- 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。

PKI管理实体

CPS/CP

受权机构

Example 1

Example 2

Example 2

Example 3

Example 4

Example 5

Example 6

Example 6

Example 7

Example 7

Example 6

Example 7

Example 7

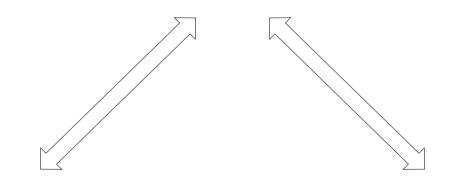
Example 8

Example 9

Example 9</t

- 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。



