沃通®
WoSign

互联网安全
与
网上隐私保护

WoSign
沃通电子
认证服务
有限公司

数字签名者：WoSign 沃通电子认证服务有限公司
DN：c=CN, st=广东省, l=深圳市, o=WoSign 沃通电子认证服务有限公司, email=wosign@wosign.com, cn=WoSign 沃通电子认证服务有限公司
日期：2015.08.03 14:28:46 +08'00'

王高华 CEO/CTO
沃通电子认证服务有限公司
WoSign CA Limited
2015.07.30

议题

一、我国互联网安全状况很不乐观—非常不安全

二、欧美互联网安全保护措施

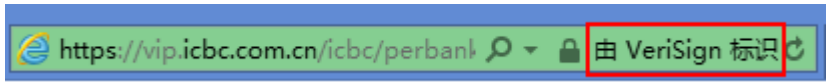
三、PKI技术是保障互联网安全的可靠技术

四、PKI技术发展趋势

五、各种证书应用实例

一、我国互联网安全状况很不乐观 – 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、我国互联网安全状况很不乐观 – 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

这些证书一旦被吊销，整个中国互联网将瘫痪！没有网络安全就没有国家安全！

一、我国互联网安全状况很不乐观 – 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！

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！

一、我国互联网安全状况很不乐观 – 非常不安全

2. 90%以上的各种重要系统都没有部署SSL证书

一、我国互联网安全状况很不乐观 – 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

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！

一、我国互联网安全状况很不乐观 – 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

一、我国互联网安全状况很不乐观 – 非常不安全

4. 各种邮件系统、微信等都没有用证书加密，泄露个人隐私和商业机密

一、我国互联网安全状况很不乐观 – 非常不安全

4. 各种邮件系统、微信等都没有用证书加密，泄露个人隐私和商业机密

一、我国互联网安全状况很不乐观 – 非常不安全

结论：我国互联网非常不安全，随时有可能瘫痪！

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”，但大家都不知道！

二、欧美互联网安全保护措施

- **政府门户网站**：欧美政府门户网站**都**部署SSL证书来保证用户浏览信息安全和保护用户隐私(安全锁标志)，防非法窃取，防非法篡改，防止被假冒。

二、欧美互联网安全保护措施

- **电子政务网站**：欧美**所有**电子政务网站**都**部署SSL证书来保证用户账户安全和系统机密信息安全(有安全锁标志、绿色地址栏)，防非法窃取，防非法篡改，防止被假冒。

