海葵鱼安全组件

岸思科技

简介

海葵鱼是一套面向开发者的用于鉴权的安全组件。

与传统的鉴权方案相比，海葵鱼解决了五个安全性问题和易用性问题。

- Password的存储
- 私钥的存储
- PKI体系的实现
- 登录管理
- 设备绑定

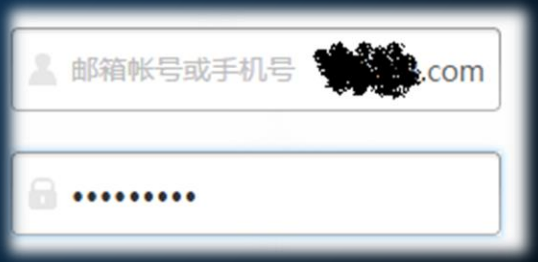
目前支持各类型服务器，iOS、Android平台。

安全性问题 · Password的存储

Password在服务端的存储一直是难题。

明文存储的危险性自然不必多说，但即使采取存储Hash值的形式，也很难称得上安全，因为存在彩虹表攻击。

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。

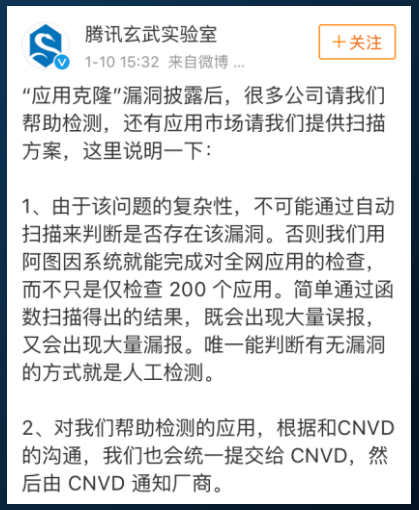


因此，Password在服务端的存储安全，在根本上取决于外围组件对数据库的保护。这在实现上很难做到滴水不漏。

安全性问题 · 私钥的存储

在很多高安全应用场景下需要使用私钥，但在客户端安全地存储私钥难度极大，尤其是在开放平台上。即使是使用白盒密码等技术，也难以抵御一些最新的攻击手段。

案例：2018年初，大量主流Android App被曝光存在“应用克隆”漏洞。借由该漏洞，攻击者可以轻易将App沙盒里的私有数据悉数拷贝。如果私钥存储在沙箱中，则也会遭到拷贝并泄露。白盒密码技术在这种攻击面前无效。



传统的私钥安全解决方案是使用SE(Security Element)，如智能卡、U盾等。但这会极大降低易用性和用户体验。

易用性问题·PKI体系的实现

在高安全应用场景中，往往需要实现客户端与服务器的双向认证，而目前双向认证是基于PKI体系的。但PKI体系流程繁琐、开发复杂，需要涉及密钥生成、数字证书颁发、签名、证书链验证、签名验证等。而且数字证书在使用上非常不灵活。

由于全套PKI体系的实现非常复杂，因此大量的产品只对其进行部分实现，并不是为每一个客户端都颁发独一无二的数字证书，在功能上只做到了单向认证或“伪双向认证”。

易用性&安全性问题 · 登录管理

当前广为运用的登录模式，需要去后台数据库获取账户的权限信息。这个过程不但逻辑复杂，而且这个过程容易受到攻击。

攻击风险示例：如果在调取数据库时存在SQL注入漏洞，并且访问权限由SQL语句控制，则攻击者可以在判断权限时注入恒真或恒假语句，跳跃权限判断逻辑，从而获取数据访问权限。

易用性&安全性问题 · 设备绑定

设备与账户的绑定普遍用于中高安全应用场景，但目前绝大多数产品都是基于数据库实现设备绑定。需要用数据库存储允许某账户登录的所有设备信息。这种方式存在存储量大和流程繁琐等问题，而且此环节同样存在攻击风险。

封闭与开放

封闭

乌云发布新漏洞，[redacted]邮箱过亿用户数据或泄漏

本文作者：小芹菜　　2015-10-19 15:02

导语：此漏洞将导致[redacted]邮箱过亿数据泄漏

传统鉴权模式都是封闭式架构，导致问题多多：

- 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

腾讯玄武实验室　　+关注

1-10 15:32 来自微博 ...

