PANEL DYSKUSYJNY

19.07.2021

SZYFROWANIE – skuteczny sposób na zabezpieczenie danych ?

TECHNICZNE i FORMALNO PRAWNE

aspekty szyfrowania i uwierzytelniania

UNIWERSYTET ZIELONOGÓRSKI

J.Jablonski@wmie.uz.zgora.pl

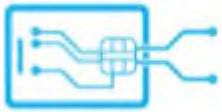
Kryptografia dla … cyber-bezpieczeństwa

Przykład – wykorzystanie certyfikatów SSL/TLS

SZYFROWANIE – skuteczny sposob na zabezpieczenie danych ?

URZĄD OCHRONY DANYCH OSOBOWYCH

Podatności i zalecenia wg. ISO/IEC 29115

Mechanizmy uwierzytelniania	Metody Kryptograficzne	Podatności	Zalecenia
 Hasła statyczne i maskowalne	Kryptografia asymetryczna AES(Adwanced Encryption Standard)	Phishing,	Wdrażanie kryptografii z kluczami jednorazowymi
 Aplikacje mobilne Blik, tPro Comarch Adres e-mail SMS, QRCode		Atak Man In The Middle	
		Atak Man In The Browser	
 sprzętowe tokeny kryptograficzne RSA i ECC	Kryptografia symetryczna ECC, RSA	Atak na dane uwierzytelniające	
 Smart-Cards RSA i ECC		Kradzież tożsamości	Poszukiwanie algorytmów o cechach Quantum Resists
 Tokeny OTP PRNG, RNG	Funkcje skrótu SHA (Secure Hash Algorithm)	Ataki powtórzeniowe	
		Kryptoanaliza	
 Certyfikaty X.509 LDAP, KERBEROS		Quantum Computing	
	PBKDF (Password –Based Key Derivation Function		

URZĄD OCHRONY DANYCH OSOBOWYCH

SZYFROWANIE – skuteczny sposób na zabezpieczenie danych ?

Cyfryzacja i bezpieczeństwo - wczoraj, dziś, jutro …

poufność
dostępność
rozliczalność
niezaprzeczalność

bezpieczeństwo danych ?

- RODO (UE) 2016/679 z dnia 27-04-2016r.
- ROZPORZĄDZENIE (UE) 2014/910 z dnia 8.09.2015 r
- ROZPORZĄDZENIE (UE) 2015/1502 z dnia 8.09.2015 r
- KNF rekomendacje z FIPS 140 L2, SecuRePay i 2FA

NSA, FIPS, NIST, ENISA poziom bezpieczeństwa 128bitów do 2023r ?

Uwierzytelnianie dostępu do e-usług – czyli danych

URZĄD OCHRONY DANYCH OSOBOWYCH

SZYFROWANIE – skuteczny sposób na zabezpieczenie danych ?

Poziom bezpieczeństwa ?

