Wskazówki dotyczące akceptacji kwalifikowanych podpisów elektronicznych
Zalecenia ekspertów Polskiej Izby Informatyki i Telekomunikacji

1 Wprowadzenie

Kwalifikowane podpisy elektroniczne stanowią elektroniczną formę oświadczenia woli i są uznawane za równoważne podpisom własnoręcznym. Ich walidacja, czyli weryfikacja prawidłowości podpisu, jest nieodłącznym elementem ich stosowania w procedurach firmowych oraz administracyjnych, jednakże nierzadko wynik tej walidacji z różnych powodów może być niejednoznaczny. W takiej sytuacji, decyzja o akceptacji lub braku akceptacji dokumentu opatrzonego podpisem elektronicznym musi nastąpić na podstawie przyjętych w danym procesie lub organizacji reguł lub przepisów. Celem niniejszego dokumentu jest opracowanie generalnych wskazówek dla podmiotów akceptujących kwalifikowane podpisy elektroniczne (tzw. stron ufających), na podstawie których mogą w pewnym zakresie przyjąć one własne, wewnętrzne reguły pozwalające odpowiednio interpretować niejednoznaczny wynik walidacji i tym samym zaakceptować kwalifikowany podpis elektroniczny.

2 Podstawowe informacje o kwalifikowanym podpisie elektronicznym

1. Definicja prawna (rozporządzenie UE 910/2014 – eIDAS):
   Kwalifikowany podpis elektroniczny oznacza zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego.

2. Kwalifikowany podpis elektroniczny to dane w postaci elektronicznej, które w szczególności zawierają między innymi następujące informacje (atrybuty):
   a. Kwalifikowany certyfikat lub jednoznaczne odniesienie do kwalifikowanego certyfikatu, który zawiera dane służące do weryfikacji podpisu oraz dane identyfikujące osobę składającą podpis.
   b. Deklaratywną datę złożenia podpisu elektronicznego
      Uwaga: Deklaratywna data wskazująca na czas złożenia podpisu nie korzysta z domniemań prawnych i nie ma mocy prawnej daty pewnej, gdyż jest to data pochodząca z komputera lub systemu informatycznego, na którym był realizowany proces podpisywania.
   c. Wyliczoną na podstawie podpisywanych danych i wcześniej dodanych atrybutów wartość funkcji skrótu pozwalającą na zabezpieczenie integralności podpisu i podpisanych danych
   d. Wyliczoną, na podstawie wartości skrótu, wartość podpisu elektronicznego, której utworzenie i weryfikacja są realizowane za pomocą funkcji kryptograficznych.
   e. Opcjonalnie – kwalifikowany elektroniczny znacznik czasu, korzystający z domniemania prawnego daty pewnej wskazującej, że podpis został złożony nie później niż w tej dacie.

3. Kwalifikowany podpis elektroniczny jest składany za pomocą kwalifikowanego urządzenia do składania podpisu (QSCD), które w oparciu o przechowywane dane do składania podpisu elektronicznego wylicza wartość podpisu. Informacja o tym, że podpis był składany za pomocą

kwalifikowanego urządzenia jest zawarta w kwalifikowanym certyfikacie podpisu elektronicznego. Ta informacja jest niezmienna dla pojedynczego certyfikatu; certyfikat jednoznacznie potwierdza, czy podpis jest składany za pomocą QSCD, czy bez jego udziału.

