# 信息安全深度剖析5：密评和信创双催化，密码产业开启从1到N

## 行业研究·深度报告

## 投资评级：超配（维持评级）

证券分析师：熊 莉 xiongli1@guosen.com.cn 证券投资咨询执业资格证书编码：S0980519030002
证券分析师：库宏垚 kuhongyao@guosen.com.cn 证券投资咨询执业资格证书编码：S0980520010001

# 报告摘要



- **密码法正式开启密码市场，数据要素让密码无处不在**。2020年《密码法》正式实施，其对核密、普密（有线、无线通信环节）、商密（密评与等保结合）均提出了明确的应用要求，密码产业进入有法可依的快速发展阶段，并有密评和信创作为政策抓手。随着数据要素市场化成为大势所趋，传统以网络为中心的安全建设，将转向以“数据为中心、结合网络边界防护”的双轴驱动，密码将嵌入在数据要素和数据安全各个环节；同时数据交易所需要的隐私计算也是密码技术的前沿方向，密码产业将长期保持稳定成长。

- **商密评估是最大推动力，市场进入从1到N阶段**。密评倒逼政企等信息系统加大密码建设，以满足评分要求。密评当前覆盖范围包括等保三级及以上信息系统、关键信息基础设施等，而大部分系统的密码建设仍十分单薄。根据密评相关产品需求，在各种密码应用中，均需要密码板卡、整机等基础产品；也包括数字证书、VPN等应用产品。根据测算和IDC数据，我国密码上游和PKI等密码核心市场，均约30亿左右。密评机构、市场当前仍处于起步阶段，可类比为2007年等保测评1.0发展时期，密评常态化推进后，商密市场将迎来数倍释放。

- **信创带动存量改造，且新信创项目国密成为标配**。我国自主研发的SM等系列算法日益成熟，且相比国际算法具备一定优势，国密替代势在必行。尤其在国家政务信息化项目中，明确了密码和项目建设的“三同步一评估”原则；而在其他关键基础设施行业，信创推动和行业政策要求中，国密应用均成为刚需，如电力行业广泛的物联网终端需求、金融行业进入核心系统的改造需求。随着行业信创进入快速推进期，国密应用和改造有望得到进一步推广，密码板卡、整机、证书、PKI等上下游产品均受益。

- **投资建议：看好密码产业高成长，维持“超配”评级**。短期密评和信创推动产业加速，长期数字要素市场化带来密码、隐私计算的持续创新，密码产业有望持续成长。当前密码行业和公司仍较小，全产业均受益于行业增速向上。上游厂商受需求拉动最为直接，建议重点关注三未信安、电科网安；军工领域的佳缘科技。应用厂商保持较高的客户粘性，重点关注吉大正元、信安世纪、数字认证、格尔软件。建议关注有密码业务的网络安全厂商，如VPN厂商深信服、天融信等；收购密码厂商弗兰科的安恒信息，持续投资密码领域的奇安信等。

- **风险提示**：商密评估政策推进不及预期；信创产业国密应用不及预期；疫情等因素反复，影响宏观经济正常运行；行业竞争加剧。

# 目录

# 密码法开启密码市场新发展

- **《密码法》已正式实施，三类密码各有应用**。密码是国家的重要的战略资源，是保障国家政治、经济、国防、能源、信息等各项安全的基础元素，因此《密码法》于2020年1月正式实施。《密码法》将密码分为三类，其中核心密码、普通密码都属于国家秘密，都用于保护国家秘密信息，核密保护的最高密级是绝密级；商密不用于保护国家秘密，主要运用在社会各个领域，包括商业、金融、能源等各行业。
- **密码法总揽密码发展，开启系统性建设**。国家秘密信息在有线、无线通信；存储、处理等各环节中，均要求按规定使用普密和核密，且要求建立检测、评估、监督等机制。例如在军工信息化发展中，带来大量普密应用场景。商密应用更为广泛，且法律规定了商密安全性评估，且要求建立监管和抽查制度，有望推动各个行业商密的应用。如果密码应用未用，法律也规定了相关整改要求和处罚措施。

## 商密、普密、核密区别


资料来源：麒麟信安、国信证券经济研究所整理

## 密码法相关要点

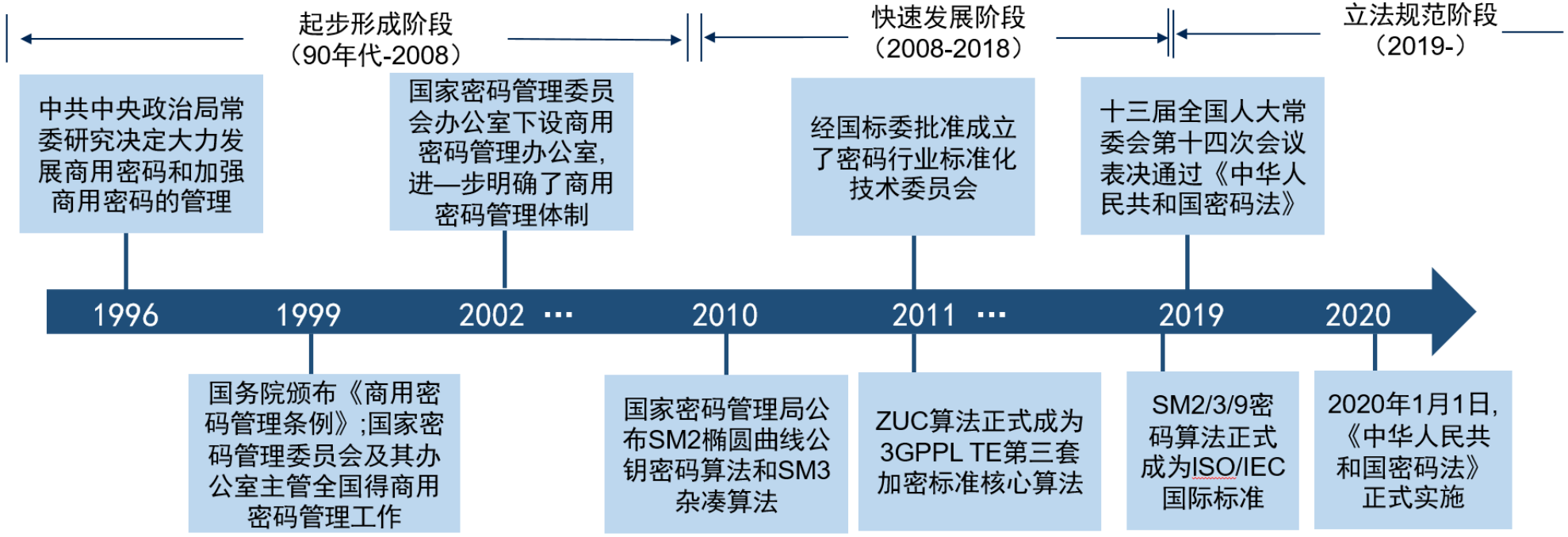
| | |
|---|---|
| 核密、普密要点 | 1、在有线、无线通信，存储、处理国家秘密信息的系统中，应当按规定使用核密和普密。<br>2、有关部门需要建立安全监测预警、安全风险评估等机制，建立监督和安全审查等制度。 |
| 商密要点 | 1、有要求的关键信息基础设施运营者，应使用商密保护，需要检测机构开展商密安全性评估；商密评估应与关基、等保评估相衔接。<br>2、有关部门建立日常监管和随机抽查相结合的商密监管制度，建立统一的商密监督管理信息平台 |
| 法律责任要点 | 1、未按照要求使用核密、普密的，处罚主要是责令整改、停止违法行为、给予警告、处分或处理责任人。<br>2、关基运营者未按要求使用商密或者开展商密评估，拒不改正的对单位处10-100万罚款，对个人处1-10万罚款 |

资料来源：《密码法》、国信证券经济研究所整理

# 我国商用密码市场进入快速发展阶段

- **我国密码规范逐步成熟，产业进入快速发展阶段**。我国商用密码的发展起步起源于20世纪90年代开启的“金字”工程，随着各行业信息化全面推进，信息安全和密码应用需求逐步兴起。从90年代开始，我国商用密码经历了起步形成、快速发展、立法规范三个发展阶段。在2008-2018年期间，商用密码率先在政府、金融等重要领域得到快速应用和发展；尤其是我国自主设计的国密算法SM系列等推出，并成为国际标准，国密算法体系也进一步成熟。当前《密码法》颁布后，伴随着商密评估的要求、信创产业的发展，我国商密产业发展速度将再提升。未来需求将在ICT基础设施、物联网、数字经济等更广泛领域渗透，商密市场规模将不断扩大。

**我国商用密码行业发展历程**



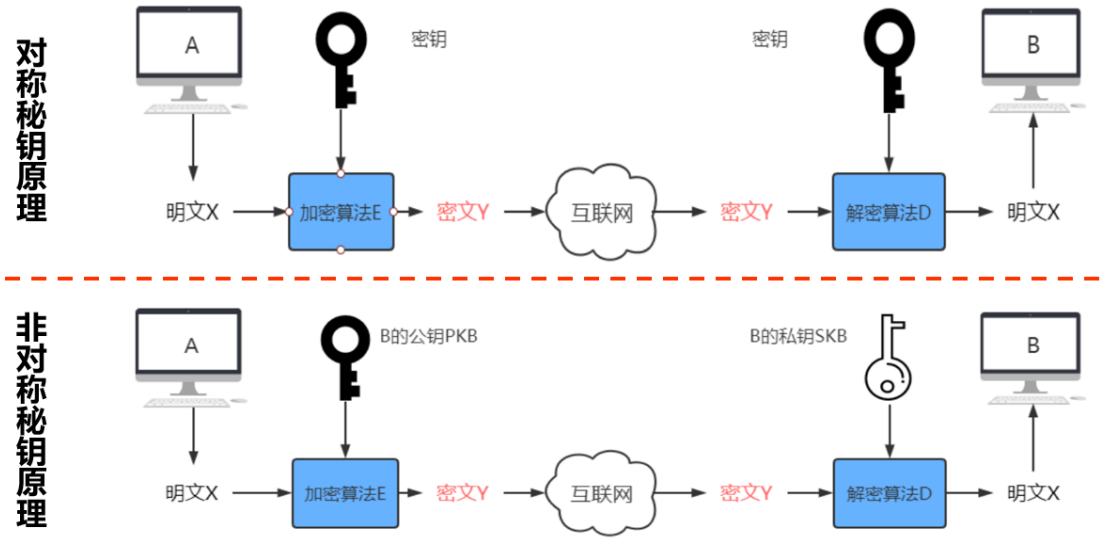

资料来源：三未信安招股说明书、国信证券经济研究所整理

# 密码本质是特定变换算法

- **密码本质是特定变换，并非口令**。密码是指采用特定变换的方法对信息进行加密保护、安全认证的技术，我们日常接触的网站密码、邮箱密码等仅是“口令”，而并非真正的密码。密码通过特定算法，实现“明文”和“密文的”变换，隐藏真实信息并完成传递或者验证，是保障信息安全的根基。常见密码体系有：对称秘钥，即加密和解密使用相同秘钥，特点是效率高，适合大量数据加密，但无法数字签名；非对称秘钥，即加密和解密使用不同的秘钥，每个用户有一对公钥和私钥，特点是能实现数字签名，适合机密数据，但速度慢。

- **秘钥核心是数学算法**。即使在当前计算机时代，大数因式分解也极其困难；常见的非对称RSA算法就是利用大数分解不对称性原理，即是2个大质数相乘来实现。例如 19801 *20201=400000001很容易计算，但是反过来分解400000001就很难。我们可以把19801和20201一个作为私钥、一个作为公钥来实现非对称加密。通过这些公钥和私钥的应用，非对称加密可以实现信息加密、身份认证等多种应用。

## 对称和非对称秘钥密码体系




资料来源：CSDN、国信证券经济研究所整理

## 非对称秘钥的典型应用


资料来源：《密码学》、国信证券经济研究所整理

# 密码是网络信任基石，产业形成多种产品类型

- **密码是保障信息安全的核心技术和基础支撑**。密码的主要功能在于加密保护和安全认证，可实现信息的机密性、真实性、数据的完整性和行为的不可否认性，是保障网络安全的最有效、最可靠、最经济的手段。密码已经成为重要的网络空间战略资源，随着公钥基础设施（PKI）的快速发展，带动密码技术的广泛应用，形成了密码芯片、板卡、整机、系统等一系列密码基础设施，并进一步衍生新的应用场景。
- **密码算法处于最底层，产品具有多种类型**。按密码产品形态划分共有6类，最上层是密码软件类，是密码算法的实现；向下游依次集成则为硬件类产品：芯片类、模块类、板卡类、整机类、系统类。按密码产品功能划分共有7类，最根本是密码算法类，不同应用下衍生出数据加解密类、认证鉴别类、证书管理类、密钥管理类、密码防伪类和综合类。

**商用密码产品6类形态划分**

| 类别 | 简介 | 典型产品 |
|---|---|---|
| 密码软件类 | 提供纯软件形态出现的密码产品 | 信息加密软件、密码算法实现软件等产品 |
| 密码芯片类 | 指以集成电路芯片形态出现的密码产品 | 密码算法芯片、密码SOC芯片等产品 |
| 密码模块类 | 指以多芯片组装的背板形态出现，具备专用密码功能，但本身不能完成完整的密码功能的产品 | 加解密模块、安全控制模块等产品 |
| 密码板卡类 | 指以板卡形态出现，具备完整密码功能的产品，作为密码产品的核心组件 | USB密码钥匙、PCI密码板卡等产品 |
| 密码整机类 | 指以整机形态出现，具备完整密码功能的产品，以密码板卡为核心组建 | VPN、网络密码机、服务器密码机、签名验证服务器等产品 |
| 密码系统类 | 指以系统形态出现，由密码功能支撑的产品，一般由多个密码整机组成 | 安全认证系统、密钥管理系统等产品 |

资料来源：三未信安招股说明书、国信证券经济研究所整理

**商用密码产品7类功能划分**

| 类别 | 简介 | 典型产品 |
|---|---|---|
| 密码算法类 | 提供基础密码运算功能的产品密码算法芯片 | 密码算法芯片 |
| 数据加解密类 | 提供数据加解密功能的产品 | 服务器密码机、VPN 设备 |
| 认证鉴别类 | 提供身份认证、密码鉴别功能的产品 | 动态口令系统、认证网关 |
| 证书管理类 | 提供证书的产生、分发、管理功能的产品 | 证书认证系统 |
| 密钥管理类 | 提供密钥的产生、分发、更新、归档和恢复等功能的产品 | 密钥管理系统 |
| 密码防伪类 | 提供密码防伪验证功能的产品 | 电子印章系统、支付密码器、数字水印系统 |
| 综合类 | 提供含上述 6 类产品功能的两种或两种以上的产品 | 电子商务安全平台、综合安全保密系统 |

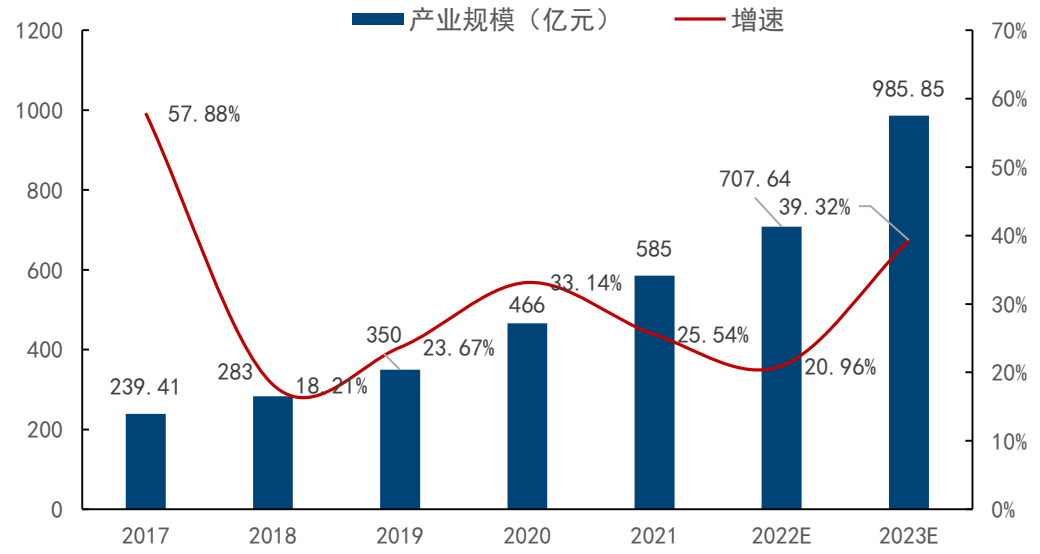
资料来源：三未信安招股说明书、国信证券经济研究所整理

# 商密市场发展有望加速

- **商业密码市场保持快速增长**。根据赛迪测算，我国商用密码产业规模不断扩大，2021年市场达到585亿元，同比增长25.54%。根据三未信安招股书说明，该统计不仅包括以密码为核心功能的密码产品，同时包含部分应用密码技术的下游网络安全产品，因此该统计市场规模会远大于商用密码产品的实际市场规模。但增速也一定程度反映了行业发展趋势，赛迪预测2022年市场达到707.64亿元（+21%），2023年市场达到985.85亿元（+39%）。在当前商密评估、信创等产业趋势下，核心密码相关产品增长有望加速。