wiadomość

A L A M A K O T A

$k = 3$

szyfrogram

D O D P D N R W D

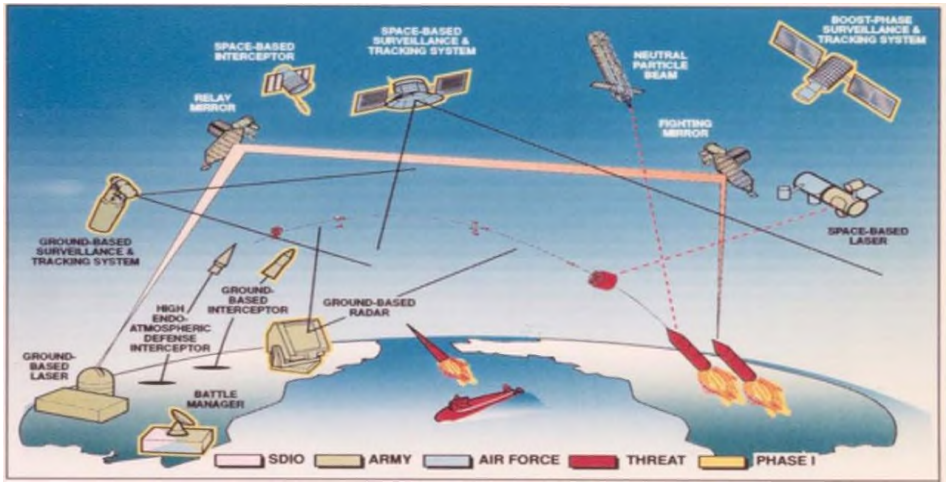
$$s_i(w_i)_k = (w_i + k) \bmod n$$

$$k \in \{1 \ldots n\} \; gdzie \; \underline{\boldsymbol{n}} < 2^5$$

$$w_i(s_i)_k = (s_i - k) \bmod n$$

k	w_0	w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8
0	D	O	D	P	D	N	R	W	D
-1	C	N	C	O	C	M	Q	V	C
-2	B	M	B	N	B	L	P	U	B
-3	A	L	A	M	A	K	O	T	A
-5	Y	J	Y	K	Y	I	M	R	Y
...	....								
-23	G	R	G	S	G	Q	U	Z	G

3



ENISA zaleca poziom bezpieczeństwa 128 do 2023r ?

… może być bezpieczniej – kryptografia z kluczami jednorazowymi

Teoria Shannona, Twierdzenie Bayes'a

Założenie i dowód dyskrecji doskonałej:

$s_i\,(w_i)_k = (w_i + k_i) \bmod n$

$K = 3$

$w_i\,(s_i)_k = (s_i -$

$p(S = s_i) =$

Jeżeli $|W| = |$ są z $p = 1/|K|$

or

dla każdej w_i k_i taki, że $s_i = f_k(w_i)$

szyfrogram

P	S	L	P	D	K	R	C	X
D	O	D	P	D	N	R	W	D
S	J	Y	F	M	O	A	I	M

{19,14,17,7,25,0,9,20,3

{3,?

,14,10,11,17,13,24,24,19}

$K_i = ?$

komunikat

K	A	M	I	E	N	I	C	A
A	L	A	M	A	K	O	T	A
M	A	T	E	M	A	T	Y	K

Wiadomość?

Jak generować i bezpiecznie wymieniać się kluczami … ?

Bezpieczeństwo danych i usługi zaufania

RODO, PSD2, Fintech …

ISAP
Internetowy System Aktów Prawnych

Baza Internetowy System Aktów Prawnych - ISAP zawiera opisy bibliograficzne i teksty aktów prawnych opublikowanych w wydawnictwach urzędowych: Dzienniku Ustaw oraz Monitorze Polskim, wydawanych przez Prezesa Rady Ministrów.

ePUAP
ELEKTRONICZNA PLATFORMA USŁUG ADMINISTRACJI PUBLICZNEJ

Uwaga!

Nie dokonujemy wyszukiwania na zamówienie, a jedynie udostępniamy swoje zasoby. Nie interpretujemy obowiązujących przepisów jak również nie udzielamy wyjaśnień w sprawach związanych z ich stosowaniem.

Dz.U. 2018 poz. 1760

Dziennik Ustaw / 2018 / poz. 1760

Rozporządzenie Ministra Cyfryzacji z dnia 10 września 2018 r. w sprawie profilu zaufanego i podpisu zaufanego

Tekst ogłoszony:	D20181760.pdf
Status aktu prawnego:	obowiązujący
Data ogłoszenia:	2018-09-11
Data wydania:	2018-09-10
Data wejścia w życie:	2018-09-11
Organ wydający:	MIN. CYFRYZACJI

Podstawa prawna (1)

Podstawa prawna z art. (1)

Akty uznane za uchylone (1)

Akty zmieniające (1)

Dyrektywy europejskie (2)

Dyrektywa	Data	Tytuł	EUR-Lex
32014R0910	2014-07-23	Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE	EUR-Lex
32015R1502	2015-09-08	Rozporządzenie wykonawcze Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Tekst mający znaczenie dla EOG)	EUR-Lex

podpis elektroniczny | informatyzacja

UODO
URZĄD OCHRONY DANYCH OSOBOWYCH

SZYFROWANIE – skuteczny sposób na zabezpieczenie danych ?

