If Mobile
Terms of Use

Table of Contents

I hereby confirm that:

- I have read and agree to If Mobile Terms and Conditions;
- I will keep If Mobile security code (PIN code) under my sole control and will immediately change it in case it might become or becomes known to another person.

Summary

This document describes the If Mobile Terms of Use, limitations of use, the rights and obligations of the parties, the procedure for providing the service and the security measures.

Document identification

The object identifier (OID) for this document is: 1.3.6.1.4.1.51321.1.1.1.2

2022.03.31

Version 02

Identifier description:

1.3.6.1.4.1.51321.x.y.z.q

1.3.6.1.4.1.51321 - organization identifier - If P&C Insurance AS;

x - country identifier, possible values - .1 – Estonia, .2 – Latvia, .3 – Lithuania;

y – product identifier, possible values - .1 – If Mobile;

z – document identifier, .1 – Terms of Use, .2 – Certificate Profile;

q – document version number.

1. Definitions

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.

User - natural person with legal capacity who uses the If Mobile services.

Electronic Signature - electronic data that is attached to the electronic document or is logically associated with it, and which the signer uses to sign the document.

Advanced Electronic Signature - electronic signature that meets the requirements of Article 26 of eIDAS.

Certificate - public key with additional information that is defined in the Certificate Profile, has been rendered non-falsifiable with encryption, using a private key issued by the Certificate Authority.

Personal identification data - set of data that allows establishing the identity of a natural or legal person.

Electronic identification - process of using electronic personal identification data that allows confirming the identity of a natural or legal person in a unique way.

Authentication - electronic process that allows electronic identification of a natural or legal person.

Authentication Certificate - electronic confirmation, certificate, that is used for authentication or encryption.

Electronic Signature Certificate - certificate that associates the electronic signature validation data with a natural person and confirms at least the name of this person.

Signer - natural person who creates the electronic signature.

Electronic document - any content that is stored in an electronic format, in particular text, sound, visual or audio-visual record.

Validation - verification and confirmation of the validity of an electronic signature.

Electronic signature creation device - configured software or hardware used for creating an electronic signature - a secure area of memory of the mobile device that is protected from unauthorized access and duplication.

Certificate Authority - Latvijas Valsts radio un televīzijas centrs VAS (Latvian State Radio and Television Centre State Joint-stock Company), reg. No. 40003011203, which issues certificates for use in the If Mobile application and ensures the verification and cancellation of issued certificates.

Certificate Policy - a document of the Certificate Authority that defines the procedural and operational requirements that the Certificate Authority adheres to when issuing and managing If Mobile certificates.

If Mobile - software package that is provided and maintained by If and is intended for use in a mobile device, and that provides the User with the means for authentication, encryption and signing electronic documents with advanced electronic signature in connection with insurance services.

Identity Provider - organization that provides means of electronic authentication and is responsible for determining the true identity of the person, for creating the electronic identity of the person and confirming it to the Registration Authority, for example, a credit institution.

OCSP - online certificate status protocol.

PIN code - activation code for the private key that corresponds to the authentication Certificate, and for the private key that corresponds to the electronic signature certificate.

Private key - the key from the key pair that must be kept confidential by the User of the key pair, and is used to create electronic signatures and/or decrypt electronic records or files that are encrypted with the corresponding public key.

Public key - the key from the key pair that the User of the corresponding private key may publicly disclose and that is used by third parties in order to verify electronic signatures that have been created with the corresponding private key of the User, and/or to encrypt messages in such a way that they could only be decrypted with the corresponding private key of the User.

Third party - person who relies on the information included in the Certificate, including electronic signatures and electronic identification.

If - If P&C Insurance AS, registered in the Commercial Register of the Republic of Estonia with the reg. No. 10100168), as well as its branches in Latvia and Lithuania: If P&C Insurance AS Latvian branch, unified registration No. 40103201449 in the Commercial Register of the Republic of Latvia, and If P&C Insurance AS filialas, registration No.4302279548 in the State Enterprise Centre of Registers of the Republic of Lithuania.

