USING THE EID CARD IN ENTRA ID ENVIRONMENT

Technical overview

Document Information	
Creation time	24.12.2024
Contracting authority	RIA
Author	Urmas Vanem, OctoX
Version	25.01/1

Version info		
Date	**Version**	**Changes/Notes**
01.01.2025	25.01/1	Public version

Introduction

Estonian ID-cards[1] can also be used in Microsoft Entra ID cloud services to authenticate the user. This can be useful if we want to provide access to Entra ID services securely and password-free.

Today, unfortunately, it is not yet possible to log in to a computer connected to the Entra ID cloud with an ID-card[2], but contacting cloud services with web browsers is already working.

[1] The concept of ID-cards in this context refers to ID-cards more broadly – ID-cards, digital ID cards and other ID1 format cards issued in Estonia, which are carriers of electronic identity.

[2] Allegedly, today, 01.01.2025, ECC certificates for logging into a computer connected to the cloud are not yet supported.

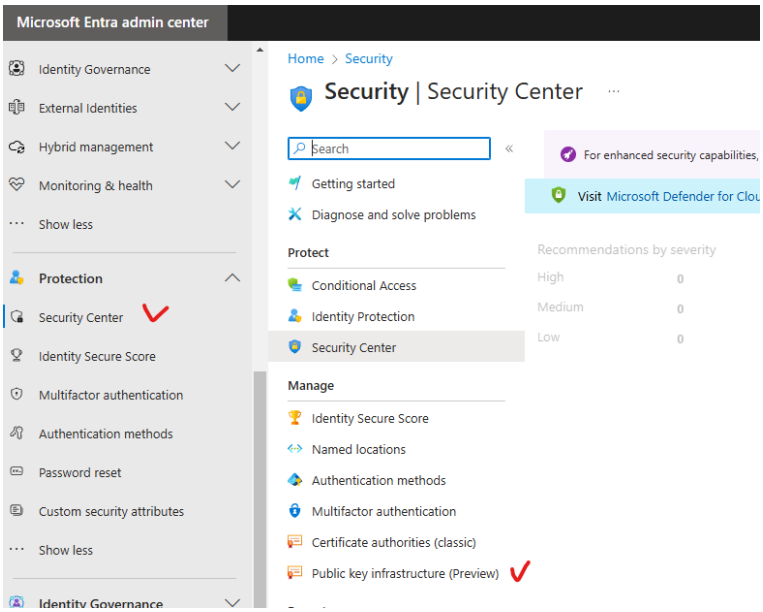
Configure the opportunity

Linking eID root certificates to the Entra ID solution

The eID root certificate, the intermediate certificate, and also the associated CRLs can be downloaded from the website https://www.skidsolutions.eu/resources/certificates/.

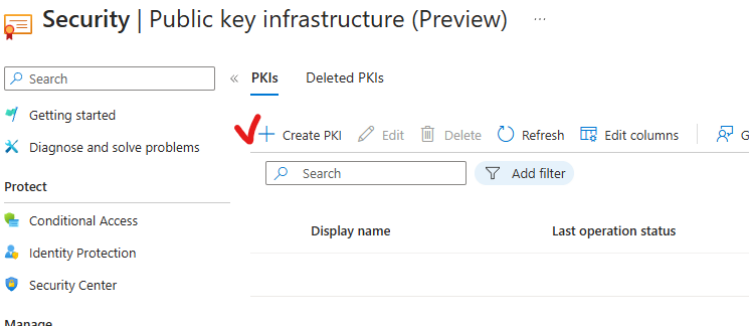
To associate them with the Entra ID solution, you must log on to the Entra Administration Center in the Policy *Administrator role*. To link certificates:

1) Select *Protection*, if necessary, click *on Show More* and now select *Security Center.* From the window that opens on the right, select *Public Key Infrastructure (Preview).*



