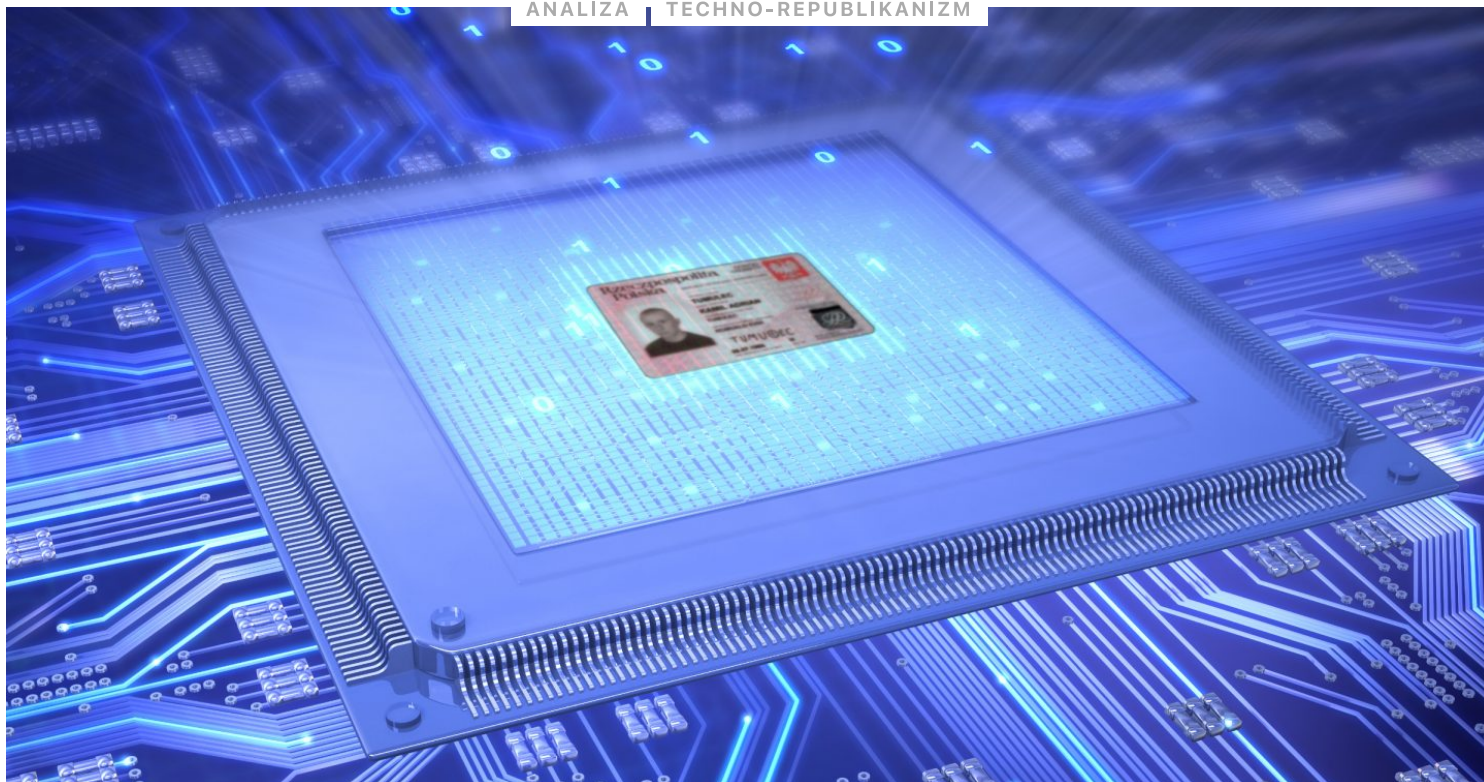


Jakub Lipiński, Bartosz Paszcza 15 lipca 2019









E-chaos. Polska, Unia i podpisy elektroniczne

🕒 przeczytanie zajmie 6 min


ANALIZA | TECHNO-REPUBLICANIZM



W SKRÓCIE

-   **Podpis osobisty, podpis kwalifikowany, profil zaufany. W Polsce mamy do rozwiązania prawdziwy węzeł gordyjski z podpisami elektronicznymi.**
-   **Nowy elektroniczny dowód osobisty ma potencjał stać się fundamentem cyfrowej tożsamości Polaków.**
-   **Do osiągnięcia pełnej funkcjonalności polskiego e-dowodu konieczna jest reforma unijnej rozporządzenia eIDAS.**
-   **Suwerenność cyfrowa i bezpieczeństwo narodowe wymagają, aby czytniki e-dowodów produkowano w Polsce i przez polskie firmy.**

