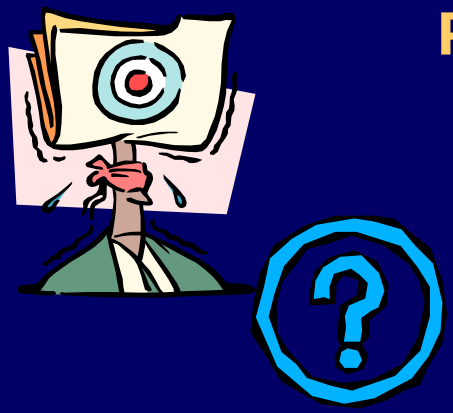


Prawna regulacja zasad zabezpieczania systemów teleinformatycznych

„Zabezpieczenie danych osobowych – aktualny stan prawny a rzeczywiste potrzeby”

Politechnika Warszawska

28 marca 2011 r.

dr Wojciech R. Wiewiórowski – WPiA Uniwersytet Gdański, Generalny Inspektor Ochrony Danych Osobowych

Nota:

Niniejsza prezentacja stanowi uzupełnienie wykładu prezentowanego podczas seminarium naukowego „Zabezpieczenie danych osobowych – aktualny stan prawny a rzeczywiste potrzeby” zorganizowanego przez Wydział Zarządzania Politechniki Warszawskiej oraz Stowarzyszenie Administratorów Bezpieczeństwa Informacji na Politechnice Warszawskiej w dniu 28 marca 2011 r.

Prezentację można kopiować i wykorzystywać w całości lub w części tylko pod warunkiem podania pełnej informacji o utworze w poniższym brzmieniu:

W.R.Wiewiórowski, „Prawna regulacja zasad zabezpieczania systemów teleinformatycznych ”, WPiA Uniwersytet Gdański 2011 (wersja z 20 marca 2011 r.)

© *W.R.Wiewiórowski*

Standard - wspólnie ustalone kryterium, które określa powszechne, zwykle najbardziej pożądane cechy czegoś, np. wytwarzanego przedmiotu czy ludzkiego zachowania

Zestaw parametrów, który zapewnia odpowiedni poziom jakości, bezpieczeństwa, wygody lub zgodności z innymi wytw

Polska Norma (oznaczana symbolem **PN**) - norma o zasięgu krajowym, przyjęta w drodze konsensu i zatwierdzona przez krajową jednostkę normalizacyjną Polski Komitet Normalizacyjny (PKN).

Normy PN są powszechnie dostępne, ale nie bezpłatne, zaś ich dystrybucję kontroluje PKN.

Normalizacja, standaryzacja

Działalność polegająca na analizowaniu wyrobów, usług i procesów w celu zapewnienia:

- racjonalizacji produkcji i usług poprzez stosowanie uznanych reguł technicznych lub rozwiązań organizacyjnych,
- usuwania barier technicznych w handlu i zapobieganie ich powstawaniu,
- zapewnienia ochrony życia, zdrowia, środowiska i interesu konsumentów oraz bezpieczeństwa pracy,
- poprawy funkcjonalności, kompatybilności i zamienności wyrobów, procesów i usług oraz regulowania ich różnorodności,
- zapewnienia jakości i niezawodności wyrobów, procesów i usług,
- działania na rzecz uwzględnienia interesów krajowych w normalizacji europejskiej i międzynarodowej,
- ułatwienia porozumiewania się przez określanie terminów, definicji, oznaczeń i symboli do powszechnego stosowania.

Wyniki tych analiz podawane są do publicznej wiadomości pod postacią norm lub przepisów technicznych.

Działalność zmierzająca do uzyskania optymalnego, w danych okolicznościach, stopnia uporządkowania w określonym zakresie, poprzez ustalenie postanowień przeznaczonych do powszechnego i wielokrotnego stosowania, dotyczących istniejących lub mogących wystąpić problemów

Ze względu na treść i obszar stosowania wyróżnia się następujące rodzaje norm

- normy podstawowe, które obejmują ogólne postanowienia dotyczące określonej dziedziny,
- normy terminologiczne obejmujące definicje terminów wraz z objaśnieniami,
- normy badań, w których zawarte są metody prowadzenia określonych badań,
- normy wyrobu lub usługi określające wymagania odnośnie konkretnego rodzaju wyrobu,
- normy procesu opisujące wymagania, które zapewnić mają funkcjonalność procesu,
- normy interfejsu, które określają wymagania odnośnie kompatybilności wyrobów w miejscach ich łączenia,
- normy danych, które zawierają wykazy cech, właściwości, które powinny zostać sparametryzowane w celu określenia wyrobu lub usługi.


