ICS 03.060
A11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0161-2018

保险电子签名技术应用规范

Specification for insurance electronic signature technology application

××××-××-××发布　　××××-××-××实施

中国银行保险监督管理委员会　发布

目　　次

前　言

本标准按照 GB/T1.1-2009 给出的规则起草。

本标准由全国金融标准化技术委员会保险分技术委员会提出并归口管理。

本标准起草单位：中国太平洋人寿保险股份有限公司、中国平安保险（集团）股份有限公司、中国人寿保险股份有限公司。

本标准主要起草人：宋威、韩梅、李豫洲、吴芳、黄飞生、邓华威、赵亮、陈刚、徐东升。

本标准为首次制定。

引　言

本规范基于对国内外保险行业和其他相关行业电子签名发展与应用情况的调研，重点研究国内保险行业电子签名应用的现状、面临的主要问题和发展趋势，总结国内保险行业电子签名应用的主要业务模式和技术架构编制而成的。

本规范作为保险业电子签名技术应用的规范，为全行业电子签名技术的应用提供必要的参考，为全行业适应移动互联时代发展要求，探索应用新技术创新服务模式打下坚实的基础。

保险电子签名技术应用规范

1 范围

本规范规定了保险电子签名技术应用中应遵循的技术要求、系统管理要求和应用要求。

本规范适用于中华人民共和国境内保险行业相关机构承保、核保、保全、理赔、调查等涉及保险电子单据签名的业务活动。

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 20518 信息安全技术公钥基础设施数字证书格式

GB/T 32918-2016 信息安全技术 SM2椭圆曲线密码公钥算法

GB/T 32905-2016 信息安全技术 SM3 密码杂凑算法

GB/T 32907-2016 信息安全技术 SM4 分组密码算法

GM/T 0018-2012 密码设备应用接口规范

GM/T 0019-2012 通用密码服务接口规范

GM/T 0020-2012 证书应用综合服务接口规范

GM/Z 0001-2013 密码术语

3 术语和定义

下列术语和定义适用于本文件。

3.1

电子签名 electronic signature

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

[《中华人民共和国电子签名法》]

3.2

保险电子单据 insurance electronic document

保险业务流程中所产生和使用的，需要实施电子签名的版式化电子文档，包括但不限于电子保单、电子投保单、电子回执单和电子理赔单等。

3.3

电子印章 digital 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。
[GM/Z 0001-2013,2.12]

3.4

电子签章 digitally seal

使用电子印章签署电子文件的过程。
[GM/Z 0001-2013,2.11]

3.5

电子证据 electronic evidence

被存储在电子设备上或被电子设备所传送的可作为证据的信息和数据。
[GM/Z 0001-2013,2.13]

3.6

电子认证服务 certificate-service

为电子签名的真实性和可靠性提供证明的活动。

注：包括签名人身份的真实性认证，电子签名过程的可靠性认证和数据电文的完整性认证三个部分，涉及数据电文的生成、传递、接收、保存、提取、鉴定各环节，涵盖电子认证专有设备提供、基础设施运营、技术产品研发、系统检测评估、专业队伍建设等各方面，是综合性高技术服务。

[工信部《电子认证服务管理办法》 第二条]
[工信部《电子认证服务业“十二五”发展规划》 P14 术语解释]

3.7

数字证书 digital certificate

也称公钥证书，由证书认证机构（CA）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种数据结构。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。
[GM/Z 0001-2013,2.115]

3.8

证书认证机构 certification authority（CA）

对数字证书进行全生命周期管理的实体。也称为电子认证服务机构。
[GM/Z 0001-2013,2.145]

3.9

证据型数字证书 evidence certificate

由证书认证机构（CA）签发，在数字证书的扩展信息中，绑定了针对本次签名的签名人行为（如手写签名笔迹、照片、录音等）及被签名文件特征数据的一种签名证书。

3.10

密码杂凑算法 hash algorithm

又称杂凑算法、密码散列算法或哈希算法。该算法将一个任意长的比特串映射到一个固定长的比特串，且满足下列三个特性：

（1）为一个给定的输出找出能映射到该输出的一个输入是计算上困难的；

（2）为一个给定的输入找出能映射到同一个输出的另一个输入是计算上困难的。

（3）要发现不同的输入映射到同一输出是计算上困难的。

[GM/Z 0001-2013,2.58]

