APPROVED
PMO GOVERNANCE
DORU VIJIIANU
JUDIT FEKETE
MIRELA OJOG

ZIPPER Terms and Conditions for Validation Services

.

Edition history			
Edition	**Date and description of the change**	**Prepared**	**Approved**
1	28.06.2023 – First edition	Mirela Ojog	Judit Fekete
2	24.10.2023 -Second edition	Judit Fekete	Mirela Ojog
3	09.11.2023 – Third Edition	Judit Fekete	Mirela Ojog
4	24.04.2024 – Fourth Edition	Judit Fekete	Mirela Ojog

Terms and Conditions & Subscriber Agreement

1. Purpose

Before entering into a contractual relationship, a Qualified Trust Service Provider (QTSP) shall inform, in a clear and comprehensive manner, any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use.[1] The Subscriber Agreement constitutes the contract between the QTSP and the Subscriber for the provision of the services and it can refer to the Terms and Conditions which the Subscriber will need to accept in order to receive the services. The general obligations specified in clause 6.2 ETSI EN 319 401 for Terms and Conditions apply. More specifically, the Terms and Conditions shall lay down at least the following information:

a) the trust service policy being applied;
b) any limitations on the use of the service provided including the limitation for damages arising from the use of services exceeding such limitations;
c) the subscriber's obligations;
d) information for parties relying on the trust service, e.g. how to verify the trust service token,
e) the period of time during which TSP's event logs are retained;
f) limitations of liability;
g) the applicable legal system;
h) procedures for complaints and dispute settlement;
i) whether the TSP's trust service has been assessed to be conformant with the trust service policy, and if so through which conformity assessment scheme;
j) the TSP's contact information; and
k) any undertaking regarding availability.

The Terms and Conditions shall be made available through a durable means of communication, in a readily understandable language and may be transmitted electronically.

2. Liability in the provision of Validation services

Liability derives from contract or law. Where consumers are involved, legal provisions may also apply which can increase the level of protection (i.e. consumer law).
It may be the case that either national or European legislation constrain the TSP's capability to limit its liability, for example. For example, it may prohibit terms that have not been individually negotiated and cause a significant imbalance in the parties' rights and obligations to the detriment of the consumer. Where these exceptions do not apply, a TSA may limit its liability.

3. Definitions and Acronyms

Term	Meaning
Qualified Trust Service Provider (QTSP)	A trust service provider that provides qualified trust services and is included in the EU trusted list.
Relying party	A natural or legal person who relies on that trusted service.
Subscriber	A Legal or Natural person to whom a validation is issued and who is bound to any subscriber obligations.
Validation Authority (VA)	A Trust Service Provider (TSP) providing Validation services
VA Policy & Practice Statement	Validation Authority Policy and Practice: Statement of the practices that a VA employs in issuing validation of certificates/seals.
eIDAS Regulation	Regulation (EU) No. 910/2014 of the European Parliament and of the Council of July 23, 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93 /EC
TSP	Trust Service Provider

[1] 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

IMPORTANT NOTICE: THESE TERMS AND CONDITIONS AFFECT YOUR LEGAL RIGHTS. PLEASE READ THEM CAREFULLY. BY ACCEPTING THESE TERMS AND CONDITIONS, YOU AGREE TO FOLLOW AND BE BOUND BY THEM.

1. General Terms

1.1 The Terms and Conditions govern Subscribers' use of ZIPPER's Qualified Validation Services (hereafter "Validation Services") and constitute a legally binding contract between Subscriber and ZIPPER.
1.2 The Subscriber has to be familiar with and accept the present Terms and Conditions.
1.3 ZIPPER has the right to amend these Terms and Conditions at any time if there is a justified need for such amendments. Current version and previous versions are published on the web page repository at https://pki.ca.ezipper.ro/repository/index.php
1.4 The Subscriber of Validation Services can be a natural person or legal person, by entering into a relevant contract with ZIPPER.

2. Qualified Signature/Seal Validation Services Applicable terms

The process for the validation of a qualified/advanced electronic signature/seal can be used to confirm the validity of a qualified/advanced electronic signature/seal and provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.

The recipients of these Terms and Conditions are Subscribers and Relying third parties.

2.1. Description of the service, regulatory and legal framework

The Qualified Electronic Signature Validation Service is provided in accordance with articles 32 and 33 of the eIDAS.

