

云计算和主机服务中的 数据安全保护策略

Entrust Datacard 尹东梅

mia.yin@entrustdatacard.com

应用场景的变化

Limited



VPN Access



Critical On-Premise
Systems & Apps



Enterprise-Wide



VPN Access



Critical On-Premise
Systems & Apps



Cloud SSO



Customer & Partner
Web Portals



Desktop Login



Mobile – the Primary
Computing Platform

多元化需求

服务中断

- ✓ Slow website performance
- ✓ Improperly installed certificates
- ✓ Expired certificates
- ✓ Misconfigured server
- ✓ User security warnings

安全威胁

- ✓ FREAK
- ✓ SuperFish
- ✓ POODLE
- ✓ Heartbleed
- ✓ BEAST
- ✓ CRIME
- ✓ Lucky Thirteen

技术革新

- ✓ SHA1→SHA2
- ✓ OCSP Stapling
- ✓ CAA
- ✓ CT
- ✓ TLS 1.2
- ✓ ECC
- ✓ HTTP/2

规范要求

- ✓ PCI
- ✓ HIPAA
- ✓ SHA1→SHA2
- ✓ Security Policy
- ✓ SSL3 deprecation

资源限制

- ✓ Do more with less
- ✓ Consolidate vendors
- ✓ Implementation costs
- ✓ De-focused staff
- ✓ Limited training
- ✓ Rapid deployment

品牌影响

- ✓ Site outage/performance
- ✓ Data breach
- ✓ SPAM blacklist
- ✓ Search engine blacklist
- ✓ Malicious impersonation

2016年11月7日颁布的，将于2017年6月1日实施的《中华人民共和国网络安全法》

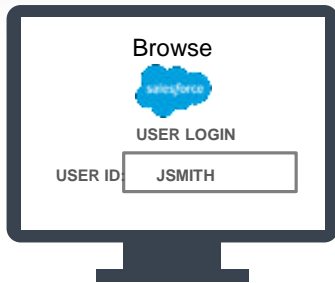
The screenshot shows the official website of the National People's Congress (NPC) of China. At the top, there is a yellow banner with the NPC emblem and the text "全国人民代表大会" (The National People's Congress of the People's Republic of China). Below the banner is a navigation menu with various links such as "首页" (Home), "宪法" (Constitution), "国家机构" (State Organs), etc. The main content area features the title "中华人民共和国网络安全法" (Cybersecurity Law of the People's Republic of China) and a sub-header indicating it was passed by the 24th meeting of the 12th NPC Standing Committee on November 7, 2016. A table of contents is visible, listing chapters from "总则" (General Provisions) to "法律责任" (Legal Liability). On the right side, there are sections for "图片报道" (Image Report) and "访谈" (Interview), with a small image of a man in a blue shirt under the "访谈" section.

需求的变化

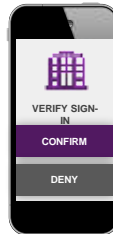
数据确保安全吗？

网络身份真实吗？

对云 / SAAS应用的身份认证



No password required
with web applications.



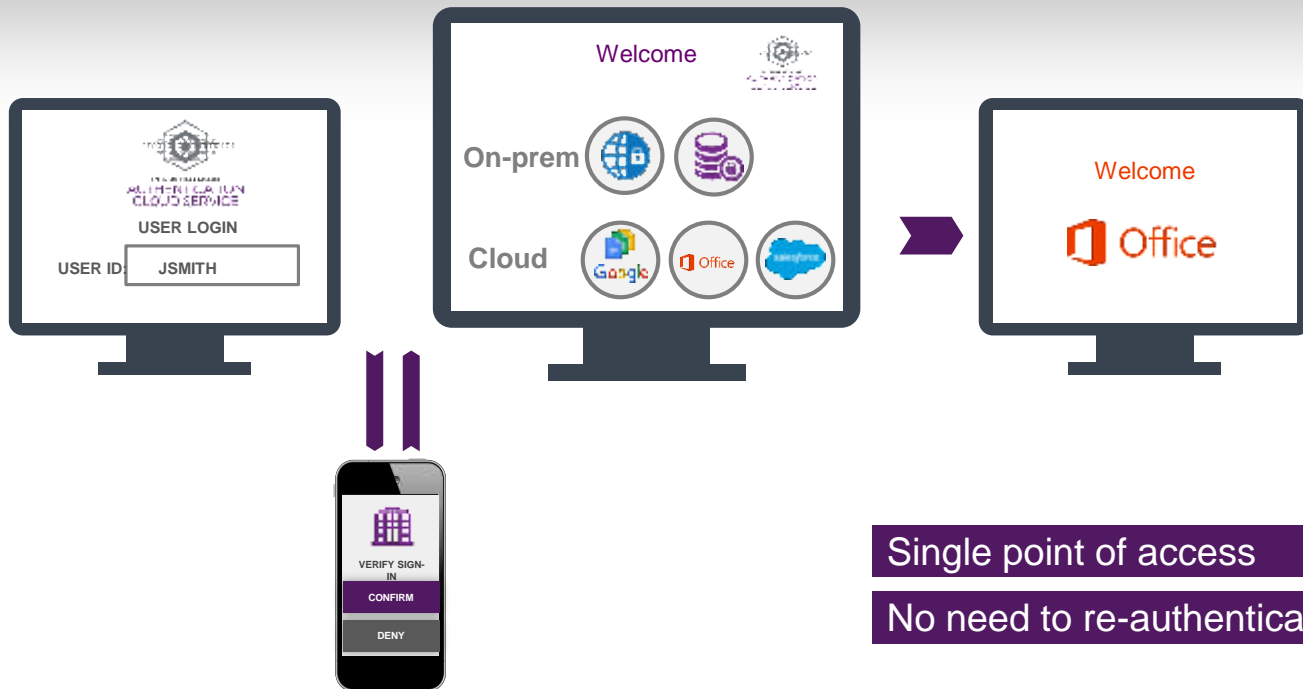
User selects "confirm"



