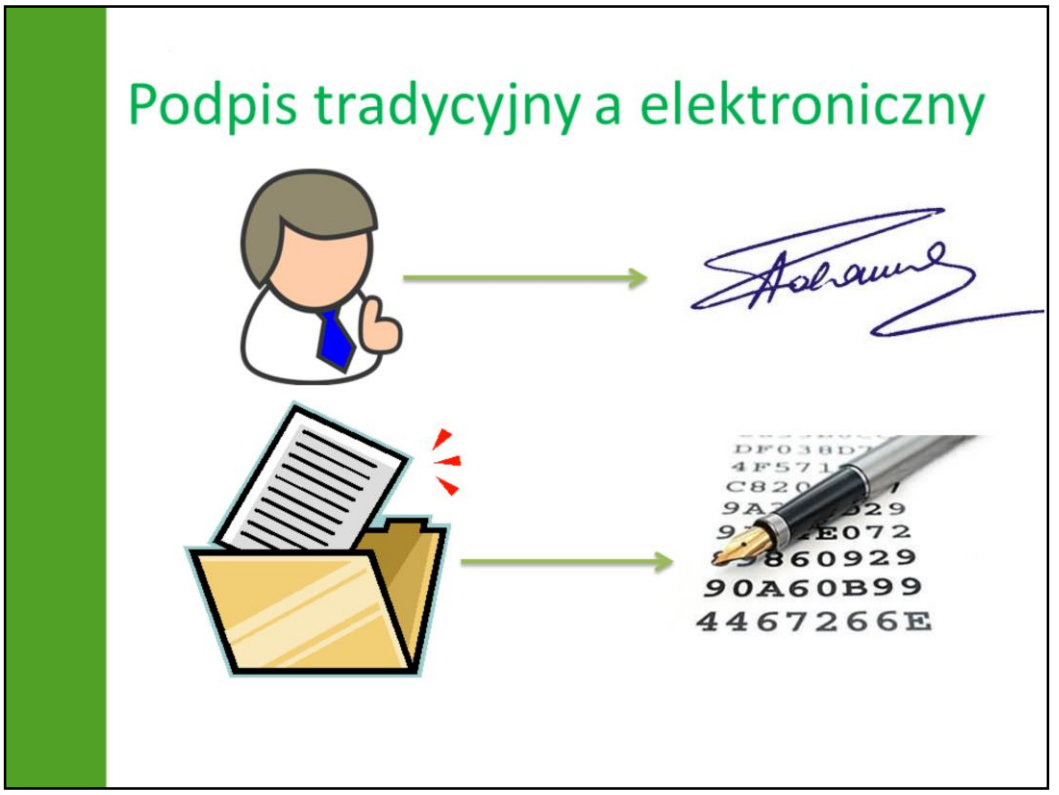
Dzień dobry Państwu, nazywam się Dariusz Kowal, jestem pracownikiem Śląskiego Centrum Społeczeństwa Informacyjnego, gdzie pełnię rolę inspektora ds. CC SEKAP. W dniu dzisiejszym przedstawię Państwu w jaki sposób podpis elektroniczny jest wykorzystywany w Systemie Elektronicznej Komunikacji Administracji Publicznej w skrócie zwanym **SEKAP**. Zacznę jednak od zdefiniowania pojęcia podpisu elektronicznego i przedstawienia kilku wybranych aktów prawnych na podstawie których możliwe jest stosowanie podpisu elektronicznego.



Podpis jest metodą autoryzacji dokumentów, którą ludzie posługują się od dość dawna. Podpis odręczny jest związany ściśle z osobą która go składa (jej cechami osobowości, motoryką itp.) dlatego widząc podpis złożony pod dokumentem papierowym z reguły możemy stwierdzić, kto go złożył, a grafolodzy mogą uzyskać jeszcze wiele innych informacji na temat cech charakteru, stanu zdrowia, a nawet zajęcia, którym składający podpis się zajmuje.

