海葵鱼安全组件

开放式安全

岸思科技

简介

海葵鱼安全组件为信息安全领域提供了一套完全开放式的鉴权解决方案。

鉴权无处不在

执行摘要

海葵鱼安全组件	
产品定位	解决传统鉴权方式弊端的，安全、高效、灵活的开放式鉴权方案。
行业痛点	互联网与物联网的传统鉴权方式弊端多多： 1. 易被攻击。敏感数据易泄露，验证措施易被绕开。 2. 鉴权高度依赖数据库。架构复杂，开发繁琐，运营成本高。 3. 扩展性差，难以跨平台鉴权和离线鉴权。
解决方案	使用全新设计的完全开放式的鉴权架构。
优势与机会	1. 大幅度提高敏感数据安全和验证安全。 2. 鉴权不基于数据库，架构与开发简单高效，降低运营成本。 3. 高扩展性，极易实现跨平台鉴权和离线鉴权。 4. 适用于所有互联网和物联网的鉴权应用场景。

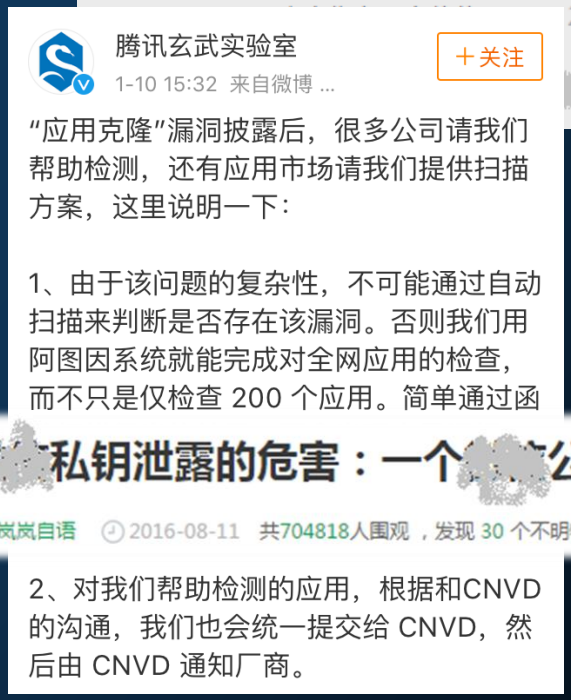
封闭与开放

封闭

传统的鉴权模式都属于封闭式，问题多多：

- 高度依赖数据库
- 口令与鉴权密钥易泄露
- 验证易被绕开（SQL注入）
- 设备上的私钥易被盗取
- 证书链模式效率低下
- 扩展性差
- 难以多用户、跨应用鉴权
- 离线验证困难

案例：国内某著名邮箱提供商曾遭受SQL注入攻击，海量Password的Hash值泄露，最终导致了大量邮箱被盗，进而导致了大量用这些邮箱注册的Apple账号被盗，进而引发了对Apple用户的勒索风波，流毒一时。



封闭与开放

开放

海葵鱼安全组件采取开放式的安全架构：

- 不使用数据库
- Token的内容完全由开发者决定
- 抗SQL注入攻击，防止验证被绕过
- 抗关键信息泄露
- 高效验签，拒绝证书链
- 任意扩展
- 便于多用户、跨应用鉴权
- 简洁的离线验证