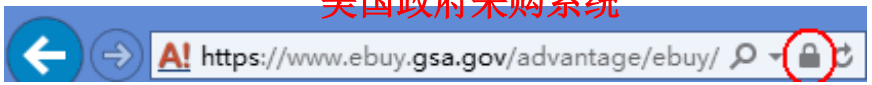
美国佛蒙特州公司注册处

英国公司注册处

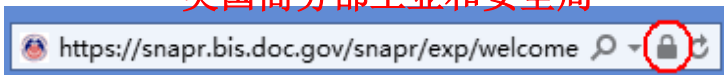
美国中情局

美国国税局

美国政府采购系统



美国商务部工业和安全局

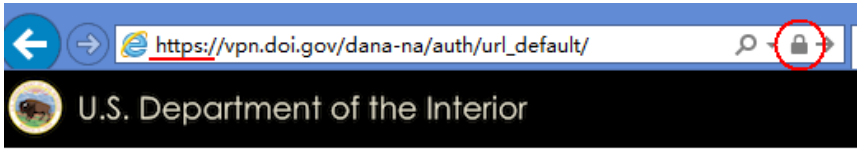


美国社会保障总署

美国联邦电子缴税系统

二、欧美互联网安全保护措施

- **政务VPN**: 美国内政部各部门远程访问系统(VPN)部署SSL证书，确保从外网安全访问内网。



Bureau of Indian Affairs - https://access.doi.gov/bia

Bureau of Indian Education - https://access.doi.gov/bie

Bureau of Land Management - https://access.doi.gov/blm

Bureau of Reclamation - https://access.doi.gov/bor

Fish and Wildlife Service - https://access.doi.gov/fws

Minerals Management Service - https://access.doi.gov/mms

Interior Business Center - https://access.doi.gov/ibc

National Park Service - https://access.doi.gov/nps

Office of Hearings and Appeals - https://access.doi.gov/oha

Office of Historical Trust Accounting - https://access.doi.gov/ohta

Office of the Inspector General - https://access.doi.gov/oig

Office of the Secretary - https://access.doi.gov/os

Office of Surface Mining - https://access.doi.gov/osm

Office of the Special Trustee - https://access.doi.gov/ost

Office of the Solicitor - https://access.doi.gov/sol

U.S. Geological Survey - https://access.doi.gov/usgs

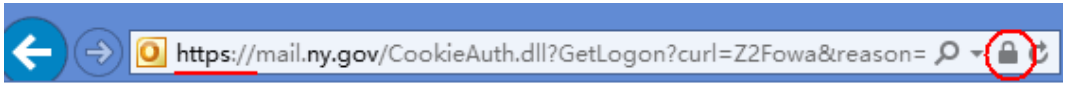
二、欧美互联网安全保护措施

- **政务邮件系统**：美国纽约州政府电子邮件系统都部署SSL证书，确保电子邮件系统安全和用户登录安全，防止邮件泄密和被非法窃取。

NYSeMail Portal Page

Service	NYeNet Access	Internet Access
Outlook Web Access 2007	https://mail.nysemail.nyenet/owa	https://mail.ny.gov/owa
NYSeMail Password Change	https://email.nysemail.nyenet/password	https://email.ny.gov/password

