Zhongshan University

电子政务与信息安全

中山大学数据科学与计算机学院
周凡
2018年6月

内容

- 电子政务安全建设中的问题与对策

公钥基础设施PKI简介

公钥基础设施**PKI**技术

1. 电子政务安全建设中存在的问题

目前，中国正处于电子政务建设的前期。关于电子政务的安全，政府有关部门缺少统一的建设标准和规范，电子政务建设的风险评估、效能评估也没有一个完整的依据，诸如技术对策、信息分类、安全域划分、责任主体、应急处理、工程实施等方面还存在这样或那样的问题，这些都需要我们采取必要的对策，应对电子政务安全所面临的挑战。

根据国家计算机网络与信息安全管理中心提供的资料显示，中美黑客大战期间，在遭受美国黑客攻击的我国大陆网站中，政府网站占了41. 5%。也就是说政府网站成为重点攻击对象。对照安全标准来衡量，中央国家部委的涉密网络有一半以上未达到安全保密要求。

电子政务安全建设中存在的问题

1. 与电子政务安全相关的法律法规的滞后和不完善问题日益明显

电子政务的工作内容和工作流程涉及国家核心政务，其安全关系到国家的主权、国家的安全和公众利益，所以电子政务的安全实施和保障，必须以国家法规形式将其固化，形成全国共同遵守的规约，成为电子政务实施和运行的行为准则，成为电子政务国际交往的重要依据，为司法和执法者提供法律依据，对违法、犯法者形成强大的威慑。

2005年4月1日，《中华人民共和国电子签名法》正式实施，规范了电子签名行为，确立电子签名的法律效力，使得电子签名与传统的手写签名和盖章具有同等的法律效力，极大的推动了电子政务和电子商务的发展。

目前，对个人数据（自然人和法人）保护的需求随着电子政务的发展日益明显，因此，加快个人数据保护法的制定是非常必要的。

电子政务安全建设中存在的问题

2. 电子政务安全管理体制尚待建立

- 建立和落实电子政务安全责任制，按照谁主管谁负责、谁运营谁负责的原则，由各主管部门和运营单位负责。
- 制定信息安全策略，规定电子政务系统中各种信息资产（软件、硬件、数据等）所允许的操作行为和不允许的操作行为。
- 建立、健全电子政务安全管理体制，制定自上而下的完善的电子政务安全管理组织体制和管理条例，从立项、招标、采购、设计、实施、运行、监理、服务、培训、管理等各环节保障电子政务系统建设过程的安全。
- 形成完整的、高水平的电子政务安全标准体系。
- 设立专业的安全工程监理单位，协助政府（即用户）与企业寻找电子政务项目建设过程中风险与安全投入的最佳平衡点。

电子政务安全建设中存在的问题

2. 电子政务安全管理体制尚待建立（续）

- 进行信息安全风险评估，有助于政府确定风险状况、风险应对措施，有助于全面掌握信息系统的安全状况。
- 需要协调一致的采购和集成商资质管理政策，安全专用产品的采购除了必须符合国家各方面的相关规定外，还必须选择有中国自主知识产权的安全产品。
- 加强专业人才的培训。
- 建立协调和应急相应机制。

电子政务安全建设中存在的问题

3. 电子政务安全保障技术构架尚待建立

- 缺少电子政务整体技术安全保障构架。技术安全保障构架包括政务内网、外网的安全控制策略；进入互联网的安全服务与控制策略；租用公网干线的安全服务与控制策略；设置政务计算环境的安全服务与机制。
- 缺少电子政务安全基础设施。电子政务安全基础设施包括网络信任基础设施、安全产品评估基础设施和系统安全评估基础设施。
- 加强安全技术和产品的自主研发和创新。由于电子政务设计国家利益，因此，电子政务系统工程的安全保障需要各种有自主知识产权的信息安全技术和产品。

电子政务安全建设中存在的问题

3. 电子政务安全保障技术构架尚待建立（续）

- 网络安全域的划分和控制问题。

国务院办公厅[2002]17号文件对政务内网和政务外网进行了划分，指出：政务内网主要是副省级以上政务部门的办公网，与副省级以下的政务部门的办公网物理隔离。政务外网是政府的业务专网，主要用于运行政务部门面向社会的专业性服务业务和不需在内网上运行的业务。

这样的划分也会带来两方面的问题：一是电子政务内网是按行政级别划分的，而不是按照涉密划分的，这样可能会造成涉密程度的扩大化，增加建设费用，增大保密管理难度；二是有的信息化发展较快的省，网络已经连到地市了。省与地、市两级断开，不利于信息沟通。