完全开放的鉴权Token

海葵鱼所使用的鉴权Token完全由开发者定义，从而广泛地适应和兼容各种应用场景。

开发者根据自己的业务需要，可以将任何信息以任何形式作为鉴权因子放入Token中。

完全开放的鉴权Token

假设我是会员登录系统的开发者，则可以设置：

Token = 用户名 + 口令 + 有效期 + 权限 + ……

若是智能建筑中门禁系统的开发者，则可以设置：

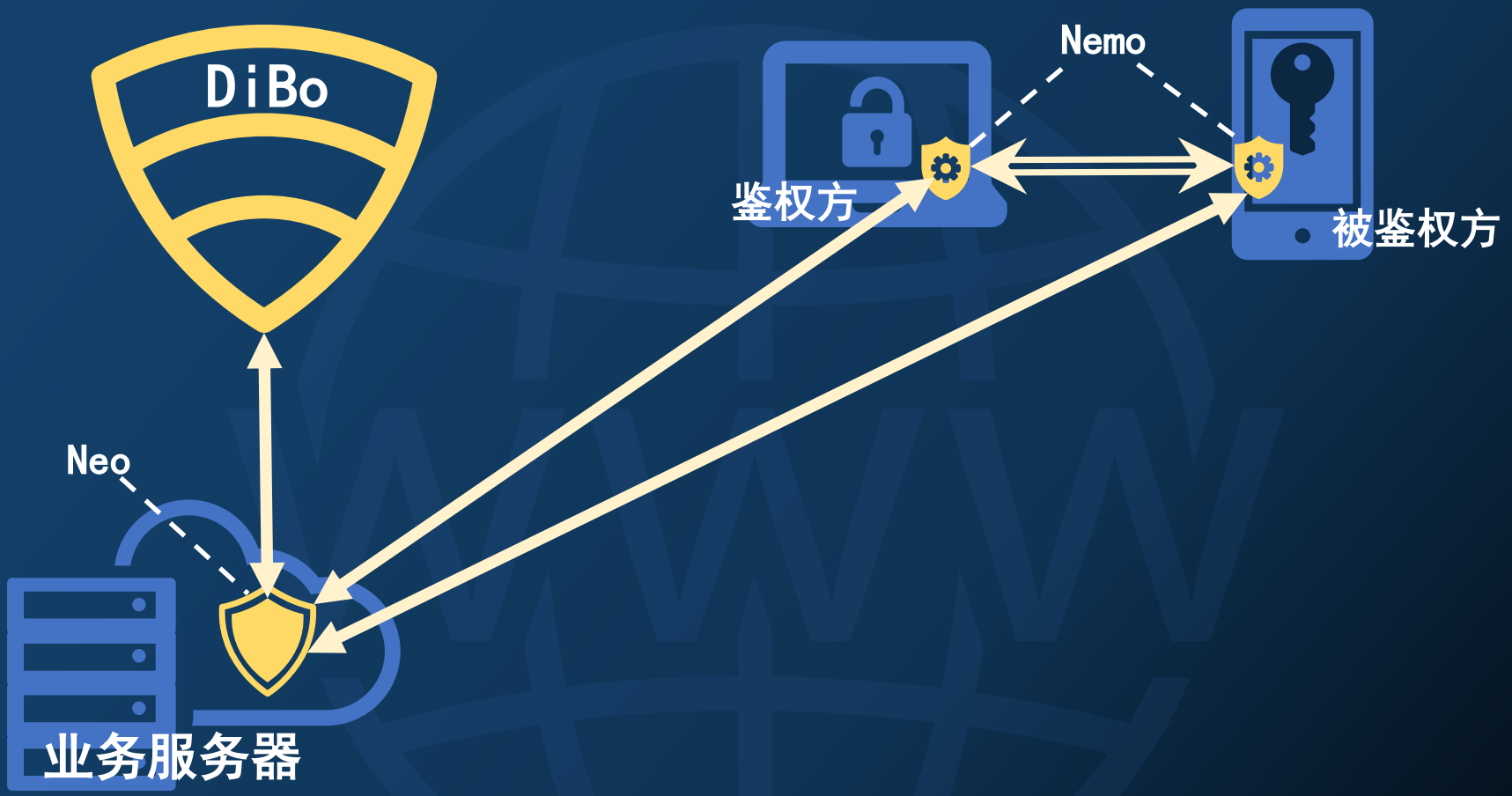
Token = 姓名 + 授权门禁列表 + 有效期 + ……

完全开放！

海葵鱼安全组件·技术特点

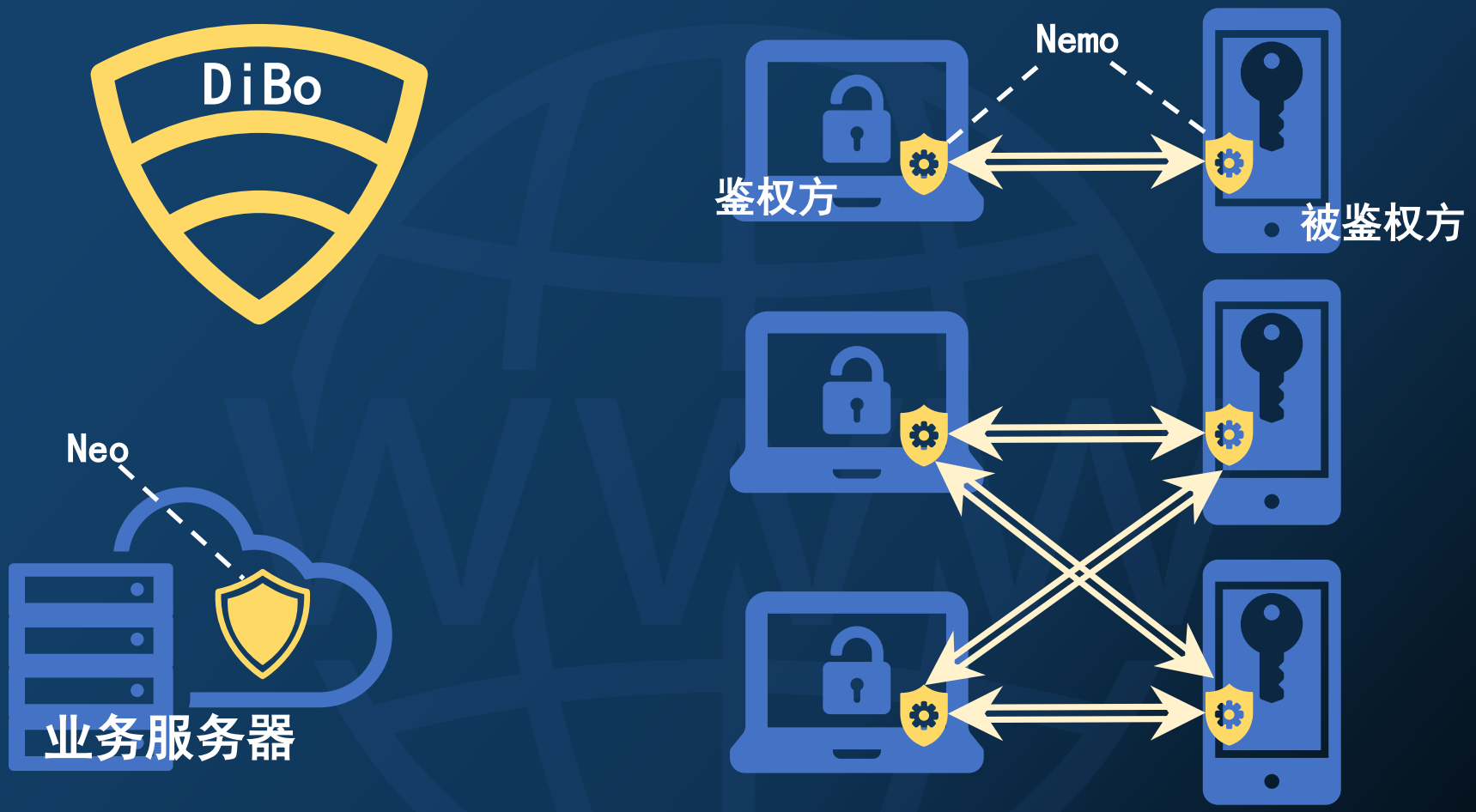