3 Ważność kwalifikowanego podpisu elektronicznego

Kwalifikowany podpis elektroniczny uważa się za ważny, jeżeli spełnione są warunki walidacji opisane w artykule 32 ust. 1 rozporządzenia eIDAS, czyli:

a) certyfikat, który towarzyszy podpisowi, był w momencie składania podpisu kwalifikowanym certyfikatem podpisu elektronicznego zgodnym z załącznikiem I rozporządzenia eIDAS;
b) kwalifikowany certyfikat został wydany przez kwalifikowanego dostawcę usług zaufania i był ważny w momencie składania podpisu;
c) dane służące do walidacji podpisu odpowiadają danym dostarczonym stronie ufającej;
d) unikalny zestaw danych reprezentujących podpisującego umieszczony w certyfikacie jest prawidłowo dostarczony stronie ufającej;
e) jeżeli w momencie składania podpisu użyty został pseudonim, zostaje to wyraźnie wskazane stronie ufającej;
f) podpis elektroniczny został złożony za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego;
g) integralność podpisanych danych nie została naruszona;
h) wymogi przewidziane w art. 26 (dotyczące zaawansowanego podpisu elektronicznego) rozporządzenia eIDAS zostały spełnione w momencie składania podpisu.

Do realizacji walidacji używa się aplikacji lub usługi walidacji podpisów elektronicznych. Zarówno aplikacja jak i usługa powinna posiadać wiarygodną deklarację producenta lub usługodawcy potwierdzającą zgodność jej działania z art. 32 rozporządzenia eIDAS, który określa wymogi dla walidacji kwalifikowanych podpisów elektronicznych. Dodatkowo warto, aby aplikacja lub usługa zawierała deklarację zgodności oprogramowania z wymaganiami normy ETSI EN 319 102-1, która ustala techniczne warunki walidacji podpisów elektronicznych.

Najwyższy poziom wiarygodności walidacji kwalifikowanego podpisu elektronicznego zapewnia użycie kwalifikowanej usługi walidacji kwalifikowanych podpisów elektronicznych, która jako jedyna korzysta z domniemania prawnego prawidłowej walidacji zgodnie z art. 33 ust. 1 rozporządzenia eIDAS.

Raport walidacji realizowanej zgodnie z normą ETSI EN 319 102-1 może zawierać jeden z trzech głównych statusów wyników walidacji:

- Podpis prawidłowy (TOTAL_PASSED – POZYTYWNIE ZWERYFIKOWANY),
- Podpis nieprawidłowy (TOTAL_FAILED – NEGATYWNIE ZWERYFIKOWANY)
- Podpis częściowo zweryfikowany (INDETERMINATE - NIEOKREŚLONY).

W przypadku statusów „negatywnie zweryfikowany” oraz „nieokreślony” raport powinien zwierać statusy podrzędne wskazujące na okoliczności, z powodu których nie można było pozytywnie zweryfikować kwalifikowanego podpisu elektronicznego.
Załącznik 1 zawiera opis statusów walidacji zgodnie wymogami normy ETSI EN 319 102-1.

