1. **ЦЕЛ**

Настоящата инструкция регламентира реда и организацията при използване на двуфакторна автентификация в системата за администриране на пазара MMS на Независимия преносен оператор.

1. **ОБЩИ ПОЛОЖЕНИЯ**

Двуфакторната автентификация има за цел да повиши сигурността на платформата за администриране на пазара MMS. Поради тази причина потребителите, освен въвеждането на име и парола за достъп, следва да въвеждат и допълнителен променлив код за сигурност, генериран чрез използване на приложението Google Authenticator (Google Удостоверител). Приложението може да се инсталира от Google Play Store (Google Play магазин) за устройства с Android или от App Store за устройства с iOS.

Двуфакторната автентификация (двустепенното удостоверяване, 2FA) е задължителна за всички потребители на системата.

1. **РЕД И ОРГАНИЗАЦИЯ ЗА ИЗПОЛЗВАНЕ НА ДВУФАКТОРНА АВТЕНТИФИКАЦИЯ (ДВУСТЕПЕННО УДОСТОВЕРЯВАНЕ)**

За всички съществуващи потребители на системата служител на ЕСО ЕАД ръчно активира режим на двуфакторна автентификация, при което MMS генерира нов случаен потребителски код за вход в платформата, който трябва да се регистрира в Google Authenticator.

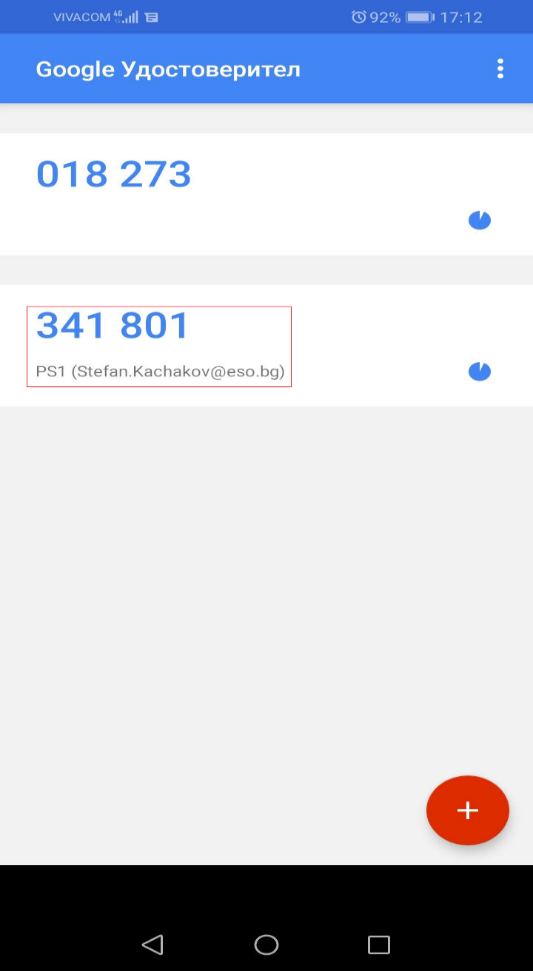
Като първа стъпка всеки потребител следва да инсталира на използваното от него мобилно или десктоп устройство приложението Google Authenticator (Google Удостоверител). Приложението може да инсталира от Google Play Store (Google Play магазин) за устройства с операционна система Android или от App Store за устройства с iOS.

На всички съществуващи потребители ще бъде включено двустепенното удостоверяване по предварително обявен от ЕСО ЕАД график или след изпратен от съответния потреби­тел email до [eto.admin@eso.bg](mailto:eto.admin@eso.bg). След активирането на двустепенното удостоверяване, всеки потребител ще трябва да влезе отново в системата, при което след въвеждане на потребителско име и парола на екрана се визуализира QR код (вижте картинката по-долу).



Съветваме потребителите да са включили предварително приложението Google Authenticator непосредствено преди да влезнат в системата. В приложението се активира бутонът със знак плюс („+“) и с помощта на камерата на устройството се сканира QR кода.

След регистрация на кода в Google Authenticator, автоматично на всеки 30 секунди, се генерира временен код за достъп до системата, който потребителят следва да въвежда при всеки вход в системата след въвеждането на потребителското си име и парола.



Google Authenticator (Google Удостоверител) е универсално приложение, което може да се използва за генериране на кодове за достъп към множество системи. За вход в системата за администриране на пазара MMS на ЕСО се използва кодът с идентификатор PS1 (e-mail адресът на потребителя) както е показано на примера по-горе.

Моля запазете QR кода и/или буквено-цифрения код по-долу на сигурно място, ако смятате да конфигурирате автентификацията на няколко устройства (например desktop компютър, лаптоп, мобилен телефон и/или таблет). Ако се налага цялостно преинсталиране на софтуера на някое от тези устройства, ще се наложи да повторно въвеждане на този код.

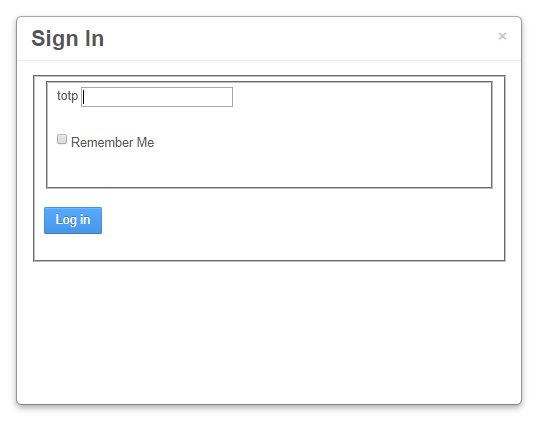
В един Google Authenticator (Google Удостоверител) могат последователно да се регистрират повече от един потребител. След това удостоверителят ще издава променливите кодове на всички потребители регистрирани в него. Например, ако са регистрирани двама потребителя в едно и също устройство (Google Удостоверител), екрана ще изглежда както е показано по-долу.



Таймерът от дясната страна на всеки генериран код показва времето до изтичане на неговата валидност. След изтичане на валидността автоматично се генерира нов код, който потребителят следва да въведе в системата своевременно преди неговото изтичане.

При вход в системата, след като потребителят въведе името и паролата си, на екрана се визуализира поле за въвеждане на временния код за достъп до системата (от примера по-горе 341801).

Екранът за въвеждане на временния код за достъп изглежда по следния начин:



Всички нови потребители в системата се създават с включена функция за двуфакторна автентификация и при първоначално влизане в системата потребителят следва освен да смени временната си парола с постоянна, да регистрира и потребителския си код за платформата в Google Authenticator.

В случай на загуба на QR кода/ кода за ръчно въвеждане, тъй като те не могат да бъдат възстановени от потребителя, то следва той да се свърже с отдел Администриране на търговията с електрическа енергия в ЕСО ЕАД (e-mail [eto.admin@eso.bg](mailto:eto.admin@eso.bg) или телефон +359 2 9691 318) и да поиска генерирането на нови кодове за достъп.

За участниците, които изпращат външни графици за обмен на електроенергия със съседни държави или участват на тръжните процедури за разпределение на преносни способности може освен на горепосочения адрес да се свържат с отдел Междусистемни обмени (тел. +359 2 9213 652 или на e-mail [eso.auction@eso.bg](mailto:eso.auction@eso.bg) ).