ICS 01.040.03
A12

# DB33

浙　　江　　省　　地　　方　　标　　准

DB33/T XXXX—XXXX

# 可信电子证照管理规范

Standard of reliable electronic certificate management

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

浙江省市场监督管理局　发布

# 目　　次

# 前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由浙江省大数据发展管理局提出并归口。

本标准起草单位：浙江省大数据发展管理局、浙江省标准化研究院、浙江汇信科技有限公司。

本标准主要起草人：徐颖、施筱玲、王宏宇、赵程遥、郑培、王忠义、吕萌学、田润家、张玮兰、陈晶。

# 可信电子证照管理规范

## 1 范围

本规范规定了可信电子证照的数据结构、可信原则、生命周期管理、数据治理以及安全要求。

本规范适用于政务及公共服务领域应用中各类电子证照数据全生命周期的管理。

## 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 20520 信息安全技术 公钥基础设施 时间戳规范

GB 32100 法人和其他组织统一社会信用代码编码规则

GB/T 33481 党政机关电子印章应用规范

GB/T 36901 电子证照 总体技术架构

GB/T 36902 电子证照 目录信息规范

GB/T 36903 电子证照 元数据规范

GB/T 36904 电子证照 标识规范

GB/T 36905 电子证照 文件技术要求

GB/T 36906 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

**数字证书 digital certificate**

由证书认证机构（CA）数字签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一系列数据。

3.2

**电子签名 electronic signature**

数据电文中以电子形式所含、所附用于识别签名主体身份并表明签名主体认可其中内容的数据。

3.3

**电子签章 electronic seal**

对数据电文进行电子签名，并通过图像处理技术将电子签名操作转化为与纸质文件盖章操作相同的可视化效果。

3.4

**时间戳 time stamp**

使用数字签名技术产生的数据，签名的对象包括了原始文件信息、签名参数、签名时间等信息。TSA对此对象进行数字签名产生时间戳，以证明原始文件在签名时间之前已经存在。

[GB/T 20520—2006 ，定义3.1]

3.5

**证照 certificate**

由机关、团体、企业事业单位颁发的、能够证明资格或权利等的凭证类文件。包括证件、执（牌）照、批文、证明等。

3.6

**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。

3.7

**可信电子证照 reliable electronic certificate**

基于“谁颁发，谁签名，谁负责”的原则，由证照颁发机构对其所颁发的电子证照的信息数据和版式文件进行电子签名后生成的符合《中华人民共和国电子签名法》的电子证照。

3.8

**证照颁发机构 certificate issuing authority**

依据法律法规或服务事项颁发证照的机构。证照颁发机构一般为实体证照上的盖印机构。如果证照上有多个印章或无印章的，则将对证照作出最终审核意见的机构判定为证照颁发机构。

3.9

**证照数源单位 certificate data source organization**

直接向电子证照库提供证照数据的部门。

## 4 缩略语

下列缩略语适用于本文件。

CA 证书认证机构(Certification Authority)

TSA 时间戳机构(Time Stamp Authority)

国密算法 中国国家商用密码算法

JSON 一种轻量级的数据交换格式(JavaScript Object Notation)

