腾讯云 | DNSPOD

国密(SM2)证书生态应用与实践

目录

01

什么是SSL证书？

腾讯云 | DNSPOD

“什么是 SSL 证书”

SSL 证书（SSL Certificates）又叫服务器证书，主要用于网站HTTPS加密和服务器身份认证，可以抵御数据泄露、数据篡改、流量劫持、钓鱼攻击等安全威胁。

根据加密算法类型划分，目前有支持RSA或ECC算法的“国际证书”，“国密证书”与支持SM2国产密码算法和国密安全协议两种类型。

腾讯云 | DNSPOD

“什么是SSL证书”

国际证书

支持RSA或ECC算法，具备广泛的兼容性，支持Firefox、Chrome等主流浏览器，支持Windows、安卓、iOS等操作系统和移动终端，支持Java和老设备。能够满足企业网站高稳定性、速度快的需求，目前能够提供的品牌也非常丰富。

国密证书

支持SM2国产密码算法和国密安全协议，使用国密算法实现高强度SSL加密连接及服务器身份认证，适合对国密合规性有要求的政企网站。兼容腾讯云国密浏览器、360安全浏览器、密信浏览器等。

腾讯云 | DNSPOD

“安装 VS. 未安装”

▲ 安装了SSL证书的服务器（网站）

▲ 未安装SSL证书的服务器（网站）

腾讯云 | DNSPOD

“没有SSL 证书将导致？”

面临数据被窃取/篡改，钓鱼网站假冒的风险

HTTPS加密保护传输数据机密性和完整性，能够防止数据在传输过程中被盗取或篡改；可验证服务器真实身份，防止钓鱼网站假冒

面临流量被劫持的风险

启用HTTPS加密可以有效解决任意网络节点的流量劫持、中间人攻击等安全威胁

浏览器将出现“不安全”警告

浏览器强力推动HTTPS加密普及，将所有HTTP页面都标记为“不安全”；浏览器推动通知、获取地理信息等新功能必须通过HTTPS请求

不利于SEO排名的提升与优化

搜索引擎会优先收录HTTPS页面，并提升HTTPS页面排名权重

无法满足微信开发平台HTTPS的强制要求

微信小程序、微信支付、企业微信等微信平台开发强制要求使用HTTPS

腾讯云 | DNSPOD

“SSL证书安全性”

