ICS 01.120
A00

T/CMA

中 国 计 量 协 会 团 体 标 准

T/CMA CC XXXX—XXXX

计量电子证书通用技术规范

General Technical Specification for Electronic Certificate in Metrology

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中 国 计 量 协 会　发 布

目　　次

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。

本文件由中国计量协会提出。

本文件由中国计量协会校准委员会归口。

本文件起草单位：

本文件主要起草人：

计量电子证书通用技术规范

1 范围

本文件规定了计量电子证书/报告（以下简称电子证书）的基本要求、系统技术架构要求、应用要求和安全要求。适用于计量技术机构和校准实验室在计量电子证书/报告的制作、传输、储存、真伪验证等方面的应用和管理。

本文件不适用计量证书/报告内容的编写、排版及测量结果处理等。

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 5271.1 信息技术 词汇 第1部分：基本术语
GB/T 10113—2003 分类与编码通用术语
GB/T 18894—2016 电子文件归档与电子档案管理规范
GB/T 20518—2018 信息安全技术 公钥基础设施 数字证书格式
GB/T 26162—2021 信息与文献 文件(档案)管理 概念与原则
GB/T 27025 检测和校准实验室能力的通用要求
GB/T 27766—2011 二维条码网格矩阵码
GB/T 33190—2016 电子文件存储与交换格式 版式文档
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
GA/T 1106—2013 信息安全技术 电子签章产品安全技术要求

3 术语和定义

GB/T 5271.1、JJF 1001和JJF 1069界定的以及下列术语和定义适用于本文件。

3.1 计量电子证书/报告（以下简称电子证书） electronic certificate in metrology

以开放式版式文档存储的，内容真实、完整且具有抗抵赖性的计量证书/报告（如检定证书、校准证书、型式评价报告、商品量及商品包装计量检验报告和能源效率检测报告等）的电子数据文件。

3.2 文件 file

作为一个单元存储和处理的命名的记录集。

［来源 ：GB/T 5271.1—2000，01.08.06］

3.3 数字证书 digital certificate

由国家认可的，具有权威性、可信性和公正性的第三方证书认证机构（CA）进行数字签名的一个可信的数字化文件。

［来源 ：GB/T 20518—2018，3.7］

3.4 元数据 metadata

描述电子文件的内容、结构、基础信息及其管理过程的数据。

注：改写GB/T 18894—2016，3.3

3.5 真实性 authenticity

电子文件的内容、逻辑结构、基础信息与形成时的原始状况相一致的性质。

注：改写GB/T 18894—2016，3.5

3.6 完整性 integrity

电子文件的内容、结构和基础信息齐全且没有破坏、变异或丢失的性质。

注：改写GB/T 18894—2016，3.7

3.7 电子证书的标识 identification of electronic certificate in metrology

赋予电子证书的唯一代码。

注：改写GB/T 36904-2018，3.4

3.8 编码 encoding

给事物或概念赋予代码的过程。

［来源 ：GB/T 10113—2003，2.2.1］

3.9 代码 code

标识特征事物或概念的一个或一组字符。

［来源 ：GB/T 10113—2003，2.2.5］

3.10 数字签名 digital signature

附加在数据单元上的数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据防止被人（例如接收者）伪造或抵赖。

