网证通
NET CA

编　　号：	
版　　本：	

药品采购 CA 安全解决方案

www.cnca.net

广东省电子商务认证中心

Guangdong Electronic Certification Authority

目 录

1 背景

1.1 药品采购系统与信息安全

1.1.1 药品采购系统面临安全挑战

药品采购系统一方面要求考虑企业内部网络的安全，另一方面要求考虑面向公众服务的网络安全。

药品采购系统涉及重大国计民生，这一特点导致来自外部或内部的各种攻击，包括黑客组织、犯罪集团或信息战时期信息对抗等国家行为的攻击。攻击包括基于侦听、截获、窃取、破译、业务流量分析、电磁信息提取等技术的被动攻击和基于修改、伪造、破坏、冒充、病毒扩散等技术的主动攻击。网络威胁包括来自内部与外部的威胁、主动攻击与被动攻击带来的威胁。网络威胁的隐蔽性、体制性、边界模糊性、突发性、易被忽视（如同恐怖的措手不及）的特点要求引起高度重视。据统计，11%的安全问题导致网络数据破坏，14%的安全问题导致数据失密。从恶意攻击的特点来看，FBI 统计的结果是 65%的攻击来自网络系统内部，如来自内部的非法窃取或非授权访问。

信息网络的可腐败性是药品采购必须考虑的另一问题。信息系统要求有相应的安全环境。目前，大部分药品采购选用的系统本身存在着安全弱点或隐患。网络硬件设备弱点如服务器、网络设备等安全问题将危害网络的可靠性和可用性。操作平台的弱点和漏洞（如操作系统、数据库系统、通用软件系统等）可能构成系统隐患。应用软件系统的脆弱性、应用系统的漏洞、代码错误、不安全代码的执行模式或不安全设计可能构成安全风险。网络的脆弱性、网络协议的开放性（TCP/IP 协议栈）、系统的相互依赖性导致网络存在安全风险。安全设计本身的不完备性可能构成网络新的安全风险。新的风险点、新的漏洞被发现、新的攻击技术手段被利用等药品采购的管理安全问题。网络安全管理人员对系统漏洞的置若罔闻是基于同样漏洞的攻击行为多次得以成功的原因之一。安全管理要求考虑网络系统的安全配置、正常运行、安全操作、应急响应、安全审计等问题。

国家也有具体的规范要求。在《计算机信息系统国际互联网管理规定》中要求：涉及国家级秘密的计算机信息系统不得直接或间接与国际互联网或其他公共信息网络相联接，必须实现物理隔离。这也是药品采购建设中需要考虑的问题。

1.1.2 让药品采购“固若金汤”

药品采购安全建设要求保护网络中信息存放、传输的安全，提高网络防护、检测、响应恢复和对抗攻击的能力，保证网络的保密性、鉴别性、完整性、可用性和可控性。其核心是保证系统数据的安全和系统的可用性，网络安全是基础环节。在安全设计时，要求技术、管理、法制、教育并举，有机综合多种安全技术，构建整体安全保障体系。

药品采购平台安全建设主要从以下方面考虑:

- **网络安全结构规划**

按照《计算机信息系统安全保护等级划分准则》（GB17985-1999）要求，对药品采购按照不同安全级别划分安全域。内部网络进行虚拟子网络隔离，边界接入网络分别采用物理隔离或隔离技术实现。

- **网络实体安全建设**

包括药品采购关键主机物理安全保障和机房安全建设。安全物理保证和信息存储介质安全保证等内容，保证网络实体运行环境的安全。

- **网络操作平台的安全建设**

主要考虑办公网络中各主机、工作站中采用的操作系统、数据库系统、通用软件系统的安全问题，建立一个可信的安全操作环境。

- **网络安全防护措施**

网络安全建设主要基于网络协议与服务的安全配置、网络安全防护、网络实时监控等措施实现。

药品采购的通用安全服务可以通过建设应用安全服务平台来实现，通过安全平台向各应用提供统一的安全服务如信息加密/解密、数字签名/验证、数据完整性校验、密钥管理等功能。安全服务平台可以基于统一的身份鉴别（如认证中心）和统一授权管理（如访问控制中心）实现。

身份标识、鉴别与授权是药品采购安全建设的重要内容。身份标识与鉴别解决“你是谁”的问题，授权解决“你能做什么”的问题。药品采购系统的身份可以为系统中网络节点、终端设备、操作用户等，并不局限于人员。

1.1.3 建立安全管理体系

通常情况下，信息网络系统的安全除安全技术作为保障措施外，必须健全相应管理措施，管理机构依据管理制度和管理流程对日常操作、运利维护、审计监督、文档管理进行统一管理。

由于网络新漏洞的出现与新威胁的增长，必须通过网络安全管理实现系统审计信息的综合分析，不断在运行中调整安全策略、完善安全设计，使安全策略更符合实际（如网络防护安全规则、入侵检测规则）、安全设计更趋合理。另一方面，要求建立各项应急响应措施与应急制度，提高系统抗攻击或抗灾难响应能力。通过网络安全管理体系的建设，保障网络安全体系的动态性和自适应性。

药品采购是一项复杂的系统工程，其安全建设要求统一考虑，长远规划，保证技术的先进性和扩展性。在技术上要求适应网络动态变化，建立自适应的安全保障体系。 同时要求有相关法律保障，加强安全管理。其关键是增强人的安全意识，要求从企业安全、社会稳定的高度认识药品采购的重要性。这样才能适应于企业信息化的发展。

1.2 我国信息安全的发展情况

为了解决药品采购发展中面临的信息安全难题，更好的推动国家药品采购和电子商务的发展，我国在 2005 年 4 月 1 日正式实施了首部信息化法律《中华人民共和国电子签名法》及其配套的《电子认证服务管理办法》，在国家层面确立了可靠的电子签名和手写签名或者盖章具有同等的法律效力，同时也确立了电子认证服务机构（CA）的法律地位和认证程序，从技术和法律层面解决了上述的问题，有力推动 PKI/CA 在药品采购及相关电子商务领域中的应用。

广东省电子商务认证中心（以下简称网证通或 NETCA）作为信息产业部批准的权威第三方认证机构，承担着解决药品采购和电子商务信息安全的重担，并已经先后为**广东省药品交易中心药品交易系统耗材交易系统、深圳全药网药品采购平台等构建基于 CA 电子认证数字证书的安全保障体系**，网证通将以优良的产品和服务为药品采购的信息化提供专业安全的解决方案，推动我国药品采购行业的信息化发展。

2 药品采购系统安全需求分析

药品采购系统基于 TCP/IP 通信网络，其安全保障是建立在“信任”的基础上，一旦这种信任关系遭受破坏，与之相关的安全性也就不复存在。从信息化建设应用系统网络的逻辑结构上来讲，其安全脆弱性主要体现在以下几方面：

信息机密性：在一个开放的网络环境中，绝大多数数据以明文形式传输，将很容易遭受搭线窃听。在一个交换环境中，无论是通过 SPAN、Monitor 的端口设定，还是通过 Sniffer 监听网络中的广播数据，都是轻易而举的事，因此不管是通过内网/外网或者恶意的 ISP 传输的明文数据都没有安全性可言。

信息完整性：数据在传输过程中一旦被窃听、截获，将很容易被篡改再重发，无论是偶尔的被动传输错误还是故意的人为攻击，数据的完整性都会被破坏。“中间人攻击”、“会话劫持”就是典型的针对数据完整性的攻击方式，而随着一些黑客使用工具的普及，使得攻击越来越容易也越来越频繁。

身份认证与授权：对于用户在系统进行的操作行为，都需要进行一定的访问控制，而对于网上审批申报、年审等是需要严格的身份认证。如果没有一个可信第三方做出权威的仲裁，那么对于随时可能被篡改的请求和回应，就无法进行安全性的校验，主客体双方身份得不到确认，自然无法保证其行为的合法性。

身份不可抵赖：如果网上任一方对其行为和提交的数据进行抵赖，出现纠纷不可避免。通常，无赖用户往往以业务应用系统和数据存储由其它用户控制为理由，声称这些系统中记录的内容不是自己操作而是其他特权用户操作，这样将为应用系统带来管理风险和法律风险。

根据平安智慧城市的要求和应用特点，结合网证通在多个大中型药品采购项目的经验总结和客户的反馈，平安药品采购系统的安全需求主要包括以下方面：

2.1 系统用户身份不可确认的需求

平安药品采购系统的用户包括：药品生产企业、经销企业、医院、监管部门（卫计委、社保、银行等等）和药品采购服务商的内部工作管理人员，他们分布在不同的网络环境中，安全保护也不尽相同。如果用户在登录和访问采用传统的“用户名+口令”方式，只要使用普通的网络扫描

软件即可获得其相关人员的用户名和密码，这样就使其他的系统内安全措施型同虚设，只要非授权用户以窃取到的人员身份进入系统，就可以做相关权限的事情，用户的合法性就无法得到保障。

2.2 对系统用户集中管理和统一认证的需求

随着平安药品采购系统的不断开发和建设，及准备实现的全省系统大集中，将来访问大集中系统的用户不但是平安药品采购系统的内部工作人员，还包括全国各类相关企业机构及企业公众用户。系统用户身份特殊、复杂，而且分布分散，这对用户的统一身份管理、统一用户认证、统一事件审核、统一安全策略等需求必将越来越强烈。对于访问控制的安全，系统管理员一般面临着如下的困惑：

- 如何安全有效地管理多种应用系统及其用户的访问权限？
- 如何有效地减少管理大量用户的认证和权限所花费的成本？
- 如何为不同的应用系统和用户制订一套统一的安全策略和操作方法？
- 如何安全有效地管理多种药品采购和其他业务应用，控制用户访问药品采购和其他业务的权限？
- 如何在多个应用系统中实现一次性身份认证？

平安药品采购系统应根据自己的实际情况和需要，对访问控制安全做一个前瞻性的规划，解决上述的问题。

2.3 企业申报信息的保密性和完整性需求

平安药品采购系统为企业提供了在线服务，企业可以在任何网络畅通的地方进行网上申报、网上合同签订等相关事宜，给企业带来了极大的便利。但是这些申报信息中包含了许多敏感的资料，其在网上传输的安全性难以得到保障。可能存在的隐患包括：

- **申报资料以明文方式传输容易被窃取。**网络技术的发展也推动的黑客技术的进步，互联网上很容易就能找到网络窃取或木马程序。如果企业的申报资料都以明文的方式传递，就很有可能造成泄密。
- **资料的接收方无法验证接收到的资料是否完整**。平安药品采购系统要真正实现网上的业务申报，首先要保证企业提交的资料完整，同时还必须保证资料在传输的过程中不能被非法的篡改。从上面的分析可以知道，企业申报数据在网络上的传输是有可能被窃取、

替换、更改的，因此如何保证企业申报材料能安全、完整的在网络中传输是网上申报系统能否正常运作的关键。

2.4 关键业务的责任认定的需求

关键业务涉及的范围比较广，执行人员或领导的意见的完整性和行为的不可抵赖性非常必要，具体体现在：

- **防止关键业务数据被篡改，维护操作人员的权益。**操作人员的操作行为通过电子的方式在网络中传输，必须用可靠的方法来实现象传统纸质文档签名一样易辨的效果，来确保操作行为的真实、完整，不会有伪签的情况出现，很好的维护操作人员的权益。
- **确保责任人对关键业务行为不可抵赖的需要。**在保证操作行为及数据意见真实、完整的前提下，每个关键业务的负责人必须对自己的关键业务结果负相应的法律责任，这样才能真正的体现关键业务的公正性，同时也为关键业务结果提供审查的手段。

2.5 交易数据的保密性和完整性需求

在平安药品采购系统中存在大量的机密交易数据，保证这些信息的完整性、机密性同样是实现交易信息化的关键之一。要真正实现交易数据完全电子化就必须解决电子交易的法律效应和权威性问题，只有利用可靠第三方的电子签名才能满足此要求。

2.6 对重要行为的时间取证需求

不管是平安药品采购系统的业务交易及和外部进行数据交换、申报资料的提交和审批，都有严格的时间要求，有一些重要的时间可能会成为将来法律的依据，因此，很有必要对某些重要行为的时间进行取证，这样可以达到以下的目的：

