1. Terms Used in the Terms of Service and Their Interpretations:

1.1. **Authentifier** – codes, passwords and other identifiers or actions, creation or use of which is possible when using the Authorisation Device and which the Bank uses for authentication of the User and/or for examination of confirmation of the Transactions initiated in the Online Banking.

1.2. **Authorisation Device** – the device or software granted by the Bank or purchased by the User and accepted by the Bank that is used for creation or use of the Authentifier, e.g., Mobile Device.

1.3. **Authorisation Device Limit** – the limit of one Payment, day limit determined by the Bank for the Authorisation Device, i.e. the maximum amount within the limit of which Payments are executed via the Online Banking within 24 hours, and monthly limit, i.e. the maximum amount within the limit of which Payments are executed via the Online Banking within one calendar month, assuming that there are 30 days in a month.

1.4. **Pricelist** – an effective pricelist for products and services of the Bank.

1.5. **Transaction** – any actions that may be performed via the Online Banking using options and methods offered by the Bank in the Online Banking environment including making Payments and conclusion of agreements.

1.6. **Terms of Transactions** – instructions of the Bank, terms and settings in the Online Banking, including on the Mobile Website related to receipt of services of the Bank.

1.7. **Electronic Document** – a set of data created via the Online Banking containing the User's Order addressed to the Bank, the Transaction processed via the Online Banking or other actions of the User performed in the Online Banking as well as materials submitted via the Online Banking, e.g., copies of paper documents.

1.8. **Limitations** – limitations of types of Transactions, Accounts and other limitations determined by the Client that are binding to the User and that are specified in the Application.

1.9. **Application** – an application in the form approved by the Bank that is completed by the Client to receive the Service.

1.10. **Information Channel** – e-mail and/or sms message sent to the e-mail address or mobile phone number, about which the Client or the User notified the Bank as well as the Mobile Website in accordance with the identifier of the Mobile Device that is used on the Mobile Website.

1.11. **Online Banking** – the system of remote access and management of the Bank's services used in the Internet, incl. the Mobile Website. The Online Banking may be accessed by opening the Bank's website www.citadele.lt or address in the Internet https://online.citadele.lv or by downloading Citadele mobile application from App Store or Google Play.

1.12. **Client** – a natural person who submits the Application to the Bank and with whom the Bank enters into the Service Agreement.

1.13. **Code Calculator** – the Authorisation Device issued by the Bank.

1.14. **Code Card** – the Authorisation Device issued by the Bank.

1.15. **Account** – any account of the Client with the Bank, incl. a current account, savings account etc., which is opened in the Client's name with the Bank.

1.16. **User's Limit** – the limit of one Payment, day limit determined by the Client for the individual User, i.e. the maximum amount within the limit of which Payments are executed via the Online Banking within 24 hours, and monthly limit, i.e. the maximum amount within the limit of which Payments are executed via the Online Banking within one calendar month, assuming that there are 30 days in a month. Payment, day and monthly limits may be defined all together or separately in any combination.

1.17. **User** – a natural person whom the Client has specified in the Application and authorised to use the Online Banking: the Client or another person.

1.18. **Payment** – an order of the form approved by the Bank of the Client/User that is made to perform a non-cash money transfer.

1.19. **Mobile Device** – a mobile phone, smartphone, tablet computer or another device which the Client or User has registered in the Bank using the Mobile Website.

1.20. **Mobile Website** – a service available in the Bank's mobile application using the Mobile Device for performing the Transactions of certain types and volume as well as for receipt of certain services of the Bank, applying the requirements that are an alternative to safe authentication.

1.21. **MobileScan** – the Authorisation Device issued by the Bank.

1.22. **Service Agreement** – an agreement of the Bank and Client on use and service of the Online Banking, the integral parts of which are the Application and Terms of Service.

1.23. **Terms of Service** – these Terms of Use and Servicing of the Online Banking.

1.24. **Service** – connection and service of Online Banking as well as other services of the Bank related to Online Banking.

1.25. **Login Password** – the Authentifier linked to the Login Name that shall be changed on a regular basis, which is a series of symbols that has been chosen by the User and known only to the User that is used by the User for authentication for getting access to the Online Banking in cases specified by the Bank.