E-dowód mógłby znacznie zmniejszyć niebezpieczeństwo podrabiania podpisów i podnieść poziom zaufania społecznego. Mógłby również pomóc przenieść analogowy świat „parafek” i skanowania dokumentów z ręcznymi podpisami w XXI wiek. Niestety

chaos wprowadzony przez europejskie rozporządzenie eIDAS dodatkowo komplikuje niełatwy temat elektronicznych podpisów i zapewne przeszkodzi w zdobywaniu ich popularności. Czas, aby zastanowić się nad zmianą tego rozporządzenia, szczególnie, że w przyszłym roku Komisja Europejska ma w planach się jej przyjrzeć. 

Od 4 marca możemy zamówić dowód osobisty z warstwą elektroniczną. To szansa na zmniejszenie niebezpieczeństwa kradzieży naszej tożsamości i podrobienia podpisu. Potrzeba wprowadzenia e-dowodów do użytku jest paląca ze względu na to, że Polsce grożą wysokie kary za niewdrożenie projektu. O burzliwej historii wprowadzania e-dowodów [pisał na naszych łamach](#) Marek Kudlicki.

NEWSLETTER

Twój email

ZAPISZ

Przypuśćmy, że na drodze pełnej zakrętów i przestojów, dostaliśmy wreszcie e-dowód. Tylko, że na obecnym cyfrowym dokumencie podpis osobisty współistnieje jednocześnie z podpisem kwalifikowanym (który także możemy na e-dowód wgrać) oraz osobnym Profilem Zaufanym. Wyjątkowym źródłem tego chaosu nie jest wcale polska administracja, lecz unijne rozporządzenie eIDAS. Postulujemy, aby to rozporządzenie stało się przedmiotem debaty zainicjowanej przez polskich eurodeputowanych w celu jej reformy. Dobry moment właśnie nadchodzi. Według Artykułu 49. eIDAS Komisja Europejska musi nie później niż 1 lipca 2020 przedstawić Parlamentowi Europejskiemu analizę działania regulacji.


Punkt wyjścia: państwo jako gwarant społecznego zaufania

Państwo za pośrednictwem ustandaryzowanego dowodu osobistego umożliwia nam bezpieczne i pewne potwierdzenie personaliów drugiej osoby. Dokument wykorzystujemy zarówno w sytuacji, kiedy musimy potwierdzić swoją tożsamość w urzędzie, jak i w innych okolicznościach „ograniczonego zaufania”, jak np. podczas wypożyczenia roweru, sprzedaży samochodu, rejestracji w hotelu lub odbioru biletu w kasie.

W interesie państwa i jego obywateli jest, aby nikt nie mógł podszywać się pod drugą osobę i zawierać wiążących transakcji w nie swoim imieniu. Niektóre czynności prawne, tj. sprzedaż nieruchomości czy założenie spółki, uznane zostały za wyjątkowo newralgiczne.

Wówczas dokonanie ich, w świetle polskiego prawa, wymaga obecności notariusza, który dodatkowo potwierdza tożsamość stron. Ustandaryzowany sposób autoryzacji tożsamości obywateli i osób prawnych jest fundamentem ładu społeczno-gospodarczego.

