INSTYTUT ŁĄCZNOŚCI
PAŃSTWOWY INSTYTUT BADAWCZY

Normy jako podstawa do opracowywania i wdrażania standardów bezpieczeństwa teleinformatycznego w projektach realizowanych przez MC w ramach POPC

Opracowanie powstało w wyniku realizacji umowy o dotację celową 1/DT z 26.04.2016r, Aneks nr 2, zadanie 4, podzadanie 12, między Ministrem Cyfryzacji a Instytutem Łączności – Państwowym Instytutem Badawczym

Spis treści

Spis tabel

Spis rysunków

1. Informacje wstępne

1.1 Podstawa opracowania dokumentu

Niniejsza ekspertyza jest efektem realizacji umowy o dotację celową, zawartej między Ministrem Cyfryzacji a IŁ - PIB, z 26 kwietnia 2016r oraz Aneksu nr 2 do tej umowy, Zadanie 4, podzadanie 12.

1.2 Zakres przedmiotu

Ekspertyza zawiera omówienie stanu normalizacji międzynarodowej, europejskiej i polskiej w obszarach bezpieczeństwa informacji i bezpieczeństwa teleinformatycznego w kontekście przyjętych w UE w ostatnim czasie aktów prawnych.

1.3 Cel dokumentu

Podstawą wdrażania nowych legislacji są normy traktowane jako powszechnie stosowane praktyki, zapewniające interoperacyjność i transparentność rozwiązań technicznych. Aktualny stan normalizacji z punktu widzenia potrzeb polskich podmiotów jest podstawą do sformułowania rekomendacji dla systemu Polskich Norm i pożądanych działań MC w kierunku spełnienia tych potrzeb.

1.4 Odbiorcy dokumentu

Ekspertyza jest przeznaczona dla Ministerstwa Cyfryzacji.

1.5 Układ dokumentu

Rozdział 1 (niniejszy) zawiera ogólną charakterystykę dokumentu.

W rozdziale 2 omówiono podstawy legislacyjne i stan normalizacji w obszarze cyberbezpieczeństwa.

W rozdziale 3 przedstawiono potrzeby normalizacyjne i aktualny stan w obszarze ochrony danych osobowych i prywatności.

W rozdziale 4 zaprezentowano niezbędny zakres normalizacji z punktu widzenia potrzeb certyfikacji bezpieczeństwa produktów i usług teleinformatycznych.

W rozdziale 5, stanowiącym podsumowanie, zebrano wszystkie szczegółowe zalecenia oraz sformułowano ogólne rekomendacje dla Ministerstwa Cyfryzacji w odniesieniu do działań w systemie Polskich Norm.

2. Normy dotyczące cyberbezpieczeństwa

2.1 Stan regulacji UE w odniesieniu do normalizacji

Działania legislacyjne Unii Europejskiej wynikają z celów określonych w Agendzie Cyfrowej 2020[1] (filar III: Zaufanie i Bezpieczeństwo) oraz wpisuje się w szereg planów działań tam opisanych i dotyczących ochrony cyberprzestrzeni, w tym:

a) Ochrony infrastruktury krytycznej z punktu widzenia ryzyk związanych z cyberbezpieczeństwem,
b) Ochrony usług komunikacji elektronicznej, jako środka wykorzystania cyberprzestrzeni do realizacji potrzeb społecznych, gospodarczych i kulturowych,
c) Zagadnień relacji między bezpieczeństwem a prywatnością, w tym ochrony praw podstawowych.

W 2013 roku Komisja Europejska opublikowała dokument strategii EU w zakresie cyberbezpieczeństwa[2] . W dokumencie tym określono m.in.:

- Pryncypia ochrony cyberprzestrzeni: ochrona praw podstawowych, powszechny dostęp do cyberprzestrzeni, nadzór demokratyczny uwzględniający interesy wielu podmiotów, podział odpowiedzialności za zapewnienie bezpieczeństwa,
- Strategiczne priorytety i działania, takie, jak:
  - Zwiększenie odporności na ataki
  - Zdecydowane obniżenie poziomu cyberprzestępczości
  - Określenie zasad ochrony cyberprzestrzeni oraz współpracy w tym zakresie
  - Zidentyfikowanie i wykorzystanie istniejących zasobów, publicznych i prywatnych, w celu stworzenia struktur cyberbezpieczeństwa,
  - Opracowanie i wdrożenie spójnej polityki na poziomie europejskim, służącej ochronie wartości EU.
- Rozdzielenie ról i odpowiedzialności za bezpieczeństwo cyberprzestrzeni, z uwzględnieniem konieczności współpracy wielu podmiotów – administracji rządowej, samorządowej, przedsiębiorców oraz organizacji branżowych zrzeszających przedsiębiorców, organizacji pozarządowych, organizacji międzynarodowych,
- Zasady współpracy i wsparcia ze strony organów Komisji Europejskiej w wypadku poważnych incydentów w cyberprzestrzeni.

W przyjęto lipcu 2016 przyjęto Dyrektywę 2016/1148/WE[3] (zwaną dalej Dyrektywą NIS) regulującą podstawowe zasady cyberbezpieczeństwa w krajach UE. W Dyrektywie NIS podkreślono znaczenie normalizacji międzynarodowej, wskazując na:

- konieczność wdrażania środków technicznych i organizacyjnych w celu zarządzania ryzykami, na jakie narażone są sieci i systemy informatyczne, przy uwzględnieniu takich elementów, jak zgodność z normami międzynarodowymi (art. 16 ust. 1),

[1] https://ec.europa.eu/digital-agenda/en/digital-agenda-europe-2020-strategy
[2] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/join/com_join%282013%290001_/com_join%282013%290001_pl.pdf

[3] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016L1148&from=EN

- stosowanie europejskich lub uznanych międzynarodowo norm i specyfikacji mających znaczenie dla bezpieczeństwa sieci i systemów informatycznych jako czynnika zapewniającego spójne wdrażanie zapisów dyrektywy w obszarze określania wymagań bezpieczeństwa i zgłaszania incydentów naruszenia bezpieczeństwa (art. 19 ust. 1)

Komisja Europejskiej rozważa zainicjowanie i koordynowanie procesu opracowania zharmonizowanych norm dla wymagań bezpieczeństwa, czego należy dokonać zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1025/2012[4].

Zgodnie z planem normalizacyjnym EU na rok 2016[5], zagadnieniami normalizacji w obszarze cyberbezpieczeństwa zajmuje się specjalnie powołana połączona grupa koordynacyjna CEN-CENELEC Focus Group on Cybersecurity[6]. Efektem jej działań w 2016 roku było uznanie 8 norm międzynarodowych ISO/IEC z obszaru informatyki śledczej jako norm europejskich (EN)[7]. Ponadto, w planie normalizacji na 2017 rok znajduje się przyjęcie kolejnych 3 norm międzynarodowych[8] jako norm europejskich (zob. też poniżej).

2.2 Normy przyjęte do systemu PN w 2016 roku

W poniższej tabeli zestawiono 8 norm międzynarodowych, przyjętych jako normy europejskie, zostało również wprowadzonych, metodą uznania[9], do systemu Polskich Norm (system PN).

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz.U. L 316 z 14.11.2012, s. 12).

