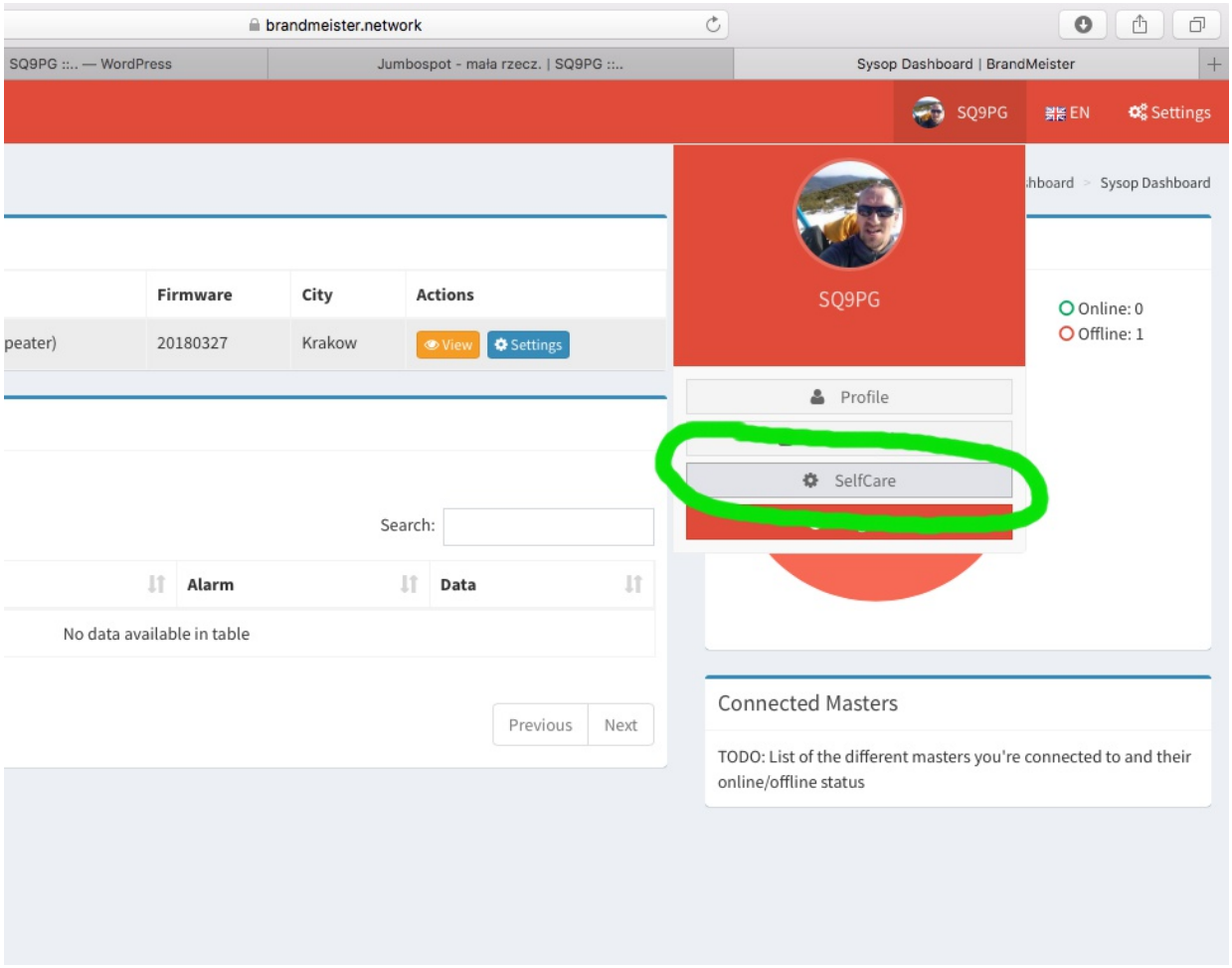
Jak chronić swoje ID w sieci DMR BM?

Praktyka używania i korzystania z sieci **DMR** Brandmeister pokazuje, że nie ma takiego ID, którego nie można przechwycić, tym bardziej, że nie jest ono zupełnie chronione, a sieć używa go tylko do identyfikacji rozmówcy.

