



2017 中国互联网安全大会
China Internet Security Conference

加密无处不在-HTTPS数据安全解决方案

唐志红

北京天威诚信电子商务服务有限公司 总裁
中国电子认证服务产业联盟 标准专家委员会 委员



中国互联网安全大会



360互联网安全中心

目录

- HTTPS发展趋势
- HTTPS应用解决方案
- 加密无处不在



中国互联网安全大会



360互联网安全中心

HTTP将成为过去

HTTPS广阔前景

- 苹果IOS 10强制要求接入的所有APP采用HTTPS协议
- Google和百度调整其搜索引擎算法采用HTTPS网站排名更靠前
- Mozilla正式宣布淘汰HTTP的方案
- Google Chrome将对所有的HTTP网站进行不安全标记

HTTP **S** Hypertext Transfer Protocol
Secure



Secure `https:// www.`



- 全球最大在线百科-维基百科默认全站开启HTTPS
- 百度全站默认开启HTTPS
- 淘宝默认全站开启HTTPS
- Google、Facebook、Twitter等早已经实现全站HTTPS

只有https才具备的强大功能

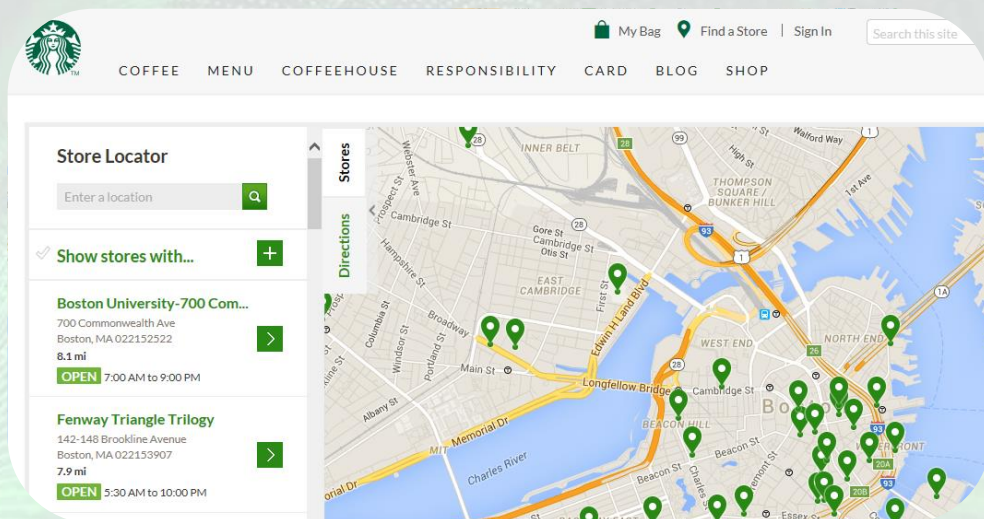


中国互联网安全大会



360互联网安全中心

1. 地理定位 (Chrome 50)
2. 设备运动/方向
3. 全屏
4. getUserMedia (摄像头/麦克风)
5. 加密媒体扩展 (数字版权管理)



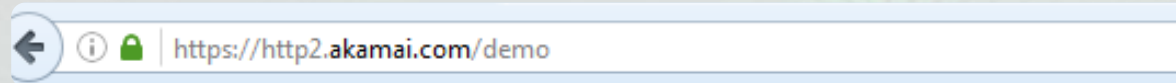
Http2仅用于https



中国互联网安全大会



360互联网安全中心



Chrome



Firefox



IE



Edge



Safari



Opera

HTTP/2 is the future of the Web, and it is here!

Your browser supports HTTP/2!

This is a demo of HTTP/2's impact on your download of many small tiles making up the Akamai Spinning Globe.