- **防止行为人推诿责任**。一些重要的工作，例如药品的申报、紧急公文的处理、行政许可的审批等都需要在指定的时限内完成。某些企业和内部工作人员因为工作繁忙或者其它原因忘记对公务进行处理，当需要追究当事人责任时无法取证其真正操作的时间，于是，其可以推诿其它原因来逃避责任，对重要的行为和文件加盖时间戳是解决这类问题的最有效方法。
- **使责任分明，责罚分明**。对重要的行为和文件加盖时间戳，可以促使内部工作人员真正

的按时操作，避免办事拖拉。而由于网络或其它非人为原因造成的公文延迟的惩罚，可通过时间戳取证，追溯到问题的所在，明确的控制了各项行为的管理。

3 药品采购安全体系建设思路

3.1 设计原则

安全体系建设是一项系统工程，应将“统筹规划、统一设计、分步实施、不断优化”的十六字方针作为平安药品采购系统安全体系建设的总体指导思想。采用先进的“平台化”建设思想，将药品采购安全平台作为整个安全体系建设的核心，避免重复投入、重复建设，充分考虑整体和局部、近期和远期利益，充分遵循以下的原则：

3.1.1 坚持统一标准、规范建设的原则

平安药品采购安全平台要按照统一的标准进行规划和设计，以保证系统间的互联、互通、互操作；要用统一的标准来规范平安药品采购系统中各个相关业务系统的建设，确保建成后各个业务系统能够进行安全的互联互通和信息共享。

3.1.2 坚持以人为本，方便适用的原则

平安药品采购安全平台的设计要以最终用户为中心，充分体现以人为本的思想，围绕系统的易用性、可管性和易维护性来设计，方便最终用户的操作和使用，简化系统的管理和维护。

3.1.3 坚持总体规划，分步实施的原则

平安药品采购安全平台的设计是一个复杂的系统工程，首先必须做好平台的总体规划工作，制订好总体实施方案；同时，为了尽快解决存在的突出问题并满足用户需求，应有计划、有步骤地实施。

3.1.4 坚持标准化、可扩展的原则

平安药品采购安全平台的设计要符合国际和国家的相关标准，因为 IT 技术的发展和变化非常迅速，只有采用符合标准的技术体系才具有良好的可扩展性和兼容性，才能更好的保护当前的投资和利益。

3.2 技术路线

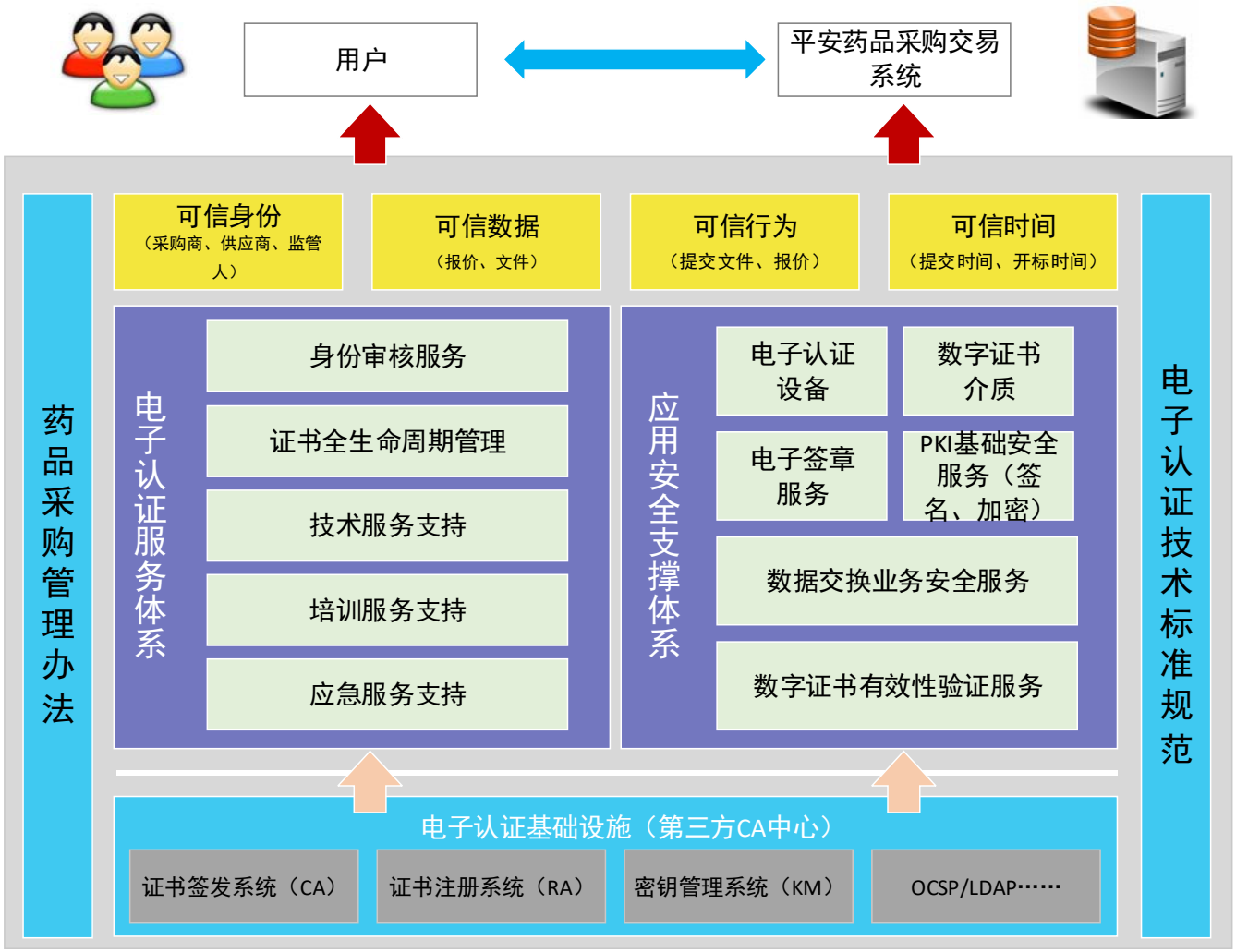
药品采购安全平台的建设要选用先进、成熟的技术，应保证整个平台具有技术领先性和持续发展性。因此，解决平安药品采购系统中存在的安全漏洞可以选用当前的主流安全技术——PKI/CA 技术。

网证通作为国内第一批从事 PKI/CA 技术研究、运营、服务的公司，具有 20 年的产品开发、应用集成和改造经验，利用网证通的 PKI/CA 安全产品能为平安解决系统登录安全、数据传输安全、电子文件签名和加密等一系列上述提到的安全问题。网证通作为国家信息产业部和国家密码管理局认可的第三方 CA 认证机构，还能为平安的药品采购提供相应的数字证书，实现可靠的电子签名。解决网上身份确认、网上操作行为以及该行为的不可否认、不可抵赖等问题，化解虚假用户、操作抵赖等法律有效性问题。

网证通完全有信心和能力为平安建设一个高标准的药品采购安全平台。

3.3 建设目标

从前面的描述中，我们可以将平安药品采购系统的安全总体目标确定为：建设功能完整、标准规范统一、系统可靠先进的安全基础设施——**电子认证安全服务平台**，解决目前平安各个系统中存在的身份认证、信息的机密性、完整性和不可抵赖性以及可信时间等方面的问题，真正实现平安各部门的公文流转无纸化，文档一体化，资料信息和办公业务动态信息共享和信息交换的药品采购安全支撑系统。



项目具体目标如下：

（1）为平安药品采购系统提供身份认证、机密性、完整性和不可抵赖性服务；

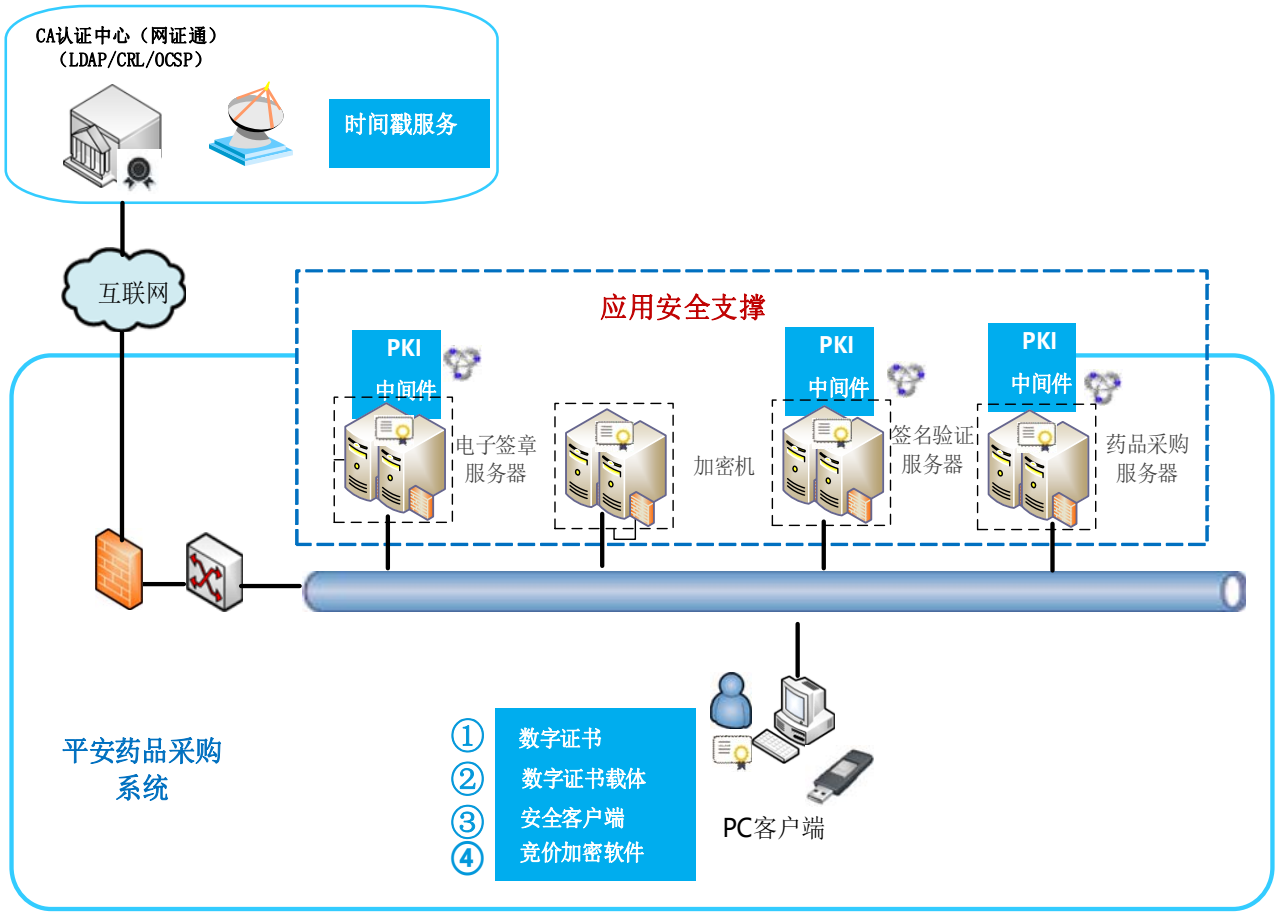
（2）建设统一用户管理和授权体系，实现所有应用的单点登录；

（3）通过证书密码服务系统和安全中间件实现应用系统的安全开发和改造；

（4）为监督部门实现过程的可管理、行为及效率的可审计提供支持；

（5）建立数字证书服务体系，提供数字证书服务、应用系统技术支持服务和售后客户服务；

3.4 整体架构及部署



如上图所示，平安药品采购系统的用户（包括内部办公用户、企业、系统管理员）等通过数字证书（装载在 USBKEY 中）统一通过省局的签名验证服务器进行身份认证。在证书的合法性校验通过后，访问用户才能获得登录指定应用系统的许可权限，并显示该用户所能访问的应用系统的界面。

3.5 备份和冗余

签名验证服务器、电子签章服务器和证书密码服务器作为平台的核心组成部分，需要考虑它们运行的稳定性和容错性。避免因为单机故障造成整个安全系统的瘫痪，网证通建议对承担主要功能的签名验证服务器和证书密码服务器采用双机热备的方式，以充分保障实时业务对安全体系的要求。

4 网证通安全产品简介

针对用户的需求，本方案将采用网证通的**电子认证服务平台**为核心，结合单位数字证书/公务员数字证书、服务器数字证书，为应用系统提供安全保护，实现身份认证等多种应用。下面对签名验证服务器平台进行简单介绍，详细内容可参阅网证通各安全产品的技术白皮书。

