

Validation Service Policy

SecuSign Validation

Change history

Date	Release	Status	Author
1. 11. 2016	V 0.1	Internal Draft	Martin Vondrouš
29. 11. 2016	V 0.2	Internal Draft	Martin Vondrouš
30. 11. 2016	V 0.3	Internal Candidate	Martin Vondrouš
15. 12. 2016	V 1.0	Release	Martin Vondrouš
17. 5. 2017	V 1.1	Release (added abbreviations)	Martin Vondrouš
20.1.2018	V 1.2	Release (GDPR adjustment, update)	Martin Vondrouš
30.5.2021	V 1.3	Logo change	Martin Vondrouš
10.4.2023	V 1.4	Update (DIA, qual. seal for a clause, audit logs, abbreviations)	Tomáš Línek



Contents

1 Introduction 9

1.1 Overview 9

1.2 Name and purpose of the document 9

1.3 Participating subjects 9

1.3.1 PostSignum 9

1.3.2 Microsoft Azure 10

1.3.3 Relying parties 10

1.4 Use of the Service 10

1.4.1 Permissible use of the Service 10

1.4.1.1 Interface 10

1.4.2 Limitations on using the Service 10

1.5 Policy management 11

1.5.1 Organization managing the TS 11

1.5.2 Contact for the Service Administrator 11

1.6 Terms and abbreviations 11

2 Responsibility for the publishing and storage of information and documentation ... 15

2.1 Storage of information and documentation 15

2.2 Publishing information and documentation 15

2.3 The periodicity of publishing information 15

2.4 Managing access to individual types of storage 16

3 Identification and authentication 17

3.1 User creation 17

3.1.1 602 ID 17

3.1.2 Service user registration 17

3.2 User verification 17

3.3 Termination of the use of the service 17

3.4 Canceling a user account 18

4 Validation service 19

4.1 Validated certificates 19

4.1.1 List of Trusted List 19

4.1.2 Trusted Lists 19

4.2 Validated signature formats 20

4.2.1 PAdES 20

4.2.2 XAdES 20

4.2.3 CAdES 20

4.2.4 ASiC 20

4.3 Validation process 20

4.3.1 Validation process selection 21

4.3.2 Validation process output 21

4.3.2.1 Valid 22

4.3.2.2 Invalid 22

4.3.2.3 Indeterminate 23

4.3.2.4 Validation schema 24

4.3.3 Grace Period 25

4.3.4 CRL and OCSP 25

4.3.5 Boundary conditions and transitional period 26

4.3.5.1 Loss of status of qualified service provider 26

4.3.5.2 Electronic time stamps 26

4.3.5.3 Recognized electronic signature and Qualified electronic signature 27

4.3.5.4 RFC 5280 27

4.4 Validation result 27

4.4.1 Structured XML data 27

4.4.2 PDF document 27

4.4.3 Validation clause 27

4.5 Service availability 28

4.5.1 Validation Service 28
4.5.2 Qualified service 28
5 Management, operational and physical security 29
5.1 Physical security 29
5.1.1 Location and construction 29
5.1.2 Physical access 29
5.1.3 Electricity and cooling 29
5.1.4 Water impact 29
5.1.5 Fire protection 29
5.1.6 Media storage 29
5.1.7 Backups 30
5.2 Process security 30
5.2.1 Trusted roles 30
5.2.2 Number of persons required to ensure specific tasks 30
5.2.3 Identification and authentication for each role 30
5.2.4 Roles requiring separation of duties 30
5.3 Personnel safety 31
5.3.1 Requirements on qualifications, experience and clean record 31
5.3.2 Evaluation of a person's reliability 31
5.3.3 Requirements on preparation for fulfilling the role, entry training 31
5.3.4 Requirements and periodicity of trainings 31
5.3.5 Periodicity and rotation sequence of employees between different roles 32
5.3.6 Sanctions for employees' unauthorized activities 32
5.3.7 Requirements for independent contractors (suppliers) 32
5.3.8 Documentation provided to employees 32
5.4 Audit logs 32
5.4.1 Types of recorded events 32
5.4.2 Periodicity of processing the logs 33

5.4.3 The storing period of audit logs 33
5.4.4 Protection of audit logs 33
5.4.5 Audit log backup procedures 33
5.4.6 The system for collecting audit logs 34
5.4.7 Procedure for announcing an event to the subject who caused it 34
5.5 Storing information and documentation 34
5.5.1 Types of information and documentation that are stored 34
5.5.2 Storage period for information and documentation 34
5.5.3 Protection of storage of information and documentation 34
5.5.4 Backup procedures for the stored information and documentation 35
5.5.5 Requirements on using time stamps when storing information and documentation 35
5.5.6 Procedures for acquiring and validating stored information and documentation 35
5.6 Restoration after an accident 35
5.6.1 Procedure in the case of an incident 35
5.6.2 Damage to computing equipment, software or data 35
5.6.3 The ability to restore operation after an incident 36
5.7 Terminating the Service 36
6 Technical security 37
6.1 Computer security 37
6.1.1 Specific technical requirements on computer security 37
6.1.2 Evaluation of computer security 37
6.2 Lifecycle security 37
6.2.1 Management of system development 37
6.2.2 Security management checks 37
6.2.3 Lifecycle security management 38
6.3 Network security 38
6.4 Time stamps 38

7 Compliance assessment and other assessments 39
7.1 Assessment periodicity or conditions 39
7.2 Assessor's identity and qualifications 39
7.3 Relation of the assessor to the subject being assessed 39
7.4 Procedure for any deficiencies found 39
7.5 Assessment result notifications 40
8 Other commercial and legal questions 41
8.1 Fees 41
8.2 Confidentiality of commercial information 41
8.2.1 List of confidential information 41
8.2.2 Information outside the scope of confidential information 41
8.2.3 Responsibility for the protection of confidential information 41
8.3 Personal data protection 42
8.4 Intellectual property rights 42
8.5 Disclaimer 42
8.6 Limitation of liability 42
8.7 Liability for damage, compensation for damage 43
8.7.1 Insurance 43
8.7.2 Assets 43
8.8 Validity period, termination of validity 43
8.8.1 Validity period 43
8.8.2 Termination of validity 43
8.9 Communication between the parties involved 44
8.9.1 Incidents 44
8.10 Changes 44
8.10.1 Change procedure 44
8.10.2 Change announcement procedure 44
8.10.3 Circumstances that require a change in the Validation process 44

8.10.4 Infrastructure changes 44

8.11 Dispute resolution 45

8.12 Governing law 45

8.13 Compliance with legislation 45

1 Introduction

1.1 Overview

The Qualified Validation Service (hereinafter referred to as "Qualified Service") is a service created and operated by Software602 a.s. (hereinafter referred to as "Software602") to validate qualified and advanced electronic signatures or stamps and electronic time stamps in compliance with ETSI specifications. Software602 is a qualified trust service provider (hereinafter also referred to as "QTSP") according to eIDAS and the Qualified Service is included in the trusted list of EU qualified service providers (LoTL – List of Trusted Lists) and the Trusted List of the Czech Republic. The Service is provided as a Qualified Trust Service (hereinafter referred to as "Service").

