Obszerny dokument

Liczymy z niego skrot

Skrot podpisujemy kluczem prywatnym

Weryfikacja podpisu do deszyfracja skrotu kluczem publicznym - jeśli takie same to prawidlowa weryfikacja

Podpis cyfrowy –

Unikalność – nikt nie ma takiego samego klucza prywatnego – rozni się od tradycyjnego podpisu tym ze tradycyjny jest praktycznie zawsze taki sam (podobny) – elektroniczny zawsze inny (szyfrogram oryginalnego dokumentu lub skrotu, szyfrogramy roznych dokumentów sa rozne - logiczne)

Integralność - jeśli oryginalny dokument zostanie zmieniony choćby na jednym bicie – podpis elektroniczny zostaje unieważniony

Niezaprzeczalność – tylko osoba podsiadajaca wlasciwy klucz prywatny może wygenerować podpis elektroniczny

Certyfikat – informacja która laczy klucz publiczny z wlascicielem tego klucza – taka jednostak podpisuje za pomocą swojego klucza prywatnego taka informacje

- kto jest wlascicielem certyfikatu

- kto poswiadcza ze to prowda

- numer seryjny – wazny – żeby identyfikować certyfikaty

Certyfikat to plik tekstowy podpisany przez urząd certyfikacyjny

- od kiedy wazny jest certyfikat

- podmiot dla którego został wydany

- klucz publiczny

Jak wierzyc centrum certyfikacyjnemu, czy ktoś się pod nie nie podszywa czasem, (to kluczem publicznym tych urzedow sa szyfrowane certyfikaty)

Infrastruktura klucza publicznego – tworzenie rozpowszechnianie zarzadzanie danymi zawartymi w certyfikatach

- RA – urzędy rejestracji – weryfikacja danych użytkownika a następnie jego rejestracja

Na slajdzie…

Jak okreslic wlasciciela klucza publicznego w certyfikacie - adres mailowy