Սարքի նույնականացման քաղաքականություն

1. Սահմանումներ

«Հավելված» -«Tradernet Armenia» որը հասանելի է Apple Store-ում, Google Play-ում և AppGallery-ում:

«Մուտքի կոդեր» - Հաճախորդի հասանելիության կոդ, ցանկացած մուտքի կոդ, գաղտնաբառ(եր), Հաճախորդի հաշվի համար, Հաճախորդի էլեկտրոնային նույնականացման միջոցները և Ընկերության էլեկտրոնային առևտրային հարթակ մուտք գործելու համար անհրաժեշտ ցանկացած տեղեկատվություն:

«SMS վավերացում» - Ընկերության կողմից տրամադրված անվտանգ մուտքի կոդերով սեանսի մեկնարկ՝ որոնք SMS ծանուցումների և Telegram-ի push ծանուցումների միջոցով ուղարկվում են Հաճախորդի կողմից տրամադրված Անդամ երկրի տարածքում գտնվող բջջային համարին:

«Ստուգված սարք» - սարք, որը Հաճախորդը հաջողությամբ ստուգել է՝ անցնելով սարքի նույնականացման ստանդարտ կամ այլընտրանքային մեթոդով:

«Ստանդարտ սարքի նույնականացում» - այն մեթոդը, որը նախատեսված է Հաճախորդի Սարքը ստուգելու համար, 8-րդ կետով սահմանված կարգով:

«Այլընտրանքային սարքի նույնականացում» - մեթոդ, որը նախատեսված է Հաճախորդի Սարքը ստուգելու համար, սույն Հավելվածով սահմանված կարգով:

«Բջջային սարք» - ձեռքի էլեկտրոնային գործիք, որը նախատեսված է անլար կապի և հաշվարկների համար, ներառյալ, բայց չսահմանափակվելով սմարթֆոններով, պլանշետներով և այլ սարքերով:

«QR կոդ» - Արագ արձագանքման կոդ, որը հանդիսանում է երկչափ շտրիխ կոդ՝ բաղկացած սպիտակ քառակուսի ցանցի վրա դասավորված սև քառակուսիներից, որը կարելի է կարդալ բջջային սարքի միջոցով՝ օգտագործելով հավելվածը: Այն պարունակում է կոդավորված տեղեկատվություն, որը ծառայում է որպես տեղեկատվության արդյունավետ պահպանման և փոխանցման միջոց՝ հավելվածները դարձնելով ավելի մատչելի, այդ թվում՝ վավերացում, նույնականացում և տվյալների որոնում:

«Ընկերության էլեկտրոնային առևտրային հարթակ» - ինտերնետային կայք, հավելված կամ այլ էլեկտրոնային միջոց, որը հնարավորություն է տալիս Ընկերության կողմից տրամադրված հասանելիության միջոցներից (մուտքի կոդերը) օգտվող հաճախորդներին գործարքներ կատարել Ընկերության հետ ինտերնետային կայքի, հավելվածի կամ էլեկտրոնային որևէ այլ միջոցներով:

«Ընկերության կայք» կամ «Ընկերության պորտալ» - https://ffin.am/ կամ ցանկացած այլ կայք, որը կարող է լինել Ընկերության կայքը:

«Աջակցություն» - Հաճախորդի համար Ընկերության հետ իրական ժամանակում հաղորդակցվելու միջոց՝ http://tradernet.am/ կայքում և Հավելվածում:

«AWS» - Amazon Web Services՝ երրորդ անձ հանդիսացող ընկերություն:

«Իրական ժամանակում ստուգում» - դեմքի ակտիվության ստուգում, որն իրականացվում է Amazon Recognition-ի (AWS) կամ SumSub-ի կողմից:

«SumSub» - Sum and Substance՝ երրորդ անձ հանդիսացող ընկերություն:

«Ինքնությունը ստուգող մոդուլ» - ընթացակարգ, որն իրականացվում է SumSub-ի և/կամ Amazon Web Services-ի կողմից:

2. Օգտագործման շրջանակը և նպատակը

2.1. Սույն Քաղաքականությունը նպատակ ունի նախատեսել համապատասխան և բավարար միջոցներ և ընթացակարգեր՝ ապահովելու Հաճախորդի անվտանգ մուտքն իր անձնական էջ՝ Ընկերության Էլեկտրոնային առևտրային հարթակում:

2.2. Սույն Քաղաքականությունն ընդունվել է կիբերանվտանգության բնագավառում սպառնալիքները կանխարգելու համար՝

1. չստուգված մուտք
2. խարդախություն
3. ակտիվների գողություն
4. լրտեսող ծրագրեր
5. ֆիշինգ

3. Ընդհանուր սկզբունքներ

3.1 Սարքի նույնականացման պարտադիր ընթացակարգն ստեղծվել է սույն Քաղաքականության նպատակներին հասնելու համար:

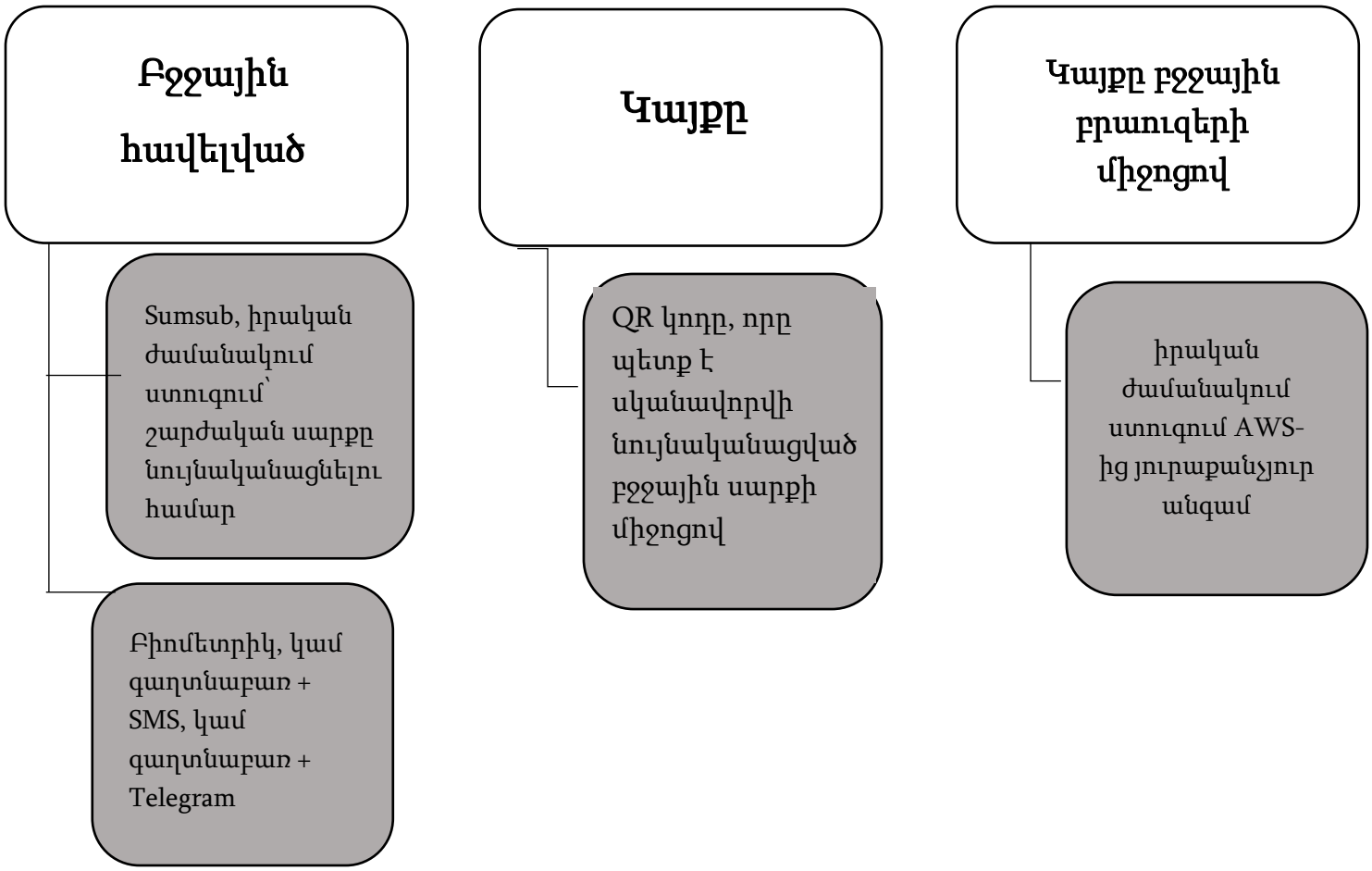
3.2 Սարքի նույնականացման պարտադիր ընթացակարգը վերաբերում է բոլոր սարքերին, որոնք օգտագործվում են Ընկերության էլեկտրոնային համակարգ մուտք գործելու համար:

