CA Owner Name:

iTrusChina Co.,Ltd.（北京天威诚信电子商务服务有限公司）

-- General information about CA's associated organization --

CA Email Alias 1:

vTrus_contact@itrus.com.cn.

Company Website:

https://www.itrus.com.cn

Organizational Type:

Private Corporation.

Geographic Focus:

China.

Primary Market / Customer Base:

iTrusChina provide electronic certification service with wide industry coverage in China. Such as e-Commerce，Banking，Securities，Insurance，Bidding and Internet Finance etc. We have many icon customer in all industry like Taobao, JingDong, Alipay, ICBC, Bank of China, UnionPay, PICC, Aliyun and Lufax(Lu.com).
So far iTrusChina's business is in China mainland.

Recognized CAA Domains:

itrus.com.cn，itrus.cn

Problem Reporting Mechanism:

The reporter should fill the Certificate Problem Report Form (Signed or Sealed) in https://www.itrus.com.cn/repository and send email to Support@itrus.com.cn, we have a team which will monitor the report email and start internal process to investigate the issue.

-- CP/CPS and Audit Statements --

Policy Documentation:

https://www.itrus.com.cn/repository

CA Document Repository:

https://www.itrus.com.cn/repository

Certificate Policy (Link):

http://www-download.itrus.com.cn/download/CPS/page2/iTrusChina%20Certificate%20Policy%20v1.3.pdf

Certification Practice Statement (Link):
http://www-download.itrus.com.cn/download/CPS/page2/iTrusChina%20Certification%20Practice%20Statement%20v1.3.pdf
Other Relevant Documents:
https://www.itrus.com.cn/repository

Auditor: PricewaterhouseCoopers Zhong Tian LLP, Beijing Branch
Auditor Location:
26/F Tower A
Beijing Fortune Plaza, 7 DongsanhuanZhong Road
Chaoyang District, Beijing 100020, PRC1
Standard Audit Statement (Link): https://www.cpacanada.ca/webtrustseal?sealid=10169
Standard Audit Type: Type 2
Standard Audit Statement Date: April 9th 2019
Standard Audit Period Start Date: October 8th 2018
Standard Audit Period End Date: January 8th 2019

BR Audit Statement (Link): https://www.cpacanada.ca/webtrustseal?sealid=10170
BR Audit Type: Type 2
BR Audit Statement Date: April 9th 2019
BR Audit Period Start Date: October 8th 2018
BR Audit Period End Date: January 8th 2019

EV SSL Audit Statement (Link): https://www.cpacanada.ca/webtrustseal?sealid=10171
EV SSL Audit Type: Type 2
EV SSL Audit Statement Date: April 9th 2019
EV SSL Audit Period Start Date: October 8th 2018
EV SSL Audit Period End Date: January 8th 2019

Audit statements must be publicly accessible, not confidential, and translated into English. Audit statements will be rejected if they do not list the Distinguished Name and SHA256 fingerprint of each root and intermediate certificate that was in scope, and if they do not meet all of the requirements listed in Mozilla's Root Store Policy.

-- Required and Recommended Practices --

BR Self-Assessment: BR self-Assessment attached.

CA's Response to Required Practices:
CP/CPS section numbers addressing each of the items listed in https://wiki.mozilla.org/CA/Required_or_Recommended_Practices

1. Publicly Available CP and CPS:
1.1 Revision Table, updated annually: See CPS.
1.2 CAA Domains listed in CP/CPS: CPS 4.2.1 & 3.2.2.7.
1.3 BR Commitment to Comply statement in CP/CPS: See CPS1.1.2.
1.4 CP/CPS Structured According to RFC 3647, appropriate use of 'No Stipulation': See CPS1.1.2.
2. Audit Criteria:
2.1 Complete Audit History: Audit report attached.
3. Revocation of Compromised Certificates: CPS 4.9.1
4. Verifying Domain Name Ownership: CPS 3.2.2.3.
4.1 Baseline Requirements:
4.2 WHOIS:
4.3 Email Challenge-Response:
5. Verifying Email Address Control:
6. DNS names go in SAN: CPS 3.1.1
7. OCSP: CPS4.9.10 and CPS 7.3
- OCSP SHALL NOT respond "Good" for unissued certs:
8. Network Security Controls:

CPS 6.7. We also have internal documents to specify the detail Network security controls we comply with it.

