CDigiDoc Programmer’s Guide

Document Version: 3.8

Library Version: 3.8

Last update: 11.12.2013

1. Document versions

Document information	
Created on	22.01.2013
Reference	CDigiDoc Programmer's Guide
Receiver	Sertifitseerimiskeskus AS
Author	Veiko Sinivee, Kersti Üts, Kristi Uukkivi
Version	3.8

Version information		
Date	**Version**	**Changes**
27.03.2006	2.2.5	The latest version of "DigiDoc C library" created by Veiko Sinivee
03.02.2012		Initial draft by KnowIT for the new version based on v2.2.5
22.02.2012	3.6	Updated to 3.6 version
22.05.2012	3.6.1	Revised configuration, certificates' usage and CDigiDoc utility program's description
22.01.2013	3.7	Updated to 3.7 version: updated instructions of PKCS#12 (software token) usage; removed EMBEDDED content type support, added description of signing and encryption/decryption operations in memory; added description of signature verification settings; added API description of decrypting large files, added description of using CNG API and minidriver for signature creation.
11.12.2013	3.8	Changed the layout of the document for better readability. Updated according to changes of v3.8 of the library: added support for Finnish CA certificates, changed the validation process of signed files (see chap. 5.2); removed utility program's command –list.

Table of contents

2. Introduction

This document describes CDigiDoc (also known as LibDigiDoc) – the C library for OpenXadES/DigiDoc system. It is a basic building tool for creating applications handling digital signatures and their verification.

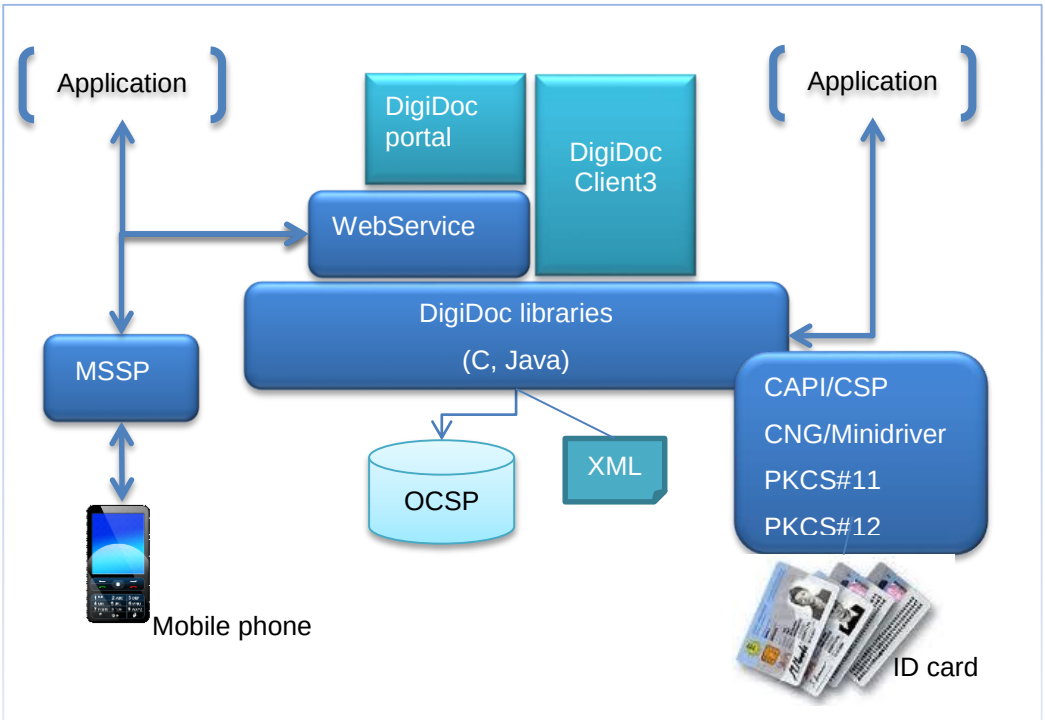
The digitally signed files are created in "DigiDoc format" (with .ddoc file extension), compliant to XML Advanced Electronic Signatures (XAdES), technical standard published by European Telecommunication Standards Institute (ETSI). CDigiDoc is also capable of encrypting/decrypting files (signed or unsigned), according to W3C XML Encryption Recommendation (XML-ENC).

This document covers the following information about CDigiDoc:

- Section 2 introduces the OpenXAdES/DigiDoc framework, its general security model and formats available for digitally signed files.
- Section 3 gives an overview of the CDigiDoc library by describing the supported functionality and additional features, the general architecture of components and describes the dependencies.
- Section 4 explains CDigiDoc configuration possibilities.
- Section 5 provides samples for handling digitally signed files by using the CDigiDoc API's classes and methods.
- Section 6 explains using the command line utility program of CDigiDoc, including sample use cases.
- Section 7 gives overview of supported Estonian and cross-border Certificate Authorities, and describes the interoperability testing of DigiDoc file formats.
- Section 8 gives an overview of CDigiDoc library's implementation notes which provide information about specific features of digitally signed files that are not defined in standards or specification documents but are implemented in CDigiDoc library.
- Appendix 1 provides a sample digidoc.ini configuration file.
- Appendix 2 describes different digital signature types that can be created with CDigiDoc library.

2.1 About DigiDoc

CDigiDoc library forms a part of the wider OpenXAdES/DigiDoc system framework which offers a full-scale architecture for digital signature and documents, consisting of software libraries (C and Java), web service and end-user applications such as DigiDoc Portal and DigiDoc Client3 according to the following figure:



1 DigiDoc framework

It is easy to integrate DigiDoc components into existing applications in order to allow for creation, handling, forwarding and verification of digital signatures and support file encryption/decryption. All applications share a common digitally signed file format (current version DIGIDOC-XML 1.3) which is a profile of XAdES.

2.2 DigiDoc security model

The general security model of the DigiDoc and OpenXAdES ideology works by obtaining proof of validity of the signer's X.509 digital certificate issued by a certificate authority (CA) at the time of signature creation.

This proof (also named as "time-mark") is obtained in the format of Online Certificate Status Protocol (OCSP, [5]) response. Also, the hash of the created signature is sent within the OCSP request and received back within the response. This allows interpreting of the positive OCSP response as "at the time I saw this digitally signed file, corresponding certificate was valid", meaning that the OCSP response gives proof for the signer certificate's validity and also proof of the time when the signature existed. Thus, the time of issuing the OCSP response is interpreted as trusted signature creation time.

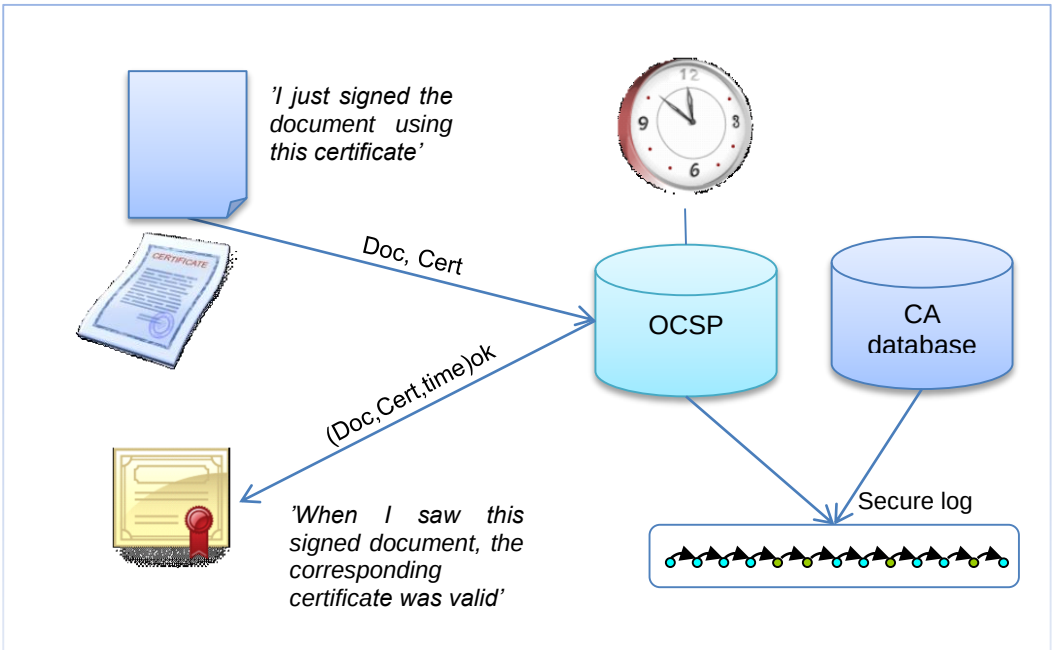
The OCSP response is stored within the signed document. This allows the signing time and signer certificate's validity to be validated later on, even after the signer's certificate has become invalid.

The OCSP service is acting as a digital e-notary confirming signatures created locally with a smart card. From infrastructure side, this security model requires a standard OCSP responder. Hash of the signature is placed on the "nonce" field of the OCSP request structure. In order to achieve the freshest certificate validity information, it is recommended to run the OCSP responder in "real-time" mode meaning that:

- certificate validity information is obtained from live database rather than from CRL (Certificate Revocation List)
- the time value in the OCSP response is actual (as precise as possible)

To achieve long-time validity of digital signatures, a secure log system is employed within the model. All OCSP responses and changes in certificate validity are securely logged to preserve digital signature validity even after private key compromise of CA or OCSP responder. It is important to notice that additional time-stamps are not necessary when employing the security model described:

- time of signing and time of obtaining validity information is indicated in the OCSP response
- the secure log provides for long-time validity without need for archival timestamps



2 DigiDoc security model

2.3 Format of digitally signed file

The format of the digitally signed file is based on **ETSI TS 101 903** standard called **XML Advanced Electronic Signatures (XAdES)**. This standard provides syntax for digital signatures with various levels of additional validity information. CDigiDoc is implementing a subset of these standards.

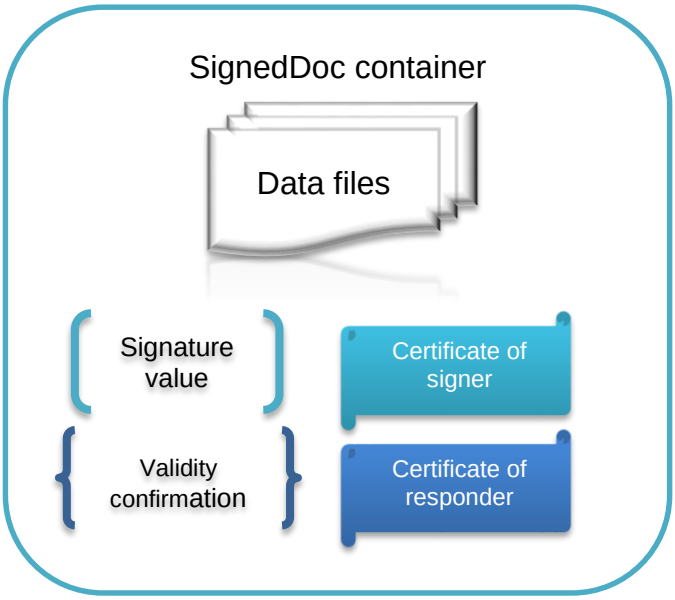
In order to comply with the security model described above, the XAdES profile **XAdES-X-L** is used in the DigiDoc system but "**time-marks**" are used instead of "time-stamps" – signing (and certificate validation) time comes with OCSP response.

This profile:

- allows for incorporating following signed properties
  - Certificate used for signing
  - Claimed signing time (the signer's computer time)
  - Signature production place (optional)
  - Signer role or resolution (optional)
- incorporates full certificate validity information within the signature
  - OCSP response
  - OCSP responder certificate

As a result, it is possible to verify signature validity without any additional external information – the verifier should trust the issuer of signer's certificate and the OCSP responder's certificate.

Original files (which were signed) along with the signature(s), validation confirmation(s) and certificates are encapsulated within container with "SignedDoc" as a root element.



3 SignedDoc container

The library currently offers DIGIDOC-XML document format to be used.

The DIGIDOC-XML document format (currently supported version 1.3) is fully conforming to XAdES standard (note however that not every single detail allowed in XAdES standard is supported).

DigiDoc system uses file extension **.ddoc** to distinguish digitally signed files according to the described file format. Syntax of the .ddoc file is described in a separate document in detail (see [1]).

The DIGIDOC-XML document's container is a single XML file which contains embedded data file(s) and signature(s). It is possible to add data files to the container by embedding binary data in base64 encoding (EMBEDDED_BASE64 mode). Embedding pure text or XML (EMBEDDED mode) and adding only reference to and external file (DETACHED mode) is no longer supported.

SHA-1 digest type is supported and set automatically.

3. Overview

The current chapter gives an overview of **CDigiDoc** software library by describing the supported functionality, the general architecture and CDigiDoc library's dependencies.

3.1 References and additional resources

[1] DIGIDOC-XML 1.3	DigiDoc format specification, version 1.3.0 http://id.ee/public/DigiDoc_format_1.3.pdf
[2] XML-DSIG	IETF RFC 3275: XML-Signature Syntax and Processing http://www.ietf.org/rfc/rfc3275.txt
[3] XAdES	ETSI TS 101 903 V1.4.2 (2010-12) – XML Advanced Electronic Signatures http://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.02_60/ts_101903v010402p.pdf
[4] XML Schema 2	XML Schema Part 2: Data types. W3C Recommendation 02 May 2001 (http://www.w3.org/TR/xmlschema-2/)
[5] RFC2560	Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C., X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol - OCSP. June 1999
[6] DSA	Estonian Digital Signatures Act http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30081K6&keel=en&pg=1&ptyyp=RT&tyyp=X&query=digitaalallkirja
[7] XML-ENC	http://www.w3.org/TR/xmlenc-core/
[8] CDOC 1.0	Encrypted DigiDoc Format Specification http://id.ee/public/SK-CDOC-1.0-20120625_EN.pdf
[9] DigiDocService Specification	EN: http://sk.ee/upload/files/DigiDocService_spec_eng.pdf ET: http://www.sk.ee/upload/files/DigiDocService_spec_est.pdf
[10] X.509 V3 Certificate Profile	ETSI TS 102 280 (V1.1.1) - X.509 V3 Certificate Profile for Certificates Issued to Natural Persons http://www.etsi.org/deliver/etsi_ts/102200_102299/102280/01.01.01_60/ts_102280v010101p.pdf
[11] ESTEID profile	Certificates on identity card of Republic of Estonia, version 3.3 https://sk.ee/upload/files/ESTEID_profiil_en-3_3.pdf
[12] Institution certificate profile	Profile of institution certificates and Certificate Revocation Lists, version 1.3 https://sk.ee/upload/files/SK_Profile%20of%20institution%20certificates%20and%20Revocation%20List.pdf
[13] DigiDoc libraries	http://id.ee/index.php?id=30486

[14] Release notes	CDigiDoc library's release notes (http://id.ee/index.php?id=35782)

3.2 Terms and acronyms

CDOC (.cdoc)	The term denotes a format of an encrypted DigiDoc document that is based on XML-ENC profile. The document format has been defined in [8].
CRL	Certificate Revocation List, a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked, and therefore should not be relied upon.
CAPI	Microsoft CryptoAPI, Cryptographic Application Programming Interface. API for implementing cryptographic operations in Windows operating systems
CNG	Cryptography API: Next Generation. Updated version of Microsoft CryptoAPI (CAPI).
CSP	Microsoft Crypto Service Provider. Software library that implements Microsoft CryptoAPI (CAPI)
DIGIDOC-XML (.ddoc)	The term is used to denote a DigiDoc document format that is based on the XAdES standard and is a profile of that standard. The profile does not exactly match any subsets described in XadES standard – the best format name would be "XadES-C-L" indicating that all certificates and OCSP confirmations are present but there are no "pure" timestamps. A DIGIDOC-XML file is basically a <SignedDoc /> container that contains original data files and signatures. The file extension for DIGIDOC-XML file format is ".ddoc", MIME-type is "application/ddoc".
Minidriver	A device driver for controlling interaction with an identity token in Windows operating systems.
OCSP	Online Certificate Status Protocol, an Internet protocol used for obtaining the revocation status of an X.509 digital certificate
OCSP Responder	OCSP Server, maintains a store of CA-published CRLs and an up-to-date list of valid and invalid certificates. After the OCSP responder receives a validation request (typically an HTTP or HTTPS transmission), the OCSP responder either validates the status of the certificate using its own authentication database or calls upon the OCSP responder that originally issued the certificate to validate the request. After formulating a response, the OCSP responder returns the signed response, and the original certificate is either approved or rejected, based on whether or not the OCSP responder validates the certificate.
PKCS#11	RSA Laboratories Cryptographic Token Interface Standard
SK	AS Sertifitseerimiskeskus (Certification Centre Ltd.). Certificate Authority in Estonia

X.509	an ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI) which specifies standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm
XAdES	XML Advanced Electronic Signatures, a set of extensions to XML-DSig recommendation making it suitable for advanced electronic signature. Specifies precise profiles of XML-DSig for use with advanced electronic signature in the meaning of European Union Directive 1999/93/EC.
XML-DSig	a general framework for digitally signing documents, defines an XML syntax for digital signatures and is defined in the W3C recommendation XML Signature Syntax and Processing

3.3 Supported functional properties

CDigiDoc is a library in C programming language offering the following functionality:

- **Creating files** in DIGIDOC-XML 1.3 format and **adding data files**.
- Digitally **signing** the DigiDoc files using smart cards or other supported cryptographic tokens.
- Adding **time marks** and **validity confirmations** to digital signatures using OCSP protocol.
- **Validating** the digital signatures.
- Digital **encryption and decryption** of the DigiDoc files.

Note: older DigiDoc file formats SK-XML, DIGIDOC-XML 1.1 and DIGIDOC-XML 1.2 are supported only for backward compatibility in case of digital signature verification and data file extraction operations (creating new files and adding signatures is no longer supported).

The following table describes functional features that are supported with CDigiDoc.

