Electronic signature Terms and Conditions of Use

Decentralized identity management on the customer side

1. Purpose and parties

The present Terms and Conditions of use (hereinafter the "TCU") define the conditions in which the electronic signature services are provided by Woleet and used by the Service Consumer, the conditions of use, and the liabilities of the following parties:

- Woleet, as the service provider of the electronic signature. Woleet is a French simplified joint-stock company with a turnover of €12,668, registered with the Rennes Companies Register under no. 819 437 450, with registered offices at 24 bis rue du Maréchal Joffre - RENNES (35000). Woleet is hereinafter defined as the "Service Provider".
- Woleet's customer, i.e the organization (for example, but not exclusively a company) that has subscribed to Woleet electronic signature service, that determines the documents or data that need to be electronically signed, and the related signatories. Woleet's customer is hereinafter defined as the "Service Consumer". The present TCU apply in cases where the Service Consumer hosts Woleet.ID Server, as described in section 3.

2. What is an electronic signature provided by Woleet?

Electronic signature is the digital way to sign an electronic document or any data in a digital (non-paper) format. By signing a document electronically, using Woleet's Services, the signatory thereby approves the content of the signed document.

The electronic signature process guarantees the integrity of the signed document and provides reliable information about the identity of the signatory (if the signature is not pseudonymous).

The electronic signature performed by Woleet abide by the applicable regulatory framework in Europe, the Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (hereinafter defined as "eIDAS"), and meets the definition of simple and advanced electronic signatures.

The characteristics of Woleet's signatures and seals include the following:

- They can apply to any format of data, including pdf, text, images etc.
- They do not impair the confidentiality of the document or data, as the cryptographic hash is computed by the Service Consumer. The signed or sealed data is not sent to Woleet.

- Woleet signature and seals, when performed with the Woleet API, are anchored in the Bitcoin blockchain, so as to get an irrevocable proof of existence of this signature or seal, with a reliable timestamp.
- Woleet signature or seal is separated from the document or data. It is provided within a proof receipt, based on a standardized format (including Chainpoint, OpenTimeStamps). Woleet publicly documents the validation rules of a signature or seal proof so that it can be verified by anybody.
- Woleet signature can either identify a physical person or an organization. In the latter case, these signatures are called seals, according to eIDAS terminology. The process as regards seals is further described in Appendix 1.

3. Terms applicable to the Service Consumers

3.1 General undertakings from the Service Consumers

The Service Consumer undertakes to comply with the present TCU and to ensure that its use of the Services (including use by the Users, Administrators, Managers and Collaborators or any other third party under its control as defined in the Appendix) complies with the TCU, including the Appendix.
If the Service Consumer is a legal entity, the signatory of the TCU represents and warrants that it has full legal authority to sign the TCU on behalf of the legal entity.
The Service Consumer shall take all appropriate measures to manage the risks in relation with conflict of interest.

3.2. Protection of critical data by the Service Consumers

The Service Consumer hosts Woleet.ID Server and uses Woleet API to use the electronic signature service, as further described in the Appendix. As a consequence, it holds personal data of signatories and their related signature key pairs (private and public keys).

These critical data must be protected as described below.

1. The Service Consumer undertakes to host Woleet.ID Server under the best conditions of security, and to take all appropriate technical and organizational measures, adapted to the risk level. Security measures shall be taken to prevent and minimize the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.
2. In particular:
    - The database used by the Service Consumer to host Woleet.ID Server and use Woleet API must be protected from unauthorized access.
    - The database must be backed-up so as to limit data loss.
    - The logging information must be exported so as to allow investigation in case of security breach.

3. The Service Consumer undertakes to publish the status of the signature keys (expired or revoked), and to make this information accessible to any party requiring to validate a signature.
4. The Service Consumer must keep the proof receipts delivered by Woleet as long as the validation of related electronic signatures is necessary. These proof receipts are required to perform the validation of a proof of signature, on Woleet validation service, or on any public validation service compatible with the format of the proof receipts used by Woleet.
5. The Service Consumer can only generate seals, following the procedure further explained in the Appendix, that refer to their own organization, either the whole organization or an entity or department. The Service Consumer shall not generate seals that would identify another organization, which would amount to identity theft.

