WERYFIKACJA PODPISU ODPOWIEDZI

W niniejszym dokumencie został opisany proces weryfikacji podpisu elektronicznego złożonego pod komunikatem zwrotnym (response) wysyłanym z Systemu P1 przez usługi sieciowe dostępne pod adresem **https://sus.ezdrowie.gov.pl** do systemu zewnętrznego w odpowiedzi na przesłane przez nich żądanie (request).

Cała komunikacja miedzy Systemem P1, a Systemami zewnętrznymi realizowana jest z wykorzystaniem protokołu komunikacyjnego SOAP rozszerzonego o profil Web Services Security X.509 Certificate Token. W związku z powyższym zarówno żądanie (request) wysyłane przez System zewnętrzny, jak i odpowiedź (response) wysyłana przez System P1, opatrzone są podpisem cyfrowym, do weryfikacji, którego służy certyfikat dołączony do komunikatu (request oraz response) w węźle `wsse:BinarySecurityToken`. Dla komunikatu request będzie to certyfikat Systemu zewnętrznego, a dla komunikatu typu response będzie to certyfikat systemu centralnego – dostawcy usługi.

Aby poprawnie przeprowadzić proces weryfikacji podpisu pod komunikatem response niezbędne jest poprawne zweryfikowanie zaufania do certyfikatów służących do weryfikacji podpisu. Należy postępować zgodnie ze standardowymi algorytmami weryfikacji opisanymi w specyfikacji XML Signature Syntax and Processing Version 2.0, w szczególności zastosować następujące zasady:

1. Weryfikacja numeru seryjnego podanego jako część atrybutu DN (`serialNumber`) certyfikatu końcowego systemu P1.
    a. Certyfikat służący do weryfikacji podpisu pod komunikatem response należy pobrać z elementu `wsse:BinarySecurityToken` komunikatu.
    b. Certyfikat służący do weryfikacji podpisów komunikatów odpowiedzi musi mieć w DN część `SERIALNUMBER = 2.16.840.1.113883.3.4424.12.3: 1`
2. Weryfikacja ścieżki certyfikacji
    a. Zbudowanie pełnej ścieżki certyfikacji począwszy od certyfikatu końcowego systemu P1, przez **CC P1 SubCA WSS**, aż po certyfikat **CC P1 RootCA** i zweryfikowanie ich ważności:
        i. czy jest już ważny - pole **Ważne od** (`notBefore`) z certyfikatu
        ii. czy nie wygasły - pole **Ważne do** (`notAfter`) z certyfikatu
        iii. czy nie zostały unieważnione na podstawie aktualnej listy CRL - pole **Punkt dystrybucji CRL** (`CRLDistributionPoints`), znajduje się w każdym certyfikacie ze ścieżki
    b. Weryfikacja zaufania do ścieżki certyfikacji na podstawie lokalnej konfiguracji tj. składnicy certyfikatów zaufanych przez stronę kliencką, w której znajdują się zaufane certyfikaty CA (trust anchor).
3. Weryfikację podpisu pod komunikatem i jego integralności – weryfikacja podpisu pod komunikatem powinna polegać na wyliczeniu funkcji skrótu wg. algorytmu podanego w węźle `ds:SignatureMethod Algorithm` z całego elementu `soap:Body` i porównanie wyliczonej wartości funkcji skrótu z wartością zapisaną w komunikacie w węźle `ds:SignatureValue`.

Zgodnie ze specyfikacją X.509, każdy certyfikat ze względów bezpieczeństwa ma z góry określony czas ważności (validity period), co implikuje dokonanie jego wymiany **przed** okresem upłynięcia jego ważności (aktualnie są to 2 lata).

W związku z powyższym, w celu zapewnienia ciągłości działania systemów zewnętrznych (w szczególności aplikacji aptecznych oraz gabinetowych) bardzo ważne jest zastosowanie zasad poprawnej weryfikacji zaufania do certyfikatu służącego do weryfikacji podpisu komunikatu odpowiedzi zwracanego z Systemu P1.