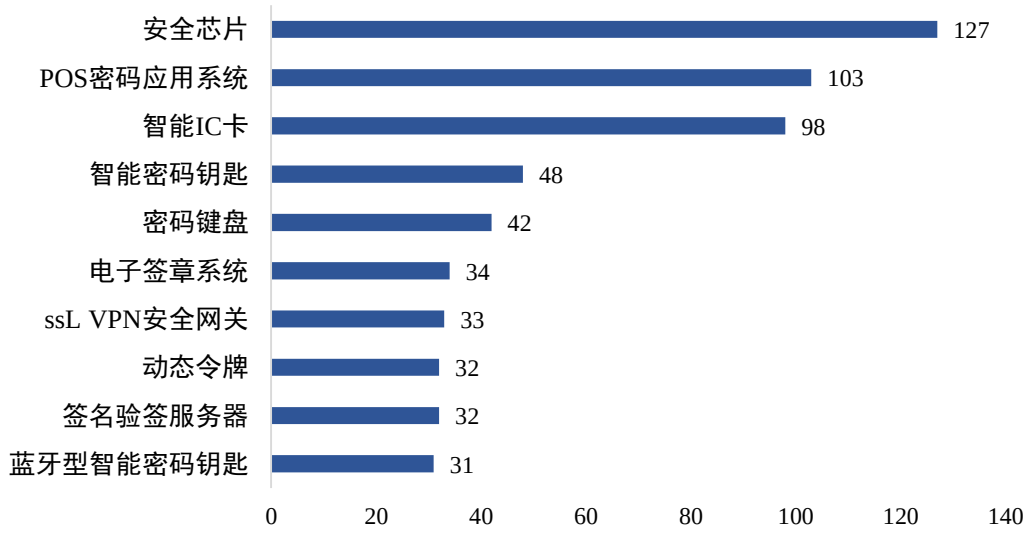
- **密码产品、应用产品种类均较多**。现有商用密码产品达到3000余款，其中2200余款产品取得商用密码产品认证证书，涵盖了密码芯片、板卡、整机等。应用密码技术的产品中，安全芯片、POS系统和智能IC卡具有最大存量改造市场；VPN、电子签章、签名验签服务器等也将充分受益。

## 商业密码产业规模预测




资料来源：赛迪网络安全研究所、国信证券经济研究所整理

## 密码各产品市场规模

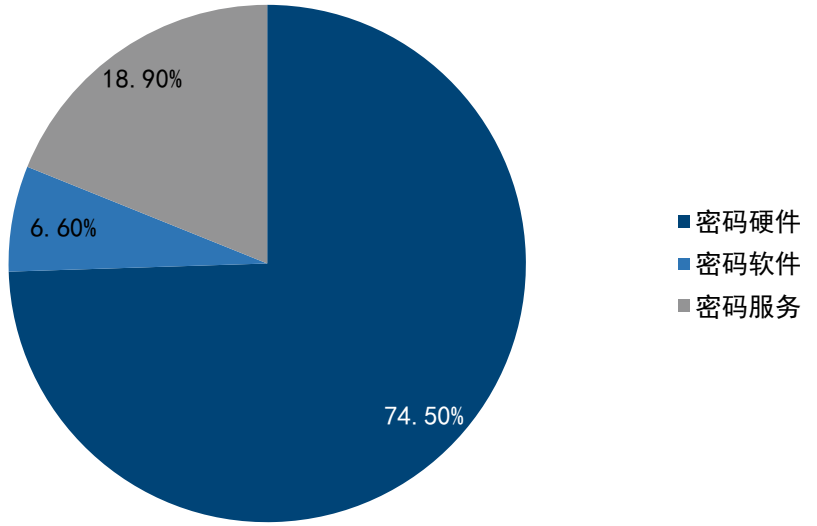



资料来源：数观天下、国信证券经济研究所整理

# 密码硬件仍是主要产品形态，关键行业应用占比高

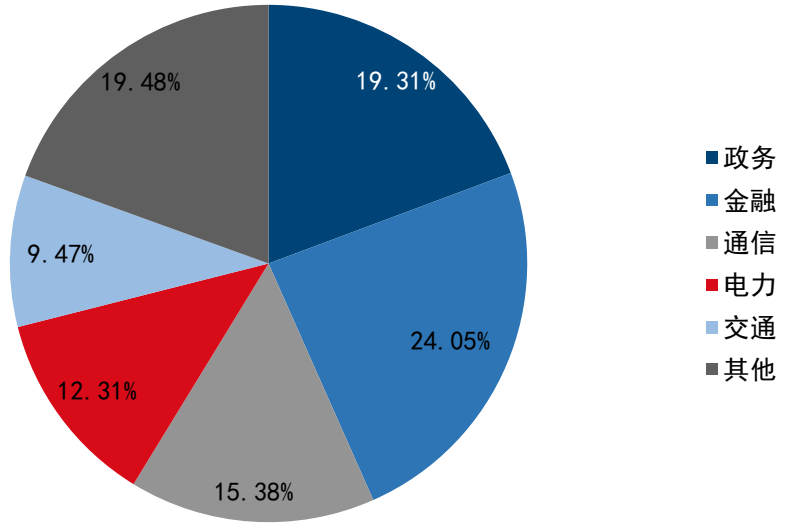
- **密码产品仍以硬件为主，新场景有望带动新应用**。根据赛迪统计，我国商密市场中硬件占比74.5%，软件占比6.6%，服务占比18.9%；相比早期硬件占比超过95%以上的结构，软件和服务占比已有所提升，但当前仍以硬件为主。随着软硬件技术的创新，新场景的结合将推动软硬件均有新发展方向：软件领域，云密码资源池和国资云等产业结合；硬件领域，国密芯片和物联网终端等产业结合。
- **政府和金融是密码应用较早领域，其他关键基础设施行业有望跟进**。理论上密码应用最终会覆盖信息化各个领域，由于早期政策推进节奏，政府安全和防伪税控等需求推动政府和金融领域应用占比较高。当前通信、电力、交通等关键行业应用占比在逐步提升，十四五均有对密码应用的相关规划，未来教育、医疗等行业国密应用也有望逐步提升。

**商密产品形态占比**




资料来源：赛迪网络安全研究所、国信证券经济研究所整理

**商用密码产品下游应用行业占比**

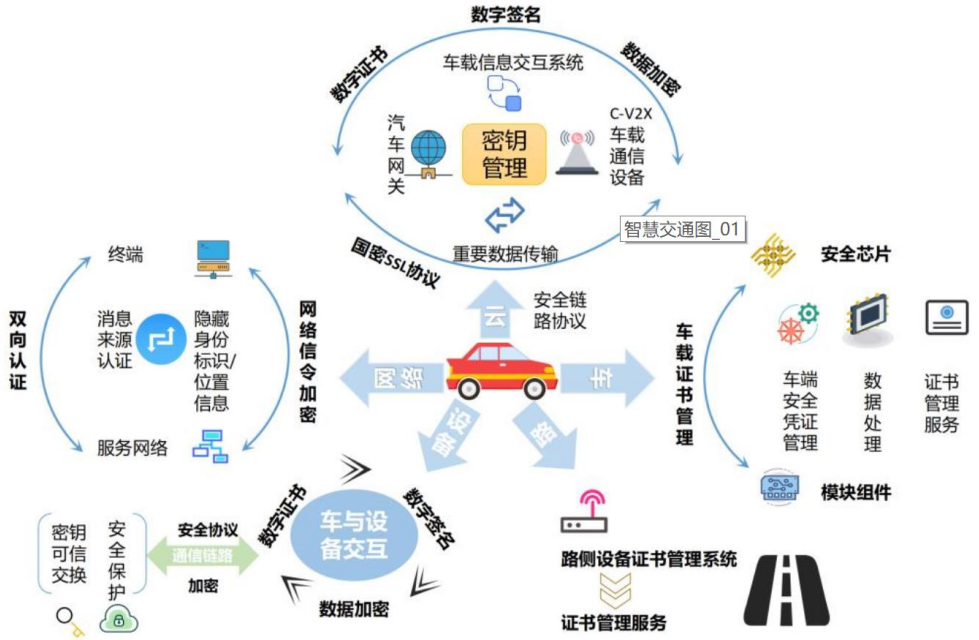



资料来源：赛迪网络安全研究所、国信证券经济研究所整理

# 密码在各种新兴场景均有广泛应用

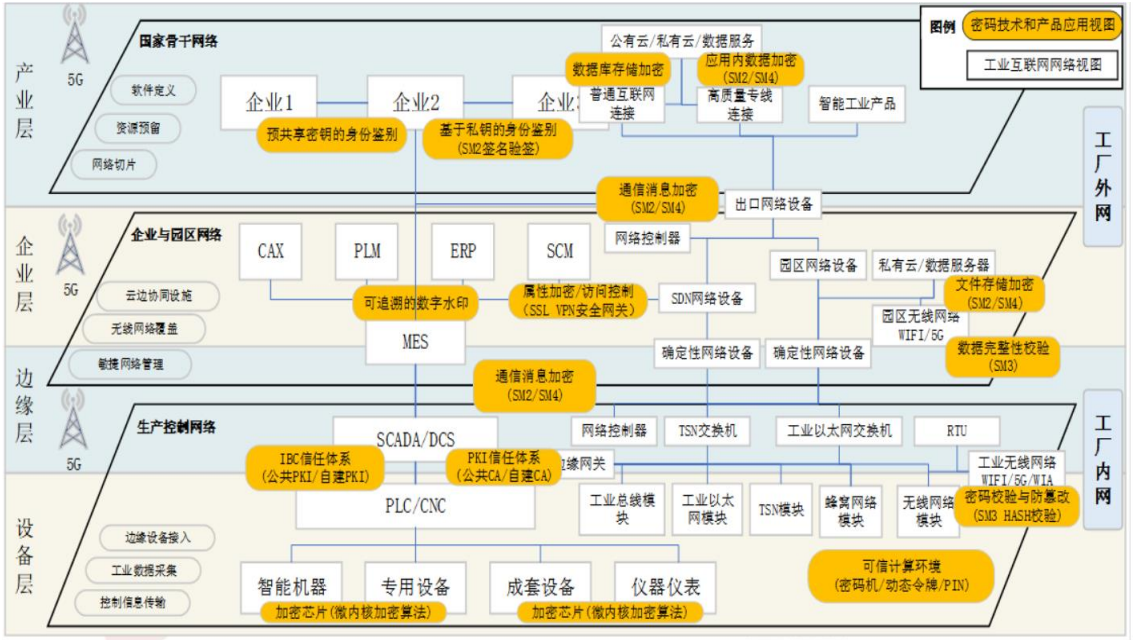
- **新兴IT应用现在要求已离不开密码建设**。除了传统信息化中密码的应用之外，车联网、物联网、工业互联网、数字货币等新领域均将密码列为必要元素。例如**车联网领域**，工信部《关于开展车联网身份认证和安全信任试点工作的通知》即是推动商密应用，保障蜂窝车联网（C-V2X）通信安全；其中车与云、车、路、设备、网络的安全通信，涉及到数字证书、数字签名、安全芯片等密码产品。在**工业互联网领域**，工信部《工业互联网创新发展行动计划（ 2021-2023 年）》要求深化商密应用，推动供需两侧有效对接，加强工业密码安全性评估等；在工业互联网平台中，设备层、边缘层、企业层、产业层需要密码芯片、PKI体系、VPN等不同产品的应用。

## 商密在车联网中运用




资料来源：《商用密码应用安全性评估白皮书》、国信证券经济研究所整理

## 商密在工业互联网中运用




资料来源：《商用密码应用安全性评估白皮书》、国信证券经济研究所整理

# 密码是数据要素的核心元素之一，隐私计算是密码前沿应用

国信证券 GUOSEN SECURITIES

- **数据要素市场化是未来方向，密码和数据安全成为重中之重**。数据成为第五大生产要素，数据安全成为刚需，密码成为数据全生命周期安全的核心；例如数字证书、数据加密、签名等密码技术贯穿于数据的采集、传输、存储、处理、交换、销毁全过程。根据国际密码厂商金雅拓统计，2018上半年泄露的45亿数据中，仅有3%是密文数据（依然安全）；因此密码在数据安全中作用极为显著。

- **隐私计算是密码前沿技术，是数据交易的关键**。隐私计算能够实现数据加密状态下的计算，以达到各参与方保护隐私的目的，是数据交易的核心技术之一。隐私计算交叉融合了密码学、人工智能等多种技术；其中密码学包括混淆电路、秘密分享、不经意传输等底层技术，以及同态加密、零知识证明、差分隐私等辅助技术。隐私计算成为密码产业发展的前沿，是突破传统应用的重要抓手。

**数据生命周期安全**


资料来源：绿盟科技、国信证券经济研究所整理

**隐私计算相关技术主要对比**

| 技术 | 性能 | 通用性 | 安全性 | 可信方 | 整体描述 | 技术成熟度 |
|---|---|---|---|---|---|---|
| 多方安全计算(MPC) | 低～中 | 高 | 高 | 不需要 | 通用性高、计算和通信开销大、安全性高，研究时间长，久经考验，性能不断提升 | 已达到技术成熟的预期峰值 |
| 可信执行环境(TEE) | 高 | 高 | 中～高 | 需要 | 通用性高，性能强，开发和部署难度大，需要信任硬件厂商 | 快速增长的技术创新阶段 |
| 联邦学习(FL) | 中 | 中 | 中 | 均可 | 综合运用MPC、DP、HE方法，主要用于AI模型训练和预测 | 快速增长的技术创新阶段 |
| 同态加密(HE) | 低 | 中 | 高 | 不需要 | 计算开销大，通信开销小，安全性高，用于联邦学习安全聚合、构造MPC协议 | 快速增长的技术创新阶段 |
| 零知识证明(ZKP) | 低 | 低 | 高 | 不需要 | 广泛应用于各类安全协议设计，是各类认证协议的基础 | 快速增长的技术创新阶段 |
| 差分隐私(DP) | 高 | 低 | 中 | 不需要 | 计算和通信性能与直接明文计算几乎无区别，安全性损失依赖于噪声大小 | 快速增长的技术创新阶段 |
| 区块链 (BC) | 低 | 中 | 中 | 不需要 | 基于带时间戳的块链式存储、智能合约、分布式共识等技术辅助隐私计算，保证原始数据、计算过程及结果可验证 | 逐渐接近技术成熟的预期峰值 |

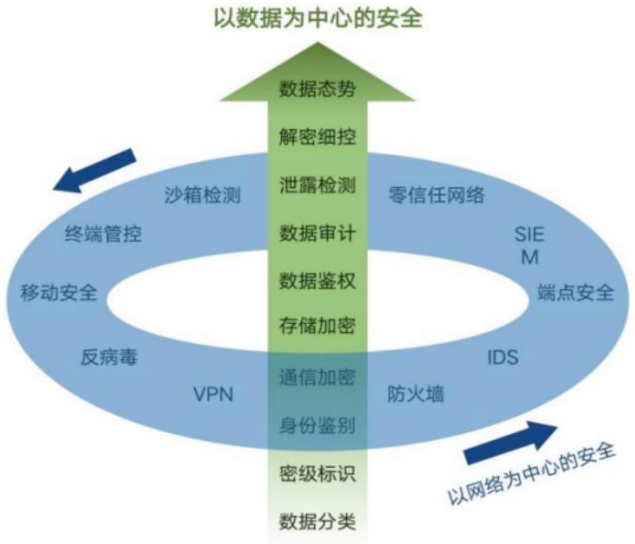
资料来源：《隐私技术白皮书2021》、国信证券经济研究所整理

# 安全建设转向以数据为中心，密码嵌入将无处不在

- **安全建设路径再树立“数据”轴心**。传统信息安全建设更多集中在网络侧，通过在边界部署防火墙等产品保障内网数据安全。随着全球正从IT时代进入DT时代，以“数据为中心、结合网络边界防护”的双轴驱动成为安全建设大势所趋。2019年美国《国防部云战略》白皮书也提出“从边界防御转向保护数据和服务”，密码和数据安全的融合应用成为安全建设的必然方向。

- **参考美国发展模式，密码模块嵌入无处不在**。美国FIPS密码模块安全评估认证是被全球广泛接受的认证体系，美国政策和产业发展中，应用内加密采用了集成密码SDK模式，催生了丰富的密码中间件产品，如各类IT产品中软硬件密码模块。从我国发展来看，信创有望推动我国IT基础设施和应用软件重塑，国密有望以各种模块形式嵌入。另一方面，即使对于已有系统，也可进行补丁增强模式进行国密改造。

## 安全建设转向以数据为中心




网络与数据并重的新安全建设理念

资料来源：《商用密码行业发展机遇报告（2022年）》、国信证券经济研究所整理

## 美国FIPS 密码模块产品分类数量TOP10


资料来源：《数据安全密码防护体系建设思路》、国信证券经济研究所整理

# 目录

# 我国商密应用仍欠缺，密评逐步推动密码应用

国信证券 GUOSEN SECURITIES

- **国内密码应用基础薄弱**。目前国内密码应用主要存在不够广泛、规范、安全、契合等问题。2018年商用密码应用安全性评估联合委员会对一万多个等保三级系统进行普查，结果显示了三大问题：第一、超过75%的系统没有使用密码；第二、普查中对118个重要系统进行安全性测评，不符合规范的比例达到85%；第三、目前仍有大量系统在使用MD5、SHA1、RSA1024、DES等具有风险的密码算法。
- **密评持续试点推动密码应用**。为了发挥密码在系统安全建设中的支撑作用，我国密码管理局在2007年就提出了商用密码应用安全性评估。伴随政策和标准要求不断明晰，在10多年积累和近年来试点后，我国密评体系已不断成熟，当前密评正在进入加速推广期。

## 商用密码应用存在的问题

| | |
|---|---|
| 应用不广泛 | 系统中密码应用比重低，不深入；大量网络数据并没有得到密码的安全防护；即使用密码，也没有正确、有效使用。 |
| 应用不规范 | 密码相关规定和制度未有效落实；系统运营者或开发者缺乏密码技能和经验，导致密码不规范使用。 |
| 应用不安全 | 现有大量系统依旧在使用有风险的密码算法，如MD5、SHA1等，导致此类系统安全性受到威胁。 |
| 应用不契合 | 工业互联网、车联网、云计算等新业态兴起，提出了不同的密码需求和性能要求，密码产业发展与之难以契合，制约密码应用。 |

资料来源：商用密码应用安全性评估白皮书、国信证券经济研究所整理

## 密评发展历程

| 发展阶段 | 时间 | 主要事项 |
|---|---|---|
| 制度奠基期 | 2007年11月27日 | 国家密码管理局《信息安全等级保护商用密码管理办法》，要求等保商用密码测评工作由国家密码管理局指定的测评机构承担 |
| | 2009年12月15日 | 国家密码管理局印发管理办法实施意见，进一步明确了与密码测评有关的要求 |
| 再次集结期 | 2017年4月22日 | 国家密码管理局印发《关于开展密码应用安全性评估试点工作的通知》，同时在七个省份、五个行业中开展密评试点工作 |
| 体系建设期 | 2017年09月27日 | 国家密码管理局印发《商用密码应用安全性测评机构管理办法（试行）》《商用密码应用安全性测评机构能力评审实施细则（试行）》《信息系统密码应用基本要求》和《信息系统密码测评要求（试行）》，初步建立密评制度体系 |
| 密评试点开展期 | 2019年10月 | 对首批密评试点机构进行评估，启动第二批密评机构试点工作 |
| | 2021年3月 | 国家市场监督管理总局、国家标准化管理委员会发布密评的关键标准，《信息安全技术信息系统密码应用基本要求》于2021年10月1日正式实施。 |
| | 2021年10月19日 | 国家密码管理局发布《信息系统密码应用测评要求》、《信息系统密码应用测评过程指南》、《随机性检测规范》等行业标准，于2022年5月1日正式实施 |