基于完全开放式的Token，结合IBC技术，海葵鱼技术特点如下：

海葵鱼安全组件·系统架构



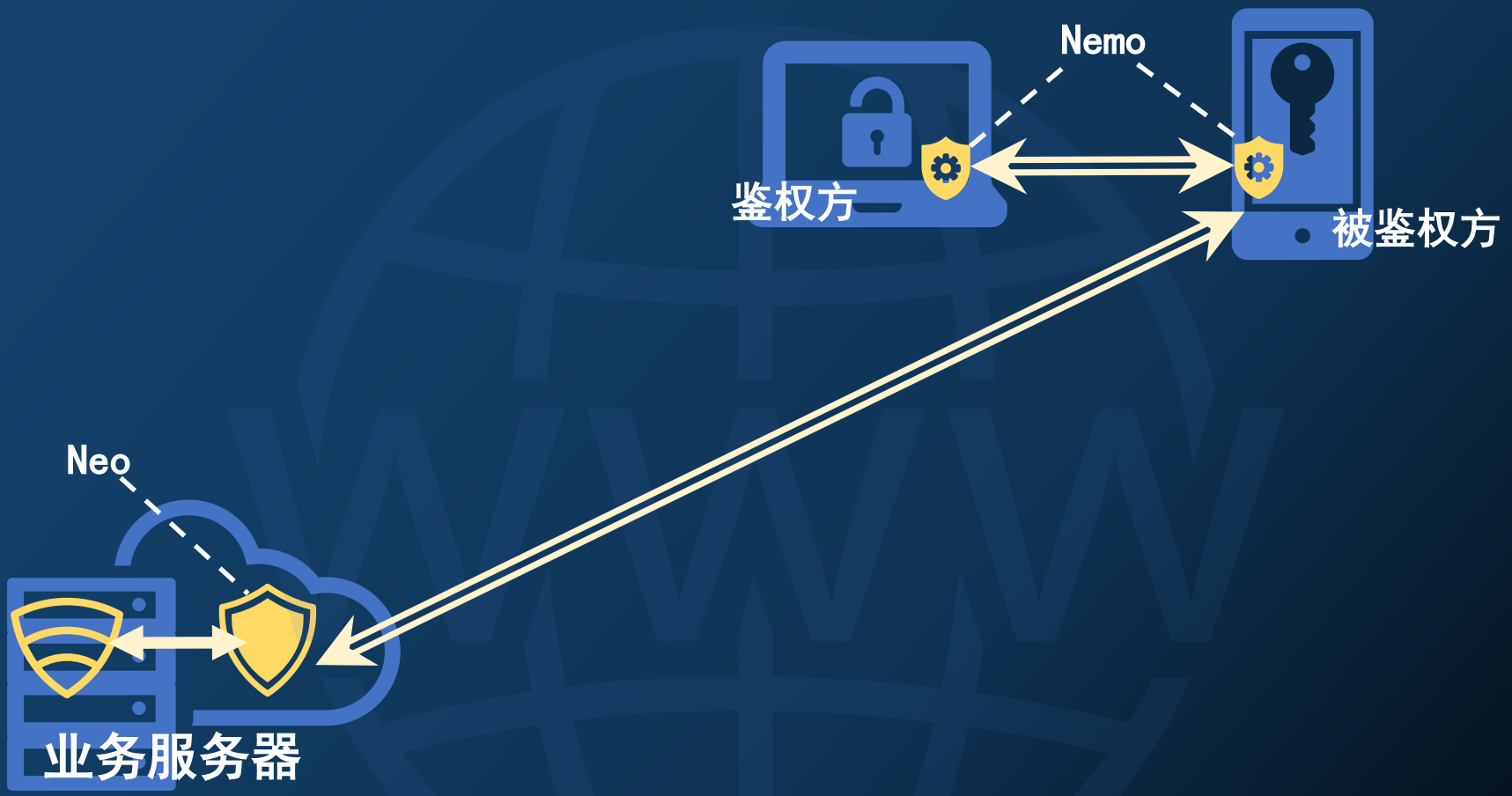
- DiBo：由岸思运营和维护的关键安全模块。
- Neo ：置于业务服务器上的安全模块。
- Nemo：置于鉴权和被鉴权客户端或设备中的安全模块。

