Macierz kompetencji eIDAS – propozycja podziału zadań w Polsce w ramach niezbędnych prac związanych z wdrożeniem rozporządzenia eIDAS w zakresie legislacji, świadczenia usług, nadzoru, dostosowania usług administracji.

Rekomendacja zespołu ds. metod uwierzytelniania (ZMU) powołanego Decyzją Nr 2/2015 Przewodniczącego KRMC.

Warszawa, 24.05.2015 r.

1 WPROWADZENIE

W Dzienniku Urzędowym Unii Europejskiej z dnia 28 sierpnia 2014 r. opublikowane zostało Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L z dn. 28 sierpnia 2014 r.). Obecnie trwają w KE prace legislacyjne nad aktami implementującymi i delegowanymi do rozporządzenia eIDAS. Akty o charakterze obligatoryjnym będą wydane do dn. 1 lipca 2016 r. Akty o charakterze fakultatywnym będą wydawane w terminie późniejszym w zależności od dostępności norm, standardów i specyfikacji technicznych. W tle przedmiotowych prac prowadzone są prace standaryzacyjne w zakresie mandatu M460, które mają doprowadzić do racjonalizacji ram standaryzacyjnych usług zaufania. Z uwagi na dynamiczny charakter zmian w otoczeniu prawnym i standaryzacyjnym przedmiotowe zestawienie zadań będzie w przyszłości dostosowywane. Urzędy zaangażowane w przedmiotowe prace mogą zgłaszać w przyszłości zidentyfikowane nowe zagadnienia lub poprawki pozostające w związku z rozporządzeniem eIDAS.

Poniżej opisano zadania koordynacyjne w zakresie systemu notyfikacji eID Krajów Członkowskich UE, w tym obowiązki wynikające z przyjęcia COMMISSION IMPLEMENTING DECISION establishing procedural arrangements of the cooperation between Member States on electronic identification pursuant to Article 12(7) of the Regulation 910/2014 on electronic identification and trust services for electronic transaction in the internal market.

23 lipca 2014 przyjęte zostało Rozporządzenie Parlamentu Europejskiego i Rady dotyczące elektronicznej identyfikacji i usług zaufania dla transakcji elektronicznych na rynku wewnętrznym (eIDAS)[1]. Rozporządzenie to od momentu wejścia w życie w dn. 17 września 2014 jest aktem prawnym obowiązującym bezpośrednio w prawodawstwie krajów członkowskich, co oznacza, że państwa członkowskie muszą ściśle stosować się do zapisów Rozporządzenia, a przepisy prawne mogą co najwyżej regulować punkt styku z prawodawstwem krajowym, oraz zagadnienia jawnie wskazane jako regulowane w prawodawstwie państw członkowskich. Zapisy Rozporządzenia wprowadzają terminy stosowania dla regulowanych obszarów identyfikacji i uwierzytelnienia, oraz usług zaufania. Rozporządzenie wchodzi do stosowania co do zasady w dn. 1 lipca 2016 roku. Odroczenie do 2018 roku stosowania przepisów rozporządzenia w obszarze eID jest podyktowane koniecznością wytworzenia norm i standardów, dostosowania prawodawstwa i systemów administracji publicznej państw członkowskich.

Rozporządzenie eIDAS zastąpi dyrektywę 99/93/WE w sprawie wspólnotowych ram prawnych dla podpisów elektronicznych. Ze względu na fakt, iż Ustawa o podpisie elektronicznym jest implementacją dyrektywy 99/93/WE, zostanie ona docelowo uchylona. Z uwagi na przypadające w roku bieżącym wybory do Sejmu RP termin realizacji tego zadania zależeć będzie od kalendarza prac parlamentarnych. Ustawa ureguluje obszary dopuszczone przez Rozporządzenie do regulacji prawem krajowym.

