DIGITAL AND POPULATION DATA SERVICES AGENCY

Technical Information on Service Certificates

Customer Instructions

8.7.2026

Tel. **+358 295 536 000** (exchange) | Contact Information: **dvv.fi/en**

Table of contents

1 General Information on the Digital and Population Data Services Agency's Service Certificates

The Digital and Population Data Services Agency's (DVV) service certificates are software certificates used to verify a service provider's server or service.

Service certificate is a general term for all service certificate products offered by DVV.

DVV's products are based on the X.509 standard and make it possible to implement SSL/TLS-protected communication between a web browser and a server or between two servers.

DVV is the only Finnish certification authority that officially offers EU-approved server certificates (server certificates, welfare application certificates), i.e. QWAC certificates (Qualified Website Authentication Certificate).

Test certificates intended for testing environments are also available for all service certificates. The content of a test certificate is the same as that of the corresponding production certificate.

DVV does not issue certificates for internal networks or wildcard certificates. As of 15 September 2023, the Digital and Population Data Services Agency no longer issues server certificates or social and healthcare server certificates solely on the basis of an IP address. Therefore, a certificate application must include either a domain name or both a domain name and an IP address.

In addition, from 15 September 2023 onwards, DVV no longer issues server certificates containing an email address. This change does not affect, for example, system signing certificates or client certificates, which are separate certificate types and are not EU-approved products.

The completed service certificate is delivered by email to the technical group email address specified in the application and to the technical contact person specified in the application in DER and PEM file formats.

Descriptions of Data Exchange (palveluväylä) certificates can be found in the service's own customer instructions. In short: the Data Exchange Layer Authentication Certificate is a Customer certificate and the Data Exchange Layer Signature Certificate is a Signature certificate.

During 2026, DVV will offer its customers the possibility to start using the ACME protocol for certificate issuance.

2 Technical Descriptions of Service Certificate Products

This document briefly describes the technical specifications of the service certificates issued by the Digital and Population Data Services Agency.

2.1 Server Certificates

The Digital and Population Data Services Agency is the only Finnish certification authority that officially offers EU-approved QWAC certificates (Qualified Website Authentication Certificate).

With the help of a server certificate, the user of a web service can verify the authenticity of the service provider. Server certificates also enable encryption of data communications between the server and its users.

Technical information for server certificates:

CN (common name)	Domain name or IP address Optional field, discontinued from 1 October 2026. ACME does not use the CN field.	Note: If the CN field contains an IP address, the SAN field must contain at least one domain name.
SerialNumber OrganizationIdentifier	Permitted content is the organization's Business ID (SerialNumber) and any organization identifier permitted under ETSI EN 319 412-1 (OrganizationIdentifier field). Optional field. From 1 October 2026 onwards, and immediately in ACME, the SerialNumber field will be replaced by the OrganizationIdentifier field.	Exception: For Finnish Customs direct customs clearance, the VAT/EORI identifier submitted to Customs in the EDI application must be entered in this field.
O (Organization)	the Organization’s official name	
C (Country)	Country where the organization operates	
L (Location)	City or municipality where the organization is registered	
S (State)	Country subdivision, region or county	Example: Uusimaa
SubjectAlternativeName (SAN)	DNSname1 DNSname2 DNSname3 IPaddress1 etc.	A single certificate request may contain a max 5 domain names and a max 5 IP addresses. A server

		certificate SHALL contain at least one domain name.
CA (intermediate CA / sub-CA)	Production certificates: DVV Service Certificates - G5R or - G5E Test certificates: DVV TEST Service Certificates - G2R or - G2E	
Key Usages	Key Encipherment (RSA) Key Agreement (ECC) Digital Signature	Key Encipherment and Key Agreement will be removed from certificates as of 1 October 2026.
Extended Key Usages	Server Authentication Client Authentication	Note: Client Authentication will be removed from server certificates from 1 October 2026 and in ACME the EKU will not be available from the start.
Key length, hash	Key length is a minimum of 2048 bits for RSA and a minimum of 256 bits for ECC; SHA384 (ECC) and SHA512 (RSA).	
Validity period	Maximum 6 months	From 15 March 2027, maximum 3 months.

Only attributes defined by the RFC 5280 standard are permitted. Certificate requests must not contain any application-specific or vendor-specific (e.g. Microsoft) custom attributes or extensions.

Only certificate requests in PKCS#10 format (.CSR).

2.2 System signature certificates

A system signature certificate is used to electronically sign documents that are not signed with personal certificates.

