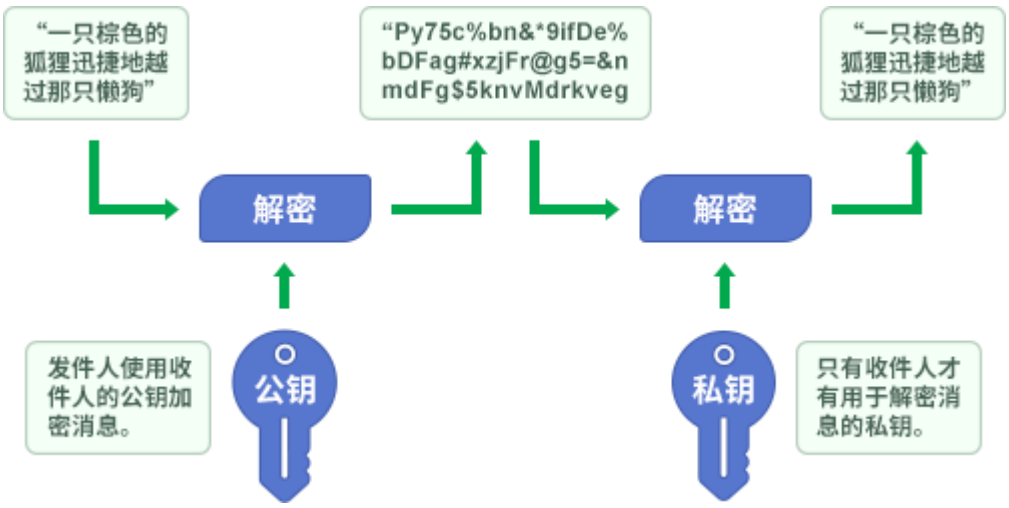
第 3 讲 什么是 PKI/CA？什么是数字证书？

PKI 是公钥基础设施(Public Key Infrastructure)的英文缩写，要解释 PKI 就得先讲一讲什么是公钥和私钥，讲清楚什么是公钥就能理解什么是公钥基础设施。

在密码体系中，有对称加密和非对称加密两种加密方式，对称加密就是用一把钥匙开一把锁，用一个密钥加密，必须用这个密钥去解密。但是，对称加密存在一个如何把密钥安全地传递给对方的难题。打个比方：你给 Word 文件设置了一个口令，打开文件时必须用这个口令，问题来了，你该如何安全地把这个口令告诉对方吗？如果你用微信把文件发给对方，同时又把口令也用微信发给对方，如果这个文件能被第三方窃取的话，则第三方可以同时获得这个 Word 文件和口令，那这个设置的口令就起不到文件保密的作用，等于没有口令。相信有很多读者都是这么干的。

但密码技术不能这么干，因为没有起到加密的作用哦。怎么干？这就出现了非对称加密技术，一个密钥拆成两份，一份称之为公钥，一份称之为私钥，至于如何拆的，我这里就不讲，有点深奥，有兴趣的读者可以自己去查阅资料自研一下。公钥是可以公开的部分密钥，大家都可以拥有，而私钥是不能公开的部分，仅限于密钥拥有人拥有。怎么实现加密呢？发件人用收件人的公钥加密，把明文信息变成了密文，就可以安全地发给收件人了，收件人收到密文后用自己的私钥解密得到了发件人发送的明文信息，这就解决了密钥安全传递的难题。因为公钥是公开的，大家都可以通过各种渠道拿到收件人的公钥或者加密之前双方先交换公钥。



为了证明这个公钥的确属于某个个体(人或物)，则需要中立的可信的第三方用其私钥数字

签名这个个体的公钥，这样大家就相信这个公钥的确是某个个体的，就可以放心地用这个公钥来加密发送机密信息了，并相信收件人一定能用其私钥来解密已加密信息。这个用于给公钥签名的系统就是公钥基础设施，为何不叫公钥系统而叫公钥基础设施呢，大家都知道“交通基础设施”、“水电气基础设施”，类比就应该能知道这个公钥系统太重要了，它是互联网安全的基础，是互联网安全必须的设施，所以才叫“公钥基础设施”。而使用公钥基础设施数字签名后的公钥就是数字证书，为何叫做证书呢？因为数字证书中含有公钥基础设施认证过的身份信息，能有效证明这个公钥的可信身份，所以叫做数字证书，以区分传统的纸质证书。