25 lutego 2015 roku opublikowano w oficjalnym dzienniku UE pierwszy akt wykonawczy Komisji Europejskiej dotyczący procedury definiującej współpracę Państw Członkowskich (Procedural Arrangement of the Cooperation), w konsekwencji głosowania Krajów Członkowskich ,które miało miejsce na pierwszym posiedzeniu eIDAS Commitee 14 stycznia 2015 r. i rekomendowało przyjęcie aktu implementującego kwalifikowaną większością głosów. Akt ten, zgodnie z zasadami wynikającymi z art. 291 Traktatu o Funkcjonowaniu Unii Europejskiej (TFUE), uzupełnia poprzez wskazanie sposobu wykonania akt podstawowy jakim jest rozporządzenie 210/2014 w zakresie ustanowienia procedury szczegółowo określając zasady współpracy Krajów Członkowskich w procesie przygotowania

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

przeprowadzenia notyfikacji narzędzi identyfikacji elektronicznej, wskazania zakresu dokumentacji niezbędnej w procesie notyfikacji i objętej obowiązkową unifikacją językową (język angielski) oraz określenia obowiązków Krajów Członkowskich pozwalających na zunifikowany kontakt różnych instytucji i kompetentnych ciał (single point of contact – pojedynczy punkt kontaktowy). Dokument określa zadania i sposób przeprowadzenia procesu poprzedzającego finalna notyfikację (peer review-ścieżka przeglądu), określa reżim czasowy tego procesu, nakłada obowiązki terminowego przekazywania dokumentów oraz określa formę organizacyjną tej współpracy (cooperation network). Dokument zapewnia też każdemu Krajowi Członkowskiemu możliwość uczestnictwa w pracach cooperation network, pozostawiając do jego suwerennej decyzji czy chce uczestniczyć w pracach tego ciała w ramach konkretnego procesu peer review.

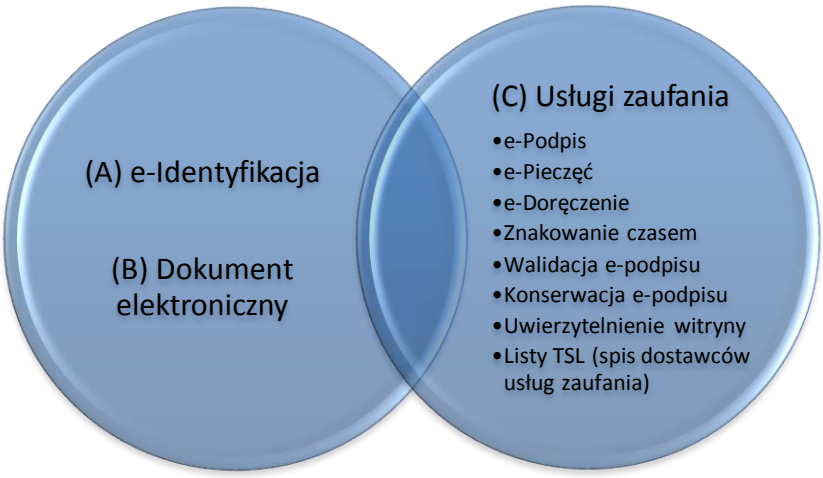
Zważywszy na postanowienie zawarte w Art. 3:

- Dla zapewnienia współpracy pomiędzy Krajami Członkowskimi stosownie do Art. 12(5) i (6) rozporządzenia (EU) No 910/214, każdy Kraj Członkowski powinien ustanowić pojedynczy punkt kontaktowy
- Każdy Kraj Członkowski powinien poinformować inne Kraje Członkowskie oraz Komisję o ustanowieniu takiego punktu kontaktowego. Komisja opublikuje listę takich punktów kontaktowych (tłum. MU) on-line

należy ustanowić podział kompetencji pomiędzy resortami przy wdrożeniu i realizacji rozporządzenia eIDAS. Niezbędne będzie wskazanie Komisji pojedynczego punktu kontaktu dla notyfikacji eID. Akt delegowany nie określa szczegółowo zakresu informacji jaka musi być przekazana, ale jest to co najmniej adres e-mailowy (tak należy rozumieć użyte określenie on-line), właściwy do otrzymywania i przekazywania informacji pomiędzy innymi Krajami Członkowskimi oraz Komisją.

Zakres Rozporządzenia

Rozporządzenie eIDAS obejmuje obszar szerszy niż dyrektywa 99/93/EC o wspólnotowych ramach dla podpisu elektronicznego. Rozporządzenie reguluje usługi zaufania oraz notyfikację elektronicznej identyfikacji. Dyrektywa obejmowała tylko podpis elektroniczny z wzmianką w preambule nt. możliwości znakowania czasem. Rozporządzenie eIDAS określiło usługi certyfikacyjne podpisu elektronicznego oraz usługi otoczenia mianem „usług zaufania". Zdefiniowano także dodatkowe usługi zaufania oraz pozostawiono Państwom Członkowskim swobodę regulowania niezharmonizowanych prawem krajowym usług. Państwa członkowskie mogą przewidzieć w tym zakresie zarówno usługi niekwalifikowane, jak i usługi krajowe kwalifikowane.



Rysunek 1 Poglądowy zarys obszarów regulacji eIDAS

Rozporządzenie nie unifikuje kwestii elektronicznej identyfikacji. Materia ta będzie mogła być nadal regulowana prawem państw członkowskich. Państwa Członkowskie będą mogły tworzyć i utrzymywać wg swojego uznania systemy elektronicznej identyfikacji. W obszarze wzajemnego uznawania elektronicznej identyfikacji Komisja Europejska w ciągu kilku ostatnich lat realizowała duże projekty pilotażowe (ang. Large Scale Pilots). Najistotniejszym w tym obszarze jest projekt STORK i STORK2, który zbudował podwaliny pod model huba elektronicznej identyfikacji dla UE/EOG.

Pojęcie usług zaufania odnosi się do usług zaufania świadczonych przez podmioty mające swoją siedzibę na obszarze UE. Są to usługi, które dotychczas znane były jako usługi związane z podpisem elektronicznym. Nadzór przewidziany explicite rozporządzeniem dotyczy wyłącznie usług zaufania. Najważniejsze usługi tego rodzaju to usługi podpisu i pieczęci elektronicznej. Usługi pieczęci elektronicznej tworzonej rozporządzeniem eIDAS będą realizowane z wykorzystaniem dotychczasowych formatów podpisu elektronicznego tak, aby do jej składania i weryfikacji mogły być stosowane aplikacje podpisu elektronicznego.

W odniesieniu do innych usług zaufania (rejestrowane doręczenia elektroniczne, znakowanie czasem, walidacja podpisów, konserwacja podpisów) zdefiniowano skutki prawne, albo co najmniej wskazano, że produkty tych usług posiadają wartość dowodową. W odniesieniu do kwalifikowanych certyfikatów witryn internetowych nie zdefiniowano ani skutków prawnych, ani nie wskazano wartości dowodowej.

Z zakresu Rozporządzenia eIDAS oraz nadzoru państw członkowskich wyłączono „systemy zamknięte" (takie jak np. DOCert w NBP).

W celu technicznego dostosowania w obszarze usług zaufania Komisja Europejska wydała mandat standaryzacyjny m460. W ramach mandatu finansowane jest wytworzenie przez ETSI i CEN standardów opisujących obszar usług zaufania.

Obowiązki wobec administracji publicznej

Rozporządzenie eIDAS nakłada szereg obowiązków stosujących się do administracji publicznej. Między innymi wprowadza obowiązki:

- Akceptowania na zasadzie wzajemności[2] **przez usługi online administracji publicznej notyfikowanych systemów identyfikacji elektronicznej** z obszaru Unii Europejskiej (art. 6) – zasadniczo w terminie do roku 2018 (w terminie 3 lat od dnia przygotowania aktów wykonawczych),
- Akceptowania na zasadzie wzajemności **podpisów i pieczęci elektronicznych zaawansowanych i kwalifikowanych[3]** z całego obszaru Unii Europejskiej (art. 27 i art. 37) – w terminie do dn. 1 lipca 2016.

