Michał Tabor, Lucjan Hanzlik

Zapewnienie wiarygodności dokumentów elektronicznych funkcjonujących w świecie papieru

Ekonomiczne Problemy Usług nr 106, 89-100

2013

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 781 EKONOMICZNE PROBLEMY USŁUG NR 106 2013

MICHAŁ TABOR
Trusted Information Consulting
LUCJAN HANZLIK
Politechnika Wrocławska

ZAPEWNIENIE WIARYGODNOŚCI DOKUMENTÓW ELEKTRONICZNYCH FUNKCJONUJĄCYCH W ŚWIECIE PAPIERU

Wprowadzenie

Informatyzacja gospodarki i administracji publicznej nie następuje całościowo, a jedynie wydzielone procesy i usługi przechodzą na postać elektroniczną. Wszędzie tam, gdzie dochodzi do styku świata papierowego z elektronicznym, mamy bardzo duży problem braku jednoczesnego współistnienia tych obu mediów. W takich sytuacjach zazwyczaj przetwarzanie przechodzi całkowicie na metody historycznie ugruntowanej biurokracji papierowej. Faktem jest także to, że nie da się wszystkich procesów zmienić na elektroniczne i nie da się przekonać wszystkich ludzi do tego, żeby przeszli wyłącznie na procesy elektroniczne. Wieloletnie przyzwyczajenie do dokumentów papierowych, utarte sposoby ich zabezpieczania i przechowywania, a także znane wszystkim ryzyko związane z dokumentem papierowym są i pozostaną powodem stosowania papieru jako nośnika dokumentów.

Małe firmy i osoby prywatne posługują się na co dzień papierem i będą się nim posługiwały dla większości obsługiwanych przez siebie procesów. Ilustracją powyższego może być fakt, że większość osób wysyłających PIT

drogą elektroniczną zarówno samą deklarację, jak i otrzymane urzędowe potwierdzenie odbioru drukuje – bo w razie postępowania skarbowego jest to wystarczający dowód wywiązania się z obowiązku fiskalnego. Dokument papierowy składowany w segregatorze nie utraci swojej integralności w wyniku awarii dysku. Może być obsłużony mimo braku dostępności komputera, a nowe rozwiązania i wymiana sprzętu nie ingerują w jego dostępność i wiarygodność. Wszelkie metody zabezpieczeń przed utratą dokumentów elektronicznych dla osoby prywatnej będą znacznie droższe niż trzymanie postaci papierowej w segregatorze.

Procesy w administracji publicznej są na bieżąco informatyzowane, łatwiej jest uzyskać dokumenty drogą elektroniczną – bo ich obsługa jest tańsza i szybsza. Niestety, dokumenty elektroniczne mają tę wadę, że powinny być przechowywane i przetwarzane elektronicznie. Co zrobić z dokumentami, które otrzymaliśmy elektronicznie i powinny być przechowywane w postaci elektronicznej – ponieważ wydrukowane na papierze tracą swoje właściwości dowodowe? Czy to oznacza, że należy zaprzestać informatyzacji administracji publicznej i pozostawić realizację procedur i procesów tylko w postaci papierowej, bo te są zrozumiałe dla zwykłych ludzi? Ależ nie – droga musi być całkiem inna i o tym będzie w dalszej części artykułu.

1. Cel

Celem pomysłu przedstawionego w niniejszym referacie jest rozwiązanie umożliwiające każdemu obywatelowi wolny wybór sposobu przechowywania dokumentu elektronicznego w domu. Użytkownik powinien wybrać sposób wygodniejszy i bezpieczniejszy dla niego – wydrukowany lub elektroniczny. Warunkiem koniecznym takiego rozwiązania jest to, aby wydrukowany dokument mógł być uznawany za równoważny z oryginałem elektronicznym, weryfikacja papierowego dokumentu była łatwa i nie wymagała specjalistycznego sprzętu, uzyskanie zaś pierwotnej postaci elektronicznej wymagało jedynie dostępu do Internetu.

