ICS 03.060
CCS A 11

JR

中华人民共和国金融行业标准

JR/T 0242—2022

电子保单商用密码应用规范

Specification for the application of commercial cryptography in electronic insurance policy

2022-11-24 发布　　2022-11-24 实施

中国银行保险监督管理委员会　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。

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。

本文件由全国金融标准化技术委员会保险分技术委员会(SAC/TC180/SC1)提出并归口。

本文件起草单位：中国人民财产保险股份有限公司、中国人寿保险股份有限公司、中英人寿保险有限公司。

本文件主要起草人：鹿慧、张鹏飞、郭斌、郭帆、李超、孙健、王海英、乔宜民、丘嫣、赵磊。

本文件为首次制定。

电子保单商用密码应用规范

1 范围

本文件规定了电子保单自投保至责任终止全业务流程中商用密码应用的要求，包括电子保单业务流程中的商用密码应用要求、商用密码技术与管理要求。

本文件适用于指导中华人民共和国境内保险行业相关机构开展电子保单业务中的商用密码管理和应用。

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 20518 信息安全技术 公钥基础设施 数字证书格式

GB/T 32918 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

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 36687—2018 保险术语

GM/Z 0001—2013 密码术语

JR/T 0161—2018 保险电子签名技术应用规范

JR/T 0174—2019 电子保单业务规范

3 术语和定义

GB/T 36687 界定的以及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。

3.2

可靠的电子签名 reliable electronic signature

电子签名同时符合下列条件的，视为可靠的电子签名：

a）电子签名制作数据用于电子签名时，属于电子签名人专有；

b）签署时电子签名制作数据仅由电子签名人控制；

c）签署后对电子签名的任何改动能够被发现；

d）签署后对数据电文内容和形式的任何改动能够被发现。

3.3

电子保单 electronic policy

通过保险人的可靠电子签名签发，用于证明保险合同关系，与纸质保单具备同等法律效力的版式电

文。包括首次签发的电子原保单、历次电子批单、电子保险标志等电子文件。

[来源：JR/T 0174—2019,3.4]

3.4

版式电文 plate type message

以固定格式的电子文件呈现，无论在何种设备上阅读、打印或印刷时，版面呈现结果均保持一致，以用户阅读为目的的固化数字纸张。

[来源：JR/T 0174—2019,3.2]

3.5

电子签章 digitally seal

使用电子印章签署电子文件的过程。

[来源：GM/Z 0001—2013,2.11]

3.6

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。

[来源：GM/Z 0001—2013,2.115]

3.7

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。

[来源：JR/T 0161—2018,3.9]

3.8

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。

[来源：GM/Z 0001—2013,2.113]

3.9

SM2 算法 SM2 algorithm

由 GB/T 32918 定义的一种非对称密码算法。

3.10

SM3 算法 SM3 algorithm

由 GB/T 32905 定义的一种密码杂凑算法。

3.11

SM4 算法 SM4 algorithm

由 GB/T 32907 定义的一种对称密码算法。

3.12

时间戳 timestamp

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。能表示一份数据在某个特定时间之前已经存在的、完整的、可验证的数据。

4 缩略语

下列缩略语适用于本文件。

OFD：开放版式文件（Open Fixed layout Document）

PDF：可移植文档格式（Portable Document Format）

PKI：公钥基础设施（Public Key Infrastructure）

CRL：证书撤销列表(Certificate Revocation List)

5 电子保单业务概述及商用密码应用框架

5.1 业务概述

电子保单商用密码应用环节包括版式文件生成、电子投保、电子保单签发、保险合同变更、保险理赔、电子保单交付、电子保单回执签收、电子保单验证以及电子保单归档。电子保单商用密码应用环节如图1所示。