One identity

Same user experience

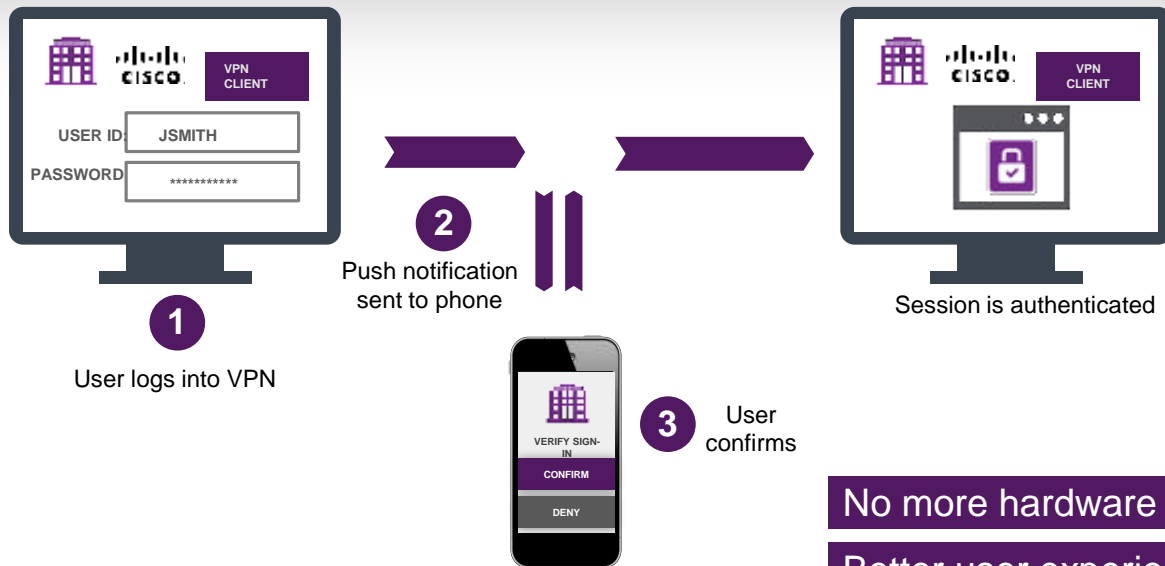
单点登录所有应用



Single point of access

No need to re-authenticate

MOBILE PUSH FOR VPN ACCESS

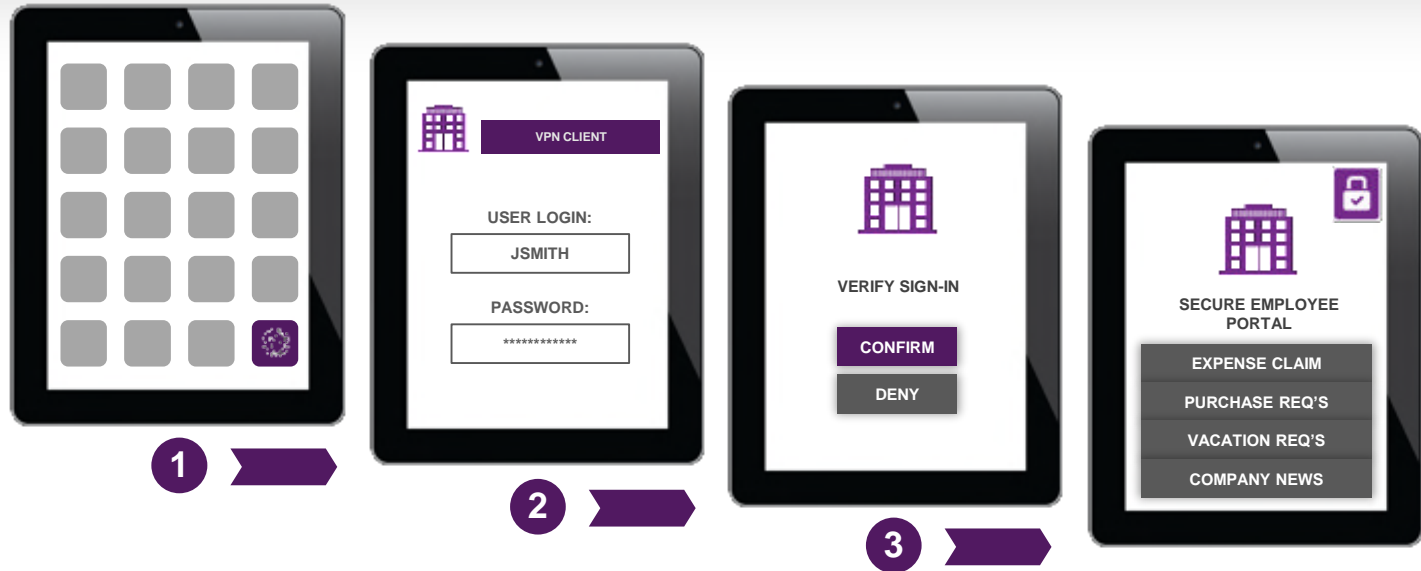


No more hardware tokens

Better user experience

Easier provisioning


TABLET EXPERIENCE: MOBILE PUSH FOR VPN ACCESS




对用户 / 合作伙伴平台的双因子身份认证

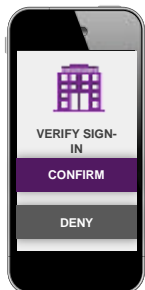


Mobile Push


 PARTNER PORTAL CLIENT

USER NAME

Go! 




Mobile OTP

 PARTNER PORTAL CLIENT


USER NAME

ENTER OTP

Go! 




SMS / GRID Token

