

ICS 35.240.99
L 76



中华人民共和国国家标准

GB/T 36901—2018

电子证照 总体技术架构

Electronic certificate—Overall technical framework

2018-11-15 发布

2019-01-01 实施

国家市场监督管理总局 发布
中国国家标准化管理委员会

目 次

前言	I
引言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 电子证照系统技术框架	2
5.1 电子证照系统	2
5.2 电子证照系统的服务对象	3
5.3 电子证照系统的部署模式	3
6 电子证照资源库要求	3
6.1 资源库组成	3
6.2 目录库	3
6.3 证照库	3
6.4 管理信息和加注件的使用	4
7 电子证照共享服务要求	4
7.1 一般要求	4
7.2 电子证照检索	4
7.3 电子证照获取	4
7.4 电子证照验证	4
7.5 持续服务能力	4
8 安全要求	5
8.1 电子证照文件安全要求	5
8.2 电子证照系统安全要求	5
附录 A (资料性附录) 政务服务中的共享服务部署模式	6
参考文献	7

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由国家密码管理局提出并归口。

本标准起草单位：中央办公厅信息中心、中国电子技术标准化研究院、福建南威软件有限公司、方正国际软件(北京)有限公司、成都卫士通信息产业股份有限公司、浪潮软件集团有限公司、北京海泰方圆科技股份有限公司、北京冠群信息技术股份有限公司、福建榕基软件股份有限公司、江苏省建设信息中心、广东省信息中心、航天福昕软件(北京)有限公司、北京数科网维技术有限责任公司、北京书生电子技术有限公司、浙江汇信科技有限公司、普华诚信信息技术有限公司、甘肃万维信息技术有限公司、广州市中智软件开发有限公司、山东省标准化研究院、中国软件与技术服务股份有限公司、中安网脉(北京)技术股份有限公司、北京东方通科技股份有限公司、北京安信天元科技发展有限公司、北京国脉信安科技有限公司、上海维豪信息安全技术有限公司。

本标准主要起草人：赵波、李海波、陈亚军、孙文龙、张鹏程、李平立、代红、黄文峰、张军、宁方刚、王凌、董建、方春燕、贾宝刚、丛培勇、李波、钟伟平、王剑、陈兆亮、薛馨枫、冯辉、陈子楚、王少康、苗宗利、王卫国、虞小平、丁曙初、杨健、王寒冰、张宇、武文高、柴德华、袁峰、刘冰、王忠义、谢超、张杰、刘丹、董卫兵、梁国杰、逢锦山、冯文化、王天顺、李易昂、李峙、苗银军、赵引华、张静、陈品、郑秉文、李丽花。

引 言

电子证照系列基础标准包括以下 6 项：

- GB/T 36901—2018 电子证照 总体技术架构；
- GB/T 36902—2018 电子证照 目录信息规范；
- GB/T 36903—2018 电子证照 元数据规范；
- GB/T 36904—2018 电子证照 标识规范；
- GB/T 36905—2018 电子证照 文件技术要求；
- GB/T 36906—2018 电子证照 共享服务接口规范。

其中：

GB/T 36901—2018 规定了电子证照系统技术框架，明确了各组成部分之间的关系并提出对应要求。本系列下的其他标准都是在该框架下，针对电子证照系统中的相关部分分别展开而形成的。

GB/T 36902—2018 规定了证照类型的元数据，提出了证照分类规则、证照目录的使用和管理要求，并提供了按业务条线梳理证照类型的示例。

GB/T 36903—2018 规定了电子证照的信息模型，定义了证照的基础信息、业务信息和电子证照加注件信息，并给出了元数据的扩展规则。

GB/T 36904—2018 提出了证照标识的编码方法和管理要求。

GB/T 36905—2018 对电子证照文件提出了承载格式、元数据、标引和通用样式等方面的要求，为充分利用 OFD 的技术特性，同时支持固定版式显现和计算机直接解析利用两种需求、实现较高级别的信息安全利用提供指导。

GB/T 36906—2018 提出了证照应用业务系统与电子证照共享服务之间的交互场景和接口定义，该接口还可用作组建大范围共享网络的核心协议。

为了实现证照信息的全面共享，还需要按照本系列基础标准确立的规则，分类梳理各类型证照的业务元数据、照面样式和其他要求。

电子证照 总体技术架构

1 范围

本标准规定了电子证照系统技术框架、电子证照资源库和共享服务要求以及安全要求。

本标准适用于电子证照系统的规划、设计、开发和利用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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—2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 36902—2018 电子证照 目录信息规范