EXPECTATIONS
REGULATIONS
REQUIREMENTS
COMPETITION
IT'S GAINING ON US!
NOW YOU UNDERSTAND WHAT CONTINUAL IMPROVEMENT IS ALL ABOUT!
ISO 9000
ISO 14000

Za główne powody obiekcji przed wpisywaniem rozwiązań o charakterze technicznym do aktów prawnych zawierających normy powszechnie obowiązujące należy zaliczyć:

- brak prawidłowych delegacji
- skomplikowany proces legislacyjny
- tendencję do tworzenia „standardów”, które „mogą łatwo ewoluować”

Prawdą jest jednakże, że ewentualne wpisywanie podobnych rozwiązań do treści aktów powszechnie obowiązujących wywołuje inne swoiste problemy.

Prawna regulacja zasad zabezpieczania systemów teleinformatycznych

Rozporządzenie o minimalnych wymaganiach dla systemów teleinformatycznych

§ 2. Systemy teleinformatyczne używane przez podmioty publiczne do realizacji zadań publicznych:

1) powinny spełniać właściwości i cechy w zakresie funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, określone w normach ISO zatwierdzonych przez krajową jednostkę normalizacyjną, na etapie projektowania, wdrażania i modyfikowania tych systemów;

2) powinny zostać wyposażone w składniki sprzętowe i oprogramowanie:

a) umożliwiające wymianę danych z innymi systemami teleinformatycznymi używanymi do realizacji zadań publicznych za pomocą protokołów komunikacyjnych i szyfrujących określonych w załączniku nr 1 do rozporządzenia, stosownie do zakresu działania tych systemów,

b) zapewniające dostęp do zasobów informacji udostępnianych przez systemy teleinformatyczne używane do realizacji zadań publicznych przy wykorzystaniu formatów danych określonych w załączniku nr 2 do rozporządzenia.

2. Przy opracowywaniu polityki bezpieczeństwa, o której mowa w ust. 1, podmiot publiczny powinien uwzględniać postanowienia Polskich Norm z zakresu bezpieczeństwa informacji.

PROTOKOŁY KOMUNIKACYJNE I SZYFRUJĄCE UMOŻLIWIAJĄCE WYMIANĘ DANYCH Z INNYMI SYSTEMAMI TELEINFORMATYCZNYMI UŻYWANYMI DO REALIZACJI ZADAŃ PUBLICZNYCH

Lp.	Nazwa skrócona protokołu oraz jego wersja	Oryginalna pełna nazwa protokołu	Opis protokołu	Organizacja określająca normę lub standard	Nazwa normy, standardu lub dokumentu normalizacyjnego albo standaryzacyjnego
1	2	3	4	5	6
1.	**Do wymiany danych z systemami teleinformatycznymi stosuje się co najmniej jeden z następujących protokołów:**				
1.1	IP wersja 4	Internet Protocol	Protokół komunikacyjny dla Internetu	IETF	RFC 0791
1.2	TCP	Transmission Control Protocol	Strumieniowy protokół komunikacyjny	IETF	RFC 0793
1.3	UDP	User Datagram Protocol	Datagramowy protokół użytkownika	IETF	RFC 0768
1.4	ICMP	Internet Control Message Protocol	Protokół komunikatów kontrolnych Internetu	IETF	RFC 0792
1.5	HTTP wersja 1.1	Hypertext Transfer Protocol	Protokół komunikacyjny sieci WWW	IETF	RFC 2616

RFC 2616

Prawna regulacja zasad zabezpieczania systemów teleinformatycznych

Załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

A. Środki bezpieczeństwa na poziomie podstawowym

I

1. Obszar, o którym mowa w § 4 pkt 1 rozporządzenia, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
2. Przebywanie osób nieuprawnionych w obszarze, o którym mowa w§ 4 pkt 1rozporządzenia, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

II

1. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.
2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:

a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;
b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

III

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

Prawna regulacja zasad zabezpieczania systemów teleinformatycznych

IV

1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 6 znaków.
3. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.
4. Kopie zapasowe:

a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;

b) usuwa się niezwłocznie po ustaniu ich użyteczności.