Realizacja powyżej postawionych wymagań może zostać zrealizowana w oparciu o znane i dostępne technologie, a tego typu rozwiązania są już dziś używane i całkiem nieźle działają. Są nimi karty pokładowe linii lotniczych,

wydruki z Centralnej Ewidencji i Informacji Działalności Gospodarczej[1], odpisy z Krajowego Rejestru Sądowego[2]. Wymienione przykłady są rozwiązaniami dla pojedynczego problemu i procesu.

Budowanie takich wyspowych rozwiązań dla pojedynczych systemów nie rozwiąże problemu całościowo i będzie powodem nowych problemów dotykających bezpieczeństwa i interoperacyjności, dlatego w niniejszym referacie zostanie wskazane, jak zrealizować cel globalnie, dostarczając rozwiązania mającego zastosowanie do wielu procesów i dla wielu użytkowników. Takie rozwiązanie musi być ogólnie dostępne, uznane prawnie, interoperacyjne i gwarantujące bezpieczeństwo wszystkim procesom, w których elektroniczny lub wydrukowany dokument elektroniczny będzie uczestniczył.

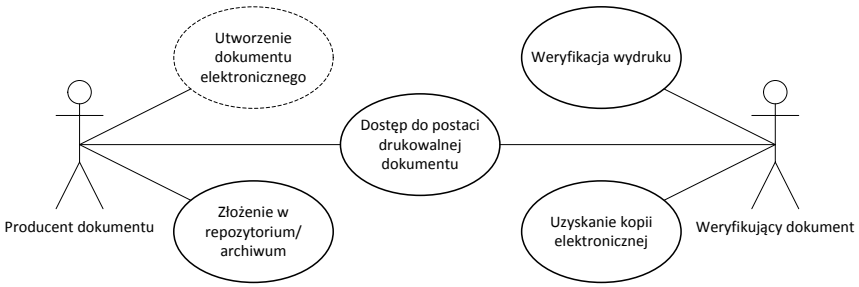
Podstawą dziś dostępnych odpisów z CEIDG, KRS, czyli dokumentów drukowalnych na papierze, nie jest dokument elektroniczny jako taki – te dokumenty powstały, żeby być wydrukowane i istnieć w postaci papierowej jako w podstawowej formie. Dlatego też nie istnieje proste przełożenie ich na dokument elektroniczny przetwarzany jako taki w innych systemach. Wobec powyższego należy stwierdzić, że dokumenty PDF udostępniane przez CEIDG czy KRS są dokumentami papierowymi tylko udostępnianymi przez kanał elektroniczny celem ich wydrukowania. To powoduje, że wymienione rozwiązania nie spełniają celu, jakim jest współistnienie dokumentu elektronicznego i papierowego oraz możliwość łatwej konwersji między tymi postaciami.

Wadą rozwiązań przypisanych do pojedynczego systemu jest fakt, że ich wartość dowodowa jest związana tylko z systemem, w którym powstały, i w przypadku zaprzestania jego działania stają się bezużyteczne. Czyli jeżeli zapis pierwotny w systemie zostanie usunięty – wskazanych dokumentów papierowych nie da się ani zweryfikować, ani uzyskać informacji o zapisach elektronicznych wskazanego dokumentu. Wobec powyższego w rozwiązaniu systemowym konieczne jest rozłączenie funkcji związanych z tworzeniem dokumentu w pierwotnym środowisku od funkcji jego zabezpieczenia postaci archiwalnej, wizualizacji i weryfikacji. Powyższe funkcje powinny być

[1] Informacje na stronie Centralnej Ewidencji i Informacji o Działalności Gospodarczej, http://www.ceidg.gov.pl.

[2] Informacje na stronie Ministerstwa Sprawiedliwości dotyczące Krajowego Rejestru Sądowego, http://ems.ms.gov.pl.

realizowane przez zaufaną trzecią stronę, niezależną od instytucji i systemu, w którym dokument elektroniczny został utworzony. Cztery podstawowe funkcje takiego podmiotu zostały zaprezentowane na rysunku 1.



