



**SMU**

Manual përdorimi (Verifikimi me dy hapa) – Version 1.0

## Përmbajtja

Manual përdorimi (Verifikimi me dy hapa) – Version 1.0.....	1
1 Verifikimi me dy hapa .....	3
1.1 Google Authentication.....	3
1.2 Email Code Authentication .....	6
1.3 SMS Code Authentication .....	7
2 Lista e figurave.....	8

# 1 Verifikimi me dy hapa

Për të rritur nivelin e sigurisë në sistemin SMU, është mundësuar që qasja e përdoruesit në sistem të bëhet përmes verifikimit me dy hapa (two step verification) pra nëse këtë modul përdoruesi e bën aktiv atëherë qasja në sistem i mundësohet duke e shënuar fjalëkalimin e tij, gjithashtu edhe nivelin e dytë të sigurisë (kemi implementuar disa lloje të nivelit të dytë). Pasi që përdoruesit kanë të bëjnë me të dhëna shumë të ndjeshme në sistem siç janë notat e studentëve, diplomat e studentëve etj., atëherë rekomandohet që qasja e përdoruesit në sistem të bëhet përmes verifikimit me dy hapa në mënyrë që përdoruesi ta sigurojë llogarinë e tij edhe përmes nivelit shtesë të sigurisë. Hapat e dytë të sigurisë të cilët janë në sistemin SMU (i cili vetëm njëri prej tyre mund të jetë aktiv) janë:

- Google Authentication,
- Email Code Authentication,
- SMS Code Authentication (Për momentin është pasiv).

## 1.1 Google Authentication

Përdoruesi për ta përdorur këtë metodë të verifikimit në sistem duhet që në telefonin e tij mobil ta instalojë aplikacionin “Google Authenticator” ashtu siç shihet në figurën e mëposhtme.

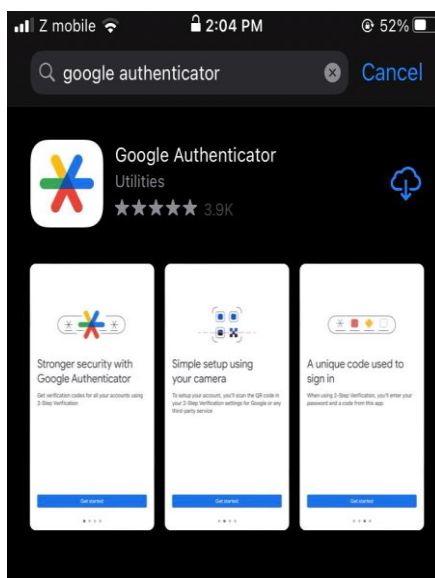
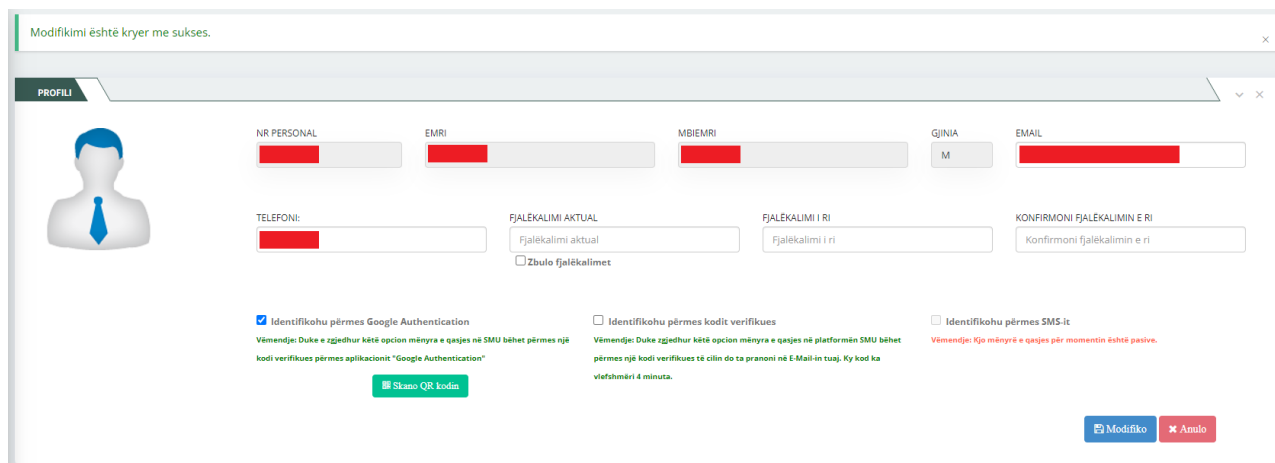