资料来源：商用密码应用安全性评估白皮书、国信证券经济研究所整理

# 政策持续推动，密评进展加速

- **政策推动密评发展**。我国近年来推出一系列政策强调对密码的应用，尤其《密码法》在2020年逐步实施，要求关键系统运营者开展密码应用安全性评估。密码重视程度与日俱增，如对党政新系统建设要求同步规划、建设和密评；且通过评估后方可上线。与早期等保测评类似，“密评”当前也“应运而生”，商用密码发展进入快速通道。

- **各个关键行业均加强密码应用落地**。2022年国务院《“十四五”数字经济发展规划》加强了密码在各行业应用。政务、金融、交通、能源、水利、医疗等各领域主管部门，均提出了密码应用明确的要求，制定了总体规划和方案。

**密评相关政策要求**

| 法律法规 | 密评要求 |
| --- | --- |
| 《中华人民共和国密码法》 | 要求使用密码进行保护的关键信息基础设施，其运营者应当使用密码进行保护，**自行或者委托密码检测机构开展密码应用安全性评估** |
| 《商用密码应用安全性评估管理办法（试行）》 | 关键信息基础设施、网络安全**等级保护第三级及以上信息系统，每年至少评估一次** |
| 《网络安全等级保护条例（征求意见稿）》 | 第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，**委托密码应用安全性测评机构开展密码应用安全性评估**。网络通过评估后，方可上线运行，并在投入运行后，每年至少组织一次评估。 |
| 《国家政务信息化项目建设管理办法》 | 项目建设单位应当落实国家密码管理有关法律法规和标准规范的要求，**同步规划、同步建设、同步运行密码保障系统并定期进行评估** |

资料来源：工信部、国家密码管理局等、国信证券经济研究所整理

**各行业密码政策**

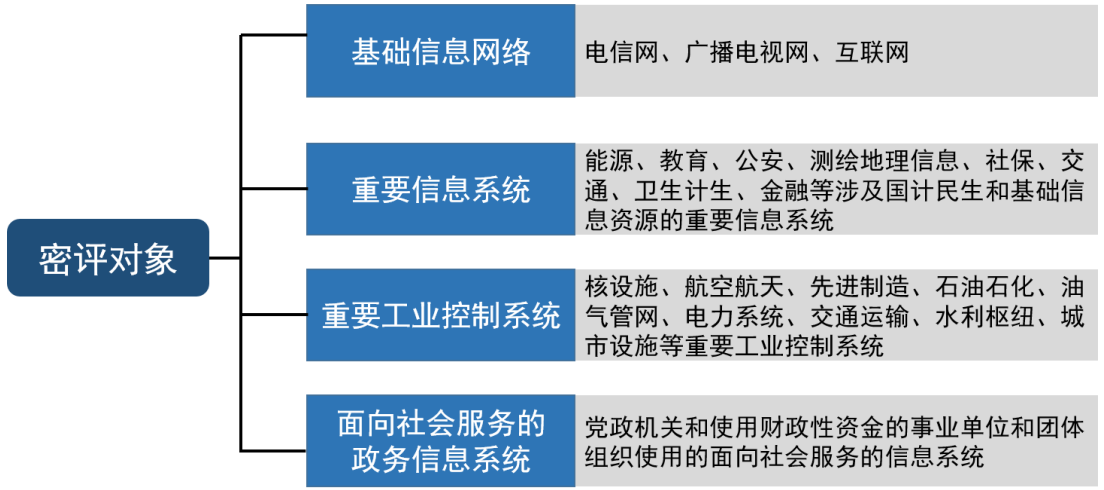
| 部门 | 政策 |
| --- | --- |
| 教育部 | 在科研网、教育管理、教育资源、电子校务、教育基础数据、教育卡等信息系统中加强密码应用。 |
| 公安部 | 在三级及以上信息系统、国家级信息化项目、公安信息网基础设施、面向社会服务的政务信息系统中加强密码应用。 |
| 财政部 | 要求采购需求应当落实国家密码管理有关法律法规、政策和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。 |
| 交通运输部 | 在ETC系统、交通一卡通系统、联网售票系统、出行服务系统、等重要信息系统加强密码应用。 |
| 水利部 | 要求，在重要水利枢纽、重要水文水利系统中加强密码应用。国务院三峡办要求，在三峡水利枢纽工业控制系统中加强密码应用。 |
| 国家卫健委 | 要求，建设卫生计生行业密码应用基础设施，在人健康信息平台、卫生计生行业重要信息系统中加强密码应用。 |
| 国家市场监督管理委员会 | 在工商部门面向社会服务的信息系统中，加快推进基于密码的网络信任、安全管理和运行监管体系建设，规范密码应用。 |
| 国家能源局 | 在电力系统、核电厂、石油天然气、油气管道等重要信息系统和重要工业控制系统中加强密码应用。 |
| 自然资源部 | 在卫星导航基准站、面向社会服务的测绘地理信息政务系统中加强密码应用。 |

资料来源：《中国密评市场分析报告》、国信证券经济研究所整理

# 密评覆盖系统广泛，体量超过等保三级

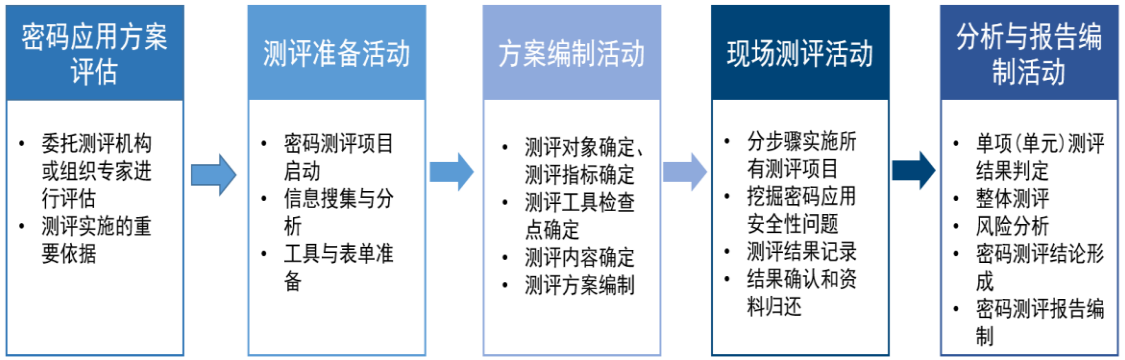
- **密评覆盖范围广泛，每年要求测评**。密评监管部门是国家密码管理局及检测中心，评估对象主要针对关键信息基础设施、网络安全保护第三级以上的系统和国家政务信息系统，要求每年至少测评一次；例如涉及国计民生的基础信息系统和网络、工业控制系统、党政机关系统等。因此密评也需要组织专家或委托测评机构进行，尤其是党政新系统的建设，要同步规划、同步建设、同步运行密码保障系统并定期进行评估；已建系统同样由测评机构评估。除了等保三级之外，有些密码应用场景，如门禁系统同样需要测评，因此密评覆盖系统体量超过等保三级。
- **密评模式与等保测评类似**。在确定密评对象后，密评中的测评部分主要包括密码应用方案评估、测评准备、方案编制、现场测评、分析和报告编制五个环节。测评完成后，则生成测评报告并上报，企业方也会据此整改以达到合格分数，如加强密码设施建设等。

## 密评对象示意图




资料来源：中科三方官网、国信证券经济研究所整理

## 密评测评工作主要环节

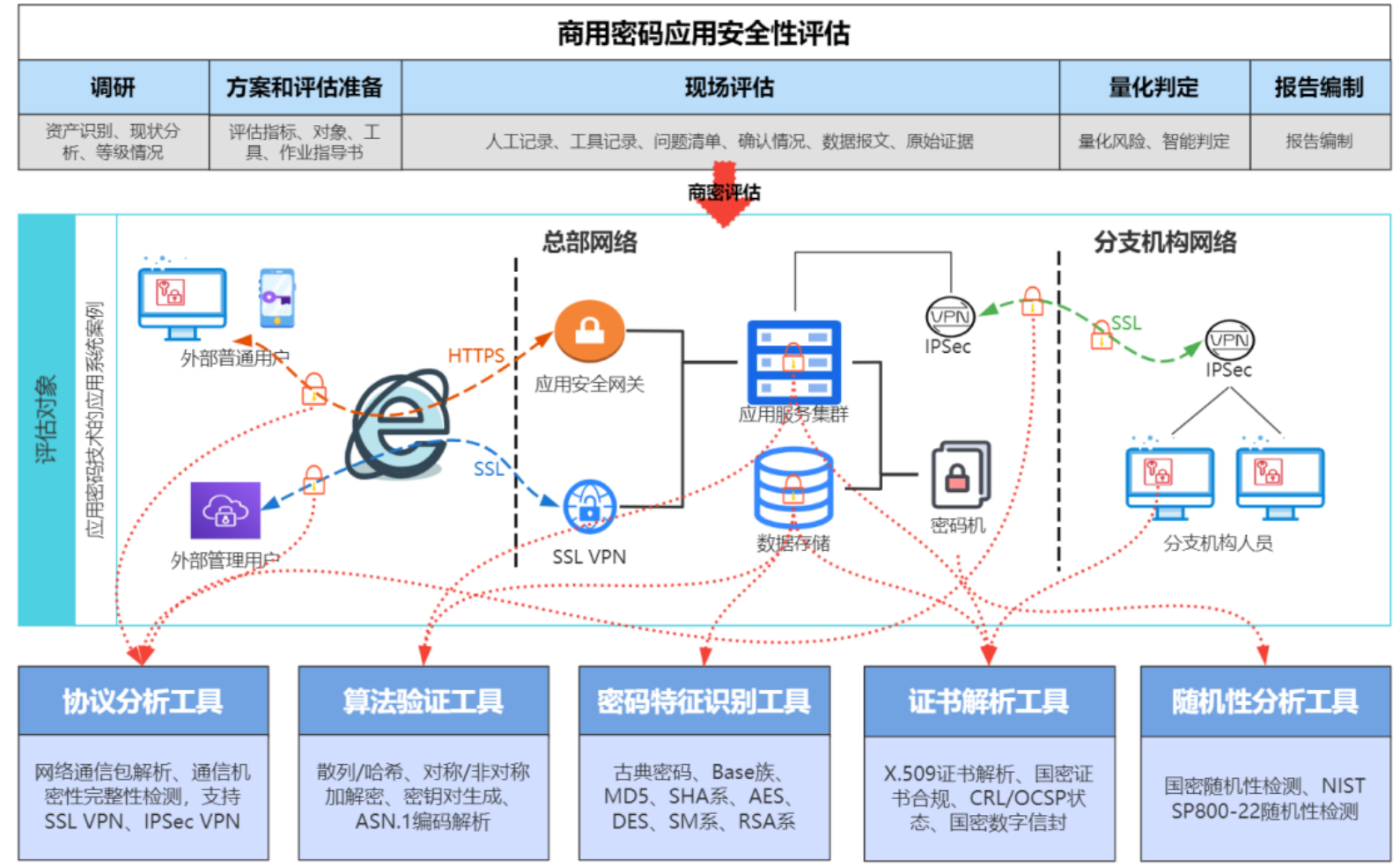



资料来源：中科三方官网、国信证券经济研究所整理

# 密评包含整个网络架构中各类密码技术

- **密评即“密码应用安全性评估”**，是指在采用密码技术、产品和服务集成建设的网络和信息系统中，对其密码应用的合规性、正确性和有效性进行评估。密评主要是为了检查信息系统中密码应用存在的问题，同时明确相关主体的责任。
- **密评要求系统多种密码技术应用**。密评并非仅仅针对系统中密码产品的评测，而是覆盖系统所有需要用到密码的地方。根据案例，在内外网、分支机构等各场景中，网络需要不同的密码技术来保证安全，如网络通信支持SSL\IPSec、应用服务支持各类算法验证、存储支持各类密码算法、加密机支持各类证书和随机性分析等。

**密评案例和相关技术点**




资料来源：北方实验招股书、国信证券经济研究所整理

# 密评多对个技术点和管理有明确要求，带动相关产品部署

国信证券 GUOSEN SECURITIES

- **密评覆盖多个技术点**。密评中技术要求包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全；共占70分。安全管理包括包括制度、人员、实施和应用四个维度，共占30分。同时，密钥管理也是其中一项，包括密钥生成、分发等。
- **密评要求相应产品部署**。根据不同的系统要求级别，其覆盖了国密门禁、VPN、密码机、USBkey、电子签章、证书等多项密码产品。

**三级系统建设套餐**

| 测评值 | 测评单位 | 权重 | 分值 | 备注 | 约束 | 部署产品 |
|---|---|---|---|---|---|---|
| 物理和环境安全（10分） | 身份鉴别 | 1 | 4.1667 | 高风险 | 宜 | 国密门禁 |
| | 电子门禁记录数据存储完整性 | 0.7 | 2.9167 | | 宜 | |
| | 视频记录数据存储完整性 | 0.7 | 2.9167 | | 宜 | 与服务器密码机对接或部署国密视频监控 |
| 网络和通信安全（15分） | 身份鉴别 | 1 | 3.9474 | 高风险 | 应 | SSL VPN或IPSec VPN |
| | 通信数据完整性 | 0.7 | 2.7632 | | 宜 | SSL VPN或IPSec VPN |
| | 通信过程中重要数据的机密性 | 1 | 3.9474 | 高风险 | 应 | |
| | 网络边界访问控制信息的完整性 | 0.7 | 2.7632 | | 宜 | SSL VPN或IPSec VPN |
| | 安全接入认证 | 0.4 | 1.5789 | | 可 | SSL VPN或IPSec vPN |
| 设备和计算安全（15分） | 身份鉴别 | 1 | 3.125 | 高风险 | 应 | 国密USBkey，双因素登录 |
| | 远程管理通道安全 | 1 | 3.125 | 高风险 | 应 | SSL VPN或IPSec VPN |
| | 系统资源访问控制信息标记完整性 | 0.7 | 2.1875 | | 宜 | 数字签名系统开发对接（需要开发） |
| | 重要信息资源安全标记完整性 | 0.7 | 2.1875 | | 宜 | 不适用(不得分) |
| | 日志记录完整性 | 0.7 | 2.1875 | | 宜 | 日志审计与服务器密码机对接开发 |
| | 重要可执行程序完整性、重要可执行程序来源真实性 | 0.7 | 2.1875 | | 宜 | USBKey或签名系统（需要开发） |
| 应用和数据安全（30分） | 身份鉴别 | 1 | 4.0541 | | 宜 | USBkey 、手机盾，或签名验签 |
| | 访问控制信息完整性 | 0.7 | 2.8378 | | 宜 | 服务器与服务器密码机或签名验签系统对接开发 |
| | 重要信息资源安全标记完整性 | 0.7 | 2.8378 | | 宜 | 不适用(不得分) |
| | 重要数据传输机密性 | 1 | 4.0541 | 高风险 | 应 | 部署SSL VPN或国密浏览器+签名服务器 |
| | 重要数据存储机密性 | 1 | 4.0541 | 高风险 | 应 | 与服务器密码机对接开发，或通过数据库加密系统 |
| | 重要数据传输完整性 | 1 | 4.0541 | | 宜 | 部署SSL VPN或签名服务器 |
| | 重要数据存储机密性 | 1 | 4.0541 | 高风险 | 宜 | 与服务器密码机对接开发，或通过数据库加密系统 |
| | 不可否认性 | 1 | 4.0541 | 高风险 | 宜 | 部署电子签章系统、时间戳服务器、签名验签服务器实现 |
| 安全管理(30分) | 可以得分 | | 25 | | | 预估分数 |

资料来源：《中国密评市场分析报告》、国信证券经济研究所整理

# 从等保到密评，密码产业持续催化

国信证券 GUOSEN SECURITIES

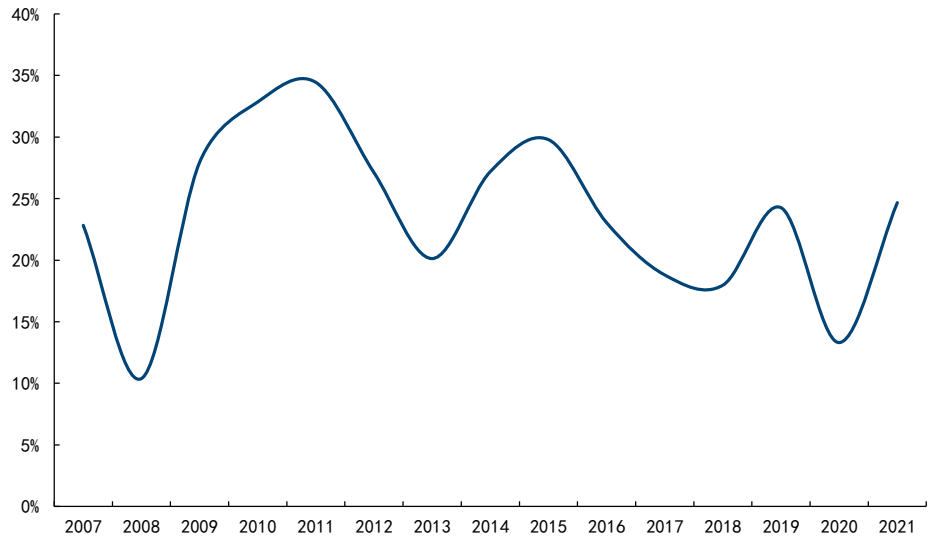
- **密评有望复制等保1.0时期的产业开拓阶段**。2007年公安部发布《信息安全等级保护管理办法》，标志等保1.0启动；行业增速从08年开始明显提升，带动启明星辰、深信服等一批网络安全厂商逐步成长。2019年随着三个网络安全标准发布，网络安全进入等保2.0时代，等保2.0加大了对新兴IT系统的覆盖。当前关保和密评处于加速推动期，而密码应用渗透率低，当前发展阶段更类似于等保1.0时期，将推动密码产业加速拓展。
- **多项法律规定了不做密评的处罚**。《密码法》要求未使用商密，或开展密评的，则责令改正，给予警告；拒不改正或导致危害安全后果的，处10-100万以下罚款，直接主管处1-10万罚款。《国家政务信息化项目建设管理办法》规定不符合密评要求或者存在安全隐患的政务信息系统，不安排运维经费，且单位不得新建、改建、扩建政务信息系统。各类信息系统通过密评已经成为刚需。

