**REPUBLIC OF TURKIYE**
**BANKING REGULATION AND SUPERVISION AGENCY**

**Issue: 77574904-010.06.02**
**Subject:** Regarding the Criteria to be Provided for Identification and Transaction Security in Electronic Banking Services and Establishment of Contractual Relationships in Electronic Environment

# CIRCULAR
# (2023/1)

As it is known, Articles 34 and 35 of the Regulation on Information Systems of Banks and Electronic Banking Services ("BSEBY"), which entered into force after being published in the Official Gazette, dated 15/03/2020 and numbered 31069, regulate how authentication and transaction security should be carried out in electronic banking service channels and that techniques should be used to enable non-repudiation and assignment of responsibility for both the bank and clients in transactions to be carried out through these channels, Articles 38 and 39 of the BSEBY include additional provisions on these issues specific to internet banking and mobile banking distribution channels.

On the other hand, in the second paragraph of Article 12 of the Regulation on Remote Identification Methods to be Used by Banks and Establishment of Contractual Relationship in Electronic Environment ("UKTY") published in the Official Gazette dated 01/04/2021 and numbered 31441, the following provisions are included by referring to Articles 38 and 39 of the BSEBY:

*"(2) Following the remote identification within the conditions set forth in this Regulation or face-to-face authentication of the client identity through the branches, in order to establish a contractual relationship that will replace the written form over an information or communication device for the transactions desired to be performed by the clients, whether remotely or not; it is essential that*

*a)* ***All terms and conditions of the said agreement are communicated to the client via internet banking or mobile banking distribution channels in a manner that the client can read,***

*b) The contract transmitted to the client according to subparagraph a) and the client's declaration of will establishing the contract together with this contract are signed with the* ***client-specific encryption secret key specified in the third paragraph of Article 38 and the first paragraph of Article 39 of the BSEBY and transmitted to the bank****,*

*c)* ***According to subparagraph (a), ensuring that the client signs only the information specified as the contract content in the contract transmitted to the client according to subparagraph (b),***

Similarly, Articles 12 and 13 of the Regulation on Remote Identification Methods to be Used by Financial Leasing, Factoring, Financing and Savings Financing Companies and Establishment of Contractual Relationship in Electronic Environment (UKTY-2) published in the Official Gazette dated 11/01/2022 and numbered 31716 include the following provisions:

***Authentication and transaction security***

***ARTICLE 12 –*** *(1) Except as otherwise provided in this Regulation, for services provided electronically, except for transactions that do not give rise to financial consequences or obligations, such as the display of client information, it is essential that the company applies an authentication mechanism consisting of at least two independent components to its clients and takes measures to ensure the confidentiality of the identification data contained in these components during their use in the identification process. These two components are selected to belong to two different classes of elements that the client "knows", "has" or "has a biometric characteristic of". Component independence means that the compromise of one component does not jeopardize the security of the other component. It is essential that the component owned by the client is unique to the client and cannot be forged.*

*...*

*(13)* ***For the identification process to be performed in accordance with the first paragraph for services provided in electronic environment, a single-use verification code shall be generated to be signed with an encryption secret key assigned to the client.*** *It is ensured that no information about any of the authentication elements specified in the first paragraph can be obtained through the verification code, no other valid verification codes can be derived from a known verification code, and verification codes cannot be forged. Where it is not possible to sign the verification code with a cryptographic secret key assigned to the client, the verification code may be transmitted to the client via SMS, without prejudice to the provision of the seventh paragraph.*

*(14) In the case of an electronic service provided through a mobile application, the two-component authentication referred to in the first paragraph shall be deemed to be fulfilled if the application PIN or a biometric authentication component belonging to the client is used to access a client-specific encryption key and, through this encryption key, a unique information relating to the client is verified online with the company.*

***Establishment of the contractual relationship following identification***

***ARTICLE 13 –*** *(1)* ***In the event that the contractual relationship for the transactions intended to be performed by the clients is established remotely through internet or mobile service channels*** *following remote identification within the conditions set forth in this Regulation or face-to-face identification of the client's identity,* ***the client's declaration of will establishing the contract must be received through the same channels after an identity verification performed in accordance with the first paragraph of Article 12.***

*(2) Following the remote identification or face-to-face identification of the client identity within the conditions specified in this Regulation, in order to establish a contractual relationship that will replace the written form through an information or communication device for the transactions desired to be performed by the clients, whether remotely or not, it is essential that*

