国家标准《信息安全技术 实体鉴别 第2部分：采用可鉴别加密技术的机制》（征求意见稿）编制说明

一、工作简况

1.1 任务来源

根据全国信息安全标准化技术委员会在2022年网络安全国家标准制修订计划，《信息安全技术 实体鉴别 第2部分：采用可鉴别加密技术的机制》由北京数字认证股份有限公司负责制订，计划号：20230240-T-469。该标准由全国信息安全标准化技术委员会归口。

1.2 制定背景

本标准是GB/T 15843系列标准的第2部分，该国标采用ISO/IEC 9798-2 *Information technology — security techniques—Entity authentication—Part 2: Mechanisms using symmetric encipherment algorithms*，定义了一系列基于对称算法的实体鉴别机制。该标准是信息系统在采用对称密码技术设计鉴别协议时所一致遵循的基础性标准，当前版本为GB/T 15853.2-2017，其内容采纳了ISO/IEC 9798-2:2008、ISO/IEC 9798-2:2008/Cor.1:2010、ISO/IEC 9798-2:2008/Cor.2:2012和ISO/IEC 9798-2:2008/Cor.3:2013。

2019年，ISO发布了最新修订版本ISO/IEC 9798-2:2019 *IT Security techniques — Entity authentication — Part2: Mechanisms using authenticated encryption*，以可鉴别加密技术代替上一版本采用的对称加密技术，并增加可唯一标识每个机制以及机制中可鉴别加密实例的常量。可鉴别加密技术由GB/T 36624-2018定义（修改采用国际标准ISO/IEC 19772），是同时实现数据机密性和完整性保护的一类对称算法工作模式。将可鉴别加密技术应用于实体鉴别机制，有助于提升这类机制在产品实现层面的安全性，并适应密码产业生态中对称算法向可鉴别加密逐步过渡的趋势。因而GB/T 15843.2计划做适应性修订，对采用可鉴别加密技术的实体鉴别机制进行规范。标准的修订将进一步完善可鉴别加密的实体鉴别机制，为我国各类密码模块、密码产品及服务实现更加完善的鉴别协议提供参考，同时也可为密码检测机构评估密码产品鉴别协议的合规性提供依据。

1.3 起草过程

2022 年 3 月-2022 年 4 月，成立编制组，提出标准修订建议，初步拟定标准草案，申请修订立项。

2022 年 4 月，全国信息安全标准化技术委员会（以下简称“信安标委”）组织 2022 年第一次工作组会议周，在 WG4 工作组 2022 年网络安全国家标准立项研讨会上，向专家和工作组其他成员单位汇报了标准草案修订工作情况，听取专家及工作组其他成员单位的意见，经投票，会议同意本标准立项。

2022 年 5 月-2022 年 6 月，编制组召开标准研讨会议，对标准题目、标准修订内容、立项会专家意见、标准试点方案等进行研讨，完善标准草案，形成新版材料提交至秘书处。

2022 年 7 月-2022 年 10 月，标准在信安标委委员范围内进行投票，同意立项。

2022 年 11 月，收到信安标委立项通知，征集标准参编单位，吸纳相关单位加入标准编制组。持续修改完善标准草案，组织标准编制组研讨会议，根据专家意见整理形成新版标准材料。根据国标委、信安标委秘书处建议，综合考虑标准内容以及中文表述习惯，将标准名称变更为《信息安全技术 实体鉴别 第 2 部分：采用可鉴别加密技术的机制》。

2022 年 12 月，在信安标委标准“会议周”上进行汇报，经会议研讨，一致同意进入征求意见稿阶段。会后编制组对标准文本进行修改完善，形成征求意见稿。

2023 年 1 月，通过函审形式请责任专家及责任编辑进行审核，均同意进入征求意见稿阶段。按照专家意见修改完善后，提交新版征求意见稿至秘书处。

2023 年 2 月-3 月，在信安标委秘书处专家审查会上进行汇报，经会议研讨，一致同意通过对本标准的审查。会后根据专家意见修改完善，形成新版标准材料。

二、标准编制原则、主要内容及其确定依据

2.1 标准编制原则

1．符合性

本标准按国家标准GB/T 1.1-2020规定的格式予以编写，遵循我国有关法律、法规、国家标准和国密局相关的最新规定和技术规范。

2．协调性

本标准中涉及的密码算法遵循国家商用密码的有关规定，与已颁布实施的相关安全标准相协调。

3. 安全性

本标准在编制过程中将召开多次专家研讨会和专家审查会，同时在征求意见稿阶段将组织标准试点工作，对收到的专家意见以及发现的问题进行研讨论证，确保各类机制安全可用，保证在产业应用的安全性。

2.2 主要内容及其确定依据

本标准规定了采用可鉴别加密技术实现实体鉴别的机制。其中有四种是两个实体间无可信第三方参与的鉴别机制，这四种机制中有两种是由一个实体针对另一个实体的单向鉴别，另两种是两个实体相互鉴别。其余的机制都要求有一个在线可信第三方参与，以便建立公共的秘密密钥，实现相互或单向的实体鉴别。

