KDPW

Załącznik 4: wykorzystanie OpenSSL do uzyskania certyfikatu do komunikacji A2A

Niniejszy załącznik stanowi instrukcję w zakresie użycia narzędzia OpenSSL do wygenerowania żądania podpisania certyfikatu, niezbędnego do poprawnego złożenia wniosku w aplikacji „Certyfikaty A2A", która wraz z wdrożeniem drugiego etapu projektu będzie udostępniona uczestnikom bezpośrednim KDPW. **Analogiczna aplikacja zostanie udostępniona uczestnikom rozliczającym KDPW_CCP.** Żądanie podpisania certyfikatu powinno być generowane bezpośrednio przez podmiot wnioskujący, w jego własnej infrastrukturze, przy użyciu narzędzi kryptograficznych zgodnych z jego polityką. Tym samym polecenia opisane w załączniku należy traktować wyłącznie jako przykład wykorzystania OpenSSL, nie zaś jako wymaganie korzystania z tego konkretnego narzędzia.

UZYSKANIE CERTYFIKATU DO KOMUNIKACJI A2A

O certyfikatach dedykowanych komunikacji A2A

Certyfikat elektroniczny służący do komunikacji A2A z usługami świadczonymi przez KDPW wystawiany jest na dany kod instytucji na podstawie przekazanego żądania podpisania certyfikatu (CSR). Certyfikat wykorzystany zostanie do ustanowienia szyfrowanego połączenia w oparciu o protokół TLS, a także do uwierzytelnienia się do odpowiedniego kanału komunikacyjnego w ramach komunikacji A2A opartej o kolejki MQ.

By zapewnić bezpieczeństwo dla generowanego certyfikatu, w ramach całego procesu jego uzyskania klucz prywatny nie może opuścić infrastruktury właściciela certyfikatu. Oznacza to, że musi on być stworzony poza infrastrukturą KDPW, a sam certyfikat powinien być wygenerowany w odpowiedzi na przekazane żądanie podpisania certyfikatu, przygotowanego zgodnie z ustalonym schematem.

W ramach komunikacji A2A z usługami KDPW należy użyć certyfikatu zgodnego z następującym schematem:

- Typ klucza (Key type): RSA
- Długość klucza (Key size): 2048
- Nazwa podmiotu X.509:
  - Organization Name (O=[A-Z0-9]{4,4}) - kod instytucji np. XXXX
  - Organizational Unit Name (OU=[PRD;TST]) - oznaczenie środowiska
  - Common Name (CN= [A-Z0-9]{4,4}+„_A2A") - nazwa powszechna np. XXXX_A2A

Dla komunikacji A2A z usługami KDPW_CCP certyfikat powinien być zgodny ze schematem:

- Typ klucza (Key type): RSA
- Długość klucza (Key size): 2048
- Nazwa podmiotu X.509:
  - Organization Name (O=[A-Z0-9]{4,4}) - kod instytucji np. XXXX
  - Organizational Unit Name (OU=[PRD;TST]) - oznaczenie środowiska
  - Common Name (CN= [A-Z0-9]{4,4}+„_CCPA2A") - nazwa powszechna np. XXXX_CCPA2A

Proces może być realizowany w oparciu o szereg narzędzi implementujących algorytmy kryptograficzne i pozwalające na wygenerowanie pary kluczy w ramach architektury PKI. Przykłady wskazane w dokumentacjach KDPW odnosić się będą do narzędzi OpenSSL, dostępnych powszechnie w ramach licencji Apache, niemniej opisane do wykonania czynności mogą też być przeprowadzone z wykorzystaniem innych narzędzi.

O OpenSSL

OpenSSL (https://www.openssl.org) jest wieloplatformowym narzędziem będącym zestawem bibliotek implementujących podstawowe operacje kryptograficzne w obszarze wsparcia protokołów SSL i TLS. Jest dystrybuowany na zasadach open source w ramach licencji typu Apache, co oznacza, że może być używany nieodpłatnie do celów komercyjnych i niekomercyjnych, z zastrzeżeniem kilku warunków licencyjnych.
Pakiet instalacyjny OpenSSL może być pobrany ze strony https://wiki.openssl.org/index.php/Binaries.
Dla poprawności procesu uzyskania certyfikatu do komunikacji A2A nie ma znaczenia na jakiej platformie systemowej zostanie uruchomiony.
Wykorzystując OpenSSL należy upewnić się, że w środowisku przygotowanym do wygenerowania żądania udostępnienia podpisanego certyfikatu jest zainstalowane odpowiednie oprogramowanie kryptograficzne, oraz jest dostępne z poziomu katalogu, w którym zostanie przeprowadzona operacja, a także czy profil, z którego przeprowadzana będzie procedura posiada odpowiedni poziom uprawnień do jego użycia.

