Chinastandards.org

ICS 35.040

GM

GM/T 0070-2019

Technical requirement for applications of cryptography in electronic insurance policy

电子保单密码应用技术要求

(English Translation)

Issued on: July 12, 2019 **Implemented on: July 12, 2019**

Issued by: State Administration of Cryptography

Preview: page 1 of 5 shown, 16 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0070-2019

Chinastandards.org

Table of Contents

Technical framework of cryptographic application of electronic insurance 1
Issuance of electronic insurance policy 2
Verification of electronic insurance policy 3
Requirements for key management 4
Requirements for certificate management 5
Requirements for digital certificate of electronic insurance 6
Basic requirements for electronic insurance policy data 7

6 Technical framework of cryptographic application of electronic insurance

policy... 9

7 Cryptographic application requirements in the management process of electronic insurance policy... 11

7.1 Application of electronic insurance policy... 11

7.2 Issuance of electronic insurance policy... 12

7.3 Storage of electronic insurance policies... 13

7.4 Delivery of electronic insurance policy... 13

7.5 Verification of electronic insurance policy... 14

7.6 Lapse of electronic insurance policy... 15

8 Cryptographic technical requirements for electronic insurance policy... 15

8.1 Requirements for cryptographic algorithms... 15

8.2 Requirement for cryptographic equipment... 15

8.3 Requirements for key management... 16

8.4 Requirements for certificate management... 16

8.5 Requirements for digital certificate of electronic insurance policy... 16

8.6 Data format requirements for electronic insurance policies... 16 Technical requirement for applications of cryptography in electronic insurance policy

1 Scope

Preview: page 2 of 5 shown, 16 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0070-2019

This standard describes the cryptographic application requirements of the electronic policy business in the insurance industry. It specifies the technical requirements for the application of cryptography in the main aspects of electronic policy management, such as insurance, issuance, storage, verification, delivery of electronic insurance policy. This standard can provide guide for the cryptographic application for electronic insurance policy.

This standard applies to the development and use of electronic insurance policy systems.

2 Normative references the following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) are applicable to this standard.

GB/T 20518 Information security technology - Public key infrastructure -Digital certificate format GB/T 20520 Information security technology - Public key infrastructure -Timestamp specification GB/T 32905 Information security techniques - SM3 cryptographic hash algorithm GB/T 32907 Information security technology - SM4 block cipher algorithm GB/T 32918 (all parts) Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves GB/T 35275 Information security technology - SM2 cryptographic algorithm encrypted signature message syntax specification GB/T 35276 Information security technology - SM2 cryptography algorithm usage specification Electronic policy the electronic insurance contract certificate issued by the insurance company with the digital signature of the insurance company for the insurance applicant, which is legally equivalent to a paper insurance document.

Electronic application form an electronic offer application made by an insurance applicant to an insurance company for the purpose of entering into an insurance contract.

SM2 algorithm

An algorithm as defined by GB/T 32918.

SM3 algorithm

An algorithm as defined by GB/T 32905.

3.10

SM4 algorithm

An algorithm defined by GB/T 32907.

3.11

Lapse of electronic policy an electronic policy after it becomes effective loses its legal effect for some reason.

4 Acronyms

Preview: page 3 of 5 shown, 16 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0070-2019

The following abbreviations apply to this document.

CA: Certificate Authority CRL: Certificate Revocation List HTTPS: Hyper Text Transfer Protocol over Secure Socket Layer premium rate;

c) Insurance acceptance: Refers to the insurance company's acceptance of the insurance application that has been successfully underwritten and paid; carries out the process of issuing, storing, delivering electronic insurance police;

d) Claims: After the insured accident occurs, the insurance applicant and the insured submit an application for premium to the insurance company based on the electronic insurance policy. The insurance company verifies the electronic insurance policy and makes compensation or payment according to the insurance contract;

e) Routine insurance process: querying policy information, renewing payment and other routine insurance processes.

5.2 Security requirements Insurance contract information is the key data in the insurance business.

Electronic insurance policies exist as data messages in the form of insurance contracts. In order to ensure that electronic insurance policies have the same legal effect as paper insurance policies, the following security requirements exist in the generation and use of electronic insurance policies:

a) Identity authentication requirements for traders of electronic insurance policy:

-- Confirm that the parties such as the insurance applicant and insured have signed and approved the insurance contract;

-- Ensure that the electronic insurance policy obtained by the customer is signed by the insurance company entrusted by the user to bear the insurance liability.

b) Confidentiality requirements of electronic insurance policies: Ensure the security of relevant information of electronic policies of insurance companies during the storage, delivery, etc.; prevent user's privacy information related to electronic policies from being stolen illegally during storage or transmission.

c) Integrity requirements of electronic policies: It is necessary to ensure that the information seen by the insurance applicant and the insurance company is completely consistent. Therefore, it is required to ensure the integrity of the electronic policy information during the generation, storage, and delivery of the electronic policy and not to be illegally tampered with.

The technical framework of cryptographic application of electronic insurance policy is composed of business support layer, cryptographic function layer, infrastructure layer:

a) Business support layer: the electronic insurance policy's business support layer involves

Preview: page 4 of 5 shown, 16 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0070-2019

the core data of network insurance, electronic insurance policy data and main management processes, including such links as the insurance application, issuance, verification, storage, delivery, lapse, etc.

of the electronic insurance policy; it achieves the secure management of electronic insurance policy by calling the cryptographic function layer.

b) Cryptographic function layer: The cryptographic function layer is an intermediate layer between the infrastructure layer and the insurance business application layer. It provides relevant cryptographic service functions for the electronic insurance policy's business support layer to ensure the security of electronic insurance policies.

The cryptographic function layer is a collection of hardware cryptographic modules and cryptographic middleware, which implements the following basic functions:

- Encryption / decryption function it is used for the encrypted protection of personnel sensible information such as ID number, bank card number, health status, biometrics and so on which relate to the user privacy in the electronic insurance policy.

Data encryption and decryption shall use block cipher algorithms as approved by the national cryptographic management department, such as SM4.

- Signature / verification function Implement digital signatures and verification of key data such as electronic application forms and electronic insurance policies. Digital signature and verification are the key cryptographic techniques applied in electronic insurance policies, which shall use the public key cryptographic algorithms (such as SM2) and hash algorithms (such as SM3) as approved by the national cryptographic management authority.

- Key management function the insurance company uses the enterprise digital certificate issued by the CA to digitally sign the electronic insurance policy. Therefore, the insurance company needs to perform strict key management on the generation, storage, use, archiving of its private signature key.

- Identity authentication function confirm the insurance intention. The application process shall meet the following requirements:

a) The insurance applicant, insured or beneficiary, or agent completes the reading of the electronic application form on the client side of the insurance business system; confirms the insurance application; signs a handwritten signature at the designated position on the electronic application form.

b) The client side of the insurance business system shall collect data such as handwritten signature's handwriting information, voice, image, to form an insurance behavior evidence chain; submit the digital certificate request to the CA with the above evidence chain, signer user information, electronic application certificate hash value. CA finishes the identity verification of the signer and issues a digital certificate. At the same time, the client side of

Preview: page 5 of 5 shown, 16 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0070-2019