PRIVREDNA BANKA ZAGREB
Intesa Sanpaolo Group

Rules for the use of digital certificates issued via Privredna banka Zagreb d.d.

1. Introductory provisions

1. These Rules for the use of digital certificates issued via Privredna banka Zagreb d.d. (hereinafter: the Rules) shall regulate the rights, obligations and responsibilities related to the provision of certification services by FINA to business entities that hold a transaction account at the Bank.
2. By signing a Request for the issuance of business certificates, the End User and the Signatory shall accept these Rules.
3. In the event of any discrepancy or conflict between the provisions of the Agreement on the performance of certification services for business entities and FINA by-laws and these Rules, the Agreement on the performance of certification services for business entities shall prevail.

Definitions

Bank– Privredna banka Zagreb d.d., 10000 Zagreb, Radnička cesta 50, Croatia (BIC/SWIFT: PBZGHR2X, account no. HR6423400091000000013, TIN (OIB): 02535697732, e-mail: com@pbz.hr, website: www.pbz.hr) entered in the register of the Commercial Court in Zagreb under the registration number: 080002817, the issuer of these Rules.
Fina – Financijska agencija [Financial Agency], the provider of certification services.
Agreement on the performance of certification services for business entities– the agreement regulating the rights and obligations of FINA, the End User and the Signatory related to the issuing of Certificates.
Certification service– encompasses the following FINA services of managing the life cycle of a Certificate: the initial Certificate issuing, Certificate renewal accompanied with the generation of a new key pair, Certificate revocation, Certificate suspension, Certificate reactivation, Certificate recovery.
Request for the issuance of FINA business certificates– the document to be signed by the Applicant – Signatory and the End User, requesting the issuance of a particular type of Certificate.
Business Entity- a legal person or a natural person operating within the scope of his/her line of business or as a self-employed professional – non-consumer.
End User– a business entity that holds a transaction account at the Bank and has been defined as the User in the contractual documentation of the Bank and has also contracted the Certificate issuance service in accordance with the Request for the FINA Certificate issuance, the Agreement on the performance of certification services for business entities and these Rules.
Applicant– a natural person employed by the Business Entity or otherwise connected with the Business Entity, authorised by that same Business Entity to be issued a certificate. Such a Certificate identifies the [natural] person and the Business Entity and indicates that the person in question is connected with the Business Entity.
Authorised representative – a natural person who represents the End User by law or under a power of attorney and who authorises other Signatories to use Certificates on behalf and for the account of the End User.
Signatory– a natural person who is issued a Certificate on the basis of the Agreement on the performance of certification services entered into by and between Fina, the End User and the Signatory.
Cryptographic device- represents a USB token, smart card or another appropriate cryptographic device used for generation of user cryptographic keys and for storing certificates on it. According to the request of the Signatory and the End User, this device can be a *qualified electronic signature creation device* within the meaning of the eIDAS Regulation or a *secure cryptographic device* representing an electronic signature creation device within the meaning of the eIDAS Regulation.
Electronic signature– data in electronic form which are attached to or logically associated with other data in electronic form and which are used by the signatory to sign.
Qualified electronic signature– an advanced electronic signature that is created by a qualified electronic signature creation device and is based on a qualified certificate for electronic signatures. A qualified electronic signature shall have the legal effect equivalent to a handwritten signature.
Advanced electronic signature– an electronic signature that is uniquely linked to the signatory, enables identification of the signatory, is created by using electronic signature creation data that the signatory can, with a high level of confidence, use under his/her sole control, and is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.
Certificate– represents two business certificates issued by Fina on the same device; specifically, a Business Authentication Certificate (NCP+) and a business qualified certificate for electronic signature within the meaning of the eIDAS Regulation. Depending on the type of the chosen Device, Fina issues the following certificates to be used for electronic signatures: a Business EU qualified certificate for e-signature (QCP-n-qscd) or a Business EU qualified certificate for e-signature (QCP-n). A certificate also represents a Business EU qualified certificate for remote e-signature (QCP-n-qscd), issued by Fina to a natural person connected with the business entity, which is used for creation of a qualified electronic signature in accordance with 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 (hereinafter: eIDAS Regulation).
Business Authentication Certificate (NCP+)– a business authentication certificate of the medium security level, whose pertaining private key is stored in a secure cryptographic device or QSCD device, pursuant to Section 6.2.1 of the Certification Practice Statement for Non-Qualified Certificates, OID: 1.3.124.1104.5.0.4.2.1.8. This type of certificate complies with the "NCP+" certificate policy under the ETSI EN 319 411-1 standard. The Certificate validity period is 2 years.
Business EU qualified certificate for e-signature (QCP-n)– a business qualified certificate for e-signature of the medium

