Instytut Autostrada Technologii i Innowacji

Cybersecurity Academy, 28.01.2016

Regulacja eIDAS – konsekwencje praktyczne

Prof. Mirosław Kutyłowski
Katedra Informatyki, WPPT

www.iati.pl

eIDAS -geneza

- biznesowa klęska koncepcji podpisu elektronicznego wg poprzedniej Dyrektywy
- powstające niekompatybilne systemy e-identyfikacji
- brak (spójnego) systemu bezpieczeństwa w obrocie elektronicznym

e-IDAS geneza

- brak legitymacji prawnej dla wprowadzenia Europejskiego Dokumentu Tożsamości
- problemy z identyfikacją online – rosnące problemy z kradzieżą tożsamości
- słabość stosowanych zabezpeiczeń

koncepcja eIDAS

- proteza dla Europejskiego Dokumentu Tożsamości
- rozszerzenie zakresu podpisu elektornicznego o nowe istotne usługi
- interoperacyjność w zakresie identyfikacji I uwierzytelniania
- jednolite poziomy zaufania
- obligatoryjna akceptacja

Z punktu widzenia władz państwowych:

- Deadline 1 lipca 2016
- obowiązek dostosowania prawa i systemów do eIDAS:
  - podpis elektroniczny, m.in. akceptowanie podpisów kwalifikowanych z innych krajów
  - akceptowanie identyfikacji i uwierzytelniania za pomocą notyfikowanych systemów z jakiegokolwiek państwa UE

Z punktu widzenia przedsiębiorcy

- wymagania na usługi zaufania
- kontrole

- zasada wolnego rynku
- standaryzacja
- wymuszona interoperacyjność

Usługi zaufania

„usługa zaufania” oznacza usługę elektroniczną zazwyczaj świadczoną za wynagrodzeniem i obejmującą:

a) tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub

b) tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; lub

c) konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami

„podpis elektroniczny” oznacza dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej, i które użyte są przez podpisującego jako podpis;

‘electronic signature’ means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;

więc praktycznie każda forma uwierzytelnienia podpada pod tę definicję:

logowanie, wpisanie PINu, otworzenie kanału VPN, …

Niekwalifikowane usługi zaufania

Produkty i usługi zaufania spełniające wymogi niniejszego rozporządzenia dopuszcza się do swobodnego obrotu na rynku wewnętrznym.

Nadzór nad niekwalifikowanymi usługami zaufania

Organ nadzoru… podejmuje, w razie konieczności, działania w odniesieniu do niekwalifikowanych dostawców usług zaufania mających siedzibę na terytorium wyznaczającego państwa członkowskiego – za pomocą działań nadzorczych ex post – gdy dowiaduje się, że niekwalifikowani dostawcy usług zaufania lub świadczone przez nich usługi zaufania rzekomo nie spełniają wymogów określonych w niniejszym rozporządzeniu.

Wymagania

… dostawcy usług zaufania przyjmują odpowiednie środki techniczne i organizacyjne w celu zarządzania ryzykiem, na jakie narażone jest bezpieczeństwo świadczonych przez nich usług zaufania.

Przy uwzględnieniu najnowszych osiągnięć w dziedzinie technologii środki te zapewniają poziom bezpieczeństwa współmierny ze stopniem ryzyka.

W szczególności należy podjąć środki zapobiegające incydentom związanym z bezpieczeństwem lub minimalizujące ich wpływ oraz należy informować zainteresowane strony o negatywnych skutkach wszelkich takich incydentów.

Wymagania 2

dostawcy usług zaufania, bez zbędnej zwłoki, a w każdym razie nie później niż 24 godziny od otrzymania informacji o wystąpieniu zdarzenia, zawiadamiają organ nadzoru i … inne właściwe podmioty o wszelkich przypadkach naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na świadczoną usługę zaufania lub przetwarzane w jej ramach dane osobowe.

Wymagania 3

W przypadku gdy prawdopodobne jest, że naruszenie bezpieczeństwa lub utrata integralności niekorzystnie wpłyną na osobę fizyczną lub prawną, na rzecz której świadczona była usługa zaufania, dostawca usług zaufania bez zbędnej zwłoki zawiadamia także tę osobę fizyczną lub prawną o tym naruszeniu bezpieczeństwa lub utracie integralności.

Wymagania 4

W stosownych przypadkach, w szczególności jeżeli naruszenie bezpieczeństwa lub utrata integralności dotyczą dwóch lub większej liczby państw członkowskich, zawiadomiony organ nadzoru powiadamia organy nadzoru w pozostałych zainteresowanych państwach członkowskich oraz ENISA.

Pieczęć elektroniczna

… oznacza dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych;

Pieczęć elektroniczna

Zaawansowana pieczęć elektroniczna musi spełniać następujące wymogi:

a) jest unikalnie przyporządkowana podmiotowi składającemu pieczęć

b) umożliwia ustalenie tożsamości podmiotu składającego pieczęć;

c) jest składana przy użyciu danych służących do składania pieczęci elektronicznej, które podmiot składający pieczęć może, mając je z dużą dozą pewności pod swoją kontrolą, użyć do złożenia pieczęci elektronicznej;

d) jest powiązana z danymi, do których się odnosi, w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna

Pieczęć elektroniczna

2. Kwalifikowana pieczęć elektroniczna korzysta z domniemania integralności danych i autentyczności pochodzenia tych danych, z którymi kwalifikowana pieczęć elektroniczna jest powiązana.

3. Kwalifikowana pieczęć elektroniczna oparta na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawana za kwalifikowaną pieczęć elektroniczną we wszystkich pozostałych państwach członkowskich.

Pieczęć elektroniczna

- Faktury
- Dokumenty bankowe
- …
- i wszędzie tam, gdzie konieczna jest automatyzacja i pewność obrotu

Wzajemne uznawanie

Jeżeli … dostęp do usługi *online* świadczonej przez podmiot sektora publicznego w jednym państwie członkowskim wymaga identyfikacji elektronicznej przy użyciu środka identyfikacji elektronicznej oraz uwierzytelnienia, w tym pierwszym państwie członkowskim na potrzeby transgranicznego uwierzytelnienia dla tej usługi *online* uznaje się środek identyfikacji elektronicznej wydany w innym państwie członkowskim, pod warunkiem że …

Wzajemne uznawanie

a) środek identyfikacji elektronicznej jest wydany w ramach systemu identyfikacji elektronicznej wymienionego w wykazie publikowanym przez Komisję na podstawie art. 9

(notyfikacja, łatwe do spełnienia dla działającego systemu)

Wzajemne uznawanie

b) poziom bezpieczeństwa środka identyfikacji elektronicznej odpowiada poziomowi bezpieczeństwa równemu lub wyższemu od poziomu bezpieczeństwa wymaganego przez odpowiedni podmiot sektora publicznego na potrzeby dostępu do tej usługi *online* w pierwszym państwie członkowskim, pod warunkiem że poziom bezpieczeństwa tego środka identyfikacji elektronicznej odpowiada średniemu lub wysokiemu poziomowi bezpieczeństwa

c) odpowiedni podmiot sektora publicznego korzysta ze średniego lub wysokiego poziomu bezpieczeństwa w odniesieniu do dostępu do tej usługi *online*.

Wzajemne uznawanie

Konsekwencje:

aby uniknąć wysiłku wdrożeniowego w systemach takich jak EPUAP można wyłączyć wszelkie uwierzytelnianie na poziomie średnim i wysokim (np. podpis kwalifikowany)

Koszt: ryzyko klientów tych systemów

Pierwsze wdrożenia uzyskają silną przewagę konkurencyjną.

Poziomy bezpieczeństwa

low – wymagania znacznie powyżej wielu dzisiejszych systemów

substantial – w istocie dość wysoki poziom

high – dziś technicznie+ekonomicznie trudne do spełnienia

Poziomy bezpieczeństwa - uwierzytelnianie

Low:

1. The electronic identification means utilises at least one authentication factor.
2. The electronic identification means is designed so that the issuer takes reasonable steps to check that it is used only under the control or possession of the person to whom it belongs.

Authentication factors: wiedza, posiadanie, biometria

Poziomy bezpieczeństwa - uwierzytelnianie

Substantial:

1. The electronic identification means utilises at least two authentication factors from different categories.
2. The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.

Poziomy bezpieczeństwa - uwierzytelnianie

High

1. The electronic identification means protects against duplication and tampering as well as against attackers with high attack potential
2. The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others.

Jak to zrobić????

Instytut Autostrada Technologii i Innowacji

Dziękuję za uwagę

i zapraszamy na kolejne spotkania

- najbliższe już 25 lutego 2016 r.

www.iati.pl