



IDENTIFICATION PRINCIPLES OF THE DIGITAL AND POPULATION DATA SERVICES AGENCY

The Digital and Population Data Services Agency as a certificate authority, as a provider of joint e-service support services for public administration (Suomi.fi) and as an implementer of the national node

The Digital and Population Data Services Agency (DVV) operates within the Ministry of Finance's branch of government. DVV started operations on 1 January 2020 when the Population Register Centre, local register offices and the steering and development unit for the local register offices merged into a new 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 Certificate Services of the Digital and Population Data Services Agency (661/2009) is also to provide certified electronic services. The Agency was also 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 Health Care and social welfare (159/2007), Act on Electronic Prescriptions (61/2007) and Act on the Population Information System and Certificate Services of the Digital and Population Data Services Agency (661/2009). The Agency's certificate authority tasks have been divided into different departments and their units, with the following departmental focus areas: The Customers division is responsible for notary and legal recognition services, the customer services for companies and authorities, and the implementation of services. The Services division is responsible for register services, support services for digitalisation, promoting interoperability, and developing and maintaining services. The Processes division is responsible for guardianship services and the joint services of the Agency (e.g. legal matters, security issues, premises and agency services, case management and assistant services, operational and financial control, as well as processes and quality). Information on the DVV and the certificate authority activity is available at <https://dvv.fi/en/individuals>.

The DVV produces high-quality electronic identification solutions to answer the society's needs. The Agency (known as the Population Register Centre until 31 December 2019) has served as a certificate authority since 1999, producing service certificates and related services for the public and private sectors. Certificate services protect information security related to electronic identities in e-services. Certificates are used to verify the certificate holder's identity and the accuracy, integrity and authenticity of data contained in the certificate. Electronic identification provides citizens with the possibility for flexible, secure online transactions anytime and anywhere. Furthermore, the electronic signature enables new types of online transactions.

The Agency's certificate management system and certificate services are based on the public key infrastructure (PKI). The DVV's certificate infrastructure consists of a certificate system, supplier of certificate data contained in the cards, a revocation list, advisory service, and directory service. The DVV's activities as a certificate authority include the





provision of certification, directory and revocation services, registration, and the creation and individualisation of the card that contains the certificate. The DVV is responsible for the functioning of the certificate system as a whole, including any registration authorities and technical suppliers it may use. The DVV's Support Services and Interoperability unit maintains Certificate Policy, Certification Practice Statement and PDS documents, which are electronically available at <https://dvv.fi/en/certificate-policy>.

The DVV's operations as a provider of strong electronic identification service and approved trust service provider (under earlier regulation, qualified certificate authority) are regulated by 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 Directive 1999/93/EC contained the regulation concerning electronic signatures. 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 demands of the Assurance Level Regulation, it is profiled as a substantial or high assurance level identification services provider in Finland. The DVV provides high-assurance level electronic identification services.

The national Act on Strong Electronic Identification and Electronic Trust Services (617/2009) provides for strong electronic identification services providing 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.

An equal status with the traditional hand-written signature is secured for signatures made with a secure signature creation device (SSCD) or a qualified signature creation device (QSCD) and an approved certificate in the aforementioned law.

The Agency (the Population Register Centre until 31 December 2019) has provided certificate-based identification means since 1999 and operated as a certification authority as of 31 March 2003. The DVV's qualified certificates produced in accordance with the Directive 1999/93/EC and the national legislation are considered eIDAS Regulation-qualified approved electronic signature certificates until their expiry. The DVV as a provider of certificate services will be considered an eIDAS Regulation-qualified trust service provider (i.a. provider of approved electronic signature certificates) when it proves that it meets the demands set for an approved trust service provider. The DVV has submitted to the supervisory body, the Finnish Communications Regulatory Authority (currently Finnish Transport and Communications Agency), the required conformity assessment reports.



The DVV is part of the national trust network of strong electronic identification service providers laid down in section 12 a of the Act on Strong Electronic Identification and Electronic Trust Services (increased and high assurance level identification services). Identification service providers belonging to the trust network may offer identification tools and/or an identification broker service.

DVV produces public administration's joint support services for electronic services (Suomi.fi) under the relevant legislation (Act on central government's joint e-service support services (571/2016)).

The DVV also has a statutory task to produce and maintain a national interface to the EU electronic identification interoperability system (national node, Act on Strong Electronic Identification and Electronic Trust Services, section 42 c). The European Commission's implementing regulation (EU) 2015/1501 lays down provisions on the national node requirements.