The subject of this document is to define the policy (hereinafter referred to as "VP") for providing the Service. VP describes the conditions and required methods that must be applied in order to maintain the accepted security standards of QTSP. The document also includes specification of the responsibility scope for the parties involved.

Maintaining the methods and conditions specified in this VP ensures that the relying parties receive the result of the validation method in an automatic manner that is reliable, effective and provided with an advanced electronic signature or advanced electronic seal of the qualified validation service provider.

An important notice to Service users: Before using the Service for the first time, the user is obliged to acquaint themselves with this VP verifiably and in full.

1.2 Name and purpose of the document

Document name: Validation Service Policy.

VP is compliant with documents listed in chapter 8.13.

1.3 Participating subjects

1.3.1 PostSignum

PostSignum is a trust service provider who provides electronic time stamps for the Validation Service in compliance with requirements of the legislative framework set up by the Czech legislative environment and EU requirements. This provider's policy of issuing time stamps is published on their website, www.postsignum.cz.

1.3.2 Microsoft Azure

Microsoft Azure provides infrastructure for the Service's runtime environment and guarantees a secure environment for processing data and storing it in compliance with requirements on the protection of personal data and location where the data is stored.

1.3.3 Relying parties

The relying parties are natural or legal persons who want to verify the signature of an electronic document or data based on this VP.

1.4 Use of the Service

1.4.1 Permissible use of the Service

The service may only be used by users who have acquainted themselves with this VP. User of the Service accepts its use based on the conditions of this VP and in accordance with the guaranteed use of the Service.

The Service can only be accessed using defined interfaces and applications published by the validation service provider.

1.4.1.1 Interface

User of the Service is obligated to protect the Service interface from unauthorized use and provide appropriate security when using the Services. This applies to any interface used to use the Service (hereinafter referred to as the “Interface”).

This Interface means in particular the web application for using the Service, integration web services, any application or integration interfaces supplied exclusively by the Service provider or an integrator specified by the Service provider.

1.4.2 Limitations on using the Service

Use of the Service not defined and permitted by this VP is considered unauthorized. The provider of the Service is not liable for unauthorized use of the Service, not even in the case of the Qualified Service. If the Interface's security or integrity is violated, the provider is not liable in any way for any damage whatsoever caused by use of this unsecured, counterfeit or any way breached Interface.

1.5 Policy management

1.5.1 Organization managing the TS

Software602, a.s., technical department, Hornokrčská 15, Praha 4, Czech Republic

1.5.2 Contact for the Service Administrator

Data Box ID: 7dcsfzg

Director of the Technical Department
Software602 a.s.
Hornokrčská 15
Praha 4

1.6 Terms and abbreviations

Acronym	Full meaning	Explanation
AdES	Advanced Electronic Signature	An advanced electronic signature that meets the requirements of Article 26 of Regulation (EU) 90/2014.
CA	Certification Authority	Provider of electronic certificate services for electronic signatures/seals/website certificates. In a narrow sense it means a component that owns a private key for signing the end certificates or certificates subordinate to the CA and issues CRLs.
Certificate		Data structure containing a public key and the details of the key owner, key issuer, permitted manner of use and other relevant information specified by the corresponding VP.
CP	Certification policy	Document that defines the parameters of a certificate issued by the CA, specifies the manner of use of the certificate and defines the certificate's life cycle. It is also a certification policy for issuing the certificates for signatures, seals or stamps from the QTSP.
CRL	Certificate Revocation List	The list of invalidated or suspended certificates whose period of validity has not expired yet, according to the RFC 5280.
ČP	Evaluation time	The time point as of which the signature is validated. It is either the current time or the time specified by the user in the validation request.
Certificate holder	Certificate holder	Natural or legal person who has the exclusive right to use the private key connected to the certificate in question.
DTBS	Data To Be Signed	The data to be signed.
Trusted role		Trusted roles on which the security of the operation depends.

Acronym	Full meaning	Explanation
eIDAS		Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
EP	Electronic signature	Data in electronic form attached to a data message that is used to validate the data message's integrity.
ETSI	European Telecommunications Standards Institute	
EU	European Union	
Grace Period		Safety period in which the Certification Authority is obliged to publish a revoked certificate on the certificate revocation list – CRL.
Data Box ID		Unique ID of a data box for a user of the Data Message Information System
DMIS	Data Message Information System	The Data Message Information System is an information system of the public administration which contains information on data boxes, their users, accesses to the box and other events related to their operation, etc.
ISO	International Organization for Standardization	
ITU	International Telecommunication Union	
Qualified service	Qualified trust service	A qualified trust service provided by a qualified trust service provider to validate qualified electronic signatures.
LoTL	List of Trusted Lists	EU: List published pursuant to Article 2 section 4 of the Commission Decision 2009/767/EC of 16 October 2009, setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market, as amended by the Commission Decision 2010/425/EU and Commission Implementing Decision 2013/662/EU, which contains information announced by the member states pursuant to Article 2 section 3 of the Commission Decision 2009/767/EC.
LT	Long-Term	
LTA	Long Term Archive	Level of extended electronic signature for long-term archiving.
LTV	Long-Term Validation	Level of extended electronic signature for long-term validation.
OCSP	Online Certificate Status Protocol	Protocol for on-line certificate validation based on RFC 6950.
OID	Object Identifier	Numeric identification of an object within unified object classification based on ISO/ITU.
PKI	Public Key Infrastructure	Infrastructures for administration and distribution of public keys in asymmetrical cryptography.

Acronym	Full meaning	Explanation
POE	Proof Of Existence	Unambiguous information on time, proving the existence of the data being validated at the time as of which the validation is performed.
Private key		Data structure for creating electronic signatures/seals or encrypting data messages.
RT	Request tracker	Reporting system
QTS	Qualified Trust Service	Qualified trust service
QTSP	Qualified Trust Service Provider	Qualified trust service provider.
Register		Aggregate of stored data to provide an overview of performed operations.
Interface	Integration interface for using the Service	Any interface specified by the Service provider for using the Service, in particular the web application for using the Service, integration web services, any application or integration interface supplied exclusively by the Service provider or a provider specified by the Service provider.
SCD	Signature Creation Device	A device for creating electronic signatures.
Validation Service	The service for the validation of electronic signatures	The Validation Service is a service created and operated by Software602 to validate qualified and advanced electronic signatures in compliance with ETSI specifications.
SVA	Signature Validation Application	An application that validates signatures.
TIER III	Datacenter classification in accordance with the Uptime Institute	With this setting, it is possible to perform maintenance without affecting the availability and performance of services on the server. These datacenters will not protect from serious incidents that might take place on various infrastructure components.
TIER IV	Datacenter classification in accordance with the Uptime Institute	The highest level of guarantee. This datacenter category is fully redundant in regard to electrical circuits, cooling and networks. This architecture will withstand the most serious technical incidents without affecting the server's availability.
TL, EU TL	Trusted List	The trusted list under the eIDAS regulation is a continuation of trusted lists under the Commission Decision 2009/767/ES. It contains information which supervisory bodies of the individual states issue so that it is possible to correctly evaluate the type, status and legal effect of trust services in compliance with current legislation.
TS	Trust Service	A service that provides trust.
TSA	Time-Stamping Authority	A provider of electronic time-stamping service.
TSP	Trust Service Provider	A provider of trust service.
Uid	Unique identifier	Assigned or entered unique identifier of a document whose electronic signatures are being processed (preserved) by the Service.
UP	User Policy	Specifies the obligations and responsibilities of certificate users.