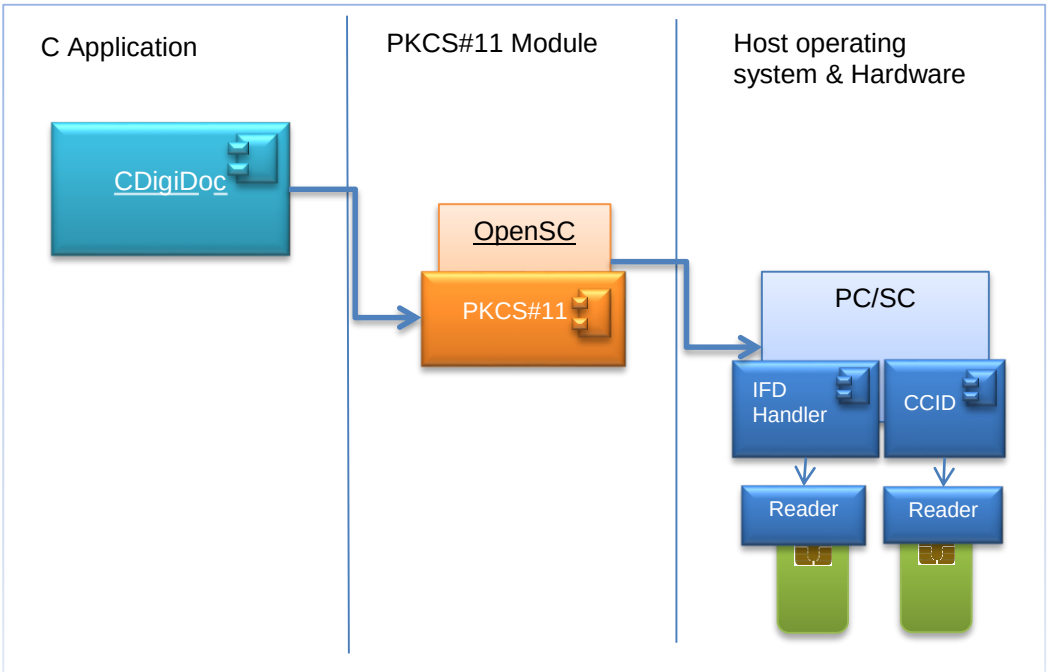
Feature	Supported values
Signed DigiDoc document format	- **DIGIDOC-XML 1.3** – the main document format to be used for signature creation, described in [1]. **Note**: older DigiDoc file formats SK-XML, DIGIDOC-XML 1.1 and DIGIDOC-XML 1.2 are supported only for backward compatibility in case of digital signature validation and data file extraction operations (creating new files and modifying existing files is not supported).
Signature creation module	- **PKCS#11 –** the default module for singing with smart card (e.g. Estonian ID card or any other smartcard provided that you have the external native PKCS#11 driver for it). - **PKCS#12 –** module for signing with a software token. - **CNG -** Microsoft CNG API and minidriver for signing with smart card in Windows environment. A dialog window is opened for the user to choose the signing certificate and enter PIN code.

Cryptographic token type	- **Smart card,** e.g. Estonian ID card. Supported signature creation module is PKCS#11 and CNG/minidriver. - **Software token -** a PKCS#12 container (.p12 or .pfx) file which includes a certificate and accompanying public and private keys in a single file. The private key is protected with a password-based symmetric key. The token is named "software token" as it is stored in the file system and not on a smartcard or other physical cryptographic device. Supported signature creation module is PKCS#12. Note that the signature that is created with a software token is a technical signature and is expected to produce verification error messages (see also Appendix 2). - **USB cryptostick** - Aladdin eToken device. Note that the usage of this token with CDigiDoc library is tested only indirectly via DigiDoc3 Client application.
Public-key algorithm	- **RSA**
Encrypted document format	- **XML-ENC 1.0**

Further information about specific functional features that are not strictly defined in specification documents but are implemented in CDigiDoc library can be found from chapter "8 CDigiDoc library's implementation notes".

3.4 Component model

The figure below describes the architecture of software and hardware components that are used when creating signatures with CDigiDoc library when using PKCS#11 module.



4 Sample CDigiDoc implementation using PKCS#11/ smart cards for digital signing

Component	Description
OpenSC	Set of libraries and utilities to work with smart cards, implementing PKCS#11
PKCS#11	Widely adopted platform-independent API to cryptographic tokens (HSMs and smart cards), a standard management module of the smart card and its certificates
PC/SC	Standard communication interface between the computer and the smart card, a cross-platform API for accessing smart card readers
IFDHandler	Interface Device Handler for CCID readers
CCID	USB driver for Chip/Smart Card Interface Devices
Reader	Device used for communication with a smart card

Note that in case of Windows environment, there can be two instances of the library installed concurrently. If you download and install the library's distribution package then it is stored to "c:\Program Files\Estonian ID Card Development\libdigidoc" directory by default. However, if you have DigiDoc Client3 program installed then the library is also included in its installation files ("c:\Program Files\Estonian ID Card" directory by default). Note that conflicts could occur between the two installations.

3.5 CDigiDoc architecture

The CDigiDoc library consists of three kinds of components:

- **Data structures** – declarations of data structures can be found in file DigiDocLib.h.
- **Constants** – a number of constants are used by the library, including error codes. Their definitions can be found in files DigiDocLib.h and DigiDocError.h.
- **Functions** – defined in *.c files of the library. Functions of public interest have been declared in file DigiDocLib.c.

For additional information about the functions and data structures of CDigiDoc library, see the full API description that is included in the CDigiDoc library's installation package, in directory /documentation/api.

3.6 Dependencies

CDigiDoc depends on the libraries listed below.

Base Component	Description
OpenSSL	Used for validating certificates and digest values. Source code is available from: http://www.openssl.org/
libxml2	XML parser. Source code is available from: http://www.xmlsoft.org/
Zlib	Compression library. Source code is available from: http://zlib.net/
iconv	Used for encoding. Source code is available from: http://www.gnu.org/software/libiconv/

4. Configuring CDigiDoc

4.1 Loading configuration settings

CDigiDoc uses functions in DigiDocConfig.h/c source files for reading configuration data from property files. Sample configuration files are included in the library's installation package.

In Windows environment, the configuration file is named **digidoc.ini**, in Linux environment the file is named **digidoc.conf**.

Configuration settings may be loaded from different configuration files if the respective files are provided in system. Every subsequent configuration file complements the already present parameter values (i.e. doesn't delete the previous entries). CDigiDoc looks for configuration files in the following sequence:

1) system directory - C:\Windows\digidoc.ini in case of Windows environment or /etc/digidoc.conf in case of Linux. Specifies global settings that have effect on all the users of the computer.
2) user's home directory - c:\Users\<username>\digidoc.ini or /home/<username>/.digidoc.conf (notice the '.'), according to your environment.
3) current working directory - digidoc.ini or digidoc.conf, according to your environment.
4) in case of utility program, the configuration file that is provided with –config command.
5) in case of Windows environment, the Windows registry entries.

It is also possible to use a different configuration file location than the default. In that case, the configuration file's full filename and path should be passed to initConfigStore() function defined in DigiDocConfig.h or in case of CDigiDoc utility program, the file's location should be passed to the program with "–config" parameter (see section 4 for more information).

Note that if a configuration file is passed directly to initConfigStore() function or CDigiDoc utility program then this file is used over other files that might be stored in the default location(s).

For a sample configuration file provided with CDigiDoc, see Appendix 1.

4.2 Configuration parameters

Below is an overview of the configuration file's main sections and entries. The following color notation is used for specific parameter values:

- ***bold*** for default values which do not usually need to be changed by the user
- purple for indicating values which should be checked and modified according to user
- # blue for listing possible alternatives, where applicable

PKCS#11 driver settings

If using the smart card over PKCS#11 module for creating signatures, then you must specify the following parameters according to your signature device here:

Parameter	Comments
DIGIDOC_DEFAULT_DRIVER	Specifies the default PKCS#11 driver library that is used to communicate with the smart card. ***1***
DIGIDOC_DRIVERS	Number of PKCS#11 drivers registered in the configuration file. Only one PKCS#11 driver at a time should be registered in a configuration file.

	1
DIGIDOC_DRIVER_1_NAME	Name of the registered PKCS#11 driver library ***OpenSC***
DIGIDOC_DRIVER_1_DESC	PKCS#11 driver's description ***OpenSC projects PKCS#11 driver***
DIGIDOC_DRIVER_1_FILE	PKCS#11 driver library's filename ***opensc-pkcs11.dll (used in Windows environment)*** *# opensc-pkcs11.so (used in Linux environment)*

OCSP responder settings

This DIGIDOC_OCSP_RESPONDER_URL setting applies to your default OCSP responder address when no other OCSP responder address for the CA is found in the OCSP responder data registered in your configuration file entries.

The default OCSP responder has been set to http://ocsp.sk.ee which can be used with real-life Estonian ID cards.

Parameter	Description
DIGIDOC_OCSP_URL	OCSP responder address ***http://ocsp.sk.ee***

Settings for signing OCSP requests or not

Whether you need to sign the OCSP requests sent to your OCSP responder or not depends on your responder.

Some OCSP servers require that the OCSP request is signed. To sign the OCSP request, you need to obtain and specify the certificates, which will be used for signing.

For example, accessing the SK's OCSP Responder service by private persons requires the requests to be signed (limited access certificates can be obtained through registering for the service) whereas in case of companies/services, signing the request is not required if having a contract with SK and accessing the service from specific IP address(es).

By default, this parameter value is set to "false" – i.e. the OCSP requests will not be signed.

If setting this to "true", you will also need to provide your access certificate's file location and password that have been issued to you for this purpose.

Parameter	Description
SIGN_OCSP	Specifies if OCSP requests are signed or not. Possible values: true – signed; false – not signed. ***false***
DIGIDOC_PKCS_FILE	Specifies your access certificate's PKCS#12 container location and filename, e.g. ***C:\temp\369787.p12d***
DIGIDOC_PKCS_PASSWD	Specifies your access certificate's PKCS#12 container's password, e.g. ***m15eTGpA***

HTTP proxy settings*

*only necessary if using a proxy to access internet. Please note that configuring the following proxy settings has only been tested with DigiDoc Client3 program.

Parameter	Description
USE_PROXY	Specifies whether proxy is used. Possible values: true – used; false – not used. ***false***
DIGIDOC_PROXY_HOST	Specifies the proxy hostname, e.g. ***proxy.example.net***
DIGIDOC_PROXY_PORT	Specifies the proxy port, e.g. ***8080***

DIGIDOC_PROXY_USER	Specifies proxy server's username
DIGIDOC_PROXY_PASS	Specifies proxy server's password

CA certificates

The CA certificates are used to check the signer's certificate's validity. The certificates have to be in PEM format.

By default, the Estonian and Finnish[1] CA's certificates (both live and test certificates) have been registered in the CDigiDoc configuration file. The Estonian live CA and OCSP certificate files have been included in the CDigiDoc distribution; Finnish live certificates have to be installed with a separate package, accessible from https://installer.id.ee/media/windows/Eesti_ID_kaart_finsertifikaadid.msi

Both Estonian and Finnish test certificates can be installed with a package accessible from https://installer.id.ee/media/windows/Eesti_ID_kaart_testsertifikaadid.msi.

More information about the supported CA-s and certificates can be found from chapter "7.1 National PKI solutions and support".

Note: test certificates should not be used in live applications as the CDigiDoc library does not give notifications to the user in case of test signatures (since the library's version v3.8, the utility program displays test signature warning to the user).

Parameter	Description
CA_CERT_PATH	Location of CA certificates. Supported Estonian CA certificates are included in CDigiDoc's installation package and will be located in the installation directory, e.g. ***C:\Program Files\Estonian ID Card Development\libdigidoc\certs***
CA_CERTS	Number of CA certificates registered in the configuration file, e.g. ***16***
CA_CERT_1 … CA_CERT_*n*	Name of a certificate file, e.g. ***ESTEID-SK 2007.crt***
CA_CERT_1_CN … CA_CERT_*n*_CN	Certificate's common name, e.g. ***ESTEID-SK 2007***

OCSP responder certificates

The following details should be provided for each OCSP Responder when OCSP responses are used in signature creation and verification. The certificates have to be in PEM format.

The DIGIDOC_OCSP_RESPONDER_CERT_*n*_URL parameter is optional and has to be specified only in case of OCSP responder certificates which are used for testing purposes. In case of OCSP responders that correspond to test certificates registered in the CDigiDoc configuration file, the OpenXAdES OCSP Responder URL has been provided (http://www.openxades.org/cgi-bin/ocsp.cgi). For more information on using the OpenXAdES testing environment, please refer to http://www.id.ee/?lang=en&id=35755.

Parameter	Description
DIGIDOC_OCSP_RESPONDER_CERTS	Number of OCSP Responder certificates registered in the configuration file, e.g. ***18***

[1] Since v3.8, the library supports validation of signatures that are created with Finnish live and test certificates.

DIGIDOC_OCSP_RESPONDER_CERT_1 … DIGIDOC_OCSP_RESPONDER_CERT_*n*	OCSP Responder certificate file's name, e.g. ***EID-SK OCSP 2006.crt***
DIGIDOC_OCSP_RESPONDER_CERT_1_1 … DIGIDOC_OCSP_RESPONDER_CERT_*n_n*	Additional certificate for the OCSP Responder, can be used if the alternative certificate is about to expire and new certificate is not yet valid, e.g. ***EID-SK OCSP.crt***
DIGIDOC_OCSP_RESPONDER_CERT_1_CN … DIGIDOC_OCSP_RESPONDER_CERT_*n*_CN	Name of the specific OCSP responder, e.g. ***EID-SK OCSP RESPONDER***
DIGIDOC_OCSP_RESPONDER_CERT_1_CA … DIGIDOC_OCSP_RESPONDER_CERT_*n*_CA	Name of the CA for the specific OCSP responder, e.g. ***EID-SK***
DIGIDOC_OCSP_RESPONDER_CERT_1_URL … DIGIDOC_OCSP_RESPONDER_CERT_*n*_URL	Address for the OCSP responder, has to be specified in case of OCSP responders for test certificates, e.g. ***http://www.openxades.org/cgi-bin/ocsp.cgi***

Encryption settings

Parameter	Description
DENC_COMPRESS_MODE	Compression mode of the original data before encryption. Possible values are 0 – always compress, 1 – never compress, 2 – best effort (compression is used only if it results in reduced data size). ***0*** # 1, # 2 Note that in CDigiDoc utility program, "always compress" mode is used by default.

Debugging settings

Parameter	Description
DEBUG_LEVEL	Specifies the amount of debugging information printed out during execution. Possible value range: 0 – 9, e.g. ***3***
DEBUG_FILE	Full filename and path of debugging log file. If the parameter is set then debugging output is written to the specified file, e.g. ***c:\Temp\debug.log*** Note that the directory has to exist before debugging, otherwise the file is not created.

Signature verification settings

Parameter	Description
CHECK_OCSP_NONCE	Specifies if the OCSP response's nonce field's ASN.1 structure is checked during signature verification. By default, the value is set to false in order to support verification of DigiDoc files created with CDigiDoc library's version below v3.7. ***false*** # true

Note: The ASN.1 prefix specifies the digest algorithm that was used to calculate the nonce field's value, the prefix is mandatory according to RFC2560 specification (see also [5]). If the

ASN.1 prefix is checked then it must contain the octet string ASN.1 identificator (0x04 0x14 in case of DDOC 1.3).

Data file content type setting

Parameter	Description
EMBEDDED_XML_SUPPORT	Specifies if CDigiDoc allows handling ddoc files that contain payload data as pure text or XML (data file content has been added in EMBEDDED mode). Should be used only to add backward compatibility for reading and validating EMBEDDED ddoc files. By default, EMBEDDED content mode is not supported (expected to produce a respective error message). Possible values are: false – not supported, true – supported.

Configuring software token usage

CDigiDoc supports using software tokens (PKCS#12 files) for creating technical signatures and decrypting files.

- No additional configuration settings have to be applied in case of decrypting with software token.
- In case of digital signing with software token, apply the following settings in CDigiDoc configuration file:

```
DIGIDOC_SIGNATURE_SLOT=0
KEY_USAGE_CHECK=0
```

Note that when verifying signatures that are created with the parameter value "KEY_USAGE_CHECK=0", an error message "Error: 39 - Signer's cert does not have non-repudiation bit set!" is produced.

5. Using CDigiDoc API

5.1 Digital signing

CDigiDoc library offers creating, signing and verification of digitally signed documents, according to XAdES (ETSI TS101903) and XML-DSIG standards. In the next chapters a short introduction is given on the main API calls used to accomplish the above mentioned.

5.1.1 Initialization

Firstly, define the required structures:

```
SignedDoc* pSigDoc;
```

This structure reflects the file format of DigiDoc. All other relevant structures are part of this basic structure.

```
DataFile* pDataFile;
```

One DataFile structure corresponds to one original data file (file-to-be-signed) in DigiDoc container. One DigiDoc container can incorporate multiple data files. The data files are embedded in the DigiDoc container.

Initialize the library with the following function:

```
initDigiDocLib();
```

This ensures all OpenSSL library parameters are properly initialized.

5.1.2 Creating a DigiDoc document

DigiDoc structure should first be created in memory:

```
SignedDoc_new(&pSigDoc,
      DIGIDOC_XML_1_1_NAME, // format of the DigiDoc document
      DIGIDOC_XML_1_3_VER); // default version number
```

Values of the constants above are defined as "DIGIDOC-XML" and "1.3" (in DigiDocLib.h source file).

Note: the functionality of creating new files in older DigiDoc file formats SK-XML, DIGIDOC-XML 1.1 and DIGIDOC-XML 1.2 is no longer supported.

In the following sections, we add a data file and a signature to the DigiDoc structure before writing it into an output file.

5.1.3 Adding data files

In order to add a data file to a container, the container has to be unsigned and there shouldn't be an existing data file with the same name in the container. Note that only the data file name without path is saved in the document ('/' and '\' characters are not allowed in the data file's name).

Data files can be added to a DigiDoc container in two alternative ways:

- by reading the data from a file on the disk and using temporary files to store any intermediary data;
- by using only internal memory buffers (e.g. data to be added has been generated dynamically or has been read from a database).

1. Adding a data file by reading the file from disk and storing intermediary data in temporary files

Firstly, call the function Datafile_new(). The function creates a new DataFile element and saves the original data file in DigiDoc container:

```
DataFile_new(&pDataFile, // data file to be added
      pSigDoc, // DigiDoc structure to which the data file is added
      NULL, // data file's id
      infile, // data file name and path
    CONTENT_EMBEDDED_BASE64, // file embedding option
      mime, // mime type of the data file
      0, NULL, 0, NULL, // optional parameters
      CHARSET_UTF_8); // fixed constant for DigiDoc character encoding
```

Third parameter in the abovementioned function is a unique identification of the data file in the DigiDoc document. If value NULL is used then the library generates it automatically.