*a)* ***All terms and conditions of this agreement are available for the client to read on the internet or to the client through mobile service channels,***

*b) The contract transmitted to the client in accordance with subparagraph a) and the client's declaration of will establishing the contract together with this contract are* ***signed with the***

***client-specific encryption secret key specified in paragraph thirteen and paragraph fourteen of Article 12 and transmitted to the company,***

*c)* ***According to subparagraph (a), ensuring that the client signs only the information specified as the contract content in the contract transmitted to the client according to subparagraph (b),***

In addition, the fourth and fifth paragraphs of Article 13 of the Regulation on the Operating Principles of Digital Banks and Bankins As A Service Model (DBY) published in the Official Gazette dated 29/12/2021 and numbered 31704 include the following provisions:

*(4) In order for the service bank to provide banking services to the client of the interface provider, a contractual relationship must be established between the client and the service bank in accordance with Article 76 of the Law.* ***In the event that the contractual relationship is established electronically, the process must be carried out in accordance with the UKTY and the identification of the client must be carried out by the service bank in accordance with the UKTY. If the process of establishing a contractual relationship between the service bank and the client is initiated through the interface provider's mobile application or internet browser-based interface and completed through these service channels, it is the service bank's responsibility to ensure that the interface provider's service channels in question comply with the security criteria set out in the BSEBY and provide assurance that only the information shown to the client as contractual content is approved by the client.***

*(5)* ***The interface provider and the service bank are jointly and severally responsible for ensuring that the interface provider's mobile application or internet browser-based interface used by the client*** *to access the services offered by the service bank* ***complies with the verification and transaction security obligations regarding electronic banking services in the third part of the BSEBY****. The service bank may not provide service model banking services or support services to interface providers that do not fulfill these obligations or whose systems are inadequate to fulfill these obligations.*

In this context, in order to clarify how to apply the provisions of the said regulation in a uniform manner without compromising transaction security and to eliminate any hesitations that may arise regarding the said provisions, it is hereby notified that the attached explanations approved by the Board Decision dated 23.03.2023 and numbered 10546 taken within the framework of the second paragraph of Article 76 and Article 93 of the Banking Law No. 5411 and Articles 15, 22, 38, 39 and 39/A of the Financial Leasing, Factoring, Financing and Savings Finance Companies Law No. 6361 should be taken into consideration in the implementation of these provisions. 03.2023 dated March 23, 2023 and approved by the Board Decision No. 10546 should be taken into consideration.

**Mehmet Ali AKBEN**
**Chairman**

**Annex: Explanations**

**ADDITIONAL EXPLANATIONS ON THE CRITERIA TO BE MET FOR IDENTIFICATION AND TRANSACTION SECURITY IN ELECTRONIC BANKING SERVICES AND THE ESTABLISHMENT OF CONTRACTUAL RELATIONSHIPS IN ELECTRONIC ENVIRONMENT[1] [2]**

***1.*** **Use of Client-Specific Encryption Secret Key and Transaction Signing (BSEBY Article 34-38-39):**

As it is known, the third paragraph of Article 38 and the first paragraph of Article 39 of BSEBY stipulate the following provisions:

*(3) For the authentication process to be performed in the internet banking distribution channel in accordance with the first paragraph of Article 34,* ***a single-use verification code shall be generated to be signed with an encryption secret key assigned to the client****. It is ensured that information cannot be obtained about any of the verification elements specified in the first paragraph of Article 34 through the verification code, that other valid verification codes cannot be derived from a known verification code, and that verification codes cannot be forged.* ***It is ensured that verification codes for transactions with financial implications are specific to the amount and recipient information approved by the client at the time of the transaction, and that any change in the amount or recipient information to which the funds will be transferred invalidates the relevant verification code generated according to this information.*** *For transactions such as fund transfers for corporate internet banking clients where bulk transactions are allowed for multiple recipients in bulk, the verification code to be generated must be specific for the total amount of the relevant bulk transaction and the recipients. Where it is not possible to sign the verification code with a cryptographic secret key assigned to the client, the verification code may be transmitted to the client via SMS, without prejudice to paragraph seven of Article 34.*

*(1) The two-component authentication referred to in the first paragraph of the Article shall be deemed to be fulfilled if* ***the application PIN defined in the mobile banking application is used to access a client-specific encryption key and, through this encryption key, a unique piece of information relating to the client is <u>verified online with the bank</u>****.*