Acronym	Full meaning	Explanation
VP	Validation policy	The policy of the service for validating electronic certificates for signatures, seals or stamps.
WS	Web Services	A technology for calling functions remotely in distributed systems based on a protocol for remote calls, SOAP, and a language for describing provided services, WSDL.

2 Responsibility for the publishing and storage of information and documentation

2.1 Storage of information and documentation

Software602 establishes and maintains an internal storage of information and documentation in the form of an internal portal.

2.2 Publishing information and documentation

The service for validating electronic signatures is provided as a commercial public service. The trust service provider is Software602.

Software602 provides this service also as QTSP in the QTS mode. This fact is always clearly announced to the user.

The basic policy of providing the service is described in this document and located at the following address:

http://602.cz/links/QVSpolicy

The basic address, where other public documents are available in printed form:

Technical department of Software602 a.s.
Hornokrčská 15
140 00 Praha 4

Basic addresses where public information is available in electronic form:

http://602.cz, https://602.cz/secusign

2.3 The periodicity of publishing information

Software602 publishes updated documents and current information related to changes in providing the Service by means of the company's website. At least at the following address: https://602.cz/.

Any changes in use of the Service will be announced to clients using the contact details listed by the client.

Any changes in providing the Service, including the intention to cease the activities, will be announced to the supervisory body (Digital and information agency) in compliance with eIDAS, Article 24, section 2, subsection a).

2.4 Managing access to individual types of storage

Access to specific types of storage is specified by Software602's internal regulations. Access with a write permission is assigned to the administrators of the corresponding data. Public data is available to read without limitations. Access management is implemented for documents with limited access.

3 Identification and authentication

This chapter specifies the requirements on identity verification for Service users.

3.1 User creation

3.1.1 602 ID

It is a unique identifier for a user of services provided by QTSP Software602. 602 ID consists of an e-mail address and a password. The details are stored in a database administered exclusively by QTSP Software602 and protection of the users' personal data is ensured. For some services, the user's unique 602 ID is accompanied by another set of data for invoicing and transactions with the user.

3.1.2 Service user registration

A Service user registers at Software602 portals and after agreeing with the service terms the user is granted access to the services. The basic details required for the primary registration are an e-mail address and a password specified by the user. After requesting the registration, a confirmation message is sent to the supplied email address to verify the owner of the email account.

3.2 User verification

User verification when signing in to the use of services through the provider's web portals is performed by basic authentication and verification of the user's identity using their 602 ID. When using the services through the web service interface, applications provided by the provider, or third parties, user verification by a certificate is required. The certificate for using the services and authentication is issued by TSP Software602 by means of an authority it manages, Software602 Root CA.

3.3 Termination of the use of the service

If the user does not comply with the terms of using the Services, the TSP Software602 reserves an exclusive right to terminate supplying the Services in full. On the part of the users, a termination of supplying the Service is possible by sending a written request signed by the user's advanced electronic signature based on a qualified certificate, or a qualified electronic signature, to the provider's data box listed in section 1.5.2.

3.4 Canceling a user account

A user account and 602 ID will be canceled following a written request signed by the user's advanced electronic signature based on a qualified certificate, or by a qualified electronic signature, sent to the service provider's data box specified in section 1.5.2. In the case of a paper document, a document signed by the user's own verified signature will be accepted.

4 Validation service

The Service receives on input a whole document signed in compliance with the standards defined by ETSI, which are referred to by the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC via the Commission Implementing Decision (EU) 2015/1506 of 8 September 2015, laying down specifications relating to formats of recognized electronic signatures and advanced seals to be recognized by public sector bodies pursuant to article 27 section 5 and article 37 section 5 of Regulation (EU) No 910/2014 of the European parliament and the Council on electronic identification and trust services for electronic transactions in the internal market.

The Service's only interface is the Interface supplied and provided by the Provider. Using the Service in another manner than which is defined by the provider is prohibited and is considered to be a breach of the terms of Service.

4.1 Validated certificates

4.1.1 List of Trusted List

The list of addresses for all published TLs of all member states is published by the European Commission in the “TL list” (LoTL - List of Trusted Lists). It is available in a machine-processable form at the following address:
https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml.

The list published pursuant to Article 2 section 4 of the Commission Decision 2009/767/EC of 16 October 2009, setting out measures facilitating the use of procedures by electronic means through the ‘points of single contact’ under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market, as amended by the Commission Decision 2010/425/EU and Commission Implementing Decision 2013/662/EU, which contains information announced by the member states pursuant to Article 2 section 3 of the Commission Decision 2009/767/EC.

The Service regularly checks the LoTLs and also all listed TLs of EU member states. Based on this check, any QTSP changes, additions or removals are recorded in the Service's internal database. Thanks to that, the Service is able to supply verifiably the information on an authority's qualification in time, and that also in retrospect even if the national TLs, local CRLs or individual authority OCSPs are unavailable.

4.1.2 Trusted Lists

The trusted list under the eIDAS regulation is a continuation of trusted lists under the Commission Decision 2009/767/EC. It contains information which supervisory bodies of the individual states issue so that it is possible to correctly assess the type, status and legal effect of trust services in compliance with current legislation.

4.2 Validated signature formats

4.2.1 PAdES

It is a signature used for signing PDF and PDF/A documents. Its technical specification, ETSI TS 103172 v.2.2.2, is available at the following address:
http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf

4.2.2 XAdES

It is a signature used for signing structured documents with data XML structure. Its technical specification, ETSI TS 103171 v.2.1.1, is available at the following address:
http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf

4.2.3 CAdES

It is a signature used for signing general binary data and documents, for which it is not possible to use an inserted signature. Its technical specification, ETSI TS 103173 v.2.2.1, is available at the following address:
http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf

4.2.4 ASiC

It is a signature for a container with an associated signature. Its technical specification, ETSI TS 103174 v.2.2.1, is available at the following address:
http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf

4.3 Validation process

The individual types of signatures allow various levels of validating the electronic signature certificate. Therefore the Service contains various validation processes based on the type of signature and information contained in it.