本次修订拟在采用对称算法的各个实体鉴别机制中，以可鉴别的加密来代替上一版本采用的对称加密；增加可唯一标识每个机制以及机制中可鉴别加密实例的常量；适应性修改部分术语和定义、章节标题等内容。

本标准适用于指导基于可鉴别的加密实现的实体鉴别系统、产品或服务的建设和研发，密码检测机构可依据本标准评估密码产品鉴别协议的合规性。

2.3 修订前后技术内容的对比[适用于国家标准修订项目]

与 GB/T 15843.2—2017 相比，主要技术变化如下：

（1） 删掉了“范围”中关于时变参数、信息传递次数的说明，将其纳入第 5 章（见第 5 章，2017 年版的第 1 章）；

（2） 用等同采用国际标准的 GB/T 15843.1 代替了 ISO/IEC 9798-1；增加了规范性引用文件 GB/T 36624（见第 2、3 章，2017 版的第 2、3 章）、GB/T 25069（见第 2、3 章）；

（3） 增加了术语“验证方”（见 3.4），更改了术语“可鉴别的加密”（见 3.1,2017 年版的 3.1）、“密文”（见 3.2,2017 年版的 3.2）、“声称方”（见 3.3,2017 年版的 3.3）、“时间戳”（见 3.5,2017 年版的 3.6）、“可信第三方”（见 3.6,2017 年版的 3.7）的定义，删除了术语“消息鉴别码”（见 2017 年版的 3.4）、“消息鉴别码算法”（见 2017 年版的 3.5）；

（4） 增加了符号 “SID^{i}_{m}”（见第 4 章、第 6 章、第 7 章、第 8 章、附录 A），

删掉了“X‖Y”原有的“注”（见 2017 年版的第 4 章）；

（5） 增加了“总则”，将鉴别机制中与时变参数、信息传递次数等相关的说明内容纳入此部分，同时补充了对附录的说明（见第 5 章，2017 年版的第 5 章）；

（6） 更改了“要求”中关于“对称加密”相关的说法，替换为“可鉴别的加密”（见第 6 章，2017 年版的第 5 章）；

（7） 更改了关于“可信第三方”的描述，替换为“在线可信第三方”（见第 7 章、第 8 章，2017 年版的第 6 章、第 7 章）；

（8） 更改了各类机制的代号，用英文缩写代替原有数字（见第 7 章、第 8 章、附录 A、附录 C，2017 年版的第 6 章、第 7 章、附录 A、附录 C）；

（9） 更改了“对象标识符”（见附录 A，2017 年版的附录 A），删掉了“符合 ASN.1 基本编码规则（BER）的编码示例”（见 2017 年版的 A.3）；

（10） 增加了对“文本域的使用”的相关说明（见附录 B）；

（11） 增加了参考文献“GB/T 15843.5”、“GB/T 16263.1”、“GB/T 17901.1”、“GB/T 32907”（见“参考文献”）。

三、试验验证的分析、综述报告，技术经济论证，预期的经济效益、社会效益和生态效益

3.1 试验验证的分析、综述报告

3.2 技术经济论证

3.3 预期的经济效益、社会效益和生态效益

可鉴别加密技术是同时实现数据机密性和完整性保护的一类对称算法工作模式。将可鉴别加密技术应用于实体鉴别机制，有助于提升这类机制在产品实现层面的安全性，并适应密码产业生态中对称算法向可鉴别加密逐步过渡的趋势。本标准的修订，将进一步完善可鉴别加密的实体鉴别机制，为我国各类密码模块、密码产品及服务实现更加完善的鉴别协议提供参考，同时也可为密码检测机构评估密码产品对鉴别协议的合规性提供依据。

四、与国际、国外同类标准技术内容的对比情况，或者与测试的国外样品、

样机的有关数据对比情况

本标准使用重新起草法修改采用 ISO/IEC 9798-2:2019《信息安全技术 实体鉴别 第 2 部分：采用可鉴别加密技术的机制》。

五、以国际标准为基础的起草情况，以及是否合规引用或者采用国际国外标准，并说明未采用国际标准的原因

目前国际上对于可鉴别的加密机制，有国际标准 ISO/IEC 19772，于 2020 年发布了最新修订版本。国内修改采用本标准的国家标准 GB/T 36624 在 2018 年发布最新版本，其结合我国技术条件进行了适应性调整。GB/T 15843.2 将基于 GB/T 36624 对采用可鉴别加密技术的实体鉴别机制进行规范。

六、与有关法律、行政法规及相关标准的关系

（一）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。

（二）与相关国内相关标准的关系

本标准引用以下标准：

GB/T 15843.1—2017 信息技术 安全技术 实体鉴别 第 1 部分：总则

GB/T 25069—2022 信息安全技术 术语

GB/T 36624—2017 信息技术 安全技术 可鉴别的加密机制

七、重大分歧意见的处理经过和依据

本标准起草过程中未出现重大分歧。

八、涉及专利的有关说明

在本标准的草案稿封面，都注明了“在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上”。截至目前，没有收到任何单位反馈的专利声明。

九、实施国家标准的要求，以及组织措施、技术措施、过渡期和实施日期的建议等措施建议

暂无。

十、其他应当说明的事项

暂无。