Approved at
Resolution of the
Management Board
of the Central Bank of the
Republic of Azerbaijan
dated 21 December 2015

Protocol №__43__

S/Register №__316_

Methodological Guidelines

on supply and security of electronic banking services in the Republic of Azerbaijan

1. General provisions

These Methodological Guidelines determine the requirements on the types, delivery and use of and recommendations on boosting reliability and security of e-banking services in the Republic of Azerbaijan.

2. Definitions

2.1. The definitions used herein bear the following meanings:

2.1.1. **electronic banking service (hereinafter – the e-banking service)** – bank operations on a related account and/or data acquisition allowing user's remote access by means of relevant software, electronic authentication and communication facilities;

2.1.2. **user** – a bank account-holder using e-banking services and a person entitled to use e-banking services;

2.1.3. **electronic authentication** – is the process of authorization of a user and an operation by means of various hardware and/or software (electronic signature, user name and password, OTPs, symmetric encryption, use of simple session keys and others) when using e-banking services;

2.1.4. **transaction's reference number** – a unique identifier assigned to each transaction conducted via e-banking service;

2.1.5. **security procedures** – information security related software and hardware and a set of organizational measures provided for identification of users and transactions during electronic development, processing, sending and receiving of payment documents.

3. Types of e-banking services

3.1. The e-banking service is divided into informational and transactional e-banking depending on functional capabilities delivered to users and the level of potential risk:

3.1.1. The informational e-banking service is based upon data acquisition by a user. A bank or the national operator of postal communication (hereinafter – the bank) delivers information to users on bank accounts, conducted transactions and on its products and services via this service.

3.1.2. The transactional e-banking service allows users to make payments, transfer funds from accounts, convert currency and conduct other banking services.

3.2. The following types of the e-banking service is included to the scope of these Methodological Guidelines:

3.2.1. PC banking – e-banking services provided by communication channels over electronic devices by installation of dedicated software;

3.2.2. Internet banking – e-banking services by communication channels over electronic devices not installing dedicated software;

3.2.3. mobile banking – e-banking services by mobile communication channels (GSM, CDMA, 3G, HSPA+, WiFi, LTE etc.) over mobile devices (mobile phones, tablets, computers etc) installing or not installing dedicated software.

4. Maintenance and use of e-banking services

4.1. The e-banking service is based upon an agreement (soft or hard copy) signed between a bank and a user.

4.2. The bank briefs the user on the terms of use of e-banking service, an integral part of the agreement.

4.3. When supplying an e-banking service the bank:

4.3.1. eunsures safety of the server room, communication facilities and devices, as well as security of software used to conduct electronic transactions;

4.3.2. may provide users with authentication means (e-token, e-signature certificates etc) and relevant software;

4.3.3. regularly implements remote e-banking attacks prevention measures, specified in Annex 1, the integral part of these Methodological Guidelines;

4.3.4. identifies and verifies users under the requirements of the Law of the Republic of Azerbaijan on Prevention of the Legalization of Criminally Obtained Funds or other Property and the Financing of Terrorism;

4.3.5. accordingly notifies users (except for the cases specified in the Law of the Republic of Azerbaijan on Prevention of the Legalization of Criminally Obtained Funds or other Property and the Financing of Terrorism) in the order and under the period provided for in the agreement, if the cases specified in Item 4.6. herein occur;

4.3.6. provides the user with information on payment transactions periodically or at his/her request to validate whether the e-banking payment transaction is ordered and executed properly;

4.3.7. provides users with statements on the current status of payment transactions and on accounts;

4.3.8. ensures maintenance of information on payment transactions in line with the legislation.

4.4. The Bank informs the user without fail on the necessity of delivery of notification to the bank if:

4.4.1. funds in the bank account are used without authorization;

4.4.2. any error or mismatch is detected in transactions with the bank account;

4.4.3. suspicious cases on unauthorized access to authentication data are detected;

4.4.4. e-banking related technical malfunction is available or error occurs in identification methods.

4.5. The Bank notifies the user on maintaining secrecy of use of e-banking service and means of electronic authentication (keys, passwords etc.) according to the rules and procedures it has established and contractual terms and conditions.