 PARTNER PORTAL CLIENT

USER NAME

PASSWORD

ENTER OTP

Go! 



WINDOWS 桌面机登录 – OTP



1

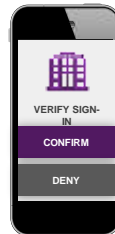
Log in Windows with first factor



2

2FA with grid, token...

OR



2

2FA with mobile push...



3

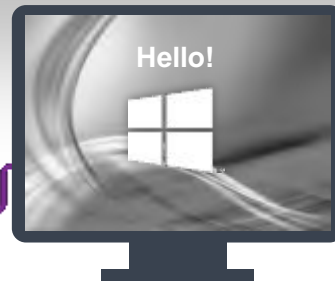
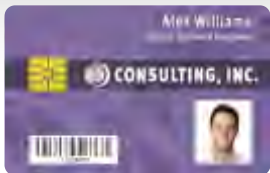
Session is authenticated

Same Identity , same UX

“Offline” mode available

WINDOWS 桌面机登录- 智能凭证

Traditional Smart Card



Mobile Virtual Smart Card

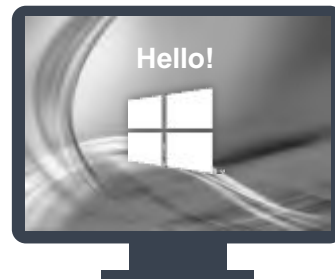


Convenient
"auto-detect"

Secure
"auto-logout"