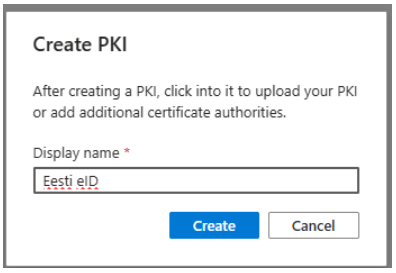
Picture 1 - path to PKI configuration

2) In the window that opens, click *on Create PKI:*



Picture 2 - Initial view of the PKI window

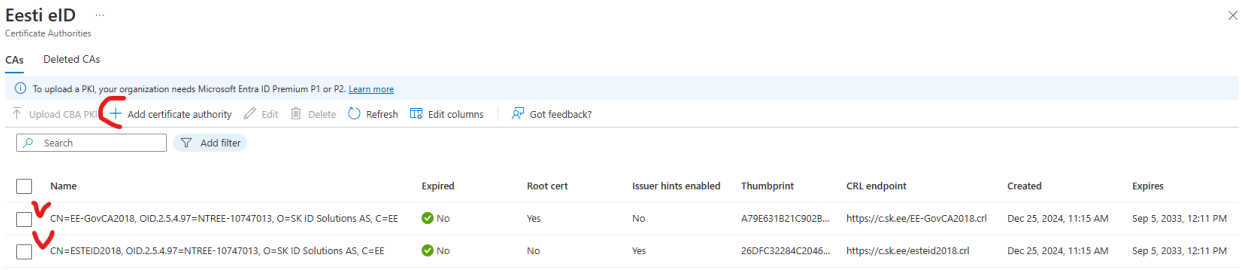
3) Assign a suitable name to the PKI configuration (here Eesti eID) and click OK.



Picture 3 - Naming PKI configuration

4) Open the newly created configuration item and add the eID root and intermediate certificate here. Also add CRL paths:
    a. On the root level certificate, this is https://c.sk.ee/EE-GovCA2018.crl;
    b. And for the intermediate level, https://c.sk.ee/esteid2018.crl.

In the case of a root-level certificate, it is also marked with the Root cert property . *And on the mid-level certificate, enable Issuer hints.*



Picture 4 - Estonian Eid configuration

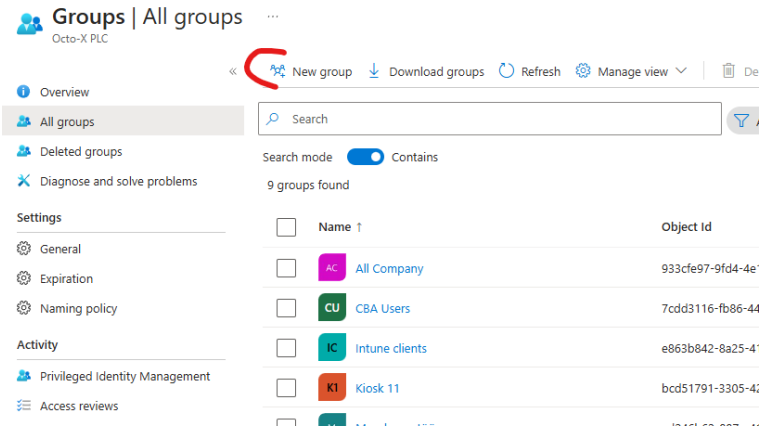
Now eID certificates are reliable for us in the Entra ID environment view.

Enable certificate-based authentication

To enable certificate-based authentication, first create a group of users who want to enable this authentication method. Of course, it can also be immediately enabled for all users, but to check the correct functioning at least during the implementation phase, I still recommend starting with a few individual users.

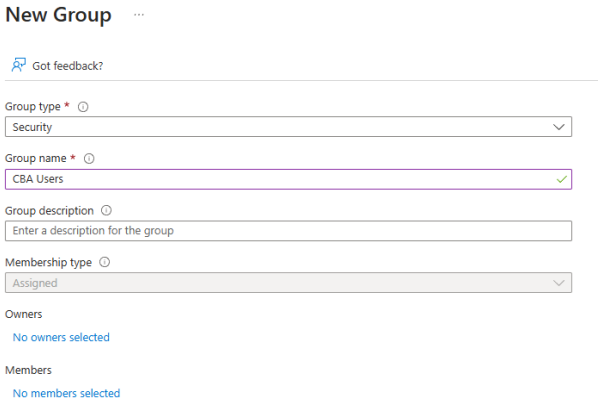
Steps:

1) Log in to the Administration Center as *Authentication Policy Administrator*;
2) To create a group, select *Groups / All Groups* and click *on New Group:*