即使是内网(内部域名)，也是有部署SSL证书的

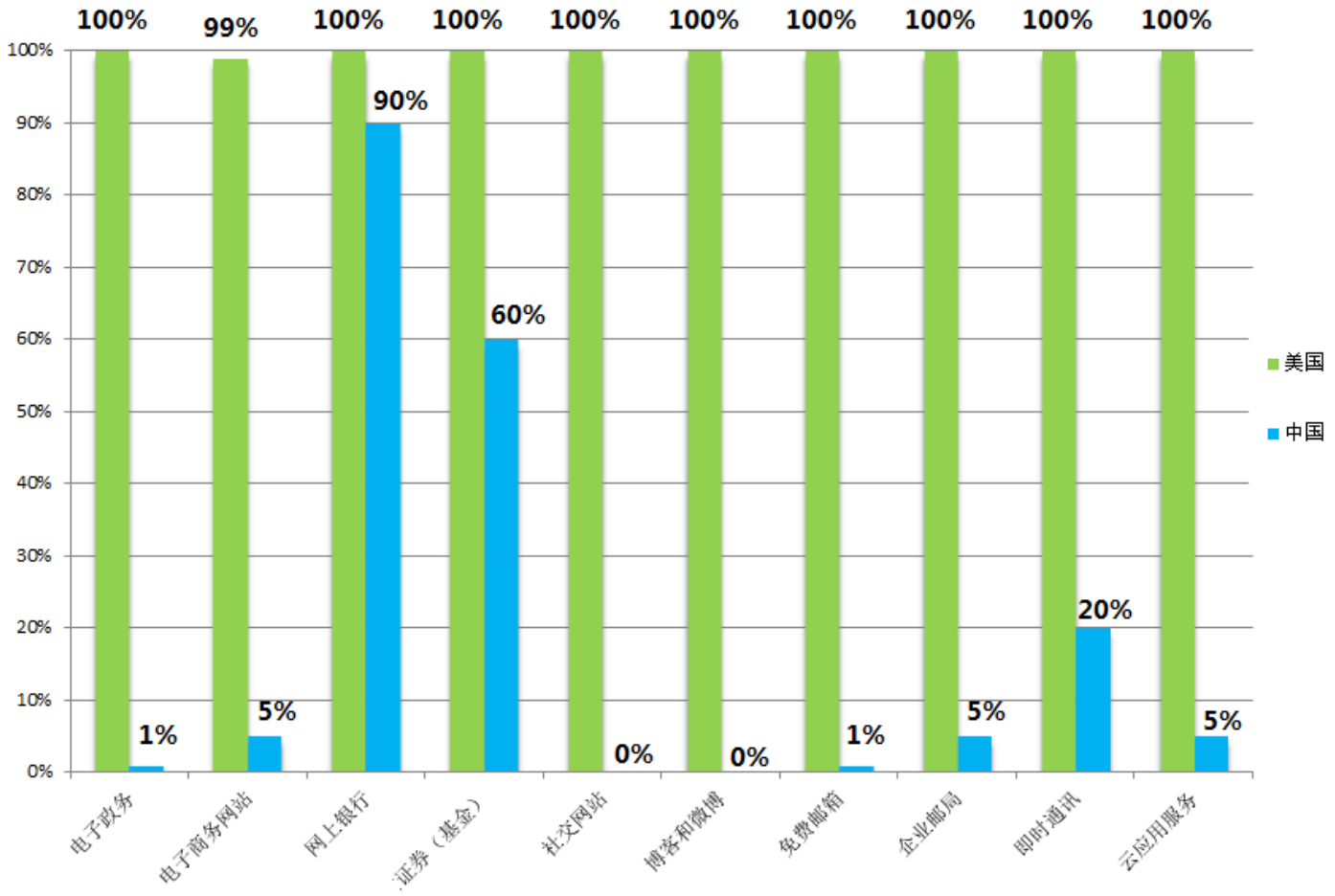


二、欧美互联网安全保护措施

- **全站https**: 美国白宫于6月8日发布了要求所有政府网站都必须在2016年12月31日之前完成全站https加密！这是确保政府网站信息的安全，保护美国公民的网上隐私。

二、欧美互联网安全保护措施

- 欧美几乎100%部署，而我国几乎100%没有部署SSL证书



WHY? 差距咋这么大呢？

- 我国没有专门的网上隐私保护法律法规；
- 我国没有相应的技术指引明确告诉并强制要求网站在用户输入隐私信息必须采取的具体技术措施；
- 美国有许多法律法规要求网站业主必须采用有效的技术措施(https)来保护用户的隐私信息！

- **我国急缺PKI技术人才，通晓国际标准的人才！**

WHY? 差距咋这么大呢？

- 1974年《联邦隐私法》、1986年《电子通信隐私法》、1987年《计算机安全法》(机密信息保护)、1996年《健康险连带责任法案》(卫生保健隐私)、1999年《金融服务现代化法案》(金融用户隐私)、2000年《儿童网上隐私保护法》等等十几部法律法规。
- 许多州都有自己的网上隐私保护法
- 美国在《网络空间可信身份国家战略》中明确指出：NSTIC: 让在线交易更安全、更快捷和**更隐私**。遵循隐私、安全、互通性与易用性四大指导原则。

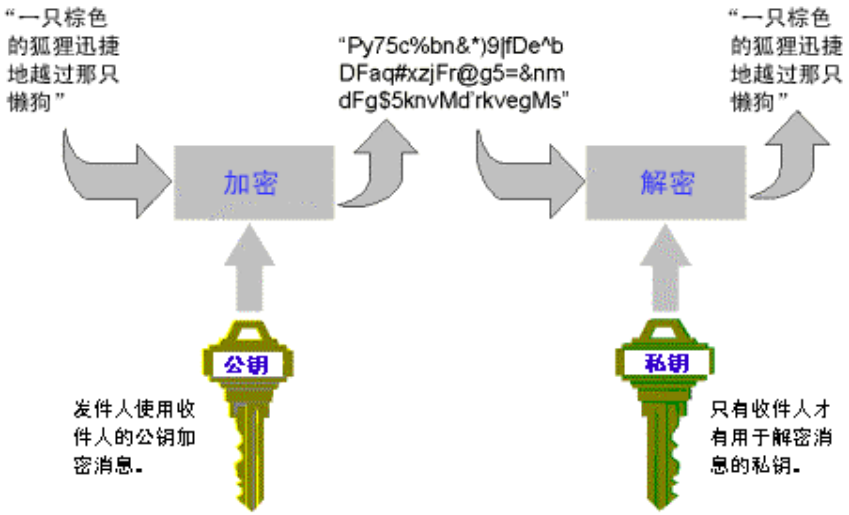
三、PKI技术是保障互联网安全的可靠技术

- PKI (Public Key Infrastructure，公钥基础设施)，是保障互联网安全和保护网上隐私的唯一可靠技术。
- 凡是涉及到用户隐私信息的数据都必须采用PKI技术来加密