As part of the DVV's above-mentioned service implementation, the DVV also has a high-assurance level identification service for transmitting the identification transactions from its identification tools to public administration e-services.

As a public body, the DVV complies with the provisions concerning confidentiality, publicity, data protection and data security laid down in the Constitution of Finland (731/1999), Act on the Openness of Government Activities (621/1999), Decree on the Openness of Government Activities and on Good Practice in Information Management (1030/1999), Government Decree on information security in central government (681/2010), Act on the Population Information System and the Certificate Services of the Digital and Population Data Services Agency (661/2009), Act on Strong Electronic Identification and Electronic Trust Services (617/2009), Data Protection Act (1050/2018), Act on central government's joint e-service support services (571/2016), Act on Electronic Services and Communication in the Public Sector (13/2003) and EU's General Data Protection Regulation (679/2016). A basic task of the Digital and Population Data Services Agency is to enable usage of the data contained in the Population Information System and the certified electronic services to support society's functions and information services. Through its activity, the Digital and Population Data Services Agency promotes the protection of privacy and personal data as well as information security and the development of and compliance with good data processing and data management practices. The binding obligations imposed on the DVV by the legislation cannot be derogated with any agreement.

The grounds for the processing of personal data related to DVV's identification service (identification tools and identification broker service) can be found in the privacy statements of the DVV's services and registers. The privacy statements are available on the DVV's website at <https://dvv.fi/en/privacy-statements>.

Digital and Population Data Services Agency certificates

The Digital and Population Data Services Agency produces Citizen Certificates for ID cards, organisation certificates for organisation cards, temporary certificates for replacement cards and healthcare certificates: professional certificates for regulated social welfare and healthcare professionals' ID cards, service provider person's certificates for non-





clinical social welfare and healthcare sector staff ID cards and non-regulated social welfare and healthcare worker's certificates for healthcare workers' ID cards. Citizen Certificate, organisation certificate, social welfare and healthcare professional certificate, service provider person's certificate, non-regulated healthcare worker's certificate, and temporary certificate consist of a certificate pair which has two different functions: 1) authentication and encryption certificate (electronic identification) and 2) signature certificate. The Digital and Population Data Services Agency verifies the correctness of identity.

Certificate applications are made in person by visiting a registration authority or an organisation's registration point. A customer may apply for a new electronic identification device with an existing strong electronic identification device of equivalent level under the Act 617/2009, if made possible by the online services. The electronic identification of a natural person must be carried out such that the requirements laid down in the Assurance Level Regulation are met. Verifying a person's identity may be based on a strong electronic identification device. In addition, the identity verification may be based on a practice previously used by a public or a private provider for another purpose than issuing a strong electronic identification device. This practice must be accepted by the Finnish Transport and Communication Agency on the grounds of the regulations concerning the issuance practice, or on the grounds of a confirmation given by an assessment body, that has assessed the conformance of the identification service.

The DVV's certificate services and certificate registration process are developed to meet the demands of electronic transactions, and as the services develop, electronic applications for certificates will be made possible.

Citizen Certificate for an identity card

The Citizen Certificate is personal data given in the standard format; an electronic identity. Among other things, it contains a first name, a last name and an electronic Unique Identification Number. The Citizen Certificate is a high assurance level tool for strong electronic identification.

A Citizen Certificate may only be issued to a Finnish national or a foreign national who is resident in a Finnish municipality as referred to in the Municipality of Residence Act, whose details are stored in the Population Information System and whose identity has been reliably established. The foreign national must also either hold a valid residence permit or card or their right of residence must have been registered.

The Citizen Certificate may be issued and stored on different kinds of technical platforms such as a chip in an ID card.

Citizen certificates can be used for electronic identification, encryption and electronic signatures. The Citizen Certificate can be used without limitation according to its purpose in applications and services from both the public government and private organisations.

The Citizen Certificate contains an electronic Unique Identification Number which functions as unique identification information.



The Identity Card Act (663/2016) is applied on applications for Citizen Certificates included in ID cards ID card applications are submitted to the police. The application can be filed electronically. The applicant must make additions to the application in person at the authority's office, subject to the Identity Card Act (663/2016), section 10 (Personal attendance when applying for an electronic ID card). The applicant does not have to make a personal visit to the authority's office when applying for an ID card electronically for example when an ID card (or a passport if they are a Finnish national), that meets the requirements, has been issued for them, and they have made a personal visit to the authority's office when applying for this earlier identification. A Finnish national residing abroad may submit an ID card application to a Finnish embassy, to a consulate managed by a seconded civil servant or to another delegation of Finland, which issues passports, and in which a Finnish national with a Foreign Ministry's authorisation to issue ID cards operates (delegation of Finland). The applicant must personally be present at the delegation of Finland, when applying for an ID card, and the application cannot be filed electronically.

