

证券研究报告

2019年06月27日

行业报告 | 行业专题研究

计算机

国产密码法落地超预期，关注CA产业链投资机会

作者：

分析师 沈海兵 SAC执业证书编号：S1110517030001

分析师 缪欣君 SAC执业证书编号：S1110517080003



天风证券

[综合金融服务专家]

行业评级：强于大市（维持评级）

上次评级：强于大市

请务必阅读正文之后的信息披露和免责声明

# 摘要

## 1、为什么现在关注国产密码？

国产密码是实现自主可控的关键，属于刚需；国密算法拥有更优越的性能，有望对RSA形成替代。

## 2、国产密码市场空间与发展节奏？

我们认为，国产密码市场间接可达百亿元规模，短期由政策推动，长期依托物联网发展而扩张。受益于密码法落地节奏加快，国密潮有望提前来临。

## 3、竞争格局与投资机会？

资质认证形成准入门槛，客户资源构筑持续竞争力；PKI市场有望维持双寡头格局。

**建议关注：**启明星辰、数字认证、格尔软件、卫士通等

**风险提示：**密码法落地节奏不及预期；国密行业竞争加剧

# 1

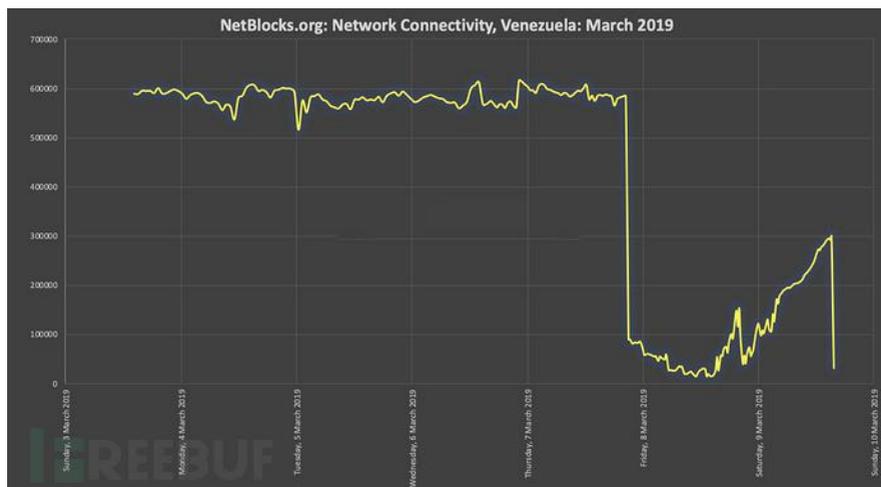
## 为什么现在关注国产密码?

# 多国电力系统遭遇攻击，密码国产化值得高度重视

根据《纽约时报》2019年6月15日消息，美国已经在俄罗斯的电力网络系统中植入进攻性的恶意软件，未来如果与俄罗斯间的网络战进一步升级的话，可以作为美方的威慑力量与筹码。据新华网消息称，2019年3月，委内瑞拉的基础设施遭遇网络攻击，导致电力中断。据环球时报消息，美媒披露美国对伊朗实施“宙斯炸弹”计划，通过该行动，美国可以令伊朗防空、通信系统以及关键性的电网瘫痪。

