东兴证券 DONGXING SECURITIES

PKI应用领域广市场前景好，密码应用大有可为

——密码行业深度系列报告之一

2019 年 04 月 24 日

看好/维持

国防军工 | 深度报告

陆洲

010-66554142 luzhou@dxzq.net.cn

执业证书编号: S1480517080001

王习

010-66554034 Wangxi@dxzq.net.cn

执业证书编号: S1480518010001

研究助理：张卓琦

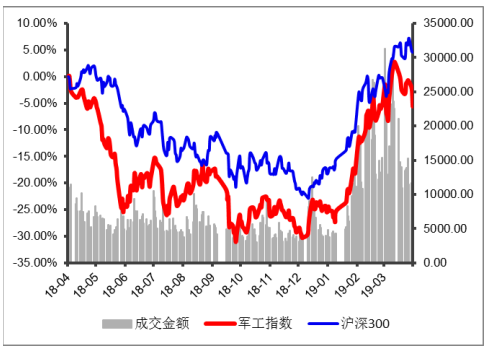
010-66554018 Zhangzq_yjs@dxzq.net.cn

执业证书编号: S1480117080010

细分行业	评级	动态
密码行业	看好	维持

行业基本资料		占比%
股票家数	53	1.46%
重点公司家数	3	
行业市值	8325.13 亿元	1.32%
流通市值	544.01 亿元	1.09%
行业平均市盈率	89.51	/
市场平均市盈率	16.54	/

行业指数走势图



资料来源：东兴证券研究所

相关研究报告

投资摘要：

PKI 系统构建网络安全防线。在网络安全中，身份认证作为第一道，甚至是最重要的一道防线。身份认证就是在网络系统中通过某种手段确认操作者身份的过程，其目的在于判明和确认通信双方和信息内容的真实性。基于公共密钥的认证机制拥有 Kerberos 的认证机制的优点，同时使用非对称加密技术，拥有极高的安全性，也解决了用户过多时密钥管理的问题，是目前应用中最为安全可靠的方法，但是实现起来较为复杂，需要建设相应的配套设施，目前较为流行和完善的是以 PKI 为核心的一套信息安全系统。当前网络技术快速升级迭代，建设基于 PKI 的网络安全系统是网络安全面临的一项紧迫任务。

受益等保 2.0，PKI 应用领域将得到极大推广，在物联网时代极具市场前景。PKI 中核心载体为数字证书，即由具有公信力的机构（CA）为个人颁发的身份证明，其可看作个人在虚拟网络世界的身份证。PKI 产品广泛应用于平时生活中，使用 PKI 技术的应用包括安全认证网管关（保证远程连接安全）、网银（Usb Key 证书或文件证书）、安全电子交易（数字签名和验签）等。目前，国内设计高等级安全性应用的相关领域，均不同程度的采用了 PKI 技术。受益等保 2.0，在金融领域、移动支付领域、云计算领域、电子政务领域都对 PKI 技术有强需求。且未来物联网有巨大市场空间，密码应用产业将是一片蓝海。

密码应用大有可为，密码相关企业将充分受益。卫士通作为我国网络安全国家队，深耕密码行业，已经围绕密码体系构建了非常完整的安全系统。新任董事长卿昱上任后管理风格变化明显，目前已经与各业务线主管签订年度目标责任书，提出奋战二季度。格尔软件作为 PKI 系统基础设施提供商，为我国政府多个部门提供产品，是 PKI 行业领军企业。数字认证作为 PKI 系统应用方，是电子认证技术优势企业，可提供一体化的电子认证解决方案，充分受益电子认证行业快速发展。

中国网安新任董事长卿昱认为，全民密码时代需要构建一个密码管理的体系和统一信任的体系，为密码的普适性提供基础的核心支撑。同时，全民密码时代也要打通密码和电力、通信、交通、金融等行业接口，实现数据的互联、互通和共享。我国密码行业受益于目前我国对安全日益重视的大趋势，在自主可控、等保 2.0 等行业利好催化下，密码行业相关公司将进一步做大做强。我们看好密码行业的发展，给予“看好”评级。

投资策略：把握密码行业投资主题，我们重点推荐卫士通（002268.SZ），背靠中国网安，持续拓展密码技术应用，已形成完整的信息安全产品体系，一季度开局顺利、成绩骄人。格尔软件（603232.SH），已形成基于 PKI 的信息安全产品系列，并不断拓宽产品应用范围，实现国际化支持；主营业务在政府、军工、电子政务、金融领域稳步推进，国产自主可控、未来业绩增长可期。数字认证（300579.SZ），是领先的网络安全解决方案提供商，提供电子认证服务、安全集成、安全咨询与运维服务，业务多点开花，已在政务、金融、医疗卫生、电信、教育、交通等领域建立领先优势，“一体化”电子认证解决方案具备竞争优势，市场占有率有望进一步提高。

风险提示：PKI 应用推广不足预期，业绩增速不及预期。

行业重点公司盈利预测

简称	EPS（元）			PE			PB
	18A	19E	20E	18A	19E	20E	
卫士通	0.19	0.65	0.96	156	45	31	5.63
格尔软件	0.84	1.09	1.42	49	38	29	5.67
数字认证	0.72	1.02	1.48	65	46	32	9.30

目录

表格目录

插图目录

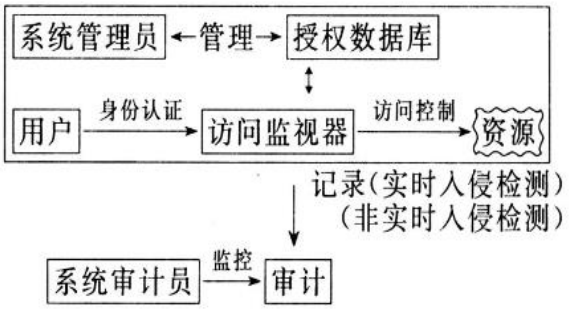
1. PKI 系统构建网络安全防线

1.1 身份认证技术是网络安全最重要的一道防线

随着信息化的快速发展，对国家、组织、公司或个人来说至关重要的信息越来越多的通过网络来进行存储、传输和处理，为获取这些关键信息的各种网络犯罪也相应急剧上升。企业以及电子政务的信息系统面临着越来越严重的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。当前，网络安全在某种意义上已经成为一个事关国家安全和社会经济稳定的重大问题，受到越来越多的重视。

在网络安全中，身份认证是第一道，甚至是最重要的一道防线。身份认证就是在网络系统中通过某种手段确认操作者身份的过程，其目的在于判明和确认通信双方和信息内容的真实性。

图 1：用户访问网络资源的流程



资料来源：百度百科、东兴证券研究所

一般情况下，用户在访问系统之前，首先要经过身份认证系统来识别身份，而后才能访问监视器。根据用户的身份和授权数据库来决定用户是否有权访问某个资源，审计系统记录用户的请求和行为，同时入侵检测系统会实时或非实时地检测是否有入侵行为。可以看出，身份认证是网络安全体系中的第一道关卡，其它的安全服务如访问控制、审计等都依赖于它。一旦非法用户通过了身份认证，就会对系统和资源的安全构成极大的威胁。因此，身份认证是网络安全中的一个重要环节。

1.2 基于 PKI 建设的身份认证系统最为安全可靠

在整个安全系统中，身份认证技术是重点，基本安全服务就是身份认证，其他安全服务也都建立在身份认证的基础上。这使得身份认证系统具有十分重要的地位，也最容易遭受攻击。因此，建立安全的身份认证系统是网络安全的首要步骤。目前常用的网络身份认证机制包括基于口令的身份认证机制、挑战/响应认证机制、基于 DCE/Kerberos 的认证机制以及基于公共密钥的认证机制。

（1）基于口令的认证机制

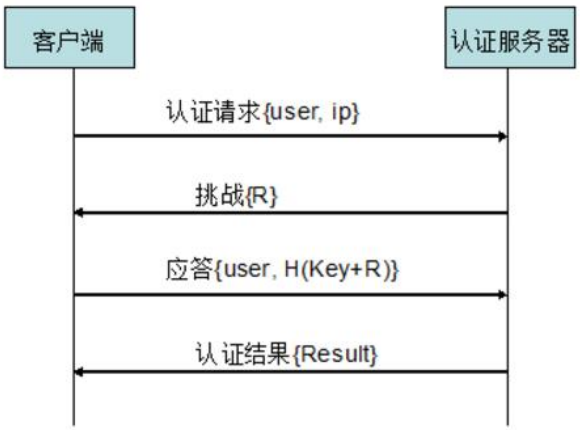
基于口令的身份认证技术一般包括账户名和密码，用户通过固定的用户名确认身份信息，通过密码验证是否是本人。因简单易用，基于口令的身份认证技术是目前使用最

为广泛的身份认证方式，一般包括基于静态口令的认证方式和动态口令认证。基于口令的身份认证系统简单效率高，但安全性比较差，仅依赖于口令，口令一旦泄露，用户即可被冒充。容易受到攻击，采用窥探、字典攻击、穷举尝试、网络数据流窃听、重放攻击等很容易攻破该认证系统。

（2）基于挑战/响应的认证机制

基于挑战/响应的身份认证机制，即认证服务器端向客户端发送不同的“挑战”码，客户端程序收到 “挑战”码后，根据客户端和服务器之间共享的密钥信息，以及服务器端发送的“挑战”码，做出相应 “应答”。服务器根据应答的结果确定是否接受客户端的身份声明。本质上讲，这种机制也是一次性口令。

图 2：典型基于挑战/响应的认证机制的认证过程



资料来源：网络公开资料，东兴证券研究所

具体认证过程为：1）客户向认证服务器发出请求，要求进行身份认证；2）认证服务器从用户数据库中查询用户是否是合法的用户，若不是，则不做进一步处理；3）认证服务器内部产生一个随机数，作为“挑战”码，发送给客户；4）客户将用户名字和随机数合并，使用单向 Hash 函数（例如 MD5 算法）生成一个字节串作为应答；5）认证服务器将应答串与自己的计算结果比较，若二者相同，则通过一次认证；否则，认证失败；6）认证服务器通知客户认证成功或失败。

基于挑战/响应认证机制的身份认证系统一定程度上加强了安全性，但并不能完全阻止黑客破坏。比如未验证黑客身份为超级用户，黑客有可能使用拒绝服务性的攻击方式，使得授权用户不能通过认证。

（3）基于 DCE/Kerberos 的认证机制

Kerberos 是为解决分布式网络认证而设计的可信第三方认证协议。网络上的每个实体持有不同的密钥，是否知道该密钥便是身份的证明。网络上的 Kerberos 服务起着可信仲裁者的作用，可提供安全的网络认证。

该认证机制下，设立可信任的第三方，即认证服务器（AS）。AS 为客户和服务器提供证明身份的身份证书以及双方安全通信的会话密钥。此外还会授予服务器(TGS)，TGS 向 AS 的可靠用户发出身份证书。除客户第一次获得的初始证书是由 AS 签发外，其他票据都是由 TGS 签发的，每个票据可以使用多次直至期限。客户方请求服务方提供服务时，不仅要向服务方发送从 TGS 领来的身份证书，同时还要自己生成鉴别码一并发送。

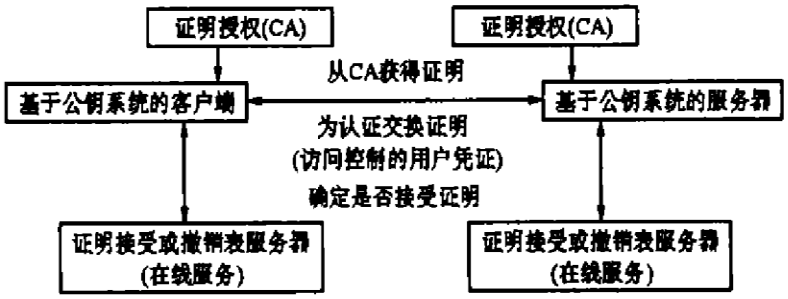
与传统的认证协议相比，Kerberos 协议具有一系列的优势。首先，它支持双向的身份认证，而大部分传统的认证协议都是基于服务器可信的网络环境，往往都是只验客户，但客户无法验证服务器。Kerberos 协议中只有 AS 和 TGS 是可信的，网络的所有工作站、服务器都是不可信的。当用户与服务器进行交互时，Kerberos 为客户抵挡了网络恶意攻击和欺骗。其次，Kerberos 实现了一次性签放，在有效期内可多次使用。假如用户在一个开放网络环境中需要访问多个服务器，如查询邮件、打印文件、访问 FTP 等都在不同的服务器上，用户通过 AS 申请 TGS 的证书后，在有效期内利用该证书与 TGS 多次请求不同访问授权票据。降低了用户输入口令次数，从而提高了用户的体验。最后，Kerberos 提供了分布式网络环境下的域间认证机制，允许客户花费少量的资源即可访问其他子域的服务，是传统的认证协议难以实现的。

Kerberos 协议也存在不足和安全隐患。Kerberos 身份认证采用的是对称加密机制，加解密都需要相同的密钥，交换密钥时的安全性不能保障。Kerberos 协议对时钟的要求比较高，必须在时钟基本同步的环境中，如果引入事件同步机制则需保证同步机制的安全；若时间不同步，攻击者可以通过调节时钟来实现重放攻击。在 Kerberos 中，客户信息和服务器认证信息都集中存放在 AS 服务器中，其安全性严重依赖于 AS 和 TGS 的性能和安全。随着用户数量的增加，Kerberos 需要维护复杂的密钥管理。

（4）基于公共密钥的认证机制

基于公共密钥的安全策略进行身份认证，即使用符合 X.509 协议的身份证明。须有一个第三方的证明授拟中心为客户签发身份证明。客户和服务器信任该证明授权中心，并各自获取证明，在会话和通讯时首先交换身份证明，其中包含了将各自的公钥交给对方，然后才使用对方的公钥验证对方的数字签名、交换通讯的加密密钥等。在确定是否接受对方的身份证明时，还需检查有关服务器，以确认该证明是否有效。

图 3：基于公共密钥的认证机制架构



资料来源：网络公开资料，东兴证券研究所

基于公共密钥的认证机制拥有 Kerberos 的认证机制的优点，同时使用非对称加密技术，拥有极高的安全性，也解决了用户过多时密钥管理的问题，是目前应用中最为安全可靠的方法。

表 1：常用身份认证机制

认证机制	优点	不足
基于口令的身份认证机制	简单，方便，应用广泛	安全性仅依赖于口令，安全性比较差
挑战/响应认证机制	简单，密码不以明文出现，有一定的安全性	抵挡黑客攻击能力差
DCE/Kerberos 的认证机制	身份双向认证；身份一次签放多次使用；适合分布式系统	对称密码技术易被破解，用户多时密钥管理不方便
公共密钥的认证机制	身份双向认证；身份一次签放多次使用；非对称加密技术安全性高；适合分布式系统；	需要建设相应的配套设施

资料来源：网络公开资料，东兴证券研究所

然而，**基于公共密钥的认证机制实现起来较为复杂，需要建设相应的配套设施，目前较为流行和完善的是以 PKI 为核心的一套信息安全系统。**

2. PKI 是网络安全的定海神针

身份认证技术是网络安全基础性和核心的技术，构成网络空间安全的第一道防线，发挥着“保底”作用。当前网络技术快速升级迭代，建设基于 PKI 的网络安全系统是网络安全面临的一项紧迫任务。

