
IN GOD WE TRUST

In Cyber-Anchors We Trust

网络空间中的信任与冲突: Web PKI

段海新, 清华大学

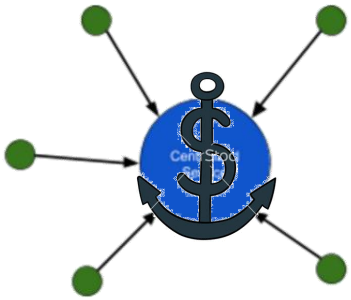
西安交通大学, 2016

Outline

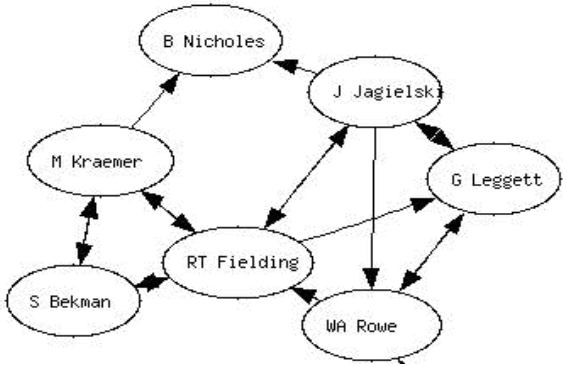
- Trust models and trust anchors
- In Routing, We Trust…
- In DNS, We Trust …
- In Web PKI, We Trust

Trust models or policies

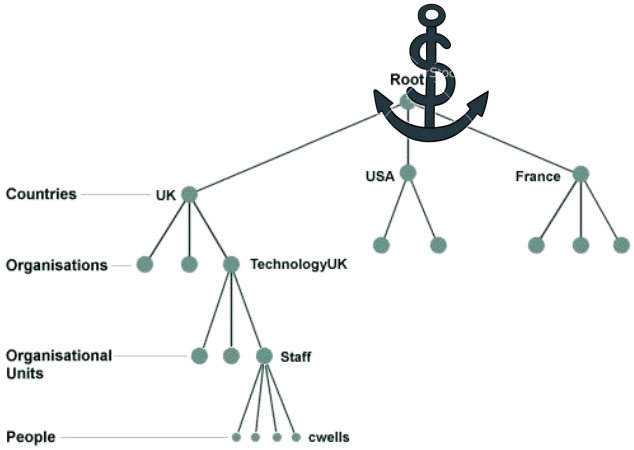
Centralized (e.g. Kerberos)



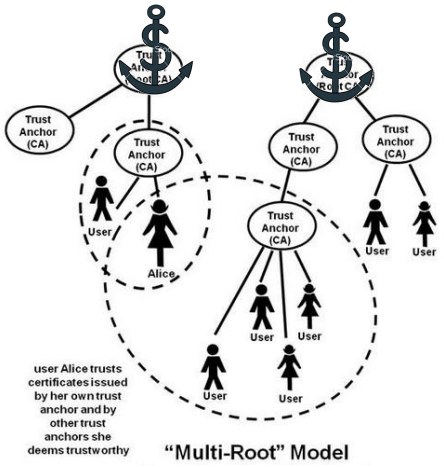
Web of Trust (e.g. PGP, BGP)



Hierarchy and delegation (e.g. DNS, X500)



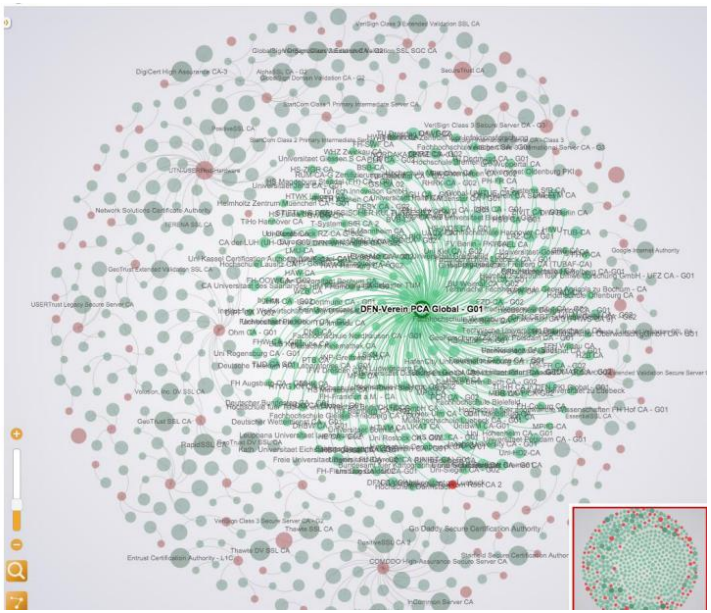
Forest(e.g. CA)

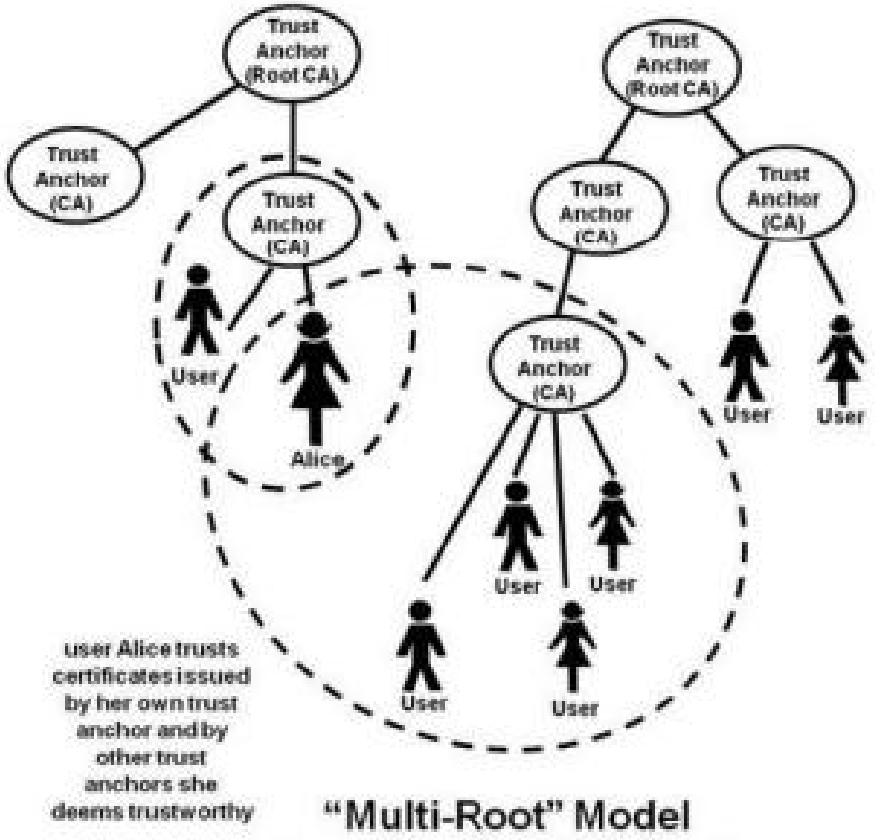


Trust on First Use, e.g. SSH, DNS/Cert Pinning

Trust model of Web PKI

- Web PKI 是 SSL/TLS 的基石，X.509 证书是 HTTPS 的关键要素
  - 树状签发结构
  - 森林状信任模型





Outline

- Why encryption?
- How CA works
- Problem of CA
- CDN problems
- Solutions

为什么加密？

We've been here (or nearby) before

IETF Technical Plenary, November 2013

Brian Carpenter

RFC 7258: Pervasive Monitoring Is an Attack

https://tools.ietf.org/html/rfc7258

Internet Engineering Task Force (IETF)
Request for Comments: 7258
BCP: 188
Category: Best Current Practice
ISSN: 2070-1721

S. Farrell
Trinity College Dublin
H. Tschofenig
ARM Ltd.

May 2014

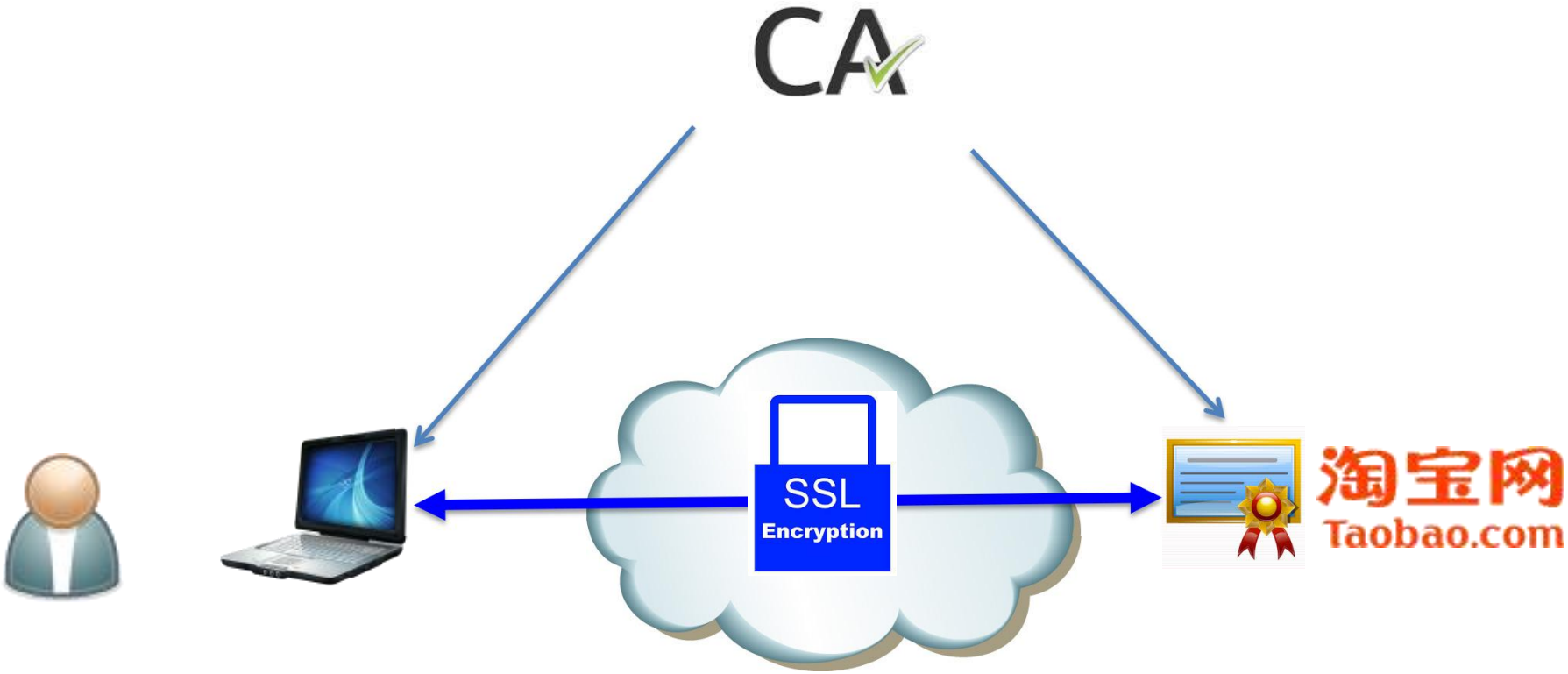
Pervasive Monitoring Is an Attack

Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible.