The Qualified Electronic Seal Validation Service is provided in accordance with article 40 of the eIDAS Regulation.

The Qualified Validation service applies the requirements established in clause 6.2 of ETSI EN 319 401, and works on the basis of a validation policy of signatures as input, that is, the validation of signatures/seals, is always carried out against a validation policy. The validation policies accepted and whose requirements are used to carry out the validation process of signatures and electronic seals are:

- Zipper Validation Policy OID 1.3.6.1.4.1.57570.4.2.2.3
- Validation Policy that meets the basic criteria ETSI TS 119 441 OID 0.4.0.9441.1.1
- Validation policy that meets the qualified validation criteria ETSI TS 119 441 OID 0.4.0.9441.1.2
- The Qualified Validation Service follows the requirements established by ETSI TS 119 102-2 and ETSI TS 119 441. In the event that QTSP decides to make any variation in them, this variation will be included in the OID Validation Policy and service subscribers will be informed by email.

The qualified service of validation of advanced/qualified signatures/seals electronic (QSVS), supports the following formats of QES/QESeal,

- XAdES - ETSI EN 319 132
- CAdES - ETSI EN 319 122
- PAdES - ETSI EN 319 142

And levels:

- XAdES - B – T - LT or LTA
- CAdES – B – T - LT or LTA
- PAdES – B – T - LT or LTA

Signature validation (according to ETSI EN 319 102-1) allows processing the validation of signature with following levels:

- BASIC_SIGNATURES - the basic signature validation process, supporting validation of signatures where the time of validation lies within the validity period of the signing-certificate and the signing-certificate is not revoked. This level corresponds to section "5.3 Validation process for Basic Signatures" of the standard.
- `TIMESTAMPS` - the validation process combines the basic signature validation process and the basic validation of embedded timestamp tokens, which signing-certificate is valid at validation time and not revoked. This level corresponds to section "5.4 Time-stamp validation building block" of the standard.
- `LONG_TERM_DATA` - performs a validation of a signature with time and signatures with long-term validation material. The signing-certificate of a signature passed to this process shall be retrospectively valid, taking into account the available signature-time-stamp and long-term validation material. This level corresponds to section "5.5 Validation process for Signatures with Time and Signatures with Long-Term Validation Material" of the standard.
- `ARCHIVAL_DATA` - performs validation of signatures providing long-term availability and integrity of validation material. The signing-certificate of a signature passed to this process shall be retrospectively valid with relation to all the available POEs (signature and archive time-stamps) and long-term validation material. This level corresponds to section "5.6 Validation process for Signatures providing Long Term Availability and Integrity of Validation Material" of the standard.

2.2. Specific terms

A.The service accepts the following levels:
- Qualified Signatures and Seals (QAdES) and Advanced Signatures and Seals (AdES)

B. In the case of multiple signatures, the signed document must be of the envelopement type (signature includes the signed document)
C. In the event that the signature includes non-current elements (eg, expired or revoked certificates, time stamps or obsolete cryptographic elements –ETSI TS 119 312-) the criteria published by the EU Commission and regulations in the matter, and especially what is established in this matter in ETSI TS 119102-1.
D. The proof of signature (PoE of the signature) is made up of the signed document and the signature, both elements can be included in a single file if the signature is envelopement.
E. The validation service may be affected by the practices, policies and SLAs of other TSPs that are not under the control of Zipper.

3. Prohibitions of use

Validation services shall not be used outside the limits and contexts specified in ZIPPER VA Policy and Practice Statement, nor for unlawful purposes, or contrary to public interest, or otherwise likely to damage the business or reputation of ZIPPER.

4. Subscriber's Obligations

According to Romanian legislation [Ref] the Subscriber of Validation Services, any person, natural or legal, (Subscriber) who wishes to benefit from Validation services must:

- provide information regarding his identity;
- comply with the limitations imposed by the Validation service provider.

The Subscriber undertakes to apply the necessary measures to guarantee the conformity of the request, providing exact data and following the procedures established for this purpose by Zipper.

The Subscriber agrees to pay the fees corresponding to the Service requested, and assumes the obligation to process the request with the sole interest of making use of the purpose for which it is marketed by Zipper.