[5] https://ec.europa.eu/digital-agenda/en/rolling-plan-ict-standardisation

[6] http://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Security/Pages/Cybersecurity.aspx

[7] https://standards.cen.eu/dyn/www/f?p=204:32:0::::FSP_ORG_ID,FSP_LANG_ID:6322,25&cs=1A52DC546C1F62EB47FBE6298107B9A9F

[8] https://standards.cen.eu/dyn/www/f?p=204:22:0::::FSP_ORG_ID,FSP_LANG_ID:6322,25&cs=1A52DC546C1F62EB47FBE6298107B9A9F

[9] Metoda uznania przez PKN Normy Europejskiej za Polską Normę polega na opublikowaniu jej w oryginalnej wersji językowej z dołączonymi stronicami krajowymi, zawierającymi: stronicę tytułową PN, przedmowę krajową i załączniki krajowe (jeśli mają zastosowanie)

Numer normy	Tytuł normy	Zakres normy	Rekomendowane działanie w systemie PN
PN-EN ISO/IEC 27037:2016-12	Technika informatyczna — Techniki bezpieczeństwa — Wytyczne do identyfikacji, gromadzenia, pozyskiwania i zachowania cyfrowych śladów dowodowych	Niniejszy dokument zawiera wytyczne do specyficznych działań w ramach postępowania z cyfrowymi śladami dowodowymi; do tych działań należą: identyfikacja, gromadzenie, pozyskiwanie i utrwalanie cyfrowych śladów dowodowych, które mogą mieć wartość dowodową. Niniejszy dokument zawiera wskazówki dla osób fizycznych w odniesieniu do typowych sytuacjach spotykanych w całym procesie postępowania z cyfrowymi śladami dowodowymi i pomaga organizacjom w ich procedurach dyscyplinarnych i w ułatwianiu wymiany potencjalnych cyfrowych śladów dowodowych pomiędzy różnymi systemami prawnymi. Niniejszy dokument zawiera wytyczne dla niżej wymienionych urządzeń i/lub funkcjonalności, które są stosowane w różnych sytuacjach: • nośniki danych cyfrowych stosowane w standardowych komputerach, takie jak dyski twarde, dyskietki, dyski optyczne i magnetooptyczne, oraz urządzenia do przechowywania danych o podobnych funkcjach, • Telefony komórkowe, palmtopy (Personal Digital Assistants - PDA), osobiste urządzenia elektroniczne (Personal Electronic Devices - PED), karty pamięci, • Mobilne urządzenia do nawigacji • Cyfrowe aparaty fotograficzne i kamery wideo (w tym monitoring wizyjny - CCTV), • Typowe komputery podłączone do sieci, • Sieci oparte na protokole TCP / IP i innych protokołach cyfrowej transmisji danych i • Urządzenia o funkcjach podobnych do wyżej wymienionych. UWAGA 1 Powyższa lista urządzeń ma charakter orientacyjny i nie jest wyczerpująca. Uwaga 2 Urządzenia z powyższej listy mogą występować w różnych formach.. Na przykład, system samochodowy może zawierać: system nawigacji mobilnej, system przechowywania danych i system czujników.	obecnie - metodą uznania, docelowo -tłumaczenie
PN-EN ISO/IEC 27038:2016-12	Technika informatyczna — Techniki bezpieczeństwa —	W niniejszej Normie Międzynarodowej przedstawiono opisy technik przeprowadzania trwałego usuwania w dokumentach cyfrowych. W niniejszej Normie Międzynarodowej określono również	pozostawienie w formie uznania

Numer normy	Tytuł normy	Zakres normy	Rekomendowane działanie w systemie PN
	Specyfikacja metod cyfrowych trwałego usuwania	wymagania dotyczące narzędzi programowych do trwałego usuwania i metod testowania bezpiecznego zakończenia trwałego usunięcia. Niniejsza Norma Międzynarodowa nie obejmuje trwałego usuwania z baz danych.	
PN-EN ISO/IEC 27040: 2016-12	Technika informatyczna — Techniki bezpieczeństwa – Bezpieczeństwo pamięci masowych	W niniejszej Normie Międzynarodowej zamieszczono szczegółowe techniczne wytyczne, dzięki którym organizacje mogą określić odpowiedni poziom ograniczania ryzyka, dzięki zastosowaniu sprawdzonego i spójnego podejścia do planowania, projektowania, dokumentowania i realizacji bezpieczeństwa pamięci masowych. Bezpieczeństwo pamięci masowych stosuje się do ochrony (bezpieczeństwa) informacji, tam gdzie jest przechowywana i do bezpieczeństwo informacji przesyłanych przez połączenia komunikacyjne związane z pamięciami masowymi. Bezpieczeństwo pamięci masowych obejmuje bezpieczeństwo urządzeń i nośników, bezpieczeństwo czynności związanych z zarządzaniem urządzeniami i mediami, bezpieczeństwo aplikacji i usług oraz bezpieczeństwo istotne dla użytkowników końcowych w okresie i po zakończeniu eksploatacji urządzeń i nośników. Bezpieczeństwo pamięci masowych jest istotne dla osób zaangażowanych w posiadanie, eksploatację, lub używanie urządzeń, nośników i sieci pamięci masowych. Dotyczy to wyższego kierownictwa, nabywców produktów i usług pamięci masowych oraz innych nietechnicznych menadżerów lubi użytkowników, dodatkowo do menadżerów i administratorów, którzy mają określone obowiązki w zakresie bezpieczeństwa informacji lub bezpieczeństwa przechowywania, eksploatacji pamięci masowych lub którzy są odpowiedzialni za program ogólnego bezpieczeństwa organizacji oraz rozwijanie polityki bezpieczeństwa. Jest to również istotne dla osób zaangażowanych w planowanie, projektowanie i wdrażanie aspektów architektury bezpieczeństwa sieci pamięci masowych. Niniejsza Norma Międzynarodowa zawiera przegląd koncepcji bezpieczeństwa pamięci masowych i pokrewnych definicji. Obejmuje ona wytyczne dotyczące zagrożeń, projektowania i aspektów zabezpieczenia związanych z typowymi scenariuszami wykorzystania i technologicznymi obszarami pamięci masowych. Ponadto, zawiera odniesienia do innych Norm Międzynarodowych i Raportów Technicznych, dotyczących istniejących praktyk i technik, które mogą być stosowane w odniesieniu do bezpieczeństwa pamięci masowych.	pozostawienie w formie uznania

Numer normy	Tytuł normy	Zakres normy	Rekomendowane działanie w systemie PN
PN-EN ISO/IEC 27041:2016-12	Technika informatyczna — Techniki bezpieczeństwa — Wytyczne do zapewnienia stosowności i adekwatności metody dochodzeniowej w związku z incydentem	W niniejszej Normie Międzynarodowej zawarto wytyczne do mechanizmów zapewniania, że metody i procesy używane w dochodzeniu w związku z incydentami bezpieczeństwa informacji „pasują do potrzeby". W Normie wskazano najlepsze praktyki określania wymagań, opisywania metod oraz zapewniania, że można wykazać spełnienie wymagań przez wdrożenie tych metod. Norma zawiera rozważania dotyczące sposobu, w jaki można używać testowania wykonywanego przez dostawcę lub stronę trzecią do wsparcia tego procesu uzasadnionej pewności. Niniejszy dokument ma na celu: – zapewnienie wytycznych do przechwytywania i analizy wymagań funkcjonalnych i niefunkcjonalnych odnoszących się do dochodzenia w związku z incydentem bezpieczeństwa informacji (IS), – podanie wytycznych do użycia walidacji jako środków zapewnienia odpowiedniości procesów, które składają się na dochodzenie, – zapewnienie wytycznych do oszacowania wymaganych poziomów walidacji oraz wymaganej ewidencji wynikającej z testu walidacyjnego, podanie wytycznych, w jaki sposób zewnętrzne testowanie i dokumentowanie może zostać włączone w proces walidacji.	obecnie - metodą uznania, docelowo -tłumaczenie
PN-EN ISO/IEC 27042:2016-12	Technika informatyczna — Techniki bezpieczeństwa — Wytyczne do analizy i interpretacji cyfrowego śladu dowodowego	W niniejszej Normie Międzynarodowej zawarto wytyczne do analizy i interpretacji cyfrowego śladu dowodowego w sposób umożliwiający zachowanie ciągłości, ważności, odtwarzalności i powtarzalności. Zawiera najlepsze praktyki odnoszące się do wyboru, projektowania i wdrażania procesów analizy oraz rejestrowania informacji w ilości wystarczającej do poddania tych procesów niezależnemu badaniu, jeśli są takie wymagania. Zawiera wytyczne do odpowiednich mechanizmów umożliwiających przedstawienie biegłości i umiejętności zespołu dochodzeniowego. Analiza i interpretacja cyfrowego śladu dowodowego może być złożonym procesem. W pewnych okolicznościach istnieje wiele metod, które można zastosować, zatem do członków zespołu dochodzeniowego może zostać sformułowane wymaganie uzasadnienia ich wyboru określonego procesu i wykazania jego równoważności w odniesieniu do innego procesu używanego przez innych specjalistów dochodzeniowych. W innych okolicznościach, specjaliści dochodzeniowi mogą być zmuszeni do zaprojektowania nowych metod sprawdzenia cyfrowego śladu dowodowego, które wcześniej nie były rozważane i udowodnienia, że wytworzona metoda „pasuje do potrzeby".	obecnie - metodą uznania, docelowo -tłumaczenie

