SJSI

Research Article

Proposed Technique For Addressing The Ban On Nationally Generated Digital Certificates In Countries Under Technical And Information Blockade

Authors:
Hosam Ahmad
Bassel AlKhatib
Mohamad Mohamad

Affiliation:
The Syrian Virtual University – Syria – Damascus

Submitted
Accepted
Correspondence:
hosam_96643@svuonline.org

ABSTRACT

Due to the sanctions imposed on Syria on an ongoing basis, the most recent of which is the “Caesar Act,” which has affected Syria in general and in particular the information sector, and whose effects included the ban on the use of digital certificates (SSL Certificate); it has become impossible to use locally generated digital certificates granted by the National Authority for Information Technology Services in Syria, because browsers will not support the use of these certificates specific to this country. Syria has previously obtained, through the Ministry of Communications and Technology, in cooperation with a friendly country, the authority to issue national digital certificates and a national digital certificate generator. However, after the issuance of the “Caesar Act,” which stipulates in one of its paragraphs the imposition of information sanctions on Syria, the authentication of the Syrian digital certificate issuance authority has been prevented by international authentication authorities, including (VeriSign, Thawte, Geotrust, Comodo, Entrust, DigiCert, and others). Consequently, the authority to issue Syrian digital certificates becomes unreliable because international browsers will not accept their use except after obtaining electronic permission to certify their authenticity and reliability by international authentication authorities, and the latter will not grant acceptance due to sanctions. This research presents a proposed technique for addressing the aforementioned ban problem, by building an open-source web browser that does not depend on international authentication authorities to authenticate nationally generated digital certificates, but rather it breaks the connection with those international authentication authorities and ensures correct operation of using these national certificates.

Keywords: Chain of Trust, TrustStore, KeyStore.

INTRODUCTION

Banning nationally generated certificates that do not have approved global security certificates is a major and fundamental problem in countries that fall under the technical and information ban, such as Iran, Syria, etc., this matter is considered as a paralysis of development wheel in most fields because the aspects of life today have become dependent on electronic transactions, such as: banking sector, electronic transfers and linking them to electronic payment cards, electronic transaction systems, applications that transfer data with a certain degree of confidentiality, custom query systems, web control systems, web ordering systems, all transactions related to electronic government … and other many uses. The root certificate for the root certification authority is issued within a highly protected information environment or system and is used to issue digital certificates to individuals or companies. These certificates and their keys are stored and saved within its private system or environment, and thus the CA is the trusted third party to verify the authenticity of the certificates or signatures that are issued by them. By using the root certificate, verification can be performed, and this is known as the concept of a national certification authority. The National certification authority is considered the cornerstone of everything related to possible applications and projects, including digital transformation, provision of electronic government services (government and civil transactions), electronic payment methods, exchange, approval, authentication and protection of documents, electronic identity, electronic passport, online elections and their integrity, etc. All of these applications or projects depend on the presence of digital certificates signed by the certification authority that issues the digital certificates. Note that these applications or projects require high capabilities to issue digital certificates to all members of the public, as the policy has been adopted in most countries. The National Digital Certification Authority project has not been invested in the optimal way planned for several reasons, the most important of which are: The technological ban on our country, Syria, as the Syrian digital certificate issuing authority is not recognized internationally, and therefore it has not obtained a signature from the global digital certification authorities that are recognized by well-known international browsers. And the inability of well-known international browsers to run applications working on the webs that use nationally generated certificates due to their failure to recognize these certificates because well-known international authentication companies do not certify these national certificates, due to the imposition of technological sanctions on our country and also on many countries that are under the ban. From the above, the need to have a web browser that can verify the authenticity of these certificates in a safe and reliable manner (safety secure way) without the need for authentication from global authorities arose (Certification Authorities). In order to build a web browser that can verify the authenticity of national digital certificates, it requires cooperation between governments and technology companies. Indeed, an agreement had previously been reached between the Network Services Regulatory Authority and a company to build a national web browser, but the project was not completed. In general, it can be said that building a web browser that can verify the authenticity of national digital certificates is necessary to solve the ban problem imposing on certificates, and gives individuals and organizations confidence in using national digital certificates for many purposes. As technology develops and more security technologies become available, this type of browser can be improved and developed to ensure that data security is maintained and authentication is confirmed in a safe and reliable manner, which is an important step in developing and improving the digital infrastructure of countries and individuals, and can help achieve the global goal of maintaining digital security and achieving digital integration between countries, institutions and individuals.