  (1) 加密所有通信：所有服务器都部署SSL证书加密所有http通信、加密POP/SMTP/IMAP 和FTP通信等，确保隐私机密数据传输安全；

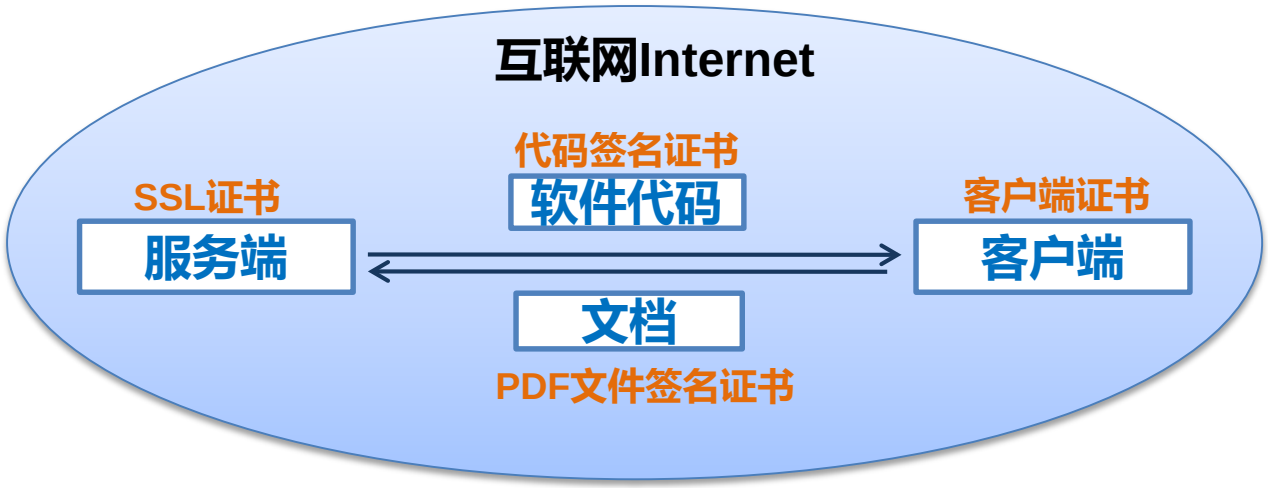
  (2) 所有含有用户隐私信息的电子邮件都必须用证书加密发送；

  (3) 所有机密隐私文件都必须用证书加密存储与传输。



三、PKI技术是保障互联网安全的可靠技术

- 应用PKI技术的3种数字证书产品能确保互联网安全可信，保护用户的隐私信息：



四、PKI技术发展趋势

- 斯诺登事件加速全站https部署，谷歌浏览器将把所有http网站标记为不安全，极力推广全站https。

Google has added a feature to Chrome that can alert users about unencrypted network connections common on many parts of the Web. The feature isn't on by default.

四、PKI技术发展趋势

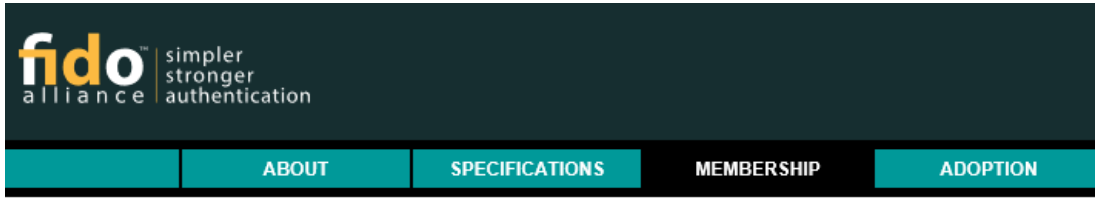
- 国际组织—OTA(在线信任联盟)和EFF(电子前沿基金会)极力推动Always On SSL (全站https)和 https everywhere(普及https)。