If Group - all together or each separately - If P&C Insurance AS (Estonia, Reg. No. 10100168) and its branches, If Skadeförsäkring Holding AB (publ) (Sweden, Reg. No. 5562417559) and its branches, If Skadeförsäkring AB (publ) (Sweden, Reg. No. 5164018102) and its branches.

If Mobile account - account that is registered by the User in the If Mobile application and that is required in order to use the If Mobile services, and that associates the If Mobile application instance with the User identity. During registration of the If Mobile account, the User proves his/her

identity to If with the help of the Identity Provider, and the Certificate Authority, on the basis of the Certificate request from If, confirms the link between that identity and the User key pairs. The If Mobile account has an advanced electronic signature key pair and an authentication key pair.

If Mobile service - authentication service, electronic document advanced electronic signature service, insurance service or other service associated with insurance and provided with the mediation of If Mobile.

If Mobile certificates - authentication and advanced electronic signature Certificates created for the User as a result of registering the If Mobile account.

Certificate Profile - requirements regarding the Certificate content.

Registration Authority - organization that is responsible for verification, registration and administration of the User identity according to

ETSI EN 319 412-1 v1.3.4 (2020-03), Electronic Signatures and Infrastructures (ESI) Certificate Profiles; Part 1: Overview and common data structures
and
RFC 3647 (November 2003), Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

2. Document versions

Version history
Date - 2021.03.31
Version - 01
Changes - initial version

Date - 2022.03.31
Version - 02
Changes - editorial changes

3. General Terms

3.1. These Terms regulate the provision of If Mobile services to the User, as well as the procedure for their use, and constitute a part of the legally binding contract between the User and If.

3.2. The User must read and agree to the Terms as a precondition to using the If Mobile services. Applying for receipt of the Certificate is assumed to be an agreement of the User to the Terms and a confirmation for signing the contract.

3.3. If shall have the right to unilaterally amend the Terms at any time by publishing them in If Mobile. If the User does not agree to such amendments, the User shall have the right to unilaterally terminate the contract for using If Mobile. If shall publish the current version of these Terms on the website of If or If branch.

3.4. The User may apply for If Mobile only in person. An If Mobile account cannot be created by a representative.

3.5. The If Mobile electronic signature meets the requirements for advanced electronic signatures defined in Article 26 of eIDAS:

3.5.1. The If Mobile electronic signature is uniquely linked to the signer;

3.5.2. The If Mobile electronic signature is capable of identifying the signer;

3.5.3. The If Mobile electronic signature is created using electronic signature creation data that the signer can, with a high level of confidence, use under his/her sole control;

3.5.4. The If Mobile electronic signature is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

4. Identification

4.1. If verifies the identity of the User and confirms that the certificate request is precise, authorized and complete in order to confirm the identity of the User.

4.2. Prior to issuing the User certificate, If collects, verifies and stores proof of the User's identity from relevant authorized sources, as well as includes this proof or reference to it in the User Certificate. If stores this proof for the entire term of validity of the Certificate and 5 years after its expiration.

4.2.1. The identity of the User is proved on the basis of information obtained from the Identity Provider and allows unmistakable distinguishing of the User from other persons.

4.3. If verifies and includes in the Certificate the following information about the User:

4.3.1. User's first name and surname;

4.3.2. User's personal identification number;

4.3.3. The mobile phone number indicated by the User and controlled by the User.

5. Receiving the certificate

5.1. If carries out the functions of a Registration Authority.

5.2. The User applies for the Certificate through If, using the If Mobile application.

5.3. If verifies the identity of the User as follows:

5.3.1. If verifies the identity of the User on the basis of the User authentication results from the Identity Provider;

5.3.2. The User applies for receiving the Certificate only after successful authentication with the Identity Provider, using the If Mobile application;

5.3.3. If verifies whether the User is reachable through the indicated mobile phone number, by sending a single-use code with a limited period of validity that the User must enter in the If Mobile application during the registration process;

5.4. After successful completion of all verifications in the registration process, the following consecutive steps must be taken:

5.4.1. The User must agree to the If Mobile Terms of Use;

5.4.2. The If Mobile User Certificates are issued only on the basis of If requests to the Certificate Authority that are drawn up according to the If Mobile Certificate Profile.

