

# INTRODUCTION TO CHINA PKI DEVELOPMENT

(ELECTRONIC CERTIFICATION SERVICE PROVIDER)

TrustAsia Technologies, Inc.

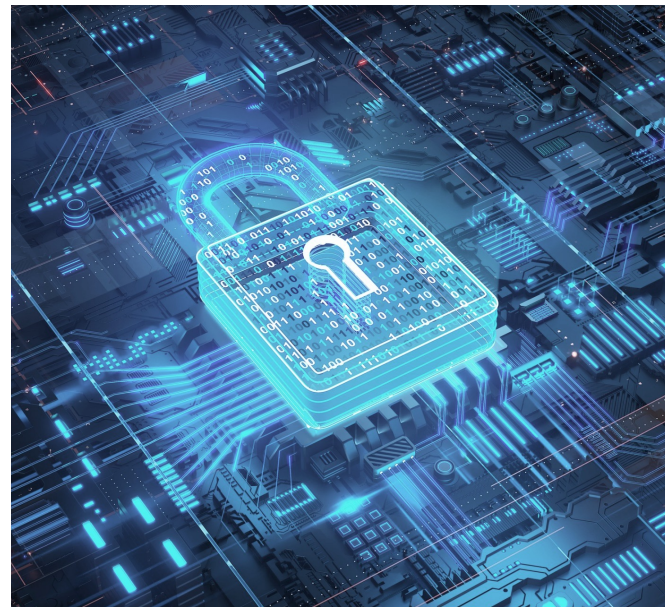
Bruce Wei

© 2023 TrustAsia Technologies, Inc. All rights reserved.



# CONTENTS

- 01 Laws & Regulations
- 02 Supervision & Administration
- 03 Service Providers
- 04 Technical Specifications
- 05 Major Applications



# 01

## LAWS & REGULATIONS

# Electronic Signature Law of the People's Republic of China



**Authority** -> Standing Committee of the NPC  
(National People's Congress)

## 中华人民共和国电子签名法

来源: 中国人大网 2019年05月07日 12:17:12

浏览字号: 大 中 小

(2004年8月28日第十届全国人民代表大会常务委员会第十一次会议通过 根据2015年4月24日第十二届全国人民代表大会常务委员会第十四次会议《关于修改〈中华人民共和国电力法〉等六部法律的决定》第一次修正 根据2019年4月23日第十三届全国人民代表大会常务委员会第十次会议《关于修改〈中华人民共和国建筑法〉等八部法律的决定》第二次修正)

### 目 录

- 第一章 总 则
- 第二章 数据电文
- 第三章 电子签名与认证
- 第四章 法律责任
- 第五章 附 则

# Measures for the Administration of Electronic Certification Services

Adopted and promulgated

2005.02.08

2009.02.18

2015.04.29

Revised

New version promulgated

Authority -> Ministry of Industry & Information Technology

## 电子认证服务管理办法

发布时间：2015-05-13 10:55 来源：政策法规司

(2009年2月18日 中华人民共和国工业和信息化部令第1号公布。根据2015年4月29日中华人民共和国工业和信息化部令第29号公布的《工业和信息化部关于修改部分规章的决定》修订)

### 第一章 总则

**第一条** 为了规范电子认证服务行为，对电子认证服务提供者实施监督管理，根据《中华人民共和国电子签名法》和其他法律、行政法规的规定，制定本办法。

**第二条** 本办法所称电子认证服务，是指为电子签名相关各方提供真实性、可靠性验证的活动。  
本办法所称电子认证服务提供者，是指为需要第三方认证的电子签名提供认证服务的机构（以下称为“电子认证服务机构”）。

向社会公众提供服务的电子认证服务机构应当依法设立。

**第三条** 在中华人民共和国境内设立电子认证服务机构和为电子签名提供电子认证服务，适用本办法。

**第四条** 中华人民共和国工业和信息化部（以下简称“工业和信息化部”）依法对电子认证服务机构和电子认证服务实施监督管理。

### 第二章 电子认证服务机构

**第五条** 电子认证服务机构应当具备下列条件：

- (一) 具有独立的企业法人资格。
- (二) 具有与提供电子认证服务相适应的人员。从事电子认证服务的专业技术人员、运营管理人员、安全管理人员和服务人员不少于三十名，并且应当符合相应岗位技能要求。
- (三) 注册资本不低于人民币三百万元。
- (四) 具有固定的经营场所和满足电子认证服务要求的物理环境。

# Measures for the Administration of Cipher Codes for Electronic Certification Services

Adopted and promulgated

2005.03.31

2009.10.28

New version promulgated

Revised

2017.12.01

Authority -> State Cryptography Administration

## 电子认证服务密码管理办法

发布日期：2017-12-06 来源：国家密码管理局

【字体：大 中 小】  打印

### 电子认证服务密码管理办法

(2009年10月28日国家密码管理局公告第17号公布，根据2017年12月1日

《国家密码管理局关于废止和修改部分管理规定的决定》修正)

第一条 为了规范电子认证服务提供者使用密码的行为,根据《中华人民共和国电子签名法》、《商用密码管理条例》和相关法律、行政法规的规定,制定本办法。

第二条 国家密码管理局对电子认证服务提供者使用密码的行为实施监督管理。

省、自治区、直辖市密码管理机构依据本办法承担有关监督管理工作。

第三条 提供电子认证服务,应当依据本办法申请《电子认证服务使用密码许可证》。

第四条 采用密码技术为社会公众提供第三方电子认证服务的系统(以下称电子认证服务系统)使用商用密码。

电子认证服务系统应当由具有商用密码产品生产和密码服务能力的单位承建。

第五条 电子认证服务系统的建设和运行应当符合《证书认证系统密码及其相关安全技术规范》。

第六条 电子认证服务系统所需密钥服务由国家密码管理局和省、自治区、直辖市密码管理机构规划的密钥管理系统提供。

第七条 申请《电子认证服务使用密码许可证》应当在电子认证服务系统建设完成后,向所在地的省、自治区、直辖市密码管理机构或者国家密码管理局提交下列材料:

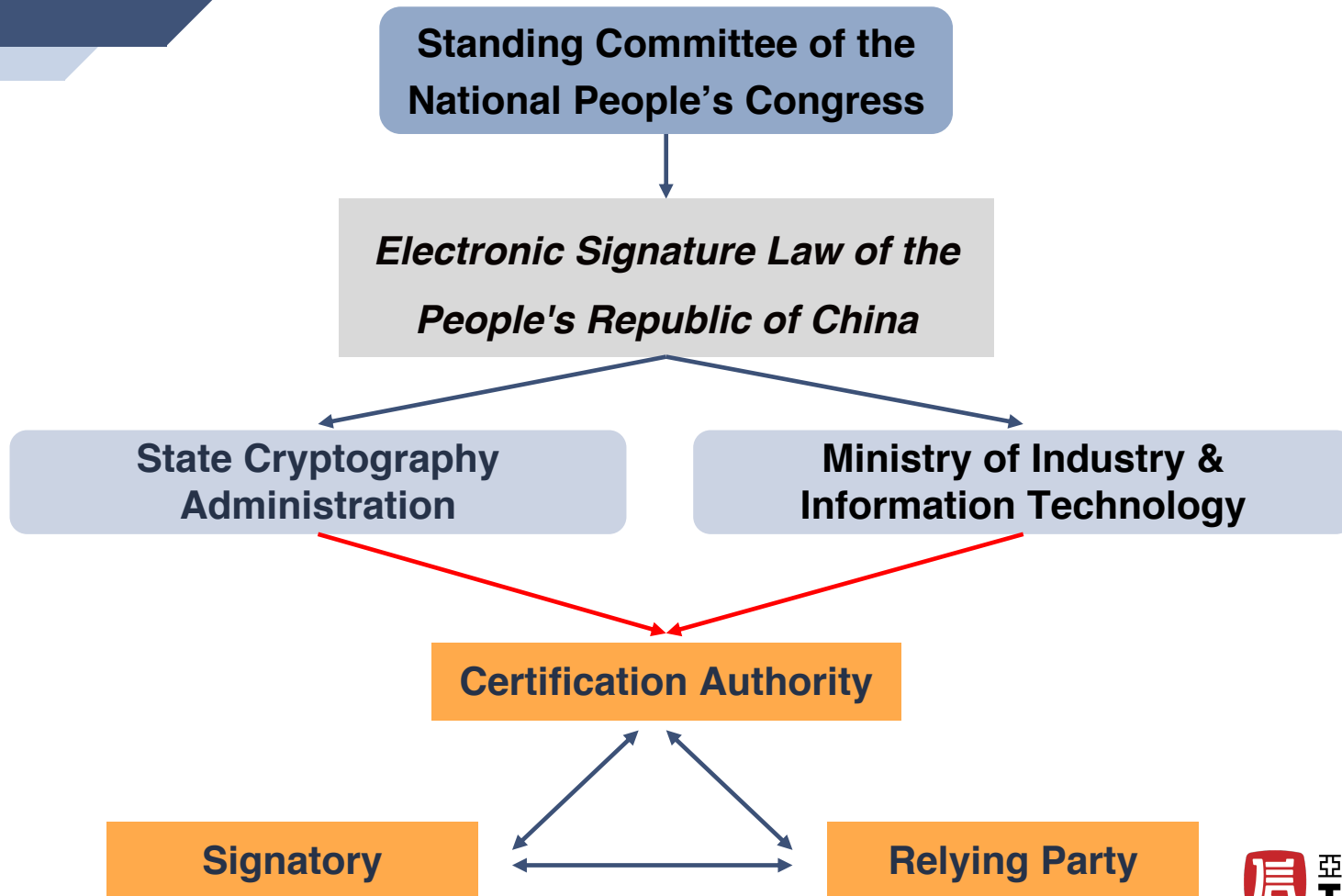
(一)《电子认证服务使用密码许可证申请表》;

(二)企业法人营业执照复印件;

(三)电子认证服务系统安全性审查相关技术材料,包括建设工作总结报告、技术工作总结报告、安全性设计报告、安全管理策略和规范报告、用户手册和测试说明;

# 02

## SUPERVISION & ADMINISTRATION





# ADMINISTRATIVE METHODS

01  
PRE

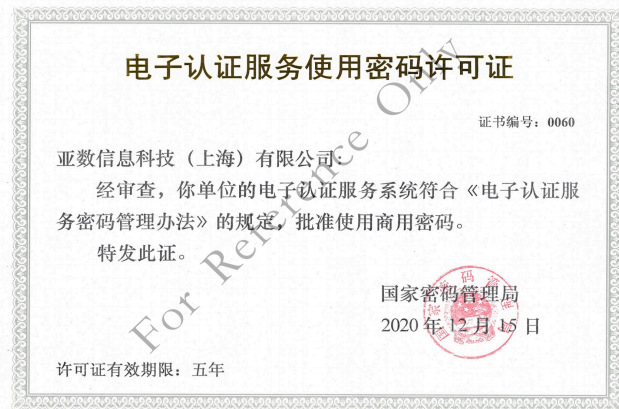
Licenses

02  
IN-PROGRESS

Supervision &  
Administration

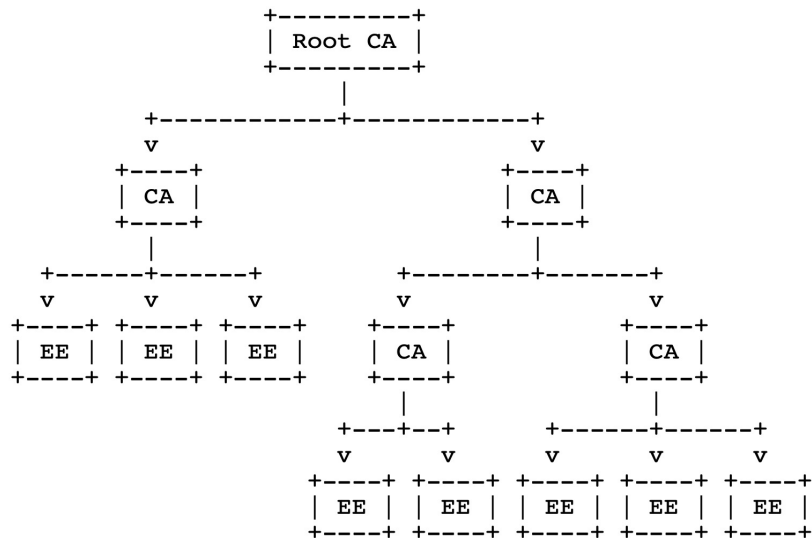
03  
AFTER

Audit

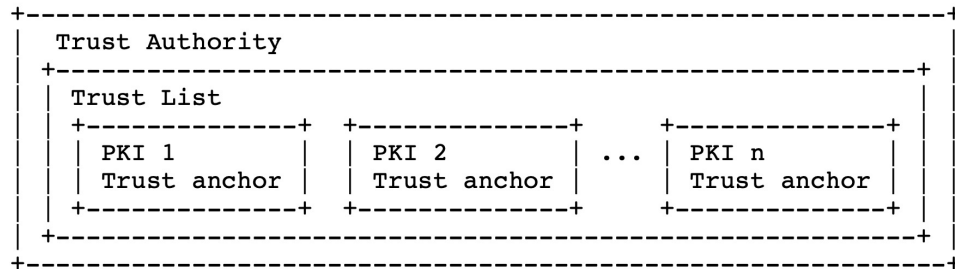


# TRUST MODEL

## Hierarchical PKI Architecture



## Trust List Model



# 03

## SERVICE PROVIDERS

# 56 CAs (QTSP)

(excluding those in  
Hong Kong, Macau,  
Taiwan)



# 04

## TECHNICAL SPECIFICATIONS

GB/T

GM/T

Application 1 -- Application N

Application Management

Responsibility Confirmation

Identity Authentication

Access Control

Time Stamp

Typical Cryptography Application Supporting Layer

TS System

Attribute Authority System

Digital Evidence Management System

Certificate Authentication System

Common Cryptography Service

Common Cryptography Application Supporting Layer

Cryptographic Device Management

Cryptographic Device

Cryptographic Resources

Cloud Environment

Cryptographic Device

Cryptographic Resources Management (Cloud)

Cryptographic Device Service Layer

Infrastructure Security Supporting Platform

Public Key Cryptographic Application Technology Framework

# 05

## MAJOR APPLICATIONS

## Fields/Areas

## Major Application Examples

### E-Government

- Online tax return
- Online government procurement
- Online customs declaration

- Online provident fund
- Government information resource sharing

### Finance

- Online banking
- Mobile online banking

- Electronic Insurance
- Credit management

### E-Commerce

- B2B, B2C
- Enterprise internal management

### Healthcare

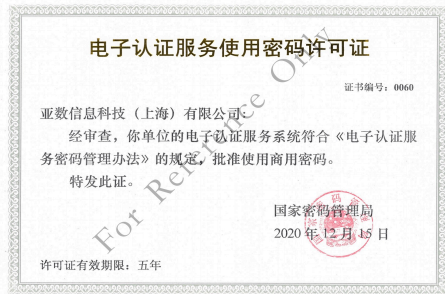
- Medical information system
- Regional medical platform
- Public health information service system

### International Certification Service

- Website/server
- Software code signing

- PDF document signing





## MIIT Certification

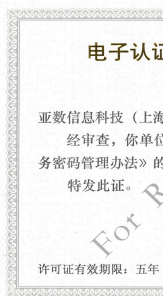
*Permit for Electronic Certification Services*

*Permit for Use of Cipher Codes for Electronic Certification Services*



## WebTrust Accredited

*WebTrust seal for Certification Authority, BR-SSL, Extended Validation and Code Signing*



MIT

Permit for Elect

Permit for Use of Digital Codes for Electronic Certification Services



Certification  
Authorized



Security, BR-  
Signing

# THE END

# THANKS



[www.trustasia.com](http://www.trustasia.com)



[bruce.wei@trustasia.com](mailto:bruce.wei@trustasia.com)

[whwn@hotmail.com](mailto:whwn@hotmail.com)

[alison.wang@trustasia.com](mailto:alison.wang@trustasia.com)

© 2023 TrustAsia Technologies, Inc. All rights reserved.