CN (common name)	System name (e.g. patient information system)	Also permitted content: organization name, domain name, or IP address.
SerialNumber	Organization Business ID	
O (Organization)	Organization official name	
C (Country)	Country where the organization operates	
L (Location)	City or municipality where the organization is registered	
S (State)	Country subdivision, region, or county	

SubjectAlternativeName (SAN)	DNSname1 DNSname2 DNSname3 IPaddress1 etc.	A single certificate request may contain a maximum of 5 domain names and 5 IP addresses. Permitted value: shared email address.
CA (intermediate CA / sub-CA)	Production certificates: DVV Service Certificates - G5R or - G5E Test certificates: DVV TEST Service Certificates - G2R or - G2E	
Key Usages	Digital Signature NonRepudiation	
Extended Key Usages	-	
Key length, hash	The key length for RSA is a minimum of 2048 bits and for ECC a minimum of 256 bits; SHA384 (ECC) and SHA512 (RSA).	
Validity period	Maximum 24 months	

Only attributes according to the RFC 5280 standard are permitted. Certificate requests must not contain application-specific or system-vendor-specific (e.g. Microsoft) custom attributes or extensions.

Only certificate requests in PKCS#10 format (.CSR).

2.3 Client certificates

A client certificate is a certificate for client authentication in interface usage (client authentication). This product was referred to as the client certificate for the VTJ interface until 28.2.2026.

CN (common name)	System name	Also permitted content: organization name, domain name, or IP address.
SerialNumber	Organization Business ID	
O (Organization)	Organization official name	
C (Country)	Country where the organization operates	
L (Location)	City or municipality where the organization is registered	
S (State)	Country subdivision, region, or county	

SubjectAlternativeName (SAN)	DNSname1 DNSname2 DNSname3 IPaddress1 etc.	A single certificate request may contain a maximum of 5 domain names and 5 IP addresses. Permitted value: shared email address.
CA (intermediate CA / sub-CA)	Production certificates: DVV Service Certificates - G5R or - G5E Test certificates: DVV TEST Certificates - G2R or - G2E	
Key Usages	Key Encipherment Digital Signature	
Extended Key Usages	Client Authentication	
Key length, hash	The key length is a minimum of 2048 bits for RSA and a minimum of 256 bits for ECC; SHA384 (ECC) and SHA512 (RSA).	
Validity period	Maximum 12 months	

Only attributes according to the RFC 5280 standard are permitted. Certificate requests must not contain application-specific or system-vendor-specific (e.g. Microsoft) custom attributes or extensions.

Only certificate requests in PKCS#10 format (.CSR).

2.4 Electronic sealing service certificates

DVV provides an electronic sealing service and a test electronic sealing service. Seal certificates and seal interface certificates are issued only to organizations that have ordered the electronic sealing service or test electronic sealing service.

2.5 E-mail certificates

An E-mail certificate is intended for verifying shared email addresses used by organizations. With an E-mail certificate, you can receive encrypted messages and sign outgoing messages. Encrypted messages sent to the organization's email address are opened using the E-mail certificate.

CN (common name)	A name describing the mailbox, for example "Company Name", "Invoicing", or similar.	
SerialNumber	Organization's Business ID	

O (Organization)	Organization's official name	
C (Country)	Country where the organization operates	
L (Location)	City or municipality where the organization is registered	
S (State)	Country subdivision, region, or county	
SubjectAlternativeName (SAN)	eMail address	Note: DVV only issues email certificates for shared email addresses where the domain portion belongs to the organization.
CA (intermediate CA / sub-CA)	DVV Enterprise Certificates	
Key Usages	Key Encipherment Digital Signature	
Extended Key Usages	eMail protection	
Key length, hash	Key length is 2048 or 4096 bits; SHA384 (ECC) and SHA512 (RSA).	
Validity period	Maximum 24 months	

The email certificate is file-based and does not require card readers or separate software for use. The E-mail certificate works in the most common email applications supporting S/MIME messages, such as Microsoft Outlook.

E-mail certificates are provided in PKCS#12 format.

2.6 Health care server certificates

An organization connecting as a user of the Kanta Services requires a server certificate for the use of ePrescription and eArchive services. The server certificate is needed to secure the data communication connection (TLS-protected) between the organization's server and the Kanta servers. This certificate is an EU-approved QWAC certificate (Qualified Website Authentication Certificate).