Identyfikacja i uwierzytelnianie – wymogi UE

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) NR 910/2014

z dnia 23 lipca 2014 r.

w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

Artykuł 8

Poziomy bezpieczeństwa systemów identyfikacji elektronicznej

1. System identyfikacji elektronicznej notyfikowany na podstawie art. 9 ust. 1 określa niski, średni lub wysoki poziom bezpieczeństwa w odniesieniu do środka identyfikacji elektronicznej wydanego w ramach tego systemu.

3. Do dnia 18 września 2015 r., przy uwzględnieniu odpowiednich standardów międzynarodowych i z zastrzeżeniem ust. 2, Komisja określi w drodze aktów wykonawczych minimalne techniczne specyfikacje, standardy i procedury, w odniesieniu do których określone zostaną niski, średni i wysoki poziom bezpieczeństwa dla środka identyfikacji elektronicznej do celów ust. 1.

1502/2015 - doprecyzowuje implementacje …

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2015/1502

z dnia 8 września 2015 r.

w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2015/1502

z dnia 8 września 2015 r.

ZAŁĄCZNIK

Specyfikacje techniczne i procedury dotyczące niskiego, średniego i wysokiego poziomu zaufania w odniesieniu do środka identyfikacji elektronicznej wydanego w ramach notyfikowanego systemu identyfikacji elektronicznej

1. **Stosowane definicje**

USŁUGI ZAUFANIA również dla RODO, eIDAS, PSD2 …

Na potrzeby niniejszego załącznika stosuje się następujące definicje:

1) „wiarygodne źródło" oznacza każde źródło, niezależnie od jego formy, co do którego można mieć pewność, że dostarcza ono dokładnych danych, informacji lub dowodów, które mogą służyć do potwierdzenia tożsamości;

2) „czynnik uwierzytelniania" oznacza czynnik, którego związek z osobą jest potwierdzony i który należy do jednej z poniższych kategorii:

   a) „czynnik uwierzytelniania na podstawie posiadania" oznacza czynnik uwierzytelniania, w przypadku którego od podmiotu podlegającego uwierzytelnieniu wymaga się wykazania jego posiadania;

   b) „czynnik uwierzytelniania na podstawie wiedzy" oznacza czynnik uwierzytelniania, w przypadku którego od podmiotu podlegającego uwierzytelnieniu wymaga się wykazania jego znajomości;

   c) „czynnik uwierzytelniania na podstawie cech przyrodzonych" oznacza czynnik uwierzytelnienia, który opiera się na rzeczywistym atrybucie osoby fizycznej, w którego przypadku od podmiotu podlegającego uwierzytelnieniu wymaga się wykazania, że tę cechę fizyczną posiada;

3) „uwierzytelnianie dynamiczne" oznacza proces elektroniczny z zastosowaniem kryptografii lub innych technik służący dostarczeniu na żądanie elektronicznego dowodu, iż podmiot podlegający uwierzytelnieniu jest w posiadaniu danych identyfikacyjnych lub dane te znajdują się pod jego kontrolą, oraz który ulega zmianie z każdym uwierzytelnieniem zachodzącym między podmiotem podlegającym uwierzytelnieniu a systemem weryfikacji tożsamości danego podmiotu;

