一种CA私钥的容侵保护机制

http://www.firstlight.cn 2008-05-18

保护CA私钥的安全性是整个PKI安全的核心。基于RSA公钥算法和(t, n)门限密码技术，采用分阶段签名方案，确保私钥在任何时候都无需重构。同时，在私钥产生、分发及使用过程中,即使部分系统部件受到攻击,也不会泄漏CA的私钥，CA仍可以正常工作(即系统具有一定的容侵性)。通过VC和Openssl对系统进行了实现。

存档文本