Smart Card User Guide

19.5.2021

Table of contents

19.5.2021

Smart Card User Guide

1 Smart card

The Digital and Population Data Services Agency (hereinafter DVV) issues smart cards containing personal certificates. The PINs required for the use of the card are personal and the card holder's identity must be verified in order to receive them. The card holder must verify that the information on the smart card is correct and that the PIN envelope has not been opened when they receive the smart card and PIN envelope.

The card holder must store the PINs in a safe place.

The terms and conditions and other information related to the smart card are available on the following webpage: https://dvv.fi/en/for-organisations. The terms and conditions are described in the certificate policy documents.

1.1 Certificate validity

As a rule, the validity period for personal certificates is 5 years unless there are special restrictions on the validity of the certificate.

1.2 Authentication of identity

The strong identification of the card applicant is always a prerequisite for issuing certificates. The Act on Strong Electronic Identification and Electronic Signatures (617/2009) requires one (1) strong identification token at the time of registration.

The requirement for strong identification is

- a personal visit to the registration point
- The applicant must have with them one of the following valid official documents issued by the police:
  - identity card,
  - passport or
  - a separate identification document issued by the police

The aforementioned identification procedure is carried out without exception each time a smart card is issued

2 Information on smart card

The information contained on the smart card is based on the information provided by the organisation represented by the applicant and the personal data obtained from the Population Information System maintained by the DVV.

The surface print on a smart card varies by organisation (for example):

Front:

- Organisation name,
- name of organisational unit,
- first name and surname,
- a unique identifier,
- the card holder’s photograph,
- expiration date,
- job title.

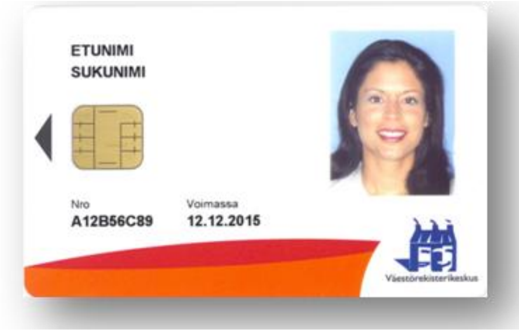


Figure 1: Front of smart card

Back:

- Return instructions,
- return address,
- possible customer-specific information.

In addition to the card holder’s information, the chip includes:

- An authentication and signature key,
- an authentication and signature certificate,
- The certificate authority’s (Population Register Centre) certificates,
- chip number.

The activation PIN code envelope contains:

- a PUK / activation PIN (8 digits) that the user uses to create two separate PIN codes:
  - a basic PIN (PIN1) 4-8 digits that the card holder uses to identify themselves as a user of systems
  - a signature PIN (PIN2) 6-8 digits, which the card holder uses for electronic signatures

Please note: The activation of smart cards changed in autumn 2017, and the PIN envelope now only contains an activation PIN. The card is activated using the activation code in the PIN envelope. During activation, personally-selected basic and signature PINs are set for the card. The card must be activated using card reader software (mPollux DigiSign client) version 4.0.12 or later. The activation PIN screen opens automatically when both PINs are locked.

3 Changing a smart card’s PIN and releasing a locked PIN

3.1 Changing a PIN

PINs for smart cards can be changed using the mPollux DigiSign Client Manager tool. Insert the card into the reader. Open the software by right-clicking the yellow chip icon in the lower-right corner of the desktop and select

- Show devices (in figure 2: Näytä laitteet)

