亞洲誠信 TRUSTAsia

让数字世界，信任无处不在！

TrustAsia – China PKI Development Updates

China PKI Supervision & Administration

Legal Framework

Electronic Signature Law of the People's Republic of China

Measures for the Administration of Electronic Certification Services

Enforced in March 2009
Revised in 2024

Ministry of Industry and Information Technology (MIIT)

Measures for the Administration of the E-government Electronic Certification Services

First implemented in 2009
Revised and implemented in 2024

State Cryptography Administration (SCA)

Other Related Legislations

Cybersecurity Law	Effective as of June 1, 2017
Cryptography Law	Effective as of January 1, 2020
Data Security Law	Effective as of September 1, 2021
Regulation on the Administration of Commercial Cipher Codes	Effective as of July 1, 2023

Revisions to Two Core Regulations

工业和信息化部 新闻动态 政务公开 政务服务 公众参与 工信数据 专题专栏

首页 > 工业和信息化部 > 机关司局 > 信息技术发展司 > 信息公开

公开征求对《电子认证服务管理办法（征求意见稿）》的意见

发布时间：2024-09-02 16:50 来源：信息技术发展司

为加强电子认证服务行业监管，规范电子认证服务行为，根据《中华人民共和国电子签名法》等有关法律法规，工业和信息化部修订了《电子认证服务管理办法》（以下简称《办法》）。为进一步听取社会各界意见，现予以公示。如有意见或建议，请于2024年10月3日前反馈。

传真：010-68208288

邮箱：miit_ca@miit.gov.cn

地址：北京市海淀区万寿路27号院8号楼工业和信息化部信息技术发展司。请在信封上注明“《电子认证服务管理办法（征求意见稿）》意见反馈”字样。

电子政务电子认证服务管理办法
（国家密码管理局令第4号）

发布日期：2024-09-10 来源：

【字体：大 中 小】 打印

国家密码管理局令

第 4 号

《电子政务电子认证服务管理办法》已经2024年8月26日国家密码管理局局务会议审议通过，现予公布，自2024年11月1日起施行。

局 长 刘东方

2024年9月4日

September 2, 2024

MIIT – Released the Measures for the Administration of Electronic Certification Services (*Draft for Public Comment*)

Electronic certification service refer to the public service activities of authenticity and reliability verification provided to all relevant electronic signatories.

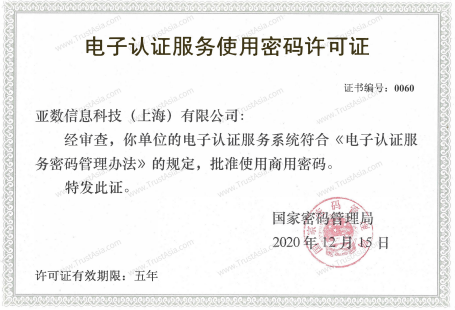
September 10, 2024

SCA – Issued the Measures for the Administration of the E-gov Electronic Certification Services, effect on November 1, 2024.

E-Gov electronic certification services refer to the activities of providing electronic signature authentication services for government activities by using commercial cryptography technology to ensure the authenticity and reliability of electronic signatures.

Licenses for Electronic Certification Authorities

- **SCA – License for Use of Cipher Codes for Electronic Certification Services**



- **SCA – License for Qualifications for E-government Electronic Certification Service Institutions**

- **MIIT – License for Electronic Certification Services**

China's Self–Developed Cryptographic System

China implements a **classified mamagement system** for cryptography, including **core cryptography, common cryptography, and commercial cryptography.**

Core Cryptography & Common Cryptography

– Securing state secret information

Commercial cryptography

– **Securing information other than state secrets**

– A citizen, legal person or any other organization may use commercial cryptography according to the law to protect cyber and information security

Type	Commercial Cryptography	International Cryptography
Symmetric Encryption Algorithm	SM1 / SM4	AES
Asymmetric Encryption Algorithm	SM2 / SM9	RSA / ECC
Hash Algorithm	SM3	SHA–256

Application Scenarios for Commercial Cryptographic Algorithms

Government Affairs | Ensuring National Data Security

- E-Government Platforms (SM2/SM4/SM3)
- Electronic Seals/Certificates (SM2/SM3)
- Government Cloud Security (SM4/SM2)

