Certificate services

10.2.2023

Terms of delivery of service certificates

General

A certificate issued by the Digital and Population Data Services Agency (DVV) is a service certificate used to authenticate a service or server by a service provider or an individual person. Before issuing a certificate, the Digital and Population Data Services Agency checks the applicant's information and the data on the application. Once the certificate has been issued, it will be delivered to the customer as agreed.

Terms of delivery

The Digital and Population Data Services Agency must have access to any domain names and information on their administration when processing the application. The Digital and Population Data Services Agency only issues server certificates for IP addresses or domains used for public administration purposes. Before issuing the certificate, the Digital and Population Data Services Agency will check the applicant's information. Domain names will be checked using any available online services or other reliable methods. A proxy should be submitted together with the application if the applicant of the certificate is acting on behalf of a company or an organisation.

A server certificate will be issued for no more than 12 months. A fee is charged for the use of the server certificate according to the price list. The delivery time for service certificates is at most five workdays, if the application has been filled in correctly and the necessary attachments have been submitted. The service certificate is delivered to the applicant or the technical support person they have specified by email in der or pem format. The application will expire if it has been pending for more than six months and it is completed incorrectly or the necessary attachments are missing.

The applicant is obliged to check the certificate after receiving it and to notify the Digital and Population Data Services Agency in writing if the product does not correspond to the order. The notification must be submitted without delay to the DVV, or no later than one week after the certificate has been installed. In this case, the DVV checks the delivered certificate and takes care of the necessary measures.

The service certificate application is binding and the revocation of the certificate or cancellation of the order does not, in principle, entitle for a refund of the fee after the certificate has been delivered.

Purpose and archiving of the certificate

The purpose of the certificate is specified in the certificate policy and certification practice statement of each certificate type and in the certificate. The certificate may only be used for the intended purpose. The relying party must check that the certificate is valid and that it does not appear on a revocation list. The trusting party cannot trust the certificate in good faith if its validity has not been checked. Before accepting certificates, the relying party must check that they are not on the revocation list. The information published by the certification authority is available on the certification authority's website (https://dvv.fi/en/service-certificates).

Confidential data used in the certificate system are stored in the certification authority's own confidential repository. The certification authority's data are archived according to the valid archiving rules. According to the authority's valid archiving rules, the archiving period is seven years after the certificate expires. The provisions of the Archives Act (arkistolaki, 831/1994) are applied as the general act on archiving.

Certificate holder's responsibilities

The certificate holder (customer) is responsible for ensuring that the data provided in the application for the certificate are correct.

The certificate holder must notify the certification authority immediately if the data content is not in compliance with the data indicated in the service certificate application. The certification authority will then revoke the certificate in question and produces a new certificate in it's place.

The certificate holder must revoke the certificate immediately if the subject's name or other subject identity information in the certificate has changed, or the subject's organisation has ceased to exist, or the certificate has been deemed redundant, or it is known or suspected that the subscriber's private key has been compromised. The certificate holder revokes the certificate via Digital and Population Data Service's Agency's E-services. The certificate holder must select a reason code for the certificate revocation. The certification authority will then revoke the certificate in question within 24 hours from when the certificate revocation request has arrived.

The certificate holder's responsibility for the use of the certificate ends when they have provided the certification authority with the information required to revoke the certificate. To end their liability the certificate holder must make the revocation request immediately after they have noticed a reason to do so.

Applicable agreements, certification practice statement and certificate policy

The certificate applicant's rights and obligations are stated in the certificate policy and certification practice statement documents. By signing the application, the applicant confirms that the information provided is correct and accepts that the certificate will be created and published. At the same time, the applicant accepts the rules and conditions pertaining to service certificate use and undertakes to protect the service certificate and report any misuse. An agreement has been concluded between the certification authority and the registration authority as well as other vendors that provide parts of the certificate services, indisputably specifying the rights, liabilities and obligations of both parties. When a certification authority issues a service certificate, it also approves the application for a certificate.