-- Forbidden and Potentially Problematic Practices --

CA's Response to Forbidden Practices:

CP/CPS section numbers addressing each of the items listed in https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices
1. Long-lived Certificates: CPS 6.3.2.
2. Non-Standard Email Address Prefixes for Domain Ownership Validation: CPS 3.2.2.3
3. Issuing End Entity Certificates Directly From Roots: CPS1.1.3
4. Distributing Generated Private Keys in PKCS#12 Files: CPS 6.1.1.2.
5. Certificates Referencing Local Names or Private IP Addresses: CPS7.1.4.
6. Issuing SSL Certificates for .int Domains: None
7. OCSP Responses Signed by a Certificate Under a Different Root: OCSP Testing.
8. Issuance of SHA-1 Certificates: None.
9. Delegation of Domain / Email Validation to Third Parties: None. CPS1.3.2.

-- Root Certificate # 1 --

Certificate Data Extracted from PEM: vTrust RSA Root certificate Attached

The CCADB will automatically extract the following information from the PEM of the root certificate.
Subject
Issuer

Valid From
Valid To
Certificate Serial Number
SHA-1 Fingerprint
SHA-256 Fingerprint
Signature Hash Algorithm
Public Key Algorithm
SPKI SHA256
Subject + SPKI SHA256

-- Audits that apply to this Root Certificate --
Standard Audit: https://www.cpacanada.ca/webtrustseal?sealid=10169
BR Audit: https://www.cpacanada.ca/webtrustseal?sealid=10170
EV SSL Audit: https://www.cpacanada.ca/webtrustseal?sealid=10171

-- Application Information --

Explanation:

iTrusChina is a compliance CA in China and also the largest SSL reseller in China mainland. We conducted WebTrust audit and plan to apply our own root included in major operation system and browsers. We issue certificate to generic public customer.

Role:

Root certificate use RSA Algorithm.

Root Certificate Download URL:
Public URL through which the CA certificate can be directly downloaded.
http://wtca-cafiles.itrus.com.cn/crl/vTrusRootCA.crl

-- Mozilla Fields --

Mozilla Trust Bits:
One or both of Email (S/MIME) or Websites (TLS/SSL)
iTrusChina issue TLS/SSL certificate so far, may issue S/MIME certificate in future.
SSL Validation Type:

DV, OV and EV, See CPS Chapater 3.2 and Chapter 10.

Mozilla EV Policy OID(s):
2.23.140.1.1

Mozilla Applied Constraints:

*Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs.*

-- CA Hierarchy Information --

Indicate/Check all of the following that apply:
Cross-Signed by another Root Cert: No.
Has Externally Operated SubCAs: No.
CP/CPS allows Externally Operated SubCAs:
Has External Registration Authorities: No
CP/CPS allows External RAs:No

See attached files for CA Hierarchy Information.

Description of PKI Hierarchy:

- *URL and/or Description of this PKI Hierarchy.*
- *Provide details related to any of the check-boxes above that are selected.*
- *Add records for the existing intermediate certs to the CCADB as described here:*
  - *https://ccadb.org/cas/intermediates#adding-intermediate-certificate-data*
- *If Mozilla accepts and includes your root certificate, then we have to assume that we also accept any of your future sub-CAs and their sub-CAs. Therefore, the selection criteria for your sub-CAs and their sub-CAs will be a critical decision factor. As well as the documentation and auditing of operations requirements that you place on your sub-CAs and their sub-CAs.*
- *If this root has any subordinate CA certificates that are operated by external third parties, then provide the information listed in the Subordinate CA Checklist in a separate document.*

Constraints on External SubCAs & RAs:

None, iTrusChina does not have external SubCAs & RAs.

