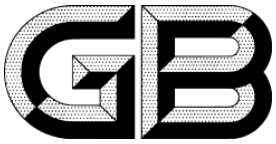
Chinastandards.org



chinastandards.org - PREVIEW

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

GB/T 34953.2-2018

Information technology -- Security techniques -- Anonymous entity authentication -- Part 2: Mechanisms based on signatures using a group public key

Issued on: September 17, 2018 **Implemented on: April 1, 2019**

Issued by: SAMR; SAC

Preview: page 1 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-34953-2-2018

Chinastandards.org

Table of Contents

Chinastandards.org - PREVIEW

Preview: page 2 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-34953-2-2018

Foreword

GB/T 34953 "Information technology - Security techniques - Anonymous entity authentication" has been issued or plans to issue the following parts.

- Part 1.General;
- Part 2.Mechanisms based on signatures using a group public key;
- Part 3.Mechanisms based on blind signatures;
- Part 4.Mechanisms based on weak secrets.

This Part is Part 2 of GB/T 34953.

This Part is drafted in accordance with the rules given in GB/T 1.1-2009.

This Part, using translation method, is identical to ISO/IEC 20009-2.2013 "Information technology - Security techniques - Anonymous entity authentication - Part 2.Mechanisms based on signatures using a group public key".

China's document which has a consistent correspondence with the international document normatively referenced in this Part is as follows.

- GB/T 34953.1-2017 Information technology - Security techniques - Anonymous entity authentication - Part 1.General (ISO/IEC 20009-1.2013, IDT).

This Part was proposed by and shall be under the jurisdiction of National Information Security Standardization Technical Committee (SAC/TC 260).

Drafting organizations of this Part. China IWNCOMM Co., Ltd., National Engineering Laboratory for Wireless Security, WAPI Industry Alliance (Wireless Network Security Industry Alliance of Zhongguancun), Commercial Cryptography Testing Center of the State Cryptography Administration, Chongqing University of Posts and Telecommunications, The State Radio Monitoring Center Testing Center, China Electronics Standardization Institute, Tianjin Radio Monitoring Station, China General Technology Research Institute, Peking University Shenzhen Graduate School, Institute of Software Chinese

chinastandards.org · PREVIEW

Preview: page 3 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-34953-2-2018

Academy of Sciences, National Computer Network Emergency Response Technical Team/Coordination Center of China, China Cyberspace Research Institute, National Research Center for Information Technology Security, National Information Security Engineering Center, Chinese People's Liberation Army Information Security Evaluation and Certification Center, The Third Research Institute of Ministry of Public Security, Beijing Institute of Computer Technology and Application, Fujian Radio Monitoring Station, Beijing Certificate Authority Co., Ltd., China Telecom Corp., Ltd. Shanghai Research Institute, China Broadband Wireless IP Standard Working Group of Ministry of Industry and Information Technology.

Main drafters of this Part. Du Zhiqiang, Cao Jun, Huang Zhenhai, Li Dawei, Song Qizhu, Li Qin, Long Zhaohua, Feng Dengguo, Shu Min, Chen Xiaohua, Li Jingchun, Ge Peiqin, Guo Xiaolei, Gao Bo, Zhu Yuesheng, Li Guangsen, Gu Jian, Li Nan, Yu Guangming, Zhang Lulu, Tie Manxia, Zhang Bianling, Xu Yuna, Hu Yanan, Yan Xiang, Zhang Guoqiang, Tong Weigang, Li Ming, Wan Hongtao, Wang Yuehui, Zheng Li, Peng Xiao, Zhu Zhengmei, Chen Zhiyu, Hou Pengliang, Xu Fuming.

1 Scope

This Part of GB/T 34953 specifies anonymous entity authentication mechanisms based on signatures using a group public key in which a verifier verifies a group signature scheme to authenticate the entity with which it is communicating, without knowing this entity's identity.

2 Normative references

The following documents are indispensable for the application of this document. For the dated references, only the editions with the dates indicated are applicable to this document. For the undated references, the latest edition (including all the amendments) are applicable to this document.

ISO/IEC 20008-1 Information technology - Security techniques - Anonymous

Preview: page 4 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-34953-2-2018

Chinastandards.org

digital signatures - Part 1.General

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 20008-1, ISO/IEC 20009-1, and the following apply.

Function that outputs one or more shared secrets, for use as keys, given shared secrets and other mutually known parameters as input.

4 Symbols and abbreviated terms

For the purposes of this Part, the following symbols and abbreviations apply.

5 Model and requirements

Clause 5 specifies the model and requirements for the anonymous authentication mechanisms.

6 Key generation process

The key generation process includes key generation algorithms that create the group membership issuing key, the group membership opening key and the group signature linking key (or keys) if they are required in the mechanism.

7 Mechanisms without an online TTP

If information contained in the text field of the message-to-be-signed of the token cannot be recovered from the group signature, then it shall be contained in the unsigned information of the token.

8 Mechanisms involving an online TTP

Unilateral anonymous authentication means that only one of the two entities is authenticated and that the identity of the authenticated entity is anonymous to the other entity.

9 The group membership opening process

This process is optional. The evidence evaluation process is run by an evidence

chinastandards.org · PREVIEW

Preview: page 5 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-34953-2-2018