Chinastandards.org

GM

GM/T 0041-2024

Cryptographic test specification for smart card

智能IC卡密码检测规范

(English Translation)

Issued on: December 27, 2024

Issued by: State Administration of Cryptography

Preview: page 1 of 3 shown, 15 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0041-2024

Chinastandards.org

Table of Contents

1 Scope
2 Normative references
3 Terms and definitions
4 Symbols and abbreviations. 5
5 Test items
5.1 COS security management function test
5.2 COS security mechanism test. 6
5.3 Cryptographic key primality test. 7
5.4 Random number quality test
5.5 Correctness test of cryptographic algorithm implementation
5.6 Performance test of cryptographic algorithm implementation
5.7 Device security testing. 8
6 Test methods
6.1 General requirements
6.2 COS security management function test
6.3 COS security mechanism test
6.4 RSA key primality test
6.5 Random number quality test. 21
6.6 Correctness test of cryptographic algorithm implementation. 21
6.7 Performance test of cryptographic algorithm implementation
6.8 Device security testing
7 Qualification criteria

1 Foreword

GM/T 0041-2024 was issued by State Administration of Cryptography on 27 December 2024.

2 About this standard

Issued by: State Administration of Cryptography

English translation: about 15 pages (approximate)

Preview: page 2 of 3 shown, 15 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0041-2024

Chinastandards.org

3 Classification and status

Prefix GM/T: recommended standard.

Preview: page 3 of 3 shown, 15 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0041-2024