Attribute certificate tasks in Certificate Manager

This article lists the attribute certificate (AC) tasks that are done by registration officers in Smart ID Certificate Manager (CM), using both the Registration Authority (RA) in Certificate Manager and the Certificate Controller (CC) in Certificate Manager.

- Issue attribute certificate in Certificate Manager
- Revoke attribute certificate in Certificate Manager

About attribute certificates

Attribute certificates are signed objects that assert additional properties with respect to some identity certificate (also called base certificate). An attribute certificate has no associated key pair and consequently cannot be used to establish identity.

Attribute certificates can be thought of as extensions to identity certificates, even if the attribute certificate may be signed by a different CA than the base certificate. When the associated attributes are mainly used for the purpose of authorization, an attribute certificate is called **authorization certificate**. Attribute certificates typically have a much shorter lifetime than X.509 certificates.

Smart ID Certificate Manager supports attribute certificates version 2, as specified in RFC 3281, as well as the ***No Revocation Available*** (`NoRevAvail`) extension as specified in RFC 5755. An attribute certificate format with this extension is included in the Certificate Manager installation. An attribute certificate with the `NoRevAvail` extension is not possible to revoke.

Related information

- Certificate Manager clients
- Smart ID Certificate Manager
- Registration Authority operation in Certificate Manager