3.3 Բջջային հավելվածի միջոցով ընկերության էլեկտրոնային համակարգ մուտք գործելու համար կարող եք օգտագործել միայն ստուգված սարքը: Բջջային սարքը ստուգելու համար դուք պետք է լրացնեք կա՛մ **Ստանդարտ սարքի նույնականացումը**, կա՛մ **Այլընտրանքային սարքի նույնականացումը**: Նույնականացումն ավարտվելուն պես ձեր սարքը կպահպանվի որպես Ստուգված:

3.4 Կայքի միջոցով Ընկերության էլեկտրոնային համակարգ մուտք գործելու համար դուք պետք է սկանավորեք QR կոդը՝ օգտագործելով Ստուգված բջջային սարք:

3.5 Բջջային բրաուզերի միջոցով Ընկերության էլեկտրոնային համակարգ մուտք գործելու համար դուք պետք է ամեն անգամ լրացնեք Իրական ժամանակում ստուգումը:

4. Սխեմա



5. Մատուցված ծառայություններ

5.1 Անվտանգության սահմանված միջոցները ներառում են՝

- Դեմքի Իրական ժամանակում հայտնաբերում Amazon Rekognition (AWS) միջոցով https://docs.aws.amazon.com/rekognition/latest/dg/face-Liveness.html:
- CompareFaces օգտագործելով Amazon Rekognition (AWS) https://docs.aws.amazon.com/rekognition/latest/APIReference/API CompareFaces.html;
- SumSub https://sumsub.com/privacy-notice-service/:
- SMS վավերացում
- QR կոդեր

6. Ստանդարտ սարքի նույնականացում, շարժական սարքեր

6.1 Բջջային սարքը, որի վրա հաճախորդը հաշիվ է բացել և ավարտել ստուգումը SumSub-ում, համարվում է Ստուգված այդ հաճախորդի համար:

6.2 6.1 կետում նշված Սարքը պահպանվում է Ստուգված մինչև հավելվածի վերատեղադրումը: Բջջային ցանցում հաստատումը վավեր է մինչև քուքի սեանսի թարմացումը, որից հետո կրկին ստուգում է պահանջվում:

6.3 Հավելվածը նոր սարքի վրա տեղադրելիս պետք է ավարտվի ստուգման ընթացակարգը՝ անվտանգ սեանս բացելու համար: Եթե որևէ երրորդ անձ մուտք է գործում այլ հաճախորդի նախկինում հաստատված սարք, դա

նույնպես ստուգման կարիք կունենա, ինչը կծառայի որպես Հաճախորդի տվյալների լրացուցիչ պաշտպանություն:

6.4 Եթե սարքը ստուգված չէ, ստուգումը պահանջվում է, երբ առաջին անգամ փորձ է արվում բացել անվտանգ սեանս հավելվածում և ամեն անգամ, երբ այն գտնվում է բջջային ցանցում:

6.5 Ստուգումը սկսվում է Հաճախորդի լուսանկարը SumSub-ի միջոցով նախկինում ստուգվածի հետ համեմատելով: Եթե SumSub-ի միջոցով նախկինում հաստատված լուսանկարն անհասանելի է, Հաճախորդը օգտագործում է SumSub ինքնության հաստատման մոդուլը՝ անձը հաստատող փաստաթուղթ վերբեռնելու համար:

6.6 Երբ 6.5, կետում սահմանված քայլն ավարտվում է, Հաճախորդը օգտագործում է AWS ինքնության ստուգման մոդուլը, որպեսզի անցկացնի Իրական ժամանակում ստուգում՝ ստուգելու համար, որ Իրական ժամանակում ստուգման ենթարկվող հաճախորդը իրական մարդ է և նման է տվյալների բազայում հաստատված լուսանկարին: Եթե Իրական ժամանակում ստուգումը ձախողվում է, հաճախորդին առաջարկվում է կրկնել ստուգումը:

6.7 Իրական ժամանակում հաջող ստուգումից հետո հաճախորդի լուսանկարը համեմատվում է տվյալների բազայում հաստատված լուսանկարի հետ: Եթե դրանք համընկնում են, Բջջային սարքը համարվում է ստուգված:

6.8 Իրական ժամանակում անհաջող ստուգման դեպքում հաճախորդը ստանում է սխալի մասին հաղորդագրություն AWS-ից:

6.9 Իրական ժամանակում ստուգման սխալի դեպքում SumSub ինքնության ստուգման մոդուլն օգտագործվում է Իրական ժամանակում ստուգումն իրականացնելու և հաճախորդի դեմքը տվյալների բազայի լուսանկարի հետ համեմատելու համար:

6.10 Ստուգումից հետո հաճախորդը կարող է սարքի վրա բացել Անվտանգ սեանս՝ օգտագործելով ստանդարտ մեթոդներ (բիոմետրիկ, SMS վավերացում):

7. Անվտանգ սեանսի բացում QR կոդի միջոցով

7.1 QR կոդը ստեղծվում և ցուցադրվում է թռուցիկ պատուհանում՝ աշխատասեղանի վրա անվտանգ սեանս բացելիս: QR կոդը պարբերաբար թարմացվում է անվտանգության նկատառումներով:

7.2 Սկանավորեք QR կոդը բջջային հավելվածի «Ավելացնել սարք» բաժնում՝ աշխատասեղանի վրա անվտանգ սեանս բացելու համար: Այս բաժին մուտք գործելը հնարավոր է միայն հավելվածում ակտիվ անվտանգ սեանսի առկայության դեպքում, որը պահանջում է սարքի ստուգում:

7.3 Բջջային հավելվածում QR կոդը հաջողությամբ սկանավորելուց հետո անվտանգ սեանսն ավտոմատ կերպով բացվում է աշխատասեղանի վրա:

7.4 Եթե QR կոդը սխալ է սկանավորվել կամ ժամկետանց է, ապա աշխատասեղանի վրայի Անվտանգ սեանսը չի բացվի, և Հաճախորդին կառաջարկվի նորից սկանավորել՝ օգտագործելով վավեր QR կոդը:

Appendix 14 To the General Terms of business

Device Authentication Policy

1. Definitions

"Application" means "Tradernet Armenia" available from Apple Store, Google Play and AppGallery;

"Access Codes" means the Client's access codes, any login code, password(s), Client Account number, Client's Electronic Authentication Means and any information required for accessing the Company's Electronic Trading Platform;

"SMS Authentication" means initiation of the Secure session with secure Access Codes provided by the Company via SMS notifications and/or via Telegram push notifications sent to the mobile number given by the Client in the Member Area;

"Verified device" refers to a device that the client has successfully verified by undergoing either the Standard or Alternative device authentication method;

"Standard Device Authentication" means the method designed for the client to verify the Client's Device, as described in clause 8 herein;

"Alternative Device Authentication" means the method designed for the client to verify the Client's Device, as described in Annex 1 herein;

"Mobile device" means a handheld electronic instrument designed for wireless communication and computation, including but not limited to smartphones, tablets, and wearable devices;

