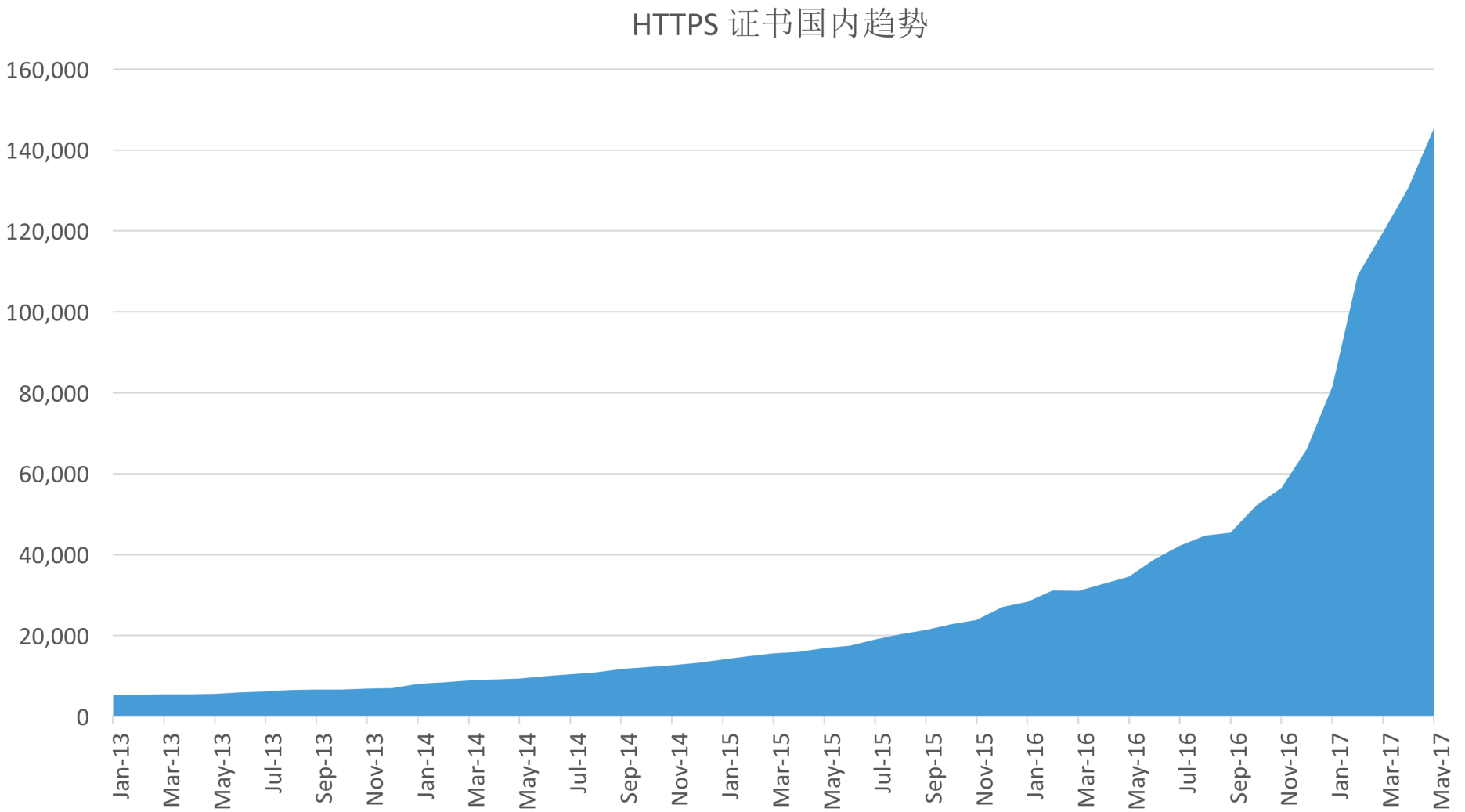
亞洲誠信® TRUSTASIA

HTTPS 最佳安全实践

亚洲诚信 余宁

HTTPS 国内发展趋势

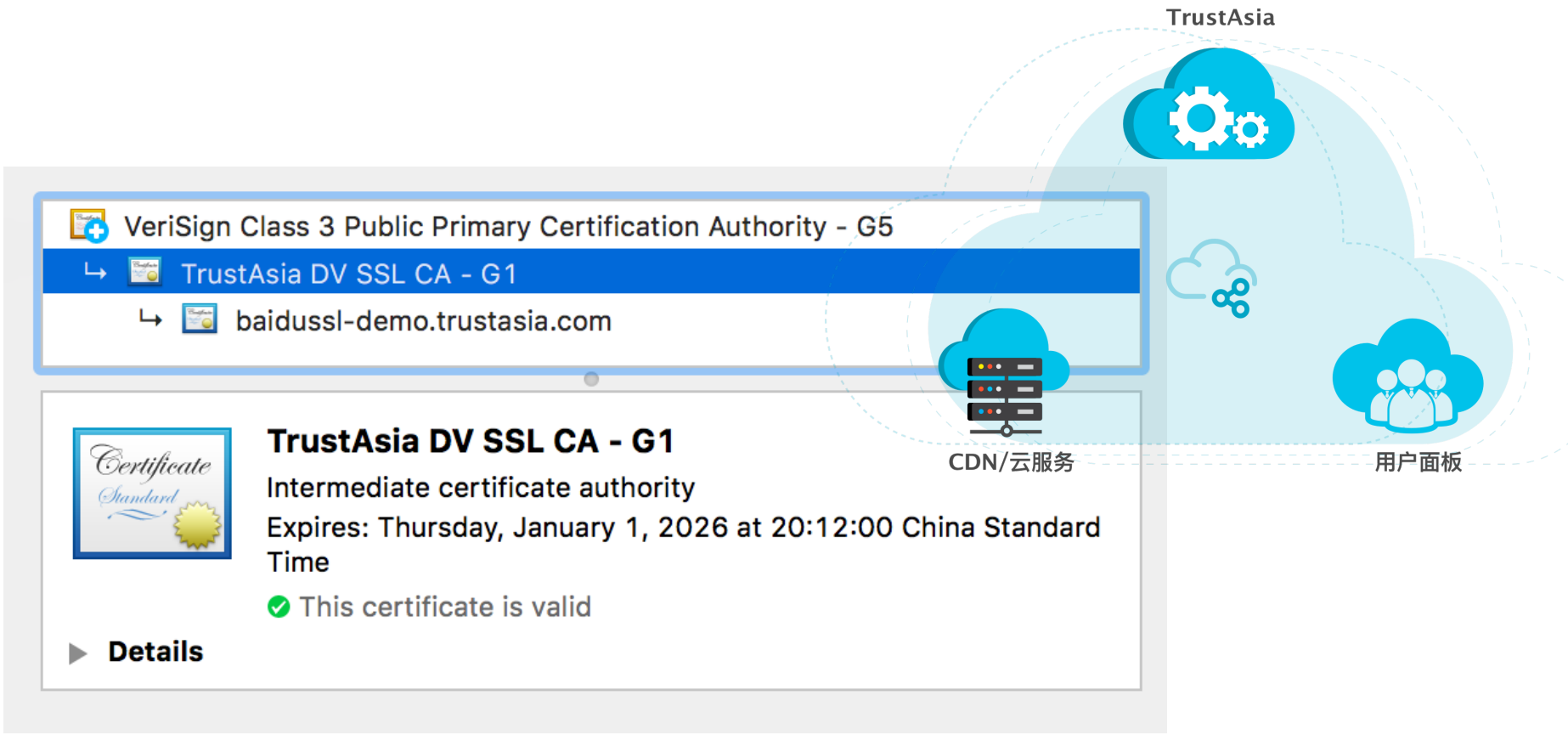


HTTPS 行业动态

- 2014~2015 搜索引擎优先收录HTTPS网站（Google，Baidu）
- 2015 国内大型互联网公司陆续实现全站HTTPS加密（Baidu，Alibaba）
- 2016 Apple 强制实施ATS标准
- 2016 微信小程序要求后台通信必须用HTTPS
- 2016 美国、英国政府机构网站实现全站HTTPS
- 2016 国家网络安全法 规定网络运营者需要保护其用户信息的安全，并明确了相关法律责任
- 2017年 Chrome、Firefox 将标示HTTP站点不安全

