1. **Chữ ký số**

var crypto=require("crypto");

//create key

const{publicKey,privateKey}=crypto.generateKeyPairSync('rsa',{

    modulusLength:2048,

    publicKeyEncoding:{

        type:'spki',

        format: 'der',

    },

    privateKeyEncoding:{

        type:'pkcs8',

        format: 'der',

    },

});

//sign

let prikey=crypto.createPrivateKey({

    key: Buffer.from(privateKey,"base64"),

    type:'pkcs8',

    format: 'der',

});

let sign=crypto.createSign("SHA256");

sign.update("some data");

sign.end();

let chuky=sign.sign(prikey).toString("base64");

console.log(chuky);

//verify

pubkey=crypto.createPublicKey({

    key: Buffer.from(publicKey,"base64"),

    type:'spki',

    format: 'der',

});

let verify=crypto.createVerify("SHA256");

verify.update("some data");

verify.end();

let kq=verify.verify(pubkey,Buffer.from(chuky,"base64"));

console.log(kq);

1. **Cài đặt ssl cho web**

1) Download openssl for windows

-- https://www.openssl.org/source/

-- https://wiki.openssl.org/index.php/Bi...

-- https://indy.fulgan.com/SSL/

2) Configure openssl it in your windows path

3) Create directory with .cfg file

4) Change config directory with open SSL

set OPENSSL\_CONF=C:\openssl\openssl.cfg

5) Generate CA - Certificate Authority - key and certificate (third-party)

openssl genrsa -out CA.key -des3 2048

openssl req -x509 -sha256 -new -nodes -days 3650 -key CA.key -out CA.pem

6) Generate certificate for your domain

- create file localhost.ext

- Generate a key: openssl genrsa -out localhost.key -des3 2048

- Generate a certificate request: openssl req -new -key localhost.key -out localhost.csr

- Generate certiticate: openssl x509 -req -in localhost.csr -CA CA.pem -CAkey CA.key -CAcreateserial -days 3650 -sha256 -extfile localhost.ext -out localhost.crt

7) Store decripted key: openssl rsa -in localhost.key -out localhost.decrypted.key

8) Install node modules for express and https: npm i express https

9) Run node program

const fs = require('fs');

const key = fs.readFileSync('localhost.decrypted.key');

const cert = fs.readFileSync('localhost.crt');

const express = require('express');

const app = express();

app.get('/', (req, res) => {

  res.send('Hello world! We are running under HTTPS! We are safe on WEB.');

});

const https = require('https');

const server = https.createServer({ key, cert }, app);

const port = 4430;

server.listen(port, () => {

  console.log(`Server is listening over HTTPs on https://localhost:${port}`);

});