---

[1]The terms “bank” in the explanations attached to this Circular shall be deemed to refer to the relevant institutions (Companies) for institutions subject to 6361 and “internet banking” or “mobile banking” distribution channels;

i. For institutions subject to Law No. 6361 and other institutions other than banks subject to the supervision and audit of the Agency, as distribution channels through which such institutions provide services to their clients via internet or mobile devices;
ii. Pursuant to the first paragraph of Article 8 of the Law No. 6361, for the information systems or platforms determined by the Board, which are permitted to carry out transactions as an exception to the prohibition of organization and agency other than branches, the distribution channels through which such information systems/platforms provide services to their customers via internet or mobile devices shall be considered as distribution channels.

[2] Pursuant to the second paragraph of Article 39 of the Law No. 6361, in order for the financing companies to establish a general contractual relationship with the sellers who provide the goods or services to be credited by using distance communication tools, the sellers in question, who are real or legal person merchants, shall be considered as the clients of the financing companies; identify these clients with the status of vendors in accordance with the Agency's regulations on remote identification of real or legal person clients and establish an electronic contractual relationship with these clients with the status of vendors in accordance with the explanations in the annex of this Circular.

*Similarly, the two-component authentication referred to in the first paragraph of Article 34 shall be deemed to be fulfilled if a biometric authentication component belonging to the client is used in a mobile banking application to access a client-specific encryption key and, through this encryption key, a unique piece of information relating to the client is verified online with the bank.*

Under these provisions, the uses of an encryption secret key assigned and personalized to the client: comprises of

1. Identification,
2. Authorization (transaction verification)

And in order to perform authentication and authorization transactions in both the internet banking distribution channel and the mobile banking distribution channel, which is a specialized version of this distribution channel, it is required to generate a "verification code" and sign it with a client-specific encryption secret key.

On the other hand, the first paragraph of Article 38 and the second paragraph of Article 39 of the BSEBY stipulate the following provisions:

*(1) The authentication process to be carried out in the internet banking distribution channel in accordance with the first paragraph of Article 34* ***must take place online at the bank, not locally offline****, and the element known to the client must not be automatically sent by the mobile banking application or internet browser by remembering or linking this element to other local authentication methods.* ***The element known to the client*** *is required to be entered by the client and, without prejudice to the provisions of the second paragraph of Article 34****, this element is verified online at the bank and not locally.***

*(2)* ***Password, PIN or biometric data, which are not under the control of the mobile banking application but under the control of the device manufacturer, cannot be used as elements that are known to the client or biometric characteristics specified in the first paragraph of Article 34.***

When these provisions of Articles 38 and 39 of the BSEBY are evaluated together, it is required that the "**client known element" such as "PIN" to be used to access the encryption secret key before content signing should be verified online at the bank, not locally on the device where the mobile application is installed**.

In this respect, if the bank uses the elements to be used by its clients for authentication and transaction signing in accordance with the explanations provided in the annex of this Circular, the provisions of Article 34, paragraph fifteen of the BSEBY shall be applied:

*(15) The Bank shall take measures to ensure that sensitive data used by banking applications on mobile devices such as smartphones, which are used to transmit multiple authentication components to the Bank, are inaccessible to other applications and running transactions on the same mobile device. In case of loss or theft of these mobile devices, the Bank shall ensure that the sensitive data on them are inaccessible to unauthorized persons. and to establish controls in accordance with the state-of-the-art technology in order to reduce the risks arising from situations such as interception of mobile devices, deterioration of their reliability, cracking or modification of the operating system software.*

The conditions of the provision will also be deemed to have been fulfilled.

**In addition, pursuant to Article 34, paragraph seven and Article 38, paragraph three of the BSEBY, clients who have installed and activated the mobile banking application, except in cases of initial installation, activation, re-activation or unavailability of the mobile banking application; it is not possible to send an OTP or "verification code" via SMS for the verification of any transaction during login or continuation of the session, and such notifications to be made via SMS should only be used in exceptional cases specified in these provisions and should not be made a routine practice. Because there is no guarantee that the OTP or verification code sent via SMS will not be read by other applications installed on the same mobile device and directed to a third party (e.g. an attacker) by these applications, and since the "SMS messaging application" on the mobile device is not a mobile application under the bank's own control, it is natural that there may not be sufficient assurance regarding the integrity or reliability of the OTP or verification code to be displayed to the client via SMS.**

***2.*** **The Principle of Ensuring that Transaction Signing/Confirmation is Performed According to the Information Provided for Client Approval (BSEBY Article 35-38 / UKTY Article 12):**

According to Article 35 of the BSEBY on "non-repudiation and assignment of responsibility", banks are required to use techniques that **enable non-repudiation and assignment of responsibility** for both themselves and their clients in transactions carried out within the scope of the electronic banking services they offer.

