Fot. Jana Werner/Mirosław Adamczyk

Jedną z podstawowych zasad postulowanych przez Dyrektywę Unii Europejskiej o podpisie elektronicznym jest ograniczanie ingerencji państwa. W Polsce jest inaczej.

Mirosław Kutyłowski

Podpis elektroniczny w przededniu wejścia Polski do Unii Europejskiej

Moment przystąpienia do Unii Europejskiej może dużo zmienić w praktyce stosowania podpisu elektronicznego w polskiej gospodarce. Polskie ramy prawne, niesprzyjające jak się okazuje wykorzystaniu tego narzędzia w praktyce gospodarczej, mogą stać się obecnie źródłem zagrożeń dla polskiej gospodarki. Wiele problemów ma swoje źródło w słabym przygotowaniu do stosowania nowoczesnych technologii i popełnianych błędach merytorycznych.

Wolność stosowania technologii podpisu elektronicznego

Jedną z podstawowych zasad postulowanych przez Dyrektywę Unii Europejskiej o podpisie elektronicznym jest ograniczanie ingerencji państwa.

Dyrektywa nie wkracza w obszar umów cywilno-prawnych i problematykę podpisu elektronicznego w zamkniętych systemach. Zasady stosowania tej technologii mają ustalać między sobą zainteresowane strony.

W Polsce jest inaczej i stanowi to bardzo istotną barierę formalno-prawną. Dla przykładu, jednym z ważniejszych pól zastosowań podpisu elektronicznego jest użycie go do uwierzytelniania wewnętrznej korespondencji i obiegu dokumentów w dużych organizacjach. Polska ustawa o podpisie elektronicznym w istocie sprawę bardzo skomplikowała.

Na problemy napotykamy się w obszarze formalno-prawnym. Wydanie certyfikatu klucza publicznego określonej osoby jest w sensie ustawy usługą certyfikacyjną. Ta zaś może być świadczona jedynie na podstawie umowy zawartej pomiędzy jednostką wystawiającą certyfikat a właścicielem klucza publicznego. Tak więc w przypadku uczelni państwowej, aby zelektronizować kontakty ze studentami, najpierw należy wykonać szereg czynności przewidzianych ustawą o podpisie elektronicznym – w tym dokonanych osobiście. Co gorsza okazuje się, że państwowa uczelnia w ogóle nie ma prawa świadczyć usług certyfikacyjnych - w tym wobec własnych studentów i pracowników – ustawa wymienia wyraźnie kto owe usługi może świadczyć. Uczelnia musiałaby zatrudnić zewnętrzną firmę. Wszystko to podnosi koszty i stawia pod znakiem zapytania sensowność całej operacji.

Podobne problemy mogą mieć miejsce gdzie indziej. Dla przykładu, międzynarodowe sieci spedycyjne z powodzeniem mogłyby zastosować podpis elektroniczny do usprawnienia i zabezpieczenia obiegu informacji. Mimo tego, że tworzony system informatyczny stanowi wewnętrzną sprawę takiej organizacji, podlega on w Polsce państwowemu nadzorowi. Należy sądzić, że istnienie takiej kontroli będzie raczej postrzegane jako nieuzasadniona ingerencja państwa i łamanie wolności gospodarczej.

Bezpieczne urządzenia do składania podpisów

W wielu kręgach pokutuje wciąż przekonanie, że kompatybilność produktów na rynku zapewnić może drobiazgowa reglamentacja stosowanych rozwiązań. Państwa bardziej doświadczone w problematyce nowoczesnych technologii tego błędu nie popełniają – de facto odchodzi się w znacznym stopniu od rozwiązań o charakterze reglamentacyjnych na rzecz standardów przemysłowych (których stosowanie jest dobrowolne). Zresztą standardy przemysłowe nie zawsze okazują się trafione, ich proces powstawania jest długi i obarczony walką grup interesów. Bywało i tak, że standardy w zakresie technik bezpieczeństwa okazywały się „dziurawe" i stosowanie się do nich byłoby błędem w sztuce. W Polsce przeważyła filozofia „gospodarki planowej" - rozporządzenia do ustawy o podpisie elektronicznym, które miały określić wymagania bezpieczeństwa w istocie stały się próbą (nieudaną zresztą pod względem merytorycznym) opisu technologii.

Istotnym problemem merytorycznym okazało się jednak samo znaczenie polskich przepisów dotyczących bezpiecznych urządzeń do składania podpisu. Jeśli postanowienia ustawy i rozporządzeń potraktuje się na serio, to stwierdzić należy, że urządzenia takie po prostu nie istnieją. Dla przykładu, polska ustawa stanowi, że bezpieczne urządzenie uniemożliwia pozyskiwanie prywatnych kluczy kryptograficznych zawartych w urządzeniu. Taka kategoryczna, stuprocentowa pewność jest nierealistyczna. Można co najwyżej mówić o aktualnie dostępnych technikach – nie wiadomo, co przyniesie postęp technologiczny w tym zakresie. Innym przykładem jest postulat, aby przed złożeniem podpisu urządzenie wyraźnie ostrzegło użytkownika, że kontynuacja operacji jest równoznaczne ze złożeniem podpisu. Przypomnijmy, że w krajach wysokorozwiniętych za bezpieczne urządzenie do składania podpisu elektronicznego uważa się kartę kryptograficzną. Jak karta kryptograficzna pracująca w trybie master-slave (i to w charakterze niewolnika!) miałaby zagwarantować ostrzeżenie użytkownika? Karty zaopatrzone w wyświetlacz, czy choćby generator dźwięku to dzisiaj ekonomiczne science fiction.

Wiele zamętu wprowadza koncepcja, że bezpieczne urządzenie do składania podpisu składa się z komponentu technicznego i oprogramowania podpisującego, działającego poza komponentem technicznym. Oprogramowanie to działa w potencjalnie wrogim (przynajmniej niekontrolowalnym) środowisku systemu operacyjnego. Jak

oprogramowanie to ma samo zapewnić łatwe rozpoznawanie istotnych dla bezpieczeństwa zmian dokonanych w nim? (a jest to wymóg ustawowy!) Kto wierzy, że oprogramowanie takie istnieje, ten wierzy w krasnoludki.

Model zastosowań

Wiele zastosowań podpisu elektronicznego może być zrealizowane w ramach infrastruktury daleko prostszej od postulowanej w ustawie o podpisie elektronicznym. Jako przykład może posłużyć kwestia podpisywania PITów i CITów w wersji elektronicznej. Użycie w tym celu kwalifikowanych certyfikatów oraz bezpiecznych urządzeń do składania podpisu nie jest wcale niezbędne. W istocie bowiem mamy do czynienia z sytuacją, w której podpisywany dokument nie jest kierowany do nieznanego z góry odbiorcy, lecz do urzędu skarbowego. Zamiast korzystać z drogiego kwalifikowanego certyfikatu, płatnik mógłby sam wygenerować autocertyfikat i zgłosić go do urzędu skarbowego. Niebezpieczeństwo podszycia się pod płatnika można ograniczyć poprzez uwiarygodnienie autocertyfikatu za pomocą kilkucyfrowego kodu przesłanego przez urząd skarbowy płatnikowi pocztą. Tak samo zrezygnować można z bezpiecznych urządzeń do składania podpisów elektronicznych. Jedyne co może płatnika spotkać w wyniku „wycieku" prywatnych kluczy, to podwójnie składane zeznania podatkowe. System informacyjny urzędu skarbowego powinien z łatwością takie przypadki zidentyfikować i podjąć odpowiednie proste czynności wyjaśniające.

Pozycja polskich podmiotów

W momencie wejścia Polski do Unii Europejskiej może okazać się, że polscy usługodawcy w zakresie podpisu elektronicznego są faktycznie eliminowani z polskiego rynku przez polskie prawo formułujące szereg uciążliwych wymagań (niemających nic wspólnego z bezpieczeństwem). Jednocześnie artykuł 4 ustawy o podpisie elektronicznym pozwala zagranicznym podmiotom omijać te wymagania. Jako przykład podać można sprawę zawartości polskich certyfikatów kwalifikowanych, gdzie obligatoryjnie znajduje się rozszerzenie z odwołaniem do polityki certyfikacji. Nie rozpoznawanie owego rozszerzenia przez zagraniczne oprogramowanie (co może być regułą) spowoduje automatyczne odrzucenie polskich certyfikatów. Zagraniczni usługodawcy mogą skutecznie to wymaganie obejść i oferować certyfikaty, którymi polscy użytkownicy mogliby się posługiwać w całej unijnej Europie.

Z kolei zaprojektowany system weryfikacji ważności polskich certyfikatów ma się nijak do weryfikacji podpisów w innych państwach Unii Europejskiej. Ponieważ dopuszczenie unijnych kwalifikowanych certyfikatów oznacza również możliwość weryfikacji podpisów przy ich użyciu, okazać się może, że i tu dużo wygodniejsze okażą się certyfikaty zagraniczne.

Obawy przed zmianami

Już w momencie uchwalania ustawy o podpisie elektronicznym głośne były opinie fachowców o szkodliwości ustawy w obecnym kształcie. Zastanawiano się nawet nad apelem do Prezydenta o zawetowanie ustawy. Przeważył pogląd, że byłoby to jednak większe zło. Nadzieje na rychłą nowelizację ustawy i poprawienie błędów okazały się niespełnione. Zagorzałymi zwolennikami ustawy były firmy posiadające monopol na wykonywanie określonych usług na rzecz Państwa. Utrzymywanie tego stanu rzeczy nie wydaje się jednak obecnie możliwe w obliczu konieczności zachowania zasad traktatu europejskiego.

Sektorem, który stosunkowo wcześnie wszedł w praktyczne stosowanie podpisu elektronicznego, są instytucje finansowe. Paradoksalnie, banki nie były lokomotywą postępu w tym zakresie w ostatnich latach. Potężnym bodźcem postępu mogłaby się okazać obowiązująca już ustawa o elektronicznych instrumentach płatniczych przenosząca ryzyko związane z zawodnością mechanizmów bezpieczeństwa z klienta banku na bank. Zasada ta stwarza bardzo silną motywację do stosowania niezawodnych technologicznie rozwiązań, takich jak bezpieczny podpis elektroniczny. Niestety, sytuacja okazuje się patowa. Drobne z pozoru szczegóły techniczne zawarte w rozporządzeniu Rady Ministrów o zabezpieczaniu elektronicznych dokumentów bankowych nie pozwalają w praktyce na korzystanie z bezpiecznego podpisu elektronicznego. Diabeł tkwi w szczegółach implementacyjnych – nie sposób bowiem określić rozmiaru elektronicznego dokumentu bankowego zabezpieczonego bezpiecznym podpisem elektronicznym. Paradoksalnie, jednocześnie nie nałożono właściwie żadnych warunków na „niebezpieczne" formy podpisu.