Fourth parameter is the name of the data file. It is recommended to include full path in this parameter; the path is removed when writing the file to DigiDoc container.

Fifth parameter reflects how data files are embedded in the DigiDoc container. The supported embedding option is `CONTENT_EMBEDDED_BASE64` (defined in DigiDocLib.h) – contents of the data file are encoded using base64-encoding before merging it into DigiDoc container.

Sixth parameter is a MIME type of the data file. For example "application/msword" or "application/pdf", depending on the type of the data file.

In most cases, the next four parameters should be left to the library to determine. The parameters determine:

- size of the original file in bytes,
- hash of the original file,
- size of the hash of the original file,
- type of hash algorithm (only SHA-1 is supported).

To calculate the values of these four parameters, call the following function:

```
calculateDataFileSizeAndDigest(pSigDoc, pDataFile->szId, infile,
DIGEST_SHA1);
```

This function reads the data file from disk, calculates and adds these four values to section pDataFile->szId based on file name given in the third parameter. `DIGEST_SHA1` is the only supported hash algorithm.

It is possible to add additional extra XML attributes to the data file, function addDataFileAttribute() is used for that. For example:

```
addDataFileAttribute(pDataFile, "ISBN", "000012345235623465");
addDataFileAttribute(pDataFile, "Owner", "CEO");
```

The first parameter is a pointer to original file structure, followed by the attribute's name and value. The data is going to be added in UTF-8 encoding.

2. Adding data by using internal memory buffers (no data is stored on the disk)

   Use the DigiDocMemBuf structure to hold the data to be added. Note that the fields of DigiDocMemBuf structure should be initialised with value 0:

```
DigiDocMemBuf mbuf; // memory buffer to hold the data
mbuf.pMem = 0; // functions will assign allocated memory address here
mbuf.nLen = 0; // length of data in number of bytes
```

   It is possible to assign data to DigiDocMemBuf as follows:

- ddocMemAssignData() – assigns data to DigiDocMemBuf memory buffer and releases previous data content if necessary; ddocMemAppendData() – appends data to memory buffer and increases its length accordingly.

  The functions are defined in source file DigiDocMem.h and can be used, for example, to assign data that has been read from database or generated dynamically.

- function ddocReadFile() defined in DigiDocConfig.h – reads data from an input file and assigns it to DigiDocMemBuf memory buffer.

Add the data in memory buffer to DigiDoc container with the following function (defined in DigiDocObj.h):

```
createDataFileInMemory(&pDataFile, // structure of the data file to be added
    *ppSigDoc, // DigiDoc structure to which the data file is added
    NULL, // data file's id
    infile, // data file name and path
    CONTENT_EMBEDDED_BASE64, // file embedding option
    mime, // mime type of the data file
    mbuf.pMem, // memory buffer's data
    mbuf.nLen); // memory buffer's size
```

The function creates a new DataFile element, adds the data and its hash value (SHA-1 is supported) to DigiDoc container.

The first six parameters of the function above have the same meaning as in function DataFile_new() described in the previous point.

The last two input parameters specify the data in memory buffer and the buffer's size.

After the new DataFile element has been created and added to the DigiDoc container, you can add additional attributes to it with function addDataFileAttribute() (described in the previous point).

Memory of the data buffer should be freed after the data has been added:

```
ddocMemBuf_free(&mbuf);
```

5.1.4 Adding signatures

You can sign either by:

- using an Estonian ID card or
- any other smartcard provided that you have the external native language PKCS#11 driver for it
- using a software token (PKCS#12 file)
- calculate the signature in some external program (web-application?) and then add the signature value to digidoc document.

Note: the functionality of adding signatures is no longer supported in case of older DigiDoc file formats SK-XML, DIGIDOC-XML 1.1 and DIGIDOC-XML 1.2.

SignatureInfo structure is needed to incorporate the necessary information about the signature before it can be created:

```
SignatureInfo* pSigInfo;
```

Signing can be done by using the function:

```
signDocumentWithSlotAndSigner(SignedDoc* pSigDoc, // SignedDoc structure
                                                  // to which the signature is added
      SignatureInfo** ppSigInfo, // SignatureInfo structure
      const char* pin, // pin2 in case of Estonian ID cards
```

```
        const char* manifest, // signer's role / resolution (optional)
        const char* city, // signature production place (optional)
        const char* state, const char* zip, const char* country,
        int nSlot, // specifies the signer's private key's slot
        int nOcsp, // add OCSP confirmation or not
        int nSigner, // signing module: 1->PKCS11, 2->CNG, 3->PKCS12
        const char* szPkcs12FileName); // PKCS#12 file name
```

Optional parameter **manifest** may be used to define the signer's role and resolution. The string can contain only the signer's role or role along with the signer's resolution, separated with a slash character, i.e. **"role / resolution"**. The value will be written to a single <ClaimedRole> xml element in the file. When adding the signer's resolution then role must also be added. Note that during signature validation, at most two <ClaimedRole elements are allowed due to historical reasons.

Optional parameters **city**, **state**, **zip** and **country** may be used to specify the signature creation location.

Parameter **nSlot** indicates the sequence number (counting from zero) of the current signing certificate among all signature certificates on the identity token. In case of Estonian ID cards, there is one signature certificate and the signature slot value is 0 (which is also the default slot value). When operating with multiple smartcards on the same system then you may need to specify a different slot. By default, in this case, the signature slots are numbered as follows:

slot 0 – signature slot of the 1st smartcard

slot 1 – signature slot of the 2nd smartcard

In case of signing with a software token (PKCS#12 file) then firstly the appropriate configuration settings should be applied (see section 3.4, subsection "Configuring software token usage") and slot value 0 should be used.

Parameter **nOcsp** can be used to specify whether an OCSP confirmation is added to the signature or not. The default value is 1, meaning that OCSP confirmation is automatically added to the signature after its creation. Value 0 indicates that the confirmation is not added.

Parameter **nSigner** specifies the module that is used for accessing the signature token. Possible values for the parameter are as follows:

- int nSigner = 1 - signing is done via PKCS#11 module which is the default module for singing with smart card.
- int nSigner = 2 – Microsoft CNG API and minidriver for signing with smart card in Windows environment. A dialog window is opened for the user to choose the signing certificate and enter PIN code.
- int nSigner = 3 - signing is done via PKCS#12 module, to be used in case of creating signatures with software tokens (PKCS#12 files).

Parameter **szPkcs12FileName** should be specified only when signing with a software token via PKCS#12 module (i.e. the nSigner parameter has been set to 3).

The function signDocumentWithSlotAndSigner() creates a new SignatureInfo structure and adds information about the data files to be signed and optional metadata of the signature (role of the signer and signature production place) to the structure. Then the signature value is calculated and stored. Finally, an OCSP confirmation is added to the signature if the value of nOcsp parameter indicates it.

5.1.5 Adding an OCSP confirmation

OCSP protocol is used to get validity confirmation from OCSP Responder to prove that certificate was valid at the time of signing.

It is possible to add an OCSP confirmation to a signature during its creation with function signDocumentWithSlotAndSigner() - value of parameter nOcsp has to be set to "1" (as described in the previous section).

Alternatively, you can add the confirmation by calling out the appropriate function yourself:

```
// Get the SignatureInfo element of the signature to be confirmed
// according to the signature's identificator

pSignInfo = getSignatureWithId(pSigDoc, szSignId);

// Get the OCSP confirmation

notarizeSignature(pSigDoc, pSignInfo);
```

Information about the signer's certificate CA and its respective OCSP responder is retrieved from CDigiDoc's configuration file. CA and OCSP Responder data have to be registered in the configuration file and the respective certificates have to be stored in the file system.

Note: there are also alternative functions for adding an OCSP confirmation to a signature but it is recommended to use the notarizeSignature() function described above. The function enables handling cases when the signer's certificate and OCSP responder's certificate are issued by different CAs and if there are several CA certificates with matching CN names.

Note: when verifying a signature that has no OCSP confirmation, an error message "Error: 128 - Signature has no OCSP confirmation!" is produced.

5.1.6 Reading and writing DigiDoc documents

Reading DigiDoc documents

It is possible to read an existing DigiDoc document from a file stored in the file system or from an internal memory buffer (e.g. buffer that stores DigiDoc document's data fetched from a database).

1. Opening and reading a DigiDoc document from disk

   Use the function:

   ```
   int ddocSaxReadSignedDocFromFile(SignedDoc** ppSigDoc,// DigiDoc structure
         const char* szFileName, // input file
         int checkFileDigest,
         long lMaxDFLen);
   ```

   Parameter checkFileDigest is a flag indicating whether checking hash value(s) of original file(s) is required at the time of opening. Parameter lMaxDFLen can be used to specify the maximum size of DataFile content to be cached in memory.

2. Opening and reading DigiDoc document from a memory buffer

   Use the DigiDocMemBuf structure to hold the initial data (see also section "3.6.3 Adding data files", under the second point for additional information about initialising and using DigiDocMemBuf):

   ```
   DigiDocMemBuf mbuf; // memory buffer to hold the data
   ```

   Define a SignedDoc structure for holding the DigiDoc document's data that is read from buffer:

   ```
   SignedDoc* pSigDoc;
   ```

   Read the DigiDoc document from DigiDocMemBuf buffer by using the following function:

   ```
   ddocSaxReadSignedDocFromMemory(&pSigDoc, // structure representing the
                                            //DigiDoc document
         mbuf.pMem, // memory buffer's data
         mbuf.nLen, // memory buffer's size
   ```

```
        mbuf.nLen + 1);//max size of DataFile content to be cached in memory
```

Writing DigiDoc documents

DigiDoc documents can be created in two alternative ways:

- creating the output (new or modified) DigiDoc document and writing it to a file on disk;
- creating the output (new or modified) DigiDoc document and storing it in internal memory buffer (no data is written to disk).

1. Writing the output DigiDoc document to a file on disk

   For creating a file in DigiDoc format and writing it to a file, the following function should be used:

```
createSignedDoc(pSigDoc, // structure representing the DigiDoc document
      oldfile, // specifies existing DigiDoc file, if necessary
      outfile); // output file's name
```

   The "oldfile" parameter value can be set to NULL if you are creating a new DigiDoc document from scratch. If you have read in an existing DigiDoc document to modify it (e.g. add signature(s) or data file(s)) and now try to write it to an output file then you have to specify the existing DigiDoc file's path and filename in the "oldfile" parameter. Otherwise the data file contents from the existing DigiDoc file might not be copied to the new container.

2. Writing the output DigiDoc document to an internal memory buffer

   Use the DigiDocMemBuf structure for storing the output DigiDoc document's data (see also section "3.6.3 Adding data files", under the second point for additional information on initialising and using DigiDocMemBuf):

```
DigiDocMemBuf* pMBuf; // output buffer
```

   Write the created or modified DigiDoc container to a memory buffer by using the following function:

```
createSignedDocInMemory(SignedDoc* pSigDoc, // structure representing
                                             // the DigiDoc document
    const char* oldfile, // specifies existing DigiDoc file, if necessary
    DigiDocMemBuf* pMBuf); // memory buffer for storing the output data
```

   The "oldfile" parameter in the abovementioned function should be used according to the analogous parameter in createSignedDoc() function (described in the previous point).

Memory should be released after end of working with DigiDoc structure:

```
SignedDoc_free(pSigDoc);
```

This also releases memory that is used for keeping the data files.

After finishing work with CDigiDoc, then the last task is to shut down the library:

```
finalizeDigiDocLib();
```

5.2 Validating signed documents

Validation of a signed DigiDoc document consists of three main steps:

1. Call out the main validation method of the library.
   a. If there are multiple validation errors then get the errors list.
2. Check for additional errors/warnings (separate implementation);

3. Determine the validation status of the document (according to the returned error codes and validation status priorities).

Note: steps 1a, 2 and 3 are additions to the validation process since the library's version v3.8.

5.2.1 Using the main validation method

Firstly, validate the DigiDoc document and its OCSP confirmation with the function:

```
int verifySignatureAndNotary(SignedDoc* pSigDoc,
             SignatureInfo* pSigInfo, const char* szFileName);
```

If the main validation method returns **error code 173** (ERR_UNKNOWN_ERROR, DigiDocError.h) then multiple errors were found by the validation process.

To get the list of all error codes, you can use functions getLastErrorsIdx(), getErrorsInfo() and getErrorString() (in source file DigiDocError.c). For example, you can print out the error list with details as follows:

```
ErrorInfo* pErr;
for(n = getLastErrorsIdx(); n >= 0; n--) {
   pErr = getErrorsInfo(n);
   pErrStr = getErrorString(pErr->code);
   fprintf(stdout, "\nWARNING: %d | %s | %s | %d | %s | %s”,
      pErr->code, pErrStr, pErr->25ilename, pErr->line,
      pErr->assertion, errorClass[getErrorClass(pErr->code)]);
}
```

5.2.2 Checking for additional errors/warnings

There are validation cases that are not checked in the default validation method of the library, instead, separate methods for checking the specific situations have to be called out by the library's user. In CdigiDoc library, checking for a **test signature** and **old file format** must be done separately.

The following subchapters describe how these checks can be implemented. After checking for additional errors/warnings, collect all of the error codes and continue with determining the validation status as described in the next chapter.

5.2.2.1 Checking for test signature

Test signature is a signature that has been created by using test certificates (e.g. signer's certificate and/or OCSP responder server's certificate have been issued for testing purposes).

Sample code for checking for test signature can be found from cdigidoc.c source file, method:

```
cmdVerify(SignedDoc* pSigDoc); //utility program's command –verify
```

For identifying if a certificate is a SK issued test certificate, you can use the following method as a sample code:

```
checkTestCert(X509* pCert);
```

The identification is done with comparing certificate policy OID values.

1.1.1.1 Checking for old file formats

You can use the sample code for checking for old formats that is implemented in cdigidoc.c utility program's method:

```
checkOldFormatVer(SignedDoc* pSigDoc);
```

Error handling sample code can be found from cdigidoc.c utility program's method:

```
cmdReadDigiDoc(SignedDoc** ppSigDoc, DencEncryptedData** ppEncData, int nMode);
//utility program's command –in
```

5.2.3 Determining the validation status

After validating the signed DigiDoc document, the validation result must be determined by the library's user. Final validation result must be one of the possible validation statuses that are described in the table below, the status must be chosen according to its priority.

The validation status priorities have to be applied in two cases:

1. **Returning a validation result of a single signature:**
   If there are more than one validation errors that occur when validating a single signature in DigiDoc container then the overall status of the signature should be chosen according to the status priorities.

2. **Returning a validation result of the whole DigiDoc container:**
   If there are more than one signatures in a DigiDoc container and the signatures have different validation statuses or validation of the container structure returns a different status then the overall status of the DigiDoc file should be chosen according to the status priorities.

NB! User of the library has to determine the validation status according to the error code that is returned by the library's validation method.

Priority	Status	Error code	Description
1	**INDETERMINATE/UNKNOWN**	**36** ERR_SIGNERS_CERT_NOT_TRUSTED	Validation process determines that one or more of the certificates included in the document are unknown or not trusted, i.e. the certificates have been issued by an unknown Certificate Authority (the CA has not been added to trusted list). **Notes**: • The file and signature(s) are not legally valid. • If the CA will later be added to the trusted list/trust store then the validation status can change to any of the other statuses described in the current table. **Suggested warning message** (also displayed in DigiDoc3 Client): "Signature status is displayed as unknown if you don't have all validity confirmation service certificates and/or certificate authority certificates installed into your computer" **More info**: http://www.id.ee/index.php?id=35941
2	**INVALID**	All errors except of the ones that are regarded as warnings by the library's user.	Validation process returns error(s), the errors have not been explicitly determined as minor error(s) by the library's user. **Note:** • The file and signature(s) are not legally valid. • No further alterations should be made to the file, i.e. no signatures should be added or removed.

Priority	Status	Error code	Description
3	**TEST**	**172** ERR_TEST_SIGNATURE	Test certificates have been used in the signed file (e.g. signer's certificate and/or OCSP responder server's certificate have been issued in testing purposes). **Notes**: • Test signature is not legally binding even if the signature is valid. • This status is used in combination with the other validation statuses described in the current table. **Suggested warning message** (also displayed in DigiDoc3 Client): "Test signature" **More info**: http://www.id.ee/index.php?id=30494 **Sample file**: aladdin3.6.ddoc
4	**VALID WITH WARNINGS**	See the next section.	Validation process returns error(s) that have been previously explicitly categorized (by the library's user) as minor technical errors. Note that this status is used only in exceptional cases, more details of which are given in the next chapter. **Notes**: • The file and signature(s) are handled as legally valid. • The error(s) are regarded as validation warnings. • Validation warnings should be displayed to the user. • No further alterations should be made to the file, i.e. no signatures should be added or removed. • Creator of the file should be informed about the error situation.
5	**VALID**	N/A	Validation process returns no errors. The signature is legally valid.

The error codes described in the table above are defined in DigiDocError.h source file.

Sample code of DigiDoc file validation can be found from cdigidoc.c utility program, from the following method:

```
cmdVerify(SignedDoc* pSigDoc); //utility program's command –verify
```

5.2.3.1 Validation status VALID WITH WARNINGS

In special cases, validation errors can be regarded as minor technical errors and the file's validation status can be regarded as VALID WITH WARNINGS instead.

NB! User of the DigiDoc library has to decide on his/her own when to use VALID WITH WARNINGS status instead of INVALID: there may be different interpretations of the severity of validation errors in different information systems then the final decision when to use this status has to be made by the library's user according to the requirements of the specific information system.

It is recommended to use the validation status VALID WITH WARNINGS in case of the error situations that are included in the table below – these error situations are regarded as VALID WITH WARNINGS in DigiDoc applications and software libraries, including:

- DigiDoc3 Client desktop application,
- JdigiDoc, Libdigidocpp and CdigiDoc software libraries' utility programs.

