Państwowa Wyższa Szkoła Zawodowa w Krośnie

Administrowanie bazami danych

Bartosz Trybus
Bartosz.Trybus@pwsz.krosno.pl

Administrowanie – dwa aspekty

- Administrowanie gotowym systemem

- Administrowanie tworzeniem systemu

- Użytkownik końcowy:
  - Korzysta z wcześniej przygotowanych interfejsów.
  - Posiada uprawnienia do odczytywania i modyfikowania wybranych danych.
- Projektant/Programista:
  - Korzysta z narzędzi do projektowania aplikacji.
  - Posiada uprawnienia do tworzenia bazy, schematów, tabel, …
- Administrator

Administrowanie gotowym systemem

- Zadania administratora
  - instalowanie
  - konfigurowanie
  - tworzenie kopii zapasowych
  - usuwanie awarii
  - zarządzanie użytkownikami (przywileje, hasła)
  - odpowiada za ciągłość pracy
  - odpowiada za wydajność
  - …
- Obszar działań: aplikacja i SZBD

Administrowanie jako zarządzanie procesem

- Zarządzanie procesem projektowym
  - nadzór nad przebiegiem
  - przydział zadań dla poszczególnych wykonawców
  - rozliczanie wykonawców z wykonanych prac
  - weryfikacja efektów poszczególnych etapów
  - organizacja i koordynacja prac
  - metody inżynierii oprogramowania
- Informatyzacja jako proces

Projektowanie i tworzenie systemu

- Projektowanie klas użytkowników aplikacji i ich ról
  - dokumenty i diagramy projektowe (np. UML, ERD)
  - rejestry użytkowników
- Problemy związane z bezpieczeństwem
  - ochrona danych (osobowych, wrażliwych, haseł)
  - tworzenie bezpiecznego kodu
  - mechanizmy uwierzytelniania
  - aspekty prawne

Zagrożenia bezpieczeństwa

- Nieuprawniony dostęp do bazy danych
- Wykradanie haseł, danych osobowych, wrażliwych, zastrzeżonych
- Nieuprawniony dostęp do funkcji programu (aplikacji) przetwarzającego dane
- Zagrożenia wynikające z umieszczania w bazie błędnych danych

Polityka bezpieczeństwa systemów baz danych

- Polityka bezpieczeństwa powinna obejmować:
  - bezpieczną strukturę bazy danych
  - zabezpieczenie aplikacji przed nieuprawnionym dostępem
  - opracowanie poziomów uprzywilejowania użytkowników aplikacji bazodanowej
  - ochronę danych podczas przetwarzania
  - ochronę danych podczas składowania w bazie
  - właściwe administrowanie systemem zarządzania bazą danych i aplikacją bazodanową

Uwierzytelnianie użytkownika w aplikacjach bazodanowych

Zarządzanie użytkownikami aplikacji

- Komputerowe aplikacje gromadzące i udostępniające dane prawie zawsze wymagają obsługi wielu użytkowników.
  - zabezpieczenie dostępu do danych przed nieupoważnionymi podmiotami
  - udostępnienie różnych funkcji programu w zależności od zadań, jakie dany użytkownik ma za zadanie realizować.
- W aplikacjach internetowych problem identyfikacji użytkownika jest jeszcze bardziej istotny.

Podstawowe pojęcia

- Identyfikacja
  - Deklaracja tożsamości
- Uwierzytelnianie (*authentication*)
  - Potwierdzenie tożsamości
  - Uwierzytelnianie dwuskładnikowe (*two-factor authentication*)
- Autoryzacja (*authorisation*)
  - Kontrola uprawnień dostępu do określonego zasobu (danych, funkcji)

Potwierdzenie tożsamości

- Dominującą metodą potwierdzenia tożsamości użytkownika jest konieczność podania przez niego danych uwierzytelniających w postaci identyfikatora i hasła lub klucza prywatnego.