-- Test Websites or Example Cert --

Test Website - Valid: https://validrsa.itrus.cn
Test Website - Expired: https://expiredrsa.itrus.cn
Test Website - Revoked: https://revokersa.itrus.cn
All the 3 websites tested in Firefox.

Notes:

If not requesting the Websites trust bit, then provide an example cert that chains up to this root.

Make sure you test your three 'Test Websites' in Firefox as follows:

1. *Create a new Firefox Profile for testing, as described in Mozilla's knowledge base articles: Profile Manager and Creating a new Firefox Profile.*
2. *Import the root certificate as described here.*
3. *Set OCSP hard fail as described here.*
4. *Clear browser history*
5. *Browse to the test websites.*
6. *Open the Web Console to check for any warnings (e.g. SHA-1, etc.) that should be addressed.*

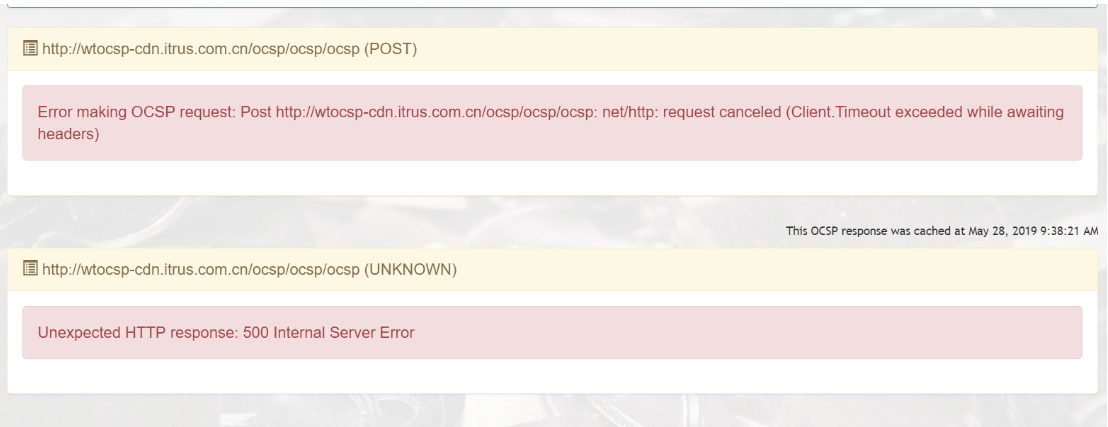
- *Intermediate CA certificates are expected to be distributed to the certificate subjects (the holders of the private keys) together with the subjects' own certificates. Those subject parties (e.g. SSL servers) are then expected to send out the intermediate CA certificates together with their own certificates whenever they are asked to send out their certificates. That is required by SSL/TLS.*
- *Certificate authorities MUST advise their subscribers that all intermediate certificates should be installed in the servers containing the dependent subscriber certificates.*

-- Test Results (When Requesting the SSL/TLS Trust Bit) --

Revocation Tested:

Test with http://certificate.revocationcheck.com/ and make sure there aren't any errors.

OCSP Post Error occurred as following picture,



http://wtocsp-cdn.itrus.com.cn/ocsp/ocsp/ocsp (POST)

Error making OCSP request: Post http://wtocsp-cdn.itrus.com.cn/ocsp/ocsp/ocsp: net/http: request canceled (Client.Timeout exceeded while awaiting headers)

This OCSP response was cached at May 28, 2019 9:38:21 AM

http://wtocsp-cdn.itrus.com.cn/ocsp/ocsp/ocsp (UNKNOWN)

