ICS 35.040
L 80
备案号：58552—2017

GM

# 中华人民共和国密码行业标准

GM/T 0047—2016

# 安全电子签章密码检测规范

**Cryptography test specification for secure electronic seal**

2016-12-23 发布　　2016-12-23 实施

国家密码管理局　　发布

# 目　　次

# 前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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。

本标准由密码行业标准化技术委员会提出并归口。

本标准主要起草单位：北京数字认证股份有限公司、国家密码管理局商用密码检测中心、兴唐通信科技有限公司、上海市数字证书认证中心有限公司、上海格尔软件股份有限公司、卫士通信息产业股份有限公司。

本标准主要起草人：刘伟、李大为、邓开勇、罗鹏、肖秋林、马爱良、李冬、朱亚飞、陈曦、韩琳、阎夏强、张周群、傅大鹏等。

# 安全电子签章密码检测规范

## 1 范围

本标准规范了安全电子签章的密码检测内容、检测要求、检测方法以及合格判定准则。

本标准适用于按照 GM/T 0031—2014 研制的安全电子签章系统密码技术的检测。

## 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 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法

GM/T 0006 密码应用标识规范

GM/T 0009 SM2 密码算法使用规范

GM/T 0031—2014 安全电子签章密码应用技术规范

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**电子文件 electronic document**

在数字设备及环境中形成，以数码形式存储于磁带、磁盘、光盘等载体，依赖计算机等数字设备阅读、处理，并可在通信网络上传送的文件。本文中签章原文指电子文件。

3.2

**电子印章 electronic stamp**

一种由制作者签名的包括持有者信息和图形化内容的数据，可用于签署电子文件。

3.3

**电子签章 electronic seal**

使用电子印章签署电子文件的过程。

3.4

**电子签章数据 electronic seal data**

电子签章过程产生的包含电子印章信息和签名信息的数据。

3.5

**电子印章系统 electronic seal system**

包含电子印章管理系统和电子签章软件，其中电子印章管理系统包括印章管理员管理、电子印章制作与管理、电子印章验证服务以及安全审计等功能。电子签章软件是使用电子印章对各类电子文件进行电子签章的软件。

3.6

**制章人 electronic stamp maker**

电子印章系统中具有签署和管理电子印章信息权限的管理员。管理员的数字证书可以是单位证书

或个人证书，电子印章中的图片和信息必须经制章人的数字证书进行数字签名。

3.7

**签章人　electronic seal signer**

电子印章系统中对电子文件进行签章操作的签章持有用户。

3.8

**SM2 算法　SM2 algorithm**

由 GB/T 32918《信息安全技术　SM2 椭圆曲线公钥密码算法》定义的一种算法。

3.9

**SM3 算法　SM3 algorithm**

由 GB/T 32905《信息安全技术　SM3 密码杂凑算法》定义的一种算法。

## 4　缩略语

下列缩略语适用于本文件。

PKCS　Public-Key Cryptography Standards 公钥密码标准

## 5　检测内容

### 5.1　检测对象

检测对象为遵照 GM/T 0031—2014 研制的电子印章系统中的密码算法应用，要求检测对象配用的密码产品应是经国家密码管理主管部门批准使用的产品。

### 5.2　数字签名算法检测

检测对象支持的算法和签名数据结构应符合 GM/T 0031—2014 的要求，应支持 SM2 算法的数字签名功能，SM2 算法签名数据结构应遵循 GM/T 0009。

### 5.3　电子印章数据检测

电子印章管理系统应能正确生成电子印章数据，电子印章数据的数据内容和编码格式需满足 GM/T 0031—2014 中 6.1.1 的要求。

### 5.4　电子印章验证检测

#### 5.4.1　概述

电子印章系统应提供电子印章验证功能，电子印章的验证应包括印章数据格式验证、印章签名值验证、制章人证书有效性验证、印章有效期验证等 4 项验证。

#### 5.4.2　印章数据格式验证检测

电子印章系统在进行电子印章验证时应提供电子印章数据格式验证功能，验证电子印章数据格式是否满足 GM/T 0031—2014 中 6.1.1 的数据格式要求。

#### 5.4.3　印章签名值验证检测

电子印章系统在进行电子印章验证时应提供电子印章签名值验证功能，根据印章信息数据、制章人

证书和签名算法标识验证电子印章签名信息中的签名值是否正确。

#### 5.4.4 制章人证书有效性验证检测

电子印章系统在进行电子印章验证时应提供制章人证书有效性验证功能，验证项至少包括：制章人证书信任链验证、制章人证书有效期验证、制章人证书是否被吊销、密钥用法是否正确。

#### 5.4.5 印章有效期验证检测

电子印章系统在进行电子印章验证时，应提供电子印章有效期验证功能，盖章时应能够根据印章属性中的印章有效起始日期和有效终止日期，验证电子印章是否过期。

### 5.5 电子签章数据检测

电子印章系统应能正确生成电子签章数据，电子签章数据的数据内容和编码格式需要满足GM/T 0031—2014 中 6.2.1 的要求。

### 5.6 电子签章验证检测

#### 5.6.1 概述

电子印章系统应提供电子签章验证功能。电子签章的验证应包括：电子签章数据格式验证、电子签章签名值验证、签章人证书有效性验证、签章人证书列表验证、签章时间有效期验证、签章原文杂凑验证、签章中电子印章有效性验证共 7 项验证。