MATERIALS AND METHODS

First, we conducted analytical studies based on field visits to the Ministry of Communications and Technology, the National Authority for Information Technology Services, the government sector, and the private sector to understand the existing problem and discuss it with stakeholders. We also depended on reference studies through books and the Internet about the use of the /SSL, TLS/ protocol in browsers and how this is done through the national digital certificate issuance authority. We followed an inductive research methodology to collect and analyze information, as well as using programming and practical experience to design and develop the national browser. We have depended on a set of programming tools for programming development, which are: Programming by java in Intellij IDE - Programming by java netbeans IDE In addition to a virtual operating system environment on the server VMware Esxi7 (platform virtualization software) Which contains: linuxubuntu server 22.04 operating system. The system for generating digital certificates (Openxpki) wasinstalled, prepared and authenticated, the Windows Server 2022 operating system, where the Wireshark network monitoring tool was installed on it. In order to test the browser's operation, we used a set of tools: Openxpki which is an open-source tool used globally to generate certificates of all kinds, as it is installed on the Apache web server within the Linux server operating system. A website on which a generated and nationally signed certificate is installed, and Wireshark, a tool used to monitor all network details, including data. The purpose of using it was to indicate whether the connection was successful and the data was encrypted through the https protocol when using national certificates, in addition to national certificates generated and signed by the National Authority for Information Technology Services.

RESULTS

Through this research, we found a solution to the ban problem by creating an open-source software application (web browser), as this browser allows the use of digital certificates approved by the National Authority for Information Technology Services. Other tasks can be added to the browser related to privacy and protection (for example, software code can be added to the browser so that it is linked with a specific web application in order to perform a specific task that may be related to privacy, Property protection, or preventing the use of the application except through this version of the browser...).

DISCUSSION

In this paragraph, we will discuss our findings and how to verify and test them.

Description of the X.509 standard:

The X.509 standard consists of a set of rules and instructions that determine the method of issuing digital certificates and authenticating digital identity. The X.509 standard is considered the approved reference within the National Digital Certification Authority in Syria. The standard includes detailed information about the entity issuing the certificate and the entity in which the certificate was used, including digital identity information and the keys used in digital signature and encryption. The certifications that depend on X.509 standard are used to authenticate the identity of users, devices, and organizations, by including the digital identity information of the entity issuing the certificate. In general, the X.509 standard forms an important basis for maintaining digital security and authenticating digital identity, as it is used in many different security applications and can be used in many industries and sectors including e-government, e-commerce, banking services, and others. This standard was chosen in our research based on the reference study [1] which confirmed that this standard is used in the majority of global browsers. It analyzed the structure of this standard and how to benefit from it to ensure the identity of servers and the confidentiality of data exchange. The structure of the X.509 standard is illustrated in Figure (3).

Solve the problem by building a national web browser:

A browser was built in the Java programming language that can browse websites using the HTTPS protocol [5]. The browser interfaces were created that resemble the interfaces of well-known international browsers, in addition to building a private trusted certificate store (TrustStore [4]), where trusted certificates are supplied to it through two methods:

A.Importing trusted certificates that exist in the operating system's trust store.

B.Importing private trusted certificates, and in our case here it is the /Root certificate/, the national root certificate for the Syrian Arab Republic, which was obtained from the Ministry of Communications and Technology - the National Authority for Information Technology Services.

Then we tested the readiness of the trusted certificate store. After that, it was adopted as the default store of the national browser instead of the trust store of the operating system. The certificates included in the Trust Store, including the approved nationally generated certificates, can be viewed in Figure (2).