3.11

对称密码算法 symmetric cryptographic algorithm

加密和解密使用相同密钥的密码算法。

[GM/Z 0001-2013,2.19]

3.12

非对称密码算法 asymmetric cryptographic algorithm

公钥密码算法 public key cryptographic algorithm

加解密使用不同密钥的密码算法。其中一个密钥（公钥）可以公开，另一个密钥（私钥）应保密，且由公钥求解私钥是计算不可行的。

[GM/Z 0001-2013,2.23]

3.13

私钥 private key

非对称密码算法中只能由拥有者使用的不公开密钥。

[GM/Z 0001-2013,2.116]

3.14

公钥 public key

非对称密码算法中可以公开的密钥。

[GM/Z 0001-2013,2.28]

3.15

公开密钥基础设施（PKI） public key infrastructure（PKI）

基于公钥密码技术实施的具有普适性的基础设施，可用于提供机密性、完整性、真实性及抗抵赖性等安全服务。

[GM/Z 0001-2013,2.29]

3.16

数字签名 digital Signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

[GM/Z 0001-2013,2.113]

3.17

SM2算法 SM2 algorithm

一种椭圆曲线公钥密码算法，其密钥长度为256比特。

[GM/Z 0001-2013,2.118]

3.18

SM3算法 SM3 algorithm

一种密码杂凑算法，其输出为256比特。

[GM/Z 0001-2013,2.119]

3.19

SM4算法 SM4 algorithm

一种分组密码算法，分组长度为128比特，密钥长度为128比特。

[GM/Z 0001-2013,2.120]

3.20

依赖方

基于对电子签名认证证书或者电子签名的信赖从事有关活动的机构或人。

[《中华人民共和国电子签名法》第三十四条（二）]

4 保险电子签名系统技术要求

4.1 概述

为保证保险电子单据具有与纸质单据相同的法律效力，应在保险电子单据的生成和使用等过程中应用可靠的电子签名技术，并符合《中华人民共和国电子签名法》第十三条的规定。

4.2 保险电子签名技术框架

4.2.1 框架简介

保险业务应用层的安全可通过保险电子签名密码应用技术框架提供密码支撑。保险电子签名密码技术框架示意图，如图1所示：

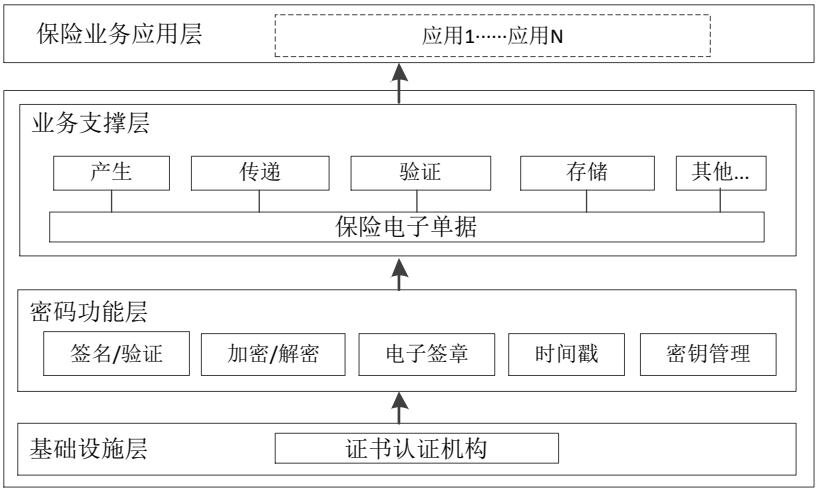

图 1 保险电子签名技术架构示意图

保险电子签名应用技术框架由业务支撑层、密码功能层和基础设施层构成。

4.2.2 业务支撑层

保险业务支撑层，涉及保险业务应用层产生的各种保险电子单据及其主要管理过程，包括保险电子单据的产生、传递、验证、存储等环节，通过调用密码功能层实现安全的保险电子单据管理。