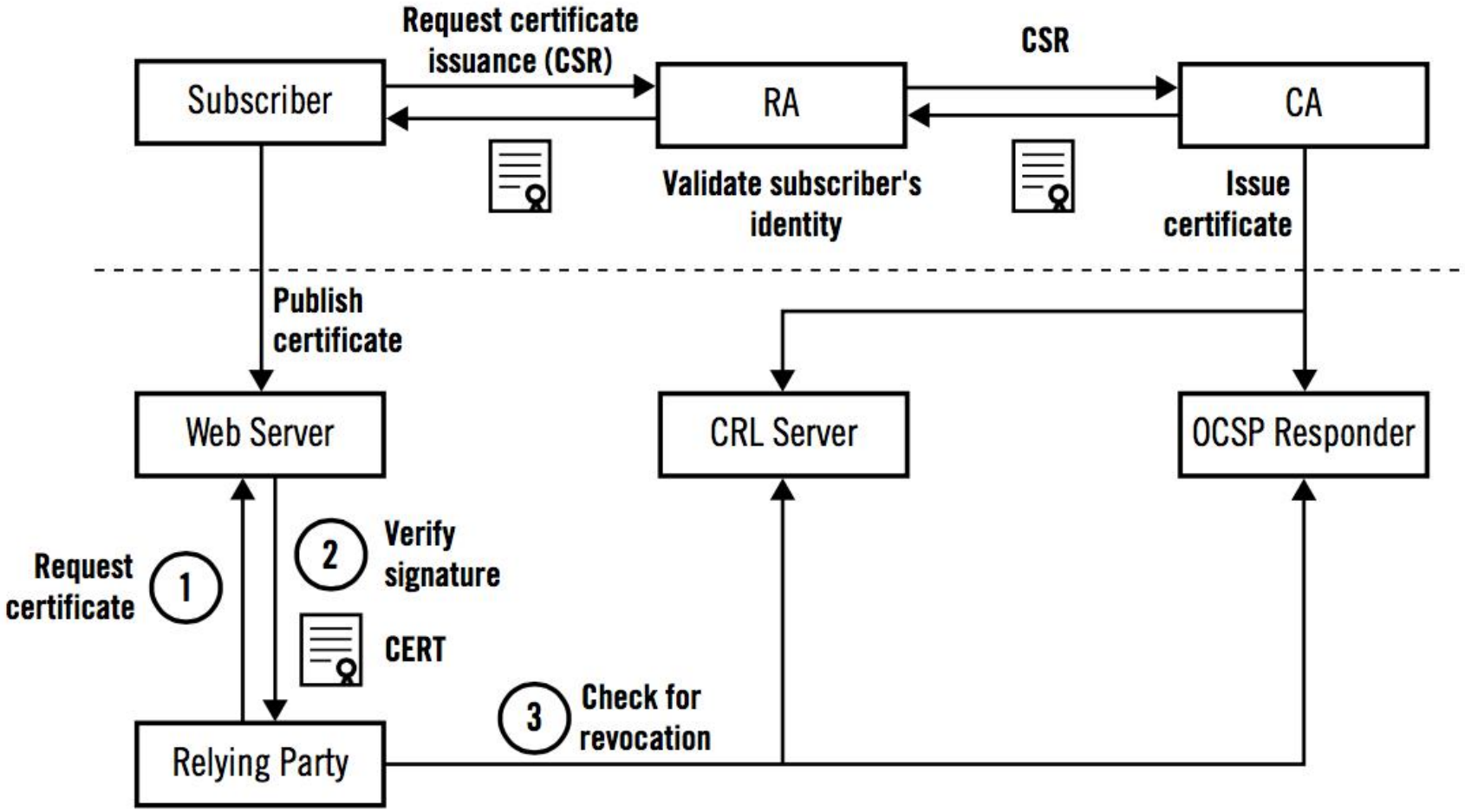
Outline

- Why encryption?
- How CA works
- Problem of CA
- CDN problems
- Solutions

开放式的通信环境中的安全通信需要可信第三方（PKI/CA）



Internet PKI certificate lifecycle

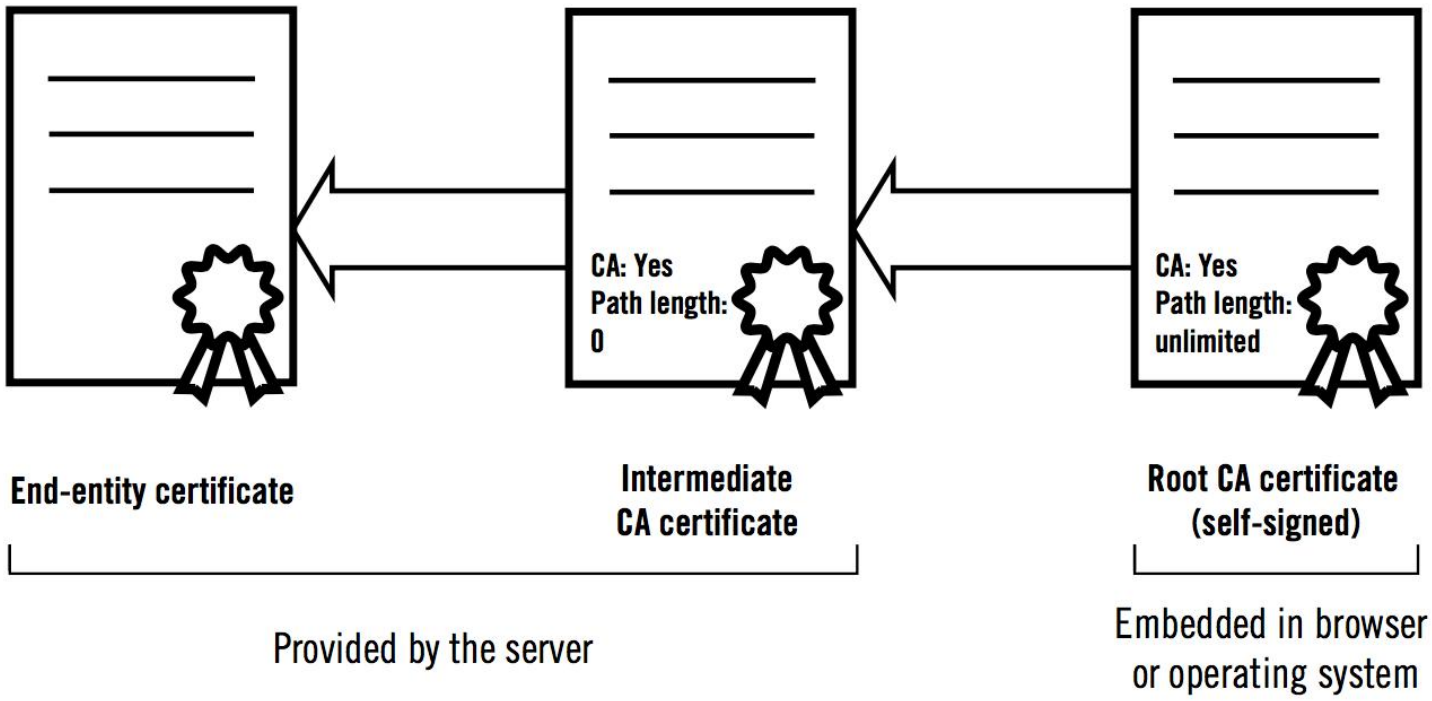


IETF PKIX 工作组开发的标准， Internet PKI or Web PKI

原理

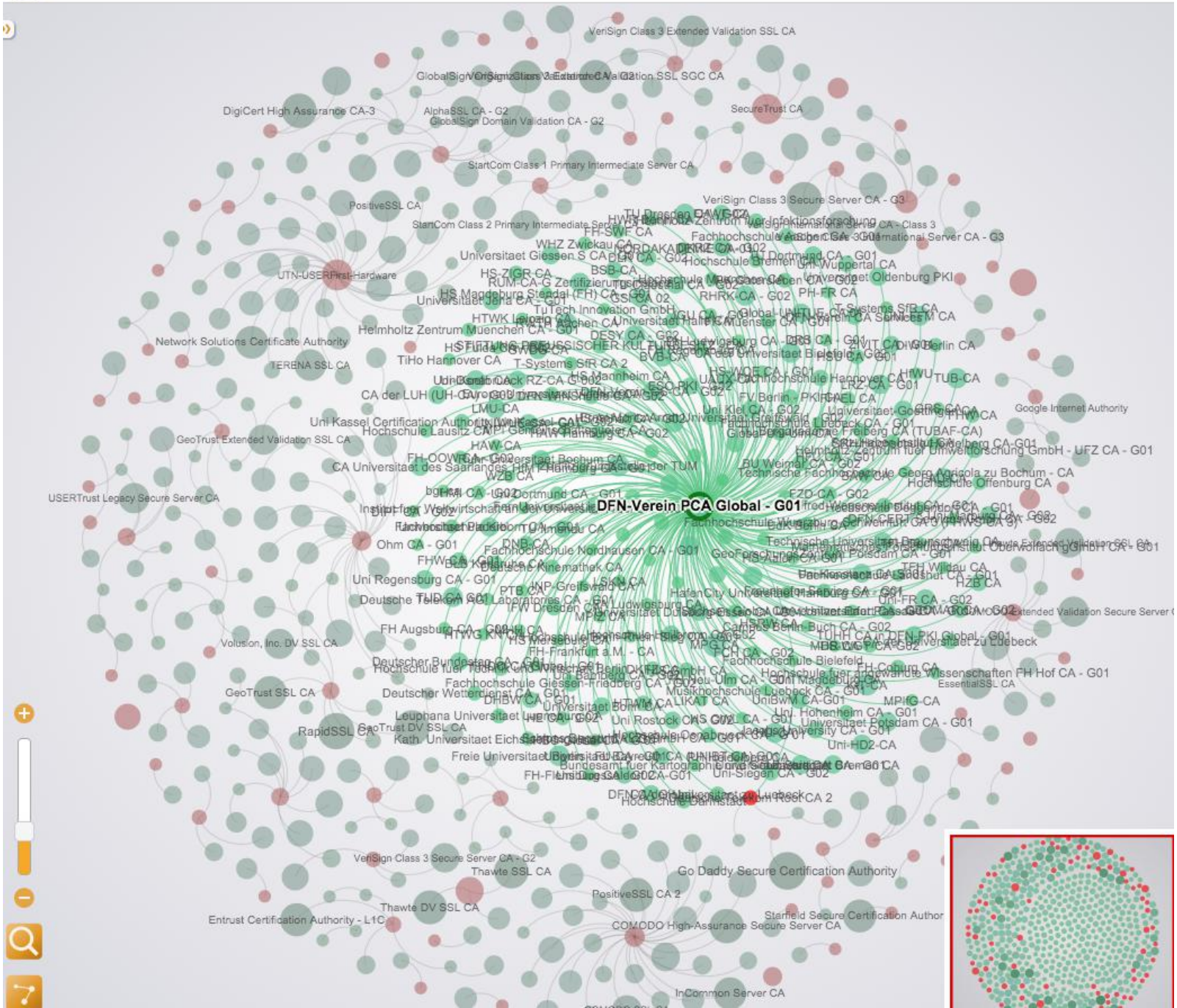
- Subscriber 提交 CSR(*Certificate Signing Request*)
- RA/CA验证 Subscriber 身份
- CA 签发证书
- 在Web服务器上部署证书
- 浏览器访问网站时：
  - 服务器在TLS握手过程中出具证书
  - 浏览器验证证书链的有效性
  - 如果验证通过，则协商会话秘钥，继续通信
  - 如果不通过，弹出告警

证书链



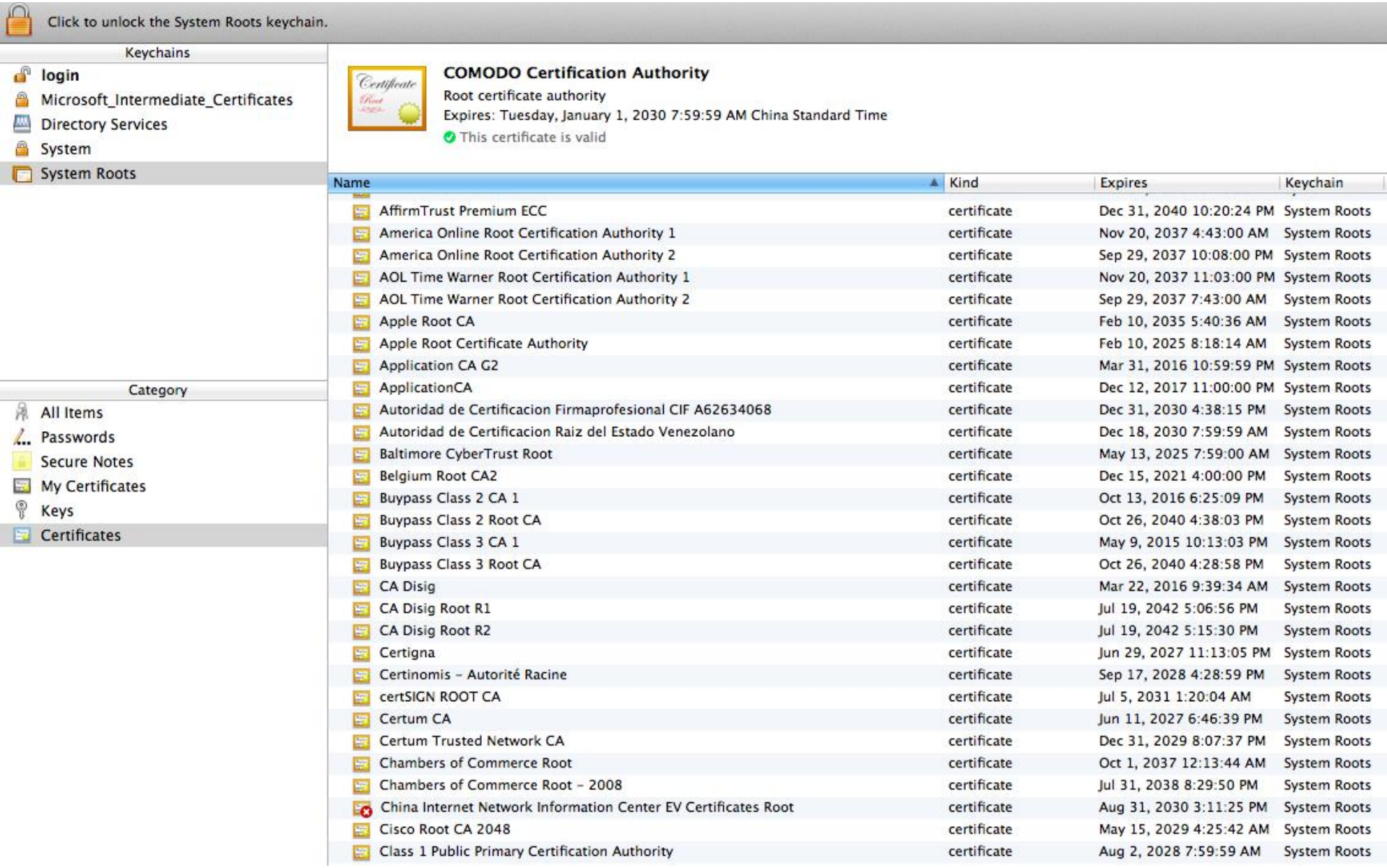
- Root CA 在操作系统或浏览器中维护
- 证书链由Server 提供

The ICSI SSL Notary: CA Certificates



Root Store in Relying Parties (i.e. OS, Browser)

- Each OS provides a root store for bootstrap
  - Mozilla is an exception, who maintains its own root store
  - Some relying parties, like hardware, cannot update its root store
- Root Certificate Programs
  - Apple :https://www.apple.com/certificateauthority/ca_program.html
  - Microsoft: https://msdn.microsoft.com/en-us/library/cc751157.aspx
  - Chrome: Certificate Transparency
  - Mozilla Certificate Program