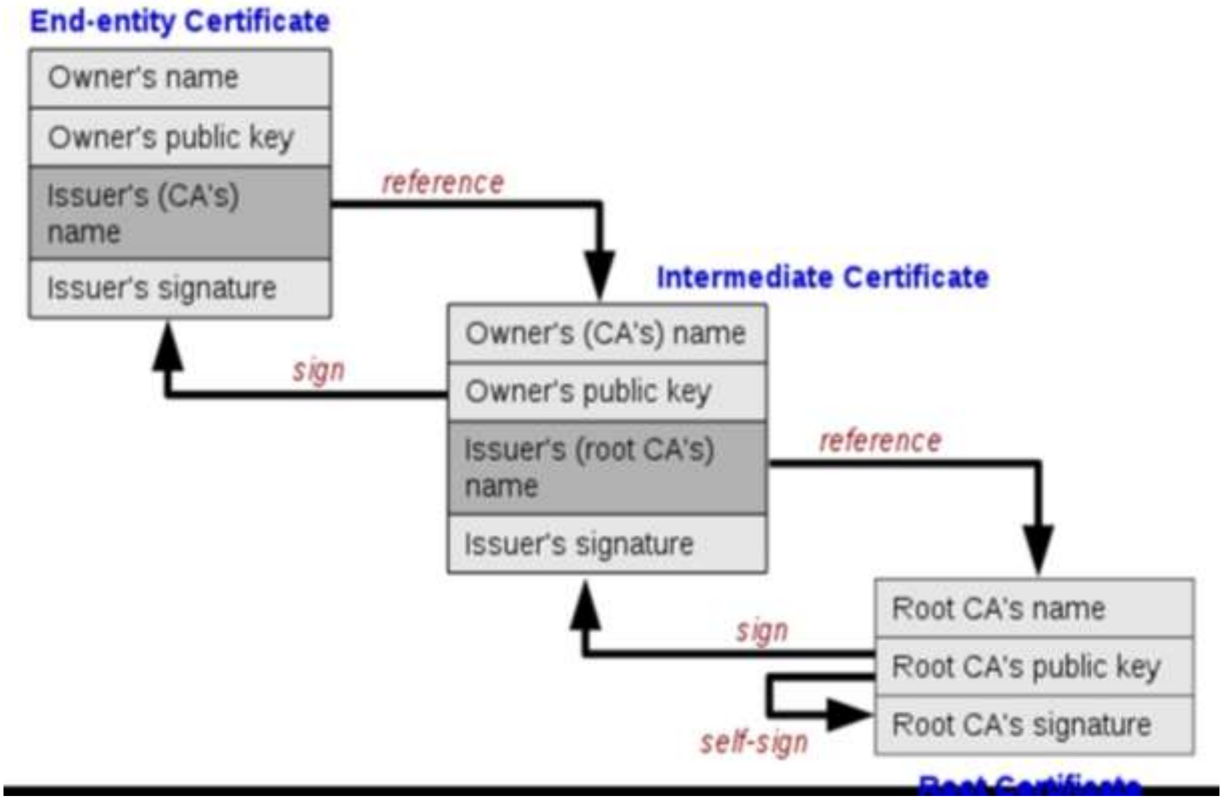
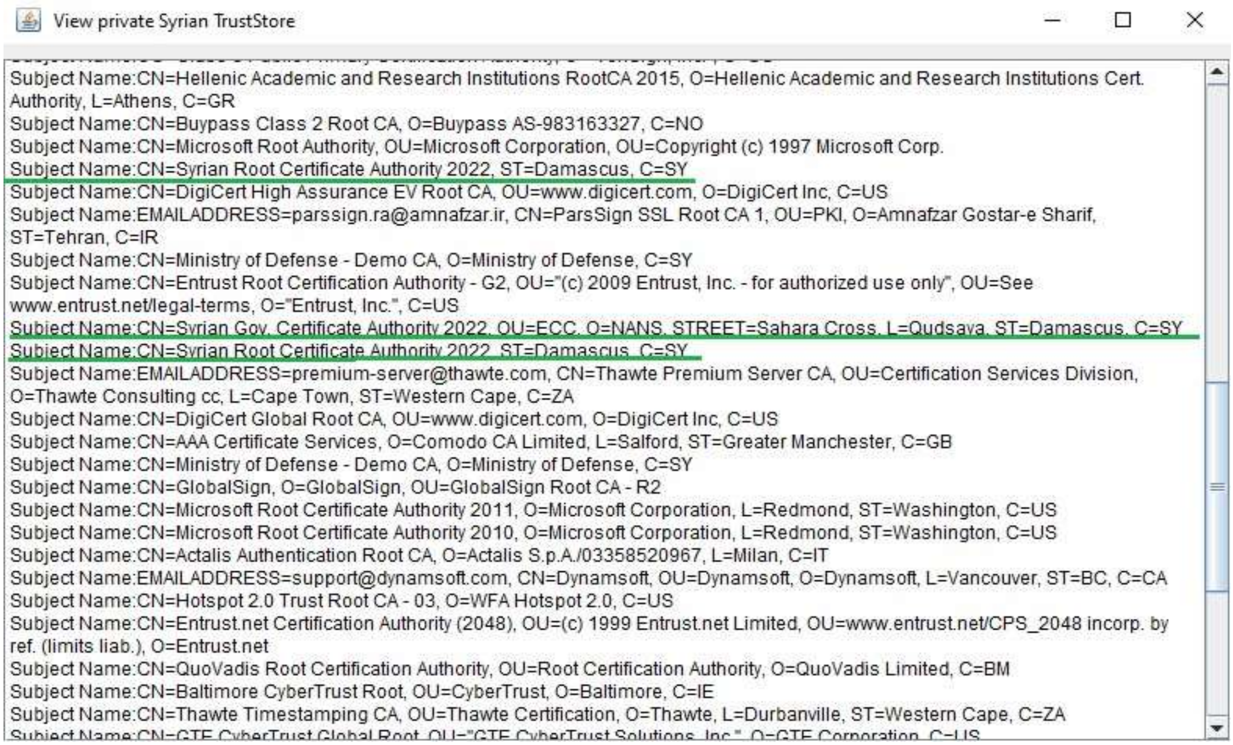


