



中华人民共和国国家标准

GB/T 42589—2023

信息安全技术 电子凭据服务安全规范

Information security technology—Specification for electronic credential
service security

2023-05-23 发布

2023-12-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	3
5 概述	3
5.1 服务框架	3
5.2 基础安全服务	4
6 安全技术要求	5
6.1 通用要求	5
6.2 外部服务安全要求	7
6.3 内部服务安全要求	9
7 安全管理要求	9
7.1 管理控制要求	9
7.2 网络接入管理要求	10
7.3 人员登记和管理制度要求	10
7.4 灾难备份和应急预案制度要求	10
7.5 安全管理教育培训制度要求	10
8 安全测评	11
8.1 测评对象	11
8.2 测评方法	11
8.3 测评过程	21
8.4 测评结论	21
附录 A (资料性) 典型电子凭据业务流程、密码/在线按需服务流程及测评记录表示例	22
参考文献	28

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：西安电子科技大学、中国科学院信息工程研究所、航天信息股份有限公司、北京立思辰新技术有限公司、中国电子技术标准化研究院、上海交通大学、大象慧云信息技术有限公司、国信电子票据平台信息服务有限公司、北京海泰方圆科技股份有限公司。

本文件主要起草人：李晖、李风华、赵兴文、王竹、李少维、侯海波、王惠莅、邱卫东、朱延超、岳强、耿魁、周曙光、朱辉、房梁、罗琦榕、贾宝刚、曹进、寇文龙、宋祁朋。

信息安全技术 电子凭据服务安全规范

1 范围

本文件规定了电子凭据核发、开具、交付、存储、核准、查验、状态管理等服务的安全要求及测评方法。

本文件适用于电子凭据服务的设计、部署、提供和测评,也可为电子凭据服务监管提供参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 22239—2019	信息安全技术	网络安全等级保护基本要求
GB/T 25069—2022	信息安全技术	术语
GB/T 28449—2018	信息安全技术	网络安全等级保护测评过程指南
GB/T 32924—2016	信息安全技术	网络安全预警指南
GB/T 35273—2020	信息安全技术	个人信息安全规范
GB/T 36635—2018	信息安全技术	网络安全监测基本要求与实施指南
GB/T 37092—2018	信息安全技术	密码模块安全要求
GM/T 0031—2014	安全电子签章密码技术规范	

3 术语和定义

GB/T 25069—2022 界定的以及下列术语和定义适用于本文件。

3.1

电子凭据 **electronic credential**

记载经济往来等活动的电子数据记录。

示例:电子发票、客票、事业单位资金往来结算票据、行政收费收据、银行回单等。

3.2

电子凭据服务 **electronic credential services**

为服务接受方提供的电子凭据相关的业务流程。

注:电子凭据服务包括核发、开具、交付、查验、状态管理等。

3.3

实体 **entity**

存在或者可能存在的任何具体或抽象的事物,包括这些事物间的关联。

示例:人、对象、事件、理念、过程。

注:实体的存在和与之有关的数据是否可用无关。

[来源:GB/T 5271.17—2010,17.02.05]