多国电力基础设施遭遇网络攻击，威胁民众生活及国家利益，网络安全值得引起重视。

图1：委内瑞拉遭遇电力攻击导致三次断电



资料来源：FreeBuf、天风证券研究所

图2：美媒称美欲“网攻”俄电网

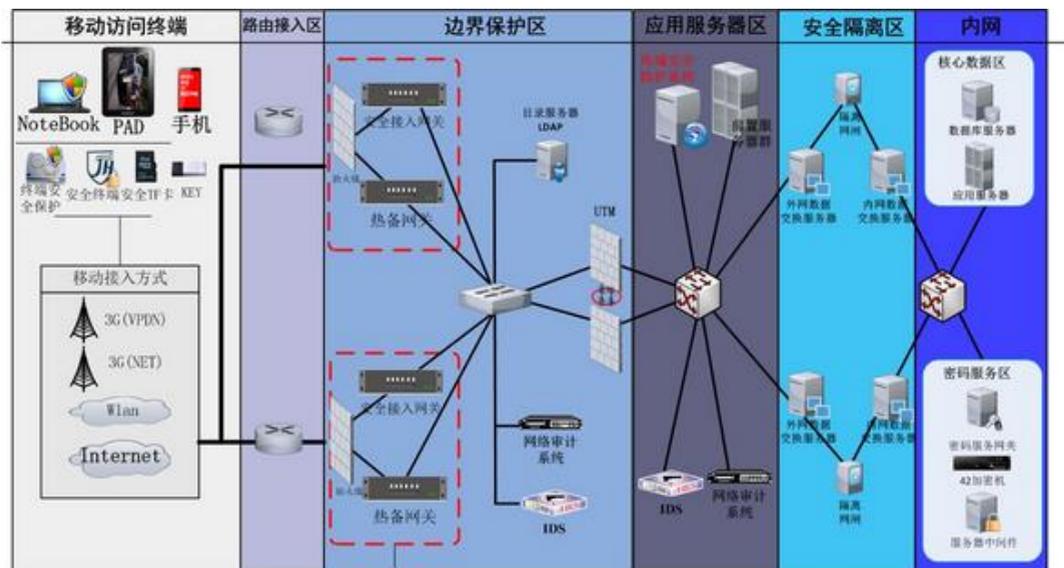


资料来源：CCTV、天风证券研究所

# 国产密码是实现自主可控的关键，属于刚需

密码技术是保障网络安全的核心技术，密码算法和密码产品的自主可控是确保我国信息安全的重中之重。当前我国大多采用国外制定的加密算法，存在着大量的不可控因素，一旦被不法分子利用攻击，所产生的损失将不可估量。实现密码产品自主可控软硬件全国产化替换，是防止后门漏洞的最有效方法，是保障网络安全的终极举措。国密算法具备自主知识产权，符合国家信息产品国产化战略。我们认为随着国产替代趋势的进一步加强，存量市场上，国密算法将有望实现对RSA等国际算法的加速替代。

图3：政府行业移动安全解决方案



资料来源：江南信安官网、天风证券研究所

## 国产密码性能优越，更快更安全

国家将密码分为核心密码、普通密码、商用密码，实行分类管理。以商用密码SM2算法为例，SM2拥有更高的安全性能和更快加密速度。目前主流的RSA算法是基于大整数因子分解数学难题(IFP)进行设计，其数学原理相对简单，单位安全强度相对较低。SM2是基于ECC（Elliptic Curves Cryptography，椭圆曲线密码编码学），单位安全强度相对较高。基于ECC的SM2证书普遍采用256位密钥长度，加密强度等同于3072位RSA证书，高于业界普遍采用的2048位RSA证书。更长的密钥意味着必须来回发送更多的数据以验证连接，产生更大的性能损耗和时间延迟。因此，SM2算法能够以较小的密钥和较少的数据传递建立HTTPS连接，在确保相同安全强度的前提下提升连接速度。

**表1：SM2在同等加密强度下采用更短的密钥长度，连接速度更快**

RSA密钥长度	ECC密钥长度	保密年限
1024	160	2010
2048	224	2030
3072	256	2040
7680	384	2080
15360	512	2120