Rys. 1. Podstawowe funkcje zaufanej trzeciej strony SmartPaper
Źródło: opracowanie własne.

2. Rozwiązanie

Osiągnięcie celu, jakim jest uzyskanie równorzędnie funkcjonujących papierowych odpowiedników dokumentów elektronicznych, wymaga zapewnienia prawnego i technicznego rozwiązania bazującego na repozytoriach dokumentów elektronicznych świadczonych jako usługa zaufanej trzeciej strony. Usługa taka będzie posiadała podstawy prawne w momencie wejścia w życie rozporządzenia Komisji i Parlamentu Unii Europejskiej w sprawie identyfikacji i usług zaufania[3] i będzie mogła być świadczona jako usługa akredytowana lub kwalifikowana. Na potrzeby niniejszego referatu w dalszej części system zaufanej trzeciej strony będzie nazywany archiwum SmartPaper.

Schemat działania takiej usługi jest następujący:

1. Dokument elektroniczny, przygotowany przez jego producenta (np. urząd wydający zaświadczenie) i zabezpieczony podpisem elektronicznym (lub

[3] *Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market*, COM(2012) 238 final, Brussels, 4.6.2012.

pieczęcią elektroniczną), przekazywany jest do repozytorium dokumentów elektronicznych stanowiącego podstawowy element archiwum SmartPaper.

2. Archiwum SmartPaper zapewnia weryfikację poświadczeń (podpisów) elektronicznych i zabezpiecza dane z tej weryfikacji, tak aby wartość dowodowa dokumentu elektronicznego mogła być zapewniona długoterminowo.

3. Archiwum SmartPaper przydziela umieszczonemu w nim dokumentowi unikatowy identyfikator, który będzie podstawowym mechanizmem dostępu do dokumentów znajdujących się w archiwum. Warunki dla mechanizmu kryptograficznego utworzenia identyfikatora opisano w dalszej części artykułu.

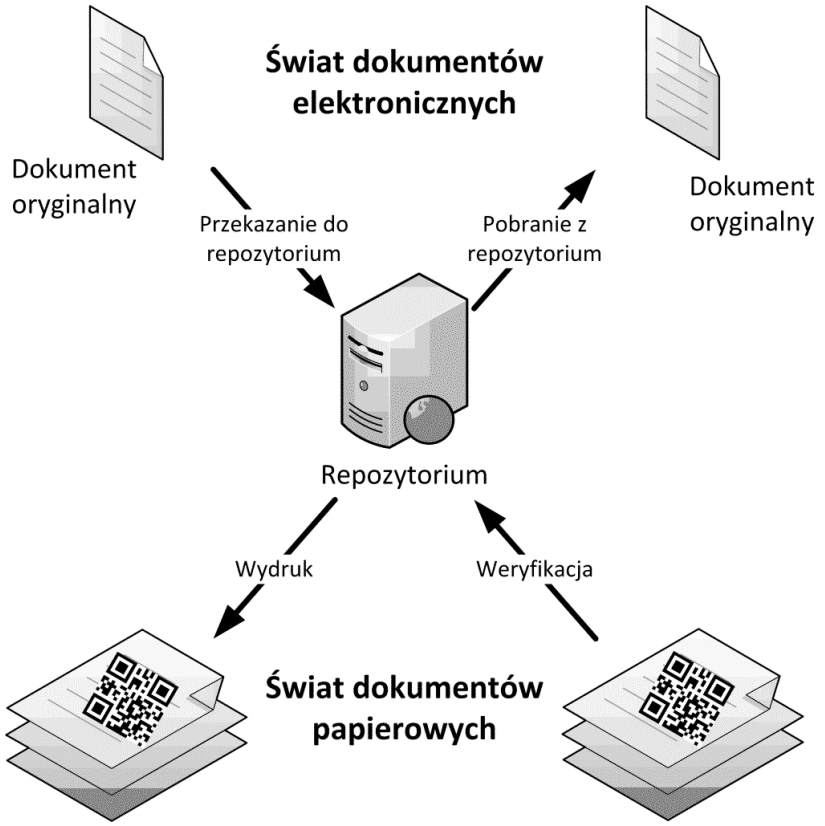
4. Archiwum SmartPaper przygotowuje postać wizualną – zamknięty plik drukowalny np. PDF. Wizualna postać zawiera przydzielony identyfikator (np. w formie kodu 2D). Plik PDF jest umieszczany w repozytorium, a jego poufność jest chroniona koniecznością znajomości identyfikatora.