2. 中国电子政务安全建设的对策建议

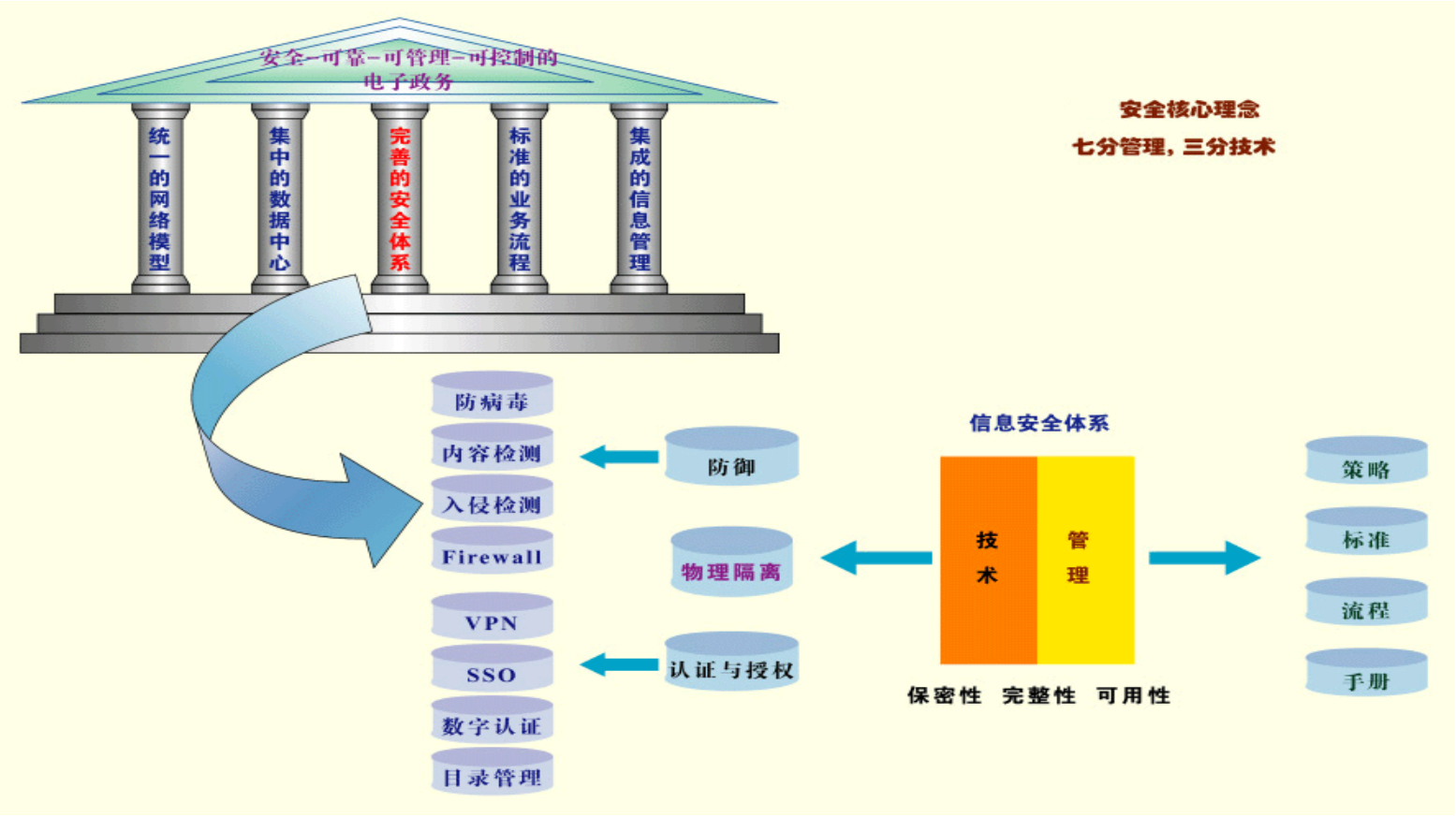
根据对我国电子政务安全建设现存问题的分析，参照国外的经验，我们认为当前急需解决的是确定中国电子政务安全建设的基本思想和指导原则。并以此为根据，对目前存在的问题，分门别类、逐项进行研究，并考虑将来电子政务安全建设、运作，提出一个电子政务安全建设的规范性文件。

规范性文件主要以《国家信息化领导小组关于加强信息安全保障工作的意见》为指南，根据电子政务安全的特点，提出电子政务安全建设的目标、任务，建立、健全电子政务安全的组织管理体制和责任制，对电子政务安全涉及的领域提出意见，保证电子政务安全建设的健康发展。

