用PKI技术来保障中国互联网的安全

演讲人：王高华

职务： 沃通电子认证服务有限公司 CTO

日期： 2014年9月24日

议题

一、中国互联网安全吗？ -- 非常不安全！

二、什么是PKI技术？

三、PKI技术在国外互联网的应用情况

四、PKI技术如何保障互联网的安全可信

五、PKI技术如何保证云计算的可信安全

六、PKI技术典型应用举例

七、小结

八、附：关于沃通CA

一、中国互联网安全吗？ - 非常不安全！

互联网安全的范围和范畴都非常大，涉及到方方面面。

本人的演讲从分析我国互联网是否已经广泛采用PKI技术来评估中国互联网是否安全。

主要从以下两个方面的问题来分析：

问题一： 几乎所有最重要系统都是部署国外CA签发的SSL证书

问题二： 90%以上的各种重要系统都没有部署SSL证书

得出结论：中国互联网非常不安全！

结论依据？TBC-->

一、中国互联网安全吗？ - 非常不安全！

技术依据：公钥基础设施(PKI)技术，是互联网安全基础技术

理论依据：木桶理论

推理依据：PKI技术是互联网安全的“底板”

问题一”都用国外的”：暴露了底板是人家的，人家可以随时拿走

问题二“都不用”：暴露了根本就没有底板

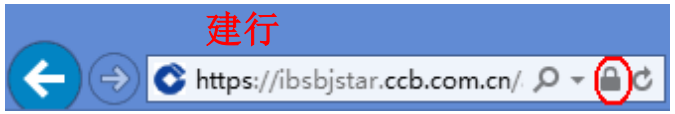
没有底板的木桶是无法装水的 – 常识，小孩都知道！

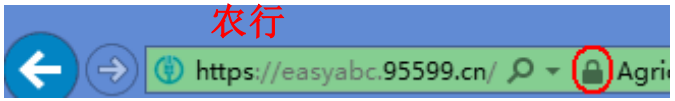
中国互联网安全的现状就是无底板的木桶，都是“裸奔”，

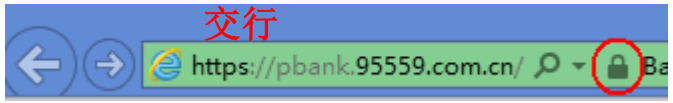
但许多人都不知道！

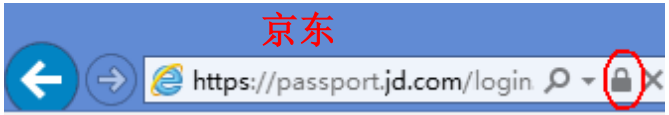
一、中国互联网安全吗？ - 非常不安全！

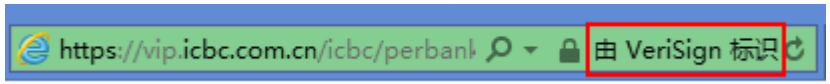
1. 几乎所有最重要系统(网银、支付、电商网站等)都是部署国外CA签发的SSL证书











一、中国互联网安全吗？ - 非常不安全！

ISC 2014

1. 几乎所有最重要系统(网银、支付、电商网站等)都是部署国外CA签发的SSL证书

去年双11节一天淘宝天猫交易额达到331亿元，2013年我国电子商务交易总额超过10万亿元，而这些交易的账户登录和支付时所用的加密证书都是国外CA签发的。服务器证书是可以被吊销的，只要国外CA一点鼠标吊销这些证书，就瞬间所有交易都终止！交易系统瘫痪、网银系统瘫痪，可能导致国家金融系统不稳定，甚至直接危害到国家安全！

这就是“没有网络安全，就没有国家安全！”的随时都有可能发生的实例！

一、中国互联网安全吗？ - 非常不安全！

1. 几乎所有最重要系统(网银、支付、电商网站等)都是部署美国CA签发的SSL证书

非常不安全的主要风险有：

(1) 服务器证书是可以被吊销的，如果由于特殊原因而导致国外CA吊销了这些重要系统 的服务器证书，则几乎整个中国的网银系统都瘫痪，电商系统都会瘫痪，轻则影响用户的使用，严重情况将影响到国家金融系统稳定，甚至是影响到国家安全！

(2) 如果发生海底光缆意外断裂(2007年就发生过)，中国用户访问不了美国互联网的话，则使用国外CA颁发的证书的各种重要系统一样无法正常使用，因为证书正常使用的前提是能访问国外CA的证书吊销列表服务器，必须在验证证书没有被吊销后才能正常显示安全锁标志。

(3) 目前，所有中国用户访问网银系统的访问信息，如什么时候访问、从哪里访问、IP地址和使用什么浏览器、每日有多少次访问中国银行的网银系统、多少次访问支付宝和淘宝网，这些重要的机密信息都完全掌握在国外CA的手中！这也是非常危险的！

一、中国互联网安全吗？ - 非常不安全！

2. 90%以上的各种重要系统都没有部署SSL证书

我国的电子政务网站几乎100%没有部署保证网站机密信息安全的服务器证书，电子商务网站90%以上没有部署证书，几乎所有邮件系统都没有部署SSL证书和使用客户端证书来加密邮件。

