Podpis elektroniczny dla firm jako bezpieczna usługa w chmurze

mgr inż. Artur Grygoruk

Czy wyobrażamy sobie świat bez podpisu? Co podpis wnosi do naszego życia?

Cisco Systems

Podpis elektroniczny - definicja

UWIERZYTELNIENIE

WALIDACJA NA PODSTAWIE ZAUFANYCH CA

PODPIS CYFROWY

„Podpis elektroniczny – dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej
podpis elektroniczny.” – art. 3 Ustawy o podpisie elektronicznym.

BEZPIECZEŃSTWO PROCESÓW

ZGODNOŚĆ Z REGULACJAMI

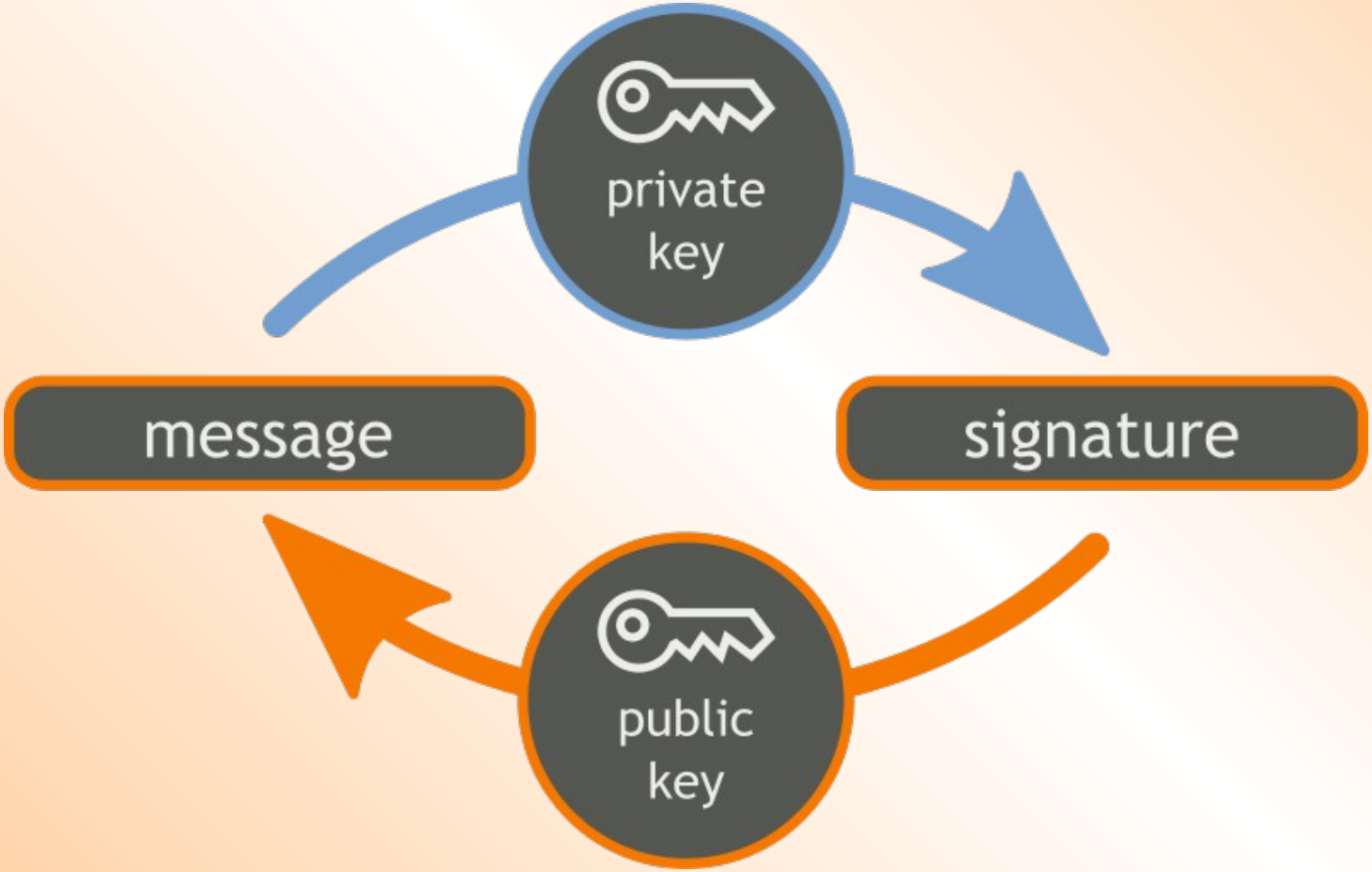
ZAPEWNIENIE INTEGRALNOŚCI DOKUMENTU

ZNACZNIKI CZASOWE

ŚLEDZENIE ZDARZEŃ

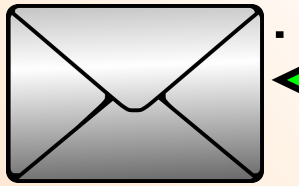
Zagadnienia związane z podpisem elektronicznym

