Idea / Approach Details

Ministry Category: Department of Defence Production, Ministry of Defence

Problem Statement: Digital Signature Verification in Local Area Network using ASP.Net & C#

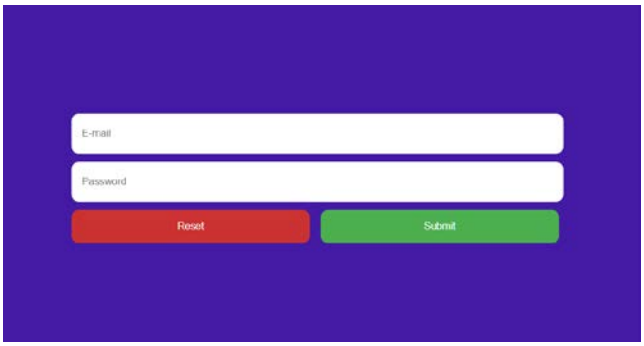
Problem Code: MOD13

Team Leader Name: MERGU ANIRUDH SAI

College Code: 5195

Prototype / Approach Details:

Problem Scenario – I: Authentication



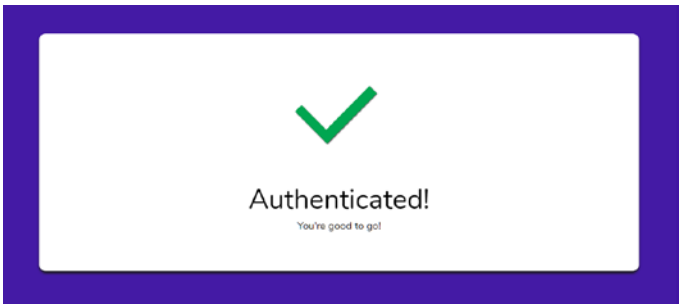
The application will follow two-step verification procedure using public key of the user stored in the server.

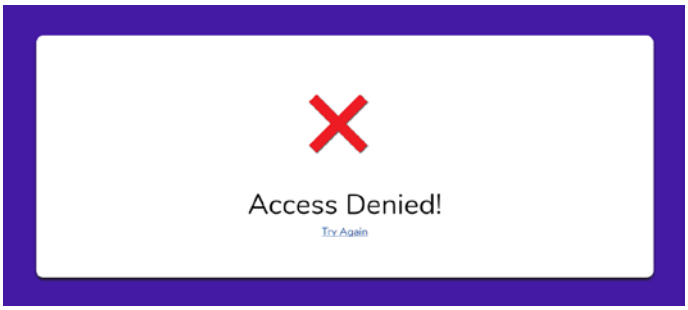
The first level of security using username (or email) and password.

The second level of security using public key encryption on the server side and private key decryption on the client side using Cryptographic APIs. The steps of authentication are listed below:

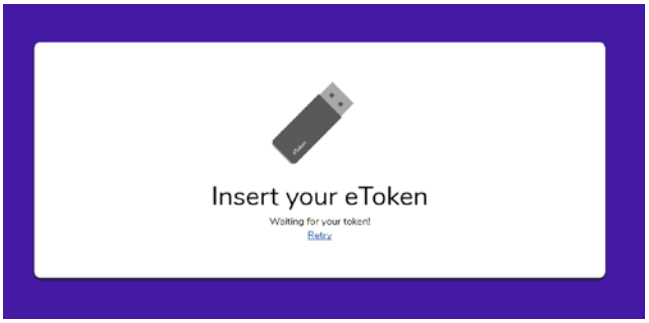
a) The user first logs in with username (or equivalent e-mail/mobile number) and password. The given credentials are checked for validity. If valid, then he/she will be redirected to the second stage of verification. Otherwise, he/she will be asked to re-check the credentials.

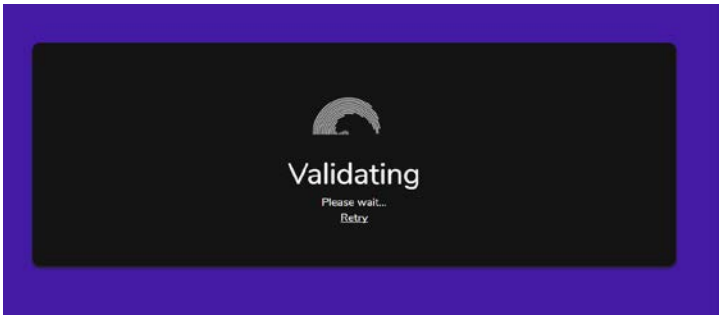
The respective screens are shown below:





b) After successful validation of the user, he/she will be asked to insert the eToken. The client-side program will detect the eToken and sends a request to the server-side program which generates a random number and encrypts it with the public key fetched from the server. Then the server-side program sends the validation request to the client-side program which will decrypt it using private key. If the initially generated random number and the decrypted number match, then the user will be authenticated successfully.





Problem Scenario – II: Digitally signing documents (PDF, Word and Excel)

1. **Signing the document:** The document uploaded will be signed automatically by the server-side C# program using the private key present in the eToken plugged in by the user. The digitally signed document will be stored in the server.

2. **Verification of the digitally signed document:** The validity of the digitally signed document can be verified using public key residing on the server by C# program.

Interfaces:

a) **Employees of the organization:** The employees of the organization can make use of the interface to digitally sign the documents (PDF, Excel, Word) and store the files in the server.
b) **IT Administration:** The IT administrators can view the documents which are being signed by the employees of the organization in the dashboard provided to them.

Technology Stack:

The technology stack which we use includes :

- PHP and Javascript for Client-Side Scripting.
- C# & ASP.NET for Server-side Scripting.
- HTML & CSS for Visually appealing Dashboard.

Use Cases:

Dependencies / Show Stopper:

- Visually appealing & user-friendly interface.
- Highly secure as we use SSL 256-bit encryption.
- Can be used across various platforms.
- Cross-browser support

Participants:

1. MERGU ANIRUDH SAI – anirudhsaim@gmail.com - +91 9515 39 5737
2. BUSIREDDY GREESHMA REDDY – greeshmareddy2697@gmail.com - +91 9441 43 0097
3. DEVULAPALLY MOURYA - mouryakashyap231297@gmail.com - +91 7416 69 4235
4. SHANTANU GUPTA – shantanu4644@gmail.com - +91 9553 15 9757
5. UPPU ANUDEEP – uppuanu53@gmail.com - +91 9705 75 0924
6. GAJANGI GANGA SRIPRIYA– sripriyagajangi2129@gmail.com - +91 9030 89 1892

CVR COLLEGE OF ENGINEERING, HYDERABAD

Mangalpally, Vastunagar, Ibrahimpatan, Ranga Reddy. Pin: 501510