CN (common name)	Domain name or IP address Optional field. The field will be discontinued on 1 October 2026. ACME does not use the CN field.	Note: If the CN field contains an IP address, the SAN field must contain at least one domain name.
SerialNumber OrganizationIdentifier	KELA/THL National Code Server OID (SerialNumber).	From 1 October 2026 onwards, the OrganizationIdentifier field

	In the OrganizationIdentifier field, the OID is entered in the format SO:FI-OID.	will be used (and in ACME already from implementation); before that, the SerialNumber field is used.
O (Organization)	Organization's official name: KELA/THL National Code Server	
C (Country)	Country where the organization operates	
L (Location)	City or municipality where the organization is registered	
S (State)	Country subdivision, region, or county	Example: Uusimaa
SubjectAlternativeName (SAN)	DNSname1 DNSname2 DNSname3 IPaddress1 etc.	A single certificate request may contain a maximum of 5 domain names and 5 IP addresses. The field must contain at least one domain name.
CA (intermediate CA / sub-CA)	Production certificates: DVV Social Welfare and Healthcare Service Certificates - G3R or - G3E Test certificates: DVV TEST Social Welfare and Healthcare Service Certificates - G3R or - G3E	
Key Usages	Key Encipherment (RSA) Key Agreement (ECC) Digital Signature	Key Encipherment and Key Agreement will be removed from certificates from 1 October 2026 onwards.
Extended Key Usages	Server Authentication Client Authentication	Note: Client Authentication will be removed from the certificate from 1 October 2026 onward, and in ACME the EKU will not be available from the start.
Key length, hash	The key length is a minimum of 3072 bits for RSA and a minimum of 256 bits for ECC; SHA384 (ECC) and SHA512 (RSA).	
Validity period	Maximum 6 months	From 15 March 2027, maximum 3 months.

Only attributes according to the RFC 5280 standard are permitted. Certificate requests must not contain application-specific or system-vendor-specific (e.g. Microsoft) custom attributes or extensions.

Only certificate requests in PKCS#10 format (.CSR).

2.7 Health care system signing certificates

When connecting as a user of the Kanta Services Patient Data Repository, a system signing certificate is required.

A system signing certificate is used to electronically sign documents that are not signed using healthcare personal certificates.

CN (common name)	System name, e.g. patient information system	Also permitted content: organization name, domain name, or IP address.
SerialNumber	KELA/THL National Code Server OID	
O (Organization)	Organization's official name: KELA/THL National Code Server	
C (Country)	Country where the organization operates	
L (Location)	City or municipality where the organization is registered	
S (State)	Country subdivision, region, or county	
SubjectAlternativeName (SAN)	Optional field: DNSname1 DNSname2 DNSname3 IPaddress1 etc.	A single certificate request may contain a maximum of 5 domain names and 5 IP addresses. Permitted value: shared email address.
CA (intermediate CA / sub-CA)	Production certificates: DVV Social Welfare and Healthcare Service Certificates - G3R or - G3E. Test certificates: DVV TEST Social Welfare and Healthcare Service Certificates - G3R or - G3E.	
Key Usages	Digital Signature NonRepudiation	
Extended Key Usages	-	
Key length, hash	The key length is a minimum of 3072 bits for RSA and a minimum of 256 bits for ECC; SHA384 (ECC) and SHA512 (RSA).	
Validity period	Maximum 24 months	

Only attributes according to the RFC 5280 standard are permitted. Certificate requests must not contain application-specific or system-vendor-specific (e.g. Microsoft) custom attributes or extensions.

Only certificate requests in PKCS#10 format (.CSR).

2.8 Health care client certificates

A client certificate is a certificate for client authentication in interface usage (client authentication). Some organizations connecting as users of the Kanta Services require a health care server certificate, while others require a health care client certificate (contact Kela if there is uncertainty regarding which certificate is needed). Some organizations will require both certificates mentioned above from 1 October 2026 onwards, when Client Authentication is removed from server certificates.

CN (common name)	System name	Also permitted content: organization name, domain name, or IP address.
SerialNumber	KELA/THL National Code Server OID	
O (Organization)	Organization's official name: KELA/THL National Code Server	
C (Country)	Country where the organization operates	
L (Location)	City or municipality where the organization is registered	
S (State)	Country subdivision, region, or county	
SubjectAlternativeName (SAN)	Optional field: DNSname1 DNSname2 DNSname3 IPaddress1 etc.	A single certificate request may contain a maximum of 5 domain names and 5 IP addresses. Permitted value: shared email address.
CA (intermediate CA / sub-CA)	Production certificates: DVV Social Welfare and Healthcare Service Certificates - G3R or - G3E Test certificates: DVV TEST Social Welfare and Healthcare Service Certificates - G3R or - G3E	
Key Usages	Key Encipherment Digital Signature	
Extended Key Usages	Client Authentication	

Key length, hash	The key length is a minimum of 2048 bits for RSA and a minimum of 256 bits for ECC; SHA384 (ECC) and SHA512 (RSA).	
Validity period	Maximum 12 months	

Only attributes according to the RFC 5280 standard are permitted. Certificate requests must not contain application-specific or system-vendor-specific (e.g. Microsoft) custom attributes or extensions.