- HTTP/2 的主流实现都要求使用HTTPS
- TLS1.3 即将发布.使HTTPS更快更安全

亚洲诚信 HTTPS加密无处不在



加密无处不在合作伙伴


Symantec


腾讯云


西部数码
www.west.cn


新浪云
Sina Cloud


GeoTrust


百度云


网宿科技


七牛云
QINIU


thawte


HUAWEI
华为企业云


又拍云


SANGFOR
深信服科技


亞洲誠信®
TRUSTASIA


UCLOUD


百度云加速
su.baidu.com


plesk

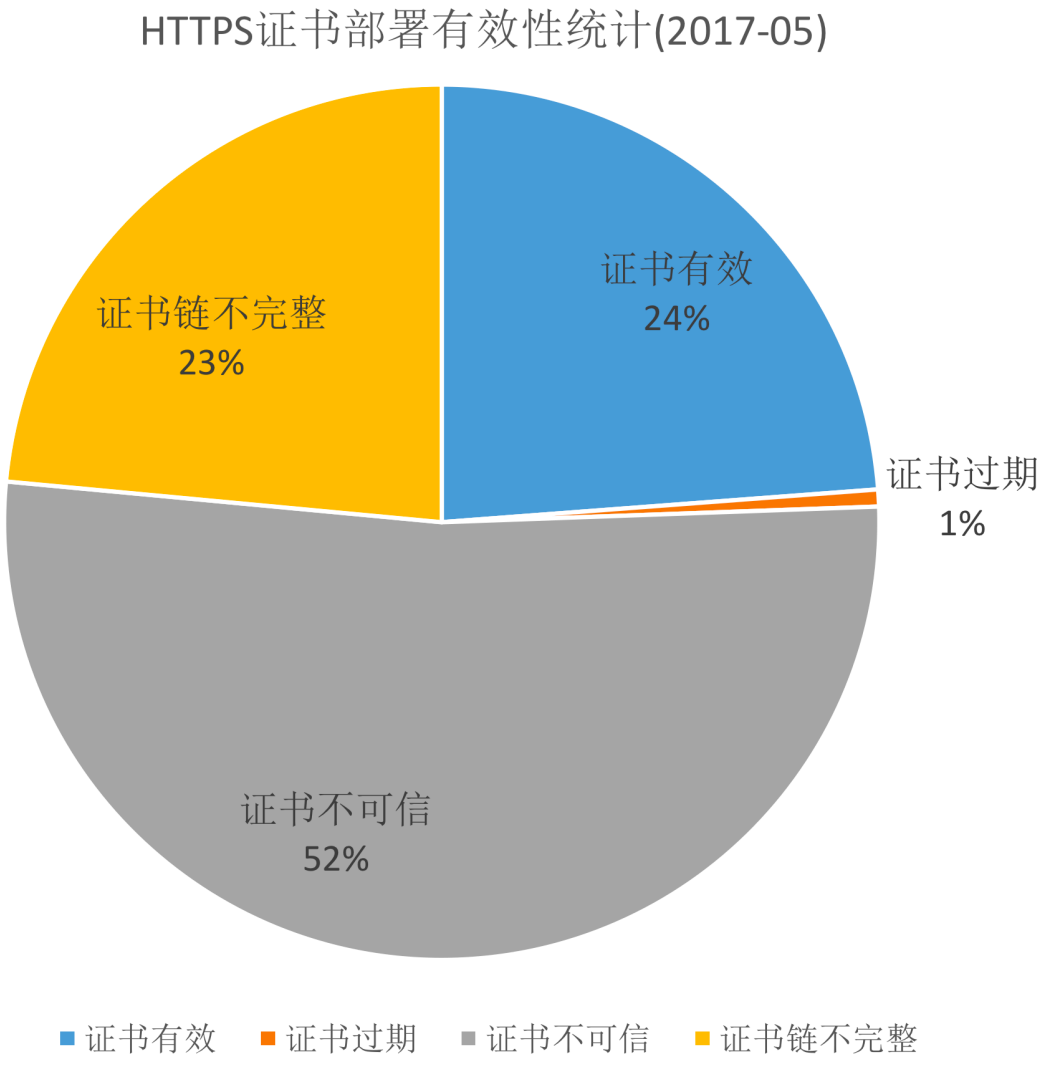

CFCA


青云 QING CLOUD

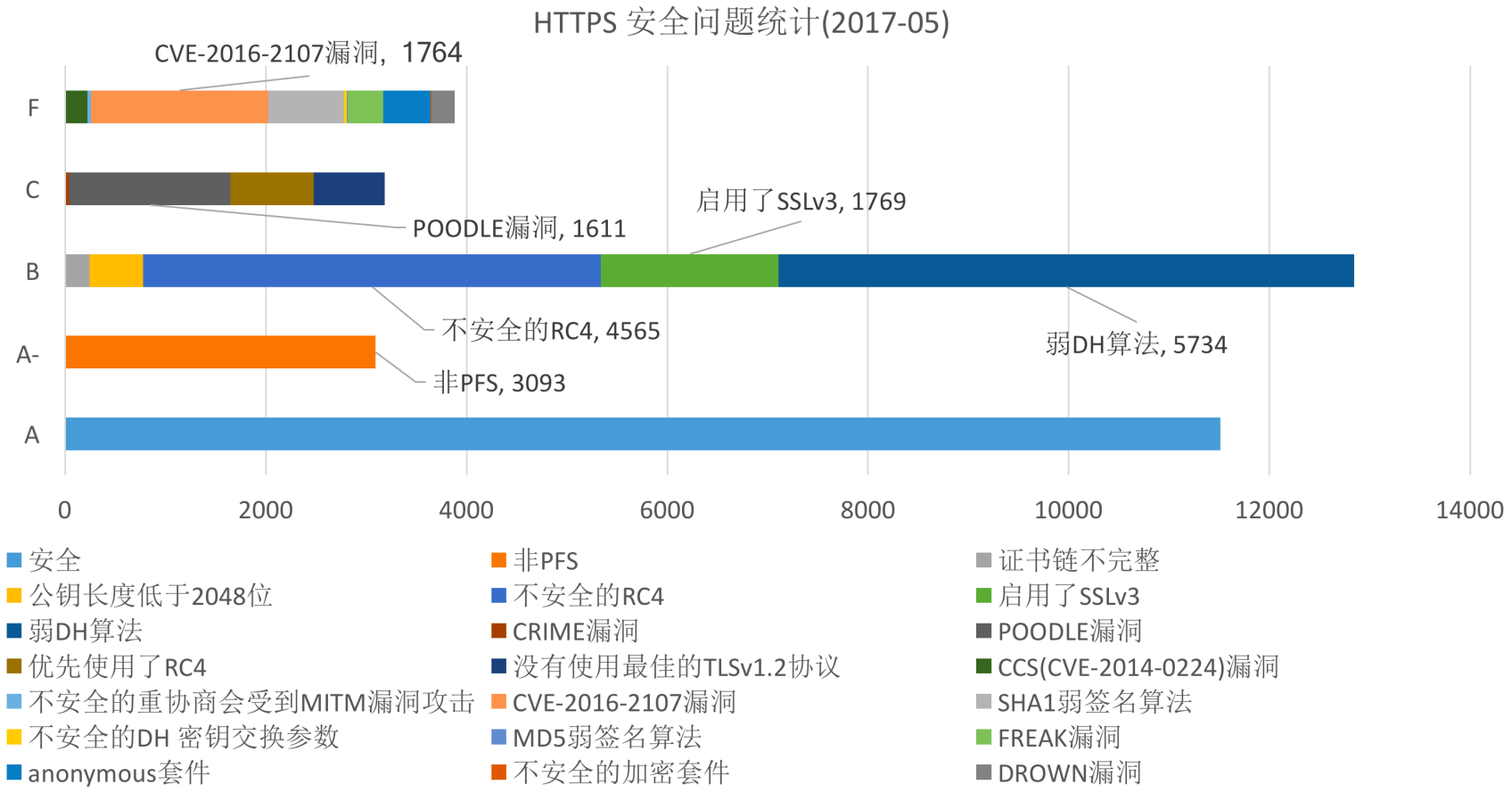

浪潮云


网易蜂巢

HTTPS 安全现状


HTTPS证书部署有效性统计(2017-05)
证书有效
24%
证书过期
1%
证书不可信
52%
证书链不完整
23%
证书有效
证书过期
证书不可信
证书链不完整

HTTPS 安全现状


HTTPS 安全问题统计(2017-05)
CVE-2016-2107漏洞, 1764
POODLE漏洞, 1611
启用了SSLv3, 1769
不安全的RC4, 4565
弱DH算法, 5734
非PFS, 3093
F
C
B
A-
A
0
2000
4000
6000
8000
10000
12000
14000
安全
非PFS
证书链不完整
公钥长度低于2048位
不安全的RC4
启用了SSLv3
弱DH算法
CRIME漏洞
POODLE漏洞
优先使用了RC4
没有使用最佳的TLSv1.2协议
CCS(CVE-2014-0224)漏洞
不安全的重协商会受到MITM漏洞攻击
CVE-2016-2107漏洞
SHA1弱签名算法
不安全的DH 密钥交换参数
MD5弱签名算法
FREAK漏洞
anonymous套件
不安全的加密套件
DROWN漏洞