其次是组织各级有关部门和技术力量，对一些公共技术问题加以研究攻关，如建立全国范围内的电子政务信用认证体系、建立统一的公钥管理、建立各类应急服务中心等。

中国电子政务安全建设的对策建议

安全保证的两大支柱是管理和技术，“七分管理、三分技术”，只有在管理方面明确思路，技术才有用武之地；



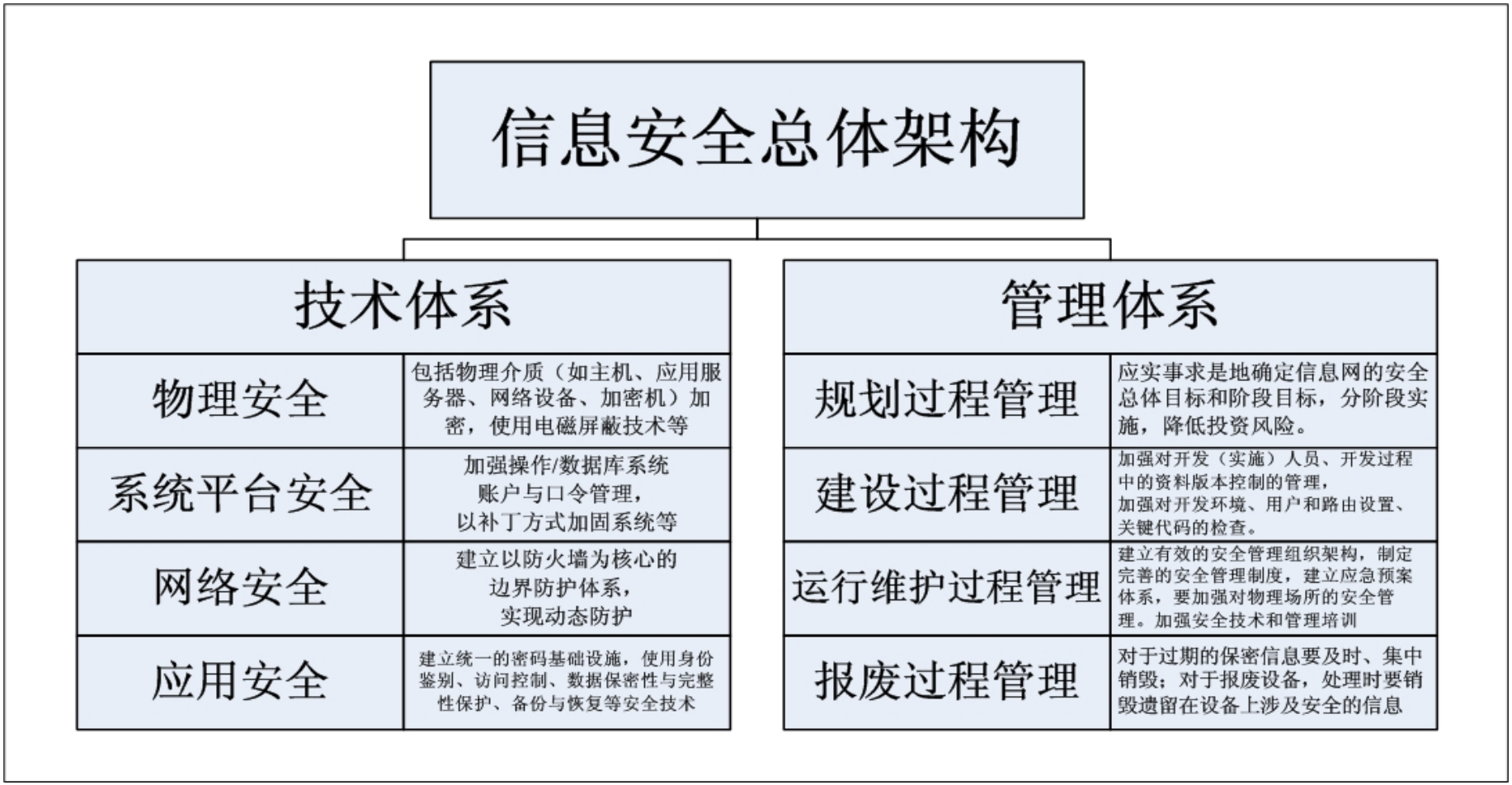
中国电子政务安全建设的对策建议

同时，还要从技术角度对电子政务安全进行合理的划分。安全的电子政务信息系统的建立包括如下三个方面的内容：

- 安全的运行环境，包括安全的环境、安全的网络和安全的系统平台；
- 安全的业务系统，即应用系统安全；
- 安全管理体系，即与安全技术相配合，共同实现安全目标的制度、规章体系。

这样，我们可以把信息安全划分为物理环境安全、网络平台安全、系统平台安全、应用系统安全和安全管理五个层次。

中国电子政务安全建设的对策建议



中国电子政务安全建设的对策建议

在中国信息化建设过程中，由于关键的网络设备和系统软件（如交换机、路由器、操作系统、数据库、服务器等）主要依赖于国外的设备和技术，因此中国信息化系统的安全建设存在着先天不足。因此,除了采取必要的安全保障措施与安全管理措施(如防火墙技术、网络隔离技术、VPN技术、入侵检测和漏洞扫描技术和防病毒技术等)来保障网络和系统的安全外，还必须从应用层着手，利用公钥密码技术建立的提供信任和安全服务的基础设施——国家PKI（Public Key Infrastructure）体系，通过加密和数字签名，为信息安全提供有效的强有力的保障，保证通信数据和交易的安全有效。

PKI涉及重大国家利益，是网络经济的制高点，也是推动互联网发展、保障事务处理安全、推动电子政务、电子商务的支撑点。因此，建立健全的国家PKI体系，将有力地促进我国电子政务以及整个国家信息化的发展，否则，如果不加快PKI的研究与建设，中国将在新一轮的竞争中处于不利地位。