V

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, o którym mowa w § 4 pkt 1 rozporządzenia, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

VI

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

1) likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;

2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;

3) naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

VII

Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego.

Prawna regulacja zasad zabezpieczania systemów teleinformatycznych

B. Środki bezpieczeństwa na poziomie podwyższonym

VIII

W przypadku gdy do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

IX

Urządzenia i nośniki zawierające dane osobowe, o których mowa w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przekazywane poza obszar, o którym mowa w § 4 pkt 1rozporządzenia, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

X

Instrukcja zarządzania systemem informatycznym, o której mowa w § 5rozporządzenia, rozszerza się o sposób stosowania środków, o których mowa w pkt IX załącznika.

XI

Administrator danych stosuje na poziomie podwyższonym środki bezpieczeństwa określone w części A załącznika, o ile zasady zawarte w części B nie stanowią inaczej.

C. Środki bezpieczeństwa na poziomie wysokim

XII

1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 1, obejmują one:
a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;
b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

XIII

Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

XIV

Administrator danych stosuje na poziomie wysokim środki bezpieczeństwa, określone w części A i B załącznika, o ile zasady zawarte w części C nie stanowią inaczej.

Prawna regulacja zasad zabezpieczania systemów teleinformatycznych

ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 25 sierpnia 2005 r.
w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego
(…)
Podstawowe wymagania bezpieczeństwa teleinformatycznego
§ 3. 1. Bezpieczeństwo teleinformatyczne zapewnia się, chroniąc informacje przetwarzane w systemach i sieciach teleinformatycznych przed utratą właściwości gwarantujących to bezpieczeństwo, w szczególności przed utratą poufności, dostępności i integralności.
2. Bezpieczeństwo teleinformatyczne zapewnia się przed rozpoczęciem oraz w trakcie przetwarzania informacji niejawnych w systemie lub sieci teleinformatycznej.

§ 4. Za właściwą organizację bezpieczeństwa teleinformatycznego odpowiada kierownik jednostki organizacyjnej, który w szczególności:
1) zapewnia opracowanie dokumentacji bezpieczeństwa teleinformatycznego;
2) realizuje ochronę fizyczną, elektromagnetyczną i kryptograficzną systemu lub sieci teleinformatycznej;
3) zapewnia niezawodność transmisji oraz kontrolę dostępu do urządzeń systemu lub sieci teleinformatycznej;
4) dokonuje analizy stanu bezpieczeństwa teleinformatycznego oraz zapewnia usunięcie stwierdzonych nieprawidłowości;
5) zapewnia przeszkolenie z zakresu bezpieczeństwa teleinformatycznego dla osób uprawnionych do pracy w systemie lub sieci teleinformatycznej;
6) zawiadamia właściwą służbę ochrony państwa o zaistniałym incydencie bezpieczeństwa teleinformatycznego dotyczącym informacji niejawnych oznaczonych co najmniej klauzulą *„poufne”*.

Prawna regulacja zasad zabezpieczania systemów teleinformatycznych

§ 5. Ochrona fizyczna systemu lub sieci teleinformatycznej polega na:
1) umieszczeniu urządzeń systemu lub sieci teleinformatycznej w strefie bezpieczeństwa, strefie administracyjnej lub specjalnej strefie bezpieczeństwa, zwanych dalej *„strefą kontrolowanego dostępu”* w zależności od:
a) klauzuli tajności,
b) ilości,
c) zagrożeń dla poufności, integralności lub dostępności
- informacji niejawnych;
2) zastosowaniu środków zapewniających ochronę fizyczną, w szczególności przed:
a) nieuprawnionym dostępem,
b) podglądem,
c) podsłuchem.

§ 6. 1. Ochrona elektromagnetyczna systemu lub sieci teleinformatycznej polega na niedopuszczeniu do utraty poufności i dostępności informacji niejawnych przetwarzanych w urządzeniach teleinformatycznych.

