Podpis elektroniczny – regulacje i praktyka

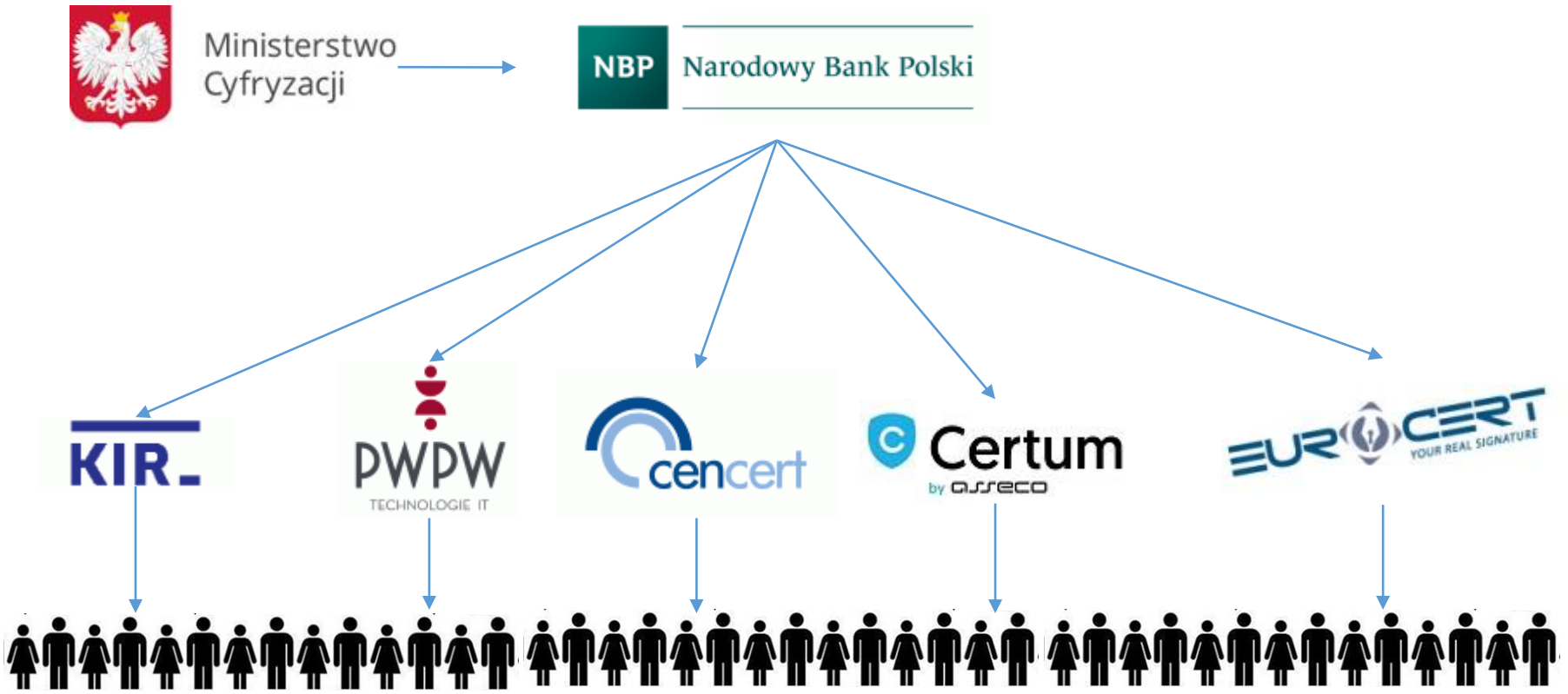
Program Operacyjny Wiedza Edukacja Rozwój

Oś priorytetowa II: Efektywne polityki publiczne dla rynku pracy, gospodarki i edukacji

Działanie 2.18: Wysokiej jakości usługi administracyjne

Bartosz Nakielski

Warszawa, 11 września 2018 r.


Ministerstwo Cyfryzacji
NBP
Narodowy Bank Polski
KIR
PWPW
TECHNOLOGIE IT
cencert
Certum
by asseco
EUROCERT
YOUR REAL SIGNATURE

Podpis elektroniczny – regulacje

Akty prawne dot. popisu elektronicznego

- 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 (eIDAS)
- Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej
- Rozporządzenia Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie krajowej infrastruktury zaufania

Decyzje wykonawcze

- Decyzja wykonawcza Komisji (UE) 2015/1505 z dnia 8 września 2015 r. ustanawiająca specyfikacje techniczne i formaty dotyczące zaufanych list (…)
- Decyzja wykonawcza Komisji (UE) 2015/1506 z dnia 8 września 2015 r. ustanawiająca specyfikacje dotyczące formatów zaawansowanych podpisów elektronicznych oraz zaawansowanych pieczęci elektronicznych, które mają być uznane przez podmioty sektora publicznego (…)

