ICS 35.040
L 80

GM

中华人民共和国密码行业标准

GM/T 0070—2019

电子保单密码应用技术要求

Technical requirement for applications of cryptography in electronic insurance policy

2019-07-12 发布　　2019-07-12 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。

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、数安时代科技股份有限公司、中金金融认证中心有限公司、上海市数字证书认证中心有限公司、江苏意源科技有限公司、北京华大智宝电子系统有限公司、天地融科技股份有限公司。

本标准主要起草人：詹榜华、高能、林雪焰、傅大鹏、张永强、邓钊汉、李超、龚怡飞、谢吉华、李静进、刘建坡、邵淼、陈景燕、候宇、张妍。

电子保单密码应用技术要求

1 范围

本标准描述了保险行业电子保单业务的密码应用需求，规定了电子保单的投保、签发、存储、验证、递送等电子保单管理主要环节的密码应用技术要求，本标准可为电子保单的密码应用提供指导。

本标准适用于电子保单系统的开发和使用。

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 20520 信息安全技术 公钥基础设施 时间戳规范

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

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 35275 信息安全技术 SM2 密码算法加密签名消息语法规范

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/T 0034 基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

保险人 insurer

即保险公司，是与投保人订立保险合同，并承担赔偿或者给付保险金责任的单位机构。

3.2

投保人 insurance applicant

向保险人申请订立保险合同，并负有缴付保险费义务的人。

3.3

被保险人 insured

其财产或者人身受保险合同保障，享有保险金请求权的人，投保人可以为被保险人。

3.4

受益人 beneficiary

人身保险合同中由被保险人或者投保人指定的享有保险金请求权的人。

3.5

依赖方 relying party

使用电子保单的电子签名及签名证书进行决策的用户或代理。

3.6

电子保单　electronic policy

保险公司为投保人签发的具有保险公司数字签名的电子化保险合同凭证，法律效力等同于纸质保险单证。

3.7

电子投保书　electronic application form

投保人为订立保险合同而向保险公司提出的电子要约申请。

3.8

SM2 算法　SM2 algorithm

由 GB/T 32918 定义的一种算法。

3.9

SM3 算法　SM3 algorithm

由 GB/T 32905 定义的一种算法。

3.10

SM4 算法　SM4 algorithm

由 GB/T 32907 定义的一种算法。

3.11

电子保单失效　lapse of electronic policy

生效后的电子保单因某种原因而失去其法律效力。

4　缩略语

下列缩略语适用于本文件。

CA　证书认证机构(Certificate Authority)

CRL　撤销列表(Certificate Revocation List)

HTTPS　安全超文本传输协议(Hyper Text Transfer Protocol over Secure Socket Layer)

5　电子保单业务的安全需求

5.1　电子保单的业务流程

通常与电子保单相关的主要保险业务流程，如图 1 所示，包括投保—核保—承保—理赔等业务。

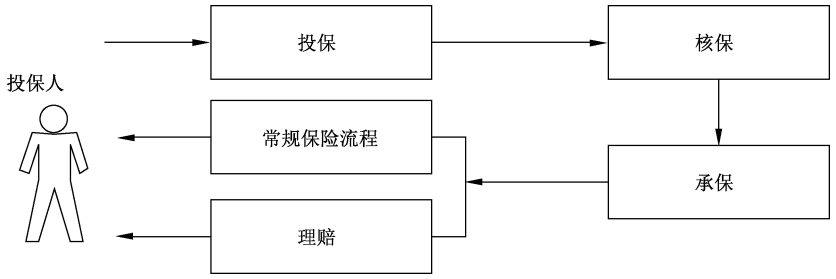

图 1　电子保单相关的主要保险业务流程

a)　投保：投保人通过保险公司的网络保险系统填写电子投保书，向保险公司提出保险请求，是电子保单的投保过程。

电子投保过程分为两类：一类是有保险代理人参与的电子投保模式，由代理人利用代理人注册账户登录网络保险系统，协助投保人录入投保申请，并指导投保人、被保险人或受益人完成电子签名，并提交电子投保书；另一类是投保人自助投保，由投保人、被保险人或受益人自行注册并录入投保申请，并生成电子签名确认提交电子投保申请；