1.26. **Login Name** – the Authentifier specified in the Application, which is a series of symbols that has been chosen by the User that is used by the User for authentication for getting access to the Online Banking in cases specified by the Bank.

1.27. **Full Mode** – the usage mode of the Online Banking, within the framework of which the User without limitations may submit (send) the Orders to the Bank for execution of the Transactions and/or other documents (applications, requests and the like) as well as to use the rights determined for the View Mode.

1.28. **Parties** – the Client and Bank, jointly.

1.29. **Order** – an assignment to perform the Transaction given on behalf of the Client to the Bank.

1.30. **View Mode** – the usage mode of the Online Banking, within the framework of which the User has the right to obtain (view) information on the state of the Account, turnover, balances, etc., to print out an account statement, but cannot submit (send) the Orders to the Bank for execution of the Transactions and/or other documents (applications, requests and the like).

1.31. **Telephone Password Question and Telephone Password** – the password question chosen by the User and specified in the Application that the Bank asks the User, and the password to be stated by the User replying to the mentioned password question for identification of the User by telephone.

1.32. **GTB** – General Terms of Business of the Bank.

1.33. **Bank** – AS "Citadele banka" Lithuanian Branch, branch code 304940934, registered office at K.Kalinausko str.13, Vilnius.

1.34. Other binding terms and interpretations thereof are specified in agreements on opening and service of Accounts concluded between the Bank and Client and the GTB.

2. **General Provisions**

2.1. By signing the Application the Client certifies that:

2.1.1. the Client shall use the Online Banking in accordance with the Application, Terms of Service, and operation manuals of the Authorisation Devices;

2.1.2. is aware of the risks related to the Service;

2.1.3. has been informed and is aware of the fact that the Bank has the right to request the User using Online Banking and the User is obliged, if it complies with the corresponding usage mode of Online Banking determined for the User, to provide to the Bank on behalf of the Client information and/or certifications that is necessary for the Bank to meet requirements of the legal acts binding upon the Bank and ensure compliance of the activity of the Bank, and provision of such information and/or certifications in the Online Banking is mandatory for execution of the Transaction in cases stipulated by the Bank as well as for execution of the Client's payments and conclusion of agreements in the Online Banking;

2.1.4. the Client shall ensure that the User, according to the usage mode of the Online Banking determined for the User, is duly authorised to execute the Transaction and provide the information and/or certifications requested by the Bank on behalf of the Client;

2.1.5. shall ensure that the User has read the Application, Terms of Service, other terms and instructions related to the Service, operation manuals of the Authorisation Devices, and the Client himself/herself shall observe all requirements stipulated in the mentioned documents;

2.1.6. is informed that the Authentifier is confidential information, and the User shall ensure that the Authentifier, Authorisation Device and Information Channel are not available to other persons; the Authorisation Device as well as the Mobile Device is protected, stored and used with due care and observing safe-keeping requirements, including the access code, if the Authorisation Device has such option, as well as the Client and User undertake to inform the Bank immediately in writing or by telephone on change or cessation of the use of the Authorisation Device, mobile phone number, e-mail address or the Mobile Device;

2.1.7. the Client or the User shall immediately notify the Bank about theft or other illegal use of the Authentifier or the Authorisation Device or suspicions that the Authentifier or the Authorisation Device is at a third party's disposal, after which the Bank blocks the use of the endangered Authentifier and/or the Authorisation Device for getting access to the Online Banking as soon as possible until the moment, when a new Authorisation Device is issued to the User on the grounds of the Client's or User's application, the limit of Transactions of which does not exceed the Authorisation Device Limit of the replaced device, or the blocked access to the Online Banking is unblocked on the grounds of the User's application;

