24.02.03

BDC- Infrastruktura Klucza Publicznego, 2003
WPPT, Politechnika Wrocławska

Lista nr 1

1. Zadanie praktyczne: zdobyć certyfikat testowy od jednego z dostawców (EuroPKI w WCSS, Signet, Unizeto, Sigillum, ...). Obejrzeć jego pola (zarówno w przeglądarce, jak i zobaczyć jak to jest kodowane). Wysłać list do prowadzącego ćwiczenia podpisany takim certyfikatem.

2. Zadanie praktyczne: wygenerować sobie klucz pgp. Zapisać w swoim keyring co najmniej 2 klucze publiczne swoich kolegów. Wysłać prowadzącemu ćwiczenia plik z tekstem „ala ma kota“ zaszyfrowany jego kluczem publicznym i podpisany. Plik ma być w formacie ASCII.

3. Zadanie praktyczne: napisać politykę certyfikacji wg schematu PKIX (znaleźć!) dla CA obsługującego wewnętrzne potrzeby Instytut podległy CA w WCSS. To jest konkurs - najlepsze 3 polityki dostaną po 3 punkty bonusowe na kolokwium.

4. Zaprojektować struktury danych dla

   - repozytorium wydanych certyfikatów (zakładamy tempo napływu certyfikatów takie jak może się zdarzyć w życiu),
   - repozytorium unieważnionych certyfikatów. Optymalizowany ma być czas odpowiedzi.
   - j.w., ale ma umożliwiać łączenie takich list.

   Pamiętajmy o efektywnym usuwaniu unieważnionych certyfikatów, którym upłynął termin ważności.

5. Zaproponuj jakąś metodę realizacji usługi generowania pary kluczy RSA przez CA, tak aby zarówno klient jak i CA nie miały kontroli nad kluczem (i nie mogły go zawrzeć w „małej przestrzeni“ umożliwiając atak przez przeszukanie).

6. Zaproponuj jakąś metodę realizacji usługi znakowania czasem przez CA, tak aby niemożliwe było antydatowanie znaków czasu.

7. Zinterpretuj algorytmiczne znaczenie definicji znakowania czasem z polskiej Ustawy o podpisie elektronicznym (znajdź ją).

/-/ Mirosław Kutyłowski