4.2.3 密码功能层

密码功能层是处在基础设施层和保险业务支撑层之间的中间层，为业务支撑层提供相关的密码服务功能以保障保险电子单据的安全。

密码功能层是硬件密码模块和密码中间件的集合体，实现以下基本功能：

a)签名/验证功能

用于对保险电子单据或其中的关键数据实施数字签名与验证。应采用国家密码管理主管部门批准的算法。

非对称密码算法可使用 SM2，遵循 GB/T 32918-2016。杂凑算法可使用 SM3，遵循 GB/T 32905-2016。

如需使用对称密码算法，可采用 SM4 算法遵循 GB/T 32907-2016。

b)加/解密功能

用于对保险电子单据中涉及用户隐私的个人敏感数据进行加密保护。

示例：身份证号、银行卡号、健康状况、生物特征等均为个人敏感数据。

c)电子签章功能

对于需要加盖保险公司电子公章的保险电子单据，应采用电子签章功能。保险公司利用 CA 颁发的企业数字证书，结合保险公司可视化电子印章，通过数字签名实现电子签章，生成安全的保险电子单据。

用户在使用保险电子单据时，要对电子签章进行验证。

d)时间戳功能

采用时间戳证明保险公司的证书及保险电子单据中的数字签名在签署生成时间点的有效性。

e)密钥管理功能

应使用国家密码管理主管部门批准的密码设备对签名密钥对的生成、存储、分发、导入与导出、使用、备份与恢复、归档、销毁等环节实现安全管理。涉及私钥的所有运算均在密码设备中完成，且私钥和对称密钥不能被从密码设备导出。

4.2.4 基础设施层

采用第三方证书认证机构为保险业务应用提供电子认证服务的基础设施。

5 保险电子签名系统管理要求

5.1 可用时间

保险电子签名系统应保证不间断服务：

a)保险电子签名系统原则上应提供7×24小时服务以满足业务需求。

b)系统停机维护，需提前三个工作日向业务管理部门报备，并告知需应用电子签名的客户。

c)单次停机维护时间原则上应少于两个小时（含）。

5.2 数据保护

采取多种措施保护电子签名相关数据：

a)保险电子单据、载明身份鉴别的相关数据应妥善保管。

b)用户口令应以不可逆转的散列值形式保存在数据库中，不应以任何明文形式保存。并于3个月至6个月之间定期更换。

c)重要数据应定期进行备份，并妥善保管备份的磁带、磁盘等存储介质，限制能够接触此类介质的人员。保存环境应满足长期保存的要求，应定期对存储数据有效性进行校验。通常重要数据应保存多个备份，并保存在不同的地理位置，并执行同样严格的保密措施。

d)保证数据库和其它文件只能被授权用户和系统访问，防止在本地存储或者网络传输的数据受到非法篡改、删除和破坏。未授权的访问不能获取明文数据。

e)充分利用安全控制策略，加强对用户网络行为的安全审计，实现对服务器数据访问的重点防护。

f)电子签名系统的数据调取应经过本单位相关管理部门的审批。

5.3 环境及设备安全

5.3.1 物理环境安全

机房应制定、执行严格的管理制度，按时对电力、制冷、消防等基础设施进行巡检并将巡检记录归档，并定期进行审核。保险公司应有明确的预案应对各种机房突发事件。

5.3.2 网络设计安全

在进行网络架构设计时，应根据保险电子签名系统特点，将不同安全域进行隔离，应在重要节点部署硬件防火墙。安全域之间应部署入侵检测设备。外联链路宜使用不同运营商互备，核心服务器、交换设备应采用多设备冗余互备。

5.3.3 密码设备安全

保险电子单据管理过程中所采用的各种密码设备，应遵循相关密码国家标准和行业标准，并得到国家密码管理主管部门认证核准。密码设备应用接口规范，遵循GM/T 0018-2012。

示例：签名验签服务器、时间戳服务器、服务器密码机、智能密码钥匙等均属密码设备。

5.4 日常评估

保险公司应采取必要的控制手段确保电子签名的签署、审核、认证、存储、调取过程符合国家法律、行政法规及规章的相关规定，遵循相关的国际、国内安全技术和行业标准，并定期检查评估物理环境、操作过程以及人员管理等环节的管理是否有效。

6 保险电子签名应用要求

6.1 应用原则

a)身份识别：保险公司需通过适当技术手段识别客户身份信息，确保身份真实可信。

b)数据传输安全：在开展业务时，需采取有效手段确保数据信息的安全性与完整性。

c)合法性：需确保各类业务电子单据与传统纸质单据具有同等的法律效力和司法地位，证明客户的签署行为与签署意愿，落实应用涉及方的责任，保证签署后电子单据的完整性和不可抵赖性。