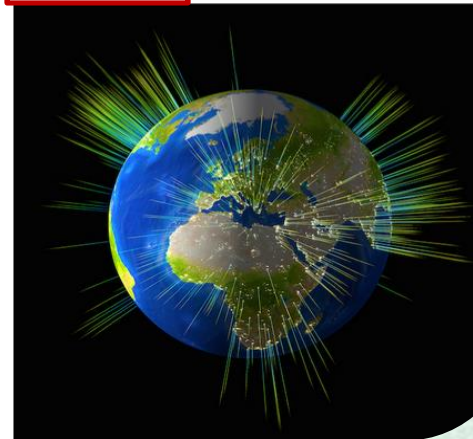
HTTP/1.1

Latency: 40ms
Load time: 17.53s



HTTP/2

Latency: 56ms
Load time: 1.11s



速度明显
加快！



云服务仍需要https

2017 年《互联网安全威胁报告》中指出：

云基础架构漏洞是网络犯罪分子的下一个目标，企业越来越依赖云服务，也因此产生了越来越多的安全漏洞。2016 年，用户因未开启身份验证而无意间泄露了旧版数据，导致数以万计的 MongoDB 云端数据库遭到网络犯罪分子的劫持和勒索。



哪些站点需启用HTTPS



中国互联网安全大会



360互联网安全中心

✓电商平台及其相关支付系统

✓银行系统、金融机构、电信行业等高私密性网站

✓政府、高校、医疗行业、科研机构及其相关网站

✓以搜索引擎为主要流量来源的网站

✓以内部办公系统为主的企业交流平台





中国互联网安全大会



360互联网安全中心

目录

- HTTPS发展趋势
- HTTPS应用解决方案
- 加密无处不在



中国互联网安全大会



360互联网安全中心

天威诚信 应用解决方案 共创安全智慧网络

@ 成立于**2000年9月**

@ 注册资金**6580万**元人民币

@ 产品公司**上市**，股票代码：835928

@ 2005年获工信部批准，成为**国内首家**

跨区域、跨行业的电子认证服务机构

@ “中国网络安全产业联盟” 理事成员

用心服务 追求卓越
400—666—3999

北京（总部）

郑州

成都

上海

杭州

宁波

深圳

我们是卓越的网络空间身份管理服务与安全服务提供商

专注于电子商务类应用的安全、可信、合法

天威诚信简介



https大面积应用面临的困扰



中国互联网安全大会



360互联网安全中心

管理不便

哪些CA供应商提供的产品？
什么时候到期？何时安排业务
切割更新？

管理难

下单繁琐

如何生成CSR？填写申请表？
邮件发送证书申请？证书签发
无提醒？证书签发邮件被拦截？

下单繁

跟踪难

未能即时跟踪

未经授权的自签名证书？攻击
者伪造证书？证书错误导致业
务连续性丧失？密钥或签名算
法过时，合规性问题？

安装难

安装故障无法检测

找不到配置指导文档？中级CA未
配置？协议版本或加密套件配置
有漏洞？

- 1 发现和监控**
无需手动搜索，自动发现网络中应用的SSL证书。定时更新数据，获取最新的证书应用状态。
- 2 生命周期管理**
多种方式的证书更新提醒，快速提交并即时签发新证书及更新证书，确保业务连续性。
- 3 分析和报告**
即时报告网络中的证书应用状态。分析和发现问题和故障，提示可行的应对方案。
- 4 分布式部署**
C/S架构，多机房管理。分布式部署，可方便的对多个机房进行分析和报告。
- 5 消息通知**
客户端即时消息通知，可集成短信、微信、邮件等多种通知模式。关注证书生命周期状态、核心服务器https服务状态，即时推送证书到期及漏洞报告分析消息。



证书智能管理系统——SSL证书综合管理平台



- ✓ **证书自动识别**
自动识别国际主流CA机构证书品牌及产品，可同时管理自签名SSL证书和企业内部CA系统SSL证书。
- ✓ **统一集中管理**
自动识别国际主流CA机构证书品牌及产品，可同时管理自签名SSL证书和企业内部CA系统SSL证书。分布式部署，支持多机房集中管理。
- ✓ **简单易用**
直观的SSL证书综合管理方案，无需培训和学习，立即上手，易于操作。

CIM证书智能管理系统功能



中国互联网安全大会



360互联网安全中心



扫描



分析报告



证书管理



订单管理



服务器管理

CIM证书智能管理系统功能



中国互联网安全大会



360互联网安全中心

天信威

CIM

您的专属证书管理专家

首页

扫描

扫描报告

证书管理

请求管理

服务器管理

反馈建议 帮助中心

z@itrus.com.cn

模糊规则

精准规则

机房扫描规则

修改时间: 2016-08-24 19:55:30

IP:

192.168.100.1-254

端口:

443,995,7002,8443

IP及端口:

192.168.100.1-254 : 443

删除

☒ 启用自动化扫描

☐ 探测服务器 OS 和 Server 类型

频率

☐ 每天

☐ 每周

周一

☐ 每月

2

 日

开始时间

10:00

添加

开始扫描

备份

程序版本: 4.0.16.823



扫描规则

支持模糊规则和精准规则，支持IP地址段扫描，支持域名和多端口扫描。



定时任务

定时任务自动刷新扫描结果。自动发信网络中的新证书。



系统探测

智能判断服务器OS及Web Server类型。

天威诚信—部分优质客户



中国互联网安全大会



360互联网安全中心





中国互联网安全大会



360互联网安全中心

目录

- HTTPS发展趋势
- HTTPS应用解决方案
- 加密无处不在



中国互联网安全大会



360互联网安全中心

加密无处不在，安全如影随形！

天威诚信-加密无处不在



中国互联网安全大会



免费+全线SSL证书



PKI/CA安全解决方案



CIM证书智能管理系统



全网HTTPS加密



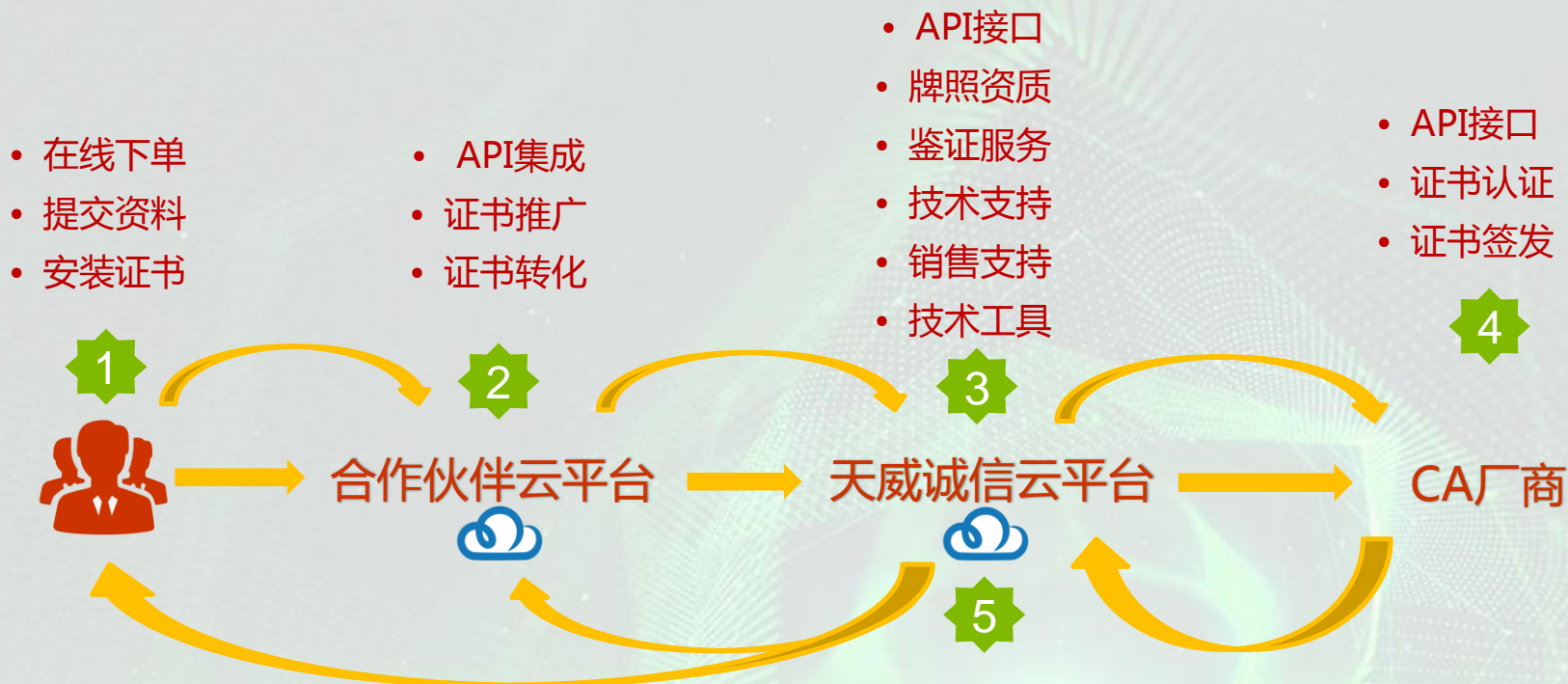
MPKI管理平台



免费API接口

高价值，低成本的安全解决方案，为托管服务提供商专属定制！

天威诚信—大客户、渠道及合作伙伴计划



- 1.最终客户（单位或个人）在合作伙伴云平台完成证书申请；
- 2.合作伙伴云平台将最终用户的订单信息通过API接口提交至天威诚信处理平台；
- 3.天威诚信将预审核通过的客户订单信息提交至CA厂商订单系统；
- 4.CA厂商通过认证后完成证书签发；
- 5.天威诚信将证书签发消息推送给合作伙伴，并为最终用户提供支持与服务。

天威诚信—服务优势



中国互联网安全大会



360互联网安全中心



合作伙伴



资质合规



产品全面



服务专业



■资质完备

可整合现有的基础架构和流程

能够轻松地与合作伙伴的系统进行无缝集成。

无缝集成

推广简单

自动化

■工信部+国密局双重监管

对于SSL的推广方式简单易复制

- 能够与合作伙伴现有产品进行整合，形成解决方案，使客户方便进行产品选择。
- 由第三方（天威诚信）完成鉴证工作，省去合作伙伴繁琐的鉴证工作。

可实现系统自动化

■专注于PKI/CA经验丰富

- 通过系统自动化的功能可以简化整个证书申请周期；
- 客户订单可以通过API接口进行下订单；
- 可以为成千上万的客户快速的签发证书；
- 如发生紧急情况，可以快速并自动化的进行证书吊销和替换的操作。