4.6. The Bank should be entitled to temporarily halt or cancel supply of the e-banking service for the user in the following cases:

4.6.1. if the user violates bank's e-banking related rules and procedures or terms and conditions of the agreement signed between the bank and the user;

4.6.2. if supply of the e-banking service is technically impossible;

4.6.3. other cases specified in the legislation.

4.7. After the cases leading to suspension of supply of the e-banking service by the bank specified in Item 4.6 herein are eliminated, the bank accordingly notifies the user in the order and under the term specified in the rules and procedures or in the order specified in the agreement.

4.8. At least the following information is stored in the bank's internal information system on bank transactions conducted via the transactional e-banking service:

4.8.1. type of the e-banking service;

4.8.2. transaction's reference number;

4.8.3. transaction date and time;

4.8.4. transaction purpose;

4.8.5. transaction amount;

4.8.6. transaction currency;

4.8.7. requisites of the issuer bank (the one serving the payer) and the beneficiary bank (the one serving the payee);

4.8.8. requisites of the payer and the payee.

5. Recommendations on e-banking security

Recommendation 1: Risk management

5.1. The bank has dedicated procedures in place on e-banking security and risk management (hereinafter – security procedures).

5.2. Bank's e-banking related security procedures are approved by the bank's authorized management body and its implementation status is checked regularly.

5.3. E-banking related security procedures should provide for at least the following:

5.3.1. methods for maintaining data security to ensure information security;

5.3.2. methods for ensuring accuracy, reliability and integrity of the data sent, processed and stored between the bank and the user;

5.3.3. means for application of electronic authentication;

5.3.4. measures for authorized and physical access to data to limit user's unauthorized access to information;

5.3.5. where a third party (software and network supplier) is involved in supply of e-banking service, measures to be taken if the third party suddenly suspends its activity or fails to fulfill its contractual obligations;

5.3.6. organization of regular workshops to ensure segregation of authorities of IT staff and increase their expertise.

Recommendation 2: Evaluation of risks

5.4. The Bank monitors e-banking related risks in light of technological solutions, third party services and users' technical environment.

5.5. The Bank analyzes risk scenarios on main scenarios likely to impact e-banking services, and evaluates adequacy and effectiveness of security measures in place.

5.6. If risk evaluation reveals that changes should be made to existing e-banking related security measures, applied technologies and procedures, as well as services, the bank takes actions to minimize the probability and effect of possible incidents and frauds over the transition period required for changes.

5.7. Risk evaluation is analyzed at least annually and findings are presented to the bank's related management body.

Recommendation 3: Monitoring and accountability of the incident occurred

5.8. The Bank registers and monitors occurred security incidents, including security related user complaints in a real time mode and delivers reports on incidents to the bank's related management body and, if necessary, information on incident to the law-enforcement bodies.

5.9. The Bank maintains a register of e-banking related incidents, which includes at least:

5.9.1. type of e-banking (PC Internet and mobile banking);

5.9.2. transaction's reference number;

5.9.3. the cause of incident;

5.9.4. the content of incident;

5.9.5. the date and time of the incident;

5.9.6. measures taken to eliminate the incident.

Recommendation 4: Security measures and control over their implementation

5.10. The bank has relevant security solutions to protect network, web-site, servers and communication channels from abuse and attacks. To restrict use of fake web-sites, the web-site of the bank that provide transactional e-banking service is identified by extended validation certificates.

5.11. The Bank has relevant functionalities to control, track and restrict logical and physical access to resources like network, systems, database and security modules. The Bank creates, maintains and analyzes relevant logs and audit files.

5.12. The Bank audits e-banking related security measures annually. Reliable and independent (internal or external) specialists are attracted to the audit.

5.13. The Bank ensures that agreements signed with third parties on e-banking services provide for recommendations on security of the service specified herein.

5.14. In the event the third party suddenly halts its activity or fails to discharge its obligations, the Bank predetermines e-banking related contingency plans, appropriate methods and facilities.

Recommendation 5: Tracking of transactions

5.15. The Bank enables users to track all e-banking transactions, including the process of confirmation to execute transactions.