## 5 数据结构

### 5.1 概述

可信电子证照包括基础数据和验证数据，其中基础数据包括证照信息和电子证照文件，验证数据包括电子签名和时间戳。可信电子证照数据结构如图1所示。

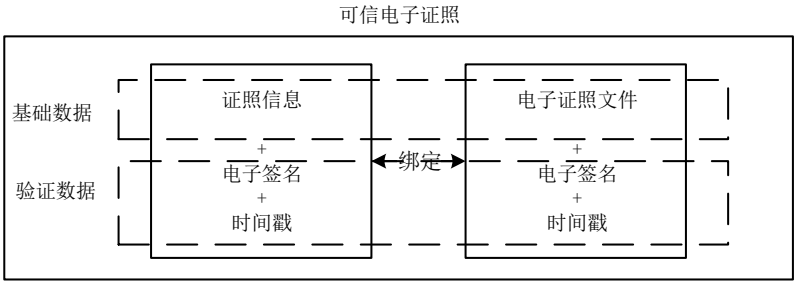



**图1　可信电子证照数据结构**

### 5.2　证照信息

证照信息是指可以用关系型数据库二维表存储的字符串、数字、时间等类型的电子证照数据，应包括照面数据、管理数据（包括状态、唯一标识、非照面的业务标识等）。

唯一标识为赋予电子证照的唯一代码，应符合 GB/T 36904 的要求。

证照信息中属于GB/T 36903 中元数据范围的，应符合其规定。

### 5.3　电子证照文件

电子证照文件是以版式文件方式存储的电子证照文件，要求载明证照的关键信息，原则上应与实体证照样式和内容基本一致的证照版式文件，支持标准版式电子文件，如OFD、PDF等。证照附带的地图、图纸、音视频、动画等附件，可以不合并到电子证照文件中，以附件的原有格式分离存储，通过在电子证照文件中保存其哈希值、索引、数量、链接等方式进行关联，以保证整个电子证照内容的完整性。

电子证照文件推荐采用OFD格式，且应符合GB/T 36905 要求和浙江省相关规范。

### 5.4　验证数据

验证数据应由证照颁发机构产生。其中电子签名用来保证电子证照的来源可追溯，内容完整，不可篡改；时间戳用来保证电子证照生成（或推送）的时间权威性，时间戳的管理、格式和时间戳系统安全管理应遵循GB 20520的要求。电子证照的电子签名应符合《中华人民共和国电子签名法》。

## 6　可信原则

### 6.1　技术要求

浙江省可信电子证照采用电子签名技术，应符合《中华人民共和国电子签名法》和国家密码主管部门的相关要求。可信电子证照出入库都应进行验签，为电子政务应用提供从业务申报、审核到归档的完整可信数据支撑。

### 6.2　签名原则

可信电子证照签名原则如下：

a)　证照数据的签名遵循“谁颁发，谁签名，谁负责”的原则。证照颁发机构或其授权机构对电子证照的证照信息数据和电子证照文件进行签名，并对签过名的电子证照的真实性、完整性、准确性负责；

b)　证照原颁发机构的颁证职能转移到其他机构的，存量证照的签名由原颁发机构负责。证照原颁发机构发生变更的，存量证照的签名由变更后的证照颁发机构负责。证照原颁发机构注销的，

存量证照的签名由职能继受机构负责。证照颁发机构已注销且该证照已不再颁发的，存量证照的签名由档案部门负责；

c) 数字签名的行为宜在颁证系统端进行，在颁证业务产生数据时，由颁证系统生成证照信息和证照电子文件，并对其进行签名。颁证系统无法实现签名操作的，应在数据归集到电子证照库之前完成签名；

d) 证照颁发机构无法申请数字证书的，可授权证照数源单位使用本单位的数字证书对颁发机构颁发的证照进行签名；

e) 证照颁发机构是证照数源单位上级部门的，由证照数源单位和电子证照库管理机构协商电子证照的签名方式。

## 7 生命周期管理

### 7.1 生命周期

证照生成、更新、归集、共享、注销，是一个可信电子证照的生命周期。各阶段完成的具体工作如下：

a) 可信电子证照生成：证照颁发机构依据法律、法规、政策文件进行审批生成证照后，将证照数据依据本规范进行电子化，统一加电子签名、时间戳后，形成可信电子证照；

b) 可信电子证照更新：证照颁发机构在证照发生变更后，重新依据本规范将变更后的证照电子化，形成可信电子证照；

c) 可信电子证照归集：可信电子证照由证照数源单位通过数据交换推送到电子证照库管理机构，然后经过清洗、验签、关联，最后保存到电子证照库；

d) 可信电子证照共享：应用系统通过电子证照库的查询、下载、验证等共享服务接口使用可信电子证照；

e) 可信电子证照注销：证照颁发机构在进行证照注销时，将电子证照状态变为注销，进行数字签名和加盖时间戳，由证照归集单位重新归集到电子证照库。可信电子证照有效期为证照颁发机构标识的证照有效期限；