The validation processes identify qualified and advanced electronic signatures. They confirm the validity of a qualified electronic signature, if it complies with the conditions stipulated in eIDAS, Article 32.

The service does not limit the use of pseudonyms in any way.

Existing validation processes for signature levels defined in Commission Implementing Decision (EU) 2015/1506 of 8 September 2015:

- B – basic,
- T – Signature with a time stamp,
- LT – Signature with a time stamp and validation data,

- LTA –Signature providing long-term validity and integrity of validation data.

Furthermore, the Service identifies and contains validation processes for the following older standards:

ETSI TS 101 733 for the CAdES format recognizing signature levels:
- CAdES-BES – Basic electronic signature
- CAdES-EPES – Electronic signature containing signature policy
- CAdES-T – Signature containing time information
- CAdES-C – Signature containing complete validation data
- CAdES-X1 – Signature containing extended validation data
- CAdES-XL – Signature containing more validation data, which can be useful in case it is not later otherwise available
- CAdES-XL1 – Adds more protection and provides integrity of validation data
- CAdES-LTV – Signature containing extended validation data
- CAdES-A – Signature containing archival validation data

ETSI TS 102 778 for the PAdES format
- PAdES-BES – Basic electronic signature
- PAdES-EPES – Electronic signature containing signature policy
- PAdES BES/EPES with a time stamp

ETSI TS 101 903 for the XAdES format
- XAdES-BES – Basic electronic signature
- XAdES-EPES – Electronic signature containing signature policy
- XAdES-T – Electronic signature containing a signature time stamp
- XAdES-C – Electronic signature containing complete revocation and certification data
- XAdES-X 1 and 2 – containing more validation data
- XAdES-XL – Signature containing extended validation data
- XAdES-A – Electronic signature containing an archival time stamp

The validation process itself takes place in compliance with the requirements of ETSI EN 319 102-1 and for the individual formats also in compliance with ETSI TS 103 172 and ETSI EN 319 142 for PAdES, ETSI TS 103 171 and ETSI EN 319 132 for XAdES, ETSI TS 103 173 and ETSI EN 319 122 for CAdES, ETSI TS 103 174 and ETSI EN 319 162 for ASiC.

4.3.1 Validation process selection

The QTSP provides smart analysis of the data to be validated and of the signature format and, based on information available in the electronic signature, the corresponding level of validation process is selected.

4.3.2 Validation process output

The QTSP provides validation process output in the format of structured XML data for integration into third-party applications and also as HTML output and an XML or PDF document with human-readable output of the validation process result.

The XML and PDF output is provided with a qualified electronic seal of the service provider based on a qualified electronic seal certificate.

If the document's electronic signature is violated, the validation process is suspended, the electronic signature's attribute validation does not continue and the validation ends with the result of signature violation error.

The validation process output recognizes several statuses. The validation process depends on the precise Evaluation time as of which the validation takes place. If the Evaluation time is specified by the user, the Service user is responsible for such detail and therefore also for interpreting the validation result, which is valid as of the specified Evaluation time.

4.3.2.1 Valid

The signature was successfully validated and is considered valid at the validation time.

4.3.2.2 Invalid

The signature was validated as of the validation date and as of this date it is verifiably invalid. Furthermore, details informing about the reason for invalidity are attached:

HASH_FAILURE
The hash of signed data, calculated during validation, does not match the hash created from the data when it was signed and stored in the signature.

SIG_CRYPTO_FAILURE
The signature value could not be successfully validated using the signing person's signature's public key.

REVOKED
The signature certificate had been revoked before the time of signing

EXPIRED
The signature certificate has already expired

FORMAT_FAILURE
The signature was not recognized. Does not meet the requirements on the signature type

SIG_CONSTRAINTS_FAILURE
The signature constraints are not met (for example some signed attributes are missing, incorrect policy, etc.)

CHAIN_CONSTRAINTS_FAILURE
An error occurred when creating the certificate chain

INVALID_NOT_YET_VALID
The signature certificate was not valid yet at the time of validation

4.3.2.3 Indeterminate

The signature was validated as of the validation date and as of this date it is not possible to unambiguously determine its validity or invalidity. The validation result is not verifiably invalid, but it is necessary to pay attention to the additional details and, if need be, repeat the validation process. The individual sub-statuses of the Indeterminate validation result are described below.

TRY_LATER
The information available is not sufficient to validate the signature. Validation might be possible if revocation information is added later. Validation might proceed successfully later.

NO_POE
No relevant POE is available for the signature certificate or CA certificate

UNKNOWN_SIGNING_TIME
The signature is not invalid, but the time of signing is not known

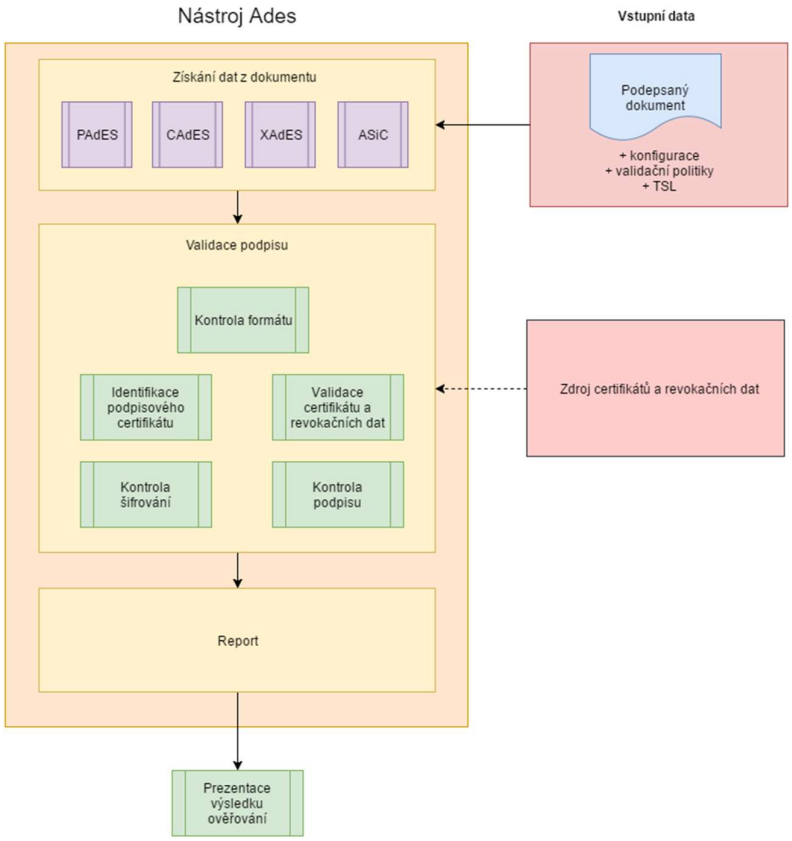
NO_SIGNER_CERTIFICATE_FOUND
No signature certificate has been found in the structure of the signature

NO_CERTIFICATE_CHAIN_FOUND
A valid path to certificate could not be created from the signature certificate (for example unknown certification authority, missing revocation data, unknown CRL distribution point, etc.)