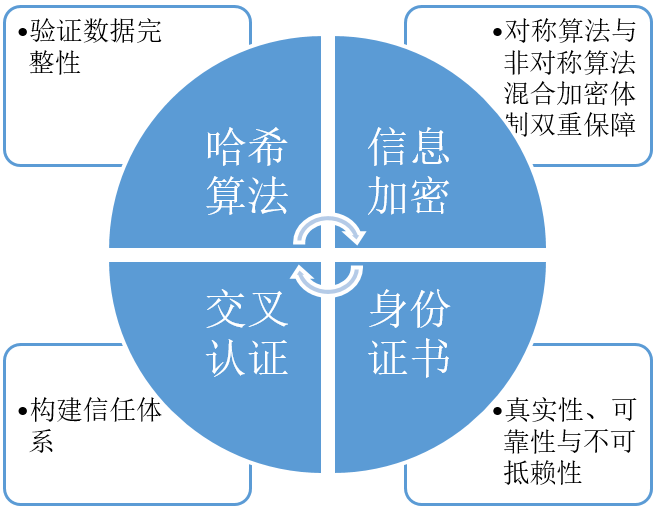
2.1 PKI 介绍

PKI 即公钥基础设施（Public Key Infrastructure），是用公钥概念与技术来实施和提供安全服务的普适安全基础设施，是产生、管理、储存、分发和撤销基于公开密钥密码学的公钥证书所必须的软件、硬件、人、策略和处理过程的集合；是国际公认的能够全面解决信息安全问题的、普遍适用的一整套信息安全系统。

2.1.1 PKI 使用哈希算法、非对称加密等技术，保障网络安全

网络安全中需要解决信息的机密性、完整性、真实性、可靠性、可用性、可控性和不可抵赖性，PKI 能够为信息系统提供密钥管理和证书管理等基础性安全服务，为应用提供认证、加密和数字签名等安全支撑，运用多种技术保障网络安全，构建国家网络信任体系的基础。

图 4：PKI 技术架构



资料来源：网络公开资料，东兴证券研究所

（1）哈希算法验证信息完整性

为保证数据的完整性，用指定算法根据原始数据计算出校验值。接收方用同样的算法计算一次校验值，如果和随数据提供的校验值一样，就说明数据是完整的。常用的几种数据校验方式有奇偶校验、CRC 校验、LRC 校验、格雷码校验、基于摘要算法的校验等。其中，基于摘要算法的校验是安全性最高的方式。

摘要算法也被称为哈希（Hash）算法、散列算法。Hash 函数其作用是对整个消息进行变换，产生一个长度固定但较短的数据序列，这一过程可看作是一种压缩编码。接受者收到发送的信息序列后，按照发送端同样的方法对接收的数据或解密后的数据的前面部分进行计算，得到相应的 r 位数字 Ar 或 Dr 而后，与接收恢复后的 As 或 Ds 逐位进行比较，若全部相同，就可认为收到的信息是合法的，否则检出消息有错或被窜改过。当主动攻击者在不知道密钥的情况下，随机选择 r 位碰运气，其成功伪造消息的概率为2^{-r}。常见的摘要算法包括 MD5、SHA、MAC 等

在 PKI 系统中使用的是 MAC(Message Authentication Code)验证方法，兼容了 MD 和 SHA 算法的特性，并在此基础上加上了密钥，因此 MAC 算法也经常被称作 HMAC 算法。使用 MAC 验证消息完整性的典型流程是：

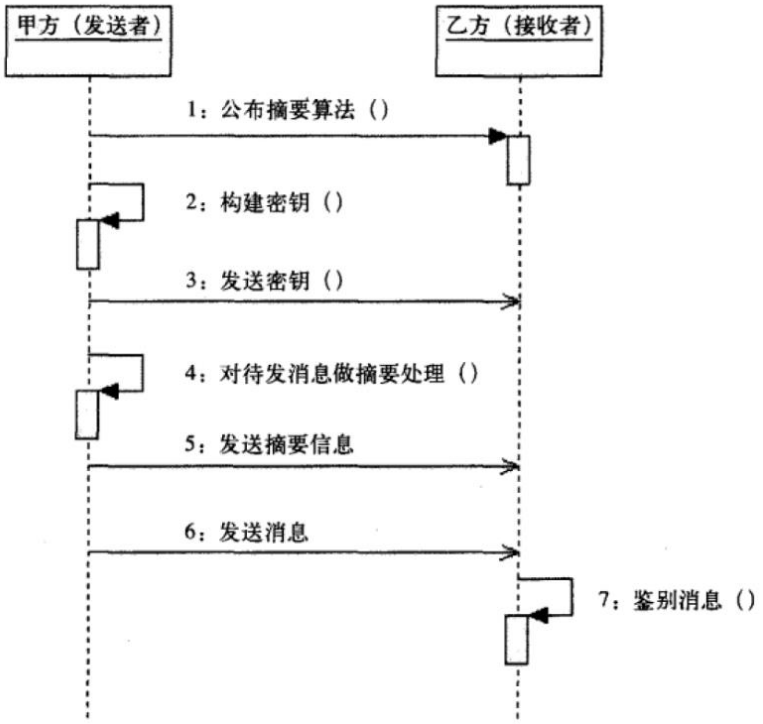
1）甲方向乙方公布摘要算法（就是指定要使用的摘要算法名）；

2）甲乙双方按照约定构造密钥，双方拥有相同的密钥（一般是一方构造密钥后通知另外一方，此过程不需要通过程序实现，为双方约定的字符串，但是这个字符串并非随便设定的，是通过相关算法获取的）；

3）甲方使用密钥对消息做摘要处理，然后将(2)生成的密钥和生成的摘要消息一同发送给乙方；

4）乙方收到消息后，使用甲方已经公布的摘要算法+约定好的密钥 对收到的消息进行摘要处理。然后比对自己的摘要消息和甲方发过来的摘要消息。甄别消息是否是甲方发送过来的。

图 5：哈希算法流程



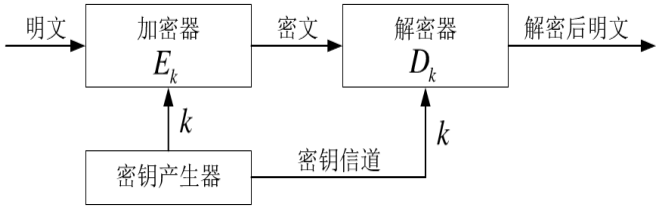
资料来源：网络公开资料，东兴证券研究所

（2）数据加密技术保障数据安全性

信息加密技术常用的方法为对称加密算法和非对称加密算法。

在对称加密算法中，数据发信方将原始数据和加密密钥经过特殊加密算法处理后，变成复杂的加密密文发送出去。收信方收到密文后，需要使用加密用过的密钥及相同算法的逆算法对密文进行解密。在对称加密算法中，只使用的一个密钥，发收信双方均使用该密钥对数据进行加密和解密。

图 6：对称算法流程

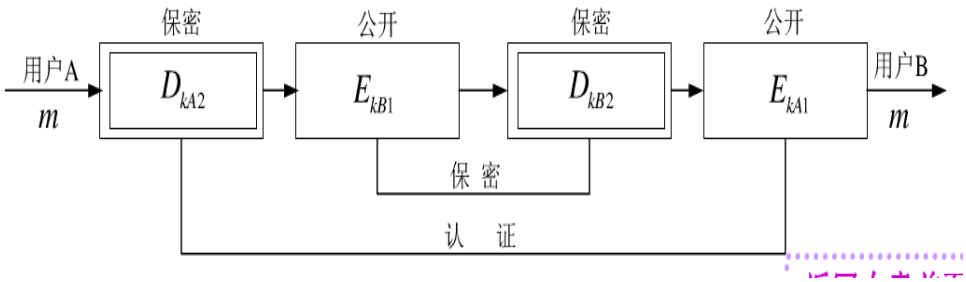


资料来源：网络公开资料，东兴证券研究所

对称加密算法的优点是算法公开、计算量小、加密速度快、加密效率高。在计算机专网系统中广泛使用的对称加密算法有 DES、IDEA 和 AES。不足之处是，交易双方使用同样的钥匙，安全性得不到保证。此外，每对用户每次使用对称加密算法时，都需要使用其他人不知道的唯一钥匙，这会使得发收信双方所拥有的钥匙数量成几何级数增长，密钥管理成为用户的负担。因为密钥管理困难，使用成本较高，对称加密算法在分布式网络系统上使用较为困难。

非对称加密算法使用两把完全不同但又完全匹配的一对钥匙——公钥和私钥。非对称加密算法实现机密信息交换的基本过程是：甲方生成一对密钥并将其中的一把作为公用密钥向其它方公开；得到该公用密钥的乙方使用该密钥对机密信息进行加密后再发送给甲方；甲方再用自己保存的另一把专用密钥对加密后的信息进行解密。甲方只能用其专用密钥解密由其公用密钥加密后的任何信息。

图 7：非对称算法流程



资料来源：网络公开资料，东兴证券研究所

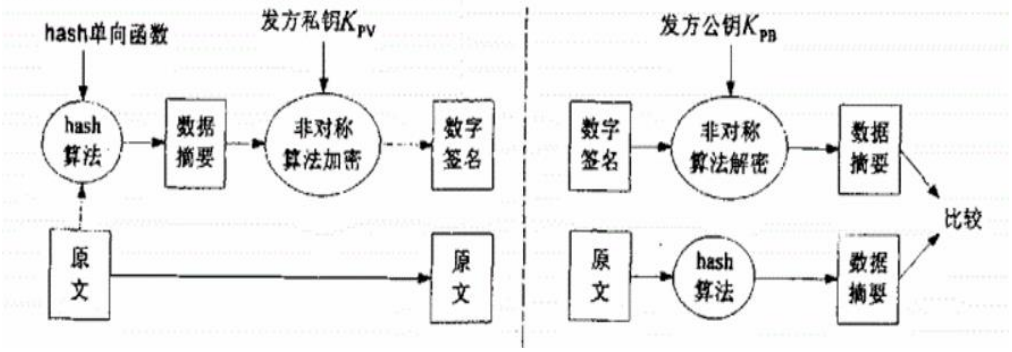
显然，采用非对称加密算法，收发信双方在通信之前，收信方必须将自己早已随机生成的公钥送给发信方，自己保留私钥。使用非对称加密算法可以将加密和解密能力分开，既可以用于实现公共通信网的保密通信，也可用于认证系统中对消息进行数字签名。由于不对称算法拥有两个密钥，密钥管理问题比较简单，特别适用于分布式系统中的数据加密。广泛应用的不对称加密算法有 RSA 算法和美国国家标准局提出的 DSA。

在 PKI 体系中使用的是双钥和单钥密码相结合的混合加密体制，即加密时采用单钥密码，密钥传送则采用双钥密码。这样既解决了密钥管理的困难，又解决了加解密速度的问题。

（3）数字证书

PKI 中最重要的就是引入了数字证书。数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息和公开密钥的文件，最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。数字签名，是指用户用自身私钥对原始数据的哈希摘要进行加密所得的数据，是非对称密钥加密技术与 Hash 摘要技术的应用。数字签名技术是将摘要信息用发送者的私钥加密，生成一段信息，与原文一起传送给接收者。这段信息类似于现实中的签名或印证，接收方对其进行验证，判断原文真伪。数字签名在 PKI 中提供数据完整性保护和不可否认性服务。

图 8：PKI 系统数字签名技术流程



资料来源：网络公开资料，东兴证券研究所

一般情况下，PKI 系统中的证书还包括密钥的有效时间、发证机关（证书授权中心）的名称、该证书的序列号等信息，证书的格式遵循 ITU-T 标准化部门定义的 X.509 协议，这是 PKI 技术体系中应用最为广泛、最为基础的一个国际标准。X.509 证书包含以下数信息：

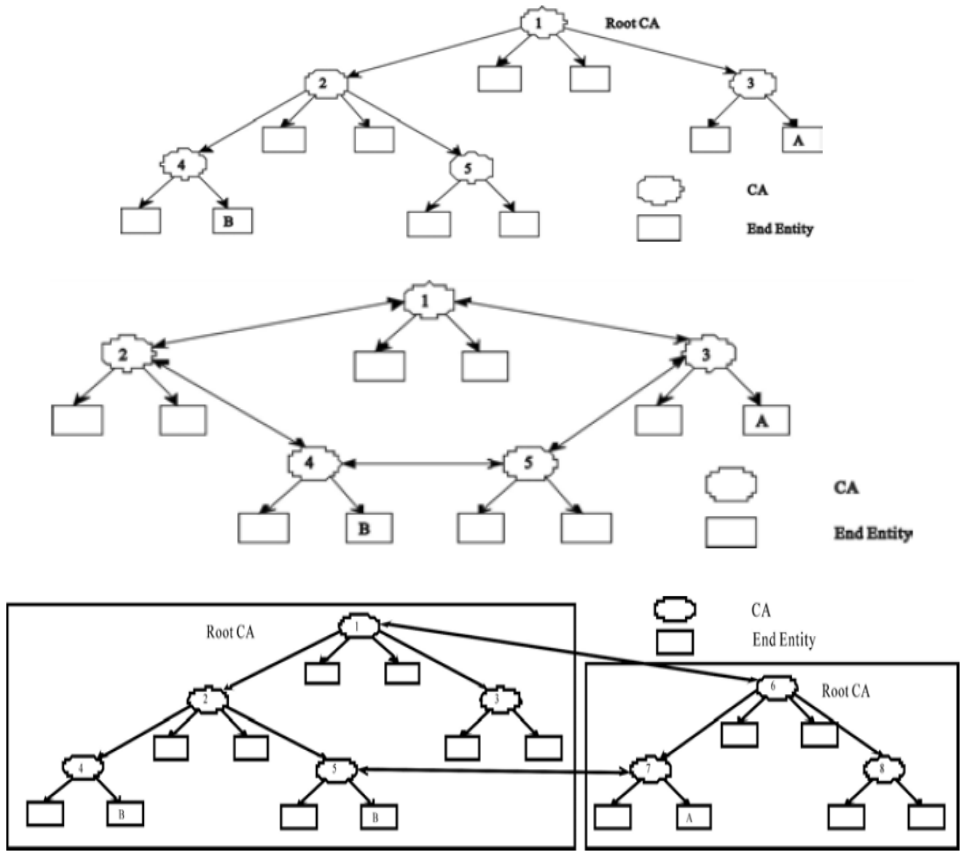
- **证书版本。**指出该证书使用了哪种版本的 X.509 标准，版本号会影响证书中的一些特定信息。
- **证书的序列号。**创建证书的实体(组织或个人)有责任为该证书指定一个独一无二的序列号，以区别于该实体发布的其他证书。序列号信息有许多用途，例如当一份证书被回收以后，它的序列号就被放入证书回收列表(CRL)之中。
- **签名算法标识。**指明 CA 签署证书所使用的算法。
- **证书有效期。**证书起始日期和时间以及终止日期和时间，指明证书何时失效。
- **证书发行商名字。**这是签发该证书的实体的唯一名字，通常是 CA。使用该证书意味着信任签发证书的实体。(注意，在某些情况下，例如根或顶级 CA 证书，发布者自己签发证书)
- **证书主体名。**证书持有人唯一的标示符，也称为 DN(Distinguished Name)，这个名字在 Internet 上应该是唯一的。
- **主体公钥信息。**包括证书持有人的公钥、算法(指明密钥属于哪种密码系统)的标示符和其他相关的密钥参数。