电子证照系统的总体架构应符合 GB/T 36901 要求。

### 7.2 生成

#### 7.2.1 生成原则

可信电子证照生成原则如下：

a) 可信电子证照数据宜由证照颁发机构或其授权机构生成，对证照信息数据和证照电子文件加上数字签名和时间戳，时间戳格式应符合 GB/T 20520 要求，证照信息数据数字签名过程参见附录 A，电子文件签名过程参见附录 B；

b) 可信电子证照库系统应提供生成标准版式电子文件的服务，以供不具备自行生成标准版式电子文件的证照颁发机构、授权机构或证照归集单位调用，生成符合标准的证照电子文件；

c) 可信电子证照库应提供符合国家标准的数字签名和时间戳服务，以供不具备自行添加数字签名和时间戳能力的证照颁发机构、授权机构或证照归集单位调用，为其生成的证照信息和电子文件加上数字签名和时间戳；

d) 生成的标准版式电子文件中若含有电子签章，电子签章应符合 GB/T 33481 要求。

#### 7.2.2 生成配置

#### 7.2.2.1 证照注册

证照数源单位应将要入库的可信电子证照的通用特征信息注册到电子证照库，形成证照目录信息。证照目录信息必须包括：证照全名、本级业务主管单位、证照类型（执照、批文、证明、其他）、证照共享状态等。

电子证照库目录信息应符合GB/T 36902要求和浙江省相关规范。

#### 7.2.2.2 证照信息配置

可信电子证照的证照信息配置要求如下：

a) 证照数源单位应将证照信息配置到电子证照库；
b) 证照信息包括照面字段、非照面字段。照面字段又叫视读字段，即显示在电子证照上的数据项；非照面字段是指实体照面上没有显示，但是又属于可信电子证照不可或缺的字段，一般包括状态字段、变更时间、变更原因等数据项；
c) 证照信息中必须包括可以唯一标识一本证照的颁证系统业务主键，用于区分证照；
d) 证照信息中必须包括持证主体信息，持证主体为组织机构的，必须有名称、统一社会信用代码。持证主体为自然人的，必须有姓名、中华人民共和国居民身份证号或其他唯一性编号；
e) 证照信息中必须包括证照颁发机构的统一社会信用代码。

#### 7.2.2.3 电子证照文件配置

可信电子证照的电子证照文件配置要求如下：

a) 证照数源单位应将电子证照文件属性信息配置到电子证照库；
b) 电子证照文件属性信息应包括关联证照信息的主键、文件存储地址、签名验证信息等；
c) 证照颁发机构不具备自行生成电子文件能力的，证照数源单位可按照可信电子证照库要求进行文件生成配置，配置方式参照附录 C。

#### 7.2.2.4 证照版本管理

为了适应同一类证照的不同版本，证照信息数据各个字段和文件模板都具有版本属性。版本编号为V+版本号数字，如V1、V2。

可信电子证照库将每个字段版本默认初始化为V1。

### 7.3 归集

证照数源单位通过本单位信息化系统采集证照数据，将生成的可信电子证照数据推送到电子证照库。

部分无法归集的证明类可信电子证照，可不将数据集中到电子证照库，但证照数源单位仍需要按照本规范要求进行生成和共享操作，并将目录信息在可信电子证照库进行注册。

### 7.4 更新与注销

当证照内容、状态变更时，证照数源单位应重新向可信电子证照库归集该证照数据，可信电子证照库中的原证照数据标识为变更，转入历史库，同时增加变更后的证照数据。

当证照注销时，证照数源单位应将证照数据标识为注销，并重新归集该证照数据，可信电子证照库中的证照数据标识为注销，转入历史库。

历史库的证照数据应长期保存，法律法规另有规定的，从其规定。

### 7.5 共享

### 7.5.1 共享要求

可信电子证照宜通过公共数据共享平台向应用系统提供共享，共享内容包括证照信息数据和电子文件两部分，共享平台应支持证照信息的单独共享。

可信电子证照库系统除支持符合 GB/T 36906 规范要求的共享服务接口外，还应支持为每一类证照提供单独的共享接口，方便数据共享平台进行接口控制。

对于无法进行数据归集的证明类电子证照，可采用实时共享的方式。

### 7.5.2 证照信息数据共享

证照信息数据共享的内容至少包括证照信息、证照电子文件属性数据、签名数据、时间戳数据。一类证照一个共享接口方式返回的数据结构参照附录D.1。

### 7.5.3 证照电子文件共享

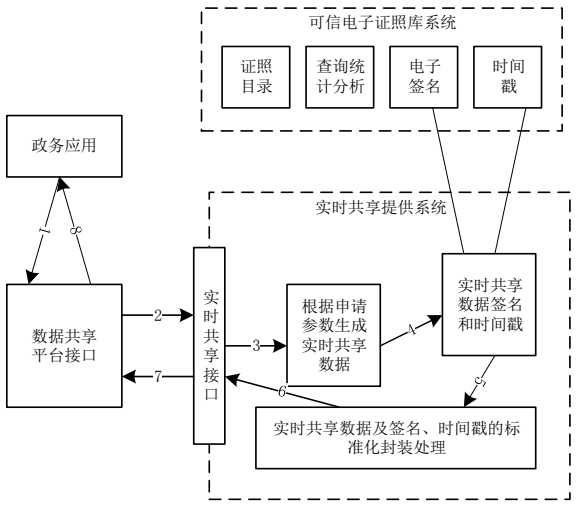
应用系统可从证照信息共享接口返回的数据中获取证照电子文件的下载地址，进而取得证照电子文件。

**注：**证照电子文件地址为临时地址，有效期5分钟。

### 7.5.4 实时共享

#### 7.5.4.1 实时共享流程

实时共享流程见图2。




说明：
1——政务应用调用数据共享服务平台的某个实时共享接口，传入实时共享申请主体等相关信息等。
2——数据共享平台转发到该实时共享提供系统的实时共享接口，传入申请主体身份信息。
3——实时共享提供系统的实时共享接口根据申请主体身份信息，查询本系统数据，提供指定的实时信息数据和电子文件。
4——实时共享提供系统对实时信息数据和电子文件进行电子签名和加盖时间戳，形成可信的实时共享数据。
5——实时共享提供系统返回可信的实时共享数据（包括信息数据、电子文件、电子签名、时间戳）。
6——实时共享提供系统将实时共享数据、电子签名和时间戳进行标准化格式封装。
7——实时共享接口将实时共享数据返回数据共享平台。
8——数据共享平台将实时共享数据返回给政务应用。

**图2 实时共享流程**

#### 7.5.4.2 实时共享目录注册

提供实时共享的证照数源单位应在电子证照库系统中进行目录注册，进行统一管理。

#### 7.5.4.3 证照信息数据实时共享要求

证照信息数据实时共享结构应参照证照信息数据共享要求，共享返回数据结构参照附录D.2。

#### 7.5.4.4 证照电子文件实时共享要求

实时共享的电子文件格式应符合证照电子文件的要求。

#### 7.5.4.5 实时共享接口要求

实时共享接口由证照数源单位负责实现，通过电子证照库系统与数据共享平台对接。

### 7.5.5 共享数据可信验证

共享数据可信验证应至少包括对证照数据正确性、完整性、来源权威性的验证。

可信电子证照应支持对证照信息的单独可信验证和对证照电子文件的单独可信验证。

可信电子证照应支持应用系统在线验证和离线验证。

在线验证是应用系统通过可信电子证照库系统提供的验证服务接口对证照信息或证照电子文件进行可信验证，返回验证成功或失败。如果是入库电子证照，同时返回该证照在电子证照库中的最新状态；如果是实时共享的电子证照，调用数源单位的实时验证接口返回最新状态。参见附录E.1。

离线验证是应用系统根据国家密码管理机构制定的数字签名标准和时间戳标准进行验证，不需要连接到电子证照库。离线验证无法获取可信电子证照库中该证照的最新状态。参见附录E.2。

## 8 数据治理

### 8.1 总则

可信电子证照数据治理主要包括数据清洗、证照共享异议/缺失申报。

### 8.2 数据清洗

可信电子证照数据清洗仅判断数据项是否符合清洗规则，不对数据项内容进行修改。

数据清洗失败的数据进入异常数据反馈流程，反馈给证照数源单位，由证照数源单位进行整改后重新归集。

清洗规则包括但不限于以下内容：

a) 校验与部门约定的字段是否必填；
b) 校验日期时间格式正确性；
c) 校验枚举值正确性；
d) 校验身份证号码合规性；
e) 校验统一社会信用代码合规性，社会统一信用代码编码规则应符合 GB 32100 的相关规定。

### 8.3 共享异议/缺失申报

在共享的过程中，证照应用部门、证照使用人可以对共享数据中存在的数据问题进行反馈，包括对数据内容有异议，或者对证照数据缺失进行申报。

证照共享异议/缺失申报流程应遵循浙江省公共数据平台数据治理相关规范要求。

# 9 安全要求

## 9.1 数据安全

可信电子证照库数据应保存在政务外网政务专有云中，所用新数据库系统和文件存储系统需符合浙江省政务云安全技术相关规定。

可信电子证照出入库时均需进行数字签名验证，保证入库出库数据的完整性，未被篡改。

为保证数据隐私，可信电子证照库管理界面上不可查询显示证照的详细数据内容。

## 9.2 共享安全

可信电子证照共享安全需满足如下要求：

a) 仅为经过合法授权的业务系统提供检索、验证与证照获取服务；
b) 经合法授权的业务系统须保证涉及隐私信息的证照被合法授权使用；
c) 经合法授权的业务系统应对证照使用者进行身份认证，仅当通过高级实名认证后方可调用共享服务；
d) 共享服务的调用及响应情况应记录日志，支持审计；
e) 共享服务的日志信息应独立存储并永久保存 。

## 9.3 系统安全

可信电子证照相关系统建设应满足信息安全等级保护三级或以上的防护标准要求。

A A

# 附 录 A
（资料性附录）
证照信息数据签名过程说明

## A.1 证照信息数据示例

可信电子证照的证照信息数据推荐以JSON格式进行组织，Key值为英文字母或英文字母+下划线。

以JSON格式描述证照信息部分数据，举例如下：

```
{
    "ZZBH": "1233**************K",
    "CZZT": "浙江省****委员会",
    "KZ_ZCDZ": "浙江省杭州市**路",
    "KZ_FDDBR": "王**",
    "KZ_ZJLY": "全额财政补助",
    "KZ_ZCZJ": "5195",
    "KZ_JBDW": "杭州市****委员会",
    "ZZBFJG": "杭州市机构编制委员会办公室",
    "KZ_ZZZT": "正常",
    "ZZYXQQSRQ": "2018-01-01",
    "ZZYXQJZRQ": "2023-01-01"
}
```

## A.2 证照信息数字签名

进行数字签名时，Key值以ASCII顺序方式转换为键值相连的字符串。

证照JSON格式Key值转换描述举例如下：

```
"CZZT":"浙江省****委员会","KZ_FDDBR":"王**","KZ_JBDW":"杭州市****委员会","KZ_ZCDZ":"浙江省杭州市**路","KZ_ZCZJ":"5195","KZ_ZJLY":"全额财政补助","KZ_ZZZT": "正常","ZZBFJG": "杭州市机构编制委员会办公室","ZZBH": "1233**************K","ZZYXQJZRQ": "2023-01-01","ZZYXQQSRQ": "2018-01-01"
```

为了降低网络带宽占用，使用签名服务时建议先对上述字符串进行哈希运算，推荐采用SM3算法或SHA256算法。

推荐使用国家认可的CA机构颁发的SM2算法的数字证书，遵循《GM/T 0009 SM2密码算法使用规范》标准对上述字符串进行签名运算，得到的签名值格式也要符合上述标准。

B B

# 附 录 B
（规范性附录）
电子文件签名过程

可信电子证照文件如果采用OFD格式，则其数字签名应符合GB/T 36905。

可信电子证照文件如果采用非OFD版式文件格式，如PDF，则将整个电子文件作为一段数据，而不用去解析电子文件格式，方便电子证照库系统处理和统一验证。为了不破坏电子文件原文，电子文件的签名值原则上不嵌入到电子文件中，进行独立存储。

签名时，遵循 GM/T 0009 对整个电子文件数据进行签名运算，得到的签名值格式也要符合上述标准。推荐使用国家认可的CA机构颁发的SM2算法的数字证书。

为了降低所需网络带宽要求，调用签名服务器时推荐先对电子文件数据进行哈希运算，推荐哈希算法为SM3算法、SHA256算法。也可采用与文件存储服务一致的哈希算法，避免重复计算，方便验证。

C C

# 附 录 C
（资料性附录）
证照电子文件生成配置方式示例

## C.1 版式文件生成方式

可信电子证照库版式文件生成可采用证照底图套显数据方式,原则上生成与实体证照样式基本一致的电子文件，符合国家政务服务平台电子证照系列标准。如证照业务主管部门有特殊要求，在取得电子证照管理机构同意后，可自行设计电子文件格式。

## C.2 版式文件生成配置过程

版式文件生成的配置过程可以参照以下过程要求：

a) 证照数源单位提供与证照信息数据相对应的空白证照底图和样例。
b) 证照数源单位提供的底图图片分辨率 150dpi 以上，24 位以上彩色 JPG 或 PNG 图片，与实体证照比例为 1:1，单页大小控制在 800KB 以内。同时附上说明文档，内容包括：
   1) 各照面字段名称和内容的文字大小、颜色、位置；
   2) 如照面上有印章则说明印章位置、大小、样式规则。
c) 可信电子证照库管理机构根据证照数源单位提供的底图制作证照模板并上传到可信电子证照库。

D

D

# 附 录 D
（资料性附录）
共享返回数据结构示例

## D.1 证照信息数据共享返回数据结构示例

电子证照共享服务接口如采用一本证照一个接口的方式，其返回的证照信息数据格式描述举例如下：

```
[{
"ELC_LICENCE_NAME": "电子证照名称",
"ELC_LICENCE_DEPT": "电子证照来源部门",
"ELC_LICENCE_CODE": "电子证照编码",
"ELC_LICENCE_FILE": {
    "URL": "电子证照文件地址"
    "SIGN_CERT": "电子证照文件签名证书",
    "SIGN_VALUE": "电子证照文件签名值",
    "TSA": "电子证照文件时间戳签名值"
    },
"ELC_LICENCE_STRUCT": {
    "SIGN_CERT": "证照信息数据签名证书",
    "SIGN_VALUE": "证照信息数据签名值",
    "TSA": "证照信息数据时间戳签名值",
    "DATA": {
        "KZ_CSRQ": "出生日期 - yyyyMMdd",
        "ZZBH": "公民身份号码",
        "KZ_CZRKMZ": "民族",
        "ZZBFJG": "签发机关",
        "KZ_CZRKXB": "性别",
        "CZZT": "姓名",
        "ZZYXQJZRQ": "有效期截止日期 - yyyyMMdd",
        "ZZYXQQSRQ": "有效期起始日期 - yyyyMMdd",
        "KZ_CZRKZZ": "住址"
    }
},
"ELC_LICENCE_RELATES": [{
    "KZ_NAME": "附件名称",
    "KZ_FILE_URL": "附件文件地址",
    "SIGN_CERT": "附件签名证书",
    "SIGN_VALUE": "附件签名值",
    "TSA": "附件时间戳签名值"
    }]
```

## D.2 实时共享返回的数据结构示例

证明类实时共享接口返回的证照信息数据组织结构描述举例如下：

```
[{
    "ELC_LICENCE_NAME": "浙江省社会保险参保证明（单位专用）",
    "ELC_LICENCE_DEPT": "杭州市社会保险管理服务局",
    "ELC_LICENCE_CODE": "54c3af309a7c4533ac39d52889efed9a",
    "ELC_LICENCE_FILE": {
        "URL": "证明文件地址"
        "SIGN_CERT": "证明文件签名证书",
        "SIGN_VALUE": "证明文件签名值",
        "TSA": "证明文件时间戳签名值"
    },
    "ELC_LICENCE_STRUCT": {
        "SIGN_CERT":"证明信息数据签名证书",
        "SIGN_VALUE":"证明信息数据签名值",
        "TSA":"证明信息数据时间戳签名值",
        "DATA": {
              各厅局定义的具体证明数据
        }
    }
}]
```

E

E

# 附 录 E
（资料性附录）
验证过程说明

## E.1 在线验证

### E.1.1 概述

可信电子证照库提供在线验证服务，以实现对已共享证照信息数据和电子文件数据的签名验证功能。签名验证服务以接口的形式提供，使用者需以JSON格式传入待验签数据、签名结果值、签名证书公钥，验签接口返回验签结果。

### E.1.2 在线验证服务示例

以JAVA语言为例，采用HTTP REST方式提供在线验证服务，以XXXX证照示例如下：

```
public void testPost() throws Exception {
String full_name = "XXXX证";
String type_code = “1110**************1";
Map<String, String> data = new HashMap<>();
data.put("ZZBH","1233**********K");
data.put("CZZT","浙江省****委员会");
data.put("KZ_ZCDZ",浙江省杭州市**路");
data.put("KZ_FDDBR","王**");
data.put("KZ_ZJLY","全额财政补助");
data.put("KZ_ZCZJ","5195");
data.put("KZ_JBDW","杭州市****委员会");
data.put("ZZBFJG","杭州市机构编制委员会办公室");
data.put("ZZYXQQSRQ","2018-01-01");
data.put("ZZYXQJZRQ","2023-01-01");
HttpClient client = HttpClients.createDefault();
HttpPost post = new HttpPost("http://x.x.x.x/api/common/verf_licence_data/V1.0");

List<NameVaulePair> urlParameters = new ArrayList<>();
urlParameters.add(new BasicNameValuePair("full_name",full_name));
urlParameters.add(new BasicNameValuePair("type_code",type_code));
for (String key : data.keySet()) {
  urlParameters.add(new BasicNameValuePair(key,String.valueOf(data.get(key))));
}

try {
  File file = new File("XXXX证电子文件路径");
```

```
      FileInputStream inputFile = new FileInputStream(file);
      byte[] buffer = new byte[(int) file.length()];
      inputFile.read(buffer);
      inputFile.close();
      String file_content = BASE64Encoder().encode(buffer);
    urlParameters.add(new BasicNameValuePair("file_content",file_content));
      UrlEncodedFormEntity urlEncodedFormEntity = new UrlEncodedFormEntity(urlParameters,
"utf-8");
      post.setEntity(urlEncodedFormEntity);
      CloseableHttpResponse response = client.execute(post);
      int statusCode = response.getStatusLine().getStatusCode();
      if(statusCode == HttpStatus.SC_OK) {
        HttpEntity resEntity = response.getEntity();
        if(resEntity != null) {
           System.out.println(EntityUtils.toString(resEntity));
        }
      } else {
        System.out.println("请求失败！");
    }
    } catch (Exception e) {
      e.printStackTrace();
    } finally {
      response.close();
      client.close();
    }


    }
```