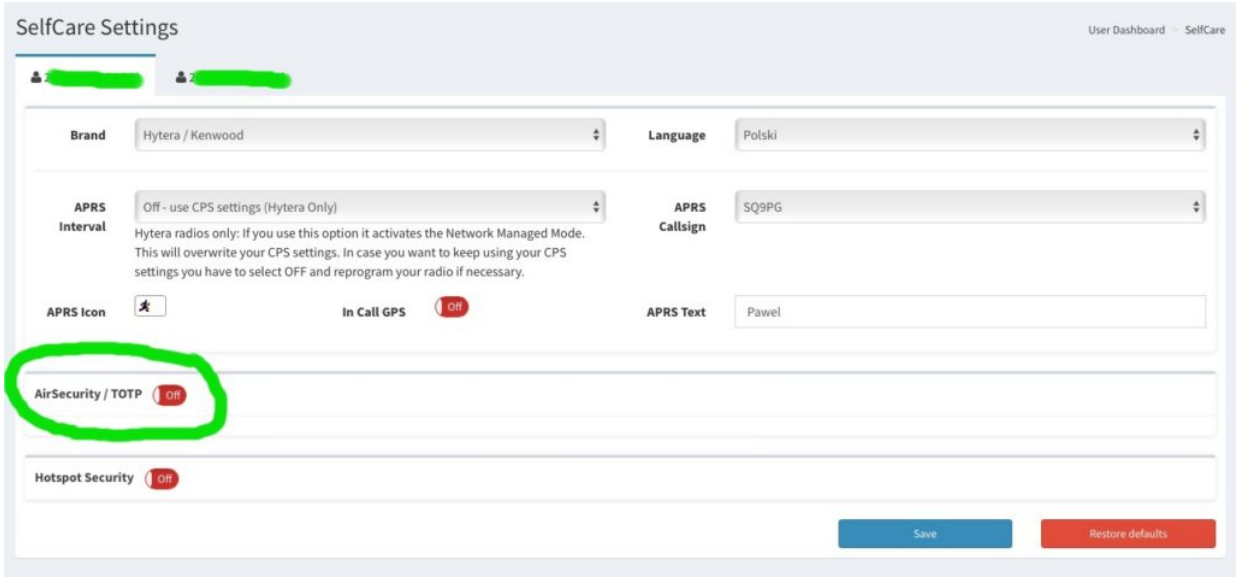
AirSecurity to mechanizm, który umożliwia ochronę Twojego identyfikatora przed nielegalnym użyciem, dzięki ograniczonemu czasowo dostępowi przy użyciu Twojego identyfikatora. Ta funkcja jest opcjonalna, możesz ją włączyć lub wyłączyć za pomocą pulpitu nawigacyjnego. W tej chwili **Air Security** może chronić połączenia, które są przesyłane tylko przez serwer główny.

Idźmy zatem do meritum:

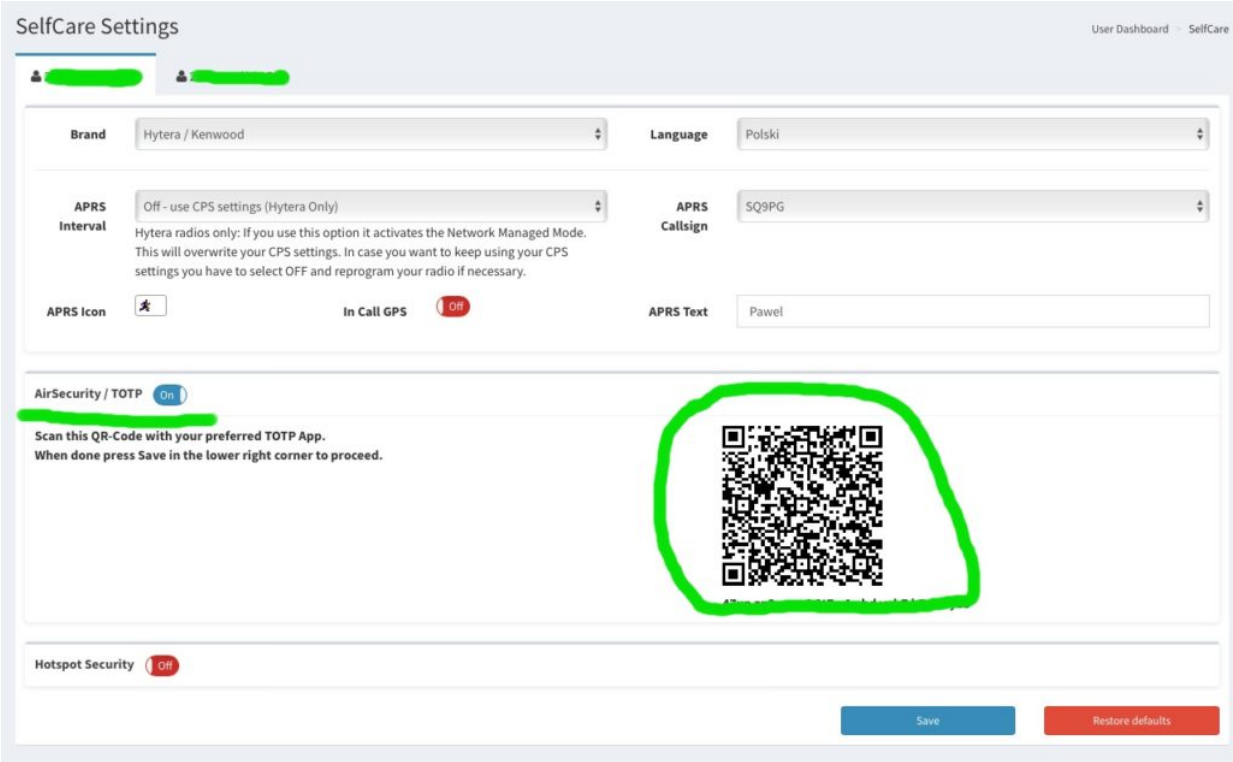
1. Potrzebujemy konta w systemie **BrandMeister**, jeśli go jeszcze nie mamy to trzeba je koniecznie utworzyć.
2. Logujemy się do BrandMeister-a, i w naszym Panelu Administracyjnymi po zalogowaniu w prawym, górnym rogu rozwijamy menu i klikamy **SelfCare.**