5.4.3. The registration process ensures that the private key, which corresponds to the public key used in the Certificate application, is controlled by the User only;

5.4.4. The Certificate Authority accepts applications that comply with the If Mobile Certificate Profile from If only;

5.4.5. The Certificate Authority issues the User Certificate only if the Certificate application complies with the technical requirements that are defined in the If Mobile Certificate Profile and in the contract signed by If and the Certificate Authority;

5.4.6. The If Mobile Certificate for the User is created according to the description included in the If Mobile Certificate Profile.

5.4.7. Upon receiving a new If Mobile Certificate, the previous If Mobile Certificates issued to the User are revoked;

5.4.8. The Certificate Authority notifies If about issuing a User Certificate or the refusal to issue it;

5.4.9. If notifies the response from the Certificate Authority to the User. The Notification of issuance confirms the delivery of the Certificate to the User. The Notification of refusal confirms that the Certificate has not been issued to the User.

6. Type and use of the Certificate

Type and use of the Certificate

The If Mobile electronic signature certificate is used for creating advanced electronic signatures complying with eIDAS.

The applied and published certificate policy

The certificate policy of the issuer of advanced signature certificates is published in

https://www.eparaksts.lv/repository,
OID: 1.3.6.1.4.1.32061.2.4.1

Type and use of the Certificate

The If Mobile authentication Certificate is used for authentication and encryption.

The applied and published certificate policy

The certificate policy of the issuer of authentication Certificates is published in

https://www.eparaksts.lv/repository,
OID: 1.3.6.1.4.1.32061.2.4.1

6.1. If Mobile Certificates may only be used for:

- Signing electronic documents with advanced electronic signature in accordance with eIDAS (only the electronic signature certificate),
- Authentication (only the authentication Certificate),
- Encryption (only the authentication Certificate),

in order to receive insurance services from the If Group, to receive insurance-related services from the If Group or Partners (as defined by If), or to provide services to the If Group.

6.2. User Certificates may not be used for any other purpose, including for:

6.2.1. Illegal activities (including cyber-attacks and attempts to change the If Mobile certificate);

6.2.2. Issuing new or derived certificates and information regarding certificate validity;

6.2.3. Tests and experiments that can result in consequences to the User or other persons;

6.2.4. Automated use of issued Certificates, that is, without the participation of the corresponding person in the actions of signing, authentication or decryption;

6.3. User Certificates may not be used if the private key has come at the disposal of another person or has been transferred to another person.

6.4. The User authentication Certificate may not be used to create advanced electronic signatures in compliance with eIDAS.

7. Certificate term of validity

7.1. The Certificate is issued with a term of validity of 3 years.

7.2. The Certificate comes into force on the date and at the time indicated in the Certificate, which the User may check in the If Mobile application.

7.3. The validity of the Certificate expires on the last day of the term of validity indicated in the Certificate, or if the Certificate is revoked.

7.4. Audit logs are stored on site at least for 7 years after the end of the certificate term of validity or after it is revoked. Physical or digital archive records regarding certificate applications, registration information and requests or applications for revoking are stored at least for 7 years after the end of the certificate term of validity.

8. Revoking the certificate

8.1. The User may unilaterally revoke his/her Certificate at any time during the term of validity of the Certificate by deleting his/her profile in the If Mobile application or by submitting a written application to If.

8.2. The revoking of one Certificate issued to the User is automatically applied to all If Mobile certificates issued to the User on the same device.

8.3. After receiving the request for revoking the certificate, If immediately terminates the validity of the Certificate.

8.4. The validity of a revoked Certificate may not be restored. In order to resume work with If Mobile, the User must apply for a new Certificate.