**等保、关保和密评的区别**

| 类别 | 等保 | 关保 | 密评 |
|---|---|---|---|
| 部门 | 公安网监部门 | 公安网监部门 | 密码管理局 |
| 保护对象 | 非涉密的涉及国计民生的重要信息系统和通信基础信息系统 | 关键基础信息设施:如电信广播电视、能源、金融、交通运输、水利应急管理、卫生健康、社会保障、国防科技等行业 | 关键基础信息设施、网络安全保护第三级以上的系统、国家政务信息系统 |
| 测评内容 | 安全物理环境<br>安全通信网络<br>安全区域边界<br>安全计算环境<br>安全管理中心<br>安全管理制度<br>安全管理机构<br>安全管理人员<br>安全建设管理<br>安全运维管理 | 合规检查<br>安全技术检测<br>分析评估 | 总体要求<br>密码功能要求<br>密码技术应用要求<br>密钥管理<br>安全管理 |

资料来源：道普信息、国信证券经济研究所整理

**等保1.0推动网络安全公司开启高增长**

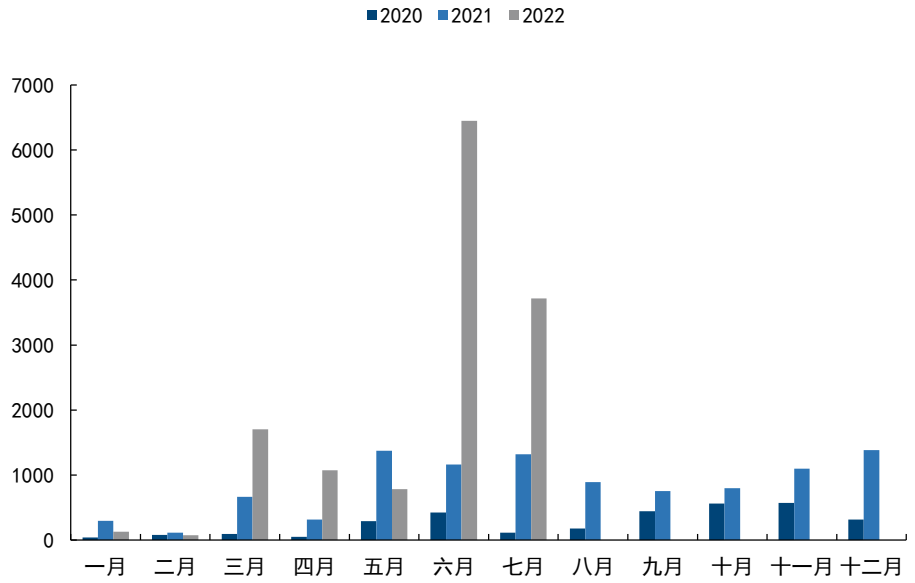



资料来源：Wind、国信证券经济研究所整理

# 密评市场快速发展，行业应用有望加速

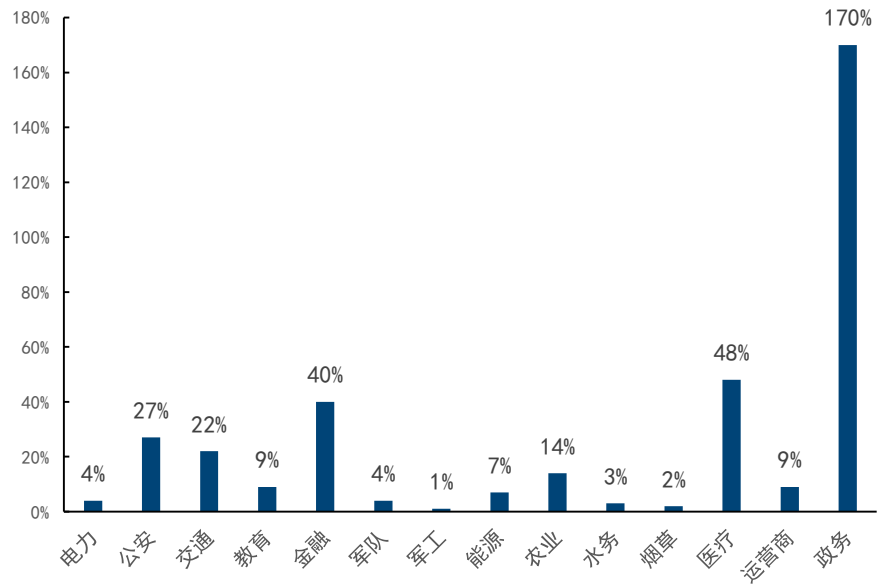
- **密评市场保持快速发展**。第三方密评机构是密评市场主要参与者，其主要提供商密评估服务并收取服务费。随着政策落地进度加快，密评试点完成后逐步开始规模化，我国密评市场呈现快速增长趋势。根据《中国密评市场分析报告》，2020年密评市场仅为3154万元，2021年市场突破1个亿，2022年前7个月市场交易额约1.39亿元，全年有望突破2亿元。
- **密评有望在更多行业加速推广**。根据数据显示，在2020-2022年整体密评市场中，政府、金融、医疗三大行业承载了当前主要的密评项目，且大部分甲方将密评、等保、咨询等合并到同一项目中。目前其他大多数行业密评开展仍然较少，未来有望加速推广。

## 密评市场近三年交易额




资料来源：《中国密评市场分析报告》、国信证券经济研究所整理

## 密评项目行业分布

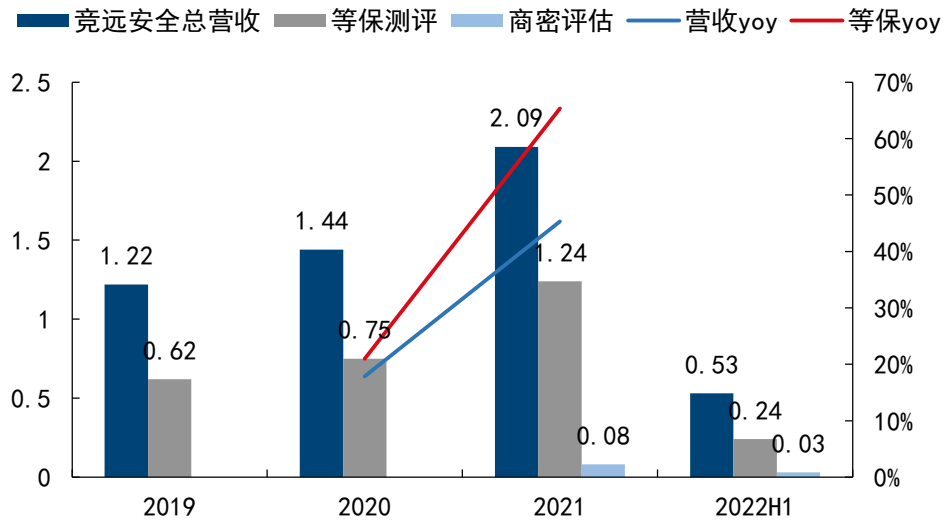



资料来源：《中国密评市场分析报告》、国信证券经济研究所整理

# 测评机构初长成，密评仍是起步阶段

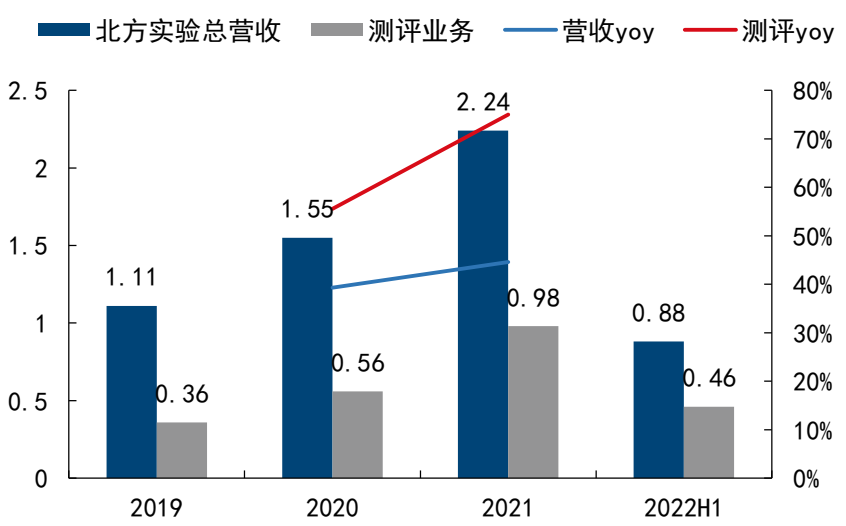
- **测评机构数量逐步增长**。相比于公安部发展多年的等保测评，其测评机构有230家；密码局体系下的密评近年来加大推广后，密评机构也达到了48家，主要分布在北京、广州、杭州等地。截止2022年9月，同时具备等保测评和密评资质的企业仅33家。
- **测评业务近年来持续高增长，密评业务仍是刚起步**。随着2019年等保2.0再次推动信息安全测评和建设，测评机构收入呈现高增长，有些厂商已初具规模，如北方实验、竞远安全等。北方实验2021年收入2.24亿元（+44.58%），归母净利润0.78亿元（+46.23%）；其中测评业务包括等保和密评，2021年收入0.98亿元（+75%）。竞远安全2021年收入2.09亿元（+45.30%），归母净利润0.51亿元（+66.06%）；其中等保测评业务收入1.24亿元（+65.33%），而密评业务2021年刚刚起步，收入仅0.08亿元。当前密评加速开展下，收入有望加速。

**竞远安全总营收和测评业务收入（亿元）**




资料来源：竞远安全招股书、国信证券经济研究所整理

**北方实验总营收和测评业务收入（亿元）**




资料来源：北方实验招股书、国信证券经济研究所整理

# 密评催化下，密码建设市场广阔

国信证券 GUOSEN SECURITIES

- **密评服务单价较低，密码建设带动相关产品放量**。根据中国政府采购网部分数据统计，密评类项目主要以测评服务为主，平均项目金额约84万，相对较低；但有些项目会包含多个系统，一些大体量项目也会包括一些改造和产品方案等。例如四川省财政信息中心密评项目，共计15个等保三级系统，总价85万。密码改造和建设类项目体量较大，平均约291万。这类项目更多是密评驱动下，甲方单位必须进行相关的密码应用建设，不仅仅是国密改造，还有大量新建。例如兰州市教育局信息系统密改项目，则采购数字证书、密码机、国密浏览器等产品。

- **密码市场将催生约500-600亿空间**。保守估计，当前我国等保3级及以上信息系统约5-6万个，且密评系统数量超过等保三级。参考密评及相关产品的项目费用，假设一条系统密码相关投资100万元，则整体市场也达到500-600亿元。密评催化下，市场有望加速释放。

**密评类项目招投标情况**

| 项目名称（密码应用安全性评估） | 中标单位 | 单价(万元) |
|---|---|---|
| 江西省智慧交通数据中心平台密码应用安全检测与评估服务采购项目 | 交通运输信息安全中心有限公司 | 29.85 |
| 山东省司法厅系统密码测评服务项目 | 山东省信息技术产业发展研究院 | 106 |
| 四川省财政信息中心密码测评服务项目 | 成都创信华通信息技术有限公司 | 85 |
| 国家税务总局青岛市税务局应用系统商用密码应用安全性评估服务项目 | 道普信息技术有限公司 | 47.5 |
| 吉林省应急管理厅(本级)政务信息系统密码应用与安全性评估项目 | 长春市博鸿科技服务有限责任公司 | 72.8 |
| 北京市人力资源和社会保障局本级行政信息系统安全等级保护及密码应用评测服务 | 北方实验室（沈阳）股份有限公司 | 198 |
| 山东省医保局购买商用密码应用安全性评估工作服务项目 | 道普信息技术有限公司 | 90 |
| 福建省农村经营管理综合信息应用平台密码应用安全改造服务及评估服务项目 | 云上密码（福建）信息技术有限公司 | 44.5 |

资料来源：中国政府采购网、国信证券经济研究所整理

**密码改造和建设类项目招投标情况**

| 项目名称（密码应用改造和建设） | 中标单位 | 单价(万元) |
|---|---|---|
| 山东省人力资源社会保障密码应用安全管理系统项目 | 同智伟业软件股份有限公司 | 135.99 |
| 国家铁路局密码应用安全性评估问题整改服务项目 | 太极计算机股份有限公司 | 151.2 |
| 国家矿山安全监察局湖南局非煤矿山远程监察系统信息安全系统密码应用建设 | 中电信数智科技有限公司 | 158 |
| 中国工业互联网研究院工业和信息化行业密码应用产业链供需对接子平台 | 三未信安科技股份有限公司 | 297 |
| 新疆维吾尔自治区人社厅信息系统密码应用改造项目 | 新疆卓信永鸿信息技术有限公司 | 489.6 |
| 国家税务总局2022年密码服务组件升级完善与运行维护项目 | 博雅中科（北京）信息技术有限公司 | 752.45 |
| 山东省危险货物道路运输安全监管系统国产商用密码应用改造项目 | 辽宁新途网络科技有限公司 | 189 |
| 兰州市电化教育中心兰州市教育局信息系统密码应用改造 | 中安云科科技发展（山东）有限公司 | 189.9 |

资料来源：中国政府采购网、国信证券经济研究所整理

# 目录

# 国密算法日益成熟，替代国际算法势在必行

国信证券 GUOSEN SECURITIES

- **我国自主研发密码算法已获得国际认可**。上世纪90年代后期，商密市场逐步开启，我国也在加大对密码技术的自研和应用。2006年，国密局公布了SM4分组密码算法，是我国第一次公布自主设计的商密算法。随后，我国全面自研并推出了对称加密、非对称加密、杂凑等算法了，形成了SM1、SM2、SM9、ZUC等一些列国密算法，且SM2、ZUC等算法顺利成为ISO/IEC国际标准。目前SM1和SM7算法并未公开，需要通过芯片接口调用；其他算法均已公开。国密算法相对于国际算法具备一定的优势，已能满足各类场景的需求。

- **国密改造对存量项目进行替代**。密码算法已经成为国家战略资源，根据《商用密码管理条例》要求，任何单位不得使用自研或者境外生产的密码产品。2010年开始，国密机构已经开始推动性能更好的SM2算法对RSA算法的替代，存量项目的国密改造、新项目国密建设势在必行。

**国密算法特点及应用**

| 算法名 | 算法种类 | 发布时间 | 特点 | 应用领域 |
|---|---|---|---|---|
| SM1 | 对称加密——分组加密算法 | 不公开 | 算法安全保密强度跟 AES 相当，仅以IP核的形式存在于芯片中，需要通过加密芯片的接口进行调用 | 芯片、智能IC卡、加密机 |
| SM2 | 非对称加密算法 | 2010年12月 | 包含数字签名、密钥交换和公钥加密，安全强度比RSA 2048位高，且运算速度快于RSA，用于替换RSA/DH/ECDSA/ECDH等国际算法 | 电子认证服务系统 |
| SM3 | 密码杂凑算法 | 2010年12月 | 在SHA-256基础上改进，用于替代MD5/SHA-1/SHA-2等国际算法，且安全性更高 | 数字签名和验证、随机数生成等 |
| SM4 | 对称加密——分组加密算法 | 2012年3月 | 与AES算法具有相同的密钥长度、分组长度，用于替代DES/AES等国际算法 | 用于无限局域网产品，数据的加密/解密运算等 |
| SM7 | 对称加密——分组加密算法 | 不公开 | 需要通过加密芯片的接口进行调用 | 非接触式IC卡，如身份识别类、票务类、支付和一卡通类应用 |
| SM9 | 非对称密码算法 | 2016年3月 | 基于双线性对的标识密码算法，将用户的标识（如邮件地址、手机号码、QQ号码等）作为公钥，可以替代基于数字证书的PKI/CA体系 | 主要用于用户的身份认证适用于互联网应用的各种新兴应用 |
| ZUC | 对称加密——流加密算法 | 2012年3月 | 祖冲之序列密码算法，是中国第一个成为国际密码标准的密码算法 | 用于移动通信4G网络中的国际标准密码算法 |

资料来源：CSDN、密码头条、国信证券经济研究所整理

**国密算法和国际算法对应关系**

| 密码分类 | | 国产商用密码 | 国际商用密码 |
|---|---|---|---|
| 对称加密 | 分组加密 | SM1/SCB2、SM4/SMS4、SM7 | DES、IDEA、AES、RC5、RC6 |
| | 流加密 | ZUC、SSF46 | RC4 |
| 非对称加密 | 离散对数 | SM2、SM9 | DH、DSA、ECC、ECDH |
| 密码杂凑 | | SM3 | MD5、SHA-1、SHA-2 |

