Certificate Services

1.11.2021

Terms and conditions of the organisation card

General

The Digital and Population Data Services Agency (DVV) is an authority that maintains the personal data register and provides support services for electronic services, notary and legal recognition services, and guardianship services. Its task under the Act on the Population Information System and the Certificate Services of the Digital and Population Data Services Agency (661/2009) is also to provide certified electronic services. The Agency was previously known as Population Register Centre until 31 December 2019. As of 1 December 2010, the Agency has also operated as the statutory certification authority for healthcare services and as of 1 April 2015, as the statutory certification authority for social welfare (Act on the Electronic Processing of Client Data in Healthcare and Social Welfare (784/2021), Act on Electronic Prescriptions (61/2007) and Act on the Population Information System and the Certificate Services of the Digital and Population Data Services Agency (661/2009).

The Digital and Population Data Services Agency grants smart cards and related certificates intended for use by organisations and communities.

The DVV's operations as a provider of an electronic identification service and a trust service provider are regulated by the the Regulation (EU) No 910/2014 of the European Parliament, which entered into force in September 2014, and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (the so-called eIDAS Regulation). The eIDAS Regulation is a law that is directly applicable in the Member States and it has been applied since 1 July 2016.

The aforementioned EU regulation is complemented by the Commission Implementing Regulation (EU) 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (the so-called Assurance Level Regulation). When a service provider meets the requirements of the Assurance Level Regulation, in Finland it is considered as a substantial or high assurance level identification services provider/provider of strong electronic identification service.

The national Act on Strong Electronic Identification and Electronic Trust Services (617/2009) regulates the provision of strong electronic identification services and electronic trust services, including electronic signatures and their legal effects. The law has been updated to meet the demands of the eIDAS Regulation and the changes have entered into force on 1 July 2016.

Organisation certificates included in certificate cards can be used for strong electronic identification, encrypting data and electronic signatures. The authentication and encryption certificate meets the requirements for a strong electronic identification means at the level "high" according to the eIDAS Regulation. A signature certificate intended solely for electronic signatures meets the requirements of an approved signature certificate in accordance with the eIDAS regulation. The Digital and Population Data Services Agency guarantees the correctness of the applicant's identity.

The validity of an organisation certificate is at most five years.

Enabling the electronic properties of the organisation card requires activating the organisation certificate.

Applying for an organisation card

Applications for an organisation certificate are made in person by visiting the registration authority's registration point. The application is filed in the certification authority's certificate information system.

The certificate application is approved by granting the certificate. If any of the prerequisites for issuing the certificate to the applicant are missing, the certificate is not issued and the application is rejected. The applicant is notified of the decision immediately, and he/she can appeal the decision in writing with the certification authority.

The certificate card applicant's identity is verified from a valid identity document issued by the police (identity card that has been issued after 1 March 1999 or passport). Other acceptable forms of identity documents are: a valid passport or identity card issued by an official government agency of an EEA member state, Switzerland or San Marino, or a valid passport issued by an official government agency of another state. If the applicant does not hold any of these documents, the police will verify their identity by other methods.

You can apply for a new certificate when the previous certificate expires if the prerequisites for issuance are still met. When you apply for a new certificate, follow the same procedures as when applying for the certificate for the first time. Only the certificate holder can apply for a new certificate.

It is also possible to apply for a new certificate if the certificate holder's information changes (insofar as it affects the data content of the certificate) or the card becomes damaged. In this case, the certificate holder must contact the registration point and apply for a new organisation card and certificate.

Based on the application information, the certification authority sends to the applicant:

- an organisation card which contains the card holder's personal key pairs and certificates
- an activation PIN envelope used by the holder of the organisation card to set PIN1 (authentication and encryption certificate) and PIN2 (signature certificate) for the card.

In addition, the certification authority sends the holder of the card the instructions for the use of the organisation card.

The activation PIN envelope required for enabling the organisation certificate is mailed either to the applicant's home address or to the organisation assigned to the applicant about four days after the card has been mailed.

Enabling the organisation certificate

To enable the electronic properties of an organisation certificate on an organisation card, the card must be activated using the activation PIN. In addition to the organisation card and the activation PIN, you also need a computer, a card reader and card reader software to activate the organisation certificate. You can activate the organisation certificate using the card reader software mPollux DigiSign Client. You can download the latest version of the card reader software for free at https://dvv.fi/en/card-reader-software.

The card reader software will start the activation process automatically when you put the organisation card into the card reader for the first time. The activation PIN allows you to create two personal PIN codes: basic PIN (PIN1) and signature PIN (PIN2). The basic PIN allows the card user to identify themselves when logging in to services, and the signature PIN allows the user to sign documents electronically.