“应用克隆”漏洞披露后，很多公司请我们帮助检测，还有应用市场请我们提供扫描方案，这里说明一下：

1、由于该问题的复杂性，不可能通过自动扫描来判断是否存在该漏洞。否则我们用阿图因系统就能完成对全网应用的检查，而不只是仅检查 200 个应用。简单通过函数扫描得出的结果，既会出现大量误报，又会出现大量漏报。唯一能判断有无漏洞

[redacted]私钥泄露的危害：一个[redacted]公众号漏洞案例分析

岚岚自语　2016-08-11　共704818人围观，发现 30 个不明物体　WEB安全　漏洞

后由 CNVD 通知厂商。

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

海葵鱼安全组件·技术背景

海葵鱼安全组件采用IBC(Identity-Based Cryptography)体系，构建出一套完全开放的鉴权架构。

IBC体系针对PKI体系中的弊端而设计的一套密码体系。

在PKI体系中，公钥为一段近乎随机的信息，无密码学以外的含义，因此需要通过数字证书来与用户的身份做绑定，因此体系复杂，验证繁琐。

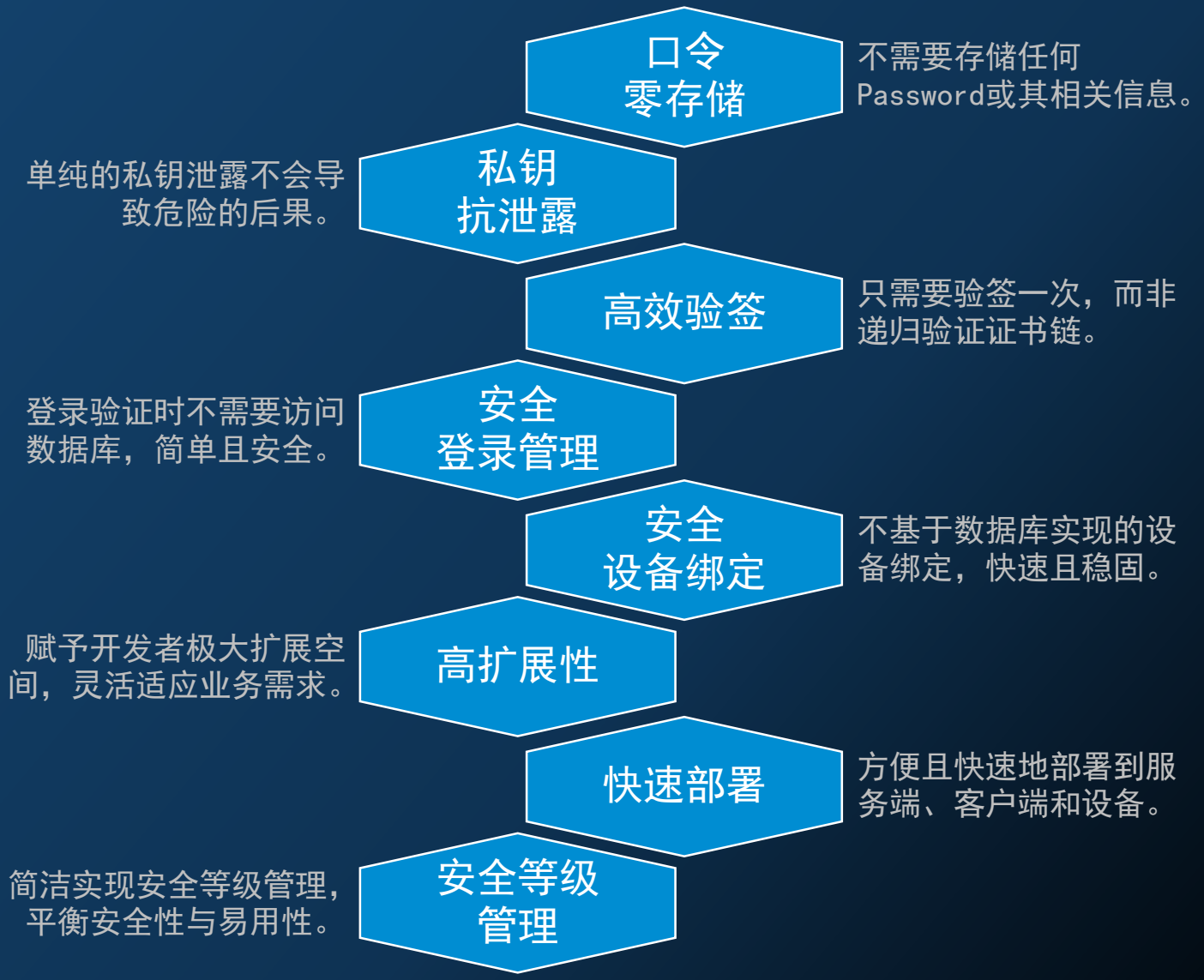
而在IBC体系中，公钥是一段有现实意义的信息，无需额外的措施来保证这一点，由此大大简化了流程，并产生了更灵活的新应用模式。