2.1.8. the User has been informed and to prevent unauthorised persons' access to the Online Banking, the User undertakes to install valid antivirus software on the device that is used for access to the Online Banking, and to set the access code on the Mobile Device, and to check safety of the device prior to commencing a session of use of the Online Banking;
2.1.9. the User shall ensure inaccessibility of settings and personalised information of the Mobile Website to third parties, as well as the User shall delete such settings, information and the Mobile Website itself, if the Mobile Device is given to third parties as well as in case, if the risks related to the use of the Mobile Website are excessive in the Client's or the User's opinion;
2.1.10. the User shall ensure that upon commencement of a session of the Online Banking and/or in case, if the User, having connected to the Online banking, notices suspicious actions, including extended intervals, requests for additional actions that usually do not result from the User's action, the User shall immediately terminate a session of the Online Banking and inform the Bank about it.
2.1.11. the Application that is signed in order to add a new User to the Online Banking or change the list of Users and Users' access modes does not require conclusion of a new Service Agreement, but it becomes an integral part of the Service Agreement in effect;
2.1.12. the Client agrees that the User is entitled to conclude an agreement on the use of the Mobile Website and services of the Bank available therein himself/herself, and such agreement shall be deemed to be amendments or supplements to the Service Agreement as if they were made by the Client himself/herself.
2.2. This Service Agreement is deemed concluded from the moment when the Bank accepts the Client's Application. The Bank accepts the Application, if it is executed in accordance with requirements of the Bank.
2.3. The Bank is entitled to refuse rendering of the Service without explaining the reasons for refusal.
2.4. The legal address of the Bank is deemed to be the place of entering into the Service Agreement.
2.5. The aspects of the legal relationship of the Parties that have not been stipulated in the Terms of Service shall be regulated by the GTB, Pricelist and the terms of opening and service of the Account to which the Online Banking is connected.

3. Provision of the Service
3.1. Actions that may be performed in the Online Banking
3.1.1. The User is entitled, within the framework of the usage mode of the Online Banking set for the User and Limitations (if any), to send the Orders to the Bank for execution of the Transactions execution of which is ensured in the Online Banking at the respective moment. Lending agreements, inter alia, may be concluded via the Online Banking, provided that such agreement may be concluded only by the User who is the Client.
3.1.2. The Client has been informed and consents to the fact that the Transactions related to investment services and ancillary investment services may be concluded as well as agreements and amendments may be concluded via the Online Banking.
3.1.3. The Client and User agree that the Electronic Document and Terms of Transaction confirmed by the correct Authentifier, in the aspect of legal force, are set equal to documents that are made in writing and duly signed pursuant to the Civil Code of the Republic of Lithuania, with all legal consequences resulting therefrom, and impose obligations upon the Client and User in accordance with the standards of the Civil Code of the Republic of Lithuania related to signatures and authorisation.
3.1.4. Execution of the Transactions on the Mobile Website is possible after installation of the Mobile Website according to the Bank's instructions (which may be provided both prior to commencement of execution of the Transaction and during execution thereof) on a mobile device that has such option.
3.1.5. All notices, information, data and documents that the Bank provides to the User via the Online Banking as well as via the Information Channels is the information binding upon the Client and User and it may be given the same status as a paper documents of the Bank according to the content of the provided information.
3.2. Authentication of the User
3.2.1. The User is authenticated according to the Authentifier, for creation or use of which the User acts in accordance with requirements of the Bank and/or developer of the Authorisation Device with regard to creation or use of the Authentifier. The Bank may determine a duty to receive/use the Authorisation Device also in addition to the existing device, by means of which new or additional Authentifiers may be created/used, if it is necessary for fulfilment of safe authentication requirements.
3.2.2. Using the Mobile Website, the User may be identified according to the Mobile Device.
3.2.3. The User may use the Information Channels for submission of the Orders under the procedure specified by the Bank as well as for submission of information and data and receipt of the Authentifiers.