也就是说：这些重要的电子政务系统和电子商务系统中的重要机密信息都是明文传输的，都可以毫不费力地被偷走并且是明文，无需费力去解密！

某知名企业的邮件被国外安全部门窃取就是实例，如果用证书加密邮件，则偷走也没用！

结论：这些中国互联网的重要组成部分的系统的不安全就是中国互联网不安全！

一、中国互联网安全吗？ - 非常不安全！

2. 90%以上的各种重要系统都没有部署SSL证书

各种移动APP中90%以上的通信连接都没有采用https加密传输用户提交的机密信息，其中包括银行的移动网银APP和各种社交APP等。而这些裸奔的APP估计有50%以上是在各种免费WIFI上运行！

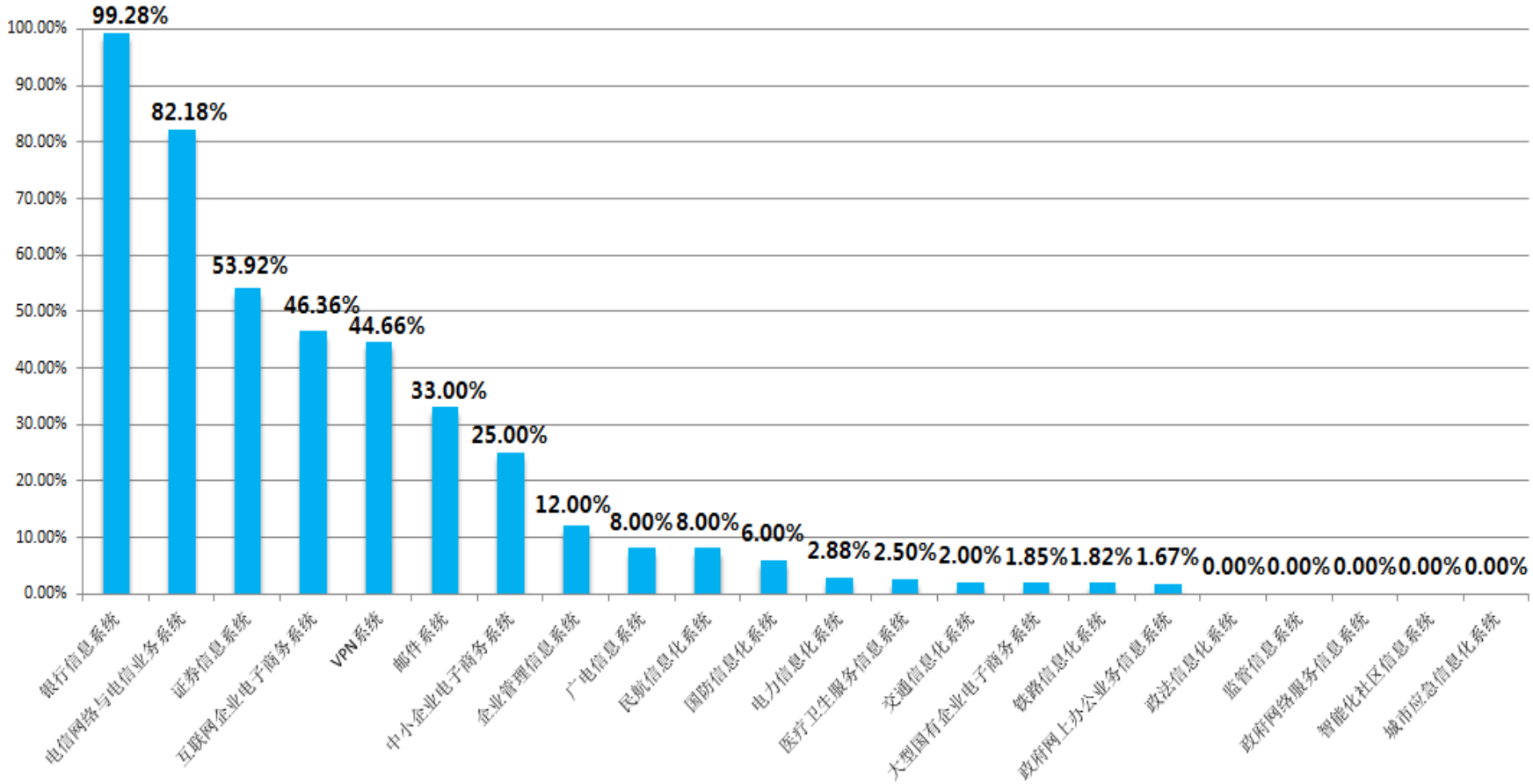
由此可见，各种移动应用包括移动支付的安全问题也是非常严峻的！

结论：这些重要的移动APP的不安全就是中国互联网不安全！

一、中国互联网安全吗？ - 非常不安全！

ISC 2014

我国各行各业的服务器证书部署情况

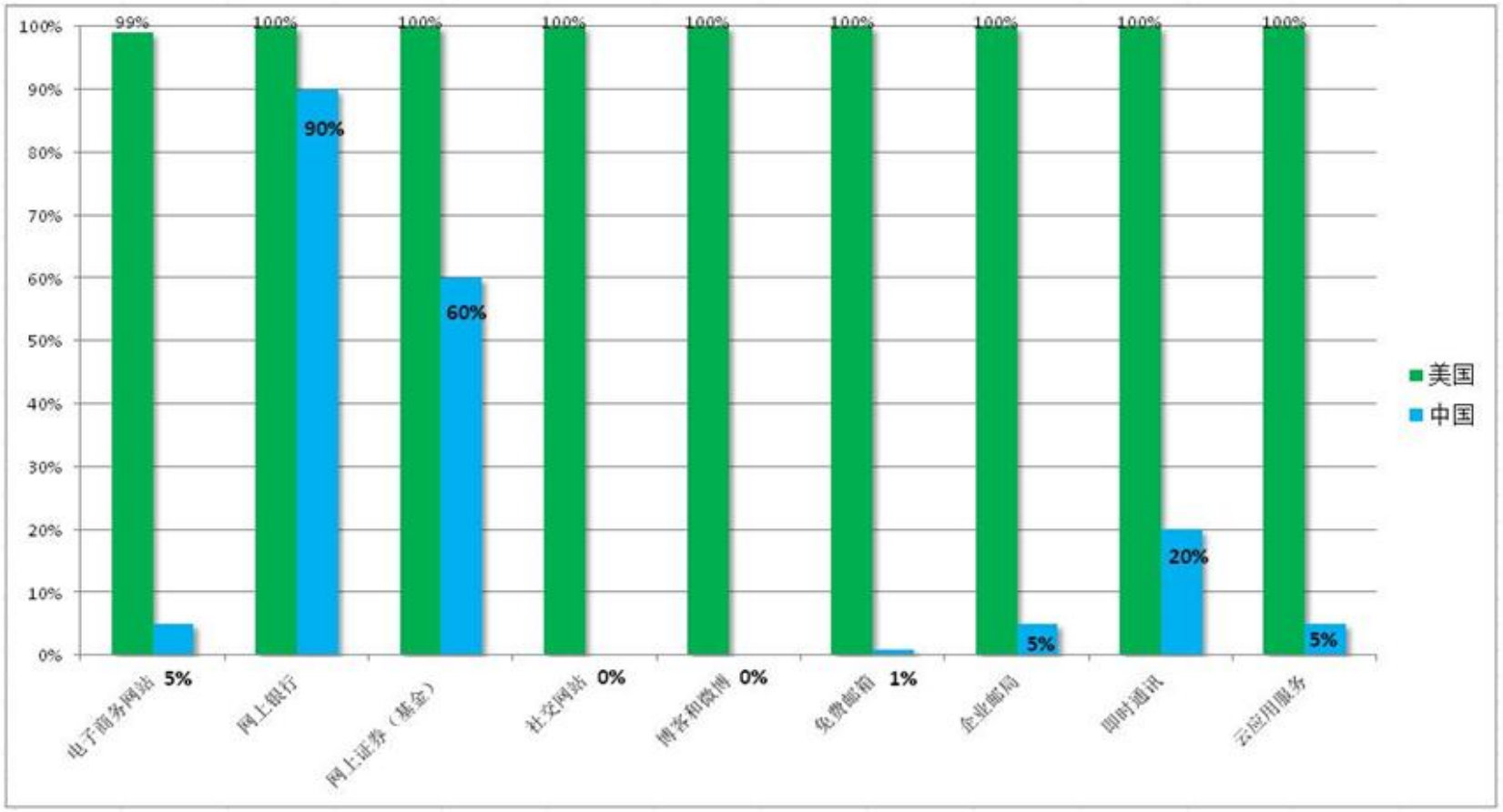


一、中国互联网安全吗？ - 非常不安全！

