Chinastandards.org

ICS 35.040
CCS L 80

GM

GM/T 0079-2020

Direct anonymous attestation specification for trusted computing platform

可信计算平台直接匿名证明规范

(English Translation)

Issued on: December 28, 2020 **Implemented on: July 1, 2021**

Issued by: State Administration of Cryptography

Preview: page 1 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0079-2020

Chinastandards.org

Table of Contents

Scope 1
Normative references 2
Terms and definitions 3
Symbols 4
Cryptographic algorithm 5
Overview 6
System composition 7
Basic process 8
Security goals 9
System initialization 2 10
Certificate issuance algorithm 3 11
Overview 12
Definition of interface input parameter 13
Process overview 14
Flow overview 15
Overview 16
Definition of interface input parameter 17
Process overview 18
Flow overview 19

1 Scope

This document specifies the functions, interfaces, data structure of the direct anonymous attestation protocol of the trusted computing platform.

This document is applicable to the development of the direct anonymous certification protocol applications, anonymous certification services, anonymous certification systems of the trusted computing platform.

2 Normative references

The provisions in following documents become the provisions of this Standard through reference in this Standard. For the dated references, the subsequent amendments (excluding corrections) or revisions do not apply to this Standard;

Preview: page 2 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0079-2020

however, parties who reach an agreement based on this Standard are encouraged to study if the latest versions of these documents are applicable.

For undated references, the latest edition of the referenced document applies.

GB/T 32918-2016 (all parts) Information security techniques - Elliptic curve public-key cryptography GM/T 0012 Trusted computing - Interface specification of trusted cryptography module GM/Z 4001 Cryptographic terms

3 Terms and definitions

The terms as defined in GM/Z 4001, as well as the following terms, apply to this document.

Trusted cryptography module; TCM A basic hardware module, which construct the trusted computing platform. It provides cryptographic computing functions for the trusted computing platform; has protected storage space.

Endorsement key; EK

The key pair, which is used in the trusted cryptographic module, to identify its own identity. It can only be used for encryption and decryption. Depending on the context, this term may represent a key pair, the public key in a key pair, or the private key in a key pair.

TCM service module

A software middleware of the trusted cryptographic module, that provides services to applications.

Direct anonymous attestation; DAA the anonymous identity authentication scheme, which is used by the trusted computing platform.

Elliptic curve-based direct anonymous attestation Direct anonymous attestation scheme, which is based on elliptic curve cryptography scheme.

4.1 Symbols

The cryptographic symbols which are defined in GB/T 32918-2016 (all parts), as well as the following cryptographic symbols, apply to this document.

0.Integer 0, bit 0, or finite field addition identity element.

5 Cryptographic algorithm

This document adopts the cryptographic algorithm, which is approved by the national cryptographic management authority.

Preview: page 3 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0079-2020

6.1 Overview

The direct anonymous attestation is used for the anonymous identity attestation of the TCM security chip.

6.2.1 System composition

The ECDAA system is mainly composed of three participants. the issuer, the prover, the verifier, as shown in Figure 1.The prover is divided into the host and the TCM security chip, according to the ECDAA calculation location. The both cooperate to complete the anonymous credential application and anonymous certification process.

6.2.2 Basic process

The main communication process between the various participants of the ECDAA system includes the following steps.

6.2.3 Security goals

The main problem solved by the ECDAA system is how the trusted computing platform/TCM chip user can prove to the remote verifier, that its platform does use the trusted cryptographic module TCM, that is, how the TCM security chip authenticates itself. While authenticating the TCM identity, it is also necessary to protect the privacy of the platform's identity; it is required that the remote verifier cannot know the exact identity of the TCM security chip AND cannot link multiple TCM sessions. In order to meet the above security requirements, the ECDAA system needs to achieve the following security goals.

6.3.2 System initialization 2

This algorithm is used by the prover host and TCM to set the public parameters of the elliptic curve system, which is generated by the issuer (see Appendix B for details). Its input, output and algorithm flow are as follows.

6.3.5 Certificate issuance algorithm 3

This algorithm is used by the prover to store anonymous credentials; its input, output and algorithm flow are as follows.

7.1 Overview

The TCM security chip shall provide support for three anonymous certification commands. TCM_ECDAA_Setup, TCM_ECDAA_Join, TCM_ECDAA_Sign,

Preview: page 4 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0079-2020

7.2.1 Definition of interface input parameter

The TCM_ECDAA_Setup command of the definition of interface input parameter can only be initiated by the TCM owner, to the security chip TCM.

7.2.3.1 Process overview

The execution of the TCM_ECDAA_Setup command is divided into several stages.

7.3.3.1 Flow overview

The execution of the TCM_ECDAA_Join command is divided into several stages. Table 6 regulates the detailed definition of the functions of each stage.

The interface input handle parameter of stage 0 is the Setup command session handle; the output parameter contains the new Join session handle, instead of the original Setup session handle, which is used for the interface input handle parameters of stage 1 and stage 2.The session handle will be cleared at the end of stage 2.

GM/T 0079-2020

CRYPTOGRAPHIC INDUSTRY STANDARD ICS 35.040 CCS L 80 Direct anonymous attestation specification for trusted computing platform Issued on. DECEMBER 28, 2020 Implemented on. JULY 01, 2021 Issued by. National Cryptography Administration

Table of Contents

Foreword... 3

1 Scope... 4

2 Normative references... 4

3 Terms and definitions... 4

4 Symbols and abbreviations... 6

5 Cryptographic algorithm... 7

6 Direct anonymous attestation function... 8

7 Direct anonymous attestation interface... 15 Appendix A (Normative) Data structure of direct anonymous attestation interface... 32 Appendix B (Informative) Direct anonymous attestation of elliptic curve parameters and auxiliary functions... 37 References... 38

1 Scope

This document specifies the functions, interfaces, data structure of the direct anonymous attestation protocol of the trusted computing platform.

This document is applicable to the development of the direct anonymous certification

Preview: page 5 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0079-2020