Uwierzytelnianie wg ISO/IEC29115 a wymogi w UE 1502/2015

Mechanizmy uwierzytelniania

Zalecane i wymagane

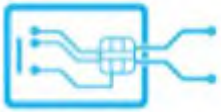
ELEKTRONICZNY DOWÓD

Hasła statyczne
i maskowalne

Aplikacje mobilne
SMS, QRCode

tokeny kryptograficzne

Smart-Cards



Tokeny OTP
PRNG, RNG

Certyfikaty

(7) Zwykle stosuje się pewne czynniki uwierzytelniania, takie jak dzielenie sekretu (ang. *shared secrets*), urządzenia techniczne i atrybuty fizyczne. Należy jednak zachęcać do korzystania z większej liczby czynników uwierzytelniania, zwłaszcza należących do różnych kategorii, w celu zwiększenia bezpieczeństwa procesu uwierzytelniania.

(11) Certyfikacja bezpieczeństwa informatycznego oparta na normach międzynarodowych jest ważnym narzędziem weryfikacji zgodności produktów w zakresie bezpieczeństwa z wymaganiami określonymi w niniejszym akcie wykonawczym.

1. Stosowane definicje

3) „uwierzytelnianie dynamiczne" oznacza proces elektroniczny z zastosowaniem kryptografii lub innych technik służący dostarczeniu na żądanie elektronicznego dowodu, iż podmiot podlegający uwierzytelnieniu jest w posiadaniu danych identyfikacyjnych lub dane te znajdują się pod jego kontrolą, oraz który ulega zmianie z każdym uwierzytelnieniem zachodzącym między podmiotem podlegającym uwierzytelnieniu a systemem weryfikacji tożsamości danego podmiotu;

§ … który ulega zmianie z każdym uwierzytelnieniem"

§ … jest w posiadaniu (…) lub dane te znajdują się pod jego kontrolą

R O Z W I Ą Z A N I E zgodne z UWIERZYTELNIANIEM DYNAMICZNYM

„Quantum Resists"

kryptografia z kluczami i/lub Hasłami Jednorazowymi

SZYFROWANIE – skuteczny sposób na zabezpieczenie danych ?

URZĄD OCHRONY DANYCH OSOBOWYCH

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2015/1502

z dnia 8 września 2015 r.

2.3. *Uwierzytelnienie*

2.3.1. Mechanizm uwierzytelniania

Poziom zaufania	Wymagane elementy	
Średni	Jak przy poziomie niskim oraz: 1. Uwolnienie danych identyfikujących osobę jest poprzedzone wiarygodną weryfikacją środka identyfikacji elektronicznej oraz jego ważności za pomocą uwierzytelniania dynamicznego. 2. Mechanizm uwierzytelniania jest sposobem realizacji kontroli zaufania na potrzeby weryfikacji środków identyfikacji elektronicznej, dzięki któremu jest mało prawdopodobne, aby takie działania jak zgadywanie, podsłuchiwanie, odtwarzanie lub manipulowanie komunikacji przez atakującego o umiarkowanym potencjale ataku mogło zachwiać mechanizmami uwierzytelniania.	(1) (2)
Wysoki	Jak przy poziomie średnim oraz: mechanizm uwierzytelniania jest sposobem realizacji kontroli zaufania na potrzeby weryfikacji środków identyfikacji elektronicznej, dzięki któremu jest mało prawdopodobne, aby takie działania jak zgadywanie, podsłuchiwanie, odtwarzanie lub manipulowanie komunikacji przez atakującego o wysokim potencjale ataku mogło zachwiać mechanizmami uwierzytelniania.	(2)

Pytania z interpelacji 1385 z dnia 16 stycznia 2020r

w sprawie bezpieczeństwa usług cyfrowych oraz transakcji elektronicznych

http://sejm.gov.pl/Sejm9.nsf/interpelacja.xsp?typ=INT&nr=1385

1. Czy zalecenia dotyczące poziomów bezpieczeństwa zostały wdrożone i są weryfikowane?

2. Czy w ramach zapewnienia średniego poziomu bezpieczeństwa wdrożono „uwierzytelnianie dynamiczne" poprzedzające uwolnienie danych identyfikacyjnych w e-recepta, e-banking, ePUAP, mDokumenty, dowód osobisty z warstwą cyfrową?