如何让HTTPS更安全---证书选择

- 证书品牌

  兼容性，技术背景，口碑，占有率

- 审核类型

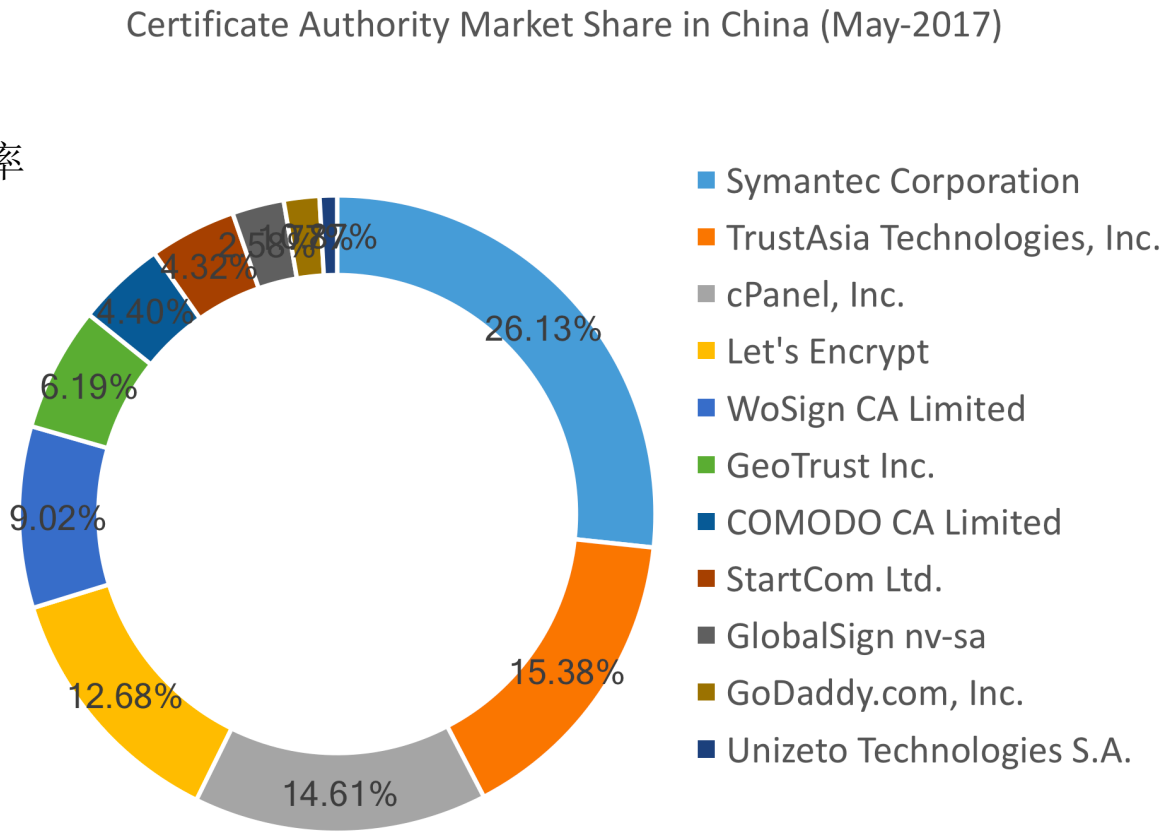
  EV,OV,DV

- 证书类型

  单域名，多域名，通配符

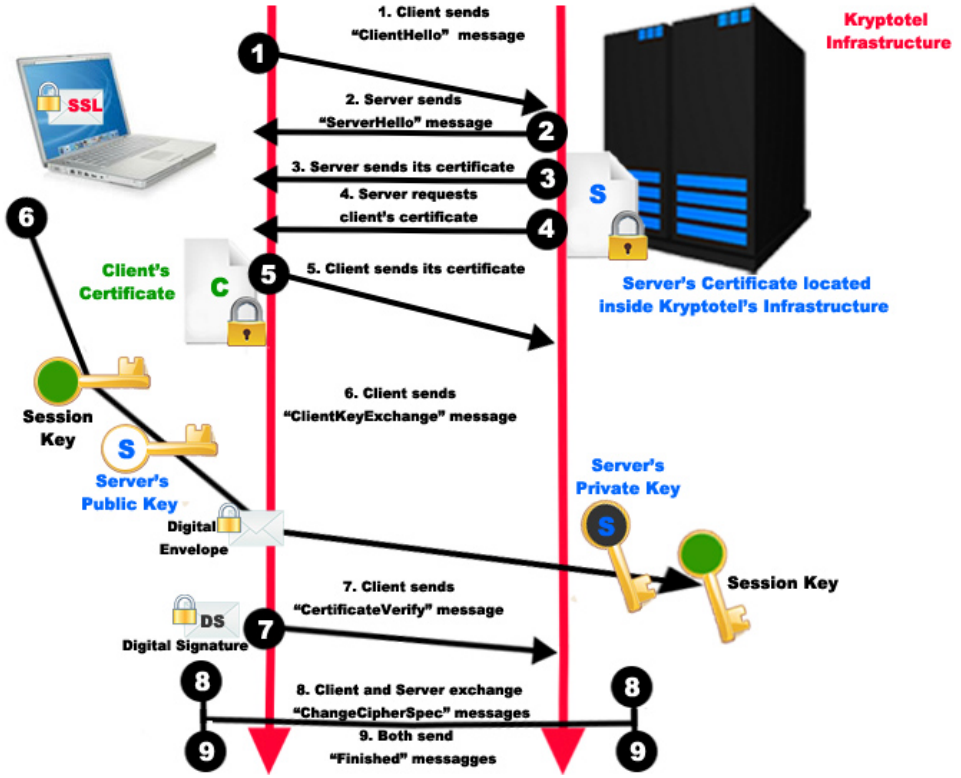
- 证书算法

  RSA，ECC



如何让HTTPS更安全---优化配置

- 证书链
  完善证书链，提升兼容性
- 协议
  启用安全协议版本 TLS1.2
  弃用不安全协议SSL3.0 ， SSL2.0
  ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
- 套件
  ECDHE,SHA256,AES256,GCM,CBC
  DH,MD5,RC4, 3DES
  ssl_ciphers ECDSA:ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL:!MD5:!ADH:!DH:!RC4;
- 会话恢复
  Session ID
  Session Ticker



如何让HTTPS更安全---漏洞修复

- Heartbleed (CVE-2014-0160)
- DROWN(CVE-2016-0800)
- CCS(CVE-2014-0224)
- Poodle (CVE-2014-3566)
- FREAK(CVE-2015-0204)
- CRIME(CVE-2012-4929)
- Openssl Padding Oracle (CVE-2016-2107)
- BEAST(CVE-2011-3389)

如何让HTTPS更安全---安全加固

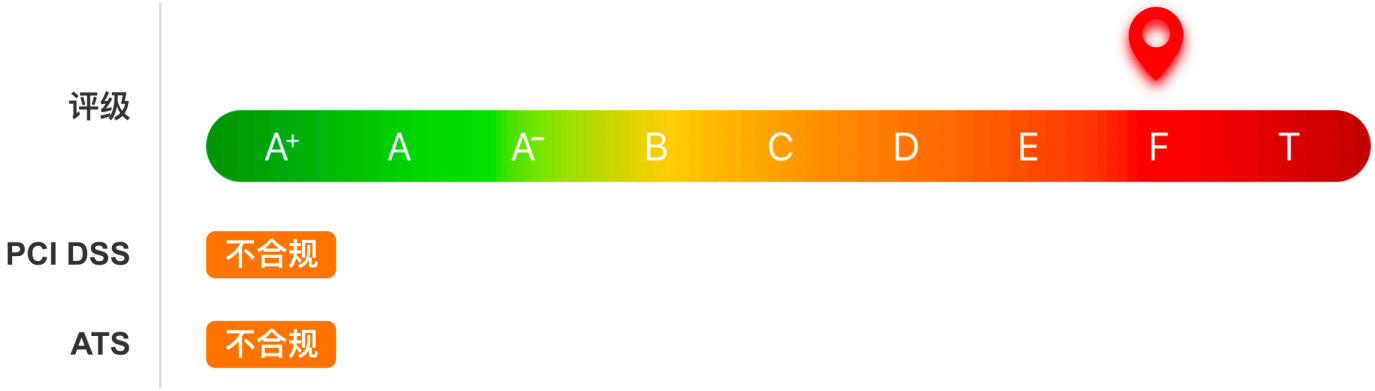
- **HSTS** (HTTP Strict Transport Security)