PKI公钥示例：1D23F5BD87256597DE985A4C01DD234……

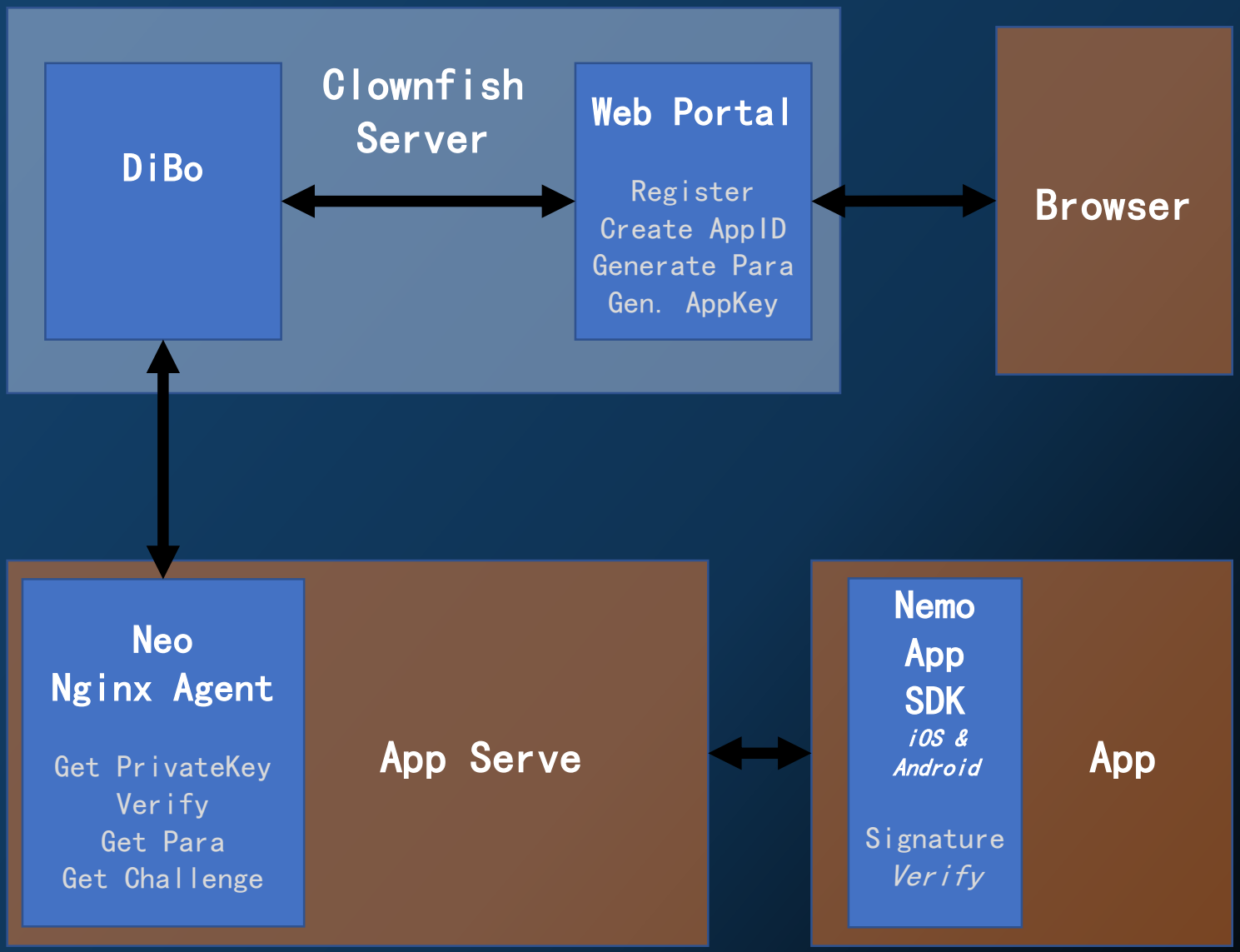
IBC公钥示例：ansikeji.r-sun.com||20181111……

海葵鱼安全组件·技术特点

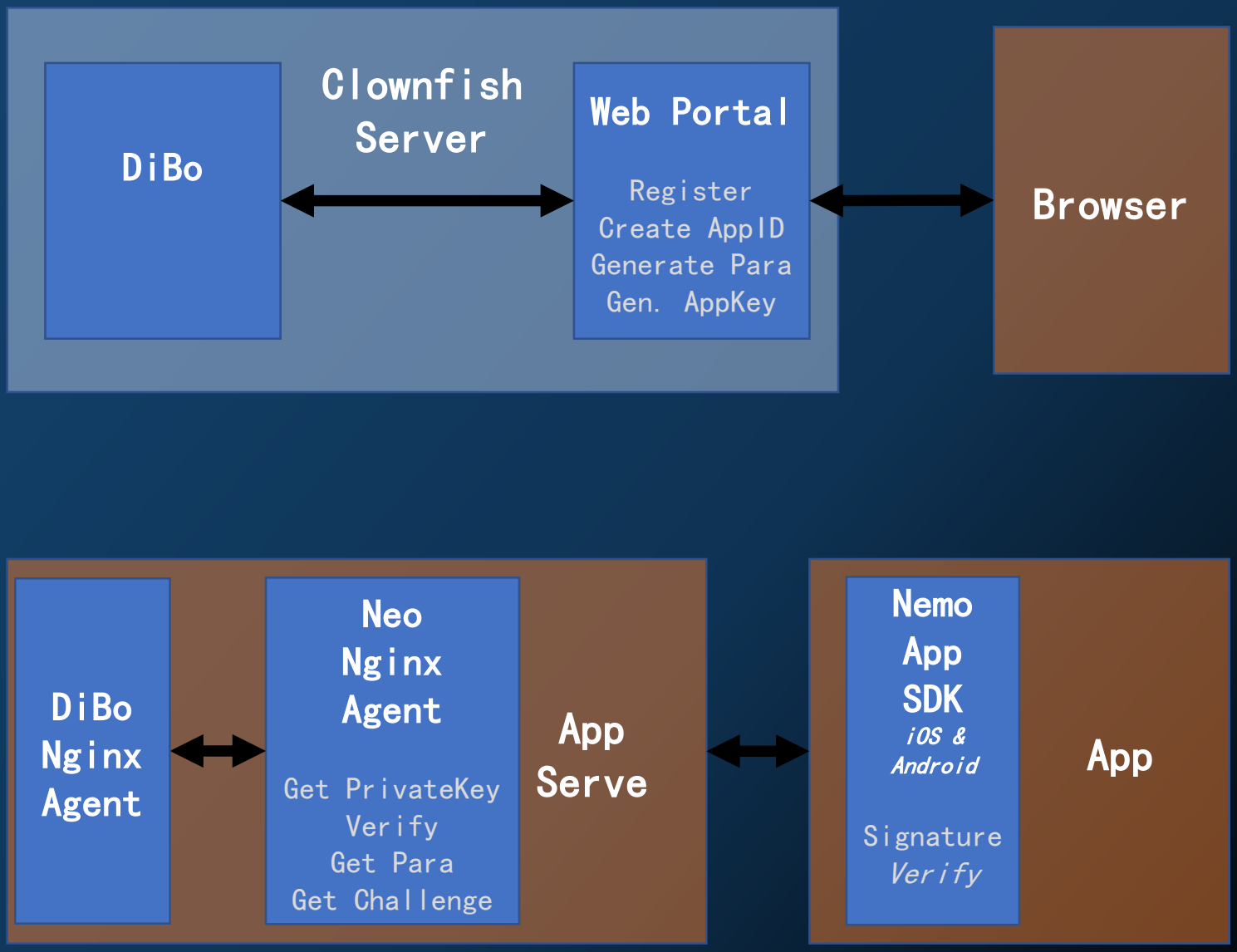
基于完全开放式的Token，结合IBC技术，海葵鱼技术特点如下：



海葵鱼安全组件 · 系统架构1



海葵鱼安全组件 · 系统架构2



海葵鱼安全组件 · Token