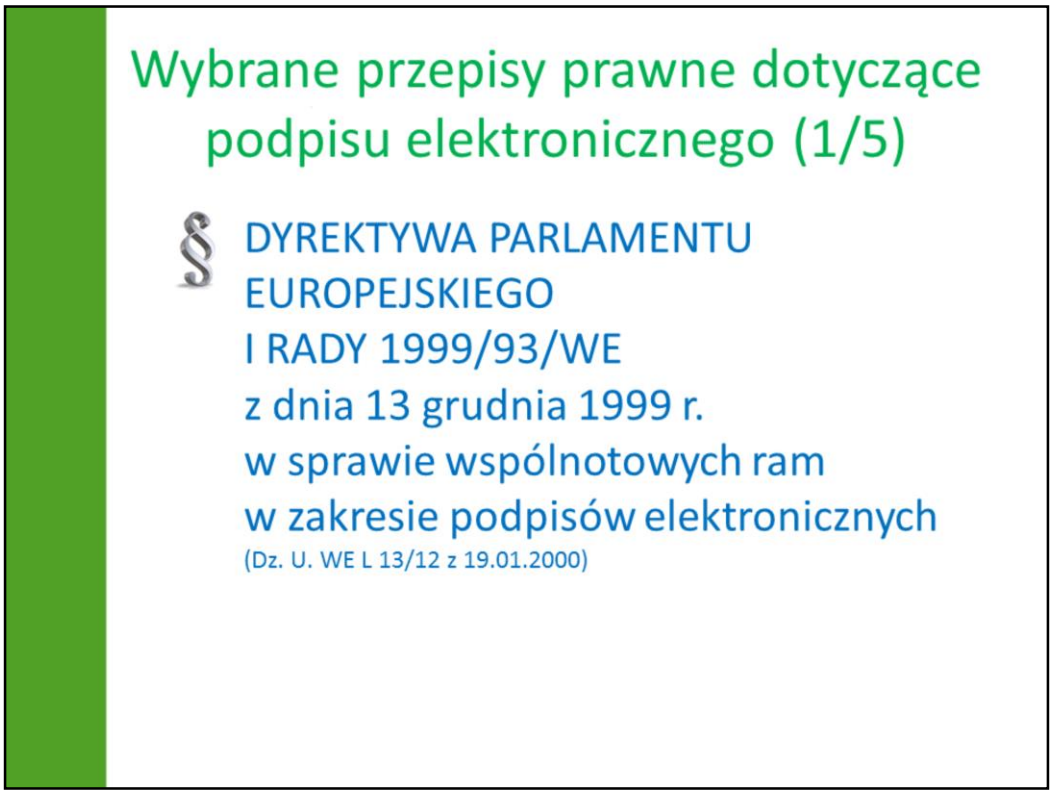
W procesie elektronicznej wymiany dokumentów jednak podpis tradycyjny staje się bezużyteczny i niewiarygodny. Cyfrowy obraz podpisu odręcznego jest łatwy do kopiowania, a przy dzisiejszej zaawansowanej grafice komputerowej, nie możliwe byłoby odróżnienie podpisu autentycznego od falsyfikatu, dlatego przy podpisywaniu dokumentów elektronicznych wykorzystuje się techniki kryptograficzne.

Polska Norma (PN-I-02000) definiuje podpis cyfrowy jako "przekształcenie kryptograficzne danych umożliwiające odbiorcy sprawdzenie autentyczności i ich integralności oraz zapewniające nadawcy ochronę przed sfałszowaniem danych przez odbiorcę”.

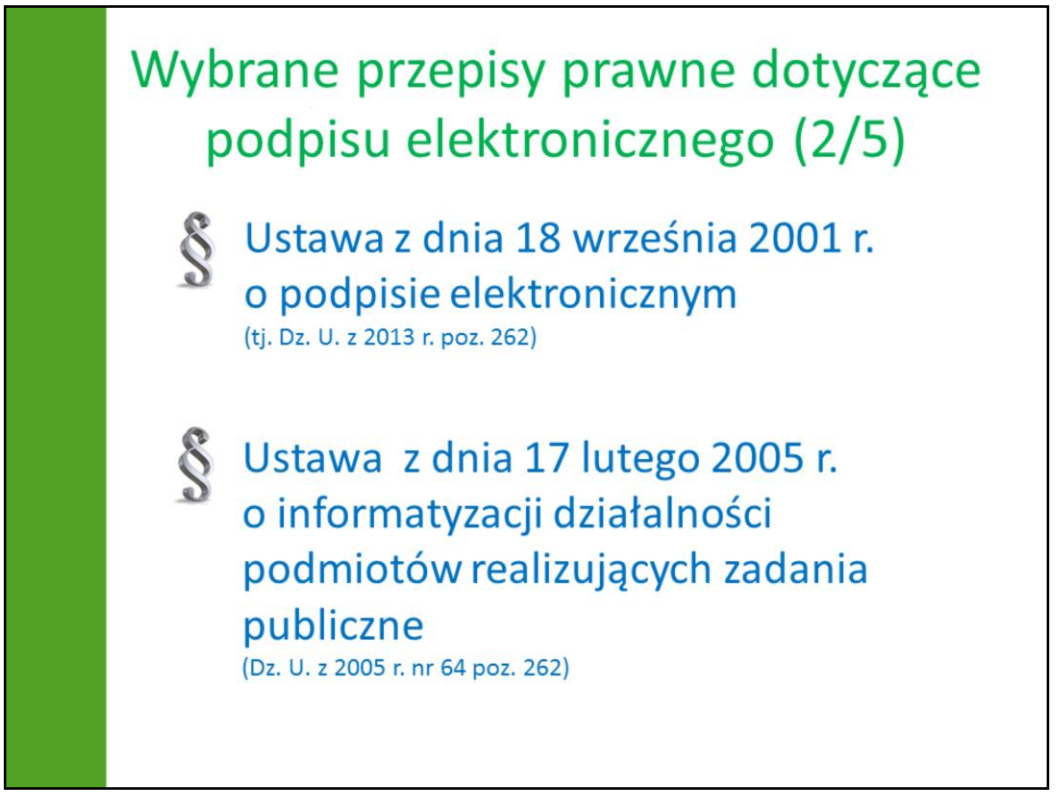
Inna definicja traktuje podpis elektroniczny jako niezbędny warunek dla bezpieczeństwa szeroko rozumianego e-biznesu, a w szczególności bankowości elektronicznej. Jej integralność, autentyczność i niezaprzeczalność może zagwarantować tylko bezpieczny podpis elektroniczny weryfikowany za pomocą kwalifikowanego certyfikatu, czyli skrót wiadomości utworzony za pośrednictwem

jednokierunkowej funkcji skrótu, podpisany (zaszyfrowany) kluczem prywatnym nadawcy, przy wykorzystaniu infrastruktury klucza publicznego. Z tej definicji wynika, iż podpis ten to mechanizm oparty na kryptografii asymetrycznej oraz jednokierunkowej funkcji skrótu.