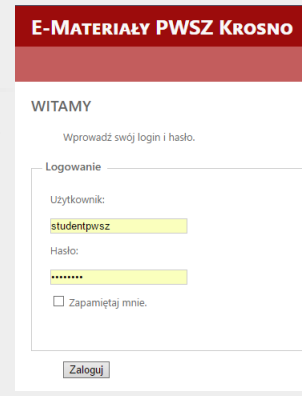
- Inne metody

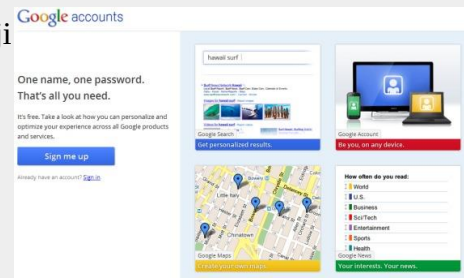
Internetowe schematy uwierzytelniania I

- ***Uwierzytelnianie w protokole HTTP***
  - część protokołu HTTP 1.0 (RFC 2617, www.ietf.org/rfc/rfc2617.txt)
  - obsługiwane przez wszystkie serwery i przeglądarki
  - Basic: hasło niechronione, proste do odkodowania (base64)
  - Digest: hasło poddawane funkcji skrótu (hash)
  - HTTPS (TLS/SSL)

Internetowe schematy uwierzytelniania II

- ***Uwierzytelnianie za pomocą formularzy***
  - stosowane przez większość z witryn
  - użytkownik wprowadza login i hasło na stronie WWW
  - dane logowania powinny być wysyłane do serwera w postaci zaszyfrowanej (SSL/TLS), w przeciwnym przypadku są jawne
  - mechanizm po stronie aplikacji sprawdza login i hasło
- ***Powiązane schematy***
  - Konta Google, FB, Microsoft

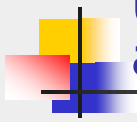




Uwierzytelnianie na poziomie aplikacji

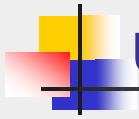
- Aplikacje wykorzystują do sprawdzenia tożsamości użytkownika dodatkowe tabele lub pliki, przechowujące informacje o identyfikatorach i hasłach użytkowników wraz z danymi o ich przywilejach.
- Odpowiedni kod aplikacji dokonuje sprawdzenia, czy wprowadzone login i hasło istnieją w spisie i jeżeli tak jest, wówczas udostępnia użytkownikowi odpowiednie funkcje programu na podstawie przydzielonych mu uprawnień

Schemat taki dobrze sprawdza się w aplikacji o strukturze klient-serwer, można wtedy bowiem oddzielić część uwierzytelniającą od reszty aplikacji użytkownika i umieścić ją po stronie serwera, który udostępni dane aplikacji tylko wtedy, gdy uwierzytelnianie się powiodło.



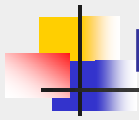
Uwierzytelnianie na poziomie aplikacji - schemat

1. klient łączy się z serwerem wysyłając odpowiedni URL
2. serwer nawiązuje połączenie szyfrowane (HTTPS) i przesyła formularz logowania do przeglądarki klienta
3. użytkownik wpisuje dane (login, hasło) na formularzu
4. dane użytkownika są wysyłane do serwera (np. metodą POST) w postaci zaszyfrowanej (SSL)
5. odpowiedni moduł aplikacji po stronie serwera (np. PHP, ASP, CGI itp.) otrzymuje login i hasło
6. aplikacja sprawdza, czy wprowadzony login i hasło istnieją w dodatkowej tabeli użytkowników
7. jeżeli dane są prawidłowe, aplikacja udostępnia swoje funkcje użytkownikowi.



Uwierzytelnianie na poziomie SZBD

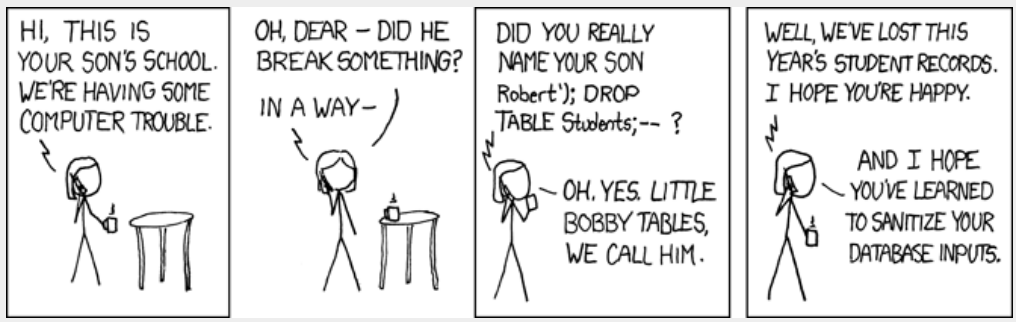
- Programy, które korzystają z serwerów baz danych mają możliwość wykorzystania dostępnych w większości z nich wewnętrznych mechanizmów obsługi użytkowników. Są one dostępne m.in. w systemach Microsoft SQL Server, Oracle Server, MySQL i in.
- Na system ochrony i obsługi użytkowników w serwerach baz danych składają się m.in.:
  - konieczność podawania identyfikatora i hasła użytkownika (logowania) przy łączeniu się z bazą danych,
  - kontrola uprawnień użytkownika przy realizacji każdej z instrukcji SQL,
  - dodatkowe funkcje SQL służące do manipulowania listą użytkowników i ich uprawnieniami.