  浏览器实现HTTPS强制跳转，减少会话劫持风险
  Strict-Transport-Security: max-age=31536000; includeSubDomains
- **HPKP** (HTTP Public Key Pinning)
  指定浏览器信任的公钥，防止CA误发证书而导致中间人攻击
  add_header Public-Key-Pins 'pin-sha256="klO23nT2ehFDXCfx3eHTDRESMz3asj1muO+4aIdjiuY="; pin-sha256="633lt352PKRXbOwf4xSEa1M517scpD3l5f79xMD9r9Q="; max-age=2592000; includeSubDomains'
- **CAA** (DNS Certification Authority Authorization)
  通过DNS指定自己信任的CA，使CA避免误发证书
- **OCSP Stapling**
  服务端SSL握手过程直接返回OCSP状态，避免用户向CA查询，保护用户隐私
  ssl_stapling on;
  ssl_stapling_verify on;
  resolver 223.5.5.5;
  ssl_trusted_certificate certs/SymantecEVCA.pem;

MySSL --- HTTPS 安全评估

MySSL --- HTTPS 安全概览

概 述

检测部署SSL/TLS的服务是否符合行业最佳实现，PCI DSS支付卡行业安全标准。



1. 服务器易受到CVE-2016-2107漏洞攻击，降级为F
2. 因为在现代的加密协议上优先使用了RC4密码套件，降级为C
3. 服务器支持弱Diffie-Hellman(DH)密钥交换参数，降级为B
4. 启用了SSLv3协议，降级为B