5.16. The Bank creates logs of any additions, changes or deletions to database on tracked transactions.

Recommendation 6: User identification and notification

5.17. Prior to delivery of the e-banking service the Bank discloses the following information to users in soft or hard copy:

5.17.1. register, technical specification, proper and safe use of equipment, software and other necessary facilities (antivirus programs, firewall etc.), as well as customized tools (PIN codes, e-tokens etc.);

5.17.2. steps of obtaining information, including entry and authorization of payment transactions in the system and/or results of each transaction;

5.17.3. measures to be taken in case of loss or theft of e-authentication facilities or devices and software to conduct payment transaction;

5.17.4. procedures applied in fraudulent and suspicious cases.

Recommendation 7: Stronger user authentication

5.18. Stronger user authentication is used depending on the amount of e-banking transaction and the level of risk.

5.19. The Bank may employ user friendly unified authentication methods for e-banking services.

Recommendation 8: Registration and supply of authentication methods and/or software delivered to users

5.20. To enable users to use e-banking services, the Bank ensures safe delivery and registration of authentication means and software to them.

5.21. Using Internet resources, the Bank ensures whole and intact delivery of software to users.

Recommendation 9: Attempts to access the system, session expiry and authentication accuracy

5.22. The Bank sets limits on attempts to enter passwords and/or the system's inactivity time during log-in to the e-banking system.

5.23. When using OTPs for authentication, the bank sets limits on their validity according to the preset minimum requirement.

Recommendation 10: Monitoring of transactions

5.24. The Bank uses the systems that detect and prevent frauds to detect suspicious transactions prior to their authorization.

5.25. The Bank has procedures in place for remote monitoring and evaluation of transactions within a reasonable timeframe for delivery and timely execution of e-banking payment transaction.

5.26. When the Bank has suspicions with regard to any payment transaction, it blocks the transaction in question and promptly notifies the user accordingly until security issues are resolved.

Recommendation 11: Protection of payment data

5.27. The Bank ensures security of all information used to identify and authenticate users and user interface means from unauthorized access and changes to them.

5.28. During exchange of e-banking payment data the Bank ensures encryption between the parties to maintain data confidentiality and integrity.

Recommendation 12: Raising awareness of users and organization of communication with them

5.29. The Bank creates at least one communication facility for ongoing communication to enable proper and safe use of e-banking services by users and informs them on directions for its use.

5.30. If any of the cases specified in Item 4.4 herein occurs, the Bank provides uninterrupted 24-hour receiving of user notifications by all possible communication means (at least telephone, mobile, Internet) (indicating the date, time (hour and minute) of receiving the notification and details of the case).

5.31. The Bank educates users on the following to minimize risks during use of e-banking services:

5.31.1. protection of e-banking service access authentication means and other information;

5.31.2. maintenance of PC security on installation and updates of security elements (antivirus programs, firewall, patches) to the computer;

5.31.3. user should take into account considerable threats and risks he may be exposed to with respect to downloading software using Internet he is not sure of;

5.31.4. use of bank's authentic website.

Recommendation 13: Setting notifications and limits

5.32. Limits on the amount of e-banking payment transactions are set in bank's internal regulations and procedures and/or on the basis of the agreements signed with users.

5.33. If the bank detects suspicious payment transactions it notifies the user by possible communication facilities (phone, SMS, e-mail etc.).

Recommendation 14: Issue of payment order and user's obtaining information on the status of execution

5.34. The Bank provides users with information on the date and time of last system use, as well as the date and time of failed access at e-banking user's appeal.

5.35. The Bank enables the user to control the status of execution of e-banking transaction he has conducted, as well as balance of the account.

Annex 1
to the Methodological Guidelines on supply and security of electronic banking services in the Republic of Azerbaijan

Types of remote attacks during e-banking services, their detection and measures for their prevention

№	Types of remote attacks	Brief description	Measures to detect and prevent attacks
1	Back doors	'Back door' is malware written to allow programmers to access software or operational systems avoiding security control and may be used both by data entry sequence and a user ID with special access rights. Programmers use backdoors to check errors in developed programs and for fast access to control them. If the backdoor is not removed after error check in software, it causes a security issue. Moreover, a hacker may develop his backdoor for his future activity after getting system access.	➢ receive certificates from third parties on lack of any undocumented backdoors in their products and receive systems only from reliable sources; ➢ apply procedures confirming lack of backdoors with tests conducted prior to real time operation of systems; ➢ test 'integrity' of systems to check integrity of systems under real time operation (undergone no changes).