海葵鱼安全组件 · 系统架构



- DiBo：由岸思运营和维护的关键安全模块。
- Neo ：置于业务服务器上的安全模块。
- Nemo：置于鉴权和被鉴权客户端或设备中的安全模块。

海葵鱼安全组件 · 系统架构



- DiBo也可用镜像的形式部署到业务服务器。
- 业务服务器也可以使用Neo直接充当鉴权方。

海葵鱼安全组件·对比

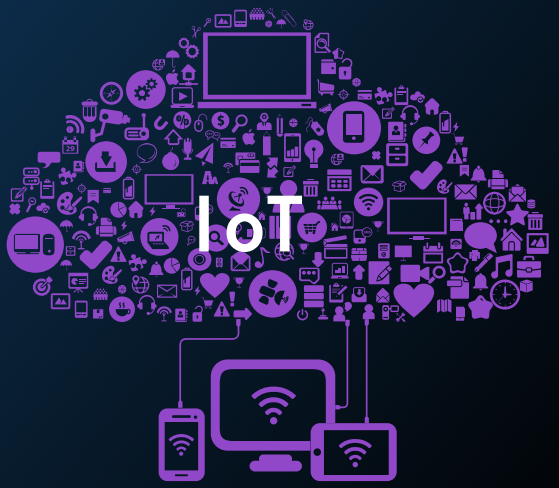
	封闭式鉴权	海葵鱼安全组件
数据库依赖	高	低
Password	存在被盗风险	被盗风险极低
私钥	一旦被盗，后果极其严重	单纯的私钥被盗不会造成实际灾害。
SQL注入攻击	有可能导致权限控制或设备绑定策略被绕过	从根本上免疫SQL注入攻击
真双向认证的实现复杂度	高	低
业务灵活性	低	高

应用场景

海葵鱼安全组件完全开放式的设计带来了广阔的应用空间，适合大量互联网和物联网应用场景：

- App账户鉴权
- 电子票务
- 电子合同
- ……

- 智能汽车
- 智能门锁
- 智能建筑
- 智能家居
- ……



应用场景 · App账户鉴权及登录

使用海葵鱼进行账户鉴权及登录，可以做到：

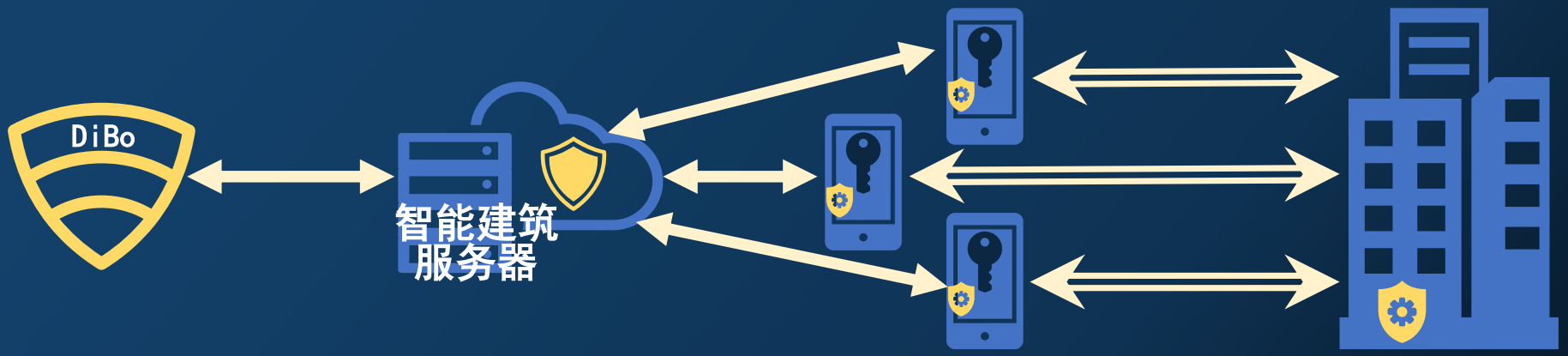
- **口令零存储：** 服务端和客户端都不需要存储口令或其相关信息，彻底杜绝口令被盗。
- **免用数据库：** 设备绑定、权限管理都可以不基于数据库来实现，口令也不需要数据库存储，降低成本和开发量。
- **免疫SQL注入：** 使用数字签名来抵御SQL注入攻击，防止登录验证与权限管理机制被绕过。
- **私钥抗泄露：** 客户端单纯的私钥泄露不会造成实质性的危害。
- **安全等级管理：** 开发者通过对Token简单的自定义就可以做到层次多样的安全等级管理，亦不需要使用数据库。