You can find detailed instructions for enabling the organisation certificate on the DVV website at https://dvv.fi/en/use-of-the-smart-card.

The certificate helpline is open from Monday to Friday at 8-21 and on Saturdays at 9-15 at 0600 96160 (local network/mobile call rate) The helpline is closed on Sundays and public holidays. The service is in Finnish, Swedish and English.

Managing the PIN codes

You can find instructions for resetting a locked PIN code and changing it on the DVV website at https://dvv.fi/en/managing-pin-codes. If you lose the activation PIN, you have to visit the organisation's own registration point in person to order a new activation PIN.

Responsibility for keeping the organisation card

Only the card holder is allowed to use the organisation card and the related activation PIN.

The certificate holder must store and manage their certificates and key pairs and the associated codes and certificate card with due care. The certificate holder must take measures to prevent the loss of the certificate card and protect PINs against unauthorised disclosure or misuse.

PIN codes used to activate the keys must not be kept together with the certificate card. The certificate holder must change their PIN codes if there is reason to believe that they may have been disclosed to unauthorised parties.

The responsibility of an organisation certificate holder ends when they have submitted the information for cancelling the card to the revocation service and received a revocation notice from the official who received your call. For more detailed instructions on revoking a certificate, see Invalidating Certificates on the Organization Card. You should make the revocation request immediately after you have noticed the reason for making the request.

You must take care of your organisation card in accordance with these terms and conditions of use and the publicly available, approved certificate policy. You must keep your organisation card in a safe place to ensure that it cannot be modified, accessed by outsiders or used without authorisation. Acting in violation of these instructions relieves the Digital and Population Data Services Agency from any responsibility arising from the organisation card's use.

Responsibility of the holder of the organisation card

The organisation certificate contains a personal identification certificate and an approved-level electronic signature certificate, as laid down in the European eIDAS regulation (910/2014).

The holder of an organisation card must commit to comply with the certificate policy when applying for and using an organisation certificate. The certificate holder is responsible for ensuring that the data provided in the application for the certificate are correct.

Before signing an organisation certificate application, see the rights and obligations of an organisation certificate applicant in the smart card user guide (https://dvv.fi/en/use-of-the-smart-card), in the terms of use of the smart card and in the certificate policy (https://dvv.fi/en/certificate-policy), which explain the rights and obligations of both parties (the certification authority and the certificate holder). By submitting your application for an organisation certificate, you also accept the general terms and conditions of use and undertake to use the certificates in accordance with the instructions.

The application document and terms and conditions of use clearly state that with their signature, the applicant for an organisation certificate confirms the correctness of the information provided and approves the creation of the organisation certificate and its publication according to the agreement with the client organisation or in a public directory. At the same time, the applicant accepts the rules and terms pertaining to the use of the organisation certificate and sees to the storage of organisation certificates and PIN codes and the reporting of any misuse or lost cards.

An organisation certificate is the electronic identity of its holder and may not be given for another person to use.

Liability for the use of the organisation certificate and for the legal actions taken with it and their financial consequences rests with the certificate holder.

The certificate card must not be left in a reader unattended or given to another person in any circumstances.

Leaving a card containing a microchip in a reader may enable the abuse of the organisation certificate. When terminating a terminal session or leaving a terminal device unsupervised, it is the responsibility of the organisation certificate holder to remove the microchip containing the organisation certificate from the reader device and close the applications used appropriately or otherwise closing the technical connection needed for the use of the organisation certificate.

If the certificate card is damaged, the card holder must arrange for the certificates held on the card to be revoked and apply for a new card at the registration point. The procedure for applying a new certificate card is the same as applying for the card and the certificate for the first time.

The certificate holder must notify the revocation service if the card is lost or the holder suspects misuse.

If the PIN code is locked and the associated PUK code/activation PIN required to open it has been lost, the card holder must contact their organisation's registration point in order to obtain the PUK code/activation PIN.

Digital and Population Data Services Agency's liability.

The Digital and population Data Services Agency's liability for the provision of certificate services is determined according to the agreement concluded with the client organisation. The Digital and Population Data Services Agency is bound by the certification authority's liability for damages under the Act on Strong Electronic Identification and Electronic Trust Services. Where applicable, the Tort Liability Act (412/1974) and Act on Electronic Services and Communication in the Public Sector (13/2003) are also applied.

In its capacity as the certification authority, the Digital and Population Data Services Agency is responsible for the security of the certificate system. The certification authority is liable for the services that it has commissioned as if for its own.

The Digital and Population Data Services Agency is responsible for ensuring that the organisation certificate has been created with following the procedures described in the Act on the Population Information System and the Certificate Services of the Digital and Population Data Services Agency (661/2009), the Act on Strong Electronic Identification and Electronic Signatures, the Act on Electronic Services and Communication in the Public Sector, the certificate policy and the certification practice statement, and according to the data provided by the applicant of the certificate. The Digital and Population Data Services Agency is only responsible for the data that it has stored in the organisation certificate.