3. Czy w ramach średniego poziomu zaufania zgodnie z definicja „uwierzytelnianie dynamiczne" zawartą w (UE) 2015/1502 to podmiot uwierzytelniany jest w posiadaniu czynnika uwierzytelniającego i czy czynnik ten ulega zmianie przy każdym uwierzytelnieniu?

4. Czy zalecenia dotyczące ograniczenia korzystania z SMS w uwierzytelnianiu dwuskładnikowym zostały uwzględnione w usługach wymagających średniego i wyższego poziomu bezpieczeństwa oraz czy Strategia Cyberbezpieczeństwa RP na kolejne lata uwzględnia inne niż SMS czyli bezpieczniejsze metody i rozwiązania?

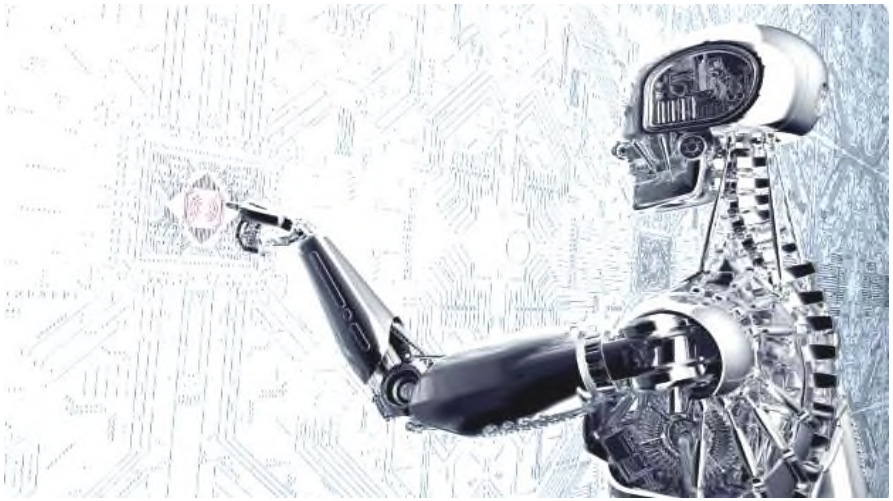
5. Czy wymagane przynajmniej raz na dwa lata audyty podmiotów świadczących usługi zaufania obejmują kontrolę spełnienia wymogu „uwierzytelniania dynamicznego" poprzedzającego uwolnienie danych identyfikacyjnych?

ODPOWIEDŹ – aktualne usługi administracji i e-banking nie spełniają „uwierzytelniania dynamicznego"

http://orka2.sejm.gov.pl/INT9.nsf/klucz/ATTBLKJX2/%24FILE/i01385-o2.pdf

Podsumowanie

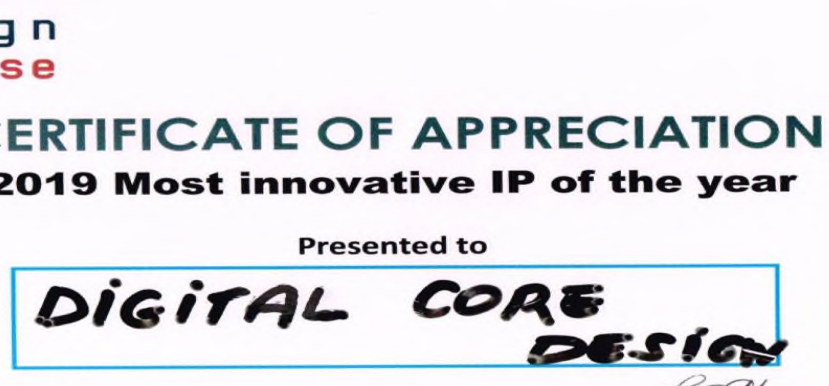
… odpowiedź na interpelację 1385 zamyka czy otwiera temat „uwierzytelniania dynamicznego” w bezpieczeństwie danychi usługach zaufania ?
Cel to podniesienie poziomu cyberbezpieczeństwa danych ?
Bezwarunkowo bezpieczna kryptografia – OTK !