Numer normy	Tytuł normy	Zakres normy	Rekomendowane działanie w systemie PN
		Zastosowanie określonej metody może wpływać na interpretację cyfrowego śladu dowodowego przetwarzanego za pomocą tej metody. Dostępny cyfrowy ślad dowodowy może wpływać na wybór metod do dalszej analizy tego już pozyskanego cyfrowego śladu dowodowego. W niniejszej Normie Międzynarodowej przedstawiono wspólną strukturę analitycznych oraz interpretacyjnych elementów obsługi incydentów związanych z bezpieczeństwem systemów, które mogą być użyte jako wsparcie we wdrażaniu nowych metod oraz zawarto minimalny wspólny standard dla cyfrowego śladu dowodowego wytworzonego na skutek tych działań.	
PN-EN ISO/IEC 27043:2016-12	Technika informatyczna — Techniki bezpieczeństwa — Pryncypia i procesy w dochodzeniach związanych z incydentami	W niniejszej Normie Międzynarodowej zawarto wytyczne, wykorzystujące modele teoretyczne, do procesów dochodzeniowych obejmujących wykorzystanie cyfrowych śladów dowodowych , dla incydentów różnego typu. Wytyczne te obejmują, zarówno procesy - od przygotowania przed incydentem do zamknięcia dochodzenia, jak i ogólne wskazówki i zastrzeżenia odnoszące się do tych procesów. W wytycznych opisano procesy i pryncypia mające zastosowanie do dochodzeń różnego rodzaju, w tym, nie ograniczając jednakże, do: nieuprawnionego dostępu, naruszenia bezpieczeństwa danych, awarii systemu lub korporacyjnych naruszeń bezpieczeństwa informacji, a także do jakichkolwiek innych dochodzeń informatycznych. Podsumowując, w niniejszej Normie Międzynarodowej zawarto ogólny opis wszystkich pryncypiów i procesów stosowanych w dochodzeniach związanych z incydentami, jednakże bez omawiania każdego tych procesów lub pryncypiów. Bardziej szczegółowe informacje dotyczące określonych pryncypiów i procesów dochodzeniowych zawarto w wielu innych odnośnych Normach Międzynarodowych.	obecnie - metodą uznania, docelowo -tłumaczenie
PN-EN ISO/IEC 30121:2016-12	Technika informatyczna — Nadzór nad strukturą ryzyka związanego z informatyką śledczą	W niniejszej Normie Międzynarodowej zamieszczono strukturę przeznaczoną dla organów nadzorujących w organizacjach (w tym właścicieli, członków rad nadzorczych, dyrektorów, partnerów, najwyższego kierownictwa, lub podobnych ciał), służącą do wyboru najlepszego sposobu przygotowania organizacji do dochodzeń informatycznych, nim one się zdarzą. Niniejsza Norma Międzynarodowa ma zastosowanie do rozwoju strategicznych procesów (i decyzji) związanych z przechowywaniem, dostępnością, dostępem, opłacalnością i ujawnianiem cyfrowych śladów dowodowych. Niniejsza Norma Międzynarodowa jest przeznaczone do stosowania w organizacji każdego rodzaju i wielkości .	pozostawienie w formie uznania

Tab. 1 Polskie Normy z zakresu cyberbezpieczeństwa

Z wysokim prawdopodobieństwem[10] należy przypuszczać, że w 2017 roku zostaną przyjęte jako normy europejskie 3 normy międzynarodowe w obszaru cyberbezpieczeństwa tzn. ISO/IEC 27000:2016, ISO/IEC 27001:2013 oraz ISO/IEC 27002:2013.

Ponieważ normy te są już w systemie PN[11] i funkcjonują jako:

- PN ISO/IEC 27000:2014-11 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Przegląd i terminologia
- PN ISO/IEC 27001:2014-12 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania
- PN ISO/IEC 27002:2014-12 Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady zabezpieczania informacji

nie są przewidywane działania normalizacyjne w celu wprowadzenia tych norm do systemu PN.

[10] Zgodnie z decyzją Zarządów CEN oraz CENELEC, normy międzynarodowe ISO/IEC są przyjmowane - bez modyfikacji - w procedurze jednokrotnego głosowania Krajów Członkowskich. Głosowanie pozytywne powoduje automatyczną publikację dokumentu jako normy europejskiej, głosowanie negatywne – automatyczne odrzucenie dokumentu. Z uwagi na powszechną akceptację wskazanych norm, i w Europie i na całym świecie, ich odrzucenie raczej nie wchodzi w rachubę.

[11] PN-ISO/IEC 27000:2014-12 jest tłumaczeniem wersji przedostatniej odpowiedniej normy międzynarodowej

3. Normy z zakresu ochrony danych osobowych i prywatności

3.1 Stan regulacji UE w odniesieniu do normalizacji

Nowe regulacje prawne dotyczące ochrony danych osobowych wskazują normy techniczne jako źródło mechanizmów ochrony tych danych. Zgodnie z nowym Rozporządzeniem[12], w krótkim czasie Komisja Europejska wskaże odpowiednie normy techniczne odnoszące się do rozwiązań dla systemów przetwarzania danych osobowych, co zapowiada art. 43 ww. Rozporządzenia:

Art. 43, ust. 9." *Komisja może przyjąć akty wykonawcze określające techniczne standardy mechanizmów certyfikacji oraz znaków jakości i oznaczeń w dziedzinie ochrony danych, a także sposoby upowszechniania i uznawania tych mechanizmów certyfikacji oraz znaków jakości i oznaczeń. (..)".*

