Laboratorium Programowania Kart Elektronicznych

Certyfikaty

Marek Gosławski

- Przygotowanie do zajęć
 - aktywne eKonto
 - wygenerowany certyfikat
 - sprawna legitymacja studencka (lub inna karta)
- Potrzebne wiadomości
 - mechanizm podpisu elektronicznego (X.509)
 - umiejętność konfigurowania klienta poczty, wysyłania poczty elektronicznej
 - umiejętność korzystania z AdobeReader,
 OpenOffice Writer, Microsoft Word

• ustawy i rozporządzenia

- od 2001 r. do 2016 r. "o podpisie elektronicznym"
- od 2014 r. Rozporządzenia Parlamentu
 Europejskiego i Rady (UE) w sprawie identyfikacji
 elektronicznej i usług zaufania (eIDAS)
- od 2016 r. "o usługach zaufania oraz identyfikacji elektronicznej"

podpis elektroniczny

- dane w postaci elektronicznej (...) służące do identyfikacji osoby składającej podpis (do 2016)
- (…) które użyte są przez podpisującego jako podpis
- zaawansowany podpis elektroniczny
 - oznacza podpis elektroniczny, który spełnia wymogi określone w art. 26 (eIDAS)
 - unikalne przyporządkowanie, możliwość ustalenia tożsamości, użyte dane znajdujące się pod wyłączną kontrolą, powiązany z danymi podpisywanymi sposób umożliwiający rozpoznanie zmiany

- certyfikat
 - elektroniczne zaświadczenie … dane … są przyporządkowane do osoby składającej podpis i które umożliwiają identyfikację tej osoby (do 2016)
- certyfikat podpisu elektronicznego
 - poświadczenie elektroniczne, które przyporządkowuje dane ... do osoby fizycznej i potwierdza co najmniej imię i nazwisko lub pseudonim tej osoby

- Middleware
 - oprogramowanie umożliwiające współpracę systemu operacyjnego komputera z kartą
- **PKI** (Public Key Infrastructure)
 - … świadczenia usług …
 - uwierzytelniania,
 - szyfrowania,
 - integralności
 - niezaprzeczalności



By Chris 論 - [1] and OpenCliparts.org, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid= 2501151

- Kryptografia symetryczna
 - w algorytmach symetrycznych klucz służy do szyfrowania i deszyfrowania wiadomości



- Kryptografia asymetryczna
 - w algorytmach asymetrycznych wyróżniamy klucz publiczny oraz prywatny:
 - prywatny powinien znać tylko właściciel
 - publiczny może być jawny
 - klucza powiązane zależnością matematyczną (Diffie W., Hellman M., 1976)
 - znajomość jednego nie pozwala na obliczenie drugiego, można upublicznić jeden z kluczy bez obniżenia poziomu bezpieczeństwa

- Kryptografia asymetryczna c.d.
 - najważniejsze funkcje kryptografii asymetrycznej:
 - szyfrowanie klucz publiczny służy do szyfrowania, a prywatny do deszyfrowania
 - podpisy cyfrowe klucz prywatny służy do generowania podpisów, klucz publiczny do ich weryfikacji



• ELS

– Elektroniczna Legitymacja Studencka

• ELD

– Elektroniczna Legitymacja Doktorancka

- Zadania
 - podpisanie wiadomości elektronicznej
 - zaszyfrowanie wiadomości elektronicznej
 - podpisanie dokumentu .pdf, .odt lub .doc(x)
 - weryfikacja podpisu kwalifikowanego
- Przesłanie na adres:
 - marek.goslawski@put.poznan.pl

Zadanie 1: podpisanie wiadomości elektronicznej Zadanie 2: zaszyfrowanie wiadomości elektronicznej Zadanie 3: podpisanie dokumentu .pdf, .odt lub .doc(x) Zadanie 4: weryfikacja podpisu kwalifikowanego

- Aktywacja funkcjonalności PKI na ELS
 - oprogramowanie AuthentIC WebPack lub ClassicClient
 - eProgramy
 - middleware
 - znajomość PUK karty
 - import certyfikatu
 - eLogin

Zadanie 1: podpisanie wiadomości elektronicznej Zadanie 2: zaszyfrowanie wiadomości elektronicznej Zadanie 3: podpisanie dokumentu .pdf, .odt lub .doc(x) Zadanie 4: weryfikacja podpisu kwalifikowanego