Picture 5 - groups view

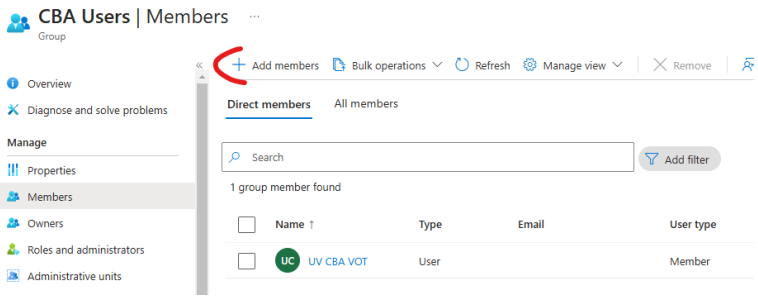
3) Configure the group, specify the name (in our example, CBA Users) and, if desired, add a description. Click *Create.*



Picture 6 - group configuration

4) Add to the group the users to whom you want to enable authentication with an eID card.[1] Open the newly created group, select *Members* and click on the Add Members button *:*

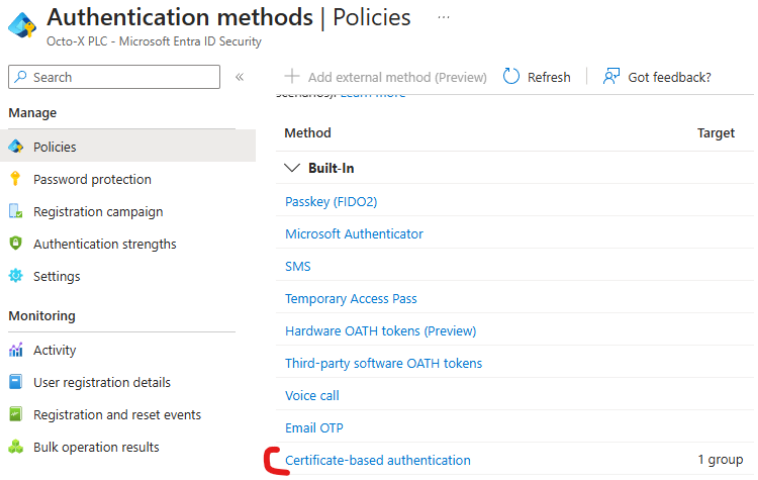
[1] Of course, you can also do this while creating a group using *the No Members Selected* button.



Picture 7 - adding members to a group

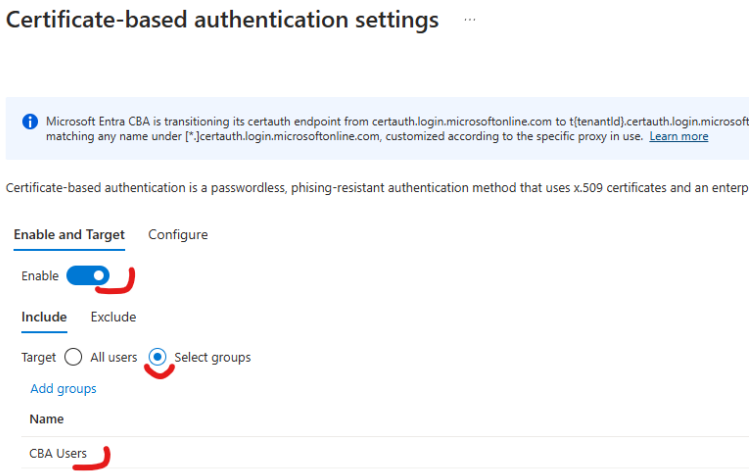
In this example, we have added the user "UV CBA VOT" to the group.

5) To enable certificate-based authentication for group members, now select *Protection / Authentication Methods* and click *on Certificate-based Authentication:*



