



Standardy

## Ramy prawne

Wymagania minimalne dla systemów teleinformatycznych podmiotów publicznych określone są w tzw. **Krajowych Ramach Interoperacyjności**. Jest to rozporządzenie wydane na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tj. Dz.U.2017.0.2247)

# Wymagania dla systemów teleinformatycznych

## Rozdział IV rozporządzenia plus załączniki do rozporządzenia

- Specyfikacja formatów danych oraz protokołów komunikacyjnych i szyfrujących, które mają być stosowane w oprogramowaniu interfejsowym
- Sposoby zapewnienia bezpieczeństwa przy wymianie informacji
- Standardy techniczne zapewniające wymianę informacji z udziałem podmiotów publicznych z uwzględnieniem wymiany transgranicznej
- Sposoby zapewnienia dostępu do zasobów informacji podmiotów publicznych dla osób niepełnosprawnych

# Interoperacyjność

Rozwiązania na poziomie organizacyjnym, semantycznym i technologicznym

- dobór środków, metod i standardów wykorzystywanych w systemach teleinformatycznych
- dobór norm, standardów i rekomendacji na wszystkich poziomach interoperacyjności
- zachowanie zasady neutralności technologicznej

Podsumowując: standaryzacja, informowanie, efektywność kosztowa.

Powinny je stosować wszystkie podmioty realizujące zadania publiczne z użyciem systemów teleinformatycznych



# Minimalne wymagania dla systemów teleinformatycznych

Określają zasady, którymi należy się kierować przy doborze systemów teleinformatycznych

# Minimalne wymagania dla systemów teleinformatycznych

## Zarządzanie usługami

- projektowanie, wdrażanie i eksploatawanie systemów teleinformatycznych przy zastosowaniu norm, standardów i metodyk
- PN-ISO/IEC 20000 – technika informatyczna – zarządzanie usługami

## Wymiana danych pomiędzy systemami

- przepisy, normy, standardy, rekomendacje polskie lub unijne (PKN / CEN)
- Internet Engineering Task Force (IETF) – Request For Comments (RFC)
- World Wide Web Consortium (W3C) – W3C Recommendation (REC)

# Minimalne wymagania dla systemów teleinformatycznych – RFC

Network Working Group  
Request for Comments: 2606  
BCP: 32  
Category: Best Current Practice

D. Eastlake  
A. Panitz  
June 1999

## Reserved Top Level DNS Names

### Status of this Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

### Copyright Notice

Copyright (C) The Internet Society (1999). All Rights Reserved.

### Abstract

To reduce the likelihood of conflict and confusion, a few top level domain names are reserved for use in private testing, as examples in documentation, and the like. In addition, a few second level domain names reserved for use as examples are documented.

### Table of Contents

<a href="#">1. Introduction.....</a>	<a href="#">1</a>
<a href="#">2. TLDs for Testing, &amp; Documentation Examples.....</a>	<a href="#">2</a>
<a href="#">3. Reserved Example Second Level Domain Names.....</a>	<a href="#">2</a>
<a href="#">4. IANA Considerations.....</a>	<a href="#">3</a>
<a href="#">5. Security Considerations.....</a>	<a href="#">3</a>
<a href="#">References.....</a>	<a href="#">3</a>
<a href="#">Authors' Addresses.....</a>	<a href="#">4</a>
<a href="#">Full Copyright Statement.....</a>	<a href="#">4</a>

### 1. Introduction

The global Internet Domain Name System is documented in [RFC 1034, 1035, 1591] and numerous additional Requests for Comment. It defines a tree of names starting with root, ".", immediately below which are top level domain names such as ".com" and ".us". Below top level domain names there are normally additional levels of names.

Status: Best Current Practice  
Updates: [7519](#)  
See Also: [BCP 225](#)  
More info: [Datatracker](#) | [IPR](#) | [Info page](#)

Stream: Internet Engineering Task Force (IETF)  
RFC: [8725](#)  
BCP: 225  
Updates: [7519](#)  
Category: Best Current Practice  
Published: February 2020  
ISSN: 2070-1721  
Authors: Y. Sheffer D. Hardt M. Jones  
*Intuit* *Microsoft*

## RFC 8725 JSON Web Token Best Current Practices

### Abstract

JSON Web Tokens, also known as JWTs, are URL-safe JSON-based security tokens that contain a set of claims that can be signed and/or encrypted. JWTs are being widely used and deployed as a simple security token format in numerous protocols and applications, both in the area of digital identity and in other application areas. This Best Current Practices document updates RFC 7519 to provide actionable guidance leading to secure implementation and deployment of JWTs.

### Status of This Memo

This memo documents an Internet Best Current Practice.



# Minimalne wymagania dla systemów teleinformatycznych

## Kodowanie znaków

- UTF-8 (ISO/IEC 10646)
- UTF-16 (dopuszczone w uzasadnionych przypadkach)

## Formaty danych

- formaty plików, rodzaje podpisów elektronicznych, standardy dla stron internetowych
- załączniki do rozporządzenia





# Minimalne wymagania dla systemów teleinformatycznych

## Zapewnienie dostępności danych

- ułatwienia dostępu
- WCAG 2.1 AA

## System zarządzania bezpieczeństwem informacji

- zapewnia poufność, dostępność i integralność informacji
- PN-ISO/IEC 27000 – system zarządzania bezpieczeństwem informacji

# Minimalne wymagania dla systemów teleinformatycznych

## Zapewnienie bezpieczeństwa w systemach teleinformatycznych

- Dbłość o aktualizację oprogramowania
- Minimalizowanie ryzyka utraty informacji w wyniku awarii
- Ochrona przed błędami, utratą, nieuprawnioną modyfikacją
- Stosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa
- Zapewnienie bezpieczeństwa plików systemowych
- Redukcja ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych
- Niezwłoczne podejmowanie działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa
- Kontrola zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa

# Minimalne wymagania dla systemów teleinformatycznych

## Rozliczalność w systemach teleinformatycznych

- logowanie zdarzeń (konto administracyjne, konfiguracja systemu, informacje chronione)
- przechowywanie logów (2 lata jeżeli nie jest to określone w innych przepisach)



# Zapewnienie bezpieczeństwa teleinformatycznego – niezbędne elementy

Zaangażowanie w proces kierownictwa organizacji

Wyznaczenie komórki organizacyjnej do realizacji wcześniej wymienionych zadań

(dedykowany zespół informatyków, zespół bezpieczeństwa, dedykowana osoba lub wynajęta firma)