3.2.4. Not only the Code Calculator specified in the Application may be used for creation of the User's Authentifier according to the Online Banking usage mode, but also the code calculator issued to the Client for remote management of the Account in the frame of another agreement entered into by the Bank and Client in cases specified by the Bank.
3.2.5. The Authentifier of the Order that includes several individual Payments is considered to be a unique confirmation of each Payment included in the Order and it is an integral part of each Payment.
3.2.6. If the User has used the Login Name also within the framework of service agreements of other clients of the Bank, in case of change of the Login Name the User may use the new Login Name for connection to the Online Banking of other clients only upon receipt of written consent of the respective client, also by submitting it via his/her Online Banking under the procedure specified by the Bank.
3.3. Registration of Several Authorisation Devices
3.3.1. The Bank has the right to determine the requirements binding to the Client with regard to compatibility of the Authorisation Devices and choice of the Authorisation Device by the User, as well as the Bank has the right to determine which Authorisation Devices shall be main Authorisation Devices and which shall be additional ones, i.e. the devices that may be used only together with the main Authorisation Device.
3.3.2. If several Authorisation Devices have not been registered simultaneously and the User acts on behalf of several clients in the Online Banking, in case of registration of another Authorisation Device, the User may use the new Authorisation Device for connection and performing operations in Online Banking of other clients only upon receipt of a written consent of the respective client, and it may be submitted via the User's Online Banking as well.
3.4. Blocking of the User's Access and/or the Authorisation Device, Replacement of the Authorisation Device
3.4.1. Authentifiers may be assigned, restored or changed upon request of the Client or the User in accordance with the Bank's instructions and procedure specified by the Bank. At the same time, the Bank is entitled to request use more safe or additional Authorisation Devices or Authentifiers.
3.4.2. Blocking and unblocking of the User's access to the Online Banking and/or the Authorisation Device may be performed on the grounds of the Client/User's written application as well as upon initiative of the Bank. The User's access is restored under the procedure determined by the Bank.
3.4.3. In case of blocking of one Authorisation Device, other Authorisation Devices shall not be blocked.
3.4.4. Only the Client or User of the respective Authorisation Device may receive the replaced Authorisation Device. If the Authorisation Device is received by the User, the Transaction limit of a new Authorisation Device cannot exceed the limit of the replaced Authorisation Device.
3.4.5. If the User has used the previous Authorisation Device also within the framework of service agreements of other clients, the User may use the replaced Authorisation Device for connection to the Online Banking of other clients only upon receipt of a written consent of the respective client, also by submitting it via the Online Banking, and the User shall timely inform the client (-s) on necessity of such consent.
3.5. Limits of Transactions
3.5.1. The Bank has the right to determine/change the Authorisation Device Limits specifying them in the Pricelist.
3.5.2. The use of the Authorisation Device Limit determined by the Bank is monitored for the respective device. Therefore, when the User confirms Payments by the Authentifiers using the Authorisation Device, the Authorisation Limit of which has been depleted, in the Online Banking of another client, such confirmation shall be rejected irrespective of the fact whether the amount of Payments made by the Client in his/her Online Banking has reached the User's limit or the Authorisation Device Limit or not.
3.5.3. The Client has the right to determine the User's Limit for each User at his/her discretion, observing the condition that the amount of the User's Limit is applied irrespective of the type of the Authorisation Device, however, if the Authorisation Device Limit of the respective device is smaller than the User's Limit, the Payment may be executed only if its amount does not exceed the Authorisation Device Limit of the device that has been used for generating or use of the Authentifier.
3.5.4. The Authorisation Device Limits and the User's Limits determined by the Bank are not applied to the money transfers that the Bank performs upon the Client's instruction within the framework of rendering regular payments service or e-invoices regular payment service as well as for Payments from one Account of the Client to another Account of the Client in the Bank. The