内容

电子政务安全建设中的问题与对策

公钥基础设施PKI简介

公钥基础设施**PKI**技术

1. 问题的提出

随着Internet 的普及，电子政务和电子商务得到了长足的发展。然而随着两者的飞速发展也相应的引发出一些Internet 安全问题。

- 保密性：如何保证电子政务、电子商务中涉及的大量保密信息在公开网络的传输过程中不被窃取；
- 完整性：如何保证电子政务、电子商务中所传输的事务处理信息不被中途篡改及通过重复发送进行虚假处理；
- 身份认证与授权：在电子政务、电子商务的事务处理过程中，如何对双方进行认证，以保证双方身份的正确性；
- 抗抵赖：在事务处理完成后，如何保证任何一方无法否认已发生的事务处理过程；

互联网的困境

"On the Internet, nobody knows you're a dog."

2. 公钥基础设施PKI简介

为解决这些Internet 的安全问题，世界各国对其进行了多年的研究，初步形成了一套完整的Internet 安全解决方案，即目前被广泛采用的PKI 技术(Public Key Infrastructure-公钥基础设施)。

PKI是信息安全基础设施的一个重要组成部分，是一种普遍适用的网络安全基础设施。PKI是20世纪80年代由美国学者提出来的概念。PKI技术采用证书管理公钥，通过第三方的可信任机构--认证中心CA (Certificate Authority)，把用户的公钥和用户的其他标识信息捆绑在一起，在Internet 网上验证用户的身份。

作为提供信息安全服务的公共基础设施，PKI是目前公认的保障网络社会安全的最佳体系。在我国，PKI建设在几年前就已经开始启动。截至目前，金融、政府、电信等部门已经建立了70多家CA认证中心。如何推广PKI应用，加强政府之间、部门之间、国家之间PKI体系的互联互通，已经成为目前PKI建设亟待解决的重要问题。

PKI的基本定义与组成

- PKI的基本定义十分简单，所谓PKI就是一个用公钥概念和技术实施和提供安全服务的具有普适性的安全基础设施；
- PKI 是一种新的安全技术，它由公开密钥密码技术、数字证书、证书发放机构（CA）和关于公开密钥的安全策略等基本成分共同组成的。从某种意义上讲，PKI包含了安全认证系统，即安全认证系统-CA 系统是PKI 不可缺的组成部分。
- PKI主要包括四个部分：X.509 格式的证书（X.509 V3）和证书废止列表CRL（X.509 V2）；CA 操作协议；CA 管理协议；CA 政策制定。

典型PKI应用系统的五个组成部分

- 认证中心CA：CA 是PKI 的核心，负责管理PKI 结构下的所有用户、应用程序的证书，把用户的公钥和用户的其他信息捆绑在一起，在网上验证用户的身份，CA 还要负责用户证书的黑名单登记和黑名单发布；
- X.500 目录服务器：X.500 目录服务器用于发布用户的证书和黑名单信息，用户可通过标准的LDAP协议查询自己或其他人的证书和下载黑名单信息；
- 具有高强度密码算法(SSL)的安全Web服务器：Secure Socket Layer (SSL)协议最初由Netscape 企业发展，现已成为网络用来鉴别网站和网页浏览者身份，以及在浏览器使用者及网页服务器之间进行加密通讯的全球化标准；
- Web（安全通信平台）：Web 有Web Client 端和Web Server 端两部分，分别安装在客户端和服务器端，通过具有高强度密码算法的SSL 协议保证客户端和服务器端数据的机密性、完整性、身份验证；
- 自开发安全应用系统：自开发安全应用系统是指各行业自开发的各种具体应用系统，例如银行、证券的应用系统等。

3. PKI的原理

- 对称密码学：加密运算与解密运算使用同样的密钥。通常,使用的加密算法比较简便高效，密钥简短，破译极其困难，由于系统的保密性主要取决于密钥的安全性，所以，在公开的计算机网络上安全地传送和保管密钥是一个严峻的问题。

- 非对称密码学：具有两个密钥，一个是公钥一个是私钥，用公钥加密的文件只能用私钥解密，而私钥加密的文件只能用公钥解密。公钥是公开的，所有的人都可以得到它；私钥是私有的，不应被其他人得到，具有唯一性；

PKI的核心思想：要证明某个文件是特定人的，该人就可以用他的私钥对文件加密，别人如果能用他的公钥解密此文件，说明此文件就是这个人的，这就是一种认证的实现。还有如果只想让某个人看到一个文件，就可以用此人的公钥加密文件然后传给他，这时只有他自己可以用私钥解密，这可以说是保密性的实现。这就是PKI 所依赖的核心思想。

新的问题产生了！

比如在现实生活中，我们想给某个人在网上传送一个机密文件，该文件我们只想让那个人看到，首先我们想到了用对称密码将文件加密，而在我们把加密后的文件传送给他后，我们又必须得让他知道解密用的密钥，这样就又出现了一个新的问题，就是我们如何保密的传输该密钥，此时我们发现传输对称密钥也不可靠。后来我们可以改用非对称密码的技术加密，此时发现问题逐渐解决了。

然而又有了一个新的问题产生，那就是如何才能确定这个公钥就是某个人的，假如我们得到了一个虚假的公钥。比如说我们想传给A一个文件，于是开始查找A的公钥，但是这时B 从中捣乱,他把自己的公钥替换了A 的公钥，让我们错误的认为B 的公钥就是A 的公钥，导致我们最终使用B 的公钥加密文件，结果A 无法打开文件，而B可以打开文件，这样B 实现了对保密信息的窃取行为。因此就算是采用非对称密码技术，我们仍旧无法保证保密性的实现，那我们如何才能确切的得到我们想要的人的公钥呢？

问题的解决——中立的仲裁机构CA

应用公钥技术的关键，便是如何确认某个人真正拥有公钥（及对应的私钥）。在PKI 中，为了确保用户的身份及他所持有密钥的正确匹配，公开密钥系统需要一个值得信赖而且独立的第三方机构充当认证中心（Certification Authority，CA），来确认公钥拥有人的真正身份。就象公安局发放的身份证一样，认证中心发放一个叫"数字证书"的身份证明。这个数字证书包含了用户身份的部分信息及用户所持有的公钥。任何想发放自己公钥的用户，可以去认证中心申请自己的证书。认证中心在鉴定该人的真实身份后，颁发包含用户公钥的数字证书。其他用户只要能验证证书是真实的，并且信任颁发证书的认证中心，就可以确认用户的公钥。认证中心是公钥基础设施的核心，有了大家信任的认证中心，用户才能放心方便的使用公钥技术带来的安全服务。

内 容

我国电子政务安全建设的对策建议

公钥密码技术的原理

公钥基础设施PKI技术

三 公钥基础设施PKI技术

1. PKI技术概述

公钥基础设施PKI（Public Key Infrastructure）是以公钥密码技术为基础，以数据的机密性、完整性和不可抵赖性为安全目的而构建的认证、授权、加密等硬件、软件的综合设施。

PKI安全平台能够提供智能化的信任与有效授权服务。其中，信任服务主要是解决在茫茫网海中如何确认“你是你、我是我、他是他”的问题。授权服务主要是解决在网络中“每个实体能干什么”的问题。

到目前为止，完善并正确实施的PKI系统是全面解决所有网络事务处理和通信安全问题的最佳途径。根据美国国家标准技术局NIST的描述，在电子政务和电子商务中，最需要的安全保证包括四个方面：身份标志和认证、保密或隐私、数据完整性和不可否认性。

PKI技术概述

- 认证：在现实生活中，认证采用的方式通常是两人事前进行协商。随着网络的扩大和用户的增加，事前协商会变得非常复杂。PKI通过证书进行认证，在这里，证书是一个可信的第三方证明，通信双方可以安全的进行互相认证。
- 密钥管理：PKI能够通过良好的密钥恢复能力，提供可信的、可管理的密钥恢复机制；
- 完整性与不可否认性：完整性可通过双方协商一个秘密来解决，但一方有意抵赖时，这种完整性就无法接受第三方的仲裁。而PKI提供的完整性是可以通过第三方仲裁的，并且这种可以由第三方仲裁的完整性是通信双方都不可否认的。

完善的PKI系统通过公钥密码技术及安全的应用设备，解决了网络社会中的很多安全问题。PKI系统具有这样的能力：它可以将一个无政府的网络社会改造成一个有政府、有管理和可以追究责任的网络社会。

2. PKI的基本组成

PKI由以下几个基本部分组成

- ✓ 公钥证书；
- ✓ 证书作废列表（CRL）；
- ✓ 策略管理机构（PMA）；
- ✓ 认证机构（CA）；
- ✓ 注册机构（RA）；
- ✓ 证书管理机构（CMA）；
- ✓ 证书存档（Repository）；
- ✓ 署名用户（Subscriber）；
- ✓ 依赖方（Relying party）；
- ✓ 最终用户（End User）；

PKI的基本组成

- 公钥证书：由可信实体签名的电子记录，记录将公钥和密钥（公私钥对）所有者的身份捆绑在一起，公钥证书是PKI的基本部件；
- 证书作废列表（ Certificate Revocation List ）：通常由同一个发证实体签名。当公钥的所有者丢失私钥，或者改换姓名时，需要将原有证书作废；
- 策略管理机构（Policy Management Authority）：监督证书策略的产生和更新，管理PKI；
- 认证机构（Certificate Authority）
  - ✓ 互联网定义：一个可信实体，发放和作废公钥证书，并对各作废证书列表签名；
  - ✓ 美国防部定义：一个授权产生，签名，发放公钥证书的实体。CA全面负责证书发行和管理（即，注册进程控制，身份标识和认证进程，证书制造进程，证书公布和作废及密钥的更换）。CA还全面负责CA服务和CA运行。
  - ✓ 美联邦政府定义：被一个或多个用户所信任发放和管理X.509公钥证书和作废证书的机构。