四、PKI技术发展趋势

- Mozilla、Akamai、EFF 、思科等将于今年9月份推出免费SSL证书自动化部署工具。

四、PKI技术发展趋势

- 谷歌、微软、高通、三星、阿里巴巴、联想、PayPal、RSA、Visa、MasterCard联合发起FIDO联盟推广实现强身份认证，目的是要让不安全的密码认证消失。



Members:
Bringing together an ecosystem

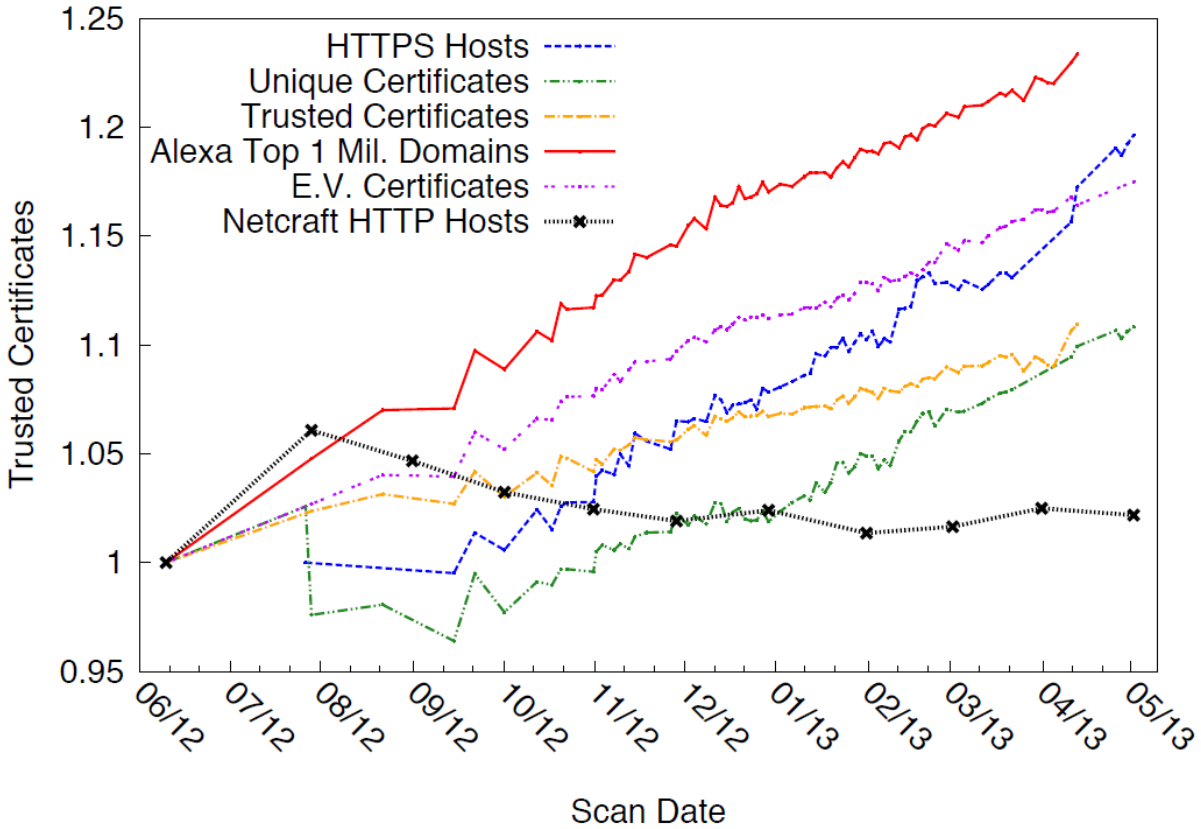
Internet Services | Component & Device Vendors | Software Stacks

四、PKI技术发展趋势

- 各知名网站(如：Twitter、Facebook、Gmail和Hotmail、网银等)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。