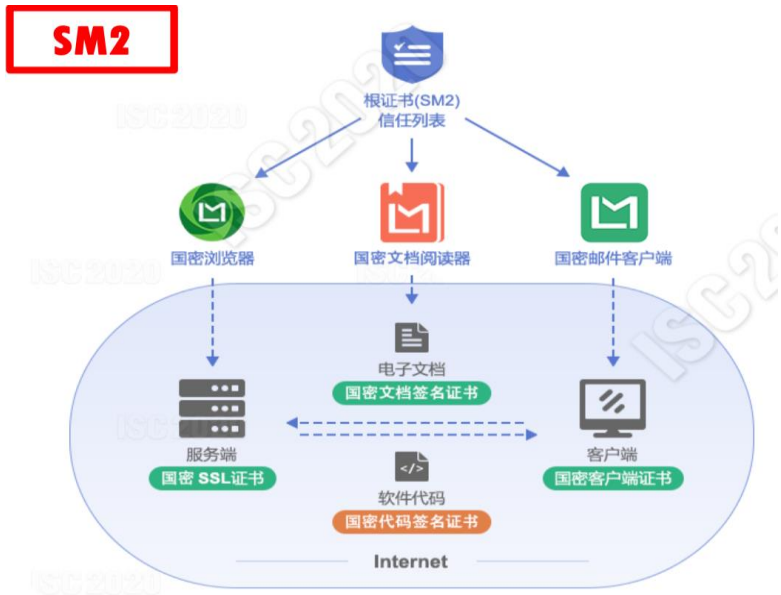
资料来源：CSDN、国信证券经济研究所整理

# 信创推动国密应用VPN、PKI体系改造

- **密码是信创产业的基础支撑**。任何网络信息系统建设都离不开底层密码应用，如链路层的MACSec加密、网络层IPSec加密、传输层SSL/TLS加密、应用层中身份认证、电子签名等。随着信创推广，密码从芯片、板卡、整机均需要支持国密体系，并完成替换和改造。

- **以VPN、PKI为代表的密码应用同样需要改造**。当前规范要求下，如VPN需要加装硬件密码卡。在应用广泛的数字证书体系中，国密PKI/CA系统已完成建设，国密SM2根证书已创建并投入使用，实现对RSA架构下PKI体系的替代。国密SM2根证书下支持签发国密SSL证书、国密代码签名证书、国密客户端证书，可覆盖信创体系下各类国密证书应用，如信创网站SSL证书、信创OS的签名证书、信创应用的文档加密、身份认证等。目前国密SM2根证书已经与国内多家CA机构达成合作，已在全国十几个省市的政务网站广泛应用。

## 国密应用体系建设




资料来源：沃通CA、国信证券经济研究所整理

## 国密证书核心产品

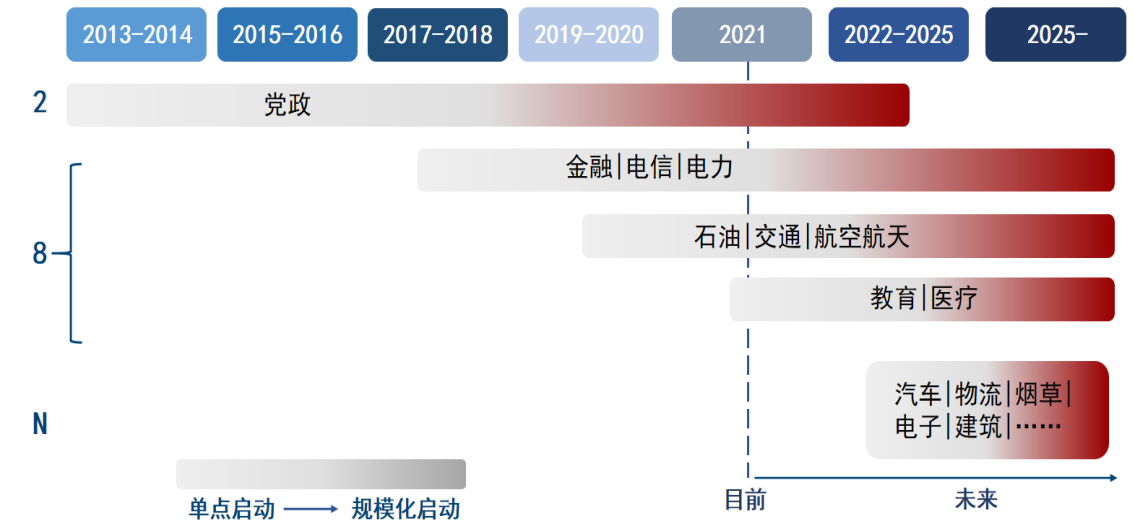

资料来源：沃通CA、国信证券经济研究所整理

# 行业信创加速发展，推动国密应用快速渗透

- **信创市场进入行业推进期，容量和节奏将进一步提升**。截止2022年，信创产业在党政领域已经初见规模，应用和生态逐步落地；行业信创加速是市场发展必然方向，且空间更为广阔。八大重点行业中，金融行业推进速度最快，电信紧随其后，之后是能源、交通、航空航天、教育、医疗也在逐步进行政策推进和试点。根据海比研究院测算，2022年信创产业规模达到9220.2亿元，预计2025年突破2万亿，近5年复合增速达到35.7%。其中2022年由IT基础设施和基础软件构成的核心市场达到2392.8亿元，占比约26%。

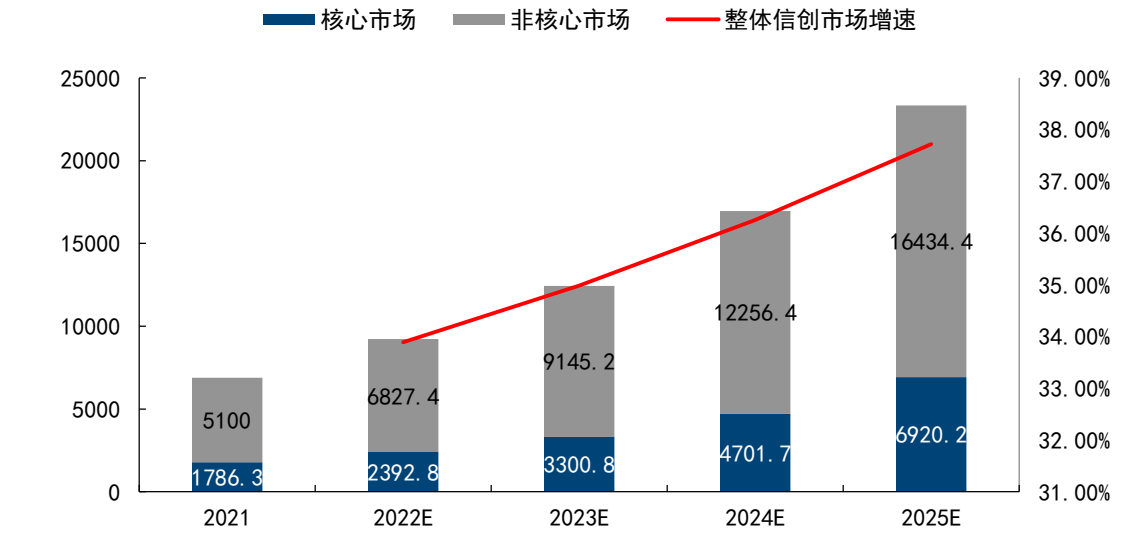
- **密码是信创建设中不可或缺的重要一环**。国密生态的全面替代已在多个行业信创建设中铺开，如金融、电力、医疗等个行业的国密改造。在2019年底国务院发布的《国家政务信息化项目建设管理办法》中，明确了密码和项目建设的“三同步一评估”原则。在未来党政、行业信创的快速推进中，各类系统从无到有的密码建设、以及已有建设但需要的国密改造，密码发展有望在信创产业基础上进一步加速。

## 信创产业推进节奏




资料来源：亿欧智库、国信证券经济研究所整理

## 我国信创市场保持快速增长




资料来源：《2022中国信创生态市场研究及选型评估报告》、国信证券经济研究所整理

# 电力行业——商密是新型电力系统的安全支撑

国信证券 GUOSEN SECURITIES

- **新型电力系统是发展趋势，叠加信创是安全建设重点**。随着新能源建设成为我国核心战略之一，我国电力系统将呈现“双高”特性：高比例新能源、高比例电力电子设备接入。新型电力系统建设中，“源网荷储”生态将催生大量新技术、系统的应用。而电力也是8大信创重点行业之一，如南网已经在推动全栈自主可控工作。十四五期间，两网规划共投入近3万亿元，以信创为基石，面向新型电力系统的信息化建设是重要方向。

- **商密支撑新型电力系统安全体系**。新型电力系统下，如营销业务的互联网化、业务系统与外界的交互、新IT技术的引入、智能终端的普及会带来更多的信息安全问题。商密从密码算法、芯片级、设备级和系统级支撑电力基础设施安全，保障能源安全。国家电网已建成了覆盖26个省/自治区/直辖市的密码基础设施，通过统一密码服务平台对人资合同、电E宝、营销2.0等各种业务应用提供密码服务。

## 商密对能源安全的支撑


资料来源：中国电力科学研究院、国信证券经济研究所整理

## 商密支撑新型电力系统体系框架


资料来源：中国电力科学研究院、国信证券经济研究所整理

# 电力行业——电力安全投入提升，密码终端市场广阔

- **电力安全投入持续提升，密码已是刚性要求**。2022年12月，国家能源局印发《电力行业网络安全管理办法》，要求网络安全投入不低于信息化总投入的5%；规划设计网络时，需要保证安全措施同步规划、同步建设、同步使用，上线前需要第三方测试；按照规定进行等保、关保、商用密码评估等测评。结合电力信创的加快推进，安全和密码建设是电力系统必备一环。

- **密码电力应用广泛，物联网终端是广阔新市场**。当前电力系统密码应用典型模型有6大类：流程类、移动终端类、采集控制类、传感设备类、边界隔离类、大数据类；根据不同的场景，提供身份认证、数据加密、数字签名、电子签章、密码模块等不同组合能力。截止2022年2月，密码服务平台已接入国网约120套重要业务系统，包括电力采集、交易等，提供服务约7.3亿次。新型电力系统背景下，电表、充电桩等海量物联网终端成为新的密码市场；仅智能电表全国已安装5.3亿支，直接经济效益1000亿元，将带动密码芯片等上下游的应用。

**商用密码在电力系统中的应用场景**


资料来源：中国电力科学研究院、国信证券经济研究所整理

# 金融行业——商密应用推进较早

- **金融领域国密应用推进领先**。2014年《金融领域密码应用指导意见》要求各金融机构5年内完成在网上银行、移动支付、网上证券等重点领域国密的应用。2018年《金融和重要领域密码应用与创新发展工作规划（2018-2022年）》进一步要求金融、政务等重点行业国密应用。2020年，人行在此基础上颁发《金融领域信息系统国产密码改造基线要求》和《金融领域国产密码改造评价指标体系》，细化金融业国密改造要求。随着《密码法》、信创、密评等产业指引落地，国密改造在各金融机构核心系统中有望持续深化。

- **商密在银行和证券业已经开展广泛应用**。根据中国人民银行国密应用要求，银行需在网银系统对安全工具、安全基础设施进行国产密码算法的应用改造，包括国密证书、USBKey、动态令牌等。对于证券行业，其早期一直沿用国际通用密码算法体系及相关标准，交易系统国密改造的内容主要集中在身份认证、安全传输、数据签名，交易接入网关作为应用系统的入口，是国密改造的重点和切入点。

## 人行对国密应用要求

需要使用包含国密数字证书和国密算法的USBKey。

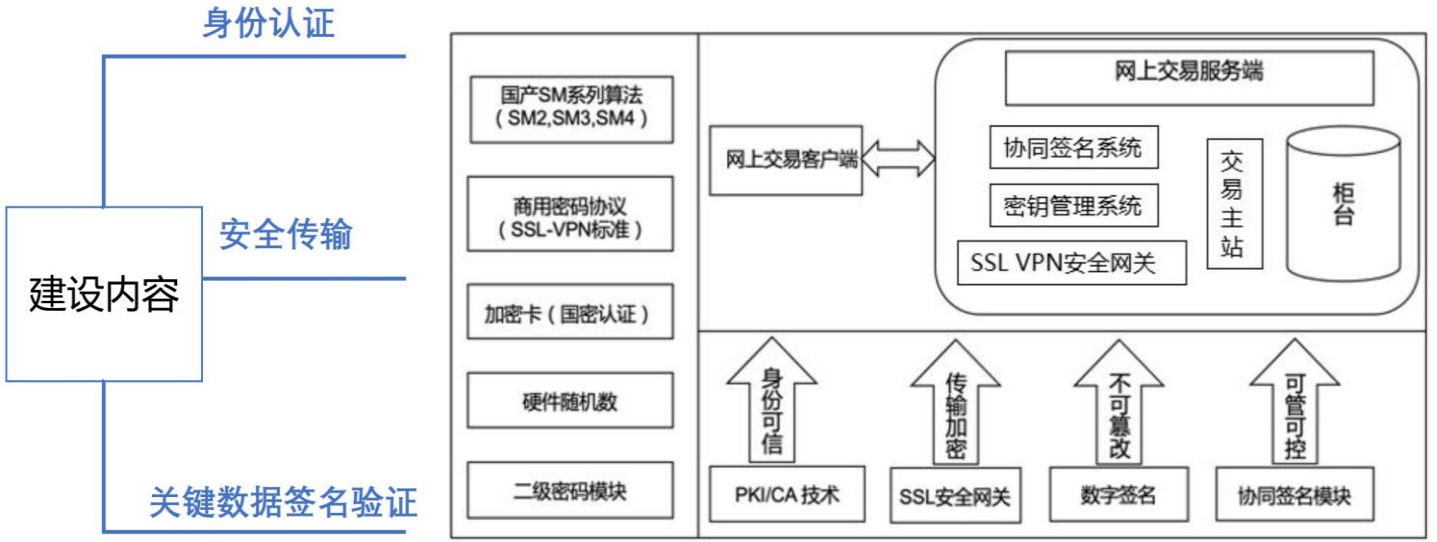
需使用基于国密算法的动态令牌。

需使用通过使用国密专用浏览器建立国密SSL隧道连接到网银系统。

需使用基于国密算法对交易等数据进行电子签名。

资料来源：金融界、国信证券经济研究所整理

## 国密在证券业应用案例



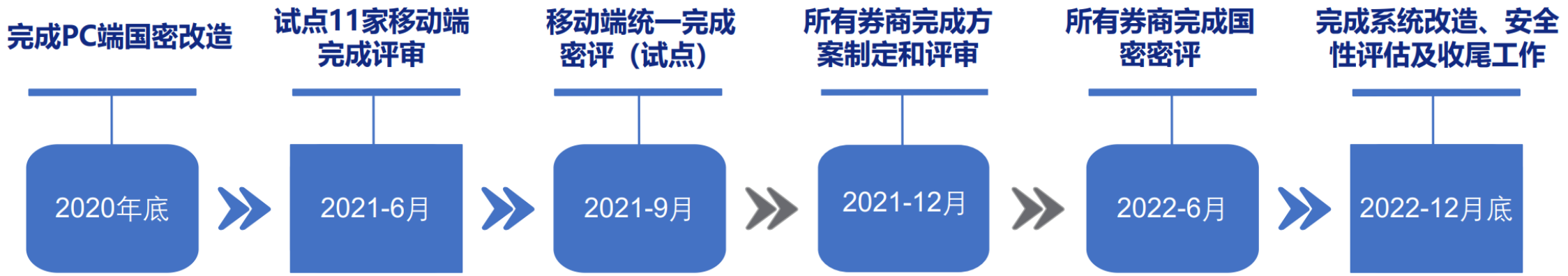

资料来源：恒生电子、国信证券经济研究所整理

# 金融行业——安全投入要求提升，信创和密码是重点

- **证券业安全投入加大，信创和国密进入核心系统改造**。2023年1月，中证协向券商下发了《网络和信息安全三年提升计划(2023-2025)》，鼓励有条件的券商未来三年信息科技平均投入金额不少于平均净利润的8%或平均营业收入的6%，其中网络和信息安全投入不低于信息科技投入的7%；同时对信息科技员工人数、网络安全员工人数均做出要求。信创将是下一阶段金融业安全建设的重点，伴随信创进入深水区，国密应用也将从PC端逐步渗透到核心系统。根据相关要求，2022年12月底券商要完成系统改造、安全性评估测试及收尾工作。

- **行业应用厂商同样受益国密改造**。国密应用会带来券商业务系统改造，金融IT厂商也将承担国密改造业务。例如恒生电子联合安恒信息，融合IT系统建设和国密算法，为机构客户提供一站式国密解决方案，陆续在证券、基金等金融机构试点运行。财富趋势于2016年就启动国密研发，在其行业交易体系产品种，形成了具备认证条件的独立密码产品；组织了近70家券商参与商密评估工作，且全部通过测评。

**证券期货基金行业国密应用最新进展**

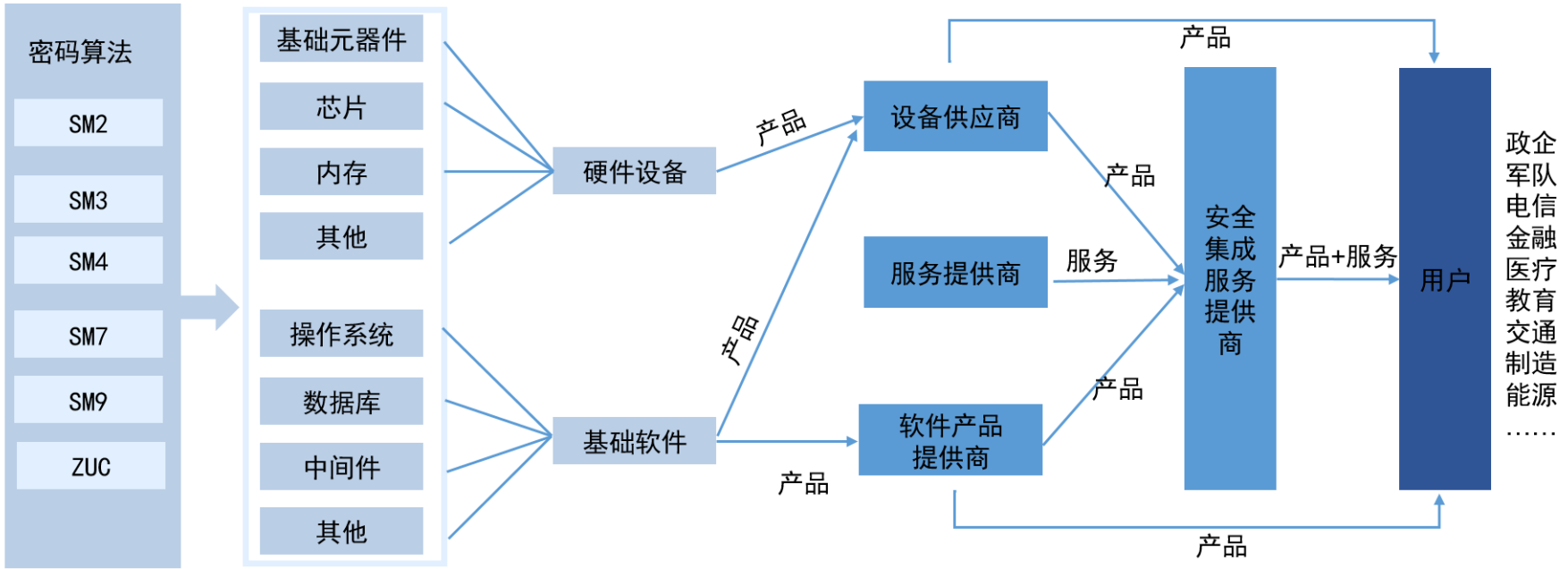



资料来源：恒生电子、国信证券经济研究所整理

# 国密驱动下全IT产业升级改造

- **国密算法成为全IT产业的底层支撑，充分受益信创发展**。国密算法是核心，也是产业链最上游，其包含公开和非公开算法，会嵌入在各种软硬件产品中。中游主要为整机及终端领域；下游主要是软件、系统集成及应用领域；最终客户包含政府、金融、能源、医疗等各个行业。随着密码应用渗透率提升，产品商、软件商、服务商、集成商均会受益。在当前IT国产化背景下，国密应用从芯片、操作系统、PC和服务器、网络通信、应用软件等多个领域均要进行升级改造，是信创不可或缺的环节。尤其是关键信息基础设施行业持续加大安全投入，未来整个IT产业中国密应用渗透将大幅提升，拉动国密产业需求快速增长。

**密码是IT产业的基础支撑**




资料来源：《商用密码行业发展机遇报告（2022年）》、国信证券经济研究所整理

# 目录

# 密码全产业链受益各政策推动

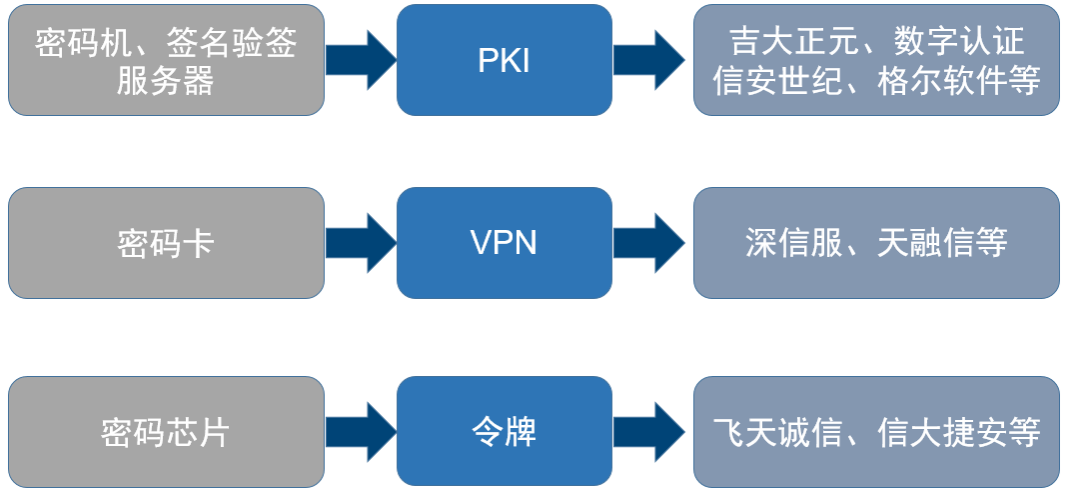
- **上中下游密码厂商均受益于当前密评、信创等产业发展。**根据商用密码行业分析报告的产业链划分，其将密码卡和密码机产品也划分为中游；但从密码产品和厂商角度来，也能把密码芯片、密码卡、密码机作为行业上游。中游密码应用最主要的是PKI和数字证书、VPN及各类网关、令牌等产品，离不开上游密码基础产品应用。例如PKI方案中的签名验签服务器也是密码机的一种；VPN网关需要装载PCI-E密码卡；令牌USBKey中需要内置密码芯片。密码管理平台是新兴的系统级产品，覆盖基础密码、密码应用和管理。

- **集成和服务也具有较高毛利率，密评机构扮演产业助推器角色。**一般中游密码应用类厂商直销占比高，在和客户深度绑定下，也会提供集成和咨询等服务；目前密码类厂商集成业务毛利率约为20-30%之间，高于网络安全类集成业务。密评机构在产业链中扮演重要角色，其测评业务的开展将推动甲方客户的密码建设，带动产业链上下游共同发展。

**密码产业链上游核心产品**


资料来源：三未信安招股说明书、国信证券经济研究所整理

**密码中游厂商和对上游产品的应用**




资料来源：《密码学》、国信证券经济研究所整理

# 商用密码产业链

国信证券 GUOSEN SECURITIES


资料来源：2021-2022商用密码行业分析报告、国信证券经济研究所整理

# 密码上游：提供基础密码能力，头部厂商陆续上市

- **上游产品提供基础密码能力**。密码芯片、密码卡、密码机均提供类似的功能，例如密钥生成、数字签名、签名验证、数据加解密等，区别主要是应用在不同的场景。该市场即硬件安全模块Hardware security module（HSM），是下游密码应用的组成部分。

- **欧洲厂商占据全球市场，国内密码上游厂商陆续上市**。再综合考虑了社会、政治、经济和目前市场动态等多种因素后，Market Research Intellect对HSM市场进行评审，选出了2020年前九大硬件密码模块公司，国内厂商电科网安、江南天安、三未信安上榜。头部密码硬件公司以欧洲厂商为主，且并购较多，业务拓展和覆盖领域更多。根据Global Info Research数据，2021年全球HSM市场收入约11.21亿美金，预计2028年达到21.90亿美金，复合增速10.9%；其中Thales、Utimaco等欧洲厂商占据主要份额。国内厂商电科网安体量最大，是密码和网安全产业链公司，其12.3亿收入包含非密码的网安部分。纯密码上游厂商三未信安于2022年上市，渔翁信息也提交招股说明书。

**全球密码硬件安全市场排名（2020年）**

| 全球排名 | 公司名称 | 核心业务 | 收入 |
|---|---|---|---|
| 1 | Gemalto金雅拓 | 智能卡，包括SIM卡、加密卡；数字身份安全；已被THALES收购 | 31亿欧元（2016年） |
| 2 | Yubico | 安全秘钥，USBKey，生物识别等 | |
| 3 | Atos SE | 综合IT服务，网络安全，云计算 | |
| 4 | THALES泰雷兹 | 军工、航空航天业务，19年收购Gemalto；同时出售了通用硬件安全模块(GP HSM)业务，该业务主要是PKI和SSL产品 | 数字安全业务收入30亿欧元（2021） |
| 5 | Ultra Electronics | 国防、军工、安全电子设备和机电系统 | |
| 6 | 电科网安 | 密码芯片、密码卡、密码机、VPN、网关、集成和服务 | 整体27.8亿元（2021） |
| 7 | 江南天安 | 密码卡、密码机、云密码、秘密系统 | |
| 8 | Ultimaco | 硬件安全模块，身份安全，数据安全 | |
| 9 | 三未信安 | 密码芯片、密码卡、密码机等 | 2.7亿元（2021） |
| 未排名 | 渔翁信息 | 密码卡、密码机等 | 1.07亿元（2021） |

资料来源：三未信安招股说明书、公司官网、国信证券经济研究所整理

**国内厂商相关数据比较**

| 公司 | 2021年收入（密码相关） | 商密产品认证数量 | 安全等级三级密码产品数量 | 参与密码行业标准数量 |
|---|---|---|---|---|
| 电科网安 | 12.3亿元（安全芯片+安全整机口径） | 38 | 0 | 51 |
| 江南天安 | | 33 | 1 | 8 |
| 三未信安 | 2.7亿元 | 44 | 2 | 18 |
| 渔翁信息 | 1.07亿元 | 23 | 0 | 1 |

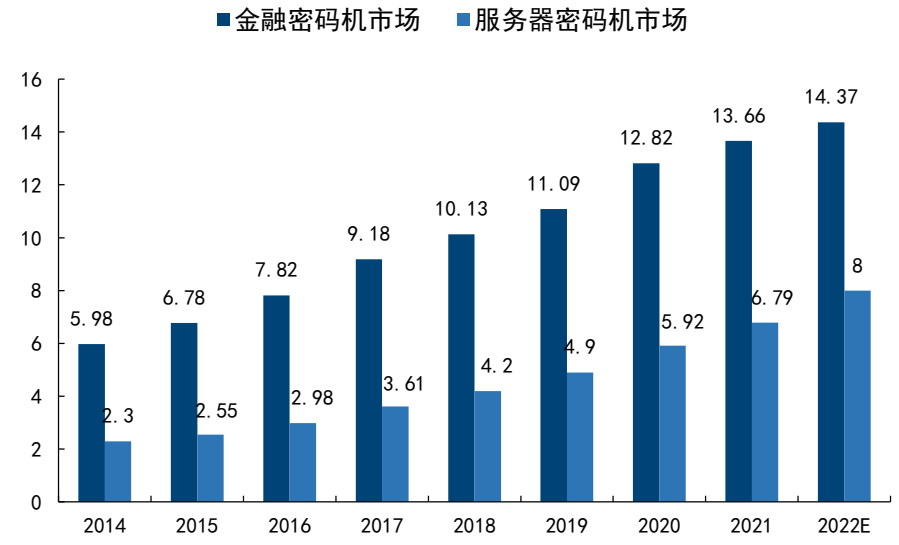
资料来源：三未信安招股说明书、国信证券经济研究所整理

# 密码上游：密码机市场稳定增长，但体量依然较小

国信证券 GUOSEN SECURITIES

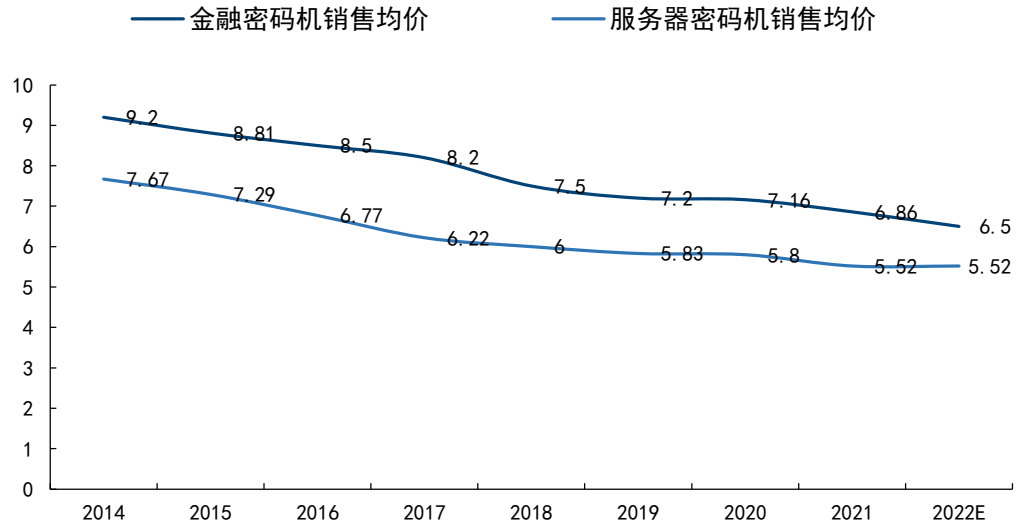
- **密码机市场当前仍较小**。密码机包括服务器密码机、金融密码机、签名验签服务器（主要用于PKI方案中）。根据共研网数据统计，2021年服务器密码机市场约6.79亿元，2022年预计达到8亿元，其中市场需求预计达到1.45万台。2021年金融数据密码机市场约13.66亿元，2022年预计达到14.37亿元，其中市场预期预计在2.2万台。
- **价格逐步企稳，量有望加速释放**。参考密码上游头部公司收入规模，以及密码机市场、叠加密码卡市场，我们预计上游市场约30亿左右。作为电子设备类产品，密码机整体销售均价处于下降阶段，当前价格已逐步企稳。随着密评、国密改造的推动，密码上游产品最为受益，需求将进一步释放，市场进入价稳量升的环节。

**中国服务器、金融密码机市场（亿元）**




资料来源：共研网、国信证券经济研究所整理

**中国服务器、金融密码机销售均价（万元）**




资料来源：共研网、国信证券经济研究所整理

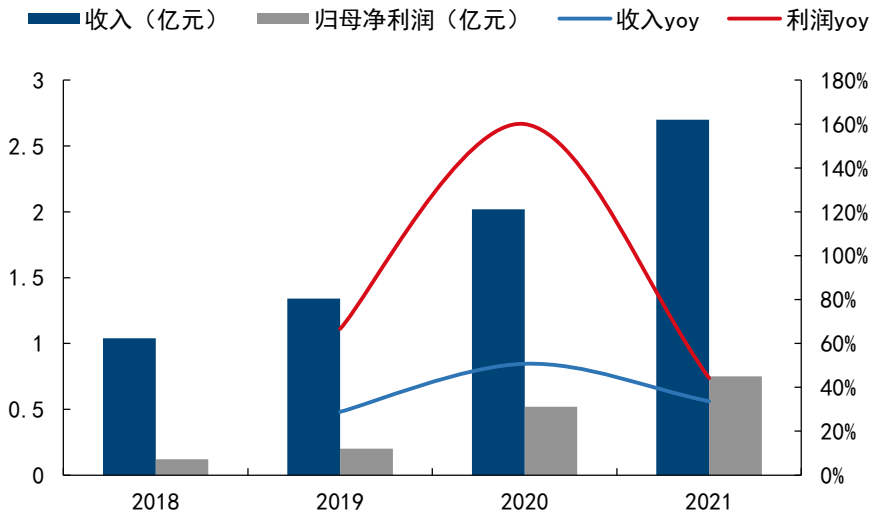
# 三未信安：上游密码产业领先者，芯片布局加强差异化竞争

国信证券 GUOSEN SECURITIES

- **公司是密码上游产品领先者，业绩保持快速增长**。公司成立于2008年，推出了国内首款安全三级密码板卡和首款安全三级密码整机。公司形成了密码芯片、板卡、整机、系统的上游产品结构；其中密码板卡资质数量在行业中排名第一，在国内有较高市场份额。公司作为上游，以合作厂商销售为主，收入占比达到87%。公司近年业绩保持快速增长，2022年疫情影响下，依然保持稳定增长。

- **密码芯片推出恰逢其时，差异化竞争有望打开新市场**。公司自15年开始布局芯片研究，于22年9月完成第一批密码芯片XS100的量产，正在全面推向市场。与国内领先者苏州国芯的密码芯片对比，双方算法性能各有优势，公司密码芯片已处于行业领先水平。密码芯片首先应用于公司自身的密码板卡和整机，以提升产品性价比；随着信创、密评在各行业的推动，公司密码芯片在物联网、国资云等市场有望打开新空间。

## 三未信安历年收入和利润水平




资料来源：Wind、国信证券经济研究所整理

## 三未信安芯片XS100

| 产品分类 | 产品图片 | 产品特点 |
|---|---|---|
| XS100 |  | ●采用 RISC-V 处理器，最高工作频率 400Mhz<br>●国内领先的高性能密码算法引擎，主流国密算法性能达到先进水平<br>●支持 SM1、SM2、SM3、SM4、SM7、SM9 国密算法<br>●支持 AES、DES、3DES、RSA1024、RSA2048、RSA4096 等国际算法<br>●真随机数发生器，符合 GM/T 0005-2012 及 NIST SP800-22 标准<br>●SR-IOV 硬件虚拟化功能，单芯片最大支持 64 个虚拟机<br>●安全可靠的密钥管理功能<br>●丰富的通信接口：UART、I2C、SPI、QSPI、SMC、GPIO 等 |

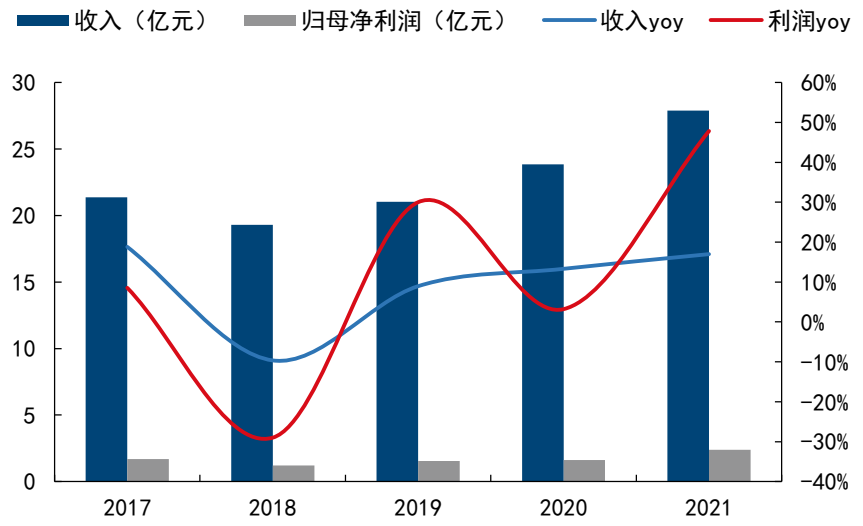
资料来源：三未信安招股说明书、国信证券经济研究所整理

# 电科网安：密码全产业链覆盖，数据安全逐步落地

- **公司是密码网安“国家队”，密码全产业链覆盖**。公司成立于1998年，是中国电科旗下中国网安控股子公司，以密码技术起家，深耕于党政、军队、大型央企等客户。公司是密码全产业链覆盖，产品包括密码芯片、板卡、整机、系统；PKI相关产品、VPN等网关应用；集成和服务。公司还横跨网络安全、数据安全等业务，近年来收入和利润保持稳定增长，22前三季度在疫情影响下仍有较好表现。

- **数据安全项目落地，数据要素密码应用有望发力**。公司21年与世纪华通签署战略合作协议，在游戏和超算领域展开合作。22年公司与盛趣游戏联合打造的国内首个互联网个人信息安全合规试点项目，以多方治理模型为总体架构，以可信第三方服务平台和安全模块为支撑，为企业提供数据合规服务，满足监管要求，且平台采用SaaS部署模式。数据要素化背景下，密码和数据安全应用将在各行业持续推进。

