

Part F
**REGULATIONS ON USING AND SERVICING OF REMOTE ACCOUNT
MANAGEMENT SYSTEMS**

Terms used in the Regulations:

User – the Customer that applied for or uses the Remote Account Management System.

Authorisation Tools – special technical devices or parameters, which the User uses for attesting of the Transaction Document and Notification and their sending for execution to the Bank, and which provide the identification of the User and the authenticity of the Transaction Document and Notification. The Authorisation Tools are as follows:

- **Signature Password** – a combination of digits and/ or letters of the Latin alphabet issued to the User by the Bank or created by the User.
- **Electronic Signature** – a combination of digits and/ or letters of the Latin alphabet generated by the User;
- **Code Card** – a plastic card with the digital Authorisation codes, issued by the Bank;
- **Digipass Device** – an electronic device issued by the Bank and generating digital signature codes.

The Digipass Device is an independent remote account management tool for execution of Transactions; it can also be used for approving the Transaction Document and Notification by fax or e-mail, as well as for the User's identification during a telephone conversation.

Privat Online (Paritate Online) – a Remote Account Management System for execution of Transactions and exchange of information between the Bank and the User in "online" regime by using the protected data transmission channels in the Internet.

To manage the user accounts in the Privat Online system, the User needs to have the access to any computer connected to the Internet and use the browser programs Netscape Navigator or Internet Explorer. The Authorisation Tools in the Privat Online system may be the Signature Password, Digipass Device, Code Card.

Privat B@nkNet (Paritate B@nkNet) – the "client-bank" Remote Account Management System for execution of Transactions and exchange of information between the Bank and the User in the Internet by using the protected data transmission channels.

To be able to operate Privat B@nkNet the User needs to install Privat B@nkNet software suit to a personal computer with the Internet connection. The Authorisation Tools for Privat B@nkNet may be the Electronic Signature, the Digipass Device.

The Bank issues the following access parameters for the use of the Privat Online and Privat B@nkNet system:

- **User Name** (log-in name) – a combination, created from the letters of the Latin alphabet, which is meant for the User's identification in the Remote Account Management System.
- **Connection Password/Access Password (access password to the program)** – a combination, created from the letter of the Latin alphabet and/or Arabic digits, which provides the initiation of the use and determines the User's access level to the Remote Account Management System.

18.1. Present Regulations on Use and Servicing of Remote Account Management Systems are applicable, if the User has applied or already uses the Remote Account Management Systems and/or Authorisation Tools.

18.2. The User agrees that the Bank is entitled unilaterally at any time to determine the limitations for conclusion to the remote management of accounts and execution of Transactions by means of the Remote Account Management System, and the User undertakes to observe them without reservation.

Application for Use of Remote Account Management System

18.3. The User submits the application to the Bank for the use of a relevant Remote Account Management System, Authorisation Tools and access modes taking into account the limitations determined by the Bank.

18.4. The Remote Account Management System Privat Online is available in the following modes:

18.4.1. the informative mode (*VIEW ACCESS*) – with the right to see the balance of accounts and receive other information about the accounts but without the right to prepare and send documents to the Bank;

18.4.2. the limited mode (*CREATE ACCESS*) – with the right to prepare documents, but without the rights to send them to the Bank, and to receive all information about the accounts;

18.4.3. full access mode (*SIGN ACCESS*) – with the rights to prepare documents and send them to the Bank, execute Transaction defined by the Bank, receive all information about the accounts, as well as receive other offers provided by the Bank and use Remote Account Management systems.

18.5. The Bank upon receiving the User's application for connection of the Remote Account Management System and Authorisation Tools and its verification generates unique parameters for access to the Remote Account Management System for the User, as well as at the User's option taking into account the limitations, determined by the Bank, generates/ prepares the Authorisation Tools.

18.6. The User account is connected to the Remote Account management system/Authorisation Tools/Access Parameters after the Bank has verified a written and signed statement from the User on receiving Remote Account Management system access parameters and Authorisation Tools if the User has an open (and activated) account at the Bank.

18.7. The User is obliged to personally familiarise himself with the Regulations, the Installation of Remote Account Management Systems manual and Authorisation Tools application regulations (User manual, User guide). The documents, mentioned in the present Paragraph are available for the User at the Bank or on the Bank's Internet homepage – www.privatbank.lv.

18.8. The Bank issues access parameters for the Remote Account Management system and Authorisation Device to the User sealed.

18.9. The access parameters and the Authorisation Tools are confidential information, which the User and the Bank undertake not to divulge to third parties, as well as undertake to take all measures to prevent the possibility of divulging it to third parties. The User is obliged to safe-keep the confidential information, as well as in due term to change the Access Password and Signature Password in accordance with the Bank's requirements.

User Identification. Security.

18.10. When the User is connecting and to operating in the Remote Account Management Systems, the Bank automatically identifies the User according to the User Password and Access Password.

18.11. In case the Authorisation device is lost or stolen, or the User name, Connection Password/Access Password and/or Signature Password has become known or could have become known to a third party due to the reasons, irrespective of the User and/ or against the User's will, the User is obliged immediately to report it to the Bank orally or in written. The Bank blocks the access to the Remote Account Management System within 1 (one) Bank Working Day of receiving the notification.

18.12. In case the User gives instruction to the Bank to block the access to the Remote Account Management System, then the Bank performs the User's identification according to the User name and other information at the Bank's disposal. Within 3 (three) Bank Working Days of

receiving an oral instruction the User is obliged to submit a written Notification to the Bank in relation to the blockage of the Remote Account Management System.

18.13. Taking into account the User's wishes the Bank generates and issues new unique access parameters for the Remote Account Management System and/ or issues the Authorisation Tools. The connection of the Remote Account Management devices and/ or access parameters to the User Account is performed after the Bank receives a signed statement from the User on new Remote Account Management system access parameters and verification of the Authorisation Tools. The Bank charges the Fee according to the Bank's Fees for the new Remote Account Management system access parameters/Authorisation Tools issuance.

18.14. If the Bank has reasonable suspicions, that the User has lost control over the confidential information, issued by the Bank by means of which the User may use the Remote Account Management Systems (User name, Connection Password/Access Password and/or Authorisation devices), as well as if the features of forgery of signature and/ or seal are stated in the Acceptance Protocol of access parameters to Remote Account Management System and Authorisation devices, the Bank is entitled, but not obliged, to block the User's access rights to the Remote Account Management Systems bearing no responsibility for it.

18.15. The User's access rights to the Remote Account Management System are automatically blocked, if during the connection to the Remote Account Management System the Access Password is input incorrectly 5 (five) times in succession or the Connection Password is input incorrectly 3 (three) times in succession.

18.16. The Authorisation Tool is automatically blocked, in case:

- the Signature Password is input incorrectly 3 (three) times in succession
- the code from the Code Card is input incorrectly 3 (three) times in succession
- the code generated by the Digipass Device is input incorrectly 3 (three) times in succession.

18.16.1. The Digipass Device is irreversibly blocked, in case:

- the 5-digit PIN-CODE is input incorrectly 3 (three) times in succession
- the User attempts to open the Digipass Device or causes other mechanical damages to it (pours it with liquid, breaks it, and other).

18.17. User access rights (parameters) to the remote account management system and means of authorization if they are automatically blocked pursuant to clauses 18.15 and 18.16 can be unblocked after presenting a written Notification by the Bank's User on their unblocking or orally via phone notifying the Bank on that pursuant to Part B of the Regulation on Submitting and Receiving Information via Telephone and Online Chat.

18.18. If the error is detected in the software of the Digipass Device the Bank shall replace the Digipass Device for the User for free.

18.19. In case of the irreversible blockage of the Digipass Device due to the reasons, provided for in Paragraph 18.16.1, the Bank shall perform the replacement of the Device, charging the Fee in accordance with the Bank's Fees.

Confirmation and Sending of Transaction Documents and Notifications to the Bank

18.20. The Transaction Documents and Notifications, in case they are compiled and confirmed with the Authorisation Tool in procedure, specified by the Bank, are considered equated with the documents, compiled and signed in written in the understanding of the Civil Code of the Republic of Latvia with full legal force and legal effects and legal consequences, arising from it. The User cannot contest the Transactions Documents and Notifications, which have been submitted to the Bank by means of the Remote Account Management System.

18.21. The Authorisation Tool serves for identification of the User or determining the authenticity of the Transaction Document and Notification. The correct Signature Password in the Transaction Document and Notification is considered to be the User's own signature, that

imposes liabilities onto the User in compliance with the norms of signatures and authorisation of the Civil Code of the Republic of Latvia.