security level, issued to Associated Persons, whose pertaining private key is stored in a secure cryptographic device, pursuant to Section 6.2.1 of the Certification Practice Statement for Non-Qualified Certificates, OID: 1.3.124.1104.5.0.4.2.1.8. This type of certificate complies with the "QCP-n" EU certificate policy for qualified certificates under the ETSI EN 319 411-2 standard. The Certificate validity period is 2 years.
Business EU qualified certificate for e-signature (QCP-n-qscd)– a business qualified certificate for e-signature of the medium security level, issued to Associated Persons, whose pertaining private key is stored in a QSCD device, pursuant to Section 6.2.1 of the Certification Practice Statement for Non-Qualified Certificates, OID: 1.3.124.1104.5.0.4.2.1.8. This type of certificate complies with the "QCP-n-qscd" EU certificate policy for qualified certificates under the ETSI EN 319 411-2 standard. The Certificate validity period is 2 years.
Business Remote Certificate (NCP+)– a business certificate of the medium security level, whose pertaining private key is stored in the e-Signature Cloud Service, pursuant to Section 6.2.1 of the Certification Practice Statement for Non-Qualified Certificates, OID: 1.3.124.1104.5.0.4.2.1.8. This type of certificate complies with the "NCP+" certificate policy under the ETSI EN 319 411-1 standard. The Certificate validity period is 2 years.
Business EU qualified certificate for remote e-signature (QCP-n-qscd)– a business qualified certificate for e-signature of the medium security level, issued to Associated Persons, whose pertaining private key is stored in an rQSCD device, pursuant to Section 6.2.1 of the Certification Practice Statement for Non-Qualified Certificates, OID: 1.3.124.1104.5.0.4.2.1.8. This type of certificate complies with the "QCP-n-qscd" EU certificate policy for qualified certificates under the ETSI EN 319 411-2 standard. The Certificate validity period is 2 years.
FINA m-Token– is a means of two-factor authentication of the Signatory for accessing the Remote e-Signature Service, in the form of a mobile application.
Mobile application FINA e-Signature in the Cloud- enables two-factor authentication of the user via a mobile phone when accessing the Remote e-Signature Service as well as electronic signing of PDF documents in conformity with the eIDAS Regulation.
PIN – a secret personal identification number of the Signatory, known exclusively to the Signatory and strictly confidential, which is used for identification of the Applicant and for access to a cryptographic device.

2. Issuance of certificates

1. The End User has to open a transaction account at the Bank as a pre-condition for the issuance of Certificates.
2. The End User and the Signatory shall complete and sign the Agreement on the performance of certification services for business entities and the Request for the issuance of FINA business certificates.
3. The End User shall be obliged to deliver to the Bank a correctly completed and signed Agreement on the performance of certification services for business entities together with the Request for the issuance of FINA business certificates, requesting the issuance of a particular type of Certificate, in paper format or in electronic format if the documentation has been created and signed electronically.
4. With regard to the issuance and use of FINA business certificates, the Bank shall charge a one-off fee for supplying the device (except for the Business Remote Certificate (NCP+) and the annual fee for the Certificate use in accordance with the Decision on fees in transactions with domestic and foreign business entities, individuals and financial institutions (hereinafter: the Decision on fees).
5. When the End User's transaction account is closed, the Certificates issued to the Signatories shall be revoked and the relevant fee shall be charged in accordance with the currently valid Decision on fees.
6. The Bank reserves the right to refuse to sign the Request for the issuance of business certificates and shall not be obliged to provide any specific explanation of the reasons for such refusal.
7. The Bank shall offer Applicants an additional service of delivery of a cryptographic device by mail, for which it shall charge the fee in accordance with the currently valid Decision on fees.
8. Technical requirements for downloading certificates are described in the instruction for installation of PBZ PKI devices, available on the web site of the Bank: https://www.pbz.hr/velika-poduzeca/transakcijsko-bankarstvo.html.

3. Obligations of the End User and the Signatory

1) The End User/Signatory:

- The Signatory undertakes not to use the private key and the associated Certificate after expiry of the validity period of the Certificate;
- The End User and the Signatory undertake to carefully safeguard the cryptographic device, usernames, passwords, codes, PINs and other identifiers, to protect them against theft, loss, damage or misuse, and not to write them down nor disclose them to other persons;
- The End User and the Signatory undertake that, after the private key has been compromised, they shall immediately and permanently discontinue its use;
- The Authorised Representative of the End User and the Signatory shall be authorised to submit a request for revocation of the Certificate;

The request for revocation must be submitted in the following cases:

  - If there is a reasonable suspicion that the private key may have been compromised or if the private key has been compromised,
  - If the private key has been lost or has become permanently unavailable,
  - If there is a reasonable suspicion that the private key or activation data may no longer be in exclusive possession of the Signatory or if the private key or activation data have been stolen.
- The Authorised Representative of the End User and the Signatory shall be authorised to submit a request for suspension of the Certificate.