- **发布者的数字签名。**这是使用发布者私钥生成的签名。

（4）交叉认证

建立和管理一个全世界所有用户都信赖的全球性系统是不现实的，比较可行的方案是建立多个信任域，独立地运行和操作，然后在不同的信任域之间建立起“交叉认证”的能力。**在网络环境中，PKI 为需要进行安全通信的双方建立了一种信任关系，这种信任关系的建立是通过对证书链的验证来完成的。**证书链由一系列彼此相连接的证书组成，起始端称为“信任锚”，是验证方信任的起始点。证书链的末端是要验证的用户证书，中间可能存在零或多个 CA 证书。“信息锚”的选择和证书链的构造方式不是唯一的，并构成了不同的信任模式。信任模式包括级联模式、网状模式、以及混合模式等。

图 9：信任模式：级联，网状，混合



资料来源：网络公开资料，东兴证券研究所

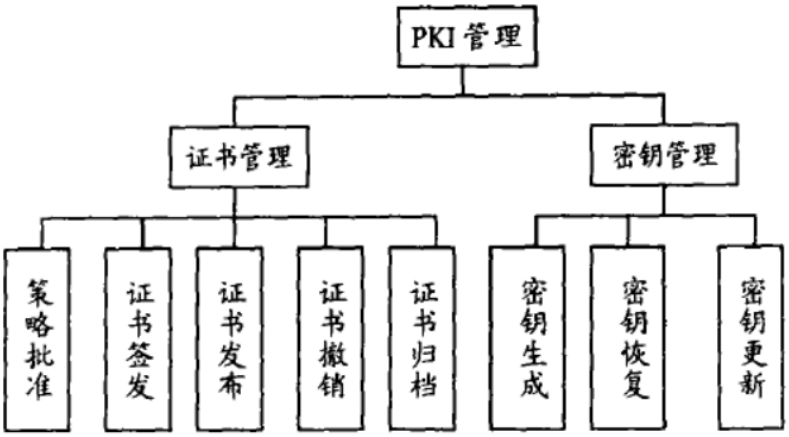
2.1.2 PKI 以 CA 为架构核心，提供全套安全服务

PKI 是目前应用最为广泛的一种加密和认证体系，其安全性建立在负载的数学运算方式上，能够有效解决身份认证、访问控制、数据安全、数字签名及验证等诸多安全

问题。PKI 中核心载体为数字证书，即由具有公信力的机构（CA）为个人颁发的身份证明，其可看作个人在虚拟网络世界的身份证。网络用户通过次身份证已确认其身份的合法性和有效性，从而彻底解决其在虚拟网络世界的身份认证和信任问题。

PKI 在实际应用上是一套软硬件系统和安全策略的集合，它提供了一整套安全机制，包括管理加密密钥和证书的公布，提供密钥管理（包含密钥更新，密钥恢复和密钥托付等）、证书管理（包含证书产生和撤销等）和策略管理等。

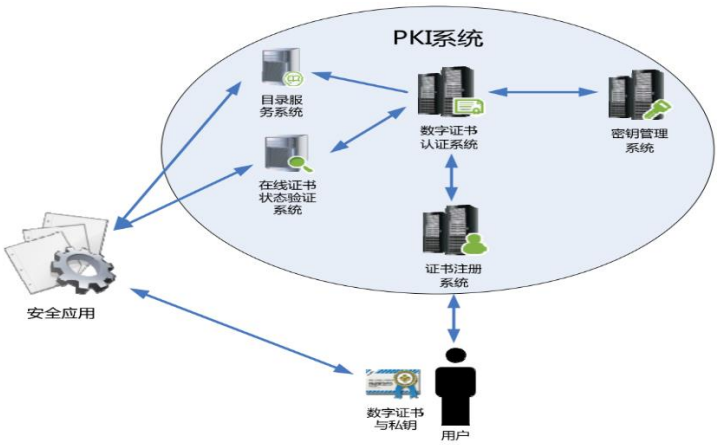
图 10：PKI 主要功能



资料来源：网络公开资料，东兴证券研究所

典型、完整、有效的 PKI 体系一般包括数字证书认证系统(CA)、证书注册系统(RA)、密钥管理系统（KM）、目录服务系统（LDAP）及在线证书状态验证系统（OCSP）等。

图 11：典型 PKI 系统组成



资料来源：网络公开资料，东兴证券研究所

1）认证中心 CA(CertificationAuthority)：是证书的签发机构，是保证电子商务、电子政务、网上银行、网上证券等交易的权威性、可信任性和公正性的第三方机构，它负责生成、分发和注销数字证书，是 PKI 的核心执行机构。

CA 的主要职责包括：

- 验证并标识证书申请者的身份。对证书申请者的信用度、申请证书的目的、身份的真实可靠性等问题进行审查，确保证书与身份绑定的正确性。
- 确保 CA 用于签名证书的非对称密钥的质量和安全性。为了防止被破译，CA 用于签名的私钥长度必须足够长并且私钥必须由硬件卡产生，私钥不出卡。
- 管理证书信息资料。管理证书序号和 CA 标识，确保证书主体标识的惟一性，防止证书主体名字的重复。在证书使用中确定并检查证书的有效期，保证不使用过期或已作废的证书，确保网上交易的安全。发布和维护作废证书列表（CRL），因某种原因证书要作废，就必须将其作为“黑名单”发布在证书作废列表中，以供交易时在线查询，防止交易风险。

由此可见，CA 是保证电子商务、电子政务等网上交易权威性、可信性和公正性的第三方机构。

2）注册机构 RA(RegistrationAuthority)：主要功能包括对证书持有者的身份信息进行审核，通知 CA 中心是否可以为该用户签发证书，维护申请数据库，将身份信息和其公钥进行绑定；

3）密钥备份及恢复系统：当用户由于某种原因（遗忘口令、介质破坏等）丢失了密钥，使得密文数据无法被解密时，PKI 提供的密钥备份和恢复解密密钥。当用户证书生成时，加密密钥即被 CA 备份存储；当需要恢复时，用户只需向 CA 提出申请，CA 就会为用户自动恢复。值得注意的是密钥备份及恢复只是针对解密密钥，签名密钥不作备份。

4）证书注销列表 CRL（CertificateRevocationList）：是 PKI 系统的一个重要组件。因为证书的有效期是有限的，因此证书和密钥必须由 PKI 系统自动进行定期的更换，超过其有效期限就要被注销处理。证书更新一般由 PKI 系统自动完成，不需要用户干预。即在用户使用证书的过程中，PKI 也会自动到目录服务器中检查证书的有效期，当有效期结束之前，PKI/CA 会自动启动更新程序，生成一个新证书来代替旧证书。

5）证书历史档案：经过一段时间后，每一个用户都会形成多个旧证书和至少一个当前新证书。这一系列旧证书和相应的私钥就组成了用户密钥和证书的历史档案。记录整个密钥历史是非常重要的。例如，某用户几年前用自己的公钥加密的数据或者其他人用自己的公钥加密的数据无法用现在的私钥解密，那么该用户就必须从他的密钥历史档案中，查找到几年前的私钥来解密数据。

6）客户端证书处理系统：为了方便客户操作，在客户端装有软件，申请人通过浏览器申请、下载证书，并可以查询证书的各种撤消信息以及进行证书路径处理，对特定的文档提供时间戳请求等。

7）数字证书库：存储由 CA 发放的有效证书和 CRL（证书废止列表）。数字证书库是 CA 颁发证书和撤消证书的集中存放地，它像网上的“白页”一样，是网上的公共信息库，可供公众进行开放式查询，获得其他用户的证书和公钥。一般来说，查询的

目的有两个：其一是得到与之通信实体的公钥；其二是要验证通信对方的证书是否已进入“黑名单”。证书库支持分布式存放，即可以采用数据库镜像技术，将 CA 签发的证书中与本组织有关的证书和证书注销列表存放到本地，以提高证书的查询效率，减少向总目录查询的瓶颈。

8）证书持有者：获得并使用由 CA 发放的证书的机关、企业、个人或服务器。

9）证书应用系统：利用最终用户的证书和密钥，提供加密、签名等应用服务。

2.2 PKI 相关产品完善，商业政务多点开花

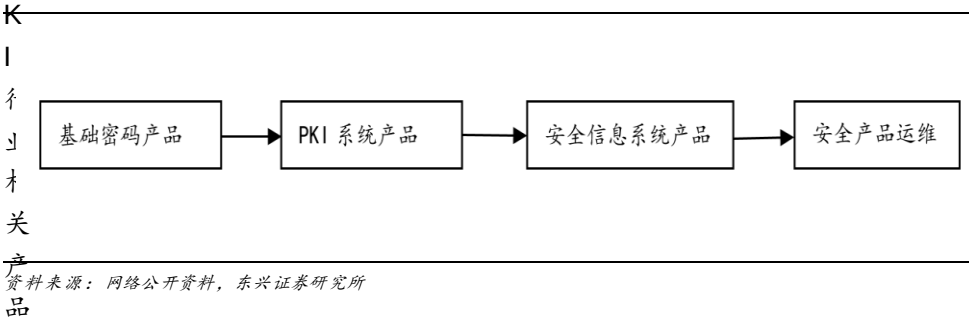
目前，国内设及高等级安全性应用的相关领域，均不同程度的采用了 PKI 技术。PKI 产品广泛应用于日常生活，我国大部分计算机操作系统包括 Windows、iOS 等和浏览器，均内置了对 PKI 技术的基础支撑，如支持数字证书管理、支持 HTTPS 连接的相关组件。其他使用 PKI 技术的应用包括：安全认证网管关（保证远程连接安全）、网银（Usb Key 证书或文件证书）、安全电子交易（数字签名和验签）等。

PKI 技术是信息安全行业的核心技术之一，亦是电子政务与电子商务等安全应用领域的关键基础技术。目前，我国 PKI 产品被广泛应用于电子政务、电子商务、电子银行等相关领域，通过实现身份认证与访问控制等功能，以保障访问安全站点、发送电子邮件、网上证券交易、网上招投标、网上签约、网上办公、网上缴费、网上税务、网上银行等网络信息传输与相关应用的安全。未来较长时期内，我国政府部门、军队和军工、金融机构、大中型企事业单位仍将继续保持对信息安全产品尤其是 PKI 产品的旺盛需求，在信息安全体系建设上不断增加资金投入。因此，加强数据安全与隐私保护并提升 IT 基础设施防御能力，已经成为信息安全产品市场发展的主要推动。

2.2.1 国内 PKI 相关产品体系趋于完善

网络安全体系是不断发展与进步的，PKI 提出已有十多年，国外相关产业早已完善，而国内在近些年也在跟随国际步伐，不断改革创新，逐步形成了比较完善的产品体系。

图 12：PKI 产品产业链



资料来源：网络公开资料，东兴证券研究所

通常包括以下三种：

1）PKI 基础设施产品

基础设施产品是由数字证书认证系统、证书注册系统、密钥管理系统等组合而成的信息安全基础设施，为信息安全提供密钥管理、数字证书生命周期管理及发布服务，是构建网络信任体系的基础。此类产品的主要功能是，通过数字证书的形式发放网络世界中的身份证，作为网络用户在网络世界中表明身份的唯一标识；是保障信息在网络传输过程中保密性、完整性、真实性和不可抵赖性的重要基础。

2）PKI 安全应用产品

PKI 安全应用产品建立在 PKI 基础设施产品发放的数字证书以及 PKI 密码技术之上，为用户提供多元化的安全服务及应用的信息系统，可以满足各种网络应用的身份认证、数据加密、操作不可抵赖及数据的完整性等一系列信息安全需求。此类产品的主要功能是，根据网络用户的身份属性，对其访问或操作信息应用系统的权限进行管控，并对其上网的行为予以全程跟踪记录；实现了数据的保密性、完整性、真实性和不可抵赖性。

PKI 安全应用产品主要分为两种模式。

- 一是，“中间件”模式，即在 PKI 基础设施产品提供密钥管理、证书管理的基础上，在用户的应用系统前端添加安全认证网管等中间件，通过对用户登录上传的数字证书和签名信息进行身份鉴别、对出入应用系统的信息实行加密、设置访问的权限以及对访问实施安全审计等手段，实现对该应用系统的网络边界和入口的守卫功能。
- 另一种为“中间件+安全应用系统”模式，即在自主研发的，诸如安全电子邮件系统、安全即时通信系统、网络保险箱等安全应用系统，集成了安全中间件，实现应用系统的安全、保密及不可抵赖等功能。

3）通用安全产品

通用安全产品是对 PKI 相关安全产品的补充，为用户提供更加完整的安全解决方案。主要包括网络审计系统和其他系统集成涉及的相关产品。其中网络审计系统是针对网络的管控与审计功能，是网络安全管理机构准确掌握网络态势、监控网络行为、定位分析安全事件、全面保障网络安全的高效工具。其他系统集成涉及的相关产品，主要指为构建一个高效的信息安全体系，而需要为用户配置不同层面的非 PKI 相关的通用安全软硬件设施设备，如防火墙、防病毒、入侵检测等。

表 2：PKI 产品介绍

产品	联系与区别	划分依据
PKI 基础设施产品	整个 PKI 安全体系的基础和框架	主要解决信息网络空间中信任问题，确保各行为主体身份唯一性、真实性和合法性
PKI 安全应用产品	建立在 PKI 基础设施产品之上，提供各系那个安全服务与应用	在 PKI 基础上构建一个完备的 PKI 安全体系，并提供身份认证、授权、网络传输安全、数据存储安全、数据完整性保证、签名和验签等一系列安全支撑系统以及安全的业务沟通平台

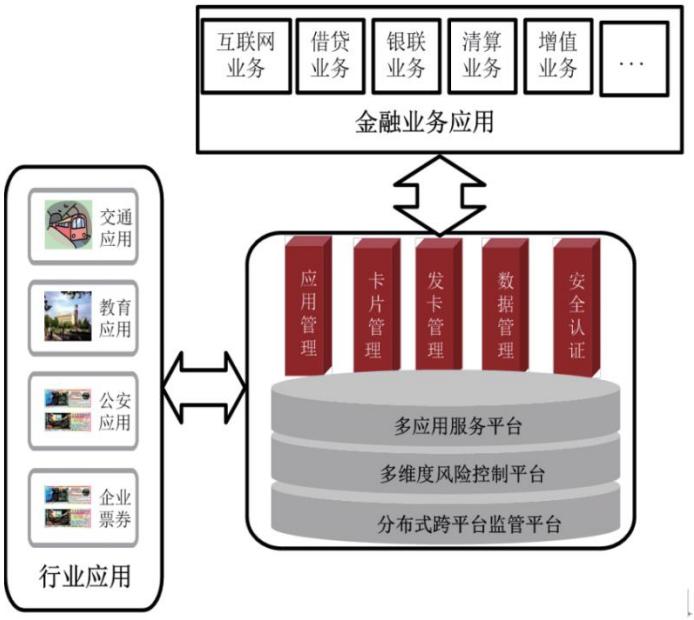
通用安全产品	与 PKI 关联度不大的其他信息安全类产品，是对 PKI 体系安全产品的补充	帮助用户解决其他非 PKI 范畴的安全问题，丰富产品结构，构建安全保障体系