5. Archiwum SmartPaper zapewnia integralność dokumentów w nim umieszczonych zarówno przez mechanizmy podpisu, jak i mechanizmy tworzenia łańcucha kolejno w nim umieszczanych elementów.

6. Na podstawie identyfikatora repozytorium udostępnia zawartość dokumentu zawierającego postać wizualną, jak i pierwotnie składowany dokument elektroniczny wraz z danymi zapewniającymi jego długoterminową wartość dowodową.

7. Archiwum SmartPaper w trybie ciągłym zapewnia mechanizmy utrzymania wartości dowodowej dokumentów w nim składowanych.

Powyżej opisane funkcje archiwum SmartPaper dostarczają funkcji umożliwiających równoległe funkcjonowanie dokumentu elektronicznego w postaci elektronicznej i papierowej (rys. 2).



Rys. 2. Konwersja pomiędzy postacią elektroniczną i papierową
Źródło: opracowanie własne.

Archiwa SmartPaper mogą być usługami zarówno publicznymi, jak i komercyjnymi oferowanymi przez prywatne firmy. Założeniem musi być jednak fakt, że Archiwum SmartPaper jako usługa zaufana jest realizowana zawsze przez zaufaną stronę trzecią – czyli nie może być świadczona na własne potrzeby ani przez producenta dokumentu, ani przez jego adresata.

Usługi publiczne archiwum SmartPaper powinny być udostępniane przez takie systemy, jak ePUAP, na potrzeby administracji publicznej, i Centrum Systemów Informacyjnych Ochrony Zdrowia, na potrzeby systemów medycznych. Osoby fizyczne i przedsiębiorstwa mogą otrzymane i wymieniane z innymi dokumenty elektroniczne archiwizować w chmurze, bazując na usłu-

gach komercyjnych udostępnianych przez akredytowane podmioty zgodnie z wymaganiami rozporządzenia[4]. Ważną rolę może odgrywać także operator pocztowy, doręczając dokumenty elektroniczne listownie, przy jednoczesnym zapewnieniu usługi zaufania w postaci archiwum SmartPaper. Należy wskazać na to, że dokument elektroniczny może być składowany w więcej niż jednym archiwum, np. zarówno na ePUAP, jak i w archiwum komercyjnym.

Takie rozwiązanie daje potencjał, aby każdy dokument powstający w jednostce administracji publicznej mógł być utworzony jako elektroniczny, doręczony elektronicznie, a następnie funkcjonował elektronicznie lub papierowo – w zależności od procesu, w którym będzie wykorzystany. Bardzo ważną rolę może odgrywać system ePUAP, dając możliwość przechowywania i udostępniania dowolnych dokumentów administracji publicznej powstałych elektronicznie. Takie podejście daje możliwość równoległego funkcjonowania administracji elektronicznej i papierowej, jednocześnie wspiera rozwój elektronizacji usług, ponieważ likwiduje barierę, jaką dotychczas był brak możliwości autoryzowanej i taniej konwersji dokumentu elektronicznego na papierowy. Dokument papierowy stanowi nośnik treści, umożliwia przetwarzanie informacji papierowej, a weryfikacja zaufania oraz autentyczności dokumentu papierowego jest wspomagana mechanizmami elektronicznego repozytorium.