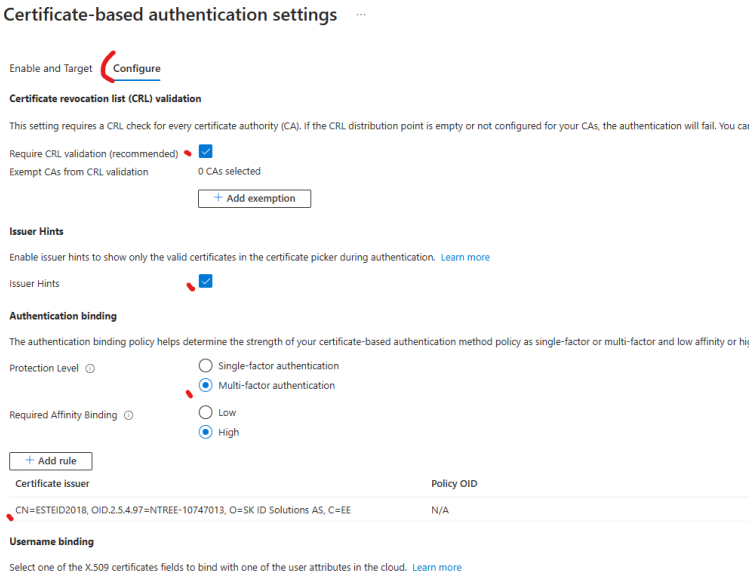
Picture 8 - CBA selection

6) Enable CBA and apply it to the group created from the previous paragraphs:



Picture 9 - Enabling and directing CBA

7) To configure the CBA, now click on *Configure*:



Picture 10 - CBA configuration view

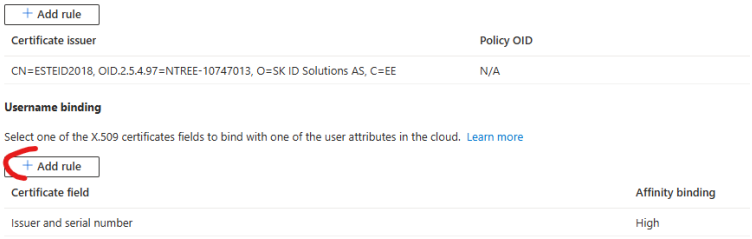
We can create different configurations. In this window we have indicated that:

- We wish to check the validity of certificates against the revocation list[1];

[1] However, I must point out here that, under certain circumstances, certificate-based authentication may not work if we require certificates to be checked against the revocation list. The problem here may be that only the OCSP path is described in the certificates themselves – it is known that Entra ID is not yet able to verify the validity of certificates in this way. In case of problems, do not make this claim if possible.

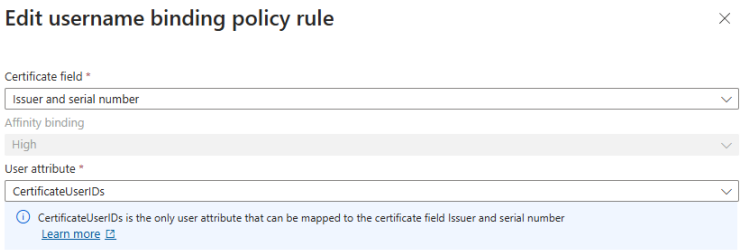
- We only show the user certificates that are issued from the intermediate level CA that we have specified;
- We use multi-factor authentication relationships;
- We trust only certificates issued by our intermediate level CA.

8) To bind a user to a certificate, you now need to move slightly down in the same window and select *Add rule* in the *Username Binding section:*



Picture 11 - creating a rule

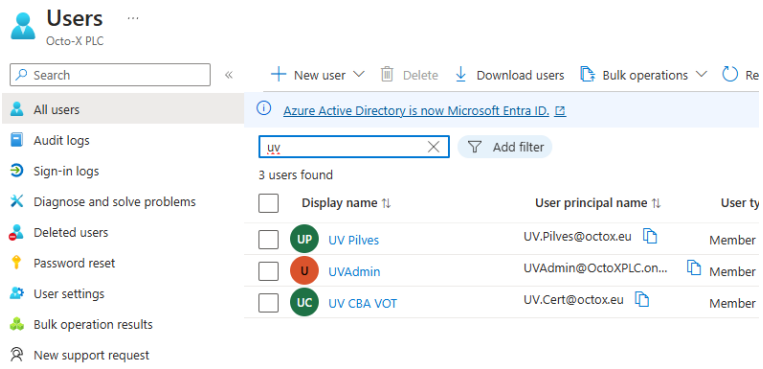
In our sample rule, we create a relationship between the user and the certificate using the *Issuer* and *Serial number* fields of the certificate. We describe these fields in the following point on the user's *CertificateUserID attribute.*