资料来源：网络公开资料，东兴证券研究所

2.2 PKI 产品在金融领域具有非常重要的作用

信息化浪潮深刻影响着金融行业。虽然金融行业仍遵循着“客户-银行-清算银行-中央银行”这样多层级、中心化、相对稳定、可靠的架构，但随着互联网的普及、移动互联的深入应用以及人工智能等新技术的兴起和应用，金融行业在产品服务、商业模式、经营理念正面临着深刻变革和创新。

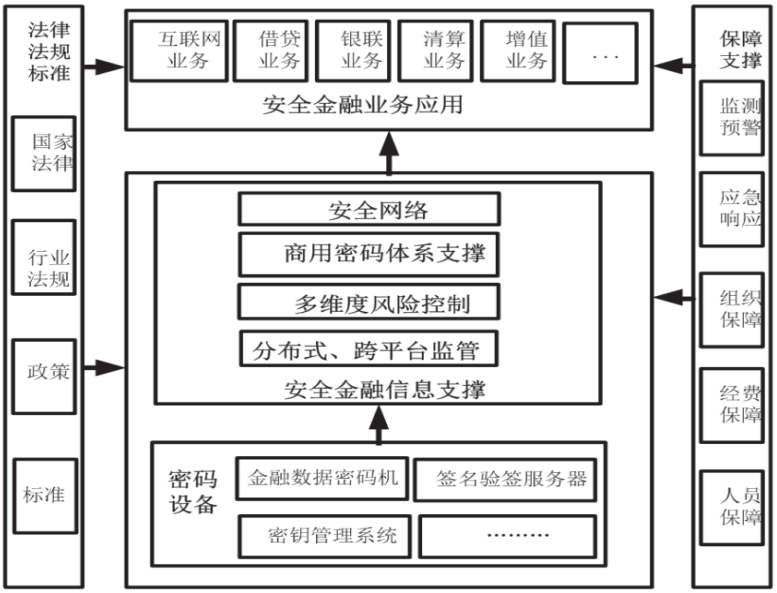
图 13：多应用安全金融信息系统框架



资料来源：网络公开资料，东兴证券研究所

当前出现了许多非传统的金融活动方式，如电子支付 （支付宝、财付通)、互联网基金（余额宝）、P2P 等。信息化同时给金融信息安全带来了极大的威胁，APT 攻击、DNS 劫持、勒索软件、软件供应链攻击等也开始锁向金融领域，并且和传统的安全问题交织在一起，触及到了国家经济、金融安全的底线和命脉。

图 14：安全金融信息系统基础设施



资料来源：网络公开资料，东兴证券研究所

PKI 系统建立在密码设备基础上，通过分布式跨平台监督，可以有效解决金融行业网络安全两个最重要的部分：网络本身不被随意假冒和窃听以及网络的接入是可信的。客户浏览器端装有客户证书，银行服务器端装有服务器证书。当客户上网访问银行服务器时，银行首先要验证客户端证书，检查客户的真实身份，确认是否为银行的真实客户；同时服务器还要到 CA 的目录服务器，通过 LDAP 协议查询该客户证书的有效期和是否进入"黑名单"；认证通过后，客户端还要验证银行服务器端的证书。双向认证通过以后，建立起安全通道，客户端提交交易信息，经过客户的数字签名并加密后传送到银行服务器，由银行后台信息系统进行划账，并将结果进行数字签名返回给客户端。这样就做到了支付信息的保密和完整以及交易双方的不可否认性。

2.2.3 移动支付同样需要 PKI 系统的保护

移动终端应该有密码服务（或个性化密码机）、密钥管理模块、业务应用模块和个人风险控制模块（或个人风险控制器）。只有满足业务应用和个人风险控制（风险控制器）条件时，金融业务才能正常进行。

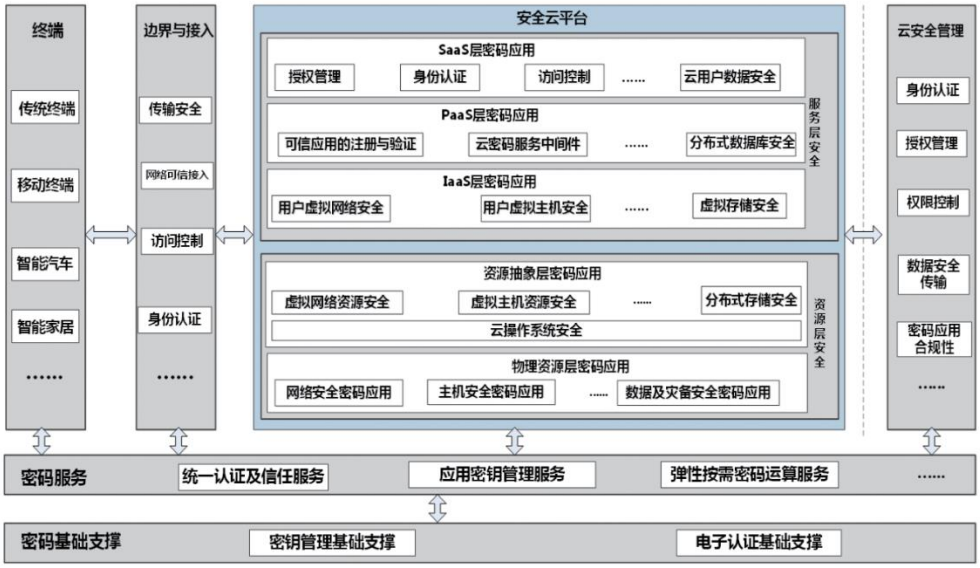
移动终端在高安全、大额度的交易应用需求中，必须采用数字签名等措施，保护交易的安全性。一般性应用中，最低应该采用软密码模块（提供数字签名、加密等功能）方式，目前软密码模块遵循的主要标准是《密码模块技术要求》和《密码模块检测要求》，这两个标准是为硬件密码模块（加密卡、USBKEY）量身打造的，对于软件的密码模块，存在一些有待完善和不足的地方，软件密码模块缺乏硬件模块那样清新的安全边界，软件密码模块运行在一个不受控、不可信的环境中，采用的密钥保护措施、密码运算安全尤为重要。PKI 系统可以提供移动支付需要的数字签名与密钥管理服务，有效的为移动支付的安全保驾护航。

2.2.4 云计算的蓬勃发展离不开 PKI 系统来保障数据安全

云计算作为信息化发展方向，为大数据应用、智能制造、人工智能、智慧城市等提供计算、网络、存储资源，已经广泛深入到我国政务、交通、能源等各个领域，出现了政务云、交通云、能源云等。云计算安全直接关系到我国关键信息基础设施的安全，因此，必须充分发挥 PKI 系统在云计算安全中的核心支撑作用。

在云计算环境下，云计算 IaaS 层、PaaS 层、SaaS 层中的云平台、各类云业务系统的安全保护都建立在 PKI 系统上，密钥管理、身份认证、访问控制等与云计算深度融合，作为云计算中的“基因”嵌入各类云计算服务平台中，实现应用、安全一体化。

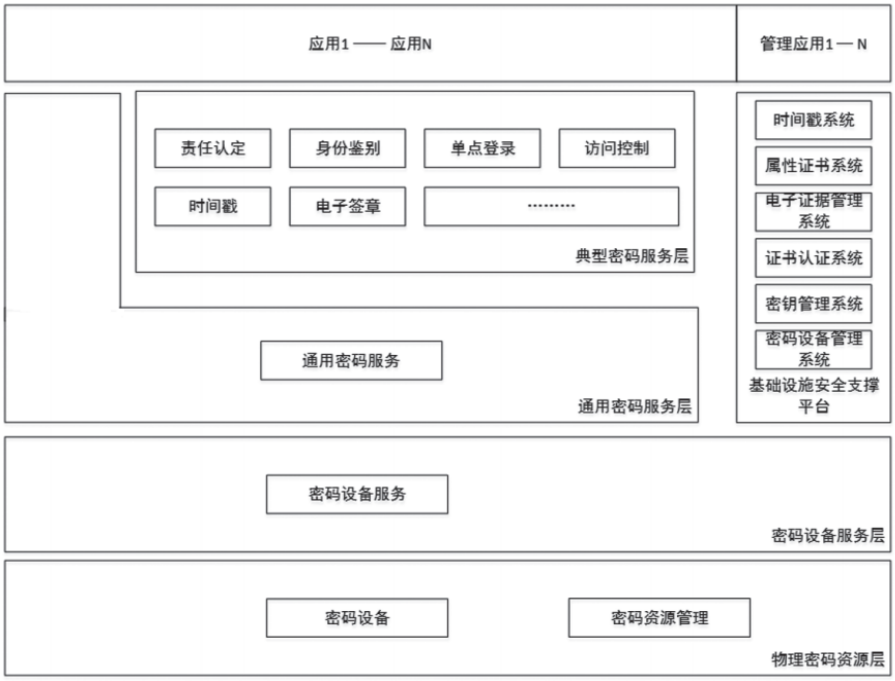
图 15：云计算数据安全体系



资料来源：网络公开资料，东兴证券研究所

对于云计算中计算资源虚拟化、软件自定义网络等特点，云计算和大数据专线组成员单位共同提出了云计算密码应用技术支撑框架，通过基于 PKI 的安全基础设施的虚拟化密码设备提供密码运算服务，通过证书认证系统、属性证书系统、时间戳系统、密钥管理系统等基础设施提供证书管理、时间管理和密钥管理等基础服务，以标准接口形式为应用系统提供统一的身份鉴别、单点登录、数据加解密、数字签名及验证等密码服务。

图 16：云计算安全层级



资料来源：网络公开资料，东兴证券研究所

2.2.5 电子政务是 PKI 系统需求量最大的领域之一

国家安全历来是我国政府工作的重中之重，财政部出台的《政务信息系统政府采购管理暂行办法》、发展改革委制定的智慧城市评价指标，切实写入了对政府网络安全的要求，实现网络安全与国家战略的融合发展。

电子政务包含的主要内容有网上信息发布、办公自动化、网上办公、信息资源共享等，一般分为政务云和移动政务。政务云安全是要保护用户与云平台之间、用户与用户之间、云平台不同数据中心之间的数据传输安全性；移动政务网络安全包括移动终端本身的安全以及移动终端与操作系统之间的数据传输安全。

无论是政务云还是移动政务，都需要身份验证和访问控制，包括办理业务的私企民企以及个人和政府员工本身。认证通过证书进行，而访问控制通过属性证书或访问控制列表完成；有些文件在网络传输中要加密以保证数据的保密性;有些文件在网上传输时要求不能被丢失和篡改，特别是保密文件的收发必须要有数字签名等。在安全防护的同时也要保护民众的个人隐私；民众和企业网上办事需要提交的各种文件需要确保真实性、有效性、抗抵赖。只有 PKI 提供的安全服务才能满足电子政务中的这些安全需求。

2.2.6 军工行业中 PKI 系统尤为重要

军工行业是国家军事装备重要的科研生产单位，随着社会信息化成都的提高，促进军工企业信息化，实现现代化信息安全管理已成为军工企业发展的必由之路。由于信息安全项目设计的复杂性，项目的设计是由许多技术人员分担完成的，因此，只有实现信息共享和资源整合才能更高效地完成设计任务。军工行业往往环境复杂，军用专网、

内网和互联网等多种平台界限分明，不同平台之间通信管控严格；系统内产生的数据和文档有高度保密性、高度敏感性，数据泄露会造成重大危险。因此，PKI 产品作为身份认证的关键技术，在军工行业尤为重要，在此领域中 PKI 产品应用非常广泛。

2.3 PKI 产品市场

目前，我国 PKI 产品市场中，格尔软件、吉大正元、成都卫士通、北京数字认证等组成该细分领域的优势企业。前述信息安全厂商掌握着 PKI 基础设施及 PKI 安全应用领域的关键技术，具备丰富的行业相关经验于客户资源，同时在技术创新于研究开发方面处于行业优势地位，主导着 PKI 产品市场的发展。

图 17：PKI 产品市场竞争格局

资料来源：网络公开资料，东兴证券研究所

2.3.1 成都卫士通 PKI 相关产品介绍

成都卫士通信息产业股份有限公司是目前国内以密码为核心的信息安全产品和系统的供应商，主要从事信息安全产品和系统的研发、生产、销售，安全集成和安全服务等业务，为用户提供加密模块、安全平台、密码产品、安全设备整机等系列密码产品，以及安全产品和安全系统集成服务。主要是 PKI 系列产品上游基础密码产品提供商，同时也提供 PKI 数字签名等产品和整套安全系统服务。

表 3：卫士通产品种类

项目	成都卫士通
主要产品种类	签名验签服务器、金融数据密码机、服务器密码机、USBKey 密码模块、PCI 密码卡、数字认证系统、密钥管理系统、安全认证网管系统、中华卫士入侵检测与防御系统、中华卫士网络行为管理与审计系统、IPSec VPN 安全网关、涉密计算机及移动存储介质保密管理系统、终端安全防护系统、卫士通安全桌面云等
主要客户	主要为党政、军队、军工、电力、金融、能源、运营商以及其他大型企业集团、中小企业及事业单位等用户提供信息

资料来源：网络公开资料，东兴证券研究所

2.3.2 格尔软件 PKI 相关产品介绍

格尔软件经过十余年的积累和研发，形成了基于 PKI 的信息安全产品系列，可以为客户提供专业的安全服务，能够为用户量身定制信息安全整体解决方案。

图 18：格尔软件产品

主要产品及类别		主要应用领域	客户类型
PKI 基础设施产品	数字证书认证系统	政府机关电子政务系统、军工单位信息管理系统、金融机构信息管理系统、大中型企事业单位运营管理系统	政府机关、军工单位、金融机构、大中型企事业单位
	密钥管理系统		
	身份认证系统	政府机关电子政务系统、军工单位信息管理系统	政府机关、军工单位
PKI 安全应用产品	安全认证网关	政府机关电子政务系统、军工单位信息管理系统、金融机构信息管理系统、金融机构网银业务	政府机关、军工单位、金融机构
	可信边界安全网关	公安网络边界防护与管理	政府机关
	移动安全管理平台		
	无线安全网关	政府机关电子政务系统	政府机关
	电子签章系统	银行电子票据业务系统	金融机构
	安全电子邮件系统	政府机关电子政务系统、军工单位信息管理系统	政府机关、军工单位
	安全即时通系统		
	网络保险箱		
	终端信息保密系统		
	局域网接入认证系统		
	签名验证服务器	政府机关电子政务系统、金融机构信息管理系统	政府机关、金融机构
	云安全服务平台系统	政府机关电子政务系统	政府机关
	打印管控系统		
	移动介质管理系统		
通用安全产品	网络审计系统	政府网络管理	
	信息安全系统集成	政府机关电子政务系统、军工单位网络安全建设	政府机关、军工单位