截止2021年02月，根据 MySSL.com和Chrome 插件 SSL/TLS安全评估报告中检测到的（中国）HTTPS可信站点客观数据：

站点数 488.6w

半年增长 90w

涨幅高达 23%

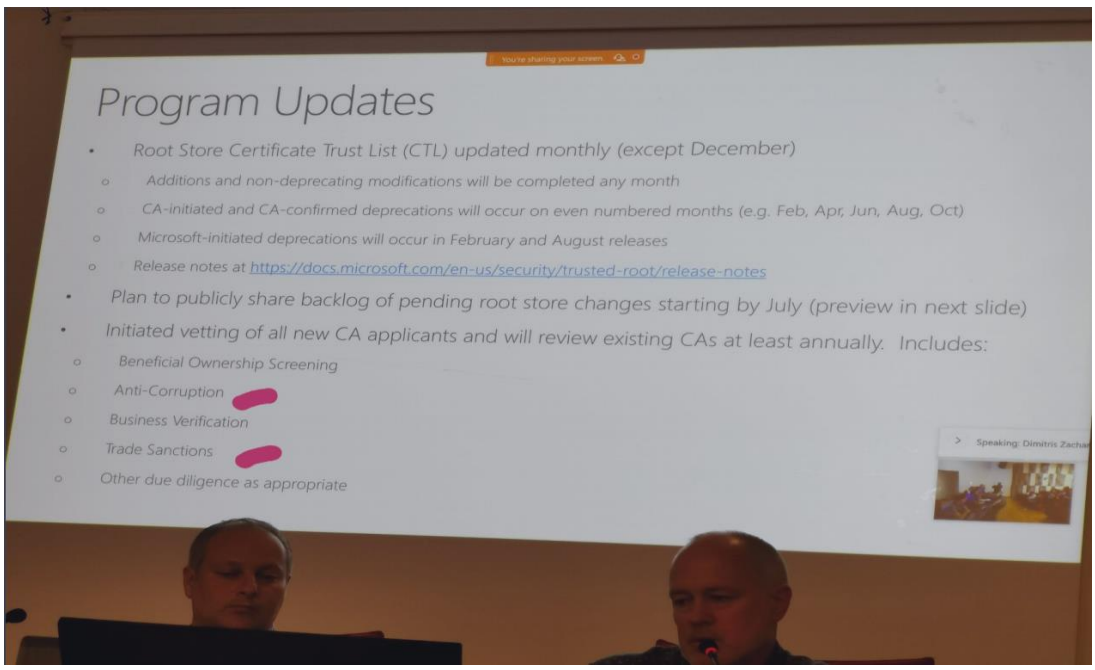
迅猛的增长等于我国网络传输安全大幅提高？

02

国密（SM2）证书的重要性

腾讯云 | DNSPOD

国密（SM2）证书的重要性



微软在 CA/B Forum发布的全球信任根认证计划

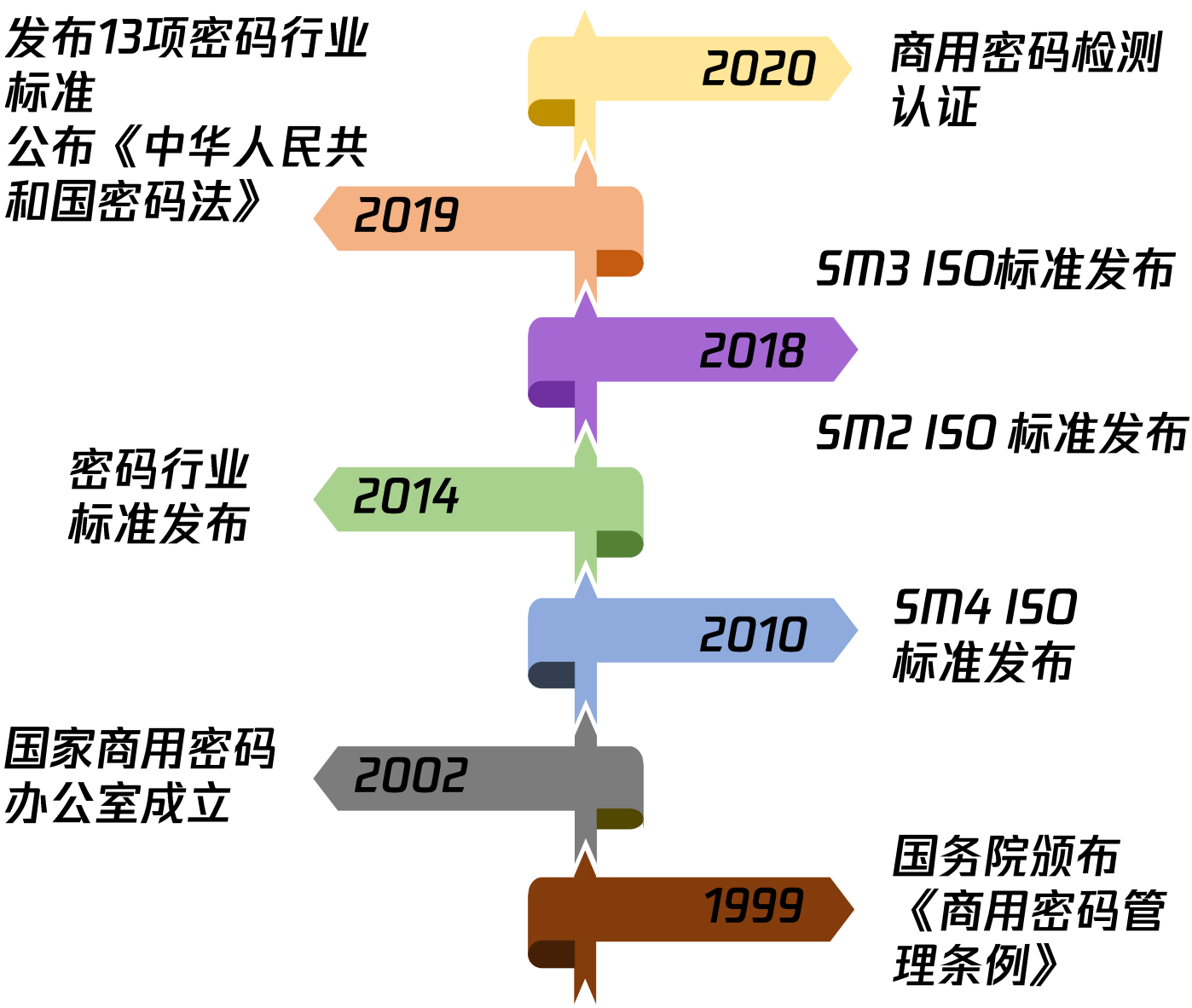
首次把“贸易制裁（Trade Sanctions）”列为微软全球信任根认证计划的评估条件之一