Virtual smart
card reader



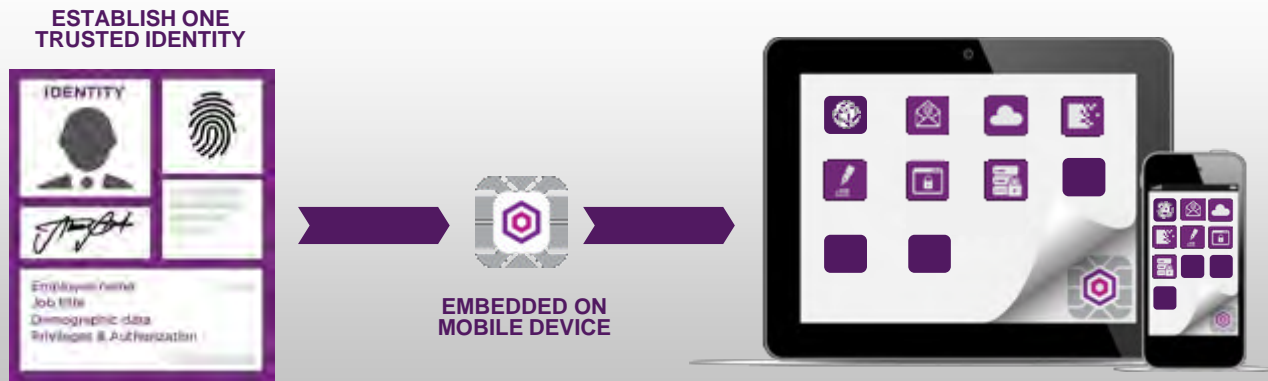
High Assurance

移动端身份认证

Smart Credential within the Mobile Desktop (virtual smart card)

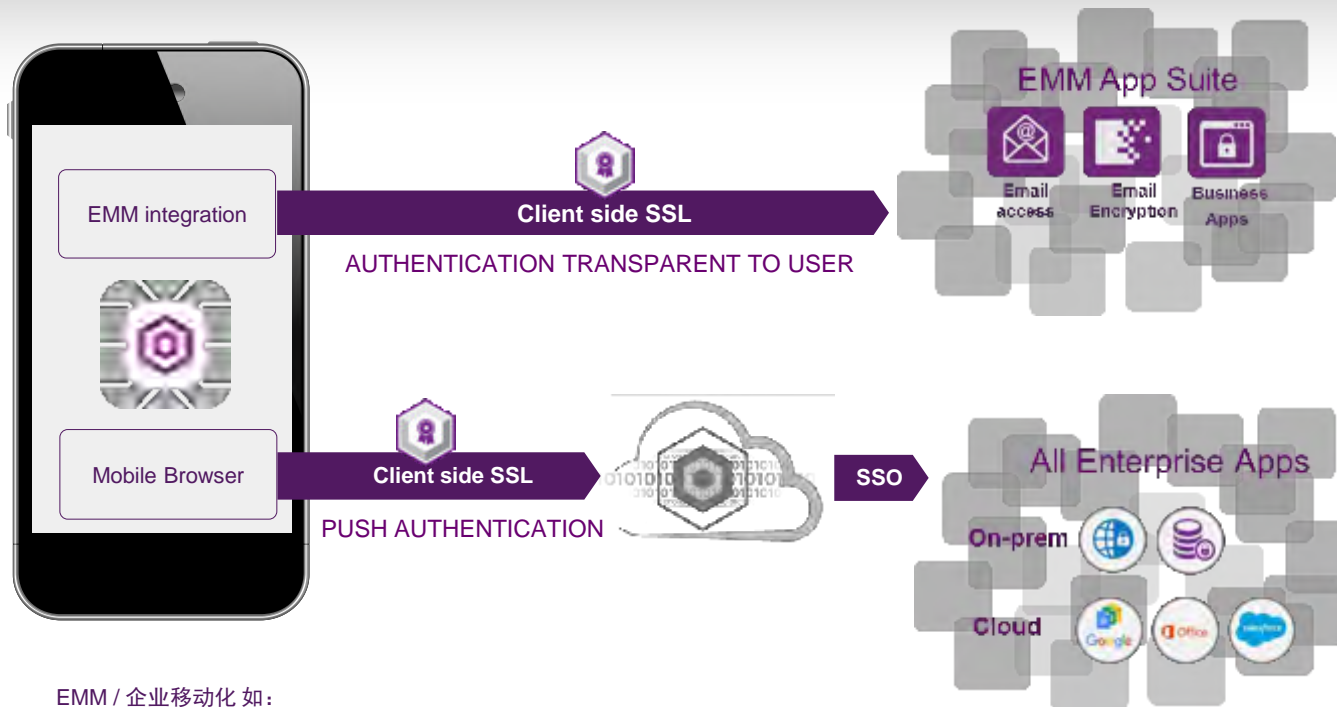
Provides smart card based security with far more convenience

Certificate/PKI authentication, encryption & signing



移动端身份认证

Quick, Simple, Secure Access To Enterprise Apps



EMM / 企业移动化 如:

Citrix, Blackberry, Mobile Iron, VMware Airwatch

广泛的身份认证方法

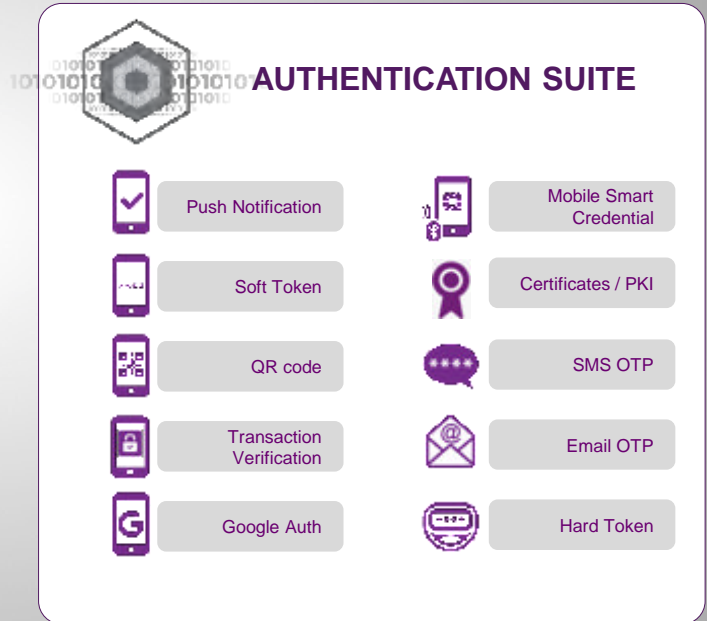
Authenticators to meet the needs
across use cases, user preferences

Fall back authentication when
primary authenticator fails /
unavailable

- SMS OTP, Email OTP

Mobile Software Dev Kits

- embed trusted identities into mobile
apps



什么是SSL? SECURE SOCKET LAYER

SSL — 标准的信息安全技术，在浏览器与服务器之间提供电子身份认证及加密数据

网络安全面临的问题

- 如何为网站访问者提供身份及数据加密服务?
- 如何保护服务器之间数据传输?
- 如何确保数据安全传输?

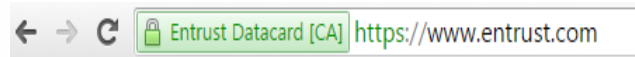
SSL 针对上述问题的解决方案

- 身份：对服务器及设备提供身份认证
- 隐私：提供加密服务

经SSL加密后展示



HTTPS://



SSL 证书

数据加密

Domain Validation
域名验证

DV



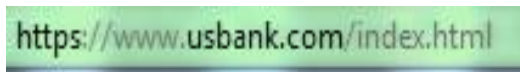
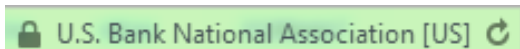
Organizational
Validation
组织机构验证