资料来源：沃通官网、天风证券研究所

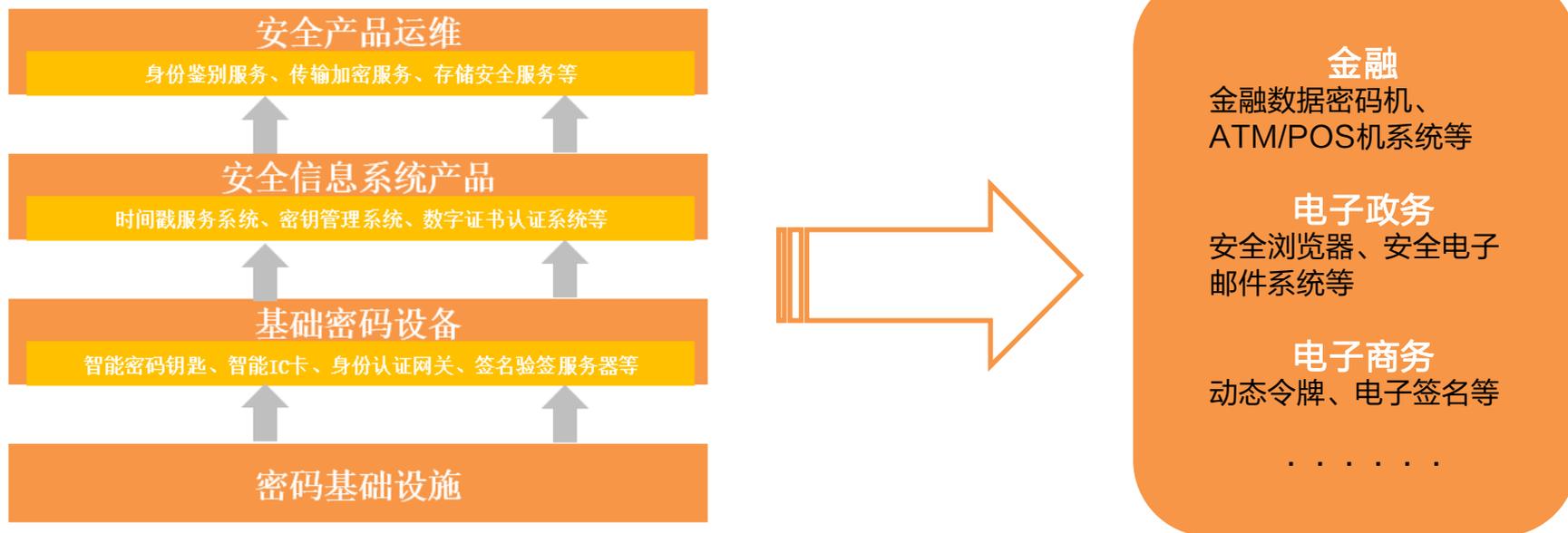
# 2

## 产业链及市场空间

# 国密算法的应用兼顾软硬件，应用空间广泛

密码作为保护网络与信息安全的重要手段，在身份识别、安全隔离、信息加密、完整性保护和抗抵赖等方面发挥着不可替代的重要作用。国产密码产业涉及以基础密码设备为主的硬件产品及安全信息系统为主的软件产品，并衍生出相关安全运维服务，运用范围广，应用场景复杂多变，目前广泛运用于金融、政务、电子商务等领域。

图4：国产密码产业链



资料来源：格尔软件官网、江南天安官网、炼石网络等、天风证券研究所

## 目前，已在金融、政务等领域得到广泛应用

金融方面，2013年，中国人民银行发布《中国金融集成电路（IC）卡规范》，首次支持SM算法；2014年，中国银联修订发布《中国银联金融IC卡技术规范》支持SM算法。自此，金融IC卡开始试点应用SM算法并逐步规模化应用。2014年以来，中国银联先后修订发布了交换系统、受理终端规范支持SM算法，并成功实施改造推广。政务方面，截至2018年上半年，随着CA系统SM2国产算法升级的加速推进，目前已有26个省及5个部委完成算法升级工作；新CA系统签发国密算法SM2证书总计60256张，同比增长近7.6倍，国密产品得到广泛应用。

图5：银行卡交易报文处理加解密示意图



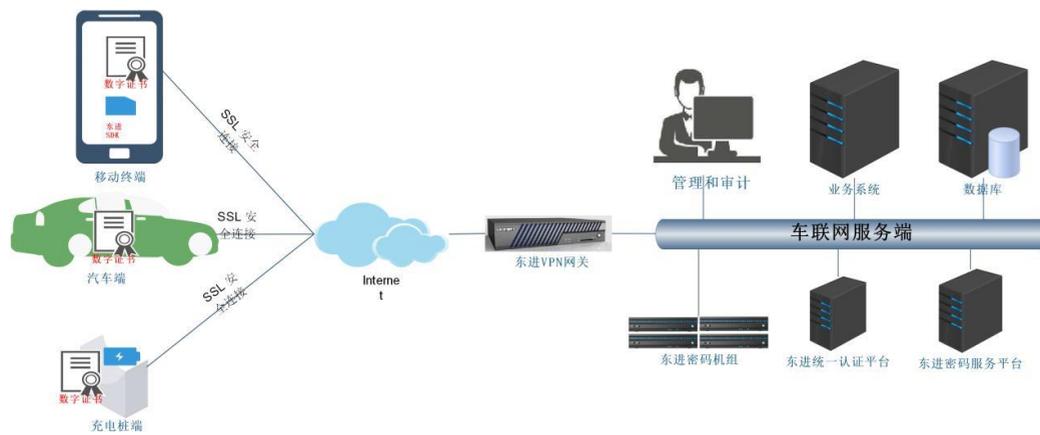
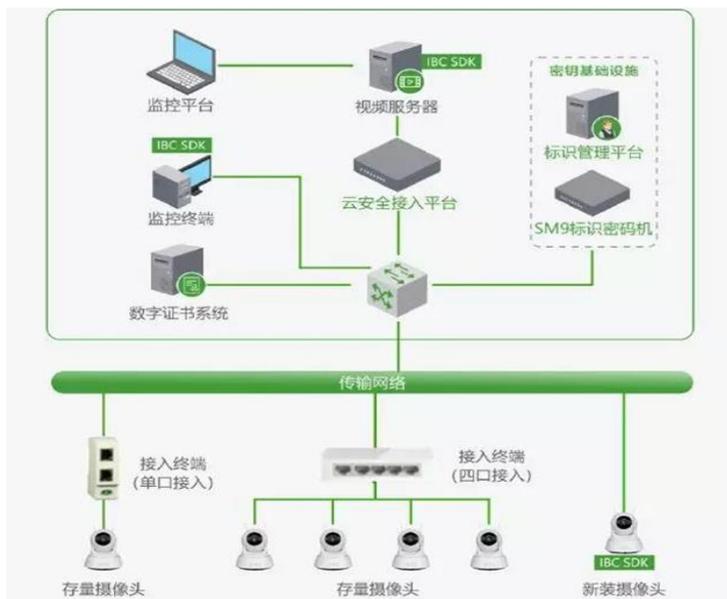
资料来源：《实战：银行卡领域SM系列算法应用技术分析》（《金融电子化》王欢、陈芳）、天风证券研究所