中国将有可能与“古巴、朝鲜、叙利亚和伊朗”一样，将不被允许使用全球签发的 RSA/ECC SSL 证书

腾讯云 | DNSPOD

国密（SM2）证书的重要性

国家高度重视商用密码工作，自1999年国务院颁布《商用密码管理条例》以来，截止目前，已经有多项政策陆续出台，推进国密算法的实施落地。



腾讯云 | DNSPOD

国密（SM2）证书的重要性

关键信息基础设施安全必须采用应用密码技术来保障

中华人民共和国密码法（草案）

第二十七条 法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，开展商用密码应用安全性评估。

关键信息基础设施的运营者和国家机关采购、使用涉及商用密码的网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国家密码管理部门等有关部门组织的国家安全审查。

1/2

中共中央办公厅 国务院办公厅关于印发《金融和重要领域密码应用与创新发展工作规划（2018—2022 年）》的通知

厅字〔2018〕36 号

2018 年 7 月 15 日

保障国家关键信息基础设施安全，着力在金融和重要领域推进密码全面应用，着力在构建自主可控信息技术体系中推进密码优先发展，构建以密码技术为核心、多种技术相互融合的新网络安全体系，建设以密码基础设施为支撑的新网络安全环境，

2/2

腾讯云 | DNSPOD

国密（SM2）证书的重要性

必须采用国产密码技术进行商用密码生态应用

8.1.2.2 通信传输 《等保2.0》三级

本项要求包括：

a) 应采用校验技术或密码技术保证通信过程中数据的完整性；

b) 应采用密码技术保证通信过程中数据的保密性。

- 网络安全等级保护2.0明确规定，要求对网络通信中的报文或会话过程全程加密(三级)
- 其中密码技术标准之一就是 SM2 算法

相关法规

常委会
《中华人民共和国密码法》

工信部
《电子认证服务管理办法》

国密局
《电子认证服务密码管理办法》
《商用密码管理条例》

腾讯云 | DNSPOD

国密（SM2）证书的重要性

基于国家相关政策和要求

DNSPod 推出了

腾讯云政企国密解决方案

使用**国密（SM2）证书**

和相关生态建设

解决政企客户在网络传输过程中的

等保合规需求

03

腾讯云政企国密解决方案

腾讯云 | DNSPOD

国密方案说明

实现一站式闭环

提出完整国密链路

国密自适应网关

“支持国密算法的自适应网关方案”

国密浏览器

“支持国密算法的浏览器”