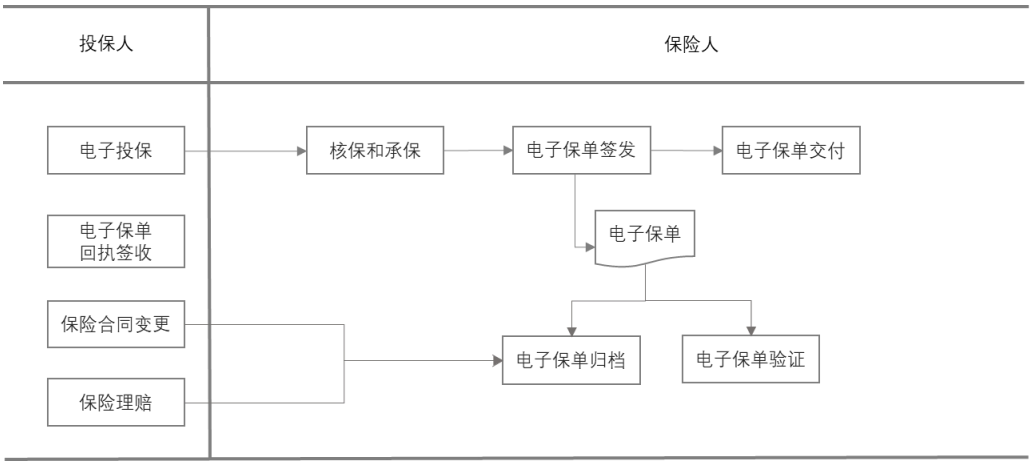

图1 电子保单商用密码应用环节概览图

5.2 电子保单商用密码应用框架

5.2.1 框架简介

电子保单商用密码应用技术框架由密码应用层、密码服务层、密码支撑层以及外部交互组成，如图2所示。

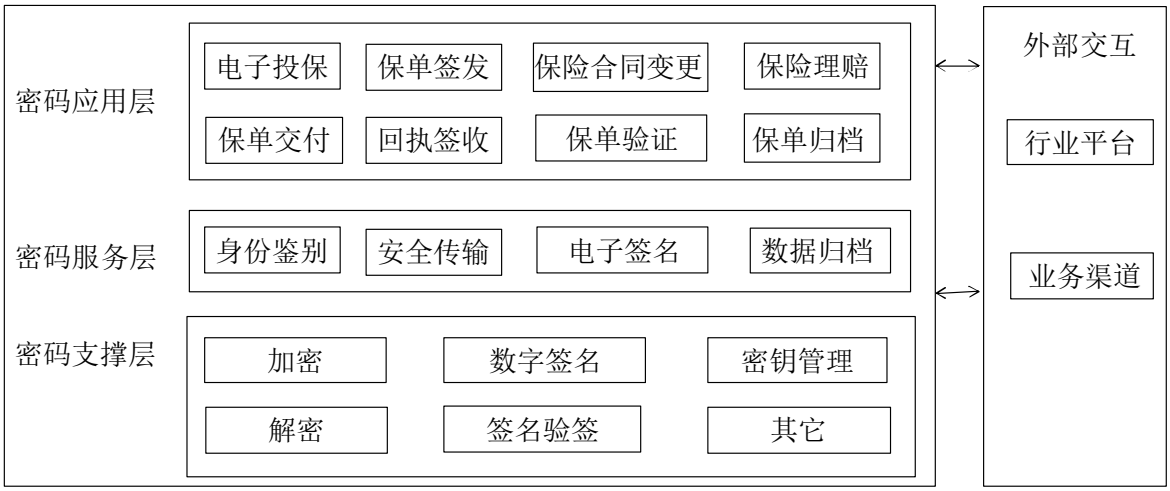

图 2 电子保单商用密码应用技术框架示意图

5.2.2 密码应用层

密码应用层，面向用户提供各类保险业务服务，并与业务渠道、行业平台进行电子保单数据交互。密码应用层包括电子投保、保单签发、保险合同变更、保险理赔、保单交付、回执签收、保单验证、保单归档环节。

5.2.3 密码服务层

密码服务层处在密码应用层和密码支撑层之间,为密码应用层提供相关的密码服务功能。具体包括：

a）身份鉴别：业务办理过程中及业务系统登录过程中鉴别用户真实身份；

b）安全传输：采用密码技术保证通信过程中数据的机密性和完整性，为保险人与外部机构、用户之间数据交互提供安全传输服务；

c）电子签名：主要指在保险用户签署、电子保单制单及交付等过程中，依据《中华人民共和国电子签名法》中可靠电子签名的要求，实现基于PDF、OFD等版式文件的电子签章、手写电子签名、时间戳等商用密码应用；

d）数据归档：主要在电子保单的归档环节，对于业务采集的回溯信息以及电子保单的归档防篡改。

5.2.4 密码支撑层

密码支撑层处在基础底层，为密码服务层提供密钥管理及运算服务，具体包括以下三大功能模块：

a）签名/验证功能：用于对保险电子单据或关键数据实施数字签名与验证；

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；

c）密钥管理功能：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。

5.2.5 外部交互

外部交互包括保险人与外部渠道及行业平台之间的电子保单数据交互。保险人与业务渠道进行电子保单数据交互，应通过系统身份鉴别、数据加解密、安全链路保障交互数据的安全性。保险人与行业平台进行电子保单数据交互，应遵循行业平台规范要求，进行数据加解密、数据签名验签等操作。

6 电子保单商用密码应用要求

6.1 电子保单文件生成

电子保单文件的生成应符合以下规定：

a）电子保单作为保险合同的数据电文形式存在，其文件形式应能够有效地表现所载内容并可供随时调取查用，应适合于长期保存的电子文档格式。至少支持PDF版式文件或标准OFD版式文件；

b）生成电子保单版式文件时可根据投保人填写的投保信息，匹配不同保险产品对应的模板文件，自动生成版式化文件，或者根据其他格式文档转换成要求的版式文件。

6.2 电子投保

采用电子化方式购买保险产品，应保证投保过程的安全性。

a）身份鉴别：非现场方式向保险人办理保险投保业务，如进行身份鉴别的，则身份鉴别中应采取电子签名、加密或者其他切实可行的安全技术措施进行数据传输及存储，保护用户信息安全；

b）信息确认：投保人须对投保要约信息进行确认，操作行为明确表达认同所签署内容这一意愿。为身份鉴别通过的操作人颁发数字证书，采用该张数字证书对应的私钥对电子投保单据进行电子签名，保证电子投保单据的完整性、抗抵赖性；

c）时间戳：电子化投保单据应采用时间戳技术，能够识别电子单据的电子签署时间。时间源宜采用国家标准时间源；

d）数据安全：电子投保中涉及用户敏感信息的应进行加密保护，数据加解密应采用国家密码管理部门批准的密码算法。

6.3 电子保单签发

核保通过之后，保险人向投保人出具电子保单，电子方式出单的保单应采用PKI公钥密码技术，将数字图像处理技术与电子签名技术进行结合，对加盖印章图像数据的电子版式文件进行数字签名，以确保文档来源的真实性以及文档的完整性，防止对文档未经授权的篡改，并确保签章行为的不可否认性。具体要求如下：

a）电子保单签发前，由保险人向电子认证服务机构申请代表其真实身份的数字证书。电子保单签发时选择拟进行电子签章的签章者数字证书，并验证该数字证书的有效性；

b）对待签名原文数据进行杂凑运算，形成原文杂凑值，使用保险人数字证书对应的签名私钥进行数字签名，生成签名值，并将签名值数据写入签名文件中指向的位置；

c）电子保单上保险人盖章位置应展现保险人印章，形成经过数字签名并印章可视化的电子保单文件；

d）电子保单宜加盖时间戳，能够识别电子单据的电子签章时间；

e）最终签发的电子保单文件，应至少包含电子保单原文、保险人印章数据、签名值、签名者数字证书；

f）电子保单经电子签名，证明其是保险人签发的有效保单文件，是与纸质保单具备同等法律效力的版式电文，不需防伪印刷图案。

6.4 保险合同变更

投保人在线上进行保单变更操作时，应保证线上变更过程的安全性。

a）身份鉴别：非现场方式向保险人办理保险合同变更业务，如进行身份鉴别的，则身份鉴别中应采取电子签名、加密或者其他切实可行的安全技术措施进行数据传输及存储，保护用户信息安全；

b）信息确认：投保人须对变更要约信息进行确认，操作行为明确表达认同所签署内容这一意愿；自然人用户，应采取可靠的电子签名，保证合同变更单据的完整性、抗抵赖性。非自然人用户，保险人应采用安全技术手段认证操作人身份，确保操作行为人不可替代，行为证据不可篡改；

c）时间戳：电子单据签署宜采用时间戳，能够识别电子单据的电子签署时间；

d）数据安全：合同变更中涉及用户敏感信息的应进行加密保护，数据加解密应采用国家密码管理部门批准的密码算法。

6.5 保险理赔

保险理赔过程如使用电子化方式生成理赔单据的，应确认操作人的身份，并应采用可靠的电子签名方式实现版式理赔文件的电子化签署。

6.6 电子保单交付

电子保单签发完成之后，应以安全方式投递给投保人。可采用Web应用下载、短信链接、邮件或者其他方式交付。交付过程中应保证电子保单数据安全及用户隐私安全。

6.7 电子保单回执签收

进行线上电子保单回执签收，应确认签收人的身份，宜采用可靠的电子签名或其他可被鉴证的特定操作方式实现签收动作不可替代、回执内容不可篡改。

6.8 电子保单验证

电子保单需支持用户对电子保单的真实性和完整性进行验证。电子保单验证通过第三方权威机构的电子保单验证平台或保险人官方验证入口进行验证。具体要求如下：

a）验证电子保单签发机构身份的真实性。解析电子保单数据，提取电子保单数据中的数字证书，并对数字证书的真实性和有效性进行验证；

b）验证电子保单的完整性。对电子签名值进行验证，判断电子签名数据、电子保单内容和形式是否被修改。

6.9 电子保单归档

保险人应妥善保管电子保单过程文件，如电子投保单、告知单、保单等。宜使用专用的电子档案系统或其他网络信息系统实现保险电子单据的归档和查询下载，具体包括：

a）电子保单过程文件的存储能有效地表现所载内容并可供随时调取查用，格式与其生成、发送或者接收时的格式相同；

b）归档时应对电子保单过程文件进行验证，保证归档时电子保单过程文件的完整性和有效性；

c）归档时宜加盖时间戳，能够识别电子单据的归档时间；

d）宜采用加密或其他保护措施保证重要数据在存储过程中的机密性；

e）应采用有效的身份鉴别手段实现重要数据的安全访问控制。

7 电子保单商用密码技术与管理要求

7.1 数字证书要求

电子保单数字签名的数字证书要求如下：

a）电子保单数字签名所使用的数字证书应由电子认证服务机构颁发，并定期进行更新；

b）电子保单使用的数字证书应采用基于SM2密码算法的证书，数字证书以及CRL格式应遵循GB/T 20518；

c）业务场景适用于证据型证书的遵循JR/T 0161—2018关于证据型数字证书及签名的要求。

7.2 商用密码算法要求

电子保单生成及使用中采用的密码算法要求如下：

a）应采用国家密码管理部门核准的商用密码算法；

b）签名算法应使用商用SM2算法，符合GB/T 32918及GB/T 35276中的规定；

c）杂凑算法应采用商用SM3算法，符合GB/T 32905中的规定；

d）数据加解密应采用商用SM4分组密码算法，符合GB/T 32907中的规定。

7.3 商用密码系统建设要求

电子保单商用密码系统建设要求如下：

a）密码系统应经过商用密码检测认证，确保商用密码应用的规范性和安全性；

b）应定期检查评估物理环境、操作过程以及人员等环节的管理是否有效；

c）对于多系统多密码应用的复杂场景，宜对密码资源进行集中管理，提供集中密码服务，降低密钥管理风险；

d）应对密钥的生成、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，私钥的运算及存储应在安全的密码设备或密码模块中，并进行定期更新；

e）密码系统登录应使用密码技术对登录的用户进行身份鉴别，以获得系统访问授权；

f）应提供密码系统的冗余备份，保证系统的高可用性。

7.4 管理制度

应制定密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等内容。

参 考 文 献

[1]中华人民共和国电子签名法，2004年8月28日全国人民代表大会常务委员会第十一次会议审议通过，自2005年4月1日起施行。2019年4月23日第十三届全国人民代表大会常务委员会第十次会议修正

[2] GB/T 22239—2019 信息安全技术网络安全等级保护基本要求

[3] GB/T 25064—2010 信息安全技术 公钥基础设施 电子签名格式规范

[4] GM/T 0031—2014 安全电子签章密码技术规范

[5] GM/T 0070—2019 电子保单密码应用技术要求

[6] GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

[7] GM/T 0034—2014 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