资讯保安动画 - 公开密码匙基础建设（旁白）

公开密码匙基础建设

公开密码匙基础建设（Public Key Infrastructure，PKI）提供安全可靠的环境在互联网上进行电子交易，这保安架构主要利用公匙加密技术来保障资讯的保密性、完整性、真确性及不可否认性。

核证机关与数码证书

公开密码匙基础建设的有效运作十分依赖核证机关（certificate authority, CA）的支援。核证机关的主要工作是以一个可信靠的第三者身分来核证进行电子交易双方的身分。

数码证书是以电子形式发出的证书，其所储存的数据可用以核实证书拥有人的身分。证书通常包含的资讯包括用户的公开密码匙、姓名及电子邮件地址等。

当注册机关（registration authority, RA）核实申请人的身分后，

核证机关便会向申请人发出一份经该机关数码签署的证书副本，并在公开目录登记该申请人的公开密码匙。

证书撤销清单（Certificate Revocation List, CRL）是一份由核证机关定期发出的清单，清单上载列在届满日期前被撤销或暂时吊销的证书。在使用他人的公开密码匙前必须核实该密码匙是否有效，以防止无效的证书被滥用。

公匙加密技术

公匙加密技术涉及为每个用户提供一对密码匙，分别是用户自己保管而不可随便向外公开的私人密码匙（private key），以及可以对外公开的公开密码匙（public key），这一对不同但互相配对的密码匙将相关的数据加密，以确保讯息的机密性。例如，若使用公开密码匙加密数据，只有使用与其相配的私人密码匙才能解密。

以传递电子邮件讯息为例，寄件人可以透过使用收件人的公开密码匙，把要寄出的电子邮件内容加密。收件人收到电子邮件后，便一定要使用自己保管而与该公开密码匙配对的私人密码匙，才可把邮件解密。这样便可以确保电子邮件内容的保密性。

另外，为了确保该电子邮件的完整性、真确性及不可否定性，寄件人会将电子邮件的内容利用数学算法产生资讯摘要（message digest），并以自己的私人密码匙加密形成数码签署，然后将电子邮件连同数码签署发送给收件人。

当收件人收到电子邮件后，会利用寄件人相应的公开密码匙核对该数码签署是否有效，以及以相同数学算法产生的资讯摘要，来核实该电子邮件是否有效。这样，收件人便可以肯定该电子邮件确实来自寄件人，确认该电子邮件的真确性；同时，寄件人亦不能否认曾经签署该电子邮件，确保电子邮件的不可否定性。

想知道更多有关资讯保安的资料，请浏览「资讯安全网」：

http://www.infosec.gov.hk