应用场景·智能汽车

将海葵鱼应用于智能汽车，可以做到：

- **手机解锁：** 可以用一部手机解锁多辆汽车，并且开锁时的鉴权不需要网络。
- **远程借车：** 可以授权他人的手机解锁自己的汽车，并且可以设定借车的期限。
- **租车管理：** 可以利用Token来有效地防止逾期不还车，只有在使用期限内或及时付费才能启动汽车，而且汽车不需要联网。
- **零部件认证：** 汽车认证重要的零部件，零部件之间的相互验证，车联网安全体系的一部分，而且此项功能依然不需要联网。

应用场景 · 智能建筑



将海葵鱼应用于智能汽车，可以做到：

- 门禁管理：用手机或可穿戴设备替代繁琐的各种门卡，在门禁管理上摆脱臃肿的数据库。
- IT系统接入：通过被授权的设备直接接入建筑的IT系统，摆脱纷杂的账号密码。
- 访客管理：生成Token赋予访客临时进出的权限，这些权限会随着Token的失效而自动失效，不需要刻意去注销，不需要额外的管理。
- 酒店管理：抛弃房卡，方便快捷，带来更好的客户体验。

应用场景·智能门锁、租房管理与智能家居

现在很多智能门锁，尤其是租房公司使用的智能门锁，绝大部分是以输入口令作为解锁方式，安全性低，并且需要时刻联网，一般做法是需要门锁之外的一个额外模块去连接wifi或网线，大大增加了成本，而且管理上极为不便。

通过使用海葵鱼安全组件：可以做到：

- **手机解锁：** 用手机app即可开启门锁。
- **脱网验证：** 门锁和手机都不需联网，所有验证和管理皆离线进行。
- **临时开门：** 授予他人临时开门的权限，可以设定该权限的使用次数和有效期。
- **租房管理：** 租房公司根据租客的缴费情况发放Token。一旦欠费，Token会自动失效导致无法开启门锁，不需要额外的管理，方便且高效。
- **智能家居：** 所使用的Token可以拿来控制各种智能家电。

应用场景·电子票务

现在票务行业依然大量使用纸质票，即使网络购票，也需要以快递或者现场交付的形式将纸质票交给购票者，不但用户体验很差，而且购票者之间转让门票更是尤为不方便。

通过使用海葵鱼安全组件：可以做到：

- **手机票务：** 票据信息以Token的形式存放在手机上，不再需要纸质票，在线购票在线取票，方便快捷。
- **离线验票：** 验票设备不需要联网，而且大部分情况可以用手机App完成验票工作。
- **在线转让：** 可以在线将门票转让出去，不再有像纸质票转让时的繁琐步骤。
- **杜绝票贩：** 通过Token将人票绑定，从根本上杜绝票贩倒卖。