Table 1. Validation error codes recommended to be handled as VALID WITH WARNINGS

Status	Error code	Related DigiDoc file format	Description
VALID WITH WARNINGS	**169** ERR_DF_WRONG_DIG	DDOC 1.0 DDOC 1.1 DDOC 1.2 DDOC 1.3	<DataFile> element's xmlns attribute is missing. **Suggested warning message** (also displayed in DigiDoc3 Client): "This DigiDoc documents has not been created according to specification, but the digital signatures is legally valid. You are not allowed to add or remove signatures to this container." **More info**: http://www.id.ee/?id=36213 **Sample file**: 18912.ddoc
	170 ERR_ISSUER_XMLNS	DDOC 1.1 DDOC 1.2 DDOC 1.3	<IssuerSerial><X509IssuerName> and/or <IssuerSerial><X509SerialNumber> element's xmlns attribute is missing. **Suggested warning message** (also displayed in DigiDoc3 Client): "This DigiDoc documents has not been created according to specification, but the digital signatures is legally valid. You are not allowed to add or remove signatures to this container." **More info**: http://www.id.ee/?id=36213 **Sample file**: 20bait_nonce.ddoc
	171 ERR_OLD_VERSION	DDOC 1.0 DDOC 1.1 DDOC 1.2	DigiDoc file's version is older than currently supported. Note that the error situation affects only the container and not the signatures, therefore, in DigiDoc libraries, it is returned and displayed only at container level. **Suggested warning message** (also displayed in DigiDoc3 Client): "The current file is a DigiDoc container that is not supported officially any longer. You are not allowed to add or remove signatures to this container" **More info**: http://www.id.ee/index.php?id=36161 **Sample file**: DigiDoc 1.0 (tartu_ja_tallinna_koostooleping).ddoc

Sample code for determining validation warnings can be found from cdigidoc.c utility program. See command –verify (cmdVerify(SignedDoc* pSigDoc)) and methods hasErrors(), isError(), isWarning().

5.2.4 Additional information about validation

5.2.4.1 Overview of validation activities

Overview of validation activities is as follows:

1. checking that all the data files and signature's meta-data (signer's role, etc.) are included in the signature by calculating the data objects' digest values and comparing them with the <Reference> element values in the signature;

2. checking that the claimed signer's certificate is the actual certificate that was used for signing; checking that the "Non-repudiaton" value is set in the "Key Usage" extension of the signer's certificate;
3. checking that the signature value is correct by decrypting the value with the signer's public key and comparing the result with digest calculated from <SignedInfo> element block;
4. checking that the OCSP response confirms the signer certificate's validity and corresponds to the signature value (by comparing the digest value of <SignatureValue> element's value and OCSP response's nonce value);
5. checking that the signer's and OCSP responder's certificates are trusted (i.e. the certificates' issuers are registered in trust store, i.e. the configuration file).

5.3 Encryption and decryption

In addition to digital signing, CdigiDoc library offers also digital encryption and decryption according to the XML-ENC standard. This standard describes encrypting and decrypting XML documents or parts of them and it also allows encrypting any binary data in Base64 encoding.

CdigiDoc additionally enables to compress the data with ZLIB algorithm before encryption. It encrypts data with a 128 bit AES transport key which is in turn encrypted with the recipient's certificate. Encryption scheme is therefore certificate-based – it is possible to encrypt data using public key component fetched from some certificate. The decryption can be performed only by using private key corresponding to that certificate.

It is possible to encrypt for multiple certificates at once.

Certificates for encryption are fetched from a file in the file system (PEM encoding is supported), possible sources for finding them can be:

- Windows Certificate Store ("Other Persons")
- LDAP directories (for Estonian ID card holders, all valid certificates are available at: ldap://ldap.sk.ee)
- ID-card in smart-card reader.

Note that in CdigiDoc library, the certificates that can be used for encryption must have the value "Key Encipherment" included in "Key Usage" attribute field.

CdigiDoc doesn't support many encrypted data objects or a mix of encrypted and unencrypted data in one XML document.

One encrypted document:

- contains only one <EncryptedData> element, which is also the documents root element
- contains one <EncryptedKey> element for every recipient (i.e. possible decrypter) of the document
- contains a set of <EncryptionProperty> elements to store any meta data.

However, it is possible to incorporate a number of data files in one encrypted document if they are firstly all added to a DigiDoc container and then encryption is performed for that container as for a single data object.

In the following chapters we review the most common encryption and decryption operations with CdigiDoc library.

5.3.1 Composing encrypted documents

Note: for compatibility with other DigiDoc software components, it is recommended to place the data file to be encrypted inside a DigiDoc container before encrypting it. This way it is also possible to incorporate multiple data files into one encrypted document (i.e. if there is more than one data file in the DigiDoc container that is encrypted).

In order to compose an encrypted document you have to:

- create the DencEncryptedData structure first
- add all recipient info and other meta-information
- add the unencrypted data
- encrypt it, possibly compressing the data
- store it in a file or another medium.

The encryption method described is most suitable for small or medium sized data objects – all operations are done in memory.

Note that in order for the encrypted document to be compatible with other DigiDoc software components then the data file to be encrypted should be placed in a DigiDoc container before encryption (if the file is not originally a DigiDoc document).

Start composing a new encrypted document by defining the required data structures:

```
DencEncryptedData** ppEncData;
```

The DencEncryptedData structure refers to the <EncryptedData> element of an encrypted file and is the main structure that is used to store information which is needed for performing the encryption. Other structures that are used should be defined as follows:

```
DencEncryptedKey* pEncKey; // transport key data for every recipient
DencEncryptionProperty* pEncProperty; // property structure for storing
      // various metadata
```

Now create the DencEncryptedData structure with the following function:

```
dencEncryptedData_new(ppEncData,
      DENC_XMLNS_XMLENC, // fixed constant for XML namespace uri
      DENC_ENC_METHOD_AES128, // fixed constant for encryption method
             // algorithm uri
      0, 0, 0); // optional attributes, not needed with the current
             // encrypted document format
```

5.3.2 Adding recipient info and metadata

Every encrypted document should have at least one or many recipient blocks, otherwise nobody can decrypt it.

For every recipient the library stores:

- the AES transport key encrypted with the recipients certificate
- the certificate itself
- possibly some other data used to identify the key.

A certificate that is appropriate for data encryption must be used. In case of Estonian ID cards it is the authentication certificate.

NB! Encryption should be done for the authentication certificates on all the recipient's valid identity tokens (e.g. the national ID-card and Digi-ID card used in Estonia), except of the Mobile-ID certificates.

Start adding recipient data by reading in the recipient's certificate (the certificate has to be in PEM format):

```
ReadCertificate(&pCert, certfile);
```

Function ReadCertificate() (defined in source file DigiDocCert.h) reads the certificate from a file in file system. Alternatively, you can also use functions ddocDecodeX509Data() (data is in binary format) and ddocDecodeX509PEMData() (data is in PEM (base64) format) to decode certificate data that is already in memory.

Encrypt the transport key with the receiver's certificate and store encrypted key in memory:

```
dencEncryptedKey_new(*ppEncData, &pEncKey,
      pCert, // reveiver's certificate
      DENC_ENC_METHOD_RSA1_5, // fixed constant for encryption method
      id, recipient, keyname, carriedkeyname); // optional attributes
```

Optional attributes "id", "recipient" and/or sub elements <KeyName> and <CarriedKeyName> can be added to identify the key object. All of the above mentioned attributes and sub elements are optional but can be used to search for the right recipient's key or display its data in an application.

You can add metadata about the CdigiDoc library that is used for creating the encrypted document and encrypted document's format and version:

```
dencMetaInfo_SetLibVersion(*ppEncData);
dencMetaInfo_SetFormatVersion(*ppEncData);
```

The name of the data file that is encrypted should be added to the DencEncryptedData structure by creating a new property:

```
dencEncryptionProperty_new(*ppEncData, &pEncProperty,
      0, 0, // property id and target. Can be omitted
      ENCPROP_FILENAME, // fixed constant, represents the data file's name
      getSimpleFileName(dataFile)); // data file's name should be added
             // without path
```

Note that the data file's name used in the previous example has to be in UTF-8 encoding. If necessary, you can convert it with function:

```
ddocConvertInput(const char* src, char** dest);
```

If the original file is a .ddoc file then you should specify its mime type and add the value to DencEncryptedData structure as a new property:

```
dencEncryptionProperty_new(*ppEncData, &pEncProperty, 0, 0,
      ENCPROP_ORIG_MIME, // name of the property: original mime type
      DENC_ENCDATA_TYPE_DDOC); // value of the property: ddoc document's
             // mime type
```

In case of DigiDoc document, mime type has to be specified as shown above so that it would be possible to decrypt the file later.

Constants that represent mime types have been defined in DigiDocEnc.h source file. In case of a DigiDoc document, use the constant

- `DENC_ENCDATA_TYPE_DDOC`

  which contains the value:

- "`http://www.sk.ee/DigiDoc/v1.3.0/digidoc.xsd`".

The value is assigned to property "MimeType" of the cdoc document. CdigiDoc library uses the property "MimeType" also to store the fact that the data has been packed with ZLIB algorithm before encryption. If data compression is used then the library assigns the value

- "`http://www.isi.edu/in-noes/iana/assignments/media-types/application/zip`"

to "MimeType" attribute which has also been defined as a constant:

- DENC_ENCDATA_MIME_ZLIB

CdigiDoc assigns this value when packing the data and if the "MimeType" attribute was not empty before then the previous value is stored in <EncryptionProperty Name="OriginalMimeType"> sub element instead. If CdigiDoc reads a document with "MimeType" value defined by DENC_ENCDATA_MIME_ZLIB then at first it decompresses the decrypted data and then restores the original mime type if one is found.

If the original data file to be encrypted is a ddoc document then after adding the mime type property, you also need to "register" its contents:

```
dencOrigContent_registerDigiDoc(*ppEncData,
      pSigDoc); // SignedDoc structure representing the ddoc document
```

The function creates a new EncryptionProperty structure for every data file contained in the DigiDoc document and stores its name, size, mime type and id values for later use.

Note that you need to have the DigiDoc document kept in memory as a SignedDoc structure before using the function in the previous example. If you are encrypting an existing DigiDoc document (not creating it directly before encryption) then read the document in as described in section "3.6.6 Reading and writing DigiDoc documents".

5.3.3 Encryption and data storage

Before encrypting, you also need to add the actual data to be encrypted to DencEncryptedData structure. Use the method:

```
dencEncryptedData_AppendData(DencEncryptedData* pEncData,
      const char* data, // unencrypted data
      int len); // length of the data
```

Finally, encrypt the data with the following function:

```
dencEncryptedData_encryptData(DencEncryptedData* pEncData,
      int nCompressOption); // compression option used before encryption
```

In the function above, three different constants can be used to specify compression option for the data to be encrypted:

- DENC_COMPRESS_ALLWAYS – data is compressed before encryption.
- DENC_COMPRESS_BEST_EFFORT – data will be compressed and if it results in reduced data size then the compressed data is encrypted. Otherwise it will be discarded and original data is encrypted with no compression.
- DENC_COMPRESS_NEVER – compression is not applied.

You can write the encrypted document to an output file with the function:

```
dencGenEncryptedData_writeToFile(DencEncryptedData* pEncData, const char*
szFileName);
```

Note that it isn't necessary to use files to store encrypted data. It can be written to any output stream and used as required. In order to write the encrypted data to a memory buffer, do as follows:

```
DigiDocMemBuf mbuf; // output buffer
mbuf.pMem = 0; // functions will assign allocated memory address here
mbuf.nLen = 0; // length of data in number of bytes
dencGenEncryptedData_toXML(pEncData, // encrypted data structure
     &mbuf); // output buffer for storing the encrypted data
```

5.3.4 Parsing and decrypting

Firstly, define structure for holding the encrypted document's data that is going to be parsed:

```
DencEncryptedData* pEncData;
```

There are two alternative options for decrypting documents, depending on the encrypted document's size.

1. Parsing and decrypting small encrypted documents.

   Encrypted document can be read in and parsed in two ways: by reading the encrypted file from disk or by reading the encrypted file's contents from an internal memory buffer (e.g. a buffer that holds the encrypted document's data fetched from a database).

   - Reading and parsing the encrypted document from file system:

     ```
     char* inFile; // input encrypted file
     dencSaxReadEncryptedData(&pEncData, // structure for holding the encrypted
                                         // document's data
           33ilename); // input encrypted file's name
     ```

   - Reading and parsing encrypted document from a memory buffer

     Use the DigiDocMemBuf structure for holding the encrypted document's initial data (see also section "3.6.3 Adding data files", under the second point for additional information about initialising and using DigiDocMemBuf):

     ```
     DigiDocMemBuf mbuf; // data buffer structure
     ```

     Parse the encrypted document from the memory buffer with the following function:

     ```
     dencSaxReadEncryptedDataFromMemory(&pEncData, // structure for holding the
                                        // encrypted document's data
           &mbuf); // memory buffer with the initial data
     ```

   After parsing the document, data can be decrypted or displayed on screen. Decryption is a separate operation and is not automatically done during parsing.

   For decrypting, you need to find the correct EncryptedKey structure for the current recipient who is decrypting the data. If you use PKCS#11 identity token from a smart card for decryption, then do:

   ```
   dencEncryptedData_findEncryptedKeyByPKCS11(*ppEncData, &pEncKey);
   ```

   Now, data can be decrypted as follows:

   ```
   dencEncryptedData_decrypt(*ppEncData,
         pEncKey, // transport key
         pin); // pin1 code in case of Estonian ID cards
   ```

   The abovementioned functions are defined in source file DigiDocEnc.h. Function dencEncryptedData_decrypt() firstly decrypts the transport key with the recipient's pin code and then decrypts the data with the transport key. Data is decompressed, if necessary.

2. Parsing and decrypting large encrypted documents.

   In order to parse and decrypt large files, use the dencSaxReadDecryptFile() function (defined in DigiDocEncSAXParser.h):

   ```
   dencSaxReadDecryptFile(const char* szInputFileName, // encrypted file's name
         const char* szOutputFileName, // output (decrypted) file
         const char* szPin, // pin1 code in case of Estonian ID cards
         const char* szPkcs12File); // set to NULL in case of Estonian ID cards
   ```

The abovementioned function reads encrypted data from the specified input file, decrypts and possibly decompresses the data during parsing and writes the decrypted data to output file. Data is not kept in memory during decryption.

Parameter szPkcs12File indicates the PKCS#12 software token's file name and path, if decryption is done with a software token. The value should be set to NULL when using PKCS#11 driver (e.g. in case of Estonian ID cards).

Note: when decrypting files then it should be taken into account that for compatibility with other DigiDoc software components, it is recommended that the data file to be encrypted is placed inside a DigiDoc container before encryption. In this case, it is also necessary to extract the original data file(s) from DigiDoc container after decryption.

6. CDigiDoc utility program

CdigiDoc library includes a command line utility program – cdigidoc.exe – which can be used to read, digitally sign, encrypt and decrypt files in OpenXadES format. Source code of the program is in cdigidoc.c file.

The general format is:

```
> cdigidoc [command(s)]
```

A list of all the available commands and their format can always be displayed by using the -? Or –help commands:

```
> cdigidoc –help
```

Output from all of the CdigiDoc utility program's commands is ended with the following information:

```
CdigiDoc|[error code or '0' in case of success]|[elapsed time in seconds]
```

Note that the error codes' definitions can be found in the file DigiDocError.h.

6.1 General commands

- **-? Or –help** – displays help about command syntax.
- **-config <configuration-file>** - specifies the CdigiDoc configuration file name.
- **-check-cert <certificate-file-in-pem-format>** - checks the certificate validity status.

Setting the configuration file

-config <configuration-file>

You can dynamically specify the configuration file used before executing each command line task.

If left unspecified, then the configuration file is looked up from default locations (see section "3.4 Configuring CdigiDoc" for more information).

Checking the certificate

-check-cert <certificate-file-in-pem-format>

Used for checking the chosen certificate's validity; returns an OCSP response from the certificate's CA's OCSP responder. Note that the command is currently not being tested.

If the certificate is valid, then the return code's (RC) value is 0. For example:

Verifying cert: MÄNNIK,MARI-LIIS,47101010033 → RC :0

Sample: setting the configuration file when creating a new DigiDoc container

```
> cdigidoc –config c:\temp\digidoc.i–i -n–w -add c:\temp\test1.txt text/pla–
n -out c:\temp\test1.ddoc

  Input:
  - c:\temp\digidoc.ini – the configuration file to be used
  - c:\temp\test1.txt   - a data file to be added to ddoc container
```

```
- text/plain          - mime type of the data file
- c:\temp\test1.ddoc  - ddoc container to be created
```

6.2 Digital signature commands

- **-in <input-digidoc-file> -** reads in a DigiDoc file
- **-in-mem <input-digidoc-file> -** reads in a DigiDoc file. The operation is conducted "in memory", meaning that the data is read into a memory buffer and no intermediary data is written to temporary files on the disk.
- **-new –** creates a new DigiDoc container
- **-add <input-file> <mime-type> –** adds a data file to a DigiDoc container
- **-add-mem <input-file> <mime-type> -** adds a data file to a DigiDoc container. The operation is conducted "in memory", meaning that the data is read into a memory buffer and no intermediary data is written to temporary files on the disk.
- **-sign <pin-code> –** signs a DigiDoc file
- **-out <output-file> –** creates a DigiDoc file at the specified location
- **-out-mem <output-file> -** creates a DigiDoc file at the specified location. The operation is conducted "in memory", meaning that the data is read from and written to a memory buffer, no intermediary data is written to temporary files on the disk.
- **-verify –** displays and verifies DigiDoc file's signature(s). Note that starting from the library's 3.8 version, warnings system is used, i.e. minor technical errors are printed out as warnings. See chapter "5.2.3.1 Validation status VALID WITH WARNINGS" for detailed information about warning situations.

  Parameter –libraryerrors can be added to the command to distinguish errors that are returned by the library.
- **-libraryerrors** – for testing purposes, may be used together with –verify command. Enables to view the validation errors as they are returned by the library (otherwise, the utility program may transform specific errors to warnings; see also description und–r -verify command). The errors are printed out with "LIBRARY-ERROR" prefix.
- **-extract <data-file-id> <output-file> –** extracts DigiDoc file's content
- **-extract-mem <data-file-id> <output-file> –** extracts DigiDoc file's content. The operation is conducted "in memory", meaning that the data is read from and written to a memory buffer, no intermediary data is written to temporary files on the disk.
- **-get-confirmation <signature-id> –** adds an OCSP confirmation to a DigiDoc file's signature.
- **-mid-sign <phone-no> <per-code> [[<country>(EE)] [<lang>(EST)] [<service>(Testing)] [<manifest>] [<city> <state> <zip>]] –** signs a DigiDoc file using Mobile-ID. **Note**: Mobile-ID functionality in CDigiDoc is experimental.