SIGNED_DATA_NOT_FOUND
Signed data could not be acquired

GENERAL_ERROR
general error

4.3.2.4 Validation schema



The validation schema provides process control and verification of all the individual points, whether:

- the certificate, on which the signature is based, was at the moment of signing a qualified electronic signature certificate in compliance with annex I of Regulation (EU) No. 910/2014 – eIDAS;
- the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;
- the signature validation data corresponds to the data provided to the relying party;
- the unique set of data representing the signatory in the certificate is correctly provided to the relying party;
- the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;
- the electronic signature was created by a qualified electronic signature creation device;
- integrity of the signed data has not been compromised.

Qualified certificates for electronic signatures, for electronic seals may only be issued by a Qualified provider of such service. Checking the properties of the certificate and its issuer on

the corresponding TLs provides compliance with the requirements of articles 28 and 32 of the eIDAS Regulation.

4.3.3 Grace Period

The validation process takes account of article 24, section 3 of the eIDAS Regulation: “If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request.”

A qualified certification service provider issues revocation information using an OCSP channel or using CRL. This information is used to validate electronic signature certificates.

If information on certificate revocation is acquired from an available OCSP channel, the validation process provides the validation result immediately.

If revocation information is required from CRL, and the CRL list is issued by a qualified certification service provider after the decisive moment, the overall validity of an electronic signature/seal/stamp is determined based on this information.

If this information is not available within 24 hours in the OCSP or in a CRL issued during the 24-hour grace period, the validation process result is still INDETERMINATE_TRY_LATER.

If the document is found invalid during the grace period, it is not necessary to wait for another validation. If the validation result is indeterminate, it is advisable to consider the arguments and partial information presented for each certificate or, in order to obtain an unambiguous result, to wait for validation result after the grace period.

4.3.4 CRL and OCSP

When checking for revocation, the service supports the OCSP protocol and also uses CRL distribution points. Primarily the OCSP is used; if the interface is not available or does not provide relevant replies, a CRL distribution point or the Service's own database is used.

The service automatically periodically checks newly issued CRLs of known authorities. This database of downloaded CRLs is archived and can be used when requested to validate a certificate as of a time that is not available at the QTSP CRL interface anymore.

The check period interval is set to 60 minutes.

These CRLs are used for validation of electronic certificates for signatures, seals, time stamps.

4.3.5 Boundary conditions and transitional period

4.3.5.1 Loss of status of qualified service provider

If the certificate was issued at a time when the certification authority was unambiguously a Qualified trust service provider and a signature based on this certificate was also created at such time, then the electronic signature based on this certificate is considered qualified (or advanced based on a qualified certificate), as long as the other requirements stipulated by the eIDAS Regulation and current legislation are met.

In other cases it is not possible to unambiguously determine whether the signature being validated is qualified, or advanced and based on a qualified certificate.

During the transitional period,*) existing qualified authorities providing qualified electronic certificate services based on previously valid legislations had the status of a Qualified trust service provider for issuing electronic signature certificates. If such QTSP lost its status or did not restore it after the end of the transitional period (July 1, 2017), the validation service is performed strictly as set by the above paragraphs.

*) Transitional period is the transitional period under the eIDAS Regulation, when the certification service providers were given time until July 1, 2017 to reacquire the QTSP status for issuing electronic signature certificates. See Article 51, eIDAS Regulation.

Another transitional period is set in the Czech legislation in the section 19 of Act no. 297/2017 on trust services. This period lasts until 19.9.2018. It specifies the option of using electronic time stamps, recognized electronic signatures and seals instead of qualified ones.

4.3.5.2 Electronic time stamps

For certificates issued during the transitional period *) the service trusts the time information on electronic time stamps whose certificate or root certificate is issued by a qualified certification service provider. Several additional conditions must be met at the same time:

- The certificate's extKeyUsage (2.5.29.37) states “timestamping” (1.3.6.1.5.5.7.3.8 9).
- The TL states ServiceTypeIdentifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC
- The ServiceStatus in the TL is listed as “granted”

When checking for certificate revocation, the conditions listed above in this chapter must be met. The certificate revocation check is primarily based on information received from the OCSP responder's address. If the OCSP function is not available, information from the CRL list available to SecuSign is used instead. The CRL list must meet the validation schema conditions, otherwise a query is sent to the CRL distribution point listed in the certificate. To check for revocation, a currently available one is used.

Information on the query, operation time, distribution list address and CRL number is recorded in the transaction log.

4.3.5.3 Recognized electronic signature and Qualified electronic signature

The legislative framework of the Czech Republic introduces the status of a Recognized electronic signature. For this type of signature, the service clearly identifies the type of this signature in the validation result and the Service provider accepts the same obligations for the validation result as for the Qualified electronic signature.

For the Recognized electronic seal, the Service clearly identifies the type of this seal in the validation result and the Service provider accepts the same obligations for the validation result as for the Qualified electronic seal.

4.3.5.4 RFC 5280

When validating the revocation of a certificate, compliance of the certification service provider with RFC 5280 is assumed. If this standard is not observed by the Certification service provider (QTSP), correct evaluation of signature certificate's validity and revocation cannot be guaranteed.

4.4 Validation result

4.4.1 Structured XML data

For an integration of the Service, structured validation result is available in XML format containing information on the validation result of electronic signature certificates used to sign the data being validated, including the overall validation status. For documents (PDF) whose nature allows changing the document's data outside their signed part, the data includes information about changes in the document performed after the signing with possible effect on the overall visual aspect of the document.

4.4.2 PDF document

The validation process output is also available as a PDF document containing the validation process result in a textual form.

4.4.3 Validation clause

The validation clause – both the XML data and the PDF document – is signed with the QTSP's electronic seal and provided with the QTSP's time stamp.

The limiting condition of using the Validation clause is its technical validability. This characteristic is the effect of using an electronic time stamp with a limited period of technical validability. To preserve the electronic signature's validity in the long term, the validity must be renewed before the validity expires. After the expiry of validity, the Validation clause cannot be considered unambiguously valid.

4.5 Service availability

4.5.1 Validation Service

Availability of the Validation service is not guaranteed.

4.5.2 Qualified service

Availability of the Qualified service is guaranteed in the 365 x 24 hours mode with the exception of necessary stoppages for system administration and maintenance. Furthermore the availability excludes the time needed to recover the Service after an accident that was beyond the Service provider's control and that the provider could not control in any way.

QTSP guarantees a high reliability of the service, as a part of its services and applications used by important clients, and also Microsoft Azure infrastructure, in which the Services are operated.