Oznacza to również, że podpis elektroniczny nie jest, tak jak to ma miejsce w przypadku podpisu tradycyjnego, związany z osobą i jego indywidualnymi cechami, ale jest ściśle powiązany z dokumentem, który jest podpisywany przy jego pomocy.

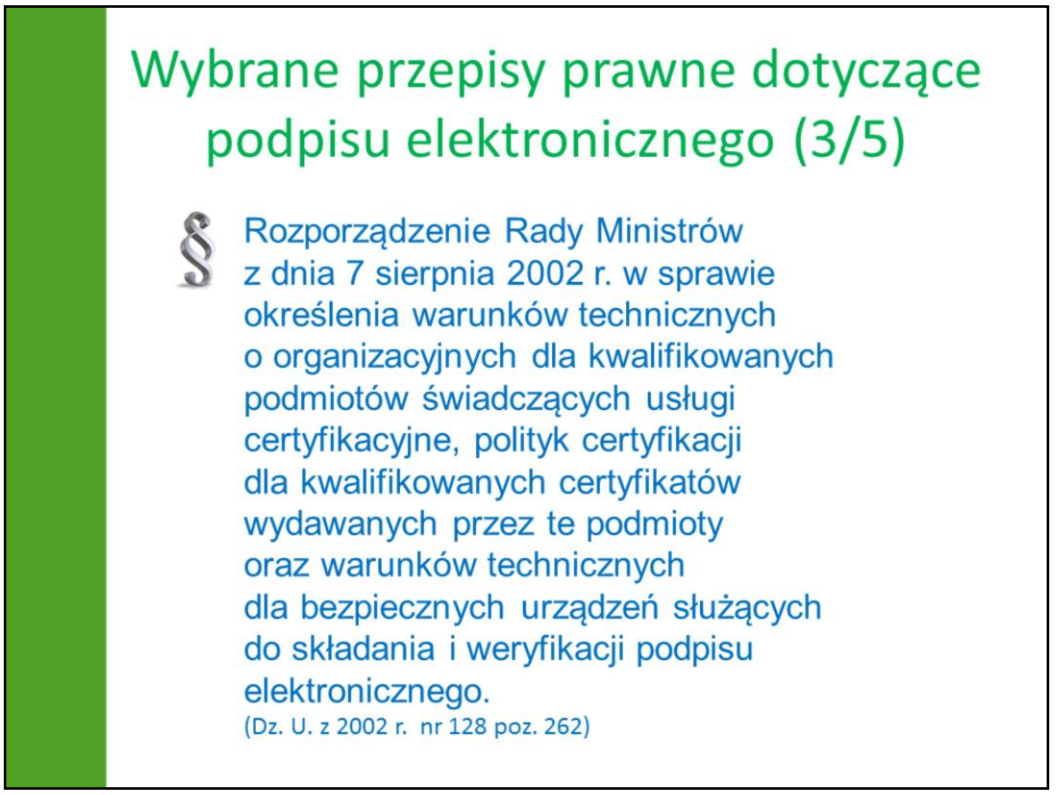


Pierwszym z nich jest widoczna na slajdzie Dyrektywa Parlamentu Europejskiego i Rady nr 1999/93/WE z 13 grudnia 1999 roku, która jest podstawową dyrektywą unijną definiującą różne rodzaje podpisu elektronicznego (w tym kwalifikowany) oraz wysokopoziomowe wymagania wobec podmiotów oraz technik składania tych podpisów.



Ustawa o podpisie elektronicznym jest implementacją przywołanej wcześniej dyrektywy UE i określa warunki stosowania podpisu elektronicznego, skutki prawne jego stosowania, zasady świadczenia usług certyfikacyjnych oraz zasady nadzoru nad podmiotami świadczącymi te usługi.

Drugim ważnym aktem prawnym jest ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne, która m. in.:
•określa zasady ustalania minimalnych wymagań dla systemów teleinformatycznych używanych do realizacji zadań publicznych oraz dla rejestrów publicznych i wymiany informacji w postaci elektronicznej z podmiotami publicznymi,
• określa zasady dostosowania systemów teleinformatycznych używanych do realizacji zadań publicznych do minimalnych wymagań dla systemów teleinformatycznych używanych do realizacji zadań publicznych,
• określa zasady dostosowania rejestrów publicznych i wymiany informacji w postaci elektronicznej z podmiotami publicznymi do minimalnych wymagań dla rejestrów publicznych i wymiany informacji z podmiotami,
•wymiany informacji drogą elektroniczną, w tym dokumentów elektronicznych, pomiędzy podmiotami publicznymi a podmiotami niebędącymi podmiotami publicznymi,
•funkcjonowania elektronicznej platformy usług administracji publicznej, zwanej dalej „ePUAP”,
•funkcjonowania centralnego repozytorium wzorów pism w postaci doku-mentów elektronicznych,



Do wymienionych ustaw został wydany szereg rozporządzeń określających zasady wydawania, oraz użytkowania podpisów elektronicznych:

Wybrane przepisy prawne dotyczące podpisu elektronicznego (4/5)

§ Rozporządzenie Ministra Finansów z dnia 16 grudnia 2003 r. w sprawie obowiązkowego ubezpieczenia odpowiedzialności cywilnej kwalifikowanego podmiotu świadczącego usługi certyfikacyjne
(tj. Dz. U. z 2003 r. nr 229, poz. 2282)