8.5. If shall have the right to revoke the User Certificate in the following cases:

8.5.1. The User applies for revoking the Certificate;

8.5.2. The User has blocked the PIN code by entering it incorrectly 5 times in a row;

8.5.3. If has obtained information that the User has lost control over his/her private keys or PIN codes used in the If Mobile application;

8.5.4. If has obtained proof that the User's private key that corresponds to the public key used in the Certificate has been compromised or no longer meets the requirements;

8.5.5. If has obtained proof that the Certificate has been used not in accordance with its intended purposes;

8.5.6. If has obtained information that the User had violated these If Mobile Terms of Use;

8.5.7. If has obtained information about changes in the facts of the information included in the Certificate;

8.5.8. If has obtained information that the Certificate has been issued in violation of the Certificate Policy, the If Mobile Certificate Profile or these If Mobile Terms of Use;

8.5.9. If has found out that any information included in the Certificate is inaccurate or misleading;

8.5.10. If terminates provision of If Mobile and the Certificate Authority does not provide revoking of the Certificates;

8.5.11. The rights of If to issue Certificates have been suspended or terminated, with the exception of cases when If continues to ensure the operation of the OCSP repository or CRL;

8.5.12. If has obtained information that the private key of the Certificate Authority used for issuing the Certificate has been compromised;

8.5.13. If has obtained information that the User has died or lost legal capacity;

8.5.14. The Certificate Policy stipulates the need for revoking;

8.5.15. The technical content or format of the Certificate poses significant threat to the User, If, or any Third person.

8.5.16. If no longer uses in the If Mobile application the services of the Identity Provider that provided the information on the basis of which the Certificate was issued.

9. Other actions with the Certificate

9.1. The following actions may not be carried out in connection with the User Certificate:

9.1.1. Changing information included in the Certificate;

9.1.2. Correcting errors in the information included in the Certificate;

9.1.3. Temporarily suspending its validity in order to restore it later;

9.1.4. Changing the key pair associated with it.

If it is necessary to carry out any of these actions, the User must revoke the valid Certificate and apply for a new one.

10. Rights and obligations of the User

10.1. The User shall have the right:

10.1.1. To submit an application for issuing an If Mobile Certificate in the If Mobile application;

10.1.2. To use the Certificate for receiving the services defined in clause 6.1;

10.1.3. The right to request that If revokes the Certificate on request of the User in the cases defined in the Terms;

10.2. The User has the following obligations:

10.2.1. To comply with the Terms;

10.2.2. To use his/her private key and Certificate in compliance with the Terms, including the applicable documents listed in Clause 16, as well as the legislation of the Republic of Estonia currently in force;

10.2.3. To ensure that the User's private key does not pass into the hands of other parties, including through the transfer of the mobile device and PIN codes to other parties;

10.2.4. To notify If immediately regarding the possibility of unauthorized use of the private key and to revoke his/her Certificate, including in cases when the User has lost control over his/her private key or PIN code;

10.2.5. To provide correct and true information in the If Mobile application;

10.2.6. To notify If regarding change of personal data, revoking a Certificate with obsolete data and applying for a Certificate with updated data.

10.2.7. Not to use If Mobile if the instructions, restrictions or security measures of the manufacturer of the device are being ignored, including using If Mobile on "jailbroken" or "rooted" devices.

11. Rights and obligations of If

11.1. If has the following obligations:

11.1.1. To provide the certification service in accordance with these Terms, eIDAS requirements regarding the Advanced Electronic Signature, the Certificate Policy, as well as the legislation of the Republic of Estonia currently in force;

11.1.2. Taking into account the state of technology, costs of implementation and nature, volume, context and purposes of data processing, as well as risks of various probability and severity in connection with the rights and freedoms of natural persons created by the provision of If Mobile services, If shall implement appropriate technical and organizational measures in order to ensure the safety of data during provision of If Mobile services;

11.1.3. Not to store the PIN codes that the User has entered in any of the environments controlled by If, including the If Mobile application;

11.1.4. To ensure that the certification keys used for the certification service are activated on the basis of shared control;

11.1.5. To ensure the possibility of verifying the validity of certificates with the involvement of the Certificate Authority;

11.1.6. To ensure the conformity of the issued Certificate to the Certificate Profile, using the information that the User and the Identity Provider have provided.

