ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0047—2024
代替 GM/T 0047—2016

安全电子签章密码检测规范

Cryptography test specification for secure electronic seal signature

2024-12-27 发布　　2025-07-01 实施

国家密码管理局　　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。

本文件代替GM/T 0047—2016《安全电子签章密码检测规范》，与GM/T 0047—2016相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 更改了“检测对象”，由笼统的“密码算法应用”细化明确为“数字签名算法”等（见4.1，2016年版的5.1）；
b) 增加了电子印章在制章者证书过期情况下的检测方法（见5.3.5）；
c) 增加了电子印章制章时间有效性的检测内容和检测方法（见4.4.6和5.3.6）；
d) 增加了电子印章时间戳的检测内容和检测方法（见4.4.4和4.6.4）；
e) 增加了电子签章时间戳的检测内容和检测方法（见5.3.4和5.5.4）；
f) 更改了电子签章中电子印章有效性验证方法，将方法中电子签章时间是否在电子印章有效期的验证步骤统一调整到电子签章时间有效性验证方法中（见5.5.7和5.5.9，2016年版的6.5.8）；
g) 更改了“送检技术文档要求”，增加了产品实物图的文档要求（见第6章，2016年版的第7章）；
h) 更改了“判定规则”，明确判定结论由“产品不合格”更改为“密码技术检测不通过”（见第7章，2016年版的第8章）。

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。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：北京数字认证股份有限公司、商用密码检测认证中心、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、中电科网络安全科技股份有限公司。

本文件主要起草人：刘岩、赵子轩、谢峰、傅大鹏、刘中、马彩云、李红芳、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、李庚昱、郑强、牛鹏飞、雷银花、高超航。

本文件及其所代替文件的历次版本发布情况为：

——2016年首次发布版为GM/T 0047—2016；

——本次为第一次修订。

安全电子签章密码检测规范

1 范围

本文件规定了安全电子签章密码技术的检测内容、检测方法、送检技术文档要求以及合格判定条件。

本文件适用于按照 GM/T 0031 研制的电子印章系统中使用的数字签名算法、电子印章数据、电子印章数据验证、电子签章数据以及电子签章数据验证相关密码技术的检测。

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 20520—2006 信息安全技术 公钥基础设施 时间戳规范

GB/T 25069 信息安全技术 术语

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32918(所有部分) 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 35276 信息安全技术 SM2 密码算法使用规范

GM/T 0031 安全电子签章密码技术规范

GM/Z 4001 密码术语

3 术语和定义

GB/T 25069、GB/T 32905、GB/T 32918 和 GM/Z 4001 界定的以及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。

注：本文件中签章原文指电子文件。

3.2

制章者 electronic seal maker

电子印章系统中具有电子印章制作和管理权限的机构。

注：电子印章中的图像和相关信息应经制章者进行数字签名，电子印章中的制章者证书应是该机构的单位证书。

3.3

签章者 electronic seal signer

电子印章的所有者。

3.4

电子印章 electronic seal

由制章者签名的包括签章者信息和图形化内容的数据，能用于签署电子文件。

3.5

电子签章　electronic seal signing

使用电子印章签署电子文件的过程。

注：电子签章能实现与纸质文件盖章操作相似的可视效果，能保障数据来源的真实性、数据完整性以及签名人行为的不可否认性。

[来源：GB/T 25069—2022，3.120，有修改]

3.6

电子签章数据　electronic seal signing data

电子签章过程产生的包含电子印章、原文信息和数字签名等信息的数据。

3.7

电子印章系统　electronic seal system

具有电子印章管理、制作、签章、验章及日志审计等功能的系统。

3.8

SM2 算法　SM2 algorithm

由 GB/T 32918 定义的一种椭圆曲线公钥密码算法。

3.9

SM3 算法　SM3 algorithm

由 GB/T 32905 定义的一种密码杂凑算法。

4　检测内容

4.1　检测对象

检测对象为电子印章系统中所使用的数字签名算法、电子印章数据、电子印章验证、电子签章数据以及电子签章验证。

注：电子印章系统所配用的密码产品，是已经获得商用密码产品认证证书且处于有效期内的产品。

4.2　数字签名算法检测

验证数字签名算法是否符合 GM/T 0031 中的要求。如果签名算法使用 SM2，则应验证签名数据结构是否符合 GB/T 35276 的要求。

4.3　电子印章数据检测

验证电子印章的内容和编码格式是否符合 GM/T 0031 中电子印章格式的要求。

4.4　电子印章验证检测

4.4.1　概述

电子印章数据验证检测包括电子印章数据格式验证、电子印章签名值验证、电子印章时间戳验证（适用时）、制章者证书有效性验证、制章时间有效性验证和电子印章有效期验证等六项检测内容。

