napędy i sterowanie

miesięcznik naukowo-techniczny

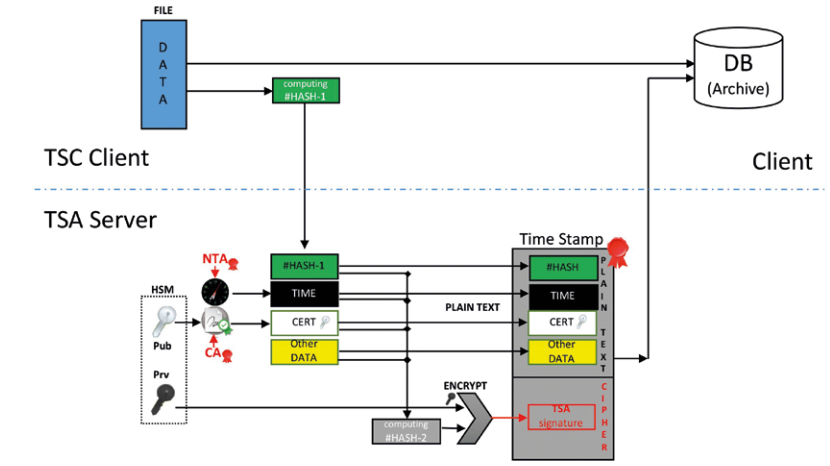
Nr 10 (210)
Rok XVIII
Październik 2016
ISSN 1507-7764
Indeks 36018X
Cena: 10,80 zł
(w tym 8% VAT)

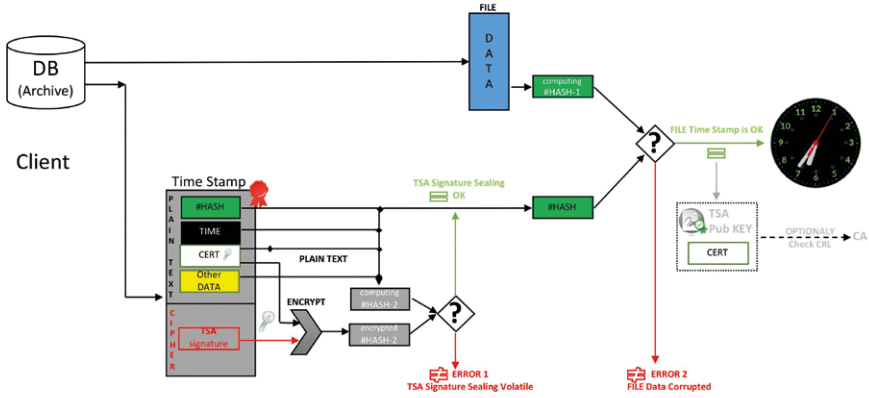
napędy ● automatyka przemysłowa ● energoelektronika ● aparatura kontrolno-pomiarowa ● mechatronika ● systemy zasilające
układy zabezpieczeń ● hydraulika ● pneumatyka ● robotyka ● systemy transportowe ● utrzymanie ruchu

Jak działa wiarygodne znakowanie czasem

Proces wiarygodnego znakowania czasem danych (np. raportów systemowych LOG) zaczyna się po stronie klienta, który tworzy na ich podstawie odcisk palca (ang. *fingerprint*), czyli unikalną sekwencję identyfikującą dane, tzw. skrót HASH-1. Czynność liczenia skrótu wykonuje się przy użyciu jednej z wielu dostępnych matematycznych funkcji; np. SHA-2 (SHA-256) lub SHA-1. Od tej pory jakakolwiek zmiana, nawet pojedynczego bitu informacji w oryginale znakowanych czasem danych, będzie wymagać rozpoczęcia operacji od nowa, dlatego do czasu zwrotnego odbioru pełnego znacznika czasu z serwera TSA (ang. *Time Stamping Authority*) oryginał danych powinien pozostawać w nienaruszonej formie. Skrót HASH-1 rozszerzony o pola dodatkowych informacji wysyłany jest przez sieć do TSA. Liczy on około 500 bajtów.

Po odebraniu żądania TSA uzupełnia odebrane dane, dodając: informacje o czasie i dacie (TIME), certyfikat z kluczem publicznym TSA (CERT) oraz nowy skrót (HASH-2) tak przygotowanej odpowiedzi. Całość podpisuje swoim kluczem prywatnym i odsyła do klienta. Odpowiedź liczy około 1500 bajtów i jest zapisywana przez klienta w postaci oddzielnego pliku. Z wyjątkiem plików PDF, wszystkie pozostałe formaty plików produkują wiarygodny znacznik czasu w formie oddzielnego RFC3161. Format PDF jako jedyny posiada specjalne wewnętrzne deskryptory zgodne z RFC3161, pozwalające w bardzo elegancki sposób przechowywać w pojedynczym pliku zarówno oryginał dokumentu, jak i znacznik czasu.





Weryfikacja wiarygodności znacznika czasu

Proces weryfikacji może być wykonany w dowolnym momencie również po wielu latach i do weryfikacji nie jest potrzebny serwer TSA. Aby zweryfikować poprawność, potrzebny jest oryginał dokumentu oraz plik znacznika czasu zawierający certyfikat z kluczem publicznym TSA. Proces weryfikacji zawiera badanie tożsamości TSA (autentykacja) i spójności danych znacznika czasu (integralność). W tym celu używany jest klucz publiczny TSA zawarty w certyfikacie (CERT) przesłanego znacznika. Niezależnie klient ponownie sprawdza i liczy skrót HASH2. Jeżeli jest on zgodny (z przesłanym wcześniej HASH-2 przesłanego załącznika), to autentykacja TSA i integralność danych znacznika są zachowane i wiarygodne. W przeciwnym wypadku zwracany jest błąd.

Na koniec pozostaje konieczność sprawdzenia, czy weryfikowany znacznik odwołuje się do oryginału danych (pliku), co jest zasadniczo podmiotem procesu weryfikacji. Dlatego klient ponownie liczy skrót HASH-1 na podstawie zarchiwizowanej kopii oryginału danych i porównuje wynik z pobranym ze znacznika skrótem HASH-1, jaki sam liczył, przygotowując zapytanie do TSA. Dopiero ta zgodność gwarantuje, że znacznik i dokument wzajemnie korespondują ze sobą. W ten sposób uzyskuje się pełną weryfikację spełniających właściwości PKI i cechy prawidłowej: autentykacji TSA, integralności znacznika, oryginalności dokumentu i znacznika oraz niezaprzeczalności wiarygodności, że dokument istniał w danej formie w określonym wiarygodnie przez znacznik czasu momencie historii. ■

Wiarygodne znakowanie czasem systemowych raportów LOG w przemyśle

Powszechność dostępu do bibliotek, takich jak OpenSSL, oraz łatwość generacji kluczy prywatny/publiczny z użyciem przeglądarek internetowych dostarcza nowe możliwości wykorzystania infrastruktury klucza publicznego PKI w przemyśle, jakie daje cyfrowe podpisywanie danych i autentykacja ich nadawcy. Funkcjonalność ta w połączeniu z serwerami czasu tworzy nową grupę usług tzw. wiarygodnego oznaczania czasem zdarzeń w przemyśle, które trwale kojarzy zdarzenia, alarmy błędy, itp. z datą i godziną ich wystąpienia.

Znaczenie synchronizacji w elektronice i przemyśle

Czas i częstotliwość są wszechobecne w przemyśle, a ich synchronizacja wymagana jest do prawidłowej pracy większości urządzeń, szczególnie tych sterowanych komputerami. Mimo tak dużego znaczenia zagadnienie nie należy do pierwszoplanowych tematów cieszących się popularnością dyskusji, mimo że skutki błędów synchronizacji są co roku powodem milionowych strat w sektorach energetycznym czy telekomunikacji. Zagadnienie pozostaje nie mniej ważne dla automatyki przemysłowej, ale również w sektorze finansowym i administracji publicznej. W listopadzie 2015 r. komisja finansów przy giełdzie w Londynie ukarała karą w wysokości 150 mln USD jeden z wiodących banków inwestycyjnych za mikrosekundowe niedozwolone wyprzedzanie w czasie zautomatyzowanych komputerowo operacji giełdowych HFT, co zdaniem komisji wpływało na wartość notowań londyńskiego parkietu i nosiło znamię nieuczciwej konkurencji. Równie dotkliwe straty wywołują błędy synchronizacji fazy dystrybuowanego sieciami energetycznymi napięcia, zwłaszcza w końcowych etapach, gdzie obniża się jego wielkość. Synchronizacja w telekomunikacji decyduje o utrzymaniu właściwych szerokości pasm transmisyjnych łączności bezprzewodowej i w światłowodach. Niedostateczna synchronizacja to gorsza słyszalność, częstsze zrywanie połączeń, echo i przesłuchy, a więc mniejsze wpływy sprzedaży do operatorów świadczących usługi. To również spowolnienie transmisji danych na łączach internetowych będące powodem częstych reklamacji. W najbliższym otoczeniu również komputery wymagają prawidłowego czasu i daty. Obsługując zdarzenia i realizując powierzone im funkcje, zapisują informacje o przebiegu pracy systemów w specjalnych plikach raportów LOG, te zaś są załącznikami sprawozdań raportów audytorskich. Z zapisów takich możemy ustalać dokładny czas i miejsce wystąpienia błędu, alarmu czy sytuacji awaryjnej.

Tam, gdzie konsekwencje mogą mieć wymiar finansowy, dotyczą kwestii bezpieczeństwa pracy ludzi lub gdy automatyzacja realizuje funkcje objęte rygorem prawa, wiarygodne znakowanie czasem jest nie mniej ważne od prawidłowej synchronizacji, ponieważ dostarcza dodatkowe niespotykane wcześniej właściwości, takie jak:

- **niezaprzeczalność** zdarzenia opisanego w systemowym dzienniku zdarzeń LOG;
- **autentykacja** serwera czasu znakującego wiarygodnie czasem;
- **oryginalność i integralność** tak oznaczonych wiarygodnym czasem informacji o zdarzeniach.

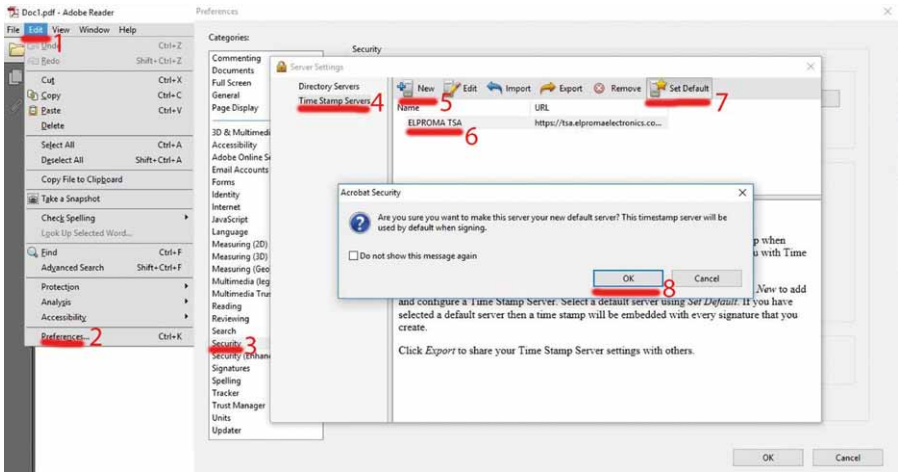
Wiarygodne znakowanie czasem RFC3161 może być wykonywane na dowolnych typach danych, najwygodniej w formie pliku o dowolnym formacie i długości. Również coraz popularniejsza dziś w przemyśle i telemetrii/M2M technologia CLOUD coraz częściej odwołuje się do wiarygodnego oznaczania czasem przesyłanych za jej pośrednictwem informacji.

Znakowanie wiarygodnym czasem nie ogranicza się wyłącznie do zastosowań w przemyśle. Można go używać również do celów indywidualnych i domowych z wykorzystaniem np. Adobe Acrobat Readera. Zawarte w dokumencie PDF informacje i multimedia (zdjęcia) mogą w przyszłości uprościć złożone procedury ochrony patentowej czy ochrony własności intelektualnej. Być może w przyszłości każdy telefon komórkowy będzie pozwalał nie tylko rejestrować dźwięk, kręcić film, robić zdjęcia, ale dzięki wiarygodnemu znakowaniu czasem będziemy mogli w prosty automatyczny sposób zagwarantować sobie pierwszeństwo praw autorskich, własność intelektualną – potwierdzić istnienie dokumentów, co znane jest dziś jako usługa daty pewnej świadczona przez notariuszy. ■

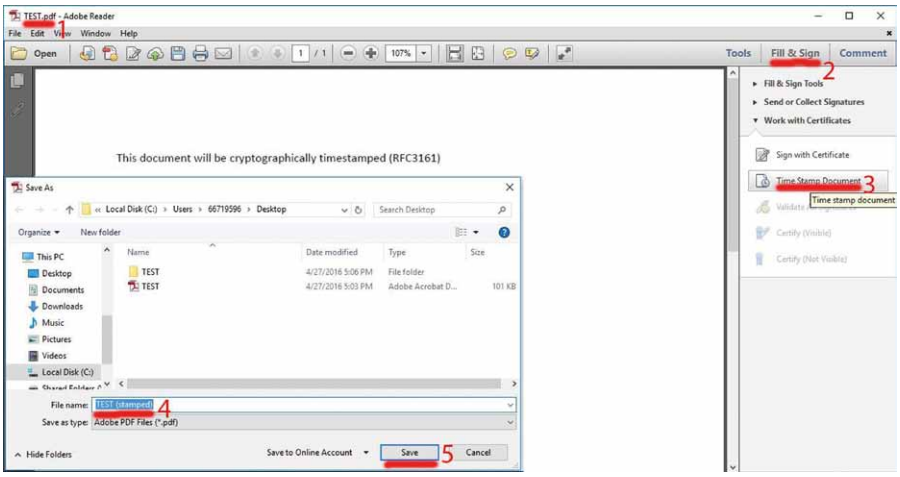
Elektroniczny notariat – przykład nieodpłatnego znakowania wiarygodnym czasem dokumentów PDF

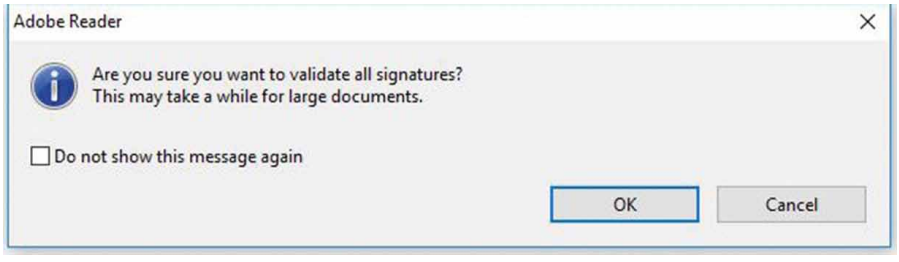
Ze stron firmy Adobe pobierz i zainstaluj najnowszą wersję nieodpłatnej wersji oprogramowania Acrobat Reader.

1. Uruchom program Acrobat Reader i przejdź do menu *Edit*.
2. Wybierz opcję *Preferences*.
3. Przejdź do kategorii *Security*.
4. Wybierz opcje *Time Stamp Servers*.
5. Kliknij *New*, aby dodać nowy adres serwera TSA o adresie: https://tsa.elpromaelectronics.com/get.aspx.
6. Nadaj serwerowi przyjazną dla siebie nazwę i opis.
7. Oznacz serwer jako domyślny.
8. Zatwierdź zmiany, klikając *OK* i zamknij wszystkie okna.



Adding the Time Stamp Server on Adobe XI for Windows 10





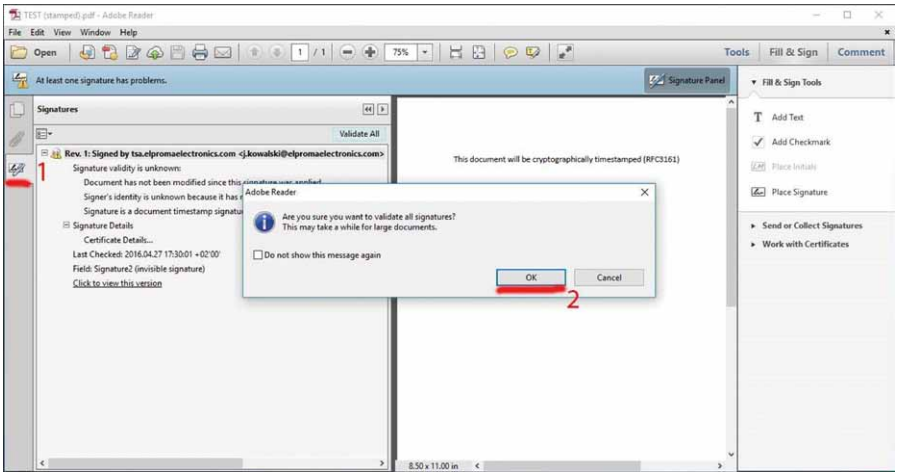
Stemplowanie dokumentów PDF

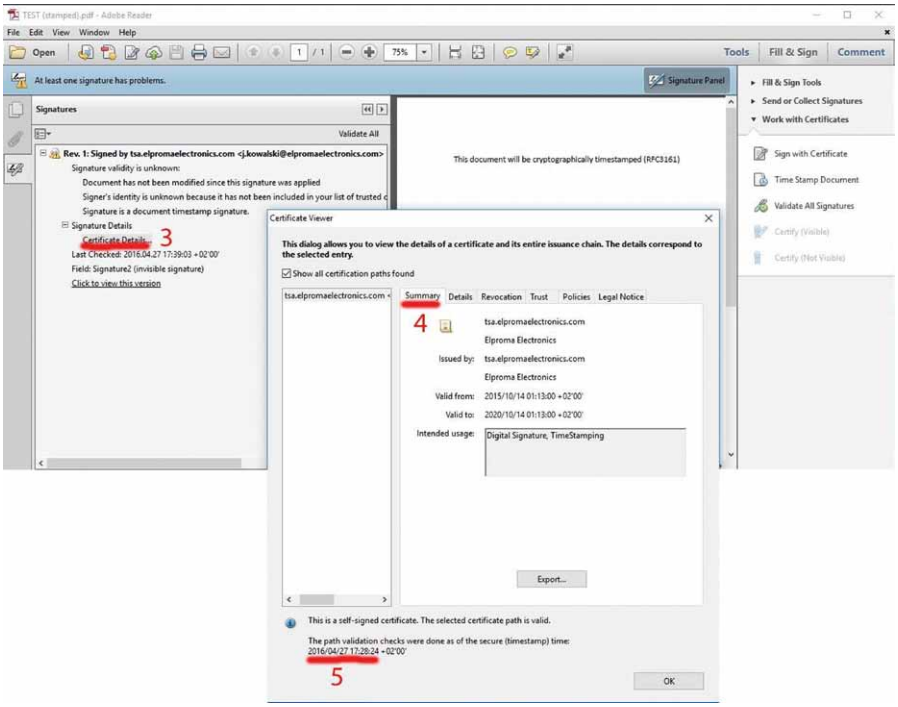
1. Uruchom ponownie Adobe Acrobat z dokumentem PDF, który chcesz oznakować.
2. Wybierz *Fill & Sign* menu z prawej strony ekranu.
3. Rozwiń kategorię *Work with Certificates* i wybierz *Time Stamp Document*.
4. Zmieniając nazwę zapisywanego pliku PDF, możesz zachować niezmienioną wersję źródłową.
5. Wybierz *Save*, aby przeprowadzić operację znakowania i zapisu dokumentu PDF zawierającego również znacznik czasu.

Podczas stemplowania lub późniejszej weryfikacji możesz zostać poproszony o akceptację zaufania do certyfikatu TSA. Wyraź na to zgodę.

Weryfikacja oznakowanego wiarygodnym czasem dokumentu PDF

1. Uruchom ponownie Adobe Acrobat z oznakowanym dokumentem PDF, który chcesz zweryfikować, oraz wybierz z lewej strony opcje obsługi certyfikatów *Signatures*.
2. Jeżeli nie potwierdziłeś wcześniej zgody na użycie niezaufanego certyfikatu TSA, uczyń to teraz.
3. Wybierz *Signature Details*.
4. Kliknij *Certificate Sumary*.
5. Punkt ten jest informacją potwierdzającą, że twój PDF został prawidłowo oznakowany.





Aplikacje i zastosowania wiarygodnego znakowania czasem RFC3161

Skanując dowolne dokumenty, w tym zdjęcia, schematy, odręcznie wykonane notatki i umieszczając je w dokumencie PDF, uzyskujemy możliwość oznaczenia ich wiarygodnym czasem pochodnym z międzynarodowych instytutów metrologii, które od niedawna coraz częściej udostępniają publicznie TSA. Większość programów biurowych, włączając Microsoft Office (Word, Excel, Power Point), również pozwala bezpośrednio zapisywać w formacie PDF. Dla każdej platformy systemowej istnieje też możliwość tworzenia plików PDF za pośrednictwem wirtualnych drukarek konwertujących strumień druku.

Tym samym możemy w precedensowych i spornych kwestiach przedstawić jako argument istnienie dokumentu i posiadanego wiarygodnego znacznika czasu świadczącego o istnieniu dokumentu w określonym momencie historii, wskazując nasze prawo pierwszeństwa. Może to mieć duże zastosowanie w usprawnieniu trudnych dziś procedur patentowych i ochrony praw autorskich. Możliwość znakowania dowolnego pliku (również filmów, dźwięku itp.) daje bardzo uniwersalne, mobilne narzędzie wsparcia.

Być może w niedalekiej przyszłości wizyty u notariuszy, oferujących usługę tzw. daty pewnej, nie będą aż tak potrzebne. Zaoszczędzony w ten sposób czas można będzie wykorzystać na inne zadania lub po prostu na wypoczynek, a zaoszczędzone u notariusza pieniądze można będzie wydać na inne cele.

Jednak zanim tak się stanie, niezbędne jest unormowanie szeregu przepisów prawnych. Prace nad tym są prowadzone w krajach UE. W Polsce instytucją odpowiedzialną jest Główny Urząd Miar RP.