GB/T 36903—2018 电子证照 元数据规范

GB/T 36904—2018 电子证照 标识规范

GB/T 36905—2018 电子证照 文件技术要求

GB/T 36906—2018 电子证照 共享服务接口规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

证照 certificate

由机关、团体、企事业单位颁发的、能够证明资格或权利等的凭证类文件。

注:证照包括证件和执照等。

3.2

证照目录 certificate catalog

依据元数据规范对证照提取特征,并按照一定的分类方法进行排序和编码形成的一组信息。

3.3

电子证照 electronic certificate

由计算机等电子设备形成、传输和存储的证照数据文件。

3.4

电子证照文件 electronic certificate file

以版式文档表示的电子证照,该文件既包含照面固定版式效果,又包含证照元数据及标识,并应用密码技术保障这些内容的真实性和完整性。

3.5

电子证照原件 electronic certificate original file

由证照颁发机构或其授权机构签署生成的电子证照文件。

3.6

电子证照加注件 electronic certificate copy file

为办理相关事项,在电子证照原件基础上附加用途、有效期限等声明信息并由制作人签署而产生的

电子证照文件。

4 缩略语

- 下列缩略语适用于本文件。
- OFD 开放版式文档(Open Fixed-layout Document)
- VPN 虚拟专用网络(Virtual Private Network)

5 电子证照系统技术框架

5.1 电子证照系统

电子证照系统分为基础设施层、数据资源层、应用支撑层、业务应用层、用户及服务层等五个层次，其应用技术框架如图 1 所示。

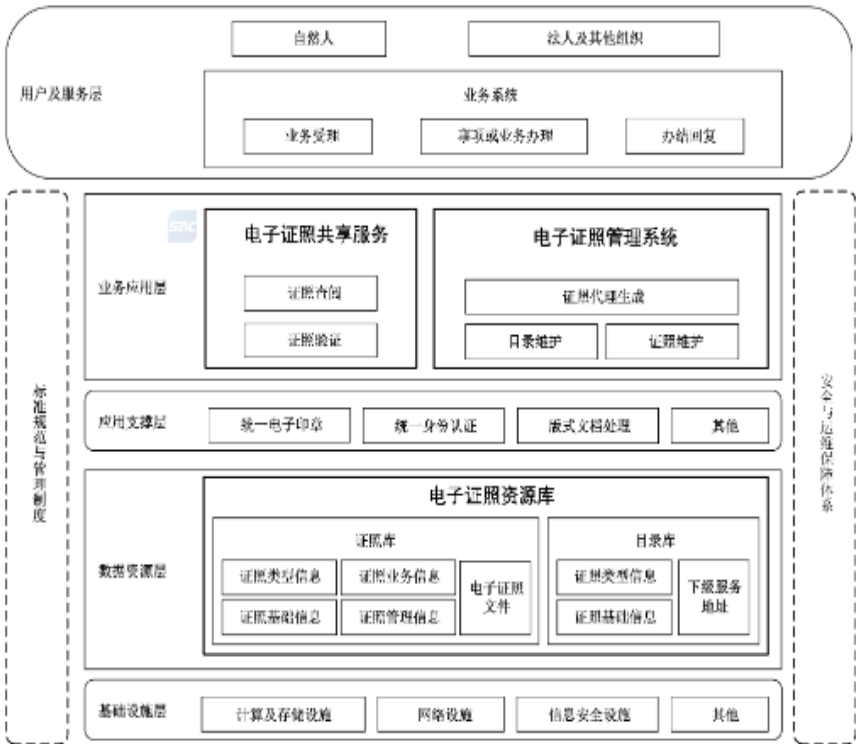


图 1 电子证照应用技术框架

- 电子证照应用技术框架各层说明如下：
- a) 基础设施层提供计算及存储、网络、信息安全和其他软硬件基础设施，为电子证照系统和业务系统运行提供基础条件；
 - b) 数据资源层为电子证照共享服务提供证照信息资源支撑；
 - c) 应用支撑层为形成和使用电子证照提供统一身份认证、统一电子印章、版式文档处理和其他共

性支撑；

- d) 业务应用层分为两部分,电子证照共享服务依托证照数据资源对外提供利用服务,电子证照管理系统负责对证照及其目录信息进行管理；
- e) 用户及服务层主要是应用或生成电子证照的业务系统及其用户。

