

OTP Internet / Mobile Banking

Ghid de utilizare aplicație Token



CUPRINS

Prefață	3
Reguli generale de securitate și utilizare.....	3
Descărcarea aplicației Token.....	3
Activarea aplicației Token	4
Generarea parolei unice (OTP) de acces	6
Generarea parolei unice (OTP) de autorizare.....	7
Blocarea aplicației Token	7
Deblocarea aplicației Token.....	8
Sincronizare aplicație Token.....	8
Schimbare cod PIN a aplicației Token.....	8
Pierderea sau furtul dispozitivului portabil pe care a fost instalată aplicația Token.....	9
Serviciul de asistență.....	9

Prefață

Stimate Utilizator, în acest Ghid veți găsi informații detaliate cu privire la funcționarea și utilizarea aplicației Token, pentru serviciul OTP Internet / Mobile Banking.

Aplicația Token reprezintă aplicația instalată pe dispozitivul portabil al Utilizatorului care este accesată pentru generarea Parolelor Unice de acces și autorizare, al căror algoritm de generare garantează caracterul irepetabil al Parolelor Unice. Aplicația MobiasToken cu numărul de serie unic poate fi atribuită doar unui singur Utilizator Autorizat, principiu care permite identificarea Utilizatorului autorizat în Serviciu. Aplicația Token a Mobiasbanca – OTP Group S.A. destinată pentru serviciul OTP Internet / Mobile Banking poate fi utilizată doar în cadrul acestuia.

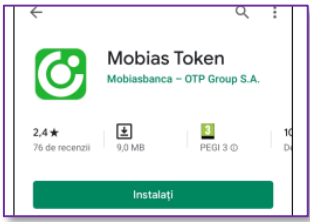
Reguli generale de securitate și utilizare.

- Pentru asigurarea unui grad înalt de securitate a aplicației Token, respectați următoarele reguli de utilizare:
- Pentru utilizarea aplicației Token este necesar să setați *codul PIN* din 4 caractere alfanumerice care va fi utilizat la fiecare generare a parolelor unice.
- Nu permiteți transmiterea dispozitivului portabil și *codul PIN* a aplicației unor persoane terțe.
- Nu indicați/salvați *codul PIN* pe suport de hârtie, memoria dispozitivului pe care a fost instalată aplicația, ambalajul / husa dispozitivului portabil, etc.
- Utilizați setări de blocare complexe a dispozitivului pe care a fost instalată aplicația Token așa ca setarea timpului minim de blocare, utilizarea parolelor sau a altor metode de deblocare.
- Nu instalați aplicații de origine dubioasă pe dispozitivul pe care a fost instalată aplicația Token.
- Dacă utilizați dispozitivul pe care a fost instalată aplicația, pentru accesul la rețeaua Internet – utilizați surse (Wi Fi) sigure.
- Instalați pe dispozitivul pe care a fost instalată aplicația Token, soluții (aplicații) de securitate.
- Nu instalați aplicația Token pe un dispozitiv *root-at* – dispozitiv la care au fost anulate restricțiile de acces la aplicațiile de sistem.

Descărcarea aplicației Token

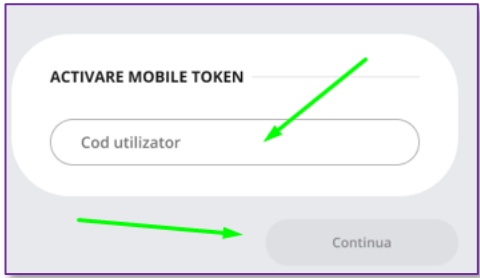
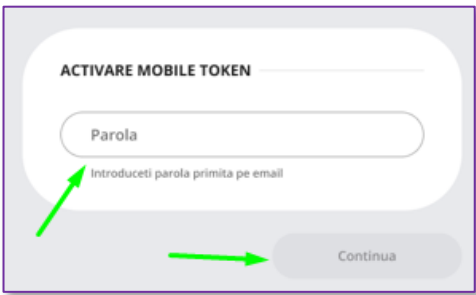
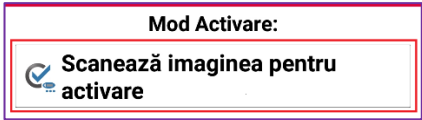
În cazul în care sunteți Utilizator Autorizat, tipul de acces a cărui a fost setat aplicația Token – este necesar de a descărca și instala aplicația Token, pe dispozitivul portabil selectat.