3. Identyfikator

Istniejące techniki kryptograficzne, stosowane także dla podpisu elektronicznego, dają możliwość takiego skonstruowania identyfikatorów dokumentów utrzymywanych w repozytorium, które poprzez swoją unikatowość i złożoność zapewniają, że nikt kto, nie ma dostępu do treści papierowej dokumentu, nie jest w stanie uzyskać dostępu do treści elektronicznej. Z drugiej strony taki identyfikator stanowi zabezpieczenie pozwalające na weryfikację swojej autentyczności nawet w sytuacji, gdyby repozytorium było niedostępne. Naturalnym mechanizmem wizualizowania identyfikatora na dokumencie jest umieszczenie go w formie kodu 2D wskazującego miejsce w repozytorium. Identyfikatory dokumentów mają następujące cechy:

[4] *Ibidem*, s. 3.

- Są unikatowe w ramach całego archiwum SmartPaper. Cecha ta zapewnia, że pod danym identyfikatorem znajdzie się tylko jeden dokument, dla którego utworzono postać wizualną.
- Utworzenie poprawnego identyfikatora dokumentu poza archiwum powinno być praktycznie niemożliwe. Cecha ta gwarantuje, że tylko osoba posiadająca poprawny identyfikator będzie w stanie uzyskać dostęp do dokumentu elektronicznego i weryfikacji autentyczności dokumentu wizualizowanego. Cecha gwarantuje ochronę danych osobowych, zapewniając, że tylko osoba posiadająca te dane osobowe w postaci papierowej lub zwizualizowanej będzie mogła dostać się do ich postaci elektronicznej.
- Weryfikacja autentyczności identyfikatora na podstawie publicznie dostępnego algorytmu jest możliwa poza archiwum. Cecha ta w połączeniu z mechanizmem tworzenia identyfikatorów zapewnia mechanizmy weryfikacji autentyczności dokumentów zwizualizowanych, nawet gdy archiwum nie jest dostępne. Stanowi to dodatkowy materiał dowodowy w przypadku katastrofy, jaką mogłoby być zniszczenie archiwum i wszystkich jego kopii archiwalnych.

Identyfikator razem z dokumentem elektronicznym i wizualizacją, do których został przypisany, powinien być chroniony pod względem integralności. Dzięki temu niezależnie od miejsca i momentu zapytania pytający uzyska zawsze ten sam dokument i tę samą jego wizualizację. Dodatkowo w sprawach o szczególnej wadze dowodowej identyfikator może zawierać dane zależne od treści dokumentu elektronicznego, do którego został przypisany (np. numer księgi wieczystej). W zależności od rozwiązania repozytorium i ryzyka związanego z ochroną poufności danych w nim się znajdujących można zastosować mechanizm szyfrowania dokumentu i wizualizacji zawartej w repozytorium za pomocą symetrycznego klucza tworzonego na podstawie identyfikatora. Mechanizm ten zapewni, że nikt, nawet administrator archiwum ani twórca dokumentu, nie uzyska dostępu do dokumentu, o ile nie będą miał identyfikatora. W takiej sytuacji archiwum nie przechowuje listy wytworzonych identyfikatorów.

Do tworzenia identyfikatorów posiadających wyżej zdefiniowane cechy można wykorzystać niedeterministyczne algorytmy podpisu. Dodatkowo, aby zapewnić krótkie identyfikatory, przy zachowaniu wysokiego bezpieczeństwa, należy skorzystać z kryptografii krzywych eliptycznych. Standardowym

algorytmem podpisu na krzywych eliptycznych jest algorytm ECDSA[5]. Przypomnijmy w skrócie, że podpisem ECDSA dla wiadomości m, losowej liczby k oraz klucza publicznego [d]G (d jest kluczem prywatnym, G jest generatorem grupy podanym jako parametr krzywej eliptycznej) są dwie długie liczby (r,s), gdzie:

$[k]G = (x,y)$,

$r = x \bmod |\langle G \rangle|$,

$s = k^{-1}(H(m)+r*d) \bmod |\langle G \rangle|$.

