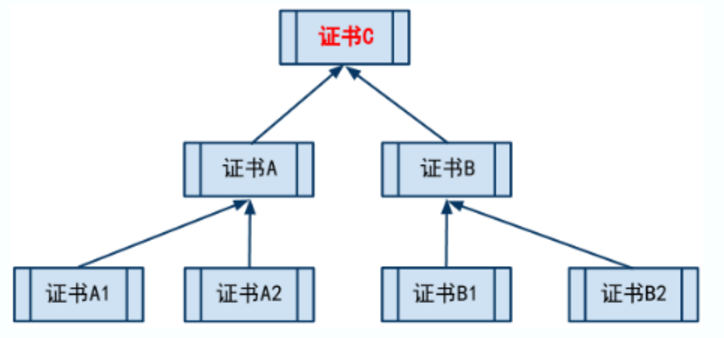
CA

1.简介

　CA是Certificate Authority的缩写，也叫“证书授权中心”。它是负责管理和签发证书的第三方机构，就好比例子里面的中介——C 公司。一般来说，CA必须是所有行业和所有公众都信任的、认可的。因此它必须具有足够的权威性。就好比A、B两公司都必须信任C公司，才会找 C 公司作为公章的中介。

2.根证书

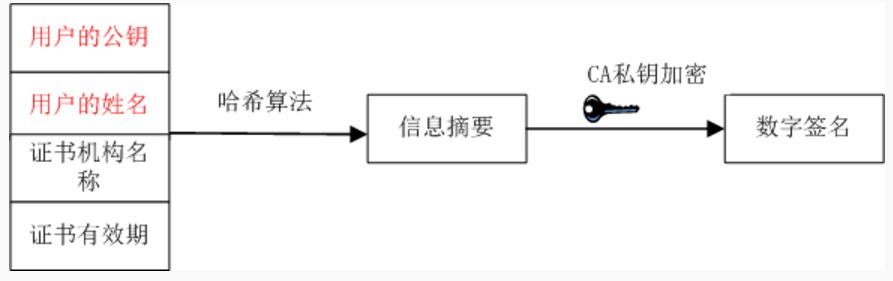
根证书”的洋文叫“root certificate”假设 C 证书信任 A 和 B；然后 A 信任 A1 和 A2；B 信任 B1 和 B2。则它们之间，构成如下的一个树形关系（一个倒立的树）。



处于最顶上的树根位置的那个证书，就是“根证书”。除了根证书，其它证书都要依靠上一级的证书，来证明自己。那谁来证明“根证书”可靠捏？实际上，根证书自己证明自己是可靠滴（或者换句话说，根证书是不需要被证明滴）。

3.ca证书

使用用户身份信息生成数字签名



用户身份信息和数字签名一起组成数字证书