An identity card is an official document that states identity. In addition, the ID card may be used instead of a passport as an official travel document in EU countries, Switzerland, San Marino and Liechtenstein.

The Citizen Certificate is applied for in connection with the ID card application by a personal visit to the police authority operating as the registration authority (in foreign countries at a delegation of Finland) or electronically. When applying for a Citizen Certificate in person at a police authority or a delegation of Finland, the applicant's identity will be verified using a valid identity document, either an ID card or a passport, which has been issued by the police. Other acceptable forms of identity 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 a foreign national, who is applying for an ID card for foreign nationals containing a Citizen Certificate, cannot present a valid identity document, they must present a valid residence permit card or a residence card. In that case, the authority receiving the application is entitled to fingerprint the applicant and compare these fingerprints to those stored in the technical part of the residence permit card or the residence card to verify the applicant's identity. If the applicant does not hold any of these documents, the police will verify their identity by other methods. The method of identification is recorded in the application form and confirmed by signature by the registration clerk. The information presented by the applicant is compared with the information in the Population Information System.

Organisation certificate for an organisation card

The Digital and Population Data Services Agency produces organisation cards for companies and organisations. The certificates on organisation cards are called organisation certificates. These certificates prove a person's connection to a company, a society or another organisation. The organisation certificate is a high assurance level tool for strong electronic identification.

The organisation certificate also enables indisputable electronic signatures defined in the law and authentication of information network users. In addition, an email address pertaining to the organisation can be included in the organisation certificate. This enables signing



and encrypting e-mails with the certificate as well as logging into networks with an organisation card containing an organisation certificate.

Applications for an organisation certificate are made in person by visiting the registration authority's registration point. The applicant's identity is verified from a valid identity document issued by the police, which can be an identity card or a passport. Other acceptable forms of identity 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 may verify their identity by other methods. The method of identification is recorded in the application form and confirmed by signature by the registration clerk.

Social welfare and healthcare sector personal certificates in social welfare and healthcare smart cards

The Digital and Population Data Services Agency produces healthcare sector staff smart cards containing social welfare and healthcare sector personal certificates for the following institutions and personnel: public and private social welfare and healthcare sectors' healthcare professionals and other staff, pharmacies' healthcare professionals and other staff, other organisations and staff that participate in providing these services. A social and healthcare sector smart card containing a social welfare and healthcare sector personal certificate proves a person's connection to a company, a society or another organisation.

The Digital and Population Data Services Agency produces a social welfare and healthcare professional certificate on the chip of the regulated social welfare and healthcare professional's ID card. The professional certificate is intended for the use of public and private social welfare and healthcare sectors' healthcare professionals as well as social welfare and healthcare professionals working in pharmacies (Act on Health Care Professionals (559/1994), Act on social welfare professionals (817/2015)).

In addition, the Digital and Population Data Services Agency produces service provider person's certificates on the chips of ID cards for non-clinical healthcare sector staff as well as non-regulated healthcare worker's certificates on the chips of ID cards for non-regulated healthcare workers.

The social welfare and healthcare sector personal certificate enables indisputable electronic signatures defined in the law and authentication of information network users. In addition, an e-mail address pertaining to the organisation can be included in the social welfare and healthcare sector personal certificate. This enables signing and encrypting e-mails with the certificate as well as logging into networks with a social welfare and healthcare sector smart card containing a social welfare and healthcare sector personal certificate.

Applications for social welfare and healthcare sector personal certificates are made in person at the registration point operating as the registration authority. When applying for a social welfare and healthcare sector personal certificate, the applicant's identity is verified from a valid identity document issued by the police, which can be an identity card or a passport. Other acceptable forms of identity 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. The method of identification is recorded in the application form and confirmed by signature by the registration clerk.

The validity of a healthcare professional's practice rights is verified from the central register of health care professionals (JulkiTerhikki), which is kept by the National Supervisory Authority for Welfare and Health (Valvira). If the applicant does not have valid professional practice rights according to the JulkiTerhikki register, the certificate will not be issued.

All social welfare licensed professionals and professionals with a protected occupational title are recorded in Valvira's register of social welfare professionals (JulkiSuosikki). If the applicant does not have valid professional practice rights according to the JulkiSuosikki register, the certificate will not be issued.