ISC 2014

中国和美国部署https的对比

中国的互联网还缺什么？缺公钥基础设施(PKI)的广泛部署应用！



一、中国互联网安全吗？ - 非常不安全！

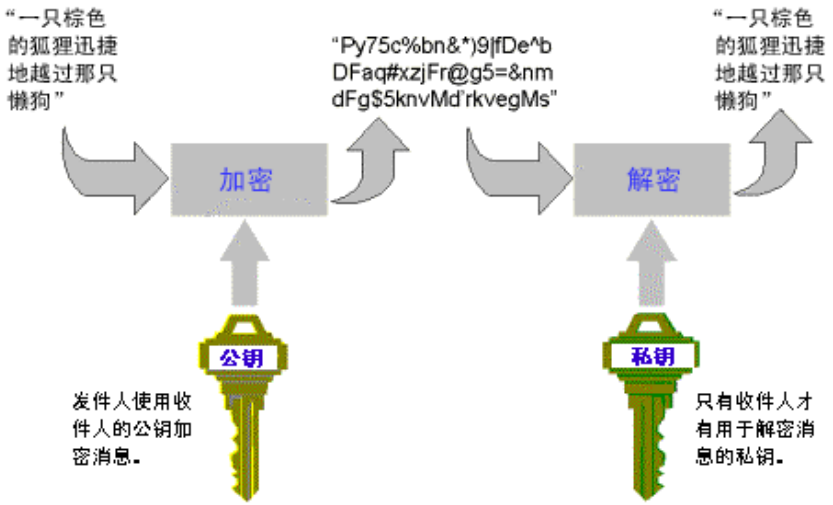
3. 许多重要的系统部署了浏览器不信任的自签证书 – 非常不安全！

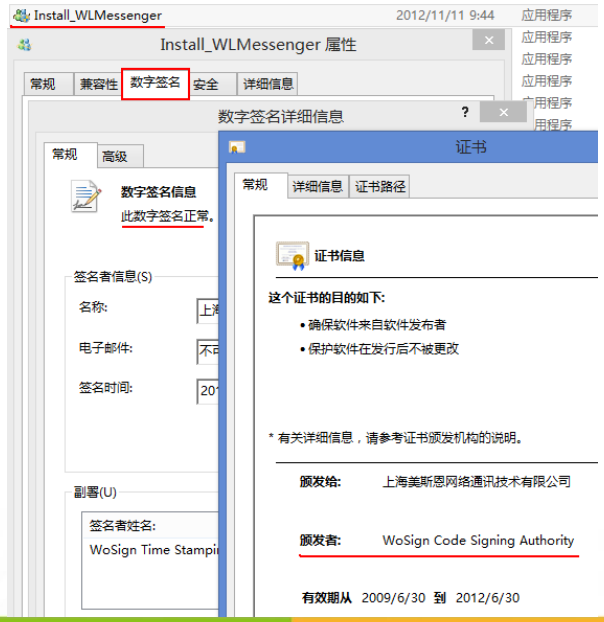
这些系统当然比不部署证书的系统安全，但是如果用户都习惯了即使浏览器不信任也继续浏览的话，这就帮了欺诈网站和假冒网站，因为假冒网站往往由于拿不到全球信任的证书而采用自签证书，浏览器会有安全警告，但由于用户已经养成了继续浏览的习惯而上当受骗！

值得一提的是：目前许多高校正在不断“培养”学生养成这种不安全的习惯！

二、什么是PKI技术？

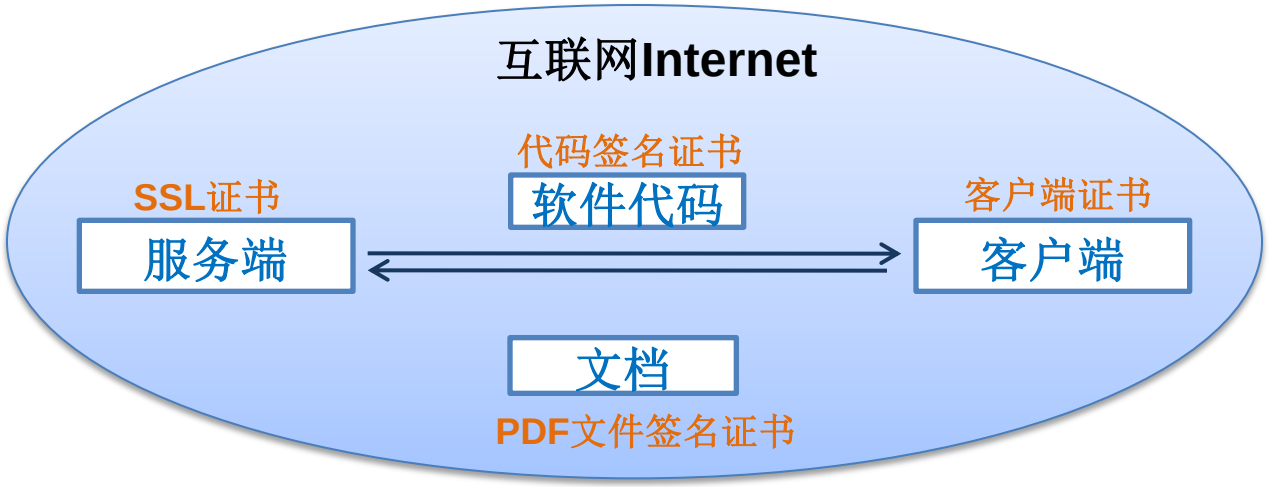
- PKI (Public Key Infrastructure，公钥基础设施)，是保障互联网安全的唯一可靠技术。