Repozytorium może wykorzystać ten schemat podpisu do tworzenia identyfikatów w następujący sposób. W pierwszej kolejności repozytorium wybiera losowo klucz prywatny d ze zbioru liczb $\{1,\ldots,|\langle G \rangle|-1\}$ oraz wylicza klucz publiczny [d]G, który następnie publikuje. Identyfikatorem nowego dokumentu jest konkatenacja aktualnej daty oraz liczb r i s:

id := RRRRMMDD||r||s

gdzie (r,s) to podpis ECDSA repozytorium pod konkatenacją daty, swojej domeny WWW oraz opcjonalnie pod treścią dokumentu.

Algorytm weryfikacji identyfikatora wygląda następująco. Weryfikator czyta kod 2D na dokumencie, dzięki czemu uzyskuje identyfikator dokumentu oraz domenę WWW. Z identyfikatora ekstrahuje wartości r i s, a następnie używając klucza publicznego repozytorium oraz jego domeny (ewentualnie również treści dokumentu), weryfikuje, czy (r,s) jest poprawnym podpisem ECDSA repozytorium.

Tak konstruowane identyfikatory posiadają wszystkie zdefiniowane wcześniej cechy. Identyfikatory będą unikatowe. Łatwo zauważyć, że konflikty mogą pojawić się jedynie, gdy dokumenty zostaną wrzucone do repozytorium tego samego dnia. Z powodu niedeterminizmu podpisów ECDSA repozytorium ma danego dnia co najmniej 2^{255} (dla standardowej 256-bitowej krzywej eliptycznej P-256[6]) różnych podpisów, gdyż wartość s może przyjmować wszystkie wartości od $\{1,\ldots, |\langle G \rangle|-1\}$. Warto jednak zauważyć, że liczba dostępnych identyfikatorów jest większa, gdyż w powyższych rozważaniach

[5] Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1998.

[6] Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), 2000.

nie uwzględniamy wartości r. Liczba ta jest aż nadto wystarczająca (liczba atomów słońca to około 10^57 < 2^190).

Kolejną cechą, jaką posiadają identyfikatory oparte na ECDSA, jest brak możliwości utworzenia poprawnych identyfikatorów poza repozytorium. Fakt posiadania tej cechy można argumentować następująco. Zauważmy najpierw, że skoro data jest częścią podpisanej wiadomości, nie można stworzyć poprawnego identyfikatora jedynie poprzez jej zamianę. Załóżmy następnie, że istnieje algorytm A, który korzystając z klucza publicznego repozytorium, tworzy poprawne identyfikatory. Można wtedy taki algorytm wykorzystać do wykonywania podpisów ECDSA w imieniu osób trzecich (tzn. bez znajomości ich kluczy prywatnych). Takie rozumowanie prowadzi do sprzeczności z założeniem bezpieczeństwa ECDSA, a zatem taki algorytm A nie istnieje, o ile założenie o bezpieczeństwie schematu podpisu ECDSA jest spełnione.

Zatem tak konstruowane identyfikatory same świadczą o swojej autentyczności. Dzięki temu mają one ostatnią wyżej wyszczególnioną cechę, a mianowicie istnieje możliwość weryfikacji autentyczności identyfikatora poza archiwum. Wystarczy, aby weryfikator miał klucz publiczny repozytorium. Istnieje również możliwość weryfikacji treści dokumentu poza archiwum. W takim przypadku, przy tworzeniu identyfikatora, repozytorium musi załączyć treść dokumentu jako część wiadomości w podpisie ECDSA, a weryfikator będzie dodatkowo musiał wczytać treść dokumentu podczas weryfikacji identyfikatora.

Warto zauważyć, że identyfikatory konstruowane, jak opisano wyżej, będą krótkie, tzn. dla wcześniej wspomniajej krzywej eliptycznej P-256 długość podpisu będzie wynosiła 512 bitów, tj. 64 bajty. Taka długość identyfikatorów gwarantuje, że tworzony na dokumencie kod 2D z identyfikatorem będzie można efektywnie używać w praktycznych zastosowaniach. Bezpieczeństwo algorytmu podpisu ECDSA dla krzywej eliptycznej 256-bitowej jest porównywalne do RSA z modułem długości 3072[7].