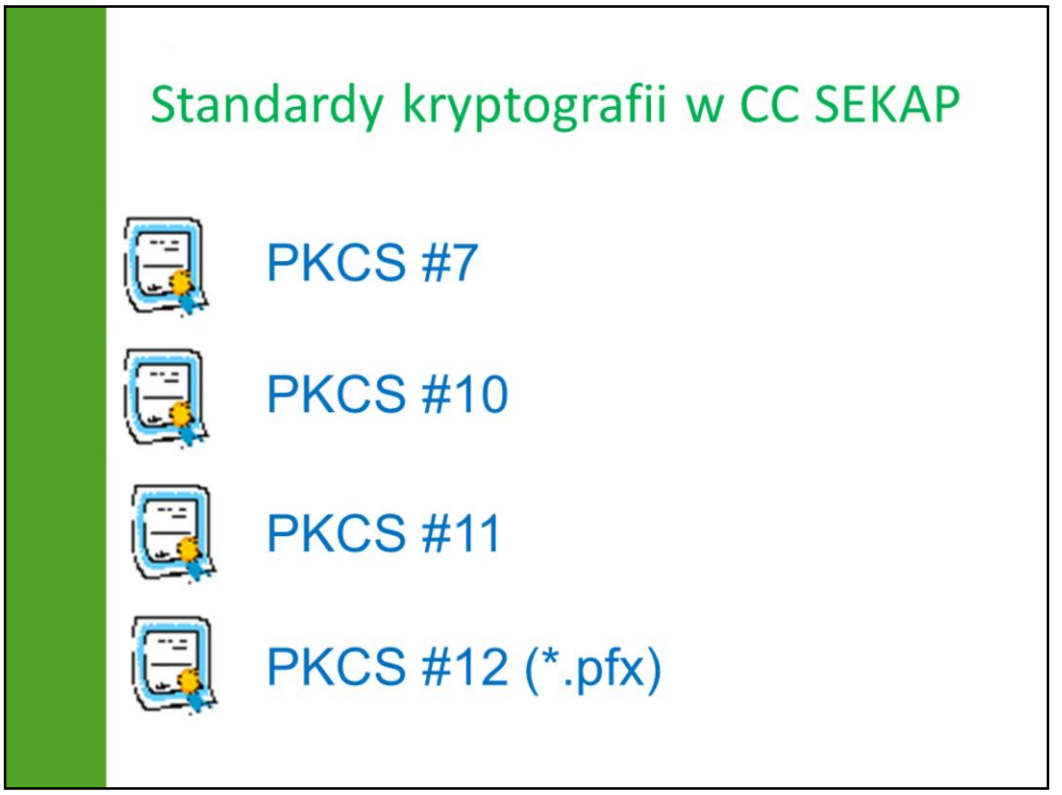
§ Rozporządzenie Ministra Gospodarki, Pracy i Polityki Społecznej z dnia 23 grudnia 2003 r. w sprawie opłat za przechowywanie dokumentów i danych związanych z usługami certyfikacyjnymi
(tj. Dz. U. z 2004 r. nr 6, poz. 48)

Wybrane przepisy prawne dotyczące podpisu elektronicznego (5/5)

- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 kwietnia 2011 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do identyfikacji użytkowników
  (tj. Dz. U. z 2011 r. nr 93 poz. 545)
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2011 r. w sprawie zasad potwierdzania, przedłużania ważności, wykorzystania i unieważniania profilu zaufanego elektronicznej platformy usług administracji publicznej
  (tj. Dz. U. z 2011 r. nr 93 poz. 547)

W systemie SEKAP w procesie elektronicznej wymiany dokumentów zastosowano następujące metody składania podpisu:

- **bezpieczny podpis elektroniczny weryfikowany kwalifikowanym certyfikatem** to podpis elektroniczny weryfikowany certyfikatem, który został wydany przez kwalifikowane centrum certyfikacji na zasadach określonych w Ustawie o podpisie elektronicznym (Dz. U. z 2001 Nr 130 poz. 1450);
- **profil zaufany ePUAP** to bezpłatna metoda potwierdzania tożsamości w elektronicznych kontaktach z administracją;
- **podpis elektroniczny CC SEKAP** to podpis elektroniczny wydawany przez działające w ramach SEKAP centrum certyfikacji, mogą go uzyskać osoby pełnoletnie będące członkami wspólnoty samorządowej województwa śląskiego;



Często podczas pracy z SEKAP spotykamy się pojęciami PKCS#7, PKCS#11, PKCS#12 (**PKCS** stanowi zbiór standardów kryptografii klucza publicznego), poszczególne pojęcia oznaczają:

- PKCS#7 – (ang. *Cryptographic Message Syntax Standard*) – format wykorzystywany do rozpowszechniania certyfikatów,
- PKCS#10 – (ang. *Certification Request Standard*) – format wiadomości do celów żądania certyfikatu,
- PKCS#11 – (ang. *Cryptographic Token Interface*) – jest to API definiujące interfejs dla tokenów (generatorów kodu). Bywa często stosowany w usłudze pojedynczego logowania,
- PKCS#12 – (ang. *Personal Information Exchange Syntax Standard*) - format pliku do przechowywania kluczy prywatnych z towarzyszącymi certyfikatami klucza publicznego, zabezpieczonych hasłem. (zmiana hasła do pliku *.pfx)

Certyfikat niekwalifikowany, jest to certyfikat, który może zostać wystawiony przez dowolny podmiot i takim jest Centrum Certyfikacji SEKAP, które wydaje następujące rodzaje certyfikatów:

- *Certyfikaty osobiste CC* – to certyfikaty, które są wykorzystywane do składania podpisów przez użytkowników portalu https://www.sekap.pl
- *Certyfikaty serwerów* – czyli certyfikaty wystawiane na potrzeby urządzeń wykorzystywanych w systemie SEKAP (np. HSM),
- *Certyfikaty VPN* – czyli certyfikaty służące do zestawiania tuneli VPN dzięki którym możliwa jest komunikacja partnerów z systemami zainstalowanymi w Śląskim Centrum Społeczeństwa Informacyjnego,
- Certyfikaty przeznaczone do komunikacji z systemami: „Pojazd" i „Kierowca" Polskiej Wytwórni Papierów Wartościowych

Oprócz tego użytkowane są również certyfikaty komercyjne służące do realizacji bezpiecznych połączeń (opartych o protokół SSL) ze stronami www: https://

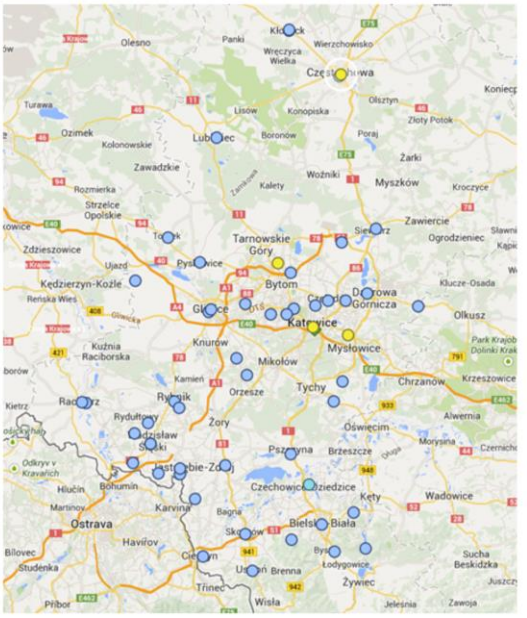
- *Certyfikaty SSL* (zakupione u dostawców komercyjnych) – to certyfikaty zabezpieczające wymianę danych użytkownika z platformą SEKAP, ze stroną Centrum Certyfikacji SEKAP (https://cc.sekap.pl)

Należy pamiętać, że certyfikaty elektroniczne mają określone okresy ważności i tak certyfikat osobisty CC SEKAP, certyfikat serwerów (hsm), certyfikaty do komunikacji z systemami PWPW są ważne 2 lata.

Certyfikaty służące do komunikacji są ważne 5 lat (ostatnia akcja wymiany była przeprowadzona w tym roku) jednak ze względu na to, że certyfikat ROOT-CA centrum certyfikacji wystawiającego obecne certyfikaty wygaśnie w I kwartale 2014 roku, konieczna będzie przed tym terminem ich ponowna wymiana)

W ramach SEKAP działa Centrum Certyfikacji, które zainaugurowało działalność **18 kwietnia 2008 roku**, od początku działalności Centrum Certyfikacji SEKAP wydało 9 880 podpisów elektronicznych (wg stanu na dzień: 04.09.2013 r.). W ramach Centrum Certyfikacji SEKAP działają obecnie 54 urzędy rejestracji (**1** w Śląskim Centrum Społeczeństwa Informacyjnego i **53** u niektórych partnerów SEKAP)

Centrum Certyfikacji SEKAP

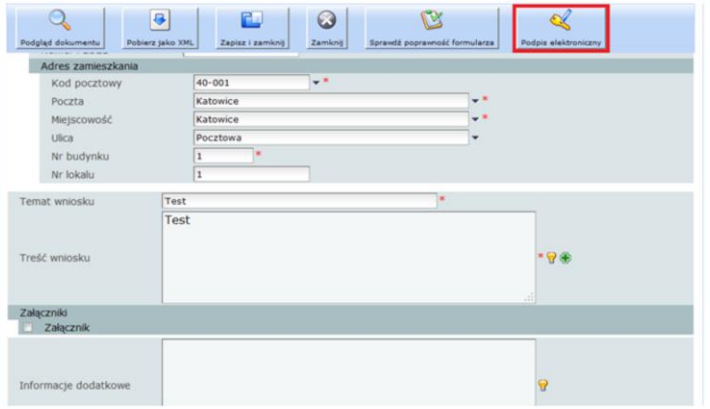


Śląskie Centrum Społeczeństwa Informacyjnego	2 830
Urząd Miasta Katowice	2 354
Urząd Miasta Częstochowy	411
Urząd Miasta Radzionków	376
Urząd Miasta Mysłowice	351