# 未来，有望进一步应用于安防、车联网等新兴领域

从安防角度，国密产品可运用于视频监控系统安全解决方案，通过终端接入管理，加强安全认证，保障视频安全传输，免受人为破坏。从车联网角度，以密码技术为核心的安全支撑平台主要由证书认证系统、授权管理系统、密钥管理系统和安全管理系统共同构成，可为智能运输系统提供身份鉴别、授权管理、安全传输、数据保护、责任认定和安全管理六项数据安全服务。从工业互联网角度，国密相关产品可用于加强平台双方的身份认证，防止数据被篡改，实现安全连接、安全执行和安全存储。

图6：基于国密算法的视频监控系统安全解决方案

图7：车联网安全认证解决方案



资料来源：奥联官网、天风证券研究所

资料来源：东进官网、天风证券研究所

# 坚定不移推进密码应用，密码应用领域和范围快速拓展

密码产业支撑能力显著增强。密码供给能力进一步提升，在国家专项支持和应用需求的有力牵引下，支持商用密码算法的密码产品已达 1390 多款，其中安全芯片 127 款。密码产品检测能力显著提升，信息系统的密码应用安全性评估试点逐步展开，首批 10 家密评机构已经国家密码管理局认定，稳步开展密码应用安全性评估试点工作。密码标准体系建设逐步健全，已发布 68 项商用密码行业标准；密码标准国际化实现重要突破，祖冲之算法成为 3GPP 标准、SM2 和 SM9 算法成为 ISO 国际标准。

图8：密码应用领域和范围快速拓展



资料来源：《中国信息安全》、国家密码局、天风证券研究所

表2：国产密码主要产品形态

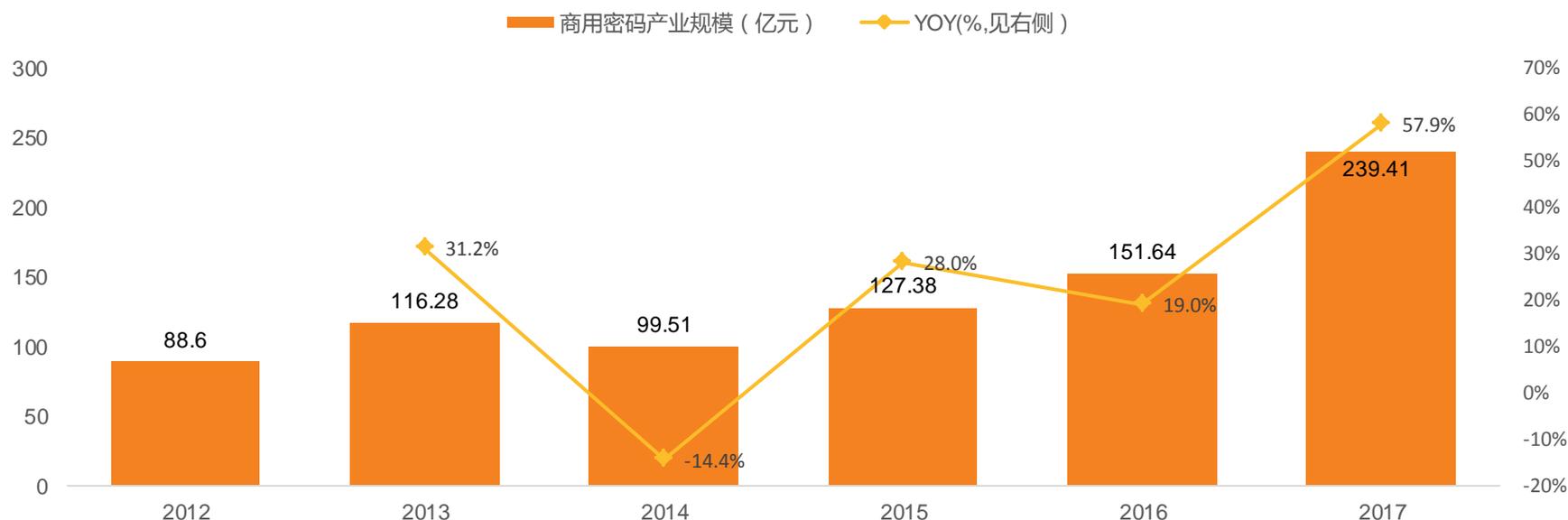
产品名称	产品型号数量（个）
安全芯片	127
POS密码应用系统	103
智能IC卡	98
智能密码钥匙	48
密码键盘	42
电子签章系统	34
SSL VPN安全网关	33
动态令牌	32
签名验签服务器	32
蓝牙型智能密码钥匙	31