Unexpected HTTP response: 500 Internal Server Error

iTrusChina tested OCSP Post query with our coding, test results successful as following,

```
Starting Post Query********************
2019-05-08 10:04:32-984 preparing OCSP
2019-05-08 10:04:32-988 Analyze the address of OCSP:
2019-05-08 10:04:32-988 OCSP Address is： http://wtocsp-
cdn.itrus.com.cn/ocsp/ocsp/ocsp
2019-05-08 10:04:32-989 OCSP return code：200
```

```
2019-05-08 10:04:33-394 OCSP return value：0
OCSP Signing Algorithm OID：1.2.840.113549.1.1.11
ThisUpdate：Wed May 08 10:04:33 CST 2019
NextUpdate：null
2019-05-08 10:04:33-400 Certificate Status：GOOD
```

CA/Browser Forum Lint Test:

Provide evidence that you have tested and verified that no certificates issued in this CA hierarchy violate any of the CA/Browser Forum Baseline Requirements (BRs).
BR Lint Test: https://github.com/awslabs/certlint

Mozilla will check that the CA is not issuing certificates that violate any of the BRs *by using crt.sh on the root and subordinate CAs via:*
https://crt.sh/?caid=<CA ID>&opt=cablint,zlint,x509lint&minNotBefore=2014-01-01
and/or
The Lint tests in https://crt.sh/?a=1

Certificate tested with lint at https://crt.sh

Test Website Lint Test:

Provide evidence that you have tested and verified that no certificates issued in this CA hierarchy violate the X.509 rules.
X.509 Lint Test: https://github.com/kroeckx/x509lint

https://wiki.mozilla.org/CA:TestErrors -- Meaning and recommended solutions to errors that CAs have run into while doing the tests listed above.

EV Tested:

If EV treatment is being requested, then provide successful output from EV Testing as described here: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version

EV Treatment Tested results OK.

-- End Root Certificate #1 --

If you are requesting inclusion for multiple root certificates that are covered in the same audit statements, then repeat the information in the “Root Certificate # 1” section for each additional root.

-- Root Certificate # 2 --

Certificate Data Extracted from PEM: vTrust ECC Root certificate Attached

The CCADB will automatically extract the following information from the PEM of the root certificate.

Subject
Issuer
Valid From
Valid To
Certificate Serial Number
SHA-1 Fingerprint
SHA-256 Fingerprint
Signature Hash Algorithm
Public Key Algorithm
SPKI SHA256
Subject + SPKI SHA256

-- Audits that apply to this Root Certificate --

Indicate/Check which of the provided audit statements apply to this root certificate. As per Mozilla's Root Store Policy, each audit statement must clearly provide the distinguished Name and SHA256 fingerprint of each root and intermediate certificate that was in scope.

Standard Audit: https://www.cpacanada.ca/webtrustseal?sealid=10169
BR Audit: https://www.cpacanada.ca/webtrustseal?sealid=10170
EV SSL Audit: https://www.cpacanada.ca/webtrustseal?sealid=10171

-- Application Information --

Explanation:

iTrusChina is a compliance CA in China and also the largest SSL reseller in China mainland. We conducted WebTrust audit and plan to apply our own root included in major operation system and browsers. We issue certificate to generic public customer.

Role:

Root certificate use ECC Algorithm.

Root Certificate Download URL:

Public URL through which the CA certificate can be directly downloaded.
http://wtca-cafiles.itrus.com.cn/crl/vTrusECCRootCA.crl

-- Mozilla Fields --

Mozilla Trust Bits:

One or both of Email (S/MIME) or Websites (TLS/SSL)
iTrusChina issue TLS/SSL certificate so far, may issue S/MIME certificate in future.

SSL Validation Type:

DV, OV and EV, See CPS Chapater 3.2 and Chapter 10.

Mozilla EV Policy OID(s):

2.23.140.1.1

Before requesting EV treatment, CAs should understand how [Firefox processes EV certificates](https://wiki.mozilla.org/CA/EV_Processing_for_CAs) and determine if they should use the standard CA/Browser Forum EV OID (2.23.140.1.1) or a CA-specific OID. Unless the CA already has a CA-specific OID enabled in Firefox, Mozilla strongly recommends that CAs use the standard CA/Browser Forum EV OID.