2	Brute force	A brute force attack may be used to obtain encrypted information. Encrypted data obtained during this attack is decoded by dedicated software that enables access to codes maintained in data, user names and passwords. The hacker may create his own backdoor for his future activity after obtaining access to data.	➢ use advanced encryption standard and certificate management to protect confidentiality of data, user names and passwords; ➢ introduce complex encryption policy (minimum password length and period for change, requirements for their reuse etc.); ➢ conduct unsanctioned external intrusion tests to detect security vulnerabilities and encryption method complexity; ➢ educate users for security measures (particularly in setting passwords).
3	Denial of service - DOS	Denial of service (DOS) does not target obtaining rights to access network or system. DOS is an attack aiming to disrupt services of both the system and the network by overloading them with data or inquiries. DOS attack may be realized from one or more sources. In a Distributed DOS attack the hacker	➢ maintain relevant network security to block unnecessary network traffic in systems operation; ➢ negotiate with Internet providers to receive traffic only from authorized sources;

		can purposefully orient his online DOS attack to some or hundreds of systems simultaneously.	➢ develop relevant backup and recovery mechanisms; ➢ Use scanning tools[1] or unauthorized external intrusion tests to check resistance of systems and network to DOS and/or distributed DOS attacks.

[1] Scanning tools are used to detect and analyze security vulnerabilities in network, operating systems and database.

4	Exploiting known security vulnerabilities	Hackers exploit known security vulnerabilities to get unauthorized access to systems. There are many sources on Internet on vulnerabilities of the kind. Hackers alternately use dedicated automated tools to detect security vulnerabilities. Security vulnerabilities may be related to devices, software in web-servers, tools used for development of software in firewalls or in web-servers. For instance, certain security vulnerabilities allow unauthorized changes to website content.	➢ delete or deactivate unused programs and computer processes from servers; ➢ introduce the latest security package assignments and updates to operating systems and system application software; ➢ select the third party supplying software and hardware with effective technological capabilities to prevent the latest hacker attack methods; ➢ use scanner tools or unsanctioned external intrusion tests to detect security vulnerabilities like software errors or flaws; ➢ conduct penetration tests for publicly accessible devices and local network at least annually.
5	Guessing passwords	Guessing passwords is the method of checking all possible password combinations to access a system or network via software. Some of password guessing attacks accelerate this	➢ apply a complex encryption policy (minimum password length and period for change, requirements for their reuse etc.);

		process by checking mostly used password combinations in the first instance.	➢ apply conditional access control mechanisms (liquidate user ID after several failed access attempts); ➢ accurately change existing passwords in critical network components; ➢ educate users on security measures (particularly on creating passwords).

6	Hijacking	Hijacking is an attack related to theft of communication after a user confirms himself in the system. In general, hijacking attacks take place over remote computers (user PC), but sometimes communication can be stolen from a computer that is on the route of a remote PC and banks' internal systems.	➢ maintain relevant network security by applying complex authentication methods to obtain remote access, e.g. to restrict access of a hijacker to confidential data require periodic halt of access to highly critical sessions and re-authentication; ➢ install properly configured firewalls in relevant places; ➢ monitor network traffic or potential intrusions on an ongoing basis; ➢ use scanning tools or unsanctioned external intrusion tests to detect hijacking related vulnerabilities;

			➢ apply encryption to highly confidential information.

