Przed przeczytaniem upewnij się, że wiesz na czym polega RSA (odsyłam do Cormena, tam fajnie jest wszystko wyjaśnione).

Ustalmy liczbę L która będzie „długością klucza". Niech zatem $L = 2048$.

1 Tworzenie, podpisywanie i rozsyłanie kluczy

1. Klient łączy się z CA, żąda certyfikatu zgodnie z **PKCS#10v1.7**
2. CA przekazuje Dealerowi żądanie, wraz z losowym **tokenem** – identyfikatorem sesji
3. CA przekazuje Klientowi adres Dealera (IP, port)
4. Dealer wykonuje swoją magiczną procedurę rozproszonego tworzenia klucza. Po wszystkim każdy i-ty Poddealer posiada trzy wartości: n, e, d_i. Parę (n, e) nazywamy **kluczem publicznym**. $d_1 + d_2 + d_3 = d$, parę (d, e) nazywamy kluczem prywatnym, którego **żadna strona nie posiada**, bo żadna z maszyn nie jest w stanie odtworzyć d. n jest tworzone tak, że jest długości L
5. Dealer wysyła do CA klucz publiczny
6. CA podpisuje ten klucz – wystawia **certyfikat X.509** i przekazuje go Klientowi (oznaczmy certyfikat literą c)
7. CA komunikuje się z Mediatorem, wysyła mu certyfikat i token.
8. Mediator korzystając z generatora liczb losowych **SP-800-90** oblicza d_m na podstawie poniższego wzoru:

   $$d_m = f(K, c)$$

   gdzie K to pewien stały, prywatny klucz Mediatora, c to certyfikat, funkcja f to pewna funkcja generująca ciąg losowy. d_m musi składać się z L bitów i tworzony jest deterministycznie (bez bitów entropii)
9. Mediator losowo dzieli d_m na trzy wartości takie, że $d_{m1} + d_{m2} + d_{m3} = d_m$. Liczby powinny mieć porównywalne długości. Mediator ma już swoją połówkę klucza prywatnego: (d_m, e)
10. Mediator łączy się (SSL) z każdym z Poddealerów, przekazując i-temu Poddealerowi d_i oraz token
11. Mediator zgłasza CA fakt, że załatwił swoją robotę, CA mówi Klientowi, że może się połączyć z Dealerem
12. Klient łączy się (SSL) z każdym z Poddealerów, przekazując każdemu token. Każdy i-ty Poddealer odsyła Klientowi różnicę $d_i - d_{mi}$
13. Klient oblicza swoje d_k na podstawie wzoru: $d_k = (d_1 - d_{m1}) + (d_2 - d_{m2}) + (d_3 - d_{m3})$. Widzimy więc, że $d = d_k + d_m$. d_k zna tylko Klient, d_m zna tylko Mediator, d nie zna nikt. Połówka klucza prywatnego, która należy do klienta jest parą liczb (d_k, e)

2 Podpisywanie wiadomości

1. Dla wiadomości M Klient liczy $h(M)$ gdzie h jest pewną ustaloną funkcją hashjującą. Oblicza też Δ, które jest paddingiem PSS na $h(M)$.
2. Klient podpisuje Δ swoją częścią klucza, tzn. liczy S_1 takie, że:

   $$S_1 = \Delta^{d_k} \mod n$$

3. Klient wysyła do Mediatora $(h(M), \Delta, S_1, c)$
4. Mediator sprawdza ważność certyfikatu c, padding Δ, po czym podpisuje Δ swoją częścią klucza:

   $$S_2 = \Delta^{d_m} \mod n$$

   Tworzy podpis $S = S_1 \cdot S_2 \mod n$, sprawdza czy jest to poprawny podpis, po czym odsyła go Klientowi w formacie **XAdES**.