GENEROWANIE ŻĄDANIA PODPISANIA CERTYFIKATU Z WYKORZYSTANIEM OPENSSL

Generowanie z wprowadzaniem informacji w sposób interaktywny

Wygenerowanie żądania podpisania certyfikatu w sposób umożliwiający wprowadzanie danych interaktywnie wymaga wprowadzenia poniższej komendy.

```
openssl req -newkey rsa:2048 -keyout private.key -out request.csr
```

Po uruchomieniu komendy konieczne będzie podanie hasła, którym będzie zabezpieczony klucz prywatny. Ustanowione hasło będzie wymagane aby uzyskać dostęp do klucza prywatnego przy kolejnych operacjach, które będą wykonywane z jego użyciem.
Na dalszym etapie tworzenia żądania podpisania certyfikatu konieczne będzie wprowadzenie dodatkowych informacji dotyczących podmiotu, dla którego tworzony będzie certyfikat. Jest istotnym, aby dane wprowadzane w odpowiednie pola były zgodne z przyjętym schematem. Wartości pól spoza schematu mogą być pominięte, co w przypadku OpenSSL oznacza wprowadzenie znaku kropki („.”).
W przypadku CSR wypełnienie pól przedstawia się następująco:

- Country Name (2 letter code) - „.”
- State or Province Name (full name) - „.”
- Locality Name (e.g., city) - „.”
- Organization Name (e.g., company) - kod instytucji np. XXXX
- Organizational Unit Name (e.g., section) - kod środowiska (PRD lub TST)

- Common Name (e.g., server FQDN) - nazwa powszechna np. XXXX_A2A
- Email Address - „.”
- A challenge password - „.”
- An optional company name - „.”

Po zakończeniu, gotowe do przesłania żądanie zostanie zapisane we wskazanym przy wywołaniu komendy pliku CSR – w przedstawionym przykładzie będzie to plik „request.csr”. Zawartość pliku CSR powinna być przekazana do KDPW w treści wniosku, składanego z wykorzystaniem aplikacji „Certyfikaty A2A”.

Generowanie automatyczne, za pomocą pełnej komendy

Jedną z dostępnych opcji podczas tworzenia żądania podpisania certyfikatu jest podanie wszystkich niezbędnych informacji w samym poleceniu za pomocą opcji -subj dostępnej dla komendy OpenSSL. W ramach wartości dla opcji możliwe jest wskazanie informacji wymaganych w ustalonym schemacie certyfikatu. W przypadku certyfikatu do komunikacji A2A w ramach usług KDPW dane powinny być wskazane w następujący sposób.

```
-subj "/O=XXXX/OU=TST/CN=XXXX_A2A"
```

Pełna komenda utworzenia żądania podpisania certyfikatu przyjmuje zatem następującą postać.

```
openssl req -newkey rsa:2048 -subj "/O=XXXX/OU=TST/CN=XXXX_A2A" -keyout
private.key -out request.csr
```

Po wywołaniu komendy należy wprowadzić hasło do zabezpieczenia klucza prywatnego, a następnie je potwierdzić. W efekcie klucz prywatny zostanie zakodowany z użyciem wprowadzonego hasła, będzie ono wymagane w przypadku konieczności użycia klucza prywatnego.
By wskazać hasło bezpośrednio w komendzie utworzenia pliku CSR należy wywołać poniższą komendę (w przedstawionym przykładzie ciąg znaków „123456789” stanowi hasło).

```
openssl req -newkey rsa:2048 -subj "/O=XXXX/OU=TST/CN=XXXX_A2A" -passout
pass:123456789 -keyout private.key -out request.csr
```

Po zakończeniu, gotowe do przesłania żądanie zostanie zapisane we wskazanym przy wywołaniu komendy pliku CSR – w przedstawionym przykładzie będzie to plik „request.csr”. Zawartość pliku CSR powinna być przekazana do KDPW w treści wniosku, składanego z wykorzystaniem aplikacji „Certyfikaty A2A”.