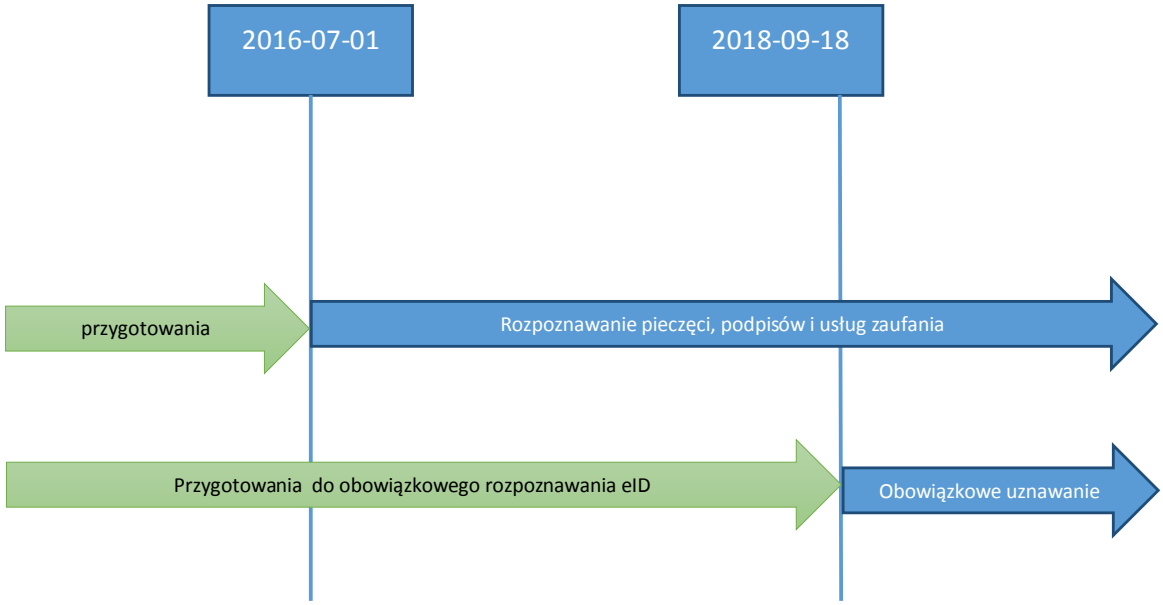
[2] W ramach Rozporządzenia wyróżniono trzy poziomy bezpieczeństwa środków identyfikacji elektronicznej, które muszą być akceptowane na zasadzie wzajemności (poziom high i substantial), albo dobrowolnie (poziom low). Środki identyfikacji na poziomie takim samym lub wyższym powinny być akceptowane w tych usługach, które wymagają krajowej identyfikacji elektronicznej na odpowiednio takim samym poziomie

[3] W przypadku usług administracji publicznej wymagających złożenia pieczęci/podpisu zaawansowanego wymaga się uznawania odpowiednio podpisów/pieczęci zaawansowanych i kwalifikowanych z całego obszaru UE, natomiast w przypadku usług wymagających złożenia podpisów/pieczęci kwalifikowanych wymaga się uznawania wyłącznie pieczęci/podpisów kwalifikowanych z całego obszaru UE.

W odniesieniu do innych usług zaufania (rejestrowane doręczenia elektroniczne, znakowanie czasem, walidacja podpisów, konserwacja podpisów) zdefiniowano skutki prawne, albo co najmniej wskazano, że produkty tych usług posiadają wartość dowodową.

W odniesieniu do kwalifikowanych certyfikatów witryn internetowych nie zdefiniowano ani skutków prawnych ani nie wskazano wartości dowodowej.

Wejście w życie obowiązków wobec administracji publicznej jest realizowane zgodnie z poniższym harmonogramem:



Rysunek 2 Kluczowe daty odnoszące się do obowiązków administracji publicznej

Termin 1 lipca 2016 dla wejścia do stosowania Rozporządzenia eIDAS w odniesieniu do obszaru usług zaufania determinuje moment wejścia w życie obowiązków odnoszących się do rozpoznawania podpisów, pieczęci i uznawania jako materiał dowodowy produktów usług zaufania.

Rozporządzenie przewiduje również termin obowiązkowego uznawania środków identyfikacji elektronicznej. Została ona określona w odniesieniu do terminów wejścia w życie aktów implementujących. Trzy lata po wejściu w życie aktów implementujących państwa członkowskie obowiązkowo muszą uznawać środki identyfikacji elektronicznej z obszaru UE. Termin publikacji aktów implementujących został określony na 2015-09-18. Po uwzględnieniu 3 lat otrzymujemy datę 2018-09-18.

Odpowiedzialność administracji publicznej

Państwa członkowskie będą mogły doregulować krajowymi przepisami ogólne zasady odpowiedzialności za usługi zaufania oraz notyfikowane systemy elektronicznej identyfikacji. O ile w przypadku usług zaufania istnieje określony dorobek w zakresie odpowiedzialności odszkodowawczej i systemu ubezpieczeń to brak jest gotowych rozwiązań w zakresie odpowiedzialności za notyfikowane systemy eID.

Odpowiedzialność Kraju Członkowskiego w którym ma siedzibę serwis publiczny do którego dostęp chce uzyskać posiadacz środka identyfikacji elektronicznej wydanego w innym kraju członkowskim to artykuł 11 ust. 5 ma zastosowanie w stosunku do stron transakcji, czyli podmiotów które w niej uczestniczyły. Oznacza to roszczenia tych podmiotów według litery prawa krajowego, nie oznacza

odpowiedzialności państwa. Państwo może odpowiadać na zasadach ogólnych, wynikających z niezastosowania się do rozporządzenia przez stronę która doznała uszczerbku w swoich interesach. Może to też uczynić Komisja Europejska.

Zagadnienia obejmujące podział kompetencji

Z wymienionymi obszarami (zarówno usług zaufania, jak i eID) wiążą się zagadnienia związane z:

- nadzorem nad świadczeniem usług,
- legislacją precyzującą obszary notyfikacji/przyznawania statusu usługi kwalifikowanej,
- legislacją związaną ze stosowaniem narzędzi w Polsce,
- koordynacją wdrożenia zmian będących skutkiem obowiązków nałożonych przez Rozporządzenie eIDAS,
- pełnieniem roli pojedynczego punktu kontaktu w zakresie notyfikacji eID.

Charakter zadań i wstępna propozycja podziału kompetencji pomiędzy resorty została zarysowana w ramach Ministerstwie Administracji i Cyfryzacji przy współpracy Ministerstwa Gospodarki. Podział został przekazany w ramach konsultacji do Ministerstwa Spraw Wewnętrznych.

Członkami ZMU są członkowie Komitetu Rady Ministrów do spraw Cyfryzacji z:

a) Ministerstwa Administracji i Cyfryzacji,

b) Ministerstwa Gospodarki,

c) Ministerstwa Finansów,

d) Ministerstwa Spraw Wewnętrznych,

e) Ministerstwa Sprawiedliwości,

f) Ministerstwa Zdrowia;

g) Szef Agencji Bezpieczeństwa Wewnętrznego.

Dodatkowo zaproszony został członek Komitetu Rady Ministrów do spraw Cyfryzacji z Ministerstwa Infrastruktury i Rozwoju.

2 MACIERZ KOMPETENCJI – ZAKRES PRAC ZWIĄZANYCH Z IMPLEMENTACJĄ EIDAS W LATACH 2016-2018

---	**2016-07-01**								**2018-09**
--	**listy TSL**	**e-podpis**	**e-pieczęć /znakowanie czasem**	**e-doręczenie**	**walidacja e-podpisu[4]**	**konserwacja e-podpisu**	**uwierzytelnienie witryny**	**dokument elektroniczny**	**Notyfikacja e-Identyfikacji (eID)**
Legislacja	MG/MAiC (w zakresie KRI)	MG/MAiC (w zakresie KRI)	MG/MAiC (w zakresie KRI)	MG/MAiC/ MS (resort)	MG	MG/MAiC	MG	MAiC/MKiDN (NDAP)	MAiC
Świadczone usługi	NBP	komercja/MZ/ MAiC (PZ)	komercja	komercja/ MAiC	komercja	komercja /NDAP	komercja	-	MAiC/MSW/ komercja
Nadzór	MG	MG	MG	MG	MG	MG	MG	-	MAiC[5]
Dostosowanie usług administracji	Urzędy/MAiC	Urzędy/MAiC	Urzędy/MAiC	Urzędy/ MAiC	Urzędy/ MAiC	Urzędy/ MAiC	Urzędy/ MAiC	-	Urzędy/MAiC