QTSP provides a guaranteed minimum availability set in the document GSA – General Terms and Conditions and furthermore in the Service Contract with the end client.

5 Management, operational and physical security

5.1 Physical security

5.1.1 Location and construction

The location is selected so that it is possible to ensure protection from access by unauthorized persons, protection from natural disasters and accidents in utility infrastructures.

Technology of the Service is located in cloud environment, Azure by Microsoft. The Azure cloud environment provides a high level of security and ensures complex compliance with regulations.

Certifications for Azure are available here:

https://www.microsoft.com/en-us/TrustCenter/Compliance?service=Azure

In practice the company's data centers are operated between the Tier III and Tier IV classifications, as is specified in the TIA 942 standard. Nevertheless, they do not rely on HW tools alone to provide availability, as was assumed by Uptime Institute in the time of housing and webhosting.

5.1.2 Physical access

Technology of the Service is located in centers compliant with TIER III.

5.1.3 Electricity and cooling

Technology of the Service is located in centers compliant with TIER III.

5.1.4 Water impact

Technology of the Service is located in centers compliant with TIER III.

5.1.5 Fire protection

Technology of the Service is located in centers compliant with TIER III.

5.1.6 Media storage

All data media is stored on premises with the same level of physical security as the primary location – they are Microsoft premises where the Azure service is run. The premises are

equipped with mechanisms to provide constant temperature and humidity and provide protection from magnetic interference.

5.1.7 Backups

Backups of the Service technology are provided within the scope of TIER III.

5.2 Process security

5.2.1 Trusted roles

All employees who can access or control cryptographic and evaluation operations run as a part of the Service are assigned trusted roles corresponding to the activities. Administration of the Service's system makes strict use of the “separation of duties” principle. Assigning staff to trusted roles follows Software602's internal regulations.

5.2.2 Number of persons required to ensure specific tasks

Numbers of employees at the individual positions correspond to the required level of separation of duties and they are specified in detail in the related documentation.

5.2.3 Identification and authentication for each role

The employees are assigned means of proper authentication to the components that are necessary for their activities. These means are shredded and revoked after the termination of the role or of the employment in accordance with Software602's internal regulations.

5.2.4 Roles requiring separation of duties

The following activities may not be combined in the system:

- Security supervision of the Service system with any other executive role in the system.
- Deployment of any changes without superiors' confirmation.
- Deployment of any changes in the production environment without proper testing and superiors' confirmation.

The roles and assignment of duties are described in more detail in the Service's documentation.

5.3 Personnel safety

The trustworthiness and reliability of the Service and the whole infrastructure depend, among others, also on the quality of its personnel. The quality of the personnel is also perceived as a combination of trustworthiness and competence. Software602 follows such rules for management of employees that, when observed, ensure the required level of trustworthiness.

5.3.1 Requirements on qualifications, experience and clean record

The candidate must meet the criteria set in Software602's internal regulations and criteria set by the Personnel department and security division for the given role.

5.3.2 Evaluation of a person's reliability

The personnel department and security division of Software602 run an initial screening of all candidates applying for work at sensitive positions. This screening covers personal and qualification areas.

Employees from the personnel department verify, where possible, the provided reference from a previous employer, ideally using other sources than those supplied by the candidate.

The Personnel department and security division of Software602 run periodical screenings of all employees already active at sensitive positions.

5.3.3 Requirements on preparation for fulfilling the role, entry training

The Personnel department and human resources division of Software602 provide for all employees the required level of entry trainings, so that they can hold their positions properly and effectively. Requirements for each role are set in internal regulations for Service operation.

5.3.4 Requirements and periodicity of trainings

The Personnel department and human resources division of Software602 provide for all employees the required level of continuing periodical trainings, so that they can hold their positions properly and effectively. The training intensity is once per twelve months at minimum.

5.3.5 Periodicity and rotation sequence of employees between different roles

Not prescribed.

5.3.6 Sanctions for employees' unauthorized activities

All employees sign a Declaration of confidentiality and follow it and other internal standards.

5.3.7 Requirements for independent contractors (suppliers)

The Service and the Service technologies do not use independent contractors (suppliers).

5.3.8 Documentation provided to employees

All employees receive information about the existence and binding character of security documentation. All employees have access to Software602's security policy.

5.4 Audit logs

5.4.1 Types of recorded events

The electronic audit log records the following types of events:

- ***system events***

  The entry is created by the operating system to record every operation taking place on computers where the *Service* processes are installed.

- ***Validation events.***
  - Identifiers of the operation performed
  - User ID
  - Operation date and time
  - Operation type
  - Operation result
  - Date and time of document's validability expiry
  - File name
  - File size
  - Number of pages (for corresponding file types)
  - Hash of the file entering the operation

- Hash of the resulting file (PDF and XML clause)
- User comment

All audit logs are created, stored and processed in the required amount while preserving the authenticity, integrity, availability, confidentiality and authenticity in time.

The audit system is designed and operated in a manner that ensures preservation of audit data, reservation of sufficient space for audit data, not overwriting the audit log automatically, presentation of audit logs for users in a suitable manner and limiting access to the audit file to specified users only.

5.4.2 Periodicity of processing the logs

Information is recorded on-line and the logs are regularly analyzed at least once a day by the Security administrator so that any possible deviations from regular activities or willful damage are detected. The records are furthermore assessed by the supervisory group.

5.4.3 The storing period of audit logs

The period for storing audit logs complies with chapter 5.5.2. The data storing period for data published in the register and data from the Service's operational systems is at least 10 years.

5.4.4 Protection of audit logs

Electronic records for audits created by Software602's systems contain a time stamp of the record's creation and can be protected from modification by a digital signature.

Files containing records for audit are physically secured, as well as other parts of the Service. The person who is authorized to access these files is the Administrator.

5.4.5 Audit log backup procedures

There are two main backup procedures:

- everyday backups using the backup bot;
- continuous replication system to the backup department (using a highly secured network) located in a secure space with the same level of security as the main location.

Storing information is described in chapter 5.5.

5.4.6 The system for collecting audit logs

All sensitive audit logs are backed up in secure QTSP systems and backed up in regular intervals. Other security logs are checked by the supervisory department in the 7 x 24 mode.

5.4.7 Procedure for announcing an event to the subject who caused it

The subject is normally not informed, but may be asked by the person responsible to give explanation.

5.5 Storing information and documentation

5.5.1 Types of information and documentation that are stored

The Service Administrator at Software602 provides a suitable manner of archiving in particular the following:

- information for audits (described in the previous chapter);
- audit results;
- certification results;
- paper and electronic documents used within the Service:
    - documents related to contracts;
    - written requests for use/termination of use of the Service;

5.5.2 Storage period for information and documentation

All documents in archives will be stored for 10 years from the expiry of the individual certificates or the end of the document's validity.