Bezwzględnie Bezpieczny System Uwierzytelniania

Polski Produkt Przyszłości

dla Usług zaufania z Uwierzytelnianiem dynamicznym



Bezpieczeństwo e-usług … jest cenne

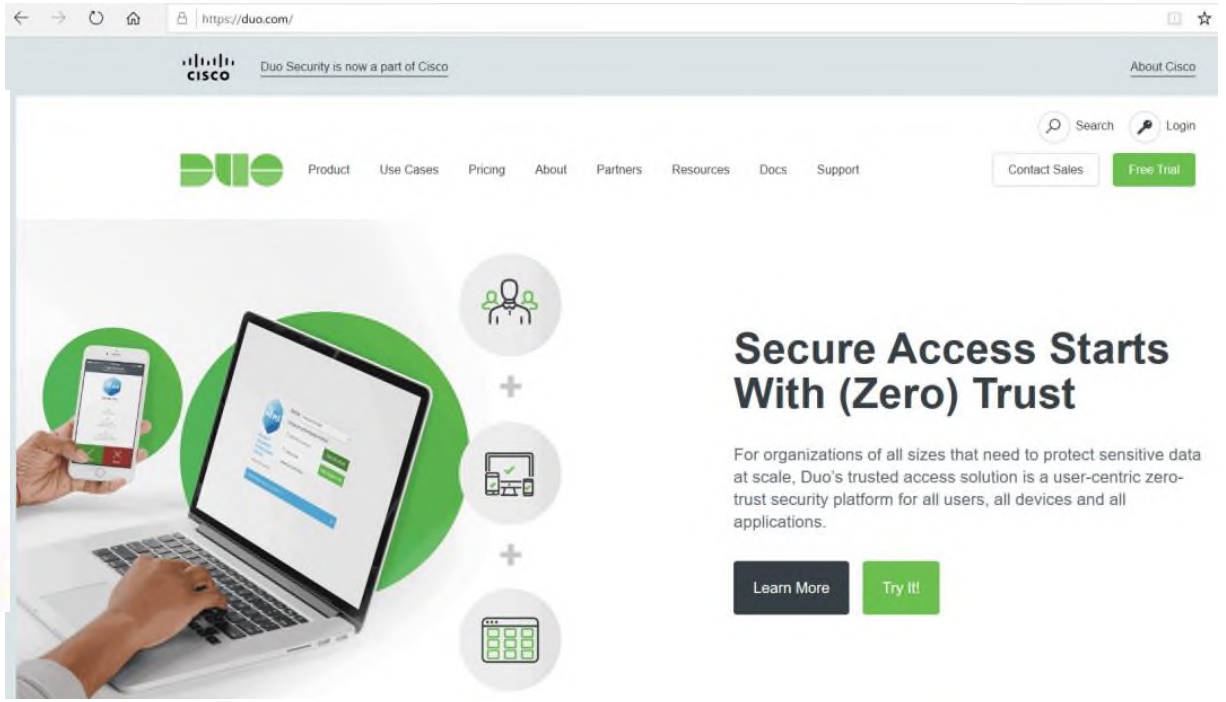
Usługi Zaufania eIDAS i e – tożsamość :

poufność
rozliczalność

wymaga

identyfikacji,
uwierzytelniania,
kontroli dostępu

CISCO przejmuje Duo security za 2,35 mld USD



URZĄD OCHRONY DANYCH OSOBOWYCH

SZYFROWANIE – skuteczny sposób na zabezpieczenie danych ?