- 数字证书(公钥和私钥，加密算法和摘要算法)、证书颁发机构(CA)、证书链(受信任的根证书颁发机构-中级根证书颁发机构-用户证书)、证书管理(申请、颁发、吊销、重新颁发、续期)。
- 数字证书主要用途：加密与解密、身份认证与数字签名。

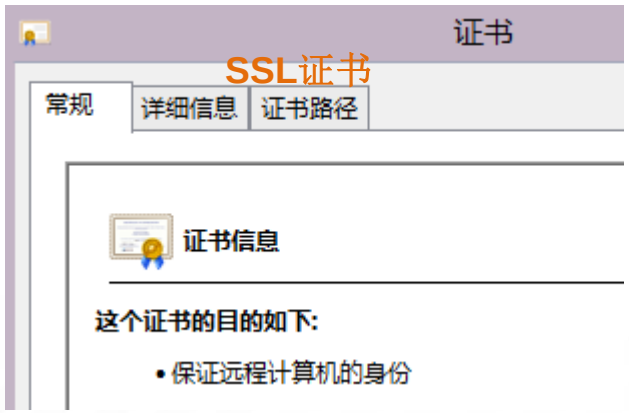




二、什么是PKI技术？

应用PKI技术的数字证书产品主要有三大类，确保互联网安全可信：





二、什么是PKI技术？

应用PKI技术的数字证书产品主要有三大类，确保互联网安全可信：

- **SSL**证书(服务器端): (1) 确保从用户浏览器到服务器之间传输的信息自动加密，防止非法篡改和非法窃取; (2) 确保服务器的真实身份。推荐显示绿色地址栏的EV SSL证书：
- 代码签名证书：(1) 确保软件代码在通过互联网或移动互联网发布时不会被非法篡改; (2) 让用户确信此代码的真实来源。
- 客户端证书：(1) 电子邮件的数字签名与加密，确保电子邮件信息的自动加密，防止非法篡改和非法窃取; (2) 确保客户端的真实身份用于强身份认证和数字签名。(3) PDF文件的数字签名与加密，确保机密文件的安全。