18.22. The Transaction Document or Notification, compiled in accordance with the regulations of the Remote Account Management System application manual (User manual/ User guide) and signed with the Authorisation Tool is considered the User's instruction to perform Transactions and provide financial services.

18.23. The Bank is entitled not to execute the User's Notification compiled as the Transaction Document, if:

18.23.1. The User does not observe the present Regulations or the relevant Remote Account Management System User guide;

18.23.2. The Bank has suspicions about the User's identity and the Bank failed to contact the User to verify his identity and content of the Transaction Document;

18.23.3. The User's Transaction Document is corrupted or not clear due to transmission interruptions;

18.23.4. The User does not observe other requirements of the Bank.

18.24. Upon the receipt of Transaction Document or Notification the Bank is entitled to contact the User repeatedly and verify if the Transaction Document or Notification is correct.

Liability

18.25. The Bank is not financially responsible for losses, which have arisen / may arise for the User due to communication line damage or interference or in cases when the Remote Account Management Systems or their separate functions are unusable/ unavailable for the User due to technical reasons for execution of Transactions and operations and/ or the Transaction Document/Statement is not received in the Bank.

18.26. The Bank bears no responsibility for the User's losses, which may arise in connection with User's registration, cancellation or changes in the User's rights in case the Bank acts according to the User's Notifications, including the case when violations of procedure of the User's decision-making are stated.

18.27. The Bank is not financially responsible for any losses, arising for the User or may arise when submitting a Notification to the Bank by means of the Remote Account Management System.

18.28. The User is responsible for his own actions and undertakes to indemnify all the losses to the Bank, which have arisen as a result of his actions.

18.29. The User bears responsibility for the User taking all the managerial security measures to prevent the access of unauthorised persons to the Remote Account Management System, User name, Access Password/ Connection Password and Authorisation Tools safekeeping and using in the way to prevent the possibilities of its use by unauthorised persons.

18.30. The Bank bears no responsibility for the User's losses in case unauthorised persons connect to and/ or use the Remote Account Management Systems (access parameters/Authorisation Tools), as well send on behalf of the User the Transaction Documents or Notifications, signed with the correct Signature Password, and the User has not reported it to the Bank.

18.31. The Bank bears no responsibility for execution of Transactions or banking operations, including the write-off of funds from the User's accounts in compliance with forged documents or otherwise unlawfully compiled/ submitted Documents, if these documents have been confirmed by the Authorisation Tool.

18.32. The User undertakes all the risk and responsibility for losses which arise:

18.32.1. In case of erroneous or corrupted transmission of the Transaction Document or Notification, including miscomprehension, lack of infrastructure of technical communications or the errors, caused by disturbance, or corruption, as well as in case of unlawful actions by third parties, so far as has not occurred due to the Bank's gross inattention;

- 18.32.2. in case of duplication of the Transaction Document or Notification;
 - 18.32.3. if the User has voluntarily passed the Remote Account Management System to a third party and this third party has managed the Remote Account Management System;
 - 18.32.4. if the User has not observed the present Regulations.
- 18.33. The Bank is entitled on its own initiative at any time to terminate the providing of Remote Account Management System services, informing the User about it.

Copyrights, Modifications

18.34. All the private and property copyrights for the Remote Account Management Systems software and related materials provided to the User (User manual, User guide, Remote Account Management Systems installation manual and other) are the property of the Bank. The User is entitled to use the systems software solely within the framework, specified in the present Regulations, i.e. in compliance with the regulations, specified in the application guide of the Remote Account Management System, determined by the Bank.

18.35. Without the Bank's consent any transformation of the Remote Account Management System software, any reproduction, publishing, any transfer to third parties and the use of technologies of the Remote Account Management Systems software in order to create other software, not stipulated in the present Regulations, which would execute the functions of the Remote Account Management Systems, is prohibited.

18.36. In case the Bank submits a new Remote Account Management System software version to the User the Bank is entitled to suspend the use of the previous software version.

18.37. The Bank guarantees the compatibility of Remote Account Management System software with the computer programs, indicated by the Bank.

Fees

18.38. The User shall pay the Fee to the Bank in accordance with the Bank's Fees for connection to the Remote Account Management System, the issuance of its access parameters/Authorisation Tools, replacement, as well as in other cases, specified in the Bank's Fees.

18.39. The Bank on a no contestation basis writes off the relevant Fees from the User's accounts with the Bank or the User pays them in cash.