Pobranie treści żądania podpisania certyfikatu

Uzyskanie certyfikatu podpisanego przez Centrum Autoryzacyjne KDPW realizowane jest poprzez aplikację „Certyfikaty A2A” dostępną w Portalu Usług, gdzie po uwierzytelnieniu oraz wybraniu właściwego kodu instytucji, istnieje możliwość złożenia stosownego wniosku. W treści wniosku (wykorzystując przewidziane do tego okno tekstowe) należy wkleić treść wygenerowanego pliku CSR.

By pobrać treść pliku można posłużyć się dowolnymi metodami. W zależności od preferencji, można otworzyć plik CSR w dowolnym edytorze tekstowym, po czym skopiować zawartość do składanego w aplikacji wniosku. Można też wyświetlić treść pliku CSR korzystając z linii poleceń i następujących komend:

- w systemie Windows

```
more .\request.csr
```

- w systemie Linux

```
cat ./request.csr
```

Wyświetlona zawartość pliku CSR wygląda podobnie do przykładu wskazanego poniżej. Co istotne, kopiując zawartość należy uwzględnić znaczniki początku i końca żądania.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICdTCCAV0CAQAwMDENMAsGA1UECgwEWFhYWDEMMAoGA1UECwwDVFNUMREwDwYD
VQQDDAhYWFhYX0EyQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKyl
otU7qeztCrG23DjSrJlPGdVwtj5Ikdid7BDgWTNMji+6rgYHosMtXT+slmMH3oSp
ryN9eKl1Ci3L5VdTuye7/qaPsAoHnTmdH8gSu67RVeRmqZkYfjorPQBWF+cKGhca
RMy2z0AoUfHEa51KV/lWBRo/ulm0a0V1E7sRrS/Fk/7pCJ3Vbh9KsrZIxNa4ZLux
tRYFOEoBBJ/Nri7mPOm+39hx98nR6czEOcBtGJ8KKPyZXbluZs5j1Gh7qGBO8h/h
0BM5RESMcls56qpANq21jrxT7shK1il6lbsxgGHCIJKqbzk9sPPkHYBpfeDZOb4p
L1KWU03PiLlOHoBdR88CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IBAQAdDCLkd+LD
4MjLWdejk0L5KCC6S97M1sagfBeWBgxcv0ncfSx8laKMb9sjFWcQW75io/E5fH69
nosWQNAWdQO37vB4cRr3ihlLTrks3VqVD7OYowTEK735VYYXM9wBnhmYbY0o9SnN
UnWx/RIise1eokj9BFbW07EOZ5MiwcZ4PTVBk1AKRBHzPVNM4bOifrJskoQ8+S4g
+Jx3LTBSJ5VZBARDxKYWnkYSFV4krUa+Xlmj89G1LP3jern6j8SCJVX3tf7s+a+o
1COGvZ576NA4n1bHLfbKU4KMJiIRcpz8iW+gkJSdz1nwr00LhwVAKxjtHPMET4s+
4L1nSrXwUx24
-----END CERTIFICATE REQUEST-----
```

POBRANIE WYGENEROWANEGO CERTYFIKATU

Po złożeniu wniosku o wydanie podpisanego przez KDPW certyfikatu oraz jego przetworzeniu przez KDPW, w aplikacji „Certyfikaty A2A" udostępniony zostanie certyfikat w formacie PEM. Może on zostać pobrany po wybraniu opcji „Zapisz", dostępnej dla aktywnych certyfikatów w widoku z listą wydanych dla danego kodu instytucji certyfikatów.

Pobrany certyfikat stanowi parę z kluczem prywatnym wygenerowanym wraz z tworzeniem pliku CSR, dlatego, zwłaszcza przy generowaniu większej liczby certyfikatów, warto zadbać o to, by nie utracić tego powiązania. Można też powiązać certyfikat z jego kluczem prywatnym w pliku PFX (format PKCS#12)

Dalsze czynności związane z wykorzystaniem certyfikatu zależą od wewnętrznej infrastruktury instytucji, dla której certyfikat został wygenerowany.

Połączenie certyfikatu i klucza prywatnego z wykorzystaniem formatu PKCS#12

Format PKCS #12 (PFX) przechowuje i certyfikat i klucz prywatny w jednym zaszyfrowanym pliku. By utworzyć certyfikat w tym formacie po jego pobraniu z KDPW (format PEM) można posłużyć się poniższą komendą.