Obligations and responsibilities of the certification authority

The certification authority provides certificate services on the terms and conditions set out in the legislation, agreement and certificate policy and assumes responsibility for their functioning. The certification authority is responsible for the functioning of the certificate system on its own behalf and on behalf of the registration authorities and technical suppliers used by it. The certificate policy documents are published and available for anyone at www.dvv.fi/cps. This certificate policy has been registered by the Digital and Population Data Services Agency. The certification authority's operation is audited every year and whenever significant modifications have been made in the system. The Digital and

Population Data Services Agency is a statutory certification authority. The certification authority shall use reliable systems and products protected against unauthorised use.

The Digital and Population Data Services Agency's liability related to the provision of certificate services is determined under the valid service contracts and pursuant to the provisions in the Tort Liability Act (412/1974).

Limitations of liability for the certification authority

The Digital and Population Data Services Agency is not liable for any damage caused by the disclosure of a private key of certificate holder unless it is a direct consequence of the Digital and Population Data Services Agency's actions. The maximum extent of the Digital and Population Data Services Agency's liability to the holder of the certificate and its trusting party is for the direct damage incurred, if the damage is the result of the Digital and Population Data Service Agency's direct actions. The Digital and Population Data Services Agency is not responsible for any indirect or consequential damage caused to the certificate holder. Neither is the Digital and Population Data Services Agency liable for the indirect or consequential damage suffered by a party trusting a certificate or by another contractual partner of the certificate holder. The Digital and Population Data Services Agency is not liable for the functioning of public telecommunications or information networks, including the Internet.

The certification authority has the right to interrupt the service to perform modifications 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. A certificate holder or a party relying on a certificate must bear their own expenses incurred for this reason, and the certification authority is not liable to compensate the certificate holder or a party trusting the certificate for any expenses caused by the certification authority's development work. The certification authority is not liable for errors in the online service or applications intended for end users and based on a certificate or any expenses arising from them.

Force majeure

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

Audits of the certification authority

The Finnish Transport and Communications Agency (Traficom), which supervises trust services, may audit the certification authority's operation under the prerequisites laid down in the Act on Strong Electronic Identification and Electronic Signatures. The Digital and Population Data Services Agency has the right to audit its technical suppliers in accordance with the audit procedure specified in the technical supply agreement in question. An audit is carried out at least once a year and at the start of each new contract period. Audits are carried out to determine the technical supplier's compliance with the agreement, taking into account the requirements of information security management standards. Technical suppliers are generally assessed on the basis of the ISO 27001 standard. The audit is carried out by the Head of Information Management at the Digital and Population Data Services Agency or an external auditor commissioned by the Digital and Population Data Services Agency who specialises in auditing technical vendors pertaining to certificate services. In the audit,

consideration is given to the implementation of eight areas of information security. Audited information security properties include confidentiality, integrity and availability. The audit covers Traficom regulations on the information security requirements of certification authorities. In the audit, the policy and the application instructions are compared with the operations of the entire certificate organisation and system. The Digital and Population Data Services Agency is responsible for the compliance of the application instructions with the certificate policy.

Processing of personal 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 Certificate Services Provided by the Digital and Population Data Services Agency (661/2009), EU's General Data Protection Regulation (679/2016) and the Data Protection Act (1050/2018).

Special attention is paid to the handling of personal data, and the Digital and Population Data Services Agency has published a specific set of procedures for the provision of certificate services in accordance with the Data Protection Act. The certification authority has also prepared a description of file for each component of the certificate system compliant with the Data Protection Act with respect to the processing of personal data. The provisions of the archive act (arkistolaki, 831/1994) are applied as the general act on archiving. The right to obtain information is determined according to the Act on the Openness of Government Activities (621/1999). With respect to the archiving of certificates, the provisions pertaining to archiving in electronic services legislation are also applied.

Appeal and dispute resolution

A certificate issued in the Digital and Population Data Services Agency is an indication of a positive administrative decision, and the rejection of an application for a certificate 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.

The certificate holder can also use dispute resolution methods as specified in the agreement.

On the basis of the 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.