资料来源：国家密码局（2019）、天风证券研究所

# 商用密码产业市场超百亿规模

根据数观天下统计，2017年我国商用密码产业规模达到239.41亿，较2016年增长57.9%。2015-2017年复合增长率为37%。我们认为，随着商用密码技术不断创新，我国商用密码产业有望持续蓬勃发展，未来市场规模持续超过百亿元。

图9：国产密码产业规模

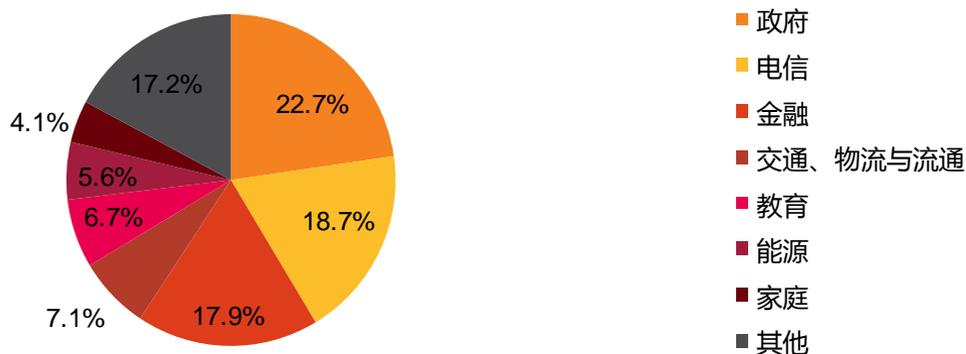


资料来源：数观天下、天风证券研究所

## 短期来看，政策通过推动渗透率，驱动行业增长

国密市场有望率先由政府及央企打开。从政府角度来看，根据《电子政务电子认证服务质量评估要求》国家政策要求，用户证书应当是基于SM2密码算法的签名证书和加密证书。根据密码法草案征求意见稿，县级以上人民政府应当将密码工作纳入本级国民经济和社会发展规划，所需经费列入本级预算。我们认为，国密产品有望实现从国家级机关到县级机关的逐步渗透。从央企角度来看，央企涉及国有资产且资产规模大，业务范围广且子公司较多，在经营过程中需要通过加强身份认证等实现安全保障。且国家密码局规定自2011年3月1日起，国家政府机关、事业单位、大型央企等都应使用SM2算法，我们认为全面推广SM2算法，提高国密产品渗透率，将为国密行业带来重大机遇。