Fig.(1) **Chain of Trust**



```
Subject Name:CN=Hellenic Academic and Research Institutions RootCA 2015, O=Hellenic Academic and Research Institutions Cert.
Authority, L=Athens, C=GR
Subject Name:CN=Buypass Class 2 Root CA, O=Buypass AS-983163327, C=NO
Subject Name:CN=Microsoft Root Authority, OU=Microsoft Corporation, OU=Copyright (c) 1997 Microsoft Corp.
Subject Name:CN=Syrian Root Certificate Authority 2022, ST=Damascus, C=SY
Subject Name:CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
Subject Name:EMAILADDRESS=parssign.ra@amnafzar.ir, CN=ParsSign SSL Root CA 1, OU=PKI, O=Amnafzar Gostar-e Sharif,
ST=Tehran, C=IR
Subject Name:CN=Ministry of Defense - Demo CA, O=Ministry of Defense, C=SY
Subject Name:CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See
www.entrust.net/legal-terms, O="Entrust, Inc.", C=US
Subject Name:CN=Syrian Gov. Certificate Authority 2022, OU=ECC, O=NANS, STREET=Sahara Cross, L=Qudsaya, ST=Damascus, C=SY
Subject Name:CN=Syrian Root Certificate Authority 2022, ST=Damascus, C=SY
Subject Name:EMAILADDRESS=premium-server@thawte.com, CN=Thawte Premium Server CA, OU=Certification Services Division,
O=Thawte Consulting cc, L=Cape Town, ST=Western Cape, C=ZA
Subject Name:CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
Subject Name:CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB
Subject Name:CN=Ministry of Defense - Demo CA, O=Ministry of Defense, C=SY
Subject Name:CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2
Subject Name:CN=Microsoft Root Certificate Authority 2011, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US
Subject Name:CN=Microsoft Root Certificate Authority 2010, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US
Subject Name:CN=Actalis Authentication Root CA, O=Actalis S.p.A./03358520967, L=Milan, C=IT
Subject Name:EMAILADDRESS=support@dynamsoft.com, CN=Dynamsoft, OU=Dynamsoft, O=Dynamsoft, L=Vancouver, ST=BC, C=CA
Subject Name:CN=Hotspot 2.0 Trust Root CA - 03, O=WFA Hotspot 2.0, C=US
Subject Name:CN=Entrust.net Certification Authority (2048), OU=(c) 1999 Entrust.net Limited, OU=www.entrust.net/CPS_2048 incorp. by
ref. (limits liab.), O=Entrust.net
Subject Name:CN=QuoVadis Root Certification Authority, OU=Root Certification Authority, O=QuoVadis Limited, C=BM
Subject Name:CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE
Subject Name:CN=Thawte Timestamping CA, OU=Thawte Certification, O=Thawte, L=Durbanville, ST=Western Cape, C=ZA
Subject Name:CN=GTE CyberTrust Global Root, OU="GTE CyberTrust Solutions, Inc.", O=GTE Corporation, C=US
```

Fig.(2) **Nationally generated (trusted) certificates that are added to the generated browser's trust store**