Only certificate requests in PKCS#10 format (.CSR).

2.9 Service certificates for wellbeing applications

A server certificate issued for secure message communications in KELA welfare applications. Examples include mobile applications through which users collect health information about an individual and transmit it to Kela's MyKanta service for further use. This certificate is an EU-approved QWAC certificate (Qualified Website Authentication Certificate).

CN (CommonName)	Domain name or IP address. Not a mandatory field. The field will be discontinued on 1 October 2026. ACME does not use the CN field.	Note: If the CN field contains an IP address, the SAN field must contain at least one domain name.
SerialNumber OrganizationIdentifier	KELA/THL National Code Server OID (SerialNumber). In the OrganizationIdentifier field, the OID is entered in the format SO:FI-OID.	From 1 October 2026 onwards, the OrganizationIdentifier field will be used (and in ACME already from implementation); before that, the SerialNumber field is used.
O (Organization)	Organization's official name: KELA/THL National Code Server	
C (Country)	Country where the organization operates	
L (Location)	City or municipality where the organization is registered	
S (State)	Country subdivision, region, or county	T.ex. Uusimaa
SubjectAlternativeName (SAN)	Optional field: DNSname1 DNSname2 DNSname3	A single certificate request may contain a maximum of 5 domain names and 5 IP addresses.

	IPaddress1 etc.	The field must contain at least one domain name.
CA (intermediate CA / sub-CA)	Production certificates: DVV Service Certificates - G5R or - G5E. Test certificates: DVV TEST Service Certificates - G2R or - G2E.	
Key Usages	Key Encipherment (RSA) Key Agreement (ECC) Digital Signature	Key Encipherment and Key Agreement will be removed from certificates from 1 October 2026 onwards.
Extended Key Usages	Server Authentication Client Authentication	Note: Client Authentication will be removed from the certificate from 1 October 2026 onward and in ACME the EKU will not be available from the start.
Key length, hash	The key length is a minimum of 3072 bits for RSA and a minimum of 256 bits for ECC; SHA384 (ECC) and SHA512 (RSA).	
Validity period	Maximum 6 months	From 15 March 2027, maximum 3 months.

Only attributes according to the RFC 5280 standard are permitted. Certificate requests must not contain application-specific or system-vendor-specific (e.g. Microsoft) custom attributes or extensions.

Only certificate requests in PKCS#10 format (.CSR) are accepted.

2.10 Client certificates for wellbeing applications

A certificate issued to secure message traffic in KELA welfare applications. Examples include mobile applications through which users collect health information about an individual and transmit it to Kela's MyKanta service for use.

CN (CommonName)	System name	Also permitted content: organization name, domain name, or IP address.
SerialNumber	KELA/THL National Code Server OID (SerialNumber).	
O (Organization)	Organization's official name: KELA/THL National Code Server	
C (Country)	Country where the organization operates	

L (Location)	City or municipality where the organization is registered	
S (State)	Country subdivision, region, or county	Example: Uusimaa
SubjectAlternativeName (SAN)	Optional field: DNSname1 DNSname2 DNSname3 IPaddress1 etc.	A single certificate request may contain a maximum of 5 domain names and 5 IP addresses. Permitted value: shared email address.
CA (intermediate CA / sub-CA)	Production certificates: DVV Service Certificates - G5R or - G5E Test certificates: DVV TEST Service Certificates - G2R or - G2E	
Key Usages	Key Encipherment Digital Signature	
Extended Key Usages	Client Authentication	
Key length, hash	The key length is a minimum of 3072 bits for RSA and a minimum of 256 bits for ECC; SHA384 (ECC) and SHA512 (RSA).	
Validity period	Max. 12 months	

Only attributes according to the RFC 5280 standard are permitted. Certificate requests must not contain application-specific or system-vendor-specific (e.g. Microsoft) custom attributes or extensions.

Only certificate requests in PKCS#10 format (.CSR).