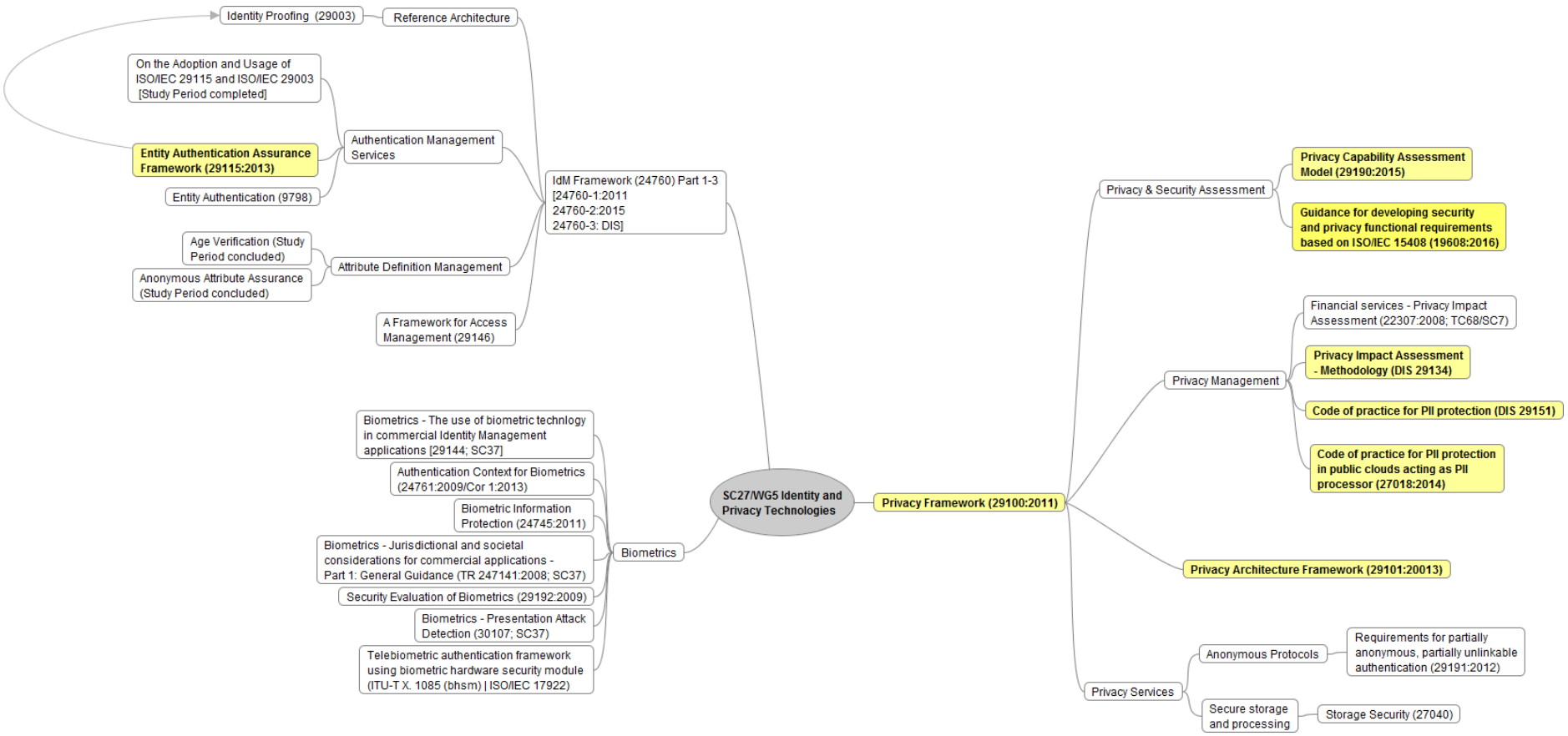
3.2 Normy międzynarodowe z punktu widzenia potrzeb normalizacji europejskiej

Analiza dotycząca potrzeb normalizacyjnych jako wsparcia dla mechanizmów ochrony danych osobowych w trakcie ich automatycznego przetwarzania, zawarta w Rocznym Planie Normalizacyjnym na 2016 rok, wskazuje na kilka źródeł norm międzynarodowych z których najważniejsze to normy oznaczane prefiksem ISO/IEC.

Wyłącznym źródłem normalizacji w zakresie technologii bezpieczeństwa w obszarze normalizacji ISO/IEC jest podkomitet techniczny SC27 „IT Security Techniques", a w kontekście ochrony danych osobowych - prace Grupy Roboczej 5 (Identity and Privacy Technologies).

Na Rys. 1 przedstawiono poglądowo zakres prac normalizacyjnych tej Grupy.

[12] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),



Rys. 1 Normy międzynarodowe w zakresie prac ISO/IEC JTC1/SC27/WG5 (kolorem żółtym zaznaczono szczególnie ważne normy, w tym normy przywołane w Rocznym Planie Normalizacyjnym na 2016 rok)

W poniższej tabeli zawarto zestawienie norm wskazanych na Rys. 1 wraz z krótką charakterystyką.

Numer normy	Tytuł normy	Zakres normy	Rekomendowany tryb przyjęcia do systemu PN
ISO/IEC 29100:2011	Privacy framework/ Ramy prywatności	W normie określono ramy prywatności, które obejmują: — określenie wspólnej terminologii dotyczącej prywatności; — zdefiniowanie aktorów i ich ról w przetwarzaniu danych — opis uwarunkowań dotyczących zabezpieczeń prywatności; — zapewnienie technologiom informatycznym odniesień do znanych pryncypiów prywatności Norma ma zastosowanie do osób fizycznych oraz organizacji uczestniczących w definiowaniu, zamawianiu, projektowaniu, opracowywaniu, testowaniu, utrzymaniu, administrowaniu i eksploatowaniu systemów teleinformatycznych lub usług, które wymagają zabezpieczeń prywatności przy przetwarzaniu PII.	tłumaczenie
ISO/IEC 29101: 2013	Privacy architecture framework/ Ramy architektury prywatności	W normie określono ramy architektury prywatności, które: — odnoszą się do zagadnień systemów teleinformatycznych przetwarzających PII; — wskazują komponenty do wdrożenia takich systemów; oraz — opisują widoki architektury zapewniających osadzenie w kontekście tych komponentów. Norma ma zastosowanie u podmiotów uczestniczących w definiowaniu, zamawianiu, projektowaniu, opracowywaniu, testowaniu, utrzymaniu, administrowaniu i eksploatowaniu systemów teleinformatycznych przetwarzających PII. W pierwszym rzędzie norma koncentruje się na systemach zapewniających interakcję z właścicielem PII.	tłumaczenie

Numer normy	Tytuł normy	Zakres normy	Rekomendowany tryb przyjęcia do systemu PN
ISO/IEC 29115:2013	Entity authentication assurance framework / Ramy uzasadnionej pewności poziomów uwierzytalnienia	W normie określono ramy zarządzania uzasadnioną pewnością uwierzytelnienia podmiotu w określonym kontekście. W szczególności, norma ta:– określa cztery poziomy uzasadnionej pewności uwierzytelnienia podmiotu;– określa kryteria i wytyczne do osiągnięcia każdego z czterech poziomów uzasadnionej pewności uwierzytelnienia podmiotu;– zapewnia wytyczne do odwzorowania innych schematów uzasadnionej pewności uwierzytelnienia na cztery zdefiniowane poziomy;– zapewnia wytyczne do wymiany wyników uwierzytelnienia, które wykorzystują koncepcję czterech poziomów; oraz – zapewnia wytyczne w odniesieniu do zabezpieczeń, które są zalecane w celu zmniejszenia zagrożeń związanych z uwierzytelnianiem.	tłumaczenie
ISO/IEC 29134*	Privacy impact Assessment - Methodology/ Metodyka szacowania skutków dla prywatności	W normie przedstawiono wytyczne do: — procesu szacowania skutków dla prywatności; oraz — struktury i zawartości raportu PIA (Privacy Impact Assessment). Norma ma zastosowanie do organizacji wszystkich typów i wielkości. Norma odnosi się do podmiotów, które uczestniczą w projektach opracowywania lub wdrażania, w tym podmioty eksploatujące systemy i usługi przetwarzania danych, które obejmują przetwarzania PII.	tłumaczenie
ISO/IEC 29151*	Code of practice for PII protection/ Praktyczne zasady ochrony PII	W normie ustanowiono cele stosowania zabezpieczeń, zabezpieczenia i wytyczne do wdrażania zabezpieczeń, tak aby spełnić wymagania zidentyfikowane w wyniku przeprowadzenia szacowania ryzyka oraz skutków w odniesieniu do ochrony danych identyfikujących osobę (Personally Identifiable Information (PII)). W szczególności, norma określa wytyczne na podstawie ISO/IEC 27002, biorąc pod uwagę wymagania wynikające z przetwarzania PII, które mogą mieć zastosowanie w kontekście ryzyka związanego z bezpieczeństwem informacji. Norma ma zastosowanie do organizacji wszystkich typów i wielkości, działających(zgodnie z definicją zawartą w ISO/IEC 29100) jako podmioty kontrolujące PII, przetwarzając PII.	tłumaczenie