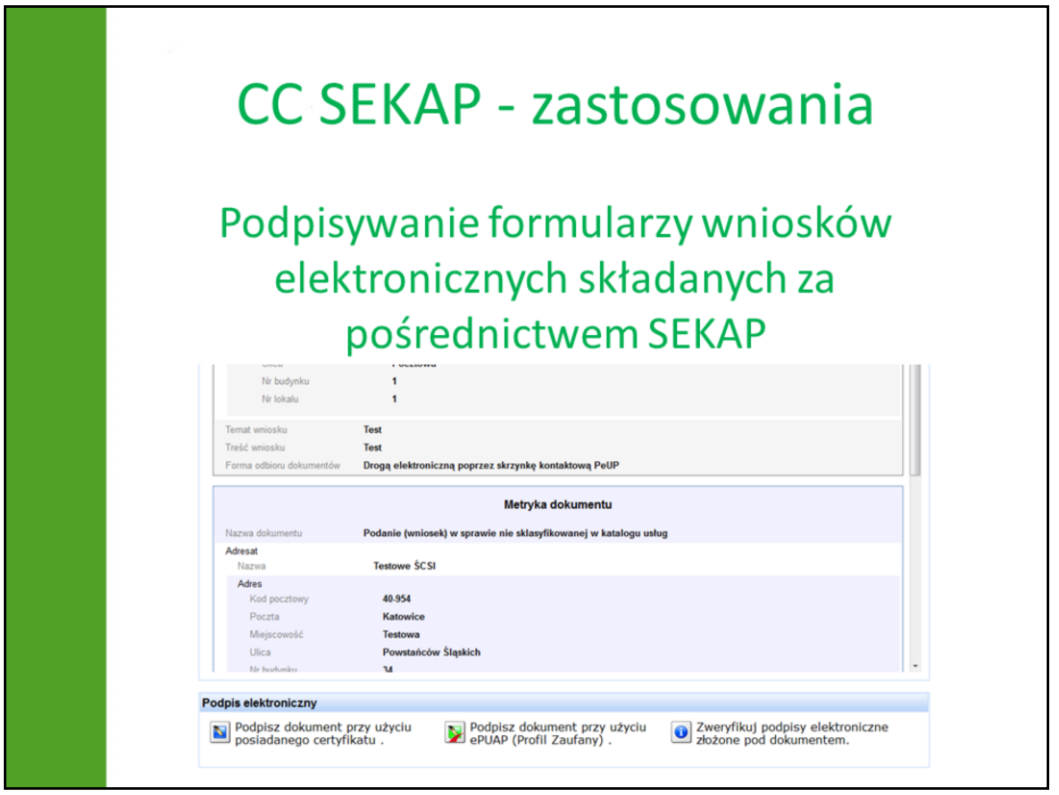
Najbardziej aktywnymi Urzędami Rejestracji (jak nazywają się punkty obsługi subskrybentów CC SEKAP) wchodzącymi w skład Centrum Certyfikacji SEKAP są: Śląskie Centrum Społeczeństwa Informacyjnego (2 830 wydanych certyfikatów), Urząd Miasta Katowice (2 354 wydane certyfikaty), Urząd Miasta Częstochowy (411 wydanych certyfikatów), Urząd Miasta Radzionków (376 wydanych certyfikatów), Urząd Miasta Mysłowice (351 wydanych certyfikatów). Pozostałe urzędy wydały mniej niż połowę ogólnej liczby certyfikatów CC SEKAP. Na zmniejszającą się liczbę subskrybentów CC SEKAP (szczególne wśród mieszkańców województwa śląskiego) ma wpływ uruchomienie usługi podpisywania dokumentów profilem zaufanym, która również może być wykorzystywana na ogólnopolskiej Elektronicznej Platformie Usług Administracji Publicznej (ePUAP), ale również może być dostępna w innych systemach służących do świadczenia elektronicznych usług publicznych. Jak jednak pokażę za chwilę nie warto rezygnować całkowicie z usług CC SEKAP na rzecz Profilu Zaufanego.

CC SEKAP - zastosowania

Podpisywanie formularzy wniosków elektronicznych składanych za pośrednictwem SEKAP



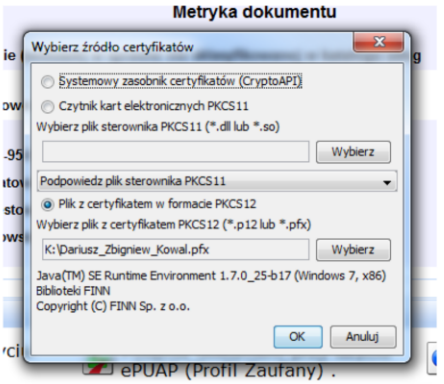
W tej części mojego wystąpienia pokażę Państwu, kilka zastosowań podpisu elektronicznego CC SEKAP, pierwszym, głównym jego zastosowaniem jest podpisywanie formularzy wniosków elektronicznych jest podpisywanie elektronicznych formularzy wniosków składanych za pośrednictwem platformy SEKAP. Po wypełnieniu formularza należy kliknąć przycisk „Podpis elektroniczny”



Wyświetlona zostanie wizualizacja i panel służący do składania podpisu elektronicznego. Po kliknięciu w przycisk „Podpisz dokument przy użyciu posiadanego certyfikatu.” Uruchomiany jest aplet Java służący do obsługi podpisu elektronicznego, w którym jest możliwość wskazania opcji dotyczących lokalizacji pliku zawierającego klucz prywatny użytkownika.

CC SEKAP - zastosowania

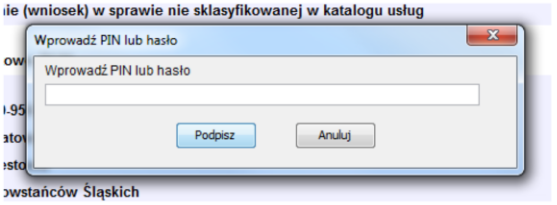
Podpisywanie formularzy wniosków elektronicznych składanych za pośrednictwem SEKAP