资料来源：网络公开资料，东兴证券研究所

2.3.3 吉大正元 PKI 相关产品介绍

长春吉大正元信息技术股份有限公司成立于 1999 年 2 月，是我国信息安全行业 PKI 基础设施产品和服务的主要提供商之一，主要从事信息安全产品的研发、生产、销售，并提供安全咨询、安全集成和行业应用开发等服务，为用户提供包括信息安全建设、应用安全建设、数据安全建设等方面的解决方案和集成服务。

表 4：吉大正元 PKI 相关产品种类

项目	吉大正元
主要产品种类	电子证书认证系统、权限管理系统、身份认证网关 G 系列、身份认证网关 I 系列、同一用户管理系统、数字证书综合统计查询系统、数字签名服务器、磐石终端安全系统、电子签章系统、安全管理子系统、行政审批电子监察平台、政务系统办公平台等
主要客户	主要为党政、机关、金融机构、军队、军工以及企业提供产品和解决方案

资料来源：网络公开资料，东兴证券研究所

2.3.4 数字认证 PKI 相关产品介绍

北京数字认证股份有限公司是领先的网络安全解决方案提供商，致力于保障余户信息基础设施安全可靠运行。面向全国客户提供电子认证服务、安全集成、安全咨询与运维服务。

表 5：数字认证 PKI 相关产品种类

项目	数字认证
主要产品种类	提供电子认证服务、安全集成、安全咨询与运维服务。电子认证服务主要包括数字证书和电子签名两类；安全集成是为客户提供适合其信息系统特点的网络安全保证解决方案，将自有产品或第三方信息系统和网络安全产品有效的与客户系统集成来保障客户系统安全；安全咨询与运维服务包括风险评估代码审计等专业安全服务。
主要客户	主要为政府、企事业单位、医院、金融企业等提供产品和解决方案

资料来源：网络公开资料，东兴证券研究所

3. 等保 2.0 推动信息安全行业，物联网时代信息安全大有可为

3.1 网络安全形势不容乐观，加强网络身份认证体系建设势在必行

3.1.1 委内瑞拉遭遇网络攻击，全球网络安全形式不容乐观

工控安全事件频发。当地时间 3 月 7 日晚，委内瑞拉发生全国范围的大规模停电，首都加拉加斯以及其他大部分地区陷入一篇漆黑，全国 18 个州电力供应中断，仅 5 个州幸免。此次突发的电力系统崩溃没有任何预兆，停电给委内瑞拉带来了重大损失，全国交通瘫痪，地铁系统关闭，医院手术中断，所有通讯线路中断，航班无法正常起降。委内瑞拉总统尼古拉斯·马杜罗(NicholasMaduro)表示，该国的电网在周再次遭受打击，许多恢复的系统再次瘫痪，该国电力系统已成为最新一轮“网络攻击”的目标。

从公开报道的马杜罗总统发言来看，有多个关键词值得我们的关注：“电网再次受到攻击”、“网络攻击”、“发电机遭受攻击”、“内部攻击”等。不言而喻，这是一起非常典型的工控安全事件，发起者目标明确，整个攻击过程有组织、有计划、多渠道、持续性展开，在遭受严重损失的同时，也充分暴露出委内瑞拉的关键信息基础设施安全防护投入的不足，安全事件的应急处理手段有待加强。该事件已成为继“乌克兰电网事件”后的又一个“网络战”的典型案例。

网络战相比于传统国家军事对抗，不受国际法限制、难以追踪隐蔽性强且可以造成重大损失。古里水电站被破坏，造成全国电力供应崩溃，手段必定是对自动控制系统的网络攻击，而这些设备往往来自美国。这种攻击很难抓到确凿犯罪证据，而且也有先例，2015 年圣诞节前乌克兰电力公司的控制系统就被攻击过，导致大面积停电，美俄相互指责。伊朗电网也被攻击过，同样找不到作案人。委内瑞拉停电事件给我们敲响了警钟，必须提升国家关键基础设施的网络攻防能力。

3.1.2 我国网络攻防能力急需提升

我国是网络高级持续性威胁攻击主要受害国，金融、能源、交通、教育等行业是“重灾区”。近年来电子政务、电子商务高速发展，但网络安全监管和防御能力严重“拖后腿”。网络安全投资占信息化建设总经费比例不足 1%，与美国 15%、欧洲 10%的水平差距甚大。既没摆脱高端技术受制于人现状，也没做到服务应用安全可控。网络攻击、信息窃取和破坏事件屡屡发生。

基础信息网络和重要信息系统隐患突出。有关部门对我政府机构、金融、电信、能源、铁路部门和军工企业等 120 多个单位 896 个信息系统检测，发现高危漏洞 1.2 万个。国家安全信息库显示，截止 2017 年 10 月，境内被植入后门的网站 2180 个，全国政务网站存在 3004 个告警信息，境内被篡改网站数量 5163 个，被木马或僵尸程序控制 IP 地址对应主机数 84 万个。仅 2018 年 12 月，境内感染网络病毒的终端数为近 78 万个；境内被篡改网站数量为 1376 个，其中被篡改政府网站数量为 80 个；境内被植入后门的网站数量为 2317 个，其中政府网站有 34 个；针对境内网站的仿冒页面数量为 5324 个；国家信息安全漏洞共享平台（CNVD）收集整理信息系统安全漏洞 1206 个，其中，高危漏洞 481 个，可被利用来实施远程攻击的漏洞有 1067 个。

3.1.3 网络身份认证信息安全发展大势所趋，前景广阔

截止到 2018 年 6 月底，我国互联网普及率增长至 57.7%，网民规模达到 8.02 亿人，较 2017 年底增长 3.8%。而 2009 年，我国网民规模仅有 3.84 人人，互联网普及率仅为 29.0%。我国网民数量快速增长，用户规模庞大，网络应用日益多样化，推动了我国互联网市场高速发展，但同时网络安全问题日益严重，2018 年，我国多个地区的多家医院遭遇勒索病毒；包括华住集团和万豪集团在内的酒店用户信息被频繁泄露；苹果手机用户账号被盗刷。这一系列网络安全事件表明我国信息安全工作正面临严峻考验，网络身份认证推行势在必行。

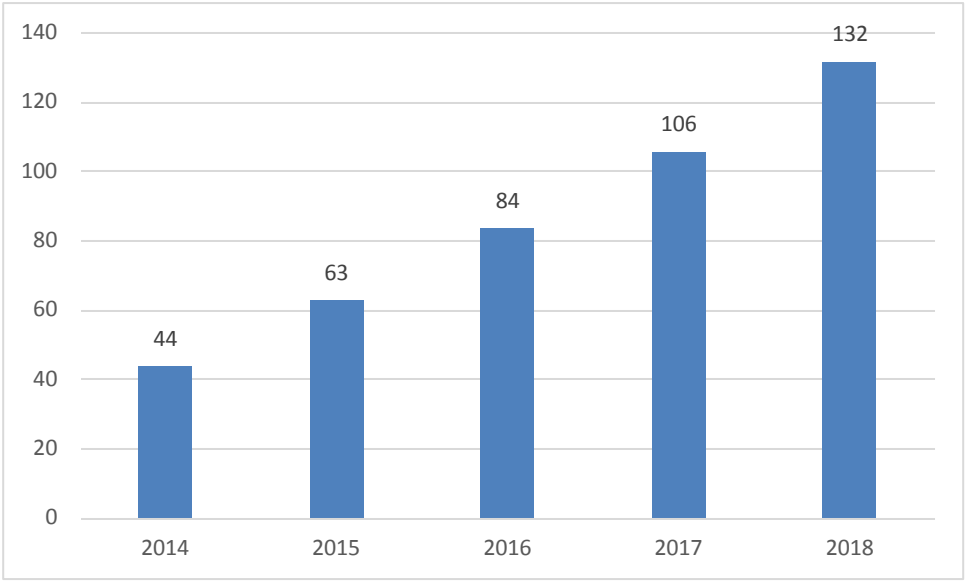
我国网络身份认证行业主要包括硬件产品、软件产品和服务产品三大细分领域。2017 年，我国网络身份认证市场中，硬件产品市场份额占比达到 50.1%；软件产品市场份额占比为 39.1%；服务产品市场份额占比为 10.8%。我国网络身份认证市场中，硬件产品占据最大市场份额，由于我国网络身份认证仍处于普及阶段，硬件市场需求较大，随着后期普及率不断上升，软件和服务市场占有率将逐步上升。

现阶段，我国网络身份认证应用主要集中在银行与金融相关领域，随着技术不断成熟，网络身份认证应用范围将逐步扩大至电子政务、企事业 OA/VPN 系统、云计算、IC 卡等各种用户信息较为密集、同样面临信息安全问题的行业中。

国内认证中心分为行业性认证中心、区域性认证中心、商业性认证中心和企业型认证中心。前三种 CA 机构已有 60 余家，58%的省市建立了区域 CA，部分部委建立了行业 CA。目前数字证书已在电子政务、网上银行、网上证券、B2B 交易等众多领域得到了应用，全国证书发放累计超过 150 万张。这些机构有力地推动了 PKI 技术在国内各行业、各地区信息化建设中的应用。

行业规模持续扩大随着下游应用市场不断扩宽，我国网络身份认证行业发展前景广阔。我国网络身份认证市场规模由 2014 年的 44 亿元增长至 2018 年的 132 亿元，年均复合增长率达到 31.6%。

图 19：2014-2018 年我国网络身份认证信息安全行业市场规模（亿元）



资料来源：，东兴证券研究所

按当前发展势头，身份认证领域占整体安全规模的比重将超 30%，据前瞻产业研究院《中国网络身份认证信息安全行业与前景分析报告》，预计到 2022 年，网络身份认证信息安全市场规模有望达到 291 亿元，前景可观。网络身份认证信息安全行业发展趋势未来将有如下五大发展趋势：

1）网络安全日益严峻，互联网及移动互联网信息安全急需加强。随着互联网的发展，尤其是商务类应用的快速发展，网络安全问题日益严峻，互联网信息安全急需加强。此外，移动支付的兴起，令移动信息安全问题也随之凸显。

2）网上银行、电子支付快速发展，将推动身份认证信息安全产品的应用。随着电子银行业的迅速发展，业务的安全性也日益受到用户的重视，安全性仍是选择手机银行品牌的核心考虑因素。因此，网上银行、电子支付快速发展将进一步推动身份认证信息安全产品的应用。

3）身份认证信息安全产品的应用范围将从银行业逐步扩展到其他行业。如电子商务、电子政务、移动支付、云计算等。

4）产品升级换代将越来越快。随着应用环境的日益复杂，各种攻击手段层出不穷，客观上将促进身份认证安全产品的不断升级换代。

5）加密算法升级换代、数字认证存在有效期、OTP 动态令牌产品电池寿命期有限等将推动存量市场的产品更新换代。

3.2 国家战略政策推动网络安全发展，等保 2.0 利好整体信息安全行业

3.2.1 国家不断完善网络安全政策

网络安全重要性凸显，国家战略出台指导行业发展。2013 年以来，我国先后成立了国家安全委员会、中央网络安全和信息化领导小组，出台了《国家安全法》、《网络安全法》、《国家网络空间安全战略》、《网络空间国际合作战略》等法律法规和重要指导文件；习近平主席更是发表了“没有网络安全就没有国家安全”的重要论述，国内自上而下对网络安全的认识和重视空前提升，我国网络安全产业进入的发展新阶段。

表 6：近年我国网络安全方面主要政策

时间	名称
2012 年 12 月 28 日	全国人大常委会通过《关于加强网络信息保护的决定》
2013 年 6 月 8 日	中美将在战略安全对话框架内设网络安全工作小组
2013 年 6 月 14 日	外交部设立网络事务办公室
2013 年 11 月 12 日	中央决定成立国家安全委员会
2014 年 2 月 27 日	中央网络安全和信息化领导小组成立
2015 年 7 月 1 日	《国家安全法》公布施行
2016 年 3 月 25 日	中国网络空间安全协会成立
2016 年 4 月 19 日	总书记在网络安全和信息化工作座谈会上发表 419 重要讲话
2016 年 8 月 22 日	中央网信领导小组发布《关于加强国家网络安全标准化工作的若干意见》
2016 年 10 月 17 日	工信部印发《工业控制系统信息安全防护指南》
2016 年 12 月 27 日	国家网信办发布《国家网络空间安全战略》
2017 年 3 月 1 日	外交部和国家网信办发布《网络空间国际合作战略》
2017 年 6 月 1 日	《网络安全法》正式实施
2017 年 6 月 9 日	网信办、公安部、工信部等四部委发布《网络关键设备和网络安全专用产品目录（第一批）》
2017 年 10 月	十九大报告提出，加强互联网内容建设，建立网络综合治理体系，营造清朗的网络空间；提高基于网络信息体系的联合作战能力等。
2018 年 4 月 20 日	全国网络安全和信息化工作会议，总书记就网络安全发表重要讲话。
2018 年 6 月 27 日	公安部发布《网络安全等级保护条例(征求意见稿)》（等保 2.0）

资料来源：网络公开资料，东兴证券研究所

3.2.2 等保 2.0 与网络安全法

网络安全等级保护已经进入 2.0 时代，等级保护制度已被打造成新时期国家网络安全的基本国策和基本制度。应急处置、灾难恢复、通报预警、安全监测、综合考核等重点措施全部纳入等保制度并实施，对重要基础设施重要系统以及“云、物、移、大、工”纳入等保监管，将互联网企业纳入等级保护管理。

等保 2.0 的标准是国内非涉密信息系统的安全集成标准，网络安全法是作为法律、中国信息安全的基本法。网络安全法中明确的提到信息安全的建设要遵照等级保护标准来做建设。

图 20：网络安全等级保护发布

资料来源：网络公开资料，东兴证券研究所

3.2.3 等保 2.0 有望带动信息安全整体市场需求增加

网络安全等级保护制度是一项把信息系统按照重要性划分成不同等级，采取相应的防护措施，让信息系统与防护措施门当户对的政策。等级保护这项工作是从 1994 年提出的，但直至 2007 年才正式发布了《网络安全管理办法》及后续的系列政策，等保工作才正式开始。随着新技术的发展，之前的制度不能很好的适应新的安全环境，等保 2.0 制度呼之欲出。等保 2.0 对信息安全行业带来的影响可以总结为以下几大方面：

- 首先，等级保护已经从原有的规定上升到了法律层面，未来等保 2.0 的执行力度和强制力度将加大。整体执行上更加严格，对于违反相关法律规定的轻则警告重则罚款。考虑到信息安全行业受政策影响大，等保 2.0 的推出将提高大家在信息安全投入的积极性，长期带动信息安全需求增加。

- 其次，等级保护首次加入了“未知攻击”的检测、SOC 等主动防御的要求，以前信息安全以防火墙、杀病毒、IDS 等被动防御为主，随着安全威胁的升级，等保制度也积极响应，提出主动防御上的要求，这将有望带动威胁情报、态势感知、APT 攻击检测与防护和 SOC 等主动防御产品的需求增加。

- 再次，信息系统除了需要满足通用要求的，还要满足云计算、移动互联、大数据、工业控制等领域的扩展要求。等保 2.0 相比于 1.0 另外一个比较大的变化就是保护对象的扩大，新增了移动互联、云计算、大数据、物联网和工业控制等新兴安全领域的内容和扩展要求，相应的新兴安全领域需求将受政策的出台推动带来需求增加。