```
openssl pkcs12 -inkey private.key -in certificate.pem -export -out certificate.pfx
```

Jeśli utworzony wcześniej klucz prywatny został zakodowany z użyciem hasła, do wykonania operacji niezbędne będzie jego podanie. Dodatkowo, w trakcie tworzenia pliku PFX możliwe będzie wprowadzenia hasła zabezpieczającego dane w tworzonym pliku.

WERYFIKACJA

Przedstawione w tym rozdziale komendy OpenSSL pokazują sposoby weryfikacji poprawności wytworzonych danych. Wykonywanie tych operacji nie jest niezbędne do uzyskania certyfikatu A2A, niemniej pozwoli na ustalenie przyczyn ewentualnych błędów w trakcie przeprowadzenia procesu.

Weryfikacja poprawności przygotowanego żądania podpisania certyfikatu

```
openssl req -text -in request.csr -noout -verify
```

Komenda pozwoli zweryfikować podpis w pliku CSR, a także wybrany algorytm i zawartość pól wprowadzonych w ramach ustalonego przez KDPW schematu.

```
Certificate request self-signature verify OK
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: O = XXXX, OU = TST, CN = XXXX_A2A
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ac:a5:a2:d5:3b:a9:ec:ed:0a:b1:b6:dc:38:d2:
                    ac:99:4f:19:d5:70:b6:3e:48:91:d8:9d:ec:10:e0:
                    96:63:07:de:84:a9:af:23:7d:78:a9:75:0a:2d:cb:
                    51:f1:c4:6b:9d:4a:57:f9:56:05:1a:3f:ba:59:b4:
                    ... (dalsza część nie została pokazana)
```

Jeśli podpis nie zostanie zweryfikowany poprawnie (wprowadzone zostały modyfikacje w zawartości pliku CSR) lub pozostałe dane nie będą odpowiadały wymaganemu przez KDPW schematowi, wniosek o wydanie certyfikatu zostanie odrzucony.

Weryfikacja zgodności kluczy

Weryfikacja zgodności plików wytwarzanych w ramach procesu uzyskiwania certyfikatu może być przeprowadzona poprzez sprawdzenie zgodności klucza publicznego, wyodrębnionego z każdego z plików. Jeśli dla wszystkich plików klucz publiczny jest zgodny oznacza to, że są one zgodne i dotyczą jednego certyfikatu. Ten sposób może też pomóc ustalić, czy klucz prywatny odpowiada certyfikatowi, w przypadku utraty pewności co do ich powiązania.
By uprościć proces porównania kluczy prywatnych można skorzystać z funkcję skrótu SHA-256 dla wyodrębnionych wartości.

By obliczyć funkcję skrótu dla poszczególnych plików z użyciem OpenSSL należy użyć następujących komend:

- SHA-256 klucza publicznego na podstawie klucza prywatnego

```
openssl pkey -pubout -in .\private.key | openssl sha256
```

- SHA-256 klucza publicznego na podstawie żądania podpisania certyfikatu (CSR)

```
openssl req -pubkey -in .\request.csr -noout | openssl sha256
```

- SHA-256 klucza publicznego na podstawie uzyskanego certyfikatu

```
openssl x509 -pubkey -in .\certificate.pem -noout | openssl sha256
```

Funkcje powinny być wywoływane niezależnie.
Wynikiem każdej z funkcji jest informacja o wartości skrótu obliczonej dla klucza publicznego wyodrębnionego z każdego z plików. Wynik przyjmuje następującą postać.

```
SHA2-256(stdin)=
afd5b3b3739493c373024416a60d42676227007a6c62dcdfa72a96cfda3edb5c
```

W przypadku stwierdzenia różnic w prezentowanej wartości, zestaw plików nie reprezentuje danych dotyczących tego samego certyfikatu. W takich wypadkach rekomenduje się powtórne wygenerowanie certyfikatu.