图10：信息安全下游行业以政府为主，短期来看市场受政策驱动明显

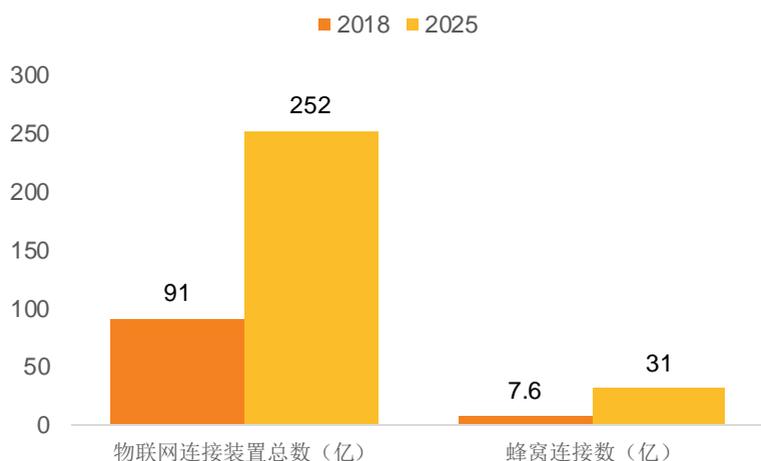


资料来源：前瞻产业研究院、天风证券研究所

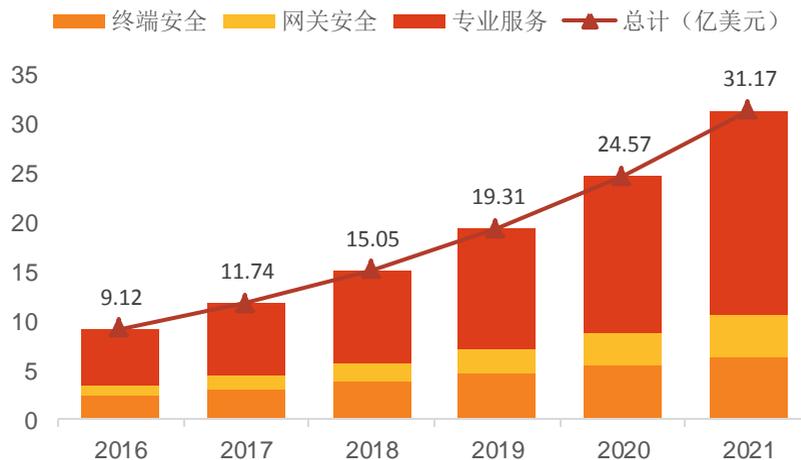
# 长期来看，物联网推动使用场景多样化，提升增长中枢

物联网安全事件频发，全球物联网安全支出将不断增加。当前，基于物联网（IoT）的攻击已经成为现实。据Gartner调查，近20%的企业或相关机构在过去三年内遭受了至少一次基于物联网的攻击。当前，大量物联网设备及云服务端直接暴露于互联网，容易遭到网络攻击，若物联网设备存在的漏洞被发起攻击，不仅用户隐私将被暴露，而且还会影响基础通信网络的正常运行。我们认为，在物联网的发展过程中，物联网安全也应该得到足够重视，万物互联的发展趋势推动安全产品的使用场景多样化发展，有望提升国密行业增长中枢。

图11：全球联网设备高速增长，万物互联成为趋势 图12：安全事件频发，物联网安全支出将不断增长



资料来源：GSMA、天风证券研究所



资料来源：Gartner、天风证券研究所

# 3

## 推进节奏和竞争格局

## 受益于政策驱动，国密产品得到进一步应用

《“十三五”国家信息化规划》提出，构建关键信息基础设施安全保障体系，要加强密码应用，国家互联网大数据平台建设，要推进数据加解密、完整性验证等安全技术的应用。银行业清算办法、网络安全等级保护管理要求、政务信息化规划，也都提出密码应用要求。我们认为，越来越多的国家相关法规落地到国密具体产品，不断强化密码应用与国家战略的融合，将促进国密产品得到进一步应用。

图13：政策驱动行业发展



资料来源：中国政府网、财政部、天津市电子认证中心、中国国家标准化管理委员会等、天风证券研究所

# 密码法草案已提交审议，落地节奏有望加快

国产密码因所处行业特殊性较容易受到政策驱动影响。《密码法》作为统领全国密码工作的国家层面综合性法律，其的出台将填补密码领域的法律空白，推动密码在网络安全与信息化发展中发挥更大作用。据中国人大网公告，密码法草案的议案于2019年6月25日至29日在十三届全国人大常委会第十一次会议进行审议，我们认为密码法落地节奏有望得以加速。

图14：密码法落地节奏加快



资料来源：中国政府网、中国人大网、天风证券研究所

图15：密码法已提交审议

The screenshot shows a news article header with a red navigation bar containing a back arrow and the text '中新网·新闻·正文'. The main title is '中国拟立密码法 明确任何组织或个人不得窃取他人加密信息', dated '2019年06月25日 11:43 中国新闻网'. The article text includes: '中新网北京6月25日电 (梁晓辉 黄钰钦)密码法草案25日提请十三届全国人大常委会初次审议。草案明确，任何组织或者个人不得窃取他人的加密信息，不得非法侵入他人的密码保障系统，不得利用密码从事危害国家安全、社会公共利益、他人合法权益的活动或者其他违法犯罪活动。' and '密码法草案中的密码，是指使用特定变换对信息等进行加密保护或者安全认证的产品、技术和服务。密码的主要功能有两个：一个是加密保护，另一个是安全认证。' The bottom of the screenshot shows the text '密码法草案共分总则，核心密码、普通密码，商用密码，法律责任，附则五章四十四条。'

资料来源：中国新闻网、天风证券研究所

# 资质认证形成准入门槛

信息安全行业具有特殊性和敏感性，专业技术水平要求较强，为了保证我国信息安全产业的稳定、规范和健康发展，国家规定信息安全行业内企业从事研发、生产和经营需要取得各类相应的资质认证。获取资质认证是新进入者参与竞争的先决条件，由于相关资质认证的要求较高且申请周期相对较长，因此新进入者难以在短期内进入市场并参与竞争。以CA为例，按照信息产业部《电子认证服务管理办法》的规定，CA的密码方案必须经过国家密码管理局的审批认证，CA信息系统必须通过国家信息安全产品的评测认证，取得国家认可的资质，才能投入运营。