Is totally prohibited:

• reverse engineer;
• any action that has the purpose of putting stress on ZIPPER's systems, applications, or products;
• any action that has the objective of analyzing, evaluating, or discovering the technology used by ZIPPER;

5. Relying Parties Obligations

A RELYING PARTY IS RESPONSIBLE FOR DECIDING WHETHER OR NOT TO RELY ON A VALIDATION. Relying Parties acknowledge and agree that their use of ZIPPER's Repository and their reliance on a Validation shall be governed by ZIPPER's applicable TSA Policy and Practice Statement as amended from time to time. The applicable CPS is published on the Repository at https://pki.ca.ezipper.ro/repository/policies.php

The business application used by Zipper must enable relying party end-user to visualize signed parts/versions of a document in order to verify whether the signed content matches with the user's expectations so that the right decisions can be taken and that prevention of fraud is better addressed.

The validation service validates all signatures and seals applied to the same input document and supplies resulting diagnostics in a single report, for all signatures/seals and applied timestamps. It does however not make any interpretation of supplied diagnostics or mutual relationship of those signatures and seals. The validation process is driven by a set of constraints that are contained in the Zipper constrain policy file.

ZIPPER shall provide the services in accordance with the present Terms and Conditions, the ZIPPER VA Policy & Practice Statement, as well as any relevant legislation and applicable standards.

6. Limited Warranty and Disclaimer/Limitation of Liability

ZIPPER is liable for the performance of its Validation Services as specified in the present Terms and Conditions and its TSA Policy & Practice Statement.

ZIPPER ensures that it has compulsory insurance contracts covering its services to ensure compensation for damages caused by breach of obligations;

ZIPPER informs all Subscribers before it terminates its services and maintains the documentation related to them.

ZIPPER is not liable for

- inadequate checks of Time Stamp validity or for uninformed decisions of a Subscriber or Relying Party;
- the improper use of validation application;
- the non-performance of its obligations if such non-performance is due to faults or security problems of the supervisory body, the data protection supervision authority, Trusted List or any other public authority; the failure to perform if such failure is occasioned by force majeure.

ZIPPER provides limited warranties and disclaims all other warranties, including warranties of merchantability or fitness for a particular purpose, limits liability, and excludes all liability, except in case of willful misconduct or gross negligence, for any loss of profits, loss of data, or other indirect, consequential, or punitive damages arising from or in connection with the use, delivery, performance, non-performance, or unavailability of the Validation Services. ZIPPER's aggregate liability to all parties (including you) shall in no event exceed the amount of the respective contract for the Validation Service, and a total maximum of 500.000 euro, regardless of the nature of the liability and the type, amount or extent of any damages suffered. The liability limitations shall be the same irrespective to the number of Validations or claims related to such Validation Service.

The limitations on liability provided herein shall apply to the maximum extent allowed under the applicable law of the applicable jurisdiction.

7. Logs Retention

Zipper monitors the usage of Validation Services by means of **event logs** that are needed as evidence. Such event logs are in any case retained for a period of at least (3) year as from their creation date. The time accuracy of logs is ensured by a time server that is synchronized with at least two-time sources that can be GPS satellite or Stratum 1 UTC sources.

8. Applicable Agreements, Policies, CP, CPS

Relevant agreements, policies and practice statements are:

- ZIPPER Validation Authority Policy & Practice Statement
- ZIPPER Terms and Conditions for Validation Services.

Current versions of all applicable documents are publicly available in the ZIPPER repository at https://pki.ca.ezipper.ro/repository/

9. Privacy Policy and Confidentiality

ZIPPER processes personal data in accordance to the applicable data protection legislation in force. For further details, please refer to ZIPPER Privacy Statement https://pki.ca.ezipper.ro/repository/compliance.php

All information that has become known while providing services and that is not intended for disclosure is confidential. The Subscriber has the right to obtain information from ZIPPER about the processing of their personal data pursuant to applicable law.

ZIPPER has the right to disclose information about the Subscriber to a third party who pursuant to relevant law or a court decision, is entitled to receive such information.

ZIPPER may publish non-personalized statistical data about its services.

10. Refund Policy

ZIPPER makes efforts to secure the highest level of quality of its services. However, Subscriber has the right to withdraw from the purchase contract for any reason in case the purchase of the Validation Service is effected via the internet or a telephone the Subscriber. The exercise of this right shall be made in writing by the Subscriber to ZIPPER, by sending an email to suport.pki@ezipper.ro within 14 days from the date of purchase.

Subject to section 12, ZIPPER may handle refunds on a case-by-case basis.