Advanced electronic signature upon eIDAS terms

The following requirements aim to fulfill the criteria of the eIDAS definition of advanced electronic signatures (note that advanced electronic seals are not concerned):

1. The Service Consumer undertakes to define the identity verification procedure to be followed by the signatories. This procedure must provide reasonable assurance concerning the identity of the signatories, so as to avoid any impersonation attempt, or any fraud concerning fake identities.
2. The Service Consumer shall collect and maintain evidence of the identity verifications implemented so as to prove, if necessary, that they were duly performed.
3. The Service Consumer shall enforce strong authentication of Users:
    - For keys stored on Woleet.ID Server: password verification and OTP sent by SMS.
    - For keys under the control of user (mobile or Ledger): PIN authentication on the device and OTP sent by SMS.
4. The creation of advanced electronic signatures requires to get signed audit trails from Woleet at the end of the signature requests.

4. Terms applicable to the Service Provider

4.1 General undertakings

1. The Service Provider undertakes to comply with the present TCU.
2. The Service Provider undertakes to provide a solution that complies with the applicable regulation, in particular, the eIDAS and GDPR.
3. The Users can exercise their right to access, modify or delete their personal data collected as part of the Service by notifying the Service Provider of their intention at the following address: privacy@woleet.com.
4. The Service Provider has defined a Signature Validation Policy describing how to check an advanced signature or seal made using Woleet service. Woleet undertakes to provide the necessary elements allowing to perform the validation of a signature,

including a description of the proof receipt format and the documentation of open source code and APIs.

5. The Service Provider undertakes to implement the appropriate security measures so as to manage the security risks, in particular:
    - The Service Provider protects data confidentiality, integrity and security. However; the Service Provider should not be held liable for the information which are not available to it. Note that the signed data are not collected and should not be sent by the Service Provider.
    - The Service Provider makes the best efforts to prevent unauthorized use of the Service and to reduce the possibility of service corruption.
6. The Service Provider has defined a Continuity Plan to manage the risks about the continuity and durability of the Service. In particular the continuity risks linked to IT infrastructure and to Bitcoin technology are addressed.
7. The Service Provider undertakes to an availability rate and to a support level defined in each customer contract.

4.2 Liability

The Service Provider will however only be held responsible for direct and foreseeable damages caused by a breach of its obligations provided in these TCU and the contract with the Service Consumer.

Limitation of liability

Subject to any contrary public policy provisions applicable, the Service Provider will not be held responsible:

- due to (i) poor use of the Service by the Service Consumer, Collaborator, Manager, Administrator or User as defined in the Appendix and/or (ii) due to any use in conditions and for purposes other than the ones set out in the TCU;
- due to disclosure, use by unauthorized third parties and/or fraudulent misappropriation of one or several Service element(s) (and in particular, private keys, personal data);
- for any dysfunction, slow-downs, interruptions, inability to use and/or poor access conditions to the Service (i) due to the nature of the Internet network, mobile telephone networks and wireless networks and/or (ii) a failure and/or saturation of data communication networks (internet, intranet or wireless network);
- regarding the consequences of delays or losses which could arise during sending of all electronic messages or API requests, and regarding the delays on alteration of the Service or other errors which could arise in sending any telecommunication to the User;
- if the User has omitted or delayed informing of any error relating to the signature key or reasons for revocation of which it is aware;

- furthermore, the Service Provider will not be held responsible for failure to comply with the TCU, the contract with the Service Consumer and all damages caused by the User, the Service Consumer, the Collaborator, the Manager, the Administrator (as defined in the Appendix) and/or any third party in relation to the Contract, its fulfilment, termination and further proceedings;
- Force majeure: If a case of force majeure were to arise in the sense of article 1218 of the French Civil Code, the obligations of the Service Provider provided in the TCU will be suspended throughout the case of force majeure and will restart on termination of the same, and the Service Provider cannot be held liable on this basis.

5. Other provisions

5.1 Applicable law

The TCU, their validity, interpretation and fulfilment are governed by French law.

5.2 Resolving disputes

Any challenge or dispute regarding the conclusion, validity, interpretation or fulfilment of the TCU and/or fulfilment of the Service which cannot be resolved amicably within one (1) month after arising will be submitted, subject to applicable regulations, to the jurisdiction of the Rennes Court of Appeal (France).

