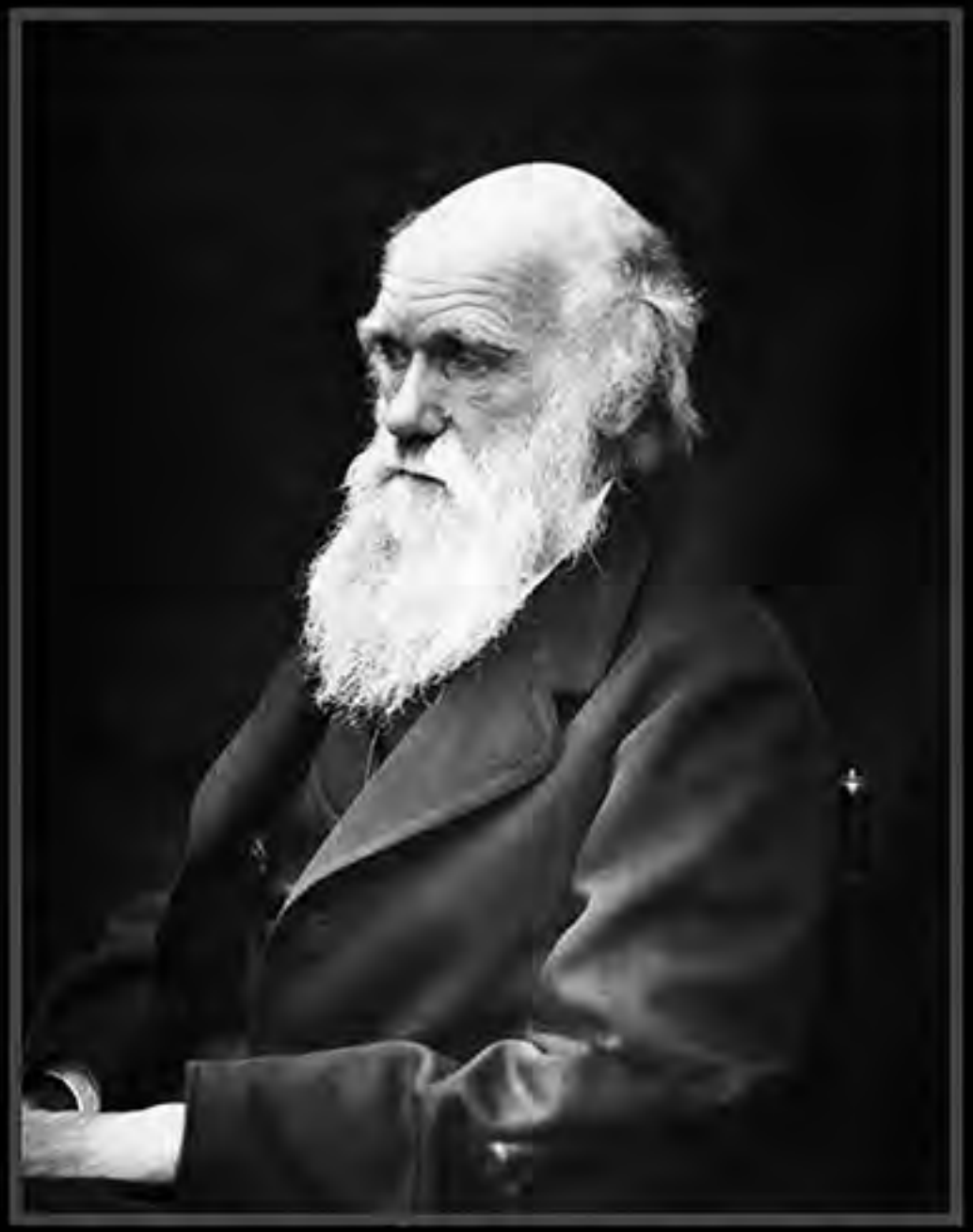
亞洲誠信®
TRUSTASIA

HTTPS时代

从HTTP到HTTPS的进化



WWW.TRUSTASIA.COM

亞洲誠信®
TRUSTAsia

感谢你！

HTTP

带我们进入互联网世界

你的进化带动了互联网的进化……

WWW.TRUSTASIA.COM

亞洲誠信®
TRUSTASIA

HTTP → HTTPS

1960年，Ted Nelson
HTTP 之父

Netscape

1994年
创建HTTPS

亞洲誠信®
TRUSTAsia

如果不进化？

HTTP

数据裸奔！

```
username=demo&password=demo123HTTP/1.1 200 OK
Date: Fri, 19 Jun 2015 09:05:30 GMT
Server: Apache/2.2.15 (CentOS)
Last-Modified: Fri, 19 Jun 2015 09:02:24 GMT
ETag: "22996-139-518db2eb7492d"
Accept-Ranges: bytes
Content-Length: 313
Connection: close
Content-Type: text/html; charset=UTF-8

<table border="userinfo">
```

亞洲誠信® TRUSTASIA

如果不进化？

HTTP

您的账户异常，请及时登录确认，以免损失

http://www.tenpay.com/v2/trade/bank_deduction.shtml?ADTAG=TENPAY_V2.NAV.TOP_RIGHT.HELP_QUERY

您的账户异常，请及时登录确认，以免损失