The Digital and Population Data Services Agency has the responsibility to ensure that when used appropriately, the organisation certificate can be used from the time it is handed over for its entire period of validity unless it has been placed on the revocation list. The organisation certificate has been given to a person identified in a manner required for organisation certificates. The certificate holder has been given instructions pertaining to the use of the organisation certificate.

When creating a certificate and signing an organisation certificate with its private key, the certification authority assures it has checked the personal data in the organisation certificate according to the policies described in the certificate policy and the certification practice statement.

The certification authority is responsible for ensuring that the right person's organisation certificate is placed on the revocation list and that it appears on the revocation list in the time specified in the certificate policy.

Limitations of the Digital and Population Data Services Agency's liability

The Digital and Population Data Services Agency is not liable for damage caused by the disclosure of PIN codes, PUK code/activation PIN or an organisation certificate holder's private keys unless said disclosure is the direct result of the Agency's direct action.

The maximum extent of the Digital and Population Data Services Agency's liability to the organisation certificate holder and a trusting party is any direct damage incurred if the damage is the result of the Agency's direct actions.

The Digital and Population Data Services Agency is not responsible for any indirect or consequential damage caused to the holder of the organisation certificate. Neither is the Digital and Population Data Services Agency liable for the indirect or consequential damage suffered by a party trusting an organisation certificate or by another contractual partner of the certificate holder.

The Digital and Population Data Services Agency is not responsible for the functioning of public data connections or information networks, such as the internet, and it is not liable for situations in which the execution of a legal act is prevented because a device or software used by the holder of the organisation certificate fails or in which the certificate is used in breach of its intended use.

The certification authority has the right to interrupt the service for changes or maintenance. Modifications and maintenance concerning the revocation list will be announced in advance.

The certification authority has the right to develop the certificate service. An organisation certificate holder or a party trusting an organisation certificate must bear their own expenses thus incurred, and the certification authority is not liable to compensate the organisation certificate holder or a party trusting the organisation certificate for any expenses caused by the certification authority’s development work.

The certification authority is not responsible for errors in the online service or applications intended for the certificate holder and organisations and based on a certificate or for any expenses resulting from them.

The certification authority is not liable for any damage caused by the conduct of the certificate holder or the party using the certificate system in violation of the law, the certificate policy, certification practice statement or other instructions.

Force majeure

The certification authority is not liable for any damages caused by natural disasters or other force majeure events.

Revocation/invalidation of certificates on the organisation card

Certificates on the organisation card are revoked by calling the revocation service 0800 162 622 (free when calls are made in Finland). If you are calling from abroad, the number is +358 800 162 622 (charges made by the local operator will be payable).

A certificate revocation request can be made by:

- the holder of the organisation card or their legal representative regarding that person’s own certificate;
- the certification authority if the conditions mentioned below are met. A certificate can be revoked:
- upon the certificate holder's request
- if the certificate holder leaves their position

- if the certificate card is lost, stolen or damaged
- if the PIN code and the certificate card are lost or stolen
- upon death of the certificate holder.

The certificate holder must immediately request the revocation of their certificate by contacting the revocation service if the above-mentioned conditions for revoking the certificate are met.

The certification authority may revoke an organisation certificate if the certificate is used in a way that violates the certificate policy, the certificate practice statement, the Act on the electronic processing of client data in social and health care or the Act on electronic prescriptions or associated regulations, requirements or guidelines.

No attempt must be made to use the certificate after the revocation request has been made.

The Digital and Population Data Services Agency will revoke a certificate it has issued if an error is found in its data content.

The Digital and Population Data Services Agency may revoke certificates signed with its private key if there is reason to believe that the Agency's private keys have become disclosed to or accessed by unauthorised parties.

All certificates that are valid and have been granted with the exposed key must be closed on one or several revocation lists whose validity period does not expire until the validity of the last revoked certificate has expired.

If the private key used by the Digital and Population Data Services Agency when creating the certificate or another technical method has been disclosed or otherwise become unusable, the Agency must duly notify all cardholders and the supervisory authority (the Finnish Transport and Communications Agency Traficom).

The Digital and Population Data Services Agency may also revoke a certificate for other special reasons.

Notifying users of the processing of their data

The handling of private information in the certification authority's systems is subject to the provisions of the law on the handling of private information and the protection of privacy, including Act on the Population Information System and the Certificate Services of the Digital and Population Data Services Agency (661/2009), EU's General Data Protection Regulation (679/2016) and the Data Protection Act (1050/2018). The handling of public information in the certification authority's systems is subject to the provisions of the Act on the Openness of Government Activities (621/1999). The certification authority ensures that private information handled in its systems is protected against unauthorised access. Information can be disclosed to authorities on the basis of acts, decrees and associated regulations.