MySSL --- HTTPS 配置建议

配置指南：

1. 需要配置符合PFS规范的加密套件，推荐配置：
ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL:!MD5:!ADH:!RC4:!DH:!DHE ；
2. 需要在服务端TLS协议中启用TLS1.2，推荐配置：TLSv1 TLSv1.1 TLSv1.2 ；
3. 需要保证当前域名与所使用的证书匹配；
4. 需要保证证书在有效期内；
5. 需要使用SHA-2签名算法的证书；
6. 需要保证证书签发机构是可信的CA机构。
7. HSTS（HTTP严格传输安全）的 max-age 需要大于15768000秒。

MySSL --- HTTPS 证书信息

证书信息

ECC | RSA

信任状态	可信
通用名称	www.trustasia.com
加密算法	ECDSA 256 bits
签名算法	ECDSAWithSHA256
证书透明(CT)	是
证书类型	EV SSL
开始时间	2016-12-28 08:00:00
结束时间	2017-09-29 07:59:59
是否吊销	否
组织机构	亚数信息科技（上海）有限公司
部门	--
备用名称	ssl.trustasia.com trustseal.trustasia.com www.alwaysonssl.cn mpki.trustasia.com

MySSL --- HTTPS 证书链详情

颁发给： **www.trustasia.com**
颁发者： Symantec Class 3 ECC 256 bit EV CA - G2
加密算法： ECDSA 256 bits
签名算法： ECDSAWithSHA256
SHA-1： C25094EC889D51C5141A2F07604A403A23AB26B8
PIN值： HnjtdvOS/vXKFjOO2W9NYcL025To/HoxrMbqTZiyfa4=
有效期： 131 天

颁发给： **Symantec Class 3 ECC 256 bit EV CA - G2**
颁发者： VeriSign Class 3 Public Primary Certification Authority - G5
加密算法： ECDSA 256 bits
签名算法： SHA256WithRSA
SHA-1： 0B69D3713F1B0584F1C88945A85B4CEB5FCFD721
PIN值： PtK3zjOppRxW+hXzyuP7gC8Nt8hPS735XLgT+lQ1KTo=
有效期： 2913 天

颁发给： **VeriSign Class 3 Public Primary Certification Authority - G5**
颁发者： VeriSign Class 3 Public Primary Certification Authority - G5
加密算法： RSA 2048 bits
签名算法： SHA1WithRSA
SHA-1： 4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5
PIN值： JbQbUG5JMJUoI6brnx0x3vZF6jilxsapbXGVfjhN8Fg=
有效期： 6997 天

MySSL --- HTTPS 协议和套件

支持的加密套件

TLS v1.0

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014) 256 bits
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013) 128 bits
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) 256 bits
TLS_RSA_WITH_AES_128_CBC_SHA (0x2F) 128 bits
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xA) 112 bits
TLS_RSA_WITH_RC4_128_SHA (0x5) 128 bits
TLS_RSA_WITH_RC4_128_MD5 (0x4) 128 bits

SSL v3

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014) 256 bits
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013) 128 bits
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) 256 bits
TLS_RSA_WITH_AES_128_CBC_SHA (0x2F) 128 bits
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xA) 112 bits
TLS_RSA_WITH_RC4_128_SHA (0x5) 128 bits
TLS_RSA_WITH_RC4_128_MD5 (0x4) 128 bits

支持协议

TLSv1.2	不支持
TLSv1.1	不支持
TLSv1.0	支持
SSLv3	支持
SSLv2	支持

名称：TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
代码：0x16
描述：DH 1024bits
加密强度：112 bits
正向加密：YES
是否安全：WEAK