4 Podstawowe reguły i rekomendacje dotyczące uznawania ważności podpisów elektronicznych

1. Kwalifikowany Podpis Elektroniczny jest ważny, jeżeli spełnia wymagania ważności zgodne z art. 32 eIDAS w momencie jego złożenia.
2. Kwalifikowany podpis elektroniczny musi być złożony w okresie ważności certyfikatu, gdyż tylko podpis złożony w okresie ważności certyfikatu korzysta z prawnego domniemania, że złożyła go osoba identyfikowana za pomocą tego certyfikatu.
3. Kwalifikowany podpis elektroniczny nie traci ważności, jeżeli był ważnym kwalifikowanym podpisem elektronicznym w momencie złożenia.
4. Kwalifikowany podpis elektroniczny korzysta z prawnego domniemania ważności w okresie ważności certyfikatu kwalifikowanego, za pomocą którego jest weryfikowany.
5. Kwalifikowany podpis elektroniczny, który został oznaczony kwalifikowanym elektronicznym znacznikiem czasu korzysta z prawnego domniemania ważności także po wygaśnięciu kwalifikowanego certyfikatu związanego z tym podpisem.
6. Deklaratywna data złożenia kwalifikowanego podpisu elektronicznego nie wystarcza dla udowodnienia w sposób jednoznaczny jego ważności po wygaśnięciu certyfikatu kwalifikowanego związanego z tym podpisem. Dowody mogą być oparte o dodatkowe informacje, niezależne od samego kwalifikowanego podpisu elektronicznego, w szczególności mogą to być maile, potwierdzenia z systemu obiegu dokumentów oraz niezależne oświadczenia podpisującego lub strony trzeciej.
7. Podstawą uznania kwalifikowanego podpisu elektronicznego za ważny powinna być jego pozytywna walidacja przeprowadzona przez wiarygodną aplikację lub usługę.
8. Korzystając z kwalifikowanej usługi walidacji, w przypadku pozytywnego wyniku, uzyskuje się raport, który stanowi dowód ważności kwalifikowanego podpisu elektronicznego. Dowód ten korzysta z prawnego domniemania prawdziwości.
9. W przypadku uzyskania raportu walidacji o statusie „nieokreślony” można lub trzeba (w zależności od sytuacji) rozważyć możliwość akceptacji podpisu uznając go za ważny kwalifikowany podpis elektroniczny. W każdym takim przypadku może okazać się, że walidowany podpis jest ważnym kwalifikowanym podpisem elektronicznym lub że nim nie jest.
10. Jeżeli akceptacji podlega dokument, w którym wygasł certyfikat do weryfikacji podpisu, a podpis nie był oznaczony kwalifikowanym znacznikiem czasu (status walidacji: OUT_OF_BOUNDS_NO_POE), to można:
    - Opierając się na dacie deklaratywnej (systemowej), zaakceptować dokument ze względu na niską ewentualną szkodę w przypadku ujawnienia dodatkowych dowodów wskazujących na nieważności podpisu lub ze względu na niskie ryzyko zmanipulowania daty deklaratywnej;
    - Zażądać raportu walidacyjnego potwierdzającego ważność podpisu, jeżeli jest to możliwe;
    - Zażądać dodatkowych dowodów złożenia podpisu w okresie ważności certyfikatu;
    - Zażądać oświadczenia przekazującego dokument, że podpis został złożony w okresie ważności certyfikatu;
    - Nie zaakceptować podpisu i dokumentu, jeżeli ryzyko biznesowe jest zbyt wysokie, a okoliczności i uwarunkowania prawne na to pozwalają.
11. W przypadku dokumentu dużej wagi opatrzonego podpisem, dla którego walidacja wskazuje status „nieokreślony” warto uzyskać ekspertyzę wykonaną przez eksperta w oparciu o analizę wszystkich możliwych dowodów i okoliczności, które mogą potwierdzić, uprawdopodobnić lub zakwestionować ważność kwalifikowanego podpisu elektronicznego.

12. Dla uniknięcia sytuacji, w której status poddanego walidacji podpisu będzie „nieokreślony”, strona akceptująca podpis elektroniczny (przyjmująca podpisany dokument) może poinformować stronę podpisującą, że w realizowanych przez siebie procedurach przyjmowane dokumenty (wszystkie lub wskazane) zawierające podpisy elektroniczne powinny umożliwiać poprawną automatyczną walidację podpisu na moment przyjęcia dokumentów i że niespełnienie tego wymagania będzie skutkowało odrzuceniem tych dokumentów.

5 Rekomendacje dotyczące utrzymania prawnej mocy dowodowej ważności kwalifikowanego podpisu elektronicznego w długim okresie.

1. Strona otrzymująca podpisany dokument powinna niezwłocznie przeprowadzić walidację podpisów. W przypadku usługi walidacji kwalifikowanej, raport walidacji stanowi dowód korzystający z prawnego domniemania potwierdzający status badanego podpisu.
2. Jeżeli podpis nie zawiera kwalifikowanego elektronicznego znacznika czasu, wykorzystanie usługi kwalifikowanego znakowania czasem stanowi pierwszy poziom konserwacji podpisu elektronicznego, pozwalający na techniczne i prawne zabezpieczenie jego wiarygodności.
3. W przypadku potrzeby długookresowego podtrzymania mocy dowodowej ważności kwalifikowanego podpisu elektronicznego przy uwzględnieniu również siły kryptograficznej użytych zabezpieczeń integralności dokumentu i struktury podpisu wskazane jest skorzystanie z usługi kwalifikowanej konserwacji kwalifikowanego podpisu elektronicznego.