2. Utrata poufności następuje w szczególności na skutek wykorzystania elektromagnetycznej emisji ujawniającej pochodzącej z tych urządzeń.

3. Utrata dostępności następuje w szczególności na skutek zakłócania pracy urządzeń teleinformatycznych za pomocą impulsów elektromagnetycznych o dużej mocy.

4. Ochronę elektromagnetyczną systemu lub sieci teleinformatycznej zapewnia się w szczególności przez umieszczenie urządzeń teleinformatycznych, połączeń i linii w strefach kontrolowanego dostępu spełniających wymagania w zakresie tłumienności elektromagnetycznej odpowiednio do wyników szacowania ryzyka dla informacji niejawnych, o którym mowa w § 12, lub zastosowanie odpowiednich urządzeń teleinformatycznych, połączeń i linii o obniżonym poziomie emisji lub ich ekranowanie z jednoczesnym filtrowaniem zewnętrznych linii zasilających i sygnałowych.

Rozporządzenie w sprawie niezbędnych elementów struktury dokumentów elektronicznych wydane na podstawie art. 5 ust. 2a ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach

§ 2. 1. Metadanymi w rozumieniu rozporządzenia jest zestaw logicznie powiązanych z dokumentem elektronicznym usystematyzowanych informacji opisujących ten dokument, ułatwiających jego wyszukiwanie, kontrolę, zrozumienie i długotrwałe przechowanie oraz zarządzanie.

2. Niezbędnymi elementami struktury dokumentów elektronicznych są następujące metadane:

1) identyfikator - jednoznaczny w danym zbiorze dokumentów znacznik dokumentu, który umożliwia jego identyfikację;
2) twórca - podmiot odpowiedzialny za treść dokumentu, z podaniem jego roli w procesie tworzenia lub akceptacji dokumentu;
3) tytuł - nazwa nadana dokumentowi;
4) data - data zdarzenia związanego z tworzeniem dokumentu;
5) format - nazwa formatu danych zastosowanego przy tworzeniu dokumentu;
6) dostęp - określenie komu, na jakich zasadach i w jakim zakresie można udostępnić dokument;
7) typ - określenie podstawowego typu dokumentu (np. tekst, dźwięk, obraz, obraz ruchomy, kolekcja) w oparciu o listę typów Dublin Core Metadata Initiative i jego ewentualne dookreślenie (np. prezentacja, faktura, ustawa, notatka, rozporządzenie, pismo);

Dublin Core® Metadata Initiative

ABOUT THE INITIATIVE | DOCUMENTS | GROUPS | RESOURCES
DCMI NEWS | TOOLS AND SOFTWARE | PROJECTS

Home > Documents > Dcmi-terms >

Enter keyword Search

DCMI Metadata Terms

Title: DCMI Metadata Terms
Creator: DCMI Usage Board
Identifier: http://dublincore.org/documents/2008/01/14/dcmi-terms/
Date Issued: 2008-01-14
Latest Version: http://dublincore.org/documents/dcmi-terms/
Replaces: http://dublincore.org/documents/2006/12/18/dcmi-terms/
Translations: http://dublincore.org/resources/translations/
Document Status: This is a DCMI Recommendation.
Description: This document is an up-to-date specification of all metadata terms maintained by the Dublin Core Metadata Initiative, including properties, vocabulary encoding schemes, syntax encoding schemes, and classes.

Table of Contents

Index of Terms

Properties in the */terms/* namespace	abstract, accessRights, accrualMethod, accrualPeriodicity, accrualPolicy, alternative, audience, available, bibliographicCitation, conformsTo, contributor, coverage, created, creator, date, dateAccepted, dateCopyrighted, dateSubmitted, description, educationLevel, extent, format, hasFormat, hasPart, hasVersion, identifier, instructionalMethod, isFormatOf, isPartOf, isReferencedBy, isReplacedBy, isRequiredBy, issued, isVersionOf, language, license, mediator, medium, modified, provenance, publisher, references, relation, replaces, requires, rights, rightsHolder, source, spatial, subject, tableOfContents, temporal, title, type, valid

