软件安全授权在汽车电子行业中的应用

朱志兴

金雅拓 - 高级产品经理

2017年11月

AGENDA

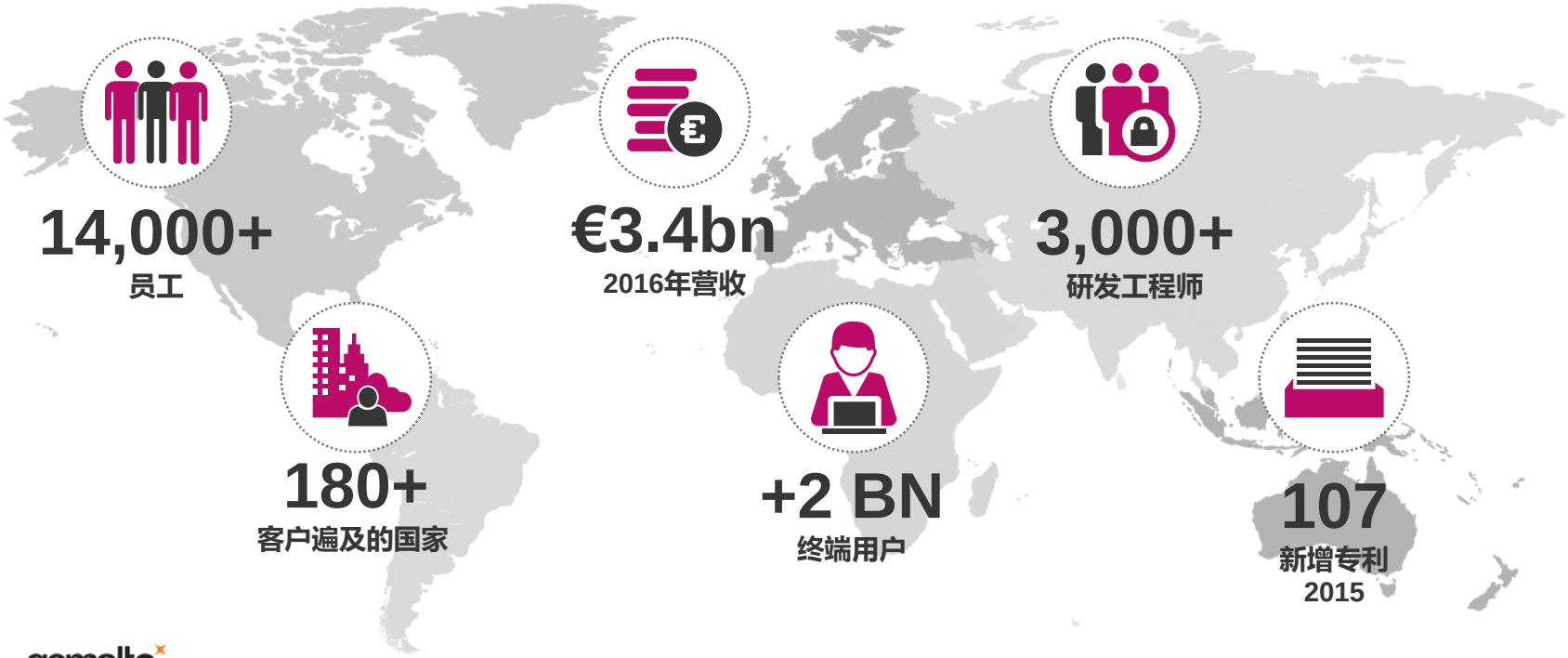
- 关于金雅拓 – 软件货币化
- 汽车电子发展的趋势与挑战
  - 金雅拓能帮助到您什么
- 圣天诺解决方案

gemalto

关于金雅拓 - 软件货币化

金雅拓-全球领先数字安全公司

金雅拓为全球企业客户提供创新的数据保护与软件货币化解决方案



14,000+
员工

€3.4bn
2016年营收

3,000+
研发工程师

180+
客户遍及的国家

+2 BN
终端用户

107
新增专利
2015

金雅拓-业务范围

我们帮助我们的客户为全球十亿人提供安全、可信的数字服务

软件货币化 - Software Monetization

- 通过专业技术把软件保护好，防止破解，防止非法拷贝，**降低损失**
- 通过灵活安全的授权技术，实现多样化的业务模式，让软件/设备卖的更好，**增加收入**

软件保护
防止非法拷贝

安全授权
灵活授权

许可授权管理系统
EMS

软件货币化 - 行业领导者

10K+
客户

100+
国家

34+
年

全球市场领先奖

52%

"Gemalto continues to dominate the market on the strength of traditional hardware sales and innovation in emerging use cases", *Frost & Sullivan*