Załącznik 1. Statusy usługi walidacji

PODPIS NIEPRAWIDŁOWY	
Opis	Informacje dodatkowe załączone w raporcie
• **co najmniej jedna z wartości skrótów podpisanych danych załączonych w procesie składania podpisu nie jest równa odpowiadającej wartości skrótu w weryfikowanym podpisie.**	Proces walidacji podpisu jednoznacznie wskazuje, który z elementów podpisanych danych spowodował negatywny wynik weryfikacji podpisu. Status podrzędny: HASH_FAILURE
• **podpis nie jest zgodny z żadnym ze wspieranych standardów do tego stopnia, że niemożliwym jest przeprowadzenie weryfikacji kryptograficznej podpisu**	Proces walidacji dostarcza wszelkich informacji wskazujących, dlaczego analiza podpisu nie powiodło się. Status podrzędny: FORMAT_FAILURE
• **wartość podpisu nie może zostać zweryfikowana za pomocą klucza publicznego zawartego w certyfikacie podpisującego.**	Proces walidacji zwraca wykorzystany do weryfikacji certyfikat podpisującego. Status podrzędny: SIG_CRYPTO_FAILURE
• **certyfikat podpisującego został odwołany oraz gdy istnieje dowód na to, że moment złożenia podpisu nastąpił po odwołaniu certyfikatu podpisującego**	Proces walidacji wraca następujące informacje: • Ścieżkę zaufania użytą w procesie weryfikacji • Czas oraz jeśli jest dostępny powód odwołania certyfikatu podpisującego • Listę CRL, jeśli jest dostępna, na której certyfikat otrzymał status odwołany • Znacznik czasu z podpisu, z niepodpisanych atrybutów, jeśli są dostępne, które mogą wskazywać na najstarszy moment istnienia złożonego podpisu Status podrzędny: REVOKED
• **data złożenia podpisu jest późniejsza niż data obowiązywania certyfikatu podpisującego**	Proces walidacji zwraca następujące informacje: • Ścieżkę zaufania użytą w procesie weryfikacji Status podrzędny:

	EXPIRED
• **data złożenia podpisu jest wcześniejsza niż data obowiązywania certyfikatu podpisującego**	Status podrzędny: NOT_YET_VALID

PODPIS CZĘŚCIOWO ZWERYFIKOWANY – NIEOKREŚLONY	
Opis	Informacje dodatkowe załączone w raporcie
• **jeden lub więcej atrybutów podpisu nie spełniają wymogów procesu walidacji**	Proces walidacji zwraca następujące informacje: • Ścieżkę zaufania użytą w procesie weryfikacji • Dodatkowe informacje na temat przyczyny Status podrzędny: SIG_CONSTRAINTS_FAILURE
• **ścieżka zaufania wykorzystana w procesie walidacji nie jest zgodna z wymaganiami procesu walidacji związanymi z certyfikatem podpisującego**	Proces walidacji zwraca następujące informacje: • Ścieżkę zaufania użytą w procesie weryfikacji • Dodatkowe informacje na temat przyczyny Status podrzędny: CHAIN_CONSTRAINTS_FAILURE
• **zbiór dostępnych certyfikatów przeznaczonych do weryfikacji ścieżki zaufania zwraca błąd z nieznanego powodu**	Proces walidacji zwraca następujące informacje: • Dodatkowe informacje na temat przyczyny Status podrzędny: CERTIFICATE_CHAIN_GENERAL_FAILURE
• **co najmniej jeden z użytych algorytmów w elementach podpisu lub długość klucza algorytmu jest poniżej wymaganego poziomu bezpieczeństwa:** ○ **element ten wygenerowano w okresie czasu, w którym dany algorytm / klucz był uznawany za bezpieczny (np. gdy data wygenerowania jest znana); oraz** ○ **element ten nie jest chroniony przez wystarczająco silny znacznik czasu zastosowany przed okresem, w którym algorytm / klucz uznawano**	Proces walidacji zwraca następujące informacje: • Identyfikacja elementu (skrót, podpis, certyfikat), który jest wygenerowany przy użyciu algorytmu lub klucza kryptograficznego niespełniającego wymaganego poziomu bezpieczeństwa. Status podrzędny: CRYPTO_CONSTRAINTS_FAILURE