［来源 ：GB/T 33190—2016，3.3］

3.11 电子签章 Electronic signature

以数字证书为基础，以数字签名为核心技术，将数字签名与印章图片以及被签章对象绑定在一起，为签章对象提供完整性和验证。它是数字签名可视化表现形式之一。

［来源 ：GA/T 1106—2013，3.1］

3.12 开放式版式文档 Open Fixed-layout Document

独立于软件、硬件、操作系统、输出设备的版式文档格式。

［来源：GB/T 33190—2016，3.2］

3.13 抗抵赖性 Non repudiation

抗抵赖性是一个活动或事件已经发生，且不可否认的能力。

［来源：GB/T 36618—2018，4.7］

4 电子证书基本要求

4.1 电子证书文件要求

4.1.1 电子证书文件应使用开放式版式文档格式。

4.1.2 一个电子文件内应仅完整的包含一份电子证书。

4.1.3 应包含提供真实性、完整性、抗抵赖性的标志数据，如电子签名产生的标志数据。

4.1.4 不应使用动态元素。

4.1.5 带有附件的计量证书/报告，附件为电子证书的组成部分，亦应使用开放式版式文档格式。

4.1.6 电子证书显现和共享所需的数据自包含。

4.2 电子证书印章

4.2.1 电子证书印章图片内容应能明确显示印章为“电子证书”，如：“XXXXX单位检定电子证书专用章”。

4.2.2 电子证书印章包括“检定电子证书专用章”、“校准电子证书专用章”、“检验电子证书专用章”、“检测电子证书专用章”及相应的骑缝章，电子证书专用章可以用作相应的骑缝章。

4.3 电子证书版式

4.3.1 电子证书发布机构应按照“简单实用、与时俱进、节能环保”的原则统一规范各类电子证书的样式。

4.3.2 电子证书版式应符合相关规定要求。

4.3.3 电子证书宜采用210×297mm（宽×高）页面（即A4纸张大小）。

4.3.4 电子证书使用的二维码，其码制应符合GB/T 27766的规定，其大小宜为25mm×25mm。二维码

宜放置在电子证书首页显著位置，且不应遮盖其他信息。

4.3.5 电子证书可视页面上的规定位置应有可视的电子证书印章图片。

4.3.6 电子证书的每一页宜明确标识“本证书为电子证书，请到发证机构官网验证”。

4.4 文件命名规则

4.4.1 电子证书文件命名应按照易于理解清晰的命名规则。

4.4.2 文件名长度应不超过 255 字符，不宜超过 50 个中文字符。

4.4.3 文件名内容可包含证书类别、“电子证书”、单位、仪器名称、证书号、发证单位等内容，至少应包含证书类别、“电子证书”、证书编号、仪器名称、出厂编号五部分内容。证书类别和“电子证书”两部分宜直接连接，其他各部分之间宜用“-”连接。如：检定电子证书-质字 20211203—2377、校准电子证书-1022CN0200036。

4.5 电子证书标识

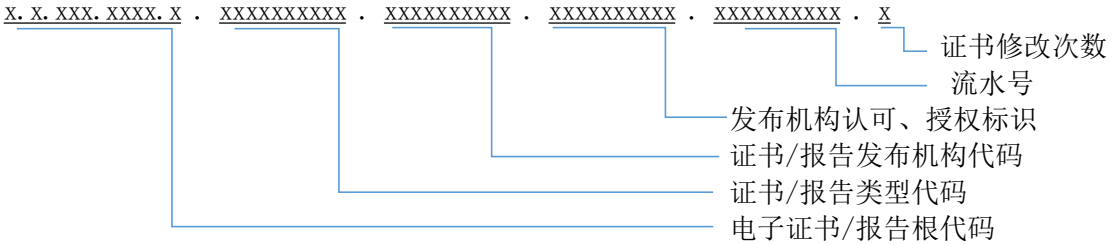
4.5.1 电子证书文件中宜存储有电子证书标识。

4.5.2 电子证书标识应遵循 GB/T33190—2016 中第 16 章“自定义标引”的相关要求。包含数据标引的证书文件应通过文档入口文件（Document.xml）指向标引列表文件。

4.5.3 电子证书标识由电子证书/报告发布机构按规则生成，并保证唯一性。

4.5.4 电子证书标识生成后，在电子文件交换、存档等过程中应保持不变。

4.5.5 电子证书标识的组成部分从左至右依次为：电子证书根代码、证书类型代码、证书发布机构代码、发布机构认可及授权标识、流水号、证书修改次数，各部分之间用点分隔符“•”分隔。具体结构如图 1 所示。



图中：电子证书根代码—用于区分电子证书和其他种类电子文件的代码，根代码的OID取值。

证书类型代码—“1”为检定证书；“2”为检定结果通知书；“3”为仲裁检定证书；“4”为型式评价报告；“5”为商品量及商品包装检验报告；“6”为能源效率标识检验报告；“7”为校准证书；“8”为其他。