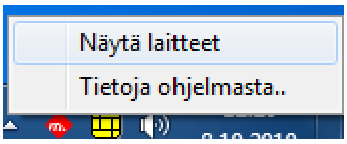


Figure 2: Card reader software selection view

1. Click on the **Identification** tab (in figure 3: Tunnistus tab).

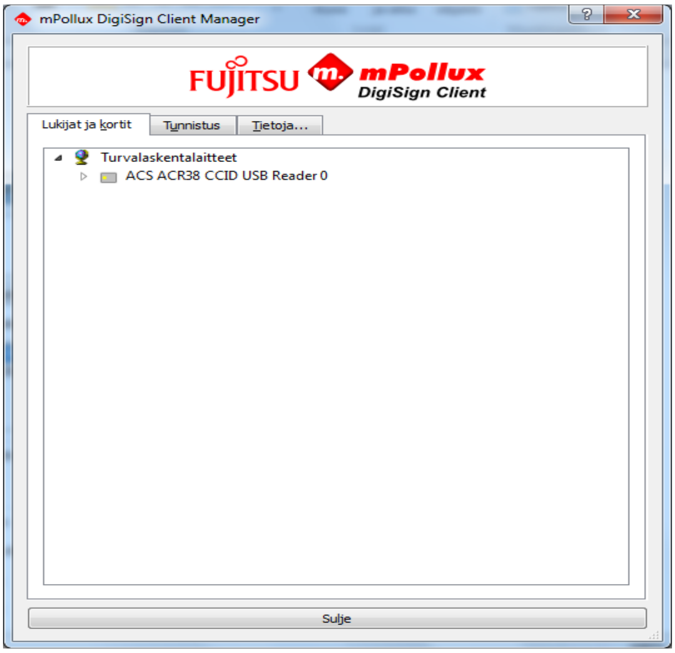
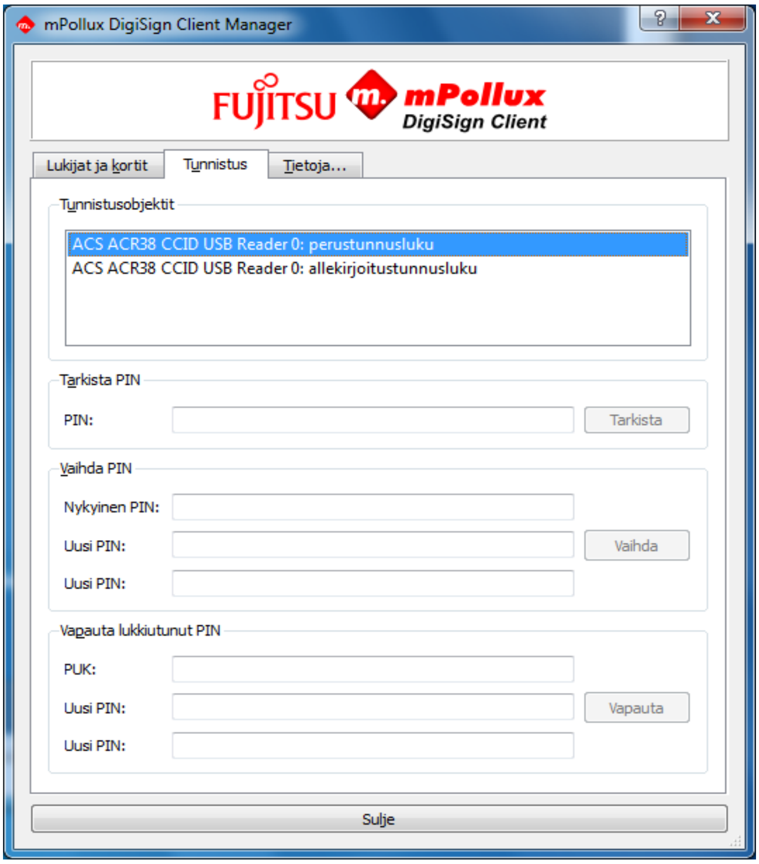


Figure 3: Card reader software start view

2. **Identification** tab (in figure 3: Tunnistus tab)

   Select which PIN you wish to change with your mouse: basic PIN (in figure 3: perustunnusluku) / signature PIN (in figure 3: allekirjoitustunnusluku)
   The basic PIN is the default.



ACS ACR38 CCID USB Reader 0: perustunnusluku
ACS ACR38 CCID USB Reader 0: allekirjoitustunnusluku

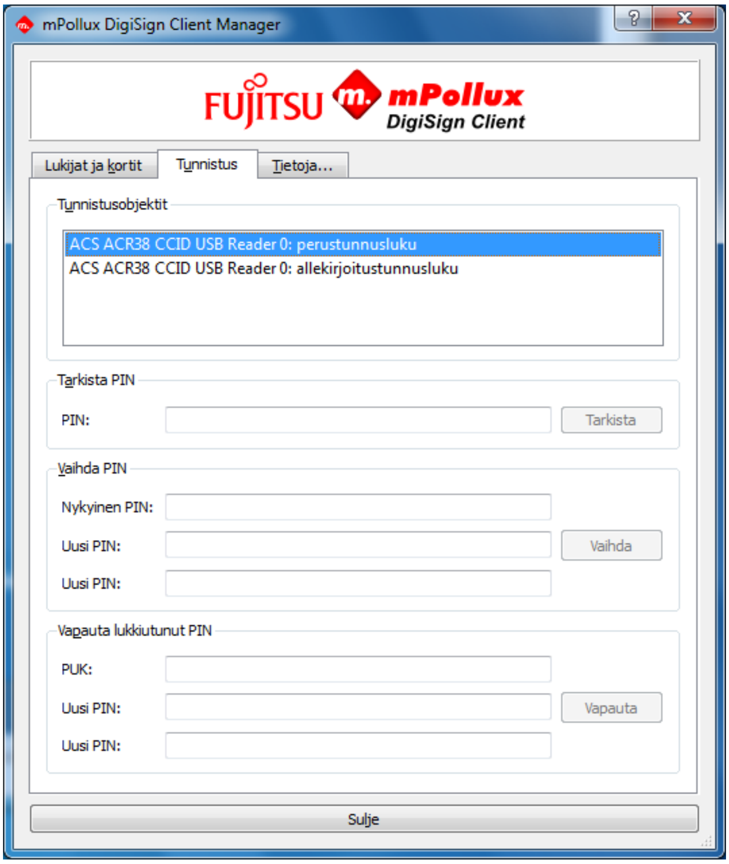
Figure 4: Choosing a PIN (basic PIN or signature PIN)

- Enter current PIN in "Current PIN” (in figure 4: “Nykyinen PIN”)
- Enter a new PIN in "New PIN” (in figure 4: “Uusi PIN”)
- Enter the new PIN again in "New PIN” (in figure 4: “Uusi PIN”)

Click on **Change / Vaihda**
The program will confirm that a PIN change has occurred
The "Check PIN" / ”Tarkista PIN” function allows you to check whether the PIN is correct.