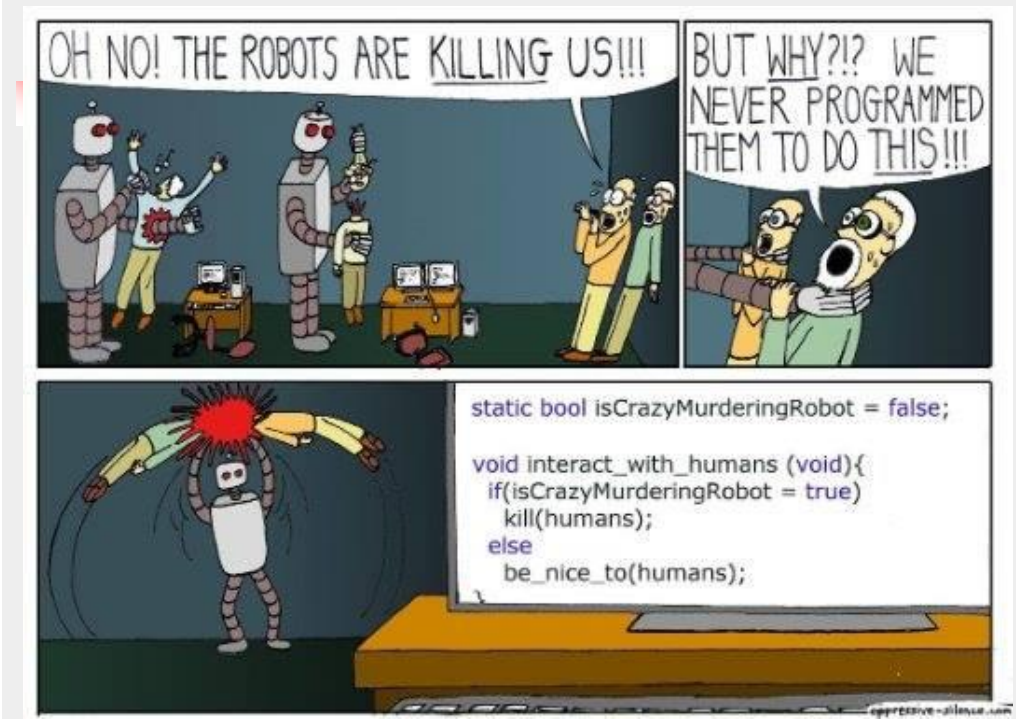


Demonstracja / warsztaty

Nie ufaj danym wejściowym

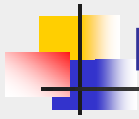
- Wszystkie dane są niepoprawne dopóki nie zostanie udowodnione, że tak nie jest.
- Dane muszą być sprawdzone pod względem poprawności w momencie, gdy przekraczają granicę między środowiskiem niezaufanym a środowiskiem zaufanym.





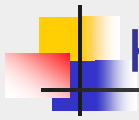
Kryptografia - podstawy

- Kryptografia to nauka dotycząca szyfrowania znaków (danych), tak aby ich znaczenie nie zostało odczytane przez osoby niepowołane.
- Istniała znaczenie wcześniej niż pierwsze komputery, lecz dopiero one umożliwiły uzyskanie kodów praktycznie nie dających się złamać.



