compendium
centrum edukacyjne

SIĘGNIJ PO PROFESJONALNĄ WIEDZĘ

# Bariery podpisu elektronicznego w Polsce i UE


**Paweł Krawczyk**

**Compendium Centrum Edukacyjne,
Internet Society Polska**

**pawel.krawczyk@compendium.pl**

# Motto

***„Należy wspierać współdziałanie produktów podpisu elektronicznego”***

**Dyrektywa 1999/93/WE o podpisie elektronicznym**

# Filary podpisu elektronicznego

- Bezpieczeństwo
- Przewaga ekonomiczna
  - Por. kartki, koperty, druk, znaczki…
- Przewaga ergonomiczna
  - Por. druk, pakowanie, wysyłka…
- Wzajemna kompatybilność

*Warunki KONIECZNE by podpis miał sens!*

# *Dyrektywa Unijna 1999/93/EC z dnia 13 grudnia 1999*

# Dyrektywa Unijna 1999/93 z dnia 13 grudnia 1999

- Rekomendacja, ramy prawno-organizacyjne, **definicje**
- „Electronic signature" – każdy podpis w formie cyfrowej (np. faksymile)
- „Advanced electronic signature"
  - *"advanced electronic signature" means an electronic signature which meets the following requirements* (art 2 pkt 2) – kryptografia (np. PGP, X.509)
- Qualified signature („podpis kwalifikowany" - nazwa potoczna)
  - *advanced electronic signatures **which** are based on a **qualified certificate** and which are created by a **secure-signature-creation device**: (a) satisfy the legal requirements of a signature in relation to data in electronic form **in the same manner as a handwritten signature*** (art 5 pkt 1)
- Warunki podpisu kwalifikowanego
  - Certyfikat kwalifikowany
  - Złożony na bezpiecznym urządzeniu (SSCD)

# Dyrektywa Unijna 1999/93 z dnia 13 grudnia 1999

- Certyfikat kwalifikowany (Annex I i inne)
  - Tożsamość posiadacza zweryfikowana przez centrum certyfikacji wg odpowiednich procedur
  - Bezpieczne wytworzenie i przechowywanie
  - **Certyfikat kwalifikowany jako łącze między tożsamością prawną z tożsamością elektroniczną**
    - Tylko na tej podstawie możliwe przyznanie praw podpisu odręcznego podpisowi kwalifikowanemu
    - (Inne tylko na podstawie umów cywilno-prawnych)

# Dyrektywa Unijna 1999/93 z dnia 13 grudnia 1999

- Bezpieczne urządzenie (Annex III)
  - nie da się odtworzyć klucza prywatnego z urządzenia
  - klucz prywatny ma być chroniony przed niepowołanymi
  - podpis ma być chroniony przed fałszerstwem
  - **urządzeniu nie wolno zmieniać podpisywanych danych *(sic!)***
- Cechy szczególne SSCD
  - Dyrektywa definiuje twór prawny, a nie techniczny
  - Nawet słoik może być SSCD jeśli spełni warunki prawne!
    - *Casus Polski*

# *Polska*
# *Ustawa o podpisie elektronicznym*
# *z dnia 18. września 2001 r.*

# Ustawa o podpisie elektronicznym

- Prawie dokładne tłumaczenie Dyrektywy 1999/93
  - Prawie… (sic!)
- Problemy w Ustawie
  1. Rozszerzenie znaczenia „advanced” na „bezpieczny”
  2. Określenie funkcji podpisu elektronicznego

## Problem 1

- „Advanced electronic signature” = „bezpieczny podpis elektroniczny”
  - Nieuzasadnione rozszerzenie znaczenia („advanced” != „secure”)

Rozwiązanie Problemu Zaawansowany vs Bezpieczny:
- Należy powrócić do oryginalnego znaczenia
- Zapowiedziane w zapowiedzi nowelizacji w maju 2006

# Ustawa o podpisie elektronicznym

## Problem 2

- Definicja podpisu elektronicznego
  - Duża różnica znaczeniowa między Ustawą a Dyrektywą
  - Kardynalne konsekwencje
- Dyrektywa 1999/93
  - *„Podpis elektroniczny" oznacza dane w formie elektronicznej dodane do innych danych elektronicznych lub logicznie z nimi powiązane i służące jako metoda uwierzytelnienia (*Art. 2, pkt. 1 Dyrektywy)
  - **Znaczenie: podpis to metoda uwierzytelnienia**
- Ustawa o podpisie elektronicznym
  - *Podpis elektroniczny - dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą **do identyfikacji osoby** składającej podpis elektroniczny (*Art. 3, pkt. 1. Ustawy)
  - **Znaczenie: podpis to identyfikacja osoby**