11.1.7. To comply with the procedure for generating and storing the key in accordance with the Certificate Policy and the eIDAS requirements regarding the Advanced Electronic Signature;

11.1.8. To assess the quality of the information about identity provided by the Identity Provider, and to ensure its sufficiency for using in the If Mobile application for its intended purposes.

11.2. If shall have the right:

11.2.1. To cease using the information about identity provided by the Identity Provider in the If Mobile application if the quality of this information is insufficient;

11.2.2. To revoke Certificates in the cases defined in the Terms.

11.2.3. Refuse If Mobile services on User devices if the instructions, restrictions or security measures of the manufacturer of the device are being ignored, including if using If Mobile on "jailbroken" or "rooted" devices.

12. Rights and obligations of third parties in connection with verifying the certificate status

12.1. Third parties shall have the right to verify the validity of a Certificate:

12.1.1. By using the OCSP service for the verification of certificate status;

12.1.2. By submitting a written application to the Certificate Authority;

12.1.3. If the proof of Certificate validity attached to the Certificate or the electronic signature is insufficient, the third party shall verify the validity of the Certificate on the basis of the Certificate validation services that If offers at the time of using the Certificate or attaching the electronic signature.

12.2. The third party shall comply with the limitations defined in the Certificate and shall verify that the accepted transaction complies with these Terms and the Certificate Policy.

12.3. The third party shall validate the identity from the If Mobile Certificate against the personal information that is known to the third party.

12.4. The third party may not allow minors to use If Mobile in providing its services.

12.5. If ensures the availability of certificate status services 24 hours a day, 7 days a week, with at least 99% total availability per year, with planned downtime that does not exceed 1% a year.

12.6. If offers the OCSP service for verifying the Certificate status provided by the Certificate Authority. The service is available through the HTTP protocol.

12.7. If offers OCSP with the following possibilities of verification:

12.7.1. The OCSP service is provided free of charge and is publicly available on the site http://ocsp.eparaksts.lv;

12.7.2. The URL of the OCSP service is included in the certificate field "Authority Information Access" (AIA) according to the Certificate Profile.

13. Partners

13.1. A partner is a third party or institution that has a valid written contract signed with If regarding the use of If Mobile for one or several of the following purposes (hereafter – Purposes):

- User authentication
- Providing services to the User
- Encrypting information for the User

13.2. If shall ensure that the Partners only use If Mobile for the Purposes defined in these Terms, in compliance with limitations defined in clause 6.1.

14. Requirements for the Certificate Authority

14.1. If shall ensure that the Certificate Authority and its operations comply with the following requirements:

14.1.1. The premises where the certificates are generated and revoked are protected from unauthorized and unregistered physical access;

14.1.2. The equipment used for generating and revoking certificates is protected from negative impacts of physical events – fire, flood, electricity outages, telecommunication disruptions, theft, malicious or accidental destruction, natural disasters, break-ins;

14.1.3. Measures have been implemented that prevent unauthorized turning off, removal from protected premises, theft or destruction of devices, information, storage media, software;

14.1.4. Ensures the backup of information and systems required for its operation as the Certificate Authority and for restoring its activity, the regular saving of backup copies, the safety of this storage and the possibility of restoring activity using such copies. Authorized and reliable personnel shall be hired for these activities;

14.1.5. A business continuity plan has been developed, implemented and maintained that allows restoring the activity of the Certificate Authority in the case of losing, compromising or potentially compromising its private keys. The plan must include actions connected with this incident:

14.1.5.1. The possibility to revoke all User certificates;

14.1.5.2. Notification of all Users and If regarding the incident;

14.1.5.3. Revoking all certificates issued by the Certificate Authority that are subordinate to the certificate that has caused the incident;