Kryptografia - nazwy

- Dane jawne, czysty tekst (*plain text*, *clear text*)
- Szyfrowanie (*encryption*) – ukrywanie znaczenia danych
- Tekst zaszyfrowany, szyfrogram (*cipher text*) – jego znaczenie nie jest widoczne
- Rozszyfrowanie (*decryption*)
- Klucz (*key*) – zbiór liczb, znaków, bitów używany do szyfrowania i rozszyfrowania



Kryptografia – początek 1

- Potrzeba szyfrowania informacji istnieje od dawna
- Szyfr Cezara (Juliusza, 100-44 p.n.e.)
- Tekst jawny ;)

  `ALEA IACTA EST`
- Tekst zaszyfrowany (przesunięcie o 3):

  `DOHD LDFWD HVW`
- Rodzaj szyfru podstawieniowego
- ROT13 – najpowszechniej stosowany (napisz w C#)

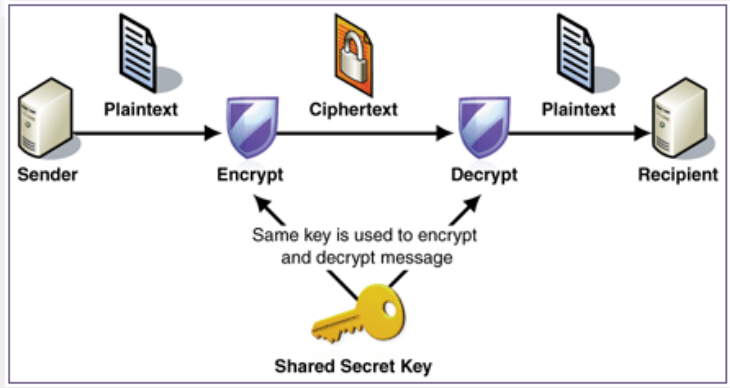
Kryptografia – początek 2

- **GA-DE-RY-PO-LU-KI :** szyfr harcerski (zuchowy) https://pl.wikipedia.org/wiki/Gaderypoluki
- W szyfrowanym wyrazie litery z sylab klucza zastępujemy drugimi.
- Jeżeli nie ma litery, to jej nie zmieniamy.
- Napisz program, który:
  - szyfruje podany wyraz wg schematu
  - rozszyfrowuje
  - umożliwia ustalenie dowolnych sylab klucza

Kryptografia symetryczna

- Jeden klucz do szyfrowania i rozszyfrowania znany nadawcy i odbiorcy
- Podstawowa metoda szyfrowania aż do lat 1970-tych
- Jej skuteczność zależy od utajnienia klucza (nie może być „skompromitowany”)
- Metoda łatwa do realizacji, nawet w przypadku ograniczonych zasobów obliczeniowych

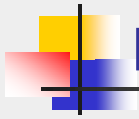
Kryptografia symetryczna - schemat



- Przykłady algorytmów: AES (Rijndael), 3DES, DES, RC2, Blowfish (blokowe)

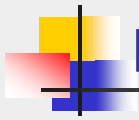
DES, 3DES, AES

- DES – symetryczny szyfr blokowy
  - Klucz 56-bit
  - Standard od 1976
  - 1998 – złamanie klucza w 3 dni
- 3DES – następca DES
  - 3 klucze (56, 112, 168 bit)
  - Duża złożoność obliczeniowa, ale obecnie możliwy do złamania
- AES (Rijndael)
  - Klucz 128, 192, 256-bitowy
  - Obecnie popularny standard dla różnych aplikacji i urządzeń



Funkcje skrótu

- Skrót (*hash*)
- Gdy nie potrzebujemy odzyskać pierwotnej wartości
- Gdy nie chcemy, aby ktokolwiek mógł ją odzyskać
- Funkcje przyjmują dowolny ciąg i transformują go do zbioru bajtów o stałym rozmiarze
- Operacja jednokierunkowa
- Stosowane zwykle do niewielkich ciągów (np. hasło)