http://www.tenpay.com.imagedetail.jm2dx9mhpv-html.com/v2/trade/bank_deduction.shtml?ADTAG=TENPAY_V2.NAV.TOP_RIGHT.HELP_QUERY

防不胜防的钓鱼网站！

亞洲誠信®
TRUSTAsia

如果不进化？

HTTP

无声无息的中间人攻击！

亞洲誠信®
TRUSTASIA

为什么很安全

HTTPS

亞洲誠信®
TRUSTASIA

HTTP

- 明文传输
- 无法验证网站身份
- 无法保证传输数据的完整性

HTTPS

- 加密传输（保密性）
- 可以验证网站身份（唯一性）
- 保证传输数据的完整性

验证身份的数字证书

SECURITY

亞洲誠信®
TRUSTASIA

HTTPS

非对称加密

RSA 37年

亞洲誠信®
TRUSTASIA

HTTPS

非对称加密

RSA

RSA目前主流的密钥长度

RSA	ECC
2048	224
3072	256
7680	384

ECC

亞洲誠信®
TRUSTASIA

安全

HTTPS

- 级别高的数字证书

具备保密性的数字证书

身份唯一性

确保数据完整性

显著可视的安全特征

同等加密强度条件

不安全

HTTPS

- 级别低的数字证书

仅具备保密性的数字证书

- 不可信的证书
- 非认可自签发证书

- 人为原因

亞洲誠信®
TRUSTASIA

真正安全的 HTTPS

亞洲誠信®
TRUSTASIA

需要解决一些问题
才是真正安全的
HTTPS

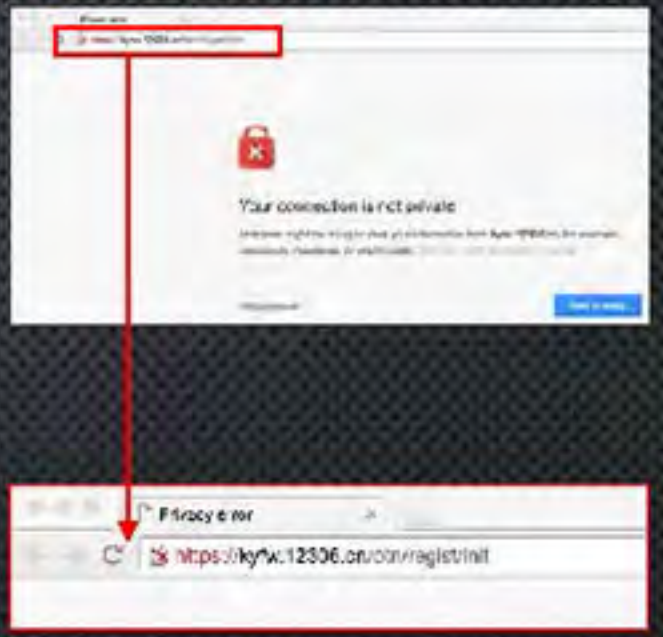
DNS解析异常
连接主机超时
与主机会话异常(通信超时 或 通信中断)

SSL 证书不可信
SSL 证书是自签名证书
SSL 使用了弱签名算法的证书
SSL 使用了低加密强度的证书
SSL 证书是为其他网站地址颁发的
SSL 使用了不安全的会话协议
SSL 使用了不安全的加密套件
SSL 证书指纹不匹配

SSL 证书时间无效
SSL 证书即将到期
SSL 证书被吊销
SSL 证书链不完整

SSL 页面包含不安全的外链
SSL 页面未强制使用HTTPS

SSL 存在Heartbleed漏洞
SSL 存在OpenSSL CCS漏洞
SSL 存在POODLE漏洞



SSL Cloud™

亞洲誠信®
TRUSTASIA

谁需要

HTTPS

亞洲誠信®
TRUSTASIA

WWW.TRUSTASIA.COM

亞洲誠信®
TRUSTASIA

HTTPS 必然性

亞洲誠信®
TRUSTASIA

Secure https://

2014.08

优先收录和排名HTTPS
建议使用2048位
及以上加密的证书

亞洲誠信®
TRUSTASIA

Secure https://

2015.05

优先收录HTTPS

WWW.TRUSTASIA.COM

亞洲誠信®
TRUSTASIA

HTTPS 全站必要性

亞洲誠信®
TRUSTAsia

HTTPS

亞洲誠信®
TRUSTASIA

HTTPS 市场数据

亞洲誠信 TRUSTASIA

HTTPS

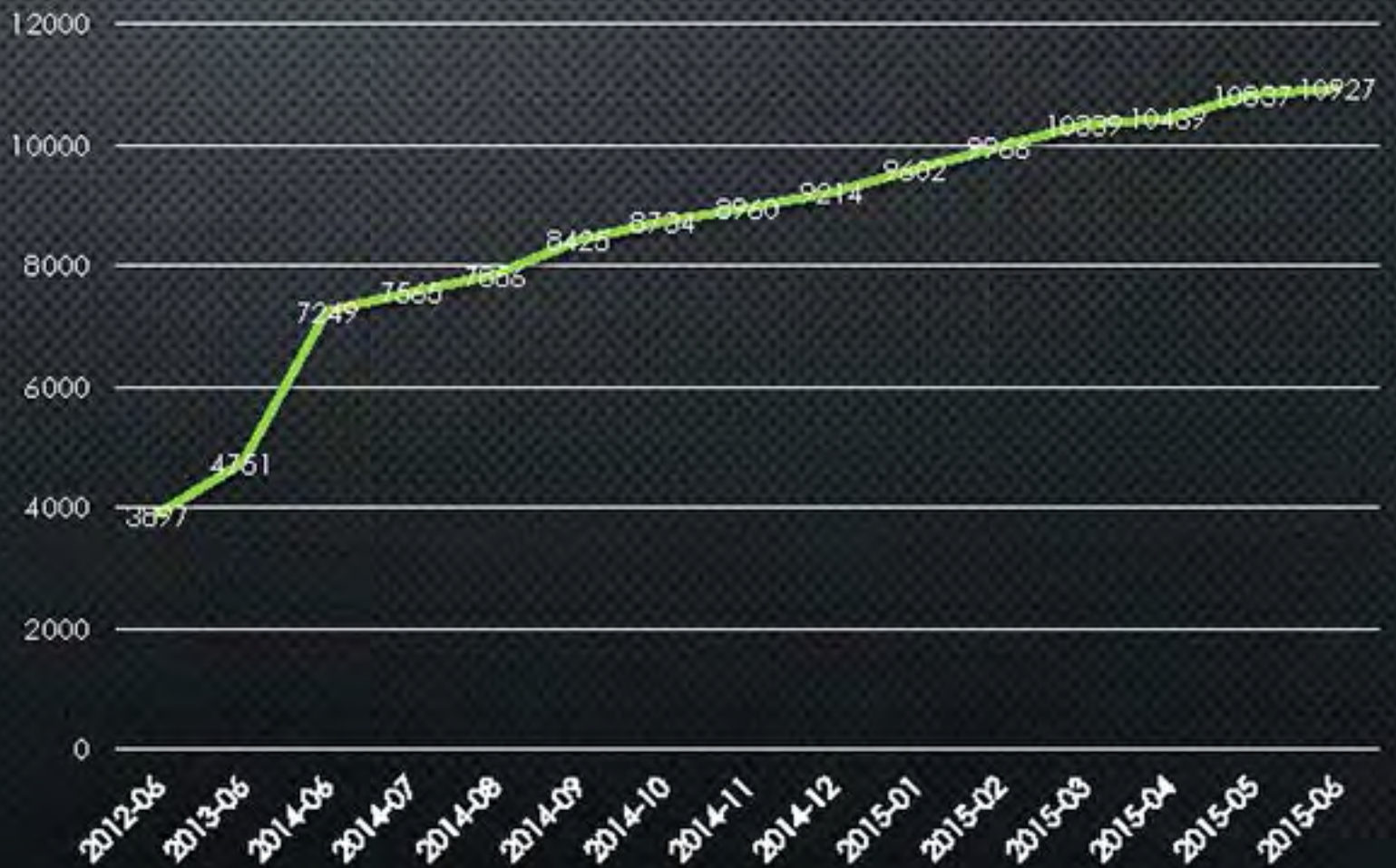
中国3年增长

2.8倍

中国数字证书增长 2012年~2015年

数据不包含：

- 不验证身份的证书（域名型证书）
- 自签发证书
- 无效证书



WWW.TRUSTASIA.COM

亞洲誠信®
TRUSTASIA

HTTPS

各品牌数字证书在中国的市场占有率

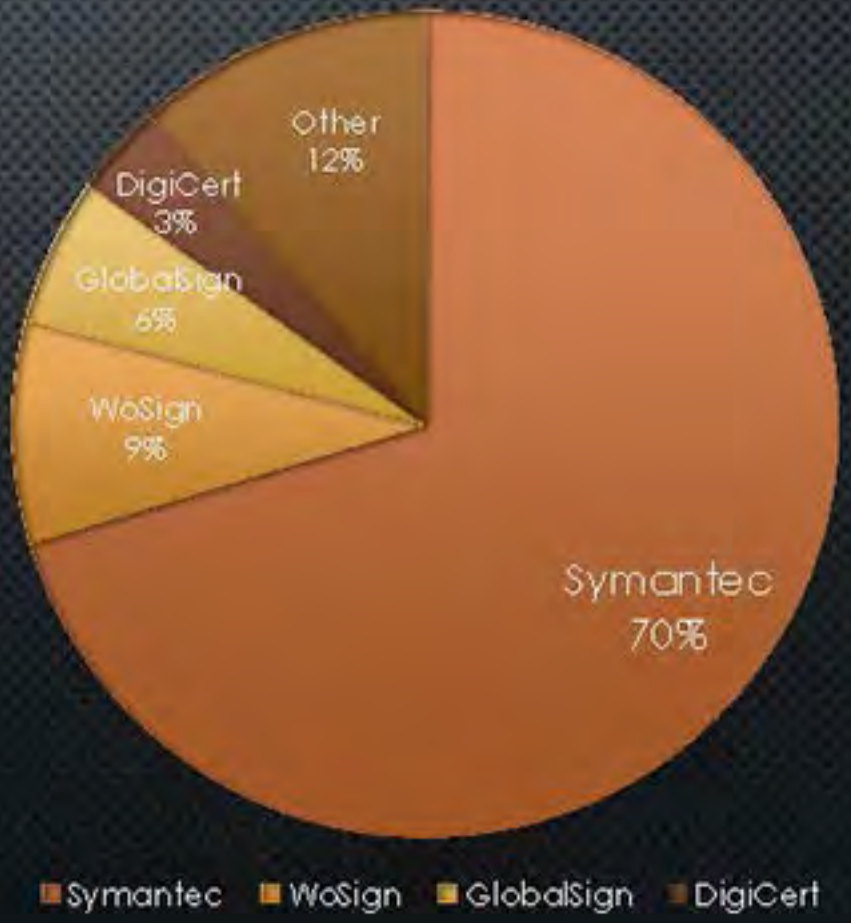
数据截止2015.06

数据不包含：

- 不验证身份的证书（域名型证书）
- 自签发证书
- 无效证书

NETCRAFT

TOP1

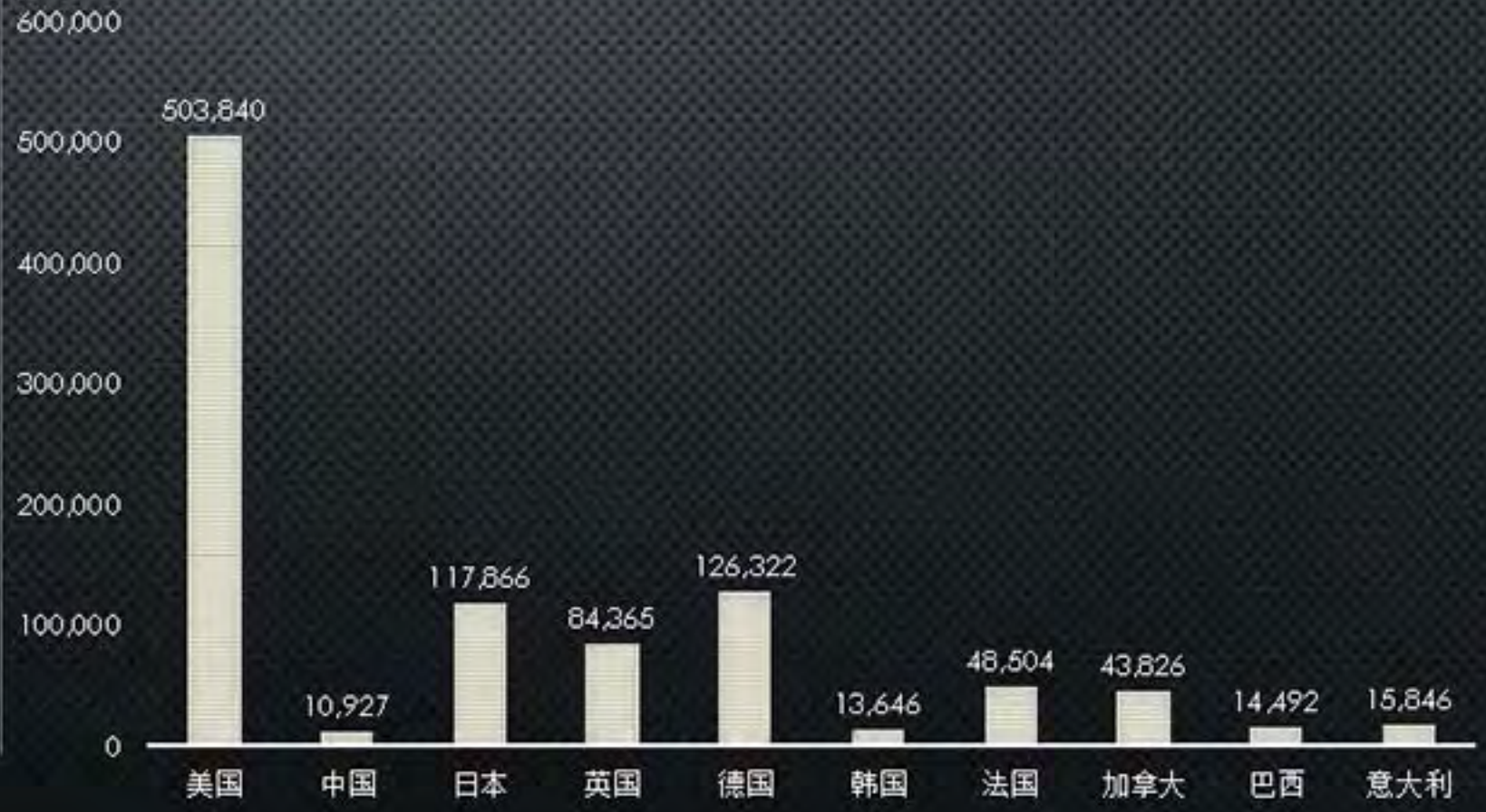


亞洲誠信®
TRUSTASIA

HTTPS

中国与世界其他国家对比
数据截止2015.06
数据不包含：

- 不验证身份的证书（域名型证书）
- 自签发证书
- 无效证书



WWW.TRUSTASIA.COM

亞洲誠信®
TRUSTASIA

HTTPS

中国域名数量与已经部署数字证书域名对比

数据截止2015.06

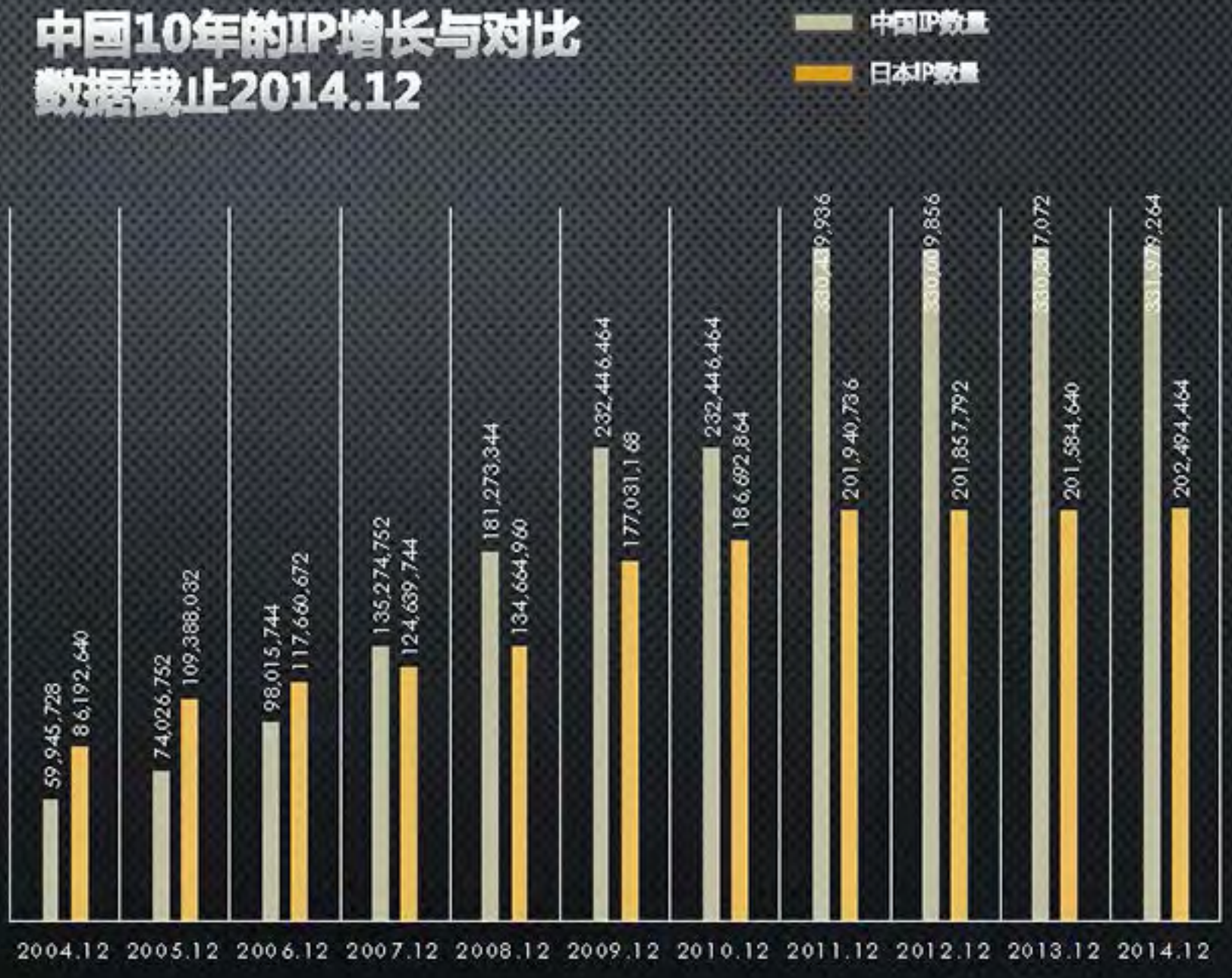
数据不包含：

- 不验证身份的证书（域名型证书）
- 自签发证书
- 无效证书

亞洲誠信®
TRUSTASIA

IP

中国10年的IP增长与对比
数据截止2014.12



WWW.TRUSTASIA.COM

亞洲誠信®
TRUSTASIA

7号展位

WWW.TRUSTASIA.COM

谢谢！

亞洲誠信®
TRUSTASIA
市场部
DERICK.XU@TRUSTASIA.COM
400 880 8600
WWW.TRUSTASIA.COM