上述各层均依赖安全与运维保障体系提供支撑,同时依赖标准规范和管理制度保证各层级、各系统之间的协作。

5.2 电子证照系统的服务对象

电子证照系统的主要服务对象是业务系统,其应满足下列要求：

- a) 业务系统服务的用户包括两类,一类是自然人,另外一类是法人和其他组织；
- b) 业务系统是指政务服务或其他行业领域中依赖证照信息或文件作为业务办理条件的应用系统,其与电子证照系统的交互关系包括：
 - 1) 电子证照系统通过共享服务向业务系统提供证照信息或文件；
 - 2) 电子证照系统可验证业务系统提交的、以其他方式收集的证照信息或文件；
 - 3) 部分业务系统事项办理中产生的新的电子证照,将在办结后交付用户；
 - 4) 交付后的证照可通过多种方式归集到电子证照系统；
 - 5) 电子证照系统可为业务系统提供证照代理生成服务。

5.3 电子证照系统的部署模式

电子证照系统之间可通过移交电子证照库数据或注册证照目录信息的方式进行跨库共享。

电子证照系统可根据不同的共享方式采用不同的系统部署模式,参见附录 A。

6 电子证照资源库要求

6.1 资源库组成

电子证照资源库由证照库及目录库组成,应满足下列要求：

- a) 证照库包含提供检索、获取、验证和下载功能所需的证照信息；
- b) 目录库包含提供检索、定位功能所需的证照目录信息；
- c) 证照库和目录库的比例取决于证照资源库实施主体辖区内的实际情况。

6.2 目录库

目录库用以支持电子证照资源的检索和定位,应满足下列要求：

- a) 由下级证照系统的证照目录内容汇集生成；
- b) 证照目录的内容包含证照类型信息以及检索、定位所需的证照基础信息；
- c) 证照类型信息符合 GB/T 36902—2018 的要求；
- d) 证照基础信息符合 GB/T 36903—2018 的要求。

6.3 证照库

证照库用以支持电子证照资源获取、验证和下载,应满足下列要求：

- a) 以证照业务信息和电子证照文件为主要内容；
- b) 证照类型信息符合 GB/T 36902—2018 的要求；
- c) 证照基础信息、业务信息符合 GB/T 36903—2018 的要求；
- d) 电子证照文件使用 OFD 格式,并符合 GB/T 36905—2018 的要求；



- e) 包含状态变更记录等证照管理信息,具体包括:
 - 1) 变更时间;
 - 2) 变更原因;
 - 3) 变更后状态;
 - 4) 变更后状态代码。

6.4 管理信息和加注件的使用

证照管理信息和电子证照加注件的使用应满足下列要求:

- a) 证照状态及时反映证照业务操作完成后的结果状态;
- b) 证照状态的变更由业务系统发起;
- c) 证照状态变更时,应记录变更原因和时间;
- d) 提供电子证照加注件时,文件中应包含加注操作相关信息;
- e) 提供电子证照加注件时,应记录制作和提供情况。

7 电子证照共享服务要求

7.1 一般要求

电子证照资源库通过接口方式对外提供证照资源共享服务并满足相应的功能及性能要求。其中,业务功能应满足典型证照应用场景的需求,包括电子证照检索、电子证照获取和电子证照验证等。

电子证照共享服务的对外接口应符合 GB/T 36906—2018 的要求。

7.2 电子证照检索

电子证照检索应满足下列要求:

- a) 可根据持证主体和证照类型检索证照;
- b) 持证主体是自然人时主要使用公民身份号码,是法人或其他组织时主要使用统一社会信用代码;
- c) 检索结果中宜包含符合 GB/T 36904—2018 要求的电子证照标识。

7.3 电子证照获取

电子证照获取应满足下列要求:

- a) 可获取该证照的多项元数据信息;
- b) 可请求下载该证照的电子证照原件或加注件;
- c) 获取证照信息或电子证照文件前应获得持证主体直接或间接的授权,法律法规明确应无条件向社会公开的除外。

7.4 电子证照验证

电子证照验证应满足下列要求:

- a) 可对给定的证照元数据信息进行核对;
- b) 可对给定的电子证照文件进行真伪验证及管理状态核对。

7.5 持续服务能力

电子证照资源库对外提供证照共享服务时应同时承诺该服务的性能和质量满足使用方实施业务的要求,包括但不限于:

- a) 服务的持续时间；
- b) 提供检索、获取和验证功能服务的平均请求响应时间；
- c) 证照共享服务的并发响应能力。

8 安全要求

8.1 电子证照文件安全要求

电子证照文件应满足下列安全要求：

- a) 使用密码技术保障文件的真实性和完整性；
- b) 文件的真实性和完整性具有可验证性；
- c) 应用的密码技术符合国家密码管理的政策、法规和相关要求；
- d) 应由证照颁发机构或其授权的机构对文件应用密码技术保护；
- e) 对文件应用密码技术保护时应遵循证照业务管理流程。