那为何说这个用于签发数字证书的“公钥基础设施”是互联网安全的基础和必须的设施呢？相信大家心目中的互联网是一个非常复杂的系统，有光纤、交换机、路由器、IP 地址、域名、网站、微信、微博等等，但这些都是表象。其实，整个互联网架构非常简单，就只有两端：一是服务端，也就是现在的云端，还有一个是客户端，也就是用户端，用户上网浏览和网上办事(购物)就是从客户端连接到服务端，中间跑的就是各种代码和文档(文件)，互联网就是这么简单的架构。

为了保障互联网安全，就得保障从客户端到服务端的连接安全，这是基础，连接不安全，什么都白搭，其他的安全防护也是空中楼阁。怎么保障连接安全？那就是美国网景(Netscape)在 1994 年发明的密码技术的最重要的应用-SSL 证书，没有之一，这个发明奠定了互联网连接的安全基础，实现了从客户端到服务端的加密连接，开启了互联网的商业应用，没有这个加密基础，互联网根本就不可能用于商业，不可能用于网上支付，根本无法保证用户的机密信息安全。SSL 证书就是 PKI 系统签发的数字证书的一种，是整个互联网架构中离不开的安全基石。

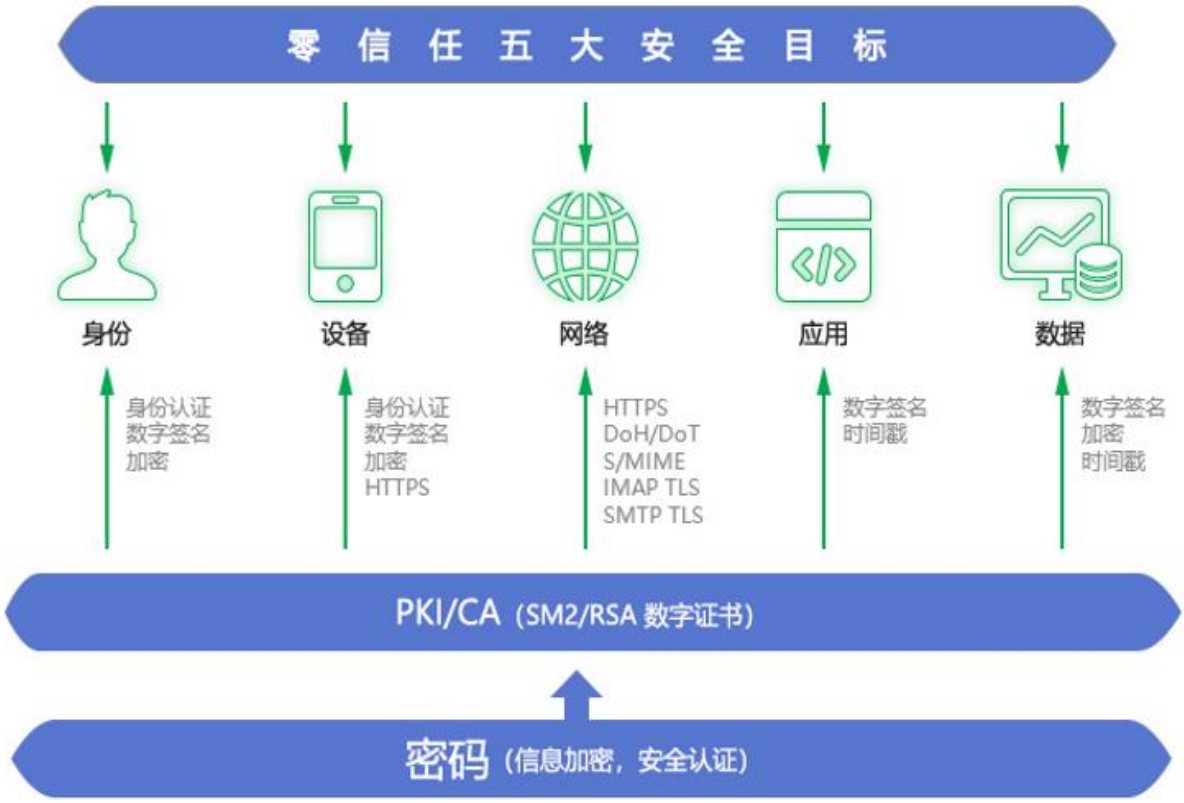
PKI 系统签发的第二种数字证书就是客户端证书了，SSL 证书用于证明服务端的 Web 服务器的身份和用于加密连接，而客户端证书则用于证明客户端的身份和加密连接，目前各个国内 CA 机构签发的 USB Key 证书就是客户端证书，还有用于电子邮件加密的电子邮件证书也属于客户端证书。第三种数字证书是代码签名证书，用于数字签名各种在两端连接中运行的代码，