According to the third paragraph of Article 38 of the BSEBY, **verification codes for transactions with financial consequences should be specific according to the amount and recipient information approved by the client when performing the transaction, any change in the amount or recipient information to which the funds will be transferred should invalidate the relevant verification code generated according to this information, and verification codes should be generated for single use, signed with an encryption secret key assigned to the client**.

Pursuant to the fourth paragraph of Article 38 of the BSEBY, it is stipulated that "***at each stage of the verification process, including the creation, transmission and use of the verification code for transactions with financial consequences carried out by the client, necessary measures shall be taken to ensure the confidentiality, reliability and integrity of the information displayed to the client and submitted for approval,*** *such as the amount and recipient information, and against the risk that data communication during the internet banking session is directed to unauthorized persons*".

It is therefore essential that the transaction verification code is securely signed with a client-specific encryption secret key and that the signed content is verified by the bank to fulfill confidentiality and integrity controls.

As such, the process of distribution of encryption secret keys to clients and how clients access these keys to sign content is equally important. The following provisions in the fourth and fifth paragraphs of Article 34 of the BSEBY underline this point:

*(4) The security of the components to be used in the authentication mechanism to be applied to the users is ensured throughout the entire process starting from the production stages until they are delivered to the user.*

*(5) Encryption keys to be used in authentication are made available to clients in a way that minimizes the possibility of these keys being intercepted, ensures their confidentiality, and includes methods that prevent them from being changed and corrupted.*

As these provisions of BSEBY make clear, even if the client is provided with a cryptographic secret key assigned to it to sign verification codes, BSEBY also expects these signing processes to incorporate techniques that enable non-repudiation and assignment of responsibility, In other words, it is necessary both to ensure that the encryption secret key assigned to the client is securely assigned to the client and that it is personalized to the client, and to establish measures to prevent its use by unauthorized persons, and to ensure that the content signed by the client is actually the content that the client has seen and approved.

Article 12 of the UKTY provides the following provisions by referring to Articles 34, 38 and 39 of the BSEBY:

*"(1) In the event that the contractual relationship is established at a distance for the transactions intended to be performed by the clients for whom any of the internet banking or mobile banking distribution channels regulated in the BSEBY are open for use following remote identification within the conditions set forth in this Regulation or face-to-face identification of the client identity through the branches, the client's declaration of will establishing the contract must be received through the said distribution channels after an* ***identification performed in accordance with the first paragraph of Article 34 of the BSEBY.***

*(2) In order to establish a contractual relationship that replaces the written form through an information or communication device for the transactions desired to be performed by the clients, whether distance or not, following the remote identification within the conditions specified in this Regulation or face-to-face identification of the client identity through the branches, it is essential that*

*a)* ***Communicating all terms of the agreement to the client via internet banking or mobile banking distribution channels in a manner that the client can read****,*

*b) The contract transmitted to the client according to subparagraph (a) and the client's declaration of will establishing the contract together with this contract* ***are signed with the client-specific encryption secret key specified in the third paragraph of Article 38 and the first paragraph of Article 39 of the BSEBY and transmitted to the bank,***

*c)****According to subparagraph (a), ensuring that the client signs only the information specified as the contract content in the contract communicated to the client according to subparagraph (b),***

Articles 12 and 13 of the UKTY-2 contain similar provisions aiming at the same issues, and all these provisions in essence express the principle (**WYSIWYS**) of ensuring that the transaction signing/approval is carried out according to the information provided to the client for approval. Therefore, the signing process to be carried out with client-specific encryption secret keys must be in compliance with these provisions and this principle in order to establish a contractual relationship at a distance with clients whose internet banking or any of the mobile banking distribution channels are open for use, or to establish a contractual relationship with clients over an information or communication device as a substitute for the written form.