8.2 电子证照系统安全要求

8.2.1 总体要求

电子证照系统建设应按照国家网络安全等级保护相关要求确定保护级别，并按照 GB/T 22239—2008 采取保护措施。

8.2.2 电子证照管理系统

电子证照管理系统应满足下列安全要求：

- a) 采取措施保证时间的准确性；
- b) 宜存储关键业务数据的摘要值；
- c) 宜支持定义持证主体的隐私数据；
- d) 对引起证照信息变动的操作记录日志，支持追溯、审计。

8.2.3 电子证照共享服务

电子证照共享服务应满足下列安全要求：

- a) 确保与业务系统之间通信的安全性(如：进行数据加密、建立 VPN 等通道)；
- b) 仅为经过认证的业务系统提供服务；
- c) 对服务的调用及响应情况记录日志，支持追溯、审计；
- d) 共享服务的日志信息独立存储并进行相应保护。

8.2.4 电子证照资源库

电子证照资源库应满足下列安全要求：

- a) 仅面向电子证照管理系统和电子证照共享服务提供数据；
- b) 宜进行证照信息与电子证照文件比对，保障文件内外元数据的一致性；
- c) 电子证照库中的关键数据加密存储或对其实施安全防护；
- d) 建立电子证照备份库。

附录 A (资料性附录)

政务服务中的共享服务部署模式

电子证照共享服务可部署于电子政务外网和互联网等网络,为各种业务系统提供服务和支撑。

通过证照共享服务接口,各部门、各地区的证照共享服务可互相连接组成“网络资源库”,提供跨部门、跨地区的电子证照信息共享。

依据《国务院办公厅关于印发“互联网+政务服务”技术体系建设指南的通知》,用于政务服务的电子证照系统一般分为国家级、省部级、地市级三级,如图 A.1 所示。

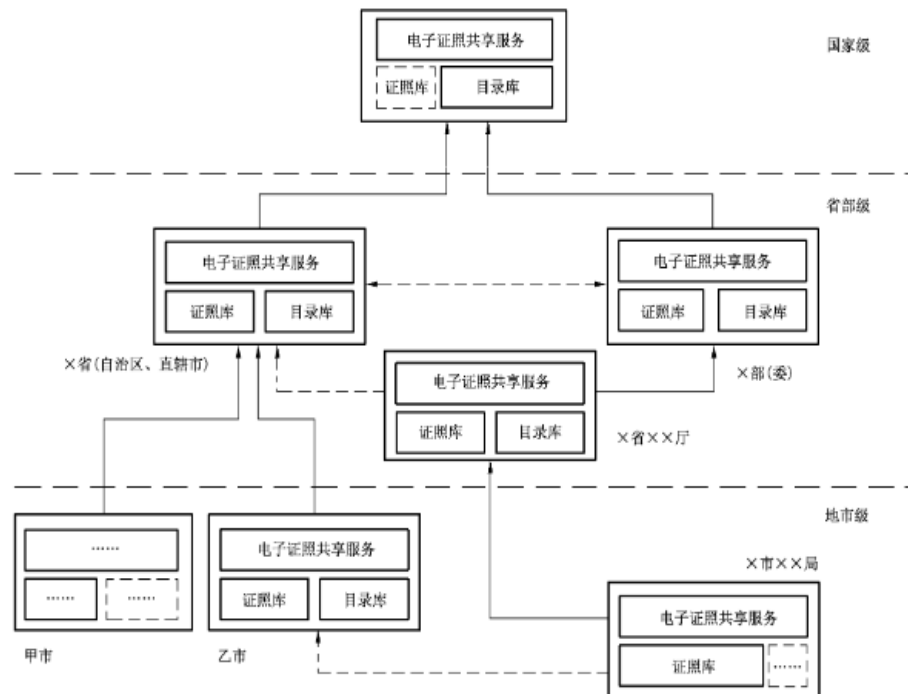


图 A.1 电子证照共享服务三级部署模式

国家级电子证照共享服务,主要基于证照目录库提供全国范围内的证照检索、定位功能,基于下级(省部级)服务提供全国范围内的证照获取和验证等功能。

省部级电子证照共享服务,基于自建电子证照库和下级(地市级)服务的目录信息提供所辖地域或领域内的电子证照检索、获取和验证等功能,并将本级证照资源库的目录信息注册到国家级证照服务中。

地市级电子证照共享服务,基于本地区证照库和下级服务的目录信息提供所辖地域的电子证照检索、获取和验证等功能,并将本级证照资源库的目录信息注册到省部级证照服务中。

参 考 文 献

- [1] 公通字[2007]43号 信息安全等级保护管理办法
 - [2] 国办函[2016]108号 国务院办公厅关于印发“互联网+政务服务”技术体系建设指南的通知
-