4.1 产品概览

平台由服务器端和客户端两大部分组成。

服务器端包括：

- 签名验证服务器
- 证书密码服务器
- 时间戳服务器
- 电子签章系统

客户端包括：

- 数字证书（单位/单位员工/公务员）
- 电子密钥（USBKEY）

4.2 签名验证服务器

签名验证服务器是平台的核心产品，它相当于房子的大门，承担着用户身份管理、权限管理、统一登录、证书有效性验证等功能。考虑到部署的便利性，该服务器采用机架式设计（内置专用密码设备、LCD 显示器、智能 IC 卡、应用安全中间件），符合《商用密码管理条例》的相关规定，能够有效保障数据的安全传输、确保用户身份的真实性、操作后的防抵赖、提交数据后的防篡改。

为满足与应用结合和将来系统扩展的需要，该产品还提供了 PKI 安全中间件（SecuInter），利用该中间件可快速、方便的实现数字证书密钥管理、读取数字证书域信息、加密、解密、签名、验证签名、CRL 查询等功能，完全屏蔽了安全技术的实现细节，向应用开发人员提供面向业务的

接口，可以方便、快速实现数字证书安全登录、加密传输信息、验证签名信息等业务应用。

签名验证服务器主要功能特点如下：

- ✧ 灵活快速的部署－－符合工业标准的硬件设备，根据客户的实际环境通过简单的初始化后即可完成部署，实现数字证书的应用；
- ✧ 数字证书用户管理－－接收并处理普通用户的 X.509 格式证书申请（PKCS＃10 及 Netscape KEYGEN 标签格式）；更新或废止证书；证书查询下载；证书验证。
- ✧ 数字证书用户认证与安全登录－－通过应用安全中间件为应用系统提供数字证书方式的用户认证，实现安全登录。
- ✧ 安全传输－－签名验证服务器与各应用服务器之间、用户与各应用服务器之间采用安全传输通道（SSL）实现通信的安全，确保通信的机密性和数据的完整性。
- ✧ 开放的应用接口－－提供 C 和 Java 标准接口（密钥管理、读取证书域信息、加解密、签名、验证等），可与多种应用无缝集成，实现基于数字证书的多种 PKI 安全应用，如数字签名、数据加解密、电子印章等；

4.3 证书密码服务器

在平安药品采购系统中，存在大量的保密信息，这些信息需要采用符合国家要求的技术手段进行加密。因此，非常有必要在安全平台中部署一台专用的密码设备，一方面为大量的数据加解密操作服务；另一方面可以作为服务器证书的存储设备，保证各个应用服务器的密钥不被窃取，从而提高整个系统的安全性。其主要功能特点如下：

- ✧ 生成密钥：可以生成 RSA/SM2 密钥，可以生成多对对称密钥（通信密钥）。由物理噪声源作为随机数，生成密钥速度快。
- ✧ 密钥存储：可以存储生成的 RSA/SM2 密钥和通信密钥。密钥存储安全 ，非法者不能获得密钥。
- ✧ 删除密钥：可以根据需要删除不使用的 RSA/SM2 密钥或通信密钥。
- ✧ 权限管理：可以初始化管理员和操作员，负责管理员、操作员权限的判断。 管理员口令采用分割权限的密钥管理机制。
- ✧ 数据加密：使用 RSA/SM2 或通信密要实现数据的加密，加密速度快、可靠。利用数据加密可以满足数据传输的机密性要求。
- ✧ 数据解密：可以实现加密数据的解密，解密速度快、可靠。

- ✧ 密钥备份：可以根据需要，在满足权限的情况下将主机加密服务器内的密钥等重要信息进行加密后备份到其他存储介质中并且可以导入相同型号的主机加密服务器中。
- ✧ 数字签名：可以根据需要利用 RSA/SM2 密钥对的私钥部分对信息进行数字签名。
- ✧ 身份识别：利用 RSA/SM2 密钥对的公钥部分实现身份识别。

4.4 时间戳服务器

为了真正的实现平安药品采购的在线服务，要求参与各方不能否认其行为。这其中需要在经过数字签名的地方上打上一个可信赖的时间戳，从而解决一系列的实际和法律问题。由于用户桌面时间很容易改变，由该时间产生的时间戳不可信赖，因此需要一个权威第三方来提供可信赖的且不可抵赖的时间戳服务，在本项目中需要部署一台时间戳服务器。它的主要功能有：

- ✧ 保证信息的时效性。对于像网上申报的材料、审批日期等对时间敏感的信息，通过加盖时间戳，可以证明某人在某一时刻拥有这一信息。
- ✧ 保证操作有时效性。可以证明某人在某一时刻完成了这项活动。
- ✧ 保证时间的法律效力。对重要法律文件的签署需要有严格的时间要求，通过申请时间戳，可以获得具有法律效力的时间证明。

4.5 电子签章软件

网证通电子签章软件（下面简称签章软件）是一套让用户能够对电子文档进行数字签名、电子签章的软件。它签署出来的 PDF 文档符合 ISO32000-1 标准，其电子签名过程遵循《中华人民共和国电子签名法》中关于“电子签名与认证”的相关法律条例。

签章软件符合当下电子商务市场中的无纸化办公的潮流，融合了先进的 PDF 和 PKI 数字签名技术，完美重现现实中签署合同、归档文件的效果，最重要的是它保证了电子文档中签名的合法性，包括电子文档的完整性和签名者身份的有效性。电子文档的完整性表示 PDF 文档的内容被篡改后能被及时发现，而签名者身份的有效性代表文档签名人身份的不可抵赖性。

签章软件提供了操作简便，功能完善的界面。它支持多种数字签名的功能以及特性，结合 PDF 文档的稳定性与 PKI 技术的安全性最大限度地保证了电子文档中签名的合法有效性。

NETCA 电子签章分为客户端组件、服务端模块两部分。其中客户端组件部分支持用户在终

端上使用在线或离线方式对文档加盖电子签章；服务端模块支持应用服务器采用单个或批量的方式对应用服务器上或 FTP 服务器上的文档加盖电子签章；支持系统管理员通过界面管理系统、管理签章；支持关键性操作记录日志，支持审查员审查日志等。

4.5.1 电子签章客户端组件

- 电子签章客户端

主要提供打开显示 PDF/Ofice 文件，用户可通过此工具对打开的文档加盖电子签章。
当用户打开的文档中包含电子签章时，此工具会自动验证电子签章文档的有效性。

- 电子签章中间件

提供二次开发接口，供应用程序打开显示 PDF/office 文件，对文档加盖或验证电子签章。

- NETCA Adobe Reader/Acrobat 插件

由 Adobe Reader/Acrobat 加载，在 Adobe Reader/Acrobat 中使用 NETCA 的签章。

4.5.2 电子签章服务端模块

- 电子签章中间件

提供二次开发接口，供应用服务端程序调用，对文档逐个或批量加盖、验证电子签章。

- 电子签章服务系统

为服务端的电子签章中间件提供实现支撑。
为系统管理提供管理系统配置，管理应用，管理签章信息提供支持。

4.6 网证通数字证书

网证通将根据本次项目的用户对象颁发三种不同类型的证书，包括：

（1）**单位数字证书**

颁发给独立的单位、组织，例如药品交易双方，在互联网上证明该单位、组织的身份。单位证书对外代表整个单位。该证书必须存储在 USB 电子密钥中。

（2）**单位员工证书**

单位员工证书对外代表单位中具体的某一位员工，主要颁发给内部的工作人员，确定他们的合法身份。该证书必须存储在 USB 电子密钥中。

（3）**服务器证书**

主要颁发给 Web 站点或其他需要安全鉴别的服务器，证明服务器的身份信息。服务器数字证书支持目前主流的 Web Server，包括但不限于：IIS、Lotus Domino、Apache、iPlant 等 Web 服务器。应保存在证书密码服务器上。

4.7 电子密钥

为了保证了用户私有密钥的安全性和唯一性，用户数字证书必要有一个很好的载体，USB 电子密钥于是应运而生。它成本低廉，小巧玲珑，支持热插拔，方便用户随身携带使用。用户无需记忆繁琐冗长的用户名和口令，只需要在拥有 USB 接口的计算机（现在 USB 接口已经是计算机的标准配置）上使用自己的数字证书，即可登录系统进行合法操作。

同时，按照《国家商用密码管理条例》规定，任何单位或者个人只能使用经国家密码管理机构认可的商用密码产品。目前网证通采用符合国家相关规定的 USB 电子密钥作为数字证书及其相关密钥的存储介质。基于 USB 接口的身份认证产品，集智能芯片和读写控制器于一体的证书存储设备，通过国家密码管理委员会的技术鉴定。内含具有国内自主知识产权的操作系统（COS），可以存储 X.509 数字证书、密钥和其他机密信息，是“不需要读卡器的智能卡”，支持热插拔。应用程序能使用它存储个人信息、私钥、密钥、许可协议、识别特征、数字证书或其它数据。可实现登录控制、电子邮件签名加密、文档签名加密、安全拨号等强大实用功能，广泛应用于网络身份认证领域。

USB 电子密钥硬件电路中集成读/写功能，包含完成存储功能的资源和高速加密引擎。它使用通用串行总行接口(USB)提供电源并且与计算机通讯。下面列出了 USB 电子密钥主要的硬件技术特性。

1. 符合 X.509 数字证书存储标准；
2. 支持 DES、3DES 密码算法及专用的分组密码算法；
3. 支持 RSA 及国密要求算法；
4. 直接在芯片内快速生成 RSA 或 SM2 密钥对，可实现签名/认证、加密/解密功能；
5. 支持 SHA-128 数据散列算法；
6. 内置硬件随机数发生器；

7. 软件控制状态指示灯，可方便观察和计算机的接通情况；

8. USB 接口，支持带电插拔，即插即用；

9. USB 电子密钥两级口令设置，密码重试次数可设定，输入 PIN 错误次数超过设定值则 USB 电子密钥锁死。

使用 USB 电子密钥具有以下四个优点：

可靠性：用户将个人信息存储在 USB 电子密钥上，可以保证即使发生系统故障仍然是安全的。

便携性： USB 电子密钥是连接在钥匙圈上的，用户永远不会忘记携带而且几乎不会丢失，USB 电子密钥是插入 USB 接口的，所以对核查在远地区通过笔记本电脑拨入一个公司虚拟专有网络(VPN)或进入 Intranet 的用户来讲是理想的。非常适合个人使用，可以完美地满足网络应用和异地工作的便携要求。

安全性：用户逐渐意识并且担心病毒和其它恶意软件能够访问保存在硬盘上的记录、控件、密码和其它个人信息。USB 电子密钥使重要信息不必保存在硬盘上，实现了“机密随身带”。同时作为双因素认证的解决方案，USB 电子密钥提供了更加安全的保障形式。

不可仿制：用户不能复制 USB 电子密钥中的信息。 这意味着你可以使用它保存获得 Internet 服务的接入授权，不用担心被人盗用。换句话说，USB 电子密钥没有密码普遍存在的共用问题。对 USB 电子密钥程序访问是通过提供的应用程序编程界面（API）完成的。