Click to unlock the System Roots keychain.
Keychains
login
Microsoft_Intermediate_Certificates
Directory Services
System
System Roots
Category
All Items
Passwords
Secure Notes
My Certificates
Keys
Certificates
COMODO Certification Authority
Root certificate authority
Expires: Tuesday, January 1, 2030 7:59:59 AM China Standard Time
This certificate is valid
Name
Kind
Expires
Keychain
AffirmTrust Premium ECC certificate Dec 31, 2040 10:20:24 PM System Roots
America Online Root Certification Authority 1 certificate Nov 20, 2037 4:43:00 AM System Roots
America Online Root Certification Authority 2 certificate Sep 29, 2037 10:08:00 PM System Roots
AOL Time Warner Root Certification Authority 1 certificate Nov 20, 2037 11:03:00 PM System Roots
AOL Time Warner Root Certification Authority 2 certificate Sep 29, 2037 7:43:00 AM System Roots
Apple Root CA certificate Feb 10, 2035 5:40:36 AM System Roots
Apple Root Certificate Authority certificate Feb 10, 2025 8:18:14 AM System Roots
Application CA G2 certificate Mar 31, 2016 10:59:59 PM System Roots
ApplicationCA certificate Dec 12, 2017 11:00:00 PM System Roots
Autoridad de Certificacion Firmaprofesional CIF A62634068 certificate Dec 31, 2030 4:38:15 PM System Roots
Autoridad de Certificacion Raiz del Estado Venezolano certificate Dec 18, 2030 7:59:59 AM System Roots
Baltimore CyberTrust Root certificate May 13, 2025 7:59:00 AM System Roots
Belgium Root CA2 certificate Dec 15, 2021 4:00:00 PM System Roots
Buypass Class 2 CA 1 certificate Oct 13, 2016 6:25:09 PM System Roots
Buypass Class 2 Root CA certificate Oct 26, 2040 4:38:03 PM System Roots
Buypass Class 3 CA 1 certificate May 9, 2015 10:13:03 PM System Roots
Buypass Class 3 Root CA certificate Oct 26, 2040 4:28:58 PM System Roots
CA Disig certificate Mar 22, 2016 9:39:34 AM System Roots
CA Disig Root R1 certificate Jul 19, 2042 5:06:56 PM System Roots
CA Disig Root R2 certificate Jul 19, 2042 5:15:30 PM System Roots
Certigna certificate Jun 29, 2027 11:13:05 PM System Roots
Certinomis - Autorité Racine certificate Sep 17, 2028 4:28:59 PM System Roots
certSIGN ROOT CA certificate Jul 5, 2031 1:20:04 AM System Roots
Certum CA certificate Jun 11, 2027 6:46:39 PM System Roots
Certum Trusted Network CA certificate Dec 31, 2029 8:07:37 PM System Roots
Chambers of Commerce Root certificate Oct 1, 2037 12:13:44 AM System Roots
Chambers of Commerce Root - 2008 certificate Jul 31, 2038 8:29:50 PM System Roots
China Internet Network Information Center EV Certificates Root certificate Aug 31, 2030 3:11:25 PM System Roots
Cisco Root CA 2048 certificate May 15, 2029 4:25:42 AM System Roots
Class 1 Public Primary Certification Authority certificate Aug 2, 2028 7:59:59 AM System Roots

Root Certs

- Mozilla Included CA Cert. List: 170(2016/4/25)
- Apple Mac OS X ~167 (my macbook pro)
- CAB Forum
  - The *CA/Browser Forum* (or *CAB Forum*) is a voluntary group of CAs, browser vendors, and other interested parties whose goal is to establish and enforce standards for certificate issuance and processing.

https://cabforum.org/members/

Home » Members

About Us » | Baseline R

MEMBERS

As of 2016 the CA/Browser Forum inclu

Certification Authorities

- Actalis S.p.A.
- Amazon
- ANF Autoridad de Certificación
- AS Sertifitseerimiskeskus
- Buypass AS
- Camerfirma
- Certinomis
- certSIGN
- Certum
- China Financial Certification Authorit
- Chunghwa Telecom Co., Ltd.
- China Internet Network Information
- Cisco
- Comodo CA Ltd
- D-TRUST GmbH
- DigiCert, Inc.
- Disig, a.s.
- DocuSign (formerly OpenTrust/KEYN
- E-TUGRA Inc.
- Entrust
- ESG de Electronische Signatuur B.V.

https://cabforum.org/members/

Entrust | About Us » | Baseline Requirements » | Extended Validation »

- ESG de Electronische Signatuur B.V.
- Firmaprofesional
- GlobalSign
- GoDaddy Inc
- Hellenic Academic and Research Institutions Certification Authority (HARICA)
- Izenpe S.A.
- Kamu Sertifikasyon Merkezi
- KPN Corporate Market BV
- Let's Encrypt
- Logius PKIoverheid
- National Center for Digital Certification
- Network Solutions, LLC
- Open Access Technology International
- Prvni certifikacni autorita, a.s.
- QuoVadis Ltd.
- Shanghai Electronic Certification Authority Center Co. Ltd
- Skaitmeninio sertifikavimo centras (SSC)
- StartCom Certification Authority
- Swisscom (Switzerland) Ltd
- SwissSign AG
- Symantec Corporation
- TAIWAN-CA Inc.
- Trend Micro Inc.
- TrustCor Systems, S. de R.L.
- Trustis Limited
- Trustwave
- TURKTRUST
- WoSign

Internet Browser Software Vendors

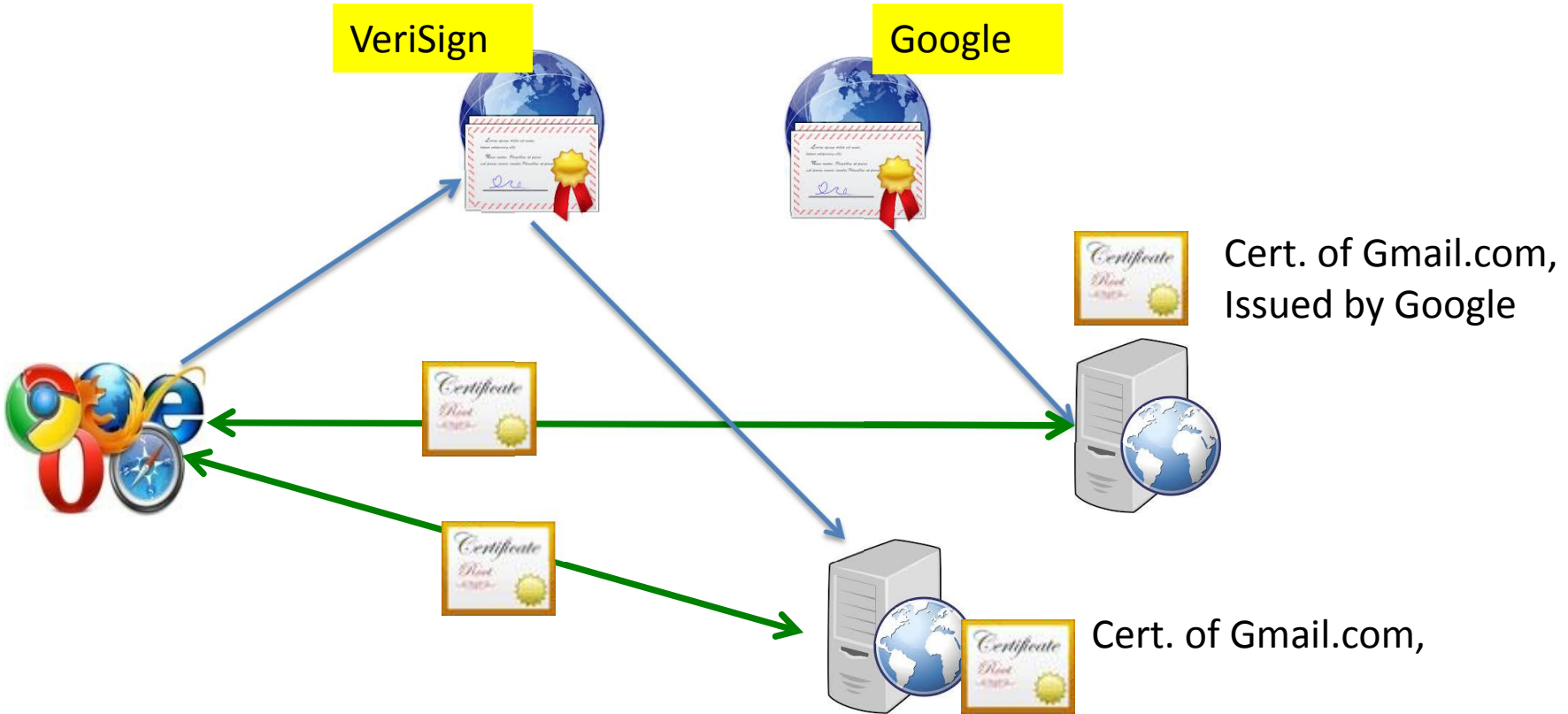
- Apple
- Google Inc.
- Microsoft Corporation
- Mozilla Foundation
- Opera Software ASA
- Qihoo 360

Problems of Web PKI

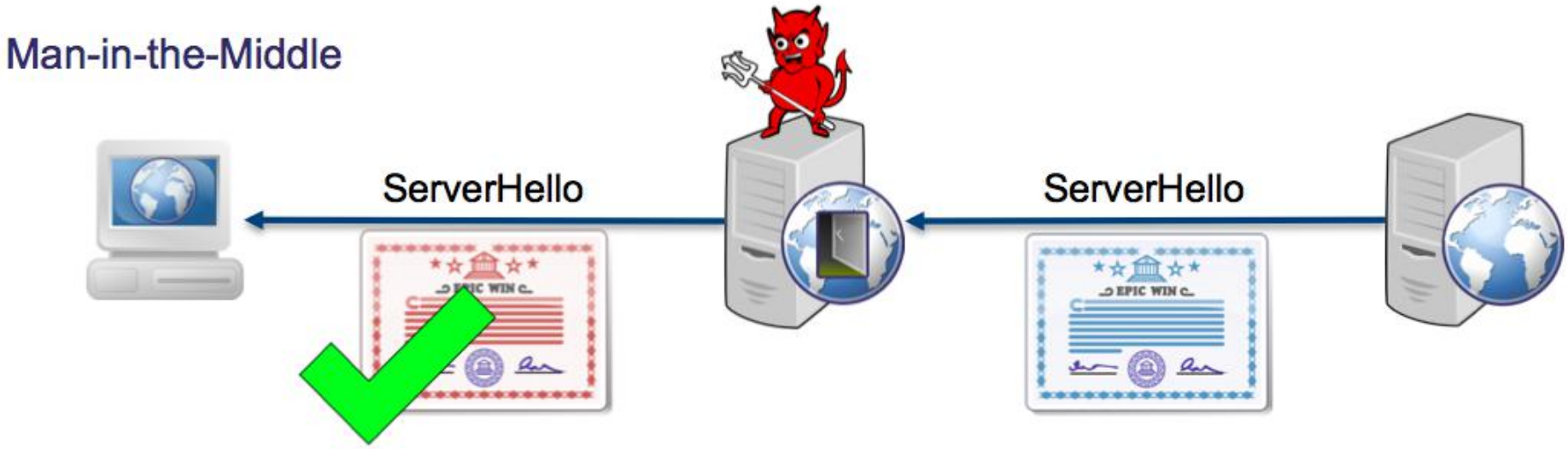
- 信任模型的问题
  - 任何一个CA可以为任何一个网站签发证书，无需网站的同意
- 自签名证书的问题
- 验证的问题
  - 如何验证申请者的身份？
- 弱密码的问题
- 用户忽略告警
- 证书撤销的问题

Problems of trust model of Web PKI

- 浏览器/OS厂商预置了数百个CA 的根证书
- 每个CA都可签发所有网站证书，被视为合法
- 一个CA被攻破，则所有商务应用可能被颠覆



Man in the Middle attack with faked but valid certificate



The (fake) certificate is…

- Not expired or revoked
- Validates with one of the many CA's
- Has a matching common name

CA故意作恶

Symantec employees fired for issuing rogue HTTPS certificate for Google

Unauthorized credential was trusted by all browsers, but Google never authorized it.

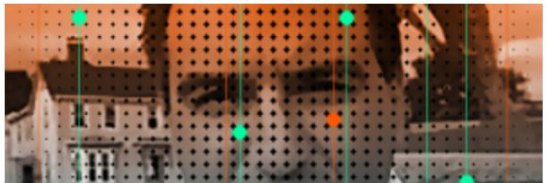
by **Dan Goodin** - Sep 22, 2015 3:35am CST

Symantec has fired an undisclosed number of employees after they were caught issuing unauthorized cryptographic certificates that made it possible to impersonate HTTPS-protected Google webpages.

"We learned on Wednesday that a small number of test certificates were inappropriately issued internally this week for three domains during product testing," Symantec officials wrote in a blog post published Friday. "All of these test certificates and keys were always within our control and were immediately revoked when we discovered the issue. There was no direct impact to any of the domains and never any danger to the Internet."

The post went on to say that the unnamed employees were terminated for failing to follow Symantec policies. Symantec officials didn't identify the three domains the test certificates covered, but in a separate blog post, Google researchers said Symantec's Thawte-branded certificate authority service issued an Extended Validation pre-certificate for the domains google.com and www.google.com.

