Walidacja podpisów kwalifikowanych

Stosowanie kwalifikowanych podpisów elektronicznych rozwiązuje wiele problemów, z którymi borykano się przy dokumentach papierowych. Nie tylko wzrosła wygoda i szybkość obiegu dokumentów, lecz również wyeliminowano problem fałszerstw, podrabiania podpisów czy antydatowania dokumentów. W teorii użytkownik otrzymując dokument elektroniczny, uruchamia odpowiedni program i uzyskuje informacje, kto podpisał dany dokument, czy podpisy są ważne oraz czy dokument nie został zmodyfikowany po podpisaniu. Niestety, w praktyce sprawa jest bardziej skomplikowana niż na pierwszy rzut oka wygląda.

W rozporządzeniu eIDAS (https://digital-strategy.ec.europa.eu/pl/policies/eidas-regulation) w artykule 18 czytamy: „Podpis elektroniczny lub pieczęć elektroniczna weryfikowane za pomocą certyfikatu wywołują skutki prawne, jeżeli zostały złożone w okresie ważności tego certyfikatu". Ta prosta i oczywista zasada jest jednak trudna do zastosowania w praktyce.

Problem z datą powstania podpisu

Po pierwsze, skąd mamy wiedzieć, kiedy został złożony podpis? Uzyskanie ścisłej informacji jest niemożliwe, gdyż podpis elektroniczny nie zawiera prawnie wiążącej daty jego powstania, a stosowanie znakowania czasem odbywa się już po złożeniu podpisu. Oczywiście różnica w czasie może być nieduża, liczona w sekundach, ale o tym, że są to sekundy, a nie godziny czy nawet dni, wie tylko podpisujący. Na szczęście ten brak precyzji nie ma dużego wpływu na proces weryfikacji.

> *Jeśli bowiem wykażemy, że certyfikat był ważny w momencie oznakowania czasem podpisu, to oznacza również, że był ważny wcześniej (w szczególności w momencie złożenia podpisu), gdyż raz unieważniony certyfikat nie może ponownie stać się ważny.*

A co jeśli podpisujący nie oznakował czasem dokumentu? W takim przypadku dowodem może być fakt wpłynięcia podpisanego dokumentu do odbiorcy. Posiłkując się zapisami kancelaryjnymi czy logami z serwerów poczty, można wykazać, że w danym momencie dokument już istniał. Niestety, ciężar takiego dowodu spoczywa na odbiorcy dokumentu. Z upływem lat, w wyniku kasowania logów, usuwania starej poczty itp. może stawać się on coraz trudniejszy do przeprowadzenia.

Aby temu zaradzić, odbiorca dokumentu może samodzielnie znakować wpływające dokumenty czasem (jeśli nie są oznaczone). Jest to jednak dodatkowy nakład pracy, koszt, a co gorsza znakowanie czasem nie rozwiązuje problemu ostatecznie. Wynika to z faktu, że znakowanie czasem również

Artur Krystosik

dyrektor Działu Rozwoju Produktów w Enigma Systemy Ochrony Informacji Sp. z o.o. Wieloletni pracownik naukowy Instytutu Informatyki Politechniki Warszawskiej. Twórca i współtwórca większości rozwiązań firmy bazujących na technologii PKI. Bierze czynny udział w życiu naukowym w kraju i za granicą. Autor wielu publikacji naukowych. Prywatnie kapitan jachtowy i taternik.

posługuje się certyfikatami, których okres ważności wynosi około 9–11 lat. Po upływie tego czasu znacznik przestaje być ważny, a użytkownik traci kryptograficzny dowód istnienia dokumentu. Wymyślono rozwiązanie i dla tego problemu. Podpisane dokumenty elektroniczne mogą być poddawane procesowi tzw. konserwacji. Polega on na tym, że przed upływem okresu ważności znacznika czasu (ściślej: certyfikatu znacznika czasu) wszystkie oznakowane czasem dokumenty opatrywane są kolejnym znacznikiem czasu, ważnym następne 9-11 lat, co przedłuża okres ważności dowodu istnienia dokumentu. Proces ten musi być powtarzany przez tyle lat, przez ile wymagana jest zdolność do udowodnienia ważności podpisanego dokumentu. Trudno sobie jednak wyobrazić, żeby te wszystkie czynności były wykonywane manualnie. Niezbędny jest do tego sprawny system przechowywania dokumentacji elektronicznej, wyposażony w takie funkcje i mający stały dostęp do dokumentów (a co z archiwami na taśmach?). Jak widać, oddalamy się od prostej aplikacji z jednym klawiszem, a to dopiero początek problemów.

Ważność certyfikatu

Zajmijmy się teraz drugą częścią artykułu 18 rozporządzenia eIDAS, czyli określeniem ważności certyfikatu zakładając, że dysponujemy posiadającą moc dowodową datą istnienia podpisu. Teoretycznie informacja o ważności certyfikatu jest łatwo dostępna. Sam certyfikat posiada zapisany w sobie okres ważności, który łatwo jest porównać z datą istnienia podpisu, a dostawcy usług zaufania publikują informacje o unieważnieniach w postaci list CRL czy usług OCSP[1].

Normy ETSI odnoszące się do weryfikacji podpisu definiują następujące wyniki weryfikacji podpisu:

- **Pozytywny oznaczający w szczególności, że certyfikat użyty do złożenia podpisu był ważny w momencie jego składania.**
- **Negatywny, którego jedną z przyczyn może być fakt nieważności certyfikatu w momencie składania podpisu.**
- **Nieokreślony, którego najczęstszą przyczyną jest brak możliwości określenia ważności certyfikatu w momencie składania podpisu. Wynik ten może ulec zmianie, np. jeśli otrzymamy nowszą niż posiadana listę CRL.**

Powodem braku możliwości określenia ważności certyfikatu zwykle jest brak odpowiednio świeżej informacji o unieważnieniach, czyli listy CRL lub odpowiedzi OCSP. Co to jest odpowiednio świeża informacja? Warunkiem uzyskania ostatecznego wyniku weryfikacji (tj. wyniku pozytywnego lub negatywnego) jest zapewnienie, aby:

1) data wystawienia listy CRL lub odpowiedzi OCSP była późniejsza niż data istnienia podpisu oraz

2) lista CRL/odpowiedź OCSP zawierała unieważnienia z okresu ważności certyfikatu.

Warunek pierwszy wynika z wymagania, że nowo wydana lista CRL nie może zawierać nowo dodanych informacji o unieważnieniach, które byłyby wcześniejsze niż data poprzednio wydanej listy CRL. Innymi słowy na listę CRL nie mogą trafiać unieważnienia antydatowane, czyli takie, które powinny znajdować się już na poprzedniej liście. Dzięki tej zasadzie – dysponując listą CRL późniejszą niż data złożenia podpisu – mamy pewność, że żadna nowa lista CRL nie zmieni statusu ważności certyfikatu na dzień złożenia podpisu, a więc wynik weryfikacji jest ostateczny.

Warunek drugi wynika z faktu, że ogromna większość dostawców usług zaufania na listach CRL publikuje wyłącznie certyfikaty znajdujące się w okresie ważności. Informacje o pozostałych certyfikatach są usuwane z list CRL celem ograniczenia ich rozmiaru.

Jakie ma to wszystko konsekwencje dla procesu weryfikacji? Po wpłynięciu dokumentu użytkownik musi czekać na pojawienie się takiej listy, aby proces weryfikacji dał wynik rozstrzygający. W zależności od dostawcy może to być od kilkunastu minut (CenCert publikuje listy CRL co 20 minut) do nawet kilkunastu godzin. Użytkownik (a właściwie jego oprogramowanie) może również skorzystać z usługi OCSP, o ile taka usługa jest przez danego dostawcę świadczona, co – niestety – nie jest regułą w krajach EU (wszyscy polscy dostawcy usług zaufania taką usługę świadczą, choć nie wszyscy robią to w sposób pozwalający wygodnie i wiarygodnie z niej skorzystać). Spełnienie warunku drugiego jest szczególnie trudne, gdy chcemy dokonać weryfikacji podpisu złożonego wiele lat temu. W tym celu musielibyśmy dysponować listą CRL wydaną w okresie ważności certyfikatu. Ponieważ archiwalne listy CRL nie są udostępniane za pomocą zestandaryzowanego mechanizmu, to ich zdobycie wymaga indywidualnego kontaktu z dostawcą usługi zaufania.

1 OCSP (ang. *Online Certificate Status Protocol*) – standard opisujący protokół komunikacyjny pomiędzy systemem informatycznym odbiorcy usług certyfikacyjnych a serwerem usługowym. Protokół ten określa format i strukturę zapytania (żądania) o status certyfikatu oraz format i strukturę odpowiedzi (tokenu), która zawiera wynik weryfikacji w postaci statusu: „poprawny", „unieważniony", „nieznany".

Rozwiązaniem może być skorzystanie z OCSP, jeśli dany dostawca udostępnia za pomocą tego protokołu informacje o certyfikatach spoza okresu ich ważności, co również nie jest regułą.

Wiarygodność dokumentu

Czy jeśli użytkownik uzyska pozytywny wynik weryfikacji wszystkich podpisów, to może on zaakceptować dokument jako wiarygodny? Niestety, nie. Niektóre formaty danych, takie jak XML czy PDF, pozwalają w jednym dokumencie umieścić dane podpisane i niepodpisane, a także obejmować podpisami różne obszary danych. Można sobie wyobrazić, że jedna strona podpisała umowę, a druga wprowadziła do niej zmiany i podpisała ją ze swojej strony. Graficznie dokument wygląda jakby był podpisany zgodnie przez obie strony, lecz faktycznie tak nie jest.

Format PDF pozwala również na umieszczenie w dokumencie aktywnej zawartości, czyli skryptów uruchamianych podczas prezentacji dokumentu. Zwykle służą one do programowania zachowania formularzy, ale mogą być również używane do zmiany prezentowanych na ekranie treści. Niestety, popularne oprogramowanie do weryfikacji podpisów na ogół nie wykrywa takich zagrożeń, pozostawiając to zadanie aplikacjom przeznaczonym do wizualizacji danego formatu (Acrobat Reader potrafi sygnalizować takie sytuacje, ale nie jest to zbyt czytelne).

Jak widać, dokonanie weryfikacji podpisanego dokumentu wcale nie jest zadaniem łatwym. Zważywszy, że:

- dzisiaj podpisy mogą pochodzić z całej Unii Europejskiej,
- podpisane dokumenty często zawierają rozmaite usterki,
- podpisy czasem nie są w pełni zgodne z normami, z którymi powinny być zgodne,
- programy do weryfikacji podpisów niejawnie przyjmują założenia wpływające na wynik weryfikacji,
- w implementacjach zdarzają się błędy,

widać, z jaką skalą trudności się mierzymy. Praktyka pokazuje, że użytkownicy mają z tym duży problem. Regułą jest stosowanie kilku programów do weryfikacji i porównywanie ich wyników, jak również korzystanie z porad ekspertów w wątpliwych i szczególnie ważnych przypadkach.

Problemami weryfikacji zajmują się również sądy i inne organy. W 2019 r. KIO wydała orzeczenie, w którym wskazała, że opatrzenie oferty podpisem kwalifikowanym wykorzystującym algorytm SHA-1 jest dopuszczalne i nie stanowi przesłanki do odrzucenia oferty. Wspominam o tym dlatego, że stosowanie SHA-1 bywa przyczyną weryfikacji nierozstrzygającej (bezpieczeństwo algorytmu zostało podważone, zademonstrowano dwa różne dokumenty posiadające sensowną i kontrolowaną przez napastnika treść i ten sam skrót SHA-1), ale na gruncie obowiązującego prawa nie można takiego dokumentu odrzucić.[2]

Dużym problemem podczas weryfikacji jest fakt, że podpisy często składane są za pomocą oprogramowania, które nie spełnia norm i standardów albo wymaga specjalnej konfiguracji, o czym przeciętny użytkownik nie ma pojęcia. Przykładowo, domyślnym trybem podpisywania w aplikacji Acrobat Reader (wersja 2023.006.20320) jest tryb niezgodny z eIDAS. Sprawia to, że certyfikat osoby podpisującej nie jest obejmowany podpisem. Jeśli dysponowalibyśmy dwoma certyfikatami wystawionymi na ten sam klucz publiczny, ale zawierającymi różne dane osobowe, to nie dałoby się stwierdzić, kto jest faktycznym autorem dokumentu. Tryb ten można oczywiście zmienić w konfiguracji, tylko kto o tym wie? Problem prawdopodobnie dotyczy ogromnej większości dokumentów podpisanych za pomocą tego oprogramowania.

Sztuka przewidywania

Załóżmy jednak, że użytkownik pokonał wszystkie rafy i używany przez niego program poprawnie zweryfikował podpisy pod dokumentem. Czy to koniec problemów? Odpowiedź na to pytanie wymaga rozważenia dwóch kwestii:

1. Co zrobić, jeśli po upływie pewnego czasu od momentu weryfikacji dokumentu dojdzie do sporu i zajdzie konieczność wykazania, że faktycznie kiedyś uzyskano pozytywny wynik weryfikacji? Narzucającym się rozwiązaniem jest użycie tego samego programu i ponowne wykonanie weryfikacji. Pytanie tylko, czy mimo upływu czasu program na pewno zwróci ten sam wynik? Niestety, mogą zdarzyć się sytuacje, w których wynik weryfikacji będzie inny niż w przeszłości. Przyczyną może być np. wygaśnięcie certyfikatu użytkownika podpisującego dokument, wygaśnięcie certyfikatu znacznika czasu czy

2 Jeśli przyjąć, że algorytm SHA-1 nie gwarantuje cechy, że podpis jest „powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna" (wymaganie z art. 26 pkt d eIDAS), to oznacza, że podpis z SHA-1 nie jest „zaawansowany", a więc nie jest też „kwalifikowany". Jest więc mechanizm prawny na usuwanie z obrotu niebezpiecznych algorytmów, ale w tej konkretnej sprawie KIO zdecydowała inaczej.

unieważnienie certyfikatu użytkownika, jeśli stosowane oprogramowanie przyjmuje czas bieżący jako datę złożenia podpisu, co się często zdarza.

2. W jaki sposób utrwalić wynik weryfikacji, aby miał on własności dowodowe i mógł być przedstawiony w sądzie? Pytanie to jest zasadne zwłaszcza w świetle negatywnej odpowiedzi na pytanie pierwsze.

Oczywiście i te kwestie daje się rozwiązywać, choćby środkami organizacyjnymi, ale jest to kolejna rzecz, o którą należy zadbać, a przecież wydawało się, że wystarczy nacisnąć jeden klawisz.

W celu zweryfikowania dokumentu należy:

- **Zadbać o posiadającą moc dowodową datę istnienia podpisanego dokumentu.**
- **Zadbać o dostęp oprogramowania weryfikującego do odpowiedniej informacji o unieważnieniach (w tym historycznych).**
- **Sprawdzić, czy mimo ważności podpisów dokument nie został zmanipulowany.**
- **Zadbać o utrwalenie wyników weryfikacji tak, aby miały one moc dowodową w przyszłości, lub zapewnić, że dokument będzie się weryfikował w przyszłości, dając identyczny wynik weryfikacji (np. poprzez przekształcenie dokumentu do tzw. postaci archiwalnej oraz okresową konserwację znaczników czasu).**