全球顶尖品牌正在使用

设备自动化

Honeywell FANUC SIEMENS ABB GE Schneider Electric TRUMPF KUKA Rexroth Bosch Group

医疗设备

HOLOGIC VARIAN WelchAllyn BRAINLAB GE Healthcare KONICA MINOLTA THALES Dräger medical stryker TOSHIBA Medical Systems

电信网络

ERICSSON cisco JDSU HUAWEI ascom JUNIPER NETWORKS Sonus BROCADE Anite

建筑管理

SIEMENS BOSCH Security Systems GE Security ThyssenKrupp Elevator Dallmeier HID SECURITON Honeywell

测量& 视觉

ZEISS Honeywell BIZERBA COGNEX ROHDE&SCHWARZ METTLER TOLEDO STEMMER IMAGING AMETEK Avery Weigh-Tronix

游戏设备

RAW THRILLS BANDAI NAMCO TAB IGS WMS psmtec SG GAMING KONAMI NOVOMATIC

数字打印

Canon hp FUJITSU RICOH InfoPrint Solutions neopost Stratasys Kodak LEXMARK Pitney Bowes DNP

gemalto

汽车电子发展的趋势与挑战

--- 金雅拓能帮助您实现什么---

软件对智能汽车越来越重要

- 摩根士丹利预估未来智能汽车 › 60%的价值来自于软件
- Bosch, Continental AG、 Honeywell… › 开始面向软件转型
- 百度提出SDV(Software Defined Vehicles) › 软件定义汽车
- 软件驱动智能汽车创新 › ADAS，电动智能化，自动驾驶，共享出行
- 金雅拓
  - “Mercedes me 连接” - 奔驰E系列“数字钥匙”
  - “奥迪Connect”-奥迪A3信息娱乐系统
  - “Connected Drive”- BMW宝马联网驾驶
  - 携手Valeo法雷奥 为InBlue®智能钥匙加密安全
  - 助力斑马打造中国首款互联网汽车-荣威RX5

商业模式多样化

软件货币化帮助汽车生产商实现更多商业模式

收入机会

Devices
1

Traditional business model based on one time sell of car, maintenance and spare parts

Software
2

Control feature and functions of devices via licensing for example: Tesla battery capacity upgrades

Services
3

Charge for mobility capability versus a “one time sell” of the car. Examples: Flinkster, Stadtmobil and Uber.

Data
4

Utilize data collected to package and sell to other drivers and municipalities; Intelligent traffic tracking, insurance companies

Eco System
5

Connected Car platform where devices and applications from different vendors and cars work together. For example car2car communication.