5.3 Intellectual property

The use of the signature service and of the signature keys does not grant any intellectual property right implied or otherwise, to the Service Consumer, the User, Service Consumer, the Administrator or any other party using the services.

As between the Parties, the Service Provider retains all intellectual property rights in the Services.

Notwithstanding the foregoing, the Service Provider grants the Service Consumer a personal and non-exclusive right which is non-transferable to use the Service for the sole purposes of signing, in France.

5.4 Confidentiality.

During the term of the TCU, the Service Consumer undertakes to keep strictly confidential all information relating to the Service Provider and to the Services, except regarding information that has entered the public domain. The Service Consumer will take the necessary measures to ensure that this obligation is fulfilled by the User, the Collaborator, the Administrator or any other party under its control.

This confidentiality commitment will remain in effect after the end of the Contract, for a period of five (5) years.

5.5 Price

The price of the use of Woleet's service is defined in Woleet pricing policy. It is applied within a commercial contract between the Service Provider and the Service Consumer. The price is not due by the Users.

Refund is not applicable.

5.6 Duration

The TCU enter into force on signing by the Service Consumer or other at the date it clicks the button to accept these TCU, and will apply until the end of the contract between the Service Provider and the Service Consumer, or at the end of use of the service.

6. Definitions

Some of the following definitions are directly taken from eIDAS European Regulation n°910/2014.

- **API**: Application Programming Interface. Interface published and documented by a service provider allowing consumers to use the service.
- **Authentication**: « means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed », according to eIDAS.
- **Cryptography**: practice and study of techniques for securing communication in the presence of third parties. Such techniques include data confidentiality, data integrity, authentication and non-repudiation. Cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary.
- **Electronic signature**: « data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign », according to eIDAS.
- **Pseudonymous signature**: property of an electronic signature that does not identify a physical person by his/her real name, but by a pseudonym.
- **Signatory**: can be either a physical person or an organization in case of seals. The signatory uses a signature key to create electronic signatures or seals.

Appendix – Technical conditions of use

This appendix defines the technical conditions in which the electronic signature services are provided by Woleet, the conditions of use, and the liabilities of the following parties:

- Woleet, as the service provider of the electronic signature. Woleet is a French simplified joint-stock company with a turnover of €12,668, registered with the Rennes Companies Register under no. 819 437 450, with registered offices at 24 bis rue du Maréchal Joffre - RENNES (35000). Woleet is hereinafter defined as the "Service Provider".
- Woleet's customer, i.e the organization (for example, but not exclusively a company) that has subscribed to Woleet electronic signature service, that determines the documents or data that need to be electronically signed, and the related signatories. Woleet's customer is hereinafter defined as the "Service Consumer".
- The collaborator, i.e a physical person who requests the signature of a document to one or several users. The collaborator is generally related to the Service Consumer by an employment contract. The collaborator is hereinafter defined as the "Collaborator". The detailed obligations of the Collaborator are described in section 3.
- The manager, i.e a physical person who checks the identity of the signatories, and enters their identity information in Woleet.ID Server, a software application edited by Woleet and hosted by the Service Consumer. The manager is generally related to the Service Consumer by an employment contract. The manager is hereinafter defined as the "Manager". The detailed obligations of the Manager are described in section 4.
- The administrator, i.e a physical person who is in charge of managing the installation and the configuration of the electronic signature service for the Service Consumer. The administrator is generally linked to the Service Consumer by an employment contract. The administrator is described hereinafter as "The Administrator". The detailed commitments of the Administrator are described in section 5.
- The user, i.e a physical person who electronically signs a document provided by the Service Consumer using Woleet service. This person may be related to the Service Consumer by an employment contract, or by a commercial agreement. Woleet user is hereinafter defined as the "User". The detailed obligations of the User are described in section 2.
- The third party, i.e. any entity interacting with Woleet service in any manner. It may be an entity wishing to verify the validity of signatures made using Woleet services, so as to be sure of the integrity of the signed data, the date of the signature(s), and the identity of the signatory(ies). It may also be an entity using Woleet open source code to create signatures in their own way. A third party is hereinafter defined as "The Third Party". The detailed obligations of the Third Party are described in section 7.