[4] Walidacja podpisu na potrzeby niniejszego opracowania obejmuje także walidację przy pomocy dedykowanych aplikacji. Jest to zakres szerszy niż w przypadku kwalifikowanych usług walidacji.

[5] Precyzyjne określenie organu właściwego do spraw nadzoru notyfikacji eID oraz zakresu tego nadzoru nastąpi w terminie późniejszym. Wprowadzenie nadzoru nad procesem notyfikacji nie wynika wprost z treści eIDAS ale z wprowadzanej przez eIDAS odpowiedzialności odszkodowawczej państwa za notyfikowane systemy eID. W konsekwencji wskazane jest, aby istniała procedura dopuszczenia oraz wycofania z notyfikacji, oraz środki do kontroli deklarowanego poziomu bezpieczeństwa. Notyfikacją mogą być objęte zarówno systemy eID sektora publicznego jak i sektora prywatnego.

3 ZADANIA WYNIKAJĄCE Z PODZIAŁU KOMPETENCJI

3.1 Zadania MAiC

Lp.	Obszar	Zadania
1.	eID	– Punkt kontaktowy – Nadzór nad notyfikacją eID – Kampania informacyjna dla urzędów – Budowa krajowego węzła eID (Hub'a) – Budowa referencyjnych bibliotek klienckich do Huba – Program dostosowania jednostek AP do HUB – Dostosowanie Dostawcy Tożsamości Profilu Zaufanego do wymagań poziomu "substantial" eID – Szkolenia, bazy wiedzy etc. – Weryfikacja zgodności, testy interfejsowe
2.	listy TSL	– Aktualizacja wsparcia dla list TSL w ePUAP – Budowa referencyjnych bibliotek do walidacji podpisu/pieczęci z wykorzystaniem list TSL
3.	e-podpis	– Kampania informacyjna w zakresie podpisów elektronicznych. – Dostosowanie ePUAP oraz skoordynowanie dostosowania pozostałych systemów informatycznych administracji- w zakresie mechanizmów podpisu do akceptacji podpisów z innych państw członkowskich UE/EOG – Dostosowanie ePUAP - nowe algorytmy kryptograficzne oraz inne zmiany standaryzacyjne (np. inny format pola serialNumber) – Budowa referencyjnych bibliotek do walidacji podpisu/pieczęci z wykorzystaniem list TSL – Kampania informacyjna dla urzędów – Program dostosowania jednostek AP do obsługi formatów podpisu (XAdES, CAdES, PAdES,ASiC) – Wsparcie dla administracji, szkolenia, wytyczne, testy (weryfikacja gotowości administracji rządowej i samorządowej do akceptowania podpisów kwalifikowanych z innych państw członkowskich UE/EOG).
4.	e-pieczęć /znakowanie czasem	– Kampania informacyjna w zakresie pieczęci elektronicznych. Dostosowanie ePUAP - mechanizmy pieczęci – Budowa referencyjnych bibliotek do składania/walidacji podpisu/pieczęci z wykorzystaniem list TSL – Kampania informacyjna dla urzędów – Program dostosowania jednostek AP do obsługi formatów pieczęci (XAdES, CAdES, PAdES,ASiC) – Wsparcie dla administracji, szkolenia, bazy wiedzy, testy.
5.	e-doręczenie	– Kampania informacyjna w zakresie rozwiązań e-delivery Standaryzacja procesu doręczeń krajowych – Wdrożenie standardu unijnego po jego wypracowaniu – Przygotowanie rozwiązań referencyjnych dla sektora publicznego i obywateli