ADAS与自动驾驶快速增长的机遇与挑战

- Intel花费153亿美元收购Mobileye

  Mobileye最大的价值来自先进视觉算法以及安装量

- ADAS与自动驾驶主要产业链包括芯片厂商，摄像头厂商，雷达厂商，以及算法公司

  有核心竞争力的算法公司可能容易取得突破

- 对最有价值算法的保护非常重要

  需要专业的IP保护

- 算法公司希望灵活的业务模式，比如根据安装量进行收费

  需要灵活的许可授权解决方案

数据来源：IHS、东方证券研究所

保护与安全需求多样化

以软件为中心的价值链给汽车制造商和供应商带来了新的挑战。

运行于MCU上
核心算法保护

运行Android，Linux,
QNX上软件的保护

手机APP加固

软件/固件安全升级

数据文件加密
数据完整性

身份认证

授权需求的挑战

1 如何快捷激活授权让软件使能，比如车机上的语音识别软件

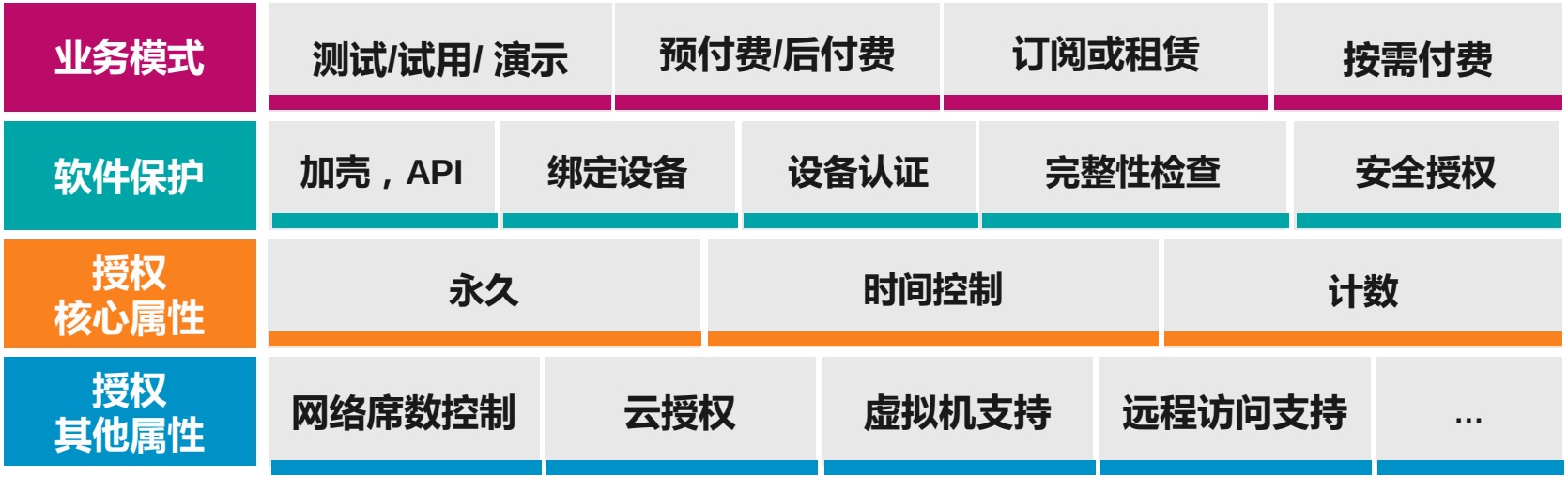
- 车机集成测试时如何快速激活短时间的授权用于测试
- 用户购车时，如何方便快捷获得一定时间（例如3年）的免费使用授权
- 免费期到了以后，如何方便快捷实现用户付费后，授权更新或者延长

2 如何降低服务成本

- 自助激活授权
- 授权自动在线升级
- ERP/CRM集成实现授权流程自动化

金雅拓帮助客户解决问题

用灵活和创新的许可模式实现多样化的业务模式



gemalto

圣天诺解决方案

圣天诺解决方案

安全，IP保护
防止非法拷贝

功能打包
许可授权

许可授权管理系统

专业化咨询
本地化服务

软件货币化-本地化支持

- 北京 – 全球三大研发中心之一
- 北京 – 亚太技术支持中心
- 北京 – 中国区销售总部
- 上海 – 华东地区销售和售前支持
- 深圳 – 华南地区销售和售前支持

gemalto

安全 & 保护

加壳加固技术 (Envelope)

- **一键保护exe,DLL,SO文件，数据文件**
  - 支持Windows, Windows嵌入式，Linux x86, Linux ARM, MAC, Android ARM, Android X86等等
- **JAVA和.Net程序基于方法级保护**
  - 方法级的代码混淆和代码加密
- **基于白盒的安全通道**
  - 安全通道保护了硬件锁 / 软锁与程序之间的通讯安全
  - 白盒技术打散密钥，使得密钥不会在内存中出现
- **AppOnChip - 全自动的硬件锁内代码执行**
  - 加壳时把代码转换成加密数据包
  - 在执行的时候按需加载，硬件内部动态执行
- **智能的非法调试检测，锁定硬件锁机制，极大增加破解成本**

锁定硬件锁（含芯片）

- 外壳检测到非法调试，直接锁定硬件锁（含芯片），黑客无法继续破解
  - 增加破解成本
  - 降低破解机率
- 开发商可以选择检测与锁定的级别
  - 检测级别越大，防止调试的强度越大
  - 检测级别越小，误报调试的可能性越小
- 价值
  - 对高价值软件起到进一步有效保护
  - 在专用的设备，包括行业设备，游戏设备中有极大的价值

可信计算： AppOnChip / AppOnChip SDK

- **业界可信计算现状 – TEE（可信执行环境）**
  - Trust Zone (ARM)
  - SGX (Intel)
- **安全元素 Secure Element (各种智能卡）**

- **AppOnChip**
  - 通过外壳动态导入代码到硬件锁，不受硬件锁空间限制
  - 算法或者代码升级，无需升级硬件锁
- **AppOnChip SDK**
  - 开发商把重要的算法，使用我们提供的工具链转化成能被虚拟机执行的字节码。算法需要使用Java来编写。
  - 动态加载和静态加载的都可以支持
- **价值**
  - 事实上创建相对独立的代码执行环境，从而有效保护IP和防止拷贝，具有最高安全性
  - 开发商可以写出各种应用来满足特定需求：比如认证，安全存储，自定义密码等

安卓APK或者SO保护

- **提供加壳工具，无需修改源代码**
  - 无需上传源码到云端进行加固
  - 支持纯IP保护，以及IP保护和许可授权
- **一键实现APK或者SO加密保护**
  - 对Java进行方法级别加密保护
  - 对Native C/C++（SO）进行加密保护
  - 对DEX文件进行加密保护
- **支持对数据文件进行加密保护**
  - 只有被保护的APK才能打开
- **支持软锁或者硬件锁**
  - 软锁绑定设备指纹ID以及私有的ID，有效防止非法拷贝

认证功能

- 可以与软件保护，许可授权，认证和数据保护等功能一起实施
- 挑战响应认证–无需分发管理数字证书
- 智能卡硬件和PIN码双因子
- PIN码本地验证，不传递，防止密码被截获
- 每个认证锁有唯一的认证秘钥
- 内嵌开发商ID，开发商的服务器只允许自己的认证锁进行认证并接入

gemalto

授权功能

丰富的授权载体或容器

硬件锁或芯片



软许可授权

- 虚拟的锁
- 与硬件锁或芯片采用统一的外壳与API，可交替互换
- 多种OS支持: Windows, Linux, MAC, Android
- 各种虚拟机环境支持

云授权

- 实时的许可授权控制
- 用户中心的许可授权模式，随时随地联网使用授权
- 支持获取离线脱网使用
- 使用数据有效获取

单芯片方案

- 32位ARM CPU：国际大厂高性能智能卡芯片
- 支持温度范围 -40°C ~ +105°C
- VQFN32封装(RoHS)
- 支持USB2.0全速率或者SPI通讯
- 内置虚拟机，支持安全运行代码或者算法
- 高达392KB的可用内存空间

授权 - 稳定 & 安全

- 硬件锁
  - 行业最稳定，特别是时钟锁，网络锁对稳定性要求高
  - 实现LicenseOnChip，通过固件来识别授权，安全有保障
- 软许可授权
  - 自带安全存储区
  - 通过绑定金雅拓私有文件系统ID，进一步防止拷贝复制
- 软锁实现稳定，可靠的指纹ID读取
  - 各种Window, MAC, Linux物理机指纹ID读取
  - 各种虚拟机指纹ID读取
  - 安卓设备指纹ID读取

授权 – 灵活 & 方便

- **Cross-Locking**
  - 硬件锁与软锁采用同一套外壳以及API, 可以交叉使用
- **方便的功能模块开/关控制与打包组合**
  - 只需一份被保护的软件，开关控制与打包组合后期通过授权实现
- **丰富的授权属性**
  - 包括永久，到期日期，使用天数，网络席数控制等等
- **用户自助在线激活**
  - 通过Customer portal实现基于激活码（ Product Key ）的自助激活
- **在线自动更新**
  - 每个硬件锁或者软许可授权都有唯一的KeyID，提供后台EMS，以及web service实现授权自动在线更新