Creating new DigiDoc files

-new [format] [version]

Creates a new digidoc container with the specified format and version. The current supported digidoc format in CDigiDoc library is DIGIDOC-XML, version is 1.3 (newest).

By using the optional paramet–r - versi–n - with this command, you can specify an alternative **version** to be created.

Note: creating new DigiDoc files in older DigiDoc file formats SK-XML, DIGIDOC-XML 1.1 and DIGIDOC-XML 1.2 is no longer supported.

-add <input-file> <mime-type> [<content-type>] [<charset>]

Adds a new data file to a digidoc document. If digidoc do'sn't exist then creates one in the default format. In order to add a data file to a container, the container has to be unsigned and there shouldn't be an existing data file with the same name in the container. Note that only the data file name without path is saved in the document ('/' and '\' characters are not allowed in the data file's name).

Input file (required) specifies the name of the data file (it is recommended to include full path in this parameter; the path is removed when writing to DigiDoc container file).

Mime type (required) represents the MIME type of the original file like "text/plain" "r "application/msword".

Content type reflects how the original files are embedded in the container: EMBEDDED_BASE64 (embedding binary data in base64 format) is supported and used by default.

Chars–t - UTF-8 encoding is supported and used by default.

-add-mem <input-file> <mime-type> [<content-type>]

Alternative version of t–e -add command. The operation is conducted "in memory", meaning that the data is read into a memory buffer and no intermediary data is written to temporary files on the disk.

-sign <pin-code> [[[manifest] [city] [state] [zip] [country]] [slot(0)] [ocsp(1)] [PKCS11/CNG/PKCS12] [pkcs12-file-name]]

Adds a digital signature to the digidoc document. Note that adding signatures to DigiDoc files in older formats SK-XML, DIGIDOC-XML 1.1 and DIGIDOC-XML 1.2 is no longer supported. You can use the command with the following parameters:

pin-code	PIN code of the identity token. In case of Estonian ID cards, PIN2 code is used for digital signing. Required when signing via PKCS#11 (the default module) and PKCS#12 module, optional in case of CNG API and minidriver (see also parameter "PKCS11/CNG/PKCS12" of the current command).
manifest	Role and resolution of the signer, as a single string, separated with a slash character, e.g. "role / resolution". It is also possible to specify only the signer's role. At most one role/resolution value is allowed for a signature, the value is written to a single <ClaimedRole> element in the singed file.
city	City where the signature is created
state	State or province where the signature is created
zip	Postal code of the place where the signature is created
country	Country of origin. ISO 3166-type 2-character country codes are used (e.g. EE)

slot	Identifier of the signer's certificate's and private key's sequence number (counting from zero) among all signature certificates on an identity token. When operating for example with a single Estonian ID card (which contains one signature key) then the key can be found in slot 0 – which is used by default. The library makes some assumptions about PKCS#11 drivers and card layouts: - you have signature and/or authentication keys on the card - both key and certificate are in one slot - if you have many keys like 1 signature and 1 authentication key then they are in different slots - you can sign with signature key that has a corresponding certificate wi"h "NonRepudiat"on" bit set. You may need to specify a different slot to be used when for example operating with multiple smart cards on the same system. In this case, the signature slots are counted as follows: - slot 0 – signature key of the 1st smartcard - slot 1 – signature key of the 2nd smartcard If the slot needs to be specified during signing, then the 5 previous optional parameters (manifest, city, state, zip, country) should be filled first (either with the appropriate data or as "" for no value).
ocsp	Specifies whether an OCSP confirmation is added to the signature that is being created. Possible values are 0 – confirmation is not added; 1 – confirmation is added. By default, the value is set to 1. Parameter value 0 can be used when creating a technical signature. Technical signature is a signature with no OCSP confirmation and no timestamp value.
PKCS11/CNG/PKCS12	Optional parameter to specify module that is used for accessing the signature token. Possible values are: - "PKCS11" - default module for signing with smart card - "CN–" - alternative module for signing with smart card, uses Microsoft CNG API and smart card's minidriver. A dialog window is opened for the user to choose a signing certificate and insert PIN code (i.e. the "pin-code" parameter of the current command may be left unspecified by inserting an empty string ""). - "PKCS1–" - module for signing with a software token (PKCS#12 file). When signing with a software token then firstly, the appropriate configuration settings should be applied (see section 3.4, subsection "Configuring software token usage"). The current command's parameter "pin-code" must be set according to the PKCS#12 container's PIN code, parameter "ocsp" must be set to 0 and parameter's "pkcs12-file-name" value should be specified.
pkcs12-file-name	Used only when signing with software token (PKCS#12 file) via PKCS#12 module (i.e. if the previous parameter's value has been set to "PKCS12"). Specifies the software token's file name.

-mid-sign <phone-no> <per-code> [[<country>(EE)] [<lang>(EST)] [<service>(Testing)] [<manifest>] [<city> <state> <zip>]]

Note: Mobile-ID functionality in CDigiDoc is experimental.

Invokes mobile signing of a ddoc file using Mobile-ID and DigiDocService.

Mobile-ID is a service based on Wireless PKI providing for mobile authentication and digital signing, currently supported by all Estonian and some Lithuanian mobile operators.

The Mobile-ID user gets a special SIM card with private keys on it. Hash to be signed is sent over the GSM network to the phone and the user shall enter PIN code to sign. The signed result is sent back over the air.

DigiDocService is a SOAP-based web service, access to the service is IP-based and requires a written contract with provider of DigiDocService.

You can use Mobile-ID signing with the following parameters:

phone-no	Required. Phone number of the signer with the country code in format +xxxxxxxxx (for example +3706234566)
per-code	Required. Identification number of the signer (personal national ID number).
country	Country of origin. ISO 3166-type 2-character country codes are used (e.g. default is **EE**)
lang	Language for user dialog in mobile phone. 3-character capitalized acronyms are used (e.g. default is **EST**)
service	Name of the service – previously agreed with Application Provider and DigiDocService operator. Maximum length – 20 chars. (e.g. default is **Testing**)
manifest	Role or resolution of the signer
city	City where the signature is created
state	State or province where the signature is created
zip	Postal code of the place where the signature is created

-out <output-file>

Stores the newly created or modified DigiDoc document in a file.

-out-mem <output-file>

Alternative version of t–e -out command. The operation is conducted "in memory", meaning that the data is read from and written to a memory buffer, no intermediary data is written to temporary files on the disk.

Sample commands for creating and signing DigiDoc files:

Sample: creating new DigiDoc file without signing, with default format and version (DIGIDOC-XML, version 1.3)

```
> cdigid-c -n-w -add c:\temp\test1.txt text/pla-n -out c:\temp\test1.ddoc

  Input:
  - c:\temp\test1.txt   - a data file to be added to container
  - text/plain          - mime type of the data file
  - c:\temp\test1.ddoc  - container to be created
```

Sample: creating new DigiDoc file with signing

```
> cdigid-c -n-w -add c:\temp\test1.txt text/pla-n -sign 123-5 -out
c:\temp\test1.ddoc
```

```
Input:
  - c:\temp\test1.txt   - a data file to be added to container
  - text/plain          - mime type of the data file
  - 12345               - id-card pin2
  - c:\temp\test1.ddoc  - container to be created

Sample: signing an existing DigiDoc container (adding signatures)
> cdigid-c -in c:\temp\test1.dd-c -sign 123-5 -out c:\temp\test1.ddoc

Input:
  - c:\temp\test1.ddoc          - container to be signed
  - 12345                       - id-card pin2
  - c:\temp\test1.ddoc          - output (modified) digidoc container

Sample: using Mobile-ID for signing (note: Mobile-ID functionality in
CDigiDoc is experimental)
> cdigid-c -n-w -add c:\temp\test1.txt text/plain -mid-sign +3706234566
411101702-0 -out c:\temp\test1.ddoc

Input:
  - c:\temp\test1.txt   - a data file to be added to container
  - text/plain          - mime type of the data file
  - +3706234566         - signer's mobile number
  - 41110170240         - signer's personal code
  - c:\temp\test1.ddoc  - container to be created

Sample: Adding multiple data files to an existing unsigned DigiDoc container
> cdigid-c -in c:\temp\test1.dd-c -add C:\temp\test3.txt text/pla-n -add
C:\temp\test4.txt text/pla-n -out c:\temp\test1.ddoc

Input:
  - c:\temp\test1.ddoc          - unsigned container to be read and modified
  - C:\temp\test3.txt           - first data file to be added
  - C:\temp\test4.txt           - second data file to be added
  - text/plain                  - mime type of the data files
  - c:\temp\test1.ddoc          - output (modified) digidoc container

Sample: signing an existing digidoc container via CAPI/CNG module
> cdigid-c -in c:\temp\test1.dd-c -sign "" "" "" "" "" "" 0 1 C-G -out
c:\temp\test1.ddoc

Input:
  - c:\temp\test1.ddoc  - unsigned container to be read and modified
  - ""                  - empty strings for PIN code and other optional
                parameter values (manifest, city, state, zip, country)
  - 0                   - signature slot
  - 1                   - OCSP confirmation is added
  - CNG                 - identifier of CAPI/CNG module usage
  - c:\temp\test1.ddoc  - output (modified) digidoc container
```

Sample commands for signing in memory

```
Sample: creating new DigiDoc file with signing, operation in memory
```

```
> cdigid-c -new -add-mem c:\temp\test1.txt text/pla-n -sign 12345 -out-mem
c:\temp\test1.ddoc

Input:
  - c:\temp\test1.txt   - a data file to be added to container
  - text/plain          - mime type of the data file
  - 12345               - id-card pin2
  - c:\temp\test1.ddoc  - container to be created
```

Sample: signing an existing DigiDoc container (adding signatures), operation in memory

```
> cdigidoc -in-mem c:\temp\test1.dd-c -sign 12345 -out-mem
c:\temp\test1.ddoc

Input:
  - c:\temp\test1.ddoc          - container to be signed
  - 12345                       - id-card pin2
  - c:\temp\test1.ddoc          - output (modified) digidoc container
```

Sample commands for signing with technical signature

Technical signature is a signature with no OCSP confirmation or a signature created with a software token. Note that when verifying a signature that has no OCSP confirmation, an error message "Signature has no OCSP confirmation!" is produced. When verifying signature that is created with a software token, an error message "Signer's cert does not have non-repudiation bit set!" is produced.

Sample: signing an existing digidoc container with a technical signature (via default (PKCS#11) module)

```
> cdigid-c -in c:\temp\test1.dd-c -sign 67890 "" "" "" "" "" 0-0 -out
c:\temp\test1.ddoc

Input:
  - c:\temp\test1.ddoc  - unsigned container to be read and modified
  - 67890               - PIN code
  - ""                  - empty strings for optional parameter values
  (manifest, country, state, city, zip)
  - 0                   - signature slot
  - 0                   - OCSP confirmation is not added
  - c:\temp\test1.ddoc  - output (modified) digidoc container
```

Sample: signing an existing digidoc container with a technical signature by using a PKCS#12 software token (via PKCS#12 module)

```
> cdigid-c -in c:\temp\test1.dd-c -sign 67890 "" "" "" "" "" 0 0 PKCS12
c:\test\pkcs12.p-x -out c:\temp\test1.ddoc

Input:
  - c:\temp\test1.ddoc  - unsigned container to be read and modified
  - 67890               - software token's PIN code
  - ""                  - empty strings for optional parameter values
  (manifest, country, state, city, zip)
  - 0                   - signature slot
  - 0                   - OCSP confirmation identifier
  - PKCS12              - identifier of PKCS12 module
  - c:\test\pkcs12.pfx  - your software token's PKCS#12 container file
  - c:\temp\test1.ddoc  - output (modified) digidoc container
```

Reading DigiDoc files and verifying signatures

-in <input-digidoc-file>

Specifies the input DigiDoc file name. It is recommended to pass the full path of the DigiDoc file in this parameter.

-in-mem <input-digidoc-file>

Alternative version of t–e -in command. The operation is conducted "in memory", meaning that the data is kept in memory buffers and no intermediary data is written to temporary files on the disk.

-verify

Displays the data file and signature info of a DigiDoc document just read in; validates all signatures. Note that starting from the library's 3.8 version, warnings system is used, i.e. minor technical errors are printed out as warnings. See chapter "5.2.3.1 Validation status VALID WITH WARNINGS" for detailed information about warning situations.

Returns:

- **Digidoc container data**, in format:

  SignedDoc | <format-identifier> | <version>

  For example: SignedDoc | DIGIDOC-XML | 1.3

- **List of all data files**, in format:

  DataFile | <file identifier> | <file name> | <file size in bytes> | <mime type> | <data file embedding option>

  For example: DataFile | D0 | test1.txt | 44 | text/plain | EMBEDDED_BASE64

- **List of all signatures** (if existing), in format:

  Signature | <signature identifier> | <signer's key info: last name, first name, personal code> | <verification return code> | <verification result>

  For example: Signature | S0 | MÄNNIK,MARI-LIIS,47101010033 | 0 | No errors

- **Signer's certificate information**
- **OCSP responder certificate information**
- **Signature validation warning** (if present), in format:

  WARNING | <error-code> | <warning message>

  For example: WARNING |172|Test signature!

Parameter –libraryerrors can be added to the command to distinguish errors that are returned by the library.

-extract <data-file-id> <output-file>

Extracts the selected data file from the DigiDoc container and stores it in a file.

Data file id represents the ID for data file to be extracted from inside the DigiDoc container (e.g. D0, D1…).

Output file represents the name of the output file.

-extract-mem <data-file-id> <output-file>

Alternative version of t–e -extract command. The operation is conducted "in memory", meaning that the data is kept in memory buffers and no intermediary data is written to temporary files on the disk.

Sample commands for reading/validating/extracting from DigiDoc files:

```
Sample: listing DigiDoc file's contents, signed
> cdigid-c -in c:\Temp\test1_s.dd-c -verify

Input:
  - c:\temp\test1_s.ddoc – the digidoc file which contents are to be listed

Returns:
SignedDoc|DIGIDOC-XML|1.3
DataFile|D0|test1.txt|44|text/plain|EMBEDDED_BASE64
DataFile|D1|test2.txt|84|text/plain|EMBEDDED_BASE64
Signature|S0|MÄNNIK,MARI-LIIS,47101010033|0|No errors
/prints out signer's and OCSP responder's certificate data/

Sample: Extracting a data file from an existing DigiDoc file
> cdigid-c -in c:\temp\test1.dd-c -extract D0 c:\temp\test_ext.txt

Input:
- c:\temp\test1.ddoc    – the digidoc file to be extracted from
- D0                    - the data file ID to be extracted
- c:\temp\test_ext.t-t - file for storing the extracted data
```

6.3 Encryption commands

- **-in <input-encrypted-file>** - reads in the specified encrypted input document
- **-in-mem <input-encrypted-file> -** reads in an encrypted file. The operation is conducted "in memory", meaning that the data is read into a memory buffer and no intermediary data is written to temporary files on the disk.
- **-out <output-decrypted-file> -** specifies the decrypted output document's name
- **-out-mem <output-decrypted-file> -** creates a decrypted output document at the specified location. The operation is conducted "in memory", meaning that the data is read from and written to a memory buffer, no intermediary data is written to temporary files on the disk.
- **-denc-list <input-encrypted-file>** - displays the encrypted document data and recipient's info.
- **-encrecv <certificate-file> -** adds recipient to an encrypted document
- **-encrypt-sk <input-file>** - encrypts the input document; recommended for compatibility with other DigiDoc software components, places the data file to be encrypted inside a new DigiDoc container–
    - *-encrypt <input-file>* - used for encrypting small files, not recommended for compatibility with other DigiDoc software component–.
    - *-encrypt-file <input-file> <output-file>* **-** used for encrypting large files, not recommended for compatibility with other DigiDoc software components.
- **-decrypt-sk <output-file> <pin> -** decrypts the input file; recommended for compatibility with other DigiDoc software components, expects the encrypted input file to be in a DigiDoc container. Alternatives ar–:

- *-decrypt <output-file> <pin>* - used for decrypting small files in any original forma–.
- *-decrypt-file <input-file> <output-file> <pin>* - used for decrypting large files in any original format.
- *decrypt-hex <input-file> <key> <output-file> - used for testing decryption operation, Previously decrypted transport key value has to be provided.*

Reading encrypted files

-in <input-encrypted-file>

Input encrypted file (required) specifies the encrypted file's name.

-in-mem <input-encrypted-file>

Alternative version of t–e -in command. The operation is conducted "in memory", meaning that the data is read into a memory buffer and no intermediary data is written to temporary files on the disk.

-denc-list

Displays the encrypted data and recipient's info of an encrypted document just read in.

Sample: Displaying encrypted file's recipient info and data

```
> cdigid–c -denc-list c:\Temp\test1b.cdoc

Input:
  - c:\temp\test1b.cdoc        – the encrypted file to be read

Returns:
  EncryptedData|||http://www.isi.edu/in-
  noes/iana/assignments/mediatypes/application/zip|http://www.w3.org/2001/04
  /xmlenc#aes128-cbc
  LIBRARy|CDigiDoc|2.7.1.59
  FORMAT|ENCDOC-XML|1.0
  EncryptedKey||MÄNNIK,MARI-
  LIIS,47101010033|||http://www.w3.org/2001/04/xmlenc#rsa-1_5|OK
  EncryptionProperties|
  EncryptionProperty|||LibraryVersion|CDigiDoc|2.7.1.59
  EncryptionProperty|||DocumentFormat|ENCDOC-XML|1.0
  EncryptionProperty|||Filename|test1.txt
  EncryptionProperty|||OriginalMimeType|http://www.sk.ee/DigiDoc/v1.3.0/digi
  doc.xsd
  EncryptionProperty|||orig_file|c:\temp\test1.txt|44|application/file|D0
  EncryptionProperty|||OriginalSize|360
  EncryptionProperty|||OriginalMimeType|http://www.sk.ee/DigiDoc/v1.3.0/digi
  doc.xsd
```

Encrypting files

-encrecv <certificate-file> [recipient] [KeyName] [CarriedKeyName]

Adds a new recipient certificate and other metadata to an encrypted document. **Certificate file** (required) specifies the file from which the public key component is fetched for encrypting the data. The decryption can be performed only by using private key corresponding to that certificate.