Only one professional practice right, selected by the applicant, will be indicated in the healthcare professional certificate and professional card if the applicant has several valid rights.

Authentication of the connection between the applicant and the organisation they represent is required of those who apply for service provider person's certificates or non-regulated social welfare and healthcare worker's certificates. The connection between the applicant and the organisation they represent is authenticated with a written document provided by the organisation in question.

Temporary certificate for a replacement card

The Digital and Population Data Services Agency provides temporary certificates that can be stored on various smart cards for temporary use.

The Digital and Population Data Services Agency provides the replacement card as a temporary card solution for organisations. It is a flexible solution, as certificates can be stored on the card via remote connection. Replacement cards can be ordered in connection with a smart card order or separately if necessary.

Temporary solutions are needed, for example, when a smart card is still in production, has been left at home or lost.

Replacement cards can also be used for signatures.

Applications for a temporary certificate are made in person by visiting the registration authority's registration point. The applicant's identity is verified from a valid identity document issued by the police, which can be an identity card or a passport. Other acceptable forms of identity 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 may verify their identity by other methods. The method of identification is entered



on the application form and the registration clerk signs the document, confirming that the applicant's identity has been checked.

Electronic signature

It is possible to make electronic approved certificate signatures in accordance with the eIDAS Regulation and Act 617/2009 with the Digital and Population Data Services Agency's Citizen Certificates, organisation certificates, social welfare and healthcare professional certificates, signature certificates in service provider person's certificates or non-regulated social welfare and healthcare worker's certificates. Using a certificate in electronic signature refers to the use of a private key in signing and to the use of the public key and certificate in verifying the signature. The field that determines the intended use in the certificate's data content specifies the intended use of the key pertaining to the certificates. The intended use of the signature certificate key is non-repudiation. The use of the key is restricted to its intended use. For example, a key intended for the non-repudiation of digital signing must be used only for this purpose and not for authentication and encryption.

Directory service

The directory service is a public Internet-based service, which can be used to retrieve the revocation lists and all certificates issued by the Digital and Population Data Services Agency, that have been published in the public directory. The directory service is available at <ldap://ldap.fineid.fi> and <https://dvv.fi/en/certificate-directory>. Expired and revoked certificates are removed from the directory service.

Using the directory service does not require identification.

Revocation service

The Digital and Population Data Services Agency's revocation service receives certificate revocation requests.

The revocation service revokes certificates that the certificate holder, or someone acting on behalf of the certificate holder (e.g. employer), requests to be revoked prior to expiry. The revocation service clerk identifies the person requesting for revocation. The revocation service operates 24/7 around the year. The serial numbers and revocation dates of the revoked certificates are published on the revocation list.

Revocation service

The revocation service is available 24/7, in case your card is lost or stolen or you no longer need a card, by calling

0800 162 622 (calls from Finland are free)

+358 800 162 622 when calling from abroad (+ local operator charges)

Advisory service

The advisory services provide further information on the use of certificates. The services also help with problems that may arise, when installing the card reader software, and with



the most common deployment-related situations such as the use of PIN codes, changing PIN codes and unlocking PIN codes. The advisory service also provides additional information and instructions on public administration's electronic identification and brokering of identification.

The phone service is available from Monday to Friday between 8 a.m. and 9 p.m. and on Saturdays between 9 a.m. and 3 p.m. The helpline is closed on Sundays and public holidays. The phone service is directed to the Public Service Info.

0600 9 6160 (local/mobile network fee) / Guidance on certificate usage
0295 000 / Guidance on the use of Suomi.fi services

You can also contact Public Service Info electronically at <https://www.kansalaisneuvonta.fi/en-US>. The website offers various service platforms.

DVV's identification broker service and DVV's national node

The above-mentioned identification transactions of DVV certificates (identification tools) are transferred to the public administration e-services via the DVV identification broker service. Out of the services/functions provided by the Digital and Population Data Services Agency, the certificate directories, revocation lists, and the facilitation of the software needed to use certificates (client software for reading the card in the user's terminal device) form the identification broker service of the Digital and Population Data Services Agency. DVV does not transfer identification transactions from identification tools provided by others. In addition, DVV certificate identification transactions can be transmitted via the DVV national node to the e-services of EU countries' public administrations.

Product and service prices

The general criteria pertaining to the charges of performances by State authorities are laid down in the Act on Criteria for Charges Payable to the State (150/1992).