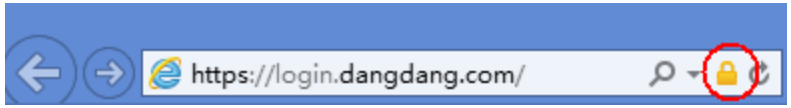
二、什么是PKI技术？

什么是浏览器信任的数字证书？

简单讲：当您用IE浏览器https访问某个网站时浏览器地址栏能正常显示安全锁标识，则表明此证书是浏览器信任的证书。

在IE浏览器中有一个“受信任的根证书颁发机构”列表，列出了全球通过微软认证的所有根证书。

中国有4家公司的根证书已经位列其中。



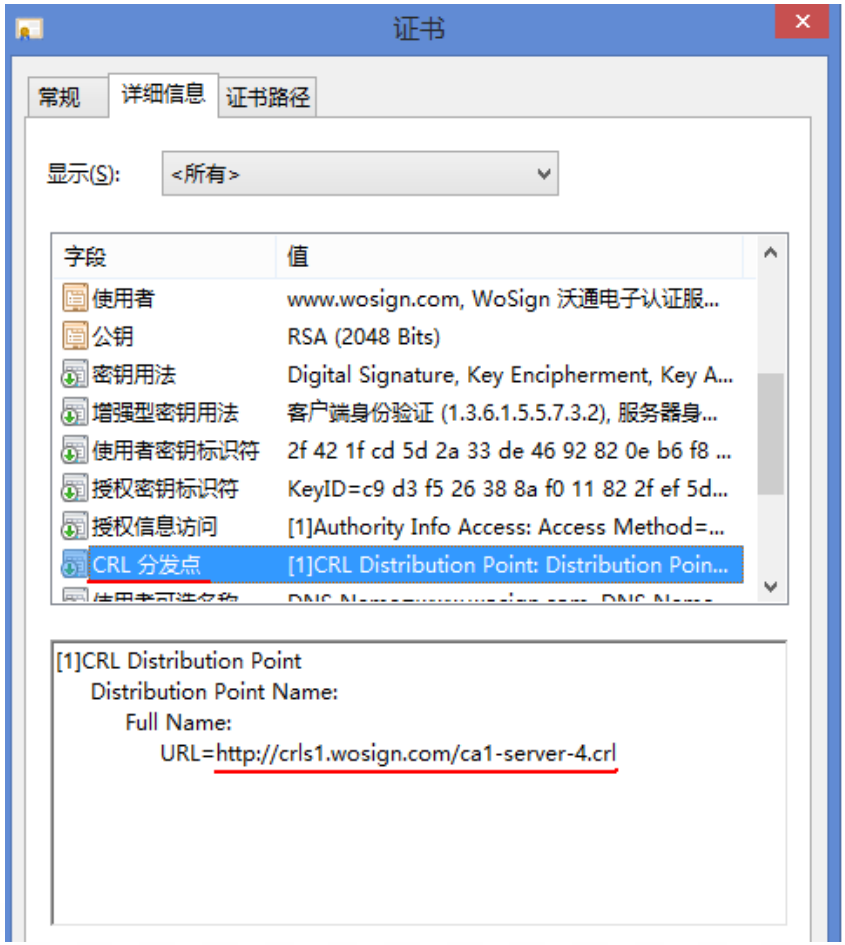
二、什么是PKI技术？

什么是证书吊销列表(CRL)？

- 是由证书签发机构发布的用于查询证书吊销状态的数据库；
- 如果某张证书的序列号被列入此数据库，则表明此张证书已经被吊销，则浏览器/服务器等软件和各种系统将不在信任此证书。浏览器会断开与服务器的连接。

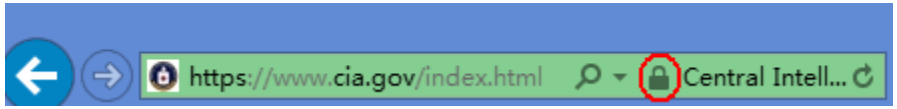
只有在用户的私钥丢失或怀疑被窃时，用户向证书颁发机构申请吊销此证书，CA在核实此申请后会吊销此证书，把此证书的序列号发布到证书吊销列表服务器上供浏览器查询。

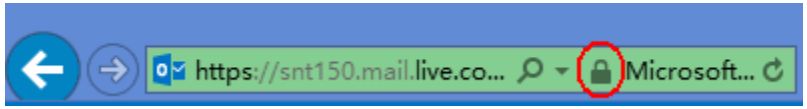
浏览器在显示安全锁标识之前必须到吊销列表服务器上查询此证书是否被吊销。证书吊销列表服务器和证书状态在线查询服务器的访问速度将影响用户访问https网站的访问速度！



三、PKI技术在国外互联网的应用情况

1. 欧美互联网：几乎所有电子政务网站和所有电商网站都部署了SSL证书来保证机密信息的安全；著名免费邮件系统（如：Hotmail/Gmail）都部署SSL证书来保证登录和邮件安全，Gmail从2010年就已经实现全站https加密，2014年3月22日： 所有Google IDC之间的Gmail服务器之间的内部数据传输也采用https加密方式。