The input certificate files for encryption must come from the file system (PEM encodings are supported). Possible sources where the certificate files can be obtained from include:

- Windows Certificate Store ("Other Persons")
- LDAP directories
- ID-card in smart-card reader

Nb! encryption should be done for the authentication certificates on all the recipient's valid identity tokens (e.g. the national ID-card and Digi-ID card used in Estonia), except of the Mobile-ID certificates.

For example the certificate files for Estonian ID card owners can be retrieved from a LDAP directory at ldap://ldap.sk.ee. The query can be made in following format through the web browser (IE): ldap://ldap.sk.ee:389/c=EE??sub?(serialNumber= xxxxxxxxxxx) where serial Number is the recipient's personal identification number, e,g.38307240240).

Other parameters include:

recipient	If left unspecified, then the program assigns a unique value to this attribute. This is later used as a command line option to identify the recipient whose key and smart card is used to decrypt the data. **Note:** Although this parameter is optional, it is recommended to pass on the entire CN value from the recipient's certificate as the recipient identifier here, especially when dealing with multiple recipients. For example if CN = MÄNNIK,MARI-LIIS,41110212444, then recipient = MÄNNIK,MARI-LIIS,41110212444
KeyName	Sub-element <KeyName> can be added to better identify the key object. Optional, but can be used to search for the right recipient's key or display its data in an application.
CarriedKeyName	Sub-element <CarriedKeyName> can be added to better identify the key object. Optional, but can be used to search for the right recipient's key or display its data in an application.

-out <output-encrypted-file>

Output encrypted file (required) specifies the name of the output file which will be created in the current encrypted document format (ENCDOC-XML ver 1.0), with file extension **.cdoc**.

-out-mem <output-encrypted-file>

Alternative version of t–e -out command. The operation is conducted "in memory", meaning that the data is read from and written to a memory buffer, no intermediary data is written to temporary files on the disk.

-encrypt-sk <input-file>

Encrypts the data from the given input file and writes the completed encrypted document in a file. **Recommended for providing cross-usability with other DigiDoc software components.**

This command places the data file to be encrypted in a new DigiDoc container. Therefore handling such encrypted documents later with other DigiDoc applications is fully supported (e.g. DigiDoc3 client).

Input file (required) specifies the original data file to be encrypted.

Note: There are also alternative encryption commands which are however **not recommended for providing cross-usability with other DigiDoc software components**:

-encrypt <input-file>

Encrypts the data from the given input file and writes the completed encrypted document in a file. Should be used only for encrypting **small** documents, **already in DIGIDOC-XML format.**

Input file (required) specifies the original data file to be encrypted.

-encrypt-file <input-file> <output-file>

Encrypts the input file and writes to output file. Should be used only for encrypting **large** documents, **already in DIGIDOC-XML format.** Note that the command in not currently tested.

Input file (required) specifies the original data file to be encrypted.

Output file (required) specifies the name of the output file which will be created in the current encrypted document format (ENCDOC-XML ver 1.0), with file extension **.cdoc**.

Command line samples for encrypting documents:

Sample: encrypting small doc (DigiDoc compatible, original in any format)

```
> cdigid-c -encrypt-sk c:\temp\test_Small.txt -out c:\Temp\test1.cd-c -
encrecv c:\temp\Rcert.cer MÄNNIK,MARI-LIIS,47101010033

Input:
- c:\temp\test_Small.txt – the input file to be encrypted
- c:\temp\test1.cdoc    - the encrypted file to be created
- c:\temp\Rcert.cer     – the recipient's certificate file
- MÄNNIK,MARI-LIIS,471010100-3 - the recipient's ID (= certificate's CN)
```

Sample: encrypting small doc (not DigiDoc compatible, unless original doc already in DIGIDOC-XML format)

```
> cdigid-c -encrypt c:\temp\test_Small.dd-c -out c:\Temp\test1.cd-c -encrecv
c:\temp\Rcert.cer

Input:
- c:\temp\Rcert.cer     – the recipient's certificate file
- c:\temp\test_Small.ddoc      – the input file to be encrypted
- c:\temp\test1.cdoc    - the encrypted file to be created
```

Sample: encrypting large doc (not DigiDoc compatible, unless original doc already in DIGIDOC-XML format)

```
> cdigid-c -encrypt-file c:\temp\test_Large.ddoc c:\Temp\test1.cd-c -encrecv
c:\temp\Rcert.cer

Input:
- c:\temp\Rcert.cer     – the recipient's certificate file
- c:\temp\test_Large.ddoc      – the input file to be encrypted
- c:\temp\test1.cdoc    - the encrypted file to be created
```

Sample: encrypting small doc for multiple recipients

```
> cdigid-c -encrypt-sk c:\temp\test1.txt -out c:\Temp\test1.cd-c -encrecv
c:\temp\R1cert.c-r -encrecv c:\temp\R2cert.cer

Input:
- C:\temp\test1.txt     – the input file to be encrypted
- C:\temp\test1.cdoc    - the encrypted file to be created
- C:\temp\R1cert.cer    – the 1st recipient's certificate file
```

```
- C:\temp\R2cert.cer    – the 2nd recipient's certificate file

Sample: encrypting small doc (DigiDoc compatible, original in any format),
operation in memory
> cdigid-c -encrypt-sk c:\temp\test_Small.txt -out-mem c:\Temp\test1.cd-c -
encrecv c:\temp\Rcert.cer MÄNNIK,MARI-LIIS,47101010033

Input:
- c:\temp\test_Small.txt – the input file to be encrypted
- c:\temp\test1.cdoc    - the encrypted file to be created
- c:\temp\Rcert.cer     – the recipient's certificate file
- MÄNNIK,MARI-LIIS,471010100-3 - the recipient's ID (= certificate's CN)
```

Decrypting files

-decrypt-sk <input-file> <pin> [pkcs12-file] [slot(0)]

Decrypts and possibly decompresses the encrypted file just read in and writes to output file. Expects the encrypted file t**o be inside a DigiDoc container**.

Input file (required) specifies the input file's name.

Pin (required) represents the recipient's pin1 (in context of Estonian ID cards).

pkcs12-file (optional) specifies the PKCS#12 file if decrypting is done with a software token.

slot (optional) specifies sequence number (counting from zero) of the recipient's decryption certificate and accompanying private key on the identity token. Slot 0 is used by default. Note that the sequence number used in the current command may not be the same as the actual slot's ID.

Note: There are also alternative commands for decryption, depending on the encrypted file's format, size and the certificate type used for decrypting it.

-decrypt <input-file> <pin> [pkcs12-file] [slot(0)]

Offers same functionality –s -decrypt-sk, should be used for decrypting **small** files (which do not need to be inside a DigiDoc container).

Input file (required) specifies the input file's name.

Pin (required) represents the recipient's pin1 (in contexts of Estonian ID cards).

pkcs12-file (optional) specifies the PKCS#12 file if decrypting is done with a software token.

slot (optional) specifies sequence number (counting from zero) of the recipient's decryption certificate and accompanying private key on the identity token. Slot 0 is used by default. Note that the sequence number used in the current command may not be the same as the actual slot's ID.

-decrypt-file <input-file> <output-file> <pin> [pkcs12-file]

Offers same functionality –s -decrypt for decrypting documents, should be used for decrypting **large files** (which do not need to be inside a DigiDoc container). Expects the encrypted data not to be compressed. Note that the command is not currently tested.

Input file (required) specifies the encrypted file to be decrypted.

Output file (required) specifies the output file name.

Pin (required) represents the recipient's pin1 (in contexts of Estonian ID cards).

pkcs12-file (optional) specifies the PKCS#12 file if decrypting is done with a software token.

-decrypt-hex <input-file> <key> <output-file>

For testing purposes. Decryption of the input file can be done by providing transport key value that has previously been decrypted with the recipient's private key.

Input file (required) specifies the encrypted file to be decrypted.

Key (required) specifies transport key's value that has previously been decrypted with recipient's private authentication key. The key should be provided in hexadecimal format.

Output file (required) specifies the output file name.

Command line samples for decrypting documents:

```
Sample: decrypting small encrypted file, inside a DigiDoc container
> cdigid-c -decrypt-sk c:\Temp\test1_small.cdoc 12-4 -out
c:\Temp\test1_d.ddoc

Input:
  - c:\Temp\test1_small.cdoc    - the encrypted file to be decrypted
  - 1234                        - the recipients pin1
  - C:\temp\test1_d.ddoc        - the decrypted file to be created

Sample: decrypting small encrypted file, in any original format
> cdigid-c -decrypt c:\Temp\test1_small.cdoc 12-4 -out c:\Temp\test1_d.ddoc

Input:
  - c:\Temp\test1_small.cdoc    - the encrypted file to be decrypted
  - 1234                        - the recipients pin1
  - C:\temp\test1_d.ddoc        - the decrypted file to be created

Sample: decrypting large encrypted file, in any original format
 > cdigid-c -decrypt-file c:\Temp\test1_large.cdoc c:\Temp\test1_d.ddoc 1234

Input:
  - c:\Temp\test1_large.cdoc    - the encrypted file to be decrypted
- MÄNNIK,MARI-LIIS,411102124-4 - the recipient's ID (= certificate's CN)
  - 1234                        - the recipients pin1
  - c:\temp\test1_d.ddoc        - the decrypted file to be created

Sample: decrypting, using PKCS#12 software token, in any original format
 > cdigid-c -decrypt-sk c:\Temp\test1_small.cdoc 123456 c:\test\pkcs12.p-x -
out c:\Temp\test1_d.txt

Input:
  - c:\Temp\test1_small.cdoc    - the encrypted file to be decrypted
  - 123456                      - pin code of the software token
  - c:\test\pkcs12.pfx          - software token (PKCS#12 container) file
  - c:\temp\test1_d.txt         - the decrypted file to be created

Sample: decrypting, specifying slot value
> cdigid-c -decrypt-sk c:\Temp\test1_small.cdoc 1234 ""-1 -out
c:\Temp\test1_d.ddoc

Input:
  - c:\Temp\test1_small.cdoc    - the encrypted file to be decrypted
  - 1234                        - the PIN code of the recipient
```

```
  - “”                          - empty string for optional PKCS#12 file
parameter
  - 1                           - slot (sequence number) of the recipient's
decryption certificate on identity token
  - C:\temp\test1_d.ddoc        - the decrypted file to be created

Sample: decrypting small encrypted file, inside a DigiDoc container,
operation in memory
> cdigid-c -decrypt-sk c:\Temp\test1_small.cdoc 1234 -out-mem
c:\Temp\test1_d.ddoc

Input:
  - c:\Temp\test1_small.cdoc    - the encrypted file to be decrypted
  - 1234                        - the recipients pin1
  - C:\temp\test1_d.ddoc        - the decrypted file to be created
```

6.4 Commands in CGI mode

CDigiDoc utility program can be used as a CGI program to add digital signature creation functionality to web sites.

Note: the CGI mode commands are not currently included in testing.

- **-calc-sign <cert-file> [<manifest>] [<city> <state> <zip> <country>]** – calculate hash of a digital signature. The certificate file has to be in PEM format, in a separate file. The calculated hash is displayed in console in base64 format.
- **-add-sign-value <sign-value-file> <sign-id> -** add a RSA-SHA1 signature. The signature has to be in base64 format in a separate file.
- **-del-sign <sign-id>** - remove a digital signature.
- **-cgimode [<output-separator>] -** output in CGI mode. Data sets in output are separated with the specified output separator symbol. '|' is used by default.
- **-consolemo–e -** output in console (not CGI) mode
- **-S–X -** use SAX parser
- **-XR–R -** use XmlReader parser

7. National and cross-border support

7.1 National PKI solutions and support

7.1.1 Supported Estonian identity tokens

Currently, CDigiDoc library has been tested with the following Estonian ID tokens:

Token	Type	Description	Supported CDigiDoc functionality
EstEID 3.5 and 1.0	Certificate–based PKI smart cards	Different Estonian ID card versions.	All CDigiDoc functionalities (authentication, signing, verification, encryption/decryption)

Digi-ID (since 2010)	Certificate–based PKI smart card	Estonian Digital ID card for use only in electronic environments	All CDigiDoc functionalities
Aladdin eToken Pro	Certificate–based PKI USB authenticator	Carrier for ID certificates issued to organizations.	**Note**: tested only indirectly via DigiDoc3 Client application.

7.1.2 Trusted Estonian Certificate Authorities

AS Sertifitseerimiskeskus (SK, http://sk.ee/en) functions as CA for all the Estonian ID tokens, maintains the electronic infrastructure necessary for issuing and using the ID cards, and develops the associated services and software.

SK issues the certificates and acts as Trusted Service Provider (TSP) for validation of authentication requests and digital signatures. SK maintains the following electronic services for checking certificate validity including:

- **OCSP validation service** (an RFC2560-compliant OCSP server, operating directly off the CA master certificate database and providing validity confirmations to certificates and signatures). There are two ways of getting access the service:
  - having a contract with SK and accessing the service from a specific IP address(es) – as practiced **by companies/services**
  - by having certificate for accessing the service and sending signed reques–s - as used **by private persons** for giving digital signatures; registering for the service is required and service is limited to 10 signatures per month
- CRL-s (mainly for backward compatibility)
- LDAP directory service (containing all valid certificates)

7.1.2.1 Supported SK live hierarchy chains

Note: no additional actions are needed for using the following CA and OCSP responder certificates with CDigiD–c - these certificate files have been:

- included in the CDigiDoc distribution
- registered in the CDigiDoc configuration file.

Certificate Common Name (CN)			Valid to	Description
JUUR-SK			26-Aug-2016	SK's 1st root certificate
	ESTEID-SK		13-Jan-2012	for ID cards issued until 2007
		ESTEID-SK OCSP RESPONDER	*24-Mar-2005*	ESTEID-SK OCSP Responder
		ESTEID-SK OCSP RESPONDER 2005	*12-Jan- 2012*	ESTEID-SK OCSP Responder
	ESTEID-SK 2007		26-Aug-2016	for ID cards, Digi-ID and Mobile-IDs issued until 06.2011
		ESTEID-SK 2007 OCSP RESPONDER	*08-Jan-2010*	ESTEID-SK 2007 OCSP Responder
		ESTEID-SK 2007 OCSP RESPONDER 2010	*26-Aug-2016*	ESTEID-SK 2007 OCSP Responder

Certificate Common Name (CN)			Valid to	Description
	EID-SK		08-May-2014	for all other personal certificates issued until 01.2007
		EID-SK 2007 OCSP RESPONDER	*15-May-2007*	EID-SK OCSP Responder
	EID-SK 2007		26-Aug-2016	for Estonian Mobile-IDs issued until 02.2011 and Lithuanian Mobile IDs issued until 06.2011
		EID-SK 2007 OCSP RESPONDER	*17-Apr- 2010*	EID-SK 2007 OCSP Responder
		EID-SK 2007 OCSP RESPONDER 2010	*26-Aug- 2010*	EID-SK 2007 OCSP Responder
	KLASS3-SK		05-May-2012	for organizational certificates issued until 10.2010
		KLASS3-SK OCSP RESPONDER	*05-Apr- 2006*	KLASS3-SK OCSP Responder
		KLASS3-SK OCSP 2006 RESPONDER	*27-Mar-2009*	KLASS3-SK OCSP Responder
		KLASS3-SK OCSP 2009 RESPONDER	*04-May- 2012*	KLASS3-SK OCSP Responder
	KLASS3-SK 2010		26-Aug-2016	for organizational certificates issued from 10.2010
		KLASS3-SK 2010 OCSP RESPONDER	*26-Aug- 2016*	KLASS3-SK 2010 OCSP Responder
EECCRCA			18-Dec- 2030	SK's 2nd root certificate
	ESTEID-SK 2011		18-Mar- 2024	for ID cards, Digi-ID and Mobile-IDs issued from 06.2011
	EID-SK 2011		18-Mar- 2024	for all other personal certificates issued from 06.2011
	KLASS3-SK 2010		18-Mar-2024	for organizational certificates.
	SK OCSP 2011 RESPONDER		*18-Mar- 2024*	common OCSP responder for all certificates issued under EECCRCA

7.1.2.2 Supported SK test certificate hierarchy chains

Note: the following test certificates have been registered in the CDigiDoc configuration file but have not been included in the CDigiDoc distribution. In order to use the test certificates with CDigiDoc, you need to install them separately (the installation package containing both Estonian and Finnish test certificates is accessible from https://installer.id.ee/media/windows/Eesti_ID_kaart_testsertifikaadid.msi).

Note that the test certificates should not be used in live applications as the CDigiDoc library does not give notifications to the user in case of test signatures.

Certificate Common Name (CN)			Valid to	Description
Test JUUR-SK			27-Aug-2016	SK's 1st test root certificate
	TEST-SK		26-Aug-2016	for all test cards and certificates issued until 04.2011
		Test-SK OCSP RESPONDER 2005	*06-Apr-2012*	TEST-SK OCSP responder
	TEST of KLASS3-SK 2010		21-March-2025	for organizational test certificates
TEST EECCRCA			18-Dec-2030	SK's 2nd test root certificate
	TEST of ESTEID-SK 2011		07-Sep-2023	for test ID cards, Digi-ID and Mobile-ID certificates issued from 04.2011
	TEST of EID-SK 2011		07-Sep-2023	for all other test certificates issued from 04.2011
	Test SK OCSP RESPONDER 2011		*07-Sep-2024*	common OCSP responder for all test certificates issued under TEST-EECCRCA

7.1.3 Supported Finnish Certificate Authorities

Population Registration Center's Certification Authority Services unit (FINeID, http://fineid.fi/) functions as certificate authority in Finland.

CDigiDoc supports only signature validation functionality in case of Finnish certificates. The CA certificates for signature validation are taken from file system.

7.1.4 Supported FINeID live hierarchy chains

Note: in order to use the Finnish certificates with CDigiDoc, you need to add them separately. The installation package is available from https://installer.id.ee/media/windows/Eesti_ID_kaart_finsertifikaadid.msi

The certificates package contains Finnish root CA certificate (http://fineid.fi/default.aspx?id=596) and certificates which are included in the Finnish national Trust Service List (TSL) (https://www.viestintavirasto.fi/attachments/TSL-Ficora.xml).