Token是一个由开发者自己定义的信息串，是整个架构的关键所在。

为了完成基础的安全功能，我们建议Token中应该包含如下信息：账户ID或账户名，设备信息，账户权限信息，Token编号，Token失效日期。

Token示例：

```
Ansi Tech.|| iPhone 7 F17RH5U12345678||Read Only||00000017||20220718
```

开发者还可以根据自己的需要，灵活地往Token中增减任意信息。

客户端存储Token时应删去设备信息等可以随时获取的信息（如设备信息、Password等），在鉴权时再实时获取并组装成完整的Token，从而确保设备绑定功能的安全性。

海葵鱼安全组件·Password

Password由使用者输入，这里的Password为设备Password，只针对当前设备，从而实现了设备强绑定。

Password也可以使用手势密码等确定性信息。

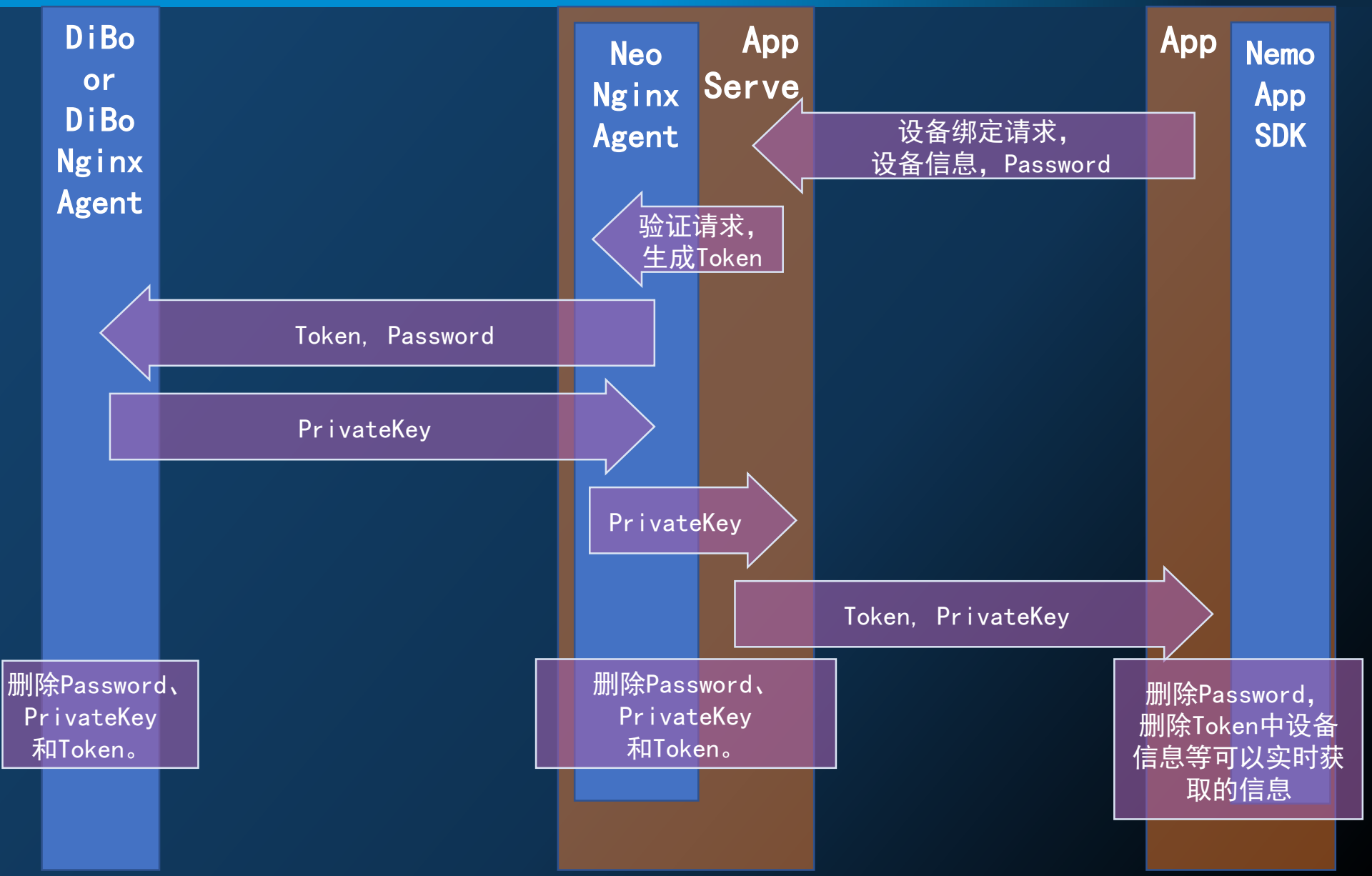
在设备绑定结束以及登录结束后，服务端与客户端都应该将Password彻底删除，以实现Password零存储的特性。