**In this respect, the methodology to be used in order to ensure that such signing operations comply with the above-mentioned provisions and the WYSIWYS principle must comply with the following explanations:**

1. First and foremost, to create a secure environment within its mobile application for use in transaction signing and to fulfill its obligations arising from Article 34, paragraph fifteen of BSEBY the bank must establish:
   i. A specific Software Development Kit (SDK), and
   ii. A Security Server (SS) configured to communicate directly with this SDK through a secure, dedicated channel.

2. The client-specific encryption secret key to be used in transaction signing and the corresponding public key (asymmetric key pair) must be stored on the client's mobile device on which the mobile banking application is installed, which can generate asymmetric key pairs and store the encryption secret key from the generated key pairs in a way that does not allow it to be copied and extracted (“Secure Enclave” for iOS devices), The cryptographic hardware (such as “hardware backed keystore” or “Strong Box” for Android devices) must be created by the SDK on the cryptographic hardware unit and the encryption secret key created by the SDK for the client must be stored on these hardware units and can only be used by the SDK for signing. The encryption secret key shall be “client specific”, meaning that it shall be a secret key specific to the mobile device binded to the client and the activated SDK instance on that device.

Algorithms and key lengths to be used in generating asymmetric key pairs must be selected in accordance with the current technology within the framework of the second paragraph of Article 9 of BSEBY.

3. It must be ensured that "signing requests" for the client-specific encryption secret key, which is generated by the SDK to the cryptographic hardware unit on the client's mobile device and can only be used by the SDK in the signing process, are sent by the SS to the SDK instance activated for the client, only after the security checks to be performed by the SS and only after being encrypted with the client-specific public key, which is the other pair of the client-specific encryption secret key among the asymmetric key pairs specified in Article 2.

4. In order for the SS to request a signature on the relevant SDK instance, the SS must perform security checks to confirm that the relevant SDK instance is running on the secure mobile application and secure mobile device through security sensors running continuously in the background, and the risk data from these security sensors must be transmitted to the SS through a separate secure out-of-band channel allocated between the SDK and the SS.

5. The safety sensors of the SDC shall generate the necessary risk data to be transmitted to the SS, in accordance with article 34, paragraph fifteen, of the BSEBY, on a continuous basis, ensuring at least the following controls
    *i.* Regarding the deterioration of mobile application reliability and integrity controls
        a) Controls to prevent sensitive data from being stolen while being entered through the user interface (**anti-keylogging**)
        b) Checks that the running SDK code is not modified at runtime and that no malicious code fragments are inserted (**anti-injection**)
        c) Checks whether the running SDK code is running in a debugger environment, emulator environment or virtual machine (**anti-debugging and anti-emulation**)
        d) Checks that the activated mobile banking application and SDK only work on the mobile device registered during activation (**device-binding**)
    *ii.* Regarding the deterioration of mobile device reliability and integrity controls
        a) Checks to see if the mobile device has been infected or compromised by malware (**anti-malware**),
        b) Checks on whether the mobile device operating system has been broken or not (**jailbreaking**),

6. In order to ensure the security of the channel between the SS and the SDK, during the initial activation of the mobile banking application and the SDK, a secure TLS connection must be established between the not-yet-activated SDK instance and the SS through the SS's server certificate, and then the encryption secret key from the asymmetric key pairs generated by the SS, specific to the activated SDK instance and the mobile device, must be transmitted to the relevant SDK instance over this secure connection and stored encrypted in a secure area under the control of the

SDK. The “secret” one of the asymmetric key pairs generated for the SDK instance activated by the SS should not be stored by the SS and should be deleted as soon as it is transmitted to the relevant SDK instance, while the “public” one of these key pairs should be signed by the SS and converted into a client certificate assigned to the relevant SDK instance and transmitted to the relevant SDK instance over the said secure connection. After these steps, it should be ensured that an end-to-end secure communication channel is established through a bidirectional mTLS connection (Mutual TLS) by using the server and client certificates in question in the communication between the relevant SDK instance and the SS, and that this communication channel is configured as a secure separate channel (Out-of-Band) separate from the communication channel between the mobile banking application and the bank back-end and dedicated only to the communication between the SS and the SDK. Algorithms and key lengths to be used in asymmetric key pair generation must be selected in accordance with the current technology within the framework of the second paragraph of Article 9 of BSEBY.

7. Provided that each SDK instance has passed the SS's reliability and integrity checks on the risk data it generates through the security sensors specified in clause 5, it must be enabled to send a verification request to the SS for the PIN/known element entered by the client through the client certificate assigned to it by the SS over an end-to-end secure communication channel established as specified in clause 6.