证书发布机构代码—证书发布机构的组织机构代码。

发布机构认可/授权标识—证书发布机构的计量授权证书编号、CNAS认可标识、CMA资质证书编号。

流水号—电子证书/报告发布机构发出的唯一、可使用的、具有定义流水号编号规则的证书编号。

证书修改次数—1位数字，从0开始，用以记录证书修改次数。

图1 电子证书标识的组成部分具体结构图

5 电子证书系统技术架构

5.1 电子证书系统的组成

5.1.1 电子证书系统分为基础设施层、数据资源层、应用支撑层、业务应用层、用户及服务层五个层次。

5.1.2 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，为电子证书系统运行提供基础条件。

5.1.3 数据资源层为电子证书服务提供电子证书信息资源支撑。

5.1.4 应用支撑层为形成和使用电子证书提供电子签章、版式文档处理等支撑。

5.1.5 业务应用层主要是业务系统，包括业务受理、版式文档处理、证书发放等；用户及服务层主要是提供电子证书下载及真伪查询的客户自助服务系统及应用电子证书的用户。

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。电子证书系统的组织框架见图 2。

图2 电子证书系统的组织框架

5.2 电子证书系统功能要求

电子证书系统的功能主要由客户自助服务系统、业务系统和电子证书资源库组成。业务系统和电子证书资源库是电子证书系统的信息来源和证书生成等的应用系统，客户自助服务系统是电子证书系统的对外服务应用系统。

5.2.1 业务系统要求

业务系统为提供计量业务受理、计量证书/报告内容信息录入和生成、计量证书/报告电子文件生成及电子证书存储等服务的应用系统，其与电子签章系统的交互关系包括：

a) 业务系统将生成的计量证书/报告电子文件传给电子签章系统进行版式文档生成和电子签章；
b) 电子签章系统将电子签章后的电子证书回传给业务系统进行电子证书的存储；
c) 电子签章系统将对业务系统请求的电子证书信息进行数据验证，确定证书的真伪，并报告结果。

5.2.2 电子证书资源库要求

电子证书资源库由证书库和电子印章库组成，应满足下列要求：

a) 证书库包含提供生成计量证书/报告电子文件所需的计量检测数据、证书模板文件、资质文件，以及电子签章后的电子证书文件；
b) 电子印章库包含提供印章制作、印章维护、印章应用所需的电子印章信息；
c) 证书资源库的大小取决于电子证书资源库实施机构的实际情况。

5.2.3 客户自助服务系统要求

客户自助服务系统是指客户或者相关机构依赖电子证书信息作为电子证书受理的应用系统，其应满足下列要求：

a) 客户自助服务系统的服务对象包括两类，一类是自然人，另外一类是法人和其他组织；
b) 为服务对象提供注册入口；
c) 仅为经过认证的用户提供服务，确保注册用户信息的安全性。

6 电子证书的应用

6.1 电子证书的传输

电子证书在互联网传输时宜使用加密方式，密钥传输方式包含但不限于：

a) 密钥可以使用身份验证时的验证码；
b) 下载页面直接弹出密钥；
c) 使用下载人的手机号；
d) 使用下载人的微信号；
e) 使用下载人制定的密钥。

6.2 电子证书的下载

电子证书在被用户下载时，应有身份识别方式，确定下载人的身份，身份认证方式包含但不限于：

a) 使用送检人的手机号短信获取验证码验证；
b) 使用送检人的邮箱邮件验证码验证；
c) 使用送检人的微信信息验证码验证；
d) 使用送检人的 QQ 信息验证码验证；
e) 使用送检人的人脸识别验证；
f) 使用送检人的预留的口令验证。

6.3 电子证书的真伪验证

电子证书应提供真伪验证方式。电子证书真伪验证方式包括但不限于：

a) 使用第三方阅读器自带的验证功能进行证书的真伪验证，主要验证电子证书的签章是否有效；
b) 使用电子证书发布机构的证书真伪验证平台进行电子证书真伪验证，将电子证书上传到真伪验证平台后，通过比对电子证书的数据与该机构业务系统中的数据是否一致判断证书的有效性，出具验证结果；
c) 通过扫描电子证书上的二维码进行证书的真伪验证，由发布机构的官方查询服务反馈证书的真伪验证信息。

