ICS 35.040
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 38647.2-2020

Information technology - Security techniques - Anonymous digital signatures - Part 2: Mechanisms using a group public key

Issued on: April 28, 2020 **Implemented on: November 1, 2020**

Issued by: State Administration for Market Regulation, China National Standardization Administration

Table of Contents

Foreword

GB/T 38647 "Anonymous Digital Signature of Information Technology Security Technology" is intended to be divided into two parts.

---Part 1.General Provisions;

---Part 2.The mechanism of using group public key.

This part is Part 2 of GB/T 38647.

This section was drafted in accordance with the rules given in GB/T 1.1-2009.

This section uses the redrafting method to modify the use of ISO /IEC.20008-2.2013 "Information Technology Security Technology Anonymous Digital Signature

Part 2.The mechanism of adopting group public key".

The technical differences between this part and ISO /IEC.20008-2.2013 and the reasons are as follows.

--- With regard to normative quotation documents, this part has been adjusted with technical differences to adapt to my country's technical conditions and adjustments

The situation is reflected in Chapter 2 "Regulatory Reference Documents", with specific adjustments as follows.

* Removed ISO /IEC 18031 and ISO /IEC 18032;

* Added GB/T 32905, GB/T 32918.2-2016, GB/T 34953.2-2018 and ISO /IEC 15946-1;

* Replaced ISO /IEC.20008-1 with GB/T 38647.1 modified to adopt international standards.

--- Chapter 5 adopts my country's national standard for cryptographic algorithms GB/T 32905 to adapt to my country's technical level.

--- Chapter 8 adds a mechanism 8 (see 8.3), which is based on GB/T 32918.2-2016 and is suitable for my country's commercial cryptographic algorithms

Anonymous digital signature technology.

--- Added content related to the mathematical assumptions and safety parameter selection of mechanism 8 (see Appendix C).

--- Added content related to the revocation mechanism of mechanism 8 (see Appendix D).

--- Added E.8, gives a numerical example of mechanism 8 (see Appendix E).

This part is proposed and managed by the National Information Security Standardization Technical Committee (SAC/TC260).

This section was drafted. Xi'an Xidian Jietong Wireless Network Communication Co., Ltd., National Engineering Laboratory for Wireless Network Security Technology,

Zhongguancun Wireless Network Security Industry Alliance, Commercial Cryptographic Testing Center of National Cryptography Administration, National Radio Monitoring Center Testing Center, National

Information Technology Security Research Center, China General Technology Research Institute, China Electronics Technology Standardization Research Institute, Tianjin Electromechanical Products Inspection

Testing Center, Chongqing University of Posts and Telecommunications, Beijing Institute of Computer Technology and Application, Ministry of Industry and Information Technology Broadband Wireless IP Standards Working Group.

Introduction

Anonymous digital signature mechanism is a special type of digital signature mechanism. In this type of digital signature mechanism, unauthorized entities cannot obtain

The identity of the signer, but it can be verified that the legal signer has produced a legal signature.

The anonymous digital signature mechanism using the group public key has the ability to provide more information to the signer. Some signature mechanisms have connection capabilities

Force, where two signatures generated by the same signer are connectable. Some signature mechanisms have the ability to open, where signatures can be

Special entities are opened to reveal the identity of the signatory. Some signature mechanisms have both connection and opening capabilities.

For each mechanism, this section specifies the opening, connection and/or cancellation procedures.

The mechanism specified in this section uses the anti-collision cryptographic hash function

specified in GB/T 32905 to calculate the entire message.

The issuer of this document draws attention to that when declaring compliance with this document, it may involve CN201810207503.4 related to 8.3,

Use of CN201810207564.0, CN201810207571.0 and other patents.

The issuer of this document has no position on the authenticity, validity and scope of the above patents.

The patent holder has assured the issuer of this document that he is willing to work with any applicant under reasonable and non-discriminatory terms and conditions,

Negotiations on patent licensing. The patent holder's statement has been filed with the issuing agency of this document. Relevant information can be contacted through the following

Way to get.

Patent holder. Xi'an Xidian Jietong Wireless Network Communication Co., Ltd.

Address. A201, Qinfengge, Xi'an Software Park, No. 68 Keji 2nd Road, High-tech Zone, Xi'an

Contact. Feng Yuchen

Postcode. 710075

Email. ipri@iwncomm.com

Phone. 029-87607836

Fax. 029-87607829

The issuer of this document draws attention to the revision of this document using ISO /IEC.20008-2.2013.Therefore, in addition to the above statement, South Korea

The "Patent Holder's Proposal for ISO /IEC.20008-2.2013 made by the Institute of Electronic Communications, Intel Corporation and NEC Corporation of Japan

The intention to negotiate permission with other parties based on non-discrimination, reasonable conditions and terms" applies to this document. Relevant information can be obtained through the following contact parties

The formula gets.

Patent holder. Electronics and Telecommunications Research Institute

Address. 161, Gajeong-dong, Yuseong-gu, Daejeon, 305-700, KOREA

Contact. HanchulShin

Email. vip123@etri.ke.kr

Phone. 82-042-860-5797

Fax. 82-042-860-3831

Patent holder. Intel Corporation

Address. IntelLegalandCorporationAfairs2200MissionColegeBlvd., RNB-150, SantaClara, CA95054

Contact. James Kovacs

Email. Standards.Licensing@intel.com

Phone. 408-765-1170

Fax. 408-613-7292

Patent holder. NECCorporation

Address. 7-1Shiba5-chomeMinato-KuTokyoJapan108-8001Japan

Contact. YoshinobuMatsumoto

Email. y-matsumoto@cp.jp.nec.com

Phone. 81-3-3798-2452

Fax. 81-3-3798-6394

Please note that in addition to the above patents, some content of this document may still involve patents. The issuer of this document is not responsible for identifying these

Responsibilities.

Information Technology Security Technology Anonymous Digital Signature

Part 2.Mechanism using group public key

1 Scope

This part of GB/T 38647 specifies the general model and requirements of anonymous digital signature mechanism using group public key

Force mechanism, mechanism with opening function, mechanism with opening and connection function.

This section gives.

a) An overview of the anonymous digital signature mechanism using group public key signatures;

b) Various mechanisms for providing such anonymous digital signatures.

For each mechanism, this section specifies.