b) 核保：保险公司对投保申请进行审核，包括电子投保书电子签名有效性、投保申请人身份的真实性、保险条款等内容，并确定保险费率的过程；

c) 承保：指保险公司对核保成功并已缴费的投保申请承接，进行电子保单签发、存储、递送等过程；

d) 理赔：保险事故发生后，投保人、被保险人依据电子保单向保险公司提出理赔申请，保险公司对电子保单进行验证，并根据保险合同进行赔偿或者给付；

e) 常规保险流程：保单信息查询、续期交费等其他的常规保险流程。

5.2 安全需求

保险合同信息是保险业务中的关键数据，电子保单作为保险合同的数据电文形式存在，为保证电子保单具有与纸质保单相同的法律效力，在电子保单的生成和使用等过程中存在如下安全需求：

a) 电子保单交易者的身份认证需求：

——确认投保人、被保险人等的当事人对投保契约的签字认可；

——确保客户获得的电子保单是由用户委托的承担保险责任的保险公司所签发出的。

b) 电子保单的机密性需求：保障保险公司的电子保单有关信息在存储、递送等过程中的安全，防止电子保单相关的用户隐私信息在存储或传输过程中被非法窃取。

c) 电子保单的完整性需求：需要确保投保人与保险公司所见信息是完全一致，因此要求在电子保单生成、存储、递送过程中，能确保电子保单信息的完整性，不被非法篡改。

d) 电子保单的防抵赖性需求：电子保单应能防止事后投保人、被保险人、保险公司等对保险合同的抵赖。

6 电子保单密码应用技术框架

投保、核保、承保、理赔等保险业务应用层的安全可通过电子保单密码应用技术框架提供密码支撑。电子保单密码应用技术框架示意图，如图2所示。

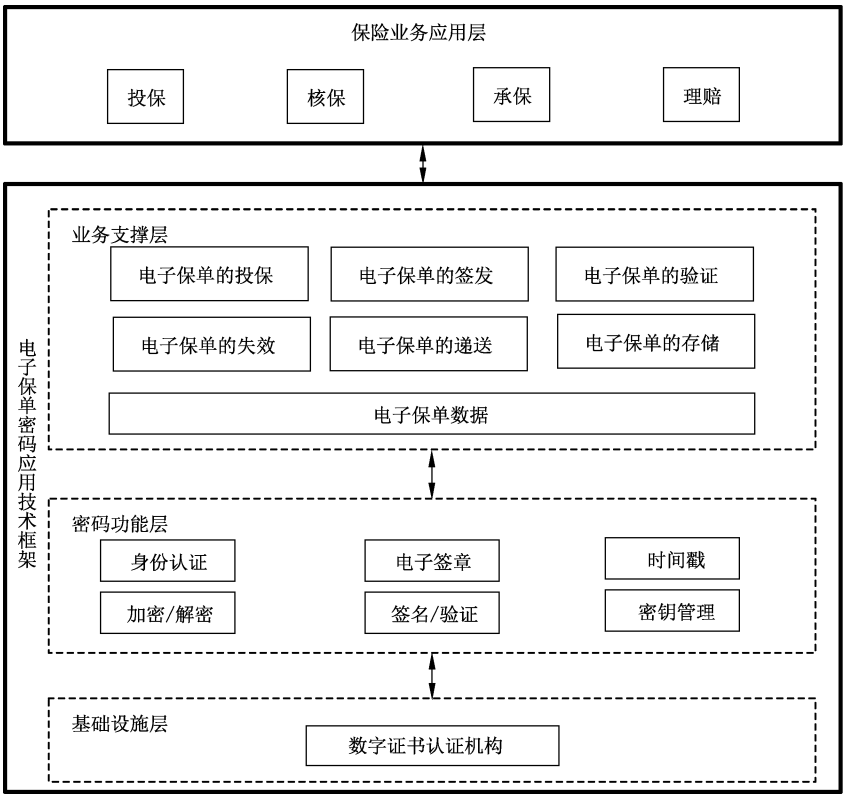

图 2　电子保单密码应用技术框架示意图

电子保单密码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：

a）　业务支撑层：电子保单业务支撑层，涉及网络保险核心数据电子保单数据及主要管理过程，包括电子保单的投保、签发、验证、存储、递送、失效等环节，通过调用密码功能层实现安全的电子保单管理。

b）　密码功能层：密码功能层是处在基础设施层和保险业务应用层之间的中间层，为电子保单业务支撑层提供相关的密码服务功能以保障电子保单的安全。

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：

——加/解密功能

用于对电子保单中涉及用户隐私，如身份证号、银行卡号、健康状况、生物特征等属于个人敏感信息的加密保护。数据加解密应采用国家密码管理主管部门批准的分组密码算法，如：SM4 等。