- 最后，等保 2.0 也特别新增了外包运维管理的管理要求，选择的外包运维服务商在技术和管理方面均具有按照等级保护要求开展安全运维工作的能力，应在与外包运维服务商签订的协议中明确所有相关的安全要求。如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。对公司内部安全运维的要求降低和对外包运维的要求增多，这也从侧面体现了等保 2.0 对安全服务的认可，体现了安全服务正越来越成为一种趋势。

因此，等保 2.0 范围更广、力度更大且对新兴领域安全提出要求，这有望带动信息安全整体市场需求增加，其中受益最大的是威胁情报、态势感知、SOC 等主动防御领域、云安全、数据安全和工控安全等新兴安全领域和安全服务领域。

图 21：网络安全等级保护变化

资料来源：网络公开资料，东兴证券研究所

3.3 物联网将成为密码产业发展的蓝海

习近平总书记指出，要加快构建高速、移动、安全、泛在的新一代信息基础设施，形成万物互联、人机交互、天地一体的网络空间。落实总书记重要指示要求，构建新一代信息基础设施和网络空间，离不开物联网技术的创新发展，离不开密码与物联网的深度融合。

3.3.1 万物泛在互联是大趋势

物联网发展的终极形态，将是万物皆可数化、万物皆可互联、万物皆可控制。广泛互联、应用融合、实时反馈、跨域交互、高度异构，将成为物联网泛在化的必然趋势，并呈现出三个主要特点：一是规模大，应用广；二是形态复杂多变；三是既有的边界被打破。从宏观的拓展而言，经济全球化、世界多极化、社会信息化、文化多样化、国际关系民主化的发展，为物联网的全球拓展创造了良好的国际氛围。从中观的延伸而言，线上线下结合的商业模式目前正在中国二三线城市进入数量增长阶段，物联网行动计划将为这一数量的进一步增长注入发展的活力，形成延伸发展的动力引擎。从微观的渗透而言，物联网行动计划将为网络向经济、社会、文化的方方面面的进一步渗透提供机遇。互联网特别是移动互联网具有泛在、随时、互联、便捷等诸多特点，在智能技术的支持下，无论是产品的智能化转型还是流程的网络版升级，无论是服务

的空间拓展，还是数据的人机传递，无论是多屏的互联融合，还是智慧高效的个性定制，物联网行动计划为人们展示了微观渗透的无限想象力。

伴随着物联网技术的兴起，5G、区块链、人工智能这三大引领未来的信息技术将对当今世界产生深远影响。从家用电器、健康监测设备、路面传感器到智能门锁和无人驾驶汽车，以物联网为代表的下一代智能联网设备，正迅速成为人们工作和生活的重要组成部分，由此带来的最大挑战是，如何在突破既有边界防护的情况下，灵活高效地解决谁是谁、谁拥有谁、谁能访问谁、谁为谁服务等问题。

3.3.2 发挥密码支撑作用，促进万物互联安全

密码是物联网安全的核心技术，是整个网络信任体系的基础支撑。物联网安全纵贯感知层、网络层、平台层和应用层，涵盖传感器、基础设施、计算处理和行业应用，涉及数据的采集、传输、存储、处理、分析和使用，关系物联网计算安全、运行安全、使用安全和管理安全，急需着眼全体系平台、全产业链条、全生命周期。系统解决不安全、不可控的问题，必须应用密码实现物联网中人、物、信息和网络的真实性、机密性、完整性和抗抵赖性系统保护，为物联网信任建立、安全保障、融通互联、溯源监管提供基础支撑。利用密码在身份鉴别、数据加密、信任传递等方面的重要作用，来维护物联网的安全秩序，构建其弹性边界，并与其他多种安全技术一道共同构建坚实的物联网安全防线。

构建以密码为基石的物联网安全新秩序，是形势所迫、安全所需、法规所律、职责所在。物联网的本质就是融合，它有四个基本特征：网络是基础，数据是资源，计算是能力，泛在是趋势。

密码是网络安全的核心技术，是网络信任的基石。密码支撑构建物联网“网络安全生态圈”，密码在物联网网络安全方面发挥保底作用，是最基础的防线。密码助力打造物联网“数据共享价值链”，同时在物联网不同角色之间建立基于密码的安全通道。密码双向促进物联网“计算发展创新力”:一方面，密码护航计算安全发展，保证算力可控可管，算法正确执行；另一方面，物联网计算需求倒逼密码技术创新，密码推动实现物联网“泛在可控有机体”，密码技术是实现大规模可信身份管理、高安全控制、多方信任等的主要途径。

在基于密码技术构建的安全秩序和边界基础上，可以将身份认证异常检测、安全访问控制、数据审计、感知预警等各种安全技术融合起来，构建以密码技术为核心、多种安全技术相互融合的新安全体系，实现综合安全防护。

3.3.3 密码让物联网时代更美好

密码是物联网产业发展的“催化剂”，应用促进发展，市场催生产业。物联网时代，安全内涵更加丰富，包括基础网络安全、数据安全、计算安全和设备控制安全等。当前，密码与物联网等信息技术相互促进、融合发展已成为普遍共识。万物互联的时代，既是一个方便快捷的好时代，又是一个失密窃密的坏时代。只有早日构建起以密码技术为支撑、多种技术相互融合的安全体系，才能保证物联网健康发展。随着 5G 商用的到来，物联网正处在爆发的前夜，密码和物联网的有机结合，进一步促进产业的蓬

勃发展、喷涌而出。在从无到有的发展过程中，密码与物联网始终相伴相生、如影随形，密码技术的每一次创新，必将带给物联网质的飞跃；而物联网的每一次重大变革，都反映出密码技术的突破。

未来，从基础网络系统到应用代码和数据，从海量边缘节点到核心网络，从智能家居到工业互联，密码将追随物联网泛在部署的脚步而无处不在。物联网将成为密码产业发展的蓝海，为提升产业供给、带动创新发展提供广阔空间。

4. 推荐标的

4.1 卫士通：背靠中国网安快速发展，形成信息安全产品体系

4.1.1 卫士通拥有信息安全完整产业链

公司自成立以来一直致力于信息安全领域的技术研究及产品开发，经过 20 年的耕耘，公司从密码技术应用持续拓展，已形成密码产品、信息安全产品、安全信息系统三大信息安全产品体系，同时，基于 ISSE 体系框架，为党政、央企、能源、金融等用户提供以“安全咨询、风险评估、运维与应急响应”为主要内容的信息系统全生命周期的安全集成与运营服务。

1）密码产品。密码产品指采用密码技术对信息进行加密保护或者安全认证的产品。经过多年的发展，公司已经形成包括密码芯片、密码模块、密码设备和密码系统在内的全系列密码产品。金融数据密码机、服务器密码机、USBKey 密码模块、PCI 密码卡等，是信息安全产业的基础部分，为 PKI 系统提供基础密码产品。

2）信息安全产品。公司的信息安全产品涵盖网络安全、主机安全、数据安全、安全应用及安全管理等多个领域。建立在密码产品之上，包括数字认证系统、密钥管理系统、安全认证网管系统等，是基于 PKI 技术的具体应用。

3）安全信息系统。卫士通近年来积极践行安全与应用紧密融合的思路，形成了移动通信安全产品、安全办公产品、自主高安全产品等三大类安全信息系统产品。包括 IPSec VPN 安全网关、涉密计算机及移动存储介质保密管理系统、终端安全防护系统，综合运用 PKI 技术，形成安全可靠的信息系统。

4）安全集成与运营服务。公司依托强大的技术支持和营销网络为各层次用户提供的咨询、规划、设计、实施和运维的全生命周期安全支持与运营服务。

公司已形成从理论研究、芯片、板卡、设备、平台、系统、到方案、集成服务的完整产业链，并具备产业链各环节的设计、制造、营销、服务能力，优化了公司在信息安全产业中的布局。

4.1.2 中国网安：用“网络安全”捍卫“光荣使命” 以“改革升级”擦亮“国字招牌”

中国电子科技网络信息安全有限公司（简称中国网安）是中国电子科技集团公司根据国家安全战略发展需要，以深耕信息安全和物理安全领域的中国电科第三十研究所、第三十三研究所所为核心，汇聚中国电科内部资源重点打造的网络信息安全子集团。

中国网安构建了包括理论、算法、芯片、产品、系统、服务的完整信息安全产业链，打造了包括卫士通公司在内的多个信息安全企业。

中国网安主要面向国家重要领域、行业、公众市场，构建信息安全产品，安全信息系统，信息安全服务与测评，安全运营和系统安全集成五大业务板块，做强网络监测预警、安全云计算与大数据、工业控制系统安全、自主高安全级网络与信息系统、移动互联网安全、电磁防护材料与工程、安全服务运营七大新兴业务，成为中国网络信息安全的旗舰企业，国内卓越，世界一流的信息安全技术、产品、服务提供商。其提供的 PKI 系统已经在多个单位得到应用。

一季度，中国网安子集团总体实现新签合同 13 亿元，相比去年同期上涨 30%。军工平台业务高质量起步，30 所签订单项合同喜获开门红；旗下部分成员单位第一季度经营业绩大幅增长，华北网安公司同比增长 393%、三零凯天公司同比增长近 300%；此外各大市场也捷报频传，上市平台卫士通公司拿下电子公文系统业务、厦门雅迅完成最新测试车上线，签订商用车 T-BOX 项目；上海三零卫士布局新业务顺利，开展工业互联网安全服务平台建设。

一季度的骄人成绩依靠的是中国网安紧跟集团公司部署，立足网络安全主责主业，推动更深层次观念创新、制度创新和核心能力创新。

签订全年责任书，并要求奋战二季度。3 月 30 日，中国网安召开 2019 年度目标责任书签订会暨一季度经营工作会议。目标责任书签订会上，在许晓平的见证下，董事长卿昱与王文胜签订了中国网安 2019 年经营目标责任书。随后，王文胜代表公司经营班子与直属研究所、控股公司、技术研发部门以及职能部门分别签订了 2019 年度目标责任书。

卿昱在讲话中指出，不忘初心、持续创新、敢打敢拼是中国网安企业发展的内生基因。国有企业家要在激烈的市场竞争中树立忧患意识，强化生存紧迫感，结合发展实际不断创新总结，才能保证企业高质量发展。她强调，公司各级经营管理者要强化合规经营意识，防范和控制风险，聚焦主责主业，主动承担起发展网络空间科技力量的战略责任，持续推动企业各项改革任务圆满落地。最后，她呼吁全体干部职工“从今天起改变自己，从今天起改变部门，从今天起奋战二季度。”

用“智慧”扛起“安全”大旗。中国网安在集团公司的引领下，聚焦主责主业，用创新驱动发展，广泛布局技术前沿，将“智慧”注入“安全”的看家本领，担当起网络空间捍卫者的责任使命，让网络更具“安全感”。

网络空间安全研究院为雄安新区铸造“安全利盾”。设立雄安新区，是党中央深入推进京津冀协同发展做出的重大战略选择，是一项历史性工程，举世关注，万众瞩目。建设这样的历史性工程，必须聚合力，凝众智，展宏图。自 2017 年 4 月 1 日，中共中央、国务院决定设立河北雄安新区的消息公布，随后的日日夜夜里，中国网安充分发挥“军工电子国家队、科技创新骨干力量、电子信息技术产业领头羊”作用，为这座承载“千年大计、国家大事”重托的未来之城积极贡献科技力量。

中国网安与雄安新区将在探索智能城市管理新模式、进一步加强创新能力建设和科技成果转化两方面加强合作。在智能城市建设方面，共同探索“数字雄安”、“未来城市”、“平安雄安”等建设，助力雄安新区管理体系和治理能力现代化，提升雄安新区管委会运行效率，提升民众获得感；在加强创新平台建设方面，共同推动“网络空间安全研究院”、“未来城市研究院”、“中国电科微系统协同设计服务平台”“‘提升政府治理能力大数据应用技术国家工程实验室’雄安实验室”等落户雄安，通过引入集团公司优势资源，推动雄安新区创新及发展。

“网安方案”走出去，向世界发出中国网络安全之声。中国网安充分发挥电子信息技术优势，统筹推进“国家信息化走出去”方案实施，梳理建立智慧城市、电子政务、海洋信息化、交通信息化等六大板块方案库，积极助力“一带一路”沿线发展中国家信息化建设，促进当地经济发展，与所在国实现互利共赢。

集团公司深入推进在“一带一路”沿线国家的安防监控业务布局，大力拓展亚洲、非洲等发展中国家新兴市场，有力支撑了相关国家的平安城市建设工作，继续巩固全球安防第一品牌地位。目前，已在亚洲建立了韩国、新加坡、迪拜、印度、哈萨克斯坦、马拉西亚 6 子公司，在非洲建立了南非和肯尼亚 2 个子公司，在亚非 50 多个非洲国家建立了销售网点，参与了多个大型项目的视频监控系统建设，如新加坡 SPF 项目、尼日利亚如国际机场项目、塞内加尔达喀尔新机场项目等建设工作，充分发挥了平安使者的重要作用。

在刚刚落下帷幕的奥地利维也纳网络安全宣传周上，中国网安受邀并作为唯一发言的亚洲企业代表，首次展示了基于“人工智能+工控安全”为设计理念的“智能时代的工业控制安全体系”，代表中国电科在世界平台亮相，发出网络安全领域的中国声音。

实力源自专业，全面完成网络安全保障任务。中国网安始终坚持以需求带动发展，密切跟踪国内外信息化发展趋势。发挥中国电科网络信息安全子集团的雄厚实力，以密码技术突破为核心、以央企、政务、金融、电信、交通、能源等深耕市场为重点成长方向，以商用密码、云计算、大数据、智慧城市、物联网、工业控制安全、移动互联网安全、政务安全、军民融合、国际业务等方面为重点发展领域积极布局，培育网络安全保障新动能。

中国网安高度重视以密码技术为基础的核心动能打造。创建卫士通摩石实验室汇聚国内知名密码研究专家，围绕国家发展战略目标和国民经济、社会发展及国家安全的重大需求，开展密码理论和相关技术的科研攻关，探讨密码在各行各业的应用。

在成长动能上，作为国家战略力量主力军，中国网安始终坚持从政治高度承担起国家安全重要责任。将为央企、电子政务、金融、能源、军队等重点行业提供关键信息基础设施安全防护整体保障方案作为企业的成长动能，

在发展动能上，作为网络信息安全国家队，面向时代需求中国网安主动转型发展，打造出一大批系统性的整体解决方案。中国网安打造的从硬件到软件、从底层到应用层、从端到云的一体化移动信息安全保护解决方案，能够能有效地解决用户在移动通信、移动办公、电子政务、应急指挥、抢险救灾等业务中的移动信息安全问题。

全国两会期间，网安公司继续受托全力保障国内多地政务网络安全，击溃并防范多起恶性攻击，提供了圆满的安全保障。同时，针对 2018 年爆发的勒索病毒升级再度袭来的危害，网安公司进行严密应对，服务的电子政务平台稳定安全，展现了网络安全“国家队”的责任与担当。