Certificate Common Name (CN)		Valid to	Description
VRK Gov. Root CA		18-Dec-2023	1st root certificate
	VRK Gov. CA for Citizen Qualified Certificates	09-Jan-2019	Citizen certificates on identity cards since 2003
	VRK CA for Qualified Certificates	13-Jan-2019	Organization certificates on organization cards since 2003

Certificate Common Name (CN)		Valid to	Description
	VRK CA for Healthcare Professionals Qualified Certificates	17-Dec-2023	Intermediary CA of the certificates for users of the nationwide healthcare information systems

7.1.5 Supported FINeID test certificate hierarchy chains

Note: in order to use the test certificates with CDigiDoc, you need to install them separately (the installation package which includes both Estonian and Finnish test certificates is accessible from https://installer.id.ee/media/windows/Eesti_ID_kaart_testsertifikaadid.msi). The test certificates are also separately downloadable from http://fineid.fi/default.aspx?id=597.

Note that the test certificates should not be used in live applications as the CDigiDoc library does not give notifications to the user in case of test signatures.

Certificate Common Name (CN)		Valid to	Description
VRK TEST Root CA		17-Dec-2023	1st test root certificate
	VRK CA for Test Purposes	12-Jan-2019	Test certificates since 2003

7.2 Interoperability testing

7.2.1 DigiDoc framework cross-usability tests

Automated cross-usability tests of digitally signed and encrypted files are periodically carried out between different DigiDoc software libraries [13]:

- Cross-usability tests of digitally signed files in **DIGIDOC-XML 1.3** format (.ddoc files) are carried out between **JDigiDoc** and **CDigiDoc** software libraries.
- Cross-usability of **BDOC 2.1** (.bdoc or .asice) file format is tested between **JDigiDoc** and **Libdigidocpp** libraries.
- Cross-usability of encrypted file format **CDOC 1.0** is carried out between **JDigiDoc** and **CDigiDoc** software libraries.

The interoperability tests are executed through the **command line utility tools of the software libraries** (for example, in case of JDigiDoc library, the utility program which is described in chapter **Error! Reference source not found.** of the current document).

7.2.2 CDigiDoc API's usage in CDigiDoc utility program

The CDigiDoc API's methods that are directly called out by CDigiDoc utility program are listed in the table below. Note that as the API is tested via the CDigiDoc utility program then the following functions have been tested the most thoroughly.

CDigiDoc utility's command	Called CDigiDoc API method(s)
`-check-cert`	**`ReadCertificate`**`(X509 **x509, const char *szCertfile);` **`ddocVerifyCertByOCSP`**`(X509* pCert, OCSP_RESPONSE **ppResp);` **`ddocCertGetSubjectCN`**`(X509* pCert, DigiDocMemBuf* pMemBuf);`
`-in <input-ddoc-file>`	**`ConfigItem_lookup_int`**`(const char* key, int defValue);` **`ddocSaxReadSignedDocFromFile`**`(SignedDoc** ppSigDoc, const char* szFileName, int checkFileDigest, long lMaxDFLen);`

CDigiDoc utility's command	Called CDigiDoc API method(s)
-in <input-encrypted-file>	**ConfigItem_lookup_int**(const char* key, int defValue); **dencSaxReadEncryptedData**(DEncEncryptedData** ppEncData, const char* szFileName);
-new	**ConfigItem_lookup**(const char* key); **SignedDoc_new**(SignedDoc **pSignedDoc, const char* format, const char* version);
-add <input-file> <mime-type>	**ddocConvertInput**(const char* src, char** dest); **getFullFileName**(const char* szFileName, char* szDest, int len); **DataFile_new**(DataFile **newDataFile, SignedDoc* pSigDoc, const char* id, const char* filename, const char* contentType, const char* mime, long size, const byte* digest, int digLen, const char* digType, const char* szCharset); **calculateDataFileSizeAndDigest**(SignedDoc* pSigDoc, const char* id, const char* filename, int digType);
-sign <pin-code>	**signDocumentWithSlotAndSigner**(SignedDoc* pSigDoc, SignatureInfo** ppSigInfo, const char* pin, const char* manifest, const char* city, const char* state, const char* zip, const char* country, int nSlot, int nOcsp, int nSigner, const char* szPkcs12FileName);
-out <output-ddoc-file>	**createSignedDoc**(SignedDoc* pSigDoc, const char* szOldFile, const char* szOutputFile);
-out <output-encrypted-file>	**dencGenEncryptedData_writeToFile**(DEncEncryptedData* pEncData, const char* szFileName);
-verify	**getCountOfSignatures**(const SignedDoc* pSigDoc); **getSignature**(const SignedDoc* pSigDoc, int nIdx); **ddocCertGetSubjectCN**(X509* pCert, DigiDocMemBuf* pMemBuf); **verifySignatureAndNotary**(SignedDoc* pSigDoc, SignatureInfo* pSigInfo, const char* szFileName); **getCountOfSignerRoles**(SignatureInfo* pSigInfo, int nCertified); **getSignerRole**(SignatureInfo* pSigInfo, int nCertified, int nIdx); **ddocSigInfo_GetSignersCert**(const SignatureInfo* pSigInfo); **getNotaryWithSigId**(const SignedDoc* pSigDoc, const char* sigId); **ddocNotInfo_GetResponderId**(const NotaryInfo* pNotary); **ReadCertSerialNumber**(char* szSerial, int nMaxLen, X509 *x509); **ddocCertGetIssuerDN**(X509* pCert, DigiDocMemBuf* pMemBuf); **ddocCertGetSubjectDN**(X509* pCert, DigiDocMemBuf* pMemBuf); **getCertNotBefore**(const SignedDoc* pSigDoc, X509* cert, char* timestamp, int len); **getCertNotAfter**(const SignedDoc* pSigDoc, X509* cert, char* timestamp, int len); **readCertPolicies**(X509* pX509, PolicyIdentifier** pPolicies, int* nPols);

CDigiDoc utility's command	Called CDigiDoc API method(s)
-extract <data-file-id> <output-file>	**ddocExtractDataFile**(SignedDoc* pSigDoc, const char* szFileName, const char* szDataFileName, const char* szDocId, const char* szCharset);
-extract-mem <data-file-id> <output-file>	**ddocGetDataFileCachedData**(SignedDoc* pSigDoc, const char* szDocId, void** ppBuf, long* pLen);
-get-confirmation <signature-id>	**getSignatureWithId**(const SignedDoc* pSigDoc, const char* id); **notarizeSignature**(SignedDoc* pSigDoc, SignatureInfo* pSigInfo);
-mid-sign <phone-no> <per-code> [[<country>(EE)] [<lang>(EST)] [<service>(Testing)] [<manifest>] [<city> <state> <zip>]]	**ConfigItem_lookup_int**(const char* key, int defValue); **ConfigItem_lookup**(const char* key); **ddsSign**(SignedDoc* pSigDoc, const char* szIdCode, const char* szPhoneNo, const char* szLang, const char* szServiceName, const char* manifest, const char* city, const char* state, const char* zip, const char* country, char* url, char* proxyHost, char* proxyPort, long* pSesscode, char* szChallenge, int nChalLen); **ddsGetStatus**(SignedDoc* pSigDoc, long lSesscode, char* url, char* proxyHost, char* proxyPort, int* pStatus);
-denc-list <input-file>	**dencSaxReadEncryptedData**(DEncEncryptedData** ppEncData, const char* szFileName); **dencMetaInfo_GetLibVersion**(DEncEncryptedData* pEncData, char* szLibrary, int nLibLen, char* szVersion, int nVerLen); **dencMetaInfo_GetFormatVersion**(DEncEncryptedData* pEncData, char* szFormat, int nFormat, char* szVersion, int nVersion);
-encrecv <certificate-file>	**dencEncryptedData_new**(DEncEncryptedData** pEncData, const char* szXmlNs, const char* szEncMethod, const char* szId, const char* szType, const char* szMimeType); **dencMetaInfo_SetLibVersion**(DEncEncryptedData* pEncData); **dencMetaInfo_SetFormatVersion**(DEncEncryptedData* pEncData); **ReadCertificate**(X509 **x509, const char *szCertfile); **ddocCertGetSubjectCN**(X509* pCert, DigiDocMemBuf* pMemBuf); **dencEncryptedKey_new**(DEncEncryptedData* pEncData, DEncEncryptedKey** pEncKey, X509* pCert, const char* szEncMethod, const char* szId, const char* szRecipient, const char* szKeyName, const char* szCarriedKeyName);
-encrypt-sk <input-file>	**ConfigItem_lookup_int**(const char* key, int defValue); **dencEncryptedData_new**(DEncEncryptedData** pEncData, const char* szXmlNs, const char* szEncMethod, const char* szId, const char* szType, const char* szMimeType); **dencMetaInfo_SetLibVersion**(DEncEncryptedData* pEncData); **dencMetaInfo_SetFormatVersion**(DEncEncryptedData* pEncData); **ddocConvertInput**(const char* src, char** dest); **dencEncryptionProperty_new**(DEncEncryptedData* pEncData, DEncEncryptionProperty** ppEncProperty, const char* szId, const char* szTarget, const char* szName, const char* szContent); **SignedDoc_new**(SignedDoc **pSignedDoc, const char* format, const char* version);

CDigiDoc utility's command	Called CDigiDoc API method(s)
	calculateFileSize(const char* szFileName, long* lFileLen); **DataFile_new**(DataFile **newDataFile, SignedDoc* pSigDoc, const char* id, const char* filename, const char* contentType, const char* mime, long size, const byte* digest, int digLen, const char* digType, const char* szCharset); **dencOrigContent_registerDigiDoc**(DEncEncryptedData* pEncData, SignedDoc* pSigDoc); **createSignedDoc**(SignedDoc* pSigDoc, const char* szOldFile, const char* szOutputFile); **ddocReadFile**(const char* szFileName, DigiDocMemBuf* pData); **dencEncryptedData_encryptData**(DEncEncryptedData* pEncData, int nCompressOption);
-encrypt <input-file>	**ConfigItem_lookup_int**(const char* key, int defValue); **dencEncryptedData_new**(DEncEncryptedData** pEncData, const char* szXmlNs, const char* szEncMethod, const char* szId, const char* szType, const char* szMimeType); **dencMetaInfo_SetLibVersion**(DEncEncryptedData* pEncData); **dencMetaInfo_SetFormatVersion**(DEncEncryptedData* pEncData); **dencEncryptionProperty_new**(DEncEncryptedData* EncData, DEncEncryptionProperty** ppEncProperty, const char* szId, const char* szTarget, const char* szName, const char* szContent); **dencEncryptedData_AppendData**(DEncEncryptedData* pEncData, const char* data, int len); **ddocSaxReadSignedDocFromFile**(SignedDoc** ppSigDoc, const char* szFileName, int checkFileDigest, long lMaxDFLen); **dencOrigContent_registerDigiDoc**(DEncEncryptedData* pEncData, SignedDoc* pSigDoc); **dencEncryptedData_encryptData**(DEncEncryptedData* pEncData, int nCompressOption);
-encrypt-file <input-file> <output-file>	**dencEncryptFile**(DEncEncryptedData* pEncData, const char* szInputFileName, const char* szOutputFileName, const char* szMimeType);
-decrypt-sk <output-file> <pin>	Functions of –decrypt command. **utf82unicode**(const char* utf8, char** unicode, int* outlen); **ddocSaxReadSignedDocFromFile**(SignedDoc** ppSigDoc, const char* szFileName, int checkFileDigest, long lMaxDFLen); **getCountOfDataFiles**(const SignedDoc* pSigDoc); **getDataFile**(const SignedDoc* pSigDoc, int nIdx); **ddocExtractDataFile**(SignedDoc* pSigDoc, const char* szFileName, const char* szDataFileName, const char* szDocId, const char* szCharset);
-decrypt <output-file> <pin>	**dencSaxReadEncryptedData**(DEncEncryptedData** ppEncData, const char* szFileName); **dencEncryptedData_findEncryptedKeyByPKCS12**(DEncEncryptedData* pEncData, DEncEncryptedKey** ppEncKey, EVP_PKEY** ppKey, const char* szPkcs12File, const char* szPasswd);

CDigiDoc utility's command	Called CDigiDoc API method(s)
	dencEncryptedData_findEncryptedKeyByPKCS11UsingSlot(DEncEncryptedData* pEncData, DEncEncryptedKey** ppEncKey, int nSlot); **dencEncryptedData_decryptWithKey**(DEncEncryptedData* pEncData, DEncEncryptedKey* pEncKey, EVP_PKEY* pKey); **dencEncryptedData_decryptUsingSlot**(DEncEncryptedData* pEncData, DEncEncryptedKey* pEncKey, const char* pin, int nSlot);
-decrypt-file <input-file> <output-file> <pin>	**dencSaxReadDecryptFile**(const char* szInputFileName, const char* szOutputFileName, const char* szPin, const char* szPkcs12File);

8. CDigiDoc library's implementation notes

The following section describes properties of DIGIDOC-XML 1.3 files that are not strictly defined in the DIGIDOC-XML 1.3 [1] specification but are used in CDigiDoc library's implementation (and also in other DigiDoc software libraries) of the file formats.

8.1 General implementation notes

Digital signature related notes:

1. One OCSP confirmation (time-mark) is allowed for each signature (due to security reasons and in order to maintain testing efficiency).
2. <Transforms> element is not supported for security purposes and in order to maintain testing efficiency.
3. It is not allowed to add two data files with the same name to the container as the signed data file must be uniquely identifiable in the container.
4. All data files in the container must be signed. All signatures in the container must sign all of the data files.
5. During signature creation, it is checked that there is only one <ClaimedRole> element in the signature, which contains the signer's role and optionally the signer's resolution. If the <ClaimedRole> element contains both role and resolution then they must be separated with a slash mark, e.g. "role / resolution". Note that when setting the resolution value then role must also be specified.
6. During signature validation, at most two <ClaimedRole> elements are allowed for a signature.
7. Altering files in older formats SK-XML 1.0, DIGIDOC-XML 1.1 and 1.2 is not supported by the library. It is possible to validate and extract data files from these documents, but validation is expected to return error code about old DigiDoc file format. CDigiDoc utility program (identically to DigiDoc3 Client application) regards this validation error as a validation warning.

Signer certificate related notes:

1. Valid signatures (qualified electronic signatures) can be created with a certificate that has "Non-repudiation" value (also referred to as "Content Commitment") in its "Key usage" field. The requirement is based on the following sources:
    - ETSI TS 102 280 (V1.1.1): "X.509 V3 Certificate Profile for Certificates Issued to Natural Persons" [10]; chap. 5.4.3;
    - Profile of certificates issued to private persons by AS Sertifitseerimiskeskus: "Certificates on identity card of Republic of Estonia", version 3.3 [11]; appendix A.3.3;
    - Profile of certificates issued to legal entities by AS Sertifitseerimiskeskus: "Profile of institution certificates and Certificate Revocation Lists", version 1.3 [12]; chap. 3.2.2.
2. Signature can be created with a certificate that doesn't have "Non-repudiation" value in its "Key-Usage" field when specific parameters have been set but validation of such signature will produce a respective error message and the signature is not considered as a qualified electronic signature.

8.2 DIGIDOC-XML 1.3 specific implementation notes

1. The only data file embedding mode that is supported, is CONTENT_EMBEDDED_BASE64 which means that the data file is included in the DigiDoc container in base64 encoding.
2. The nonce value's calculation in case of time-marking mechanism of DIGIDOC-XML 1.3 file format is implemented as follows:
   - the contents of <SignatureValue> element (i.e. the value without XML tags) is taken and decoded from base64 encoding;
   - digest of the value found in the previous step is calculated by using SHA-1 algorithm.
   - the digest value is included in the OCSP request's "nonce" field and must be present in the respective field of the OCSP response.
3. In case of DigiDocService web service [9] and DIGIDOC-XML 1.3 file format, CDigiDoc software library supports HASHCODE data file mode for intermediary ddoc files. The mode allows sending only the data file's digest value to the service, instead of embedding the whole data file to the container. In this case, it is possible to add larger data files than 4MB to the container (which would otherwise be the maximum data file size allowed in DigiDocService).
4. Embedding data files to the container as pure XML (EMBEDDED data file mode) and signing data files that are not included in the container (DETACHED data file mode) are not supported.
5. <DataFile> element's Id attribute value is set as "D<seq_no>" when adding the file to DigiDoc container. During verification, the Id attribute "DO" is also accepted as valid.
6. In case of DIGIDOC-XML 1.3 documents, the following validation errors are regarded as minor technical errors and are treated as validation warnings in cdigidoc utility program (identically to DigiDoc3 Client application):
   - <DataFile> element's xmlns attribute is missing.
   - <IssuerSerial><X509IssuerName> and/or <IssuerSerial><X509SerialNumber> element's xmlns attribute is missing.
7. It is possible to use CDigiDoc configuration file's parameter CHECK_OCSP_NONCE with DIGIDOC-XML 1.3 files, which, if set to "true", means that the presence of OCSP response's (the contents of <EncapsulatedOCSPValue> element) nonce value's ASN.1 prefix is not required during signature validation. Otherwise, it is required by RFC 2560 specification ("Online Certificate Status Protocol - OCSP") that the OCSP response's nonce value must have the corresponding ASN.1 prefix (OCTET STRING tag (04_{hex}) followed by the length of the nonce value in hexadecimal format). By default, the nonce value's ASN.1 prefix is not checked in order to support validation of DIGIDOC-XML 1.3 files created with CDigiDoc library's version below v3.7.

Appendix 1: CDigiDoc configuration file

A sample CDigiDoc configuration file may consist of the following sections and possible entries:

- user-specific values to be always checked and possibly modified in purple
- optional and alternative settings in *blue*
- section headers in **green**
- # is indicating all out-commented parameters and additional notes

```
#--------------------------------------------------
# DigiDoc library global configuration file
#--------------------------------------------------

# PKCS#11 module settings - change this according to your signature device!!!
DIGIDOC_DEFAULT_DRIVER   =       1
DIGIDOC_DRIVERS  =       1
DIGIDOC_DRIVER_1_NAME    =       OpenSC
DIGIDOC_DRIVER_1_DESC    =       OpenSC projects PKCS#11 driver
DIGIDOC_DRIVER_1_FILE    =       opensc-pkcs11.dll
# for Linux: DIGIDOC_DRIVER_1_FILE = opensc-pkcs11.so

# Digital signing settings
# Identifier of the signer's private key's slot on an identity token.
DIGIDOC_SIGNATURE_SLOT   =       1

# Default OCSP responder URL
DIGIDOC_OCSP_URL         =       http://ocsp.sk.ee
# OpenXAdeS test responder URL
#DIGIDOC_OCSP_URL         =      http://www.openxades.org/cgi-bin/ocsp.cgi


# Sign OCSP requests or not. Depends on your responder
# Set this parameter value to "true" if OCSP requests need to be signed
SIGN_OCSP        =       false
# The PKCS#12 file used to sign OCSP requests
# DIGIDOC_PKCS_FILE = <your-pkcs12-file-name>
# Password for this key
# DIGIDOC_PKCS_PASSWD = <your-pkcs12-passwd>

# Your HTTP proxy if necessary
USE_PROXY        =       false
# DIGIDOC_PROXY_HOST = <your-proxy-hostname>
# DIGIDOC_PROXY_PORT = <proxy-port>
# DIGIDOC_PROXY_USER = <proxy-username>
# DIGIDOC_PROXY_PASS = <proxy-password>

# Signature verification settings
CHECK_OCSP_NONCE         =       false

# CA certificates
CA_CERT_PATH     =       C:\Program Files\Estonian ID Card Development\libdigidoc\certs
CA_CERTS         =       23

CA_CERT_1        =       JUUR-SK.crt
CA_CERT_1_CN     =       Juur-SK
CA_CERT_2        =       ESTEID-SK.crt
```

```
CA_CERT_2_CN    =       ESTEID-SK
CA_CERT_3       =       ESTEID-SK 2007.crt
CA_CERT_3_CN    =       ESTEID-SK 2007
CA_CERT_4       =       KLASS3-SK.crt
CA_CERT_4_CN    =       KLASS3-SK
CA_CERT_5       =       KLASS3-SK 2010.crt
CA_CERT_5_CN    =       KLASS3-SK 2010
CA_CERT_6       =       KLASS3-SK 2010 EECCRCA.crt
CA_CERT_6_CN    =       KLASS3-SK 2010
CA_CERT_6       =       EID-SK.crt
CA_CERT_6_CN    =       EID-SK
CA_CERT_7       =       EID-SK.crt
CA_CERT_7_CN    =       EID-SK
CA_CERT_8       =       EID-SK 2007.crt
CA_CERT_8_CN    =       EID-SK 2007
CA_CERT_9       =       EECCRCA.crt
CA_CERT_9_CN    =       EE Certification Centre Root CA
CA_CERT_10      =       ESTEID-SK 2011.crt
CA_CERT_10_CN   =       ESTEID-SK 2011
CA_CERT_11      =       EID-SK 2011.crt
CA_CERT_11_CN   =       EID-SK 2011

# Certificates for Estonian test ID-cards
CA_CERT_12      =       TEST Juur-SK.crt
CA_CERT_12_CN   =       TEST Juur-SK
CA_CERT_13      =       TEST-SK.crt
CA_CERT_13_CN   =       TEST-SK
CA_CERT_14      =       TEST EECCRCA.crt
CA_CERT_14_CN   =       TEST of EE Certification Centre Root CA
CA_CERT_15      =       TEST ESTEID-SK 2011.crt
CA_CERT_15_CN   =       TEST of ESTEID-SK 2011
CA_CERT_16      =       TEST EID-SK 2011.crt
CA_CERT_16_CN   =       TEST of EID-SK 2011
CA_CERT_17      =       TEST KLASS3 2010.crt
CA_CERT_17_CN   =       TEST of KLASS3-SK 2010

# Certificates for Finnish test ID-cards
CA_CERT_18      =       TEST VRK TEST Root CA.crt
CA_CERT_18_CN   =       VRK TEST Root CA
CA_CERT_19      =       TEST VRK CA for Test Purposes.crt
CA_CERT_19_CN   =       VRK CA for Test Purposes

# Certificates for Finnish ID-cards
CA_CERT_20      =       VRK ROOT.crt
CA_CERT_20_CN   =       VRK Gov. Root CA
CA_CERT_21      =       VRK CQC.crt
CA_CERT_21_CN   =       VRK Gov. CA for Citizen Qualified Certificates
CA_CERT_22      =       VRK HCPQC.crt
CA_CERT_22_CN   =       VRK CA for Healthcare Professionals Qualified Certificates
CA_CERT_23      =       VRK QC.crt
CA_CERT_23_CN   =       VRK CA for Qualified Certificates

# OCSP responder certificates
# Note: if you add or remove some of these certificates, update the following number,
# also pay attention to proper naming
DIGIDOC_OCSP_RESPONDER_CERTS    =       24

DIGIDOC_OCSP_RESPONDER_CERT_1=TEST-SK OCSP 2005.crt
DIGIDOC_OCSP_RESPONDER_CERT_1_CN=TEST-SK OCSP RESPONDER 2005
DIGIDOC_OCSP_RESPONDER_CERT_1_CA=TEST-SK
DIGIDOC_OCSP_RESPONDER_CERT_1_URL=http://www.openxades.org/cgi-bin/ocsp.cgi
```

```
DIGIDOC_OCSP_RESPONDER_CERT_2=KLASS3-SK OCSP 2009.crt
DIGIDOC_OCSP_RESPONDER_CERT_2_CN=KLASS3-SK OCSP RESPONDER 2009
DIGIDOC_OCSP_RESPONDER_CERT_2_CA=KLASS3-SK

DIGIDOC_OCSP_RESPONDER_CERT_3=ESTEID-SK OCSP 2005.crt
DIGIDOC_OCSP_RESPONDER_CERT_3_CN=ESTEID-SK OCSP RESPONDER 2005
DIGIDOC_OCSP_RESPONDER_CERT_3_CA=ESTEID-SK

DIGIDOC_OCSP_RESPONDER_CERT_4=ESTEID-SK 2007 OCSP.crt
DIGIDOC_OCSP_RESPONDER_CERT_4_CN=ESTEID-SK 2007 OCSP RESPONDER
DIGIDOC_OCSP_RESPONDER_CERT_4_CA=ESTEID-SK 2007

DIGIDOC_OCSP_RESPONDER_CERT_5=EID-SK 2007 OCSP.crt
DIGIDOC_OCSP_RESPONDER_CERT_5_CN=EID-SK 2007 OCSP RESPONDER
DIGIDOC_OCSP_RESPONDER_CERT_5_CA=EID-SK 2007

DIGIDOC_OCSP_RESPONDER_CERT_6=EID-SK OCSP 2006.crt
DIGIDOC_OCSP_RESPONDER_CERT_6_1=EID-SK OCSP.crt
DIGIDOC_OCSP_RESPONDER_CERT_6_CN=EID-SK OCSP RESPONDER
DIGIDOC_OCSP_RESPONDER_CERT_6_CA=EID-SK

DIGIDOC_OCSP_RESPONDER_CERT_7=ESTEID-SK OCSP.crt
DIGIDOC_OCSP_RESPONDER_CERT_7_CN=ESTEID-SK OCSP RESPONDER
DIGIDOC_OCSP_RESPONDER_CERT_7_CA=ESTEID-SK

DIGIDOC_OCSP_RESPONDER_CERT_8=KLASS3-SK OCSP 2006.crt
DIGIDOC_OCSP_RESPONDER_CERT_8_1=KLASS3-SK OCSP.crt
DIGIDOC_OCSP_RESPONDER_CERT_8_CN=KLASS3-SK OCSP RESPONDER
DIGIDOC_OCSP_RESPONDER_CERT_8_CA=KLASS3-SK

DIGIDOC_OCSP_RESPONDER_CERT_9=EID-SK 2007 OCSP 2010.crt
DIGIDOC_OCSP_RESPONDER_CERT_9_CN=EID-SK 2007 OCSP RESPONDER 2010
DIGIDOC_OCSP_RESPONDER_CERT_9_CA=EID-SK 2007

DIGIDOC_OCSP_RESPONDER_CERT_10=ESTEID-SK 2007 OCSP 2010.crt
DIGIDOC_OCSP_RESPONDER_CERT_10_CN=ESTEID-SK 2007 OCSP RESPONDER 2010
DIGIDOC_OCSP_RESPONDER_CERT_10_CA=ESTEID-SK 2007

DIGIDOC_OCSP_RESPONDER_CERT_11=KLASS3-SK 2010 OCSP.crt
DIGIDOC_OCSP_RESPONDER_CERT_11_CN=KLASS3-SK 2010 OCSP RESPONDER
DIGIDOC_OCSP_RESPONDER_CERT_11_CA=KLASS3-SK 2010

DIGIDOC_OCSP_RESPONDER_CERT_12=SK OCSP 2011.crt
DIGIDOC_OCSP_RESPONDER_CERT_12_CN=SK OCSP RESPONDER 2011
DIGIDOC_OCSP_RESPONDER_CERT_12_CA=EE Certification Centre Root CA

DIGIDOC_OCSP_RESPONDER_CERT_13=SK OCSP 2011.crt
DIGIDOC_OCSP_RESPONDER_CERT_13_CN=SK OCSP RESPONDER 2011
DIGIDOC_OCSP_RESPONDER_CERT_13_CA=ESTEID-SK 2011

DIGIDOC_OCSP_RESPONDER_CERT_14=SK OCSP 2011.crt
DIGIDOC_OCSP_RESPONDER_CERT_14_CN=SK OCSP RESPONDER 2011
DIGIDOC_OCSP_RESPONDER_CERT_14_CA=EID-SK 2011

# OCSP responder settings for Estonian test ID-cards
DIGIDOC_OCSP_RESPONDER_CERT_15=TEST SK OCSP 2011.crt
DIGIDOC_OCSP_RESPONDER_CERT_15_CN=TEST of SK OCSP RESPONDER 2011
DIGIDOC_OCSP_RESPONDER_CERT_15_CA=TEST of EE Certification Centre Root CA
DIGIDOC_OCSP_RESPONDER_CERT_15_URL=http://www.openxades.org/cgi-bin/ocsp.cgi
```

```
DIGIDOC_OCSP_RESPONDER_CERT_16=TEST SK OCSP 2011.crt
DIGIDOC_OCSP_RESPONDER_CERT_16_CN=TEST of SK OCSP RESPONDER 2011
DIGIDOC_OCSP_RESPONDER_CERT_16_CA=TEST of ESTEID-SK 2011
DIGIDOC_OCSP_RESPONDER_CERT_16_URL=http://www.openxades.org/cgi-bin/ocsp.cgi

DIGIDOC_OCSP_RESPONDER_CERT_17=TEST SK OCSP 2011.crt
DIGIDOC_OCSP_RESPONDER_CERT_17_CN=TEST of SK OCSP RESPONDER 2011
DIGIDOC_OCSP_RESPONDER_CERT_17_CA=TEST of EID-SK 2011
DIGIDOC_OCSP_RESPONDER_CERT_17_URL=http://www.openxades.org/cgi-bin/ocsp.cgi

DIGIDOC_OCSP_RESPONDER_CERT_18=TEST SK OCSP 2011.crt
DIGIDOC_OCSP_RESPONDER_CERT_18_CN=TEST of SK OCSP RESPONDER 2011
DIGIDOC_OCSP_RESPONDER_CERT_18_CA=TEST of KLASS3-SK 2010
DIGIDOC_OCSP_RESPONDER_CERT_18_URL=http://www.openxades.org/cgi-bin/ocsp.cgi

# OCSP responder settings for Finnish ID-cards
DIGIDOC_OCSP_RESPONDER_CERT_19=TEST SK OCSP 2011.crt
DIGIDOC_OCSP_RESPONDER_CERT_19_CN=TEST of SK OCSP RESPONDER 2011
DIGIDOC_OCSP_RESPONDER_CERT_19_CA=VRK CA for Test Purposes
DIGIDOC_OCSP_RESPONDER_CERT_19_URL=http://www.openxades.org/cgi-bin/ocsp.cgi

DIGIDOC_OCSP_RESPONDER_CERT_20=TEST SK OCSP 2011.crt
DIGIDOC_OCSP_RESPONDER_CERT_20_CN=TEST of SK OCSP RESPONDER 2011
DIGIDOC_OCSP_RESPONDER_CERT_20_CA=VRK TEST Root CA
DIGIDOC_OCSP_RESPONDER_CERT_20_URL=http://www.openxades.org/cgi-bin/ocsp.cgi

DIGIDOC_OCSP_RESPONDER_CERT_21=SK OCSP 2011.crt
DIGIDOC_OCSP_RESPONDER_CERT_21_CN=SK OCSP RESPONDER 2011
DIGIDOC_OCSP_RESPONDER_CERT_21_CA=VRK Gov. Root CA
DIGIDOC_OCSP_RESPONDER_CERT_21_URL=http://ocsp.sk.ee/_proxy

DIGIDOC_OCSP_RESPONDER_CERT_22=SK OCSP 2011.crt
DIGIDOC_OCSP_RESPONDER_CERT_22_CN=SK OCSP RESPONDER 2011
DIGIDOC_OCSP_RESPONDER_CERT_22_CA=VRK Gov. CA for Citizen Qualified Certificates
DIGIDOC_OCSP_RESPONDER_CERT_22_URL=http://ocsp.sk.ee/_proxy

DIGIDOC_OCSP_RESPONDER_CERT_23=SK OCSP 2011.crt
DIGIDOC_OCSP_RESPONDER_CERT_23_CN=SK OCSP RESPONDER 2011
DIGIDOC_OCSP_RESPONDER_CERT_23_CA=VRK CA for Healthcare Professionals Qualified Certificates
DIGIDOC_OCSP_RESPONDER_CERT_23_URL=http://ocsp.sk.ee/_proxy

DIGIDOC_OCSP_RESPONDER_CERT_24=SK OCSP 2011.crt
DIGIDOC_OCSP_RESPONDER_CERT_24_CN=SK OCSP RESPONDER 2011
DIGIDOC_OCSP_RESPONDER_CERT_24_CA=VRK CA for Qualified Certificates
DIGIDOC_OCSP_RESPONDER_CERT_24_URL=http://ocsp.sk.ee/_proxy

# Encryption settings
# Compression mode of data before encryption. Possible values: 0 – always compress, 1 – never
compress, 2 – best effort
DENC_COMPRESS_MODE      =       0
# DENC_COMPRESS_MODE    =       1
# DENC_COMPRESS_MODE    =       2

# Debugging settings
# Specifies the amount of information printed out. Possible value range: 0-9
# DEBUG_LEVEL   =       3
# Note that the directory where you want to store the output file has to exist before
# debugging, otherwise the file is not created.
# DEBUG_FILE    =       <your-debugging-log-file>
```

Appendix 2: Signature types

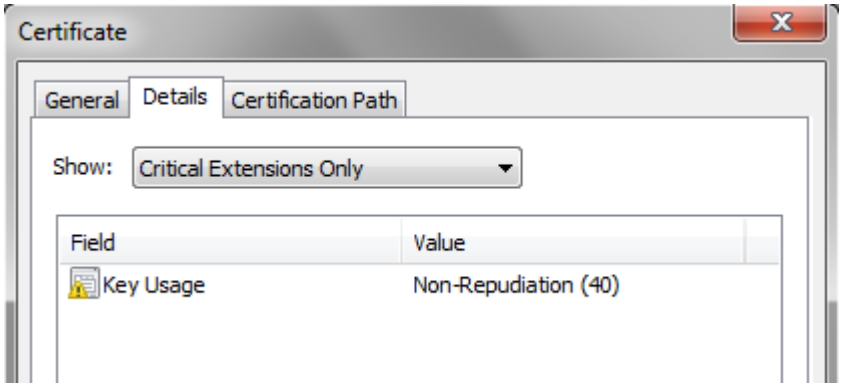
The signatures which are created can be either digital stamps, qualified electronic signatures or technical signatures depending on the certificate which is used for signing and whether OCSP confirmation is added or not.

Qualified electronic signature, i.e. ordinary digital signature

Qualified electronic signatures have the following characteristics:

- the certificate for signing has been issued to a private person,
- the signer's certificate has "Non-repudiation" value in its "Key usage" field (see also figure 1),
- the signature has OCSP confirmation.

Certificates which can be used for qualified electronic signature creation are stored on physical identity tokens: ID-card, Digi-ID, Mobile-ID or cryptostick.



A certificate with "Non-Repudiation" value in its "Key Usage" field

Digital stamp

Digital stamps are same as qualified electronic signatures, except of the certificate type that has been used for creating the signature. Digital stamps have the following characteristics:

- the certificate for signing is a "digital stamp" certificate issued to an organization (i.e. legal entity),
- the certificate has "Non-repudiation" value in its "Key usage" field (see also figure above),
- the signature has OCSP confirmation.

Digital stamp certificates are issued by AS Sertifitseerimiskeskus (SK) (see also https://www.sk.ee/en/services/Digital-stamp/), the certificates are stored on cryptosticks.

Technical signature

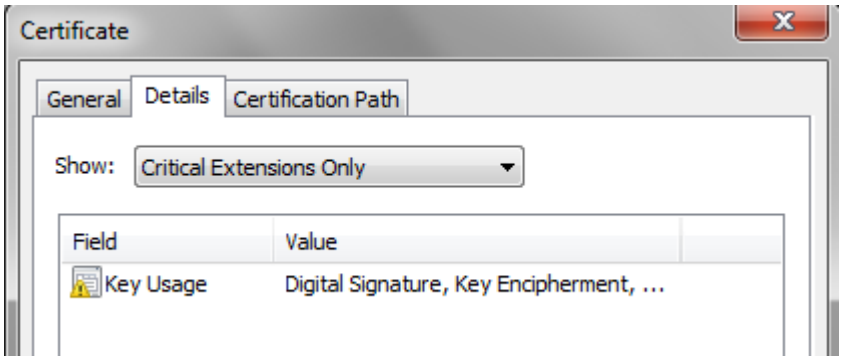
Technical signatures are signatures which have at least one of the following characteristics:

- the signer's certificate does not have "Non-repudiation" value in its "Key usage" field (see also figure below),
- OCSP confirmation has not been added to the signature.

Technical signatures can be created both by private persons and organizations.

Note: verification of a technical signature is expected to produce specific error message(s) depending on the signature's properties:

- technical signature with no OCSP confirmation is expected to produce error message "Signature has no OCSP confirmation!".
- technical signature which has been created with a certificate that doesn't have "Non-repudiation" value in its "Key usage" field is expected to produce error message "Signer's cert does not have non-repudiation bit set!".



A certificate with "Key Encipherment" value in its "Key Usage" field

Note that in the meaning of Estonian legislation (see [6]), qualified electronic signatures and digital stamps are equivalent to handwritten signatures whereas technical signatures are not.