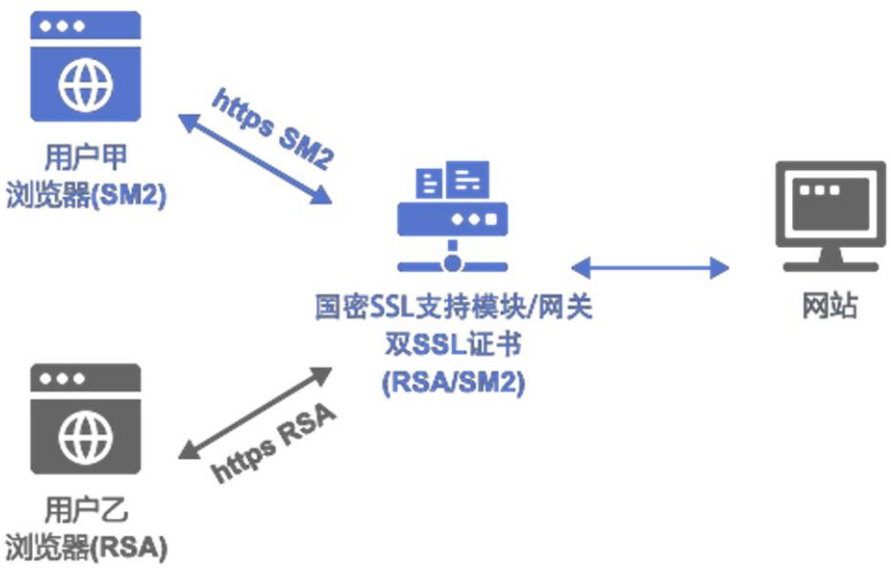
国密+国际SSL证书

“国密+国际算法SSL双证书部署”

腾讯云 | DNSPOD

双轨制方案执行

HTTPS 国密应用思路
双轨制方案的执行



1.服务器端同时部署国际RSA/ECC SSL证书和国密SM2 SSL证书

2.采用支持国密算法的自适应网关以支持国密算法和国密SSL证书:

- 不支持国密的浏览器使用RSA SSL证书;
- 支持国密的浏览器则使用国密SM2 SSL证书，确保网站HTTPS支持所有浏览器

3.使用浏览器访问服务端，根据支持的算法进行自适配操作

腾讯云 | DNSPOD

方案部署模式

Web用户

- 腾讯云国密浏览器（SM2协议）
- Chrome浏览器（RSA/ECC协议）
- Firefox浏览器（RSA/ECC协议）

SSL建立

数据加密

国密安全网关

SSL加速	高速缓存	TCP复用
证书自动化	多机热备	负载均衡
HTTP压缩	国密支持模块	SM2证书

数据分发

资源缓存

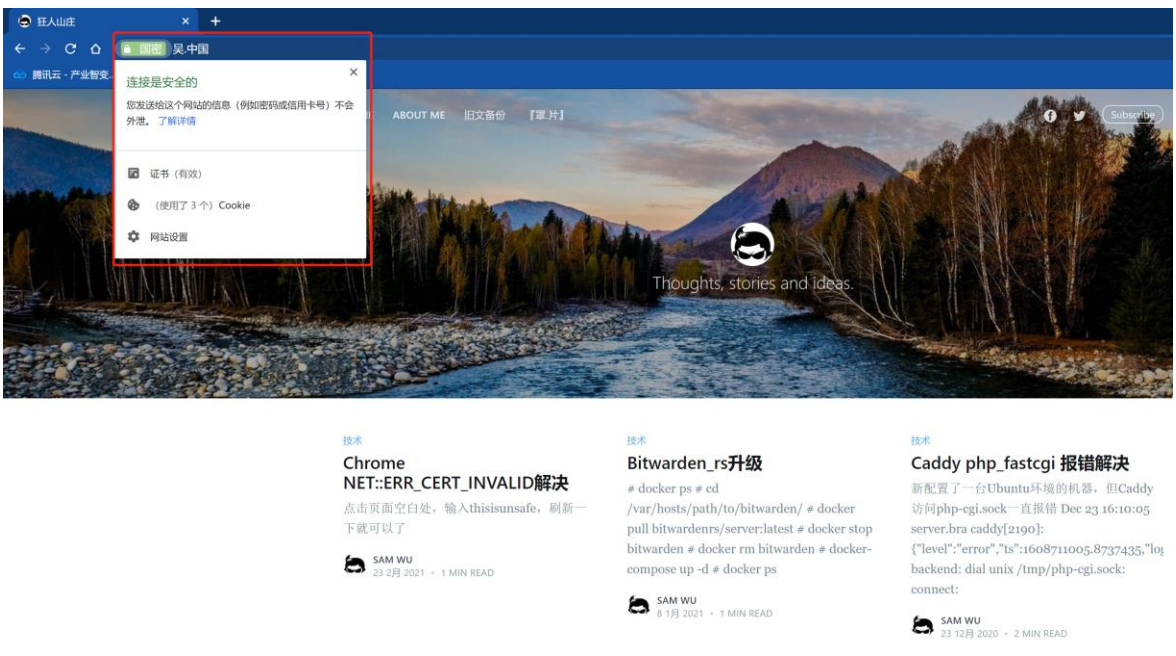
TCP链接

Web服务集群

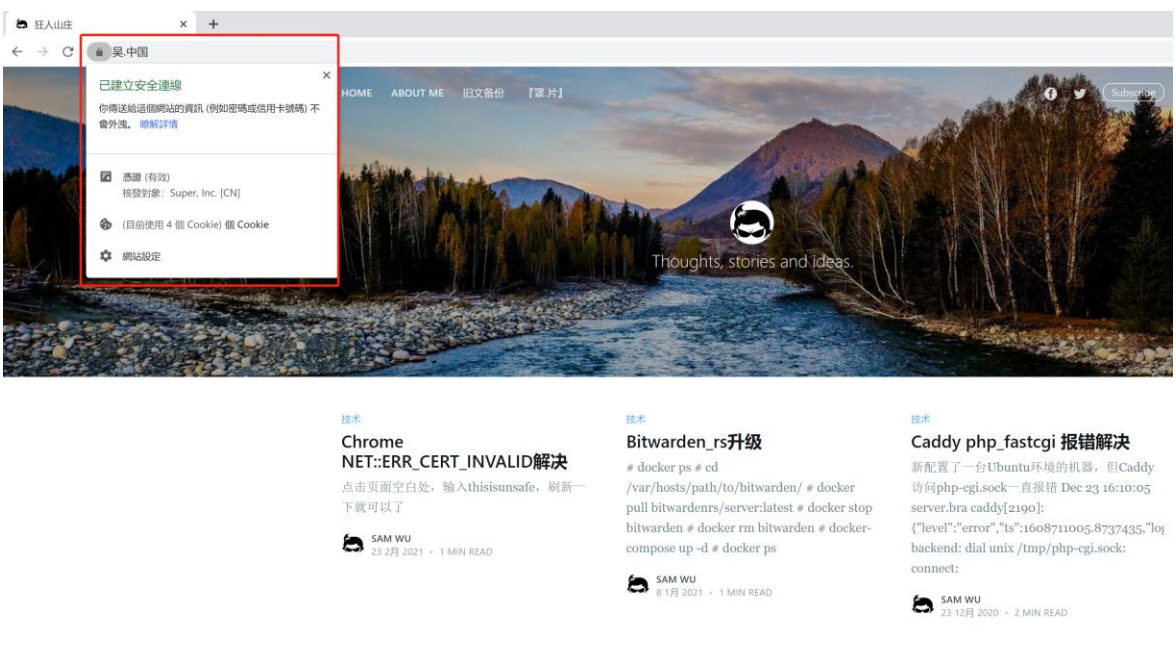
- 服务器 A
- 服务器 B
- 服务器 C
- ……
- 服务器 N

腾讯云 | DNSPOD

国密HTTPS 实际实施效果



腾讯云国密浏览器访问效果



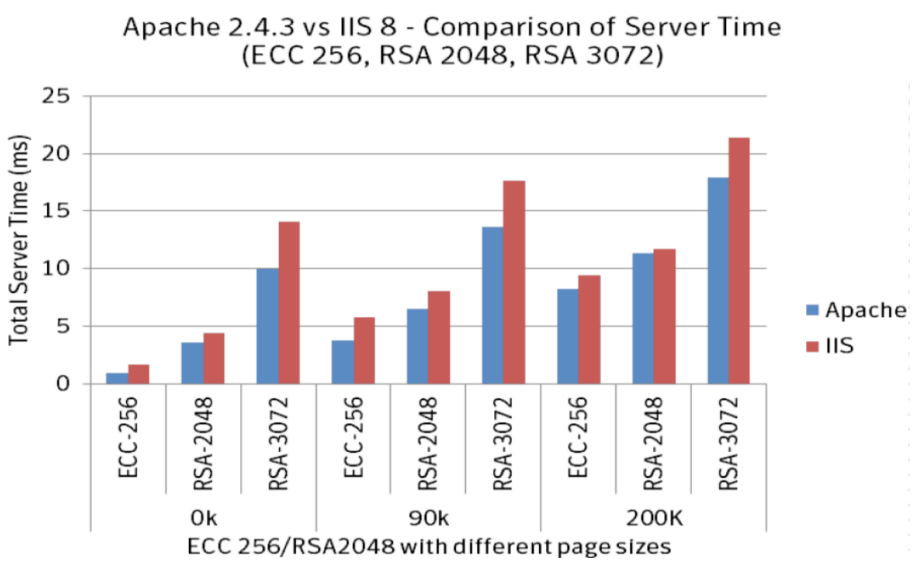