d)易用性：保险电子单据的签署，宜从流程设计、签名操作模式等环节，充分考虑用户体验需求。

6.2 应用涉及方

a)保险电子单据提供方，一般为保险公司或其授权的代理机构。

b)电子签名方，在保险电子单据进行电子签名或电子签章的自然人或机构。

c)证书认证机构，需满足《电子签名法》第十七条规定。为保证签名各方的公平公正性，宜由依法设立的第三方证书认证服务提供者提供认证服务。

6.3 应用方式

6.3.1 流程概述

保险公司或其授权的机构/人员应首先确认签字客户的身份，在客户查看并确认保险公司提供的保险电子单据信息后，应向其提供使用国家密码主管部门认证核准的签名设备或签名控件，供客户签名或签章。签名人包括但不限于自然人，签名形式包括但不限于手写笔迹签名，签名设备包括但不限于 PAD、手写屏、手写板等。带有签名内容的保险电子单据应进行电子签名认证，并加盖时间戳，生成最终带有签名的保险电子单据。

6.3.2 待签名保险电子单据的生成

由保险公司或其授权的机构/人员在电子签名系统中申请并生成需要客户签字确认的文件材料。

6.3.3 身份核验

6.3.3.1 签名人身份核验

签名前，保险公司或其授权的机构/人员应对所有签名人身份的真实性进行核验，身份核验的方式可包括但不限于人/证一致性检验、人脸识别、声纹识别等手段。身份核验与签名动作宜保持时间连续性。

当采用证据型数字证书标识签名人身份时，保险公司可在签名关键环节中采集能够识别签名人身份及表现签署意愿的电子证据，如签名人照片、录音、录像等，并委托电子签名认证机构将上述证据信息绑定固化到签名人用于此次签名的证据型数字证书中。

6.3.3.2 电子签章企业身份核验

保险公司应调用相关密码设备中的企业数字证书在保险电子单据上加盖保险机构的电子印章，密码设备应得到国家密码管理主管部门的认证核准，具有商用密码产品型号证书。

保险企业电子签章数据格式、电子签章生成及验证流程应符合国家密码管理主管部门的要求。

6.3.4 保险电子单据的签署要求

a)当客户在签署现场，由保险公司或其授权的机构/人员在设备上展示需客户签署名字的保险电子单据，确认客户身份后请客户阅读及完成电子签名。

b)当客户不在签署现场，由保险公司或其授权的机构/人员将需客户签署的保险电子单据通过网络发送至客户自助终端，并提示客户阅读及完成电子签名。

c)重要的保险电子单据签署应配套身份识别等功能。

d)进行保险电子单据签名时，应确保签名私钥仅由签名人控制。

e)保险电子单据如有多人签名，后一人签名时必须展示前一人签名内容。

f)待所有合同缔约方全部完成电子签名后，保险公司需及时向签署方展示签署结果。

6.4 纠纷处理

6.4.1 电子签名技术鉴定相关方

a)保险公司或签名人作为当事人，是电子签名技术鉴定委托主体，负责鉴定材料准备。

b)第三方证书认证机构为签名验证服务提供方，可直接出具电子签名验证报告；如需实施司法鉴定的，也可作为技术证据提供方，负责提交补充证明材料、协助鉴定实施。

c)实施司法鉴定时，应选择经过司法行政机关审核登记并取得《司法鉴定许可证》的司法鉴定机构作为鉴定实施主体，行使和履行检验鉴定义务，出具司法鉴定报告。

6.4.2 当事人送检材料

当事人所提供的送检材料，应基本包含以下内容：

a)具有当事人当时签名的保险电子单据或纸质文件。

b)其他辅助证明材料。

6.4.3 第三方证书认证机构送检材料

宜包含以下内容：

a)电子签名相关材料：电子签名验证报告、证书签发系统中当事人的签名图片及证书签发记录，均需纸质报告加盖公章。

b)认证机构资质材料：第三方证书认证机构证书签发系统产品的资质材料、第三方证书认证机构的相关资质证明材料，纸质复印件。

参考文献

[1] 公钥密码基础设施应用技术体系框架规范
[2] 公钥密码基础设施应用技术体系密码设备应用接口规范
[3] 公钥密码基础设施应用技术体系通用密码服务接口规范
[4] GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求
[5]GB/T 25064-2010 信息安全技术公钥基础设施电子签名格式规范
[6]商用密码管理条例（国务院令 1999 年第 273 号）
[7]《中华人民共和国保险法》
[8]《电子认证服务管理办法》
[9]《电子认证服务业“十二五”发展规划》
[10]《中华人民共和国电子签名法》