OV



Extended Validation
增强型验证

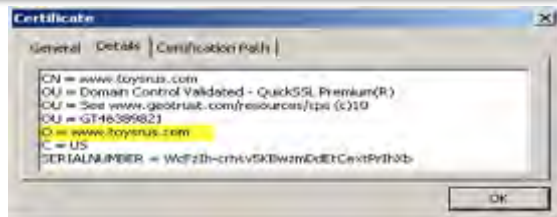
EV



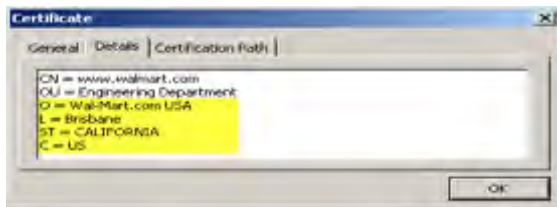
&

网络身份认证

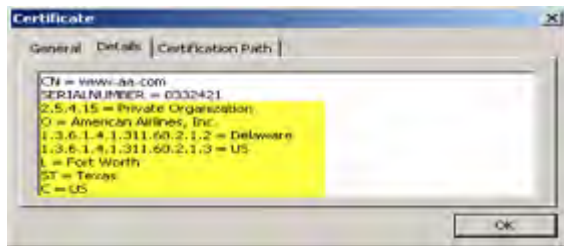
低



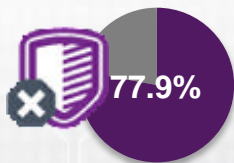
中



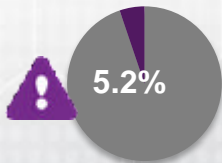
高



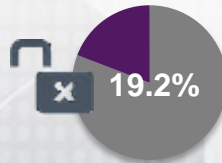
无处不在的安全隐患



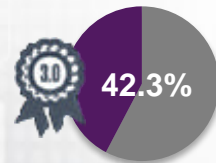
77.9% 的网站仍在使用HTTP



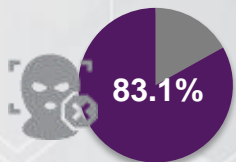
5.2% 的网站拥有不完整的证书链



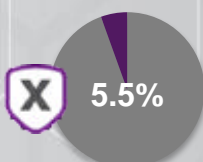
19.2% 仍然支持脆弱/不安全的加密网站



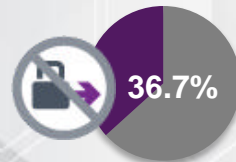
42.3% 的网站仍支持SSL 3.0



83.1% 的主动攻击来自于“心脏流血”



5.5% 容易受到CRIME 的攻击



36.7% 不支持Forward Secrecy

<https://www.trustworthyinternet.org/ssl-pulse/>

攻击、漏洞频现



Heartbleed

- Exploit of Heartbeat extension in OpenSSL 1.0.1. (widely used in web servers, O/S's) - Anything with OpenSSL is vulnerable

Fix:

- Update your version of OpenSSL
- Replace any keys and certificates on those machines
- Ask users to change passwords

Remaining vulnerabilities:

- Many certificates replaced without replacing keys!!



POODLE

- Padding Oracle On Downgraded Legacy Encryption
- Attacker can downgrade SSL/TLS session

Fix:

- Stop supporting SSL 3.0 (Browsers already doing this)
- Patch servers to avoid TLS vulnerabilities

Remaining vulnerabilities:

- Check your server at entrust.ssllabs.com



DROWN

- ***Decrypting RSA using Obsolete and Weakened eNcryption***
- Adapts an old SSLv2 vulnerability
- Can be used against any TLS protocol with same RSA key

Fix:

- *SSL v2 needs to be disabled everywhere, without exception.* But, this has always been the case, given that we've known about the various SSL v2 vulnerabilities for more than 20 years now



FREAK

- Factoring RSA Export (Android) Keys
- A MITM attack that forces browser to use weaker encryption key, providing attacker access to all encrypted info
- Result of US gov't policy preventing stronger encryption from being exported

Fix:

- At server, disable support for insecure ciphers
- Check your server at entrust.ssllabs.com

Remaining vulnerabilities:

- 36% of servers still accept "export grade crypto"

SSL 数字证书应用场景



信用卡在线交易



LOGIN

系统登录



任何线上敏感信息
接入入口



邮箱接入



虚拟桌面登录



基于Https 及FTP的
网络文件传输服务



云、移动应用



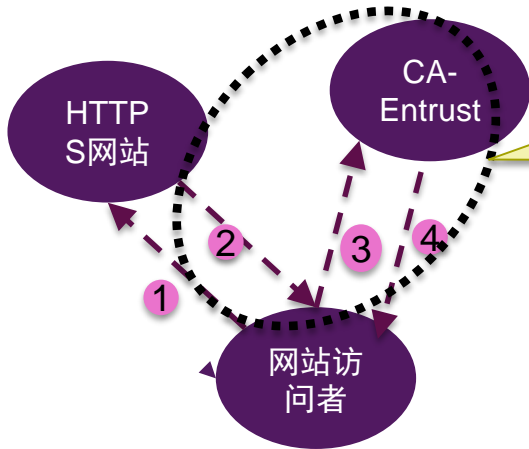
内网通信
(如networks,
文件共享, 等)



VPN登录

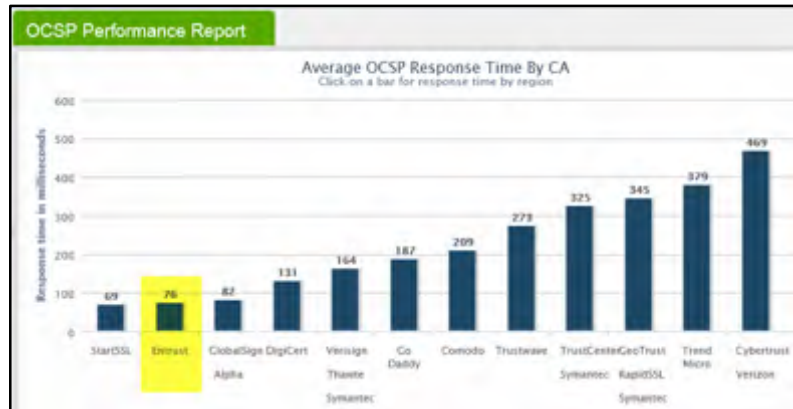


网站反馈速度的重要性



- Entrust 完成网站认证只需不到 80 毫秒
- 大多数服务商需要200多毫秒
- 直接对访问速度和易用性造成影响

1. 访问者点击要访问的网站
2. 网站回吐证书，浏览器对证书的有效性及相关证书是否可信进行校验
3. 浏览器向CA中心对证书吊销状态进行检查
4. CA向浏览器反馈Yes/No 值
5. 完成整个验证流程