大力培养人才，用创新引领前行。依托集团公司各大研究所，中国网安优化人才培养机制，鼓励创新。高技能人才的选拔体现所内对生产制造领域人才培养的关注，创新驱动的最终落脚点仍是设计与制造，生产制造作为产品实现不可或缺的部分，目前开展的高技能人才培养工作调动了技能群体的积极性，实现了良性互动，多方共赢。建议系统性开展技能人才培养工作，高技能人才要不断学习与提升，展现绝活；部门要给条件、给平台、给资源，提供充足的组织保障；所里要给政策、给激励、给导向，要将规划变为具体的计划，促进技能人才成长成才。

在 3 月 25 日发布的四川省科技进步表彰决定中，网安公司牵头的科技成果独占一等奖两项，三等奖一项，成为区域内网络安全领域创新的主力军；网安公司中青年骨干主持的多个网络安全研究项目获得国家科技部门立项，多个行业解决方案在信息安全领域获得奖项。创新，正促生网安公司前沿技术储备越来越浓厚的灵气。

4.2 格尔软件：PKI 产品领军企业

上海格尔软件股份有限公司成立于 1998 年 3 月，注册资本 3500 万元，下设北京格尔国际、上海格尔信息、上海格尔卫信及宁波格尔天屹等子公司。公司以“应用+安全，创造新价值”为理念，专注于信息安全行业 PKI 领域，主要从事以 PKI 为核心的商用密码软件的研发、生产和销售及服务业务，为用户提供基于 PKI 的信息安全系列产品、安全服务和信息安全整体解决方案。当前，公司的产品和技术已为政务、金融、军工、企业重要信息系统提供安全支撑与保障，参与承建了我国多个第三方数字认证中心系统，并在电子商务、互联网网络实名、金融电子支付、云计算平台、虚拟化、移动互联网、智慧城市等领域的业务安全方面发挥作用。

4.2.1 专注 PKI 领域，拥有显著竞争优势

经过在 PKI 领域十余年的发展与积累，格尔科技在技术研发、人才、专业资质、客户资源、品牌价值和营销服务体系等方面形成了显著的竞争优势。

1）行业内领先优势

公司是国内首批商用密码产品定点生产与销售单位，是国家保密局批准认定的涉及国家秘密的计算机信息系统集成甲级资质单位，是全国信息安全标准化技术委员会成员单位，是国家“863”计划信息安全示范工程金融子项目的责任承担单位，是国家科技支撑计划商用密码基础设施项目的牵头单位。公司是国家火炬计划重点高新技术企业、国家高新技术企业。

2）技术创新和研发优势

公司坚持自主创新，对网络安全及数据安全等领域尤其是 PKI 领域的技术理论进行长期研究。同时，公司在国产密码算法方面进行了长期的研究和开发工作，并成为国内

首批通过国家密码管理局审查、支持 SM2 算法的、省级电子认证服务机构的建设单位。

公司拥有以 PKI 为核心的身份认证、访问控制、加解密等技术。公司继续致力于研究开发，获得了 2 项发明专利、8 项软件著作权。截至报告期末，公司持有拥有 33 项相关发明专利与 65 项相关软件著作权。

近年来，公司作为主要参与单位完成的“面向重要专网的边界安全防御关键技术及应用”项目和“国家信息安全应用示范关键技术研究与应用（S219 工程）”项目分别荣获国家科学技术进步奖二等奖。另外，公司还荣获上海市科学技术进步奖一等奖、党政密码科技进步一等奖（省部级）等奖项。

3）人才优势

公司的研发团队集中了信息安全技术领域的资深技术专家、博士、高级工程师。同时，公司是国内信息安全领域国家级重点科研项目的主要承担者之一，先后承担了 12 项国家级、省部级的重点信息安全科研项目的研究与开发工作。

4）专业资质优势

在信息安全行业，企业获取经营资质或许可的多少成为衡量信息安全厂商竞争力的重要因素。公司是目前国内同行业中拥有各类经营资质或许可较全的企业之一。公司先后取得了涉及国家秘密的计算机信息系统集成资质证书（甲级）、计算机信息系统安全专用产品销售许可证，以及各类涉密信息系统产品检测证书、商用密码产品技术鉴定证书、信息技术产品安全测评证书等多项经营资质或许可。子公司格尔安全获得上海市武器装备科研生产叁级保密资格单位认定，以及上海市软件行业协会颁发的《软件企业证书》。

5）品牌价值优势

经过十余年发展，公司已成为国内信息安全行业 PKI 领域的优势企业之一，通过了 CMMI3 认证和 ISO9001 质量认证，为用户提供功能完善、质量可靠的 PKI 产品。公司是全国信息安全标准化技术委员会网站可信国家标准项目组成员单位、中国密码学会第二届理事会理事单位，同时亦是国家科技支撑计划商用密码基础设施项目的牵头单位。截至报告期末，公司共发起、参与研制行业标准规范 26 项；其中，作为发起单位研制的相关标准为 6 项，作为主要参与单位研制的相关标准达 20 项。

6）营销服务体系优势

公司推进以“行业服务专业化”和“区域服务本地化”相结合的客户服务体系建设。即对于行业客户，由格尔国信、格尔安全等子公司和公司的电子政务、军工、公安等事业部，分别提供专业的行业服务指导与支撑；对于区域客户，形成以上海、北京、广州、西安、乌鲁木齐、郑州为区域中心，辐射其他区域的二级联动管理的营销服务网络。

公司的“行业与区域协同发展”营销战略，有利于提高公司对用户需求响应的及时性，拓宽公司产品的市场占有率和客户深度开发能力，增强公司的综合竞争力。

7）客户资源优势

公司客户主要为国家部委、地方政府部门、军工企业、金融机构、大中型企事业单位，客户资源稳定。由于信息安全行业的特性，稳定优质的客户资源有利于公司进一步开拓新市场，促进公司的持续快速发展。

4.2.2 PKI 产品体系完整丰富

格尔软件是中国首批研制和推出 PKI 公钥基础设施产品的厂商。经过十余年的发展，公司已成为信息安全行业 PKI 产品市场的优势企业之一。整体上，公司的产品包括 PKI 基础设施产品、PKI 安全应用产品和通用产品三大类。

图 22：格尔软件 PKI 产品

资料来源：网络公开资料，东兴证券研究所

公司产品主要以软硬件结合的方式（公司不生产硬件，所需硬件设施设备等原材料均向第三方进行采购）实现相应的功能和用途。

表 7：格尔软件 PKI 产品

主要产品及服务		主要功能简述	详细功能及用途
PKI 基础设施产品	数字证书认证系统	为用户（数量 规模较大）生 成数字证书的信息系统	该系统由证书认证系统（CA）、证书注册系统（RA）、 目录服务系统（LDAP）、在线证书状态验证系统 (OCSP)及时间戳系统等子系统组成完整的 PKI 公钥 基础设施，该系统同时支持 SM2 和 RSA 算法，提供完 备的数字证书全生命周期的管理，主要包括用户证书管 理、机构证书管理、设备证书管理、代码签名证书管理、 日志审计、统计报表、下级 RA 授权、安全通讯等功能 模块

	身份认证系统	为用户（数量 规模较小）生 成数字证书的一体化信息系 统	而向小规模应用的一体化电子认证中心产品，系统以硬 件服务器形式提供。它集成丫 PKI 体系中 CA/RA；KM/LDAP 等子系统的功能于一身，提供了数 字证书和黑名单全生命周期管理功能，可以签发个人、 服务器和域控等多种类型证书，证书格式遵循 X.509 V3 标准.可以与微软域服务器结合，提供基于硬件的智 能卡登录服务；系统同时支持 HTTP 和 LDAP 两种方 式的黑名单查询；系统遵循国际通用标准规范，采用基 于 B/S 架构的管理界面，具有使用方便，维护简单等特 点
	密钥管理系统	为数字证书认 证系统提供密 钥服务	该系统是 PKI 公钥基础设施的重要组成部分；系统实 现对加密密钥的全生命周期管理，该系统严格遵循国家 密码管理局的标准和规范，具备对多个第三方数字认证 中心并行支持的能力，兼容支持 SM2 和 RSA 算法，具 南完备的司法取证机制，系统采用格尔专利技术，完整 地实现丫双中心双证书机制
PKI 安全应用产品	安全认证网关	防 ih 非法身份 进入应用系 统，同时对合法用户传递的 信息进行加密	该产品基于 PKI 技术实现 SSL 加密传输和强身份认证， 提供身份鉴别、传输加密、权限控制和访问审计等功能。 该产品支持国家标准密码兑法，支持标准 CA 证书和黑 名单，支持 4-7 层的各类应用协议，产品配套提供 Android、iOS、Windows Mobile 等多种安全客户端软 件。公司 S 新推出的基于 64 位架构的高性能网关，支持超大并发访问、支持热备部署、支持自负载的集群
	可信边界安全网关	安全认证网关 的一种，主要 用于公安部门 等领域	—款支持在不同的物理网络，不同等级的安全域之间实 现边界防护的网关设备。该网关可以在两个不同信任域 的网络边界进行部署。在不同信任域之间发生访问时， 支持对连接进行动态身份转换，保证不同的信任域只处 理自身信任的身份凭证。该产品基于 PKI 技术实现强 身份认证，终端接入认证，用户角色分组，资源访问授 权，URL 级别的日志审计，以及对敏感数据进行加密 传输。同时也可以与多种系统进行联动，并可作为边界 入口与安全认证网关产品进行对接
	无线安全网关	安全安认证网关的一种，主要以无线方式进行接入	该产品是一款针对无线应用场景的身份认证网关设备，对移动网络中的慢速连接进行了特殊处理，支持 PKI 技术实现的身份认证，访问控制，传输加密，日志审计 等功能，该产品还支持对移动应用中的各类智能终端进行管理，包括设备准入检查，终端锁定，应用推送等功 能
	电子签章系统	以电子化的签 章代替传统的 纸质签字盖章 流程，帮助用户真正实现无 纸化应用	该系统基于国际公认的公钥基础设施（PKI)体系，结 合 CA 数字认证技术，将电子印章系统和电子签名技术 完整的结合在一起，实现对数据电文的电子签名以及印 章的吋视化展现；系统通过直观的、符合用户操作习惯 的图形化印章形式，实现数据电文的真实性、完整性和 防抵赖
	安全电子邮件系统	基于 PKI 技术 的电子邮件系 统	—款基于 PKI 技术实现的、具有强大安全功能的、WEB 方式的电了•邮件系统，跟传统邮件系统的相比，增加丫 以下安全功能:①支持使用数字证书进行邮箱账户的认 证；②支持邮件加密，实现电子邮件的保密性；③支持 邮件的数字签名，实现对电子邮件操作的不吋抵赖性； ④邮件加密存储，保障信息资产的安全
	安全即时通信系统	基于 PKI 技术 的即时通讯系统	该产品部署在网络中，向用户提供安全的即时通信服 务，不仅能够确保收发即时消息的机密性、完整性和不 可抵赖性，还可以保证即时消息的隐私性和存储安全性，在满足国家关于敏感信息系统的标准要求以及安全 管理要求的同时，有效解决政府机关、军工涉密单位以 及各企事业单位在即时通信软件使用需求和安全管理要求之间的矛盾
	工信部印发《网络保险箱	基于 PKI 技术 服务器端的电 子文件存储与 管理的安全系统	采用加密技术实现的安全电子文件管理系统，由安全管 理服务器和客户端软件组成，系统结合用户的文件存储 系统，可以组成完整的安全电子文件存储与管理系统。 系统支持高强度的基于数字证书的用户认证，支持电子 文件的客户端加密、传输加密和存储加密，系统支持安 全策略的集中管理，支持加密文件的授权共享
	终端信息保密系统	基于个人终端 设备中电子文 件存储与管理 的安全系统	该产品的基本功能主要包括：①文件保险箱功能，实现 PC 电子文件的加密存储；②文件加解密功能，实现文 件的加解密应用；③文件碎纸机功能，通过以随机数多 次重写确保机密文件在删除后不可恢复。同时，该产品 支持多种安全功能的拓展，包括高强度的证书开机认 证、屏保认证等
	签名验证服务	而向各类电子 数据	—款基于 PKI 技术实现的密码服务产品，该产品由服 务器，服务器 API 和客

	器	提供数字 签名和数字签 名验证的专用硬件服务器	户端签名控件三大部分组成； 服务器采用专用设备实现密码的安全高效运算，产品支 持每秒 20000 次以上的签名和验签；服务器 API 支持 Java、.NET、C 等多种语言； 客户端签名控件支持标准 版木正浏览器
	局域网接入验证系统	用于保障合法 身份接入单位 内部局域网络	该系统可以确保非授权用户或计算机无法接入内部局 域网络，从而强化整个内部局域网络的保护和控制力 度，防止网络资源被非授权人员滥用，达到防.lh 信息泄密的目的。系统基于正 EE 802.lx 协议，采用基于 PKI 数字证书强身份认证，通过系统及交换机的配置，提供接入认证、接入绑定、接入日志审计、非认证接入的自 动阻断等功能；实现阻断无授权接入、禁止私接终端、 禁止私接 hub 等网络接入控制管理;从根本上杜绝/外 来计算机和网络设备随意接入内部网络的安全隐患
PKI 安全应用产品	移动安全管理平台	为移动终端设 备建立全生命 周期的安全保 障体系	基于 PKI 体系，以移动终端生命周期管理为核心，从 终端、网络、应用、数据等层面进行安全保护，实现对 移动终端的安全加间，对网络边界的可信接入，对业务 行为的授权访问，对数据的安全存放及传输。移动安全 管理平台对移动终端从注册-> 使用->销毁整个生命周 期进行集中统一管理,通过采取集中管控手段形成立体 化的管理体系，并对终端的使用全过程进行有效的 i 己 录，形成一条完整有效的行为轨迹，实现关联事件的倒 查取证
	云安全 平台系统	为云计算环境 提供可信的安 全服务及安全 应用服务	通过“云安全服务平台（Cloud Security Services Platform System， 简称 CSSPS)”为云计算环境提供安全服务， 该平台以“安全即服务(Securityasa Service)”为理念， 基于 PKI 公钥基础设施，为云计算环境提供基础的安 全服务及安全应用服务，服务内容包括:数字证书服务、 身份认证与访问控制服务、数据加密服务、签名验证服 务和证书审计服务
	打印管控系统	对办公环境中 打印设备的管 控与使用市计	打印管控系统（Print Managemenl: and Contiol Systems， 简称 PMCS)是一套管理和控制办公环境中打印行为的 系统。该系统通过增加打印审批过程来规范打印行为， 通过记录详细的打印日志强化打印管理，通过采用加密 技术保障打印内容安全
	移动介质管理系统	用于 USB 存储 设备等移动介 质的安全使用 管理	—款对 USB 存储设备进行完善管理、严格控制的产品。 该产品将系统分为内部计算机与外部计算机，将 USB 存储设备分为内部 USB 存储设备与外部 USB 存储设 备，实现外部计算机无法识别内部 USB 存储设备、内 部计算机拒绝外部 USB 存储设备接入，同时根据相应 策略对内部 USB 存储设备的接入和使用进行细致、有 效的控制，以有效防止内部信息通过 USB 存储设备泄 密
通用安全产品	网络审计系统	对网络行为进 行管理、控制 与记录	该系统综合采用了多种国际和国内先进技术，实现对全 网的多维管控与审计；经国家权威机构检测，产品最大 吞吐量超过 20Gbps,适用于我国大型网络和骨干网络 的高速审计和海量数据处理，该产品是网络安全管理机 构准确亨握网络态势、监控网络行为、定位分析安全事 件、全而保障网络安全的有效丁具
	信息安全系统集成	为构建一个高 效的信息安全 体系，而需要 为用户配置不 同层面的通用安全软硬件设施设备	涵盖计算机应用系统 T 程和网络系统工程的安全需求 界定、安全设计、建设实施、安全保证等内容，即通过 提供分级保护、等级保护等信息安全咨询及建设服务，依托专业的信息安全专家团队及雄厚的技术底蕴，以良 好的政策及规范标准解读能力， 通过需求识别、安全界定、风险评估、安全测评、解决方案设计、安全管理策略设计、安全规划、项目建设、系统运维、应急响应等各项内容，为政府机关、据弄个单位、金融机构、大中型企事业单位等进行安全规划设计及实施建设工作，帮助客户构建安全保障体系