Figura 1: Instalimi i Google Authenticator

Pasi që të instalohet aplikacioni i lartshënuar atëherë përdoruesi duhet që në sistemin SMU të shkojë tek profili i tij dhe nëse dëshiron që këtë metodë ta ketë aktiv në sistem atëherë duhet të klikoj tek check-boxi Identifikohu përmes Google Authentication dhe të klikoj butonin Modifiko ashtu siç shihet në figurën e vijim:

Figura 2: Aktivizimi i Google Authentication (1)

Pasi që përdoruesi të klikoj në butonin Modifiko e cila u sqarua në figurën e mësipërme sistemi e lajmëron që modifikimi është kryer me sukses si dhe i shfaqet një buton tjetër i cili e mundëson skanimin e QR kodit për google authentication kjo shihet ashtu si në figurën në vijim:



The screenshot shows a web interface for profile management. At the top, a green message states 'Modifikimi është kryer me sukses.' Below this is a 'PROFILI' section with a user icon and several input fields: NR PERSONAL, EMRI, MBIEMRI, GJINIA (set to 'M'), and EMAIL. There are also fields for TELEFONI, FJALEKALIMI AKTUAL (with a 'Zbulo fjalëkalimet' link), FJALEKALIMI I RI, and KONFIRMONI FJALEKALIMIN E RI. Three authentication options are presented with checkboxes: 'Identifikohu përmes Google Authentication' (checked), 'Identifikohu përmes kodit verifikues', and 'Identifikohu përmes SMS-it'. A green 'Skano QR kodin' button is visible under the first option. At the bottom right, there are 'Modifiko' and 'Anulo' buttons.

Figura 3: Aktivizimi i Google Authentication (2)

Pasi që përdoruesi të klikoj butonin Skano QR kodin nga figura e mësipërme atëhere sistemi na e shfaq QR kodin e gjeneruar nga sistemi e cila shihet përmes figurës në vijim:

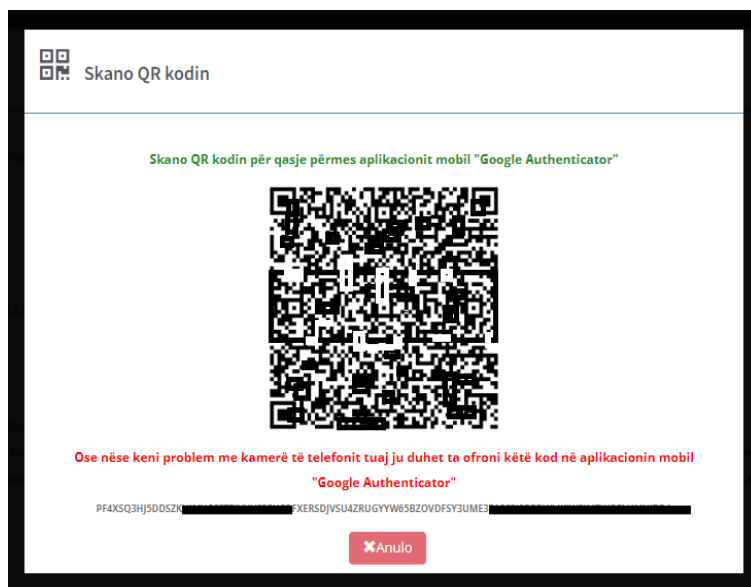


Figura 4: QR Kodi

Pas shfaqjes së QR kodit siç shihet nga figura e fundit përdoruesi duhet të hap aplikacionin e Google Authenticator të cilin u tregua më lart se si instalohet ashtu si në figurën në vijim:

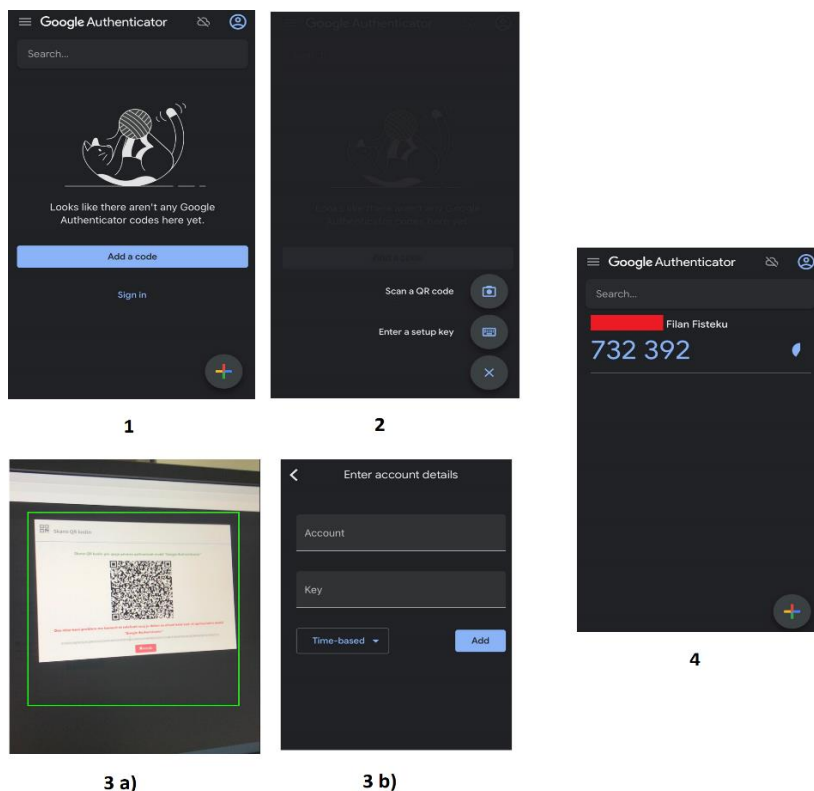


Figura 5: Google authenticator përdorimi

Nga figura e fundit përdoruesi pasi që të hap aplikacionin na shfaqet hapi 1 i figurës së fundit tek hapi 1 përdoruesi duhet të klikoj plusin i cili shihet në të dhe pastaj na shfaqet hapi 2, në hapin e 2-të përdoruesi i ka dy mundësi të skanoj QR kodin ose të shkruaj kodin manualisht, nëse përdoruesi zgjedh të skanoj QR kodin përmes opsionit Scan QR code atëherë aplikacioni e hap kamerën e telefonit ku pastaj duhet të skanohet QR kodi sikurse është e treguar në hapin 3 a), ku menjëherë pas hapit 3 a) pastaj shfaqet hapi i 4 ku na gjenerohet kodi 6 shifror i google authenticator i cili kod është i vlefshëm vetëm 30 sekonda dhe pas çdo 30 sekondave aplikacioni gjeneron kod të ri në mënyrë rastësore (random). Por nëse përdoruesi ka probleme me kamerën e tij të telefonit mobil dhe nuk i funksionon atëherë mundet që të zgjedh opsionin Enter a setup key nga hapi i 2-të, ku pas klikimit në këtë opsion shfaqet hapi 3 b) në të cilin përdoruesi duhet që manualisht të shkruaj kodin i cili gjendet **Figura 4 QR Kodi** ndërsa tek fusha Account mund të shkruaj emrin dhe mbiemrin e tij dhe pas klikimit të butonit Add na shfaqet hapi i 4 me kodin 6 shifror të gjeneruar nga Google Authenticator.

Pas aplikimit të gjitha hapave deri më tani, përdoruesi ka implementuar me sukses Verifikimin me dy hapa (two step verification) në SMU përmes Google Authentication ku tani kurdo që përdoruesi dëshiron të qaset në sistem pas ofrimit të kredencialeve të tij atëherë sistemi i'a kërkon edhe një hap të dytë të sigurisë pra që ta shënoj edhe kodin 6 shifror të gjeneruar nga Google Authentication të cilin mund ta shikoj tek telefoni i tij në aplikacionin Google Authenticator (Figura 5 hapi i 4-të). Kjo shihet përmes figurës në vijim.