Picture 12 - creating a policy of user and certificate relationships

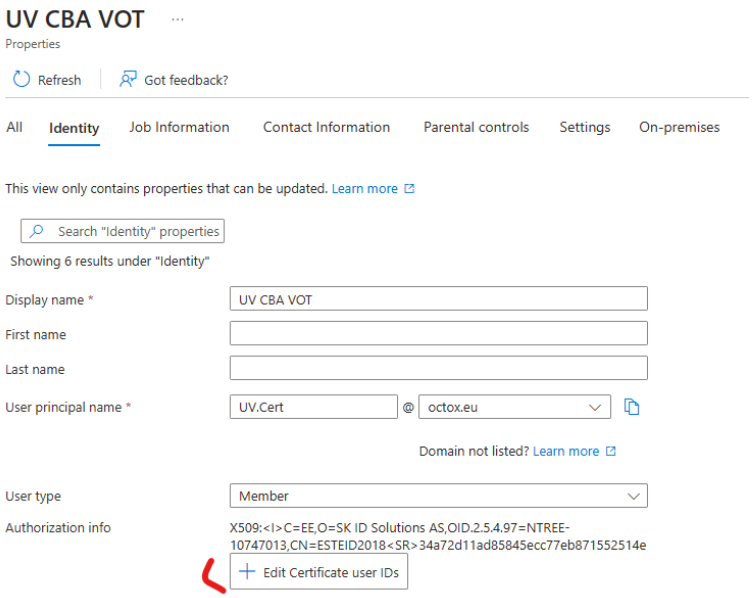
I also note that it is possible to create different user and certificate relationships, as well as several policies can apply at the same time. An example given here is our tested recommendation for linking eID certificates to the Entra ID user.

9) In order for the solution to truly understand that this particular certificate is related to that particular user, we need to add the data in the certificate to the CertificateUserID attribute for the user. To do this, we first open the users view by selecting *Users / All Users,* then click on the user we are interested in (in our example, UV CBA VOT).



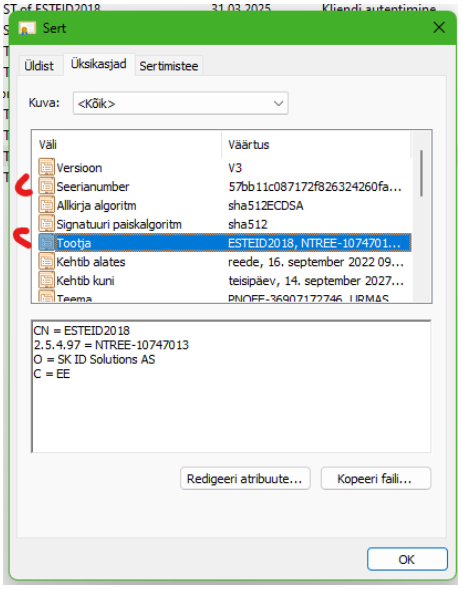
Picture 13 - user view in Entra IDs

10) In the user's view we will be able to click on the *Edit Properties button*, as a result of which we can modify the user object if we wish. At the moment, we want to change the content of the user's CertificateUserID attribute and for this we will in turn click on the Edit *Certificate in user IDs*:



Picture 14 - user configuration window

11) Now in the window that opens, we will add here the fields Issuer and SerialNumber, taken from the certificate. When we open the certificate we will see these fields in the details window:



Picture 15 - Certificate Issuer

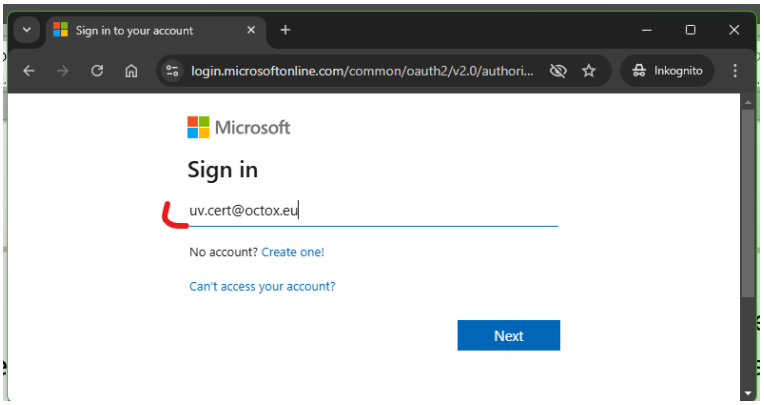
The value must be added in the format: X509:<I>C=EE,O=SK ID Solutions AS,OID.2.5.4.97=NTREE-10747013,CN=ESTEID2018<SR>34a72d11ad85845ecc77eb871552514e

IMPORTANT! The serial number must be inverted by two symbols for the solution to work. In other words, if the series number read in the certificate is 4e51521587eb77cc5e8485ad112da734, then it must be used inverted 34a72d11ad85845ecc77eb871552514e.

