

**Paweł Krawczyk**

# Interoperacyjność w praktyce

## Studium przypadku

### **GIODO (kwiecień 2009) – Elektroniczna Skrzynka Podawcza**

- Wymagania: Windows, Internet Explorer, uprawnienia administratora
- Elementarne problemy z obsługą typów plików
- Błędy w weryfikacji ścieżki certyfikacji w podpisie

### **UM Kraków (luty 2008) – Elektroniczna Skrzynka Podawcza**

- Wymagania: Windows, Internet Explorer, uprawnienia administratora
- Dokumenty przyjmuje w jednym formacie, zwraca w drugim, UPO w trzecim

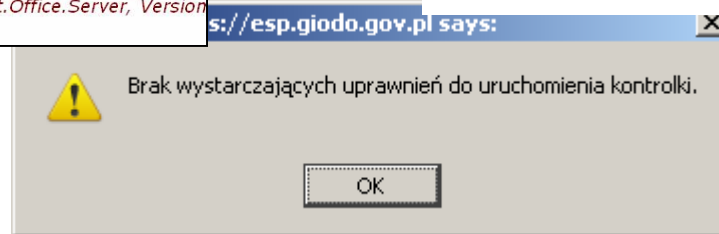
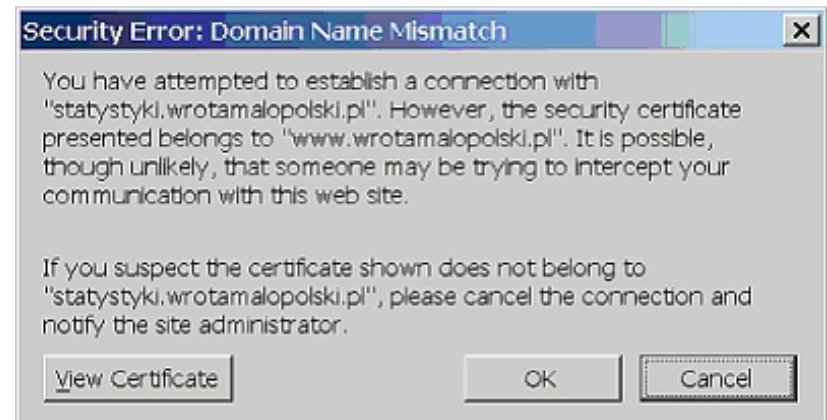
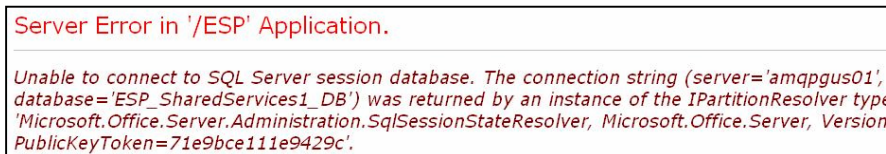
### **Formaty podpisanych dokumentów w Polsce**

- 2005 – 4 formaty, 2 częściowo kompatybilne
- 2008 – 14 formatów, 2 częściowo kompatybilne

## Studium przypadku

"A co do internetowej rejestracji firmy to kierowniczka nie ukrywa, że aby poprawnie wypełnić wniosek (dostępny na stronie [www.bialystok.pl](http://www.bialystok.pl)) trzeba być doskonale przygotowanym pod kątem ekonomicznym, ale i informatycznym."

Ewa Sokólska, „Jedno okienko i masa problemów”,  
Gazeta Wyborcza, 2009



## Dwa przykłady pozytywne

### E-Deklaracje

- „Specyfikacja wejścia-wyjścia” systemu e-Deklaracje (2008)
- Platforma testowa
- Darmowy program PITY 2008 obsługuje wysyłanie PIT z podpisem kwalifikowanym i bez podpisu (2009)

### Kompleksowy System Informatyczny ZUS

- Specyfikacja KSI MAIL ujawniona wyrokiem sądu z 2007 roku (d.i.p.)
- „Wymagania dla oprogramowania interfejsowego” EWD (2009)
- Platforma testowa

# Nos dla tabakiera, czy tabakiera dla nosa?

## Rok 1999 – nowe narzędzie

- ▣ Dyrektywa 1999/93/EC o podpisie elektronicznym (QES)
- ▣ Silne narzędzie do uwierzytelnienia osób fizycznych

## Lata 1999-2009

- ▣ Państwa Członkowskie bez skutku dostosowują problemy do narzędzia udostępnionego przez KE

## Część PCz daje sobie spokój z QES

- ▣ 2001 UK – Government Gateway
- ▣ 2005 Dania – OCES
- ▣ 2008 Polska zapowiada zaufany profil
- ▣ 2009 Polska – PIT-36 bez QES



## Jaki problem chcemy rozwiązać?

### Najlepiej wszystkie na raz

- Tak się nie da... Efekt taki jak obecnie

### Właściwy porządek pracy

1. Jaki mamy Problem? (koszty fakturowania? koszty papieru? poufność?)
2. Jakie mamy dla niego Rozwiązania?

### Czy jeden rozmiar może pasować wszystkim?

- Korzyść – jedno Rozwiązanie rozwiązuje wiele Problemów
- Ryzyko – Rozwiązanie może nie rozwiązywać żadnego z problemów skutecznie
- Ryzyko – konieczność dostosowania poziomu bezpieczeństwa do **najbardziej** wymagającej procedury (równanie w górę)

## Pytania kontrolne

- Czy to Rozwiązanie rzeczywiście zmniejsza dotkliwość Problemu?
- Czy to Rozwiązanie nie czyni Problemu jeszcze bardziej dotkliwym?

### Przykład

- Jaki problem *miał* rozwiązać podpis kwalifikowany w **ZUS** (nowelizacja 2005)?
- Skutki
  - Koszt dla przedsiębiorców ~32 mln zł rocznie
  - Koszt dostosowania KSI ZUS
  - Zamiast 1 certyfikatu „na firmę” konieczne kilka certyfikatów „na osobę”
  - Konieczny dodatkowy certyfikat atrybutu

# **Bezpieczeństwo jako czynnik kosztów i wykluczenia**

## **Racjonalne planowanie bezpieczeństwa**

# Czy „więcej bezpieczeństwa” oznacza „lepiej”?

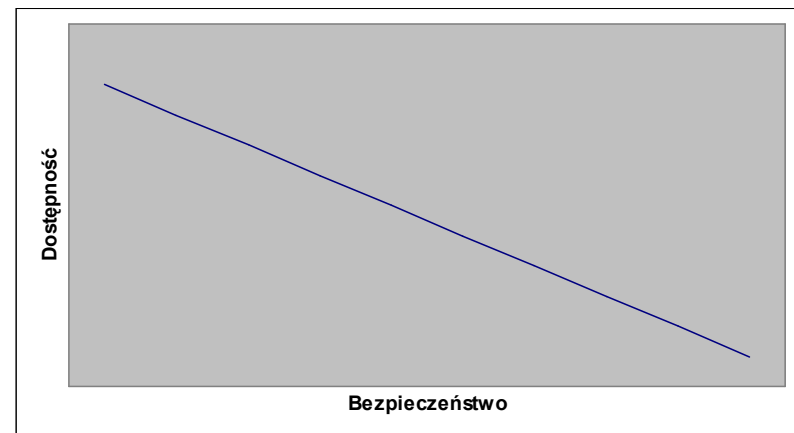
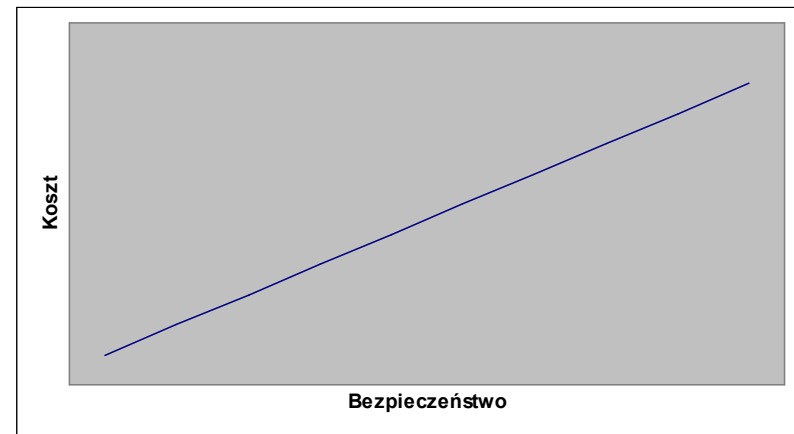
**Praktyka od 1999 roku – maksymalizacja siły mechanizmów bezpieczeństwa**

- ▣ E-faktura, dowód rejestracyjny samochodu, KPA, DIP, ZUS

**Wraz z wzrostem bezpieczeństwa**

- ▣ Rosną koszty inwestycyjne i operacyjne
- ▣ Maleje dostępność

**100% bezpieczeństwa = 0% działania**



# Konsekwencje nieuzasadnionego podnoszenia wymagań

## Niższa dostępność usług

- Ograniczenie prawa obywateli do usług publicznych
- Warunki progowe nieproporcjonalne do wagi procesu

## „Wysoki poziom bezpieczeństwa” – tylko na papierze

- „Bezpieczny w rozumieniu rozporządzenia”
- Niepodpisany PDF plus podpis kwalifikowany w oddzielnym pliku

## Gorszy zwrot z inwestycji (ROI)

- Koszt inwestycji / liczba beneficjentów

## W kwestii zwrotu z inwestycji

*„Brak zainteresowania elektronicznym podpisem widać również w Urzędzie Miasta. – W praktyce nikt z niego nie korzysta. W tym roku były może 3-4 korespondencje podpisane w ten sposób – zdradza Piotr Malcharek, dyrektor Wydziału Informatyki UMK. W Punkcie Obsługi Przedsiębiorcy z takiego rozwiązania korzysta średnio 5-10 przedsiębiorców miesięcznie.”*

Katarzyna Ponikowska, „Podpiszesz bez długopisu”, Echo Miasta Krakowa, 30 listopada 2009

*„Przez cztery lata na stworzenie biur RUM wydano ok. 200 mln zł (...) Największą kompromitacją okazał się centralny przetarg na sprzęt i oprogramowanie dla 300 szpitali, realizowany ze środków Banku Światowego. Dużą część tych środków po prostu zmarnowano, a resztę przeznaczono na zakup sprzętu, na którym później miały być zainstalowane systemy. Niestety, druga część przetargu dotycząca oprogramowania nie odbyła się do dziś, a sprzęt zakupiony jeszcze w 1995 r. zdążył się zestarzeć „*

Computerworld, "Paradoksy reformy", 6 grudzień 1999

# Poziom bezpieczeństwa musi wynikać z analizy ryzyka

## Dane wejściowe

- Wartość aktywu (skutku prawnego)
- Prawdopodobieństwo zdarzenia

## Procesy o różnej wadze skutków prawnych

- ❑ Różne poziomy ryzyka

## Jeśli gradacja poziomów ryzyka...

- ❑ ...to gradacja zabezpieczeń

# Gradacja zabezpieczeń w praktyce

	Klienci indywidualni	Bankowość korporacyjna
Profil użytkownika	Bardzo dużo średnich i małych klientów	Pewna liczba dużych klientów
Hasło dla logowania i autoryzacji transakcji	Podatne na phishing (ryzyko: klienci tracą pieniądze, bank traci klientów)	Podatne na phishing (ryzyko: klienci tracą pieniądze, bank traci klientów)
Hasło do logowania plus kod SMS	<u>Wystarczająco dobre dla większości klientów i dla banku</u>	Niewystarczający poziom bezpieczeństwa i niezaprzeczalności dla klienta i dla banku (ryzyko: klienci tracą pieniądze, bank traci klientów)
Token sprzętowy (hasła jednorazowe)	Nieuzasadniony koszt zarządzania tokenami ze strony banku do (ryzyko: bank traci pieniądze, frustracja klientów)	<u>Wystarczająco dobre rozwiązanie dla większości klientów. Zwiększona możliwość rozstrzygnięcia sporów przez bank (silna niezaprzeczalność)</u>
Kwalifikowany podpis elektroniczny	Nieuzasadniony koszt po stronie klienta, znaczny koszt zarządzania po stronie banku (ryzyko: klient nie zainwestuje pieniędzy i cierpliwości, zwiększone wymagania odnośnie systemu po stronie klienta)	<u>Rozwiązanie dobre dla klientów o zwiększonych potrzebach dotyczących bezpieczeństwa. Zwiększona możliwość rozstrzygnięcia sporów przez bank (silna niezaprzeczalność)</u>

## Studium przypadku

### Przykłady

- ▶ Płatność abonamentu RTV „przez Internet”
  - Po co dwukrotna wymiana korespondencji pocztą?
- ▶ E-deklaracje
  - PIT za 2007 – wymagany QES: <1000 deklaracji
  - PIT za 2008 – bez QES: >70 tys. deklaracji
    - > Zero postępowań o oszustwa lub „żarty”
- ▶ Weryfikacja poprawności danych w dowodzie rejestracyjnym
  - Po co uwierzytelnienie?

You can verify the validity of a VAT number issued by selecting that Member State from the drop-down and entering the number to be validated.

Member State *	<input type="text" value="PL-Poland"/>
VAT Number *	<input type="text" value="PL 9451335954"/>
Current Date	01/12/2009 (dd/mm/yyyy)
Requester Member State:	<input type="text" value="PL-Poland"/>
Requester VAT Number:	<input type="text" value="PL 9451335954"/>

## Zasady najlepszej praktyki

### Jaki konkretnie problem chcemy rozwiązać?

- Czy problem rzeczywiście istnieje?

### Dla kluczowych regulacji

- Rzetelna analiza ryzyka – jaki poziom regulacji jest wymagany?
- Rzetelna analiza kosztów i zysków – czy koszt regulacji nie przewyższy zysku?

### Nie traćmy z oczu celu biznesowego regulacji

- Jeśli dane rozwiązanie ma „ułatwiać i obniżać koszty”...
- ...to nie może ostatecznie utrudniać i podrażać
- „Z celowościowego punktu widzenia ma Pan rację ale...”

5. **Wpływ na konkurencyjność gospodarki i przedsiębiorczość,** w tym na funkcjonowanie przedsiębiorstw

Obowiązki związane z prowadzeniem działalności w obszarze gier hazardowych nie będą stanowić bezpośredniego zagrożenia **dla rozwoju branży.**

**Techniczne aspekty interoperacyjności**  
**Standardyzacja**  
**Formaty**

## Minimalne wymagania – kwestie techniczne

### Rozporządzenie o minimalnych wymaganiach do ustawy o informatyzacji

- Pomieszanie „najlepszych praktyk” z „minimalnymi wymaganiami”
- Problemem nie jest PDF 1.3 (formalnie niezgodny ale każdy go czyta)
  - Wsteczna kompatybilność jest powszechnym zjawiskiem
- Realne problemy dla interoperacyjności - formaty
  - PNG vs GIF (stare systemy)
  - OOXML vs DOC (stare pakiety biurowe)
  - DOC vs DOC (różne wersje MS Office)
  - ODF vs DOC (stare pakiety biurowe)
  - PDF w postaci bitmapy (niemożliwe przeszukiwanie i kopiowanie)
  - PDF z XFA („zbyt nowy PDF”)

## **Minimalne wymagania – kwestie techniczne**

### **Niektóre problemy dla interoperacyjności – elementy aktywne**

- Microsoft ActiveX (systemy inne niż Windows, uprawnienia, dziury)
- Sun Java (wersje, uprawnienia)
- Adobe Flash, Flex, Shockwave, RIA (wersje, systemy, uprawnienia, dziury)
- Adobe XFA (niby PDF, ale XFA)

### **Priorytet w wyborze rozwiązania**

- Patrz: „Jaki problem chcemy rozwiązać?”
- To problem determinuje wybór rozwiązania

# Od wymagań do wyboru platformy

## Więcej funkcji = mniej interoperacyjności

- Maksymalna interoperacyjność – HTML
- Średnia interoperacyjność – JavaScript
- Maksymalna funkcjonalność – Java, ActiveX

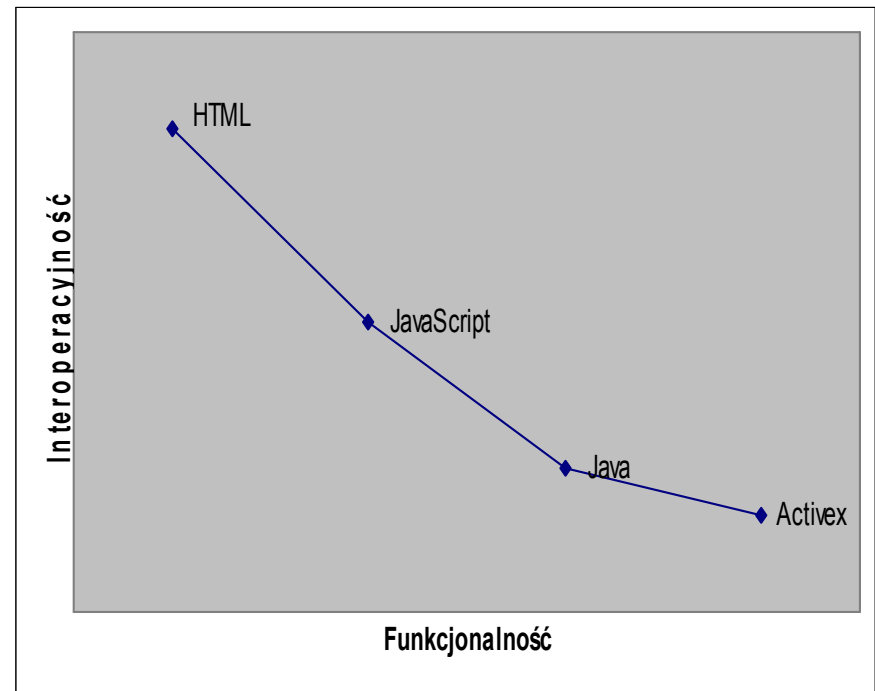
## Platforma determinuje interoperacyjność

- Lub jej brak...

## Podpis elektroniczny

- Nieuniknione użycie elementów aktywnych (Java, ActiveX)
- Efekt – problemy umiarkowane (Java) lub duże (ActiveX)

**Wniosek = im prostsze tym większa dostępność i niższy koszt**



# Propozycja – wymagania wobec systemów administracji

## ▣ Lista A – wymagane

- Zamknięty, wspólny mianownik gwarantujący interoperacyjną komunikację z administracją publiczną (G2B, G2C) w maksymalnym stopniu
- Możliwy audyt na zgodność

## ▣ Lista B – zalecane

- Ustabilizowane, sprawdzone standardy – kandydaci do listy A
- Możliwa ocena poziomu zgodności

## ▣ Lista C – tolerowane

- Wsteczna kompatybilność ze standardami *de facto* (RTF, Gadu-Gadu)
- Rozwiązania eksperymentalne (kandydaci do B)
- Rozwiązania dla zastosowań specjalnych (uzasadnione potrzebami biznesowymi)

## ▣ „Szara strefa” – zamiast nadregulacji

- Objąć rekomendacjami i najlepszymi praktykami

## **Obowiązkowy test interoperacyjności**

- 1. Złożyć wniosek w urzędzie A przez Internet**
- 2. Otrzymać od urzędu A dokument elektroniczny przez Internet**
- 3. Złożyć ten dokument w urzędzie B ze skutkiem prawnym**

### **Weryfikowane problemy**

- Kompatybilność formatów i systemów obiegu dokumentów
- Resortowość
- Referencyjność danych

### **Opcje dodatkowe**

- A - administracja centralna, B - samorząd
- A - podlega u.o.i., B - nie podlega u.o.i.

**Uzależnienie technologiczne**  
**Wymiana informacji**  
**Transparentność**

## **Długoterminowe problemy dla interoperacyjności**

- **Uzależnienie technologiczne**
- **Brak praw do aplikacji pisanych na wyłączny użytek administracji**
- **Brak dostępu do kodu źródłowego i specyfikacji w/w**
- **Radosna twórczość w zakresie formatów i standardów**
- **Konspiracja urzędowa**

## **Uzależnienie informatyczne w praktyce**

***„Uzależnienie zamawiającego od pierwotnego wykonawcy systemu lub producenta sprzętu lub oprogramowania gotowego uniemożliwiające nabycie niezbędnych usług lub dostaw w trybach konkurencyjnych„***

***„Zamówienia w trybie z wolnej ręki związane z systemami informatycznymi (...) skutkują wydatkowaniem wielomilionowych kwot rocznie, osiągając w skrajnych przypadkach poziom około 100 mln złotych rocznie wydatkowanych przez jednego zamawiającego”***

**„Rekomendacje udzielania zamówień publicznych na systemy informatyczne”,**

**Urząd Zamówień Publicznych, 2009**

## Ale polska branża IT ma określone zwyczaje...

***„Rekomendacje winny uwzględniać zwyczaje i specyfikę branży. Zwłaszcza branża technologii IT jest bardzo specyficzną, w której praktyki i zwyczaje handlowe dostawców rozwiązań informatycznych oraz producentów sprzętu odgrywają dużą rolę przy formułowaniu konkretnych postanowień umowy o udzielenie zamówienia publicznego”***

B. Tomaszewski, W.Pfadt,

„Rekomendacje dla zamówień publicznych na systemy IT”,

Computerworld, 6 listopada 2009

## Propozycje i zalecenia

### **Dla systemów pisanych na wyłączny użytek urzędu**

- Depozyt kodu źródłowego i dokumentacji technicznej systemu
- Przeniesienie praw majątkowych

### **Dla systemów możliwych do wykorzystania przez większą liczbę urzędów**

- Rozdzielenie zakupu systemu (patrz w/w) od zakupu usług jego instalacji i serwisowania
- Licencje typu „Government Purpose Rights” (GPR)
- Sens ekonomiczny zachowany także jeśli cena będzie wyższa

### **Dla systemów ogólnego przeznaczenia**

- Gwarancja możliwości migracji lub eksportu danych do jawnych i otwartych formatów
- Jawne i standardowe protokoły komunikacji (API)

## Ponowne wykorzystanie informacji wewnątrz administracji

- „Mit jednego systemu” (W. Drożdż, „Siedem mitów na temat rządowej informatyzacji”, 2009-10-5)
  - Nie chodzi o „zadekretowanie jednego systemu” dla wszystkich
- O co chodzi?
  - **Umożliwienie** skorzystania z wcześniej zakupionych dóbr jeśli ma to sens ekonomiczny i użytkowy
    - > Systemy i aplikacje dedykowane
    - > Opracowania, analizy, interpretacje, ekspertyzy
  - Ograniczenie wielokrotnego kupowania usług i produktów do wyłączonego użytku jednego urzędu

## Opracowania, analizy, ekspertyzy, interpretacje

### ▣ „Prywatyzacja” materiałów urzędowych

- „Wojna rowerowa” między Warszawą i Łodzią (wątek praw majątkowych)

### ▣ Konspiracja urzędowa

- Ile kosztował 5-letni proces ZUS z Sergiuszem Pawłowiczem o ujawnienie 15 stron specyfikacji KSI MAIL?

### ▣ Ignorowanie art. 4 ustawy prawo autorskie

### ▣ Nieracjonalne wydatkowanie środków publicznych

- opracowania na ten sam temat i o zbliżonej treści

**Pytania, komentarze**

**[pawel.krawczyk@hush.com](mailto:pawel.krawczyk@hush.com)**

## Europejskie Ramy Interoperacyjności – UP 2.2

### Subsidiarity and Proportionality:

„The proportionality principle limits EU actions to what is necessary to achieve agreed policy objectives.”

- ▣ Warunek – muszą być zdefiniowane cele
- ▣ Środki muszą być proporcjonalne do wagi celów

## Europejskie Ramy Interoperacyjności – UP 2.3

### User Centricity:

„Public services are provided to serve the needs of citizens and businesses.”

**Cel nadrzędny – interes użytkownika (obywatela i przedsiębiorcy)**

### Częste cele w praktyce

- Otrzymanie „darmowych” funduszy unijnych
- „Harmonizacja z przepisami unijnymi”

## Europejskie Ramy Interoperacyjności – UP 2.4

### Inclusion and Accessibility:

„The use of ICT should create equal opportunities for all citizens and businesses due to open, inclusive services that are publicly accessible without discrimination.”

## Europejskie Ramy Interoperacyjności – UP 2.5

### Security and Privacy

„public administrations must guarantee that the privacy of citizens and the confidentiality of information provided by businesses are respected (...) decide whether this information may be used for purposes other than those for which it was originally supplied.”

## Europejskie Ramy Interoperacyjności – UP 2.6

### Multilingualism:

„A trade-off is to be made between the expectation of citizens and businesses to be served in their own language(s) and the possibility of Member State public administrations to offer services in all official EU languages.”

„certain choices at the level of data representation may limit the possibilities to support different languages.”

**Ograniczenie nadmiernych zapędów egalitarnych?**

## Europejskie Ramy Interoperacyjności – UP 2.7

### Administrative Simplification:

„Businesses compile large amounts of information, often solely because of legal obligations, which is of no direct benefit for them and not necessary for achieving the objectives of the legislation imposing the obligations”

„Repeated requests by different administrations for the same information place a similar administrative burden on citizens who waste time compiling data and filling in forms with the same information over and over again.”

- Ograniczenie urzędowego apetytu na informacje
- Ograniczenie redundancji wynikającej z niedoskonałości procesów

## Europejskie Ramy Interoperacyjności – UP 2.8

### Transparency

„Citizens and businesses should be able to understand administrative processes. They should have the right to track administrative procedures that involve them, and have insight into the rationale behind decisions that could affect them.”

## Europejskie Ramy Interoperacyjności – UP 2.9

### Preservation of Information

„In order to guarantee long-term preservation of electronic records and other kinds of information, formats should be selected so as to ensure long-term accessibility, including preservation of associated electronic signatures and other electronic certifications, such as mandates.”

## Europejskie Ramy Interoperacyjności – UP 2.10

### Openness :

„Interoperability involves the sharing of information and knowledge between organisations, hence implies a certain degree of openness.”

„Recommendation 5. Public administrations should favour openness when working together to establish European Public Service while taking into account their priorities and constraints.”

## Europejskie Ramy Interoperacyjności – UP 2.11

### Reusability:

„Re-use means that public administrations confronted with a specific problem seek to benefit from the work of others by looking at what is available, assessing its usefulness or relevancy to the problem at hand, and decide to use solutions that have proven their value elsewhere.”

## Europejskie Ramy Interoperacyjności – UP 2.12

### Technological Neutrality and Adaptability:

„When establishing European Public Services, public administrations should focus on functional needs and defer decisions on technology as long as possible in order to avoid imposing specific technologies or products on their partners and to be able to adapt to the rapidly evolving technological environment.

Public administrations should render access to public services independent of any specific technology or product.”

## Europejskie Ramy Interoperacyjności – UP 2.13

### Effectiveness and Efficiency:

„Public administration should ensure that solutions serve businesses and citizens in the most effective and efficient way and provide the best value for taxpayer money.”

## UK versus Polska

Hi,

Sorry, it took me about 4 months of chasing our tax authorities to get that letter, so I can't release the original. Getting another one would be a ton of hassle.

Cheers

-----Original Message-----

From: Pawel Krawczyk

Sent: 23 November 2009 15:54

To:

Subject: RE: Pro license

Hello,

Were you able to send the paper version of certificate of fiscal residence by a chance?