Acțiuni:

În dependență de sistemul operativ al dispozitivului portabil accesați (<i>Sursa de descărcare</i>):	<i>Sistemul operativ</i>	<i>Sursa de descărcare</i>	<i>Iconița sursei din ecranul dispozitivului mobil</i>
	iOS	App Store	
	Android	Play Store	
Găsiți aplicația Token (<i>Iconița</i>) în sursele menționate (Fig. 1).			
Atenție! Aplicația poate fi instalată și utilizată doar de pe dispozitivele care întrunesc următoarele cerințe tehnice: Sistemul operativ: – Android 4.1. (și ulterioare) – iOS 8.0. (și ulterioare) – Cameră de luat vederi. – Autentificare biometrică (după caz)			
Instalați aplicația Token pe dispozitivul portabil.		Figura 1	

Pentru a putea fi utilizată aplicația Token, este necesar ca persoana din cadrul structurii Abonatului să fie setată în serviciul OTP Internet / Mobile Banking ca Utilizator autorizat cu tipul de acces – aplicație Token.

Acțiuni:

1. Accesați pagina de acces a serviciului OTP Internet / Mobile Banking. (Fig. 2) 2. Selectați link-ul <i>Activează aplicație Token</i>	 Figura 2
3. În fereastra apărută introduceți codul utilizatorului. Tastați butonul Continuă (Fig. 3) 4. Serviciul va trimite pe poșta electronică Parola de activare aplicație Token. Verificați poșta electronică. ATENȚIE! Parola de activare aplicație Token (primită prin email) este valabilă doar pe durata a 5 minute de la primire.	 Figura 3
5. Introduceți Parola de activare aplicație Token (primită prin email) în câmpul respectiv a ferestrei browserului și tastați butonul Continuă (Fig. 4)	 Figura 4
6. Accesați aplicația Token instalată pe dispozitivul portabil. 7. Selectați meniul de scanare a imaginii Scanează imaginea pentru activare din aplicație (Fig. 5).	 Figura 5

8. Scațați **prima imagine** generată de serviciu (Fig. 6)
9. În baza imaginii scanate, aplicația va genera **Codul dispozitivului** (Fig. 7)
10. Introduceți în câmpul **Cod dispozitiv**, a paginii serviciului (11 cifre), codul dispozitivului generat de aplicație (Fig. 6). Tastați butonul **Continuă**.

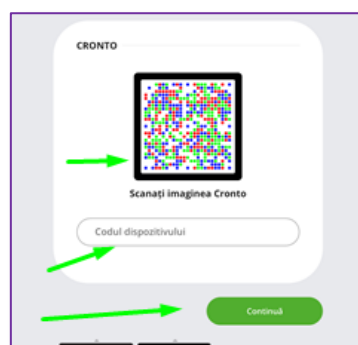


Figura 6

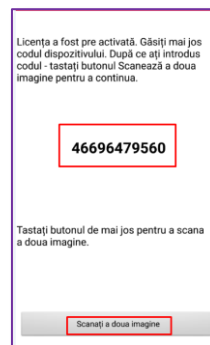


Figura 7

11. Aplicația va genera a **doua imagine**.
12. Tastați butonul **Scațați a doua imagine**, din aplicație. Scațați **a doua imagine** generată de serviciu. (Fig. 8)

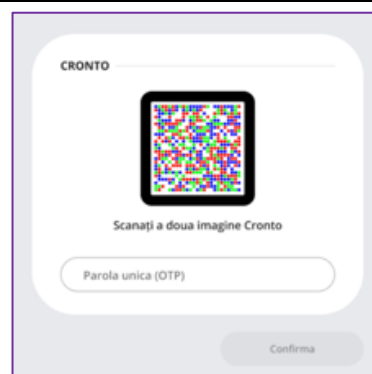


Figura 8

13. Aplicația va solicita setarea codului PIN (Fig. 9)
14. Setati **codul PIN** format din **4** caractere alfanumerice.
15. Reintroduceți **codul PIN**. Tastați butonul **OK** (Fig. 9).

Dacă dispozitivul portabil este dotat cu senzor de amprentă aplicația Token va solicita activarea securității biometrice, astfel veți putea ulterior să utilizați funcționalitatea respectivă – veți aplica amprenta digitală fără a fi necesar de a introduce codul PIN al aplicației.

- Tastați butonul:
 - **Da** – dacă optați pentru activarea securității biometrice și aplicați amprenta digitală asupra senzorului de amprentă.
 - **Nu** – pentru a nu utiliza funcționalitatea respectivă. (Fig. 10)

16. Aplicația va genera parola unică din 6 cifre (Fig. 11)

17. Introduceți în câmpul **Parola unică (OTP)**, a paginii serviciului, parolă unică generată de aplicație (Fig. 8) și tastați butonul **Transmite**.