5.5.3 Protection of storage of information and documentation

Protection is provided by the following set of measures:

- Archives in electronic form are stored in a database / file storage in the infrastructure of the Azure cloud service provider with a long lifespan. All data created by the Service's systems is secured from modification by an electronic signature.
- Log files are physically protected.

- Access to these files is only available to specified members of *Service Administration* and members of Software602's independent team of auditors or members of an external audit authorized by the Service Administrators.
- Secure transport of paper documents is provided by the Administrator.

5.5.4 Backup procedures for the stored information and documentation

Backup procedures are provided for by an internal regulation and other relevant Software602's internal documentation.

5.5.5 Requirements on using time stamps when storing information and documentation

Electronic time stamps used when storing electronic documentation and related information are from a QTSP.

5.5.6 Procedures for acquiring and validating stored information and documentation

The Service Administrator verifies inviolation and integrity of the archive at least once a year as a part of a regular internal audit. Access to the archive is only available to the Service Administrator and members of an independent team of auditors appointed by Software602 in accordance with procedures described in internal documentation.

The Service Administrator may authorize a member of the Supervisory group to check the archive continuously.

5.6 Restoration after an accident

5.6.1 Procedure in the case of an incident

The specific procedure is stipulated by Software602's corresponding internal implementing regulation.

5.6.2 Damage to computing equipment, software or data

It is provided for by measures in accordance with chapters 5.1.7, 5.5, and the specific procedure is stipulated by Software602's corresponding internal implementing regulation.

5.6.3 The ability to restore operation after an incident

In the case of an incident, Software602 proceeds in compliance with internal incident regulations; the Service operation can only be interrupted for the time absolutely necessary to migrate the affected subsystems to the backup location. For a quick recovery, it is possible to restore the whole Service infrastructure within Azure from existing backups.

5.7 Terminating the Service

Termination of the Service's operation must be announced in writing to all Service users, the supervisory body and the subjects who have concluded a contract related to operation and use of the Service. This fact must be at the same time announced on the QTSP's website.

The Provider undertakes to provide the Service for 6 months from the day of announcing the termination.

The Service administration shall take measures to secure archived records for the length of time prescribed in chapter 5.5.2.

6 Technical security

This chapter defines the security requirements for specific areas to ensure the quality of the Service provided under this VP.

6.1 Computer security

6.1.1 Specific technical requirements on computer security

They are defined within the internal regulations for Software602's operation and they follow these principles:

- Software602's critical systems are located in a physically protected environment with controlled access.
- Software602's critical systems are located in a cloud environment with a high level of security with controlled access and the corresponding certification (Tier III and similar).
- These computers are running or have installed only the programs that are related to operating Software602's critical system.
- Operation of these systems is monitored and regularly audited.
- Testing and development systems are strictly separated from production systems.

6.1.2 Evaluation of computer security

Evaluation of computer security is based on international and national standards and is performed by Software602's employees.

6.2 Lifecycle security

6.2.1 Management of system development

System development proceeds in accordance with internal documentation and best practice procedures for software development. The following principles are strictly observed:

- Separation of development, testing and production environments.
- Implementation of the PDCA principle (Plan – Do – Check – Act).

6.2.2 Security management checks

Compliance with standards is verified by regular audits and security compliance checks.

6.2.3 Lifecycle security management

Change control proceeds in terms of Software602's internal regulation.

6.3 Network security

Network security is described in Sotware602's internal operation regulations. Maximum emphasis is placed on thorough security of all components:

- Testing and development systems are strictly separated from production systems.
- Computer networks of Software602's critical systems are separated from the company's regular network by an internal firewall.
- Operation of these systems is monitored and regularly audited.
- Checks and verifications of network throughput are run regularly by technical administrators within Software602's internal structure.

6.4 Time stamps

The provided Service uses time stamps from a Qualified Trust Service Provider.

Issuing qualified time stamps is governed by the Qualified Time Stamp Issuing Policy of the corresponding QTSP.

7 Compliance assessment and other assessments

7.1 Assessment periodicity or conditions

The Service Administrator is entitled to request regular or irregular inspections and audits of any location and infrastructure section or component of the Service. These audits will be performed with the aim to verify that Service operation complies with security methods and procedures as they are set by this policy and internal regulations.

To ensure compliance of practice with the stipulations of the current VP and the corresponding regulations, the Service will undergo an internal audit at regular intervals. These intervals are not longer than 12 months.

Additional regular audits stipulated by the eIDAS Regulation and performed by a specified, accredited compliance assessor are always run at intervals shorter than 24 months.

7.2 Assessor's identity and qualifications

The assessor responsible must be a qualified assessor and must know the principles of QTSP, QTS and related information and regulations as stipulated by eIDAS.

7.3 Relation of the assessor to the subject being assessed

The assessor must be sufficiently organizationally separated from the Service and QTSP being revised, so that the assessment can be truly independent and not biased.

7.4 Procedure for any deficiencies found

Any discrepancies between the Service operation and the stipulations of its VP and/or the QTSP's internal regulations must be recorded and resolved without delay or in the prescribed period.

Any remedy may contain instructions for permanent or temporary suspension of operation of a part of the Service, and several factors, including among others the severity of the discrepancy, risks incurred and the detriment of such disruption to the subjects using the Service, must be considered before making such a decision.

The decision which steps to take will also depend on the manner of previous reactions to problems that occurred, severity of the deviations and the auditor's recommendations.

7.5 Assessment result notifications

The final results of the audit will be presented to the management of Software602. The final result means information on all discrepancies that could affect the relying party's trust in the certificate, including an adequate assessment of severity, but not detailed information that could be used to attack the system.

In compliance with the stipulations of section 7.4, any part of the Service that is proven not to work in compliance with this VP must be assessed immediately after the audit's conclusion and its remedy provided. To lower the risks as much as possible, it is necessary to announce the instructions for the required remedy as soon as possible. The Service Administrator must be informed of the implementation of instructions to the remedy. A special audit may be requested to verify the agreed remedy and its effectiveness.

8 Other commercial and legal questions

8.1 Fees

The Service is provided for a fee based on the TSP and QTSP's price list.

8.2 Confidentiality of commercial information

8.2.1 List of confidential information

The QTSP's confidential information is:

- All information related to the validation process and stored in records within the Service.
- Other cryptographically significant information used for the Service's operation.
- Selected commercial information.
- All information and documentation related to providing trust services.
- All personal data.

All other information described by one of the subjects as especially confidential is also considered protected. Protected information, regardless of the type of media, is treated in a way that ensures its confidentiality and integrity.

8.2.2 Information outside the scope of confidential information

The following is not considered confidential:

- public parts of certificates,
- CRL lists,
- information on invalidation and suspension of validity,
- certification policies.

8.2.3 Responsibility for the protection of confidential information

Protection of confidential information is the responsibility of the organizational unit or person who manages such information. Every employee who comes into contact with information considered confidential under chapter 8.2.1 must not release it to a third person.