1. Conditions for using the electronic signature and seal services

1.1 Presentation of the services

The electronic signature and seal service is a combination of a SaaS service and of a software specifically developed by Woleet, called Woleet.ID Server, hosted by the Service Consumer.

More precisely:

- Via the Woleet API, the Service Provider allows to create electronic signature requests, to authenticate the signatory, to get signatures and seals, and to create proofs of existence of the signatures and seals, as explained in the following paragraphs.
- The Service Consumer hosts a software provided by Woleet, called Woleet.ID Server, with a database containing notably the identity information of the users, and the related signature keys.
- If the private keys are not held by the signatories (via a compatible physical hardware like Ledger, or via the mobile application Woleet.ID Mobile), they are created and used to sign by Woleet.ID Server.
- Otherwise (if the private keys are created in a mobile or a Ledger), it is possible to register a public key in Woleet.ID Server and to link it to an identity (see Enrolment).
- The identity information of the Users or the organization name (in case of a seal) is associated to the signature or seal in the signature proof receipt, allowing the identification of the signatory(ies), and the identification of the organization that has signed, in case of a seal.

1.2 Access to the electronic signature and seal services

Within the terms of a contract between Woleet and its customer (the Service Consumer), access to Woleet's electronic signature and seal services is granted either via the integration of Woleet API, or via a web application, called ProofDesk, hosted by Woleet.

In the case of API integration, Woleet delivers an API token to the Service Consumer, so as to authenticate the requests coming from the Service Consumer.

If the web application ProofDesk is used, collaborators must create an account (email required and password setting) to be able to make electronic signature requests.

Users are not required to create an account to proceed with the electronic signature.

1.3 Pre-requisites before creating electronic signatures and seals

1.3.1 Case of electronic signatures

1) Each electronic signature requires the use of a key pair, generated with algorithms of asymmetric cryptography. The key pair can be generated in several media:

- On a smartphone, by using a dedicated mobile application made by Woleet called "Woleet.ID Mobile Edition".
- On a cryptographic token supported by Woleet (e.g. Ledger Nano S), and using the embedded Woleet application called "Woleet.ID Ledger Edition".
- On Woleet.ID Server, a Woleet software solution that is hosted by the Service Consumer.

Key pairs created apart from a Woleet tool can also be used if they are compatible with Woleet pre-requisites regarding key type and size and signature algorithm.

In case the key pair is stored on the mobile or on a Ledger, it must be protected by a secret allowing to create and restore backups of this key. This secret shall comply with BIP-0039 norm (see https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki), i.e the secret shall be composed of 12 words to be chosen by the User.

2) If not pseudonymous, the electronic signature provides identity information of the signatory. For physical persons, the identity information includes at least a full name, and an email address, and may also contain a telephone number, a business role, and a related organization. This information shall be entered in the database of Woleet.ID Server by a Manager, before proceeding with any electronic signature. Pseudonymous signatures identify the signatory via a Bitcoin address only.

1.3.2 Case of electronic seals

1) Each electronic seal requires the use of a key pair, generated with algorithms of asymmetric cryptography. The key pair must be generated in Woleet.ID Server.

2) The electronic seal provides identity information of the organization issuing the sealed data. The identity information contains at least the name of the entity or organization, the department or service, and the country of origin of the organization.

1.4 Signature request (for electronic signatures)

In case of signature of natural persons, a signature request may be made by a Collaborator to request that one or multiple Users be able to sign the data or the document.

The signature request, when identifying a signatory, shall at least indicate:

- A signature request name;
- The data or document to be signed;
- The identification of the signatory(ies) (being at least email address, or Bitcoin address).

The signature request can also indicate a deadline for the signature to be made.

The creation of a signature request for physical persons leads to the creation of one or several URL(s) to a signature page, depending on the number of signatory(ies).

These URLs are dedicated for each signatory who has been mentioned in the signature request. They are sent by email to the signatories if their email is known.

1.5 Signature by physical persons (electronic signatures)

The User shall go to the URL mentioned in the signature request.
The User can check the integrity of the data or document to be signed.
The User shall authenticate himself so as to confirm their identity information. Email confirmation, password, OTP sent by SMS and the use of a personal device (mobile phone, Ledger) are supported authentication methods.
The acceptation of the present TCU are required to create an electronic signature.
The User can cancel the signature for any reason.

