INTRODUCTION TO CHINA PKI DEVELOPMENT

(ELECTRONIC CERTIFICATION SERVICE PROVIDER)
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

Adopted and promulgated: 2004.08.28
First revision: 2005.04.01
Came into force: 2005.04.01
Second revision: 2015.04.24
Came into force: 2015.04.24
Third revision: 2019.04.23
Came into force: 2019.04.23

Authority -> Standing Committee of the NPC (National People’s Congress)
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
Measures for the Administration of Cipher Codes for Electronic Certification Services

Adopted and promulgated

2005.03.31

Revised

2009.10.28

New version promulgated

2017.12.01

Authority -> State Cryptography Administration
Standing Committee of the National People's Congress

Electronic Signature Law of the People's Republic of China

State Cryptography Administration

Ministry of Industry & Information Technology

Certification Authority

Signatory

Relying Party
ADMINISTRATIVE METHODS

01 PRE
02 IN-PROGRESS
03 AFTER

Licenses
Supervision & Administration
Audit
Hierarchical PKI Architecture

Trust List Model
03
SERVICE PROVIDERS
56 CAs (QTSP)
(excluding those in Hong Kong, Macau, Taiwan)
TECHNICAL SPECIFICATIONS
Application 1 — Application N

Responsibility Confirmation
Identity Authentication
Access Control
Time Stamp

Typical Cryptography Application Supporting Layer

Common Cryptography Application Supporting Layer

Common Cryptography Service

Cryptographic Device Service Layer

Cryptographic Device
Cryptographic Resources
Cloud Environment

Infrastructure Security Supporting Platform

Public Key Cryptographic Application Technology Framework

TS System
Attribute Authority System
Digital Evidence Management System
Certificate Authentication System
Cryptographic Device Management
Cryptographic Resources Management (Cloud)

GB/T
GM/T
MAJOR APPLICATIONS
<table>
<thead>
<tr>
<th>Fields/Areas</th>
<th>Major Application Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>E-Government</strong></td>
<td>• Online tax return</td>
</tr>
<tr>
<td></td>
<td>• Online government procurement</td>
</tr>
<tr>
<td></td>
<td>• Online customs declaration</td>
</tr>
<tr>
<td></td>
<td>• Online provident fund</td>
</tr>
<tr>
<td></td>
<td>• Government information resource sharing</td>
</tr>
<tr>
<td><strong>Finance</strong></td>
<td>• Online banking</td>
</tr>
<tr>
<td></td>
<td>• Mobile online banking</td>
</tr>
<tr>
<td></td>
<td>• Electronic Insurance</td>
</tr>
<tr>
<td></td>
<td>• Credit management</td>
</tr>
<tr>
<td><strong>E-Commerce</strong></td>
<td>• B2B, B2C</td>
</tr>
<tr>
<td></td>
<td>• Enterprise internal management</td>
</tr>
<tr>
<td><strong>Healthcare</strong></td>
<td>• Medical information system</td>
</tr>
<tr>
<td></td>
<td>• Regional medical platform</td>
</tr>
<tr>
<td></td>
<td>• Public health information service system</td>
</tr>
<tr>
<td><strong>International Certification Service</strong></td>
<td>• Website/server</td>
</tr>
<tr>
<td></td>
<td>• Software code signing</td>
</tr>
<tr>
<td></td>
<td>• PDF document signing</td>
</tr>
</tbody>
</table>
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
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
THE END

THANKS

www.trustasia.com
bruce.wei@trustasia.com
whwn@hotmail.com
alison.wang@trustasia.com