SVXReflector protokół V3

SVXReflector V3 ma dodaną obsługę certyfikatów X.509 do uwierzytelniania i szyfrowania połączenia z serwerem. Połączenie TCP jest szyfrowane przy użyciu protokołu TLS, a połączenie UDP jest szyfrowane przy użyciu niestandardowego schematu klucza współdzielonego. Realizacja jest oparta na OpenSSL. Zarówno serwer, jak i klient wymagają uwierzytelnienia. Proces generowania certyfikatów jest w większości zautomatyzowany.

Poniżej opis, który ma na celu przybliżenie, w jaki sposób działa mechanizm autoryzacji w nowej wersji svxreflectora z protokołem V3.

SVXReflector V3 nadal obsługuje nody przy pomocy autoryzacja hasła podanego w AUTH_KEY w svxlink.conf oraz przy pomocy certyfikatów.

Warto zapoznać się z propozycją autora svxlink, w jaki sposób przeprowadzić migracje reflektora z V2 na V3: https://groups.io/g/svxlink/message/2421

Kiedy mamy uruchomiony SVXReflecotr V3 mamy następujące możliwości logowania w zależności od ustalonej lokalnej polityki podłączania się do reflektora (o szczegóły pytaj administratorów reflektora)

Metoda autoryzacji stosowana dla reflektora z obsługą protokołu V2.

Logowanie przy pomocy hasła:
W svxlink.conf należy używać ustawień w **[ReflectorLogic]**:
SVXLink wersje 1.8 i niższe: **TYPE=Reflector**
SVXLink wersja 1.8.99.0 i wyższe: **TYPE=ReflectorV2**
I następnie dla wszystkich wersji svxlink:
CALLSIGN= (znak noda)
AUTH_KEY= (hasło do logowania)

Autoryzacja przy pomocy hasła dla reflektora z obsługą protokołu V3

Tylko użytkownicy nowych wersji svxlink 1.8.99.x mogą logować się przy pomocy hasła i korzystać z protokołu v3, muszą w svxlink.conf mieć ustawione w **[ReflectorLogic]**
TYPE=Reflector
CALLSIGN= (znak noda)
AUTH_KEY= (hasło do logowania)

Przy pierwszym logowaniu będzie generowany certyfikat, ale dopóki certyfikat nie będzie podpisany przez svxreflector, będzie używane hasło do autoryzacji. Możemy podać nasz adres email w **CERT_EMAIL** może on pozwolić/ułatwić komunikacje sysopa svxreflectora z użytkownikiem.

Autoryzacja przy pomocy certyfikatu X.509 dla reflektora z protokołem w wersji V3

Tylko użytkownicy nowych wersji svxlink 1.8.99.x mogą logować się przy pomocy certyfikatu, muszą w svxlink.conf mieć ustawione w **[ReflectorLogic]**
TYPE=Reflector
CALLSIGN= (znak noda)
CERT_EMAIL= (**obowiązkowe**, adres email SYSOP'a noda) - podany adres posłuży do komunikacji z sysopem noda, może być wysłana informacja o akceptacji certyfikatu (sprawdzaj folder SPAM, bo może tam wylądowywać powiadomienie, jeśli takie serwer wysyła i ma to skonfigurowane). Ważne, aby adres był działający i ten sam który używany był podczas rejestracji via formularz na stronie FM POLAND
W zależności od lokalnej polityki reflektora z obsługą protokołu V3 i logowania via certyfikat może być wymagane usunięcie hasła w **AUTH_KEY=** w pliku /etc/svxlink.conf po otrzymaniu podpisanego certyfikatu przez serwer (o szczegóły pytaj administratorów reflektora).

Upewnij się, czy Twój lokalny svxreflector obsługuje protokół V3 (na obecną chwilę pisania tego dokumentu tj. Marzec 2025 FM POLAND nie obsługuje/podpisuje certyfikatów do logowania tylko można używać hasła do logowania dla protokołu V3)

Info w logu serwera dla autoryzacji przez hasło: **ZNAK: Received valid auth key**
Info w logu serwera dla autoryzacji podpisanym certyfikatem: **ZNAK: CN = ZNAK**

UWAGA:
Brak poprawnych wpisanych danych w certyfikacie szczególne dotyczy to **CERT_EMAIL** może skutkować brakiem akceptacji przez SYSOP'ów Reflectora tego certyfikatu.