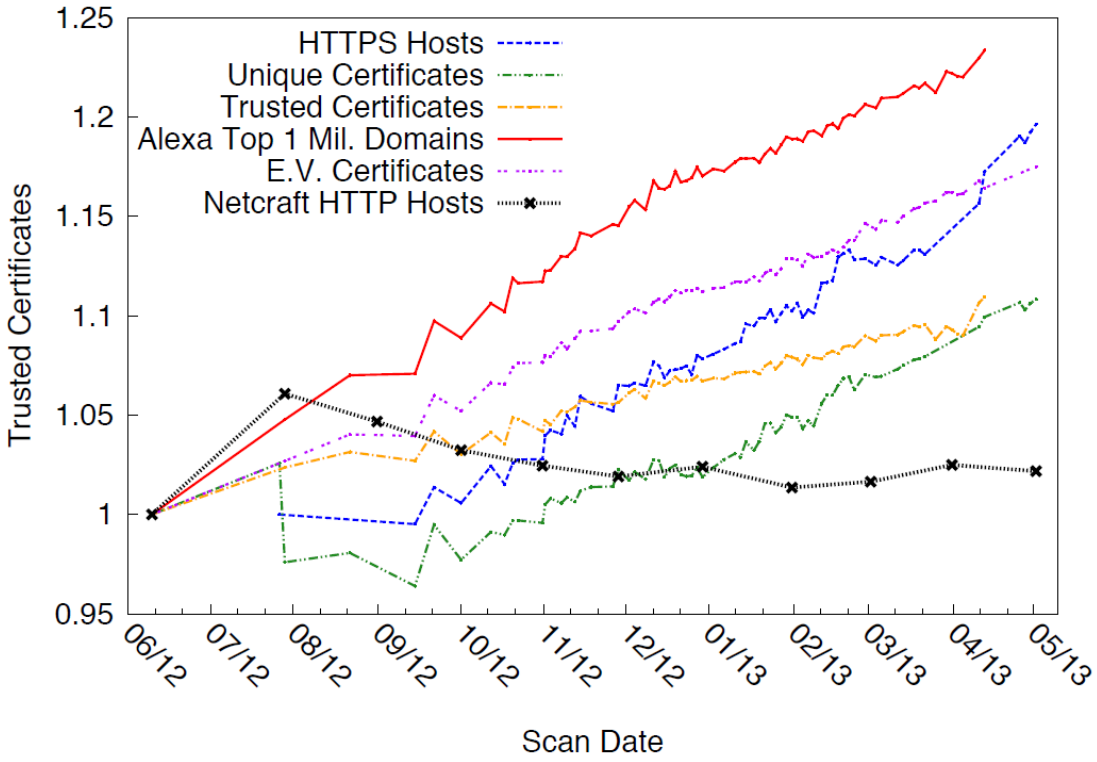


三、PKI技术在国外互联网的应用情况

2. 各大知名网站(如：PayPal, Twitter, Facebook, Gmail, Hotmail等)纷纷采用Always On SSL(**全站https**)技术措施来保证用户机密信息安全和交易安全(防止会话攻击和中间人攻击)，以前仅仅是登录页面采用https。

三、PKI技术在国外互联网的应用情况

3. 密歇根大学的研究人员利用Zmap 工具进行追踪研究后发现，在过去一年时间里，排名前100万名的网站对于https的使用量已经增长了23%左右，而https的整体数量则已经增长了将近20%。而EV SSL证书(绿色地址栏)部署量增长了18%。



三、PKI技术在国外互联网的应用情况

4.德国 (http://www.hb.xinhuanet.com/2014-08/21/c_1112167426.htm)

德国将通过“可信赖的硬软件”打造为“全球第一加密大国”。德国电邮用户发送的信息将使用加密技术传送。所有加密数据信息都将存储在德国境内的数据中心里。德国将鼓励各个企业数据加密，政府给予技术支持。德国国家工作人员的手机配备上，也应逐步加入德国加密芯片。德国将扩大数字安全基础建设，在技术上独立于美国，实现加密技术本土化。

5. 目前国际上已经有包括香港、澳门和台湾在内的25个国家和地区的政府CA根证书已经通过微软认证并预置到Windows中，具体有：奥地利、巴西、芬兰、法国、香港、印度、日本、韩国、拉脱维亚、立陶宛、澳门、墨西哥、葡萄牙、塞尔维亚、斯洛文尼亚、南非、西班牙、瑞典、瑞士、台湾、荷兰、美国、突尼斯、土耳其、乌拉圭。

据了解，25个国家中韩国和印度是采用了国家根模式，并且韩国是采用自己的加密算法SEED，此加密算法已经列入国际标准序列(RFC 4269)，国际领先的Safenet公司的硬件加密设备(HSM)都支持SEED加密算法。

中国已经有4家公司的根证书通过微软认证并预置到Windows中。

四、PKI技术如何保证互联网安全可信

- 鉴于目前各种硬件、软件、操作系统、芯片等无法做到完全国产化的现实，建议国家把**数据加密**列为第一重要大事，所有数据都用证书**加密**了，即使采用国外的产品也可以防止信息泄露！

(1) PKI技术的核心应用之一是“**加密**”。也就是说：为了确保重要机密信息的安全，只有**加密**这些机密信息，才是目前唯一可靠的解决方案，当然，首选采用国产密码算法SM2来加密。