Bank has the right to determine the application of the Authorisation Device Limit and the User's Limit unilaterally in the cases referred to in this Clause.
3.6. Changes in the Online Banking
3.6.1. The Bank has the right to change unilaterally the volume and procedure of rendering of the services rendered within the framework of the Online Banking. If during validity of this Service Agreement the Bank ensures technical possibility to perform such financial transactions, which have not been available as of the moment of conclusion of the Service Agreement, execution of such financial transactions shall automatically become available to all Users, observing their Online Banking usage modes and the Limitations.

4. Liability of the Parties
4.1. To ensure execution of the Orders and other documents the Bank is entitled to use services of third parties. In this case the Bank is not responsible for losses and inconveniences of the Client, should this be a result of action or inaction of third parties.
4.2. The Client is responsible for all actions of the Users performed in the Online Banking.
4.3. The Client has been informed and undertakes the risk that when the User uses services of the Mobile Website such services, inter alia, the Transactions of a small volume and simplified Transactions as well as the data available in the Mobile Device may become available to third parties in cases, if the Mobile Device is not duly protected or gets into possession of third parties.
4.4. The Bank is not responsible for the Client's claims arising in connection with registration, revocation of the Users or change of the volume of their rights, if the Bank acts in accordance with instructions of the Client's authorised person, including in cases, if instructions of the Client's authorised person do not comply with the Client's decisions.
4.5. The Bank is not responsible for execution of the Transaction, which have not be authorised by the Client/User, if such Transaction has become possible due to illegal action of the Client/User, acting intentionally or by gross negligence as well as not observing the duties stipulated in Clauses 2.1.6, 2.1.7 or 2.1.9 of the Terms of Service.
4.6. Derogating from the Service Agreement in case specified in Clause 4.4 of the Terms of Service, if the Authorisation Device and the Mobile Device has been lost or stolen, as a result of which the Transactions that have not been authorised by the Client/User have been executed, but it is not the Client's and User's fault and the Client/User has not allowed gross negligence, as a result of which loss or theft has become possible, as well as has not allowed breaches of Clauses 2.1.6-2.1.9 of the Terms of Service, and the Client/User has immediately notified the Bank about loss/theft, the maximal amount of responsibility of the Client is EUR 50.
4.7. The Client is responsible for taking measures to prevent access of unauthorised persons to the Online Banking, Mobile Website and Information Channel as well as for storage and use of the Authentifiers, Authorisation Devices, Telephone Password Question and Telephone Password and other personalised information in such manner as not to allow getting of the same into unauthorised persons' discretion and to prevent unauthorised use thereof.
4.8. The Bank is not responsible for losses sustained/may be sustained by the Client:
4.8.1. due to damage of communication lines or interruption in their operation or in cases, when the Online Banking or some of its functions cannot be used by/are not accessible to the User due to technical reasons, and/or the Electronic Document has not been received by the Bank;
4.8.2. if the User cannot execute the Transaction as well as conclude agreements with the Bank and/or make Payments in the Online Banking due non-provision of the information and/or certifications that have been requested by the Bank in accordance with the procedure stipulated in Clause 2.1.3 of the Terms of Service.
4.8.3. due to interruptions in operation of the Information Channels or in case if the respective Information Channels are not accessible for the User including for receipt of the Authentifiers;
4.8.4. he information stored in the User's Information Channels has become available to third parties;
4.8.5. if the User's mobile phone number, e-mail address or Mobile Device have been transferred to third parties.
4.9. The User is not a party to this Service Agreement, therefore the Bank is not responsible to the User for his/her claims, except for the case when the Client is the User as well as with regard to the issues arising with regard to the use of the Mobile Website;
4.10. If the person who signs the Application on behalf of the Client is not authorised to represent the Client, the signatory undertakes to compensate to the Bank all losses inflicted upon the Bank as a result of such action of the signatory.

5. Amendments of the Service Agreement, Term of Validity and Termination of the Service Agreement
5.1. The Service Agreement is concluded for an indefinite period of time.
5.2. The Bank is entitled to amend the Terms of Service unilaterally.
5.3. Information about any planned amendments of the Terms of Service before they come into force is available to the Clients in client servicing structural divisions of the Bank, website of the Bank www.citadele.lt as well as the Client may receive it by calling the call centre of the Bank.
5.4. The Bank is entitled to introduce amendments, which are less favourable to the Client in comparison with the previous ones, only in case if there is a well-grounded reason. The Bank shall timely inform the Client about such amendments of the Terms of Service not later than 2 (two) months before they come into force via the Online Banking.
5.5. If the Client does not agree with amendments of the Terms of Service, GTB or Pricelist, the Client has the right to terminate the Service Agreement until the day when the proposed amendments come in force, informing the Bank about it and making all payments resulting from the Service Agreement to the Bank, if such payments are to be made and result from the Service Agreement.
5.6. The Client is entitled to unilaterally terminate the Service Agreement submitting a respective application to the Bank. The Bank terminates the Service Agreement within 5 (five) calendar days from the day of receipt of the Client's application for termination of the Service Agreement.
5.7. The Bank is entitled to terminate the Service Agreement unilaterally, informing the Client about it in writing 2 (two) months in advance.
5.8. The Bank is entitled, without observing the term specified in Clause 5.7 of the Terms of Service, to terminate immediately the Service Agreement unilaterally, informing the Client in writing, in any of the following cases:
5.8.1. the Client does not discharge or discharges his/her obligations stipulated in this Service Agreement improperly;
5.8.2. the Bank has reasonable grounds to suspect that the Online Banking is used for the purposes it is not meant for or actions are performed that may block and/or hinder operation of the Online Banking;
5.8.3. all Accounts of the Client with the Bank are closed.
5.9. If the Service Agreement is terminated upon the Client's initiative earlier than 6 (six) months after the day of conclusion of the Service Agreement, the Bank is entitled to charge a commission fee for termination of the Service Agreement, if such fee is stipulated in the Pricelist.