5 关键业务实现

5.1 竞价加密解密软件/中间件

目前竞价加密业务主要可分为三种应用实现方式（如下文），各有优缺点，推荐采用方式三；网证通也可以根据系统要求，进行定制与项目更贴切的应用模式；

5.1.1 自己加密-自己解密的方式

该方式加密解密过程描述：

1、加密时，用使用人的证书对报价信息进行加密；

2、解密时，用使用人的证书对报价信息进行解密；

优点：

1、改造简单，集成快；

2、基本不依赖第三方；

3、安全性高，基本不可能被破解；

4、自己加密自己解密，责任认定清晰；

缺点：

1、用户需等待，两次操作；比如：上午加密；下午还需进行解密。

2、人为错误率较高；比如忘了谁加的，拿错 KEY 解密等等；

5.1.2 分散加密-集中解密的主-子密钥方式

该方式加密解密过程描述：

竞价交易前，在系统中配置好以下内容：

1、“主密钥”（私钥）的存储地址，例如：保存在 FTP 服务器上；

2、“主密钥”（公钥，数字证书）的字符串，存到数据库中；

3、用解密人“子密钥”（如周睿）的数字证书加密“主密钥的私钥的使用密码”，保存到数据库中；

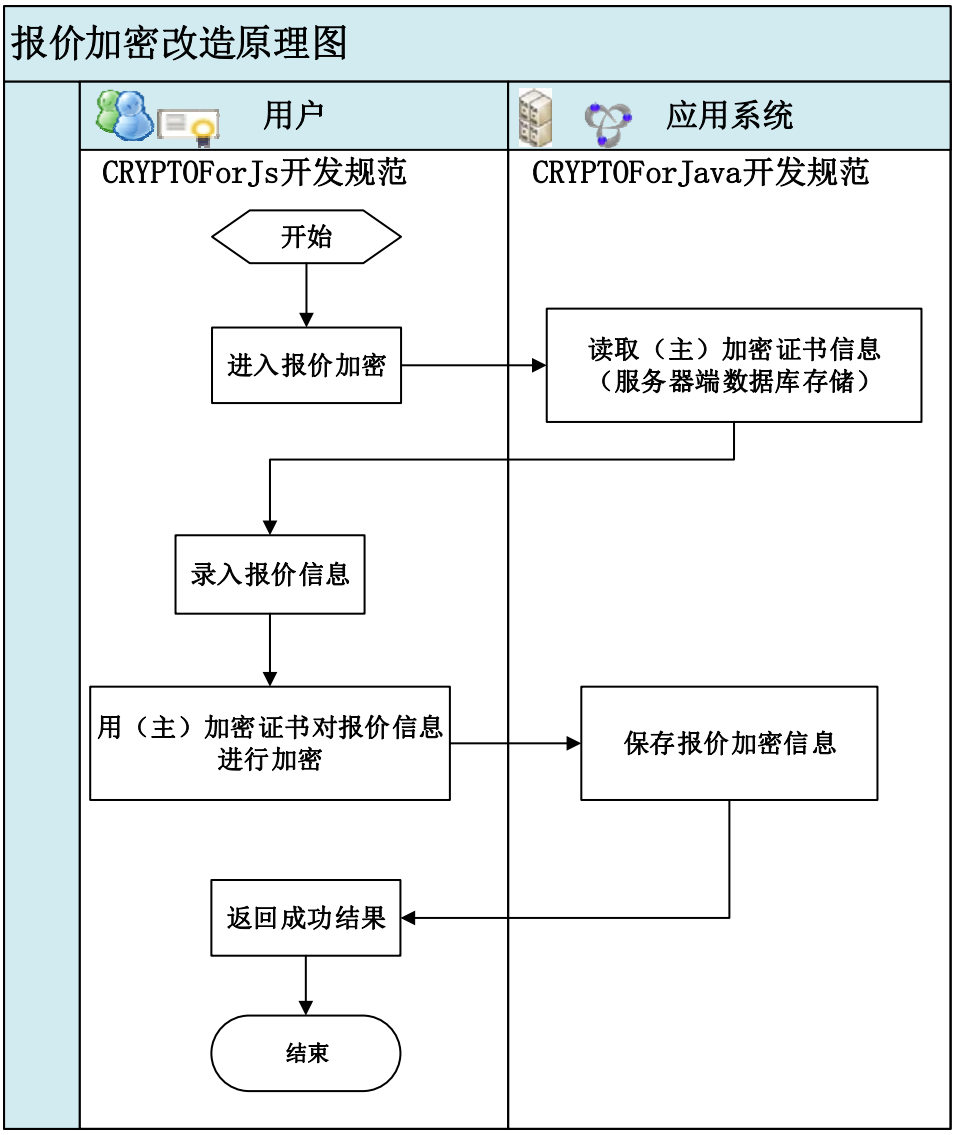
加密时（见下图）

1、交易用户无需数字证书 USBKEY，使用主密钥的公钥（数字证书中）进行竞价的本地加密；

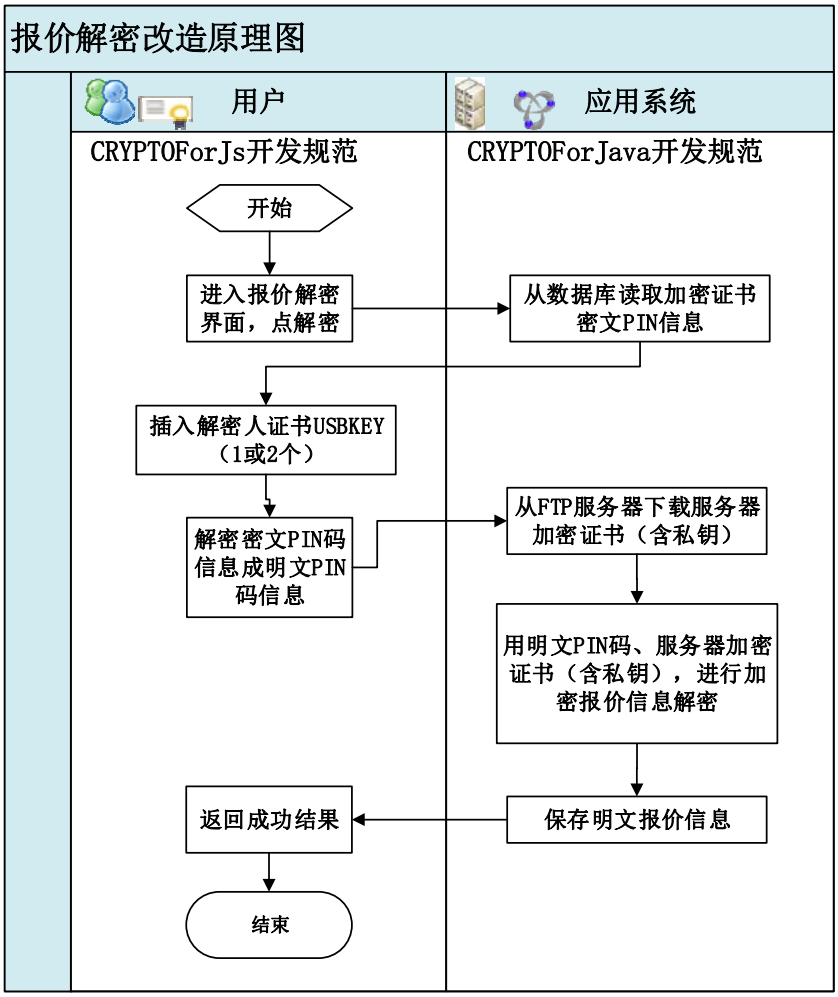
2、通过 SSL 方式，报价上传到服务端，进行存储；

解密时（见下图）

解密人通过含“子密钥”数字证书 USBKEY 解密主密钥的私钥密码；解密成功后，用主密钥的私钥密码调用主密钥的私钥解密加密后的竞价信息；



采用“主密钥”的竞价流程图



解密流程图

5.1.2.1 优缺点

优点：

1、改造简单，集成快；

2、基本不依赖第三方；

3、用户无需等待，加密后，无需再次操作，减少了操作的失败率。

4、解密性能高；

缺点：该过程存在一定风险：

1、“主”密钥的安全风险，主密钥存储在 FTP 服务器上，为文件型证书；

2、文件型证书不符合安全管理要求，存在“密钥被泄露”的安全管理风险；

3、解密规则风险，未到达解密时间，可人为操作解密，存在“操作人员提前解密竞价信息”

的安全管理风险；

4、主密钥 PIN 码信息防护不当，存在提前解密风险；上述过程中，如果代码开发人员，监控到明文 PIN 码信息，并可获取竞价加密信息，可提前解密竞价信息，存在“对开发人员防护不当”安全技术风险；

