先事项，对于金融机构和运营商尤其如此。

5 为了应对此类漏洞，需要对现有和未来的协议采取一些安全措施。ITU-T第11研究组一直在为此制定一套标准，包括用于支持现有网络与新兴网络的可信赖网络实体之间互连互通的信令架构和要求。此外，ITU-T第11研究组还侧重于为核查使用信令安全网关(SSGW)的、有待插入不同协议的数字证书定义算法，该网关验证其他运营商证书的签名，并且允许或阻止信令数据包。这种方法可以帮助金融机构与其客户建立可信赖的连接。

6 因此，此研讨会的目的是，针对应对现有网络、服务和协议的脆弱性的不同措施交换意见。头脑风暴会议的重点放在讨论加强不同协议安全机制的潜在方法。会议还将讨论实现申请证书方身份验证流程的标准化、可信赖的信令认证机构(TSCA)的颁发进程以及将颁发的证书分发给运营商的必要性。最后但同样重要的一点是，头脑风暴会议还将讨论为此目的而利用现有GT号码（Global Title，GT）颁发进程的可能性。

7 国际电联成员国、部门成员、部门准成员和学术机构以及国际电联成员中愿为此项工作做出贡献的任何个人均可参加此讲习班。这里所指的“个人”亦包括作为国际、区域性和国家组织成员的个人，以及包括电信运营商、监管机构、标准化组织和金融机构在内的相关利益攸关方。参加讲习班不收取任何费用，也不提供与会补贴。讲习班将仅用英文以虚拟方式进行。

8 与此次讲习班有关的所有相关信息，包括日程草案、演讲人、远程连接的链接和注册细节，均将在活动的网站上提供：<https://itu.int/go/WS-SSP>。随着新信息或修订信息的提供，此网站将定期更新。请参会者定期查看最新信息。

顺致敬意！

电信标准化局主任
李在摄