1.6 Validation of electronic signatures and seals

Any electronic signature provided by Woleet can be checked using a validation page provided by Woleet following proof creation. In the case of signatures made by physical persons, the URL of this validation page is sent to the User and to the Collaborator following signature creation. In the case of seals, it is recommended that the Service Consumer includes in the original document a mention of the validation service, so as to inform of the existence of a validation tool.

The signature or seal validation page displays all the details regarding the signature or seal, including:

- The identification of the signed document or data, and the possibility to verify that this data corresponds to the data known by the verifier (via an integrity check function);
- The signatory's identity information;
- The identification of the organization having verified the signatory's identity;
- The signature proof with a timestamp corresponding to the date of the block in which the signature was anchored;
- The status about the validity of the proof and related details (location in Bitcoin blockchain etc.);

- The status about the validity of the signature (depending notably on the revocation or expiration of key);
- In case of seals, the status concerning the possession of the private key by the related organization.

Woleet documents a validation policy for advanced electronic signatures and seals, so that independent verifiers can be implemented.

The elements required to validate a signed document are at least the original document, and the signature proof receipts.

In the case of advanced electronic signatures, the signed audit trail shall be used to check that the signature process was done in conformity with Woleet Signature Policy.

1.7 Protection of signature keys and revocation

Signature keys are critical data as they allow for the signature, thus making the User's or the organization accountable. The keys need to be protected so as to avoid theft, usurpation or loss. Woleet provides security measures adapted for the protection of the key (Mobile, Ledger or Woleet.ID Server).

Keys created on Woleet.ID Server and linked to the identity of a physical person can be « one-shot keys », i.e. these keys can only be used for a given signature request. After the signature is made, the private key is deleted.
In case of suspicion regarding the security of the key(s), the User can revoke a key by connecting to Woleet.ID Server, or by contacting a Manager, provided that either the private key is stored by Woleet.ID Server or the public key is registered in Woleet.ID Server. The key will definitively be blocked. The revoked status of the key and the revocation date will be visible on the signature validation page.

To limit the risks of misuse of the keys that are not « one-shot » (for example, keys used to create seals), it is possible to set an expiration date.

1.8 Enrolment (for electronic signatures)

It is possible to enroll a key that was not generated by Woleet.ID Server, including keys generated by Woleet.ID Mobile or Ledger, or even a key generated with another tool (as long as it is compatible with Woleet criteria concerning signature keys).

Enrolment means checking User identity information, checking the possession of a private key and registering the related public key in Woleet.ID Server database. In any case, the private key remains under the control of the User (on his/her mobile or on a Ledger).
Enrolment allows to associate identity information to a signature key, so that this identity information can be associated with the electronic signature.

An enrolment invitation email is sent by a Manager to a User. The enrolment consists in confirming identity information and signing the present TCU. Different levels of authentication (including email verification and OTP) can be required from the User.

2.Terms applicable to the Users

1. The User commits to comply with the present TCU.
2. The User commits to comply with the security policy of the password protecting the use of his/her signature keys, and to keep this password confidential. This password allows to keeping the signature key under his/her sole control.
3. In the case the User holds signature keys (on his/her mobile or on his/her Ledger), the User commits to take care of his/her keys, so as to avoid endanger, theft or loss of the key(s). These incidents would affect the validity of the electronic signatures made using these keys.
4. Any suspicion that the signature key may be compromised shall lead to revocation, if the key is not already expired. Revocation can be done either by the User or by the Manager.
5. The User commits to check his/her identity information at the time of signing so as to ensure they are accurate.
6. The User commits to keep the signature receipts sent by Woleet following signature creation. The signature receipt, along with the original document that was signed, may be required to check the existence and the validity of any electronic signature.

3. Terms applicable to the Collaborators

1. The Collaborator commits to respect the present TCU.
2. The Collaborator has access to identity information (in particular, telephone number, email) of the Users, which may be confidential information, and commits not to breach or attempt to breach their confidentiality.
3. The Collaborator commits not to use identity information of Users for any other purpose than creating a signature request.
4. The Collaborator commits not to create signature requests for unjustified or malicious purposes.