8. During the first activation of the mobile banking application and SDK, it is required that

*i.* The PIN or password that the client will use as a “known element” is converted into a cryptographic hash by the SDK and sent to the SS, and this cryptographic hash is converted into a salted hash and stored in an encrypted form in the SS database;

*ii.* The activated SDK instance generates a client-specific asymmetric key pair as per point 2 and transmits the “public” key to the SS,

*iii.* The SS also acts as a “Certificate Authority”, generating a client-specific certificate for the client-specific public key transmitted to it by the activated SDK instance, using that certificate to verify the content signed by the client, and invalidating that certificate when the SDK instance needs to be retired

9. The PIN/known element information referred to in Article 8 or the cryptographic hash data related to this element shall not be stored by the SDK in any way and shall be deleted by the SDK immediately after the verification request is sent and the PIN/known element or the cryptographic hash data related to this element shall not be stored in plain text in the SS database, in that database, the hash data sent by the SDK must be converted into a salted-hash and stored in the SS database only in encrypted form.

10. The verification request for the PIN/known element that the SDK sends to the SS shall be verified online by comparing the hash of the PIN/known element entered by the client with the salted-hash of the PIN/known element in the SS database, as specified in section 1 of the explanations annexed to this Circular and in accordance with the third paragraph of Article 11 of the BSEBY.

11. If the customer successfully completes the PIN/known factor authentication process as outlined in Article 10, the following steps must be ensured;
    *i.* The SS must send an authentication-specific "transaction signing request message" (challenge) to the SDK, encrypted using the public key contained in the customer-specific certificate specified in Articles 3 and 8, through a dedicated secure channel between the SS and SDK,
    *ii.* Upon receiving this message, the SDK must decrypt it using the customer-specific encryption private key stored in the cryptographic hardware unit of the customer's mobile device. The SDK must then sign an authentication-specific "transaction signing approval message" (response) with the same key to generate an authentication-specific verification code and transmit it to the SS,
    *iii.* The SS must verify the validity of the verification code received from the SDK by decrypting it with the customer-specific public key,
    *iv.* For the verified verification code, the SS must send a message through its end-to-end secure communication channel with the bank's back-end system, instructing the back-end to log the user in. The back-end must then complete the login process for the user,
    *v.* Upon completion of these steps, a timestamp must be created for the relevant verification code and transmitted to the bank's log server.

    To prevent replay attacks on the challenge-response messages, it is mandatory to include a unique, single-use value (nonce).

12. Using the customer-specific encryption private key stored in the cryptographic hardware unit of the customer's mobile device—accessible exclusively by the activated instance of the SDK—the following must be ensured,
    *i.* The authentication-specific verification code generated by the SDK,
    *ii.* The verification code generated by the SDK for financial transactions, tailored specifically to the amount and recipient information confirmed by the customer based on the information displayed by the SDK,
    *iii.* The electronic signing by the customer of agreements to be established electronically, reflecting the customer's approval and declaration of intent based on the information displayed by the SDK.

    must be securely signed with the customer's electronic signature

13. Within the scope of Article 12, before the content is displayed to the customer by the SDK for signing financial transactions or electronic agreements (12.ii and 12.iii), the transactions initiated by the customer must first be transmitted by the mobile banking application to the back-end server. The back-end server must then forward this customer request via an end-to-end secure channel to the Security Server (SS) for verification. Following the transmission of the customer request from the back-end to the SS, the process must include the following steps:

    *i.* The SS, via the dedicated secure channel between the SS and the SDK, sends a "transaction signing request message" (challenge) to the SDK. This message must be encrypted using the public key from the customer-specific certificate specified in Articles 3 and 8,

    *ii.* Upon receiving this message, the SDK decrypts it using the customer-specific encryption private key located in the cryptographic hardware unit of the customer's mobile device. The SDK then displays a confirmation screen for the customer,

    *iii.* If the customer approves the information displayed on the confirmation screen, the SDK signs the approved information with the customer-specific encryption private key to generate a "transaction signing approval message" (response) and sends the corresponding verification code to the SS,

    *iv.* The SS verifies the validity of the verification code sent by the SDK by decrypting it using the customer-specific public key and compares the decrypted data with the information transmitted from the back-end to ensure data integrity and accuracy.,

    *v.* For the verified verification code, the SS sends a message to the back-end via the end-to-end secure communication channel between the SS and the back-end, instructing it to process the relevant transaction. Subsequently, the back-end executes the transaction for which the verification code was generated,

    *vi.* Upon completion of these steps, a timestamp is generated for the relevant verification code and transferred to the bank's log server.