(2) PKI技术的核心应用之二是“**数字签名**”。各种原先是纸质的签名和盖章都可以依据《电子签名法》来使用数字签名来代替，彻底实现网络化、数字化和无纸化！

四、PKI技术如何保证互联网安全可信

具体技术措施有：

(1) 服务器端部署SSL证书来实现传输通道**加密**，确保机密数据传输安全；同时，服务器上机密数据用证书**加密**存储，解密后在https下浏览；

(2)各种代码(PC代码和移动 APP代码)都要有**数字签名**，来保证代码的真实可信身份和防止代码被恶意篡改；

(3)所有电子邮件都必须有**数字签名**来确保邮件的真实身份，含有机密信息的电子邮件都必须用证书**加密**发送；

(4)所有机密文件都必须转换成PDF格式后并用证书**加密**，这些加密后机密文件就算丢在大街上也没有人要！

(5)所有网上提交的材料都必须有**数字签名**，确保网上办事的法律效力和不可抵赖。

(6)所有联网设备都一个可信计算证书，用于证明设备可信身份和**加密**各种数据与各种通信。

五、PKI技术如何保证云计算的可信安全

- EMC信息安全事业部RSA首席技术官Bret Hartman概括云安全领域中的可用技术主要有：一是对身份的保护，二是基础架构的保护，三是对信息的保护。他同时强调了可信云计算，其中云的认证很关键，在访问云服务时，要证明访问人是谁、是否有权限进行访问。

具体技术措施有：

(1) 加密所有通信：服务器部署SSL证书加密所有http通信、加密POP/SMTP/IMAP 和FTP通信等；用客户端证书加密所有电子邮件；

(2) 加密放在云中的所有文件：不是简单的自编算法加密，必须用用户的客户端证书加密各种文件保存在云端，用户下载到自己的电脑用证书私钥解密。这样，用户才放心把机密文件放到云中；

(3) 用客户端证书实现强身份认证登录云服务，能保证用户身份的真实可信；

(4) 用服务器主板中内置的可信计算EK证书来加密用户的文件系统，仅在启动实例时解密；用EK证书签名所有系统文件，在系统运行时验证这些文件，确保系统可信。

五、PKI技术如何保证云计算的可信安全

- 沃通CA提供PKI云服务，让用户无需购置昂贵的 PKI 系统，也无需配备专业的 PKI 技术人才，通过一个 Web 管理界面就能签发所需的各种全球信任的数字证书，包括服务器端 SSL 证书、代码签名证书和客户端证书。
- 沃通CA免费提供基础安全类数字证书，包括SSL证书和客户端证书。
- 沃通CA免费提供API，方便各个系统集成沃通PKI云服务。

推荐的典型应用有：

(1) 为电子邮件客户端软件免费配套提供电子邮件签名和加密证书；

(2) 为各种云平台、统一身份认证平台免费提供客户端证书用于强身份认证；

(3) 为各种需要签名的应用提供符合《电子签名法》的电子签名所需的数字证书和解决方案，并配套提供免费时间戳服务；

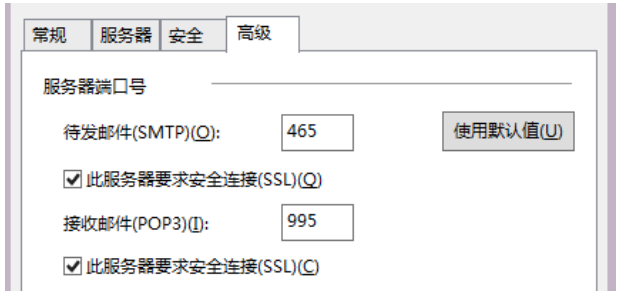
(4) 免费集成沃通PKI云服务，为用户提供一站式数字证书采购服务，为互联网企业带来新的利润增长点，带来更多的用户流量。

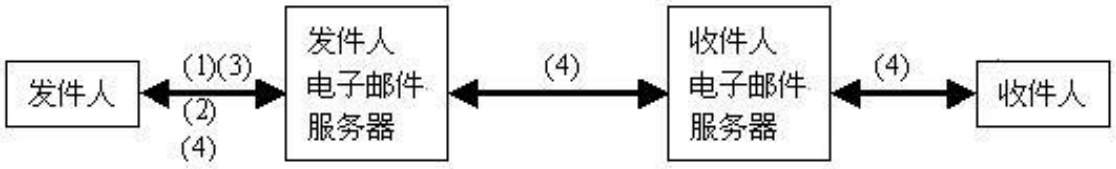
六、PKI技术典型应用举例

- 各种互联网应用系统都部署国产SSL证书来保证各种机密信息安全，防窃取，防篡改！ 最重要的是：要部署国产服务器证书，让中国互联网安全保障权完全掌握 在中国人手中！

六、PKI技术典型应用举例

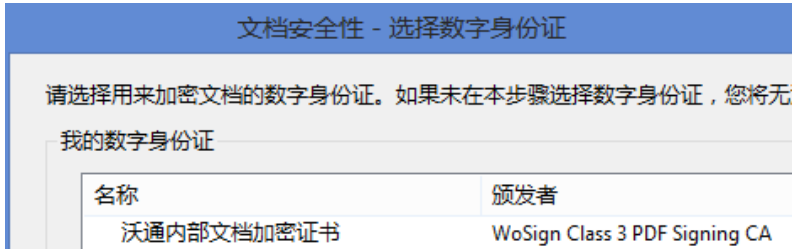
- 电子邮件全程加密



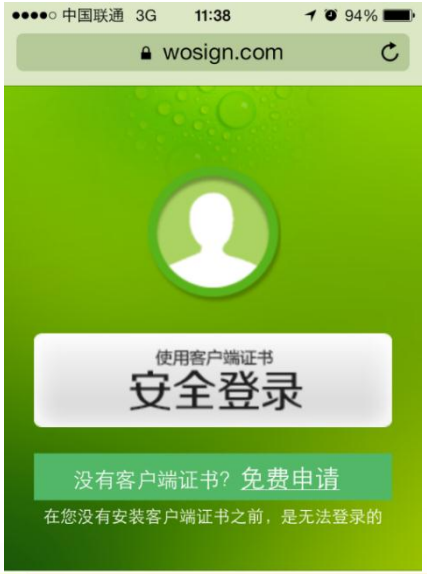


六、PKI技术典型应用举例

- 证书加密用户文件(如：PDF文件用证书加密和数字签名)