3. Naszym oczom ukaże się taki ekran:



Domyślnie opcja **AirSecurity** jest wyłączona, więc trzeba ją włączyć. Po włączeniu na naszym ekranie zobaczymy kwadrat z kodem, który pomoże nam wygenerować jednorazowe hasło.



4. Potrzebna nam będzie aplikacja, najlepiej w smartfonie. Może to być np: **Google Authenticator** albo dowolna inna aplikacja dająca możliwość generowania haseł jednorazowych opartych na algorytmie generowania jednorazowych haseł w kilkudziesięciosekundowych odstępach czasowych – [standard RFC 6238](). (W telefonach Apple może to być np: **OPT Auth**).
5. Aplikacja generuje unikalne hasło co 30 sekund, które pomoże nam otworzyć sesję dostępu, a więc:
   – uruchamiamy aplikację i skanujemy kod z ekranu,

   – klikamy przycisk **ZAPISZ** na pulpicie nawigacyjnym **BrandMeister-a** (w komputerze),
   – w aplikacji klikamy na nasz przed chwilą zeskanowany

kod,
– w radiu inicjujemy prywatne połączenie do odbiorcy, którego **ID** wygenerowała nam przed chwilą aplikacja, pamiętając, aby **zawsze** najpierw wpisać cyfrę **9** a następnie **6 cyfr**, które wygenerowała nam aplikacja w telefonie,

– naciskamy PTT (przez około 2 sekundy) aby zainicjować połączenie,
– i wszystko gotowe !

6. Utworzona w ten sposób sesja dostępu będzie aktywna **tylko przez 15 minut**. Po tym czasie przy wciśnięciu PTT na grupie 260 usłyszymy komunikat: „*Access denied*„, czyli **Brak dostępu**.Wtedy trzeba już tylko:
– uruchomić sobie naszą sprytną aplikację w smartfonie,
– przepisać aktualnie wygenerowane przez nią hasło jako numer ID dla połączeń prywatnych (**nie zapomnijmy dodać** na początku cyfry **9**),
– wcisnąć PTT przez około 2 sekundy,
– i gdy usłyszymy komunikat: „*Access code accepted*” – znów będzie można bezpiecznie prowadzić korespondencję na dowolnej grupie (niekoniecznie na grupie 260).

Włączenie tego sposobu zabezpieczenia spowoduje, że każdy kto będzie chciał używać naszego ID zostanie odrzucony przez BrandMeistera i poinformowany o tym przez komunikat „*Access denied*” problemem jest konieczność ponawiania autoryzacji co 15 minut.

Mechanizm **AirSecurity** nie działa dla TG9, ponieważ połączenia lokalne (ze swej natury) nie przechodzą przez serwer centralny

i nie mogą być przez niego weryfikowane.

- *dwie ostatnie grafiki pochodzą ze strony: https://wiki.brandmeister.network/index.php/AirSecurity*
- *grafika ilustracyjna w nagłówku: pixabay.com*