普通浏览器访问效果

腾讯云 | DNSPOD

产品亮点

DNSPod 国密 SM2 证书

主要特点



自主品牌

- 腾讯云自主品牌，符合国家标准，完全自主知识产权，满足监控需求，无惧证书断供风险，服务及售后有保障

性能优越

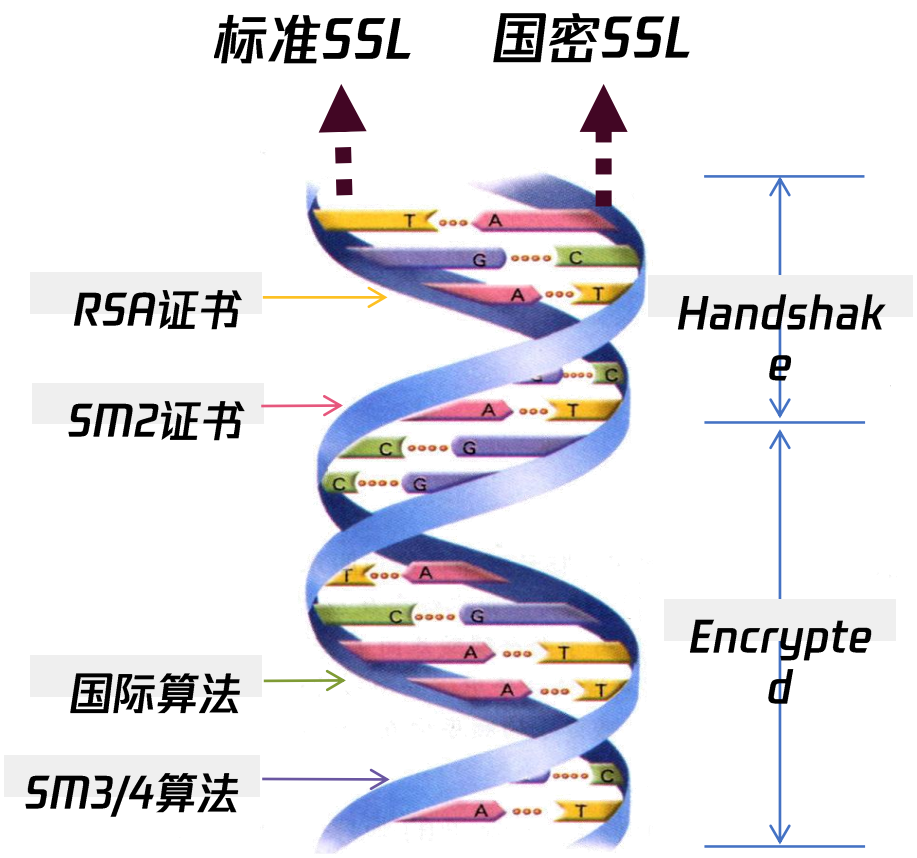
- 根据国外ECC加密算法性能研究报告：采用ECC算法，Web服务器响应时间比RSA要快出10倍以上
- 同时SM2的加密强度要远比RSA 3072高