Warto korzystać z usług walidacji

Wychodząc naprzeciw problemom weryfikacji podpisów elektronicznych, eIDAS zdefiniował kwalifikowaną usługę walidacji dokumentów, która ma zdjąć z użytkownika większość przedstawionych tu problemów. Obecnie w Polsce działają dwaj tacy usługodawcy na terenie państw UE jest ich jeszcze kilku. Korzystanie z usługi walidacji jest bardzo łatwe. Użytkownik przesyła dokument, który chce zwalidować, a dostawca usługi wykonuje wszystkie niezbędne kroki procesu walidacji, zwracając raport na ogół w formacie PDF.

Raport określa m.in.:

- liczbę i rodzaj podpisów oraz pieczęci. Usługi krajowe powinny rozróżniać podpisy/pieczęcie kwalifikowane oraz niekwalifikowane pochodzące od dostawców usług zaufania z krajów UE umieszczonych na listach zaufanych usług TSL, polskie podpisy osobiste wykonane dowodem osobistym oraz podpisy platformy ePUAP;
- status weryfikacji każdego z podpisów (pozytywny, negatywny lub nieokreślony);
- dane osobowe poszczególnych sygnatariuszy;
- szczegóły walidacji poszczególnych podpisów, a jeśli wynik walidacji jest inny niż pozytywny – listę przyczyn takiego stanu.

W zależności od dostawcy usługi taki raport może zawierać także ostrzeżenia o możliwych manipulacjach treścią dokumentu (aktywna zawartość, obszary niepodpisane czy podpisy obejmujące różne obszary dokumentu).

Raporty opatrywane są pieczęcią elektroniczną usługi walidacji i z mocy eIDAS mają bezpośrednią wartość dowodową. Przechowanie raportu wraz z dokumentem eliminuje potrzebę ponownej weryfikacji dokumentu w przyszłości. Odpadają więc problemy przekształcania dokumentów do postaci archiwalnej i konserwacji podpisów. Przy czym należy pamiętać, że konserwując podpisy pod dokumentem gwarantujemy, że dokument będzie w przyszłości bez problemu walidowany. Natomiast przechowując raport gwarantujemy zachowanie dowodu dołożenia należytej staranności i uzyskania właściwego wyniku walidacji, czego nie daje nam sama usługa konserwacji.

Wysłanie dokumentu do walidacji nie oznacza, że dokument musi być przesyłany na serwery usługodawcy. Po stronie klienta może być zainstalowana tzw. bramka, do której za pośrednictwem aplikacji webowej użytkownicy przekazują dokumenty. Bramka pobiera z dokumentu podpisy, oblicza wymagane skróty z danych i przesyła je do serwerów usługodawcy, gwarantując, że żadne dane należące do klienta nie opuszczają infrastruktury klienta. Na podstawie przesłanych danych realizowana jest walidacja dokumentu. Służy do tego dedykowane oprogramowanie walidacyjne, którego zadaniem jest realizacja wszystkich kroków niezbędnych do uzyskania rozstrzygającego wyniku walidacji. Serwery usługi automatycznie pobierają niezbędne informacje o unieważnieniach. W przypadku braku wystarczająco świeżej informacji aktywnie oczekują na jej dostępność, co uwalnia użytkownika od konieczności ponawiania procesu walidacji. Dla walidacji dokumentów historycznych oprogramowanie może sięgać do archiwum gromadzącego listy CRL pochodzące o dostawców usług zaufania całej Unii Europejskiej. Usługi walidacji są dostępne również w formie uproszczonej, która nie wymaga instalacji po stronie klienta żadnego oprogramowania. W takim przypadku wymagane jest przesyłanie całych dokumentów na serwery usługodawcy. Zwykle odbywa się to poprzez stronę www.

Czy usługi walidacji to panaceum na wszystkie problemy walidacji dokumentów? Oczywiście nie, ale są one znacznym ułatwieniem w codziennej pracy z dokumentami elektronicznymi.