### E.1.3 验证输入参数示例

输入参数以JSON格式描述部分数据，举例如下：

```
    {
        "paramMap": {// 如果为空则不验证证照信息数据
        "ZZBH": "1233**************K",
        "CZZT": "浙江省****委员会",
        "KZ_ZCDZ": "浙江省杭州市**路",
        "KZ_FDDBR": "王**",
        "KZ_ZJLY": "全额财政补助",
        "KZ_ZCZJ": "5195",
        "KZ_JBDW": "杭州市****委员会",
        "ZZBFJG": "杭州市机构编制委员会办公室",
        "KZ_ZZZT": "正常",
        "ZZYXQQSRQ": "2018-01-01",
        "ZZYXQJZRQ": "2023-01-01"
```

```
        },
        "full_name":"XXXXX证",// 证照名称
        “type_code”:”111000000000****65001”,// 以国家政务平台发布的证照类型代码为准
        “file_content”:”文件base64编码”//如果为空，则不验证文件件
    }
```

### E.1.4 验证返回结果示例

返回结果以JSON格式描述举例如下：

```
    {
        "sdata_result": true //返回证照信息数据验签结果true(成功)或false(失败),表明证照信息是正确。
        “file_result”:true//返回电子文件验签结果true(成功)或false(失败),表明证照信息是正确
        “current_status”: 正常 // 返回证照当前状态，可能是吊销或注销等
        “collect_time”: “20190412122315 ” // 返回证照库当前数据归集时间（注：实时共享证照此返回值为证明生成时间），格式YYYYMMddHHmmss
    }
```

## E.2 离线验证

### E.2.1 概述

对于电子文件离线验证，如果签名前进行了哈希计算，需按照指定哈希算法进行哈希运算得到哈希值，然后使用共享接口返回的数字证书，遵循 GM/T 0009 进行签名验证。

对于证照信息数据离线验证,首先将证照信息数据按照共享接口返回的JSON格式进行组装,保持KEY值和VALUE值一致。

### E.2.2 证照信息验证示例

以XXXX证照为例，部分数据格式描述举例如下：

```
    {
        "ZZBH": "1233**************K",
        "CZZT": "浙江省****委员会",
        "KZ_ZCDZ": "浙江省杭州市**路",
        "KZ_FDDBR": "王**",
        "KZ_ZJLY": "全额财政补助",
        "KZ_ZCZJ": "5195",
        "KZ_JBDW": "杭州市****委员会",
        "ZZBFJG": "杭州市机构编制委员会办公室",
        "KZ_ZZZT": "正常",
        "ZZYXQQSRQ": "2018-01-01",
        "ZZYXQJZRQ": "2023-01-01"
    }
```

进行数字签名验证时，以上JSON串的Key值以ASCII顺序方式转换为键值相连的字符串。类似如下：

"CZZT":"浙江省****委员会","KZ_FDDBR":"王**","KZ_JBDW":"杭州市****委员会","KZ_ZCDZ":"浙江省杭州市**路","KZ_ZCZJ":"5195","KZ_ZJLY":"全额财政补助","KZ_ZZZT": "正常","ZZBFJG": "杭州市机构编制委员会办公室 ","ZZBH": "1233**********K","ZZYXQJZRQ": "2023-01-01","ZZYXQQSRQ": "2018-01-01"

## 参考文献

[1] GM/T 0009 SM2密码算法使用规范