The person's unique identifier and other information provided in the application are stored in the DVV certificate system. The authentication certificates and person's unique identifier on the organisation card are also stored in the DVV public directory (https://dvv.fi/en/certificate-directory) unless otherwise agreed with the client organisation. Anybody has the right to access information contained in a public directory, as laid down in the Act on the Openness of Government Activities. The data archiving period is the card's validity period + 5 years.

The certification authority has published specific policy rules under the Data Protection Act with regard to the certificate services.

Controller and statements

The personal data contained in the organisation card are collected in the following systems: The Population Information System, the certificate system and the revocation list. For the Population Information System, the controllers are the Digital and Population Data Services Agency and the State Department of Åland. For the certificate system and revocation list, the controller is the Digital and Population Data Services Agency.

In accordance with the Data Protection Act, statements on the registers have been prepared and can be viewed at https://dvv.fi/en/privacy-statements.

The DVV services and registers' privacy statements detail how, where and why personal data is processed.

Certificate data content

The following data are saved on the organisation certificate issued by the Digital and Population Data Services Agency:

- Certificate holder unique identifier (formerly SV number)
- Certificate serial number
- First and last name of the certificate holder
- UPN field
- Organisation name
- Certificate period of validity
- Title (optional)
- Organisation unit (optional)

For more detailed technical specifications of the data content of certificates, visit https://dvv.fi/en/fineid-specifications.

The details of the certificate and their correctness are confirmed with the electronic signature of the certification authority.

The certification authority publishes the certification authority's certificates and revocation lists in a non-chargeable, publicly available, public directory. Depending on the agreement on the certificate and/or the agreement concluded with the customer organisation, the certification authority publishes the granted verification and encryption certificates in either a public or non-public directory. Signature certificates are not published in a directory.

Implementation of the right of inspection of personal data and rectification in accordance with data protection legislation

The holder of a certificate has the right to access their information, such as personal data, in accordance with the applicable legislation.

The right of data subjects to check their own register data and the data subject's right to prohibit the controller from processing their register data as well as the rectification of an error are provided for in Regulation (EU) No 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) repealing Directive 95/46/EC, the Data Protection Act (1050/2018) and the Act on the Population Information System and the Certificate Services of the Digital and Population Data Services Agency (661/2009), regarding the protection of natural persons in the processing of personal data and the free movement of such data. The requests for accessing data and rectification made in accordance with the Data Protection Act must be submitted to the controller of the register concerned.

Responsibility of the controller and processing of personal data

The handling of private information in the CA's systems is subject to the provisions of the law on the handling of private information and the protection of privacy. The handling of public information in the certification authority's systems is subject to the provisions of the Act on the Openness of Government Activities (621/1999). The certification authority ensures that private information handled in its systems is protected against unauthorised access. Information can be disclosed to authorities on the basis of acts, decrees and associated regulations.

Additional information related to the organisation card

Certificate policy documents concerning the organisation card can be found at https://dvv.fi/en/certificate-policy

Identification principles of the Digital and Population Data Services Agency can be found at https://dvv.fi/en/certificates

You can download the software for changing PIN codes and releasing locked PIN numbers (mPollux DigiSign Client) free of charge at https://dvv.fi/en/card-reader-software

Appeal and dispute resolution

An organisational card issued in the Digital and Population Data Services Agency is an indication of a positive administrative decision, and the rejection of an application for an organisational card is an indication of a negative administrative decision. The instructions for claiming a revised decision and appeal instructions are attached to the Agency's decision.

If you are dissatisfied with the Agency’s decision, you may request a revised decision from the Digital and Population Data Services Agency. A claim for a revised decision to the Agency must be made in writing. The claim for a revised decision may be free-form but it must include the matters and appendices mentioned in the instructions for revised decisions and appeals.

If you are still dissatisfied with a decision made during revision procedures, it can still be appealed to the Administrative Court. An appeal to the Administrative Court is filed must be submitted in writing. The appeal for a revised decision may be free-form but it must include the matters and appendices mentioned in the instructions for revised decisions and appeals. The appeal must be submitted to the administrative court in whose jurisdiction the

Digital and Population Data Services Agency is located. The period for appeal starts when the appeal instructions have been appropriately appended to the decision and served to the client.

On the basis of the registration agreement, disputes concerning the agreement that cannot be settled in negotiations between the Parties will be handled in the Helsinki District Court in Finnish. Within the central government, disputes are resolved through negotiations.