Uruchomiony svxlink z ustawionym adresem email w CERT_EMAIL wygeneruje klucz prywatny i CSR (prośba o podpisanie certyfikatu) w którym będzie informacja o adresie

email i następnie łącząc się z SVXReflector V3 pobierze pakiet CA i wyśle CSR do serwera reflektora (Certificate Signing Request)

CSR jest to żądanie podpisania certyfikatu niezbędne w procedurze certyfikacji. Plik CSR jest to plik zawierający fragment zaszyfrowanego tekstu wygenerowanego przez serwer, na którym ma działać certyfikat. Zawiera informacje, które będą użyte w certyfikacie, takie jak np.: Znak stacji/noda oraz adres email właściciela noda. Zawiera także klucz publiczny, służący szyfrowaniu przesyłanych informacji. Równocześnie z plikiem CSR generowany jest klucz prywatny (rozszyfrowujący), który musi pozostać do wyłącznej wiadomości właściciela certyfikatu.

Użytkownik, który łączy się z SVXReflectorem, jeśli certyfikat jego został podpisany zostaje on przesłany do SVXLink który zapisuje na komputerze użytkownika podpisany plik crt w katalogu /var/lib/svxlink/pki/CALLSIGN.crt

Od tego moment użytkownik/nod posiadający ważny certyfikat będzie się mógł łączyć z serwerem SVXReflectora Użytkownik musi zachować kopie plików .csr, .crt .key i w sytuacji, kiedy będzie uruchamiał nowy system, musi wkopiować pliki crt, csr, key do katalogu /var/lib/svxlink/pki/ aby móc zalogować sie do SVXReflectora. Właściciele węzłów powinni zadbać o bezpieczeństwo klucza węzła /var/lib/svxlink/pki/CALLSIGN.key i przechowywać kopie ich poza hotspotem.

Utracenie podpisanych certyfikatów przez użytkownika powoduje, że należy rozpocząć ponowny proces akceptacji podpisania certyfikatu. W takiej sytuacji należy na serwerze usunąć pliki CSR i CRT użytkownika/noda i czekać na przesłanie przez użytkownika/noda nowego CSR pliku do akceptacji Istnieje funkcja bezpieczeństwa, która uniemożliwia węzłowi zarejestrowanie nowego CSR, jeśli węzeł utworzył nowy klucz prywatny/publiczny.

Certyfikat użytkownika jest ważny 90 dni. Certyfikaty węzła będą automatycznie odnawiane za każdym razem, gdy węzeł zostanie podłączony, od 60 do 90 dnia okresu ważności. Nie trzeba go podłączać od razu w momencie wygaśnięcia certyfikatu.

Usunięcie certyfikatu naprawdę nie jest możliwe po stronie reflektora. Nawet jeśli usuniesz zarówno CSR, jak i certyfikat dla węzła, węzeł nadal będzie mógł zalogować się przy użyciu wystawionego mu certyfikatu. To jest funkcja, a nie błąd. Drugi (zapasowy) reflektor powinien być w stanie zaakceptować połączenie z węzła, nie wiedząc o tym nic.

Blokowanie tymczasowe konta.
Dopóki użytkownik operuje otrzymanym podpisanym certyfikatem może łączyć się z SVXReflector. W ramach protokołu V3 jest dostępna opcja w konfiguracji do blokowania noda (np. do czasu wyjaśnienie problemu). Opcja ta działa dla protokołu V2 i V3

System powiadomień via email.

SVXReflector posiada system powiadamiania poprzez email o operacjach związanych z certyfikatami. Wymagana jest konfiguracja ze strony serwera, aby wysyłał takie powiadomienia.

Jeśli użytkownik pierwszy raz będzie się łączył z reflektorem przy pomocy protokołu V3 (w svxlink.conf TYPE=Reflector dla wersji v1.8.99.x) i jeśli poda działający swój adres email w konfiguracji (CERT_EMAIL w svxlink.conf) to na ten adres może zostać wysłana informacja o wygenerowanym nowym certyfikacie. Jeśli SYSOP na reflektorze zaakceptuje certyfikat to użytkownik noda dostanie powiadomienie na adres email, który podał w swojej konfiguracji (użytkownik musi sprawdzić pocztę w folderze SPAM czy przypadkowo nie została tam umieszczony). Dlatego tak ważne jest podanie poprawnego adresu email w konfiguracji svxlink bo adres ten też będzie używany do komunikacji SYSOPów z właścicielem noda i sprawdzany, czy z tego samego adresu email zostało wysłane zgłoszenie o przyznanie konta.