4. Terms applicable to the Managers

1. The Manager commits to respect the present TCU.
2. The Manager can create and modify the identity information (in particular, telephone number, email) of the User(s) in Woleet.ID Server. The Manager shall not breach their confidentiality.

3. If they are in charge of verifying the identity of the Users account they are creating in Woleet.ID Server, the Managers must comply with the identity verification procedure of their organization (i.e. the Service Consumer).
4. The Manager commits not to create false identities neither to usurp someone's identity. In particular, the organizations referred to in seals shall not be different from these of the Service Consumer.
5. The Manager should not be technically able to create signature requests with Woleet tools so as to avoid identity usurpation.
6. The Manager shall not abusively revoke a key: in particular revocation shall be required by the User or by circumstances putting the security of the key at risk.

5. Terms applicable to the Administrators

The Administrator is in charge of installing and configuring Woleet.ID Server, the software component that is hosted by the Service Consumer. In particular the Administrator has access to the database containing the user accounts and the signature private keys.

1. The Administrator commits to respect the present TCU.
2. The Administrator shall not breach the confidentiality of the identity information of the User database.
3. The Administrator shall neither compromise the signature keys nor use them for any reason.
4. The Administrator shall not abusively delete any data, including identities, signature keys, or logs.

6. Terms applicable to the Service Consumers

The terms applicable to the Service Consumer are further described in the TCU.

7. Terms applicable to Third Parties

Third Parties may be interested in validating signatures made via Woleet services.

1. Any entity wishing to validate a signature made by Woleet can use Woleet Signature and Validation Policies.
2. Any entity is free to use Woleet open source code. Though, Woleet does not commit responsibility on the validity or eIDAS conformity of electronic signatures or seals that do not respect the Signature and Validation Policies issued by Woleet.

8. Definitions

Some of the following definitions are directly taken from eIDAS European Regulation n°910/2014.

- **API**: Application Programming Interface. Interface published and documented by a service provider allowing consumers to use the service.
- **Asymmetric key pair**: set of private and public keys that are generated together with an asymmetric cryptographic algorithm so as to be uniquely related. The private key allows to sign while the public key allows to verify the signature.
- **Authentication**: « means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed », according to eIDAS.
- **Bitcoin address**: public key that was encoded using Base58Check format. Bitcoin addresses are notably used to identify the senders and the recipients of Bitcoin transactions.
- **Cryptographic hash**: result of a hashing function applied to a data, allowing to prove its integrity. The hash is unique for the data. A hash alone cannot reveal the original data. Any modification of the original data would lead to a very different hash.
- **Cryptography**: practice and study of techniques for securing communication in the presence of third parties. Such techniques include data confidentiality, data integrity, authentication and non-repudiation. Cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary.
- **Data integrity**: property of a data that has not been modified. The integrity, or non-modification of the data can be proven via a cryptographic algorithm called hashing function.
- **Electronic seal**: « data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity », according to eIDAS.
- **Electronic signature**: « data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign », according to eIDAS.
- **Enrolment**: procedure that binds a signature key that was not generated in Woleet.ID Server (for example, key created in a mobile or in a Ledger) with the identity of a Signatory. This allows to attach identify information to signatures made with such keys. See dedicated section for more details.
- **Identity URL**: an URL published by Woleet.ID Server contributing to the validation of an electronic signature or seal.
- **Key holder**: the key holder is the person or entity that is uniquely linked to a signature key. The key holder is a signatory.
- **Non-repudiation**: property of electronic signatures when the signatory cannot deny the validity of the signature.
- **Pseudonymous signature**: property of an electronic signature that does not identify a physical person by his/her real name, but by a pseudonym.
- **Revocation**: security procedure that definitively blocks a signature key, upon request of the user or manager. This information is published by Woleet.ID Server. A signature cannot be done with a revoked key. See dedicated section for more details.
- **SaaS**: Software as a Service. Software service hosted by a provider and remotely accessible by its customers.

- **Signatory**: can be either a physical person or an organization in case of seals. The signatory uses a signature key to create electronic signatures or seals.
- **Signature key**: private key in an asymmetric key pair that allows to create an electronic signature. In Woleet service, a private key is uniquely linked to a signatory. A private key is confidential and shall be kept under the control of the signatory.