4.4.2　电子印章数据格式验证

验证电子印章数据格式是否符合 GM/T 0031 中电子印章格式的要求。

4.4.3　电子印章签名值验证

根据印章信息数据、制章者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。

4.4.4 电子印章时间戳验证

如果电子印章包含时间戳，则应验证时间戳格式是否符合 GB/T 20520—2006 中 8.4.2 规定的 TimeStampToken 格式要求，验证时间戳的验证方法是否符合 GB/T 20520—2006 中 7.5.2 规定的要求。

4.4.5 制章者证书有效性验证

验证制章者证书是否有效，验证项至少包括：制章者证书信任链验证、制章者证书有效期验证、制章者证书是否被吊销、密钥用法是否正确。

4.4.6 制章时间有效性验证

根据制章者证书有效期、时间戳的时间验证制章时间是否有效。

4.4.7 电子印章有效期验证

根据印章属性中的印章有效起始日期和有效终止日期，验证电子印章是否在有效期。

4.5 电子签章数据检测

验证电子签章数据的内容和编码格式是否符合 GM/T 0031 中电子签章数据格式的要求。

4.6 电子签章验证检测

4.6.1 概述

电子签章数据验证检测包括电子签章数据格式验证、电子签章签名值验证、电子签章时间戳验证（适用时）、签章者证书列表验证、签章者证书有效性验证、电子签章时间有效性验证、电子签章原文杂凑验证和电子签章中电子印章有效性验证等八项检测内容。

4.6.2 电子签章数据格式验证

验证电子签章数据格式是否符合 GM/T 0031 中电子签章数据格式的要求。

4.6.3 电子签章签名值验证

根据签章信息、签章者证书和签名算法标识验证电子签章签名值是否正确。签章信息包括：版本号、电子印章、签章时间、原文杂凑值、原文属性、自定义数据。

4.6.4 电子签章时间戳验证

如果电子签章包含时间戳，则应验证时间戳格式是否符合 GB/T 20520—2006 中 8.4.2 规定的 TimeStampToken 格式要求，验证时间戳的验证方法是否符合 GB/T 20520—2006 中 7.5.2 规定的要求。