腾讯云 | DNSPOD

产品亮点

国密
自适应网关

主要特点



国际+国密双算法自适应

负载均衡： 对Web应用深度优化；支持IP会话保持、会话应用保持、深度健康检查、URL重定向、双机热备

Web加速： 支持动态压缩、告诉存储、连接复用等加速技术；支持阈值上线限及告警、用户证书透传、页面智能预加载

SSL加速： 支持 RSA/ECC/SM2 加速、SSL v3.0、TLS v1.0—V1.3；支持国密双证书、国密算法 SM1/2/3/4，国密浏览器

腾讯云 | DNSPOD

产品亮点

腾讯云国密浏览器

主要特点

支持国密+国际双证书:

- 支持国密（SM2）、国际标准SSL证书访问

兼容性好:

- 支持GB/T 38636-2020(GM/T 0024-2014）标准（TLCP）
- 提供Windows版本 & 提供Mac版本

深度可定制:

- 腾讯云国密浏览器支持企业级的深度定制方案，可根据用户的不同需求进行浏览器各种配置的深度定制

04

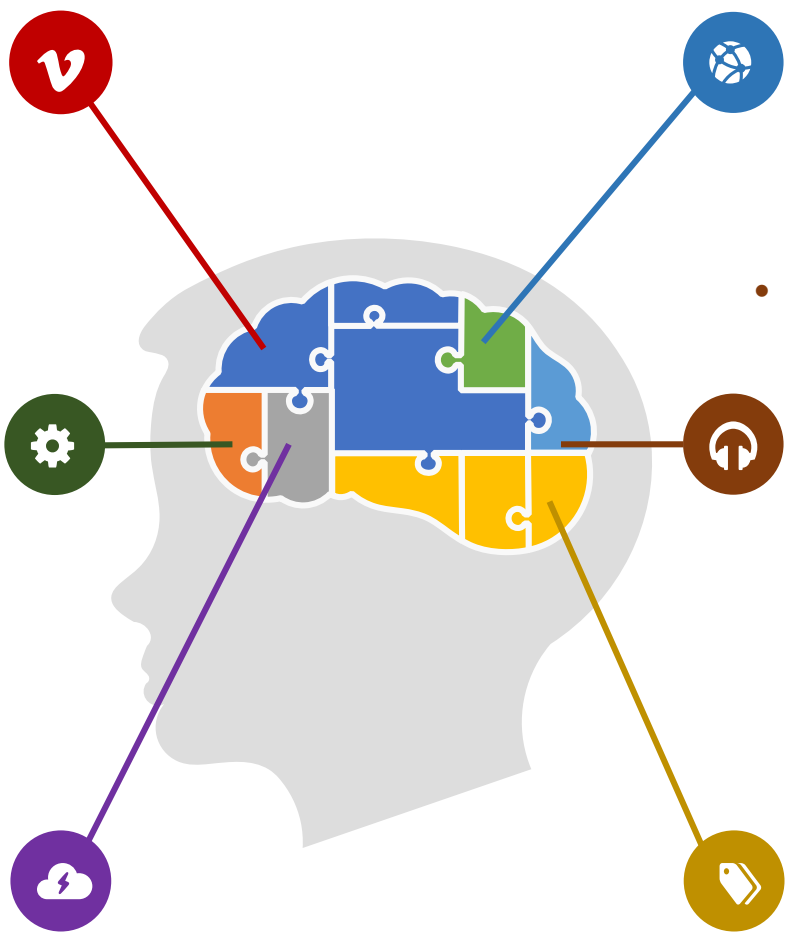
目标客户及案例

腾讯云 | DNSPOD

六大用户痛点

- 客户企业有国家安全监控需求，有国产化和自主可控的保护要求
- 有潜在受到外部国际环境影响和限制的风险，需要对风险进行规避

需要实现国产化以进行等保合规建设，需要技术自主可控，但国产化方案却不知道从何入手



- 单有国密（SM2）证书，没有配套服务，用户搭建国产化应用生态困难

- 对网站和信息安全保护有加强防护的需求
- 相关方案没有售后服务，整套系统不知道如何维护

腾讯云 | DNSPOD

七大目标客户

政府机关单位

高校等教育单位

电信网等提供公共信息网络服务单位

国防科工等科研生产单位

广播电台、通讯社等新闻单位

卫生医疗、金融、交通等公共服务单位

涉军、涉政及涉研行业的客户

腾讯云 | DNSPOD

目标客户及案例一

——金融

典型公司：**证券

人员规模：1000+

目前状况：

国家近期强制要求依照相关法律法规进行网络安全建设，对网络安全、等保合规等概念有一定了解但不全面，自身业务急需进行网络安全体系搭建

核心需求

- 国家强制要求依法建立安全体系
- 安全建设需满足等保合规需求
- 需要云服务提供整体打包的解决方案

关键标签

- 等保合规
- 政策要求
- 整体解决方案
- 国产解决方案

腾讯云 | DNSPOD

目标客户及案例二

——教育

典型公司：上海**大学

人员规模：3W+

目前状况：

大学基于提高学校网络信息中心建设国产化率，计划进行国密改造，其中的第一步就是网络传输安全国产化

核心需求

- 提高网络安全建设国产化比率
- 需要一站式的解决方案
- 性价比高

关键标签

- 国产化比率
- 一站式解决方案
- 性价比

腾讯云 | DNSPOD

目标客户及案例三

——政府政务

典型公司：山东省**保障局

人员规模：1000+

目前状况：

提供民生基础服务的政务单位及部门是国产密码应用改造的第一梯队，以保障关键信息基础设施、重要网络和数据安全，从而保护人民群众的合法权益

核心需求

- 国家法规要求
- 政务处于改造第一线，急需国产化改造
- 基于本身环境所致，需要进行定制化开发

关键标签

- 法律法规要求
- 政务改造一线
- 定制化服务

腾讯云 | DNSPOD

价格说明

腾讯云政企国密方案一览

类别	企业版	高级版	尊享版
国际标准证书	√	√	√
国密标准证书	√	√	√
网关	T100型	T200型号	T500型号
国密专属浏览器	国密+国际 双证书访问	双证书访问 + 定制化功能	双证书访问 + 定制化功能
政企国密 支持服务	部署、培训、技术 支持一体化	部署、培训、技术 支持一体化	专属VIP服务 1V1技术支持

若需详细方案可提交产品申请:
https://cloud.tencent.com/product/ssl/sm2

腾讯云 | DNSPOD

谢 谢

编著：赵晶、张静雨