**电科网安历年收入和利润水平**




资料来源：Wind、国信证券经济研究所整理

**电科网安和盛趣游戏个人信息安全合规试点项目**

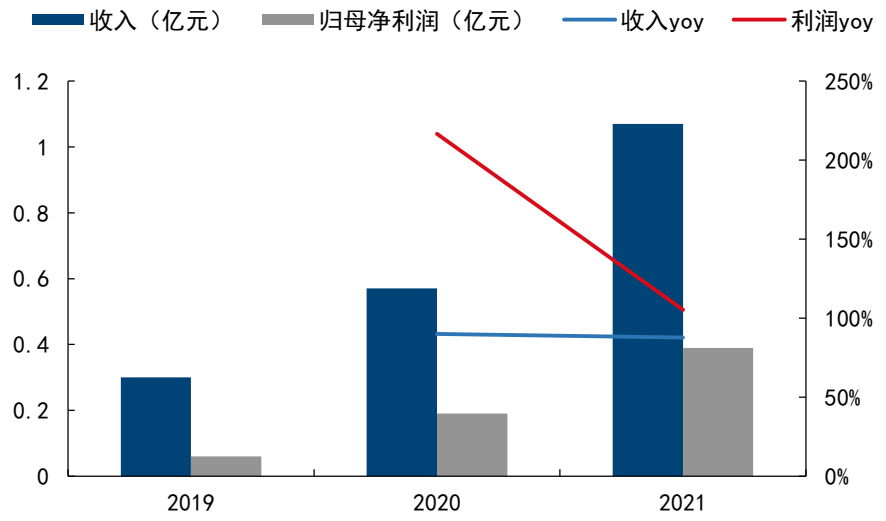

资料来源：电科网安、国信证券经济研究所整理

# 渔翁信息：当前处于快速成长期

- **公司是密码上游厂商，正处于快速成长期**。公司成立于1998年，在2006年推出国内首款“高性能PCI-E密码卡”，将国产密码卡性能带入“千兆时代”。公司以信创为牵引，密码技术为支撑，向产业链下游拓展，形成了“基础密码+云数据安全+工控安全”三大密码产品和服务体系。公司产品形态以密码卡、密码机为主，同时布局工控安全领域。受益于当前密码行业多轮政策推动，公司收入保持快速增长，21年收入达到1.07亿元，同比增长约87%，利润水平也大幅提升，进一步验证当前行业处于高景气中。

- **公司在信创密码产业处于领先地位**。公司是国家“信创工委会”密码应用组组长单位，是国家商用密码产品信创战略的重要推动者。公司2018年布局信创产品，多款产品入围政府采购目录；2019年在某部政务云信创应用试点项目中负责项目密码技术体系搭建。

## 渔翁信息历年收入和利润水平




资料来源：Wind、国信证券经济研究所整理

## 渔翁信息产品布局

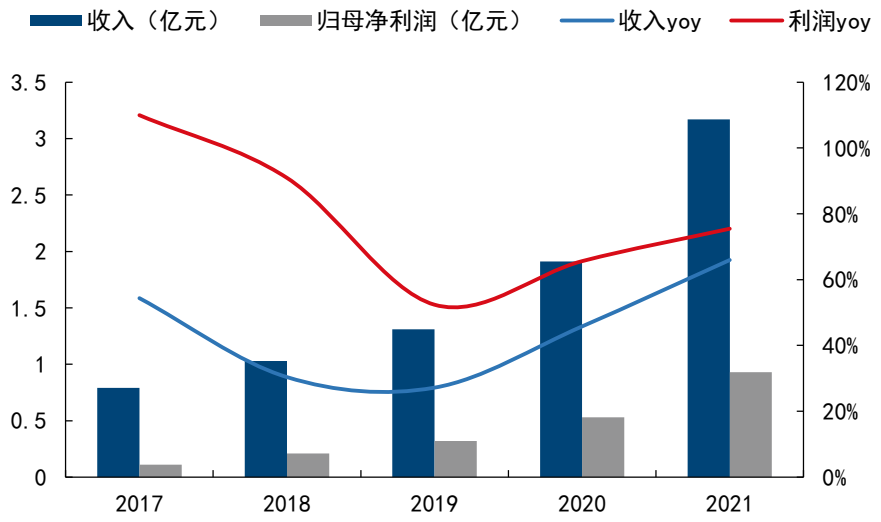

资料来源：渔翁信息招股说明书、国信证券经济研究所整理

# 佳缘科技：军工领域加密应用，与商密市场高增长共振

- **公司是军工领域加密安全厂商，侧重无线侧加密。**公司成立于1994年，早期以信息化为主业，19年开始军工网络安全业务加快成长。与商密不同，公司主要从事军工领域加密和安全业务，以无线侧星载、机载等场景为主。公司安全产品在发出端对发出信号进行信息编码、完整性保护、防篡改设计，在接收端对接受信号进行解码和身份鉴别，实现数据传输的安全性、完整性、防重放攻击。

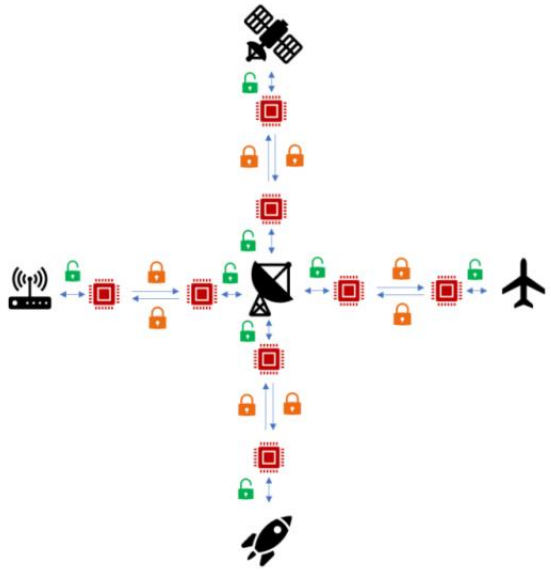
- **卫星下游高景气，23年有望重回高增长。**2022年由于疫情干扰，公司高成长节奏受到影响。随着2022年10月星网完成通信卫星招标，我国低轨通信卫星建设进入加速期，公司有望受益星网建设发展。同时，公司发布了股权激励，给予了较高的收入增长目标，2023年业绩有望重回高增长。《密码法》对商密、普密均提出明确要求，民用密码和军用密码市场有望共振，均迎来快速发展期。

**佳缘科技历年收入和利润水平**




资料来源：Wind、国信证券经济研究所整理

**佳缘安全产品简要原理和场景**

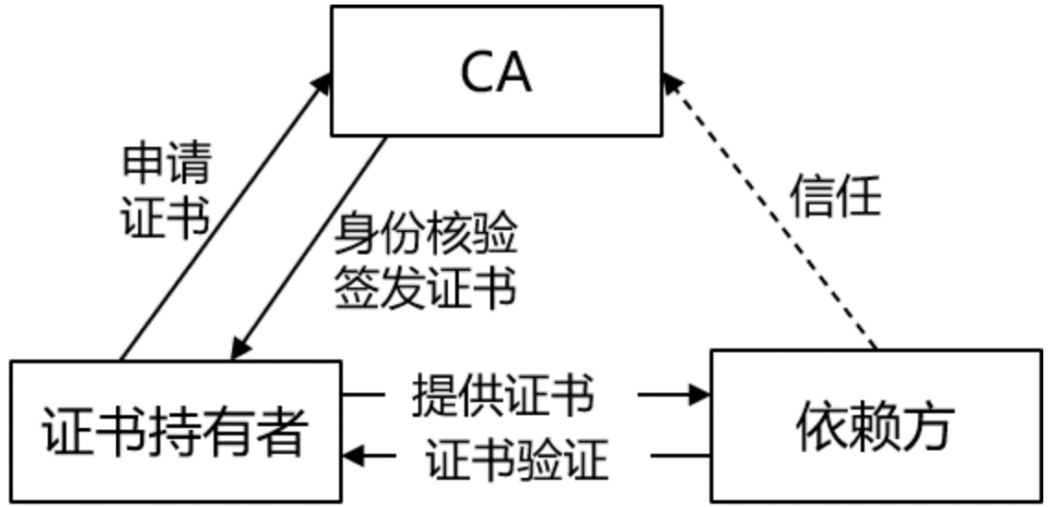


资料来源：佳缘科技招股说明书、国信证券经济研究所整理

# 密码应用：PKI是密码最主要应用之一

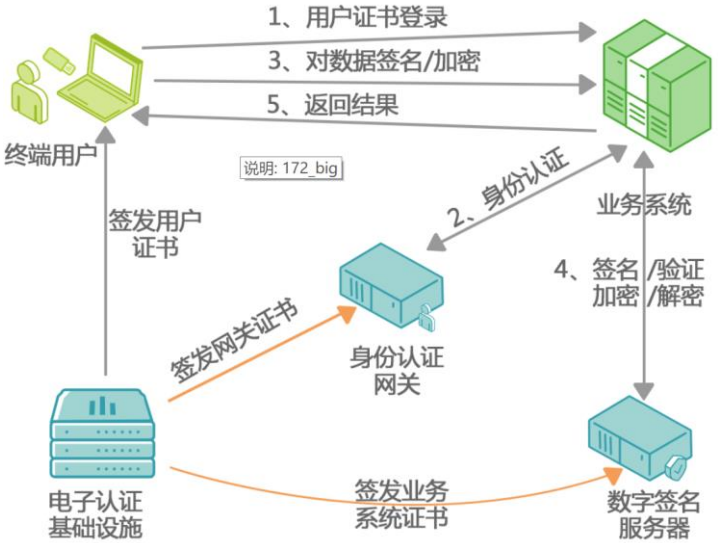
- **数字证书是PKI体系核心，CA是重要角色。**PKI是公钥基础设施，基于非对称密码算法原理，以数字证书为核心的安全认证体系。PKI系统主要有五部分组成：认证机构（CA）、数字证书库、秘钥备份及恢复系统、证书作废系统、应用接口。从逻辑上，PKI可分成三方，CA是独立可信第三方，主要是签发证书，工信部许可了55家CA机构；证书持有者和依赖方则依据证书进行可信交互，且均需要CA的验证。
- **PKI基础设施涵盖多种产品，是密码最广泛应用之一。**PKI基础设施产品主要包括电子证书认证系统、移动终端制证系统、目录服务器、智能密码钥匙和服务器密码机等；其运行逻辑也是基于证书的认证。PKI能够实现密钥和证书的产生、管理、存储、分发和撤销等功能，为应用提供认证、加密、数字签名等安全支撑。PKI目前主要应用在网上银行、电子政务等领域，物联网、车联网是未来广泛市场空间。

**PKI系统组成结构**




资料来源：中国电信研究院、国信证券经济研究所整理

**PKI基础设施产品和业务逻辑**




资料来源：吉大正元招股说明书、国信证券经济研究所整理

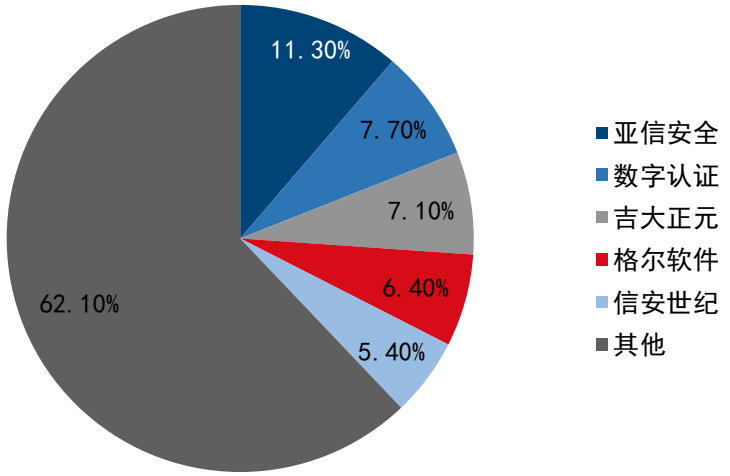
# 密码应用：PKI头部厂商均已上市，集成业务毛利率较高

- **上市公司位居行业前列**。根据IDC中国IT安全软件市场跟踪报告，身份和数字信任软件市场保持稳定增长，2021年预期身份和数字信任市场约38.3亿元；其中五家上市公司占据领先市场份额。IDC对该领域的定义包括了身份管理/单点登录、数字证书、身份治理等多个细分；其中亚信安全在该领域的核心业务是统一身份认证（IAM），数字认证、吉大正元、格尔软件、信安世纪核心业务是PKI领域。
- **密码应用厂商多数有集成业务，且毛利率较高**。以PKI为代表的密码应用类厂商由于和客户直接服务，在帮助客户完成PKI解决方案中，也会提供大量集成业务，其中吉大正元、格尔软件、数字认证均有该业务。相比于网络安全厂商集成业务约10%以下的毛利率，密码应用厂商集成业务20%-30%的毛利率保持较高水平。密码应用厂商整体收入规模大于纯上游厂商。

**中国身份和数字信任软件市场（亿元）**

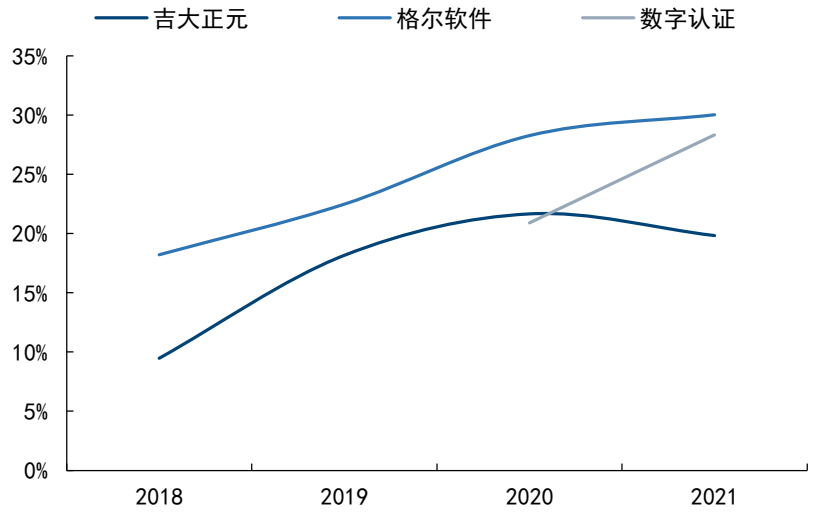

资料来源：IDC、国信证券经济研究所整理

**中国身份和数字信任市场份额（2021）**




资料来源：IDC、国信证券经济研究所整理

**PKI厂商集成业务毛利率水平**



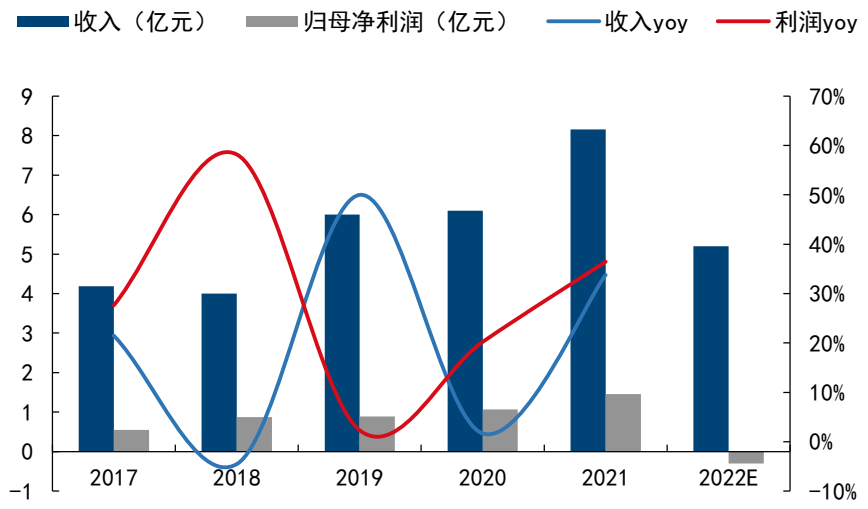

资料来源：Wind、国信证券经济研究所整理

# 吉大正元：军工下游有望高增长，八大策略开启新发展

国信证券 GUOSEN SECURITIES

- **公司是综合密码应用厂商，军工业务高增长**。公司成立于1999年，最早以帮助CA机构建设PKI电子证书系统起家，在财政部、人民银行等政府、金融、军工领域占据优势。目前公司已经形成了PKI、身份安全、数据安全、物联网安全等综合产品体系。2022年疫情对公司在吉林、北京、上海三大区域经营产生较大负面影响，公司预计22年收入约4.9-5.4亿元，归母净利润亏损0.31-0.36亿元，下降较大。21年公司军工下游收入占比约22%，22年军工业务保持较快增长，占比有望进一步提升。23年政府市场恢复及军工高增长下，公司有望实现业绩反弹。
- **八大策略助力公司进入发展新阶段**。公司发布2023-2025战略发展规划，提出以密码为核心，强化PKI品牌，全力打造新一代数字安全体系—“元安全”。公司加大生态、渠道的布局，向关基、中小企业和个人终端行业倾斜；在密评和信创推动下，公司业务有望稳步快速增长。

## 吉大正元历年收入和利润水平




资料来源：Wind、国信证券经济研究所整理

## 吉大正元八大业务策略

| | |
|---|---|
| 打造芯片级密码能力，布局抗量子密码体系 | 一、打造软硬一体嵌入式密码产品，密码板卡、物联网芯片等；二、围绕数据流通的数据安全，隐私计算；三、布局抗量子密码 |
| 构建新一代数字安全体系“元安全”，塑造新型安全能力 | 推出以密码为基础的新一代数字安全体系——“元安全”，由数字安全防护设施、数字安全智能操作系统、数字经济安全运行环境组成。 |
| 形成四大产品系列，扩展服务，提供应用整合方案 | 面向党政军客户的“昆仑”系列，面向央企、国企的“长江”系列，面向中小企业的“黄河”系列，面向个人的“大狼狗”系列。 |
| 构建生态平台“昆仑森林”，共同促进产业良性发展 | 围绕数字经济、数字政府和数字社会、企业数字化转型、数据安全及隐私保护、云大物移智技术五个方面，加大生态战略投入。 |
| 业务重心转向关键基础设施、中小企业和个人终端 | 基础设施行业以军队军工、公检法、财政金融等为主。与运营商、大型应用开发商、头部平台企业合作拓展中小企业和个人终端市场。 |
| 优化“行业主营、区域主战”能力，提升体系竞争力 | 不断优化公司的营销架构，提升协同作战能力，提高客户满意度 |
| 承接“南移”战略，深耕本地构建区域化特色业务 | 配合公司区域南移战略，重点打造“4+14”城市体系。立足本地特点，构建区域化特色业务。 |
| 加快渠道化转型，形成渠道地图，实现行业区域全覆盖 | 推行全员渠道营销，制定渠道分层分类拓展方案，形成渠道地图，实现在行业、区域的精准全覆盖。 |

