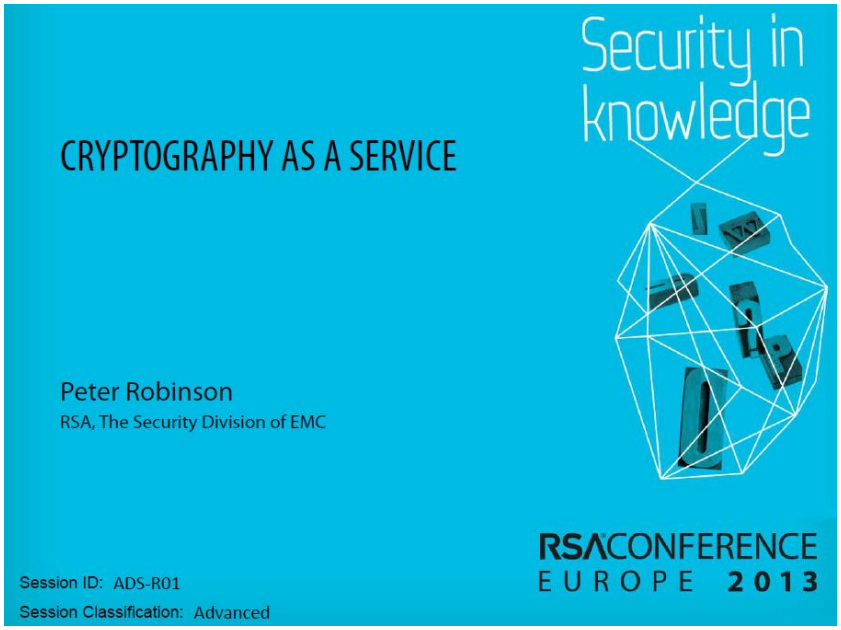
# 解读 RSA 大师第一次提出“密码即服务”的 PPT

(2021 年 5 月 6 日)

云密码服务正在成为一个云计算服务的热点，不仅亚马逊云、微软云、谷歌云、阿里云、腾讯云、华为云等都已经提供云密码服务，密码设备生产厂商、密码系统开发厂商和 CA 机构也都纷纷开始提供云密码服务，这说明大家都已经认识到了要保护云数据安全可信，必须采用密码技术来保障。把密码技术、密码设备和密码系统的密码能力变成云计算服务中的一种资源来提供服务，这就是**云密码服务**。

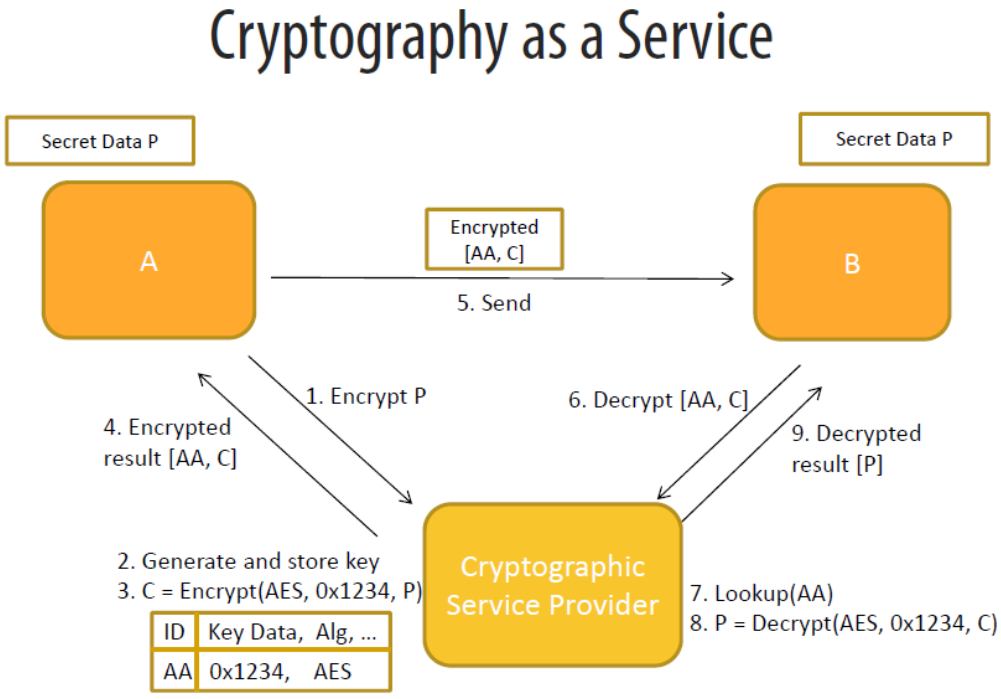
但是，笔者在研究了各家提供的各种形态的云密码服务后，似乎有些迷茫，感觉各种云密码服务大多数都是提供密码设备和密码系统的共享租用服务，有点像云计算服务发展的初期的虚拟主机服务一样，只是提供服务器租用服务。如果我的理解正确的话，则可以类比的认为云密码服务还在发展的初期阶段，都在探索和摸索中。笔者写本文的目的也是希望同云密码服务业界和用户共同探讨我们应该如何发展云密码服务，应该提供哪些云密码服务才能满足用户对密码应用的需求。