LATEST FEATURE STORY



CA管理员失职

https://technet.microsoft.com/library/security/ms01-017

Microsoft | TechNet

United

Security TechCenter

Search TechNet with Bing

Home Security Updates Tools Learn Library Support

Collapse All Any suggestion

- Security Advisories and Bulletins
- Security Bulletins
  - 2001
    - MS01-060
    - MS01-059
    - MS01-058
    - MS01-057
    - MS01-056
    - MS01-055
    - MS01-054
    - MS01-053
    - MS01-052
    - MS01-051
    - MS01-050
    - MS01-049
    - MS01-048
    - MS01-047
    - MS01-046
    - MS01-045
    - MS01-044
    - MS01-043

Microsoft Security Bulletin MS01-017 - Critical

Erroneous VeriSign-Issued Digital Certificates Pose Spoofing Hazard

Published: March 22, 2001 | Updated: June 23, 2003

Version: 2.3

Originally posted: March 22, 2001
Updated: June 23, 2003

Summary

Who should read this bulletin:
All customers using Microsoft® products.

Impact of vulnerability:
Attacker could digitally sign code using the name "Microsoft Corporation".

Recommendation:
All customers should install the update discussed below.

Affected Software:

- Microsoft Windows® 95

为啥不通过URL撤销证书呢？

https://technet.microsoft.com/library/security/ms

Knowledge Base a

CRL 1 of 37

Patch availability

Download locations for this patch

- http://www.microsoft.com/downloads/details.aspx?FamilyId=43FD979A-03C1-4008-B38D-70E9BCD67454&displaylang=en

Additional information about this patch
Installation platforms:

The update has been tested on the following operating systems, when running Internet Explorer 4.01 Service Pack 2, Internet Explorer 5.01 Service Pack 1 or Service Pack 2, or Internet Explorer 5.5 Service Pack 1:

- Windows 95
- Windows 98
- Windows 98 Second Edition

VeriSign has revoked the certificates, and they are listed in VeriSign's current Certificate Revocation List (CRL). However, because VeriSign's code-signing certificates do not specify a CRL Distribution Point (CDP), it is not possible for any browser's CRL-checking mechanism to locate and use the VeriSign CRL. Microsoft has developed an update that rectifies this problem.

Google to drop China's CNNIC Root Certificate Authority after trust breach

by OWEN WILLIAMS — 1 year ago in INSIDER

Lenovo Superfish Adware

https://www.us-cert.gov/ncas/alerts/TA15-051A

Alert (TA15-051A)

More Alerts

Lenovo Superfish Adware Vulnerable to HTTPS Spoofing

Original release date: February 20, 2015 | Last revised: February 24, 2015

Print Tweet Send Share

Systems Affected

Lenovo consumer PCs that have Superfish VisualDiscovery installed.

Overview

Superfish adware installed on some Lenovo PCs install a non-unique trusted root certification authority (CA) certificate, allowing an attacker to spoof HTTPS traffic.

Description

Starting in September 2014, Lenovo pre-installed Superfish VisualDiscovery spyware on some of their PCs. This software intercepts users' web traffic to provide targeted advertisements. In order to intercept encrypted connections (those using HTTPS), the software installs a trusted root CA certificate for Superfish. All browser-based encrypted traffic to the Internet is intercepted, decrypted, and re-encrypted to the user's browser by the application – a classic man-in-the-middle attack. Because the certificates used by Superfish are signed by the CA installed by the software, the browser will not display any warnings that the traffic is being tampered with. Since the private key can easily be recovered from the Superfish software, an attacker can generate a certificate for any website that will be trusted by a system with the Superfish software installed. This means websites, such as banking and email, can be spoofed without a warning from the browser.

Although Lenovo has stated they have discontinued the practice of pre-installing Superfish VisualDiscovery, the systems that came with the software already installed will continue to be vulnerable until corrective actions have been taken.

To detect a system with Superfish installed, look for a HTTP GET request to:

superfish.aistcdn.com

The full request will look like:

CA被攻破: DigiNotar

- CA , Root CA, issue commercial and gov cert.
- June,20, 2011, COO :“We believe that DigiNotar's certificates are among the most reliable in the field.”
- July. 10, 2011, issued a certificate for *.google.com , used in multiple Iranian ISPs
- DigiNotar belatedly admitted dozens fraudulent certificates, including Yahoo!, Mozilla, Wordpress, and Tor
- DigiNotar detected intrusions, but did not disclose to browser vendors.
- Microsoft, Mozilla, Google, Apple and Opera browser revoke Root Certificate of DigiNotar

Validation of

- Server Certificate serves as website identity
  - Domain Validation (DV)
    - Trust Domain Name ➔ Email address?
  - Organization Validation (OV)

  - Extended Validation (EV)

Mike Zusman, Criminal charges are not pursued: Hacking PKI (DEFCON, 2008)

Action Required - thawte certificate application approval

From: **customers@thawte.com**
Sent: Tue 7/29/08 9:40 AM
To: sslcertificates@live.com

Hi,

You have been identified as the authorizing contact person for a thawte digital certificate that will be issued t

LOGIN.LIVE.COM

As the authorizing contact for this order, you are required to approve this application by clicking on the link p

This order will only be completed once you have approved the application. Follow[illegible] the technical c
an e-mail containing further instructions on how to activate the certificate.

To approve this application please click here and follow the two-step process:
https://www.thawte.com/process/retail/processSSL123Pickup?lang=en&secretCode=2660bc2cc006c094613d6b473df00c74

Should you require more information concerning the migration please contact our Technical Support Help Desk at su

Thank you for choosing thawte as your trusted partner. Kind regards,

Customer Support

Thawte accepted for authentication was sslcertificates@live.com, and that one was available for registration.

历史重演：2015，Comodo

A Finnish man created this simple email account - and received Microsoft's security certificate

JAA ARTIKKELI

A Finnish IT professional was able to obtain an HTTPS certificate for the Finnish version of Microsoft's Windows Live service simply by asking for it.

The browser-trusted certificate authority Comodo was fooled by an e-mail address that should not have been given to a normal user in the first place.

It all started when the Finnish man, working as an IT manager, noticed in January that it is possible create multiple aliases in Microsoft Live e-mail service.

“I was wondering whether I could create an address resembling one of an admin. And just for laughs I gave it a go”, he tells Tivi.fi.

A few moments later, he had created the alias hostmaster@live.fi. He decided to give the address a test run by trying to get a trusted certificate.

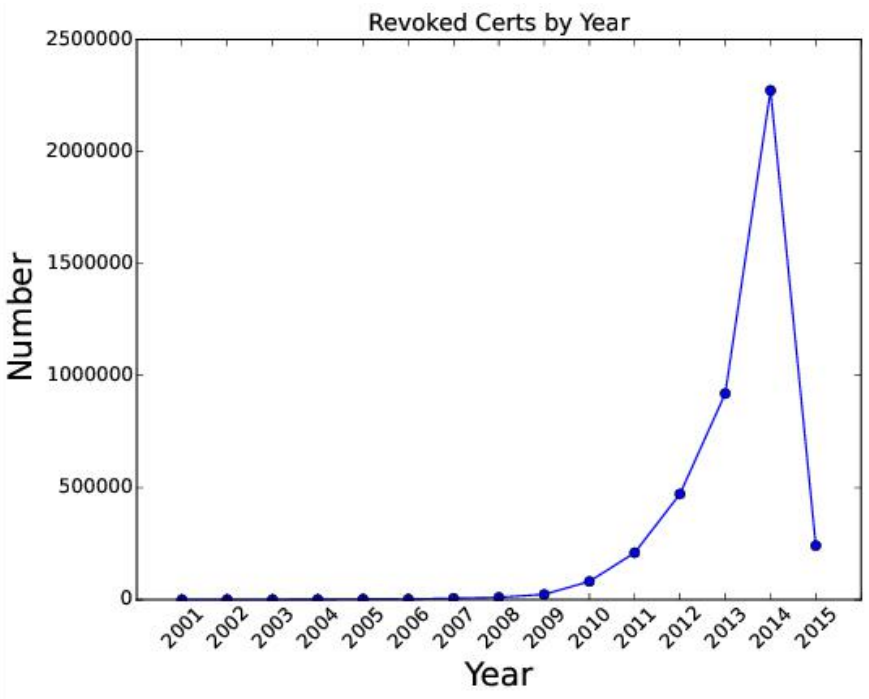
To his surprise, Comodo issued the certificate, no questions asked.

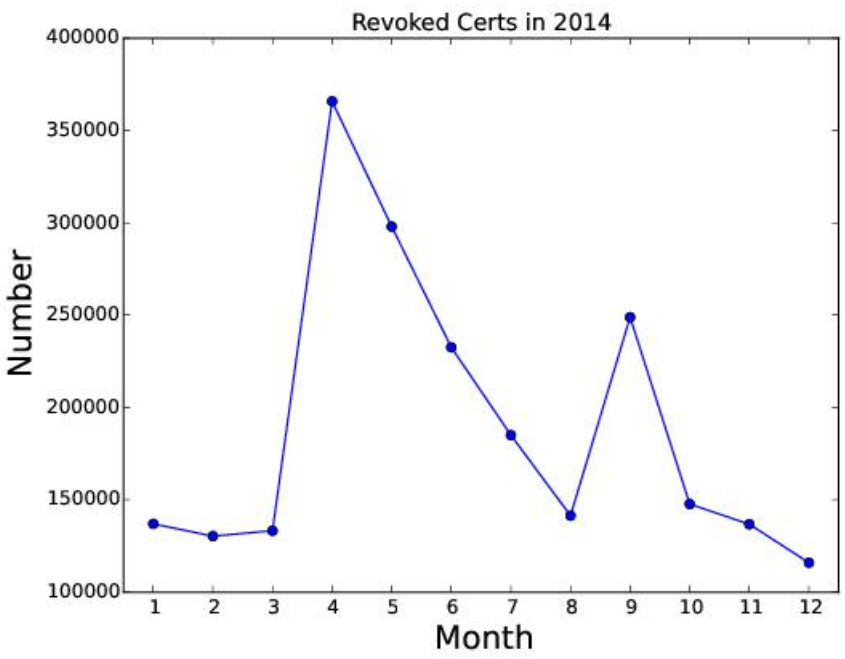
弱密码算法：MD5, SHA-1

- **1991-1996**: MD5, 很快流行
- 2004. 王小云教授展示了可以产生MD5的collision
- 2005: 王小云展示可以产生两个同样签名的证书，但是秘钥不同
- 2006：Stevens, Lenstra, and de Weger， *chosen prefix collision*， 可以制造两个ID不同、签名相同的证书
- 2008: 从CA获得了一个假冒的CA证书
- 2012: Flame 病毒用伪造的CA证书签发微软的补丁更新

被撤销的证书数目庞大

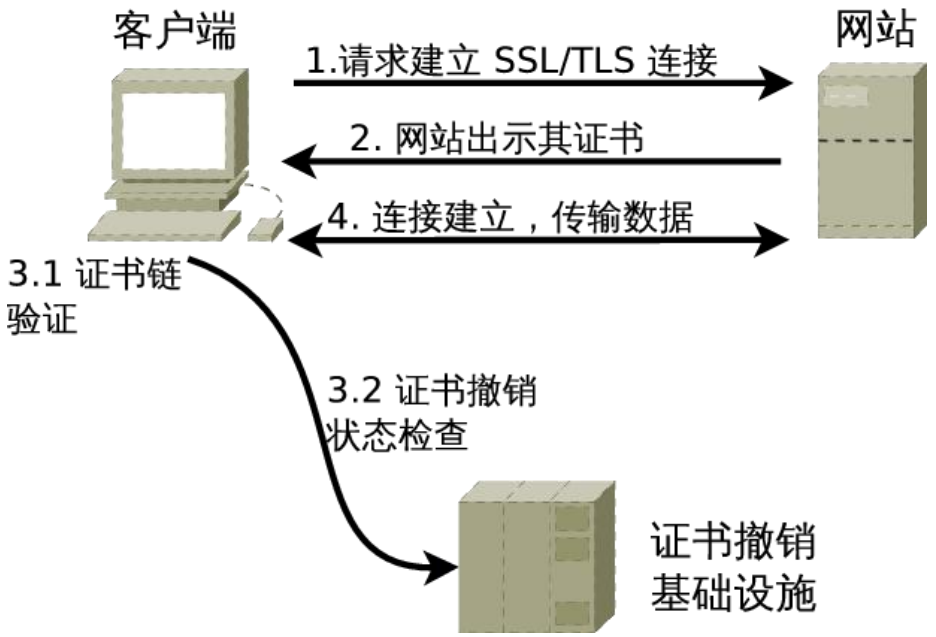
- 1881个CRL，涉及894个issuer（其中 1485 CRL 有撤销记录）
- 被撤销证书的条目数： 4,246,382





撤销机制的背景介绍

- 作用：在证书过期之前使其失效
  - 证书安全最后的防线，例如 Key Compromise
  - 近期案例：Heartbleed
- 撤销检查流程
- 四种工作机制
  - CRL
  - OCSP
  - OCSP Stapling
  - CRLset



Case study: self-signed CA of 12306

站车风采

北京西站

更多>>>

旅客服务质量调查问卷

最新动态

为保障您顺畅购票，请下载安装根证书。

- 关于2014年上半年京沪、京广高铁部分G字头动车组列车商务、特等、一... NEW! (2014-03-27)
- 关于2014年短途卧铺优惠有关事宜的公告 NEW! (2014-03-05)
- 铁路互联网购票身份核验须知 (2014-02-23)
- 沈阳铁路局关于五一期间加开管内临客的公告 (2014-04-20)
- 昆明铁路局关于五一期间加开管内临客的公告 (2014-04-23)
- 广铁集团公司关于2014年4月30日至5月3日临时加开部分列车的公告 (2014-04-22)
- 广铁集团公司关于"五一"期间临时加开部分旅客列车的公告 (2014-04-21)

更多>>>

新版售票 点击进入>>

网上购票用户注册

购 票

退 票

余 票 查 询

旅客列车时刻表查询

旅客列车正晚点查询

全文搜索: 请输入搜索条件 搜 索

网上购票常见问题 | 铁路常识 | 货运办理常见问题

- 在互联网购买了儿童票，如何在售票窗口换取纸质车票?
- 注册用户时，系统提示身份信息重复怎么办?
- 购买实名制车票后丢失了怎么办?
- 网上购票由于安全警告无法登录问题说明
- 我在网站购票时，扣款成功但购票不成功怎么办?
- 我在网站购票时不小心重复支付了，重复扣的票款没有及时到帐，怎么办?