    The challenge-response messages must include a one-time value (nonce) to prevent replay attacks.

14. Under Article 10, following the successful verification of the PIN/known factor and, under Article 11, the creation of a valid verification code using the customer-specific encryption private key classified as the possession factor, the user session opened after the two-factor authentication-based login will remain valid for its duration.
    During this session;

*i.* The verification code generated by the SDK for financial transactions must be specific to the amount and recipient information approved by the customer, as displayed by the SDK,

*ii.* The electronic agreements to be established in the electronic environment reflecting the customer's approval and declaration of intent, as displayed by the SDK, must be signed using the customer-specific encryption private key in accordance with Article 12.

In these processes, the customer is not required to repeat the PIN/known factor verification. However, under the third paragraph of Article 39 of the Regulation on the Principles of Information Systems of Banks (BSEBY), provided that no more than 90 days have passed since the customer's last session, which was opened through two-factor authentication, re-verification of the PIN/known factor is not necessary for transactions that can be carried out using only the possession-based authentication factor. Nonetheless, for login processes and financial transactions conducted under this paragraph, a verification code must be generated using the customer-specific encryption private key in accordance with Articles 11 and 13.

**If the client only uses the internet banking distribution channel and has not activated the mobile banking distribution channel, or if both internet and mobile banking distribution channels are active but the mobile banking distribution channel is not available to the client due to a compelling reason;**

- **In the execution of login transactions**, after the client enters the known element, the hash of the known element is compared with the salted-hash values stored encrypted in the bank's database, and if they are compatible with each other, a one-time verification code for the login transaction is generated and sent to the client via SMS, and the login transaction is executed after the client enters the one-time verification code on the screen.
- **In order to execute transactions with financial implications**, it is mandatory to have a session that remains valid after a successful login. If a transaction with financial consequences is to be executed during such a session, the bank receiving the transaction request must generate a single-use verification code specific to this transaction (specific to the recipient and amount information) and transmit it to the client via SMS. After a successful login, the client enters the single-use verification code sent to him/her via SMS on a session screen that remains valid, and the relevant transaction is executed. **However, this process must be repeated every time the client wishes to perform a transaction that has financial consequences and a new verification code specific to each transaction must be sent to the client via SMS and entered on the screen.**
- **It is not possible for a client whose mobile banking distribution channel is not active and therefore does not have a "client-specific encryption secret key" to establish a contractual relationship subject to written form electronically through the internet banking distribution channel.**
- **It is possible for the client to submit the request to conclude a contract at a distance and the declaration of intent to conclude a contract via the internet**

**banking distribution channel**. For this purpose, it is mandatory to have a session that remains valid after a successful login. During such a session, the bank is required to generate a single-use verification code specific to the client's request to establish a contract submitted through the internet banking delivery channel or any other channel and transmit it to the client via SMS. After a successful login, the client must enter the verification code sent to him/her via SMS on a session screen that remains valid after a successful login and thereby transmit his/her declaration of will to the bank regarding the establishment of a distance contract.

**In cases where both the client's mobile banking distribution channel and internet banking distribution channel are active, but transactions are initiated through internet banking,**

- **In the execution of login transactions**, after the client enters the known element, the hash of the known element is compared with the salted-hash values stored encrypted in the bank database, and if they are compatible with each other, **the flow specified in Article 11 above for the login transaction is applied and a verification code is generated to be signed with the client-specific encryption secret key.**
- **In order to execute transactions with financial implications**, it is mandatory to have a session that remains valid after a successful login. If a transaction with financial consequences is intended to be executed during this session, the transactions initiated by the client through the internet banking distribution channel must first be transmitted to the back-end server and the back-end server must transmit this client request to the SS through the end-to-end secure channel for verification. After the client request is transmitted from the back-end to the SS, **the bank receiving the transaction request must execute the flow specified in Articles 11 and 13 above**.
- **It is possible for the client to initiate the process of establishing a contractual relationship subject to written form via the internet banking distribution channel**. For this purpose, it is mandatory to have a session that remains valid after a successful login. In the event that the client requests to establish a contractual relationship subject to written form during such a session, this request initiated by the client through the internet banking distribution channel must first be transmitted to the back-end server and the back-end server must transmit this client request to SS through an end-to-end secure channel for verification. After the client request is transmitted from the back-end to the SS, **the bank receiving the transaction request must execute the flow specified in Articles 11 and 13 above**.
- **It is possible for the customer to submit a request to establish a remote agreement and their declaration of intent to enter into such an agreement through the internet banking distribution channel**. For this purpose, it is mandatory to have an active session established following a successful login. During such a session, if the customer submits a request to establish a remote contractual relationship via the internet banking distribution channel or another channel, the back-end server must transmit this customer request to the Security Server (SS) for verification via an end-to-end secure channel.

