Azure PaaS服务密钥的安全性

Azure PaaS服务，比如存储，Redis缓存，服务总线，IoT中心等等，一般通过密钥来认证客户端，也就是说只有提供正确密钥的客户端才能访问和使用对应的Azure PaaS服务，所以这个密钥是很重要很重要的，那么该如何保证密钥的安全性呢？接下来将以问答的形式来阐述。

**问：密钥能否被暴力破解？**

**答：**我们先看看几个密钥的例子来分析密钥的组成。

|  |  |
| --- | --- |
| 存储账户 | 5+kWqp1jIGQdGPVp6o7pgT/8DlRYnE55jJbxh51h7WHU4yGqAbMYdCYbSfR2CaFsi1/pfmL+d/QJbeAmDn6FQg== |
| Redis | R4W4Ol+yHUJ9Z25VHSrQdn9sGw9ApNe00EvpvVXn05Y= |
| 服务总线 | /TCLOykE3mgZ8Lxe2/N7VAZAo3pSn5K48y54Xoss4Pw= |
| IoT中心 | xv8FF7ja0QpPHcWE9B1wB3Ge7pLyj0ZvickxQAOdk/Y= |

这里的密钥字符串其实是经过base64编码的，根据base64编码规则，44长度的字符串可以表示33个字节，再去掉末尾用来填充的字符‘=’，那么实际上原本密钥应该是32个字节，这样的话，一个字节是8位，每一位的可能值为0或1，因此，密钥的可能性就是

2^（8\*32）= 2^256

也就是2的256次方，而存储账户密钥的可能性更是多达2的512次方，可想而知，这种情况下要暴力破解，可操作性实在不强。

**问：密钥是否会在传输的过程中被截取？**

**答：**客户可能会有这样的疑问，在客户端使用Azure PaaS的SDK时，一般需要提供连接字符串，或者是密钥直接作为参数，感觉密钥就跟普通的用户名密码一样，会被传输到服务端来做对比验证，因此觉得密钥有可能在传输过程中被截取。

首先，所有的传输都是加密的（SSL\TLS）。但这还不是关键点，更关键的是，密钥其实压根就不会被传输，被用来传输和验证的是令牌（Token）。也就是说SDK拿到提供的密钥，会根据密钥生成相应的令牌，再传输令牌到服务端做验证。而令牌本身是被限制了访问范畴和生命周期的，因此比起密钥的安全性会高得多。

**问：在客户端，密钥无论是明文写在代码里，还是配置文件中，都不安全，有没有更安全的方式？**

**答：**当然有。就跟生活中把贵重物品放在保险箱里一样，我们也可以把密钥放在保险箱里。Azure密钥保管库就是这样一个服务，可以将密钥保存到其中，授权的客户端在需要的时候再从中获取。这样的话，既使得密钥能被集中管理，而且能使密钥管理者和使用者分离，提高了安全性的同时，更提供了便捷性。更多了解Azure密钥保管库，可参阅以下文章：

* [Azure密钥保管库介绍](https://docs.azure.cn/zh-cn/key-vault/key-vault-whatis)
* [Azure密钥保管库入门](https://docs.azure.cn/zh-cn/key-vault/key-vault-get-started)
* [Azure密钥保管库使用](https://docs.azure.cn/zh-cn/key-vault/key-vault-use-from-web-application)

那么除了这种方式之外，还有没有别的办法呢？上一个问题中我们提到通过令牌来认证，也就是说客户端其实不一定要知道密钥，它只要能提供正确的令牌就可以了，因此我们可以创建一个专门生成令牌的集中管理服务，授权的客户端只需要调用这个服务，就可以拿到目标资源的访问令牌，这样也可以避免密钥被客户端显示的知道。当然这种方法需要自己创建一个专门生成令牌的服务，所以比起使用Azure密钥保管库的方式要复杂些。