Contents

Description .................................................................................. 4

Introduction..........................................................................................4
Glossary...............................................................................................5
Reference .............................................................................................6
System Requirements ...........................................................................6
Related Requirements ..........................................................................7

Authorization, Evidence and Validation ................................. 8

Document Analysis .............................................................................8
Document Registration .........................................................................8
Registered Document Update ...............................................................10
Document Status Information ..............................................................10
Document Unregistration .................................................................10
Documents to Refresh .........................................................................10
Direct Document Signing ..................................................................10
Attaching a Time Stamp Directly to the Document .........................10

Conversion and other services ................................................. 11

Documents conversion to PDF or PDF/A ...........................................11
Documents conversion to PDF or PDF/A (Print2PDF) .........................11
Conversion webpage to PDF and PDF/A file ....................................11
File conversion from URL .................................................................11
PDF to PDF/A conversion .................................................................11
PDF/A Compliance Check .................................................................12
Getting Conversion Profiles ...............................................................12
Getting a Timestamp ........................................................................12
PDF Text Export with OCR Option ....................................................12
Reading Barcodes from PDF Files ....................................................12
Generating Barcodes into PDF or Images ..........................................12
Generating Payment Orders in QR Codes into PDF or Images ..............12
Adding an Attachment to a PDF File ........................................................................................................... 12
Compression PDF file................................................................................................................................. 13
Long-Term Docs Current Version Information ............................................................................................. 13

Service Test Methods .............................................................. 14

Document Conversion Test ......................................................................................................................... 14
OCR Engine Test ......................................................................................................................................... 14
PDF/A Format Check Test ............................................................................................................................ 14
Conversion Profile Availability Test ............................................................................................................ 14
Time Stamp Service Test .............................................................................................................................. 14
Long-Term Docs Web Service Test ............................................................................................................ 14

Testing, TRIAL version .......................................................... 15
Description

Introduction

Software602 Long-Term Docs is a completely server-based software solution for creating and archiving PDF documents that comply with international standards and requirement specifications for long-term storage of documents' electronic originals. It provides an interface for handling digital signatures in not just PDF documents but also Microsoft Office documents, structured XML data and general CMS data. This software allows users to digitally sign documents, provide them with qualified time stamps and store them in the long term in compliance with CAdES, PAdES and XAdES standards.

The concept and quality of this technical solution complies with the requirement for creating a trust service in accordance with Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. Especially in regard to the service for validating qualified electronic signatures and the service for the preservation of qualified electronic signatures.

To run this solution, an active user account at LongTermDocs.eu is needed to provide qualified time stamp services, verification services for checking electronic certificate validity and metadata registration for the individual documents and files to be archived.

Long-Term Validity (LTV) services and qualified time stamp (TSA) services are provided by Secustamp.eu.

Thanks to these services and options of the Software602 Long-Term Docs application, it is possible to provide creation or conversion of PDF documents in the archival format, PDF/A, and also provide their adequate security by a digital signature in PAdES format to ensure their long-term validity and provability.

The Long-Term Docs SDK allows integration of functions and operations on documents using the following interfaces:

- Web Service Methods
- .NET libraries AdES_NET.dll and Software602.Converter.dll

.NET libraries are included in the Engine folder after installation of SDK. .NET method interface is provided with comments as an .xml documentation. Most of the .NET Assembly methods use the same interface as web service methods described below. Therefore it is easy to integrate into other information systems or web applications.
Glossary

PAdES - digitally signed PDF documents in compliance with ISO-32000-1 standard or standards of the PAdES family - PAdES Basic, PAdES-BES, PAdES-EPES and PAdES-LTV.

CMS, PKCS7, CAdES - digitally signed (internally or externally) general data in CMS/PKCS7/CAdES format. It can be, for example, signed e-mail communication, audio or video recordings, etc. One of the examples of internally signed data compliant with CAdES are also DMIS Data Messages.


PDF - file format for storing document independently from the SW and HW used to acquire them. Follows the ISO 32000-1:2008 standard.

PDF/A - official archival version of the PDF file format. This is a narrowing of the PDF definition so that files saved as PDF/A could be opened without information loss by all future version of software tools. Defined by ISO 19005:1-2008 and ISO 19005-2:2011 standards.

Document - signed PDF document or other signed data.

ISDOC - Information System Document - electronic invoicing format in the Czech Republic.

DMIS - Data Message Information System.

OID - Object Identifier.
**CRL** - Certificate Revocation List issued by the certification authority, the certificate is revoked eg. due to lost or theft of private key

**Grace period** - time during which sign in the document is too fresh for verification towards the CRL list. It is usually 24 hours. After this time, it is possible to clearly evaluate validity of electronic signatures.

**Refresh** - refreshing a document means a validation of previous signature certificates, download of CRL lists and other metadata necessary for later validation of these signature certificates, attachment of all this information to the document and attachment of another qualified time stamp.

**CBA** - Czech Banking Association

**Reference**

ETSI TS 103 171 v2.2.1: “Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile”

ETSI TS 103 173 v2.2.1: “Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile”

ETSI TS 103 172 v2.2.2: “Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile”

ETSI TS 103 174 v2.2.1: “Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile”

ETSI TS 102 778-1: “Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES”

ETSI TS 102 778-2: “Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1”

ETSI TS 102 778-3: “Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles”

ETSI TS 102 778-4: “Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES LTV Profile”


IETF RFC 3161: “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)”

**System Requirements**

64-bit MS Windows Server 2008 or Windows Server 2012 (R2) or Windows Server 2016 operating system

Two or multicore processor

Including WebServer with ASP.NET and .NET Framework 3.5 and also 4.0 or higher

To ensure high throughput it is advisable to provide adequate memory size and communication interface speed.

For proper functioning Long-Term Docs SDK is needed that the server (or firewall, proxy, etc.) does not block communication with addresses: https://www.secustamp.com/ and https://wsc.secustamp.com/

You also need to have a permit addresses to check server certificate revocation. Currently these are certificates issued by thawte SSL CA - G2:

tj.symcd.com:80
Related Requirements

Active user account at LongTermDocs.eu from which the user draws conversion, evidence and long-term validation services.

Figure 2: An overview of document operations in the long-term archiving process
Authorization, Evidence and Validation

A set of web service methods for documents authorization, evidence and ensuring long-term document validation. Provides storage of document's AdES metadata at a Long-Term Docs registration server, which allows to quickly find out which documents need to be refreshed before a given date or to check the state of a specific document.

Document Analysis

Checks the status of a document and its format (includes certificate validation of digital signatures, marks and time stamps, their check against the CRL list, document hash inviolation check). Digital signature format check. If the analyzed document passes the check, it can be accepted for long-term archiving and therefore its digital continuity will be maintained.

First it must be verified whether the registration requirements to the Long-Term Docs Server are fulfilled for the document. This is provided by the ltvAnalyze method, whose output to the users is a block of information about the document and its certificates. Its result will determine the circumstances under which the document's long-term validity operation can be run.

Document Registration

The document is registered to the Long-Term Docs Server, assigned a unique ID and AdES document metadata. The document is provided with a proper archival time stamp. After the registration, the document's signature structure complies with PAdES, CAdES or XAdES specification.

A document can enter the registration - ltvRegister method - if it contains at least one time stamp or one signature and time stamp and if the so-called grace period have passed so that it is possible to verify that the signature certificate has not been revoked, that it has been issued by a trusted authority, and this verification is successful. If the document signatures are found valid, the registration process provides revocation data acquired on the previous document analysis and attaches time stamp to the document. Document's metadata registration to the Long-Term Docs Server follows. Upon registration, the document receives a unique ID and the user can select sorting data.

It follows from the above information that whenever document registration is requested, the document's integrity check and signature validation - ltvAnalyze method - is run first. If the document passes, its hash is calculated and time stamp for the hash requested. The hash calculation algorithm is recorded along with the hash. The time stamp request and the request response are compliant with RFC 3161 specification. Once the time stamp is received, the document is signed and this time stamp attached to it in compliance with PAdES ETSI TS 103171 v.2.1.1 specification

http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf

CAdES ETSI TS 103173 v.2.2.1

http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf

XAdES ETSI TS 103171 v.2.1.1

http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf
The response is Docld, a registration number of the registered document. Software602 Long-Term Docs creates the document in compliance with LTV requirements for long-term document validity.
Registered Document Update

Update of a previously registered document before the expiry of the last archival time stamp. The document is provided with a new archival time stamp.

Upon document update, the document's signature certificates are always checked by the `ltvAnalyze` method to ensure legitimacy of the document's further maintenance.

Document Status Information

The `ltvGetInfo` function returns information on the entered document ID or on a group of documents matching the entered filter. The response structure defines the contents of the Long-Term Docs registration server output.

The query can be related to a specific ID or a specific document expiry date.

Document Unregistration

Every document can be removed from the long-term archiving process and its information removed using the `ltvUnregister` method.

Documents to Refresh

Used to find out which documents need a refresh before a given date. The result of the `ltvGetForUpdate` method is a list of document IDs. The list can be narrowed down to just a specific number of documents, they are ordered chronologically. It is also possible to narrow the selection down to a selected archival folder - to set a sorting piece of data for selection filtering.

Direct Document Signing

If needed, a document can be signed by a digital signature with no connection to archiving. The document can be signed by the `ltvSign` function. Path to the certificate in PFX/PEM format and its password can be set in the Web.config file located in the WebService folder.

Attaching a Time Stamp Directly to the Document

If needed, a digital time stamp with no connection to archiving can be attached to the document. The time stamp can be attached to the document using the `ltvTimestamp` function.
Conversion and other services


Documents conversion to PDF or PDF/A

The web service allows for conversions of any document on the server to the PDF or PDF/A format, depending on the defined requirements in the requirement’s configuration structure. The following parameters can be set: conformance level pursuant to the given PDF/A specification, document signature by an electronic sign, furnishing documents with a qualified time stamp and/or watermark and other parameters.

The server has to have an application that can read the format of the document that is supposed to be converted - for example, Microsoft Word for documents of the *.docx format. More information about the application requirements and settings for the conversion service can be found in the Long-Term Docs Admin Guide.

Documents conversion to PDF or PDF/A (Print2PDF)

Web service provides a server-side conversion of any document into PDF or PDF/A according to the selected conversion profile. It is possible to set the level of compliance with the PDF/A specification, sign the document with a digital mark, attach a qualified time stamp to the document, provide it with a watermark and other settings within each profile.

Webpage conversion to PDF and PDF/A file

Web service allows convert any webpage to the standard PDF and also to the archiving PDF/A format. To create an archive PDF/A document with the downloaded referenced files (pdf, office, etc.) and the source files (SSL certificate, images, etc.) from the webpage, it is possible to use parameters DownloadReferencedFiles and DoArchive.

File conversion from URL

This is an internal method for communicating with the filing service. The web service allows conversion of any document from entered URL on the server to the PDF or PDF/A format, depending on the defined requirements in the requirement’s configuration structure and the resulting file upload to another server. For the resulting file the following parameters can be set: conformity level pursuant to the given PDF/A specification, document signature by an electronic sign, furnishing documents with a qualified time stamp and/or watermark and other parameters.

PDF to PDF/A conversion

The PDF/A format is defined at several conformance levels. This level can be set and will be converted to the PDF/A format, provided the document does not include errors and discrepancies, which cannot be corrected when checked against the selected conformance level.
PDF/A Compliance Check

The PDF/A format is defined in several compliance levels. The level can be set and the document analyzed in regard to the selected level.

Getting Protocol of verification signatures from the document

Web service allows to get a verification signature report using method call `GetSignatureReport`. The verification signature report contains the overview of all digital signatures, the certificate issuers, their validity, verifiability and other information from the source document.

Getting Conversion Profiles

Web service can work with premade conversion profiles that contain conversion settings. Find out which ones are currently available using the `GetProfileList` method.

Getting a Timestamp

Web service allows to acquire a timestamp from the SecuStamp.eu server using the `GetTimeStamp` method. The method is paired with the SecuStamp.eu server on a username or a certificate basis.

PDF Text Export with OCR Option

The web service allows to export text from any document in PDF format and also to scan text from images using OCR technology.

Reading Barcodes from PDF Files

The web service can read the contents of QR, PDF417, DataMatrix a 1D barcodes. The `ReadBarcodeToString` method returns only the data item from the barcode, the `ReadBarcode` method also returns its location and, in the case of 1D code, also the subtype and checksum.

Generating Barcodes into PDF or Images

The web service can generate 1D and 2D barcodes into images and PDF files. QR, PDF417, DataMatrix and a range of 1D codes are supported. The input parameters are the required code type, data, size, location on the page and page number. In case of specific barcodes other parameters can be set, such as encoding or error correction.

Generating Payment Orders in QR Codes into PDF or Images

The web service can generate QR barcodes containing data for payment orders into images and PDF files. These QR codes comply with the CBA standard for data sharing domestic payments in Czech republic. The web service takes the payment data as the method’s input data, uses it to generate the QR code and provides the correct formatting.

Adding an Attachment to a PDF File

The web service allows to add any attachment to the input PDF file. The attachment’s format, name and type must be specified.
Compression PDF file

Web service method for compressing PDF file. Compresses data within the PDF document, as well as embedded images and their format and resolution.

Long-Term Docs Current Version Information

Web service can provide information concerning installed version of the Long-Term Docs web service and verify the licence certificate validity.
Service Test Methods

Marked by prefix “test”, they are used by the administrator when installing and testing the service functionality. Their advantage is no need to set input parameters and they return a simple string.

If the service runs in a web browser on the computer where the service is installed, the Call button is available. This generates the corresponding test service method and the response is displayed.

Document Conversion Test

This test method checks the functionality of the conversion service and provides information on conversion options for specific file formats. It converts test files from the TestFiles folder and displays conversion results.

Product Licence Test

Checks the correct licence of the installed product.

OCR Engine Test

Checks whether your Long-Term Docs version contains a functioning version of OCR Engine. The check is run on the Convert.htm.htm file in Long-Term Docs/TestFiles folder. The test file is a part of the installation.

PDF/A Format Check Test

Checks the functionality of PDF/A operations.

Conversion Profile Availability Test

Checks the availability of conversion profiles.

Time Stamp Service Test

Checks the functionality of the service that provides communication with the server issuing time stamps in compliance with RFC 3161 protocol.

Long-Term Docs Web Service Test

Checks the functionality of communication with the web service.
Testing, TRIAL version

The web service methods described here can be integrated into existing information systems or web applications. They can be used as a basis for an electronic archive for a records management service using conversion functions.

TRIAL version for direct implementation testing including the complete documentation is available here:

TRIAL product version