Notă!

- La setarea codului PIN utilizați cifre și litere aleatorii (nu consecutive). În cazul în care codul PIN setat va conține cifre sau litere identice setate consecutiv – aplicația va atenționa asupra faptului respectiv.



Figura 9

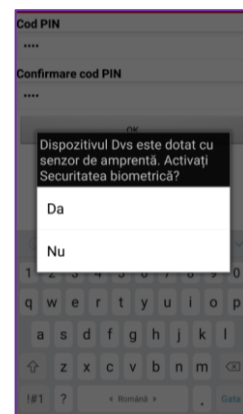
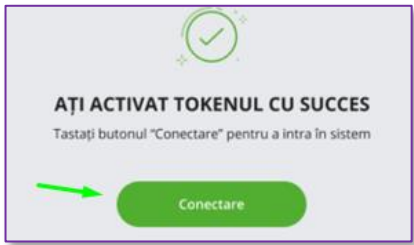


Figura 10



Figura 11

– În procesul instalării aplicația va solicita accesul sau permisiunea la anumite funcționalități ale dispozitivului portabil – acceptați toate solicitările pentru instalarea cu succes a acesteia.	
18. Aplicația Token este gata de funcționare. Tastați butonul Conectare a serviciului pentru a accesa pagina serviciului. (Fig. 12)	 Figura 12

Generarea parolei unice de acces

Accesul la serviciu poate fi efectuat doar în baza parolei unice de acces generată de aplicația Token.¹

Acțiuni:

1. Accesați aplicația Token. Selectați opțiunea **Acces** (Fig 13)
2. Introduceți *codul PIN* setat anterior și tastați butonul **OK** (Fig 13) sau **aplicați amprenta digitală** dacă ați activat securitatea biometrică.
3. Aplicația va genera *Parola unică de acces* (Fig 14).

Notă! Orice **parola unică** generată de aplicația Token va fi valabilă **60 secunde** de la momentul generării. Timpul rămas a valabilității parolei unice este reflectat în partea de jos a ecranului printr-o bară orizontală în descreștere.

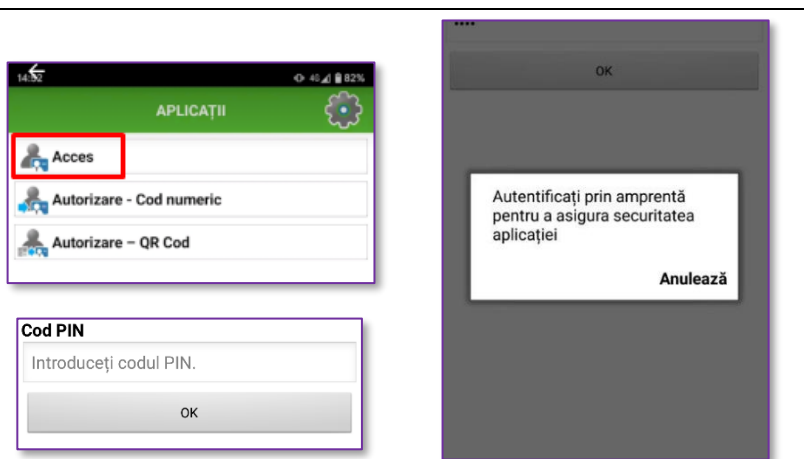


Figura 13



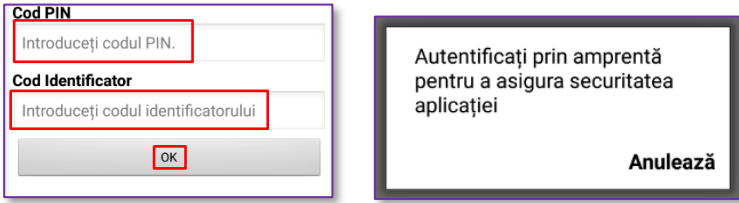
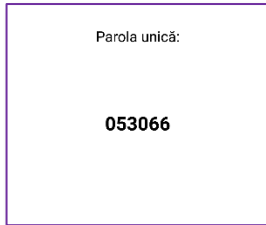
Figura 14

¹ Condiție obligatorie doar pentru utilizatori Persoane juridice

Generarea parolei unice de autorizare

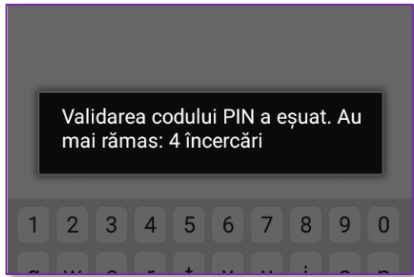
În cadrul utilizării serviciului OTP Internet / Mobile Banking, Utilizatorilor Autorizați cu drept de semnătură, pentru autorizarea operațiunilor, le va fi necesar generarea parolelor unice de autorizare².