"QR Code" refers to a Quick Response code, which is a two-dimensional barcode consisting of black squares arranged on a white square grid, which can be read by a mobile device using an Application. It contains encoded information that serve as a means of efficiently storing and transmitting information, facilitating various applications, including but not limited to authentication, identification, and data retrieval;

"Company's Electronic Trading Platform" an internet website, Application or another electronic medium that enables Clients using the facility (access codes) provided by the Company to enter into Transactions or carry on dealings with the Company via an internet website, Application or through some other electronic medium;

"Company's website" or "**Company Portal"** means https://ffin.am/ , or any other website that may be the Company's website;

"Live Support" means a way for the Client to have real-time, back-and-forth communication with the Company available at http://tradernet.am/ and within the Application;

"AWS" means Amazon Web Services, a third-party company;

"Liveness check" means Detecting face liveness procedure executed by Amazon Recognition (AWS) or SumSub;

"SumSub" means Sum and Substance, a third-party company;

"identity verification module" means the procedure executed by SumSub and/or Amazon Web Services .

2. Scope and purpose

2.1. This Policy aims to set appropriate and sufficient measures and procedures to ensure secure access of the Client to its member area within Company's Electronic Trading Platform.

2.2. This Policy is adopted to prevent cybersecurity threats:

i. unverified access;

ii. fraud;

iii. stealing assets;
iv. spyware;
v. phishing.

3. General Principles

3.1. The mandatory device authentication procedure has been implemented to achieve the purposes of this Policy.

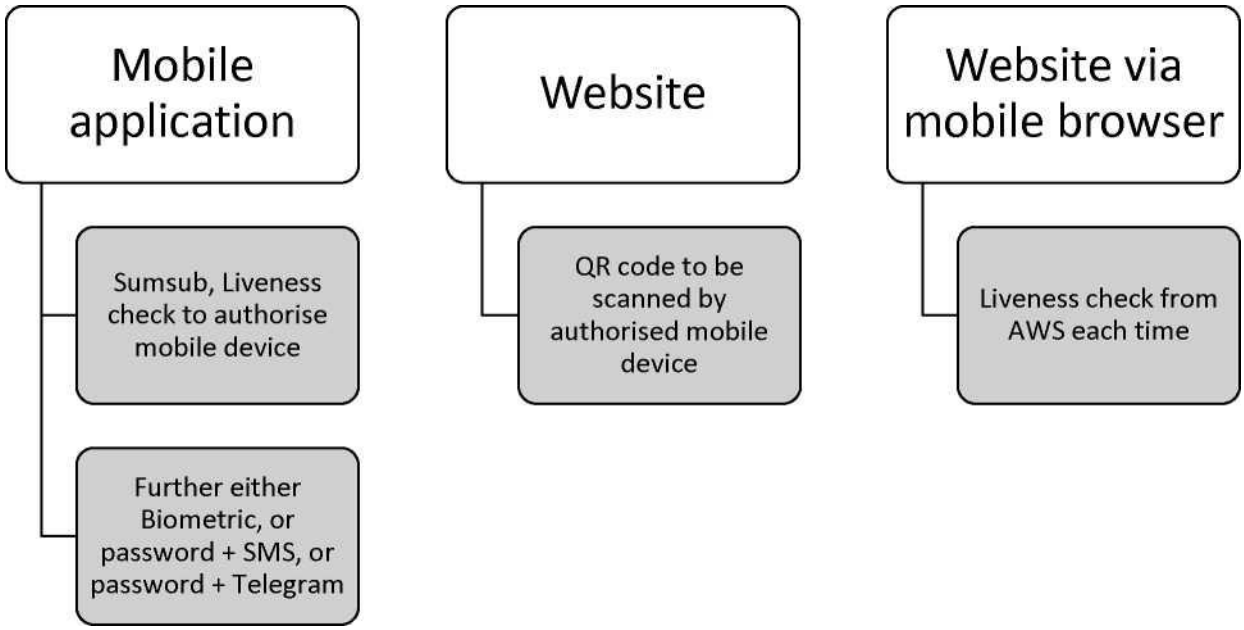
3.2. The mandatory device authentication procedure applies to all devices you use to access the Company's Electronic System.