PKI的基本组成

- 注册机构（Registration Authority）
  - ✓ 互联网定义：一个可选PKI实体（与CA分开），不对数字证书或证书作废列单（CRL）签名，而负责记录和验证部分或所有有关信息（特别是主体的身份），这些信息用于CA发行证书和CLR以及证书管理中。RA在当地可设置分支机构LRA。
  - ✓ PKIX用语：一个可选PKI实体与CA分开，RA的功能随情况而不同，但是可以包括身份认证和用户名分配，密钥生成和密钥对归档，密码模件分发及作废报告管理。
  - ✓ 美国防部定义：对CA负责当地用户身份（标识）识别的人。
- 证书管理机构（Certificate Management Authority）：将CA和RA合起来称CMA；
- 证书存档（Repository）：一个电子站点，存放证书和作废证书列表（CRL），CA在用证书和作废证书。

PKI的基本组成

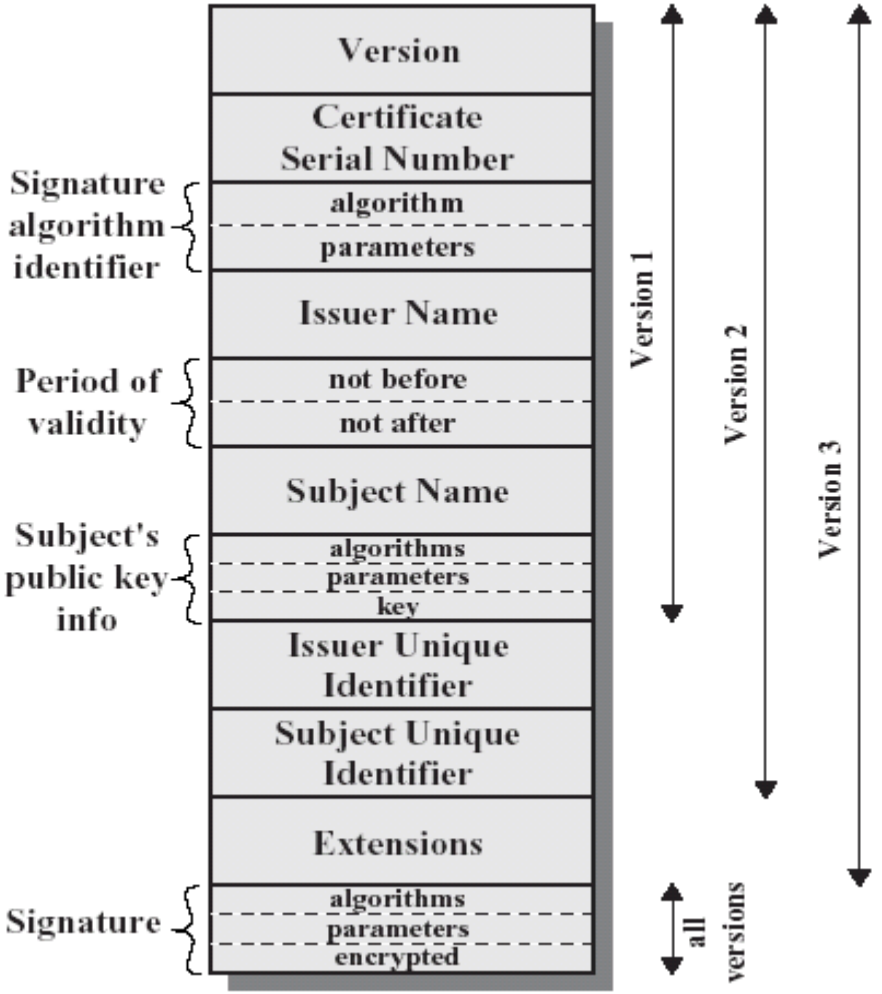
- 署名用户（Subscriber）：署名用户是作为主体署名证书并依据策略使用证书和相应密钥的实体；
- 依赖方（Relying Party）：一个接收包括证书和签名信息的人或机构，利用证书提供的公钥验证其有效性，与持证人建立保密通信，接收方处于依赖的地位。
- 最终用户（End User）：署名用户和依赖方的统称，也称末端实体（End-entity）,可以是人，也可以是机器，如路由器，或计算机中运行的进程，如防火墙。

3. PKI中的证书

- 证书(Certificate)，有时候简称为cert；
- PKI适用于异构环境中，所以证书的格式在所使用的范围内必须统一；
- 证书是一个机构颁发给一个安全个体的证明，所以证书的权威性取决于该机构的权威性；
- 一个证书中，最重要的信息是个体名字、个体的公钥、机构的签名、算法和用途；
- 签名证书和加密证书分开；
- 最常用的证书格式为X.509 v3；