14.1.6. The Certificate Authority generates its private keys in a safe environment and maintains their secrecy:

14.1.6.1. The generation of private keys in a physically protected environment and a high security network environment is carried out by reliable and authorized personnel, reducing its number to the minimum required, but not less than two persons who can only generate the key together. Each person participating in the generation of the Certificate Authority keys uses multifactor authentication for this activity;

14.1.6.2. Keys are generated using algorithms that are appropriate for current security risks and that ensure compliance with eIDAS requirements regarding advanced electronic signature;

14.1.6.3. Prior to the expiry of the term of validity for the Certificate Authority's certificates used for generating User certificates, the Certificate Authority shall, in a timely way, generate and introduce a new certificate that will be used for generating User certificates in order to ensure uninterrupted fulfilment of the functions of the Certificate Authority. Such actions must be notified to If in a timely way and the actions must be executed a sufficient period of time in advance in order to allow If and other parties to adapt their operation and information systems to such changes and thereby ensure the continuity of services provided to the Users.

14.1.6.4. After introducing a new certificate of the Certificate Authority, the Certificate Authority shall notify If and confirm with the signature of its manager the successful completion of the key generation ceremony of the Certificate Authority, confirming that it has been carried out according to the defined procedure, that it was implemented only by reliable and authorized persons, that the confidentiality and integrity of the key pair was ensured, that the public keys of the generated key pairs are publicly available, that the private keys of the generated key pairs are stored and used in safe encryption devices and are protected with technical, physical and organizational means according to the risk level, that all the private keys previously used by the Certificate Authority for generating User certificates have been destroyed.

14.1.7. Only reliable and authorized personnel has access to the root private key of the Certificate Authority that is used for signing subordinate certificates of the Certificate Authority;

14.1.8. The Certificate Authority notifies all Users and If when any of the algorithms used becomes inappropriate for its purpose, and plans the revoking of the impacted certificates in cooperation with If;

14.1.9. There is no single person that could sign the subordinate certificates of the Certificate Authority independently, control of signing is carried out by at least two reliable and authorized employees.

14.1.10. All of the following security incidents connected with issuing and revoking certificates are registered: turning systems on and off, operational errors, equipment faults, communication faults, certificate registration and revoking requests, data of such requests and resulting answers, User certificate life cycle events, root key life cycle events;

14.1.11. When receiving and processing User data, its confidentiality and integrity is ensured, this data is used only for executing the functions of the Certificate Authority;

14.1.12. Any certificates intended for testing include clear and unambiguous tags noting the purpose of testing, for example, in the name of the User;

14.1.13. The Certificate Authority is independent from other organizations in regard to implementation of its Certificate Authority functions: generation, revocation and verification of User certificates. In implementing these functions, the Certificate Authority and its management are not subject to commercial, financial, political or other pressure that could form a basis for questioning the reliability of its services.

15. Responsibility and its limitations

15.1. The User shall be responsible for storing, maintaining and using his/her private key.

15.2. The User shall be fully responsible for any consequences of authentication and use of the Electronic signature, using his/her Certificates, both during their term of validity and afterwards.

15.3. The User shall be responsible for any damage caused due to non-fulfilment or insufficient fulfilment of User's obligations indicated in current terms and conditions.

15.4. The User understands that the Electronic signatures issued on the basis of the Certificates that are no longer valid or have been revoked are not valid.

15.5. The User is responsible for any damage caused in case If Mobile is used on the device while ignoring the instructions, restrictions or security measures of the manufacturer of the device, including if using If Mobile on "jailbroken" or "rooted" devices.

15.6. The User must use his/her chosen additional PIN code that is known only to him/her to confirm the Advanced Electronic Signature each time it is attached to electronic data. The entering of this additional PIN code for confirming actions is assumed to be the agreement of the User to the corresponding action and is required for instantaneous creation of the User's Advanced Electronic Signature and its attachment to the electronic data displayed to the User.