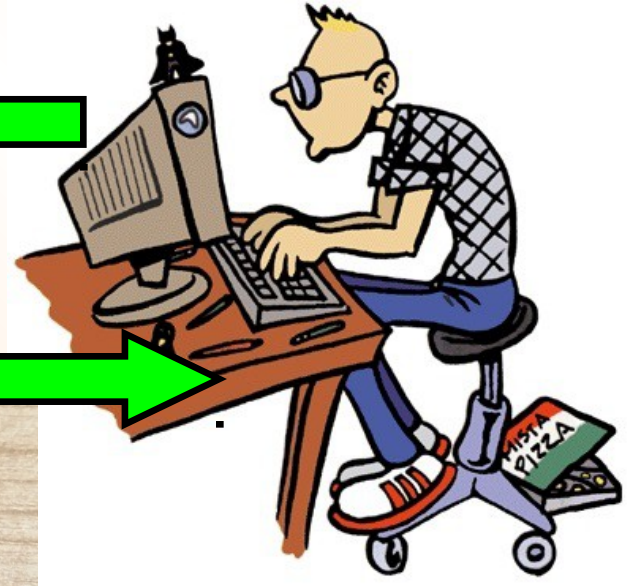
- znaczenie podpisu w świecie „papierowym” i „cyfrowym”
- specyfika usług SaaS związanych z podpisywaniem dokumentacji
- moduły HSM i ich rola w przechowywaniu certyfikatów
- zalety i wady rozwiązań wykorzystujących PKI w chmurze
- narzędzia realizujące podpis elektroniczny dla firm
- prawne skutki złożenia podpisu elektronicznego



Podpis w świecie „papierowym” i „cyfrowym”

- ekologiczne podejście: oszczędzajmy lasy!
- podpisy równoważne w świetle prawa
- dokument elektroniczny i podpis elektroniczny pasują jak klucz do zamka
- większe bezpieczeństwo, zapobieganie fałszywemu podpisowi





Homo informaticus

Przeglądarka certyfikatów

familyterminal.waw.pl

WYSTAWIONY DLA

Nazwa pospolita (CN)
familyterminal.waw.pl

Numer seryjny
2E:D5:59:60:E6:E9:A8:64:B4:61:95:8F:5F:BA:1E:E6

WYSTAWIONY PRZEZ

Nazwa pospolita (CN)
Certum Class I CA SHA2

Organizacja (O)
Unizeto Technologies S.A.