7	Random dialing or war dialing	A random dialing attack is random or consecutive dialing of numbers existing in telephone network by a hacker to detect modems beyond network protectors and other security mechanisms and ensure unsanctioned access.	➢ ensure adequate network security to issue authorization for and control all modems, e.g. detect unsanctioned modems to simulate random dialing by dialing all numbers in the organization's telephone network; ➢ install all modems in the same physical location; ➢ network segments need to be separated in terms of criticality of systems in the network and access rights. At that when a hacker gets unsanctioned access to one network segment, he will fail to access to other critical network segments; ➢ configure modems and other similar devices in a dial-back mode to ensure remote access to network only by sanctioned modems;

			➢ detect random dialing related vulnerabilities, use scanning tools or unsanctioned external intrusion tests.
8	Sniffer	Sniffer software known as network controllers capture information transferred via network by detecting keystrokes stored in PCs.	➢ maintain relevant network security to prevent unauthorized capture of information (issue the rights to confidential data only to appropriate user groups by means of segregation of LANs to segments, firewalls and router adjustments); ➢ monitor network traffic or possible intrusions in an ongoing manner; ➢ use scanning tools or unsanctioned external intrusions tests to detect vulnerabilities related to unsanctioned capture of data transferred over network; ➢ educate users on security measures (avoid users' downloading sniffers to machines); ➢ apply strong encryption authentication methods to maintain data confidentiality.

9	Social engineering[2]	Social engineering is a socio-technical method used to obtain information or access. At that a hacker may present himself as an authorized person (helpdesk employee or supplier) and try to inform a user on his ID and password. Moreover, the hacker may apply for opening of a new user account for his future activity. The hacker can call the organization's helpdesk by alienating the authorized user to obtain information on the system (the hacker asks the helpdesk to change the real system password etc.)	➢ realize relevant security measures to prevent unauthorized external access; ➢ hold trainings for helpdesk employees to make them precautious on technical methods of social engineering (other related staff) and instruct the above staff on the policy of the organization on development of information on data resulting from unauthorized access to confidential data; ➢ provide users with relevant rules related to security measures to fight social engineering.

[2] Phishing is a social engineering related attack and is defined as opening fraudulent card accounts on the name of a person for later illegal use by obtaining enough sensitive information on a person by various means (telephone, e-mail address, etc.).

10	Spoofing	In spoofing attack, a hacker tries to deceive network masquerading unauthorized system as authorized one to access network or confidential data. E.g., a user under attack creates authenticated session with organization's web-site entering user name and password from his personal device (e.g. PC). Capturing the session, hacker can steal user's IP address and access the system imitating the device. At that, as it has no influence on sanctioned user's session, he may be unaware of external intrusion.	➢ apply authentication methods based upon not only IP addresses, but also session specific encrypted identification based authentication to maintain security of data transferred over authenticated session; ➢ install properly configured firewalls in relevant places; ➢ monitor network traffic or external intrusions on a continuous basis.
11	Trojan horses	Trojan horse is any malicious computer program which has no negative impact on systems' ordinary operations, but collects information or captures system management. Trojan horses may be attached to e-mails (as computer games) and create a backdoor (see above) authorizing system access. Not to track hacker's activities Trojan horse may not store logging and other data. One of the most initial forms of these programs is software allowing to get user enter name and password displaying a fake access screen in the system.	➢ apply critical changes management procedures related to systems real commissioning and conduct tests confirming lack of Trojan horses; ➢ check integrity of programs in use on a regular basis; ➢ formulate a data security policy and conduct relevant trainings for internal staff on relevant security measures to fight Trojan horses (e.g., tough policy against

			improper use of e-mail addresses or Internet); ➢ provide users with relevant rules on security measures related to opening files attached to e-mails and use of Internet.
12	Viruses	Computer viruses are computer programs that may be inserted to another code and self-activate. When activated, may cause harmful activities resulting in network or system collapse. Virus programs may spread to many platforms, databases, devices in the system and many systems connected via the network. They can be inserted to attachments to e-mails and activate when files are opened.	➢ when a third party agreement is signed, incorporate an article to third party liabilities 'checking information protocols entering the bank against viruses'; ➢ use updated virus scanners; ➢ formulate a data security policy and conduct relevant trainings for internal staff on relevant security measures to fight computer viruses (e.g., tough policy against improper use of e-mail addresses or Internet); ➢ provide users with relevant rules on security measures related to opening files attached to e-mails and use of Internet.