——签名/验证功能

实施对电子投保书、电子保单等关键数据的数字签名与验证。数字签名与验证是电子保单应用的关键密码技术，应采用国家密码管理主管部门批准的公钥密码算法（如 SM2）和杂凑算法（如 SM3）。

——密钥管理功能

保险公司利用 CA 颁发的企业数字证书对电子保单进行数字签名，因此保险公司需要对自己的签名私钥的产生、存储、使用、归档等进行严格的密钥管理。

——身份认证功能

在电子保单的使用中，投保人或依赖方需要验证保单的真伪，对电子保单的签发者进行身份认证，确认是由用户信任的承担保险责任的保险公司所签发，而不是假冒保险公司名义签发的。

——电子签章功能

为了符合用户传统使用习惯，电子保单通常应都具有加盖保险公司的电子公章的业务要求，为了便

于查看、验证和打印，需要采用电子签章功能。

保险公司利用CA颁发的企业数字证书，结合保险公司电子印章，通过数字签名实现电子签章，生成安全电子保单。

用户在使用电子保单时，要对电子签章进行验证。

——时间戳功能

采用时间戳证明保险公司的证书及电子保单数字签名在签署生成时间点的有效性。

时间戳以是一个字符序列形式显示，用于标识电子保单签发的精确日期和时间。时间戳应包含时间戳服务提供方的数字签名。

c) 基础设施层：由数字证书认证机构为电子保单提供第三方电子认证服务的基础层。

7 电子保单管理过程中的密码应用要求

7.1 电子保单的投保

电子保单签订之前，投保人先向保险公司提交电子投保申请，确认投保意向。投保过程应满足以下要求：

a) 投保人、被保险人或受益人，或代理人在保险业务系统客户端完成电子投保书阅读，确认投保，在电子投保书上的指定位置处进行手写签名。

b) 保险业务系统客户端应采集签名者的手写签名笔迹信息、声音、影像等数据，形成投保行为证据链，并将上述证据链、签名者用户信息、电子投保书杂凑值向CA提交数字证书请求。CA完成签名者身份核验，颁发数字证书。同时保险业务系统客户端利用该数字证书私钥完成电子投保申请的数字签名，从而实现投保人身份认证与本次投保签名行为有效绑定。

c) 对上述已签名的电子投保书加盖时间戳。

d) 业务系统应根据业务安全需要对投保过程中的敏感信息采用加密措施保障其传输、存储、使用等过程安全。

e) 保险业务系统收到电子投保书，应对电子投保书数字签名有效性进行验证。

7.2 电子保单的签发

投保人电子投保完成并缴费核保通过之后，业务系统就可以开始签发电子保单。电子保单的签发应满足以下要求：

a) 电子保单系统应该根据投保人填写的投保资料，根据险种的不同结合相应的保单内容模板，自动生成格式化保单数据，并在电子保单的保险公司签章位置进行电子签章操作；

b) 电子保单应加盖时间戳。

7.3 电子保单的存储

电子保单作为保险公司与投保人之间权利与责任的凭证，是双方履约、主张各自权益的依据，应采用适当的密码技术手段保证电子保单在法定有效期内的存储安全，防止非法访问与获取，防止非法篡改，维持签名有效性等。

电子保单的存储安全管理应满足以下要求：

a) 应采用加密或其他保护措施实现鉴别信息存储的机密性；

b) 宜采用加密或其他保护措施确保重要数据存储的机密性；

c) 应采用适当的身份鉴别手段确保重要数据合法授权访问。

7.4 电子保单的递送

电子保单签发完成之后，需要及时递送给投保人。电子保单的电子递送分为两种：一种是需要投保人签署电子回执的电子递送，另一种是无需签名的直接递送。

对于需要投保人签署电子回执的递送方式的密码技术要求是：

a) 投保人应在收到电子保单并验证之后，在电子回执单上的指定位置处进行手写签名。

b) 保险业务系统客户端应采集签名者的手写签名笔迹信息、声音、影像等数据，形成回执签署行为证据链，并将上述证据链、签名者用户信息、电子回执单杂凑值向 CA 提交数字证书请求，产生与本次手写签名及证据链有效对应的数字证书，数字证书中应包含签名者用户信息、手写签名笔迹信息、待签名原文杂凑值、证据链杂凑值等信息。同时保险业务系统客户端利用该数字证书私钥完成电子回执单的数字签名。