Normy i standardy techniczne

- Formaty podpisu
  - ETSI TS 103 171 / ETSI EN 319 132 - XAdES
  - ETSI TS 103 172 / ETSI EN 319 142 - PAdES
  - ETSI TS 103 173 / ETSI EN 319 122 - CAdES
  - ETSI TS 103 174 - ASiC
- Algorytmy kryptograficzne
  - ETSI TS 119 312
- Profile certyfikatów
  - ETSI EN 319 412

Podpis elektroniczny – praktyka

Obsługa zagranicznych podpisów

- *Kwalifikowany podpis elektroniczny oparty na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawany za kwalifikowany podpis elektroniczny we wszystkich pozostałych państwach członkowskich*. (art. 25 eIDAS)

- *Kwalifikowana pieczęć elektroniczna oparta na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawana za kwalifikowaną pieczęć elektroniczną we wszystkich pozostałych państwach członkowskich*. (art. 35 eIDAS)

Zaufane listy

- *Każde państwo członkowskie sporządza, prowadzi i publikuje zaufane listy zawierające informacje dotyczące kwalifikowanych dostawców usług zaufania, za których jest ono odpowiedzialne, wraz z informacjami dotyczącymi świadczonych przez nich kwalifikowanych usług zaufania.* (art. 22 eIDAS)

- *Państwa członkowskie sporządzają, prowadzą i publikują – w zabezpieczony sposób – elektronicznie podpisane lub opatrzone pieczęcią elektroniczną zaufane listy, (…) w postaci dostosowanej do automatycznego przetwarzania.* (art. 22 eIDAS)

Jak wygląda zaufana lista ?

- Polska zaufana lista
  - https://www.nccert.pl/tsl/PL_TSL.xml
- Wygodniejsze narzędzie
  - https://webgate.ec.europa.eu/tl-browser

Algorytmy kryptograficzne (PL)

- Zgodnie z art. 137 ustawy o usługach zaufania do dnia 1 lipca 2018 r. do składania zaawansowanych podpisów elektronicznych lub zaawansowanych pieczęci elektronicznych możliwe było stosowanie funkcji skrótu SHA-1.
- Obecnie najczęściej stosowanym zestawem algorytmów jest SHA256-RSA(2048)

Algorytmy kryptograficzne (UE)

- ETSI TS 119 312 v 1.2.1 (2017-05)

Table 9: Recommended signature suites for algorithm resistance during X years

Entry name of the signature suite	1 year	3 years	6 years
sha256-with-rsa	≥ 1 900	≥ 1 900	not recommended
sha512-with-rsa	≥ 1 900	≥ 1 900	not recommended
rsa-pss with mgf1SHA-256Identifier	≥ 1 900	≥ 1 900	≥ 3 000
rsa-pss with mgf1SHA-512Identifier	≥ 1 900	≥ 1 900	≥ 3 000
rsa-pss with mgf1SHA3-Identifier	≥ 1 900	≥ 1 900	≥ 3 000
sha256-with-dsa	2 048	2 048	3 072
sha512-with-dsa	2 048	2 048	3 072
sha224-with-ecdsa	legacy		
sha2-with-ecdsa	recommended		
sha2-with-ecsdsa	recommended		
sha3-with-ecdsa	recommended		
sha3-with-ecsdsa	recommended		

Wykorzystanie znacznika czasu

- Znacznik czasu dostarcza wiarygodną i dokładną informację nt. czasu złożenia podpisu elektronicznego.
- Przykłady:
  - Podpis bez znacznika czasu
  - Podpis ze znacznikiem czasu
- Określenie czasu weryfikacji
  - „na teraz”,
  - na pewien określony moment w czasie,
  - na moment złożenia podpisu.

Podpis elektroniczny „po latach” - problem

- Jak zweryfikować podpis elektroniczny po X latach ?
  - Certyfikat podpisującego utracił ważność
  - Brak odpowiedniej listy CRL / odpowiedzi OCSP
  - Certyfikat dostawcy usług zaufania utracił ważność
  - Dostawca usług zaufania utracił status kwalifikowanego (albo nie istnieje)
- Przykład – weryfikacja podpisu (1341 dni później)

Podpis elektroniczny „po latach” - rozwiązania

- Zapewnienie „papierowego” dowodu
- Usługa walidacji
- Odpowiedni poziom podpisu – podpis na poziomie LT i LTA zapewnia wieloletnią możliwości weryfikacji
- Podniesienie poziomu podpisu podczas weryfikacji

- Przykład – weryfikacja podpisu (1341 dni później)

Czy są jakieś pytania ?

Dziękuję za uwagę

NBP Narodowy Bank Polski

Bartosz Nakielski
Wydział Kryptografii
Departament Bezpieczeństwa
Narodowy Bank Polski

tel. +48221851804

Bartosz.Nakielski@nbp.pl
nccert@nccert.pl