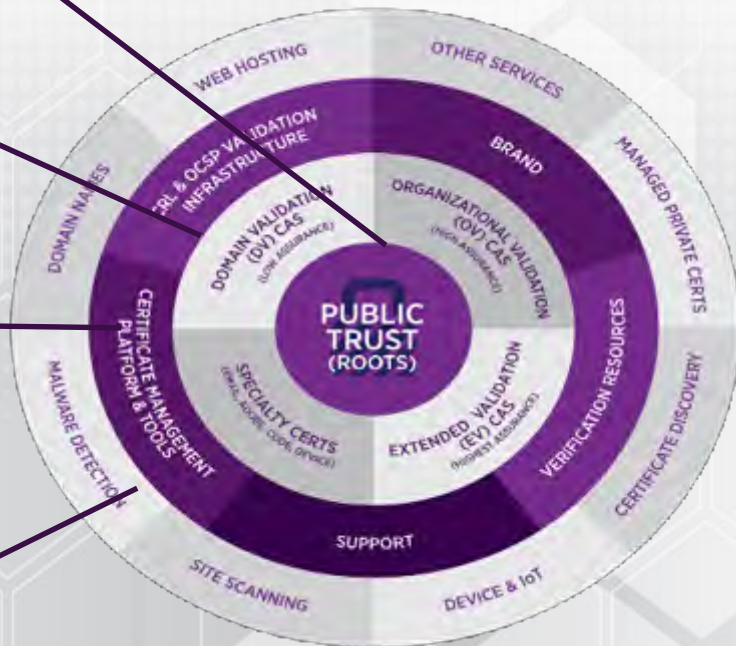
ENTRUST SSL 核心价值

全球可信的根证书服务商
广泛根内置

SSL证书类型
提供 OV、EV、DV 证书

与众不同的Cloud服务平台
提供多类自助服务
实现自动化鉴证

集成Discovery服务
免费网站安全服务包
提供CT（证书透明）服务



ENTRUST CLOUD证书类型

SSL 类证书

DV SSL 证书

标准版(单域名)
优选版(双域名)
通配符
多域名
私有型SSL

Entrust网站签章

普通型网站附加安全包
增强型网站附加安全包

EV SSL 证书

EV 多域名, 最多可扩展250个域名

Entrust/SSL Labs

网站 配置测试

电子签名类证书

代码签名证书

普通代码签名
EV代码签名

文件签名证书

个人型
部门型
企业增强型

用户类证书

安全邮件证书

个人版
企业版

设备类证书

Mobile Device
Certs

Entrust 证书搜索和证书管理系统

Entrust Discovery

商业问题

Application Outages
(due to unexpected expiry of certificates)

Compliance Concerns
(due to inability to inventory certificate population)

Complexity of Certificate Management
(due to certificates from multiple sources)

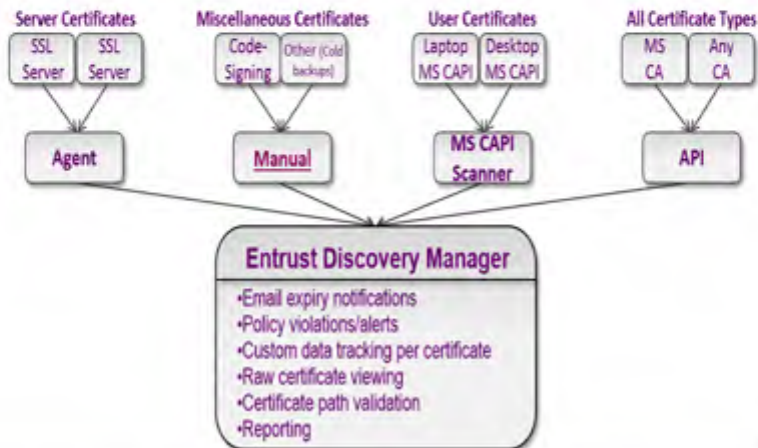
Discovery — 最好的解决方案

Scan your network for certificates

- from any vendor
- any type
- public or private

Manage all your certificates

- Multi-person, multi-level email notifications
- Policy management
- Custom tracking data w/ auto-population rules



什么是证书透明 (CT/CERTIFICATE TRANSPARENCY) ?