5.1.3 依赖于第三方竞价规则的安全加密解密方式

引入竞价加密规则文件，通过加密规则文件信息，约束整个竞价过程的加密和解密过程，真正实现“管、办、防”分离的三位一体管控；

主要涉及以下流程环节：

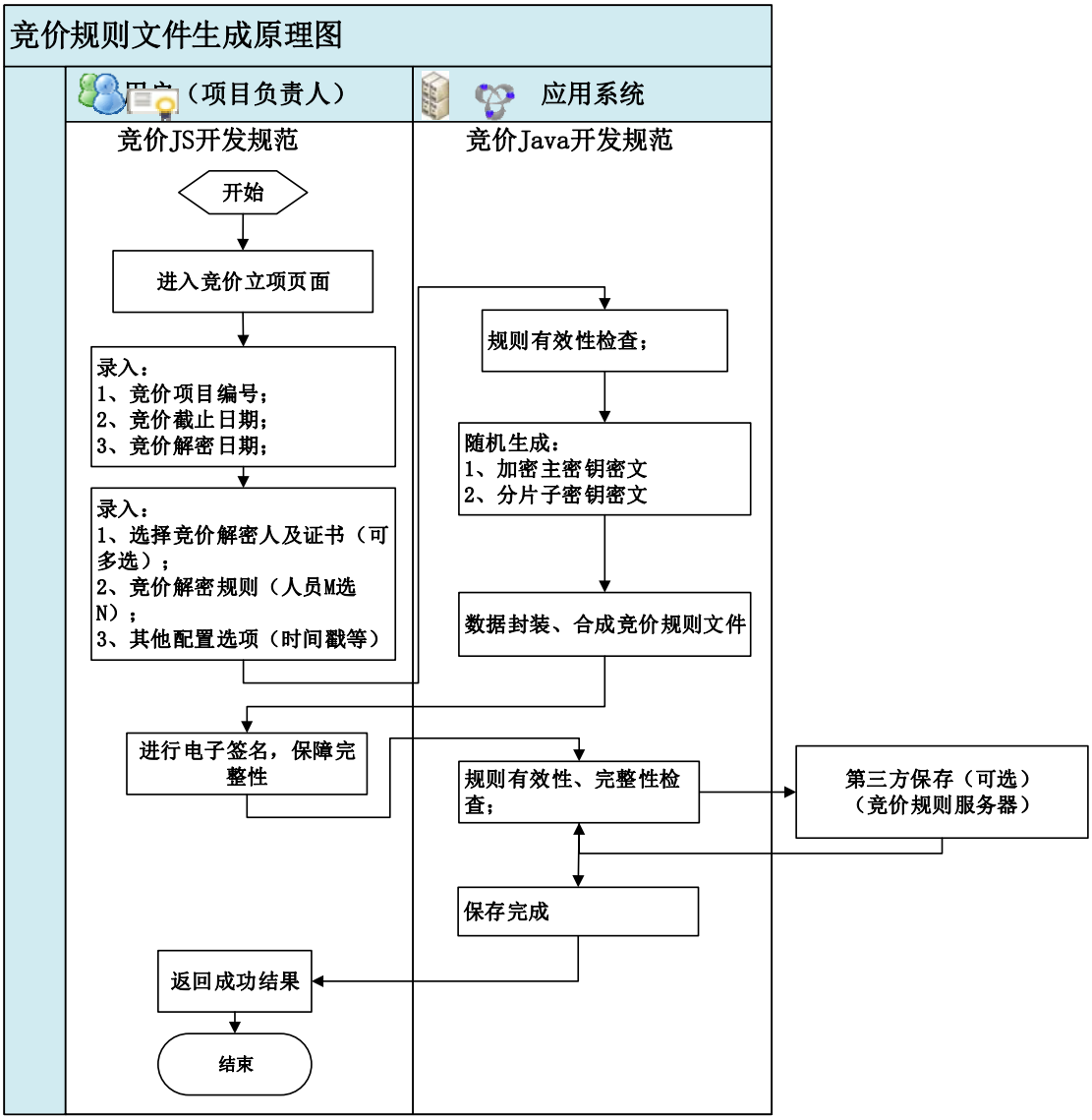
5.1.3.1 竞价规则文件生成

竞价过程，设立一定的规则，加密和解密，都采用相同的规则进行业务处理；

规则发生改变，竞价过程应暂停作废，重新进行竞价；

每个规则中包含随机生成的加密主密钥，该密钥由多个子密钥保护，避免被攻击；

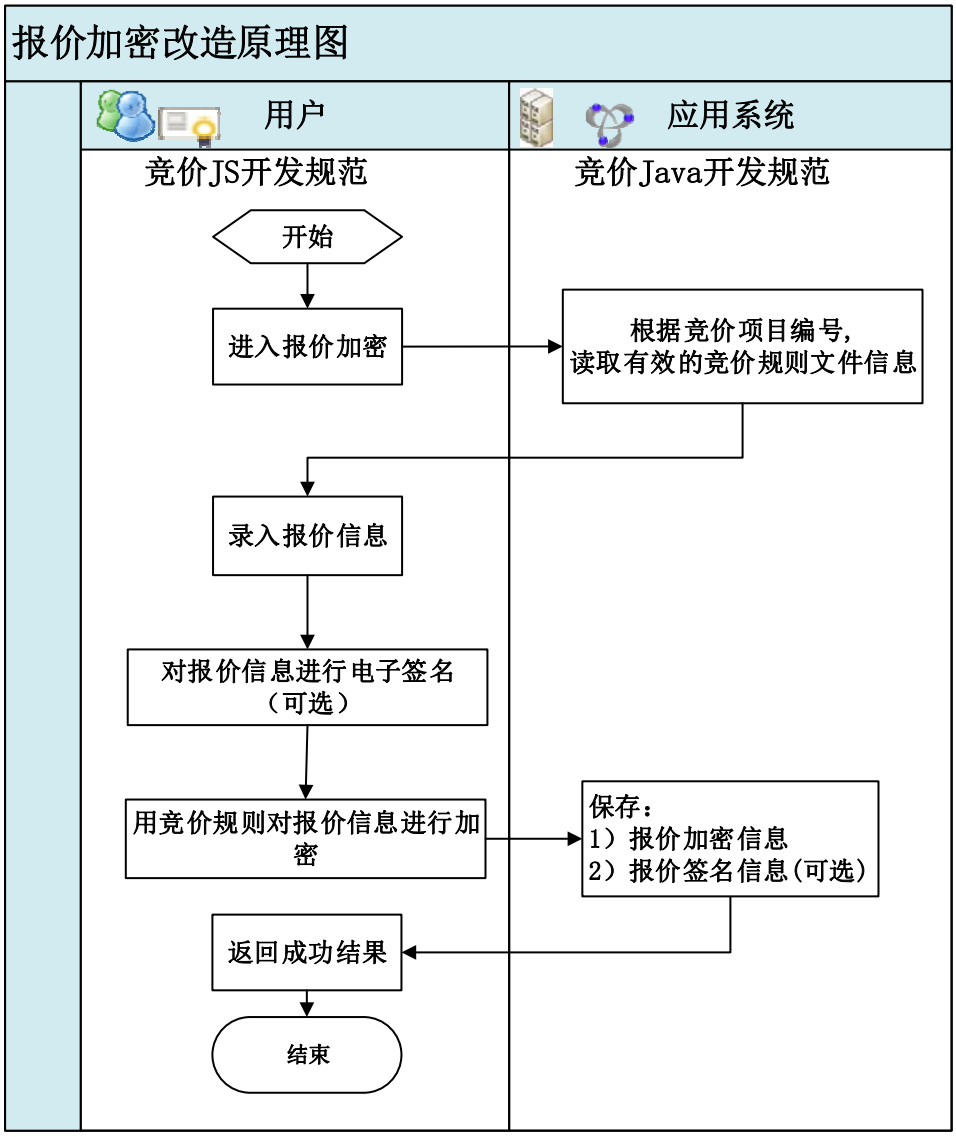
采用相同规则，每次生成的加密报价信息不同，防止重放攻击；



竞价规则文件生成流程图

5.1.3.2 竞价加密过程

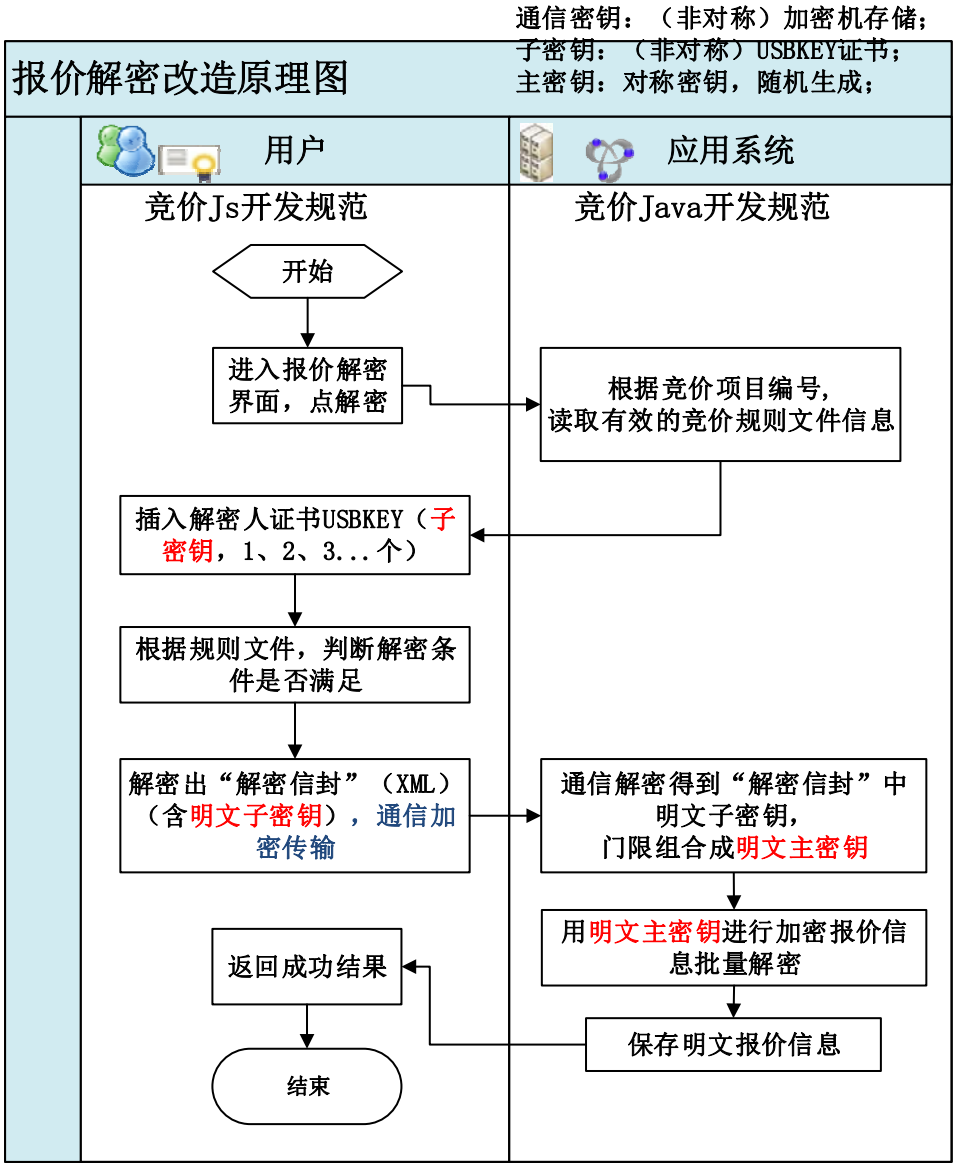
竞价人，报价时，采用竞价规则文件，进行报价的信息加密；



采用竞价规则的竞价加密流程图

5.1.3.3 竞价解密过程

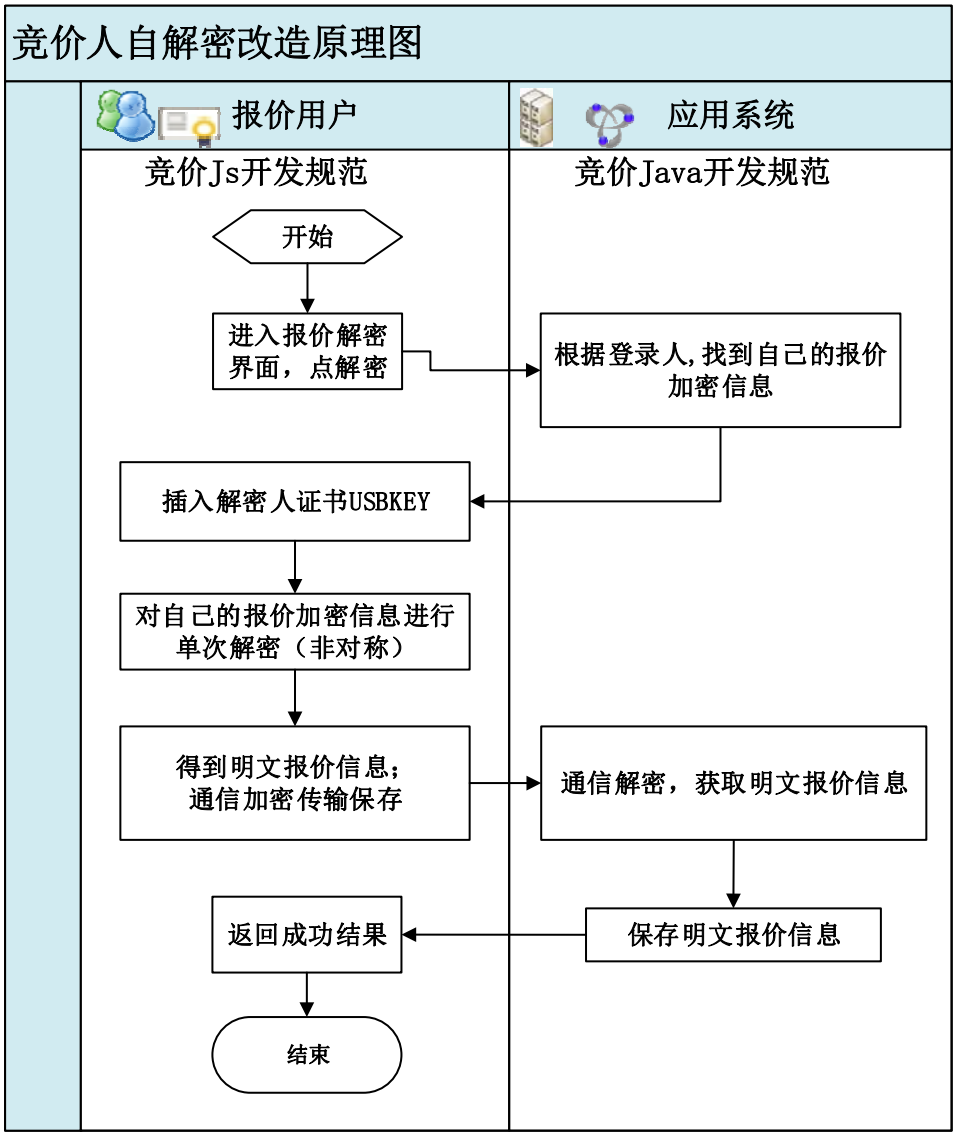
所有竞价信息的解密过程，由竞价规则所设置的解密人进行批量解密；



采用竞价规则的竞价解密流程图

5.1.3.4 竞价人自解密过程

某竞价人，能使用自己的加密证书，只解密自己的报价信息；但不能解密查看其他人的报价信息；



采用竞价规则的竞价自解密流程图

5.1.3.5 优缺点

优点：

1、支持多种算法，兼容现有 RSA 及国密 SM2 数字证书；

2、摒弃文件型证书的管理困难和风险，采用随机主密钥，防止密钥泄露复制；

3、避免现有的易篡改、易伪造、提前解密的安全风险；

4、“管、控、防”分离，构建全方位安全的竞价环境；

5、加密解密过程，安全方面由网证通负责；集成业务由平安负责，完成业务集成，伪造和篡

改都能被发现；

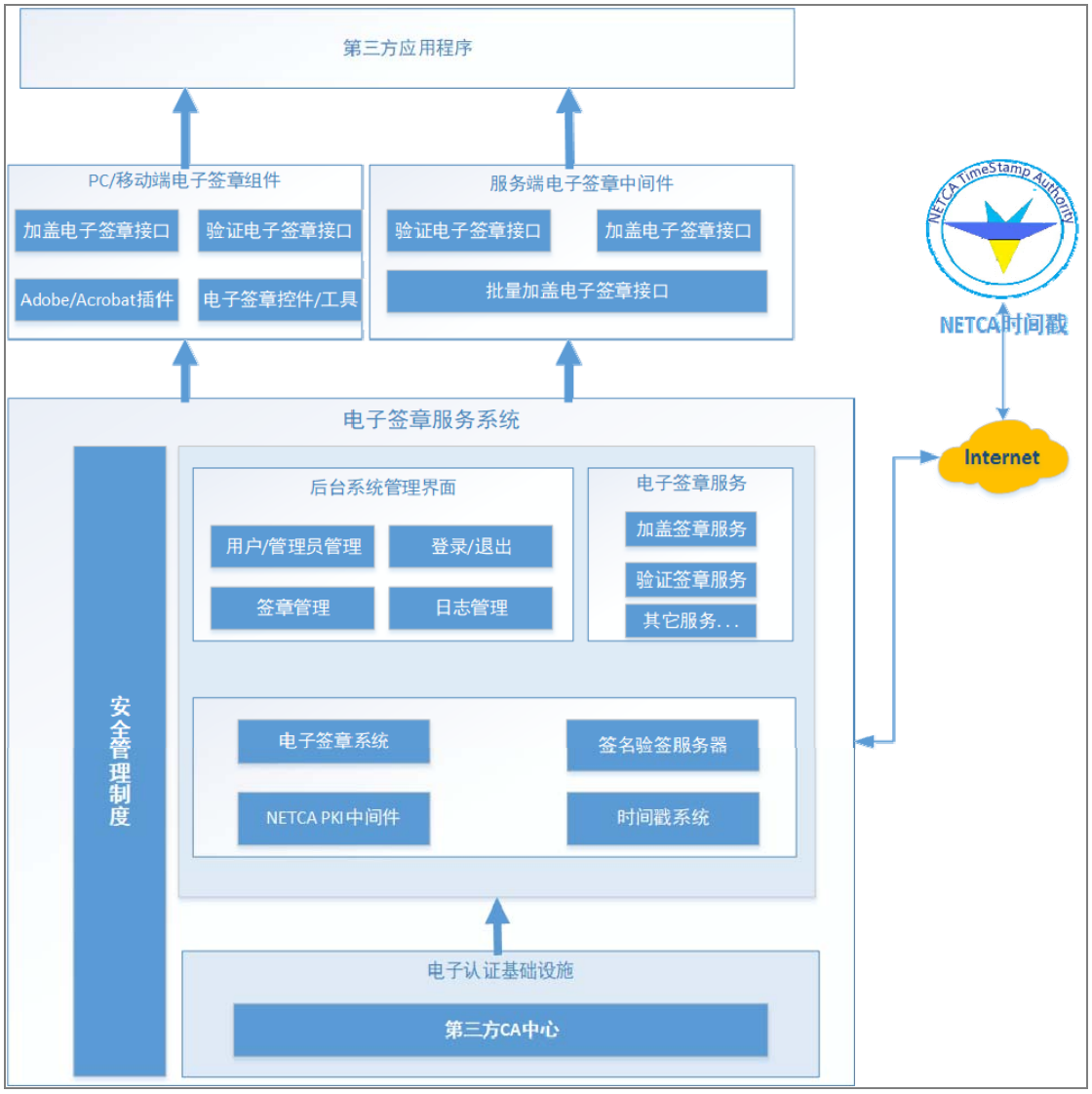
缺点在于：有一定的改造复杂性，由网证通全程协助平安完成；

5.2 电子签章及电子合同

电子印章也是公文或合同类业务系统中的一个重点。首先电子印章是基于 CA 中的数字签名这一技术的应用，表现层给人看到的是一个电子印章的图片，实际上其底层是使用数字证书的持有者的私钥对电子报文进行数字签名，并将签名值随原电子报文传输给接收方。同时签名的校验机制与电子印章的图片显式表示进行同步。即一旦原电子报文发生篡改，签名值可以立即验证出来此篡改，并马上进行提示，这样接收方可以及时知道文档的是否完整如初。并且电子印章及数字签名的不可抵赖性安全保障也为事后的审计提供了有效的法律保障。

5.2.1 产品架构