The prices of the Digital and Population Data Services Agency's products and services, that are subject to public law, are determined by the Ministry of Finance's effective decree on the charges of the Digital and Population Data Services Agency's performances.

The Digital and Population Data Services Agency's commercial products and services' prices are determined in the price list that is valid at the time.

Digital and Population Data Services Agency's partners and subcontractors

The Digital and Population Data Services Agency and the police provide ID cards, that contain the DVV's certificates and are issued by the police, to Finnish nationals and foreign nationals, who have a Finnish home municipality referred to in the Municipality of Residence Act. Further information on the ID card and the Citizen Certificate are available at <http://www.poliisi.fi>.

The Digital and Population Data Services Agency and the Ministry for Foreign Affairs offer Finnish citizens residing abroad a personal identity card with DVV certificates issued by a



Finnish mission. More information on the network of missions and how to apply for an identity card abroad is available at the Ministry for Foreign Affairs (<https://um.fi/frontpage>).

The Digital and Population Data Services Agency provides social welfare and healthcare workers with social welfare and healthcare sector smart cards, that contain the DVV's certificates, and smart card-related certificate services. In addition, the DVV provides other services related to the social welfare and healthcare sector certificate service production together with the National Supervisory Authority for Welfare and Health, Valvira.

The Digital and Population Data Services Agency's technical subcontractors have been selected through open EU-tendering and the subcontractors operate on behalf of and at the risk of the Agency.

The following information technology enterprises operate as subcontractors:

- Valtori: certificate management system (use services), hardware, maintenance and management
- Tieto Finland Oy: Vartti software, application management
- Valtori: communications
- Idemia Finland Oy: card production, cards, individualisation, card logistics, maintenance and management
- Fujitsu Finland Oy: card reader software
- Nets A/S, Finnish branch: revocation service, certificate revocation service for end users
- DVV/Public Service Info: advisory services
- Valtori: VRK.FINEID.FI site - certificate retrieval and testing services
- Insta DefSec Oy: Insta Certifier CA software
- Entrust Ltd: Entrust CA software (BIO2)
- Thales e-Security Ltd (nCipher Corporation Ltd): HSM devices
- Valtori (Suomi.fi/identification brokering): access service (incl. telecommunications) and production's application management

The subcontractors maintain the competence of their personnel regarding the hardware, software, methods and data security used as part of the service provision. In addition, the subcontractors ensure that their personnel are familiar with the data-processing tasks of the certificate service as required by the service.



Auditing and certificates

The Digital and Population Data Services Agency has a data security certificate and the Agency's certificate services also have a quality certificate. Both certificates were issued by Inspecta Sertifiointi Oy. The certificates are not permanent. Instead, their retention requires regular monitoring, information security and quality audits, at least annually. The organisation maintains and develops its data security and quality systems and ensures that processes, work performances and services are implemented in accordance with the certified system.

Data security certificate

The Digital and Population Data Services Agency's data security certificate is in accordance with the ISO/IEC 27001:13 standard. It includes information security policy, information security organisation, classification and supervision of protected objects, personnel security, physical information security, management of data traffic and operations, access control, system development and maintenance, and business continuity management and compliance. The standard defines the level of good information security, which is implemented by means of protection mechanisms selected by the organisation.

Certificate services quality system's certificate

The certificate issued to the Digital and Population Data Services Agency's certificate services' quality system complies with SO 9001:2015. The quality system is an important tool in the planning and development of community activities. Its certification, on the other hand, gives the activities and the system public credibility. The purpose of certification is therefore to create a method of continuous improvement while providing global evidence of the quality system's standard conformance.

As per the eIDAS Regulation (applicable as of 1 July 2016), the following accounts must be delivered to the Finnish Transport and Communications Agency: an audit opinion regarding strong electronic identification services prepared by an assessment body (conformance evaluation body), an assessment account regarding trust services prepared by an accredited and approved conformance evaluation body. The services' conformance with eIDAS must be assessed at the intervals laid down in the Act.

By virtue of the collaboration with the police, the Ministry for Foreign Affairs and Valvira, the Digital and Population Data Services Agency delivers an account of its operations to the National Police Board, the Ministry for Foreign Affairs, the Ministry of Social Affairs and Health and Valvira annually/upon request.

Appendices

Service description: the DVV's Citizen Certificate on ID card or another technical platform (only available in Finnish and Swedish)

Certificate services service description: Commercial (only available in Finnish and Swedish)





Social welfare and healthcare sector service description Digital (only available in Finnish and Swedish)

and Population Data Services Agency's certificate services price list (only available in Finnish and Swedish)