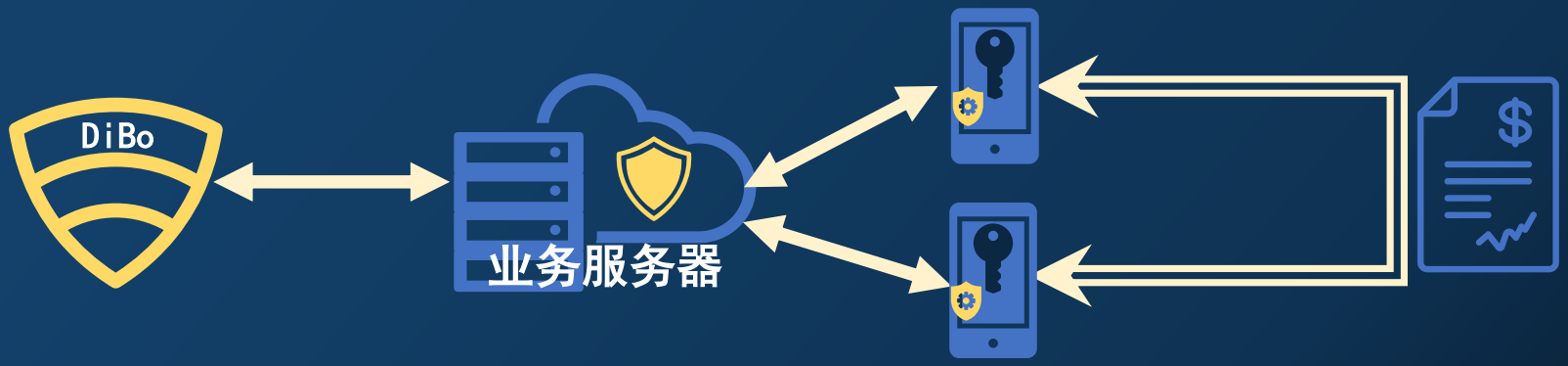
应用场景·电子票务

现在票务行业依然大量使用纸质票，即使网络购票，也需要以快递或者现场交付的形式将纸质票交给购票者，不但用户体验很差，而且购票者之间转让门票更是尤为不方便。

通过使用海葵鱼安全组件：可以做到：

- **手机票务：** 票据信息以Token的形式存放在手机上，不再需要纸质票，在线购票在线取票，方便快捷。
- **离线验票：** 验票设备不需要联网，而且大部分情况可以用手机App完成验票工作。
- **在线转让：** 可以在线将门票转让出去，不再有像纸质票转让时的繁琐步骤。
- **杜绝票贩：** 通过Token将人票绑定，从根本上杜绝票贩倒卖。

应用场景·电子合同



现在的远程合同签署，要么是以快递交换纸质合同，要么是在网站上点“确认”操作。前者成本高且不方便，后者因为不符合“电子签名法”而存在法律风险。

将海葵鱼安全组件应用于电子合同签署，可以做到：

- **不可抵赖：** 使用Token和私钥对合同进行签名后，参与签署的任何一方都无法抵赖。
- **高效快捷：** 通过手机App即可完成合同签署。
- **合乎法律：** 签署出来的签名完全符合《中华人民共和国电子签名法》以及其他各国的相关法律。

海葵鱼安全组件 · 结语

我们将这套组件命名为“海葵鱼”，是化用了海葵鱼（又称小丑鱼）与海葵之间的共生关系：一种海葵鱼栖身于一种海葵之中，其他物种包括其他种类的海葵鱼闯入都会遭到海葵的攻击，这正好是一种自然界的鉴权操作。

海葵鱼安全组件所使用的
开放式安全架构
将会为大量的产品和应用场景增添全新的安全与开发体验。

希望能像海葵守护海葵鱼一样，
为您的产品保驾护航。

谢谢！

岸思科技