四、PKI技术发展趋势

- 密歇根大学研究人员利用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%。



四、PKI技术发展趋势

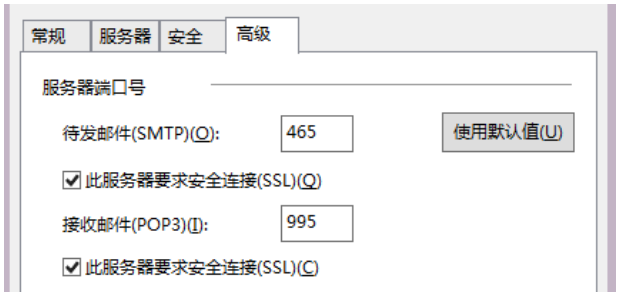
- Startcom、WoSign等全球知名CA纷纷推出完全免费的低端DV SSL证书，大受全球用户的欢迎。全球超过120个国家和地区用户在使用WoSign免费SSL证书。

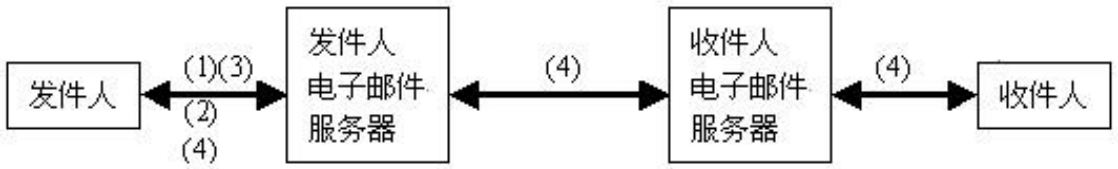
五、各种证书应用实例

- 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！

五、各种证书应用实例

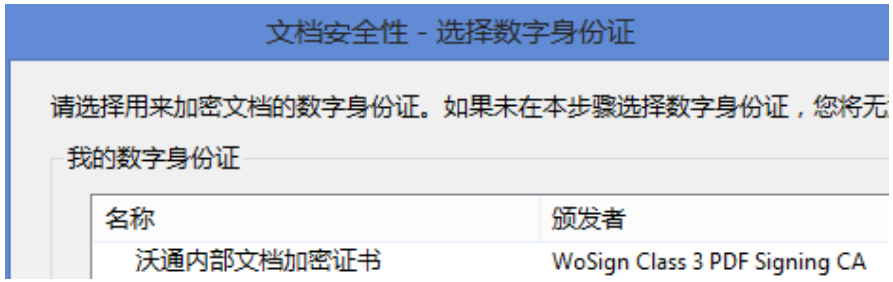
- 电子邮件全程加密



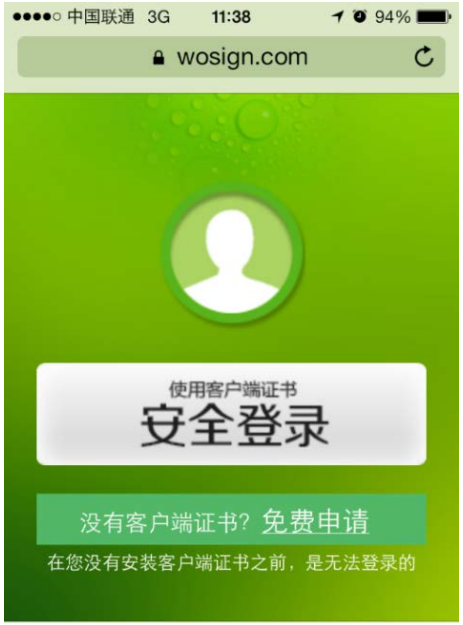


五、各种证书应用实例

- 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

六、结束语

- 我们的生活和工作都需要保护个人隐私和数字资产安全，只有PKI技术才是最可靠的技术来保证隐私机密数据的安全！
- 我国奇缺PKI技术人才，奇缺懂国际标准的PKI人才，奇缺能制定PKI中国标准和国际标准的人才，希望哈工大的同学能在PKI技术领域有所建树。
- **欢迎PKI人才到沃通(WoSign)来工作！**

六、结束语

- 欢迎PKI人才到沃通(WoSign)来工作！
- 沃通(WoSign)，我国唯一一家拥有全球信任的中文根证书、国际标准组织成员单位、中国市场领先的、唯一能完全取代国外证书产品的、拥有工信部CA牌照的民营国家高新技术企业。
- 沃通证书用户覆盖全球超过120个国家和地区，超过10万个网站正在使用沃通证书，是一个名副其实的国际化高科技企业。

多谢！

www.wosign.com