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) 112 bits

MySSL --- HTTPS 协议属性

协议详情

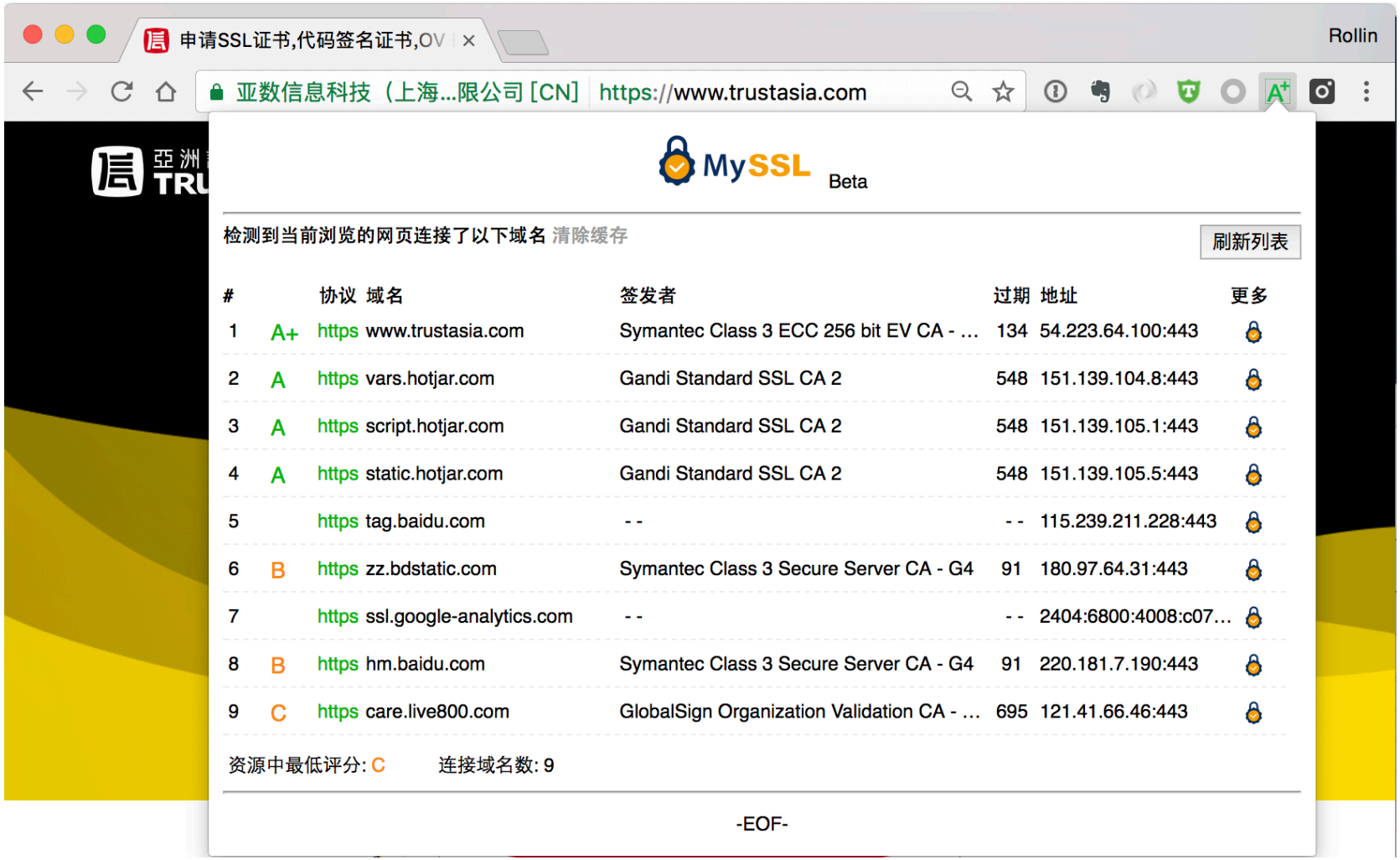
预防降级攻击	不支持	
支持RC4套件	支持	
正向保密	支持	
HPKP Report-Only（仅报告）	不支持	
HSTS（HTTP严格传输安全）	不支持	
HPKP（公钥固定）	不支持	
NPN	不支持	
ALPN	不支持	
OCSP装订	支持	
心跳（扩展）	不支持	
支持的EC椭圆曲线	支持	secp256r1,secp384r1

MySSL --- HTTPS 漏洞检测

SSL漏洞

	是否影响	危险系数	说明
DROWN 漏洞	是	高	CVE-2016-0800
OpenSSL CCS 注入漏洞	否	高	CVE-2014-0224
心血漏洞(Heartbleed)	否	高	CVE-2014-0160
OpenSSL Padding Oracle 攻击	否	高	CVE-2016-2107
不安全的客户端重协商(MITM)	否	高	
FREAK漏洞	否	低	CVE-2015-0204
POODLE漏洞	是	低	CVE-2014-3566
CRIME漏洞	否	低	CVE-2012-4929

MySSL --- Chrome 插件



MySSL --- HTTPS 最佳安全实践

www.trustasia.com

IP地址： 54.223.64.100:443 服务器： nginx

站点标题：申请SSL证书,代码签名证书,OV EV SSL证书 - 亚洲诚信

检测时间：2017-05-21 03:37:32

概 述

检测部署SSL/TLS的服务是否符合行业最佳实现，PCI DSS支付卡行业安全标准。

PCI DSS 合规

ATS 合规

THANKS