6. Other Provisions
6.1. The Bank ensures the processing of the private individual data in accordance with the Personal data Protection Principles approved by the Bank, which are available on the website of the Bank in internet.
6.2. For a telephone contact with the User, in accordance with for change of the Login Password, blocking of the Login Name, access to the Online Banking and/or blocking of the Authorisation Device as well as submission of information with regard to the issues related to the use of the Online Banking and performing other actions in the frame of the powers assigned to the User, the Bank authenticates the User using the Telephone Password Question and Telephone Password. However, for identification of the User by telephone, the Bank is entitled to use also such data that is specified for the purposes of identification of the User in other service agreements concluded by the Bank and User or which are applicable in accordance with the GTB.
6.3. The User has the right to ask the Bank to change the Telephone Password Question and Telephone Password at any time. If the Telephone Password Question and Telephone Password has already been determined for the User as the Client or another Client's User, the User may use it in the frame of this Service as well.
6.4. Any dispute, disagreement or claim resulting from the Agreement, connected with it or its violation, termination or invalidity, shall be considered in accordance with the effective laws of the Republic of Lithuania in a court of the Republic of Lithuania in Vilnius according to jurisdiction.
6.5. Claims and complaints of the Clients' shall be handled in accordance with the procedure specified in the GTB.
6.6. Operation of the Bank is supervised by the Financial and Capital Market Commission of the Republic of Latvia. The address of the Financial and Capital Market Commission: Kungu iela 1, Riga, LV-1050.

Appendix to the Terms of Use and Service of Citadele Online Banking – Terms of the Quick Access Service and Other Functions Available in Citadele Mobile Application

1. Terms Used in the Annex and Their Explanations:

1.1. **Quick Access** – the Bank's service that enables the User to perform certain types of Transactions as well as to receive additional services in the Bank's mobile application, inter alia, on the Mobile Website, including the use of alternate requirements for secure authentication.

1.2. **Biometric Authenticator** – the Authenticator based on a person's unique physical characteristics or properties, such as fingerprint or facial image, and it is registered in the Mobile Device.

1.3. **Annex** – these Terms of the Quick Access Service of Citadele Mobile App that are an integral part of the Terms of Use and Service of Citadele Online Banking.

1.4. **Access Code** – a combination of digits, fingerprint, combination of forms or any other protection option ensured by a device.

1.5. **PIN Code** – a user-created five-digit combination that shall be entered to use MobileScan in the Mobile Device.

1.6. **Mobile Notification** – a type of notification that is delivered to a device via a mobile application in the form of a sound or text alert or emblem (push notification). The terms used in this Annex, the explanation of which is not provided herein, may be found in the Terms of Use and Service of Citadele Online Banking.

2. General Provisions

2.1. To use the Quick Access, the User:

2.1.1. downloads Citadele mobile application to a mobile device;

2.1.2. registers on the Mobile Website using Authenticators in accordance with the procedure determined by the Bank and safe authentication requirements;

2.1.3. if the User does not have MobileScan, he/she enters the unique confirmation code sent by the Bank in the Mobile Website and activates MobileScan in the Mobile Device, creating the PIN Code, as well as activates the use of the Biometric Authenticator if the Mobile Device supports it.

2.2. After the creation or entering of the PIN Code in the mobile application, the Quick Access is activated without the User's separate order.

2.3. The Bank has the right at any time to add new services to the mobile application, incl. Mobile Website, and such new services will be available to the User, incl. with the Quick Access, as well as the Bank has the right to partially or completely disable the Quick Access or disable the Quick Access for some types of Transactions or ancillary services without the User's consent.

2.4. When creating or entering the PIN Code, the Quick Access service is activated on each User's Mobile Device separately.

2.5. The Bank has the right to charge a fee for the use of the Quick Access and ancillary services, indicating it in the Pricelist.