- Google mandate intended to make certificates transparent by enabling anyone to inspect CT logs
- Required for all CA's on EV certificates in January 2015
- Required for all CA's on OV/DV certificates in April 2018
- If a CA doesn't support CT for an EV certificate, it loses the special UI treatment that EV certificates get in the Google Chrome browser, effectively downgrading the certificate in Chrome.
- Google has imposed full CT on some other CA's due to mis-issuance



HOW DOES IT WORK?

CA AUTHORIZATION

*“**Certification Authority Authorization (CAA)** allows a domain owner to specify in their DNS or DNSSEC which Certification Authority (CA) is authorized to issue certificates to their domain”*

- CA/Browser Forum Policy effective Sept 8, 2017
- DNS/DNSSEC specifies which CA's are authorized to issue for that specific domain
 - Optional for web site owners
 - Becoming mandatory for CA's to check/respect CAA Policy
- Intended to prevent mis-issuance
 - pre-issue prevention, vs CT which is post-issue audit

<https://www.entrust.com/new-mandatory-caa-checking-horizon/>

CA AUTHORIZATION

- CAA supported properties
 - Issue: Permits a CA to issue certificates
 - Issuwild: Permits a CA to issue Wildcard, but not non-Wildcard
 - IODEF: Provides an email where CA can report violating requests
- Response...
 - No CAA record, CA can issue
 - CAA record uses that CA's Issuer Domain Name from CPS, CA can issue
 - CAA record does not contain CA's Issuer Domain Name from CPS, CA MUST not issue
- If planning to use CAA, ensure ALL allowed CA's are in CAA record, or it will prevent certificate issuance

<https://www.entrust.com/new-mandatory-cao-checking-horizon/>

CERTIFICATE LIFETIMES

- In 2012: 5 year certificates
- In 2015: Reduced to 39 months (EV at 27 months)
- In 2018: SSL Certificate Lifetimes reduced to 27 months (all types)
 - ***Effective March 1, 2018***
 - 825 days for computational ease
 - As determined for CA/Browser Forum, governing body
 - Previous ballot (Google) to reduce lifetimes to 13 months failed

ENTRUST DATACARD

- 成立于1969年，1997年在中国设立直属服务机构
- 全世界 2,000 多名员工，在 150 多个国家进行销售，提供服务和
支持
- 我们在中国致力于本地化生产，并已建立符合国家有关部门需求
以及符合资质的生产基地
- 我们与中国的业务伙伴及机关合作机构大力推行本地化优质高效
的解决方案，更好服务于中国客户

在“支付”和“身份”
认证领域，每天签发的
凭证量为千万级

年交易处理量
超过十亿条



市场聚焦——可信身份及安全数据传输

主要市场

电子支付



信息安全

主要客户群体



消费者

Revolutionize the
Consumer Experience



居民

Enhance Citizen
Satisfaction & Security



企业

Streamline Access
Anytime, Anywhere

FOCUS AREAS

Trusted Identities | Secure Transactions



ENTRUST 产品线

身份 & 权限 管理

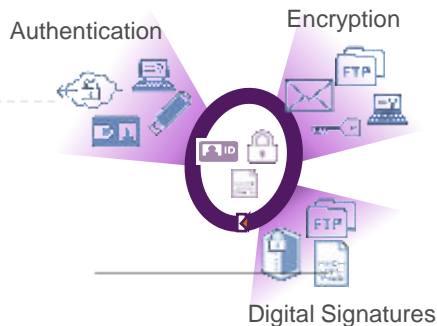


Entrust GetAccess Web access control and single sign-on for online transactions

Entrust IdentityGuard Extensible software authentication platform for mobile, cloud and physical and logical environments

Entrust TransactionShield Transaction monitoring, fraud detection, behavior and identity analytics

Public Key Infrastructure (PKI)



Entrust Authority PKI Certification Authority; digital certificate issuance

Entrust Intelligence Secure, encrypted file sharing and communication



Entrust 云证书服务



ENTRUST DATACARD 全球众多客户的信赖之选

- 17 of top 22 Global e-Governments
- 7 of top 10 Global Commercial Savings Banks
- 8 of top 10 Global Telecom Companies
- 7 of top 10 Global Pharmaceuticals
- 8 of top 10 Global Aerospace & Defence
- 4 of top 5 Global Petroleum





Thank you