MCU/DSP设备的IP保护与授权

- **通过提供源码，示例代码调用API方式支持授权**
  - 支持永久，到期日期
  - 行业最小的运行时
  - RSA 34KB Flash, 13KB RAM
  - AES 8KB Flash, 2KB RAM
  - 强大的许可授权管理系统EMS
- **提供代码混淆工具，防止反编译**
  - 对运行在MCU/DSP上的代码进行混淆
  - 支持兼容LLVM的编译器，包括GNC, GCC等通用编译器

gemalto

许可授权管理系统EMS

许可授权管理系统EMS

- **统一的授权管理平台**
  - 用户授权生命周期管理
- **直观的用户界面**
  - 无需客户端（在浏览器中打开）
  - 基于角色的授权管理,包括代理商角色支持
- **第三方ERP或者CRM接入，实现授权自动化**
  - Oracle
  - SAP
  - Salesforce

主要功能

授权创建和管理

客户自助授权激活

Web service支持
授权自动在线升级

使用情况&报告

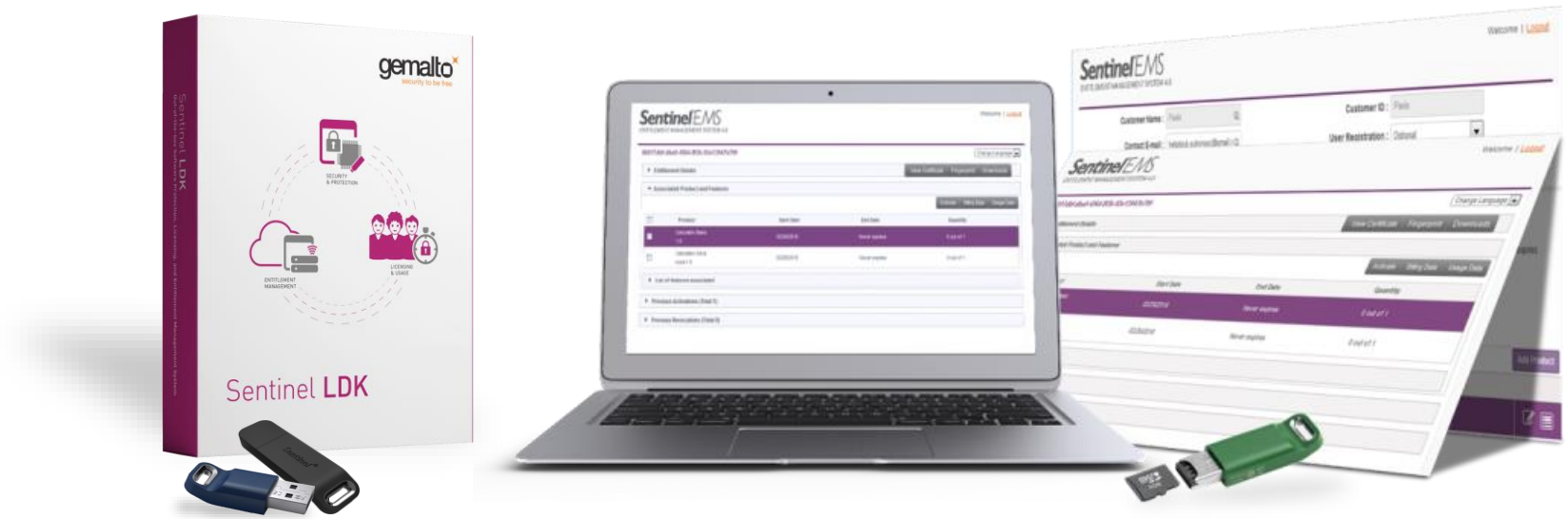
代理商角色支持

支持与ERP,CRM集成

基于订单的ESD
电子软件下载

提供托管服务
99.99%级别

圣天诺产品家族



Sentinel **LDK** | Sentinel **EMS** | Sentinel **RMS** | Sentinel **Fit**

EMBRACING CHANGE

金雅拓帮助客户实现转变

This presentation brought to you by Gemalto

THANK YOU！

金雅拓
www.gemalto.com

金雅拓 软件货币化
www.gemalto-sm.cn