图16：涉密信息系统集成资质证书



资料来源：吉大正元官网、天风证券研究所

表3：格尔软件相关资质证书

格尔软件资质
软件企业认定证书
涉及国家秘密的计算机信息系统集成资质证书（甲级）
涉及国家秘密的计算机信息系统集成资质证书单项（软件开发）
商用密码产品生产定点单位证书
商用密码产品销售许可证
高新技术企业证书
国家火炬计划重点高新技术企业证书
CMMI3级认证证书
质量管理体系认证证书
计算机信息系统集成企业资质三级

资料来源：格尔软件官网、天风证券研究所

# 优质客户资源保障持续发展

由于行业的特殊性，信息安全行业的下游客户对上游产品供应厂商存在一定的依赖性，优质的客户资源不仅是上游厂商业务收入的稳定来源，也是宣传和扩大知名度的良好载体。信息安全行业的客户主要为国家部委、地方政府部门、军工企业、金融机构等，由于涉及安全保密问题等特殊性的，其对信息安全厂商的选择极为慎重，且通常存在一定的路径依赖，不会轻易更换厂商。我们认为，拥有优质客户资源，可以为公司提供持久竞争力。

**表4：信息安全厂商主要为国家部委及政府部门**

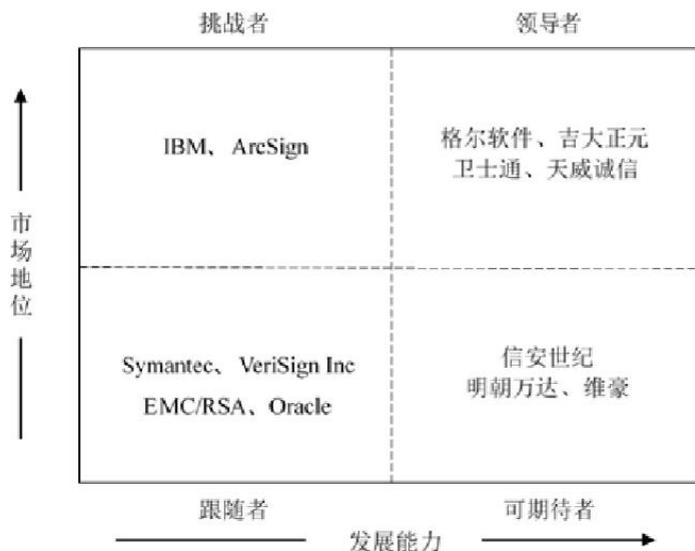
所属行业	客户名称
国家部委	国家发改委、国家安全部、全国人大、最高人民法院、公安部、外交部、民政部、国土资源部、国家统计局、国家药监局、国家密码管理局、国家审计署、国家信息中心、国家气象局、全国总工会、国务院法制办、国家外汇管理局、国家知识产权局等
地方政府部门	上海经信委、天津经信委、福建经信委、浙江工信厅、上询市委机要局、云南省委机要局、江苏省委机要局、新疆党委机要局、湖两省委机要局、福建省委机要局、河北省委机要局、陕西司法厅、安徽司法厅、安徽财政厅以及全国多地政府信息中心等
公安	各省市自治区公安厅局、公安部第一研究所、公安部第三研究所等
军工	中国航空工业集团公司、中国航天科技集团公司、中船重工集阳公司、中国工程物理研究院、中核工业集团公司等
金融机构	中国人民银行、中国银联、中国银行、中国工商银行、中国农业银行、中国建设银行、交通银行、招商银行、广发银行、平安银行、反洗钱监测中心、印钞造币总公司、上海银行、上海农商银行、山东省城市商业银行合作联盟、山东省农村信用联社、浙江省农村信用社联合社等
CA公司	新疆CA公司、浙江CA公司、安徽CA公司、湖南CA公司、河北CA公司、天津政务CA公司、福建CA公司、云南CA公司等
大中型企事业单位	中海运集团、歌华集团、广东电信、福建联通、华力微电子、湖北电力、福建电力、深圳超算中心、新疆众和等

资料来源：格尔软件招股书、天风证券研究所

## 以PKI市场为例，双寡头格局有望持续

结合目前国产密码厂商在参与业内标准制定情况、身份和数字认证软件的市占率情况，我们认为，以在国产密码细分行业下PKI领域，形成以吉大正元和格尔软件为首的双寡头格局。鉴于信息安全行业的特殊性和敏感性，对专业技术水平要求较强，客户忠诚度较高，资质认证要求较高且周期较强，我们认为当前PKI市场的双寡头格局有望延续。