After the transmission of the customer request from the back-end server to the SS, the bank must follow the process outlined **in Articles 11 and 13. Even if the remote contractual relationship being established is not subject to a written form requirement, the customer's declaration of intent to establish this agreement must be signed using the customer-specific encryption private key, and a corresponding verification code must be generated.**

### *3.* Ensuring that the Interface Provider's Mobile Application or Internet Browser Based Interface Complies with Authentication and Transaction Security Obligations (WBM Article 13):

As it is known, the fourth and fifth paragraphs of Article 13 of the DBY include the following provisions:

*(4) In order for the service bank to provide banking services to the client of the interface provider, a contractual relationship must be established between the client and the service bank in accordance with Article 76 of the Law.* ***In case the said contractual relationship is established electronically, the process must be carried out in accordance with the UKTY and the client identity must be determined by the service bank in accordance with the UKTY. If the process of establishing the contractual relationship between the service bank and the client is initiated through the interface provider's mobile application or internet browser-based interface and completed through these service channels, it is the responsibility of the service bank to ensure that these service channels of the interface provider comply with the security criteria set forth in the BSEBY and that the information shown to the client as the content of the contract is qualified to provide assurance that only that information is approved by the client.***

*(5)* ***The interface provider and the service bank are jointly and severally responsible for ensuring that the interface provider's mobile application or internet browser-based interface used by the client to access the services offered by the service bank complies with the authentication and transaction security obligations regarding electronic banking services in the third part of the BSEBY.*** *The service bank may not provide service model banking services or support services to interface providers that do not fulfill these obligations or whose systems are inadequate to fulfill these obligations.*

In this context, in addition to the fact that the mobile application or internet browser-based interface of the interface providers must comply with the authentication and transaction security obligations set out in the third section of the BSEBY, the authentication and transaction signing to be performed by the service bank client through the mobile application-based interface of the interface providers must comply with the explanations set out in sections 1 and 2 of the annex of this Circular. **On the other hand, it is not possible for interface providers to offer banking services of the service bank to their clients through internet-based service channels without a mobile application service channel.**

**In this respect, in accordance with the DBY, it is mandatory for those who will be engaged in interface provider activities to have mobile application service channels and to have the SDK of the service bank embedded in this mobile application interface and to execute transaction signing flows through the service bank Security Server (SS) configured to communicate with the service bank SDK embedded in this mobile application interface and this SDK through a separate dedicated end-to-end secure channel in accordance with the explanations specified in section 2 of the annex of this Circular.**

***4.*** **Adaptation of Products Used, Developed and Purchased for Authentication and Transaction Signing to the Descriptions in the Annex of this Circular:**

It is mandatory to ensure that the products and services used for authentication and transaction signing, developed or purchased in-house, comply with the explanations in the annex of this Circular.

The products and services developed or purchased within the Bank **must be addressed within the scope of the information systems audit to be performed** in accordance with the Regulation on Independent Audit of Information Systems and Business Processes published in the 6th Repeated Official Gazette dated 31.12.2021 and numbered 31706.

If the entities sell products or provide external services to banks, other institutions under the supervision and oversight of the Banking Regulation and Supervision Agency (the Agency), and interface providers within the scope of the DBY for use in authentication and transaction signing **they are required to demonstrate that their products and services comply with the explanations provided in the annex to this Circular. To do so, they must submit a report prepared by an independent audit firm listed in the "Authorized Independent Audit Firms for Information Systems Audits in Banks" document published by the Agency. These entities are obligated to apply to the Agency with this report and obtain authorization** to provide products and services in the fields of authentication and transaction signing to banks, other institutions under the Agency’s supervision, and interface providers.