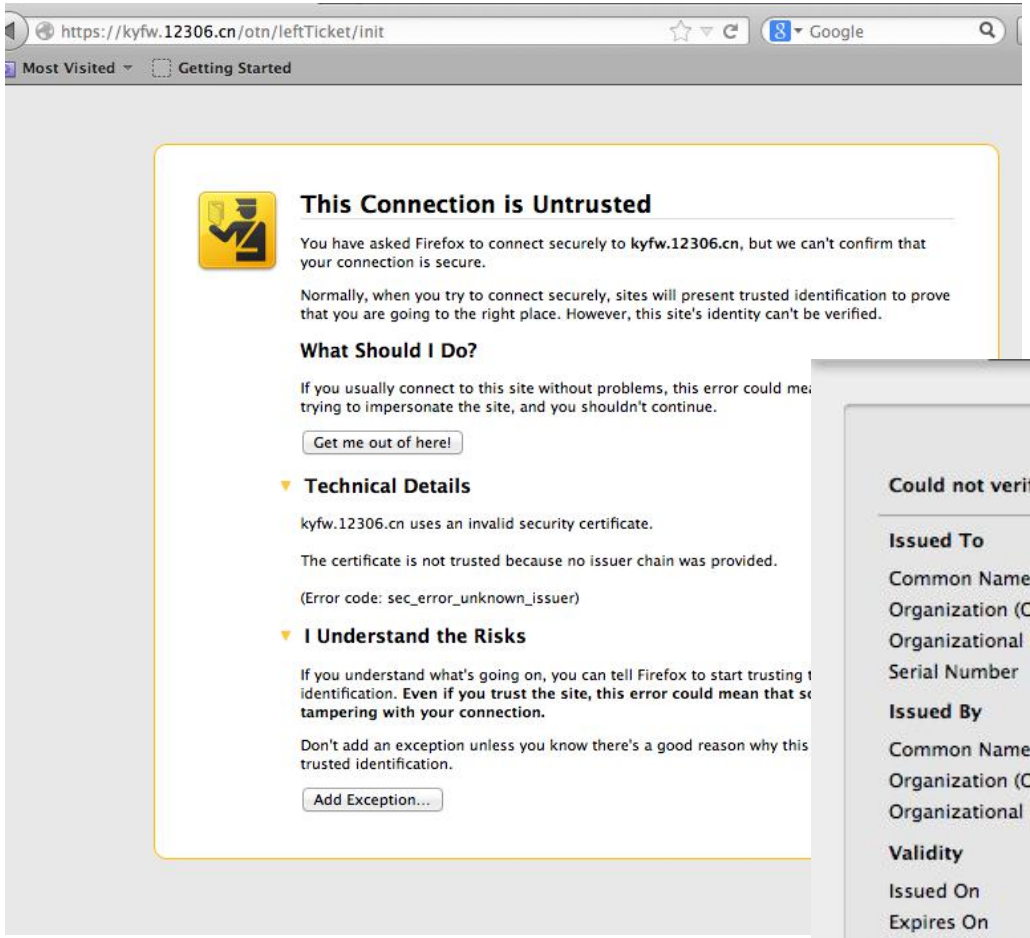
货运主要营业站受理服务电话

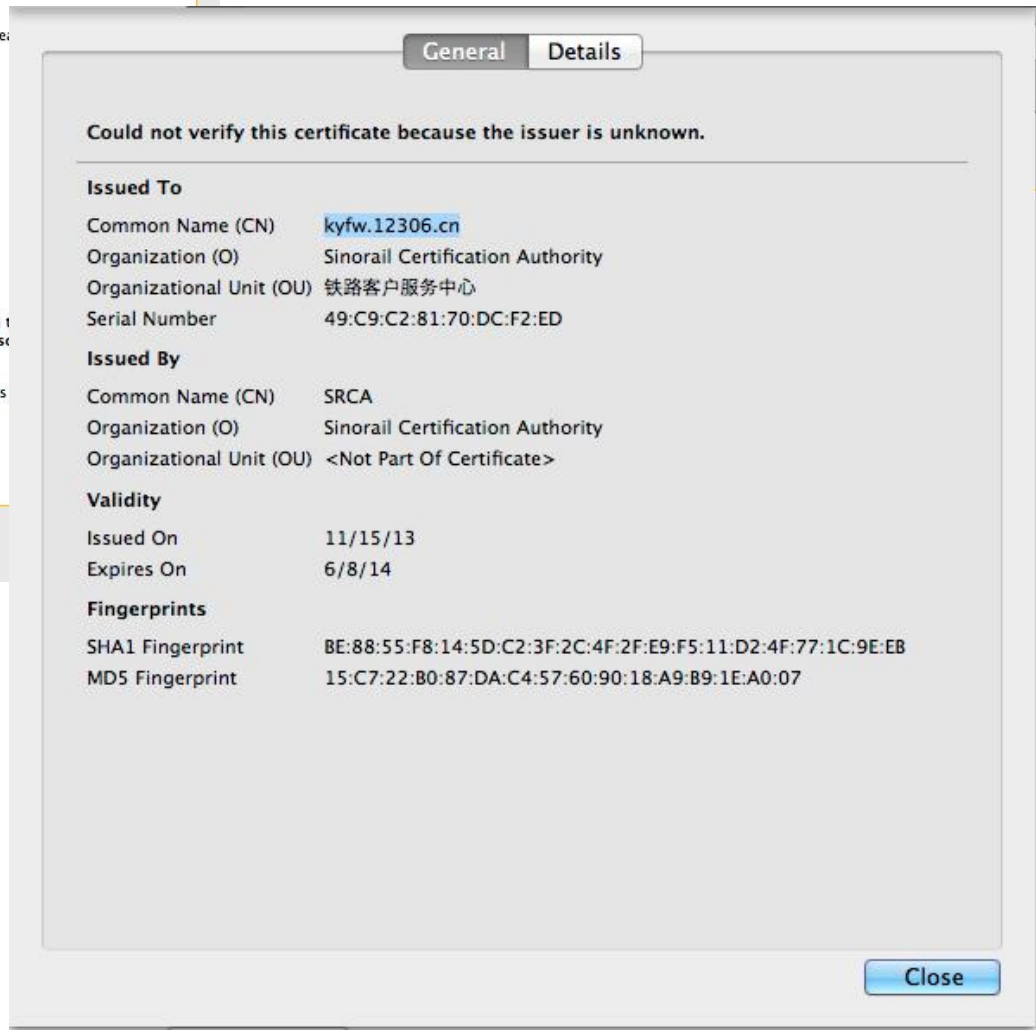
货运运费查询

货运业务咨询

相关链接

中央政府门户网站
外交部
发展改革委
教育部
科技部
国家民委


https://kyfw.12306.cn/otn/leftTicket/init
Google
Most Visited
Getting Started
This Connection is Untrusted
You have asked Firefox to connect securely to kyfw.12306.cn, but we can't confirm that your connection is secure.
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
What Should I Do?
If you usually connect to this site without problems, this error could mea
trying to impersonate the site, and you shouldn't continue.
Get me out of here!
Technical Details
kyfw.12306.cn uses an invalid security certificate.
The certificate is not trusted because no issuer chain was provided.
(Error code: sec_error_unknown_issuer)
I Understand the Risks
If you understand what's going on, you can tell Firefox to start trusting t
identification. Even if you trust the site, this error could mean that s
tampering with your connection.
Don't add an exception unless you know there's a good reason why this
trusted identification.
Add Exception...


General
Details
Could not verify this certificate because the issuer is unknown.
Issued To
Common Name (CN) kyfw.12306.cn
Organization (O) Sinorail Certification Authority
Organizational Unit (OU) 铁路客户服务中心
Serial Number 49:C9:C2:81:70:DC:F2:ED
Issued By
Common Name (CN) SRCA
Organization (O) Sinorail Certification Authority
Organizational Unit (OU) <Not Part Of Certificate>
Validity
Issued On 11/15/13
Expires On 6/8/14
Fingerprints
SHA1 Fingerprint BE:88:55:F8:14:5D:C2:3F:2C:4F:2F:E9:F5:11:D2:4F:77:1C:9E:EB
MD5 Fingerprint 15:C7:22:B0:87:DA:C4:57:60:90:18:A9:B9:1E:A0:07
Close

```
DuanHaixins-MacBook-Pro:12306 duanhx$ openssl x509 -in kyfw.12306.cn  -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            38:3b:70:e9:b6:44:1f:59
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C = CN, O = Sinorail Certification Authority, CN = SRCA
        Validity
            Not Before: May 26 01:44:36 2014 GMT
            Not After : May 25 01:44:36 2019 GMT
        Subject: C = CN, O = Sinorail Certification Authority, OU = \E9\93\81\E8\B7\AF\E5\AE\A2\E6\88\B7\E6
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:bc:0b:19:73:f9:5f:f8:2a:45:24:f1:84:f1:57:
                    1c:e2:8b:bc:69:da:06:4f:5a:eb:95:06:2c:10:ea:
                    2c:0b:f7:c8:ad:ef:95:8d:1a:26:02:51:ab:03:5f:
                    2d:ce:f3:06:3e:3e:d6:45:be:01:0a:92:91:ea:43:
                    55:3a:b9:e9:a2:1d:2b:6d:85:44:b5:c5:30:6c:53:
                    f4:ee:5c:5e:80:1d:cf:a8:76:e3:fa:cc:21:8a:71:
                    49:c7:44:09:2c:45:bf:01:19:28:33:04:0f:d7:dc:
                    1f:42:50:a9:d8:6b:d6:00:d8:40:48:61:c7:2b:cc:
                    88:7a:69:10:23:0c:76:ef:61
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:79:5E:B6:77:B7:E2:52:83:43:ED:C7:51:88:4C:63:85:2C:00:43:58
```

https://mail.tsinghua.edu.cn

mail.tsinghua.edu.cn

This site uses a weak security configuration (SHA-1 signatures), so your connection may not be private.

Details

Permissions | Connection

Chrome verified that GlobalSign Domain Validation CA - G2 issued this website's certificate. The server did not supply any Certificate Transparency information.

The certificate for this site expires in 2017 or later, and the certificate chain contains a certificate signed using SHA-1.

Certificate Information

Your connection to mail.tsinghua.edu.cn is encrypted using an obsolete cipher suite.

The connection uses TLS 1.2.

The connection is encrypted using AES_128_CBC, with HMAC-SHA1 for message authentication and RSA as the key exchange mechanism.

What do these mean?

大學 电子邮件系统（教工版）

学生版

2014年4月23日 星期三 | 首 页 | 客运服务 | 货运服务 | 行包服务 | 车站引导 | 铁路常识 | 站车风采 | 客户信箱

站车风采

北京西站

更多>>>

旅客服务质量调查问卷

最新动态

为保障您顺畅购票，请下载安装根证书。

- 关于2014年上半年京沪、京广铁路部分G字头动车组列车商务、特等、一... NEW! (2014-03-27)
- 关于2014年短途卧铺优惠有关事宜的公告 NEW! (2014-03-05)
- 铁路互联网购票身份核验须知 (2014-02-23)
- 沈阳铁路局关于五一期间加开管内临客的公告 (2014-04-20)
- 昆明铁路局关于五一期间加开管内临客的公告 (2014-04-23)
- 广铁集团公司关于2014年4月30日至5月3日临时加开部分列车的公告 (2014-04-22)
- 广铁集团公司关于"五一"期间临时加开部分旅客列车的公告 (2014-04-21)

更多>>>

新版售票 点击进入>>

网上购票用户注册

购 票

退 票

余 票 查 询

旅客列车时刻表查询

旅客列车正晚点查询

全文搜索: 请输入搜索条件 搜 索

网上购票常见问题 | 铁路常识 | 货运办理常见问题

- 在互联网购买了儿童票，如何在售票窗口换取纸质车票?
- 注册用户时，系统提示身份信息重复怎么办?
- 购买实名制车票后丢失了怎么办?
- 网上购票由于安全警告无法登录问题说明
- 我在网站购票时，扣款成功但购票不成功怎么办?
- 我在网站购票时不小心重复支付了，重复扣的票款没有及时到帐，怎么办?

