



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.

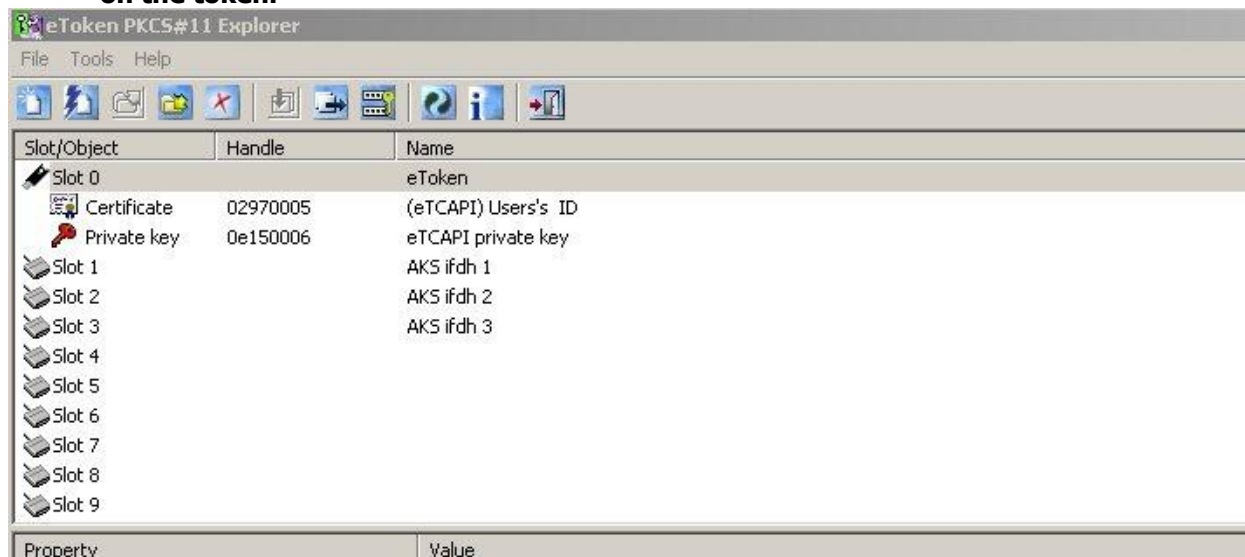
Problem description: When enrolling certificate to the token with CAPI, the public key object is not restored on the token, and cannot be retrieve with PKCS#11 API.

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.



The screenshot shows the 'eToken PKCS#11 Explorer' window. It has a menu bar (File, Tools, Help) and a toolbar with various icons. Below the toolbar is a table with three columns: 'Slot/Object', 'Handle', and 'Name'. The table lists objects in Slot 0 and Slot 1 through Slot 9.

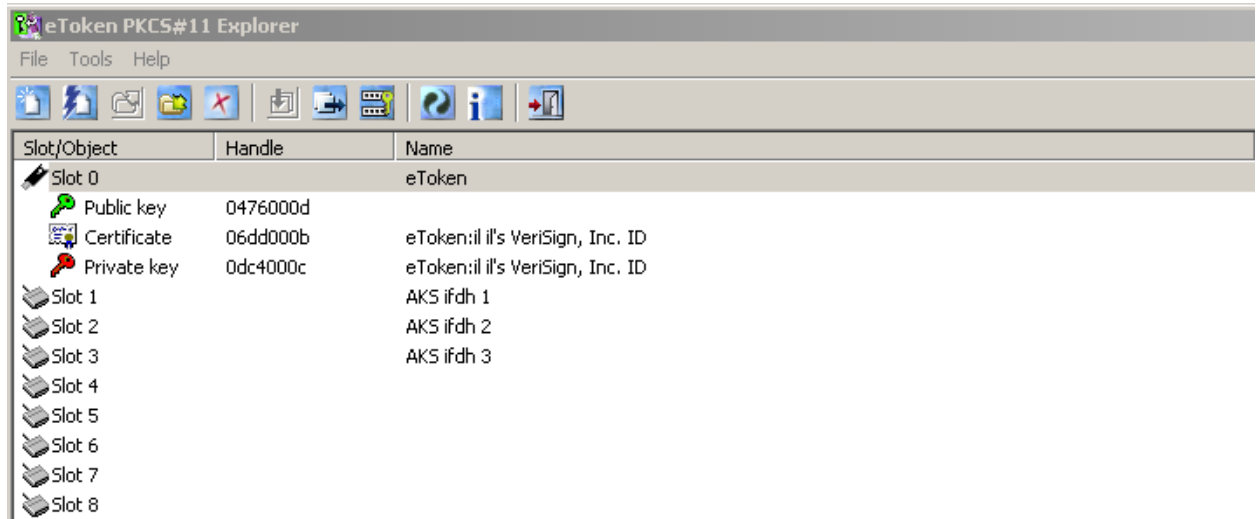
Slot/Object	Handle	Name
Slot 0		eToken
Certificate	02970005	(eTCAPI) Users's ID
Private key	0e150006	eTCAPI private key
Slot 1		AKS ifdh 1
Slot 2		AKS ifdh 2
Slot 3		AKS ifdh 3
Slot 4		
Slot 5		
Slot 6		
Slot 7		
Slot 8		
Slot 9		

Below the table is a 'Property' and 'Value' section.



Knowledge Base Article

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



The screenshot shows the 'eToken PKCS#11 Explorer' window. It has a menu bar (File, Tools, Help) and a toolbar with icons for file operations and token management. Below the toolbar is a table listing the objects on the token.

Slot/Object	Handle	Name
Slot 0		eToken
Public key	0476000d	
Certificate	06dd000b	eToken:il il's VeriSign, Inc. ID
Private key	0dc4000c	eToken:il il's VeriSign, Inc. ID
Slot 1		AKS ifdh 1
Slot 2		AKS ifdh 2
Slot 3		AKS ifdh 3
Slot 4		
Slot 5		
Slot 6		
Slot 7		
Slot 8		