2.6. The Bank has the right to use Mobile Notifications sent via the Information Channel for communication with the User, incl. for informing the User regarding issues related to the use and service of the Online Banking, Mobile Website and other services of the Bank. Mobile Notifications are prepared and sent to the Client 24/7 in the language selected on the Mobile Website.

2.7. In order to receive Mobile Notifications, the User shall activate this option in the Mobile Website of the respective Mobile Device. The Bank is entitled to send notifications that are part of the Mobile Website functionality, for which the Client does not have to apply separately.

2.8. The Client is aware that an internet connection is required to receive mobile notifications. The Bank deletes mobile notifications to be sent within the framework of the Service and does not send them to the Client, if the Mobile Website is disconnected from the internet for the period exceeding 24 hours.

2.9. The User is aware that the content of Mobile Notifications will be available even if the Mobile Device is blocked by the Access Code, except if the User has deactivated such option in the Mobile Device. 2.9. The Bank has the right to temporarily disable access to Mobile Notifications, if required, in order to perform a checkout of the hardware used for the provision of the Service.

2.10. The Terms of Use and Service of Citadele Online Banking may also apply to the issues regulated in this Annex. The Terms of Use and Service of Citadele Online Banking shall apply to the issues not covered by this Annex.

3. Quick Access Procedure

3.1. Using the Quick Access, the User may execute the following Transactions:

3.1.1. make any payments that are available to the User in accordance with the usage mode stipulated in the Service Agreement and which are supported on the Mobile Website;

3.1.2. temporarily block payment cards, unblock them, and use other options of management of the User's cards available on the Mobile Website;

3.1.3. access the templates available in the Online Banking, create new ones, change the existing templates and delete them;

3.1.4. change settings of the Mobile Website, including the activation and deactivation of the actions and services offered on the Mobile Website;

3.1.5. log in to and make payments on websites of other goods/service providers as well as log in to the Bank's mobile application for the use of additional services offered in the application;

3.1.6. receive information about the balances of the Accounts and performed transactions;

3.1.7. manage the User's Citadele loyalty program account;

3.1.8. receive additional services offered in the Bank's mobile application and Mobile Website.

3.2. The User shall use the Quick Access in accordance with the provisions of the Annex and Service Agreement, including the Transaction Terms, which the Bank is entitled to change at any time without prior notice.

3.3. Upon performance of the actions referred to in Sub-paragraphs 2.1 of the Annex, the User may access the Quick Access services provided on the Mobile Website using the PIN Code or Biometric Authenticator if the User has activated the use of the Biometric Authenticator on the Mobile Device and the Mobile Website.

3.4. Payments initiated using the Quick Access:

3.4.1. are performed taking into account all limits set in the Online Banking as well as special restrictions set by the Bank separately for Payments to be executed using the Quick Access;

3.4.2. are executed in accordance with the GTB and Terms of Account Opening and Service as well as by applying fees specified in the Pricelist or an agreement, unless otherwise specified in the Annex or the Transaction Terms;

3.5. For execution of some types of Payments, the Bank is entitled to request the User to perform full connection to the Online Banking in accordance with procedures established by the Bank or to take other additional security measures before execution of the Payment.

3.6. The Bank is entitled not to execute the Payment initiated using the Quick Access if:

3.6.1. the User's access to the Online Banking is blocked or annulled;

3.6.2. Payment amount exceeds the limit;

3.6.3. The User has failed to comply with the Transaction Terms;

3.6.4. other circumstances specified in regulatory enactments, GTB, Service Agreement or Bank's Service Agreements occurred.

3.7. Information about the Transactions initiated using the Quick Access is available in the Online Banking as well as in the Bank's premises.

3.8. If the Order submitted using the Quick Access has not been executed, the Bank shall inform the User thereof by sending an appropriate notice via Citadele mobile application if the Client has applied for receiving notifications via Citadele mobile application.

3.9. The User may use the Quick Access for execution of Transactions on behalf of the Clients - both natural and legal persons - who have authorized the respective User to use MobileScan in accordance with the procedure established by the Bank.

4. Security Requirements

4.1. In order to use the Quick Access service, the User's connections and Mobile Devices as well as other necessary tools shall comply with the Bank's technical and security requirements. Otherwise, the Bank is entitled to set restrictions on the use of the Quick Access or to prohibit the use completely.