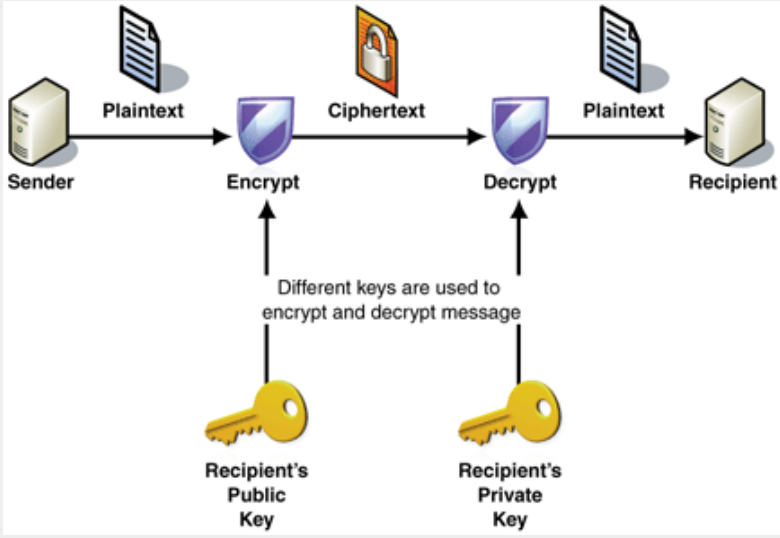
Funkcje skrótu MD5 i SHA

- MD5 - Message Digest 5
  - Wynik128-bitowy
- Secure Hash Algorithm (SHA)
  - 160-bit

Kryptografia asymetryczna

- W przeciwieństwie do k. symetrycznej, asymetryczna obejmuje dwa oddzielne klucze, pozostające w relacji matematycznej.
- Jeden z kluczy – *publiczny* – jest współdzielony przez nadawcę i odbiorcę.
- Drugi klucz, *prywatny* jest ukryty u odbiorcy.
- Klucz prywatny i publiczny tworzą *parę kluczy*.

Kryptografia asymetryczna - schemat



Rola klucza publicznego

- Klucza prywatnego nie da się praktycznie odtworzyć na podstawie publicznego
- Klucz publiczny odbiorcy służy do szyfrowania przez nadawcę
- Nie szyfrujemy kluczem prywatnym, bo wówczas ktokolwiek mając nasz klucz publiczny może odszyfrować wiadomość
- Zastąpienie miejscami klucza publicznego i prywatnego jest używane do podpisu elektronicznego

Algorytm RSA

- Ron Rivest, Adi Shamir and Leonard Adleman (1977)
- https://www.rsa.com
- Oparty na liczbach pierwszych
- Klucz RSA o długości 768 bitów został złamany (zajęło to 2 lata na setkach komputerów)
- Obecnie bezpieczne długości to 2048 i 3072
- .NET: System.Security.Cryptography.RSA

Dokument elektroniczny (DE)

- Rekord zawierający informacje zapisana na namacalnym nośniku takim, jak np. dyskietka, dysk twardy, CD-ROM, DVD, karta elektroniczna, itp., który umożliwia jej przechowywanie, zapis i odczyt przy zastosowaniu technologii informatycznych.

Problemy z dokumentem elektronicznym

- Problemy przy traktowaniu DE jak dokumentu papierowego:
  - Nie ma różnicy między kopią dokumentu a oryginałem
  - Wprowadzenie zmian w dokumencie elektronicznym nie pozostawia żadnych śladów
  - Stwierdzenie autentyczności dokumentu elektronicznego musi opierać się na dowodach zawartych w samej informacji

Elektroniczna wymiana dokumentów

- Kompleksowa informatyzacja – zastąpienie tradycyjnych dokumentów wersjami elektronicznymi
- Komunikacja ze światem zewnętrznym – Internet (problem bezpieczeństwa danych, spójności i autentyczności)
- Dokument elektroniczny może dobrze funkcjonować jedynie w przypadku, gdy odbiorca dokumentu elektronicznego jest przekonany, że utworzył go ten podmiot, który podaje się za jego twórcę.
- W przypadku dokumentu papierowego gwarancje taka dawał odręcznie złożony podpis, w przypadku dokumentu jest nią podpis elektroniczny (PE)

Podstawy prawne dokumentu elektronicznego

- Wola osoby dokonującej czynności prawnej może być wyrażona przez każde zachowanie się tej osoby, które ujawnia jej wolę w sposób dostateczny.
- Jeżeli przepis szczególny tak stanowi, pisma procesowe wnosi się na urzędowych formularzach lub na elektronicznych nośnikach informatycznych
- Minister sprawiedliwości określi, w drodze rozporządzenia, szczegółowe zasady i termin wprowadzenia techniki informatycznej, warunki, jakim powinny odpowiadać elektroniczne nośniki informatyczne, na których pisma procesowe maja być wnoszone, tryb odtwarzania danych na nich zawartych oraz sposób ich przechowywania i zabezpieczania, uwzględniając stan wyposażenia sądów w odpowiednie środki techniczne i poziom rozwoju technik informatycznych.
- Każde pismo procesowe powinno zawierać m.in. podpis strony albo jej przedstawiciela ustawowego lub pełnomocnika

Dokument w ustawie

- Art. 115
  - § 14. Dokumentem jest każdy przedmiot lub inny zapisany nośnik informacji, z którym jest związane określone prawo, albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne.