Jednostka organizacyjna (OU)
Certum Certification Authority

OKRES WAŻNOŚCI

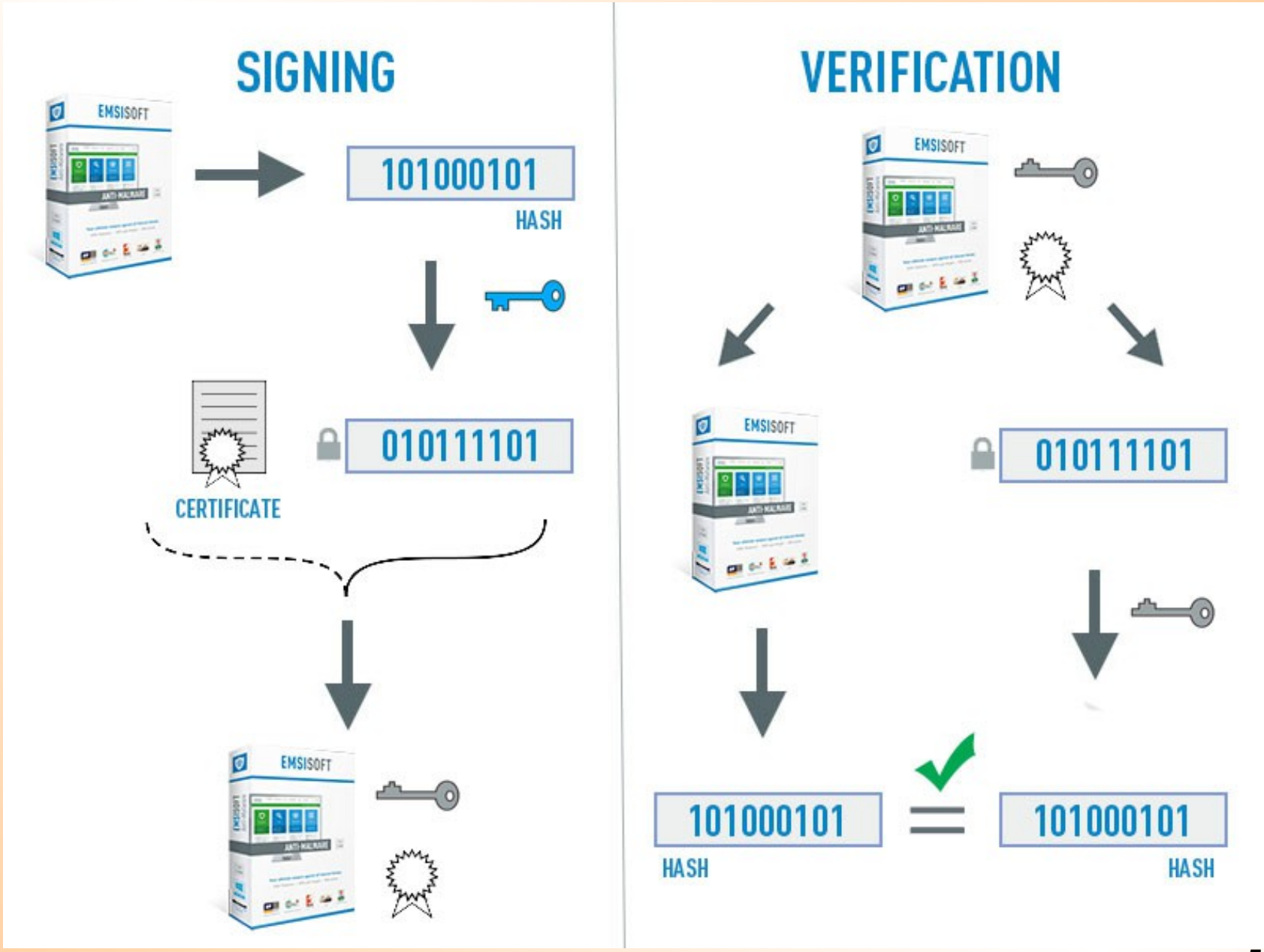
Wystawiony dnia
27.11.2015

Wygasa dnia
27.12.2015

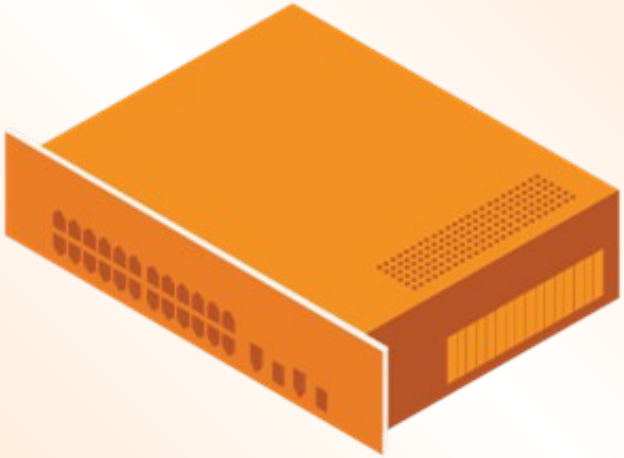
ODCISKI CYFROWE

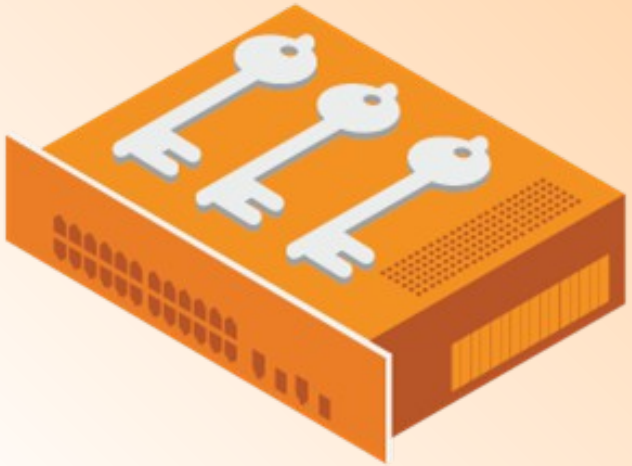
Odcisk cyfrowy SHA-256
B9 DE D6 1B 8C C2 34 CE 21 AE 7B 95 D9 4F F1 9D 00 D8 94 DE E8 D3 B9 FF 71 D1 46 CA 83 22 1B 2D

Zasada działania podpisu elektronicznego i jego weryfikacja



Rola modułu HSM w przechowywaniu certyfikatu



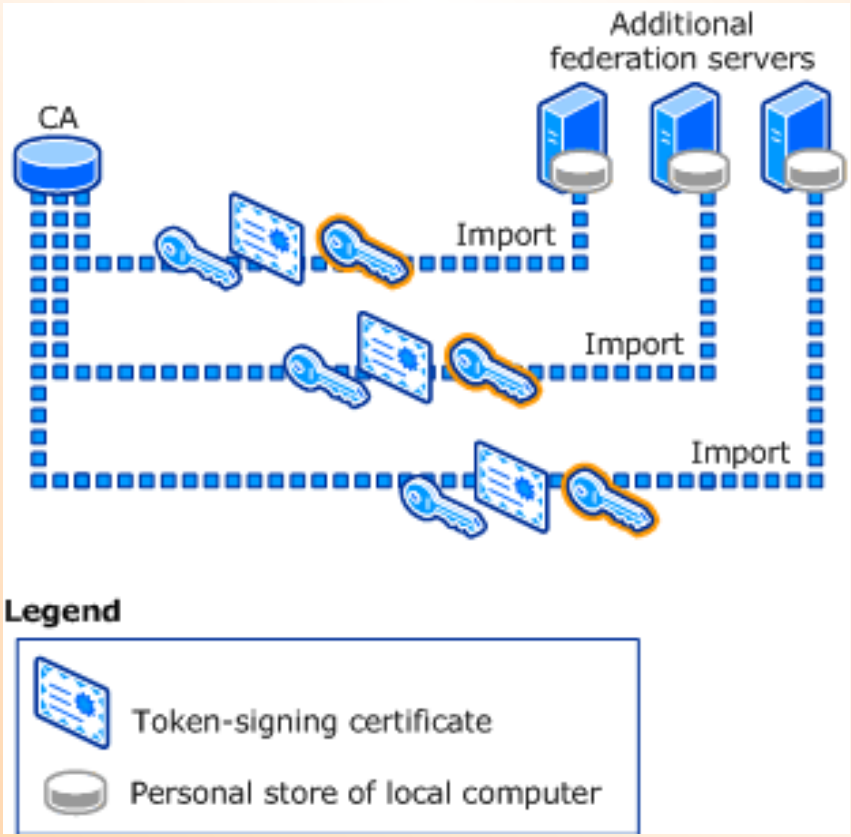


Hardware Security Module (HSM) to element przechowywania certyfikatów i kluczy, które są udostępniane klientowi przy użyciu tuneli SSL.

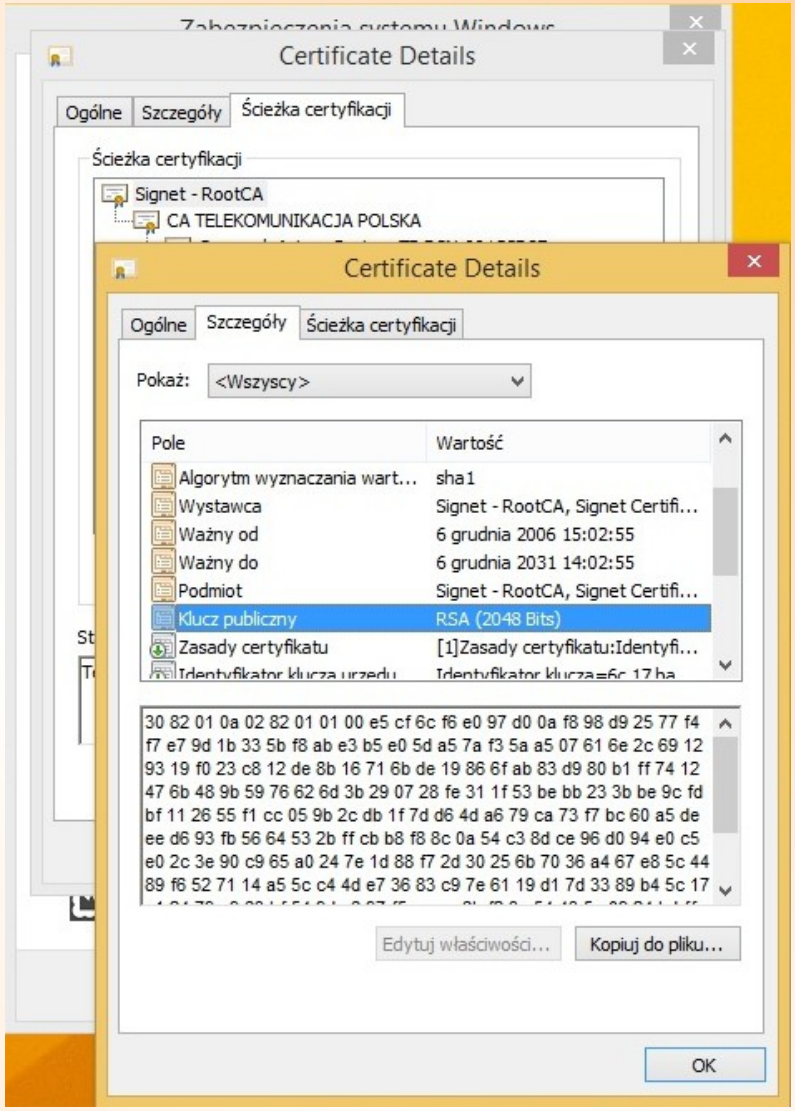
Internal Card PCI (łatwy do zintegrowania, wydajny kosztowo, natywny)

HSM module (szybsze działanie, wiele obliczeń realizowanych równolegle, wysoka wydajność)

Token – nośnik informacji o certyfikacie



Podmiot CA poświadcza wiarygodność certyfikatu używanego przez serwer, stację



Token przechowuje certyfikat (podmiot wystawiający, algorytm szyfrowania, zdefiniowane pole opcji)

Podpis elektroniczny w chmurze w usłudze SaaS

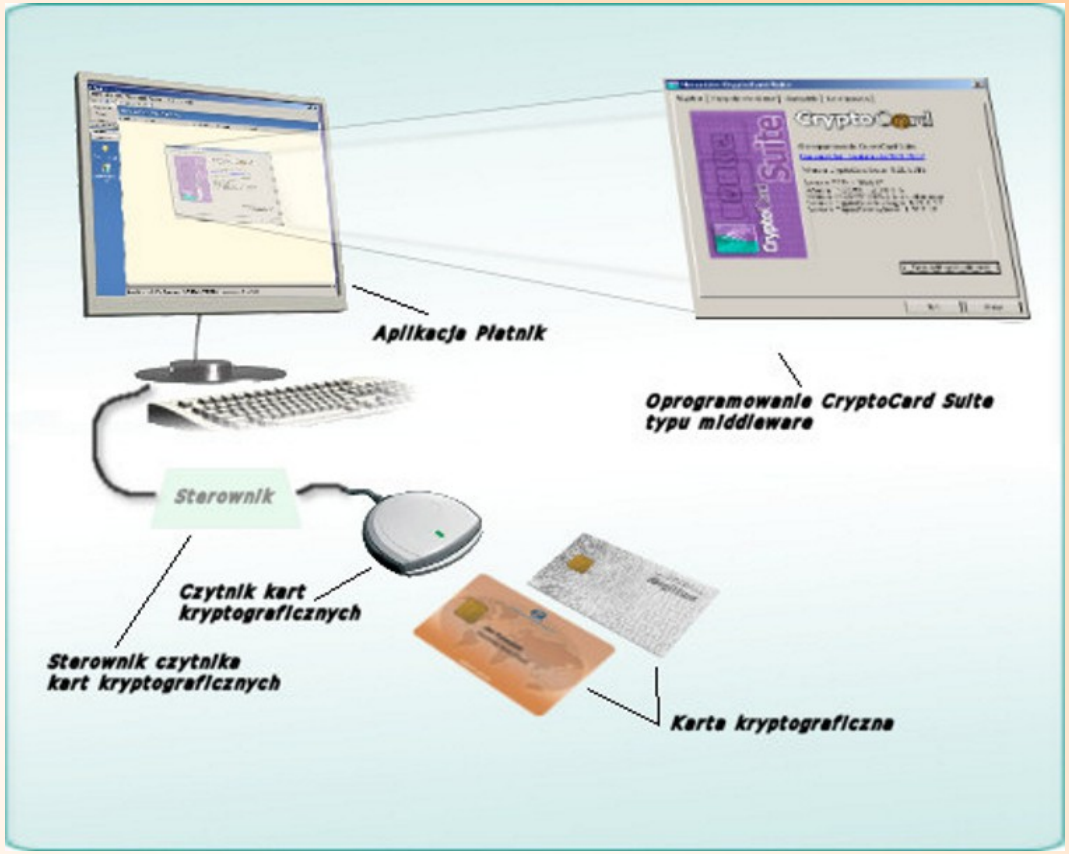
- sprawny proces obliczeń w chmurze
- projektowanie aplikacji dla firmy
- szybko działająca usługa w chmurze

Programy dla podpisu elektronicznego dokumentu:

- rozwiązanie DocuSign
- rozwiązanie Adobe Cloud Document

Dlaczego podpis w chmurze zapewnia bezpieczną metodę podpisywania dokumentów w firmie?

Podpisywanie dokumentu w ZUS (od dn. 21 lipca 2008 r.)

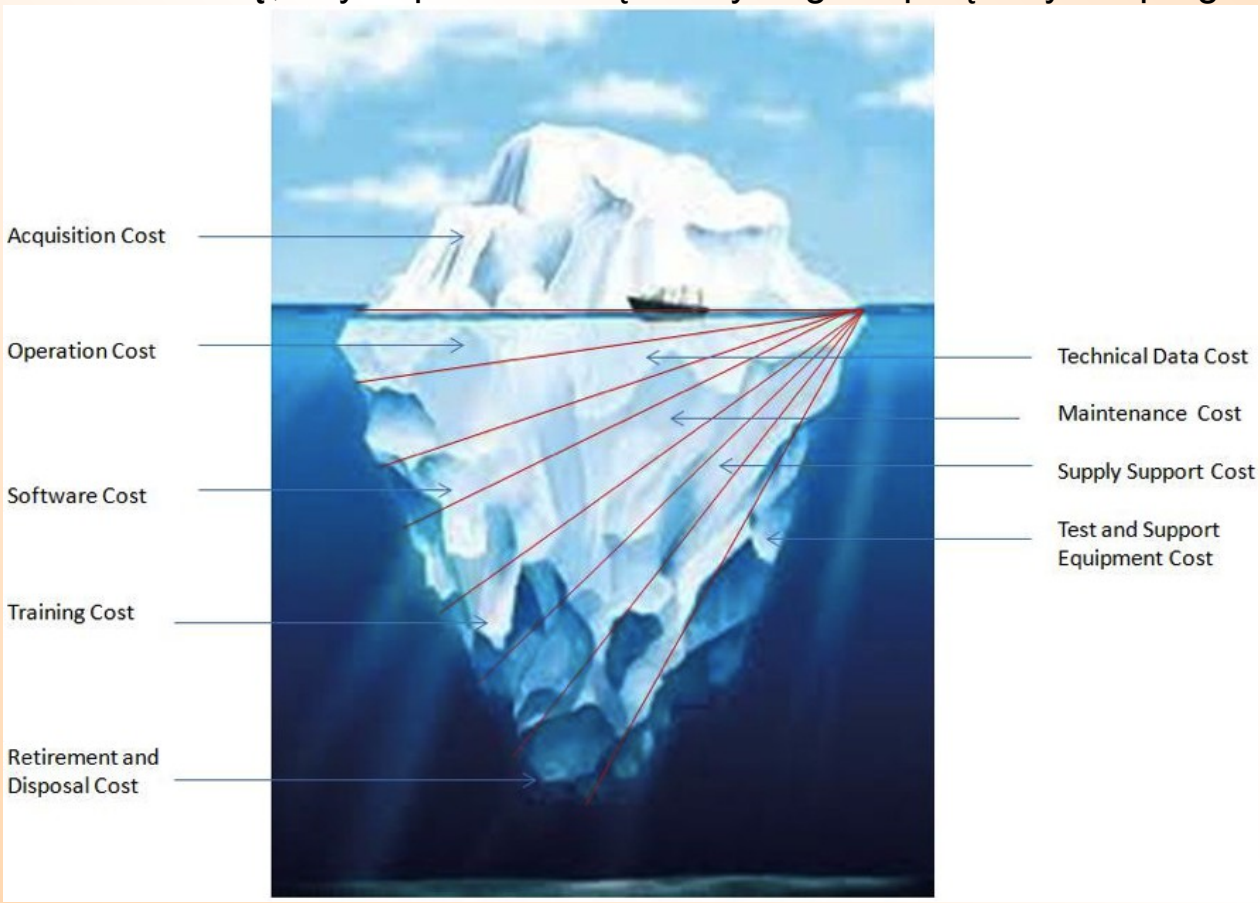


Aby móc podpisywać dokumenty bezpiecznym podpisem elektronicznym, należy dysponować:

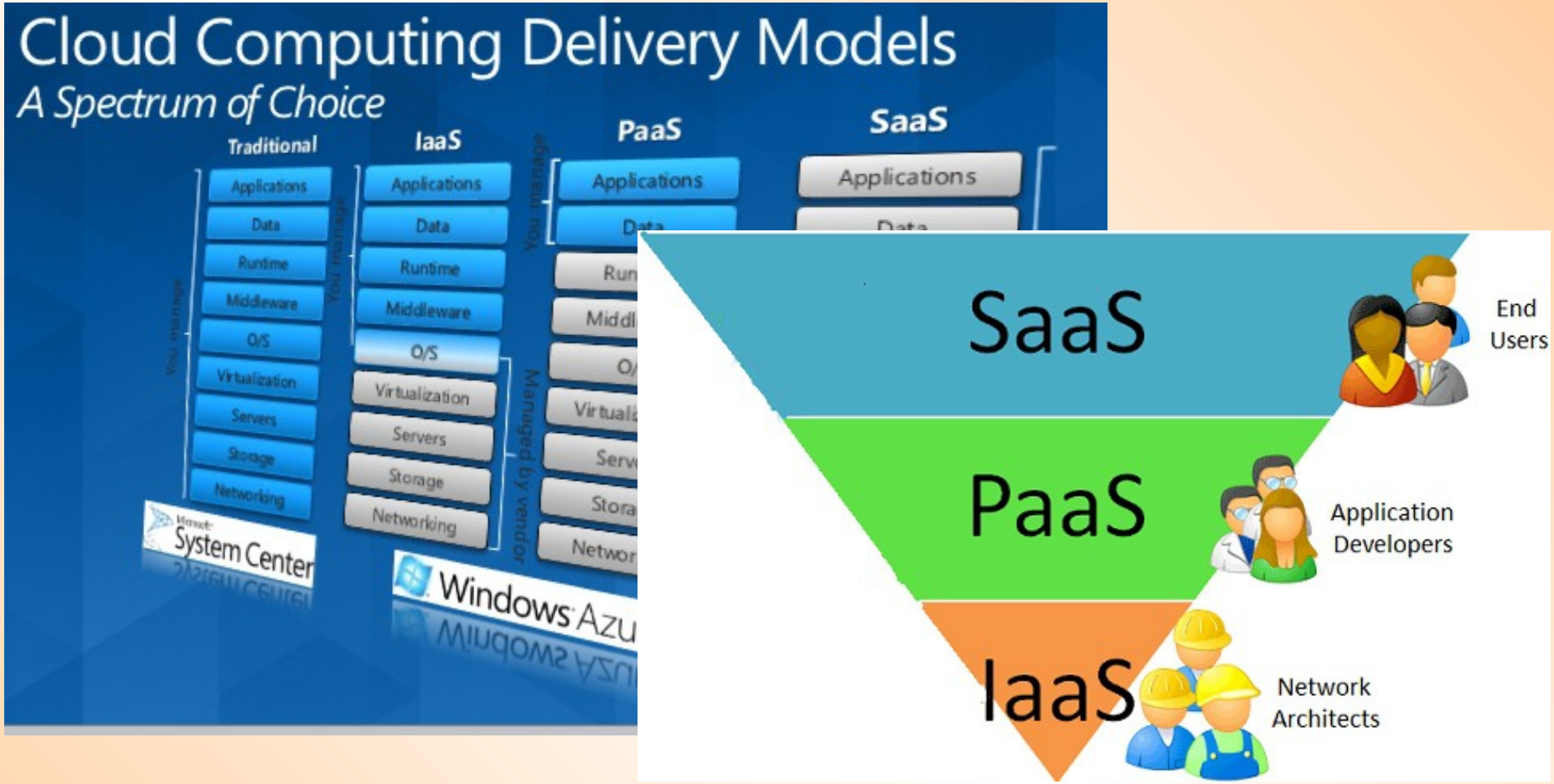
- odpowiednią aplikacją umożliwiającą złożenie bezpiecznego podpisu elektronicznego
- odpowiednim oprogramowaniem typu ***middleware***
- kartą kryptograficzną z certyfikatem kwalifikowanym
- czytnikiem kart kryptograficznych
- certyfikatem kwalifikowanym ważnym przez 1 lub 2 lata

Zalety rozwiązania SaaS – oprogramowanie w chmurze!☺

1. Po pierwsze model SaaS to **oszczędności dla firm**. Nie płacisz od razu za całe oprogramowanie, co kiedyś wiązało się często z koniecznością ponoszenia dużych inwestycji.
2. Po drugie model SaaS **nie wymaga** kosztownego i czasochłonnego **wdrożenia**. Oprogramowanie jest praktycznie dostępne „od ręki”, wymagając co najwyżej drobnych zmian lub dopasowania indywidualnych do potrzeb bardziej wymagających klientów.
3. Po trzecie oprogramowanie w modelu SaaS nie wiąże się z koniecznością ponoszenia **inwestycji w infrastrukturę**, aby dopasować się do wymagań sprzętowych oprogramowania.



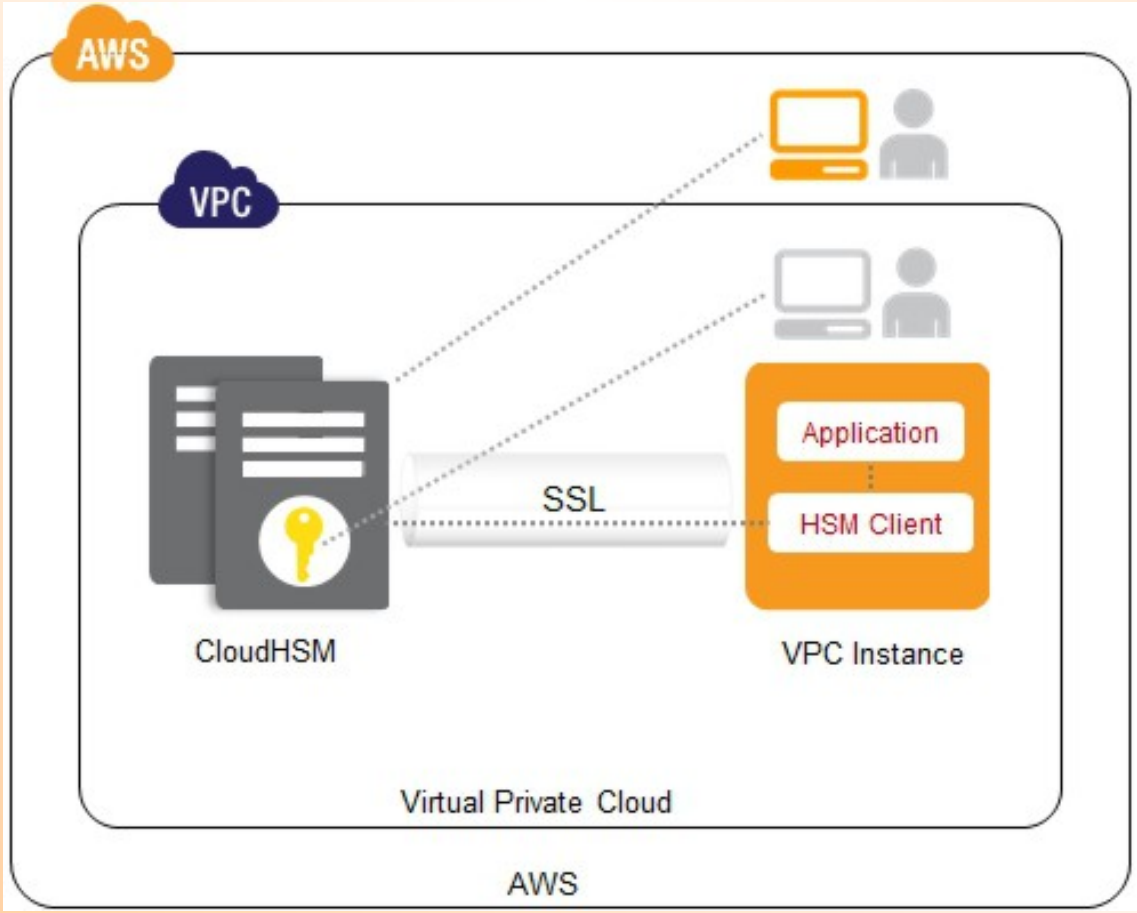
Platforma usługowa SaaS



- Zarządzanie i integracja danych, które są pod kontrolą różnych systemów i domen
- Brak ponoszenia znacznych nakładów na rozwój infrastruktury
- Właścicielem oprogramowania pozostaje usługodawca (***SaaS***)
- Podział odpowiedzialności na wypadek zaistnienia zagrożenia? **Brak problemów**
- Wszystko przejmuje usługodawca udostępniający oprogramowanie (***SaaS***)