货运主要营业站受理服务电话

货运运费查询

货运业务咨询

相关链接

中央政府门户网站
外交部
发展改革委
教育部
科技部
国家民委

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            6f:26:6b:e7:f8:ca:1f:a4
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C = CN, O = Sinorail Certification Authority, CN = SRCA
        Validity
            Not Before: May 25 06:56:00 2009 GMT
            Not After : May 20 06:56:00 2029 GMT
        Subject: C = CN, O = Sinorail Certification Authority, CN = SRCA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:c
                    6f:c
                    4f:1
                    a3:e
                    b7:c
                    d3:2
                    0f:c
                    c7:5
                    99:3
                Exponent:
        X509v3 extensions:
            X509v3 Authority Key Identif
                keyid:79:5E:B6:77:B7:E2:                    :68:4C:63:85:2C:00:43:58

            X509v3 Basic Constraints:
                CA:TRUE
            X509v3 CRL Distribution Po

                Full Name:
                  URI:http://192.168.9.149/crl1.crl

            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement, Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                79:5E:B6:77:B7:E2:52:83:43:ED:C7:51:88:4C:63:85:2C:00:43:58
    Signature Algorithm: sha1WithRSAEncryption
```

X509v3 CRL Distribution Points:
URI:http://192.168.9.149/crl1.crl


子
中国特色社会主义的样
却不得不和我一同建设
我就是喜欢你看不惯我，

中美银行网站CA和HTTPS测量

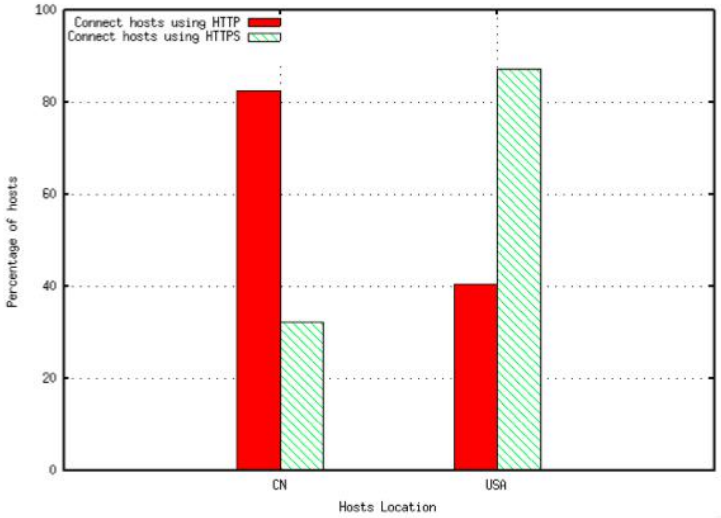


图1 中美银行网站HTTPS和HTTP支持率

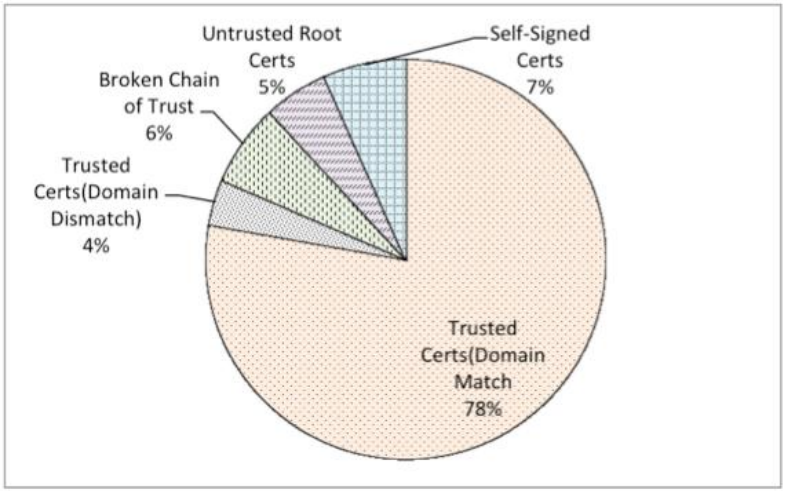


图 3 中国银行网站证书链验证结果统计

表 2 CA分布统计表

CA名称	中国	美国
VeriSign	67.26%	64.77%
Entrust	7.08%	11.36%
UserTrust	4.42%	0.00%
CFCA	4.42%	0.00%
Equifax	3.54%	2.27%
BeijingTopsec	1.77%	0.00%
StartCom	0.88%	0.00%
ABC	0.88%	0.00%
GeoTrust	0.00%	5.68%
AddTrust	0.00%	7.95%
Thawte	0.00%	2.27%
GTE	0.00%	2.27%
