DSS (Digital Signature Service) – este o biblioteca software open-source, care vizeaza implementarea standardelor pentru crearea, augumentarea si validarea de semnatura

Cum functioneaza autentificarea cu smart card?

* Smart card-ul este introdus in cititor, iar placa de contact a cardului face contact fizi cu cititorul pentru a transmite date.
* Utilizatorul introduce PIN-ul asociat si are loc un schimb de chei cu sistemul de operare sau aplicatia pentru a valida certificatul si cheile associate.

**Pasi:**

1. Utilizatorul vizitează un serviciu web pe dispozitivul său și începe procesul de conectare.
2. Serviciul solicită utilizatorului să se autentifice folosind token-ul hardware prin emiterea unei „provocare”, care este un mesaj care conține informații despre serviciu împreună cu un număr aleatoriu. Dacă utilizatorul folosește un autentificator de roaming, acesta este punctul în care trebuie să îl conecteze (prin USB, NFC, Bluetooth sau similar).
3. Dispozitivul utilizatorului trimite această provocare de autentificare tokenului hardware.
4. Indicatorul hardware solicită utilizatorului un gest de autorizare, cum ar fi:

* Scanarea unei amprente
* Apăsând un buton
* Introducerea unui PIN

1. Presupunând că gestul de autorizare este valid, tokenul semnează provocarea folosind cheia sa privată și o trimite înapoi ca răspuns la dispozitivul utilizatorului.
2. Dispozitivul returnează răspunsul jetonului către serviciul web.
3. Serviciul web recunoaște răspunsul ca fiind semnat de cheia privată corectă și că conține numărul aleatoriu pe care serviciul web l-a trimis mai devreme.
4. Serviciul web autentifică utilizatorul.

<https://anvil.works/blog/two-factor-auth-with-hardware>

Smart cardurile sunt dispozitive de stocare sigure ce conțin un microprocesor capabil să execute operațiuni criptografice, cum ar fi generarea de semnături digitale. Când se efectuează o semnătură digitală, smart cardul primește o solicitare de a semna electronic o porțiune de date, cunoscută sub numele de "challenge" în contextul autentificării. În loc să exporte cheia privată pentru a efectua semnătura într-un mediu potențial nesigur (cum ar fi pe un computer sau un server la distanță), smart cardul efectuează operația de semnătură în interiorul său securizat. Acest lucru asigură că cheia privată nu părăsește niciodată dispozitivul fizic securizat, protejând-o împotriva furtului sau a expunerii.

Procesul de semnătură pe smart card se desfășoară astfel:

Solicitarea de semnătură: Sistemul sau aplicația care necesită autentificarea generează un challenge și îl transmite către smart card prin intermediul unui software de interfatare, cum ar fi NexU în contextul descris.

Introducerea PIN-ului: Pentru a autoriza utilizarea cheii private în scopul semnăturii, utilizatorul este solicitat să introducă un PIN pe dispozitivul care interacționează cu smart cardul. Acest pas asigură că doar deținătorul legitim al cardului poate iniția o semnătură.

Generarea semnăturii: Odată autorizată, cheia privată stocată pe smart card este folosită pentru a semna challenge-ul. Operațiunea criptografică se desfășoară integral pe chipul smart cardului.

Transmiterea semnăturii: Semnătura digitală generată este apoi trimisă înapoi la sistemul solicitant prin intermediul software-ului de interfatare, fără ca cheia privată să fie expusă în acest proces.

Verificarea semnăturii: Sistemul care primește semnătura folosește cheia publică a utilizatorului, care este de obicei stocată într-o bază de date sau într-un director public, pentru a verifica autenticitatea semnăturii. Dacă semnătura corespunde cu challenge-ul folosind cheia publică, autentificarea este considerată un succes.

Acest mecanism nu numai că asigură integritatea și autenticitatea semnăturii, dar protejează și cheia privată împotriva compromiterii. Utilizarea smart cardurilor pentru semnătura digitală și autentificare reprezintă o soluție robustă în ceea ce privește securitatea informatică, oferind un echilibru între accesibilitate, securitate și confidențialitate.