#### 5.6.2 电子签章数据格式验证检测

电子印章系统应提供电子签章数据格式验证功能，验证电子签章数据格式是否满足 GM/T 0031—2014 中 6.2.1 的数据格式要求。

#### 5.6.3 电子签章签名值验证检测

电子印章系统应提供电子签章签名值验证功能，能够基于待验证数据验证电子签章签名值是否正确。待验证数据包括：版本号、电子印章、时间信息、原文杂凑值、原文属性信息、签章人证书、签名算法标识。

#### 5.6.4 签章人证书有效性验证检测

电子印章系统应提供签章人证书验证功能，验证签章人证书有效性，验证项至少包括：签章人证书信任链验证、签章人证书有效期验证、签章人证书是否被吊销、密钥用法是否正确。

#### 5.6.5 签章人证书列表验证检测

电子印章系统应提供签章人证书是否在电子印章签章人证书列表中的验证功能。

#### 5.6.6 签章时间有效期验证检测

电子印章系统应提供电子签章时间有效期验证功能。能够根据签章人数字证书有效期和电子签章中的时间信息，判断签章时间的有效性。支持以下判断规则：

a) 如果签章时间处于签章人数字证书有效期内，并且证书有效，则签章时间有效；

b) 如果签章时间不在签章人数字证书有效期内，则签章时间无效；

c) 如果签章时间处于签章人数字证书有效期内，但是证书在签章之前已被吊销，则签章时间

无效；

d） 如果签章时间处于签章人数字证书有效期内，但是证书在签章之后被吊销，则签章时间有效。

#### 5.6.7 签章原文杂凑验证检测

电子印章系统应提供电子签章原文杂凑验证功能，如果签章原文改变或电子签章数据中的原文杂凑值改变，都会导致验证失败。

#### 5.6.8 签章中电子印章有效性验证检测

在验证电子签章时，电子印章系统应提供电子印章有效性验证功能和签章时间是否处于印章有效期内的验证功能。

## 6 检测方法

### 6.1 数字签名算法检测

依据签名原文对签名结果进行验证，并查看签名结果数据格式，如果符合 5.2 检测内容，则测试通过；否则，测试失败。

### 6.2 电子印章数据检测

把被检测电子印章管理系统生成的电子印章数据转化为可视化格式，检查数据内容和编码格式的正确性。如果数据内容和编码格式符合 5.3 检测内容要求，则测试通过；否则测试失败。

### 6.3 电子印章验证检测

#### 6.3.1 概述

电子印章的验证应包括印章数据格式验证、印章签名值验证、制章人证书有效性验证、印章有效期验证共 4 项验证，本检测分别针对这 4 个方面进行验证，若 4 项验证的检测均通过，则电子印章验证功能的检测通过。

#### 6.3.2 印章数据格式验证检测

检测步骤如下：

a） 输入满足 GM/T 0031—2014 中 6.1.1 的数据格式要求的电子印章数据，然后使用电子印章系统进行验证，如果验证通过，则本步测试通过；否则，测试失败。

b） 输入不满足 GM/T 0031—2014 中 6.1.1 的数据格式要求的电子印章数据，然后使用电子印章系统进行验证，如果验证失败，则本步测试通过；否则，测试失败。

上面 2 步都通过，则本项测试通过；否则，测试失败。

#### 6.3.3 印章签名值验证检测

检测步骤如下：

a） 输入正确的电子印章数据，然后使用电子印章系统进行验证，如果验证通过，则本步测试通过；否则，测试失败。

b） 输入签名值错误的电子印章数据，然后使用电子印章系统进行验证，如果验证失败，则本步测试通过；否则，测试失败。

c） 更改正确电子印章数据的签名原文，然后使用电子印章系统进行验证，如果验证失败，则本步

测试通过；否则，测试失败。

上面3步都通过，则本项测试通过；否则，测试失败。

#### 6.3.4 制章人证书有效性验证检测

检测步骤如下：

a) 电子印章系统使用正确的证书信任链，验证在有效期内、未吊销、密钥用法正确的制章人证书是否有效。如果验证通过，则本步测试通过；否则，测试失败。

b) 电子印章系统使用错误的证书信任链，验证制章人证书是否有效。如果验证失败，则本步测试通过；否则，测试失败。

c) 电子印章系统使用制章时间处于制章人证书有效期之外的电子印章，验证制章人证书是否有效。如果验证失败，则本步测试通过；否则，测试失败。

d) 电子印章系统验证已吊销的制章人证书是否有效。如果验证失败，则本步测试通过；否则，测试失败。

e) 电子印章系统验证非签名密钥用法的制章人证书是否有效。如果验证失败，则本步测试通过；否则，测试失败。

上面5步都通过，则本项测试通过；否则，测试失败。

#### 6.3.5 印章有效期验证检测

检测步骤如下：

a) 当前系统时间处于印章有效期之内，验证印章有效期，如果验证通过，则本步测试通过；否则，测试失败。

b) 当前系统时间处于印章有效期之外，验证印章有效期，如果验证失败，则本步测试通过；否则，测试失败。

上面2步都通过，则本项测试通过；否则，测试失败。

### 6.4 电子签章数据检测

使用电子签章数据可视化工具，把被检测的电子印章系统生成的电子签章数据转化为可视化格式，检查数据内容和编码格式的正确性。如果数据内容和编码格式符合5.5检测内容要求，则测试通过；否则测试失败。