2) The End User shall be required:

- to promptly notify the Bank of any loss, theft, misuse or unauthorised use of a cryptographic device and/or a Certificate, and shall, without delay, request in person at the Bank the suspension and revocation of Certificates and the issuance of new Certificates, in which case the End User and the Signatory shall submit to the Bank a new Request for the issuance of FINA business certificates, while paying a fee in accordance with the Decision on fees;
- to notify the Bank of any changes in personal data included in the content of the certificate. If the End User fails to do so, the Bank shall regard as relevant the latest data provided to the Bank by the User and the Bank cannot be held responsible for any damage caused by information not being up-to-date;
- to notify the Bank of a change in any data on the End User from the Court Register and/or any personal data of the Signatory (name, surname, TIN (OIB), name of a business entity, etc.) and, if necessary under the Bank's and/or Fina's terms, shall be required to submit a Request for revocation of the issued Certificates and to request the issuance of new Certificates, while paying a fee in accordance with the Decision on fees ;
- to notify the Bank of any change of other personal data of the Signatory (e.g. address and place of one's permanent residence, e-mail address), in which case a fee shall be paid in accordance with the Decision on fees;
- to submit without delay a Request for revocation of the Certificates issued to the particular Signatory for that End User, when the Signatory's authorisation is revoked, while paying a fee in accordance with the Decision on fees.

4. Liability of the Bank

1. The Bank shall not be liable if Fina refuses to sign the Agreement on the performance of certification services for business entities.
2. The Bank shall not be liable if the certificate issuer Fina is unable to provide the service of issuing Certificates.
3. The Bank shall not be liable if Fina refuses to issue Certificates to an End User/Applicant.
4. The Bank shall have no liability whatsoever in relation to the process of Certificate downloading.

5. Security

1. The Signatory shall take delivery of a cryptographic device and shall be required to use it as described in Article 3 of these Rules.
2. The Signatory shall be required to keep secret all data related to Certificates, as described in the chapter "Obligations of the End User and the Signatory".
3. The End User shall bear any potential damage caused by non-compliance with these provisions by the End User/Signatory and/or in the event that a third party has in any way come into possession of data on the Signatory's Certificates.
4. The End User shall bear the entire risk of entry of incorrect data in all documents referred to in these Rules.
5. The Bank shall not be liable for any loss or destruction of data on a cryptographic device.

6. Replacement of a cryptographic device

In the event that a cryptographic device on which Certificates are stored happens to be damaged, broken-down, worn-out, lost or stolen, the End User shall be entitled to request the Bank to replace/issue a new device and, in addition, the End User shall be obliged to request the issuance of new Certificates. In that case, the End User shall be required to pay a fee to the Bank for the replacement/issuance of a new device and for the revocation and issuance of new Certificates stipulated by the currently valid Decision on fees, as defined in the General Operating Terms of Privredna banka Zagreb d.d. for Transaction Accounts and Performance of Payment and Other Services for Non-Consumers.

7. Fees

1. For the issuance of a cryptographic device and Certificate, the Bank shall charge a fee in accordance with the Decision on fees, as defined in the General Operating Terms of Privredna banka Zagreb d.d. for Transaction Accounts and Performance of Payment and Other Services for Non-Consumers.
2. If the End User pursuant to Article 6 of these Rules requests the replacement or the issuance of a new device, then the End User shall be required to pay a fee to the Bank in accordance with the Decision on fees, as defined in the General

Operating Terms of Privredna banka Zagreb d.d. for Transaction Accounts and Performance of Payment and Other Services for Non-Consumers.

3. The User shall be required to provide funds in its transaction account at the Bank necessary for the collection of fees mentioned in this article in accordance with the provisions of the General Operating Terms of Privredna banka Zagreb d.d. for Transaction Accounts and Performance of Payment and Other Services for Non-Consumers.
4. The level of fees is subject to change in accordance with the provisions of the General Operating Terms of Privredna banka Zagreb d.d. for Transaction Accounts and Performance of Payment and Other Services for Non-Consumers.