And our configuration is ready to authenticate the user with the "UV CBA VOT" eID card certificate against Entra ID services.

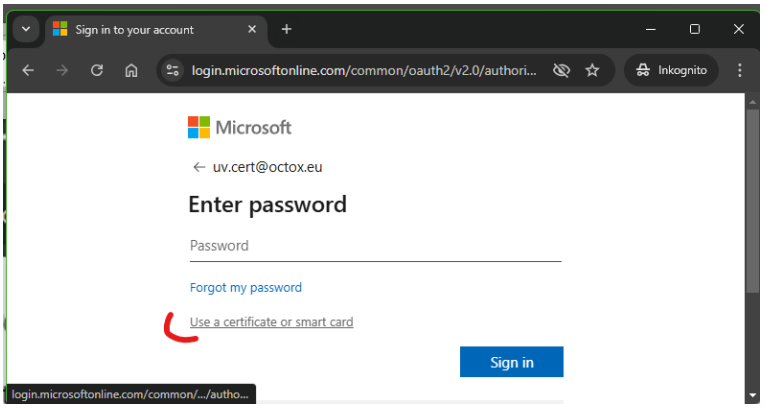
Use

To use the solution, you must now turn to our Entra ID cloud services over the browser. For testing it is convenient to use, for example, the site https://myapps.microsoft.com/. When we first go there, we will be asked for the username as usual (we will use the technical, e-mail name of our test account here):



Picture 16 - logging into web services, entering a username

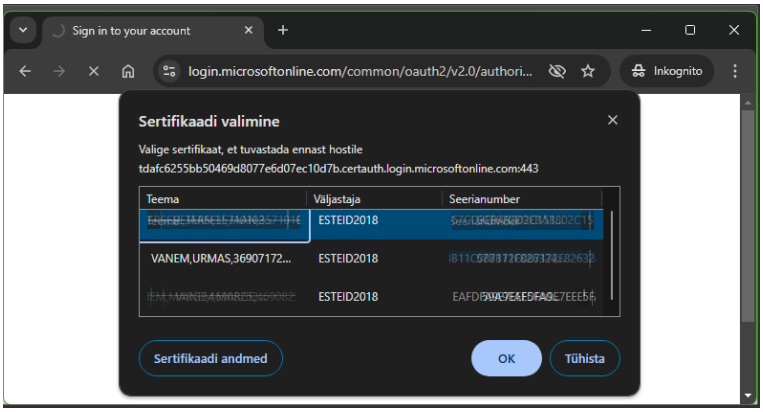
After *clicking Next*, we will have the opportunity to use certificate-based authentication in the next window that opens:



Picture 17 - I can choose authentication with a certificate instead of a password

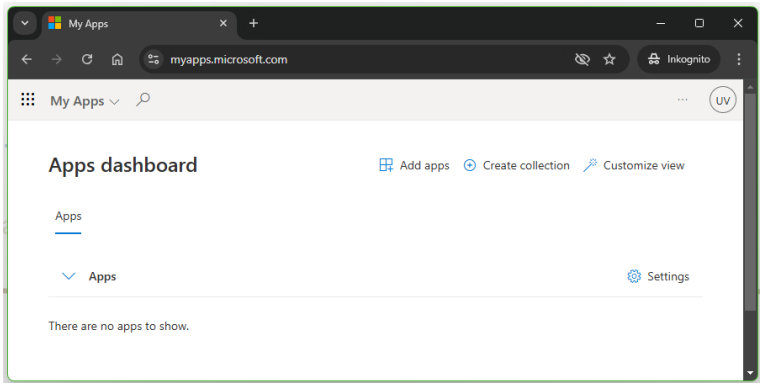
I also note here that after enabling certificate-based authentication in your organization, this option is offered to all users when logging in, including those who cannot actually do so.

Now, by clicking on the Use *a certificate or smart card* button , I am offered all the certificates registered on the computer and issued by our previously described mid-level CA:



Picture 18 - certificate selection

And after entering the PIN code, we will be allowed access to Entra ID services.



Picture 19 - Entra ID Myapps portal

Happy use!