### 6.5 电子签章验证检测

#### 6.5.1 概述

电子签章的验证应包括：电子签章数据格式验证、电子签章签名值验证、签章人证书有效性验证、签章人证书列表验证、签章时间有效期验证、签章原文杂凑验证、签章中电子印章有效性验证共7项验证，本检测分别针对这7个方面进行验证，若7项验证的检测均通过，则电子签章验证功能的检测通过。

#### 6.5.2 电子签章数据格式验证检测

检测步骤如下：

a) 输入正确数据格式的电子签章数据，然后使用电子印章系统进行验证，如果验证通过，则本步测试通过；否则，测试失败。

b) 输入错误数据格式的电子签章数据，然后使用电子印章系统进行验证，如果验证失败，则本步测试通过；否则，测试失败。

上面 2 步都通过，则本项测试通过；否则，测试失败。

#### 6.5.3 电子签章签名值验证检测

检测步骤如下：

a) 输入签名值正确的电子签章数据，然后使用电子印章系统进行验证，如果验证通过，则本步测试通过；否则，测试失败。

b) 输入签名值错误的电子签章数据，然后使用电子印章系统进行验证，如果验证失败，则本步测试通过；否则，测试失败。

上面 2 步都通过，则本项测试通过；否则，测试失败。

#### 6.5.4 签章人证书有效性验证检测

检测步骤如下：

a) 电子印章系统使用正确的证书信任链，验证在有效期内、未吊销、密钥用法正确的签章人证书，如果验证通过，则本步测试通过；否则，测试失败。

b) 电子印章系统使用错误的证书信任链，验证签章人证书，如果验证失败，则本步测试通过；否则，测试失败。

c) 电子印章系统验证处于非电子签章有效期内的签章人证书，如果验证失败，则本步测试通过；否则，测试失败。

d) 电子印章系统验证非签名密钥用法的签章人证书，如果验证失败，则本步测试通过；否则，测试失败。

e) 电子印章系统验证吊销时间在签章时间之前的签章人证书，如果验证失败，则本步测试通过；否则，测试失败。

f) 电子印章系统验证吊销时间在签章时间之后的签章人证书，如果验证通过，则本步测试通过；否则，测试失败。

上面 6 步都通过，则本项测试通过；否则，测试失败。

#### 6.5.5 签章人证书列表验证检测

检测步骤如下：

a) 输入签章人证书在电子印章签章人证书列表中的电子签章，使用电子印章系统进行验证，如果验证通过，则本步测试通过，否则，测试失败。

b) 输入签章人证书不在电子印章签章人证书列表中的电子签章，使用电子印章系统进行验证，如果验证失败，则本步测试通过，否则，测试失败。

上面 2 步都通过，则本项测试通过；否则，测试失败。

#### 6.5.6 签章时间有效期验证检测

构造符合本标准 5.6.6 检测内容的电子签章和签章人证书，依次进行验证；

如果 5.6.6 所述 4 步测试全面通过，则本项测试通过；否则测试失败。

#### 6.5.7 签章原文杂凑验证检测

检测步骤如下：

a) 输入正确的电子签章及对应的签章原文，使用电子印章系统验证签章原文杂凑值，如果验证通过，则本步测试通过，否则，测试失败。

b) 输入正确的电子签章及修改后的签章原文，使用电子印章系统验证签章原文杂凑值，如果验证

失败，则本步测试通过，否则，测试失败。

c) 输入修改了杂凑值的电子签章及对应的签章原文，使用电子印章系统验证签章原文杂凑值，如果验证失败，则本步测试通过，否则，测试失败。

上面3步都通过，则本项测试通过；否则，测试失败。

#### 6.5.8 签章中电子印章有效性验证检测

检测步骤如下：

a) 电子印章有效性检测方法依据6.3。

b) 输入签章时间处于电子印章有效期内的电子签章，使用电子印章系统进行有效性验证，如果测试通过，则本步测试通过；否则，测试失败。

c) 输入签章时间处于非电子印章有效期内的电子签章，使用电子印章系统进行有效性验证，如果测试不通过，则本步测试通过；否则，测试失败。

上面3步都通过，则本项测试通过；否则，测试失败。

## 7 送检技术文档要求

按照国家密码管理主管部门检测要求提交相关文档资料，作为检测依据。文档资料应包含但不限于以下内容：

a) 软件的结构框图、流程图和基本功能的源代码；

b) 技术工作总结报告；

c) 安全性设计报告；

d) 用户手册。

## 8 合格判定条件

本标准中任何一项检测结果不合格，即判定为产品不合格。