Acțiuni:

1. Accesați aplicația Token. 2. Selectați opțiunea: a) Autorizare – Cod numeric, pentru introducerea codului identificatorului din pagina de autorizare a transferului/cererii electronice /etc (Fig 15). b) Sau Autorizare – QR Cod, pentru scanarea codului QR din pagina de autorizare a transferului/cererii electronice/etc (Fig 15).	 Figura 15
3. În dependență de opțiunile selectate: introduceți manual în aplicația Token <i>codul numeric a identificatorului</i> sau scanați QR Cod. 4. Introduceți <i>codul PIN</i> și tastați butonul OK (pentru ambele opțiuni) sau aplicați amprenta digitală dacă ați activat securitatea biometrică (Figura 16)	 Figura 16
5. Aplicația va genera <i>parola unică de autorizare</i> (Fig 17).	 Figura 17

Blocarea aplicației Token

Blocarea aplicației Token poate fi efectuată:

Involuntar: În cazul introducerii eronate a codului PIN de 5 ori consecutiv – aplicația Token se va bloca automat. La fiecare introducere a codului PIN eronat aplicația va reflecta mesajul – Validarea codului PIN a eșuat. Au mai rămas X încercări, unde cifra reflectă numărul rămas de încercări (Fig. 18). Pentru introducerea repetată a codului PIN atingeți ecranul în orice punct al acestuia. La a cincea introducere eronată a codului PIN aplicația va reflecta numărul 0 de încercări rămase.	 Figura 18
La solicitarea utilizatorului:	

² în dependență de regulile de autorizare setate. Obligaoriu pentru persoane juridice.

În cazul în care apare necesitatea de a bloca aplicația Token instalată pe dispozitivul portabil care este pierdut sau furat, se va contacta serviciul **Business.Support / Call Centru** cu indicarea tuturor informațiilor solicitate de către operatorul serviciului.

Deblocarea aplicației Token

În cazul blocării involuntare:

După introducerea eronată, de **5 ori consecutivă**, a codului PIN, aplicația Token **va genera parole unice eronate**.

Pentru a debloca aplicația este necesar:

- De a părăsi aplicația Token.
- De a o accesa repetat și de a introduce codul PIN corect.
- În cazul în care **ați uitat codul PIN**, este necesar ca:
 - a) în cazul utilizatorului persoană juridică: **Administratorul** persoanei juridice să contacteze serviciul **Business.Support**.
 - b) în cazul utilizatorului persoană fizică să contacteze serviciul CallCentru.

În cazul blocării la solicitarea Utilizatorului:

Deblocarea aplicației Token poate fi solicitată la serviciul de asistență **Business.Support³ / Call Centru⁴**, doar de **Administratorul** Abonatului / **Abonatul persoană fizică**. În prealabil de a efectua solicitarea de deblocare, asigurați-vă că dețineți toată informația aferentă Utilizatorului Autorizat a cărui aplicație Token urmează a fi deblocată și parola de identificare deținută de **Administrator / parola secretă a Utilizatorului persoană fizică**.

Sincronizare aplicație Token

În cadrul utilizării aplicației Token pot apărea cazuri în care, parolele de acces sau autorizare, generate de aceasta în baza unui cod PIN corect, nu sunt acceptate de serviciul OTP Internet / Mobile Banking. Aceasta presupune **desincronizarea** aplicației Token – decalajul dintre parametrii setați de timp a aplicației și a serviciului OTP Internet / Mobile Banking.

Pentru a putea fi utilizată în continuare, aplicația Token necesită a fi **sincronizată**.

Acțiuni:

1. Accesați meniul *Setari/Sincronizare* offline (Fig. 19)
2. În fereastra meniului respectiv indicați/corectați *Ora/Data* corectă a serverului (daca este cazul). Ora serverului necesită a fi setată ora **GMT+0 (Greenwich Mean Time)**.
3. Tastați butonul – **OK**.

Notă! În setările dispozitivelor portabile în special telefoane mobile, datele de timp sunt setate implicit în baza datelor furnizate de operatorul mobil și nu necesită a fi reajustate.