GoDaddy	0.00%	1.14%
Valicert	0.00%	1.14%
DigiCert	0.00%	1.14%
Self-Sign	9.73%	0.00%

网络银行HTTPS部署问题

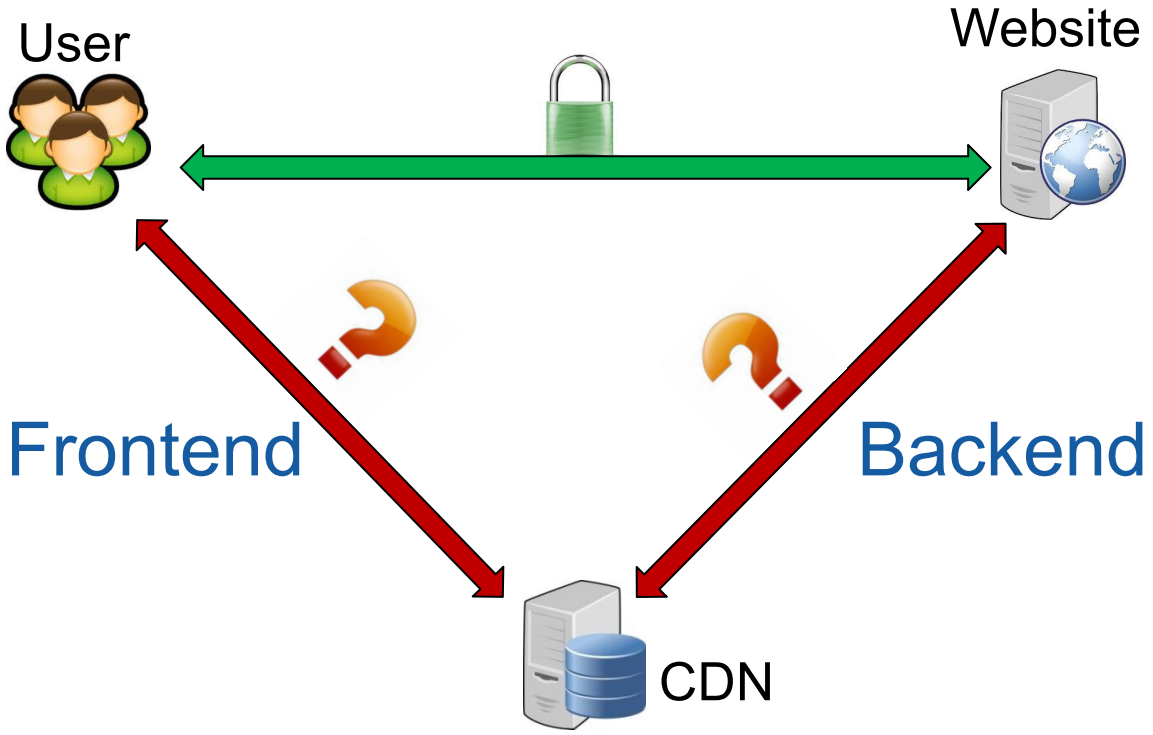
- 对中国300多家网上银行和100家美国银行网站的HTTPS及证书进行了测量和对比分析
- 一些重要的结果：
  - HTTPS支持率：中国32%, 美国82%
  - 使用可信证书：中国78%， 美国100%
  - 证书中增强验证EV证书: 中国14%, 美国51%
  - 使用被破解的MD5算法：中国2%, 美国0%
  - 秘钥长度：中国的短秘钥(512,1024)比例高于美国

Outline

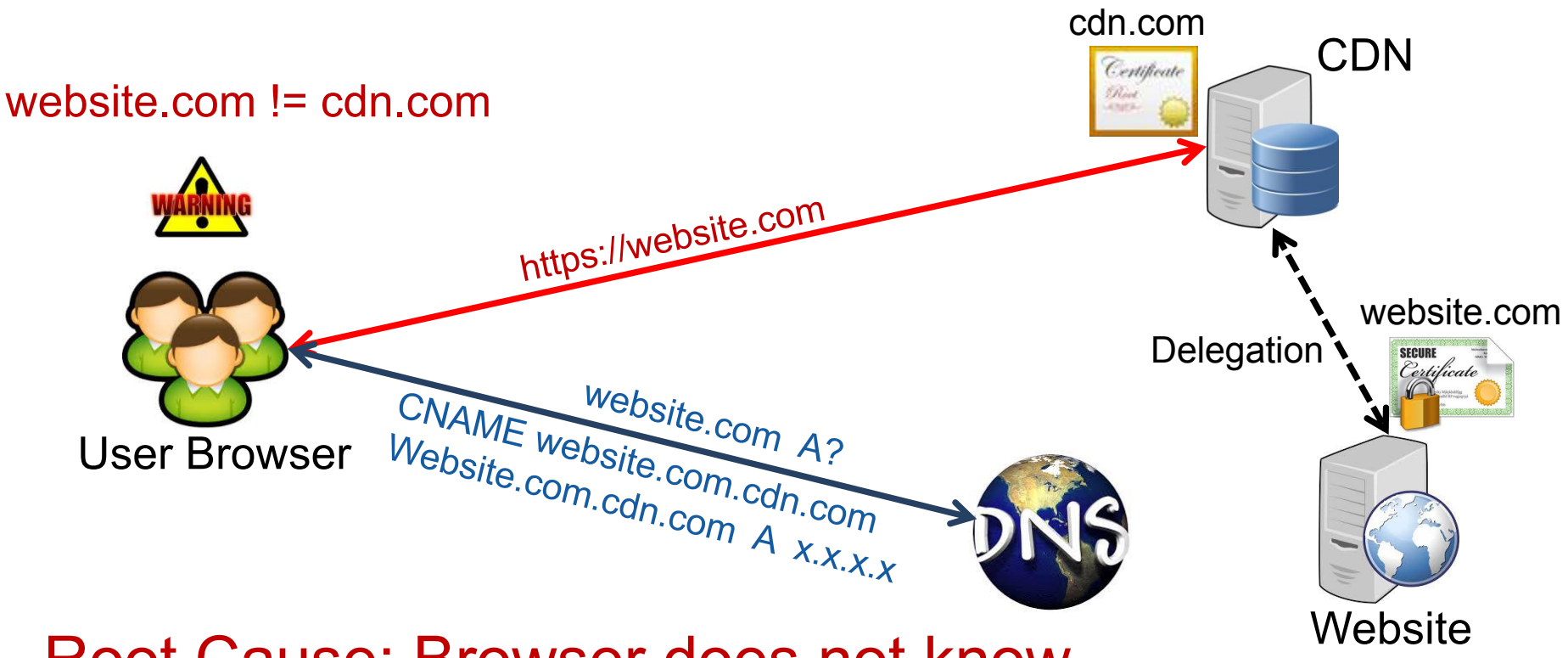
- Why encryption?
- How CA works
- Problem of CA
- CDN problems
- Solutions

When HTTPS Meets CDN

- From 2 parties to 3 parties
- Break into Frontend and Backend



Broken HTTPS Authentication
in DNS Based Request Routing



Root Cause: Browser does not know the delegation from website to CDN!

Survey on CDNs and Websites

- 20 popular CDN providers

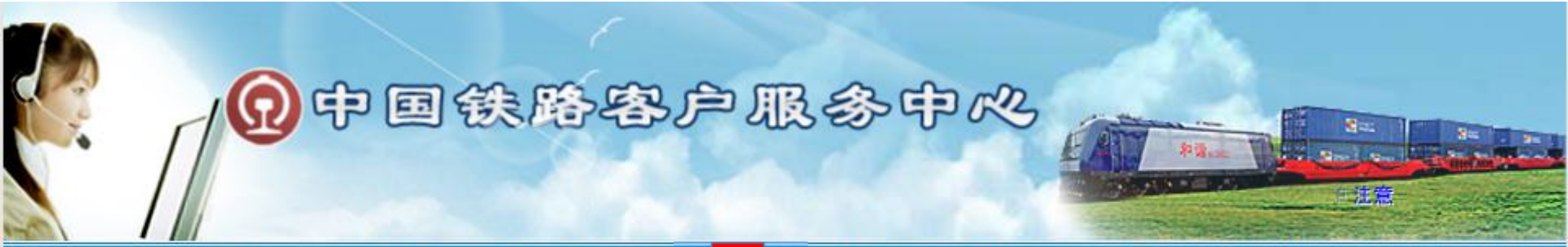
Support DNS Routing	Support HTTPS
20	19

- Alexa Top 1M websites
  - 10,721 use CDN and HTTPS

Invalid Certificate		Valid Certificate	
Status 200	Other	Custom Cert	Shared Cert
15%	54%	20%	11%
69%		31%	

有可能原始网站没有启用HTTPS

它们如何解决无效证书问题的呢？



2014年4月23日 星期三 | 首 页 | 客运服务 | 货运 | 行包服务 | 车站引导 | 铁路常识 | 站车风采 | 客户信箱

站车风采

北京西站

最新动态

为保障您顺畅购票，请下载安装根证书。

- 关于2014年上半年京沪、京广高铁部分G字头动车组列车商务、特等、一... NEW! (2014-03-27)
- 关于2014年短途卧铺优惠有关事宜的公告 NEW! (2014-03-05)
- 铁路互联网购票身份核验须知 (2014-02-23)
- 沈阳铁路局关于五一期间加开管内临客的公告 (2014-04-20)
- 昆明铁路局关于五一期间加开管内临客的公告 (2014-04-23)
- 广铁集团公司关于2014年4月30日至5月3日临时加开部分列车的公告 (2014-04-22)

https://kyfw.12306.cn/otn/leftTicket/init

旅客服

新版

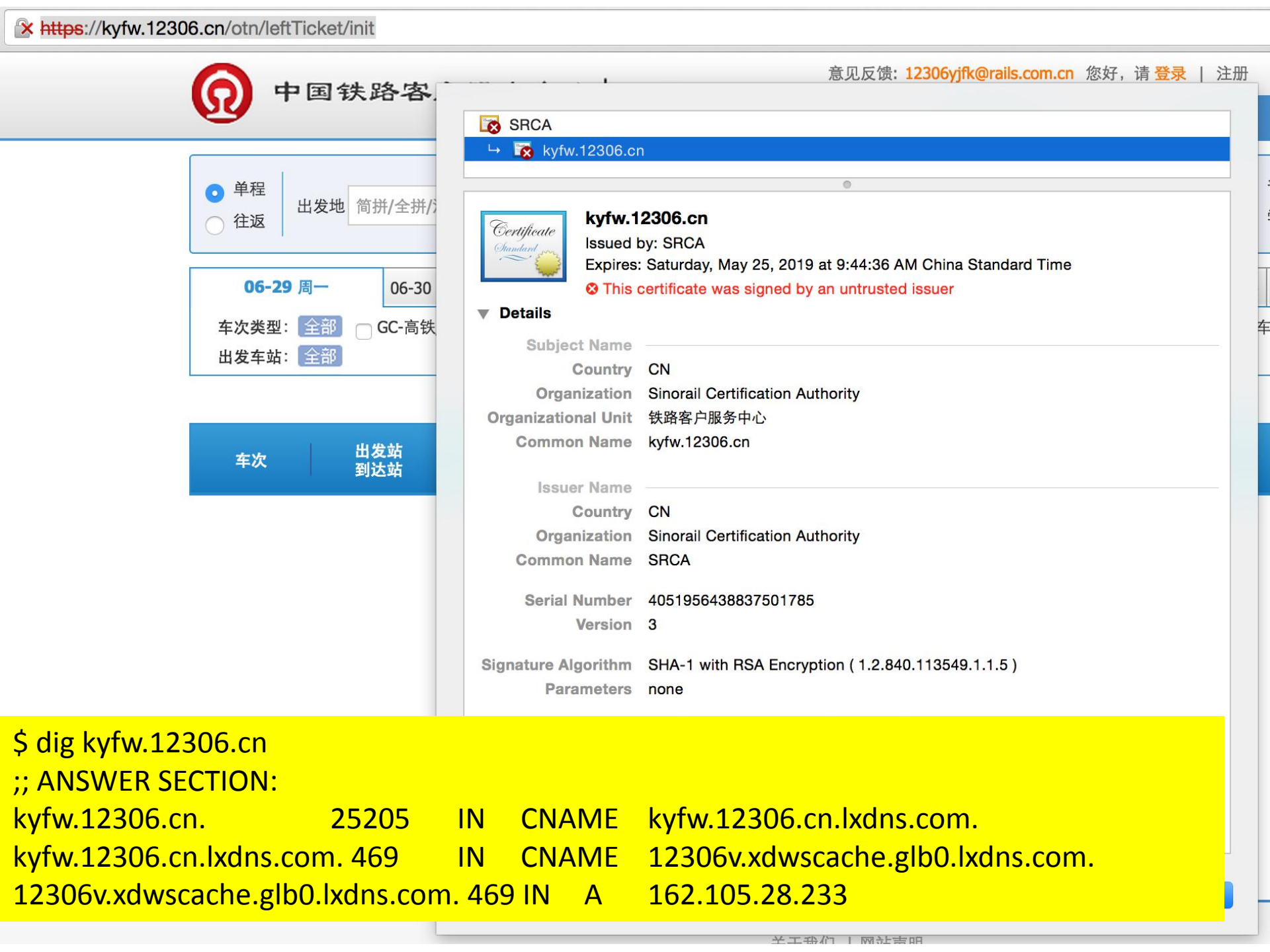
The site's security certificate is not trusted!

You attempted to reach **kyfw.12306.cn**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

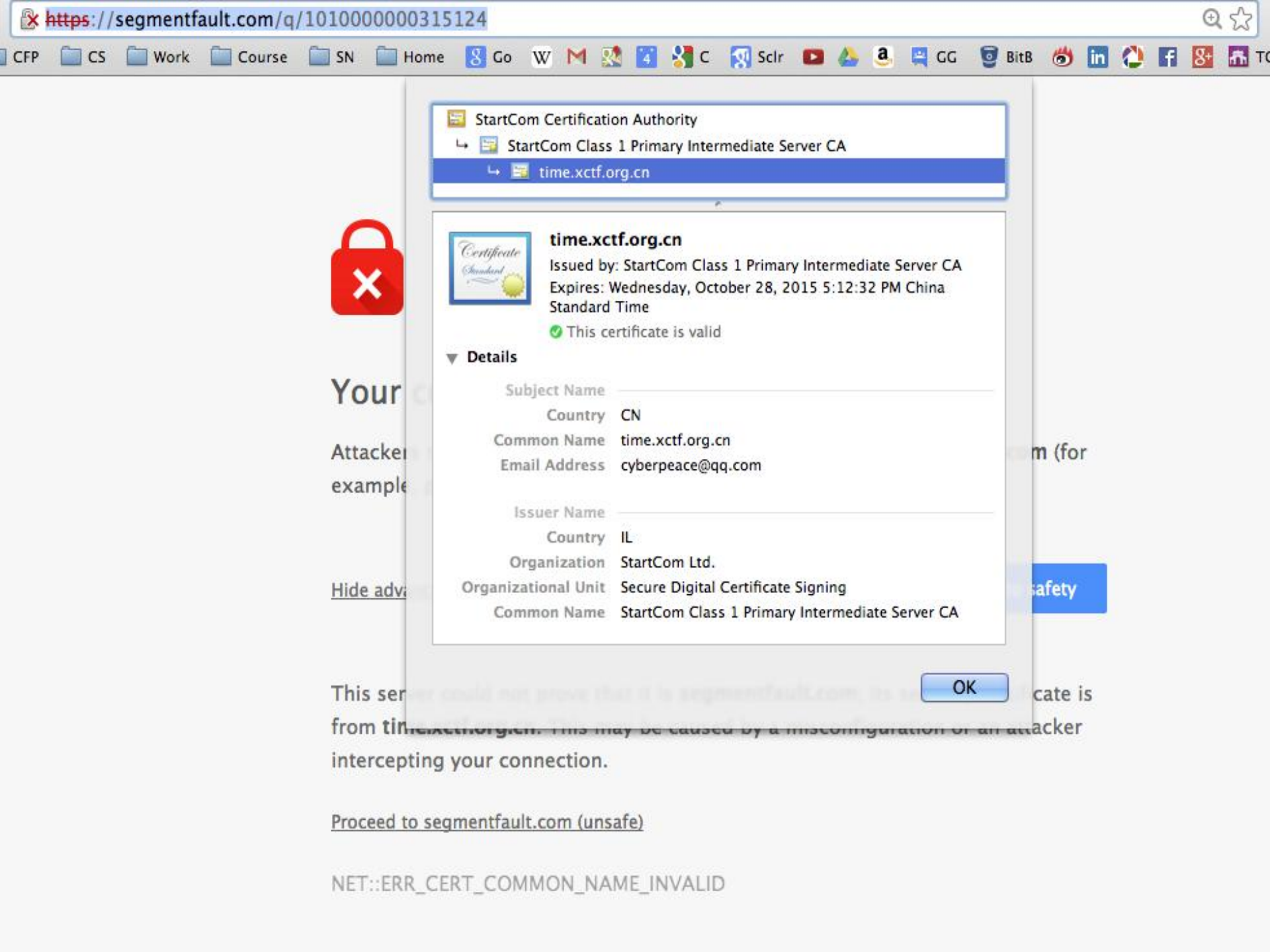
You should not proceed, **especially** if you have never seen this warning before for this site.

Proceed anyway | Back to safety

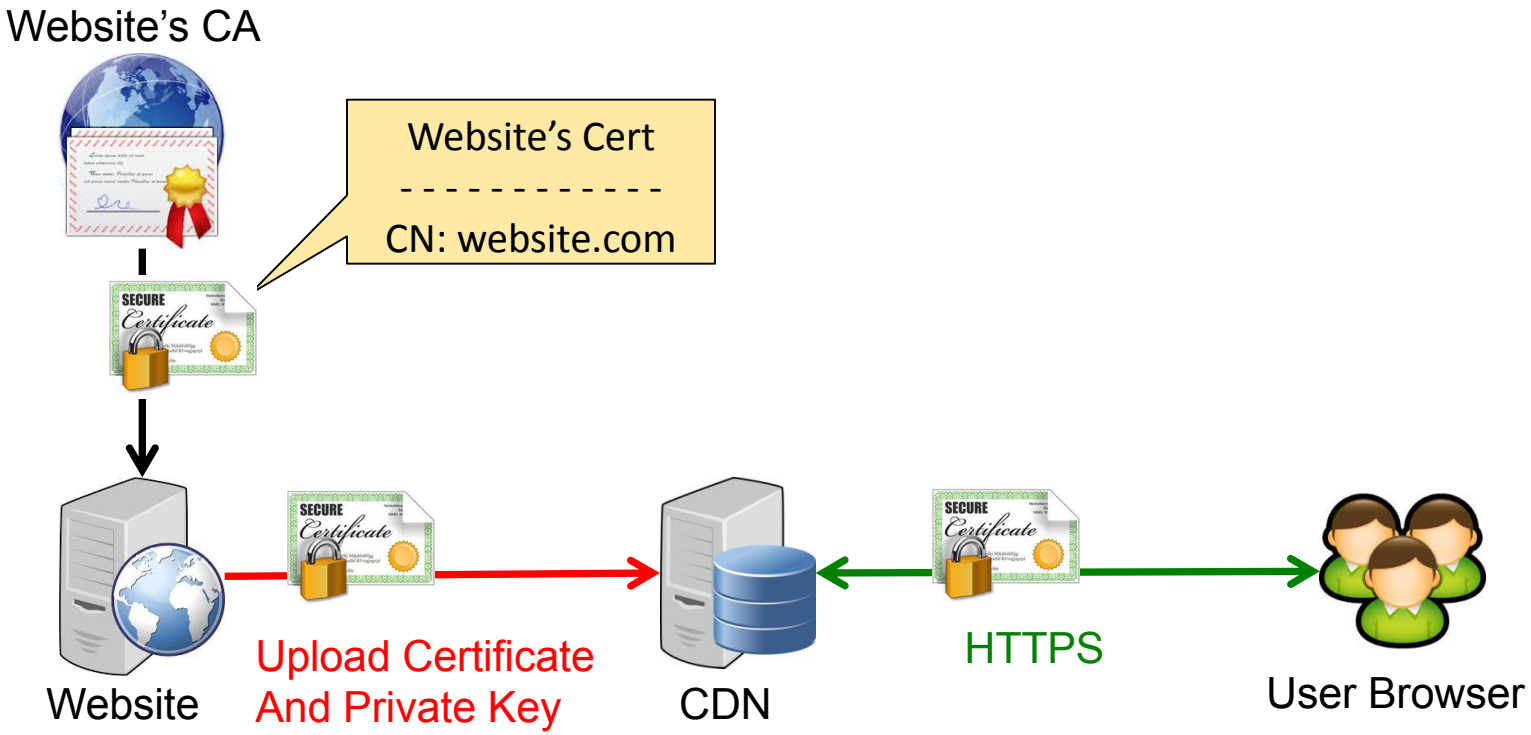
▶ Help me understand