# Ustawa o podpisie elektronicznym

- Konsekwencje zmiany definicji
  - Niespójność, bo „metoda uwierzytelnienia” != „identyfikacja osoby”
  - Identyfikacja osoby wymaga osoby *(sic!)*
  - Podpis **kwalifikowany** może być składany **tylko przez osobę**
- Sens ekonomiczny i ergonomiczny podpisu elektronicznego
  - Wyeliminowanie człowieka z niektórych czynności
    - Oszczędność czasu, pieniędzy
  - Po to zlikwidowano wymóg podpisywania faktur papierowych
    - Automatyczny druk i wysyłka z systemu księgowego
- Jakie są konkretne konkretne konsekwencje dla polskiego biznesu i administracji?

# Ustawa o podpisie elektronicznym

- Rozporządzenie o e-fakturach (2005) wymaga podpisu **kwalifikowanego**
  - W/w niespójność ponownie wprowadza wymóg obecności człowieka
- Rozporządzenie wywołało kontrowersje
  - Ale rozporządzenie jest OK – definicja w Ustawie jest zła!
  - Kwalifikowany podpis konieczny ze względu na weryfikację tożsamości
- Gdybyśmy jednak trzymali się definicji z Dyrektywy…
  - „Metoda uwierzytelnienia" zapewnia co najmniej
    - **Identyfikację osoby** (niezaprzeczalność, oświadczenie woli)
    - **Autentyczność** (potwierdzenie pochodzenia, integralność)
  - E-faktura wymagałaby podpisu kwalifikowanego tak jak dzisiaj…
    - …Ale ten mógłby być składany bez udziału człowieka
    - Sens ekonomiczny i ergonomiczny zostałby zachowany

# Ustawa o podpisie elektronicznym

- Gdzie potrzeba autentyczności a nie niezaprzeczalności?
  - **Faktury elektroniczne** (wystawia system F-K, ważne by nr konta był autentyczny)
  - **Publikacje elektroniczne** (interpretacje, SIWZ, akty prawne)
  - **Elektroniczne poświadczenie odbioru**
- W obecnej sytuacji konieczne sztuczki i kruczki
- Kruczek I: jak podpisać 1000 faktur z niezaprzeczalnością?
  - **Podpis wielokrotny** (*multiSign*)
  - **Jedno wpisanie PIN, wiele podpisów**
  - **Pokrętny ze względu na istotę niezaprzeczalności**
    - 1) Przeczytaj dokument, 2) wpisz PIN, 3) przeczytaj ostrzeżenie, 4) potwierdź wolę podpisania
  - **Sprzeczny z Ustawą**
    - „ostrzeżenie poprzedza złożenie **podpisu**”, a nie „podpisów”
- Kruczek II: Jak zapewnić autentyczność przez niezaprzeczalność?
  - Pełnomocnictwo osoby prawnej dla osoby fizycznej
  - W rezultacie niezaprzeczalnym autorem np. faktury lub ustawy jest jakiś Jan Kowalski
- **Wszystko przez ograniczenie definicji podpisu!**

# Ustawa o podpisie elektronicznym

- Rozwiązanie Problemu Definicji Podpisu
  - Powrót do definicji z Dyrektywy („metoda uwierzytelnienia”), ale…
  - Konieczne osadzenie podpisu „autentycznego” w prawie i procedurach
  - Wymagana dodatkowa analiza prawna
  - Rozwiązanie konieczne, bo paraliżuje rynek…

?

# *Pozostałe problemy*

- Fikcyjne bezpieczne urządzenie
- Bałagan z formatami podpisu
- „Amerykańskie” poświadczenie odbioru
- Chaos w administracji publicznej

# Fikcyjne bezpieczne urządzenie

- Podpis kwalifikowany
  - Musi być składany przy pomocy bezpiecznego urządzenia (SSCD)
  - Klucz musi być przechowywany na bezpiecznym urządzeniu
- Po co SSCD?
  - Bezpieczne środowisko do przechowywania klucza
  - Bezpieczne środowisko do wyświetlania dokumentu (groźne makra)
  - Bezpieczne środowisko do składania podpisu (wirusy, konie trojańskie)
- Mówię „bezpieczne urządzenie", a myślę:
  - Informatyk: *„taki mały bankomat z czytnikiem i ekranikiem… bo ja wiem, coś w tym stylu…"*
  - Prawnik: *„wszystko co spełnia wymagania definicji bezpiecznego urządzenia"*
  - Biznesmen*: „wszystko co pasuje do SIWZ, spytać Prawnika"*

# Fikcyjne bezpieczne urządzenie

- Bezpieczne urządzenie wg Dyrektywy **oraz** Ustawy
  - Wymogi funkcjonalne – co ma zapewniać, czego ma nie robić
  - Np. *„Bezpieczne urządzenie służące do składania podpisu elektronicznego **powinno** (…) **nie zmieniać danych, które mają zostać podpisane”** (art. 18 pkt 1 Ustawy)*
  - Pasuje jak ulał do karty elektronicznej
- Bezpieczne urządzenie wg „Rozporządzenia o warunkach technicznych”
  - Komponent sprzętowy (karta) – OK, zgodne z w/w
  - Komponent programowy - znaczne rozszerzenie definicji SSCD!
  - Szereg zabezpieczeń sprzętowych i programowych
    - „bezpieczny kanał” i „bezpieczna ścieżka” (par. 1, pkt 13 Rozporządzenia)
  - **SSCD wg rozporządzenia - typowa „Wizja Informatyka”**
  - Oparte o CWA 14169 (Europejski Komitet Standaryzacji – CEN)

# Fikcyjne bezpieczne urządzenie

- Cechy Wizji Informatyka
  - Bardzo bezpieczna, ale..
  - Bardzo droga
  - Równie ergonomiczna jak bankomat – i zbliżony popyt…
- Przykład trudności
  - Bezpieczny kanał i bezpieczna ścieżka wymagają zaufanego systemu operacyjnego w zaufanym środowisku sprzętowym
  - Zaufane środowisko jest droższe, nierozpowszechnione i mniej używalne
- Jak to rozwiązano w Rozporządzeniu?
  - Wyłączono z drogich zabezpieczeń pewną klasę „urządzeń”
  - Intencja – stworzenie „low-end” SSCD do powszechnych zastosowań
- Rezultat
  - Udziwniona Wersja Informatyka z Lukami
  - Chaos i nieużywalność podpisu elektronicznego w Polsce
  - Jak to się stało?

# Fikcyjne bezpieczne urządzenie

- Rozporządzenie wprowadza
  - Komponent sprzętowy i komponent programowy
  - Wymóg certyfikatu bezpieczeństwa (komp. sprzętowy)
  - Wymóg deklaracji zgodności (komp. Programowy)
  - Bezpieczny kanał (dokument-system-sprzęt)
  - Bezpieczna ścieżka (klucz-system)
  - **Wynik**: mały bankomat (głównie przez ścieżkę i kanał)
- Zaraz potem rozporządzenie znosi
  - Bezpieczny kanał i ścieżkę dla tzw. „oprogramowania niepublicznego”
- Pytania
  - Co to jest „oprogramowanie niepubliczne”?
  - Dlaczego jest z założenia bezpieczne?

# Fikcyjne bezpieczne urządzenie

- Zabezpieczenia znosi się dla oprogramowania niepublicznego:
  - *Oprogramowanie publiczne - oprogramowanie podpisujące, do którego w normalnych warunkach eksploatacji może mieć dostęp każda osoba fizyczna;*
  - *Oprogramowaniem publicznym **nie jest** w szczególności oprogramowanie używane w mieszkaniu prywatnym, lokalu biurowym lub telefonie komórkowym* (par 1 pkt 9 Rozporządzenia)
- Kuriozalne kryterium bezpieczeństwa
  - „Używanie w mieszkaniu prywatnym i biurze”
- Błędne kryterium bezpieczeństwa
  - Do komputera podłączonego do Internetu **ma dostęp** każda osoba fizyczna z każdego miejsca na świecie
  - Rozporządzenie nie mówi o „dostępie fizycznym” tylko o „dostępie”

# Fikcyjne bezpieczne urządzenie

- Konsekwencje „oprogramowania niepublicznego”
  - Podpis kwalifikowany można składać tylko przy pomocy:
    - Karty elektronicznej – OK.
    - **Aplikacji „zgodnej z Rozporządzeniem”**
  - W rezultacie regulacji Rozporządzenia
    - Centra certyfikacji musiały zaoferować „SSCD zgodne z Rozporządzeniem” czyli „jakąś aplikację”
  - Aplikacje zgodne z Rozporządzeniem
    - KIR SafeDevice, proCertum Sign, Signet Proofer, Sigillum Sign
    - Tylko pod Windows
    - Nie zapewniają ani bezpiecznego kanału ani ścieżki (niemożliwe pod Windows) - ale też nie muszą…
    - Wysoce nieużywalne i niezintegrowane z niczym (tylko „podpisz plik”)
    - To po co ich używać? Chyba, że nas zmuszą…
    - Nie zmusili, więc r**ynek zagłosował butami…**

# Fikcyjne bezpieczne urządzenie

- Czy „polskie SSCD” są przynajmniej bezpieczne?
  - **NIE!** Aplikacja działająca pod Windows pomimo najszczerszych chęci **nie może** być bezpieczna bez dodatkowych mechanizmów sprzętowych (TPM)
- Demonstracja praktyczna w październiku 2005
  - Firma G DATA pokazuje konia trojańskiego, który kryjąc się w Windows „podkłada” fałszywy dokument do podpisania
- Kłótnia o bezpieczeństwo „polskiego SSCD”
  - *G DATA nie zrozumiała Rozporządzenia*
  - *„Bezpieczny” to znaczy „bezpieczny w rozumieniu Rozporządzenia”* (Prawnik)
  - *Przecież można dopisywać do podpisanego dokumentu notatkę, o tym co jest w środku* (Informatyk)
  - *Użytkownik powinien sam sobie zabezpieczyć swoje SSCD* (Adam Słodowy???)
- Gwóźdź do trumny
  - *„Bezpieczne urządzenie służące do składania podpisu elektronicznego powinno (…)* ***nie zmieniać danych****, które mają zostać podpisane”* (art. 18 pkt 1 Ustawy)
  - **Nie może zmieniać i koniec - a zmieniło!**

# Fikcyjne bezpieczne urządzenie

- Rozwiązanie Problemu Bezpiecznego Urządzenia
  - Powrócić do definicji SSCD = karta elektroniczna
  - Co z bezpieczeństwem?
    - Ryzyko kradzieży klucza >> ryzyko jednorazowego fałszerstwa
    - Obowiązek korzystania z karty = wysokie bezpieczeństwo klucza prywatnego
    - Ryzykujemy tylko trudny technicznie (ale możliwy) atak trojana
  - Zezwolić na podpisywanie dowolnym oprogramowaniem
    - MS Office, Adobe Distiller, OpenOffice 2, Outlook, Lotus, Mozilla…
    - Godzimy się z ryzykiem stosowania popularnych systemów operacyjnych, ale robimy to w pełni świadomie
    - Radykalnie większa używalność
  - Być może wymóg stosowania „prawdziwego” SSCD (CWA 14169) dla niektórych transakcji - kryterium finansowe (limit), kryterium „ważności” (Niemcy)
- Jak to zrobili inni?
  - Czechy – bardzo liberalnie i pragmatycznie
    - Każdy trzyma klucz gdzie chce
    - Zostaje tylko funkcja weryfikacji tożsamości, ale co z niezaprzeczalnością?
  - Niemcy – restrykcyjnie ale bez udziwnień
    - SSCD to urządzenie CWA 14169
    - Bardzo małe wykorzystanie certyfikatów w skali kraju

# *Formaty podpisu elektronicznego*

czyli ile mamy tak naprawdę
podpisów elektronicznych w Polsce?

# Formaty podpisu elektronicznego

- Format podpisu elektronicznego
  - Format binarny, w którym zapisywany jest plik z podpisanym dokumentem
  - Wiele formatów ma wbudowany podpis (MS Word, XML OASIS OpenDocument, PDF…)
  - Podpis kwalifikowany ma specyficzne wymagania

Specyficzne wymagania = specyficzne formaty

- Jakie formaty są dopuszczone w Polsce?

# Formaty podpisu elektronicznego

- Rozporządzenie o warunkach technicznych
  - *Poświadczenia elektroniczne (…) powinny spełniać wymagania (…) określone w dokumentach (…) Specyfikacja techniczna ETSI TS 101 733 – Electronic Signature Format (…) specyfikacja techniczna ETSI TS 101 903 – XML Advanced Electronic Signature (XAdES), dokument PKCS#7, Cryptographic Message Syntax* (par. 30, ust. 1, pkt. 1 oraz par. 49, ust. 2, pkt 3,4,5 Rozporządzenia)
- A konkretnie:
  - ETSI TS 101 733, CMS (Cryptographic Message Syntax), binarny
  - PKCS#7, przodek CMS, binarny
  - ETSI TS 101 903, XAdES, format XML
- Ta lista jest rozszerzalna:
  - *W przypadku gdy bezpieczne urządzenie (…) stosuje inny format podpisu elektronicznego (…) podmiot świadczący usługi certyfikacyjne (…) format ten rejestruje i opatruje identyfikatorem obiektu zawartym w odpowiednim atrybucie podpisu.* (par. 30, ust. 2 Rozporządzenia)

# Formaty podpisu elektronicznego

**Co na to producenci?** (stan na styczeń 2006)

- Na trzy dopuszczone formaty firmy zastosowały… cztery!
  - Certum – **CMS**
  - KIR – **PKCS#7**
  - Signet – **XAdES**
  - Sigillum – SDOC (proprietary)
- Wszystkie cztery całkowicie niekompatybilne ze sobą
- Czy ktoś mówił coś o wzajemnej kompatybilności?

*„Należy wspierać współdziałanie produktów podpisu elektronicznego”*
Dyrektywa 1999/93/WE o podpisie elektronicznym

# Formaty podpisu elektronicznego

## Co na to rynek?

- „Podpis elektroniczny” czy „cztery podpisy czterech firm”?
- Scenariusze wymiany dokumentów z kontrahentami
  - Wysyłam w CMS, otrzymuję w CMS (jedna aplikacja)
  - Wysyłam w CMS, otrzymuję w PKCS#7 (dwie aplikacje)
    - Ups… obie aplikacje zawłaszczają rozszerzenie .SIG
  - Wysyłam w CMS, otrzymuję w PKCS#7 i XAdES (trzy aplikacje)
  - Wysyłam w CMS, otrzymuję w PKCS#7, XAdES i SDOC (cztery aplikacje)
- Gdzie motyw ekonomiczny i ergonomiczny do korzystania z podpisu?
- **Rynek znowu zagłosował butami**
- Wystarczyło się dogadać i zastosować **jeden** z dopuszczonych formatów!

# Formaty podpisu elektronicznego

- Rozwiązanie Problemu Formatów
  - **Narzucenie jednego określonego formatu tylko dla administracji**
  - Stworzy to standard *de facto* i zapewni wspólną platformę
  - Dla pozostałych zostawić tylko wymogi funkcjonalne bez wskazywania na konkretny format (firmy mogą mieć różne potrzeby)
- Pozostają pewne kwestie dyskusyjne związane z implementacją portali administracji publicznej…

# Formaty podpisu elektronicznego

- Jaki format do **publikacji**? Wiele przemawia za **XAdES**
  - Większość systemów przetwarzania dokumentów oparta o XML
  - Jedyny standard w wielu krajach Unii (Austria, Estonia)
  - Wydruk dokumentu zachowuje podpis elektroniczny (XML=ASCII)
  - Funkcje dla długoterminowej konserwacji podpisu (XAdES-A)
- Jaki format **przyjmować** od petentów?
  - W emailu standard *de facto* to S/MIME (PKCS#7)
  - Projekt e-Deklaracje oparty o portal WWW i XAdES – znowu problem czym podpisywać składane dokumenty?
  - Formaty MS Word, PDF i inne formalnie niekompatybilne z podpisem kwalifikowanym – czy S/MIME jest?
  - Brak satysfakcjunojącego rozwiązania
  - **Konieczne dalsze analizy żeby formalną poprawnością nie zabić używalności**

# Formaty podpisu elektronicznego

- Drobna niespójność w Ustawie o Informatyzacji
  - Rozporządzenie o warunkach technicznych wprowadza CMS, XAdES i PKC#7
  - „Rozporządzenie o minimalnych wymaganiach” wymienia jako format podpisu XML-Dsig
    - *XMLsig – XML Signature Syntax and Processing – Podpis elektroniczny dokumentów w formacie XML – W3C* (załącznik nr. 2, tablica A, pkt 1.2 Rozporządzenia)
  - XML-Dsig jest **podzbiorem** XAdES (brak mu rozszerzeń kwalifikowanych)
  - Właściwe byłoby wskazanie administracji XAdES, bo formalnie XML-Dsig nie nadaje się dla podpisu kwalifikowanego

# *Amerykańskie poświadczenie odbioru*

czyli gminny podpis za 30 tys. USD

# Amerykańskie poświadczenie odbioru

- Urząd odbiera dokument i generuje dla niego poświadczenie odbioru
  - Dowód doręczenia dla petenta
  - Wiążący prawnie
- „Rozporządzenie w sprawie warunków organizacyjno-technicznych doręczania dokumentów elektronicznych podmiotom publicznym”
  - *System teleinformatyczny (…) do wytworzenia urzędowego poświadczenia odbioru zawiera sprzętowy moduł bezpieczeństwa (Hardware Security Module) spełniający wymagania normy* ***FIPS 140-2*** *(…) poziom 3 lub wyższy, wydanej przez* ***National Institute of Standards and Technology*** *(NIST)* (załącznik, par. 1, pkt 1 Rozporządzenia)
- Dlaczego narzucono akurat normę wystawianą w USA?
  - Do ochrony informacji niejawnej dopuszcza się ITSEC i Common Criteria, certyfikowane choćby przez DBTI ABW i inne ośrodki w NATO
  - Rozporządzenie o warunkach technicznych wprost wskazuje na ITSEC i Common Criteria (par. 49, 1.4 i 2.2 Rozporządzenia)
- Realia rynkowe
  - Trzy urządzenia HSM spełniające FIPS 140-2 na świecie
  - Kilkanaście do kilkudziesięciu tys. USD za sztukę
- Czy budżety jednostek administracji są na to przygotowane?

# Amerykańskie poświadczenie odbioru

- Rozwiązania Problemu Poświadczenia Odbioru
  - **Dopuszczenie poziomów ITSEC i Common Criteria** równoważnych FIPS 140-2 poziom 3
  - Nadal pozostaje problem małych jednostek
    - Po co HSM, żeby poświadczać jeden dokument na miesiąc?
  - Rozwiązaniem jest **outsourcing** – i takie były zamierzenia…
  - …ale w Rozporządzeniu one zaginęły (wszędzie jest „urząd wystawia”)
  - Najtaniej **- dopuszczenie kwalifikowanego podpisu elektronicznego** w charakterze poświadczenia
    - Wymaga poprawienia definicji podpisu w Ustawie (oświadczenie woli zbędne, potrzebna autentyczność poświadczenia)

# *Chaos w administracji publicznej*

# Chaos w administracji publicznej

- 16. sierpnia 2006 jako Miecz Damoklesa
- Jednostki administracji chaotycznie poszukują rozwiązań zgodnych z aktualnym stanem prawnym
- Przykład z SIWZ: „zamawia się podpis elektroniczny zgodny z Ustawą o podpisie elektronicznym…”
- Aktualny stan prawny **uniemożliwia** zbudowanie normalnie działającego systemu

**Pieniądze wydane bez naprawienia podpisu będą pieniędzmi wyrzuconymi w błoto!**

# Chaos w administracji publicznej

- Brak wytycznych ze strony odpowiednich ministerstw
- Zapowiedzi nowelizacji bez konkretów
- Brak odpowiedzi na kluczowe pytanie: co z 16. sierpnia?

# Chaos w administracji publicznej

- Prawdopodobne Rozwiązania
  - Nowelizacja ustawy o podpisie elektronicznym i rozporządzeń
  - Zniesienie obowiązku stosowania SSCD (za: Marek Słowikowski, dyrektor Departamentu Informatyzacji MSWiA )
  - Odsunięcie terminu 16. sierpnia (nowelizacja + *vacatio legis*)

**Jeśli ministerstwa nie podadzą wytycznych jednostkom administracji, to będą one zmuszone wyrzucać pieniądze w błoto.**

**Decyzje konieczne są dzisiaj!**

# Zakończenie

- **Pytania? Paweł Krawczyk**
  - Tel.: 602-776959
  - Email: kravietz@post.pl
  - Aktualności i ta prezentacja: http://ipsec.pl/podpis_elektroniczny/
  - Stanowisko i rekomendacje Internet Society Polska: http://www.isoc.org.pl/

**Podziękowania**: Marcin Cieślak (ISOC-PL), Nicolas T. Courtois (Axalto), Wojciech S. Czarnecki (ISOC-PL), Józef Halbersztadt (ISOC-PL), Vizvary II Istvan (Cryptigo), Łukasz Jachowicz (RWO), Tomasz Kokowski (Politechnika Poznańska), Mirosław Kutyłowski (PWr), Dariusz Lewicki (Cryptotech), Zbigniew Łukasiak (ISOC-PL), Władysław Majewski (ISOC-PL), Sergiusz Pawłowicz (IT ZONE), Jacek Pokraśniewicz (Enigma SOI), Gerald Scheer (Utimaco), Piotr Waglowski (Vagla.pl), Reinhard Wobst, Polska Izba Informatyki i Telekomunikacji (PIIT)