如果代码没有数字签名则无法保证代码的合法身份，在 Windows 系统中是不允许安装的。第四种数字证书是文档签名证书，用于数字签名各种电子文档，常见是 PDF/OFD 版式文件，如电子合同、电子发票。其他各种证书如物联网证书都可以归类到以上讲的四种数字证书类型中。

SSL 证书，现在国际上也称 TLS 证书，这是因为 SSL 协议已经被淘汰了，现在用的是 TLS 协议，但作为一种证书产品，我国还是继续延用老名词—SSL 证书，这与实际使用 SSL 协议还是 TLS 协议没有关系，只是一种约定俗成的产品名词而已，没有必要改名。SSL 证书、客户端证书、代码签名证书和文档签名证书这四种数字证书保障了整个互联网的安全可信，包括连接安全(网站安全)、应用安全、文档安全、邮件安全和身份可信等，这就是为何称之为公钥基础设施的原因，它太重要的，离开了它互联网就玩不转了，就像我们离不开水电气基础设施一样。

再简单讲一下 CA，CA 是 Certificate Authority (证书颁发机构)的简称，就是运营 PKI 系统的机构，一个负责使用 PKI 系统为用户签发各种数字证书的机构。CA 有时也指 CA 系统，实际上是指 PKI 系统加上一些证书管理功能的系统，有时统称为 PKI/CA 系统，所以，一般用 CA 机构来指使用 PKI/CA 系统签发各种数字证书的单位。

PKI/CA 系统是采用密码技术签发数字证书用于信息加密和安全认证的系统，密码算法可以是 RSA 算法或 SM2 算法，PKI/CA 系统签发的四类数字证书用于实现零信任安全的五大安全目标：身份可信、设备可信、网络安全、应用安全和数据安全，从而保障全球互联网安全。



最后需要特别讲一下的是，目前全球互联网所依赖的公钥基础设施、网络基础设施和各种应用系统都是基于 RSA 密码体系建设的，如果从 SSL 证书发明开始计算，这些基础设施已经在全球范围建设和运行了将近 30 年，可以说互联网中的任何一个元素都已经完美地集成了采用 RSA 密码体系的 PKI 技术，并已成功保障了全球互联网的安全可靠运行。所以，读者现在应该能理解我国正在进行的基于国产密码体系的系统改造(密改)有多难了，一个已经成熟运行了 30 年的体系要实现替代难度非常大，这就像要把一个已经运行了 30 年的城市供水管网系统的所有水管全部都换成新的水管一样的难度。所以，采用基于商用密码体系的公钥基础设施来保障我国互联网安全任重道远，必须探索一条快速实现改造的新路子，这也算是留给读者的一个思考题，笔者也会同大家一起思考和探索这个难题。

-----下一讲内容预告-----

第 4 讲 什么是 SSL 证书？什么是国密 SSL 证书？

从本讲开始重点讲 SSL 证书和 HTTPS 加密，这是全球互联网安全的基础，也是国外 CA 机构和国外互联网巨头抢占的制高点，非常值得我国 CA 机构和我国互联网巨头们借鉴。

王高华

2023 年 2 月 20 日于深圳

请关注公司公众号，实时推送每一期精彩讲座。