一个典型的 PKI 应用系统由哪几部分组成

用户，证书认证中心（CA），证书注册机构（RA）和证书数据库。

1. 用户：PKI 应用系统中的用户是指需要使用和管理数字证书的个人或实体。用户可以包括个人用户、组织、企业等。他们需要向证书认证中心（CA）提交证书请求，获取数字证书，并使用数字证书进行身份验证和加密通信等操作。
2. 证书认证中心（Certificate Authority，CA）：CA 是 PKI 系统的核心组件之一，负责颁发和管理数字证书。CA 验证证书请求者的身份，签发包含公钥和身份信息的数字证书，并对这些数字证书进行签名。CA 是 PKI 系统的信任根，其他实体依赖于 CA 的信任来验证和接受数字证书。
3. 证书注册机构（Registration Authority，RA）：RA 是 CA 的辅助机构，负责处理证书请求和验证申请者的身份信息。RA 可以进行身份验证、收集必要的数据，并将这些数据提交给 CA 进行证书签发。RA 可以帮助减轻 CA 的工作负担，并加强对证书请求者身份的验证和审查。
4. 证书数据库（Certificate Database）：证书数据库用于存储已签发的数字证书。它是一个中央数据库或仓库，包含由 CA 签发的所有数字证书。其他实体可以通过访问证书数据库来获取需要的数字证书，以进行验证和身份认证等操作。

这些组成部分共同构成了一个典型的 PKI 应用系统。用户通过向 CA 提交证书请求获取数字证书，然后使用数字证书进行身份验证和加密通信等操作。CA 负责验证用户的身份，颁发数字证书，并对数字证书进行签名。RA 在协助 CA 处理证书请求和验证用户身份时发挥重要作用。证书数据库存储已签发的数字证书，为其他实体提供访问和获取数字证书的功能。整个系统的目标是确保数字证书的安全性、可信度和合法性，从而实现安全的身份验证和保护通信的目的。

认证机构 CA 的职能有哪些

在 PKI 体系中有一个公认的、值得信赖的且公正的第三方机构，它就是负责颁发及撤销公钥证书的 CA。颁发及撤销数字证书是 CA 的核心功能，具体来说，CA 的职能包括用户注册、颁发证书、注销证书、恢复及更新密钥等。

1. 用户注册：CA 负责验证证书请求者的身份信息。用户在向 CA 提交证书请求时，CA 会进行身份验证和身份信息收集，以确保申请者的身份合法和真实。
2. 证书颁发：CA 根据验证用户身份的结果，签发数字证书。数字证书中包含了用户的公钥和身份信息，并由 CA 进行数字签名。颁发证书后，CA 将证书分发给用户，供其在 PKI 体系中进行身份验证和加密通信等操作。
3. 证书注销：在某些情况下，用户可能需要注销其证书，例如证书过期、用户丢失私钥、用户不再需要证书等。用户向 CA 申请注销证书，CA 会在确认用户身份合法性后，将该证书标记为注销状态，并将该信息传播给相关的实体。
4. 证书恢复：当用户的证书被意外注销或者过期后，用户可能需要申请证书的恢复。CA 会对用户的身份进行再次验证，并在验证通过后重新颁发证书，使用户能够继续使用数字证书进行安全通信。
5. 密钥更新：为了保持安全性，用户的密钥需要定期更新。用户向 CA 申请更新密钥，CA 会验证用户的身份，并重新颁发具有新密钥的证书，以确保用户可以使用最新的密钥进行加密和解密操作。

除了上述职能外，CA 还承担着证书撤销列表（Certificate Revocation List，CRL）的管理和发布，用于指示已被注销或无效的证书列表。CA 还可能提供其他辅助服务，如安全策略制定、密钥管理、证书生命周期管理等，以支持 PKI 体系的运行和安全性。