15.7. In case of interruptions in the provision of certification services, If shall notify all Users in a timely manner and shall maintain documentation and information regarding the interruption of the certification services for at least 7 years after the interruption of the certification services.

15.8. If shall not be financially responsible for information included in the If Mobile Certificates. In any case If shall not be responsible for indirect damages caused to the User or to third parties, including for loss of earnings.

15.9. If shall not be responsible for damages to the User or to third parties that have been caused or are connected with:

15.9.1. The secrecy of the User's private keys, incorrect use of the Certificates or incorrect verifications of the certificates, or for incorrect decisions of third parties or any consequences arising from errors or shortcomings in the certificate validation checks;

15.9.2. The non-fulfilment of the obligations of If in case such non-fulfilment has been caused by the faults or security problems of supervision authorities, data protection supervision authorities or any other state authorities;

15.9.3. The inability to carry out obligations if it is caused by force majeure circumstances.

16. Applicable documents

16.1. The use of If Mobile is regulated by the following documents:

16.1.1. [1] The Certificate Policy that is published in https://www.eparaksts.lv/repository;

16.1.2. [2] The If Mobile Certificate Profile that is published in https://www.if.ee/if-mobile#dokumendid;

16.1.3. [3] These Terms;

16.1.4. [4] ETSI EN 319 412-1 v1.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI) Certificate Profiles; Part 1: Overview and common data structures;

16.1.5. [5] RFC 3647 (November 2003), Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;

16.1.6. [6] 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;

16.1.7. [7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

16.1.8. [8] The If insurance privacy protection policy, https://www.if.ee/isikuandmed

16.1.9. Other legal acts.

17. Protection of information and privacy

17.1. In processing personal information and registration information, If complies with the General Data Protection Regulation and other legislation in force in the Republic of Estonia.

17.2. The User has been notified and agrees that his/her personal data, which has been defined in the If Mobile Certificate Profile, will be transferred to the Certificate Authority for inclusion in the User Certificate, as well as for administration of this Certificate according to these If Mobile Terms of Use.

17.3. The User has been notified and agrees that, during authentication or encryption, the person who carries out identification or encryption is sent the User's authentication Certificate included in the User's If Mobile and containing the User's first names, surname, personal identification number and mobile phone number.

17.4. The User has been notified and agrees that the User's If Mobile Electronic Signature Certificate is attached to his/her signed documents, is inseparably associated with them, contains the first names, surname, personal identification number and mobile phone number of the User, as well as that this information becomes available to the recipients of the signed document.

17.5. If shall have the right to use the information received for offering and providing If Group insurance services or the services of Partners defined by If and connected with insurance, as well as for receiving services.

17.6. Any information that has become known during the provision of services and is not intended for disclosure (for example, information that has become known as a result of managing and providing If Mobile certification services) is confidential. The User shall have the right to obtain information from If regarding himself/herself in accordance with the law.

17.7. Through reasonable and proportional technical and organizational security measures, If protects confidential information and information intended for internal use, prevents it becoming compromised and prevents its disclosure to third parties.

17.8. If shall have the right to disclose information about the User to a third party that has the right to receive such information in accordance with the law.

18. Applicable legislation and dispute resolution

18.1. If provides If Mobile services in accordance with the legislation currently in force in the Republic of Estonia.

18.2. The If Mobile certification service complies with trust service requirements described in eIDAS in regard to the Advanced Electronic Signature.

18.3. Any disputes between the parties shall be resolved by negotiation. If the parties cannot reach an agreement, the dispute shall be resolved in the courts of the Republic of Estonia.

18.4. The User or any other person may submit a claim or a complaint to the following e-mail address: info@if.ee.

19. Contact information

19.1. If Mobile services in Estonia are provided by
If P&C Insurance AS (Estonia, Reg. No. 10100168):
KMRK EE100305320

Legal and central office address:
Lõõtsa 8A, Tallinn 11415

Telephone number (working 24/7): +372 7771211
E-mail - info@if.ee
If website and If Portal: www.if.ee