		– Projekt gateway'a translującego pomiędzy e-delivery UE, a skrzynką podawczą. – Przygotowanie konkursu na dostosowanie do e-delivery końcówek klienckich
6.	walidacja e-podpisu	– Kampania informacyjna w zakresie walidacji podpisów/pieczęci. Skoordynowane dostosowanie systemów administracji publicznej do obsługi podpisów z krajów UE/EOG. – Wykorzystanie SD-DSS i/lub budowa referencyjnych bibliotek do walidacji podpisu/pieczęci z wykorzystaniem list TSL – Program dostosowania jednostek AP do walidacji pieczęci i podpisów (XAdES, CAdES, PAdES,ASiC) – Wsparcie dla administracji, szkolenia, bazy wiedzy, testy.
7.	konserwacja e-podpisu	– Kampania informacyjna – Budowa referencyjnych bibliotek do konserwacji podpisu - patrz rozwiązania niemieckie – Program dostosowania jednostek administracji i archiwów do wymogów eIDAS – Wsparcie dla administracji, szkolenia, bazy wiedzy, testy
8.	uwierzytelnienie witryny	– kampania informacyjna - urzędy nie muszą wymieniać certyfikatów witryn, no chyba że z wprowadzanym przez eIDAS kwalifikowanym certyfikatem uwierzytelnienia strony powiązany zostanie jakiś skutek prawny
9.	dokument e-elektroniczny	– Zgodnie z Krajowymi Ramami Interoperacyjności oraz przepisami o zasobach archiwalnych.

3. 2 Zadania MG

Lp.	Obszar	Zadania
1.	legislacja	– opracowanie projektu ustawy o usługach zaufania
2.	nadzór	– dostosowanie nadzoru do możliwości kontroli nowych usług kwalifikowanych i nadzór ad hoc usług niekwalifikowanych
3.	nadzór	– dostosowanie nadzoru do pozostałych wymagań eIDAS
4.	nadzór	– wzmocnienie obsady nadzoru – MG we współpracy z Prezesem RM, Szefem Służby Cywilnej (art. 17. 1 eIDAS - Organom nadzoru przyznaje się uprawnienia i odpowiednie zasoby niezbędne do wykonywania ich zadań)
5.	usługi zaufania	– skoordynowanie dostosowania kwalifikowanych dostawców usług zaufania do wymogów eIDAS
6.	certyfikacja	– opracowanie przez PCA we współpracy z MG programu akredytacji dla systemu oceny zgodności usługodawców zaufania
7.	e-podpis	– wdrożenie przez NBP we współpracy z MG zmian w listach TSL

3.3 Zadania urzędów

Lp.	Obszar	Zadania
1.	eID	– Udział w programach integracji z Hub – Dostosowanie systemów własnych, zgłaszanie potrzeb dostosowania programu
2.	listy TSL	– Udział w programach dostosowania – Dostosowanie systemów własnych, zgłaszanie potrzeb do programu
3.	e-podpis	– Udział w programach dostosowania – Dostosowanie systemów własnych w zakresie składania i weryfikacji podpisu (do obsługi przynajmniej podpisów kwalifikowanych z państw UE/EOG przy użyciu list TSL), zgłaszanie potrzeb do programu
4.	e-pieczęć	– Udział w programach dostosowania – Dostosowanie systemów własnych, zgłaszanie potrzeb do programu
5.	e-doręczenie	– Udział w programach dostosowania – Dostosowanie systemów własnych, zgłaszanie potrzeb do programu
6.	walidacja e-podpisu	– Udział w programach dostosowania – Dostosowanie systemów własnych, zgłaszanie potrzeb do programu
7.	konserwacja e-podpisu	– Udział w programach dostosowania – Dostosowanie systemów własnych, zgłaszanie potrzeb do programu
8.	uwierzytelnienie witryny	– Stosowanie
9.	dokument elektroniczny	– Uznawanie

Dokument opracowany przez zespół ekspertów na zlecenie MAiC

Wszelkie uwagi i komentarze w sprawie ewentualnych nowo zidentyfikowanych zagadnień, celem dostosowania dokumentu, należy kierować na adres: krmc@mac.gov.pl