- 使用证书实现可靠的强身份认证和不可抵赖的数字签名



- 各种移动应用的https加密传输和用证书实现安全快捷身份认证和登录
- 各种代码都有数字签名来保证软件的真实身份

七、小结

1. 中国互联网非常不安全，理由是：

(1) 几乎所有最重要系统都是部署美国CA签发的SSL证书，一旦被吊销，则所有系统瘫痪；

(2). 90%以上的各种重要系统都没有部署SSL证书，导致各种机密信息泄露。

建议解决方案：

1.应该出台有关政策强制要求关系到金融和民生等最重要信息必须部署国产服务器证书！

2.应该像欧美一样从立法层面强制要求各种含有用户机密信息的系统都必须部署SSL证书来保证用户的机密信息安全！

七、小结

2. 沃通(WoSign)数字证书产品能完全取代国外CA的数字证书产品，以保障中国互联网的信息安全！

- 一样支持所有浏览器和所有设备，但具有更高的性能价格比！便宜一半以上！
- 证书吊销查询速度比国外CA快几十倍！目前每日查询量超过1.5亿次！
- 证书签发速度最快5分钟，国外CA至少要3-5天！
- 平安银行、当当网、苏宁、 1号店、139邮箱等上万个网站系统7年考验，值得信赖！
- 国际/国内双认证，完全国产品牌、安全可控、合规、受我国《电子签名法》保护!

七、小结

3. 沃通(WoSign)10年来一直在为保障中国互联网安全默默做出自己的贡献：

- **用于电子邮件加密的证书完全免费，已经有上百万用户在免费使用，保障其邮件安全；**
- **用于加密网站机密信息的服务器证书中，有一款低端SSL证书完全免费，已经有上万个网站在免费使用，零成本地保障了系统机密信息安全！**
- **免费开放API，零成本地集成各种证书应用！**
- **积极推动全球信任的、采用SM2国产加密算法的SSL证书的部署应用，以保障我国各种重要信息系统的信息安全！**

八、附：关于沃通CA

沃通电子认证服务有限公司(WoSign CA Limited)是同时获得工信部电子认证服务许可证和通过国际认证的全球信任的数字证书颁发机构(CA)，提供基于PKI技术的各种数字证书产品和可信身份认证服务。

沃通(WoSign) 经过将近十年的历练，已经成为国产数字证书技术领导者和市场领先者，始终致力于用PKI技术构建安全可信的互联网环境，推进数字证书的国产化、中文化和国际化。

中文根，沃通造！

八、附：关于沃通CA

- 沃通于2013年8月20日获得国家密码管理局颁发的《电子认证服务密码使用许可证》第0036号; 于2014年3月14日拿到工信部颁发的《电子认证服务许可证》编号：ECP44030514036；
- 沃通是中国唯一一家支持所有终端设备和操作系统、支持所有浏览器和服务器、通过严格的国际审计、拥有全球信任的顶级根证书的CA；
- 沃通是中国第一家 国际CA/浏览器联盟 成员单位;
- 沃通是中国唯一一家通过Adobe认证的CA(PDF签名加密证书);
- 沃通是中国唯一一家拥有1999年创建的全球信任根证书的CA;
- 沃通是全球唯一一家拥有全球信任的中文根证书的CA;
- 沃通是中国唯一一家OCSP日查询量超过一亿次的CA。
- 沃通是中国唯一一家能签发全球信任的SM2算法的SSL证书的CA。


电子认证服务许可证

经审查，深圳市沃通电子认证服务有限公司具备《电子认证服务管理办法》规定的电子认证服务机构条件，特发此证。

许可证编号：ECP44030514036

许可证有效期：2014 年 3 月 14 日至 2019 年 3 月 13 日

发证机关

仅用于沃通资质证明，不得有其他用途！


电子认证服务使用密码许可证

证书编号：0036

深圳市沃通电子商务服务有限公司：

经审查，你单位的电子认证服务系统符合《电子认证服务密码管理办法》的规定，批准使用商用密码。

特发此证。

国家密码管理局

2013 年 8 月 20 日

许可证有效期限：五年

仅用于沃通资质证明，不得有其他用途！

八、附：关于沃通CA

已经有几万家知名网站系统正在使用沃通(WoSign)SSL证书，中国市场占有率超过50%：

为保障中国互联网安全
沃通(WoSign)已经准备好了！

您准备好了？

欢迎访问：www.wosign.com 了解更多详情。

沃通电子认证服务有限公司(WoSign CA Limited)
地址：中国深圳市南山区南海大道1057号科技大厦二期A座502
电话： 0755 – 86008688
网站：www.wosign.com

多谢！
Thanks!

沃通微信

王高华微信