4.6.5 签章者证书信息列表验证

验证签章者证书是否包含在电子印章签章者证书信息列表中。

4.6.6 签章者证书有效性验证

验证签章者证书是否有效，验证项至少包括：签章者证书信任链验证、签章者证书有效期验证、签章

者证书是否被吊销、密钥用法是否正确。

4.6.7 电子签章时间有效性验证

根据签章者数字证书有效期、电子印章有效期、时间戳的时间，验证签章时间是否在有效期内。

4.6.8 电子签章原文杂凑验证

根据原文和杂凑算法验证杂凑值是否正确。如果杂凑算法使用 SM3，则应对原文依据 GB/T 32905 进行杂凑处理。

4.6.9 电子签章中电子印章有效性验证

按照 4.3 和 4.4 的检测内容验证电子签章数据中电子印章是否有效。

5 检测方法

5.1 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。

检测判定：符合 4.2 检测内容要求，则本项测试通过；否则，测试不通过。

5.2 电子印章数据检测

使用电子印章数据可视化工具，把被检测电子印章系统生成的电子印章转化为可视化格式，检查内容和编码格式的正确性。

检测判定：内容和编码格式符合 4.3 检测内容要求，则本项测试通过；否则，测试不通过。

5.3 电子印章验证检测

5.3.1 概述

电子印章验证检测主要对 4.4 电子印章验证相关检测内容进行检测。下面六项测试均通过，则电子印章验证检测通过。

5.3.2 电子印章格式验证

检测步骤：

a) 输入符合 GM/T 0031 中电子印章格式要求的电子印章，使用电子印章系统进行验证；
   检测判定：验证通过，则本步测试通过；否则，测试不通过；

b) 输入不符合 GM/T 0031 中电子印章格式要求的电子印章，使用电子印章系统进行验证；
   检测判定：验证失败，则本步测试通过；否则，测试不通过。

上面 2 步都通过，则本项测试通过；否则，测试不通过。

5.3.3 电子印章签名值验证

检测步骤：

a) 输入正确的电子印章，使用电子印章系统进行验证；
   检测判定：验证通过，则本步测试通过；否则，测试不通过；

b) 输入签名值错误的电子印章，使用电子印章系统进行验证；
   检测判定：验证失败，则本步测试通过；否则，测试不通过。

上面 2 步都通过，则本项测试通过；否则，测试不通过。

5.3.4 电子印章时间戳验证

如果电子印章中包含时间戳，则应进行时间戳的验证。其中时间戳格式应符合 GB/T 20520—2006 中 8.4.2 规定的 TimeStampToken 格式要求，时间戳的验证方法应符合 GB/T 20520—2006 中 7.5.2 的要求。

检测步骤：

a) 输入符合时间戳格式要求的电子印章，使用电子印章系统进行验证；
   检测判定：验证通过，则本步测试通过；否则，测试不通过；
b) 输入不符合时间戳格式要求的电子印章，使用电子印章系统进行验证；
   检测判定：验证失败，则本步测试通过；否则，测试不通过；
c) 输入符合时间戳验证方法要求的电子印章，使用电子印章系统进行验证；
   检测判定：验证通过，则本步测试通过；否则，测试不通过；
d) 输入不符合时间戳验证方法要求的电子印章，使用电子印章系统进行验证；
   检测判定：验证失败，则本步测试通过；否则，测试不通过。

上面 4 步都通过，则本项测试通过；否则，测试不通过。

5.3.5 制章者证书有效性验证

检测步骤：

a) 输入正确的证书信任链和正确制章者证书的电子印章，使用电子印章系统进行验证；
   检测判定：验证通过，则本步测试通过；否则，测试不通过；
b) 输入错误的证书信任链，使用电子印章系统进行验证；
   检测判定：验证失败，则本步测试通过；否则，测试不通过；
c) 输入制章者证书已过期，且制章时间处于证书有效期之内的电子印章，使用电子印章系统进行验证；
   检测判定：验证通过，则本步测试通过；否则，测试不通过；
d) 输入制章者证书吊销时间在制章时间之前的电子印章，使用电子印章系统进行验证；
   检测判定：验证失败，则本步测试通过；否则，测试不通过；
e) 输入制章者证书吊销时间在制章时间之后的电子印章，使用电子印章系统进行验证；
   检测判定：验证通过，则本步测试通过；否则，测试不通过；
f) 输入制章者证书密钥用法为非签名密钥用法的电子印章，使用电子印章系统进行验证；
   检测判定：验证失败，则本步测试通过；否则，测试不通过。

上面 6 步都通过，则本项测试通过；否则，测试不通过。

5.3.6 制章时间有效性验证

检测步骤：

a) 如果电子印章中包含时间戳，则输入制章时间不在时间戳时间之后的电子印章，使用电子印章系统进行验证；
   检测判定：验证通过，则本步测试通过；否则，测试不通过；
b) 如果电子印章中包含时间戳，则输入制章时间处于时间戳时间之后的电子印章，使用电子印章系统进行验证；
   检测判定：验证失败，则本步测试通过；否则，测试不通过；
c) 输入制章时间处于制章者数字证书有效期内，并且证书有效的电子印章，使用电子印章系统进

行验证；

检测判定：验证通过，则本步测试通过；否则，测试不通过；

d) 输入制章时间不在制章者数字证书有效期内的电子印章，使用电子印章系统进行验证，验证失败；

检测判定：验证通过，则本步测试通过；否则，测试不通过；

e) 输入制章时间处于制章者数字证书有效期内，但是证书在制章之前已被吊销的电子印章，使用电子印章系统进行验证；

检测判定：验证失败，则本步测试通过；否则，测试不通过；

f) 输入制章时间处于制章者数字证书有效期内，但是证书在制章之后被吊销的电子印章，使用电子印章系统进行验证；

检测判定：验证通过，则本步测试通过；否则，测试不通过；

g) 如果电子印章中包含时间戳，则按照步骤 c)～步骤 f)验证时间戳中时间的有效性；

检测判定：全部验证通过，则本步测试通过；否则，测试不通过。

上面 7 步都通过，则本项测试通过；否则，测试不通过。

5.3.7 电子印章有效期验证

检测步骤：

a) 输入当前系统时间处于电子印章有效期之内的电子印章，使用电子印章系统进行验证；

检测判定：验证通过，则本步测试通过；否则，测试不通过；

b) 输入当前系统时间处于电子印章有效期之外的电子印章，使用电子印章系统进行验证；

检测判定：验证失败，则本步测试通过；否则，测试不通过。

上面 2 步都通过，则本项测试通过；否则，测试不通过。

5.4 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。

检测判定：数据内容和编码格式符合 4.5 检测内容要求，则测试通过；否则，测试不通过。

5.5 电子签章验证检测

5.5.1 概述

电子签章数据验证检测主要对 4.6 电子签章验证相关检测内容进行检测。下面八项测试均通过，则电子签章验证检测通过。

5.5.2 电子签章数据格式验证

检测步骤：

a) 输入正确数据格式的电子签章数据，使用电子印章系统进行验证；

检测判定：验证通过，则本步测试通过；否则，测试不通过；

b) 输入错误数据格式的电子签章数据，使用电子印章系统进行验证；

检测判定：验证失败，则本步测试通过；否则，测试不通过。

上面 2 步都通过，则本项测试通过；否则，测试不通过。

5.5.3 电子签章签名值验证

检测步骤：

a) 输入签名值正确的电子签章数据，使用电子印章系统进行验证；

检测判定：验证通过，则本步测试通过；否则，测试不通过；

b） 输入签名值错误的电子签章数据，使用电子印章系统进行验证；

检测判定：验证失败，则本步测试通过；否则，测试不通过。

上面 2 步都通过，则本项测试通过；否则，测试不通过。

5.5.4 电子签章时间戳验证

如果电子签章数据中包含时间戳，则应进行时间戳的验证。其中时间戳格式应符合 GB/T 20520—2006 中 8.4.2 规定的 TimeStampToken 格式要求，时间戳的验证方法应符合 GB/T 20520—2006 中 7.5.2 的要求。

检测步骤：

a） 输入时间戳格式符合要求的电子签章数据，使用电子印章系统进行验证；

检测判定：验证通过，则本步测试通过；否则，测试不通过；

b） 输入时间戳格式不符合要求的电子签章数据，使用电子印章系统进行验证；

检测判定：验证失败，则本步测试通过；否则，测试不通过；

c） 输入符合时间戳验证方法要求的电子签章数据，使用电子印章系统进行验证；

检测判定：验证通过，则本步测试通过；否则，测试不通过；

d） 输入不符合时间戳验证方法要求的电子签章数据，使用电子印章系统进行验证；

检测判定：验证失败，则本步测试通过；否则，测试不通过。

上面 4 步都通过，则本项测试通过；否则，测试不通过。

5.5.5 签章者证书信息列表验证

检测步骤：

a） 输入签章者证书在电子印章签章者证书列表中的电子签章数据，使用电子印章系统进行验证；

检测判定：验证通过，则本步测试通过；否则，测试不通过；

b） 输入签章者证书不在电子印章签章者证书列表中的电子签章数据，使用电子印章系统进行验证；

检测判定：验证失败，则本步测试通过；否则，测试不通过。

上面 2 步都通过，则本项测试通过；否则，测试不通过。

5.5.6 签章者证书有效性验证

检测步骤：

a） 输入正确的证书信任链及正确签章者证书的电子签章数据，使用电子印章系统进行验证；

检测判定：验证通过，则本步测试通过；否则，测试不通过；

b） 输入错误的证书信任链，使用电子印章系统进行验证；

检测判定：验证失败，则本步测试通过；否则，测试不通过；

c） 输入签章者证书已过期，且签章时间处于证书有效期之内的电子签章数据，使用电子印章系统进行验证；

检测判定：验证通过，则本步测试通过；否则，测试不通过；

d） 输入签章者证书吊销时间在签章时间之前的电子签章数据，使用电子印章系统进行验证；

检测判定：验证失败，则本步测试通过；否则，测试不通过；

e） 输入签章者证书吊销时间在签章时间之后的电子签章数据，使用电子印章系统进行验证；

检测判定：验证通过，则本步测试通过；否则，测试不通过；

f） 输入签章者证书密钥用法为非签名密钥用法的电子签章数据，使用电子印章系统进行验证；

检测判定：验证失败，则本步测试通过；否则，测试不通过。

上面 6 步都通过，则本项测试通过；否则，测试不通过。

5.5.7 电子签章时间有效性验证

检测步骤：

a) 如果电子签章数据中包含时间戳，则输入签章时间不在时间戳时间之后的电子签章数据，使用电子印章系统进行验证；

检测判定：验证通过，则本步测试通过；否则，测试不通过；

b) 如果电子签章数据中包含时间戳，则输入签章时间处于时间戳时间之后的电子签章数据，使用电子印章系统进行验证；

检测判定：验证失败，则本步测试通过；否则，测试不通过；

c) 输入签章时间处于签章者数字证书有效期内，并且证书有效的电子签章数据，使用电子印章系统进行验证；

检测判定：验证通过，则本步测试通过；否则，测试不通过；

d) 输入签章时间不在签章者数字证书有效期内的电子签章数据，使用电子印章系统进行验证；

检测判定：验证失败，则本步测试通过；否则，测试不通过；

e) 输入签章时间处于签章者数字证书有效期内，但是证书在签章之前已被吊销的电子签章数据，使用电子印章系统进行验证；

检测判定：验证失败，则本步测试通过；否则，测试不通过；

f) 输入签章时间处于签章者数字证书有效期内，但是证书在签章之后被吊销的电子签章数据，使用电子印章系统进行验证；

检测判定：验证通过，则本步测试通过；否则，测试不通过；

g) 输入签章时间处于电子印章有效期内的电子签章数据，然后使用电子印章系统进行有效性验证；

检测判定：验证通过，则本步测试通过；否则，测试不通过；

h) 输入签章时间不在电子印章有效期内的电子签章数据，然后使用电子印章系统进行有效性验证；

检测判定：验证失败，则本步测试通过；否则，测试不通过；

i) 如果电子签章数据中包含时间戳，则按照步骤 c)～步骤 h)验证时间戳中时间的有效性；

检测判定：全部验证通过，则本步测试通过；否则，测试不通过。

上面 9 步都通过，则本项测试通过；否则，测试不通过。

5.5.8 电子签章原文杂凑验证

检测步骤：

a) 输入正确的电子签章数据及对应的签章原文，然后使用电子印章系统验证签章原文杂凑值；

检测判定：验证通过，则本步测试通过；否则，测试不通过；

b) 输入正确的电子签章数据及修改后的签章原文，然后使用电子印章系统验证签章原文杂凑值；

检测判定：验证失败，则本步测试通过；否则，测试不通过；

c) 输入修改了杂凑值的电子签章数据及对应的签章原文，然后使用电子印章系统验证签章原文杂凑值；

检测判定：验证失败，则本步测试通过；否则，测试不通过。

上面 3 步都通过，则本项测试通过；否则，测试不通过。

5.5.9 电子签章中电子印章有效性验证

检测步骤：

电子印章有效性检测方法依据 5.3。

检测判定：验证通过，则本项测试通过；否则，测试不通过。

6 送检技术文档要求

按照商用密码检测认证机构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) 电子印章系统的结构框图、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；
e) 产品实物图。

7 判定规则

本文件在第 5 章中给出了具体每项检测内容对应的检测步骤和检测判定，其中任何一项检测的检测结果不通过，则判定电子印章系统密码技术检测不通过。

中华人民共和国密码
行业标准
安全电子签章密码检测规范
GM/T 0047—2024
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
网址 www.spc.net.cn
总编室:(010)68533533　发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1　字数 23 千字
2025年6月第1版　2025年6月第1次印刷
*
书号:155066·2-39151　定价 31.00 元

GM/T 0047-2024