合作伙伴服务层

云服务商

CDN服务商

其他合作伙伴

天威诚信接口层

证书申请
操作取消

证书补发
审核通知

证书吊销
签发通知

API

天威诚信业务层

企业管理
渠道管理
合作伙伴

销售机会
系统管理
任务管理

订单管理
通知管理
CA引擎

第三方CA层

CA厂商

API

合作伙伴界面示例



中国互联网安全大会



360互联网安全中心

基本配置

保护类型：☒ 1个域名 ☐ 多个域名 ☐ 所有子域名

域名个数： 1个

证书类型：☐ 免费版SSL ☐ DV SSL ☒ OV SSL ☐ EV SSL

选择品牌： Symantec

购买清单 0列

当前配置

保护类型：☒ 1个域名
域名个数： 1个
证书类型：☒ OV SSL
选择品牌： Symantec
购买时长： 2年
配置费用：

¥

立即购买

加入清单

购买量

购买时长：☐ 1年 ☒ 2年 ☐ 3年

合作伙伴 | 产品管理 | 订单管理 | 账单管理 | 渠道管理 | 资源中心 | 消息中心



用户名

2级 34/50

折扣率：新

订单管理

订单审批

快速搜索

证书续订

收款管理

订单管理

订单号	订购日期	域名	附加域名	产品	状态	有效期	成本价格	公开价格	操作
2123094	2016-05-13	www.doomain.com	domain.com, www.domain.cn, etrade.domain.com	Symantec Secure Site Pro	待审查 (2016-05-15)				批准
2123120	2016-05-13	mail.domain.com	pop3.domain.com, smtp.domain.com, ---	GeoTrust	待验证 (2016-05-17)				催单
2123178	2016-05-13	crm.domain.com	crmsh.domain.com	GeoTrust	待签发 (2016-05-18)				更新
2123183	2016-05-13	www.itrus.cn		Symantec Secure Site	已签发	2016-05-15 至 2017-05-15			替换 取消 下载证书

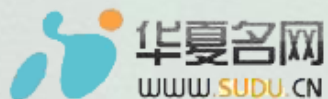
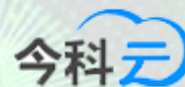
已实现HTTPS自动化合作伙伴



中国互联网安全大会



360互联网安全中心





中国互联网安全大会



360互联网安全中心

问题环节 Q&A

谢 谢



中国互联网安全大会



360互联网安全中心