Numer normy	Tytuł normy	Zakres normy	Rekomendowany tryb przyjęcia do systemu PN
ISO/IEC 29190:2015	Privacy capability assessment model / Model oceny zdolności do prywatności	Norma zawiera ogólne wytyczne do sposobu, w jaki organizacja może ocenić swoją zdolność do zarządzania procesami związanymi z prywatnością. W szczególności, w normie:– opisano kolejne kroki procesu oceny w celu wyznaczenia poziomu zdolności w odniesieniu do prywatności; – określono zbiór poziomów oceny zdolności do prywatności;– sformułowano wytyczne do kluczowych obszarów procesów, dla których przeprowadza się ocenę zdolności do prywatności;– sformułowano wytyczne co do sposobu wdrożenia procesu oceny;– sformułowano wytyczne, w jaki sposób integrować prywatność [w procesach biznesowych].	tłumaczenie
ISO/IEC 27018:2014	Code of practice for PII protection in public clouds acting as PII processors / Praktyczne zasady ochrony PII w chmurach publicznych działających jako przetwarzający PII	W normie wskazano powszechnie uznawane cele stosowania zabezpieczeń, zabezpieczenia oraz wytyczne do wdrażania środków ochrony danych identyfikujących osobę (PII - Personally Identifiable Information) zgodnie z pryncypiami zdefiniowanymi w normie ISO/IEC 29000, dla środowiska przetwarzania w chmurze. Wytyczne zawarte w normie zostały zaprezentowane w układzie normy ISO/IEC 27002, przy uwzględnieniu wymagań Regulatora co do ochrony PII, które mogą mieć zastosowanie w kontekście środowisk ryzyka związanego z bezpieczeństwem informacji dostawcy usługi chmury publicznej. ISO/IEC 27018 jest przeznaczona dla organizacji wszystkich typów i wielkości, które świadczą na rzecz innych organizacji usługi przetwarzania informacji jako przetwarzający PII w postaci chmury.	tłumaczenie

Numer normy	Tytuł normy	Zakres normy	Rekomendowany tryb przyjęcia do systemu PN
ISO/IEC TS 19608**	Guidance for developing security and privacy functional requirements based on ISO/IEC 15408	Specyfikacja techniczna zapewnia wytyczne do:– opracowywania wymagań funkcjonalnych odnoszących się do prywatności jako rozszerzonych komponentów mających za podstawę pryncypia określone w ISO/IEC 29100 oraz paradygmat opisany w ISO/IEC 15408-2;– wyboru i definiowania wymagań funkcjonalnych odnoszących się do bezpieczeństwa (Security Functional Requirements (SFRs)) z ISO/IEC 15408-2 w celu ochrony danych identyfikujących osobę (Personally Identifiable Information (PII);– procedury definiowania, w skoordynowany sposób, wymagań funkcjonalnych odnoszących się do bezpieczeństwa i prywatności.Zamierzonymi odbiorcami tej specyfikacji są:– projektanci wdrażający produkty lub systemy ,w których są przetwarzane PII, pragnący poddać te produkty ocenie bezpieczeństwa z użyciem ISO/IEC 15408. Znajdą oni wytyczne, jak wybierać wymagania funkcjonalne dotyczące bezpieczeństwa do Przedmiotu [oceny] bezpieczeństwa (Security Target) dla swoich produktów lub systemów odwzorowane na pryncypia prywatności zdefiniowane w ISO/IEC 29100;– ewaluatorzy, używający ISO/IEC 15408 i ISO/IEC 18045 do oceny bezpieczeństwa; – autorzy Profili Ochrony (Protection Profiles), które odnoszą się do ochrony PII;Specyfikacja Techniczna jest w zamierzeniu w pełni spójna z ISO/IEC 15408; jednakże, w wypadku jakiejkolwiek niespójności między Specyfikacją Techniczną a ISO/IEC 15408, ta ostatnia, jako norma referencyjna przeważa.	metodą uznania
* Normy w końcowej fazie prac; spodziewany termin publikacji: koniec 2016 lub początek 2017 roku			
** Spodziewany termin publikacji: 2017 rok			

Tab. 2 Rekomendacje dla przyjęcia norm międzynarodowych z zakresy ochrony danych osobowych i prywatności do systemu PN

4. Normy dotyczące oceny bezpieczeństwa produktów i usług teleinformatycznych

4.1 Stan regulacji UE w odniesieniu do normalizacji

Działania na poziomie UE wynikają z identycznych przesłanek prawnych, jak te, które opisano w Rozdziałach 2.1 oraz 3.1. a także z Rozporządzenia 910/2014[13] (zwanego dalej Rozporządzeniem eIDAS).

W szczególności, w Rozporządzeniu eIDAS, wskazano normy jako źródło:

a) wymagań akredytacji dla jednostek oceniających zgodność oraz zasad audytu oceny zgodności kwalifikowanych dostawców usług zaufania,
b) oceny zgodności dla wiarygodnych produktów i usług stosowanych przez kwalifikowanego dostawcę usług zaufania,
c) oceny zgodności dla zaawansowanych podpisów elektronicznych,
d) oceny zgodności dla kwalifikowanych certyfikatów podpisów elektronicznych/ pieczęci elektronicznej,
e) wymagań dla kwalifikowanych urządzeń do składania podpisów elektronicznych/pieczęci elektronicznej
f) wymagań **certyfikacji** dla kwalifikowanych urządzeń do składania podpisów elektronicznych/pieczęci elektronicznej,
g) wymagań dla kwalifikowanej usługi walidacji kwalifikowanych podpisów elektronicznych/pieczęci elektronicznej,
h) wymagań dla kwalifikowanej usługi konserwacji kwalifikowanych podpisów elektronicznych/pieczęci elektronicznej,
i) wymagań dla kwalifikowanej usługi uwierzytelnienia witryny internetowej.

Przegląd normalizacji europejskiej dla wszystkich powyższych zagadnień zawiera raport ETSI TR 119 000 V1.1.1 (2015-09)[14]. W zakresie niniejszej ekspertyzy pozostaje zagadnienie certyfikacji urządzeń do składania podpisów elektronicznych/ pieczęci elektronicznej oraz innych urządzeń będących elementami mechanizmów identyfikacji elektronicznej lub uwierzytelniania w usługach on-line.

W dokumencie COM (2016) 410 final[15] wskazano kierunki działań wynikające z konieczności wdrożenia Dyrektywy NIS. Jednym z obszarów wymagających pilnego uregulowania jest certyfikacja bezpieczeństwa produktów i usług informatycznych. Zagadnienie to jest postrzegano jako czynnik mogący stanowić zagrożenie dla Jednolitego Rynku UE. Fragmentacja rynku może stać się faktem, jeśli zostaną wprowadzone różne wymagania bezpieczeństwa w różnych krajach UE jako wymogi certyfikacji bezpieczeństwa produktów i usług teleinformatycznych.