4.2. The User shall protect access to his/her Mobile Device by means of the Access Code and shall ensure that the Access Code is not accessible to third parties. The Access Code used for the Mobile Device shall not be recorded on data carriers and stored together with the Mobile Device.

4.3. The User undertakes to use the Quick Access only himself/herself, not to disclose the PIN Code and Access Code of the Mobile Device, and to ensure that third parties cannot get access to such codes.

4.4. If the Mobile Device is lost or stolen, the User shall immediately inform the Bank and the Bank shall block the Mobile Device, or the User immediately shall block such device on the Online Banking depending on which action may be taken faster.

4.5. The User shall ensure that only the Biometric Authenticators of the respective User are stored in the Mobile Device, and Biometric Authenticators of other persons that may be registered in the User's device are deleted before activation of Biometric Authenticators on the Mobile Website.

4.6. Use of the Biometric Authenticator on the Mobile Website is activated together with MobileSCAN. Authentication using the Biometric Authenticator is carried out using the technology of the manufacturer of the Mobile Device, therefore the Bank does not process or store the User's biometric information.
4.7. All Orders that are submitted or Transactions that are confirmed using the PIN Code or Biometric Authenticator are binding upon the Client/ User.
4.8. The Bank is entitled, at any time, without prior notice, including for security purposes (for example, if the Login Name or any Authorization Device is blocked), to deactivate the Quick Access on one or more Mobile Devices, on which the Quick Access have been activated.

5. Liability of the Parties
5.1. The Bank is liable for non-execution or improper execution of the User's Orders, unless otherwise provided for in the Annex, Service Agreement or regulatory enactments.
5.2. The Bank is not responsible for non-execution or late execution of the Order, if the Order was not received or received with a delay for reasons beyond control of the Bank, including due to the fault of a mobile operator or other persons providing mediation services in connection with the Order.
5.3. The User is responsible for the security of his/her Mobile Device and connections.
5.4. The Client/User is responsible for:
5.4.1. for all Orders and Transactions, unless otherwise provided for in the Annex, Service Agreement or regulatory enactments;
5.4.2. the accuracy and timeliness of the data provided to the Bank using the Quick Access service.

6. Amendment of the Annex and Termination of Use of the Quick Access Service
6.1. The Bank is entitled to amend the Annex unilaterally. The amending procedure is stipulated in the Terms of Service.
6.2. The User is entitled to discontinue the use of the Quick Access service on the respective Mobile Device by disabling MobileSCAN in the settings of the Mobile Website at any time.
6.3. Deactivation of the Quick Access service is performed on each Mobile Device separately.
6.4. The Bank is entitled to deactivate the Quick Access on the Mobile Device unilaterally, without any prior notice, if:
6.4.1. The Bank has information that shows that:
6.4.1.1. the Mobile Website is used against the Client/User's will, or when the User carries out fraudulent or other illegal activities;
6.4.1.2. a mobile communications agreement between the Client/User and a mobile network operator has been terminated, or the Client/ User's mobile telephone number has been changed;
6.4.2. The User has not used the Quick Access for three consecutive calendar months;
6.5. The Annex loses force and the Quick Access is annulled when the Service Agreement is terminated.

7. Use of Cookies
7.1. The Bank uses functional cookies stored on the Mobile Device to maintain and improve Citadele mobile application:
7.1.1. FireBase (statistics and analysis). It accumulates event data when the User performs actions on the Mobile Website, for example, the User has connected to the Mobile Website. The User's activity data is used in an anonymized way to understand how the Users use the application and the Mobile Website, which functions they use. It is not possible to identify a particular User using the accumulated data.
7.1.2. Fabric (crash and problem analysis). It accumulates data on the use of the Mobile Website, in particular about its crashes and errors and installation data of Citadele mobile application. Information about the device and the version of Citadele mobile application installed in it and other information is used to help detecting and troubleshooting problems, in particular with regard to Citadele mobile application software and the use of the Mobile Website. For this type of analysis, Fabric uses a device identifier. It is not possible to identify a particular User using such data.
7.2. The Bank is entitled to change functional cookies at its own discretion. Information about the cookies that were used the User may receive at the Bank, incl. in Citadele mobile application.