《信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制》（征求意见稿）编制说明

一、工作简况

1、 任务来源

根据2020年8月11日全国信息安全标准化技术委员会下达的“信安字[2020]24号 全国信息安全标准化技术委员会关于2020年网络安全标准项目立项的通知”，GB/T 15843.3-2016《信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制》的修订工作由西安西电捷通无线网络通信股份有限公司承办。该标准由全国信息安全标准化技术委员会归口。

2、 主要起草单位和主要起草人

本标准由西安西电捷通无线网络通信股份有限公司主要负责起草，北京数字认证股份有限公司、公安部第一研究所、国家信息技术安全研究中心、中科院软件研究所等单位共同参与该标准的起草工作。

3、 主要工作过程

1) 2019年12月至2020年3月，标准起草组讨论并确定标准的范围、框架及主要技术内容。
2) 2020年4月至5月，根据ISO/IEC 9798-3:2019标准范围与内容，开展实体鉴别机制的国际标准翻译及编写工作。
3) 2020年5月至6月，标准起草组分工开展草案稿起草工作，形成草案初稿。
4) 2020年7月11日，召开起草组内部评审会征求意见。
5) 2020年8月至9月，根据起草组内征求意见情况，标准起草组经过多次讨论和修订，形成第一版工作组草案稿。
6) 2020年10月27日，参加TC260/WG4工作组组织的专家评审会，标准草案稿通过评审。
7) 2020年11月3日，根据评审会专家意见修改完善标准草案，待TC260会议周讨论。

8）2020年11月9日，参加TC260/WG4工作组会议，会议讨论了标准文本，同意本标准进入征求意见稿阶段。

9）2020年12月3日，根据TC260/WG4工作组会议意见，对标准文本进行了修改，形成征求意见稿。

10） 2020年12月8日，根据TC260/WG4工作组秘书处以及标准责任编辑的意见对征求意见稿进行修改完善并提交。

4、 各阶段意见处理情况

草案稿第1稿阶段，2020年10月27日，TC260/WG4组织专家评审会，共收到两条意见，全部采纳。

草案稿修改稿阶段，2020年11月9日，TC260/WG4工作会议上，共收到三条意见，对其中一条意见做了解释，另外两条意见采纳。

二、标准编制原则和确定主要内容的论据及解决的主要问题

1、 本标准基于以下原则编制：

a）遵循现行国家标准，采用和借鉴国内外先进标准

本标准按国家标准GB/T 1.1-2020规定的格式予以编写。

b）贯彻国家有关政策与法规

本标准中涉及的密码算法遵循国家商用密码的有关规定。

2、 本标准的主要内容

本文件规定了采用基于非对称技术的数字签名的实体鉴别机制。数字签名用于验证实体的身份。

本文件规定了两类机制，第一类共五种机制不引入在线可信第三方，第二类共五种机制引入在线可信第三方。在这两类机制中，分别各有两种机制实现单向鉴别，各有三种机制实现双向鉴别。

附录A规定了分配给本文件所规范的实体鉴别机制的对象标识符。

三、主要试验[或验证]情况分析

本项目对国家标准GB/T 15843.3-2016《信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制》进行修订，增补我国自主提出并已正式在国际标准ISO/IEC 9798-3:2019发布的3项新的实体鉴别机制：三元对等多可信第三方实体鉴别机制、三元对等用户侧发起单向实体鉴别机制、三元对等网络侧发起单

向实体鉴别机制，在无线网络安全技术国家工程实验室、WAPI产业联盟等单位联合研制的样机设备上进行了验证，试验效果良好。

四、知识产权情况说明

本项目等同采用由我国参与制定的国际标准ISO/IEC 9798-3:2019。ISO/IEC 9798-3:2019 标准中涉及西安西电捷通无线网络通信股份有限公司相关专利，专利权人在标准推进过程中已按照ISO/IEC相关要求针对ISO/IEC 9798-3:2019提交了专利声明。

本项目草案涉及西安西电捷通无线网络通信股份有限公司相关专利，专利权人按申请书要求，针对已识别出的专利情况，已随申请书、草案同步提交专利信息披露表和相关证明材料。

五、产业化情况、推广应用论证和预期达到的经济效果

本标准作为基础共性信息安全技术，可广泛应用于电子商务、电子投票、电子身份证、社交网络、可信计算等。可用于确认实体的身份是否是其所声称的身份，其中引入在线可信第三方的机制能够实现两个实体间的对等鉴别；可解决网络通信领域“接入实体没有独立身份，无法保障终端实体和接入实体的对等双向鉴别”的重大问题；适用于物联网、可信计算、局域网和IP网络等领域，能够抵抗中间人攻击、伪造攻击等，可有力支撑我国信息安全产业的发展。

六、采用国际标准和国外先进标准情况

本项目等同采用由我国参与制定的国际标准ISO/IEC 9798-3:2019“IT Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques”，该国际标准中的在线实体鉴别技术都由中国贡献。

七、与现行相关法律、法规、规章及相关标准的协调性

1、 贯彻国家有关政策与法规

本标准中涉及的密码算法遵循了国家商用密码的有关规定。

2、 与相关国内相关标准的关系

本标准与我国现行的法律、法规及国家标准、国家军用标准、行业标准不存在冲突问题。本标准发布后，既可以为相关的行业标准和国家标准的制定提供依据，进而成为政府监管的依准，又可以指导网络平台和设备的设计与开发，为网络的部署、实施与运营提供实体鉴别服务等安全保障。

八、重大分歧意见的处理经过和依据

本标准目前未出现重大分歧，妥善处理了各阶段收到的专家意见和建议。

九、标准性质的建议

本标准应作为一项推荐性国家标准。

十、贯彻标准的要求和措施建议

本标准的技术已较为成熟，实施难度不大，建议本标准的发布日期与实施日期相隔六个月的时间。

为了使标准的规定得到有效贯彻，建议信安标委及时通知行业内各单位本标准的发布信息，在过渡期内组织编写标准宣贯材料及宣贯活动。

十一、替代或废止现行相关标准的建议

本标准发布后，建议废止GB/T 15843.3-2016。

十二、其它应予说明的事项

暂无。

《信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制》

标准起草组

2020-12-8