[13] Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE, http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32014R0910

[14] Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview, http://www.etsi.org/deliver/etsi_tr/119000_119099/119000/01.01.01_60/tr_119000v010101p.pdf

[15] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, https://ec.europa.eu/digital-single-market/en/news/communication-strenghtening-europes-cyber-resilience-system-and-fostering-competitive-and

Z powyższego względu są prowadzone na poziomie UE prace nad przyjęciem planu działań dla ogólnoeuropejskich ram certyfikacji bezpieczeństwa. Komisja Europejska zaproponowała następujący plan działań:

- Publiczne konsultacje zostaną przeprowadzone w 1. kwartale 2017r. W trakcie tych konsultacji Komisja będzie oczekiwać stanowiska wszystkich zainteresowanych (np. producentów komponentów i urządzeń ,operatorów infrastruktury krytycznej oraz użytkowników z sektora prywatnego i publicznego, krajów członkowskich, organizacji społecznych);
- Ocena skutków – planowana na 2. kwartał 2017r., wymagana w sytuacji gdy Komisja zamierza rozpoznać wariant regulacyjny w celu harmonizacji rynku za pośrednictwem ogólnoeuropejskich ram certyfikacji;
- Propozycja Komisji oczekiwana w 4. kwartale 2017r.

Jedną z zasad uzgodnionych na spotkaniach eksperckich organizowanych przez Komisję Europejską w odniesieniu do certyfikacji bezpieczeństwa produktów i usług teleinformatycznych jest przyjęcie jako podstawy ram certyfikacji bezpieczeństwa powszechnie uznawanych norm.

W tym kontekście należy wykazać dwie równoległe inicjatywy w postaci przyjmowania norm międzynarodowych (ogólne zasady, metody i techniki oceny bezpieczeństwa produktów i usług teleinformatycznych oraz norm europejskich (normy specyficzne, w odniesieniu do produktów związanych z wdrożeniem Rozporządzenia eIDAS).

4.2 Normy międzynarodowe w zakresie oceny bezpieczeństwa produktów i usług teleinformatycznych

W poniższej tabeli zestawiono normy, które mają znaczenie dla europejskich ram certyfikacji bezpieczeństwa produktów i usług teleinformatycznych, o których mowa w rozdziale 2.3 wspomnianego powyżej dokumentu COM (2016) 410 final.

Norma	Tytuł	Zakres	Rekomendowany tryb przyjęcia do systemu PN
Ocena bezpieczeństwa zgodnie z ISO/IEC 15408 oraz ISO/IEC 18045			
PN-ISO/IEC 15408-1:2016-10	ISO/IEC 15408-1 Technika informatyczna — Techniki pieczeństwa — Kryteria oceny zabezpieczeń informa-ɜnych -- Część 1: Wprowadzenie i model ogólny	W tej części ISO/IEC 15408 ustanowiono ogólne koncepcje i pryncypia oceny bezpieczeństwa informatycznego oraz zdefiniowano ogólny model oceny zgodnie z różnymi częściami tej Normy Międzynarodowej, którą należy używać w całości jako podstawy do oceny właściwości bezpieczeństwa produktów informatycznych. Niniejszy dokument zawiera przegląd wszystkich części ISO/IEC 15408. Opisano w nim różne części normy; zdefiniowano terminy ora skróty używane we wszystkich częściach Normy Międzynarodowej; ustanowiono podstawową koncepcję Przedmiotu Oceny (TOE – Target of Evaluation); kontekst oceny; oraz wskazano odbiorców, do których kryteria oceny są kierowane. Zawarto w nim wprowadzenie do podstawowych koncepcji bezpieczeństwa koniecznych do oceny produktów informatycznych. W niniejszym dokumencie zdefiniowano różne działania, dzięki którym komponenty: funkcjonalne oraz uzasadnionego zaufania, opisane w ISO/IEC 15408-2 i ISO/IEC 15408-3, mogą być dostosowane na zasadzie dozwolonych operacji. Opisano w nim kluczową koncepcję profili zabezpieczeń (PP – protection profiles), a także zagadnienie zgodności oraz konsekwencje oceny i wyników oceny. W niniejszej części ISO/IEC 15408 zawarto wytyczne do definiowania zadania zabezpieczeń (ST - Security Targets) oraz opisano organizację komponentów w całym modelu. Przedstawiono informacje ogólne o metodyce oceny opisanej w ISO/IEC TR 18045 i zakres schematów oceny.	obecnie - metodą uznania, docelowo - tłumaczenie

Norma	Tytuł	Zakres	Rekomendowany tryb przyjęcia do systemu PN
PN-ISO/IEC 15408-2:2016-10	ISO/IEC 15408-1 Technika informatyczna — Techniki bezpieczeństwa — Kryteria oceny zabezpieczeń informatycznych -- Część 2: Komponenty funkcjonalne zabezpieczeń	W niniejszej części ISO/IEC 15408 zdefiniowano wymaganą strukturę oraz zawartość komponentów funkcjonalnych zabezpieczeń w celu wykonywania ocen zabezpieczeń. Zawiera katalog komponentów funkcjonalnych spełniających wymagania funkcjonalne bezpieczeństwa wspólne dla wielu produktów IT	pozostawienie w formie uznania
PN-ISO/IEC 15408-3:2016-10	Technika informatyczna -- Techniki bezpieczeństwa -- Kryteria oceny zabezpieczeń informatycznych -- Część 3: Komponenty uzasadnienia zaufania do zabezpieczeń	W niniejszej części ISO/IEC 15408 zdefiniowano wymagania uzasadnienia zaufania ISO/IEC 15408. Zawiera poziomy uzasadnienia zaufania (EALs - evaluation assurance levels), które określają skalę pomiaru uzasadnienia zaufania do elementów TOE, złożone pakiety uzasadnienia zaufania (CAP – composed assurance packages), określające skalę pomiaru uzasadnienia zaufania do złożonych TOE, indywidualne komponenty uzasadnienia zaufania, z których są złożone poziomy uzasadnienia zaufania i pakiety oraz kryteria oceny PP i ST.	pozostawienie w formie uznania
PN-ISO/IEC 18045:2016-10	Technika informatyczna -- Techniki bezpieczeństwa -- Metodyka oceny zabezpieczeń informatycznych	Niniejsza Norma Międzynarodowa jest dokumentem towarzyszącym dla kryteriów oceny zabezpieczeń informatycznych zdefiniowanych w ISO/IEC 15408. W tym dokumencie określono minimalne działania, które oceniający mają wykonać w celu przeprowadzenia oceny zgodnie z ISO/IEC 15408, z użyciem kryteriów oraz dokumentacji oceny, określonych w ISO/IEC 15408. W niniejszej Normie Międzynarodowej nie określono działań oceniających w obszarze specyficznych komponentów ISO/IEC 15408 o wysokim poziomie uzasadnienia zaufania, co do których do tej pory nie wypracowano ogólnie uzgodnionych wytycznych.	pozostawienie w formie uznania