Bezpieczeństwo systemu sprzed powstania e-dowodów bazuje na czterech fundamentach. Po pierwsze, państwo weryfikuje tożsamość obywateli, a wydawane im dowody osobiste naszpikowane są zabezpieczeniami przed fałszerstwem. Po drugie, dokumenty zawierają wzór

podpisu (nieobecny już w nowych e-dowodach) i zdjęcie właściciela. Po trzecie, za posługiwanie się fałszywymi dokumentami, podrabianie dowodu lub podpisu grożą sankcje karne. Po czwarte  wreszcie, państwo prowadzi rejestr zagubionych lub skradzionych dowodów i każdy może zweryfikować, czy prezentowany dokument jest wciąż ważny.

Aż dziw bierze, że ten system wciąż działa. W internecie kwitnie proceder handlu tzw. dowodami kolekcjonerskimi, które możemy zamówić sobie z dowolnymi danymi osobowymi i wybranym zdjęciem – ustawa walcząca z tym procederem weszła w życie zaledwie 12 lipca. Takie dokumenty nie posiadają oczywiście wszystkich wymaganych zabezpieczeń, ale dla laika są nieodróżnialne od oryginału. Wbrew przepisom nasze dowody są nagminnie kopiowane w różnych instytucjach, więc istnieją już bazy skanów dokumentów, które można nabyć komercyjnie.

Weryfikacja podpisu pod dokumentem na podstawie wzoru z dowodu budzi już tylko rozbawienie. Jeden z członków naszej redakcji był świadkiem, gdy pani notariusz zabrała dokument przedstawiony przez jedną ze stron w celu – jak to określiła – „zweryfikowania jego oryginalności przy pomocy specjalnego urządzenia, które znajduje się w drugim gabinecie”. Wychodząc na chwilę na korytarz, Jakub niechcący zobaczył panią notariusz pochylającą się nad dokumentem ze... szkłem powiększającym.

Czas na zmiany. E-rewolucja na horyzoncie

Na czym więc będzie polegać przejście ze świata analogowego w cyfrowy? W dużej mierze bezpieczeństwo kryptograficzne podpisów cyfrowych opiera się na parze kluczy (ciągu znaków): publicznym i prywatnym. Ten pierwszy jest ogólnie dostępny, a w przypadku e-dowodów przypisany przez państwo do konkretnego obywatela. Ten drugi służy do podpisywania dokumentów i, jak nazwa wskazuje, powinien być prywatną własnością. Jeśli ktoś inny uzyska do niego dostęp, może podszyć się pod posiadacza i podpisywać dokumenty w jego imieniu. Klucze związane są ze sobą w taki sposób, by przy pomocy klucza publicznego można jednoznacznie zweryfikować, że dany dokument został podpisany skojarzonym z nim kluczem prywatnym.

Właściciel generuje swój klucz prywatny i tylko on ma do niego dostęp. Na tym opiera się bezpieczeństwo całego rozwiązania. Dodatkowo technologia umożliwia zapisywanie kluczy w warstwie elektronicznej mikroprocesora karty w taki sposób, że w ogóle nie da się go odczytać. Można jedynie użyć go do złożenia podpisu cyfrowego poprzez autoryzację np. przy pomocy kodu PIN.

To tak, jakby zamknąć klucz do kłódki w pudełku. Nie można go wyciągnąć i zobaczyć, jak wygląda, ale można do pudełka włożyć ręce z kłódką i po omacku użyć klucza do jej otwarcia. Najbardziej cenieni na rynku dostawcy kluczy zabezpieczających oferują nagrodę każdemu, komu udać się złamać zabezpieczenia i odczytać klucz prywatny z mikroprocesora.

Klucze prywatne w e-dowodach zostały „zaszyte” w chipie znajdującym się wewnątrz plastiku. Podczas transakcji potwierdzania klucz nie jest w żaden sposób kopiowany przez jakikolwiek czytnik. Jak zapewnia nas rząd, nie jest możliwe wydostanie klucza prywatnego z e-dowodu.

Wiele z wcześniej opisanych słabości tradycyjnego systemu może być rozwiązane przez wykorzystanie e-dowodów i podpisów elektronicznych. Konstrukcja e-dowodu pozwala podnieść poziom społecznego bezpieczeństwa. Zamiast „specjalnych urządzeń weryfikujących oryginalność podpisu” czy innego „organoleptycznego sposobu kontroli podobieństwa twarzy”, używając e-dowodu do złożenia podpisu, musimy nie tylko przyłożyć go fizycznie do czytnika, ale też wpisać sześciocyfrowy kod PIN.

Polski węzeł gordyjski podpisów elektronicznych

Tutaj dochodzimy do sedna problemu. Na e-dowodzie znaleźć się mogą cztery osobne certyfikaty pomagające potwierdzić naszą tożsamość. Pierwszym z nich, obowiązkowo znajdującym się na dowodzie i niewymagającym podania kodu PIN, jest potwierdzenie obecności. To usługa umożliwiająca na przykład potwierdzenie, że faktycznie lekarz nas przyjął i NFZ powinno mu za to zapłacić. Drugi ma umożliwić na przykład logowanie do serwisu ePUAP czy obywatel.gov.pl.

Trzecim, opcjonalnym certyfikatem jest podpis osobisty. To on wykorzystuje sześciocyfrowy PIN do podpisywania dokumentów. Czwarty, również opcjonalny, jest z kolei podpis kwalifikowany. Ten, w odróżnieniu od dwóch poprzednich, jest dostarczany przez prywatne firmy za coroczną opłatą.

Ministerstwo Spraw Wewnętrznych i Administracji pisze na swojej stronie, że podpis osobisty jest „analogiczny” do podpisu kwalifikowanego. Obecnie trwa procedura zmiany kilkudziesięciu czy kilkuset ustaw, rozporządzeń i regulaminów, aby w Polsce umożliwić używanie podpisu osobistego na równi z podpisem kwalifikowanym. Po co nam to zamieszanie? Dlaczego podpis osobisty nie stał się po prostu kwalifikowanym?

Unia na straży interesów prywatnych firm kosztem obywateli

Wszystko z powodu europejskiego rozporządzenia eIDAS, która określa zasady certyfikowania elektronicznych podpisów oraz ich wymagania techniczne. Według regulacji podpis osobisty (wydawany przez państwo, opcjonalny i darmowy dostępny w e-dowodzie) jest kwalifikowany jako „podpis zaawansowany”, który od podpisu kwalifikowanego (wydawanego przez firmy prywatne, który także można wgrać na e-dowód, ale kosztuje kilkaset złotych) nie różni się technicznie. Odmienny jest jedynie fakt, że podpis kwalifikowany jest wystawiany przez instytucję (najczęściej firmę) posiadającą certyfikat kwalifikowanego dostawcy usług zaufania.

Brzmi skomplikowanie? Owszem, bo to po prostu jest niepotrzebnie skomplikowane, jednak mimo wszystko kryje się za tym pewna logika. Państwo ma monopol na potwierdzanie tożsamości (choć eIDAS pozostawia furtkę, aby w przyszłości robiły to inne podmioty), jednak do czasów cyfrowych nie było to jego rolą. Dlatego tworząc eIDAS, UE zobowiązała kraje do liberalizacji rynku dostawców podpisów.

Stanowisko Polski w sprawie dostarczanego przez państwo podpisu osobistego mającego rangę kwalifikowanego jest uzasadnione. Rząd uznał, że najpewniej państwo zostałoby narażone na proces wytoczony przez rynkowych dostawców. Za darmo bowiem świadczyłyby usługi, za które firmy każą sobie słono płacić.

Dlatego obecnie Polska dostarcza za darmo podpis, który faktycznie jest kwalifikowanym, ale prawnie nie ma takiej rangi. To oznacza, że przyda się w komunikacji z administracją (jeśli tylko uda się skończyć długotrwały proces zmiany kilkudziesięciu czy kilkuset dokumentów), ale już nie w komunikacji między obywatelami czy w biznesie.

Podpis kwalifikowany jest według prawa obecnie po prostu równoważny analogowemu i nie można go nie uznać, a w przypadku podpisu osobistego obie strony muszą się umówić na taką formę sygnatury.

Teoretycznie mogłaby istnieć hybrydowa, państwowo-prywatna ścieżka rozwiązania obecnego węzła gordyjskiego podpisów elektronicznych. Państwo mogłoby oferować obywatelom podpis kwalifikowany, który dostarczałaby firma prywatna – wybrana w przetargu lub na przykład przez obywatela przy urzędowym okienku. W takim procesie mogłaby wystartować na równych z podmiotami prywatnymi zasadach Polska Wytwórnia Papierów Wartościowych, która obecnie dostarcza m.in. blankiety e-dowodów i czytniki. Wadą takiego rozwiązania jest cena, którą musiałoby wziąć na siebie państwo, chcąc upowszechnić usługę.

Z podpisami kwalifikowanymi jest jeszcze jeden zasadniczy problem: ani nie gwarantują wyższej jakości usług, ani nie zapewniają niskich cen. W przypadku Polski intuicyjność i wygoda stosowanych rozwiązań jest po prostu niska. Z funkcjonującymi dziś na rynku podpisami problemy mają nawet ludzie z wykształceniem informatycznym (sic!).



Pracować po republikańsku. Marzenie o państwie jako
dobrym pracodawcy

Nierealne oczekiwania. Bilans i perspektywy stosunków
polsko-chińskich

Po dywersyfikacji. Polski rynek
zmian

E-dowód w świecie fake newsów

Musimy pamiętać także o tym, że liberalizacja rynku dostawcy podpisów kwalifikowanych to także pewna liberalizacja zarządzania cyberbezpieczeństwem. Motywacja rynkowa i biznesowa, jak widzimy w przypadku innych technologicznych firm w ostatnich latach, nie sprzyja priorytetowemu traktowaniu cyberbezpieczeństwa. To bowiem głównie wysokie koszty i ograniczenie wygody usług.

Nasz podpis w formie elektronicznej staje się jednym z kluczowych i najbardziej wrażliwych elementów cyfrowego świata (obok potwierdzania tożsamości). Ewentualny wyciek danych lub kluczy prywatnych z tzw. chmurowych podpisów kwalifikowanych (gdzie klucz prywatny przechowywany jest przez firmę w chmurze, nie w e-dowodzie) może spowodować, że złodziej będzie miał możliwość podrobienia naszego podpisu nie pod jednym dokumentem, ale pod tysiącami dokumentów na sekundę. Idźmy w spekulacjach o krok dalej. Co się stanie, jeśli dostawcą podpisów kwalifikowanych zostanie firma należąca do chińskiego, rosyjskiego czy arabskiego funduszu inwestycyjnego?

W czasach sceptycyzmu wobec ponadnarodowych korporacji zbierających i handlujących naszymi danymi dobrze zaprojektowana i sprawnie wdrożona cyfrowa tożsamość (razem z e-podpisem) może zwiększyć zaufanie do państwa i współobywateli. Szczególnie, że w dobie fake newsów i fabrykowania dowolnych materiałów zdjęciowych czy filmowych cyfrowe poświadczenie

autentyczności informacji przy pomocy e-dowodu może być jedynym ratunkiem pozwalającym odróżnić prawdę od fałszu.



A co z polską suwerennością cyfrową?

Kontynuując temat cyberbezpieczeństwa, należy zwrócić uwagę na jeszcze jeden aspekt: cyfrową suwerenność. Dziś nie kupimy polskiego czytnika e-dowodów. Wszystkie, nawet te oferowane przez Polską Wytwórnę Papierów Wartościowych, to produkty zagraniczne. W czasach, w których Chińczycy instalują mikroprocesory szpiegowskie w serwerach produkowanych na rynek amerykański, suwerenność cyfrowa to podstawa niezależności państwa.

Państwo suwerenne cyfrowo to także takie, które w pełni kontroluje wszystkie kluczowe komponenty swojej infrastruktury. Projektowanie oraz produkcja elektronicznych czipów i czytników nie jest czymś, co przerasta naszych inżynierów i producentów elektroniki. Sprzętowe komponenty systemu (czipy, czytniki) powinny powstawać w Polsce. Co więcej, należy tak zadbać o bezpieczeństwo całego łańcucha dostaw, aby chronić system przed kompromitacją na każdym etapie wytwarzania i dystrybucji.

Nie oznacza to oczywiście, że powinniśmy wynajdywać koło od nowa. Tam, gdzie jest to możliwe (a jest tak w większości sytuacji), należy wykorzystać otwarte standardy i protokoły. Całość oprogramowania powinna być dostępna na otwartej licencji, tak aby rzesze naszych najlepszych programistów i architektów bezpieczeństwa mogły zaudytować całość systemu.

Panie i Panowie Europosłowie, przemysłmy eIDAS

Dlatego postulujemy, żeby polscy europosłowie przyjrzeni się eIDASowi. Jakie są zalety, a jakie wady liberalizacji rynku dostawców podpisów kwalifikowanych? Czy potwierdzanie podpisów obok potwierdzania tożsamości nie powinno stać się jedną z podstawowych funkcji państwa cyfrowego? Według nas rachunek jednoznacznie wskazuje, że obecne regulacje tworzące bariery przed rozpowszechnieniem e-podpisów są mniej bezpieczne i mniej wygodne, a także droższe w użyciu.

Polskie państwo jest skupione na sobie, a nie zwrócone w stronę obywatela. E-dowody w obecnej postaci przede wszystkim ułatwiają działanie administracji. Ich podstawowe wykorzystanie to potwierdzenie obecności, tożsamości i zleceń w urzędach. Najważniejsza okazuje się więc relacja państwo-obywatel.

Zatem w centrum zainteresowań administracji jest ... sama administracja. Nasze wcześniejsze rozważania pokazują jednak, że najważniejszą funkcją dowodów osobistych, a co za tym idzie –ich największym potencjałem, jest usprawnianie relacji obywatel-obywatel. Przy pomocy

e-dowodu powinniśmy móc podpisać kontrakt z operatorem telekomunikacyjnym lub umowę na wynajem letniego domku.

Liberalizacja rynku usług elektronicznych w ciągu ostatnich trzech lat od wejścia w życie wcale nie przyniosła świetnie działających, zrozumiałych dla przeciętnego obywatela systemów w rozsądnej cenie.



Tymczasem za nasze pieniądze właśnie rozpoczęliśmy dystrybucję dokumentu, którym w ciągu 10 lat będzie dysponować każda dorosła Polka i dorosły Polak. Mamy też system, który spełnia technologiczne wymagania unijne, aby stać się uniwersalnym polskim e-podpisem. Dlaczego nie możemy tego wykorzystać?

Autorzy artykułu serdecznie dziękują Krzysztofowi Wojdyle za konsultację.

Artykuł został skorygowany 22.07.2019. Korekta obejmowała status eIDAS (które jest rozporządzeniem, a nie jak błędnie wskazano – dyrektywą) oraz ilość certyfikatów mogących znaleźć się na e-dowodzie (cztery zamiast trzech). Za błędy przepraszamy.

WESPRZYJ NAS

Klub Jagielloński to republikańskie, niepartyjne stowarzyszenie, łączące społeczników, ekspertów, publicystów i naukowców młodego pokolenia, chcących działać razem na rzecz dobra wspólnego. Pracujemy na rzecz sprawnego państwa i podmiotowości obywateli. Dołącz do grona naszych Darczyńców!

Zebrana kwota: 17 375 PLN
Docelowa kwota: 32 000 PLN

54%

Wspieram



UDOSTĘPNIJ

Jakub Lipiński

Szef Rady Klubu Jagiellońskiego. Pomysłodawca i koordynator prac nad aplikacją Pola. Przedsiębiorca, założyciel firmy Polidea, programista. Mąż Małgosi, ojciec Krzysia, Szymka, Frania i Poli

Bartosz Paszcza

Członek zarządu Klubu Jagiellońskiego zajmujący się nowymi technologiami, szef działu "Techno-republikanizm" na naszym portalu. Prowadzi podcast „ScepTech”. Magister studiów nad internetem na Uniwersytecie w Southampton. Współzałożyciel Fundacji Polonium – organizacji łączącej polskich naukowców za granicą.