11. Service availability

Zipper ensures that the availability of the services is in accordance with the terms and conditions described in its Policies and Practices and in these General Terms and Conditions. Zipper will use its best efforts to ensure an availability of the Validation Services of 99,7% on Business hours - defined as 24 hours a day, seven days a week, excluding planned maintenance periods. Planned maintenance periods will be announced by email at least 24 hours in advance. In case of unavailability due to a catastrophe, failure of infrastructure outside the control of Zipper or any other reason, Zipper will make best effort to reinstate availability of the service within 24 hours.

12. Applicable law, complaints and dispute resolution

Any disputes related to the trust services provided under these terms shall be governed in all respects by and construed in accordance with the laws of Romania.

To the extent permitted by law, the parties shall initially seek to solve any dispute amicably and if the dispute is not

resolved within thirty (30) days after the initial claim, then the Courts of Bucharest, Romania shall have exclusive jurisdiction to hear and resolving it.

Any dispute requests or claims should be sent to the contact information provided in these Terms and Conditions.

13. ZIPPER and Repository Licenses, Trust Marks and Audit

ZIPPER's Qualified Validation Services are registered in the EU Trusted List of Qualified Trust Service Providers: https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home

ZIPPER's Qualified Validation Services have been audited by Conformity Assessment Body which is accredited in accordance with Regulation (EC) No 765/2008 as competent to carry out conformity assessment of Qualified Trust Services. Audit certificates, which are based on audit results of the conformity assessment conducted pursuant to the eIDAS Regulation and standards, are published on ZIPPER's website at https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home

14. Contact Information

ZIPPER SERVICES: Validation Authority
Strada Tăietura Turcului, Nr. 47, Imobilul Novis Plaza, Corp A, Et. 2,
Cluj-Napoca, 400285, România

Working Point:
B-dul 1 Decembrie 1918 nr. 1G,
Sector 3, Bucuresti, 032451, Romania

Working Point:
str. Nikola Tesla, nr. 2, cod 400221
Cluj-Napoca, 400285, Romania

https://ezipper.ro/en/
E-mail: office@ezipper.ro
Telephone +40 21.340.4638 / +40 31.101.1020
Fax +40 21.340.4636 / +40 31.101.1022
(Mon-Fri 09.00. – 18:00 Eastern European Time)

15. Validity of Terms and Conditions

If any provision of these Terms and Conditions, or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder shall not be affected by such finding of invalidity or unenforceability, and shall be interpreted in a manner that shall reasonably carry out the intent of the parties.

16. References

The following references contain provisions which are relevant to the ZIPPER Certificate Policy & Certification Practice Statement:

1. 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 and repealing Directive 1999/93/EC.

2. ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

3. ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

4. ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Validation protocol and time-stamp token profiles".

5. IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)".

6. ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

7. ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

8. TS 119 441: Policy requirements for TSP providing signature validation services

9. ETSI TS 119 441 (Signature/seal validation)

Romanian Regulations:

8. Government Decision no. 89/2020 on the organization and functioning of the Romanian Digitization Authority

9. ORDER no. 449 of May 30, 2017 regarding the procedure of granting, suspending and withdrawing the status of provider of Qualified reliable services in accordance with Regulation (EU) no. 910/2014 of the European Parliament and of the Council of 23 July 2014

Subscriber Agreement Template

Application and Agreement for the provision of Validation Services

Date:	S/N:

APPLICANT-SUBSCRIBER'S DATA

Name:	Surname:
E-mail address:	Telephone number:

APPLICANT-SUBSCRIBER'S Public IP address

Public IP address:
(from wich the Applicant will use the service)

TERMS & CONDITIONS ACCEPTANCE

This Application constitutes the agreement between the Subscriber and ZIPPER for Validation Services. Validation Services are governed by ZIPPER TSA Policy & Practice Statement, as well as ZIPPER Terms and Conditions for Validation Services, as amended from time to time and published at https://pki.ca.ezipper.ro/repository/policies.php

You may contact ZIPPER Customer Support at suport.pki@ezipper.ro

□ **I have read and accept ZIPPER's General Terms and Conditions for the Use of Qualified Trust Services.**

PERSONAL DATA PROCESSING

The use, processing and storage of information included in this Application is conducted in accordance with ZIPPER's Privacy Policy which is available at https://pki.ca.ezipper.ro/repository/compliance.php

□ **I have been sufficiently notified about the processing of my personal data.**

The Applicant-Subscriber

Name/ Surname:

Signature: