ICS 35.040
L 80

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 …… Ⅰ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　电子保单业务的安全需求 …… 2
5.1　电子保单的业务流程 …… 2
5.2　安全需求 …… 3
6　电子保单密码应用技术框架 …… 3
7　电子保单管理过程中的密码应用要求 …… 5
7.1　电子保单的投保 …… 5
7.2　电子保单的签发 …… 5
7.3　电子保单的存储 …… 5
7.4　电子保单的递送 …… 6
7.5　电子保单的验证 …… 6
7.6　电子保单的失效 …… 6
8　电子保单密码技术要求 …… 6
8.1　密码算法要求 …… 6
8.2　密码设备要求 …… 7
8.3　密钥管理要求 …… 7
8.4　证书管理要求 …… 7
8.5　电子保单数字证书要求 …… 7
8.6　电子保单数据格式要求 …… 7

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。