Norma	Tytuł	Zakres	Rekomendowany tryb przyjęcia do systemu PN
ISO/IEC TR 15443:2012	A framework for IT security assurance/ Ramy dla uzasadnionego zaufania do bezpieczeństwa informatycznego	Niniejszy dokument zawiera wytyczne dla profesjonalistów bezpieczeństwa informatycznego odnośnie do wyboru właściwej metody uzasadnienia zaufania przy określaniu, wyborze, lub wdrażaniu usługi, produktu lub elementu środowiskowego, takiego jak organizacja lub personel.	metodą uznania
ISO/IEC TR 15446:2009	Guide for the production of Protection Profiles and Security Targets/ Przewodnik do tworzenia profili zabezpieczeń oraz przedmiotów oceny	Niniejszy dokument zawiera wytyczne odnoszące się do budowania profili zabezpieczeń (Protection Profiles (PPs)) oraz przedmiotów oceny (Security Targets (STs)), które w zamierzeniu mają być zgodne z ISO/IEC 15408 (3 wyd.).	tłumaczenie
ISO/IEC 19608*	Guidance for developing security and privacy functional requirements based on ISO/IEC 15408	Niniejsza specyfikacja techniczna zawiera wytyczne do opracowywania wymagań funkcjonalnych dla prywatności jako rozszerzone komponenty, na podstawie pryncypiów prywatności zdefiniowanych w ISO/IEC 29100, w paradygmacie opisanym w ISO/IEC 15408-2.	tłumaczenie
ISO/IEC TR 20004:2015	Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045/ Doprecyzowanie analizy podatności oprogramowania zgodnie z ISO/IEC 15408 oraz ISO/IEC 18045	W tym raporcie technicznym doprecyzowano działania rodziny AVA_VAN w odniesieniu do identyfikowania, wyboru i oceny odpowiednich potencjalnych podatności w celu przeprowadzenia oceny programowego przedmiotu oceny zgodnie z ISO/IEC 15408.	metodą uznania
ISO/IEC TS 30104:2015	Physical security attacks, mitigation techniques and security requirements/ Ataki na bezpieczeństwo fizyczne. Techniki ograniczania oraz wymagania bezpieczeństwa	W tym raporcie technicznym omówiono, w jaki sposób określić uzasadnienie zaufania do bezpieczeństwa w odniesieniu do produktów, dla których środowiskowe ryzyko bezpieczeństwa wymaga stosowania mechanizmów ochrony fizycznej.	metodą uznania
Wymagania bezpieczeństwa dla modułów kryptograficznych i metody testowania			

Norma	Tytuł	Zakres	Rekomendowany tryb przyjęcia do systemu PN
ISO/IEC 19790:2012	Security requirements for cryptographic modules/ Wymagania bezpieczeństwa dla modułów kryptograficznych	W niniejszej normie międzynarodowej określono wymagania bezpieczeństwa dla modułów kryptograficznych wykorzystywanych w systemach bezpieczeństwa chroniących wrażliwe informacje w systemach komputerowych i telekomunikacyjnych.	metodą uznania
ISO/IEC 19792:2009	Security evaluation of biometrics/ Ocena bezpieczeństwa dla biometrii	W niniejszym dokumencie opisano zagadnienia, do których należy odnieść się podczas oceny bezpieczeństwa systemu biometrycznego.	metodą uznania
ISO/IEC 17825:2016	Testing methods for the mitigation of non-invasive attack classes against cryptographic modules/ Metody testowania w celu ograniczenia klas nieinwazyjnych ataków na moduły kryptograficzne	W niniejszej normie określono metryki testów ograniczających nieinwazyjne ataki w celu określenia zgodności z wymaganiami wskazanymi w ISO/IEC 19790:2012 dla poziomów bezpieczeństwa 3 i 4.	metodą uznania
ISO/IEC 18367:2016	Cryptographic algorithms and security conformance testing/ Algorytmy kryptograficzne i testowanie zgodności bezpieczeństwa	Dokument zawiera opis metod testowania zgodności algorytmów kryptograficznych oraz mechanizmów zabezpieczeń wdrożonych w module kryptograficznym .	metodą uznania
ISO/IEC 24759:2015	Test requirements for cryptographic modules/ Wymagania testowania dla modułów kryptograficznych	W niniejszej normie międzynarodowej określono metody, które mają być stosowane przez laboratoria dokonujące oceny w celu przetestowania, czy dany moduł kryptograficzny jest zgodny z wymaganiami wskazanymi w ISO/IEC 19790:2012.	metodą uznania
Pozostałe			
ISO/IEC 29128:2011	Verification of cryptographic protocols/ Weryfikacja protokołów kryptograficznych	Niniejszy dokument stanowi podstawę techniczną dla przeprowadzenia dowodu bezpieczeństwa specyfikacji protokołów kryptograficznych.	metodą uznania

Norma	Tytuł	Zakres	Rekomendowany tryb przyjęcia do systemu PN
ISO/IEC 29147:2014	Vulnerability Disclosure/ Ujawnienie podatności	Niniejszy dokument zawiera wytyczne do ujawniania potencjalnych podatności w produktach oraz usługach on-line.	metodą uznania
ISO/IEC 30111:2011	Vulnerability handling processes/ Procesy postepowania z podatnościami	Niniejsza norma zawiera wytyczne, w jaki sposób postępować z informacjami o potencjalnych podatnościach w produktach lub usługach on-line.	metodą uznania

* będzie dostępna w połowie 2017 roku

Tab. 3 Rekomendacje dla przyjęcia norm międzynarodowych z zakresy certyfikacji bezpieczeństwa do systemu PN

4.3 Normy europejskie w systemie PN, zawierające profile zabezpieczeń

Profile zabezpieczeń są przyjętą w normie ISO/IEC 5408 metodą opisu wymagań bezpieczeństwa dla konkretnej klasy produktów jako podzbioru wszystkich wymagań opisanych w tej normie. Przygotowanie produktu zgodnie z profilem zabezpieczeń ułatwia i skraca okres badań i testów służących do oceny, a następnie certyfikacji bezpieczeństwa. Taka metoda została przyjęta jako podstawa dla certyfikacji produktów z obszaru Rozporządzenie eIDAS, a opracowane profile zabezpieczeń wydano jako normy europejskie. Te normy zostały następnie przyjęte do systemu PN metodą uznania, co przedstawiono w poniższej tabeli.

Norma	Tytuł	Zakres	Rekomendowany tryb przyjęcia do systemu PN
PN-EN 419211-1:2014	Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu. Część 1: Przegląd	W niniejszej normie europejskiej: — zdefiniowano terminy używane w określonych profilach zabezpieczeń dla bezpiecznych urządzeń do składania podpisów, — określono wymagania funkcjonalne i operacyjne dla bezpiecznych urządzeń do składania podpisów, — opisano cele oceny dla tych profili zabezpieczeń.	pozostawienie w formie uznania
PN-EN 419211-2:2014	Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu. Część 2: Urządzenie z generowaniem kluczy	W niniejszej normie europejskiej określono profil zabezpieczeń dla bezpiecznego urządzenia do składania podpisów, które może wewnętrznie generować klucze podpisujące (secure signature creation device with key generation (SSCD KG)).	pozostawienie w formie uznania
PN-EN 419211-3:2014	Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu. Część 3: Urządzenie z importem kluczy	określono profil zabezpieczeń dla bezpiecznego urządzenia do składania podpisów, z możliwością importu kluczy (secure signature creation device with signing keys import possibility: SSCD with key import (SSCD KI)).	pozostawienie w formie uznania
PN-EN 419211-4:2014	Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu. Część 4: Rozszerzenie dla urządzenia z generowaniem kluczy i bezpiecznym kanałem z aplikacją generującą certyfikaty	W niniejszej normie europejskiej określono profil zabezpieczeń dla bezpiecznego urządzenia do składania podpisów, które może wewnętrznie generować klucze podpisujące oraz eksportować w bezpieczny sposób klucz publiczny (secure signature creation device with key generation and trusted communication with trusted channel certificate generation application (SSCD KG TCCGA)).	pozostawienie w formie uznania