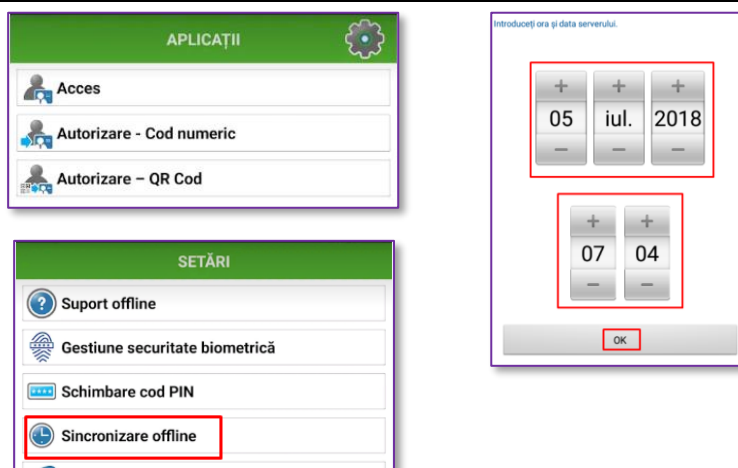


Figura 19

Schimbare cod PIN a aplicației Token

În procesul de utilizare a aplicației Token pot apărea cazuri în care apare necesitatea de a schimba codul PIN a acesteia, setat anterior.

³ **Business.Support** – serviciu de asistență dedicat utilizatorilor persoane juridice

⁴ **Call Centru** – serviciu de asistență- dedicat utilizatorilor persoane fizice.

Acțiuni:

1. Accesați meniul **Setări**, opțiunea **Schimbare cod PIN** (Fig 20)
2. În fereastra meniului indicați **codul PIN curent**, **codul PIN nou** și confirmați acesta prin introducerea repetată.
3. Tastați butonul **OK**. Asigurați-vă că codul PIN a fost schimbat cu succes generând o parolă unică de acces și accesând prin intermediul acesteia serviciul OTP Internet / Mobile Banking.

Notă! La setarea codului PIN utilizați cifre și litere aleatorii (nu consecutive și identice).

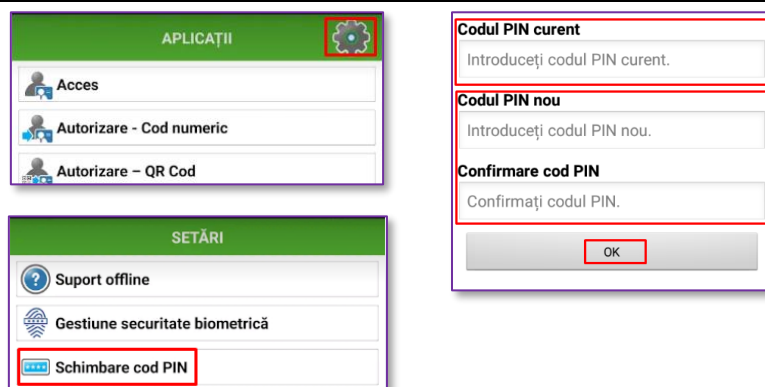


Figura 20

Pierderea sau furtul dispozitivului portabil pe care a fost instalată aplicația Token.

- Păstrați dispozitivul portabil pe care a fost instalată aplicația Token **în maximă siguranță și inaccesibilitate** pentru persoanele terțe.
- În cazul în care s-a produs pierderea sau furtul dispozitivului portabil pe care a fost instalată aplicația Token, imediat contactați serviciul **Business.Support⁵ / Call Centru⁶** și solicitați blocarea acesteia.
- Descărcați aplicația Token pe un alt dispozitiv portabil. Administratorul companiei / Utilizatorul persoană fizică necesită să solicite deblocarea utilizatorului blocat anterior. Repetați acțiunile de activare descrise în prezentul Ghid.

Atenție!

La descărcarea repetată a aplicației Token, setările precedente nu sunt păstrate. Reluați procesul de activare și setare descris mai sus.

Serviciul de asistență

În cazul apariției situațiilor incerte aferente utilizării aplicației Token ce nu sunt descrise în prezentul Ghid, sau situațiilor de compromiterea securității aplicației Token - solicitați suportul serviciului de asistență **Business.Support / Call Centru**.

Datele de contact ale serviciului:

Business.Support:	Call Centru
▪ Tel.: +373 (22) 812 555 ▪ Email: business.support@mobiasbanca.md	▪ Tel.: +373 (22) 256 456 ▪ Email: info@mobiasbanca.md
▪ Serviciul de mesagerie securizată a serviciului OTP Internet / Mobile Banking / Chat	

⁵ **Business.Support** -serviciu de asistență dedicat utilizatorilor persoane juridice

⁶ **Call Centru** – serviciu de asistență- dedicat utilizatorilor persoane fizice.