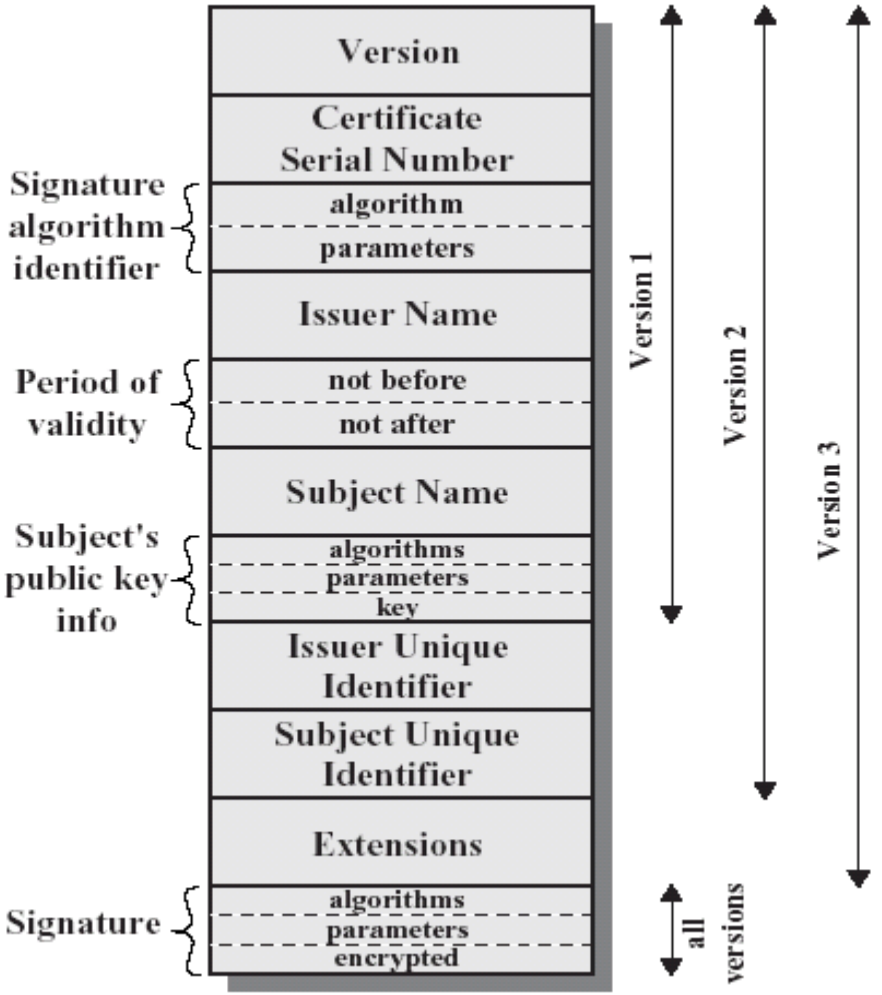
X.509证书格式

- 版本1、2、3
- 序列号
  - 在CA内部唯一
- 签名算法标识符
  - 指该证书中的签名算法
- 签发人名字
  - CA的名字
- 有效时间
  - 起始和终止时间
- 个体名字



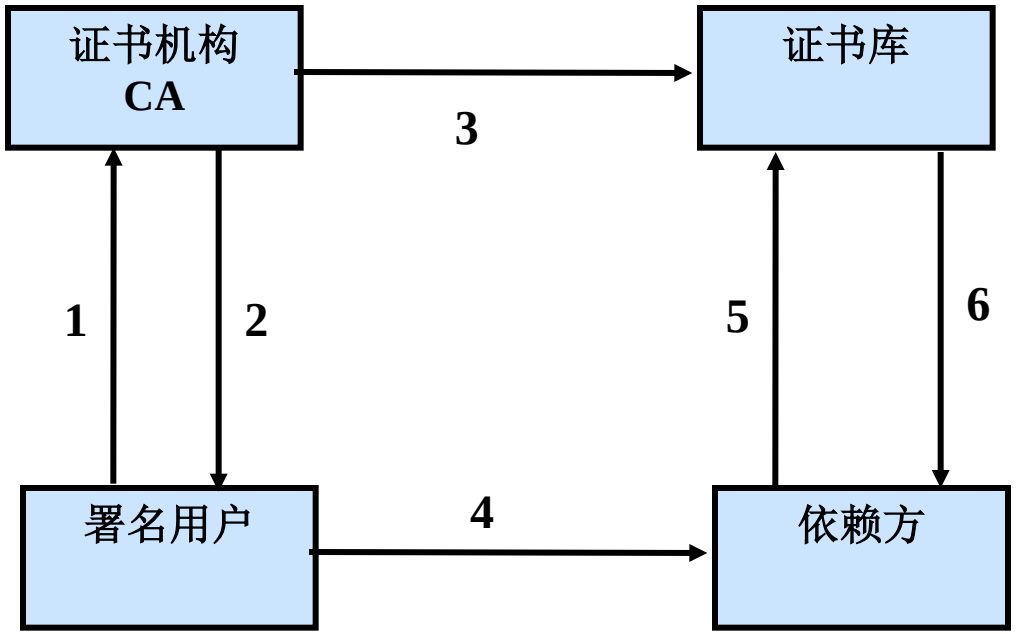
X.509证书格式（续）

- 个体的公钥信息
  - 算法
  - 参数
  - 密钥
- 签发人唯一标识符
- 个体唯一标识符
- 扩展域
- 签名



4. PKI的运行过程——X509标准PKIX

1. 署名用户向证明机构（CA）提出数字证书申请；
2. CA验明署名用户身份，并签发数字证书；
3. CA将证书公布到证书库中；
4. 署名用户对电子信件数字签名作为发送认证，确保信件完整性，不可否认性，并发送给依赖方。
5. 依赖方接收信件，用署名用户的公钥验证数字签名，并到证书库查明署名用户证书的状态和有效性；
6. 证书库返回证书检查结果；

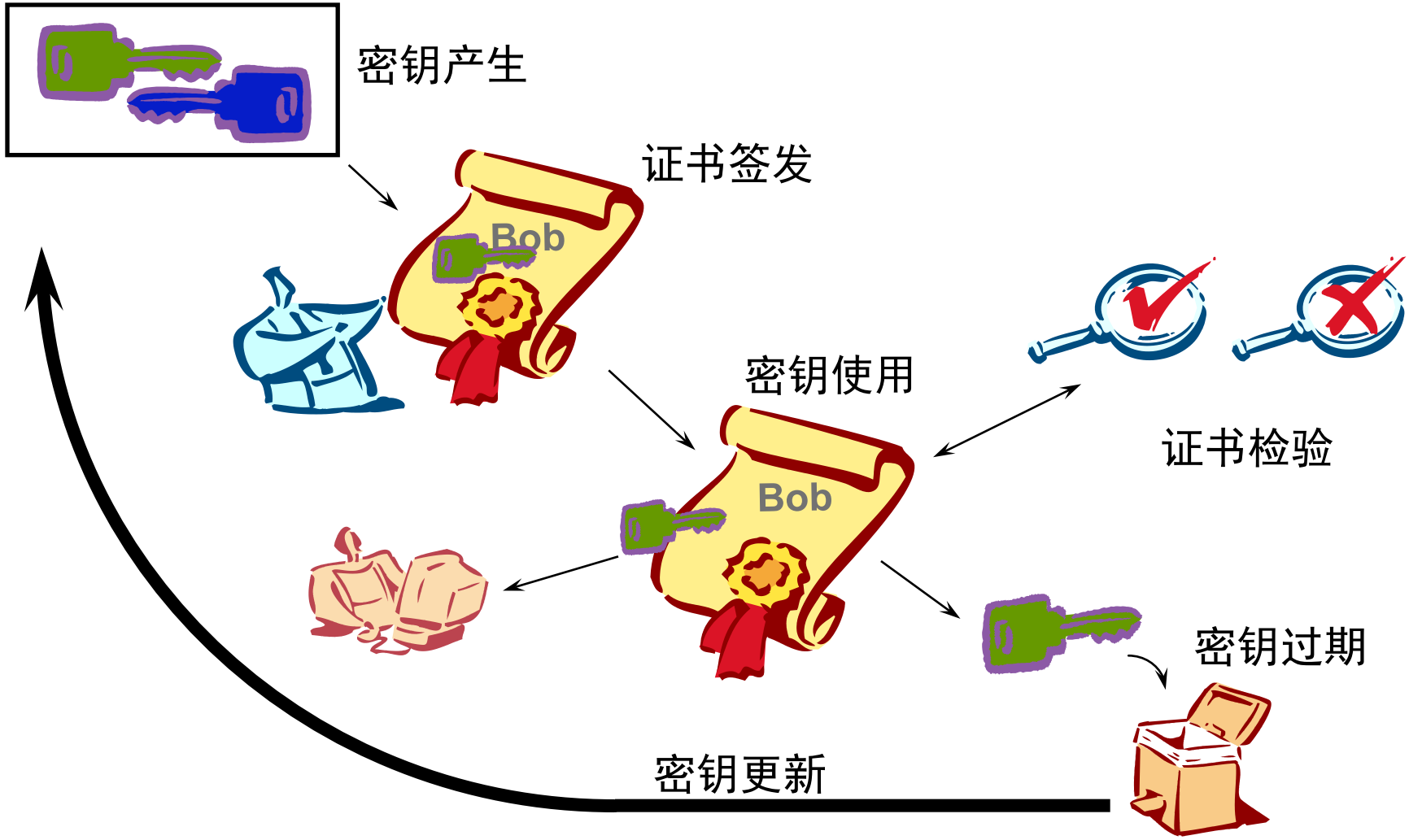


5. PKI中密钥和证书的管理

密钥/证书生命周期管理的各个阶段：

- 初始化阶段
- 颁发阶段
- 取消阶段
  - 证书过期
  - 证书撤销

密钥的生命周期



The end. Thanks

课堂练习

谈谈你对“统一的”电子政务应用平台的理解。