8. Renewal and revocation of Certificates

1. Up until expiry of Certificates issued via the Bank, it is possible to obtain renewal of such Certificates, while after their expiry, the issuance of new Certificates shall be required. For renewal and re-issuance of Certificates that are issued and renewed via the Bank, the Bank shall charge fees in accordance with the Decision on fees.
2. If the End User wishes to revoke i.e. permanently render impossible the use of a Certificate issued via the Bank to a particular Signatory, the persons who are, by law, the End User's authorised representatives shall be required to submit a Request for revocation of the Certificate and pay a fee in accordance with the Decision on fees. Likewise, a Signatory may revoke i.e. permanently render impossible the use of a Certificate issued via the Bank, in which case he/she shall be required to submit a Request for revocation of the Certificate, while the End User shall be required to pay a fee in accordance with the Decision on fees. The Request for revocation may be signed independently by the authorised representative of the End User or by the Signatory.
3. In the event of cancellation of the contractual relationship, regardless of which contracting party has cancelled the contract, the Bank shall be entitled to submit to Fina, on behalf and for the account of the End User, a Request for revocation of the Certificates, if the Certificates were issued via the Bank, and the End User shall be required to pay a fee in accordance with the Decision on fees.
4. If the End User, after the Certificates have been revoked, wishes to have new Certificates issued, then the End User/Signatory shall submit to the Bank a new Request for the issuance of FINA business certificates and shall pay a fee in accordance with the Decision on fees.

9. Blocking of a cryptographic device and suspension of Certificates

1. In the event of loss, theft, misuse or unauthorised use of a cryptographic device, the End User/Signatory shall without delay notify the Bank of such loss, theft, misuse or unauthorised use of the cryptographic device and shall immediately send to the Bank a request for suspension of its use, i.e. for temporary blocking of the use of Certificates stored on that cryptographic device. The End User/Signatory shall without delay notify the Bank of loss, theft, misuse or unauthorised use of Certificates, in which connection the End User must immediately send to the Bank a request for suspension of the use, i.e. for temporary blocking of the use of Certificates. The request for suspension may be signed independently by the authorised representative of the End User or by the Signatory.
2. If the End User/Signatory, after implemented suspension of Certificates issued via the Bank, finds a cryptographic device, then the End User/Signatory shall be required to inform the Bank of this fact in person, either by visiting the Bank in person or by making a call to the call centre of the Bank, and shall submit a Request for reactivation of certificates, while the Bank shall – upon receipt of the Request and upon verification of the identity of the End User and the Signatory – reactivate the suspended Certificates. After three business days have passed from the date of suspension becoming effective, the Bank shall no longer be under an obligation to reactivate the certificates. The Request for reactivation of certificates shall be signed jointly by the End User's authorised representative and the Signatory.
3. The End User shall be liable for and shall bear any damage incurred as a consequence of the loss or theft or unauthorised use or misuse of a cryptographic device and/or Certificates up until the moment when they are reported to the Bank.
4. Reporting of the loss or theft or unauthorised use or misuse of a cryptographic device and/or Certificates shall be done in writing by contacting the organisational unit responsible for managing the business relationship with the End User or by making a call to the call centre of the Bank (valid phone numbers of the call centre are posted on the website of the Bank).

10. Obligations of FINA

All obligations of FINA shall be defined by the Agreement on the performance of certification services for business entities as well as by FINA's documents related to the provision of certification services.

11. Final provisions

1. These Rules are available throughout the branch network of the Bank and on the website of the Bank (www.pbz.hr) .
2. The Bank reserves the right to amend these Rules. The Bank shall make available to the End User any amendments to these Rules, including a change of the title of these Rules or their replacement with new rules, in writing or via telecommunication/ electronic channels, *at least 15* days prior to entry into force of the amendments to these Rules, the new terms/rules or other internal documents of the Bank the application of which is referred to in these Rules or Fina's terms and conditions related to the provision of certification services to business entities. It shall be deemed that

the End User has accepted the amended Rules if, by the proposed date of their entry into force, the End User has not informed the Bank in writing that he/she/it does not accept them.

3. If the End User notifies the Bank in writing, within the time limit referred to in the previous paragraph of this article, that he/she/it does not accept the amendments to these Rules and/or [the amendments to] the internal documents of the Bank referred to in these Rules or [the amendments to] Fina's terms and conditions related to the provision of certification services to business entities, it shall be deemed that the End User does not wish to continue the use of a Certificate issued via the Bank and the Bank shall revoke the Certificate, while the End User shall be required to settle all obligations due and payable to the Bank.
4. These Rules have been drawn up in Croatian and in English. In the event of any discrepancy between the texts in Croatian and in English, the Croatian version shall prevail.
5. These Rules shall enter into force on 17 July 2024 and shall apply also to FINA Business Certificates issued previously via the Bank on the basis of Requests for contracting electronic banking services and the Agreement on the performance of certification services.