Podrabianie dokumentów

- **Art. 270**
  - § 1. Kto, w celu użycia za autentyczny, podrabia lub przerabia dokument lub takiego dokumentu jako autentycznego używa, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności od 3 miesięcy do lat 5.
  - § 2. Tej samej karze podlega, kto wypełnia blankiet, zaopatrzony cudzym podpisem, niezgodnie z wolą podpisanego i na jego szkodę albo takiego dokumentu używa.
  - § 2 a. W przypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
  - § 3. Kto czyni przygotowania do przestępstwa określonego w § 1, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Tajemnica korespondencji

- **Art. 267**. **§ 1.** Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie,
- podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
- **§ 2.** Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.
- **§ 3.** Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.
- **§ 4.** Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie.

Niszczenie informacji

- **Art. 268. § 1.** Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
- **§ 2.** Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.
- **§ 3.** Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Oszustwo komputerowe

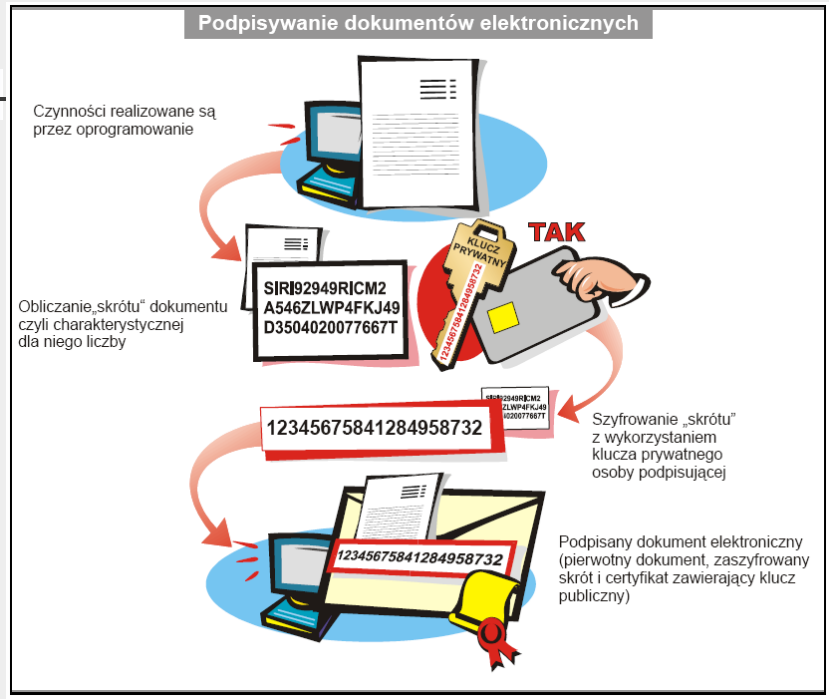
- Art. 287 § 1. Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. § 2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Bezpieczny dokument elektroniczny

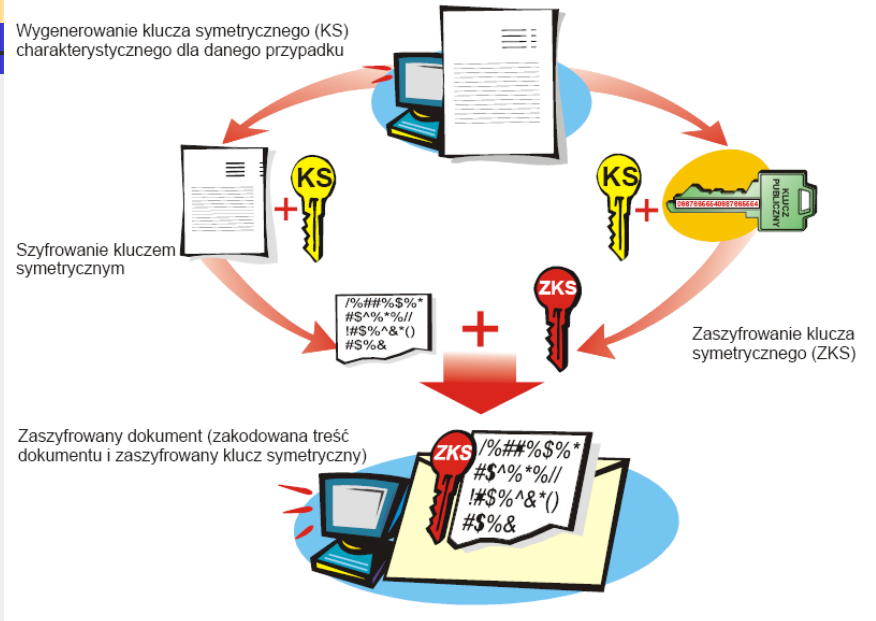
- Integralność
- Poufność
- Niezaprzeczalność

- Zastosowanie kryptografii:
  - szyfrowanie kluczem tajnym lub kluczem publicznym (poufność),
  - szyfrowanie kluczem prywatnym (integralność),
  - podpis elektroniczny (autentyczność, niezaprzeczalność).

Podpisywanie dokumentów elektronicznych



Szyfrowanie informacji



Podpis elektroniczny – akty prawne

- Rozporządzenie eIDAS Parlamentu Europejskiego i Rady (UE) NR 910/2014 z dnia 23 lipca 2016r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE
- Ustawa z dnia 5 września 2016r. o usługach zaufania oraz identyfikacji elektronicznej Dz.U. z 2016 r. nr 1579

Podpis i pieczęć elektroniczna

- **Podpis elektroniczny** - dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej, i które użyte są przez podpisującego jako podpis.
- **Pieczęć elektroniczna** - dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych

Podpis zaawansowany

- Zaawansowany podpis elektroniczny musi spełniać następujące wymogi:
  - a) jest unikalnie przyporządkowany podpisującemu;
  - b) umożliwia ustalenie tożsamości podpisującego;
  - c) jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą; oraz
  - d) jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna.

Podpis kwalifikowany

- **Podpis kwalifikowany** - zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego

Certyfikat kwalifikowany

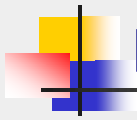
- **Kwalifikowany certyfikat podpisu elektronicznego** - wydawany przez kwalifikowanego dostawcę usług zaufania
- Zawiera następujące informacje:
  - a. wskazanie - co najmniej w postaci pozwalającej na automatyczne przetwarzanie - że dany certyfikat został wydany jako kwalifikowany certyfikat podpisu elektronicznego;
  - b. zestaw danych jednoznacznie reprezentujących kwalifikowanego dostawcę usług zaufania wydającego kwalifikowane certyfikaty, obejmujący co najmniej państwo członkowskie, w którym dostawca ma siedzibę, oraz — w odniesieniu do osoby prawnej: nazwę i, w stosownym przypadku, numer rejestrowy zgodnie z oficjalnym rejestrem, — w odniesieniu do osoby fizycznej: imię i nazwisko tej osoby;
  - c. co najmniej imię i nazwisko podpisującego lub jego pseudonim; jeżeli używany jest pseudonim, fakt ten jest jasno wskazany;
  - d. dane służące do walidacji podpisu elektronicznego, które odpowiadają danym służącym do składania podpisu elektronicznego;
  - e. dane dotyczące początku i końca okresu ważności certyfikatu;
  - f. kod identyfikacyjny certyfikatu, który musi być niepowtarzalny dla kwalifikowanego dostawcy usług zaufania;
  - g. zaawansowany podpis elektroniczny lub zaawansowaną pieczęć elektroniczną wydającego kwalifikowanego dostawcy usług zaufania;
  - h. miejsce, w którym nieodpłatnie dostępny jest certyfikat towarzyszący zaawansowanemu podpisowi elektronicznemu lub zaawansowanej pieczęci elektronicznej, o których mowa w lit. g);
  - i. miejsce usług, z którego można skorzystać w celu złożenia zapytania o status ważności kwalifikowanego certyfikatu;
  - j. w przypadku gdy dane służące do składania podpisu elektronicznego powiązane z danymi służącymi do walidacji podpisu elektronicznego znajdują się w kwalifikowanym urządzeniu do składania podpisu elektronicznego, odpowiednie wskazanie tego faktu co najmniej w postaci pozwalającej na automatyczne przetwarzanie

Infrastruktura zaufania

- eIDAS zakłada powstanie krajowych infrastruktur zaufania w każdym z Państw członkowskich.
- W Polsce odpowiedzialność za jej stworzenie została przypisana Ministerstwu Cyfryzacji.
- Krajowa infrastruktura zaufania składa się z:
  - rejestru dostawców usług zaufania;
  - zaufanej listy;
  - narodowego centrum certyfikacji.

Narodowe centrum certyfikacji

- Zadania:
  - wydawanie certyfikatów dla dostawców usług zaufania, które pozwalały im będą świadczyć usługi zaufania;
  - zarządzanie tymi certyfikatami, w tym publikację list certyfikatów unieważnionych (CRL).
- Ministerstwo może upoważnić Narodowy Bank Polski do realizacji tych zadań.



Dostawcy usług zaufania

- obowiązek zachowania w tajemnicy danych związanych ze świadczonymi usługami;
- obowiązek przechowywania danych i dokumentów dla świadczonych usług (np. list CRL) przez 20 lat od chwili ich utworzenia.
- konieczność posiadania **p**olityki świadczenia usług w której znajdzie się zbiór reguł i zasad według których świadczone są usługi.
- zapewnienie przez dostawcę całodobowej możliwości zgłaszania żądań unieważnienia certyfikatów
- dostawca nie odpowiada za szkody będące wynikiem nieprzestrzegania przez użytkownika zasad polityki.

Ważność podpisu

- Podpis elektroniczny lub pieczęć elektroniczna weryfikowane za pomocą certyfikatu wywołują skutki prawne, jeżeli zostały złożone w okresie ważności tego certyfikatu.
- Podpis elektroniczny lub pieczęć elektroniczna złożone w okresie zawieszenia certyfikatu wykorzystywanego do jego weryfikacji nie wywołują skutków prawnych.
- Po uchyleniu zawieszenia certyfikatu, skutek prawny podpisu elektronicznego lub pieczęci elektronicznej weryfikowanych tym certyfikatem złożonych w trakcie zawieszenia następuje z chwilą uchylenia tego zawieszenia.

Przepisy karne

- Art. 40. 1. Kto składa kwalifikowany podpis elektroniczny lub zaawansowany podpis elektroniczny z wykorzystaniem danych do składania podpisu elektronicznego przyporządkowanych do innej osoby, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3. 2. Tej samej karze podlega, kto składa kwalifikowaną pieczęć elektroniczną lub zaawansowaną pieczęć elektroniczną, nie będąc do tego uprawnionym.
- Art. 41. Kto bez uprawnienia kopiuje lub przechowuje nieprzyporządkowane do niego dane do składania zaawansowanego podpisu elektronicznego lub pieczęci elektronicznej lub inne dane, które mogłyby służyć do ich odtworzenia, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.
- Art. 42. 1. Kto, świadcząc usługi zaufania, wydaje certyfikat zawierający nieprawdziwe dane w celu popełnienia czynu zabronionego, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.
- 2. Tej samej karze podlega, kto składa podpis elektroniczny lub pieczęć elektroniczną weryfikowane certyfikatem, o którym mowa w ust. 1, w celu popełnienia czynu zabronionego.
- Art. 43. 1. Kto, będąc obowiązanym do zachowania tajemnicy związanej ze świadczeniem usług zaufania, ujawnia lub wykorzystuje, wbrew warunkom określonym w przepisach o usługach zaufania, informacje objęte tą tajemnicą, podlega grzywnie.
- 2. Jeżeli sprawca dopuszcza się czynu określonego w ust. 1 jako kwalifikowany dostawca usług zaufania albo w celu osiągnięcia korzyści majątkowej lub osobistej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.
- Art. 44. Kto, wydając środek identyfikacji elektronicznej w ramach notyfikowanego systemu identyfikacji elektronicznej, wydaje taki środek osobie nieuprawnionej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.