http://dublincore.org/documents/dcmi-terms/

Section 7: DCMI Type Vocabulary

Term Name: Collection	
URI:	http://purl.org/dc/dcmitype/Collection
Label:	Collection
Definition:	An aggregation of resources.
Comment:	A collection is described as a group; its parts may also be separately described.
Type of Term:	Class
Member Of:	http://purl.org/dc/terms/DCMIType
Version:	http://dublincore.org/usage/terms/history/#Collection-003
Term Name: Dataset	
URI:	http://purl.org/dc/dcmitype/Dataset
Label:	Dataset
Definition:	Data encoded in a defined structure.
Comment:	Examples include lists, tables, and databases. A dataset may be useful for direct machine processing.
Type of Term:	Class
Member Of:	http://purl.org/dc/terms/DCMIType
Version:	http://dublincore.org/usage/terms/history/#Dataset-003
Term Name: Event	
URI:	http://purl.org/dc/dcmitype/Event
Label:	Event
Definition:	A non-persistent, time-based occurrence.
Comment:	Metadata for an event provides descriptive information that is the basis for discovery of the purpose, location, duration, and responsible agents associated with an event. Examples include an exhibition, webcast, conference, workshop, open day, performance, battle, trial, wedding, tea party, conflagration.
Type of Term:	Class
Member Of:	http://purl.org/dc/terms/DCMIType
Version:	http://dublincore.org/usage/terms/history/#Event-003