Norma	Tytuł	Zakres	Rekomendowany tryb przyjęcia do systemu PN
PN-EN 419211-5:2014	Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu Część 5: Rozszerzenie dla urządzenia z generowaniem kluczy i bezpiecznym kanałem z aplikacją podpisującą	W niniejszej normie europejskiej określono profil zabezpieczeń dla bezpiecznego urządzenia do składania podpisów, które może wewnętrznie generować klucze podpisujące oraz komunikować się w bezpieczny sposób z aplikacją do składania podpisów (secure signature creation device with key generation and trusted communication with signature creation application (SSCD KG TCSCA)).	pozostawienie w formie uznania
PN-EN 419211-6:2014	Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu. Część 6: Rozszerzenie dla urządzenia z importem kluczy i bezpiecznym kanałem z aplikacją podpisującą	W niniejszej normie europejskiej określono profil zabezpieczeń dla bezpiecznego urządzenia do składania podpisów, które może importować klucze podpisujące oraz komunikować się w bezpieczny sposób z aplikacją do składania podpisów (secure signature creation device with key import and trusted communication with signature creation application (SSCD KI TCSCA)).	pozostawienie w formie uznania
PN-EN 419212-1:2015	Interfejs aplikacyjny dla kart elektronicznych stosowanych jako bezpieczne urządzenia do składania podpisu elektronicznego. Część 1: Usługi podstawowe	W niniejszej normie europejskiej określono mechanizmy zainstalowane na kartach elektronicznych wykorzystywanych jako bezpieczne urządzenia do składania podpisów, obejmując: • tworzenie podpisów; • weryfikację użytkownika; • uwierzytelnienie na podstawie hasła; • uwierzytelnienie urządzenia; •ustanowienie bezpiecznego kanału. Zdefiniowane mechanizmy są przydatne do innych celów, takich jak usługi w kontekście identyfikacji, uwierzytelniania i podpisów cyfrowych.	pozostawienie w formie uznania

Norma	Tytuł	Zakres	Rekomendowany tryb przyjęcia do systemu PN
PN-EN 419212-2:2015	Interfejs aplikacyjny dla kart elektronicznych stosowanych jako bezpieczne urządzenia do składania podpisu elektronicznego. Część 2: Usługi dodatkowe	Niniejsza norma międzynarodowa zawiera opisy usług identyfikacji, uwierzytelniania i podpisów cyfrowych (IAS) jako dodatkowych w stosunku do mechanizmów SSCD opisanych już w EN 419212-1 w celu umożliwienia interoperacyjności i wykorzystania usług IAS na poziomie krajowym lub europejskim. Ponadto opisano w niej dodatkowe mechanizmy, takie jak odszyfrowywanie klucz, uwierzytelnianie klient - serwer, zarządzanie tożsamością oraz usługi związane z prywatnością.	pozostawienie w formie uznania
PN-EN 419251-1:2013	Wymagania bezpieczeństwa dla urządzenia do uwierzytelniania. Część 1: Profil zabezpieczeń dla funkcjonalności podstawowej	Niniejsza norma międzynarodowa zawiera profil zabezpieczeń, który określa wymagania bezpieczeństwa dla urządzenia służącego do uwierzytelnienia.	pozostawienie w formie uznania
PN-EN 419251-2:2013	Wymagania bezpieczeństwa dla urządzenia do uwierzytelniania. Część 2: Profil zabezpieczeń dla rozszerzenia o wiarygodny kanał komunikacyjny z aplikacją generującą certyfikaty	Niniejsza norma międzynarodowa zawiera profil zabezpieczeń, który określa wymagania bezpieczeństwa dla urządzenia służącego do uwierzytelnienia.	pozostawienie w formie uznania
PN-EN 419251-:2013	Wymagania bezpieczeństwa dla urządzenia do uwierzytelniania. Część 3: Dodatkowa funkcjonalność dla zadań zabezpieczeń*	Niniejsza norma międzynarodowa zawiera pakiety, który określają wymagania bezpieczeństwa dla urządzenia służącego do uwierzytelnienia. W części 1 i 2 zawarto opisy profili zabezpieczeń, (PP), których podstawą są pakiety zdefiniowane w niniejszym dokumencie. Pakiety zawarte w tym dokumencie mogą być dodane do celu bezpieczeństwa (ST), spełnianego przez PP z części 1 lub 2.	pozostawienie w formie uznania

Tab. 4 Normy europejskie z zakresu certyfikacji bezpieczeństwa w obszarze Rozporządzenia eIDAS w systemie PN

5. Podsumowanie – rekomendacje do działań MC

Normalizacja jest postrzegana przez Unię Europejską jako bardzo ważny czynnik zwiększenia konkurencyjności przedsiębiorstw, ułatwiając w szczególności swobodny przepływ towarów i usług, interoperacyjność sieci, funkcjonowanie środków komunikacji, rozwój technologiczny i innowacyjność. Normy są podstawą do przeprowadzenia oceny lub domniemania zgodności produktów lub usług z wymaganiami wskazanymi w prawodawstwie Unii. Normy zawierające szczegółowe specyfikacje techniczne dają producentom lub dostawcom pewność, że nie dokonują błędnych interpretacji ogólnych wymagań zawartych w przepisach prawa. Z kolei konsumenci mogą polegać na zapewnieniu zgodności z odpowiednimi normami, potwierdzonej przez niezależne jednostki oceny zgodności, jako podstawy zaufania do bezpieczeństwa oferowanego produktu lub usługi.

Z zawartych w poprzednich rozdziałach informacji wynika bezpośredni związek wprowadzonych przepisów prawa unijnego z mechanizmami ich wdrażania na podstawie odpowiednich norm.

Podkreślając dobrowolność stosowania norm, w przepisach prawa unijnego znajdują się zachęty i pośrednie wskazanie korzyści ze stosowania norm międzynarodowych, w tym w szczególności europejskich.

W Dyrektywie NIS wskazuje się zgodność z określonymi normami jako metody zapewnienia wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych na poziomie Unii. Odpowiednie akty prawa krajowego wdrażające Dyrektywę powinny powstać przed terminem jej wejścia w życie (lipiec 2018 roku).

W Rozporządzeniu 2016/679/WE przewiduje się wygaśnięcie obowiązywania Dyrektywy 95/46/WE w dniu 25 maja 2018 roku oraz odpowiednich przepisów prawa krajowego (w Polsce Ustawy o ochronie danych osobowych). Należy przewidzieć modyfikacje wymagań odnoszących się do przetwarzania danych osobowych zawartych w polskich przepisach prawa. Warto podkreślić, że Rozporządzenie to stanowi podstawę ujednolicenia specyfikacji technicznych, wytycznych i dobrych praktyk w krajach UE, zawartych w normach międzynarodowych lub normach unijnych.

W Rozporządzeniu eIDAS wskazuje się na potrzebę certyfikacji urządzeń do składania podpisów elektronicznych/ pieczęci elektronicznej oraz innych urządzeń będących elementami mechanizmów identyfikacji elektronicznej lub uwierzytelniania w usługach on-line.

Działania związane z wdrażaniem wskazanych przepisów prawa będą znacznie zintensyfikowane w 2017 roku.

Z powyższych względów rekomenduje się następujące działania:

1. Uwzględnienie przy tworzeniu lub modyfikacji aktów prawnych Polskich Norm, będących odpowiednikami norm europejskich lub norm międzynarodowych, przez odniesienie do tych norm jako referencyjnych, wskazanych na poziomie UE;
2. Wsparcie dla działań normalizacyjnych skierowanych na wprowadzanie norm międzynarodowych do systemu PN; pod rozwagę podaje się podjęcie współpracy z Ministerstwem Rozwoju w celu opracowania długofalowego planu działań (strategii) dla normalizacji jako czynnika wsparcia rozwoju społeczno-gospodarczego w ogólności, nie tylko w sektorze teleinformatyki i komunikacji;
3. Upowszechnianie i wsparcie dla edukacji w zakresie norm technicznych jako podstawy do certyfikacji bezpieczeństwa i prywatności produktów i usług teleinformatycznych w zakresie wynikającym z przepisów prawa unijnego.