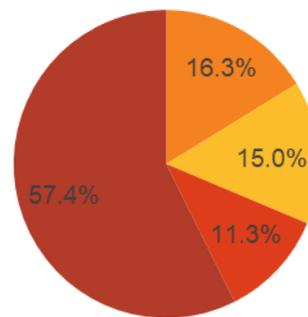
图17：PKI竞争格局



资料来源：赛迪顾问、天风证券研究所

图18：2018年身份和数字信任软件市场格局

■ 吉大正元 ■ 亚信安全 ■ 上海格尔软件 ■ 其他



资料来源：IDC、天风证券研究所  
注释：国密产品不是亚信安全主要业务

# 4

## 投资机会

## 投资机会

我们认为，密码法节奏加快，国密潮有望提前来临。短期来看，政策推动国密产品渗透率提高；长期来看，国密产品有望在物联网行业得到进一步应用，相关上市公司长期成长空间有望打开。

基于此，我们建议关注标的：启明星辰、数字认证、格尔软件、卫士通等。

# 5

## 风险提示

## 风险提示

- 1、密码法落地节奏不及预期。存在密码法推进过程遇到阻碍，导致落地进度不及预期的风险。
- 2、国密行业竞争加剧。行业存在竞争加剧，毛利率下降风险。

## 分析师声明

本报告署名分析师在此声明：我们具有中国证券业协会授予的证券投资咨询执业资格或相当的专业胜任能力，本报告所表述的所有观点均准确地反映了我们对标的证券和发行人的个人看法。我们所得报酬的任何部分不曾与，不与，也将不会与本报告中的具体投资建议或观点有直接或间接联系。

## 一般声明

除非另有规定，本报告中的所有材料版权均属天风证券股份有限公司（已获中国证监会许可的证券投资咨询业务资格）及其附属机构（以下统称“天风证券”）。未经天风证券事先书面授权，不得以任何方式修改、发送或者复制本报告及其所包含的材料、内容。所有本报告中使用的商标、服务标识及标记均为天风证券的商标、服务标识及标记。

本报告是机密的，仅供我们的客户使用，天风证券不因收件人收到本报告而视其为天风证券的客户。本报告中的信息均来源于我们认为可靠的已公开资料，但天风证券对这些信息的准确性及完整性不作任何保证。本报告中的信息、意见等均仅供客户参考，不构成所述证券买卖的出价或征价邀请或要约。该等信息、意见并未考虑到获取本报告人员的具体投资目的、财务状况以及特定需求，在任何时候均不构成对任何人的个人推荐。客户应当对本报告中的信息和意见进行独立评估，并应同时考量各自的投资目的、财务状况和特定需求，必要时就法律、商业、财务、税收等方面咨询专家的意见。对依据或者使用本报告所造成的一切后果，天风证券及/或其关联人员均不承担任何法律责任。

本报告所载的意见、评估及预测仅为本报告出具日的观点和判断。该等意见、评估及预测无需通知即可随时更改。过往的表现亦不应作为日后表现的预示和担保。在不同时期，天风证券可能会发出与本报告所载意见、评估及预测不一致的研究报告。

天风证券的销售人员、交易人员以及其他专业人士可能会依据不同假设和标准、采用不同的分析方法而口头或书面发表与本报告意见及建议不一致的市场评论和/或交易观点。天风证券没有将此意见及建议向报告所有接收者进行更新的义务。天风证券的资产管理部门、自营部门以及其他投资业务部门可能独立做出与本报告中的意见或建议不一致的投资决策。

## 特别声明

在法律许可的情况下，天风证券可能会持有本报告中提及公司所发行的证券并进行交易，也可能为这些公司提供或争取提供投资银行、财务顾问和金融产品等各种金融服务。因此，投资者应当考虑到天风证券及/或其相关人员可能存在影响本报告观点客观性的潜在利益冲突，投资者请勿将本报告视为投资或其他决定的唯一参考依据。

## 投资评级声明

类别	说明	评级	体系
股票投资评级	自报告日后的6个月内，相对同期沪深300指数的涨跌幅	买入	预期股价相对收益20%以上
		增持	预期股价相对收益10%-20%
		持有	预期股价相对收益-10%-10%
		卖出	预期股价相对收益-10%以下
行业投资评级	自报告日后的6个月内，相对同期沪深300指数的涨跌幅	强于大市	预期行业指数涨幅5%以上
		中性	预期行业指数涨幅-5%-5%
		弱于大市	预期行业指数涨幅-5%以下

THANKS