Software602 employees, cooperating persons or companies who come into contact with sensitive information are obliged to maintain the confidentiality of such information. This obligation continues after the termination of employment or other similar relationship or after finishing the contracted work.

As an organizational and legal provision to fulfill the above mentioned conditions, a contractual agreement (in the form of an addendum to the employment agreement, confidentiality agreement, etc.) is concluded with all subjects.

8.3 Personal data protection

Protection of personal data is governed by generally binding legislation of the Czech Republic, namely Act 110/2019 Sb., on personal data protection, and furthermore by Regulation (EU) 2016/679 of the European Parliament and of the Council ("GDPR").

8.4 Intellectual property rights

This VP, all related documents, website contents, certificates, CRLs, procedures and regulations that provide the Service's operation are protected by Software602's rights and constitute its important know-how and intellectual property rights.

8.5 Disclaimer

QTSP Software602 refuses any guarantees on the operation of the Service and the results supplied by the Service, if the Service or the Service Interface has been used in contradiction with the Service Terms and this policy.

The service allows on its input defining validation process conditions that can be used to affect the standard validation process result. If an integrator of the Service makes use of such user settings, QTSP Software602 refuses any guarantees on the Service operation and results provided by the Services.

8.6 Limitation of liability

Under no circumstances shall Software602, its representatives, directors, employees, partners, licensors or suppliers bear any liability to the user or another person for any special, accidental, indirect, secondary or penal damage, including damage arising from the loss of data or loss of profit, whether they are foreseeable or the Service provider was notified of the possibility of such damage, or based on any theory of liability, including a breach of contract or guarantee, negligence or other infringement, or any other claim arising from the use or access to websites, services or materials or related to such use. No provision of the terms may limit or exclude the Service provider's liability for gross negligence or willful damage or injury by the Service provider or its employees or for death or injury to persons.

8.7 Liability for damage, compensation for damage

Software602's liability to provide compensation for any damage whatsoever for the violation of the company's obligations whatsoever and/or obligations related to providing the Validation Service shall be limited to CZK 100,000 (ten thousand Czech crowns), which is the amount that shall be, in terms of the provisions of section 2898 of Act 89/2012 Sb., the Civil Code, as amended, the maximum damage that Software602 shall be liable for and, as the case may be, Software602 shall be obliged to pay.

If the Validation Service is provided, the burden of proving intention or negligence of the TSP shall lie with the natural or legal person claiming the damage referred to in Article 13, first subsection, second sentence of eIDAS.

If the Qualified service is provided, the burden of proof shall lie with the QTSP and it shall be the QTSP's right to prove that the damage in terms of Article 13, first subsection, third sentence of eIDAS occurred without the QTSP's intention or negligence.

8.7.1 Insurance

Software602, a.s. declares that it has concluded a suitable business risk insurance to cover the damage that might arise.

Software602, a.s. also declares that the employees responsible have arranged for a liability insurance with a reasonable scope in case of damage incurred to the employer.

8.7.2 Assets

Software602, a.s. declares that it has sufficient financial cover available to provide qualified trust services in regard to the risk of liability for damage. More details can be found in Software602, a.s.' Annual Reports.

8.8 Validity period, termination of validity

8.8.1 Validity period

This document shall stay valid until the end of providing the Service based on this VP.

8.8.2 Termination of validity

The termination of this VP's validity must be approved by Software602's management in writing and unambiguously. This fact must be published in places specified in chapter 2.2.

8.9 Communication between the parties involved

Individual communication can make use of all types of contacts that the parties involved exchanged with mutual authentication.

Public communication takes place using channels specified in chapter 2.2. of this VP.

8.9.1 Incidents

The Qualified Service provider identifies a unified communication point for entering requests, incidents and proposals. Such unified contact place is RT or the e-mail address hotline@602.cz. This interface is connected to an automated request tracking system, which assigns a unique number to every request and ensures timely resolution of the requests with the option of tracking.

8.10 Changes

8.10.1 Change procedure

Software602 is entitled to amend this VP in the future by provisions whose necessity is yet to be recognized. Such changes will be published in places specified in chapter 2.2 of this VP. Such changes, if any, will not be retroactive.

Changes of non-material character will enter into force from the moment they are duly published in accordance with this section.

Changes with material character will enter into force 15 days after they are duly published, unless Software602 announces their withdrawal before the end of the 15-day period.

8.10.2 Change announcement procedure

Governed by the rules and procedures specified in chapter 2.

8.10.3 Circumstances that require a change in the Validation process

The validation process is defined by several technical specifications and standards defined in eIDAS. The validation process is governed by these legislative requirements and change is only possible as long as it meets the legislative requirements.

8.10.4 Infrastructure changes

Infrastructure has an effect on security and trustworthiness of the provided Service. If continuous internal audits find that the quality of the provided infrastructure is insufficient, a transfer of the Service to another infrastructure will be provided in accordance with

Software602's internal regulations. Such a change will be performed in a way that does not affect the service's continuity. Changes will be announced in accordance with section 2.2. of this VP.

8.11 Dispute resolution

The user agrees that any request or claim made against the Provider must be dealt with by the competent court of the system of municipal courts of the Czech Republic in the Czech Republic, unless the parties agree explicitly otherwise in written form. The user undertakes that for the purpose of legal proceedings of such claims or disputes the user will submit to the jurisdictions of the courts in the Czech Republic. The language of the case shall be Czech and the place of the proceedings shall be the seat of the competent court determined by Software602's registered office.

8.12 Governing law

The governing law is the law of the Czech Republic. At the same time European legislation, the eIDAS Regulation and rules stipulated by this Regulation must be taken into account.

8.13 Compliance with legislation

This document complies with the requirements of eIDAS Regulation, legislation of the Czech Republic and recommendations of EU authorities, namely with the following documents:

[1] ETSI EN 319 102-1 – Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures

[2] ETSI TS 103 171 – Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile

[3] ETSI TS 103 172 - Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile

[4] ETSI TS 103 173 - Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile

[5] ETSI TS 103 174 - Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile

[6] ETSI TS 319 401 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Provider

[7] ETSI EN 319 142-1 - Electronic Signatures and Infrastructures (ESI); PAdES Digital Signatures

[8] ETSI EN 319 132 - Electronic Signatures and Infrastructures (ESI); XAdES Digital Signatures

[9] ETSI EN 319 122 - Electronic Signatures and Infrastructures (ESI); CAdES Digital Signatures

[10] ETSI EN 319 162 - Electronic Signatures and Infrastructures (ESI); ASiC

[11] RFC3647 – Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework

TSP is furthermore certified in accordance with:

[12] ISO 27001 – Information security management system

[13] ISO 9001 – Quality management system

[14] ISO 10006 – Quality management system

[15] ISO 20000 – IT service management system

[16] ISO27017 – IT – BT – Code of practice for information security management based on ISO/IEC 27002 for cloud services

[17] ISO 27018 – Code of practice to protect personal data