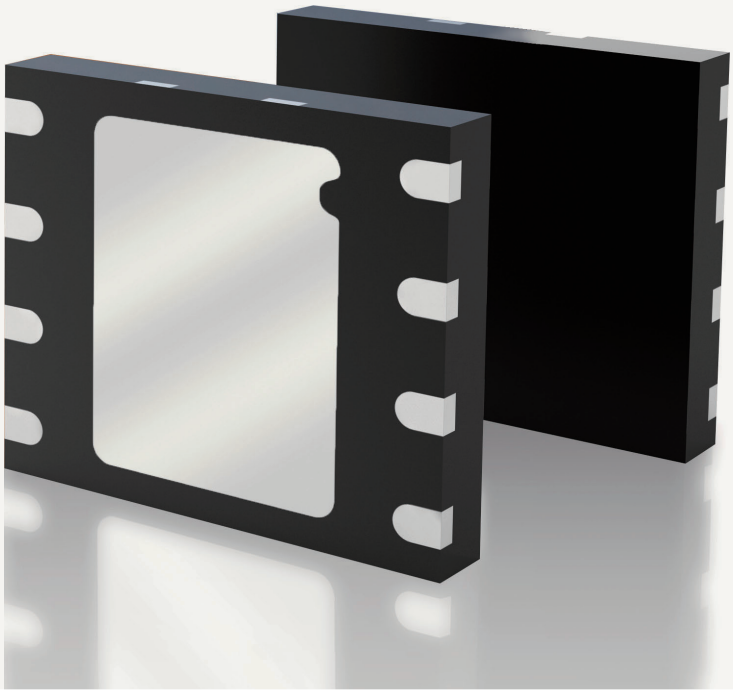
gemalto
security to be free

Cinterion® 安全芯片



建立信任的基础：

CINTERION®安全芯片

为汽车和物联网解决方案提供防篡改高级保护

Cinterion®安全芯片
为汽车和物联网解决方案提供防篡改高级保护

物联网(IoT)、智慧城市、联网汽车和智能住宅的崛起，为我们带来了一个充满无限可能的世界 – 更高的生产力、更强的安全性、时间和成本越来越省、丰富的服务种类、新商机、生活简化，充满便利。预计未来十年将会新增数十亿的联网物体，因此，设计值得信赖的解决方案变得前所未有重要起来。

金雅拓Cinterion安全芯片为物联网解决方案奠定了可信赖的基础。作为嵌入在汽车、工业连接设备和物联网解决方案中的防篡改硬件组件，Cinterion安全芯片可提供智能卡级数字安全并实现设备的生命周期管理。此外，它还能作为高级端到端安全架构中的一部分保护数据完整性、抵御数字和物理攻击。

Cinterion安全芯片经过加固处理，可在M2M和物联网应用的典型极端环境条件下确保可靠性和使用寿命，从而保证将数据存储在安全的地方，只允许得到授权的应用程序和人员访问它们。

该产品还允许您在解决方案的整个生命周期内对安全凭证、软件更新和不断演变的安全功能进行无线管理。Cinterion安全芯片可兼容任何垂直市场应用，包括联网汽车、智能电网及智慧城市解决方案等，是为整个物联网生态系统保驾护航的关键工具。

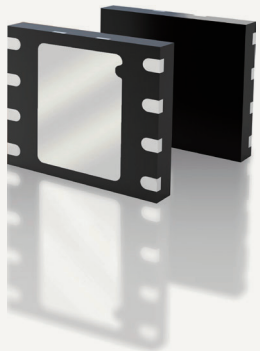
为安全而生

金雅拓能给M2M和物联网解决方案提供内在保护。我们的方法为安全而生，这套针对M2M进行优化的解决方案能够保护设备、数据、网络和云生态系统，令个人用户和企业信任我们的互联世界。金雅拓在多个垂直市场和地区拥有数十年的丰富经验，是您值得信赖的风险评估和安全架构合作伙伴，可在设备的整个生命周期中为数据提供适当级别的保护。