Mozilla Applied Constraints:

*Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs.*

-- CA Hierarchy Information --

Indicate/Check all of the following that apply:

Cross-Signed by another Root Cert: None.
Has Externally Operated SubCAs: None.
CP/CPS allows Externally Operated SubCAs:
Has External Registration Authorities: None.
CP/CPS allows External RAs: No.
See attached files for CA Hierarchy information.

Description of PKI Hierarchy:

- *URL and/or Description of this PKI Hierarchy.*
- *Provide details related to any of the check-boxes above that are selected.*
- *Add records for the existing intermediate certs to the CCADB as described here:*
    - *https://ccadb.org/cas/intermediates#adding-intermediate-certificate-data*
- *If Mozilla accepts and includes your root certificate, then we have to assume that we also accept any of your future sub-CAs and their sub-CAs. Therefore, the selection criteria for your sub-CAs and their sub-CAs will be a critical decision factor. As well as the documentation and auditing of operations requirements that you place on your sub-CAs and their sub-CAs.*
- *If this root has any subordinate CA certificates that are operated by external third parties, then provide the information listed in the Subordinate CA Checklist in a separate document.*

Constraints on External SubCAs & RAs:

iTrusChina does not have any external SubCAs & RAs.

-- Test Websites or Example Cert --

If requesting Websites trust bit provide 3 URLs to 3 test websites (valid, expired, revoked) whose TLS/SSL cert chains up to this root.

Test Website - Valid: https://validecc.itrus.cn
Test Website - Expired: https://expiredecc.itrus.cn
Test Website - Revoked: https://revokeecc.itrus.cn
All the three websites tested in Firefox.

Make sure you test your three 'Test Websites' in Firefox as follows:

7. *Create a new Firefox Profile for testing, as described in Mozilla's knowledge base articles: Profile Manager and Creating a new Firefox Profile.*
8. *Import the root certificate as described here.*
9. *Set OCSP hard fail as described here.*
10. *Clear browser history*
11. *Browse to the test websites.*
12. *Open the Web Console to check for any warnings (e.g. SHA-1, etc.) that should be addressed.*

- *Intermediate CA certificates are expected to be distributed to the certificate subjects (the holders of the private keys) together with the subjects' own certificates. Those subject parties (e.g. SSL servers) are then expected to send out the intermediate CA certificates together with their own certificates whenever they are asked to send out their certificates. That is required by SSL/TLS.*
- *Certificate authorities MUST advise their subscribers that all intermediate certificates should be installed in the servers containing the dependent subscriber certificates.*

-- Test Results (When Requesting the SSL/TLS Trust Bit) --

Revocation Tested:

Test with http://certificate.revocationcheck.com/ and make sure there aren't any errors.

CA/Browser Forum Lint Test:

Provide evidence that you have tested and verified that no certificates issued in this CA hierarchy violate any of the CA/Browser Forum Baseline Requirements (BRs).
BR Lint Test: https://github.com/awslabs/certlint

Mozilla will check that the CA is not issuing certificates that violate any of the BRs *by using crt.sh on the root and subordinate CAs via:*
https://crt.sh/?caid=<CA ID>&opt=cablint,zlint,x509lint&minNotBefore=2014-01-01
and/or
The Lint tests in https://crt.sh/?a=1

Certificate tested with lint at https://crt.sh

Test Website Lint Test:

Provide evidence that you have tested and verified that no certificates issued in this CA hierarchy violate the X.509 rules.

X.509 Lint Test: https://github.com/kroeckx/x509lint

https://wiki.mozilla.org/CA:TestErrors -- Meaning and recommended solutions to errors that CAs have run into while doing the tests listed above.

EV Tested:

If EV treatment is being requested, then provide successful output from EV Testing as described here: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version

EV Treatment Tested results OK.

-- End Root Certificate #2 --