ROZPORZĄDZENIE MINISTRA FINANSÓW

w sprawie struktury logicznej zgłoszeń,

sposobu ich przesyłania

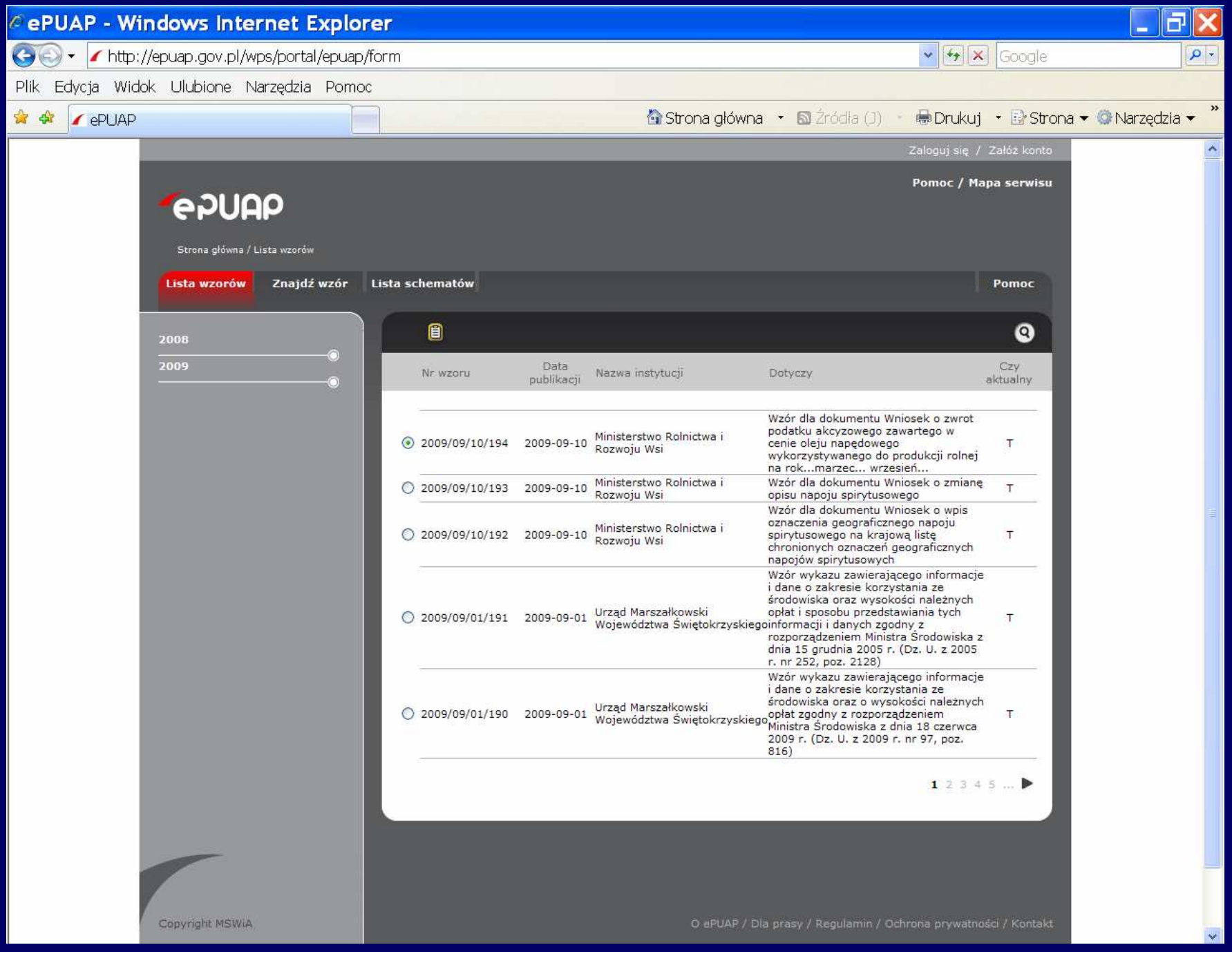
oraz rodzajów podpisu elektronicznego,

którymi powinny być opatrzone

Nazwa pliku XSD:
http://e-deklaracje.mf.gov.pl/Repozytorium/Definicje/ElementarneTypyDanych_v2-0.xsd

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified" version="1.0" xml:lang="PL">
        <xsd:include schemaLocation="http://e-deklaracje.mf.gov.pl/Repozytorium/Slowniki/KodyUrzedowSkarbowych_v2-
0.xsd"/>
        <xsd:include schemaLocation="http://e-deklaracje.mf.gov.pl/Repozytorium/Slowniki/KodyKrajow_v3-0.xsd"/>
        <xsd:annotation>
                <xsd:documentation>Definicje podstawowych typów używanych w deklaracjach elektronicznych. Na
podstawie poniższych typów można budować deklaracje</xsd:documentation>
        </xsd:annotation>
        <xsd:simpleType name="TZnakowy">
                <xsd:annotation>
                        <xsd:documentation>Typ znakowy ograniczony do jednej linii</xsd:documentation>
                </xsd:annotation>
                <xsd:restriction base="xsd:normalizedString">
                        <xsd:minLength value="1"/>
                        <xsd:maxLength value="240"/>
                        <xsd:whiteSpace value="replace"/>
                </xsd:restriction>
        </xsd:simpleType>
        <xsd:simpleType name="TTekstowy">
                <xsd:annotation>
                        <xsd:documentation>Typ znakowy ograniczony do 3500 znaków</xsd:documentation>
                </xsd:annotation>
                <xsd:restriction base="xsd:string">
                        <xsd:minLength value="1"/>
                        <xsd:maxLength value="3500"/>
                </xsd:restriction>
        </xsd:simpleType>
        <xsd:simpleType name="TProcentowy">
                <xsd:annotation>
                        <xsd:documentation>Wartość procentowa z dokładnością do 2 miejsc po
przecinku</xsd:documentation>
                </xsd:annotation>
                <xsd:restriction base="xsd:decimal">
                        <xsd:totalDigits value="5"/>
                        <xsd:fractionDigits value="2"/>
                        <xsd:minInclusive value="0"/>
                        <xsd:maxInclusive value="100"/>
                        <xsd:whiteSpace value="collapse"/>
                </xsd:restriction>
        </xsd:simpleType>
        <xsd:simpleType name="TCalkowity">
                <xsd:annotation>
                        <xsd:documentation>Liczby naturalne</xsd:documentation>
                </xsd:annotation>
                <xsd:restriction base="xsd:int">
                        <xsd:whiteSpace value="collapse"/>
                        <xsd:totalDigits value="14"/>
                </xsd:restriction>
        </xsd:simpleType>
        <xsd:simpleType name="TNaturalny">
```

Prawna regulacja zasad zabezpieczania systemów teleinformatycznych



I tym optymistycznym akcentem

kończąc

zachęcam do zadawania pytań