```
$ dig kyfw.12306.cn
;; ANSWER SECTION:
kyfw.12306.cn.              25205   IN  CNAME   kyfw.12306.cn.lxdns.com.
kyfw.12306.cn.lxdns.com.    469     IN  CNAME   12306v.xdwscache.glb0.lxdns.com.
12306v.xdwscache.glb0.lxdns.com. 469 IN  A     162.105.28.233
```


https://segmentfault.com/q/1010000000315124
CFP
CS
Work
Course
SN
Home
Go
C
Sclr
GG
BitB
StartCom Certification Authority
StartCom Class 1 Primary Intermediate Server CA
time.xctf.org.cn
time.xctf.org.cn
Issued by: StartCom Class 1 Primary Intermediate Server CA
Expires: Wednesday, October 28, 2015 5:12:32 PM China Standard Time
This certificate is valid
Details
Subject Name
Country CN
Common Name time.xctf.org.cn
Email Address cyberpeace@qq.com
Issuer Name
Country IL
Organization StartCom Ltd.
Organizational Unit Secure Digital Certificate Signing
Common Name StartCom Class 1 Primary Intermediate Server CA
OK
Your
Attacker
example
Hide adv
This ser
from tim
intercepting your connection.
Proceed to segmentfault.com (unsafe)
NET::ERR_CERT_COMMON_NAME_INVALID

Custom Certificate (Type I)



- Have to share private key
- Heavy key management overhead

Custom Certificate (Type II)

This certificate has been verified for the following usages:

SSL Server Certificate

Issued To

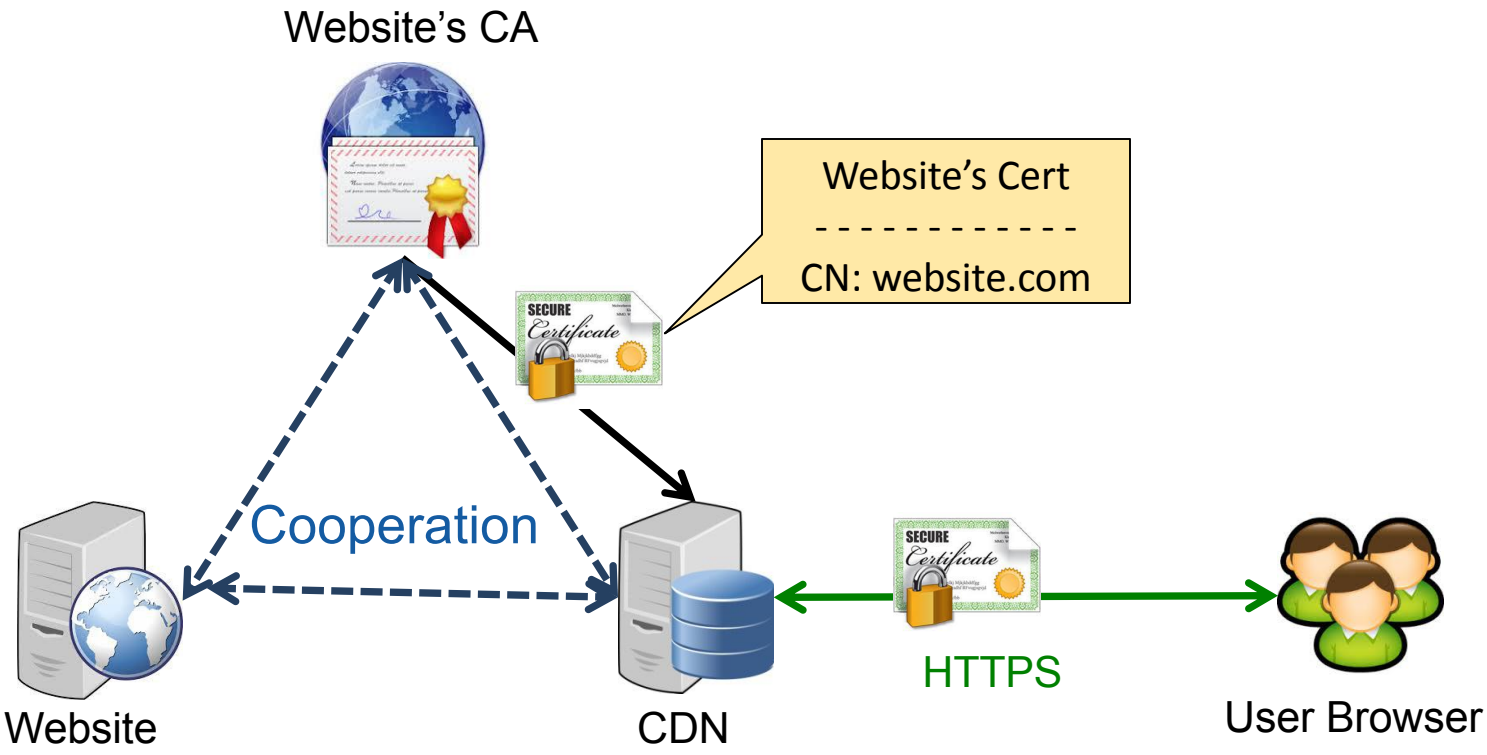
Common Name (CN)	www.apple.com
Organization (O)	Apple Inc.
Organizational Unit (OU)	Internet Services for Akamai
Serial Number	52:C3:FD:89:F2:C5:37:84:50:FE:53:AC:1A:74:79:74

Issued By

Common Name (CN)	Symantec Class 3 EV SSL CA - G3
Organization (O)	Symantec Corporation
Organizational Unit (OU)	Symantec Trust Network

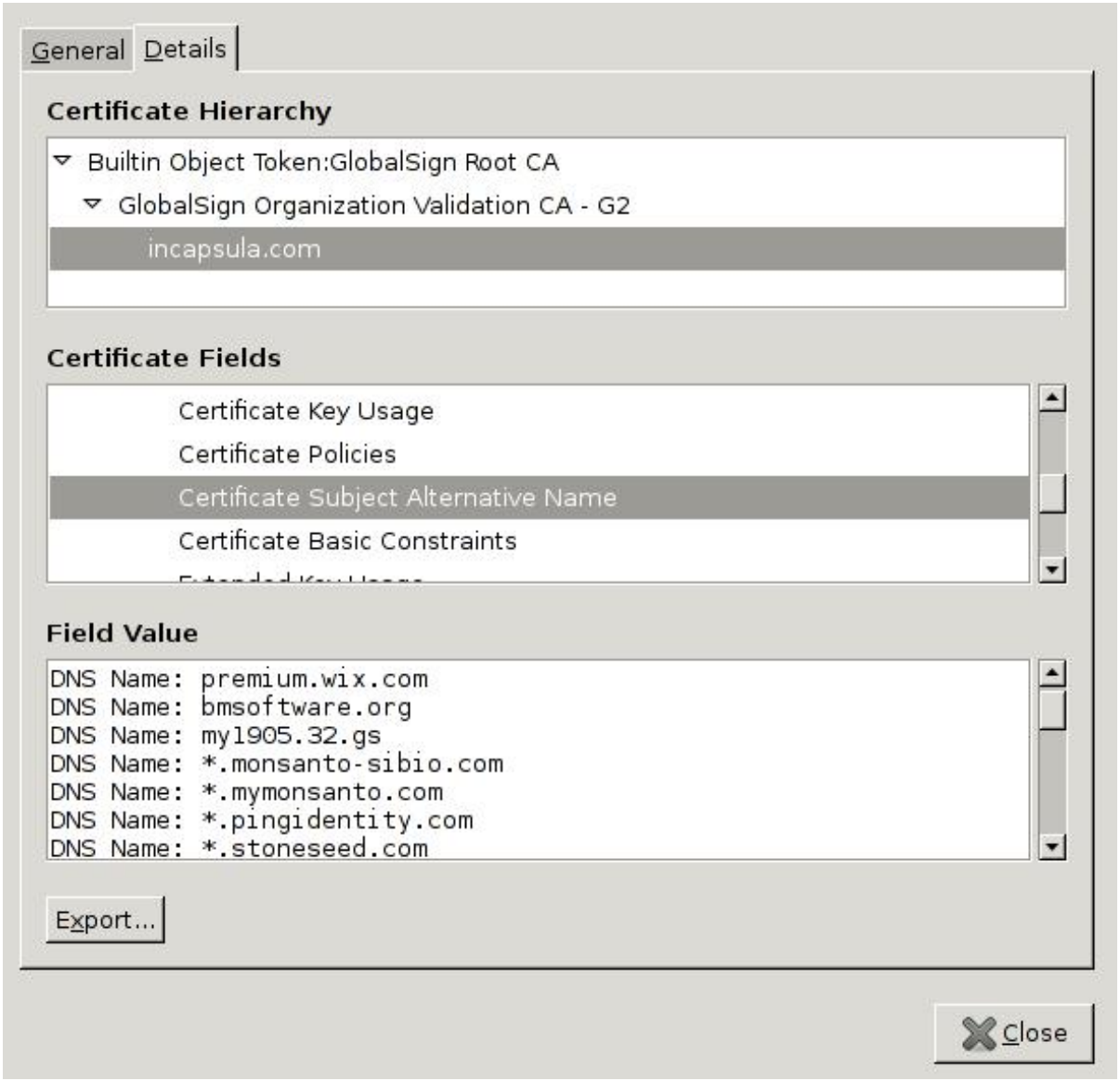
Custom Certificate (Type II)

Not covered in the paper

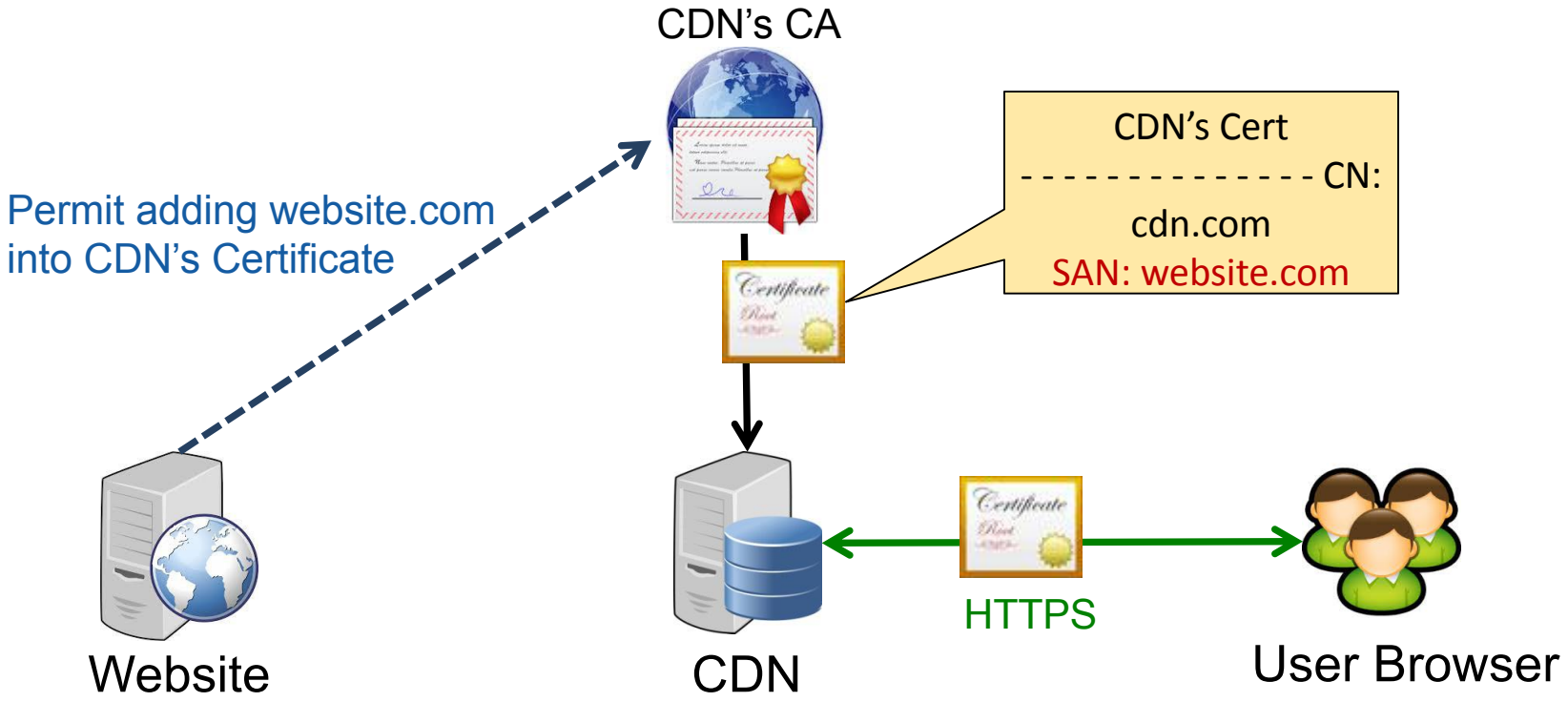


- Heavy key management overhead
- Inefficient issuance and revocation

Shared Certificate



Shared Certificate



- Improper security indicator (e.g. website has EV but CDN has DV/OV)
- Website can not revoke the certificate

Case Study on Shared Certificate

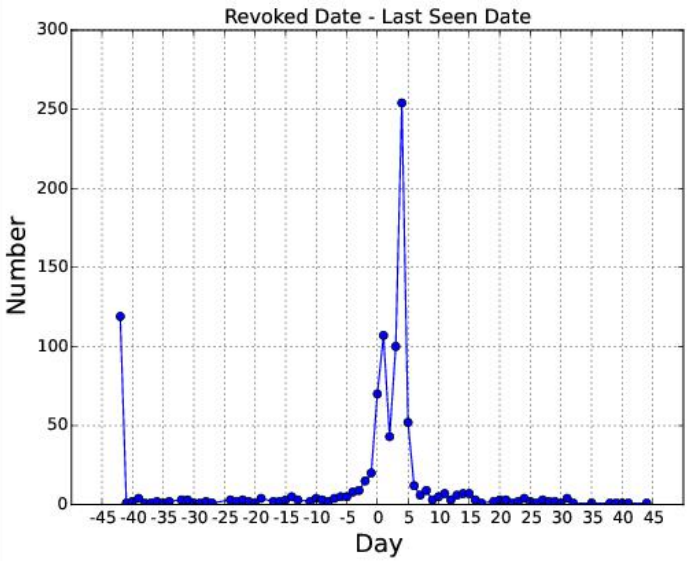
- CDN: Incapsula (CA: GlobalSign)
  - Issuance: Email confirmation from CA
  - Revocation
    - Incapsula removed our website domain name in a new shared certificate
    - But our stale certificate was not revoked by CA
    - Contacted GlobalSign, but no response
- Incapsula said they would work on this problem with their CAs

Revocation Problem of Shared Certificate

- 1198 websites using shared certificate
- Certificate update, CRL and OCSP
- Last for 3 months
- 1865 certificate updates from 5 CDNs, but none was revoked
- Also discovered by Web PKI (NDSS 2014)
  - "this form of operation should be more strongly regulated"

证书更换与撤销的信息统计

- Alexa Top 1M 网站，7个星期的测量
  - 发生 67,290 次证书更换
  - 983个证书被撤销
    - 时间间隔在 0~5 天
    - 251 个证书被撤销却依然被使用



  - 约 30% 的证书撤销与更换只更改了密钥，其他信息不变
  - 73% 的证书更换后没有被撤销
    - 绝大部分是 CDN 共享证书

In WHAT, we TRUST ?

Q & A

duanhx@tsinghua.edu.cn