6.4 电子证书的修改

6.4.1 电子证书发放后，如因证书修改需要发放新的电子证书，新的电子证书标识应记录证书修改次数，原电子证书再次下载、真伪验证或在已发放的电子证书封面上的二维码扫描时，应出现“该证书作废，按照证书修改处置要求，修改后的证书号为XXXXXXX”的提示。

6.4.2 电子证书发出后，如需对电子证书修改可以不发放新的电子证书，只是以追加电子文件内容变更的形式修改，则原电子证书再次下载、真伪验证或在已发放的电子证书封面上的二维码扫描时，应出现系统包括“对序号为……的证书/报告的补充文件”等声明，作为证书文件的加注信息。

6.5 电子证书的存储及处置

电子证书的发布机构在确保电子证书的真实、完整、可用和安全的基础上，统筹制订电子证书的备份方案和策略，实施电子证书、电子证书系统及其配置数据、日志数据等备份管理。电子证书发放机构应采用电子证书系统和数据库的热备份，并参照GB/T 20988等标准进行电子证书的灾难备份和灾难恢复。

电子证书存储及处置要求包括但不限于：

a) 电子证书存储服务器应有一定的安全防护策略。防止电子证书被病毒感染、丢失、失窃、损坏、篡改。
b) 电子证书应采用“321”证书文件存储策略:“3”是至少保存三份电子证书；“2”是电子证书至少采用两种不同的存储介质来保存；“1”是制作至少 1 套电子证书离线备份。
c) 电子证书存储时间应根据法律法规、客户、法定管理机构、资质认定机构的规定要求确定，至少不少于 6 年。
d) 对电子证书存储服务器的访问应有审计日志。
e) 电子证书系统应配置与发布机构业务系统相适应的在线存储设备。

f） 发放机构的电子证书系统宜在计算机存储器中分门别类、集中有序地存储电子证书。
g） 在线存储系统应实施容错技术方案，定期扫描、诊断硬磁盘，发现问题应及时处置。
h） 当电子证书的存储期限期满时，应进行电子证书的删除、销毁等处置，提出被处置对象的续存或销毁等处置意见，处置意见经审核、批准后方可实施；已经在业务系统中删除处置的电子证书，在被真伪验证或下载时，应出现“超过存储期限，不提供真伪验证”。
i） 电子证书销毁时应防止数据泄露，进行格式化处理，证书文件存储的介质应防止恢复。

7 安全要求

7.1 电子证书文件安全要求

电子证书文件应满足下列安全要求：
a） 使用加密技术保障文件的真实性和完整性；
b） 电子证书文件的真实性和完整性应可验证；
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） 应由获得中华人民共和国工业与信息化部电子认证服务许可资质的电子认证服务商对电子证书文件应用密码技术保护；
e） 电子证书的文件管理应遵守发证机构相关要求。

7.2 电子证书系统安全要求

7.2.1 总体要求

电子证书系统应按照国家网络安全等级保护相关要求确定保护等级，并按照GB/T 22239采取保护措施。

7.2.2 电子证书系统

电子证书系统应满足下列安全要求：
a） 电子证书系统时间应溯源至国家授时中心标准时间；
b） 对电子证书加密签章的操作记录日志，支持追溯、审计；
c） 确保与业务系统通信的安全性（如进行数据加密、建立 VPN 通道等）；
d）与业务系统之间数据的交互及响应情况记录日志，支持追溯、审计。

7.2.3 电子证书资源库

电子证书资源库应满足下列安全要求：
a） 电子证书仅为经过认证的用户提供下载服务；
b） 电子证书下载的时间、身份信息等记录日志，应支持追溯、审计；
c） 电子证书在互联网传输时应确保安全性；
d） 电子证书资源库中的关键数据应加密存储或对其实施安全防护。