资料来源：网络公开资料，东兴证券研究所

4.2.3 利润持续增长，未来可期

网络安全已逐渐成为维护国家安全的工作重点。2018 年公司实现营业收入 30,858.54 万元，较上年同期增长 13.60%；实现归属上市公司股东净利润 7,179.99 万元，较上年同期增长 2.21%。公司拟 10 转 4.2 股派 2.8 元。

2018 年，在政府、军工、电子政务等领域稳步推进主营业务，有序进行身份认证体系的顶层布局与规划。公司实现了大数据云平台下统一门户、统一身份和统一权限管理系统，经历了首届中国国际进口博览会“大用户高并发”的考验，为进博会安保保障作出了贡献。同时，公司进一步拓展金融领域，参与并完成部分省市的财税及银行项目。公司加大对云计算安全、物联网安全、移动互联网安全、工业互联网的产品研发以及与客户群体业务对接工作的投入，提升公司的竞争。

公司继续保持技术研发投入力度，以不断提升公司的科技创新能力。2018 年陆续投入研发费用约 5,593.82 万元，对主要产品进行了全面的改造和适配，推出支持车辆网环境的信息安全产品，完善身份认证与管理产品，为移动设备支持 PKI 应用提供解决方案并实现了国际化支持。

公司秉承“技术领先、做精产品”的研发理念，通过持续创新和改进，不断完善和优化以 PKI 为核心的信息安全产品和服务体系；积极推进“行业与区域协同发展”的营销战略，以国家信息安全等级保护和分级保护政策为导向，深入开展面向国家部委和行业总部机关的总部营销战略，持续推进覆盖全国的区域营销体系建设；进一步推进以“行业服务专业化”和“区域服务本地化”相结合的客户服务体系建设；不断巩固和提升公司在信息安全行业尤其是 PKI 领域的竞争优势，在风险可控的前提下，及时把握市场新需求，积极开拓与创新，进一步拓展以 PKI 为核心的相关产品的应用范围，致力于将公司打造成为稳健发展、国内一流、国际知名的信息安全公司。

4.3 数字认证：电子认证技术优势企业

北京数字认证股份有限公司是北京市国有资产经营有限责任公司控股的国有企业，是国内领先的信息安全解决方案提供商，主要业务为电子认证服务、电子认证产品及可管理的信息安全服务。公司为用户提供涵盖电子认证服务和电子认证产品的整体解决方案，建立起覆盖全国的电子认证服务网络和较完善的电子认证产品体系。应用领域覆盖政府、金融、医疗卫生、彩票、电信等市场，在电子政务领域的市场占有率位居行业前列，并已在医疗信息化、网上保险、互联网彩票等重点新兴应用领域建立了市场领先优势。公司是高新技术企业和软件企业，是具有工业和信息化部颁发的电子认证服务许可证资质，国家密码管理局颁发的商用密码销售、使用许可资质和电子政务电子认证服务许可资质、卫生系统电子认证服务资质的电子认证服务商;是具有国家风险评估资质、国家应急处理资质、国家信息安全服务安全工程类资质和北京市信息安全服务资质的信息安全服务提供商。

4.3.1 公司主要业务

公司是领先的网络安全解决方案提供商，坚持“共建可信任的数字世界”的企业愿景、以“提供高品质的网络安全服务，帮助用户构建安全可信的网络空间”作为公司使命，始终致力于保障用户信息基础设施安全可靠运行、保护用户信息化业务安全可信开展、

保卫用户数字资产。公司面向全国客户提供电子认证服务、安全集成、安全咨询与运维服务，并在政务、金融、医疗卫生、电信、教育、交通等领域建立领先优势。

公司主要产品和服务：电子认证服务、安全集成、安全咨询与运维服务。其中电子认证服务业务占比较大，2018 年营业收入占总收入的 59%。

1）电子认证服务

公司电子认证服务主要包括数字证书和电子签名两类服务。

- 公司的数字证书服务是为用户提供数字证书的生产和管理。数字证书是基于密码技术生成的一种电子文件，在网络世界中作为身份认证、电子签名和信息保护的基础。公司签发数字证书前需要对用户身份进行鉴别，数字证书的有效期一般为 1 年，用户应在到期前更新。公司在用户新办数字证书和每年更新数字证书时收取数字证书年服务费，对于存放在 USBKEY 等证书介质中的数字证书，公司在用户新办数字证书时同时收取证书介质费用。
- 公司的电子签名服务主要向客户提供电子签名生成、电子签名验证、电子签名信息管理等服务，并在此基础上向用户提供电子合同管理、证据保全、司法鉴定等解决方案。电子签名是一种在电子文件中起到表明签名人身份和签名人对电子文件内容认可的电子技术手段，是一类反映电子交易事件事实的关键电子证据，在《中华人民共和国电子签名法》中规定："可靠的电子签名与手写签名或者盖章具有同等的法律效力"。目前公司基于密码技术构建了可靠电子签名服务体系，向用户提供可靠电子签名服务，客户不需要建设自己的电子签名系统，就可直接使用公司的服务来满足电子签名生成及相关管理需求。公司的电子签名服务业务已面向全国进行推广，开始进入快速发展阶段。根据应用领域及具体项目情况，收费方式有按签名次数、包年、阶梯式定价等不同的模式。

2）安全集成

公司安全集成业务是根据客户自身需求，为客户提供适合其信息系统特点的网络安全保障解决方案。公司的解决方案是将自有产品（如：身份管理产品、电子签名产品）、第三方信息系统和网络安全产品（如：防火墙产品、入侵检测与入侵防御产品、统一威胁管理产品等）有效的与客户信息系统集成，从而提高客户信息系统的安全保障能力。安全集成业务的销售模式分为直销和与渠道商合作两种模式，其中自有产品定价采用生产成本加上合理利润方式，第三方软硬件产品定价方式为采购成本加上合理利润，集成服务费按照项目总金额一定比例收取。安全集成业务一般按照合同约定进度收款，在合同签署、产品到货、初验和终验等环节约定不同收款比例。

3）安全咨询与运维服务

公司的安全咨询与运维服务包括：风险评估、合规性咨询、代码审计、脆弱性检查、渗透测试、安全巡检等多项专业安全服务，相关服务按照不同内容、频次与工作量收取服务费。业务收入受项目数量、项目规模以及实施周期等因素影响，存在一定波动。

安全咨询与运维服务通常以年度（12 个月）为服务周期，合同款项通常分两次收取，首次收款在合同签订时，尾款在服务结束时收取。

公司进一步增强安全咨询与运维服务能力，通过深度挖掘客户需求为原有客户提供更多高质量服务，并进一步积极开拓新的优质客户，2018 年公司安全咨询与运维服务营业收入较 2017 年增长约 3,345 万元，同比增长 30.11%。

4.3.2 提供“一体化”电子认证解决方案

信息安全风险日益复杂，身份欺诈、非授权访问、行为抵赖等安全风险日益严峻，为保障网上业务的健康有序开展，需要同时满足身份认证、授权管理、责任认定等客户安全需求。因此，单一的产品或服务无法满足用户的综合保障需求，只有综合利用服务和多种产品形成“一体化”的解决方案，才能满足客户的网络信任需求。“一体化”的解决方案已成为行业发展趋势，具备电子认证“一体化”解决方案能力的企业将更易形成竞争优势。

数字认证是获得工信部电子认证服务许可证的第三方电子认证服务机构，同时公司也具备较强的电子认证产品的自主研发能力，是行业内少数整合电子认证服务和电子认证产品，能够为客户提供“一体化”电子认证解决方案的公司之一，具备突出的市场竞争优势。公司电子认证解决方案以《电子签名法》为依据，以密码技术为基础，主要用于以身份认证、授权管理和责任认定为主要内容的网络信任体系建设以及信息保护，能帮助客户建立起身份可信、电文可信、行为可信的安全可信网络空间。

图 23：数字认证一体化电子认证解决方案

资料来源：网络公开资料，东兴证券研究所

在基础平台方面，公司建立了数字证书认证系统、电子签名服务系统等基础平台，为电子认证服务、电子认证产品提供可靠的基础技术支撑。在电子认证服务方面，公司构建了数字证书和电子签名服务体系，不仅能可信规范地提供可信数字身份服务，还在国内率先形成了可靠电子签名服务支撑能力，建立了提供网络信任服务的全面基础。在电子认证产品方面，公司拥有自主知识产权的产品体系，涵盖了电子认证基础设施、可信数字身份管理、可靠电子签名等主要产品。在此基础上，通过对应用业务的深入研究，整合电子认证服务和电子认证产品，公司能够快速和有效地为多个行业、多种业务应用建立完整的电子认证解决方案，以满足快速发展的可信数字身份、可信数据电文、可信网络行为等一体化网络信任需求。

4.3.3 公司将受益于电子认证行业快速发展

面对日益严峻的网络安全形势，近年来针对网络安全的政策、法规、指导意见不断推出，《网络安全法》、《国家网络空间安全战略》、《关于推动资本市场服务网络强国建设的指导意见》、《网络安全等级保护条例（征求意见稿）》等法律法规和配套文件陆续出台，网络安全建设受到政策大力支持，行业呈现出加速发展的趋势。

公司的客户主要为政府、企事业单位、医院、金融企业等。在政务方面，2018 年 6 月国务院办公厅发布国办发〔2018〕45 号文《进一步深化“互联网+政务服务”推进政务服务“一网、一门、一次”改革实施方案》，提出“进一步深化‘互联网+政务服务’，充分运用信息化手段解决企业和群众反映强烈的办事难、办事慢、办事繁的问题”，将有利于公司业务的推广和应用。在医疗卫生方面，2018 年 4 月国务院办公厅发布国办发〔2018〕26 号文《关于促进“互联网+医疗健康”发展的意见》，指出“加快建设基础资源信息数据库，完善全员人口、电子健康档案、电子病历等数据库。大力提升医疗机构信息化应用水平”，国家卫健委发布的《医疗质量安全核心制度要点》明确“病历应准确反映医疗活动全过程，实现医疗服务行为可追溯，维护医患双方合法权益，保障医疗质量和医疗安全”，这些政策的推出更有利于公司产品和服务在医疗卫生领域的推广。在金融方面，中国证监会《证券期货投资者适当性管理办法》和中国银保监会《保险电子签名技术应用规范》的发布均对公司电子认证业务起到推动作用。

经过十多年的创新发展，公司成为以自主知识产权技术为核心、国内领先的网络安全解决方案提供商。公司是网络信任与数字安全领域标准规范的倡导者，也是行业应用的引领者。公司凭借优良的产品质量、良好的售后服务及不断扩大的市场占有率，成功树立并享有较高的品牌知名度和信誉度。随着公司业务的不断拓展，新技术的不断应用，新产品的不断推出，公司行业领先地位进一步巩固。

表 8：重点跟踪公司

公司名称	盈利预测				PE 估值			
	2017A	2018A	2019E	2020E	2017A	2018A	2019E	2020E
卫士通	0.20	0.19	0.65	0.96	148	156	45	31
格尔软件	1.15	0.84	1.09	1.42	36	49	38	29
数字认证	1.05	0.72	1.02	1.48	45	65	46	32

资料来源：东兴证券研究所

分析师简介

单击此处输入文字。

陆洲

北京大学硕士，军工行业首席分析师。曾任中国证券报记者，历任光大证券、平安证券、国金证券研究所军工行业首席分析师，华商基金研究部工业品研究组组长，2017 年加盟东兴证券研究所。

王习

香港理工大学硕士，4 年证券从业经验，曾任职于中航证券，长城证券，2017 年加入东兴证券军工组。

研究助理简介

张卓琦

清华大学工业工程博士，3 年大型国有军工企业运营管理培训、咨询经验，2017 年加盟东兴证券研究所，关注新三板、军工领域。

单击此处输入文字。

分析师承诺

负责本研究报告全部或部分内容的每一位证券分析师，在此申明，本报告的观点、逻辑和论据均为分析师本人研究成果，引用的相关信息和文字均已注明出处。本报告依据公开的信息来源，力求清晰、准确地反映分析师本人的研究观点。本人薪酬的任何部分过去不曾与、现在不与，未来也将不会与本报告中的具体推荐或观点直接或间接相关。

风险提示

本证券研究报告所载的信息、观点、结论等内容仅供投资者决策参考。在任何情况下，本公司证券研究报告均不构成对任何机构和个人的投资建议，市场有风险，投资者在决定投资前，务必要审慎。投资者应自主作出投资决策，自行承担投资风险。

免责声明

本研究报告由东兴证券股份有限公司研究所撰写，东兴证券股份有限公司是具有合法证券投资咨询业务资格的机构。本研究报告中所引用信息均来源于公开资料，我公司对这些信息的准确性和完整性不作任何保证，也不保证所包含的信息和建议不会发生任何变更。我们已力求报告内容的客观、公正，但文中的观点、结论和建议仅供参考，报告中的信息或意见并不构成所述证券的买卖出价或征价，投资者据此做出的任何投资决策与本公司和作者无关。

我公司及其所属关联机构可能会持有报告中提到的公司所发行的证券头寸并进行交易，也可能为这些公司提供或者争取提供投资银行、财务顾问或者金融产品等相关服务。本报告版权仅为我公司所有，未经书面许可，任何机构和个人不得以任何形式翻版、复制和发布。如引用、刊发，需注明出处为东兴证券研究所，且不得对本报告进行有悖原意的引用、删节和修改。

本研究报告仅供东兴证券股份有限公司客户和经本公司授权刊载机构的客户使用，未经授权私自刊载研究报告的机构以及其阅读和使用者应慎重使用报告、防止被误导，本公司不承担由于非授权机构私自刊发和非授权客户使用该报告所产生的相关风险和责任。

行业评级体系

公司投资评级（以沪深 300 指数为基准指数）：

以报告日后的 6 个月内，公司股价相对于同期市场基准指数的表现为标准定义：

强烈推荐：相对强于市场基准指数收益率 15%以上；

推荐：相对强于市场基准指数收益率 5%～15%之间；

中性：相对于市场基准指数收益率介于-5%～+5%之间；

回避：相对弱于市场基准指数收益率 5%以上。

行业投资评级（以沪深 300 指数为基准指数）：

以报告日后的 6 个月内，行业指数相对于同期市场基准指数的表现为标准定义：

看好：相对强于市场基准指数收益率 5%以上；

中性：相对于市场基准指数收益率介于-5%～+5%之间；

看淡：相对弱于市场基准指数收益率 5%以上。