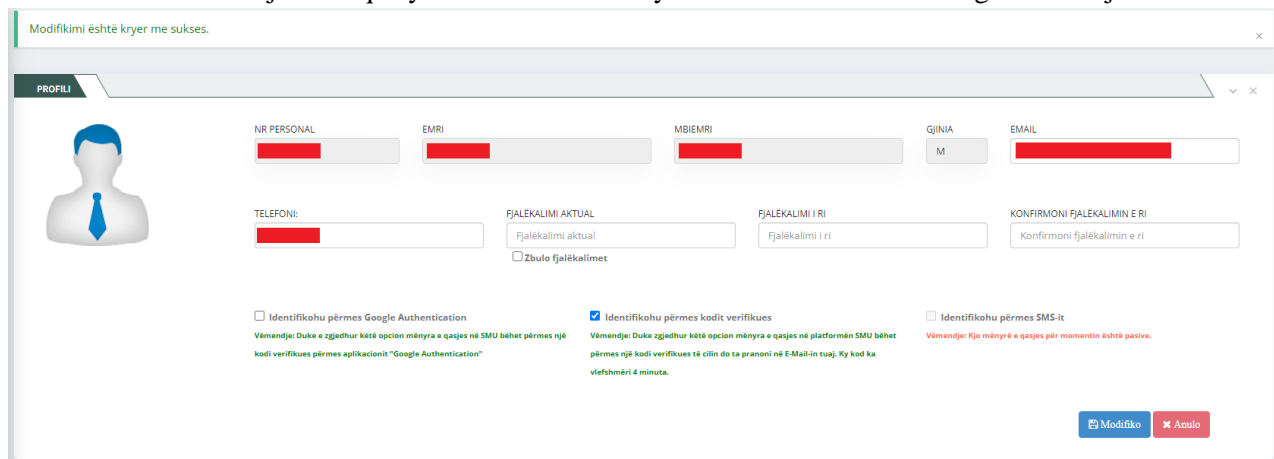


Figura 6: Qasja përmes Google Authenticator

Vërejtje nëse e keni aktivizuar Verifikimin me dy hapa përmes Google Authenticator sistemin nuk lejon qasjen pa e ofruar kodin e gjeneruar pra në parim edhe këtu është qëllimi që llogaria juaj të sigurohet edhe përmes hapit të dytë shtesë të sigurisë, nëse ka raste kur telefoni i juaj prishet apo ju ka humbur, deaktivizimin e verifikimit me dy hapa mund ta bëni tek administrata e Universitetit.

## 1.2 Email Code Authentication

Përdoruesi për ta përdorur këtë metodë të verifikimit në SMU, duhet që tek profili i tij në SMU ta zgjedh checkbox-in Identifikohu përmes kodit verifikues dhe të klikoj butonin Modifiko ku pas klikimit të butonit modifiko sistemi na lajmëron që ky modifikim është kryer me sukses ashtu si në figurën në vijim:



The screenshot shows a web interface for profile modification. At the top, a green notification bar states 'Modifikimi është kryer me sukses.' Below this is a 'PROFILI' section with a user icon and several input fields: NR PERSONAL, EMRI, MBIEMRI, GJINIA (M), and EMAIL. There are also fields for TELEFONI, FJALEKALIMI AKTUAL, FJALEKALIMI I RI, and KONFRIMONI FJALEKALIMIT E RI. At the bottom, there are three checkboxes for authentication methods: 'Identifikohu përmes Google Authentication' (unchecked), 'Identifikohu përmes kodit verifikues' (checked), and 'Identifikohu përmes SMS-it' (unchecked). A 'Modifiko' button is visible at the bottom right.