c) 对上述已签名的电子回执单加盖时间戳。

对于无需签名的直接递送方式的密码技术要求：

a) 电子保单递送应通过在线或离线的递送方式递送到投保人手中，应包含至少一种的递送方式：电子邮件递送、登录 Web 下载；

b) 投保人登录 Web 应用下载时，宜使用 HTTPS 等安全传输通道。

7.5 电子保单的验证

投保人收到电子保单之后，可以通过保险公司或 CA 提供的电子保单验证功能对保单进行验真。在理赔业务中，保险公司在处理业务过程中，也需要对电子保单进行验证。

电子保单的验证应通过对电子保单中的数字签名及时间戳的验证，来验证电子保单保险公司签署者身份的真实性，验证电子保单文件的完整性，确保保险交易契约的不可抵赖性，以及电子保单的签名时间有效性等。电子保单的验证过程要求如下：

a) 对电子保单数字签名者(即保险公司)的数字证书进行验证，包括证书信任链验证、证书有效期验证、证书状态是否被吊销、密钥使用策略是否正确；

b) 对电子保单数字签名进行验证，应能正确识别电子保单是否被篡改，并能即时提示签章无效；

c) 应验证时间戳的有效性；

d) 根据保险业务情况，检查电子保单失效名单，以核实保单的有效性。

7.6 电子保单的失效

电子保单的失效是指在电子保单生效后，如投保人未按规定及时交纳分期保费且超过了宽限期，导致电子保单效力暂时终止。要求如下：

a) 应定期生成电子保单的失效列表，每条记录包含保单号和失效时间；

b) 保险人应对电子保单失效名单进行数字签名；

c) 应定期发布电子保单失效名单，以供验证平台或验证程序验真使用；

d) 在电子保单复效后，应将该电子保单对应的记录在电子保单失效名单中删除。

8 电子保单密码技术要求

8.1 密码算法要求

电子保单中使用的密码算法，应采用国家密码管理主管部门批准的算法。

签名算法应使用 SM2，遵循 GB/T 32918 及 GB/T 35276，杂凑算法应采用 SM3 算法，遵循 GB/T 32905。

数据加解密应采用SM4分组密码算法，遵循GB/T 32907。

8.2 密码设备要求

电子保单管理过程中所采用的各种密码设备，如电子签章服务器、数字签名验证服务器、时间戳服务器、服务器密码机、智能密码钥匙等，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。

8.3 密钥管理要求

电子保单签名设备中的主要密钥是电子保单签名密钥对，必须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。

8.4 证书管理要求

电子保单应用中的证书管理应由专门负责发放和管理数字证书的CA提供，作为电子保单业务交易中受信任的第三方电子认证服务提供者，应具有合法的电子认证服务许可证资质，承担公钥体系中公钥的合法性检验的责任，为电子保单应用提供具有法律效力的认证服务。

提供电子认证服务的CA，应提供基于SM2密码算法的证书服务，遵循GM/T 0034。

8.5 电子保单数字证书要求

电子保单应采用由获得电子认证服务主管部门许可的第三方CA颁发的数字证书，数字证书以及CRL格式应遵循GB/T 20518。

8.6 电子保单数据格式要求

8.6.1 电子保单数据基本要求

需要签名保护的电子保单内容包含保单号、投保人信息、被保险人信息、受益人信息及投保金额等保险信息以及相应保单的版式属性信息。

8.6.2 电子保单数字签名格式要求

电子保单数字签名格式应包含：

a) 电子印章数据。保险公司制作电子保单时，应在电子保单的“保险人签章”处加盖电子印章。电子印章的样式规格，应与电子保单签发保险公司的有效公章保持一致。电子印章遵循GM/T 0031。电子印章数据包括印章图片数据以及其他属性信息，以及电子保单中电子印章的盖章位置坐标等信息，视具体应用要求可包括数字签名操作的时间信息、地理位置等属性信息。

b) 数字签名值。代表保险公司对需要签名保护的电子保单内容、保险公司电子印章数据、电子保单其他属性信息的数字签名值。

c) 签名者证书。签名者证书是保险公司对保单数字签名的机构数字证书。

d) 时间戳格式应遵循GB/T 20520。

e) 电子保单数字签名格式应支持基于SM2密码算法的签名消息数据类型，遵循GB/T 35275。