za bezpieczny (na przykład, gdy data wygenerowania jest znana);	
• **certyfikat podpisującego nie może zostać zidentyfikowany.**	Status podrzędny: NO_SIGNING_CERTIFICATE_FOUND
• **dla wskazanego certyfikatu podpisującego nie udało się zbudować ścieżki zaufania.**	Status podrzędny: NO_CERTIFICATE_CHAIN_FOUND
• **certyfikat podpisującego został odwołany w dacie/czasie procesu walidacji. Jednakże algorytm walidacji podpisu nie może stwierdzić czy data złożenia podpisu znajduje się przed czy po dacie odwołania certyfikatu.**	Proces walidacji zwraca następujące informacje: • Ścieżkę zaufania użytą w procesie weryfikacji • Czas oraz jeśli jest dostępny powód odwołania certyfikatu podpisującego Status podrzędny: REVOKED_NO_POE
• **certyfikat podpisującego jest przedawniony lub nie jest jeszcze aktywny w czasie procesu walidacji oraz algorytm walidacji podpisu nie może stwierdzić czy data złożenia podpisu znajduje się w przedziale ważności certyfikatu podpisującego.**	Status podrzędny: OUT_OF_BOUNDS_NO_POE
• **co najmniej jeden z użytych algorytmów w elementach podpisu lub długość klucza algorytmu jest poniżej wymaganego poziomu bezpieczeństwa oraz nie istnieje dowód, że wskazane elementy podpisu zostały wygenerowane w okresie czasu, w którym dany algorytm / klucz był uznawany za bezpieczny**	Proces walidacji zwraca następujące informacje: • Identyfikacja elementu (podpis, certyfikat), który jest wygenerowany przy użyciu algorytmu lub klucza kryptograficznego o długości poniżej wymaganego poziomu bezpieczeństwa. Status podrzędny: CRYPTO_CONSTRAINTS_FAILURE_NO_POE
• **brakuje dowodu umożliwiającego jednoznacznie stwierdzić, że obiekt został podpisany zanim nastąpiło skompromitowanie algorytmu;**	Proces walidacji identyfikuje co najmniej jeden obiekt, dla którego POE jest niedostępne. Proces walidacji powinien dostarczyć dodatkowych informacji o występującym błędzie. Status podrzędny: NO_POE
• **nie wszystkie wymogi mogą zostać spełnione ze względu na brak informacji; jednakże istnieje możliwość ponownego wykonania procesu walidacji z wykorzystaniem dodatkowych informacji dotyczących odwołania**	Status podrzędny: TRY_LATER

certyfikatu, które będą dostępne w późniejszym czasie;	
• **podpisane dane nie mogą zostać pobrane;**	Proces walidacji zwraca następujące informacje: • Identyfikacja miejsca, w którym znajdowały się dane których nie można było pobrać (np. URL) <u>Status podrzędny:</u> SIGNED_DATA_NOT_FOUND
• **wystąpił jakikolwiek inny błąd nie opisany w tej tabeli;**	Proces walidacji zwraca następujące informacje: • Dodatkowe informacje, dlaczego status walidacji został uznany jako nieokreślony <u>Status podrzędny:</u> GENERIC

Ekspert PIIT: