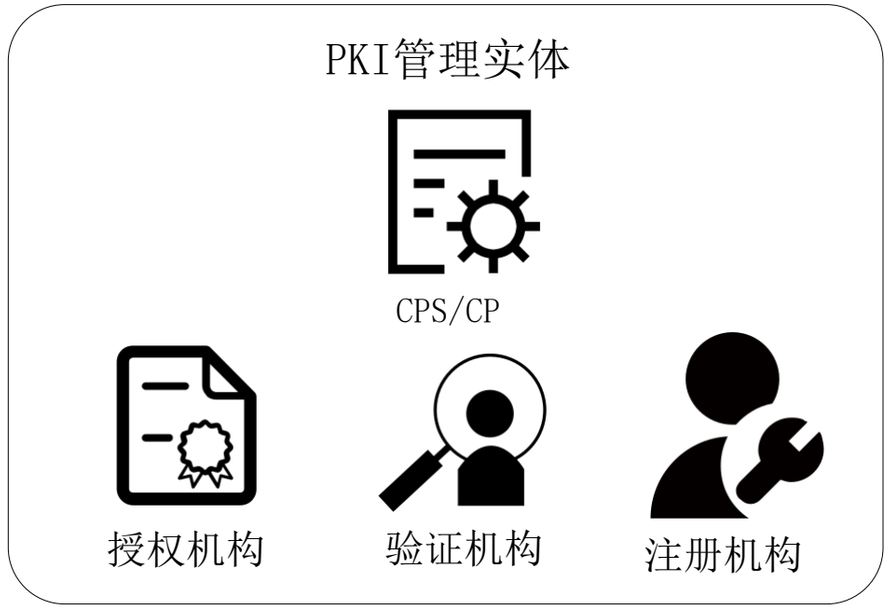
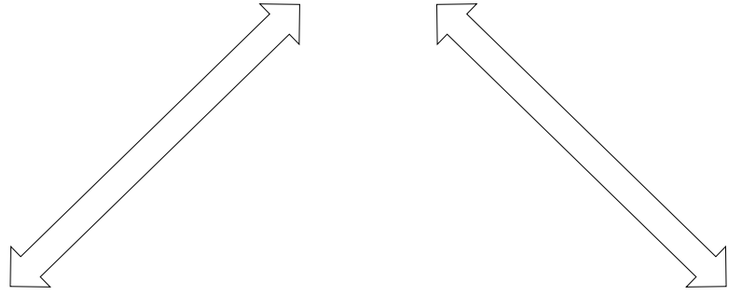
- 注册机构(RA)：执行身份验证和处理新的数字证书请求、更新数字证书请求和吊销数字证书请求，并将这些请求递交给授权机构。
- 授权机构(CA)：创建和发布数字证书以及管理证书吊销列表（CRLs)。
- 验证机构(VA)：检查数字证书的有效性，当证书的签发者和证书的状态管理服务由不同的实体提供时，将使用到VA。



- 证书策略(CP)：一组安全规则要求，适用于一类应用系统的共同安全需求。
- 认证运作规范(CPS)：述CA提供数字证书服务的规则和处理方式，其中可能会包括提供服务描述，证书生命周期的管理细则、业务信息、法律义务和金融责任等。

- 用户：证书书持有者，向PKI管理实体申请证书并在通信过程中发送给依赖方。



- 依赖方(Relay)：接收、验证数字证书的有效性，并使用其完成信息的安全交换。