2015年互联安全创新奖

Cinterion®安全芯片在World Smart Week展会（法国马赛）赢得“2015年互联安全创新奖”。该奖项由世界领先的行业分析师、权威人士和预言家组成的评审团评出并在World Smart Week展会现场颁奖，在业界颇具声望。Cinterion安全芯片获此殊荣主要是因为它所提供智能连接安全特性能够推动移动、机器对机器(M2M)、物联网(IoT)和云环境创新。

建立信任的根源



> **信任的基础**
确保数据存储在安全的地方，只允许得到授权的应用程序和人员访问它们

> **前瞻性安全保证**
将智能卡级安全性与多应用程序功能相结合，实现生命周期管理和自适应安全性，确保始终提供最新的安全保护

> **防篡改**
坚固耐用可适用于极端环境；防篡改可实现高可靠性并抵御物理攻击

Cinterion®安全芯片的特性

一般特性

- 操作系统
  Javacard 3.0.1 Classic
- Global Platform 2.2
  SCP01实施5和15
  SCP02实施5、15、45和55
- 通信接口
  符合ISO/IEC 7816-3要求
  T=0，最大可达TA1=96的PPS
  频率1到5Mhz的外部时钟
- 电压和电流消耗
  支持1,62V到5,5V的电压
  可配置的电流消耗模式：2G/3G/自由模式
  支持时钟停止模式(电流消耗低于<100µA)
- NVM
  用户NVM可配置，范围在80KB到480KB之间

安全特性

- 加密算法特性
  DES、3DES(ECB, CBC)、最大可达256位的AES
  最大可达2048位的RSA密钥
  224到384位的椭圆曲线支持
  SHA-1、SHA-256和SHA-384位
  依据ISO 9796-2或PKCS#1 v2.1 (PSS-OAEP)提供RSA支持
  机载密钥生成
  可更新的算法配置文件以满足不同客户需求
- 安全性
  符合AIS31要求的真正RNG
  操作系统中内置了基于软件和硬件的多重防攻击策略可以有效抵御如下攻击：
  侧信道攻击（SPA、DPA、定时攻击等...）
  侵略式攻击
  高级故障攻击
  其他类型的攻击（频率、光亮、温度、电子脉冲和电压等）

附加特性

- 可焊性
  MSL1包装(Jedec J-STD-020)
  Ni/Pd/Au PPF电镀
  封装分类回流焊温度：260°C
  符合欧洲有害物质限制指令（RoHS指令）的无铅封装
- ESD保护 > 4 kV (H
- 用户数据个人化
  SE在个人化过程中加载了默认配置文件：
  SE特殊标识符
  主安全域默认配置密钥集（含3个密钥）
- 配置文件可通过更新以下内容来满足客户需求：
  — 辅助安全域
  — 客户应用Applet
  — 补充密钥集/密钥
  — 客户特定的多元化算法
  — 客户特定的DF / EF
- 打印个人化
  金雅拓主张在包装顶部使用激光技术对字符实施个性化处理。
  — 第一行预留用于追溯硅提供商
  — 最多2行10个字符用于客户个性化。我们强烈建议您打印可视标识符
  — 1行用于客户标识符(TRIGRAM)..

“对物联网解决方案的日益依赖及高调网络攻击的频繁出现，使得各行各业都将安全技术视为支持他们实现持续增长的必要条件。这个级别的安全性绝不能是事后诸葛亮，而是必须从一开始便融入到新产品开发项目中。Cinterion安全芯片兼备灵活性与高级安全性，能满足这一需求。”

— Robin Duke-Woolley，领先的技术分析公司Beecham Research的CEO

欲知详情，请访问
gemalto.com/m2m或www.facebook.com/gemalto或在twitter上关注我们
(@gemaltom2m)。

金雅拓物联网中国
讯亦无线通信科技（上海）有限公司
上海 宜山路425号光启商务楼2109室
200235，上海
中国
Tel：+86 21 61032660

GEMALTO.COM/M2M

gemalto
security to be free