带着这个研究题目，笔者在网上找到了“CRYPTOGRAPHY AS A SERVICE”(密码即服务)的演讲 PPT，这是 RSA 高级工程经理 Peter Robinson 第一次在 2013 年 10 月 29-31 日的 RSA 欧洲大会上使用的 PPT，首次提出了“密码即服务(Cryptography as a Service, CaaS)”的概念。笔者认真看了每页 PPT，虽然 PPT 只是列出了大概的演讲内容，但基本上还是能理解 Peter 所讲的核心思想是什么，本文就同大家分享笔者的读后感。



Peter 在第一页 PPT 说明了为何提出“Cryptography as a Service (密码即服务)” ，他认为：将加密密钥部署到诸如智能手机、公共云中的虚拟机和智能电网设备等终端设备中是有安全风险的。所以，本次演讲提出了“Cryptography as a Service (CaaS)”的模型，该模型允许在不暴露加密密钥的情况下执行密码操作，并提出建议如何克服与该技术相关的陷阱。这是业界公认的第一次在大型国际安全专业会议上提出“密码即服务”的概念和应用场景。

Peter 在 PPT 的第 23 页明确地定义了密码即服务：密码服务提供商通过 Web 服务 API 代表终端设备执行密钥加密和解密操作。用于执行这些操作的加密密钥存储在密码服务提供商的密钥管理系统中，终端设备在任何时候都不拥有这些密钥。如下图所示为 PPT 中展示的加解密示意图。




用户 A 要把机密数据 P 发给用户 B，用户 A 就把数据 P 提交给密码服务提供商请求加密 P，密码服务提供商为此生成加密密钥和保管此密钥，并用此密钥加密数据 P 返回给用户 A，用户 A 把密文发给用户 B，用户 B 收到后把密文提交给密码服务提供商请求解密，密码服务提供商用加密密钥解密后把原文数据 P 返回给用户 B。整个过程是用户 A 和 B 都不拥有加密密钥，以此方法来解决加密密钥在终端设备上的安全问题。

Peter 还分析了采用密码即服务后可能的影响，其优势在于改进了密钥的安全，各种不可信的终端上都没有密钥，这些重要的密钥都保存在一个安全的地方-密钥管理系统中。其不足之处有：服务提供商必须有密码基础设施，由于网络延迟使得密码服务可能有延时而影响加解密性能，也有可能密码服务提供商遭遇拒绝服务攻击而导致无法为终端设备提供密码服务。其最大的挑战在于终端设备请求密码服务时的身份认证，其次就是网络连接的随时可用性。

关于密码算法，Peter 建议在一个 Web 服务调用中组合多个密码服务，例如数字签名和加密。并且推荐采用加密消息语法标准(CMS/PKCS＃7)来实现安全消息传递，提供各种标准封装类型，如数字签名和数字信封。

Peter 还用发送签名邮件作为应用示例来说明如何采用密码服务来实现邮件数字签名的。同时， Peter 也提出了智能电网如何管理密钥的解决方案，这是一个云端密钥管理和密钥下发到终端的方案，既解决了用户的密钥管理难题，也解决了仅仅依赖于密码服务而效率太低和对网络要求太高的问题。同时，Peter 也指出这种方式下，应该将密码服务提供商的密钥管理系统的熵混合到终端设备的熵中，以显著提高终端设备上生成密钥的熵质量，将大大提高终端设备上产生密钥的质量。

Peter 最后总结了云密码服务的几个要点：(1) 终端设备不宜生成和存储密钥；(2) 密码服务可以代表终端设备执行加解密服务，而无需将重要的加密密钥暴露给终端设备；(3) 密码服务必须与强身份认证结合使用，可以大大提高系统的安全性；(4) 密码服务不适用于所有密码应用；(5) 虽然密码服务对于某些应用环境(如嵌入式设备)具有挑战性，但是密码服务仍可以在这些情况下使用以提高安全性。

也就是说，Peter 提出“密码即服务”的最初想法就是为了解决密钥安全问题而设计的，是为了解决密钥管理问题。现在看来，密信全自动邮件加密的密钥管理解决方案是非常创新的，虽然我们三年前采用云密钥管理技术来解决邮件加密的难题时并没有看到 Peter 这个 PPT。密信技术之所以能实现全自动邮件加密，正是得益于采用了云密钥管理技术，并且是不同用途的证书采用了不同的密钥管理方式，不仅方便了用户随时随地可以获取加密密钥来解密已加密邮件，彻底解决用户自己管理密钥带来的各种难题；而由于数字签名行为是有法律效力的，所以，签名密钥是在云密钥管理系统的协同下在本地生成和安全保存的。密信 App 在验证了用户邮箱控制权后下发加密密钥，方便用户在本地快速解密已加密邮件，而无需依赖于云密码服务来解密，因为用户每天有大量的邮件需要解密，如果完全仅仅依赖云密码服务，则效率太低，对网络带宽要求比较高，会影响用户体验的，不适合于智能手机中管理加密邮件。这是笔者读了 Peter 的 PPT 后的第一个收获，更加坚信密信基于云密钥管理的邮件全自动加密解决方案是科学的、先进的和创新的。