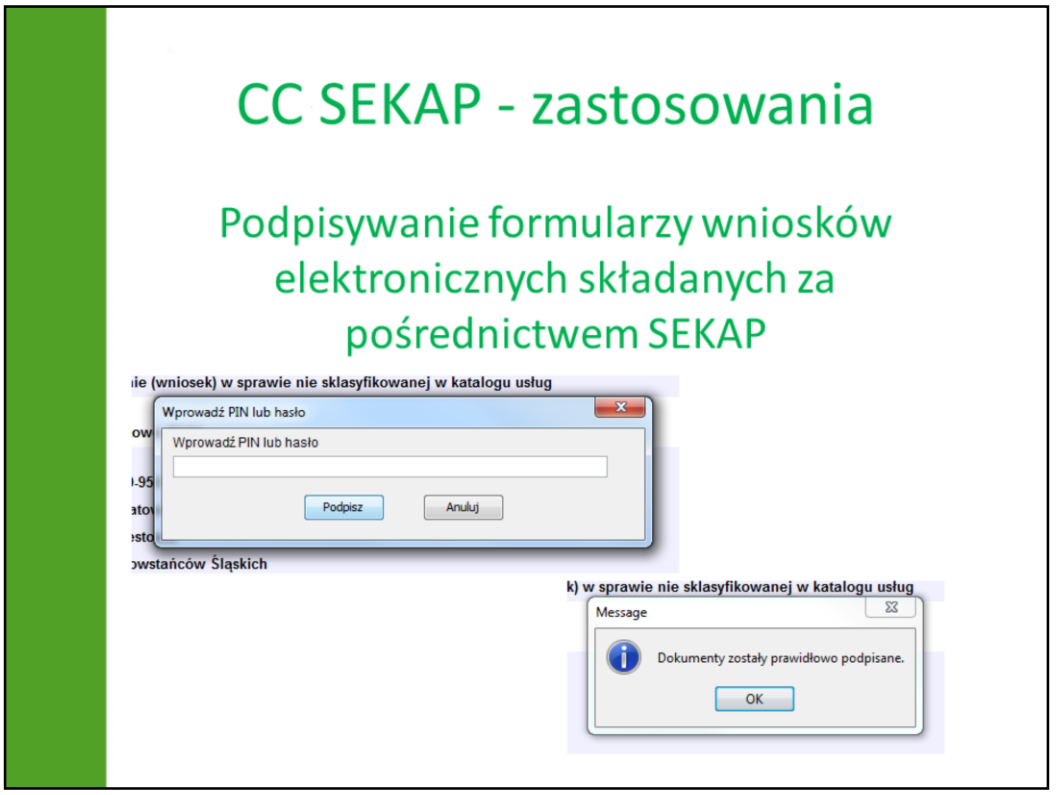


W oknie jest możliwość wyboru źródła klucza prywatnego użytkownika, a w przypadku wskazania pliku w formacie PKCS#12 wskazania jego lokalizacji. Po poprawnej konfiguracji i kliknięciu klawisza „Podpisz” użytkownik powinien zobaczyć na ekranie okienko do wpisania hasła.

CC SEKAP - zastosowania

Podpisywanie formularzy wniosków elektronicznych składanych za pośrednictwem SEKAP



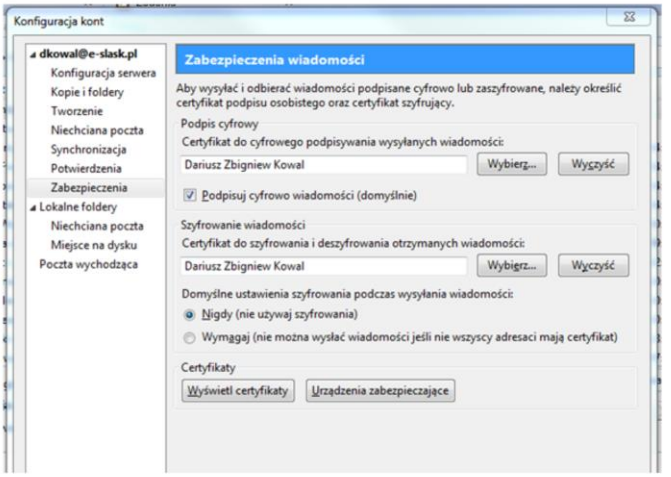


A po poprawnym wprowadzeniu hasła powinien zostać wyświetlony komunikat „Dokumenty zostały prawidłowo podpisane”

CC SEKAP - zastosowania

Podpisywanie poczty elektronicznej

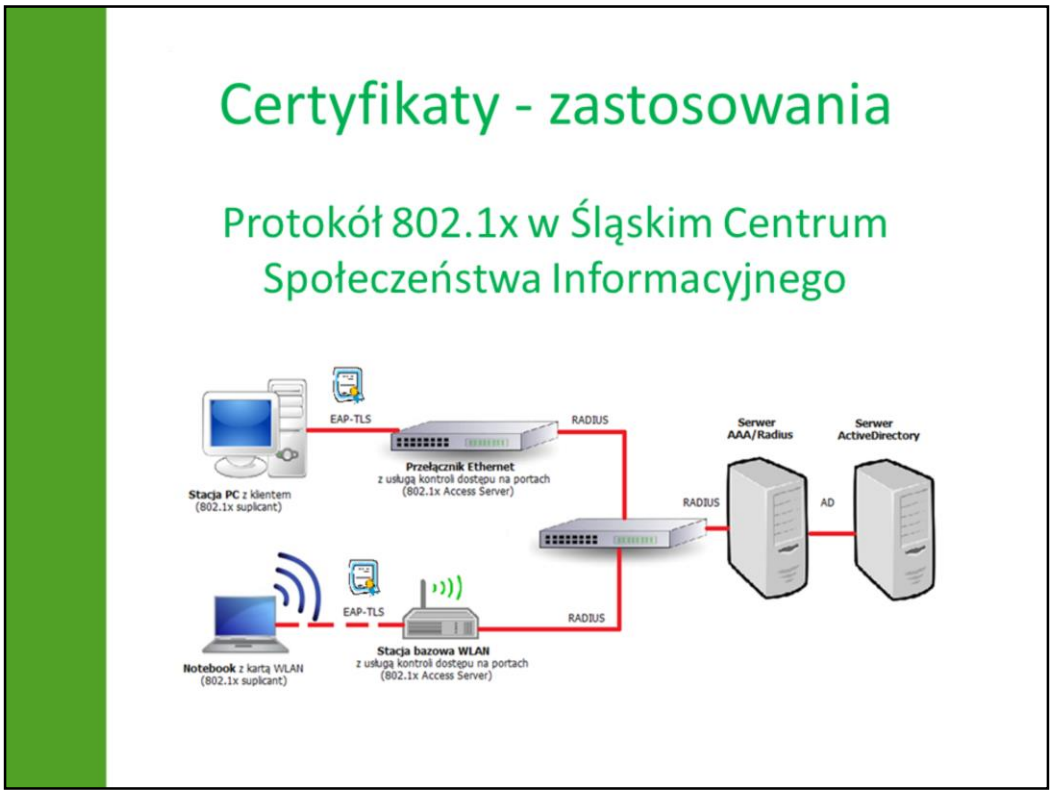
(na przykładzie klienta pocztowego „Thunderbird”)