Figura 7: Aktivizimi i Email Code Authentication

Pas aplikimit të hapit të lartshënuar, përdoruesi ka implementuar me sukses Verifikimin me dy hapa (two step verification) në SMU përmes Email Code Authentication ku tani kurdo që përdoruesi dëshiron të qaset në sistem pas ofrimit të kredencialeve të tij sistemi i'a dërgon një email me një kod 4 shifror të gjeneruar në mënyrë rastësore (random) dhe vlefshmëria e tij është vetëm 2 minuta, ku pastaj vetëm pasi që ta shkruan atë kod sakt atëhere mund të qaset në sistem. Emaili i dërguar nga sistemi shihet ashtu si në figurën në vijim:

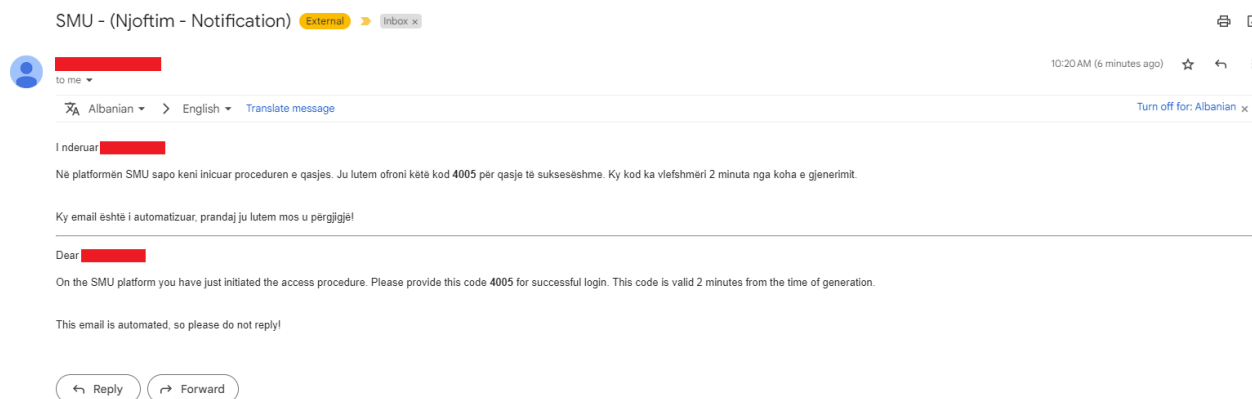


Figura 8: Kodi përmes Email Code Authentication

Nga figura e fundit shihet kodi i cili duhet të jepet si hap i dytë shtesë i sigurisë në sistem dhe ky kod duhet të shkruhet ashtu si në figurën në vijim:

## JU LUTEM OFRONI KODIN 4 SHIFROR PËR QASJE

Kodi

Kodi

1m 56s

Kërko kod të ri për qasje

Figura 9: Qasje përmes Email Authentication

Vërejtje nëse e keni aktivizuar Verifikimin me dy hapa përmes Email Authenticator sistemin nuk lejon qasjen pa e ofruar kodin e gjeneruar pra në parim edhe këtu është qëllimi që llogaria juaj të sigurohet edhe përmes hapit të dytë shtesë të sigurisë, nëse ka raste kur ju e harroni fjalëkalimin e email-it tuaj që e keni në sistem ose edhe për ndonjë arsye tjetër nuk mund të qaseni në email-in tuaj, atëherë deaktivizimin e verifikimit me dy hapa mund ta bëni tek administrata e Universitetit

### 1.3 SMS Code Authentication

Kjo mënyrë e verifikimit me dy hapa në sistemin SMU është pasive, sepse duhet të krijohet një marrëveshje institucionale me ndonjërin prej operatorëve të telekomit që ofrojnë shërbime në Kosovë në mënyrë që t'i mundësohet sistemit SMU të dërgoj SMS pa limit pra duhet të shikohen kushtet financiare të cilat duhet të aplikohen. Në mënyrë që pastaj sistemi të gjeneroj kodin në mënyrë rastësore (random) dhe t'ia dërgoj atë kod përdoruesit përmes SMS-it në mënyrë që ta përdor si hap shtesë të sigurisë për qasje.

## 2 Lista e figurave

Figura 1: Instalimi i Google Authenticator .....	3
Figura 2: Aktivizimi i Google Authentication (1) .....	3
Figura 3: Aktivizimi i Google Authentication (2) .....	4
Figura 4: QR Kodi .....	4
Figura 5: Google authenticator përdorimi.....	5
Figura 6: Qasja përmes Google Authenticator .....	5
Figura 7: Aktivizimi i Email Code Authentication .....	6
Figura 8: Kodi përmes Email Code Authentication .....	6
Figura 9: Qasja përmes Email Authentication .....	7