Financial Sector | Safeguarding Financial Transaction Security

- Bank Core Systems (SM1/SM2/SM4)
- Third-Party Payments (SM2/SM4)
- Financial Communication (Commercial Cryptographic SSL/TLS)

Communications & Internet | Building Endpoint Security Defenses

- Wireless Communication (WAPI-SM4)
- IoT Devices (SM7/SM9)
- 5G Communication (SM2/SM4)

Civil Services | Protecting Daily Life

- Social Security Cards (SM1)
- HTTPS Websites (GMSSL)

Digital Identity Development

National Digital Identity Authentication

Key Components

Online ID Number + Online ID Certificate

APP Downloads

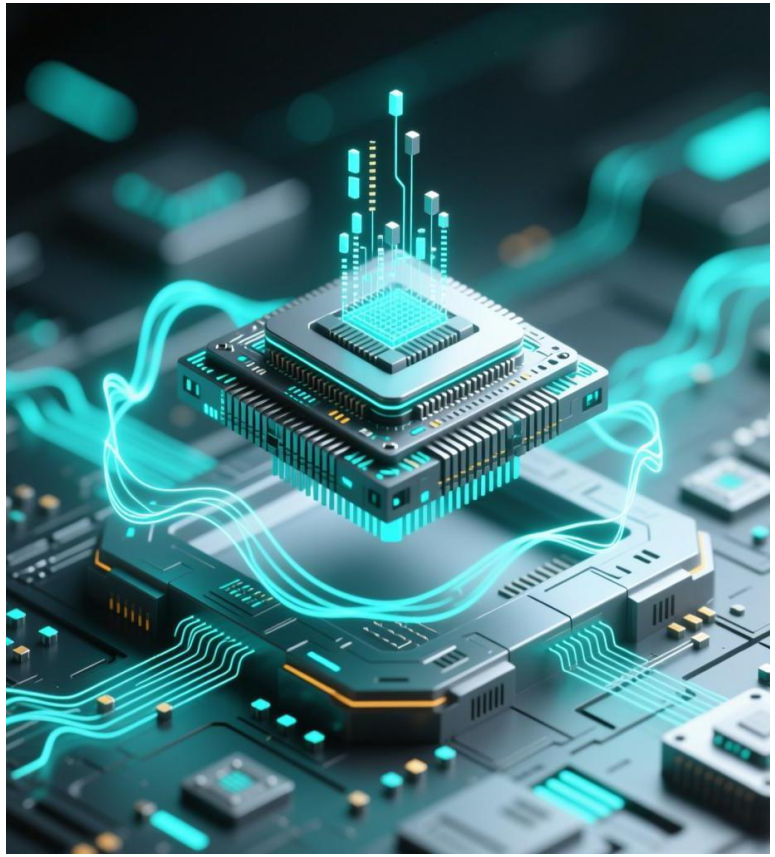
>16,000,000

Services Provided

>12,500,000

*Measures for the Administration of National Public Services for Online Identity Authentication comes into force on July 15, 2025.

China's Path Toward a Quantum-Resilient Future



Theoretical Research and Algorithmic Breakthroughs

- **Lattice-Based Cryptography**

Successfully entered into the third round of the NIST standard evaluation

- **Multivariate Cryptography**

The "Rainbow" signature scheme, proposed by Professor Jintai Ding, offers advantages such as high security and short signature size, and has been applied in areas like digital signatures.

- **Hash-Based Signatures**

The "SPHINCS-256" scheme, proposed by Tsinghua University, provides benefits including high security and short signature length, and has been utilized in fields such as blockchain technology.

China's Path Toward a Quantum-Resilient Future

International Standardization

In 2025, a team of Chinese experts initiated the ***Guidelines for Communication Network Security Protocols Against Quantum Attacks*** project, which was unanimously approved by the **ISO/IEC JTC 1/SC 6 committee**.