3.2 Releasing a locked PIN

Select which PIN to release (basic or signature PIN) / (perus- or allekirjoitustunnusluku)



Tunnistusobjektit

ACS ACR38 CCID USB Reader 0: perustunnusluku
ACS ACR38 CCID USB Reader 0: allekirjoitustunnusluku

Tarkista PIN

PIN:

Vaihda PIN

Nykyinen PIN:
Uusi PIN:
Uusi PIN:

Vapauta lukkiutunut PIN

PUK:
Uusi PIN:
Uusi PIN:

Figure 5: Releasing a PIN

- Enter Release locked PIN in the PUK/Activation PIN section (in figure 5: Vapauta lukkiutunut PIN)
- Enter a new PIN in "New PIN” (in figure 5: ”Uusi PIN”)
- Enter the PIN again in "New PIN” (in figure 5: ”Uusi PIN”)

Select with mouse: **Release** (in figure 5: Vapauta)
The program will confirm the release of a locked PIN.

3.3 Ordering a new PUK/Activation PIN

Reordering an Activation PIN letter will require that the card holder visits a registration point. The card holder must present a valid police-issued identity document: a passport, ID card, or a separate identification document issued by the police.

4 Card holder's responsibility and lost cards

The smart card is intended only for the use of the card holder to whom the card was granted. All functions performed on the card are in the card holder’s name and are therefore the card holder’s responsibility. The card must be stored in a safe place and separate from its PIN codes.

If the card is damaged, lost, stolen or unnecessary, the revocation service must immediately be informed of the revocation of the certificates to prevent abuse of the card. The card holder's responsibility for the card will end as soon as the revocation service has received the notification.

5 Revocation of certificates

- The serial numbers and revocation dates of the revoked certificates are published on a revocation list.

- A request to revoke a certificate must be made immediately after the card holder has lost the card or it has broken.

- Certificates for an old smart card must be revoked no later than when the use of a new smart card begins.

- A certificate revocation request is made by the organisation registrant or the certificate holder.

The revocation service is available 24/7 every day of the week.

- Tel. 0800 162 622 (calls from Finland are free).
- When calling from abroad, dial +358 800 162 622 (charges made by the local operator will be payable).

- Revoked certificates cannot be reinstated.

- A certificate is valid for up to 5 years from the date of issue.

6 Testing the functionality of a smart card

The following is a list of procedures the card holder can use to test the card's functionality.

The card holder should report a card that fails to work or is faulty to the registration administrator for further measures.

- Check the surface of the chip on the card for folds and for deep scratches or signs of impact. If these are visible, the card may have been mishandled, the chip is physically damaged and is therefore not covered by warranty.

- If there is dirt on the microchip, wipe the chip with a clean, flint-free cloth.

- To ensure that the workstation and the connected card reader work, try a card that works on the workstation. If a card known to be well-functioning does not work in the workstation, contact support services. The problem may be caused by the card reader, the card reader software or card reader driver installation.

- Check whether the card reader software will read the card’s data (when using Windows, see the mPollux Digisign Client user guide by selecting Start - Fujitsu - Installation and User Guide.pdf). If the Digisign Client icon remains in the "unexpected error” or "Waiting for smart card(s)” status, it is likely that the card or card reader is faulty.

- Check whether you can check or change PIN1, the basic PIN (see the mPollux Digisign Client user guide). Changing and releasing PIN codes is described in the PUK/Activation PIN instructions.

- To release a locked PIN, use the PUK/activation PIN. Before using the PUK/Activation PIN to unlock the PIN, you should make sure that the PIN really is locked by entering an invalid PIN five (5) times. If necessary, a PUK/Activation PIN can be reordered for the card holder (PIN codes cannot be ordered again for the same smart card already issued).

- If the PIN cannot be changed as instructed and the PIN is not locked, the chip is faulty, and the product can be exchanged.

- If the PIN is not locked but you still cannot access the applications to which the card should give you access, check that the chip works by logging in to DVV’s test service at https://dvv.fi/en/test-the-use-of-a-certificate. If login fails, it is likely that the chip is faulty, and it should be exchanged.

- If you are able to successfully log in to the DVV test service, but the card still does not have access to the desired applications, or you have access to services and network resources that are related to another user, contact IT support or another authority that your organisation has specified to be responsible for access rights. Your access rights to the applications may be incomplete or incorrect, or an error may have occurred in the card certificate content when the card was ordered.

  The public certificate data related to the card holder on the card can be viewed using the card reader software (see the mPollux Digisign Client User Guide by selecting Start - Fujitsu - Installation and User Guide.pdf).