登录时再让用户输入Password，从而组装出完整的Token进行鉴权。

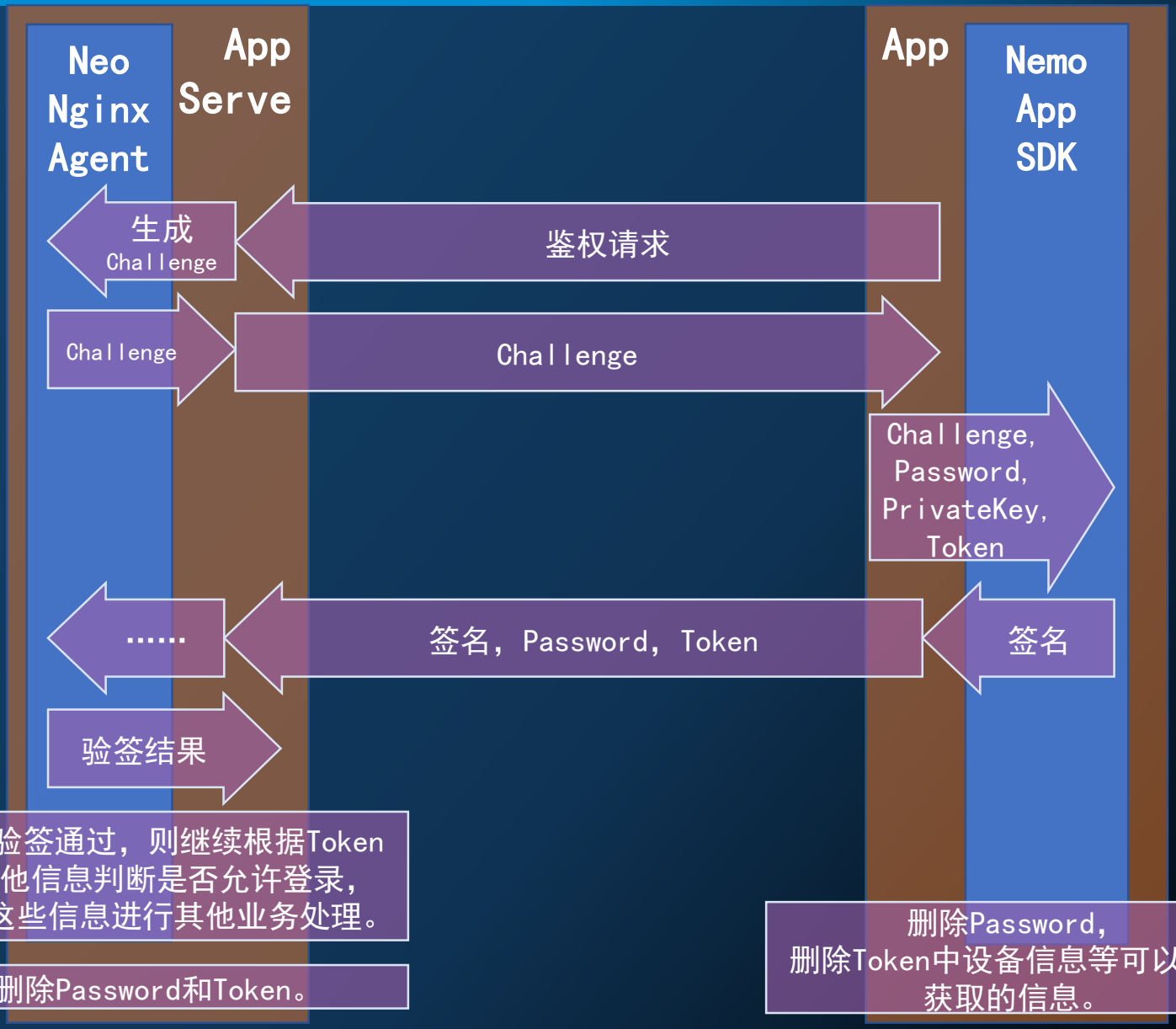
Tips:

开发者可以给客户端准备两个Token，一个使用Password，另一个不使用Password。这样，前者可以用于高安全需求的鉴权，如支付等；后者用于低安全需求的鉴权，如自动登录等，提高用户体验。

海葵鱼安全组件·设备绑定



海葵鱼安全组件·鉴权及登录



海葵鱼安全组件·安全性分析

海葵鱼安全组件可以高效且安全地完成服务端对客户端的鉴权。从而让开发者可以低成本地实现双向认证。

在安全性上，海葵鱼安全组件可以抵御如下攻击：

- **盗取Password：**由于架构中服务端与客户端都不存储Password及其相关信息，使得Password被盗取的可能性大大降低。即使Password泄露，但攻击者无法获取私钥的话，依然无法攻击成功。
- **盗取私钥：**在开放平台的客户端中，确实存在私钥被盗取的可能，但是因为攻击者没有获得Password，所以无法计算出有效的数字签名并通过验签。
- **非绑定设备登录：**攻击者无法获取正确的设备信息组成有效的Token，因此无法登录成功。

Password、私钥和设备信息，构成三位一体的防护盾，只要三者不同时被攻击者获取，安全性就可以保障。即使存在“应用克隆”等严重漏洞，相关攻击也难以达成。

海葵鱼安全组件·安全性分析

- **对访问权限的SQL攻击：**由于访问权限可以直接写在Token中，因此可以不依赖数据库直接进行权限管理，从根本上杜绝了SQL攻击的可能。即使攻击者企图通过修改Token来完成SQL攻击，但因为验签是所有验证的第一步，此企图会随着验签失败而被挫败。
- **对设备绑定的SQL攻击：**同样，由于设备信息是Token的一部分，而不需要由数据库存储，所以此项攻击不可行。

SQL攻击一直是服务端的重大威胁，经常防不胜防。通过使用海葵鱼安全组件，即使攻击者找到了可以进行SQL攻击的漏洞，但因为对Password、访问权限和设备绑定的攻击皆无法达成，损失将大大减少。

海葵鱼安全组件·易用性分析

海葵鱼安全组件通过全新的架构和密码学技术，将易用性提升上新一个台阶。

- 减少数据库依赖：Password及其相关信息、权限信息、设备绑定信息皆不需要服务端存储，大大减少了对数据库的依赖，提高了开发和维护的效率。
- 轻松实现真双向认证：开发者在实现真双向认证时，不需要再苦恼于数字证书的颁发、证书链的验证等操作，调用海葵鱼安全组件高度集成的接口就能轻松实现真双向认证。
- 使用灵活：开发者可以在Token中加入更多的信息以完成更多的业务功能。开发者也可以为同一台绑定设备制作多个Token以实现客户端在用户体验与安全上的平衡。如：可以额外制作一个无需用户输入Password的Token来应对低安全需求的应用场景。

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

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