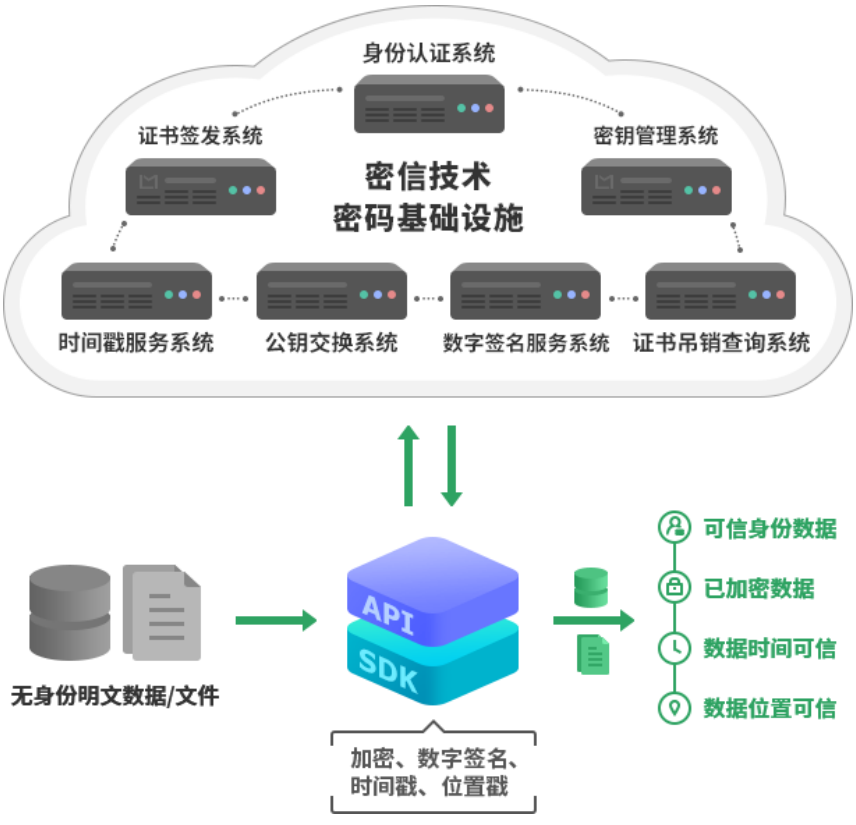
从 Peter 首次在 2013 年提出了“密码即服务”的概念，到现在已经过去了 7 年多，这期间无论是密码服务理论研究和应用实践都做了很多探索，并取得了一定的实际应用成果，已经成为了云计算服务的一个重要组成部分，所以把各种密码相关服务统称云密码服务。密信技术在计划提供云密码服务之前做了一些市场调研，发现用户的确需要密码技术来保障云数据安全和可信，但是绝大多数用户都不懂密码技术，不懂如何编程实现加密、数字签名和时间戳应用，怎

么办呢？

或者说，什么样的云密码服务才是用户所需的服务呢？笔者认为：提供云密码机租用服务不能解决用户的密码应用需求，不仅涉及到不同厂商有不同的技术对接要求，而且更重要的是用户根本就不知道如何编程使用密码机来实现数字签名和加密。用户所需要的是输入“未签名和未加密的数据”一键输出“已签名和已加密的数据”，这才是真正的服务，用户真正想要的密码服务。

密信技术在 3 年前就建设了云密码基础设施，赋能自己研发的客户端软件-密信 App，云端和客户端紧密协同，为全球用户完美提供了全自动邮件加密服务和文档数字签名服务，实现了传统的独立客户端软件不可能实现的各种功能，这是一个技术创新，也是云计算和客户端软件的未来发展方向。现在，密信技术把成熟的云密码基础设施作为一个云密码服务开放给所有互联网应用开发商和服务提供商，把密码能力变成云计算的一种资源服务赋能所有客户端软件和互联网应用，让所有开发商和服务商无需重复投资建设云密码基础设施，而是根据自己的应用需要按需选购密码服务即可。

密信技术以 SDK 或 API 方式交付密码服务，能满足用户业务的数据加密保护(证书加密)、数据身份可信(数字签名)、数据产生和使用时间可信(时间戳)以及数据产生和使用位置信息可信(位置戳)等各种密码应用需求，而用户根本无需懂密码编程技术，只需懂简单的 Web 服务调用即可。



密信云密码服务让用户可以实现快速运用密码能力，助力业务数据安全可信，这不仅满足了用户的密码应用合规要求，而且保护了用户的宝贵的数据资源和数据资产，大大增强了企业的核心竞争力。欢迎选用密信云密码服务。

----------END----------


想联系我讨论此话题？请使用 密信 App（ - ）扫码发加密邮件给我，我一定会回复您的加密邮件。