[7] NIST Special Publication 800-57: Recommendation for Key Management – Part 1: General, 2007.

4. Dodatkowe wymagania

Niezbędne wydaje się uregulowanie prawne rozwiązania gwarantujące, że dokument elektroniczny przechowywany w repozytorium, do którego udostępniono papierowy wydruk wskazujący miejsce weryfikacji dokumentu papierowego i źródło dokumentu elektronicznego, jest równorzędny z dokumentem papierowym. Uregulowanie to powinno istnieć zarówno w sferze prawa administracyjnego, jak i cywilnego, aby umożliwić posługiwanie się takimi dokumentami osobom prywatnym i przedsiębiorstwom w ich procesach biznesowych. Należy też rozważyć, czy odpowiednia regulacja nie powinna zostać zrealizowana w przepisach fiskalnych, aby umożliwić posługiwanie się w tym schemacie dokumentami księgowymi.

Działanie repozytoriów obwarowane jest kilkoma wymaganiami pozafunkcjonalnymi, które wymagają uregulowania prawnego i implementacji technicznej. Najważniejszym z nich jest zapewnienie zaufania do repozytoriów – rozumianego jako odpowiednie ich umocowanie prawne i narzucenie najwyższych standardów jakościowych, włączając w to realizację wymagań dotyczących jakości usług zgodnie z normą ISO 9001, wymagań dotyczących bezpieczeństwa zgodnie z normą ISO 27001 oraz objęcie nadzorem podobnym do tego, który jest realizowany dla podmiotów świadczących kwalifikowane usługi certyfikacyjne. Podobnie jak dyskredytacja kluczy centrum certyfikacji dla usług podpisu elektronicznego, tak naruszenie dostępności, integralności lub poufności danych w repozytorium ma ogromne znaczenie dla zaufania publicznego związanego z tego rodzaju rozwiązaniami.

Inteligentny papier (Smart Paper) jest rozwiązaniem prawnym, organizacyjnym i technicznym, jego różne implementacje pojawiają się jak samotne wyspy i mają dobre przyjęcie społeczne. Zapewnienie schematu opisanego w niniejszym referacie pozwoli w sposób płynny zmieniać świat z papierowego na elektroniczny przy poszanowaniu przyzwyczajeń tych, którzy trochę bardziej ufają temu, co na papierze.

Literatura

Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), 2000.

Centralna Ewidencja i Informacja o Działalności Gospodarczej, http://www.ceidg.gov.pl.

Ministerstwo Sprawiedliwości, http://ems.ms.gov.pl.

NIST Special Publication 800-57: Recommendation for Key Management – Part 1: General, 2007.

Proposal for a Regulation of The European Parliament and of The Council on electronic identification and trust services for electronic transactions in the internal market, COM(2012) 238 final, Brussels 2012.

Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1998.

ENSURING THE RELIABILITY OF ELECTRONIC DOCUMENTS FUNCTIONING IN THE WORLD OF PAPER

Summary

According to the visionaries of computerization, in the next few years, paper documents should go out of date both in public administrations and in the daily habits of citizens. The reality is that paper has a long history, is part of habits of people and everyone knows how to deal with paper documents. In addition it should be noted that the switching to computer processing creates barriers of social exclusion. Does not this mean that we computerize for nothing – because the people will always use paper? We offer a legal and technical solutions to enable every citizen the free choice of the form in which an electronic document will be stored at home. Any document, which has a electronic counterpart, can be stored in a form that is more convenient and safer for the user i.e. printed or stored on electronic media. Necessary condition for this solution is that there is no special equipment required to easily verify that a printed document is equivalent to the original and to obtain the original electronic format we only require access to the Internet.

Translated by Michał Tabor and Lucjan Hanzlik