NETCA 电子签章分为客户端组件、服务端模块两部分，配套的软硬件设施包括 NETCA PKI 中间件，网证通安全客户端，NETCA 时间戳，电子认证网关服务器。产品架构如下图所示：



产品架构图

网证通电子签章客户端组件包括电子签章客户端、电子签章中间件和 Adobe Reader/Acrobat 插件，支持 Win XP、Win7、Win8、Win10、Android 和 IOS 系统。

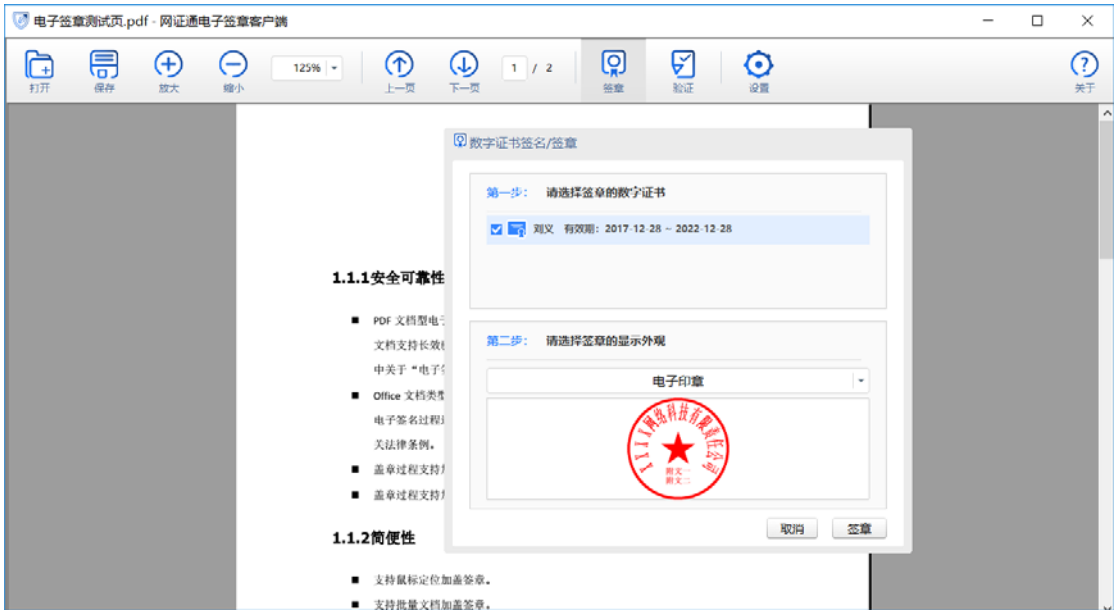
网证通电子签章服务端软件部分包括电子签章中间件、电子签章管理系统，支持 RedHat 企业版 5、6 和 7，包括 32 位和 64，Windows Server 2008 及以上。

5.2.2 使用功能

- 电子签名

签章软件支持两种方式的数字签名，一种是文字外观的电子签名，另一种是加盖印章的电子

签章。



客户端盖章操作

电子签章效果图

- 验证签名

签章软件可以实时地验证电子文档中数字签名的有效性，其主要体现在两个方面：

1. 自签名以来电子文档是否被篡改。
2. 签名者的身份是否合法有效。

除了数字签名与验证两个基本的功能外，签章软件还支持以下特性：

- 实时定位

  用户可以实时地通过鼠标点击的方式指定在文档中的签名位置。

- 批量处理

用户可以同时处理多份电子文档，实现多文档的批量签名、签章以及验证。

- 嵌入时间戳

支持在签名时使用安全的时间戳时间并嵌入到电子签名中，保证了签名时间的可靠性。

- 支持文档的长期验证

为了使电子文档能够长时间保存并合法地验证，NETCA 提供了 CRL 或 OCSP 的服务，签章软件可以利用这两种服务以提供电子文档长期验证的支持。

  - CRL（Certificate Revocation List）

    签章软件会在签名、签章时自动下载 CRL 并将其嵌入到电子文档中。

  - OCSP（Online Certificate Status Protocol）

  为了提高实用性，签章软件支持在签名、签章时优先获取 OCSP 并将其嵌入到电子文档中。

5.2.3 电子合同功能实现

在药采系统中，涉及电子签章使用环节最多的功能点在于电子合同。

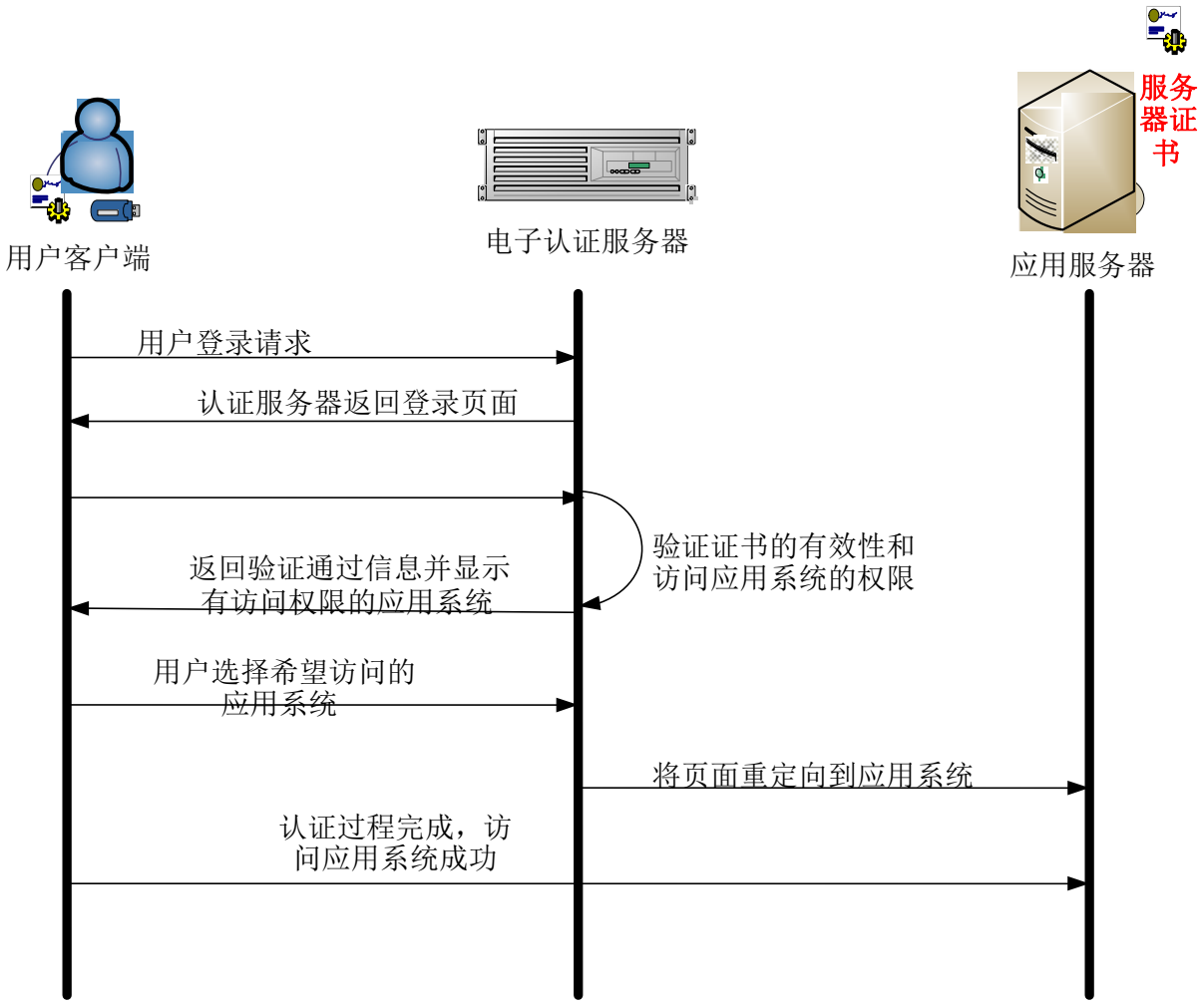
主要实现环节有：

1. 药采业主批量盖章：在服务器端，使用的业主的印章，批量对电子合同加盖电子签章。
2. 甲方、乙方网页盖章：在网页上，显示合同，自动定位盖章;
3. 配送方网页盖章：在网页上，显示合同，自动定位盖章;
4. 服务器端验证签章文件：盖章后的电子合同，上传后，在服务器端验证，通过后保存。

6 基于网证通产品的安全保障实现

6.1 统一用户管理和强身份认证的实现

利用签名验证服务器可以实现统一身份的认证和登录，其实现流程如下图所示：



用户通过签名验签服务器统一门户进行身份认证的过程如下：

1、用户通过浏览器访问统一登录门户，统一门户接收到用户的请求后返回登录的页面；

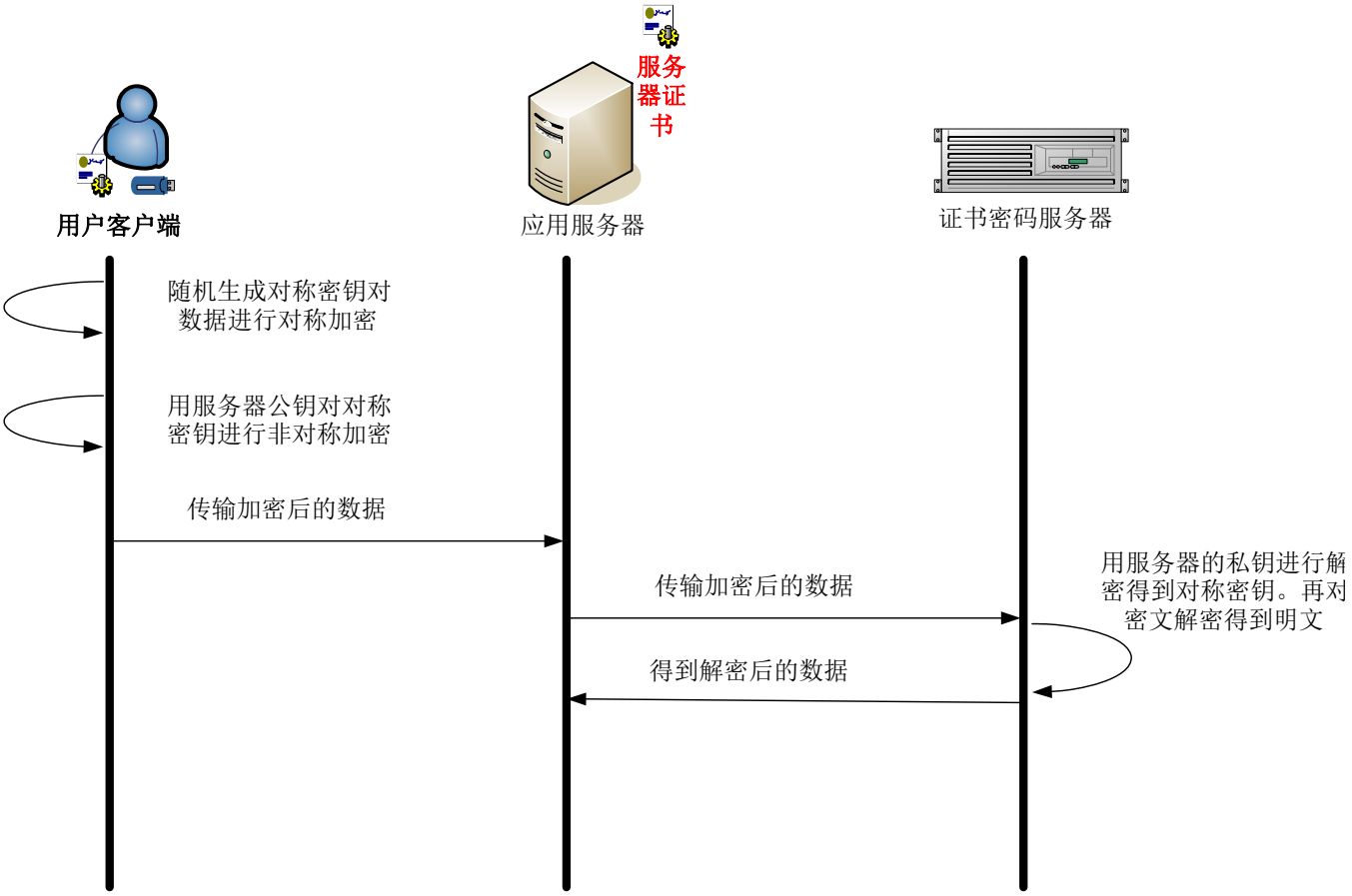
2、用户根据登录提示插入带数字证书的电子密钥，录入 PIN 码后，用户的数字证书会以 SSL 的安全方式传输到认证服务器；

3、签名验签服务器在验证证书的合法性后，再判断该证书拥有者所具备的应用访问权限，显示在页面上；

4、用户选择自己希望访问的系统，签名验签服务器根据用户的请求将页面重定向到指定的应用系统，整个验证和授权过程完成。

6.2 网上提交信息的保密性和完整性的实现

对于药品采购系统中的敏感数据，我们可以利用数字证书的密钥对完成数据的加解密过程。如果是私人数据，可以用客户端的个人证书进行加密，如果是公共数据，可以用服务器证书并结合证书密码服务器进行加密。具体的实现流程如下：



1、用户客户端使用指定的对称算法对需要加密的数据进行处理，组成一个加密数据包；

2、客户端利用在证书密码服务器上下载的应用服务器的证书（公钥）对对称密钥进行非对称加密；

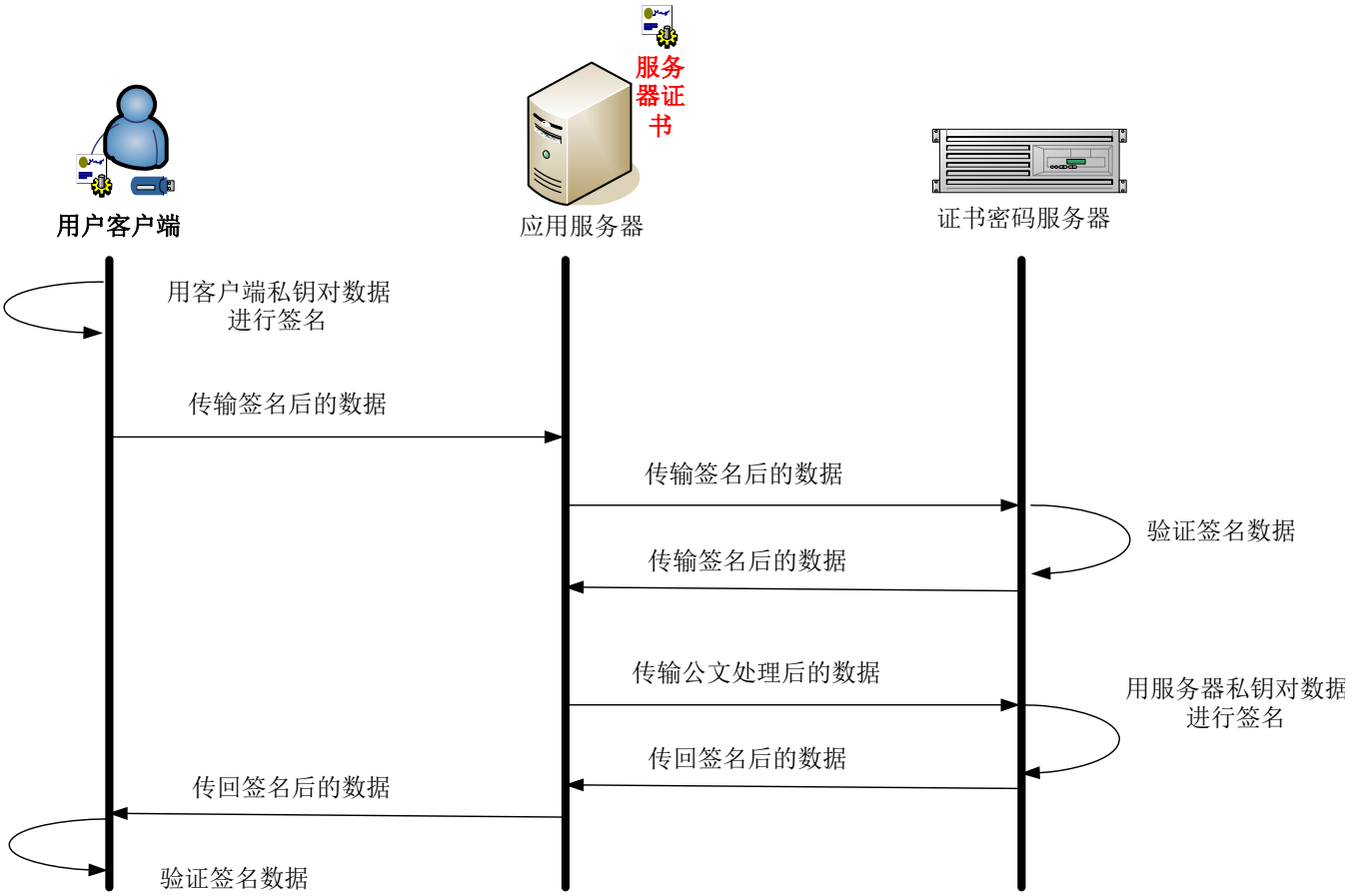
3、将数据包和加密密钥对传输到应用服务器及证书密码服务器，应用服务器与密码服务器间采用专用的通信接口，保证它们之间的传输安全；

4、由于服务器的私钥保存在证书密码服务器中，因此可以在密码服务器中用服务器的私钥进行解密得到对称密钥，再对密文解密得到明文；

5、将明文信息传输到应用服务器，完成加密传输的过程。

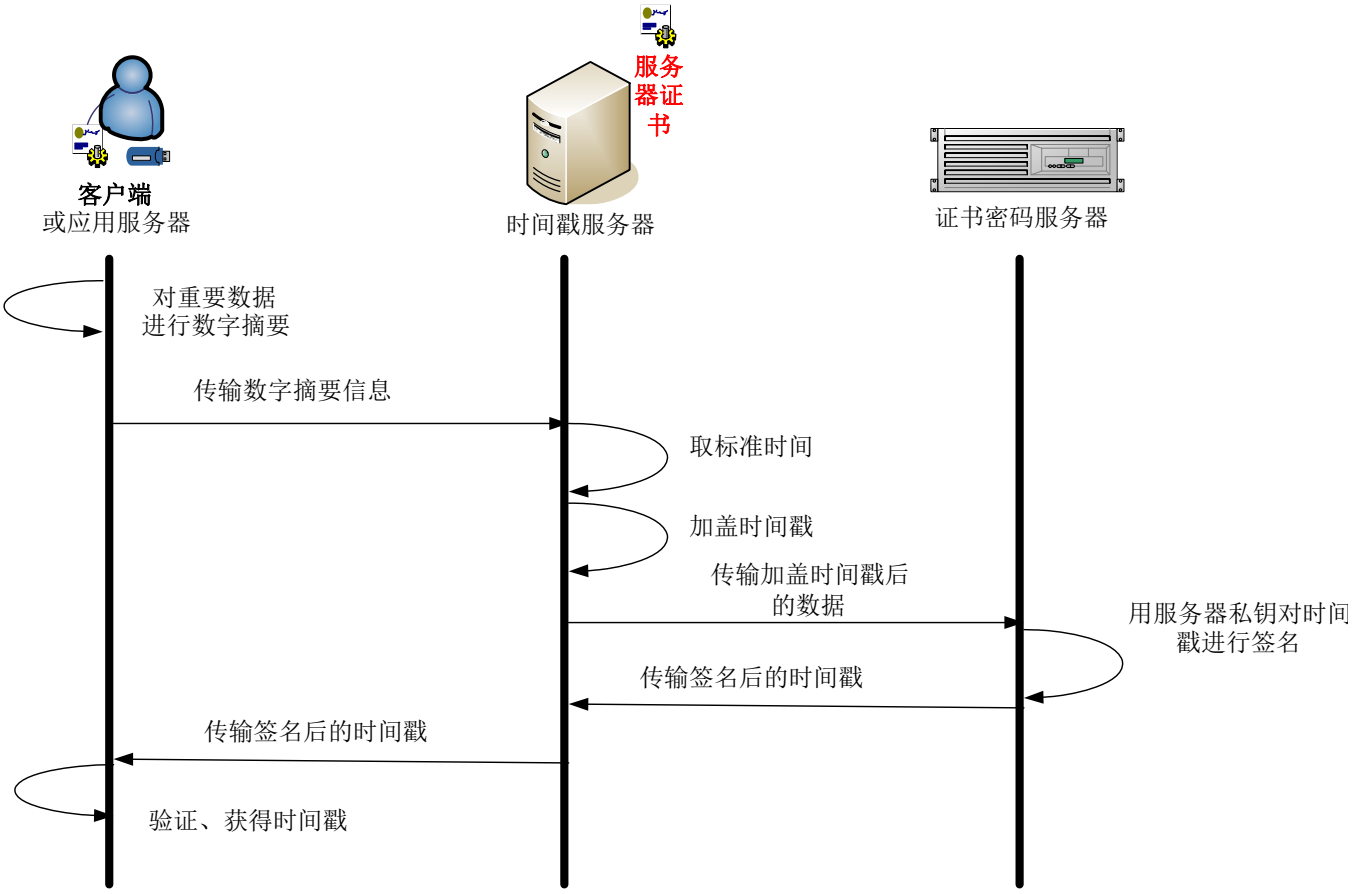
6.3 对网上重要操作行为不可抵赖的实现

电子签名是实现网上操作行为不可抵赖的最有效方法，对数据的签名和验签，是利用用户的签名私钥，对数据进行签名运算，并把签名结果保存起来。因为用户的私钥只有他自己才能使用，因此这个签名的数据就具有唯一性和法律效力，不能被修改。当需要对数据的有效性进行验证时，只要再用用户的证书进行一次运算就可以了。具体的实现流程如下图所示：



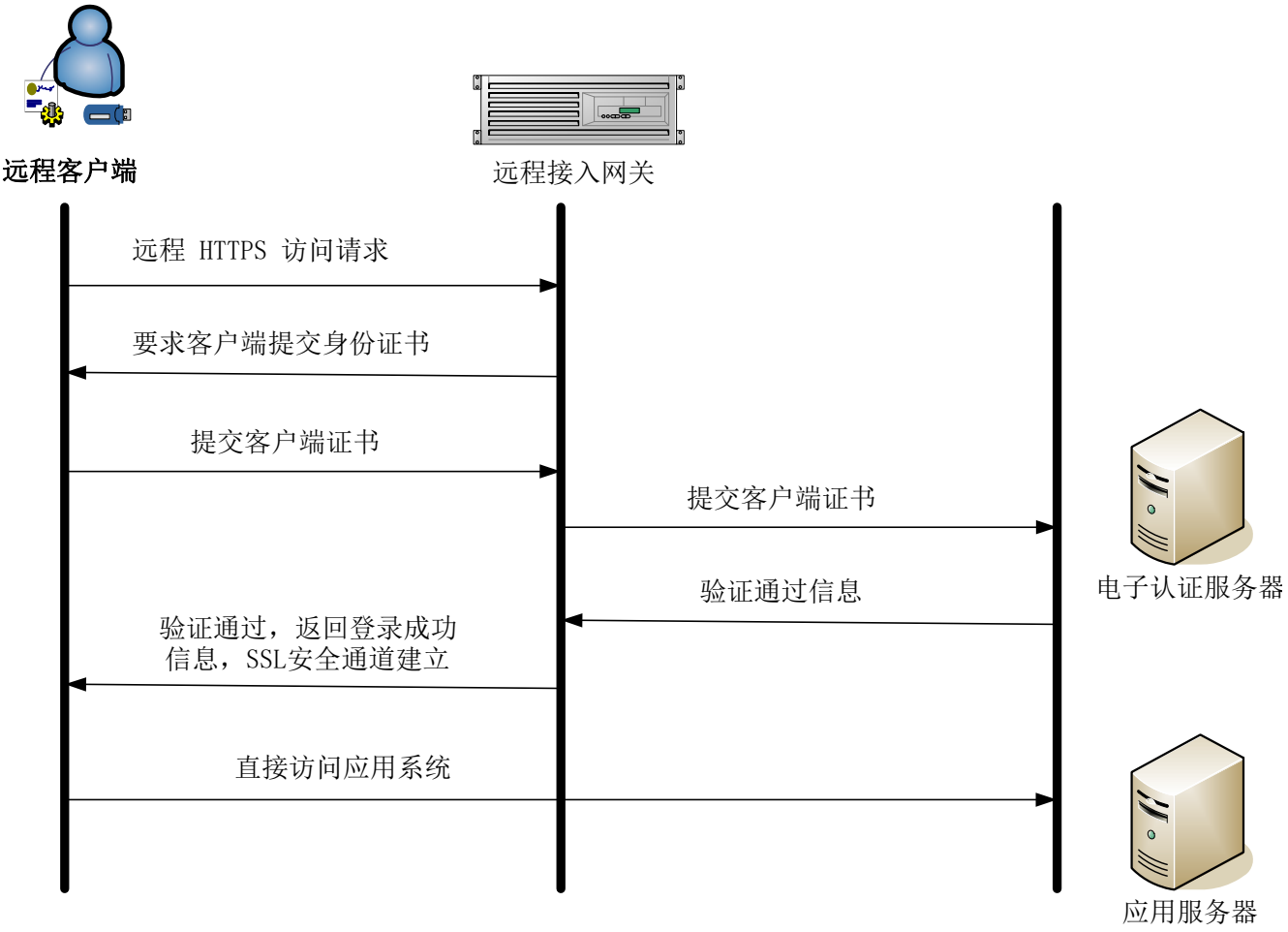
6.4 对重要时间确认的实现

在各种药品采购的处理流程中，时间是十分重要的信息。对于本项目来说，数字时间戳服务同样十分重要。在公文的处理中，文件签署的日期和签名一样，均是十分重要的防止文件被伪造和篡改的关键性内容。由于用户桌面时间很容易改变，由该时间产生的时间戳不可信赖，因此需要一个权威第三方来提供可信赖的且不可抵赖的时间戳服务。时间戳服务的具体实现过程如下：



6.5 远程安全办公的实现

远端用户要使用安全的方式访问内部的应用系统，可以利用 SSL VPN 技术，这是目前国际上解决安全传输的主流技术，通过如下几个流程实现：



1、首先使用标准浏览器访问远程接入网关，出现登陆界面。

2、经过 SSL 的握手，交换证书，加密参数协商等步骤进行用户的认证和鉴权。鉴权方式可以采用平台已有的统一认证方式。

3、认证成功后，客户端就会显示可访问的系统，所有数据的传输都将经过加密。对于 C/S 结构的应用需要从网关上下载 java applet 或 ActiveX 来作为安全代理来访问。

7 培训和技术支持

7.1 培训

为保证最终用户（公务员和企业）能方便的使用数字证书，网证通将采用分批集中培训的方式，每个应用单位派 2－3 名业务人员参加，在不同的时间段（例如每月）安排一次集中培训。如果不能参加现场培训的用户，可以制作使用手册和录像，随证书产品的发放一起提供给用户或放在公众网站上供用户下载学习。

培训内容包括：

1、 PKI/CA 基础

2、 数字证书的安装

3、 数字证书在集团信息系统中的使用

4、 其它相关知识

7.2 网证通提供的技术支持

网证通就所提供的 PKI 应用开发接口、PKI 软硬件产品的应用和维护为有关编程人员提供免费培训，并现场协助系统开发人员进行系统调试工作。力求使应用系统开发人员完全掌握本项目各产品的知识和操作使用技能。

用户方自购买产品之日起，为用户方提供技术咨询服务，包括：

- 安装配置说明
- 产品的应用接口使用技术培训。
- 网络安全常识问题的解答；
- 安全产品介绍；
- 安全策略的制定；
- 常见疑难问题解答；
- 数字证书办理流程及使用的咨询；

- 指导用户安装数字证书；
- 受理数字证书用户的证书服务相关投诉；
- 排除数字证书在各业务系统中的使用故障；
- 提供对证书硬件载体客户端工具以及驱动程序的开发和维护；
- 提供对使用数字证书的各业务系统的技术指导及支持。

NET CA 将通过以下方法与用户方保持联系，提供包括产品介绍、使用相关问题的解答、安装配置说明、常见疑难问题解答等服务内容。NET CA 设立专业的技术服务支持队伍，提供现场技术支持服务、电话技术支持服务、电子邮件技术支持服务等多种方式，务求在最短时间内解决问题。

7.2.1 现场支持服务

对于严重影响用户方系统正常运作的产品故障，在电话支持无法解决的情况下，NET CA 派工程师到现场为用户方解决产品故障。系统开发和调试阶段，NET CA 负责对有关编程人员的培训和现场开发人员共同进行系统的调试；

7.2.2 7*24 小时在线支持

广东省电子商务认证有限公司 7*24 小时运作的互联网站点可以提供客户服务和技术支持信息，您还可以通过电子邮件与我们的客户服务人员取得联系，解决在证书申请和使用过程中遇到的问题。

客服免费电话：400－830－1330

服务邮箱：support@cnca.net。

7.3 产品保修

电子密钥保质期为一年。在质保期内发生质量问题的电子密钥广东省电子商务认证中心免费更换。其它产品购买之日起一年内出现的正常使用下发生的系统软件故障，广东省电子商务认证中心负责免费维修。对于以下几种情况，不在保修范围，用户方若申请服务，广东省电子商务认证中心在进行服务时将酌情收取一定的材料成本费或维修劳务费：

- 产品或其部件已超出免费保修期；
- 因使用环境不符合产品使用要求而导致的硬件故障；

- 因不良的电源环境（如无规定的稳压设备）或异物进入设备所引起的故障或损坏；
- 因带电热拔插等误操作而引起的硬件故障；
- 未经广东省电子商务认证中心授权而对产品进行拆卸、修理、升级、改装而造成的故障；
- 由于未能按使用操作手册上所写的使用方法和注意事项进行操作而造成的故障；
- 由于不可抵抗力如：雷电、水火灾等自然因素而造成的故障。

8 方案小结

8.1 网证通解决方案特点

8.1.1 遵循国际标准、符合国家规定

➢ **双证书**

双证书是 NETCA 数字证书的特征之一。是指分配给每个证书持有人的密钥是两对，其中一对专用于数字签名，叫签名密钥对；一对专用于加密，叫加密密钥对。双证书机制将用户的签名密钥对与加密密钥对相分离。为满足对密钥管理和国家安全的需要，NETCA 对加密密钥实施强制托管，以便授权的政府部门在紧急情况下能对加密的信息进行恢复。同时，为提供对用户隐私（签名权）的保护，NETCA 对签名密钥不予托管。因此，采用双证书机制，能够有效地避免因密钥托管而导致用户隐私泄漏的问题。NETCA 为进一步强化证书实体对签名私钥的独占性，签名密钥对在证书持有人的客户端设备－电子签名证书载体中产生。使用时，也是在该设备中完成签名运算，签名密钥对的私钥从不出此密码设备。

➢ **安全性**

CA 系统体系结构在系统设计与开发时重点考虑了对标准 X.509 证书及 CRL 的签发及管理，同时全面考虑了系统的安全性，主要包括环境安全控制、流程安全控制、人员安全控制、系统设计安全、日志安全管理、网络安全设计等方面

➢ **可靠性**

合理的系统设计以及软件能够适应长期的、多样的运行环境的特点，可靠地保证了 CA 系统体系高效，准确运转。签发服务器对多线程的支持和目录服务接口设计的合理，使系统支持大量事务处理。

支持多平台，可移植性好，证书查询与验证支持一主多从，支持高容错，大批量数据查寻，

同时满足实时性要求。

在设计中采用了数据备份技术，可以保证系统的高可靠性。

- **灵活性**

CA 采用分布式、可配置的模块化设计，确保系统的灵活性和适用性。在 CA 中心的建设过程中，用户可从本组织的实际应用需求出发进行灵活的配置。

- **标准性**

严格遵守国际和国家的相关标准，证书格式和内容：X.509 V3

8.1.2 全面、灵活、按需扩展的应用安全解决方案

全面的应用安全解决方案－－提供梯度式、渐进式的应用安全解决方案，从低层的 PKI 安全改造、统一用户管理、证书查询验证到高层的应用扩展、证书管理，构建全面的应用安全保障体系，满足不同安全等级的安全管理需求；

灵活多变的应用安全组合－－提供多种类型的数字证书，为多种实体提供证书服务，快速应对不断增长的业务需求；兼容多个厂家和品牌的安全产品（包括加密设备、存储介质等），能有效降低使用单一来源厂商和产品的风险。

可扩展、可按需定制的数字证书－－根据业务发展需要，可定制数字证书相应的扩展域、支持个性化信息写入，满足业务不断变化的需求。

8.1.3 与应用高度耦合的安全中间件接口

应用安全中间件接口基于 PKI 技术、与具体的设备和厂家无关，能够实现数字证书密钥管理、读取数字证书域信息、数据加解密、数字签名及验证、证书状态查询等功能，屏蔽安全技术的实现细节，可方便、快速地实现数字证书安全登录、加密传输信息等应用。

安全中间件接口已在多个政府部门、行业、大中型企业成功实施、实际运行、历经长时间的考验，产品成熟可靠；遵循国际标准，非封闭、非依赖厂商、具有自主知识产权，可按需增加或修改接口以满足应用需求，能与应用高度耦合。

丰富的应用安全改造经验、拥有 CA 平台和各 PKI 应用安全产品完整的自主知识产权、实力强大的技术支持队伍，积极走“以应用推动证书发展、以证书保障应用安全相结合”道路，拥有大量的证书与应用的快速结合案例。