3.3. To access the Company's Electronic System through a mobile application, you can only use a Verified device. To verify a mobile device, you should complete either the **Standard Device Authentication** or the **Alternative Device Authentication**. Once authentication is complete, your device will be saved as Verified.

3.4. To access the Company's Electronic System through the website, you must scan a QR code using a Verified mobile device.

3.5. To access the Company's Electronic System through a mobile browser, you should complete the Liveness check each time.

4. Scheme



5. Services implemented

5.1. The security measures adopted include:

i. Detecting face Liveness using Amazon Rekognition (AWS) https://docs.aws.amazon.com/rekognition/latest/dg/face-Liveness.html:
ii. CompareFaces using Amazon Rekognition (AWS) https://docs.aws.amazon.com/rekognition/latest/APIReference/API CompareFaces.html;
iii. SumSub https://sumsub.com/privacy-notice-service/:
iv. SMS Authentication:
v. QR ^des.

6. Standard Device Authentication, Mobile devices

6.1. The Mobile device on which the client opened an account and completed verification in SumSub is considered

Verified for that client.

6.2. The Device mentioned in clause 6.1 remains Verified until the application is reinstalled. On mobile web, verification is valid until the session cookie is updated, after which re-verification is required.

6.3. When installing the application on a new device, the verification procedure must be completed to open a secure session. If a third party logs into another client's previously verified device, they will also need verification, which serves as additional protection of the Client's data.

6.4. If the device has not been verified, verification is required the first time an attempt is made to open a Secure session in the application and each time it is on the mobile web.

6.5. The verification starts with comparing the Client's photo with the one previously verified through SumSub. If the photo previously verified through SumSub is unavailable, the Client uses the SumSub identity verification module to upload an identity document proving the client's identity.

6.6. When the step under clause 6.5. is completed, the Client uses AWS identity verification module to conduct a Liveness check to verify that the client undergoing the Livness check is a real human and looks like on the verified photo in the database. If the Liveness check fails, the client is prompted to repeat the check.

6.7. After a successful Liveness check, the client's photo is compared with the verified photo in the database. If they match, the Mobile device is considered verified.

6.8. In case of a failed Liveness check, the client is shown an error message from the AWS.

6.9. In case of a Liveness check error, the SumSub identity verification module is used to conduct the Liveness check and compare the client's face with the photo from the database.

6.10. After verification, the client can open a Secure session on the device using standard methods (biometrics, SMS Authentication).

7. Opening a Secure Session via QR Code

7.1. A QR code is generated and displayed in a pop-up window when attempting to open a Secure session on desktop devices. The QR code is periodically updated for security purposes.

7.2. Scan the QR code in the mobile application's "Add Device" section to open a Secure session on a desktop device. Access to this section is possible only with an active Secure session in the application, which requires device verification.

7.3. After successfully scanning the QR code in the mobile application, the Secure session is automatically opened on the desktop device.

7.4. If the QR code is scanned incorrectly or has expired, the Secure session on the desktop device will not open, and the Client will be prompted to rescan using a valid QR code.

Այլընտրանքային սարքի նույնականացման ուղեցույց

Այլընտրանքային սարքի նույնականացումը կարող է իրականացվել Աջակցության հետ կապվելու միջոցով, իրական ժամանակում Ընկերության հետ ուղիղ կապի միջոցով, հասանելի՝ https://ffin.am կայքում և Հավելվածում և էլ. փոստի միջոցով:

QR կոդի թույլտվության սխեման կարող է անջատվել հաճախորդի պաշտոնական խնդրանքով բացառիկ դեպքերում՝ միայն Ընկերության հայեցողությամբ:

Guidance for Alternative Device Authentication

Alternative Device Authentication can be done through contacting Live Support, real-time, back- and-forth communication with the Company available at https://ffin.am and within the Application and or via email.

QR code authorization scheme may be disabled at the customer's official request in exceptional cases, solely at the Company's discretion.