- Logowanie certyfikatem na stronie eLogin
 - certyfikat musi być umieszczony w zasobniku systemu operacyjnego lub przeglądarki
 - klucz prywatny może być na karcie

Formularz logowania					
Użyj poniższego formularza w celu uwierzytelnienia się w systemie podając nazwę konta oraz hasło c	Wybór certyfikatu				
Nazwa konta 🥹	Wybierz certyfikat, aby uwierzytelnić się na serwerze elogin.put.poznan.pl:443				
	Podmiot	Wystawca	Numer seryjny		
Hasio 🥑	marek.goslawski@put.poznan.pl	EMPLOY-CA	16955817000200004545		
Zaloguj się					
Inne sposoby logowania					
• logowanie certyfikatem – logowanie się za pomocą certyfikatu wystawionego przez Politechnikę					
	Informacje o certyfikacie		OK Anuluj		

- Bezpłatne certyfikaty S/MIME
 - do podpisywania poczty
 - wystawcy certyfikatów, przykłady (09.2018)
 - Actalis
 - Instant SSL (Comodo?)
 - Comodo
 - <u>https://www.comodo.com/home/email-security/free-email-certificate.php</u>

- Konfiguracja klienta poczty (Thunderbird)
 - konfiguracja konta
 imie.nazwisko@student.put.poznan.pl
 - dane konfiguracyjne: ePoczta

Zadanie 1: podpisanie wiadomości elektronicznej Zadanie 2: zaszyfrowanie wiadomości elektronicznej Zadanie 3: podpisanie dokumentu .pdf, .odt lub .doc(x) Zadanie 4: weryfikacja podpisu kwalifikowanego

• Konfiguracja klienta poczty (Thunderbird)

konfiguracja konta do współpracy z kartą

- ustawienia konta → zabezpieczenia → urządzenia
 zabezpieczeń → "wczytaj" (wersja 32bit i 64bit!)
 - C:\Program Files (x86)\Oberthur Technologies\AuthentIC
 Webpack\DLLs\OCSCryptoki.dll
 - C:\Program Files (x86)\Gemalto\Classic Client\BIN\gck2015x.dll
- konfiguracja konta do podpisania wiadomości
 - wybór certyfikatu, wskazanie certyfikatu na karcie

Zadanie 1: podpisanie wiadomości elektronicznej Zadanie 2: zaszyfrowanie wiadomości elektronicznej Zadanie 3: podpisanie dokumentu .pdf, .odt lub .doc(x) Zadanie 4: weryfikacja podpisu kwalifikowanego

- Konfiguracja klienta poczty (Thunderbird)
 - konfigurowanie konta do szyfrowania wiadomości
 - <u>https://elogin.put.poznan.pl/</u>
 - manager certyfikatów
 - − "urzędy certyfikacyjne" → dodanie certyfikatu ADENA/EMPLOY → "zaufaj … wiadomości"!
 - "twoje certyfikaty"
 - "inne osoby" → dodanie certyfikatu marek.goslawski@put.poznan.pl → "zaufaj …"

Zadanie 1: podpisanie wiadomości elektronicznej Zadanie 2: zaszyfrowanie wiadomości elektronicznej Zadanie 3: podpisanie dokumentu .pdf, .odt lub .doc(x) Zadanie 4: weryfikacja podpisu kwalifikowanego

• Certyfikat w zasobniku Windows

mmc, "dodaj przystawkę", "certyfikaty"

 – IE, "Narzędzia", "Opcje internetowe", "Zawartość", "Certyfikaty"

Zadanie 1: podpisanie wiadomości elektronicznej Zadanie 2: zaszyfrowanie wiadomości elektronicznej **Zadanie 3: podpisanie dokumentu .pdf, .odt lub .doc(x)** Zadanie 4: weryfikacja podpisu kwalifikowanego