Domestic Standardization

- **The National Cryptography Industry Standardization Technical Committee**

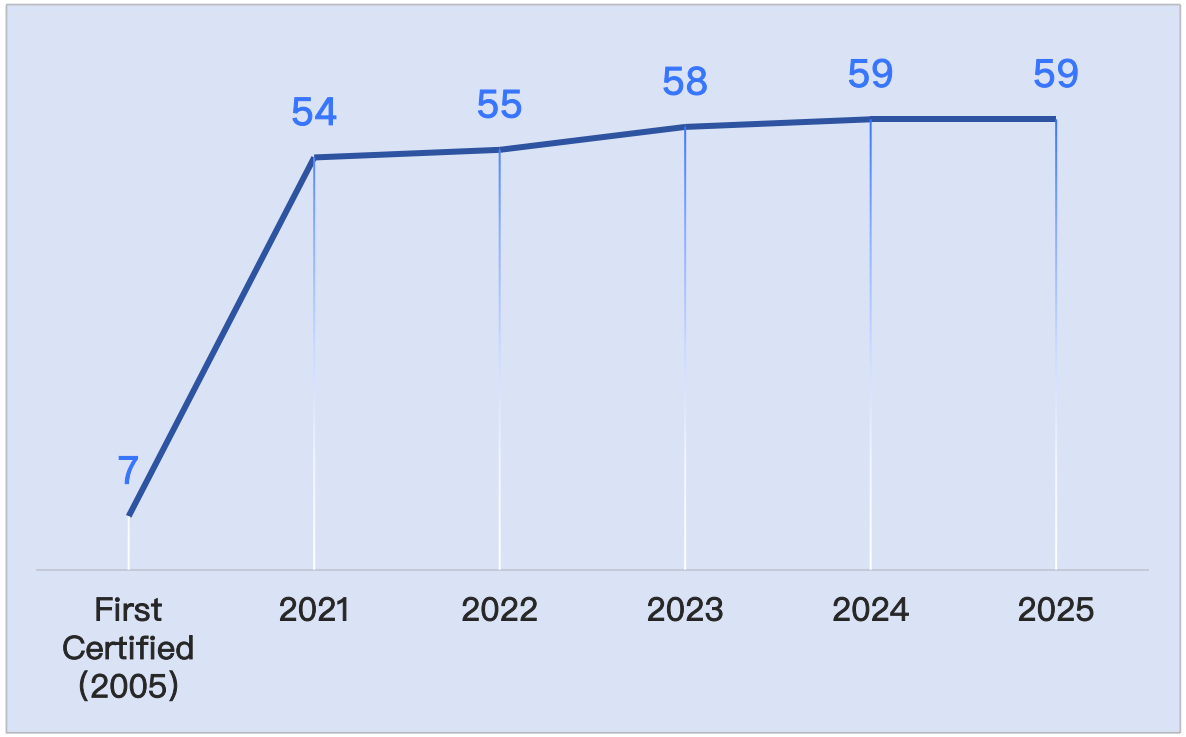
Initiated development of PQC standards, covering algorithm specifications, application guidelines, and testing standards.

- **The State Cryptography Administration (SCA)**

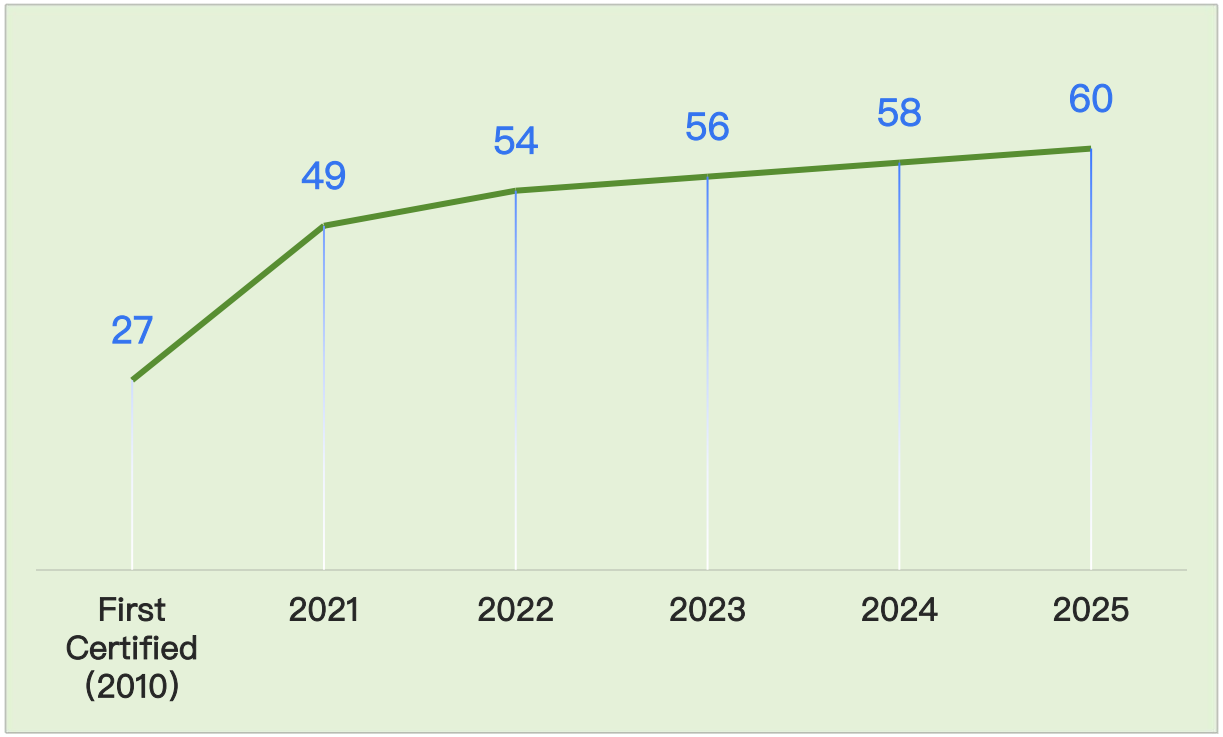
In 2023, issued *Post-Quantum Cryptographic Algorithm Design Specification*, requiring compatibility with SM2/SM9 algorithms and 128-bit (or higher) quantum-attack resistance

Increase on Certified CA Numbers

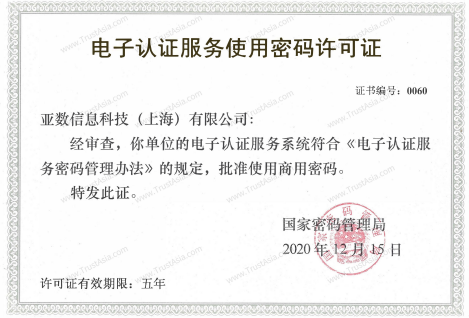
Electronic Certification Service Provider



E-Gov Electronic Certification Service Provider



TrustAsia – Certification Authority Accreditations



China MIIT Certification

License for Electronic Certification Services
License for Use of Cipher Codes for Electronic Certification Services

State Encryption Administration

License for Qualifications for E-government Electronic Authentication Service Institutions

WebTrust Accredited

WebTrust seals for Certification Authority, BR–SSL, Extended Validation, Code Signing, Network Security and S/MIME

Participation in Developing National Standards

- Member of WG3 and WG4, **China Cybersecurity Standardization Committee**
- Working Group Member, **Cryptography Industry Standardization Technical Committee**
- Participate in **developing mutiple national/industry/group standards**, covering areas including ACME, Certificate Transparency (CT), Timestamping, Security Technical Requirements for PKI Systems and Cryptographic Algorithms

TrustAsia CA Business Profile

01

WebTrust CA

– TLS/SSL – Code Signing

– S/MIME – Doc Signing

02

Chinese-Cryptography CA

– TLS/SSL – ID Cert

All based on Chinese cryptography

03

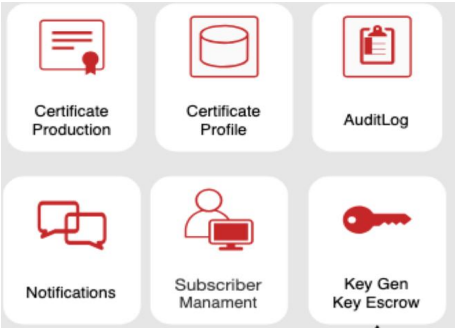
Matter CA

Provide device identity & trust solution for the Matter smart home ecosystem

04

Private CA

Build private CA hierarchies for enterprises to secure network and data



Strict Compliance

– WebTrust Audits

– China Government Standards

– CABF BR/EV Requirements

– Matter Specifications

Scalable Products & Solutions

– Digital Certificates

– PKI as a Service

– Certificate Lifecycle Management

– Matter PKI Solutions

亞洲誠信®
TRUSTAsia

让数字世界，信任无处不在！

Build Trust Everywhere in the Digital World!

www.trustasia.com

F/32 Building B, No 391 Guiping Rd,
Shanghai China

joanna.zhu@trustasia.com