W odróżnieniu od certyfikatów kwalifikowanych, które nie są przeznaczone do podpisywania poczty elektronicznej, certyfikat CC SEKAP może być również wykorzystywany jako certyfikat do podpisywania poczty elektronicznej wysyłanej z klienta pocztowego. Wystarczy w konfiguracji klienta pocztowego wskazać właściwy certyfikat będący w magazynie certyfikatów (należy pamiętać o tym, że klient poczty „Thunderbird” posiada własny magazyn certyfikatów i tam właśnie powinien zostać zaimportowany. Dodatkowo w ustawieniach konta należy wskazać właściwy certyfikat. Należy również pamiętać, że certyfikat powinien być wystawiony na adres poczty elektronicznej, który będzie używany do wysyłania wiadomości pocztowych. Podpisywanie wiadomości poczty elektronicznej powoduje zabezpieczenie integralności przesyłanych wiadomości i gwarantuje, że wiadomość nie zostanie zmodyfikowana przez niepowołane osoby. To jest właśnie powód dla którego nie warto rezygnować całkowicie z certyfikatów niekwalifikowanych, na rzecz innych metod podpisywania jak chociażby „Profil zaufany ePUAP”
Za pomocą certyfikatu CC SEKAP możliwe jest również szyfrowanie wysyłanej korespondencji (pod warunkiem, że użytkownik posiada klucz publiczny użytkownika do którego wysyła korespondencję)

Krótkie porównanie podpisów składanych przy pomocy podpisu niekwalifikowanego i podpisu potwierdzanego profilem zaufanym ePUAP zostało przedstawione w tabeli. Zastosowałem pięć kryteriów porównania: sposób składania podpisu, możliwość wykorzystania, odpłatność i okres ważności. (kod otrzymywany jest za pośrednictwem e-mail, planowane jest wysyłanie kodów SMS)

Na koniec przedstawię jeszcze jedno zastosowanie certyfikatów elektronicznych, niezwiązanych już ściśle z infrastrukturą SEKAP, tym razem będzie to zastosowanie w infrastrukturze sieci komputerowej Śląskiego Centrum Społeczeństwa Informacyjnego.



Śląskie Centrum Społeczeństwa Informacyjnego jest w trakcie wdrażania autoryzacji użytkowników w oparciu o protokół 802.1x, który pozwala na pozwala na stworzenie jednolitej struktury mechanizmów uwierzytelniania w złożonej sieci komputerowej, obejmującej zarówno klasyczne sieci LAN, sieci bezprzewodowe WLAN, łącza VPN czy dostępowe łącza abonenckie.

Do celów autoryzacji wykorzystywane są: certyfikaty stacji roboczych, oraz certyfikaty użytkownika.

W centrum jako mechanizm służący do uwierzytelniania wykorzystano protokół EAP-TLS.

Podczas procesu uwierzytelniania EAP-TLS przy użyciu certyfikatu komputer przedstawia swój certyfikat użytkownika serwerowi dostępu zdalnego, a serwer przedstawia swój certyfikat komputerowi, umożliwiając wzajemne uwierzytelnianie.

Serwerem uwierzytelniającym jest kontroler domeny oraz CC SEKAP (opisane tutaj jako Server Active Directory).

Takie rozwiązanie znacznie ułatwia zarządzanie infrastrukturą i zwiększa jej bezpieczeństwo, dlatego właśnie zdecydowano się na jego wdrożenie w infrastrukturze ŚCSI.

DZIĘKUJĘ ZA UWAGĘ

Dariusz Kowal
Telefon: 0 32 700 78 28
E-mail: dkowal@e-slask.pl

Śląskie Centrum Społeczeństwa Informacyjnego
ul. Powstańców 34, 40-954 Katowice
www.e-slask.pl

Zastosowanie certyfikatów elektronicznych w infrastrukturze „SEKAP” jest szerokie: od podpisywania wniosków i pism na platformie SEKAP, poprzez infrastrukturę techniczną, a na infrastrukturze śląskiego centrum kończąc. Zatem naprawdę warto zapoznać się z istniejącymi rozwiązaniami w tej dziedzinie i rozważyć ich wykorzystanie.