Certyfikaty
Zamierzony <u>c</u> el:
Osobisty Inne osoby Pośrednie urzędy certyfikacji Zaufane główne urzędy certyfikacji 🔹 🖈
Wystawiony dla Wystawiony przez Data wyg Przyjazna nazwa
Imarek.goslawski@p PUT Root Certification 2010-06-10 <brak> Imarek.goslawski@p PUT Root Certification 2012-02-10 <brak> Imarek.goslawski@p PUT Root Certification 2013-02-10 <brak> Imarek.goslawski@p PUT Root Certification 2011-02-10 <brak> Imarek.goslawski@p PUT Root Certification 2011-02-10 <brak> Imarek.goslawski@p PUT Root Certification 2014-01-11 <brak> Imarek.goslawski@p PUT Root Certification 2009-11-06 <brak></brak></brak></brak></brak></brak></brak></brak>
Importuj Eksportuj Usuń Zaawansowane Zamierzone cele certyfikatu Importuj Importuj Importuj
Wyświed Dowiedz się więcej o certyfikatach Zamknij

- Podpisanie dokumentów
 - 01. podpisywanie dokumentu AdobeReader (0/1/2).pdf
 - 01. podpisywanie dokumentu OpenOffice Writer.odt
 - 01. podpisywanie dokumentu MsWord.docx

Zadanie 1: podpisanie wiadomości elektronicznej
Zadanie 2: zaszyfrowanie wiadomości elektronicznej
Zadania 2. nodnicania dakumantu ndf. odt lub. dac(v)
Zadame 5: podpisame dokumentu .pdi, .odt iub .doc(x)

pis	Zabezpieczenia Czcionki Własne Zaawansowane		
Zabe	zpieczenia dokumentu		
Met	toda zabezpieczania dokumentu ogranicza możliwości ec	dycji dokumentu.	
Metoda zabezpieczenia: Brak zabezpieczeń Pokaż szczegóły			
N	łoże być otwarty przez: Wszystkie wersje programu Acr	obat	
Pods	umowanie ograniczeń dokumentu		
	Drukowanie:	Dopuszczone	
	Zestaw dokumentów:	Nie dopuszczalny	
	Kopiowanie zawartości:	Dopuszczone	
к	opiowanie zawartości ze względu na lepszą dostępność:	Dopuszczone	
	Wydzielanie stron:	Dopuszczone	
	Komentowanie:	Dopuszczone	
	Wypełnianie pól formularza:	Dopuszczone	
	Podpisywanie:	Dopuszczone	
	Tworzenie stron szablonowych:	Nie dopuszczalny	

- Weryfikacja podpisu kwalifikowanego
 - 03_zweryfikowanie podpisu kwalifikowanego.txt.XAdES

Wynik weryfikacji	×
Plik zawierający podpisy	
03_zweryfikowanie podpisu kwalifikowanego.txt.XAdE5	
Weryfikacja podpisów	
Podpis	
CN=Marek Ernest Gosławski, O=Politechnika Poznańska, C=PL	
Wynik weryfikacji	
Podpis został poprawnie zweryfikowany certyfikatem kwalifikowanym	
Szczegóły podpisu Podgląd danych Zapisz podpisane dane	
Zamknij	

Zadanie 1: podpisanie wiadomości elektronicznej
Zadanie 2: zaszyfrowanie wiadomości elektronicznej
Zadanie 3: podpisanie dokumentu .pdf, .odt lub .doc(x)
Zadanie 4: weryfikacja podpisu kwalifikowanego

- Weryfikacja podpisu kwalifikowanego
 - jak?

podać kroki weryfikacji

- 1. Weryfikacja integralności dokumentu
- Weryfikacja certyfikatu CN=Marek Ernest Gosławski,O=Politechnika Poznańska,C=PL

3. ...

Szczegóły weryfikacji podpisu

Wynik weryfikacji Treść podpisanych danych Przebieg weryfikacji

2016-09-24 12:13:08	: Weryfikuję referencje XAdES: ID-320c7aea-f0f9-4f1c-9408-3a1cd2be69db do URI 03_zweryfikowanie%20podpisu%20kwalifik 🔨
016-09-24 12:13:08	Referencja zweryfikowana poprawnie
016-09-24 12:13:08	: Weryfikuję referencje XAdES: ID-7b394b33-2e5c-4945-a9af-a526d2b8c358 do URI #ID-db14e663-af13-4a0b-a11d-d043f799d3
16-09-24 12:13:08	Referencja zweryfikowana poprawnie
)16-09-24 12:13:08	Veryfikuję podpis RSA
.016-09-24 12:13:08	: Weryfikacja podpisu RSA zakończona pomyślnie
016-09-24 12:13:08	Weryfikuję certyfikat => CN=Marek Ernest Gosławski,O=Politechnika Poznańska,C=PL
016-09-24 12:13:08	: Pobieram certyfikat CA z pliku z podpisem => C=PL, O=Krajowa Izba Rozliczeniowa S.A., CN=COPE SZAFIR - Kwalifikowany, se
016-09-24 12:13:08	c Certyfikat pobrany z pliku z podpisem poprawnie => C=PL, O=Krajowa Izba Rozliczeniowa S.A., CN=COPE SZAFIR - Kwalifikow
016-09-24 12:13:08	: Weryfikuję czas ważności certyfikatu
16-09-24 12:13:08	c Certyfikat ważny w weryfikowanym czasie
16-09-24 12:13:08	: Weryfikuję atrybut określający użycie klucza
016-09-24 12:13:08	č Atrybuty określające użycie klucza zweryfikowane pomyślnie
016-09-24 12:13:08	: Weryfikuję podpis RSA
016-09-24 12:13:08	: Weryfikacja podpisu RSA zakończona pomyślnie
6-09-24 12:13:08	: Pobieram listę CRL => CA: CN=COPE SZAFIR - Kwalifikowany,O=Krajowa Izba Rozliczeniowa S.A.,C=PL URL: http://elektronicz
6-09-24 12:13:08	c Dekoduję listę CRL
16-09-24 12:13:08	: Lista CRL zdekodowana poprawnie
16-09-24 12:13:08	: Weryfikuję listy CRL z numerem seryjnym: 8691 wystawioną przez: SERIALNUMBER=Nr wpisu: 6, CN=COPE SZAFIR - Kwalifikc
16-09-24 12:13:08	: Lista CRL zweryfikowana prawidłowo
)16-09-24 12:13:08	: Sprawdzam ważność certyfikatu => CN=Marek Ernest Gosławski,O=Politechnika Poznańska,C=PL na CRL z numerem seryjnym
16-09-24 12:13:08	c Certyfikat jest ważny => CN=Marek Ernest Gosławski,O=Politechnika Poznańska,C=PL
016-09-24 12:13:08	K Weryfikacja certyfikatu zakończona pomyślnie => CN=Marek Ernest Gosławski,O=Politechnika Poznańska,C=PL
016-09-24 12:13:08	K Weryfikuję certyfikat => CN=COPE SZAFIR - Kwalifikowany,O=Krajowa Izba Rozliczeniowa S.A.,C=PL
016-09-24 12:13:08	8 Pobieram certyfikat CA z pliku z podpisem => C=PL, O=Minister własciwy do spraw gospodarki, CN=Narodowe Centrum Certyfik
016-09-24 12:13:08	c Certyfikat pobrany z pliku z podpisem poprawnie => C=PL, O=Minister własciwy do spraw gospodarki, CN=Narodowe Centrum
016-09-24 12:13:08	2 Wervfikule czas ważoński certyfikału 💦 🎽 🎽

×

Zadanie 1: podpisanie wiadomości elektronicznej Zadanie 2: zaszyfrowanie wiadomości elektronicznej Zadanie 3: podpisanie dokumentu .pdf, .odt lub .doc(x) **Zadanie 4: weryfikacja podpisu kwalifikowanego**

• ePUAP, PZ

– <u>https://obywatel.gov.pl/</u>

- Konfigurowanie oprogramowania VeraCrypt
 - Ustawienia \rightarrow Tokeny bezpieczeństwa
 - wskazanie biblioteki PKCS#11
 - "użyj plików kluczowych"
 - "dodaj token/bilet"

Zadanie 1: podpisanie wiadomości elektronicznej Zadanie 2: zaszyfrowanie wiadomości elektronicznej Zadanie 3: podpisanie dokumentu .pdf, .odt lub .doc(x) Zadanie 4: weryfikacja podpisu kwalifikowanego



- Nie zapomnij usunąć:
 - konta z klienta poczty (Thunderbird'a)!
 - certyfikatu z zasobników!

- marek.goslawski@put.poznan.pl
- +48 61 665 3680
- +48 694 949 750
- pl. Marii Skłodowskiej-Curie 5 (Wilda) Budynek B1 (Rektorat), pok. 405

http://mcp.poznan.pl/