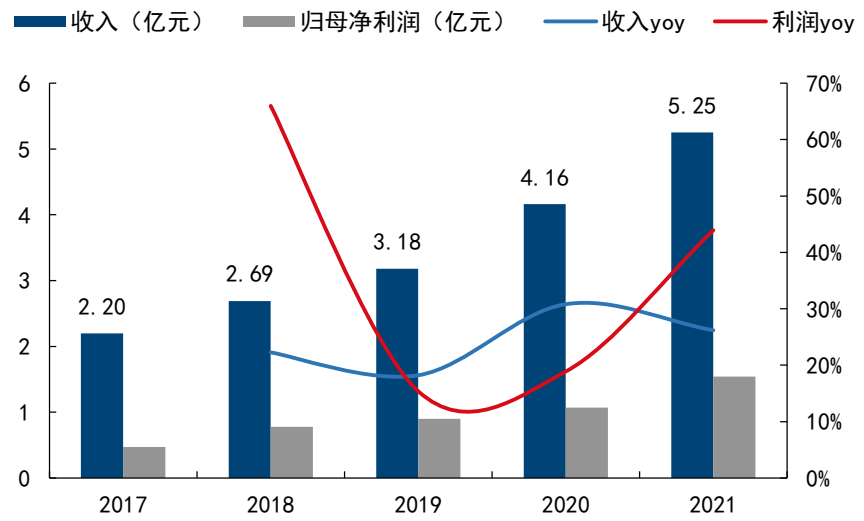
资料来源：吉大正元公告、国信证券经济研究所整理

# 信安世纪：PKI和应用交付双驱动，布局军工拓展新领域

- **公司拥有PKI和应用交付双核心业务，业绩保持稳定增长**。公司成立于2001年，以密码技术为支撑，形成了通信安全（核心是应用交付）、身份安全、数据安全（这两个板块核心是PKI）等业务体系。公司整体业绩保持稳定增长，17-21年复合收入增速为24.29%，归母净利润复合增速为34.54%。2022前三季度，公司在疫情中仍保持增长。其中2022年Q2，公司在应用交付领域市场份额排名提升至第四位。

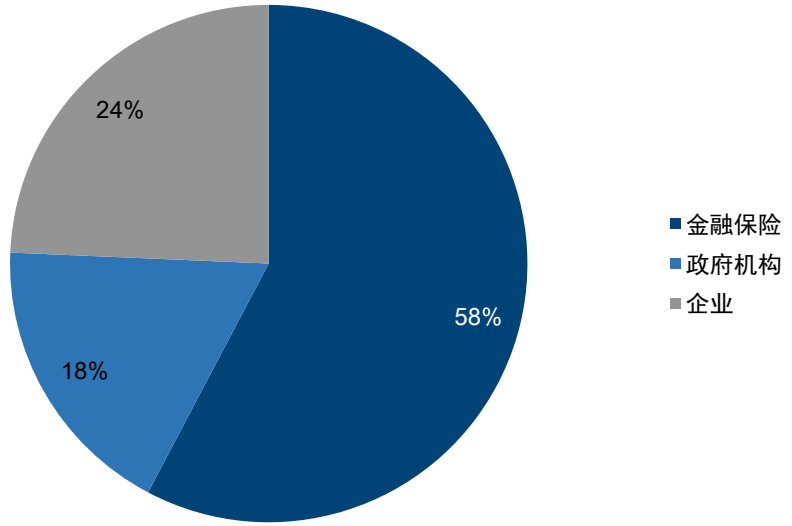
- **金融行业占比高，继续拓展军工行业**。公司早期即在银行领域深耕PKI业务，当前金融保险市场占公司收入约58%，优质的客户资源保障了公司业绩的稳定增长。2022年11月，公司发布公告，拟收购普世科技80%股权。普世科技主营在军工领域，围绕数据全生命周期，形成了跨网隔离交换、终端安全管控、数据安全归档三条产品线。收购完成后，公司有望进一步丰富产品线，加大拓展军工市场。

**信安世纪历年收入和利润水平**




资料来源：Wind、国信证券经济研究所整理

**信安世纪下游收入结构**



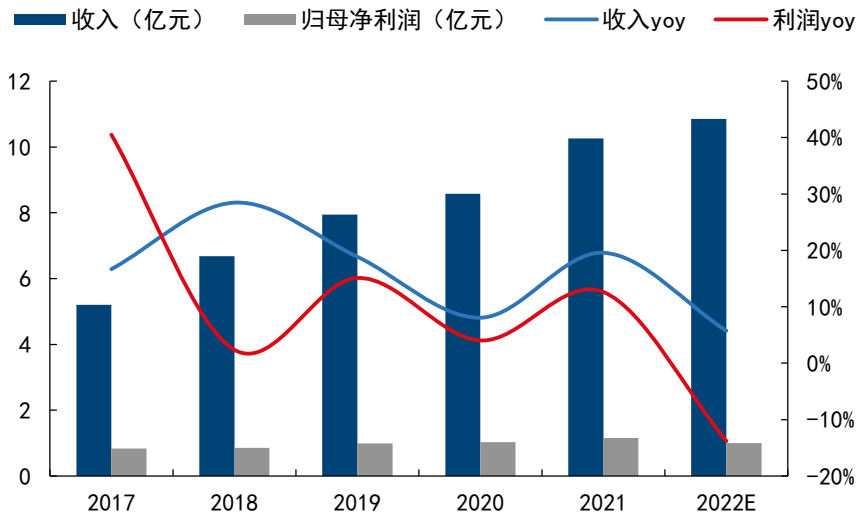

资料来源：Wind、国信证券经济研究所整理

# 数字认证：具备CA业务，保持高研发投入

- **公司以CA起家，形成PKI产品体系**。公司成立于2001年，前身为北京数字证书认证中心（北京CA）；公司加大技术投入，逐步形成了完成的PKI产品线，并进一步拓展电子签名、电子合同等新业务。CA是PKI体系中重要角色，需要一定的资质；公司是上市公司中唯一具备CA业务的密码厂商，该业务每年保持稳定收入和利润贡献。公司近10年发展整体保持稳定的增长，2022年受到疫情影响较大，公司预计2022年收入约为10.85亿元（+5.75%）；归母净利润为0.93-1.08亿元，下滑6.92%-19.85%。

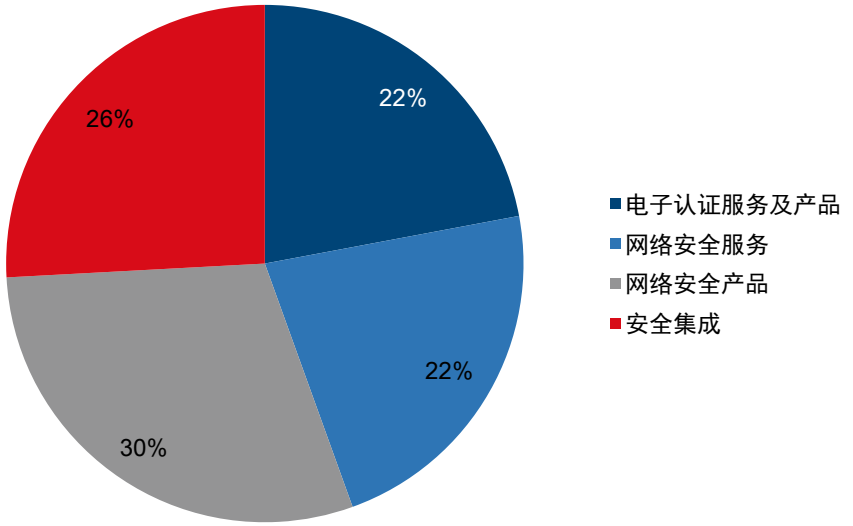
- **研发高投入，安全产品增长较快**。公司研发投入绝对金额在4家PKI厂商中保持最高，因此自研安全产品增长较快，21年收入突破3亿。叠加CA业务，公司“一体化”方案具备优势。物联网市场有望带动CA服务保持稳定增长；密评和信创推动下，公司产品、服务、集成均受益。

**数字认证历年收入和利润水平**




资料来源：Wind、国信证券经济研究所整理

**数字认证收入结构**



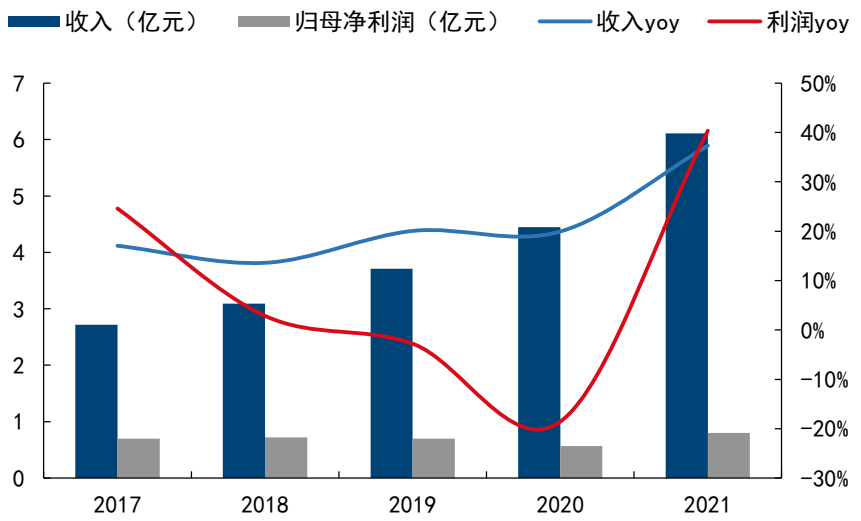

资料来源：Wind、国信证券经济研究所整理

# 格尔软件：信创集成快速发展，加大密码新领域拓展

- **公司以PKI为核心，加大市场拓展**。公司成立于1998年，是国内首批研制和推出PKI公钥基础设施产品的厂商，深耕于党政机关、军工军队、国企央企、金融等领域。2022年疫情背景下，公司PKI等业务开展受到较大影响，预计2022年归母净利润-1200至-800万，扣非归母净利润-8000至-7000万。公司22年加大了营销和市场投入，抓住国密改造的机会，在证券、保险等领域实现业务高增长。

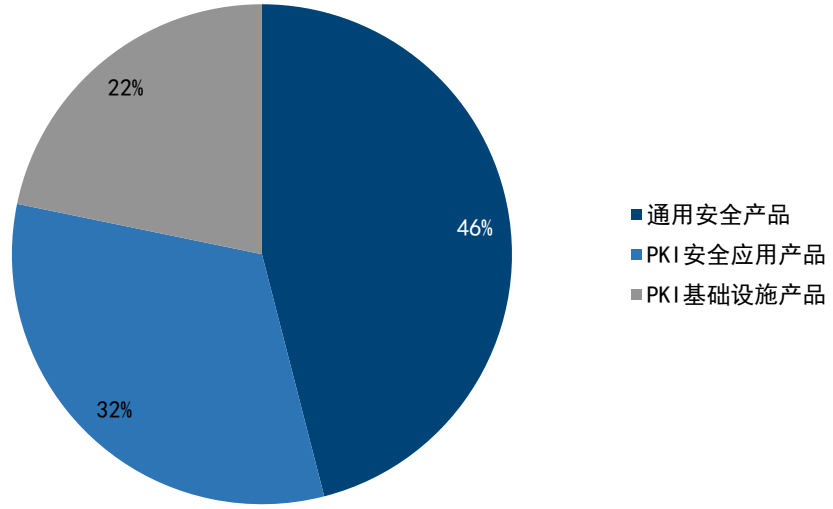
- **信创集成和密码结合发展，新领域加大布局。**公司通用安全产品主要为安全集成业务，2022年在信创推动下保持快速增长，公司毛利率有所下降。公司11条产品线100余项密码产品均符合信创建设要求，10多个产品入围国家信创目录；公司已在上海市区两级信创云实现全面覆盖，相关经验已在多地、多行业、多平台推广。公司密码应用在车联网、视频物联网等新领域已有场景落地，启动了后量子密码技术储备。

**格尔软件历年收入和利润水平**




资料来源：Wind、国信证券经济研究所整理

**格尔软件收入结构**




资料来源：Wind、国信证券经济研究所整理

# 目录

# 投资建议：看好密码行业高成长，维持“超配”评级

国信证券 GUOSEN SECURITIES

- **看好密码产业在政策推动下加速成长**。2020年《密码法》正式实施，其对核密、普密（有线、无线通信环节）、商密（密评与等保结合）均提出了明确的应用要求，密码产业进入有法可依的快速发展阶段。根据赛迪网络安全研究所测算，我国商密市场2021年达到585亿元，且增速持续向上。结合当前数字经济是发展背景，密码在各类场景的应用将无处不在。短期来看，**密评催化增量市场**，密评带动广泛等保三级信息系统，从无到有建设密码设施；**信创重塑存量市场**，存量IT系统需要国密改造，同时新建信创项目中，国密也成为标配。因此密码产业短期迎来需求释放期，行业有望加速成长。长期来看，随着数据要素市场化成为大势所趋，传统以网络为中心的安全建设，将转向以“数据为中心、结合网络边界防护”的双轴驱动，密码将嵌入在数据要素和数据安全各个环节；同时数据交易所需要的隐私计算也是密码技术的前沿方向，密码产业长期仍能保持持续成长。

- **密码上游受益密评、信创等最为显著**。密评倒逼政企等信息系统加大密码建设，以满足评分要求。密评当前覆盖范围包括等保三级及以上信息系统、关键信息基础设施等，而大部分系统在密码建设仍十分单薄。根据密评相关产品需求，在各种密码应用中，均需要密码板卡、整机等基础产品。信创和国密改造驱动下，也是底层密码算法的国密替代，也需要密码上游产品的更替。上游厂商受需求拉动最为直接，因此建议重点关注密码上游厂商，三未信安、电科网安；军工领域的佳缘科技。

- **密码应用厂商同样受益，终端客户粘性高**。密码应用以PKI厂商为代表，长期与客户服务建立了较强的客户粘性。数字证书、PKI相关产品也是密评和信创推动的应用，客户需求容易传导给密码应用厂商，且该类厂商可以一并完成相关服务和集成。当前密码集成业务依然保持着较高的毛利率水平，因此以PKI为代表的应用厂商需重点关注，如吉大正元、信安世纪、数字认证、格尔软件。另一方面，部分网络安全类厂商也同样有部分密码业务，如VPN厂商深信服、天融信等；收购密码厂商弗兰科的安恒信息，持续投资密码领域的奇安信等。

# 风险提示

- 商密评估等政策推进不及预期；
- 信创产业密码应用不及；
- 疫情等因素反复，影响宏观经济正常运行；
- 行业竞争加剧。

# 免责声明

| 国信证券投资评级 | | |
|---|---|---|
| **类别** | **级别** | **定义** |
| 股票投资评级 | 买入 | 预计6个月内，股价表现优于市场指数20%以上 |
| | 增持 | 预计6个月内，股价表现优于市场指数10%-20%之间 |
| | 中性 | 预计6个月内，股价表现介于市场指数±10%之间 |
| | 卖出 | 预计6个月内，股价表现弱于市场指数10%以上 |
| 行业投资评级 | 超配 | 预计6个月内，行业指数表现优于市场指数10%以上 |
| | 中性 | 预计6个月内，行业指数表现介于市场指数±10%之间 |
| | 低配 | 预计6个月内，行业指数表现弱于市场指数10%以上 |

**分析师承诺**

作者保证报告所采用的数据均来自合规渠道，分析逻辑基于本人的职业理解，通过合理判断并得出结论，力求客观、公正，结论不受任何第三方的授意、影响，特此声明。

**风险提示**

本报告基于已公开的资料或信息撰写，但我公司不保证该资料及信息的完整性、准确性。本报告所载的信息、资料、建议及推测仅反映我公司于本报告公开发布当日的判断，在不同时期，我公司可能撰写并发布与本报告所载资料、建议及推测不一致的报告。我公司或关联机构可能会持有本报告中所提到的公司所发行的证券头寸并进行交易，还可能为这些公司提供或争取提供投资银行业务服务。我公司不保证本报告所含信息及资料处于最新状态；我公司将随时补充、更新和修订有关信息及资料，但不保证及时公开发布。

本报告仅供参考之用，不构成出售或购买证券或其他投资标的要约或邀请。在任何情况下，本报告中的信息和意见均不构成对任何个人的投资建议。任何形式的分享证券投资收益或者分担证券投资损失的书面或口头承诺均为无效。投资者应结合自己的投资目标和财务状况自行判断是否采用本报告所载内容和信息并自行承担风险，我公司及雇员对投资者使用本报告及其内容而造成的一切后果不承担任何法律责任。

**证券投资咨询业务的说明**

本公司具备中国证监会核准的证券投资咨询业务资格。证券投资咨询业务是指取得监管部门颁发的相关资格的机构及其咨询人员为证券投资者或客户提供证券投资的相关信息、分析、预测或建议，并直接或间接收取服务费用的活动。

证券研究报告是证券投资咨询业务的一种基本形式，指证券公司、证券投资咨询机构对证券及证券相关产品的价值、市场走势或者相关影响因素进行分析，形成证券估值、投资评级等投资分析意见，制作证券研究报告，并向客户发布的行为。

国信证券
GUOSEN SECURITIES

# 国信证券经济研究所


**深圳**

深圳市福田区福华一路125号国信金融大厦36层

邮编：518046　总机：0755-82130833

**上海**

上海浦东民生路1199弄证大五道口广场1号楼12楼

邮编：200135

**北京**

北京西城区金融大街兴盛街6号国信证券9层

邮编：100032