Zalety i wady implementacji infrastruktury PKI w chmurze

Zalety rozwiązania:
1. szybkość działania (porównanie ***tokenu BPTP*** a ***modułu HSM***)
2. scentralizowane zarządzanie certyfikatami i dostępem do systemu
3. redukcja kosztów operacyjnych



Rozwiązanie CloudHSM firmy Amazon dla klienta HSM

Wady rozwiązania:
1. ryzyko **awarii** infrastruktury sieciowej (niezawodność, SLA)
2. naruszenie prywatności danych (**wyciek poufnych certyfikatów**)
3. ryzyko nagłego zakończenia działania usługi w chmurze

Powrót do podstaw dla aplikacji

1. Poufność: Confidentiality (C)
2. Integralność: Integrity (I)
3. Dostępność: Availability (A)

Zasięg i zastosowanie kwalifikowanego podpisu elektronicznego

1. Oszczędność czasu
2. Szybkość identyfikacji tożsamości
3. Łatwiejsza dostępność
4. Automatyzacja procesów
5. Ekologiczne podejście (oszczędność papieru)
6. Większe bezpieczeństwo informatyczne

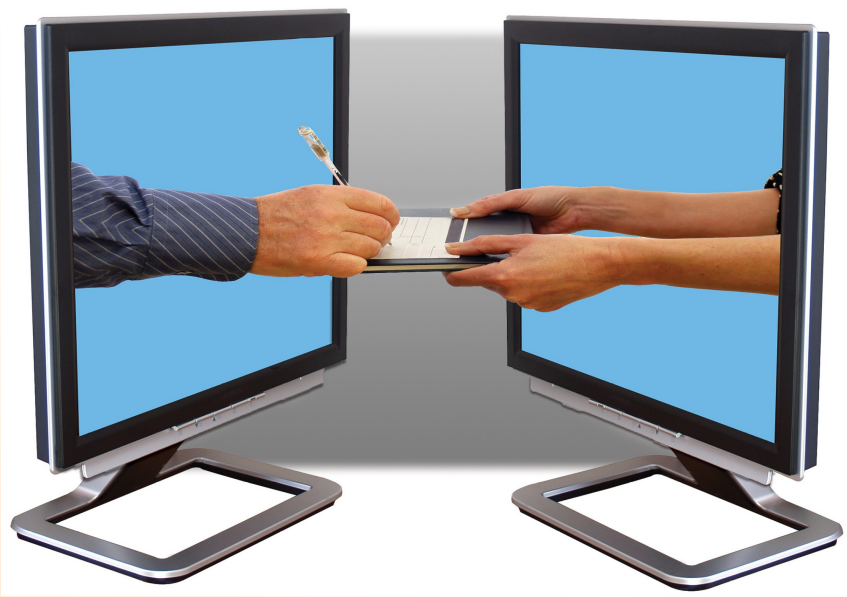
Zastosowanie - wybory parlamentarne:
A może zorganizować głosowanie zdalne?
Jak zabezpieczyć tożsamość wyborcy?
Czy takie rozwiązania istnieją już na świecie?

Prawne aspekty złożenia podpisu elektronicznego

- ✓ Podpis elektroniczny (certyfikat przechowany na tokenie)
- ✓ Zaawansowany podpis elektroniczny
- ✓ Kwalifikowany podpis elektroniczny
- ✓ Ustawa (18 września 2001 roku o podpisie elektronicznym) i ***akty prawne***

Tak mówi Unia Europejska, jednak co Nas najbardziej interesuje?

- ➢ bezpieczny podpis elektroniczny (***Integralność Danych***)
- ➢ podpis elektroniczny (***Identyfikacja Osoby***)
- ➢ bezpieczny podpis elektroniczny weryfikowany kwalifikowanym certyfikatem (***Wiarygodność gwarantowana przez podmiot trzeci***)



Wnioski końcowe

- ✓ Podpis cyfrowy jest odpowiednikiem naszego dowodu tożsamości
- ✓ Podpisywanie wiadomości zapewnia integralność, niezaprzeczalność, autentyczność
- ✓ Szyfrowanie wiadomości zapewnia poufność
- ✓ Algorytmy wykorzystywane w systemach z kluczem mogą być stosowane

a) do podpisywania dokumentów i wiadomości e-mail
b) szyfrowania transmisji

wybór: HSM vs HSM?
a może e-sign w SaaS?