Knowledge Base Article

Document details – Creation of public key object on the eToken

Publish Date -
Revision – 1
Author – Yoni Salman

Classification

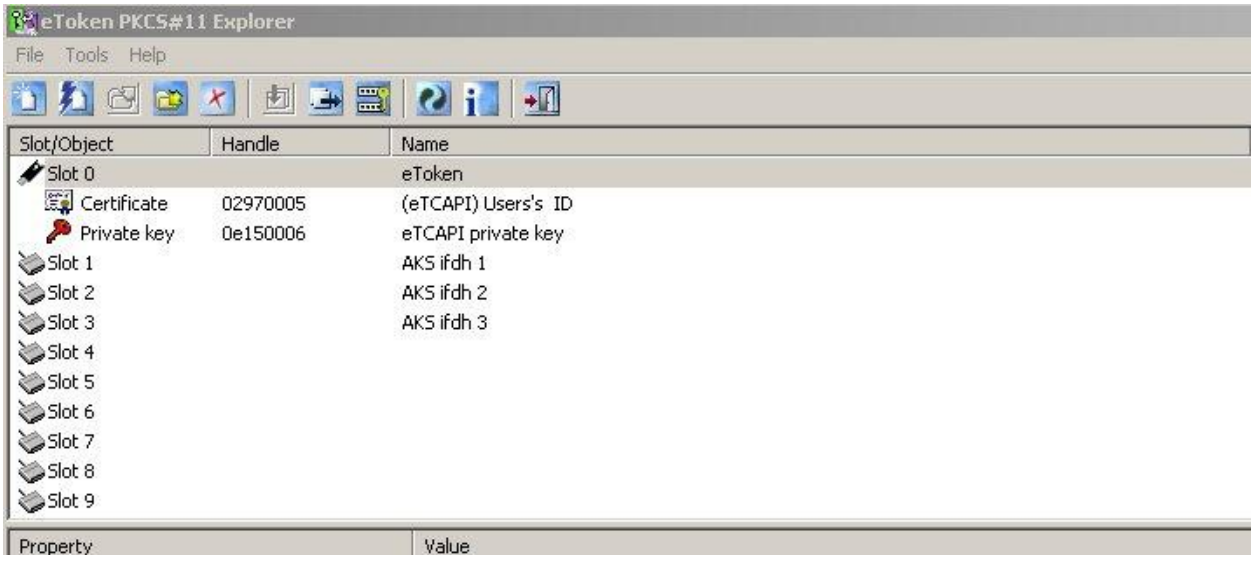
Affected products – PKI Client, SAC, token.
Keywords – Public key, token, CAPI,PKCS#11.

Problem description: When enrolling certificate to the token with CAPI, the public key object is not restored on the token, and cannot be retrieve with PKCS#11 API.

Problem solution: When enrolling certificate to a token with CAPI, 2 PKCS#11 objects are created on the token, the private key and the certificate.
The PKCS#11 public key is not created on the token; the public key material is part of the certificate and can be extracted from the X509 certificate using MS helper functions or a deferent API that can extract the public material.

Examples:

1. **When enrolling token with MSCA, only privet key and certificate objects are created on the token.**



2. **When enrolling token with FireFox (PKCS#11) 3 objects are created on the token: Certificate, public key and private key.**