

网络空间安全导论 · Ch11

计01 容逸朗 2020010869

Q1.

一个典型的 PKI 应用系统由哪几部分组成？

- 通常由终端实体用户、证书认证机构（CA）、证书注册机构（RA）、证书数据库和安全服务器组成。

Q2.

认证机构 CA 的职能有哪些？

- 主要功能是发放和管理数字证书；
- 产生自身证书并传输给安全服务器；
- 验证用户的身份，产生、分配并管理 PKI 架构下的所有用户的证书；
- 负责用户证书的黑名单登记和发布。