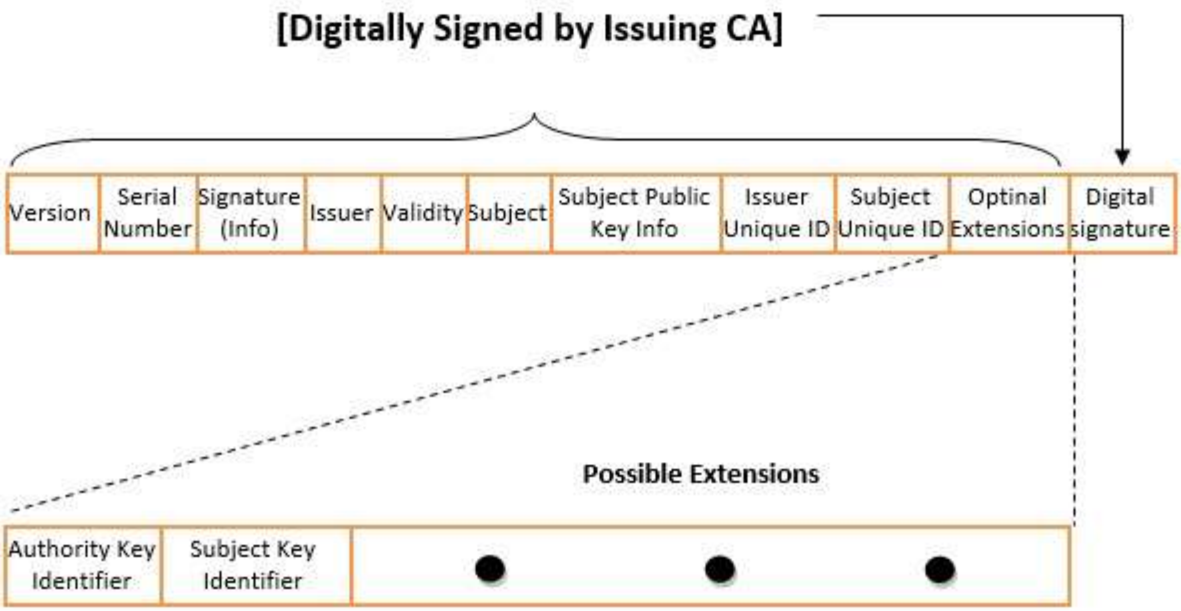


Fig.(3) **Structure of the X.509 standard [researchgate.net]**

How the browser verifies the validity and reliability of the certificate:

When you browse a secure site (sites that start with the prefix "https://") instead of "http://"), the browser uses a security protocol called SSL/TLS (Secure Sockets Layer/Transport Layer Security) to secure the connection between the browser and the server [10]. An SSL/TLS certificate is used to authenticate the server's identity and encrypt the data that is exchanged between the browser and the server. To verify the validity of the certificate, the browser checks the existence of the certificate and whether it was sent by the server. The browser then verifies that the certificate has been signed by a trusted certificate authority (CA) located within the TrustStore [4] that the browser uses, and that the server’s name included in the certificate matches the server’s name in the URL being browsed. Then the browser determines the server’s address of the Online Certificate Status Protocol (OCSP) and the Certificate Revocation List (CRL) server’s address in the digital certificate file that is signed by the certificate issuing institution [10]. The validity of the certificate is checked for revocation or expiration in one of the following two ways:

A.Through the OCSP protocol, this method includes the following steps:

1. The browser connects to the OCSP server through the URL included in the certificate.

2.The browser sends a request that includes the information of certificate that is needed to be verified, such as the certificate ID number, issuer name, etc.

The OCSP server responds to the request after verifying the validity of the certificate. If the certificate is valid, a positive response is returned confirming its validity, and if it is invalid, a negative response is returned indicating its invalidity. As shown in Figure (4):

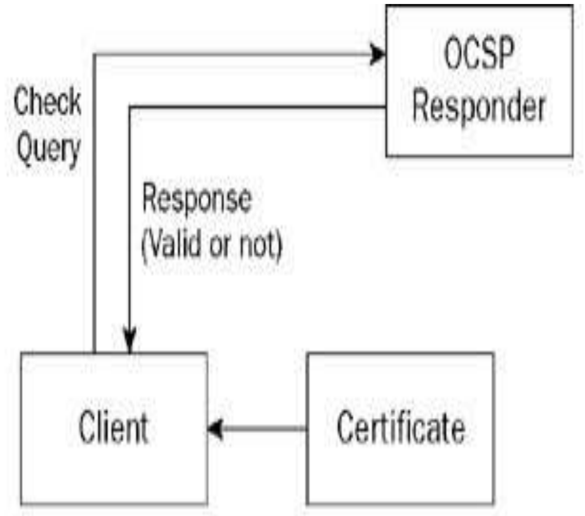


Fig.(4) **Verify the certificate through OCSP protocol [10].**

***B. By using Certificate Revocation List (CRL), this method includes the following steps*:**

1. The browser connects to the CRL server through the URL included in the certificate.

2. A list of withdrawn and revoked certificates is loaded.

3. Within this list, a research is done to check whether the certificate is revoked or not, using the certificate's ID number.

4. Verify that the certificate has not expired. As shown in Figure (5):

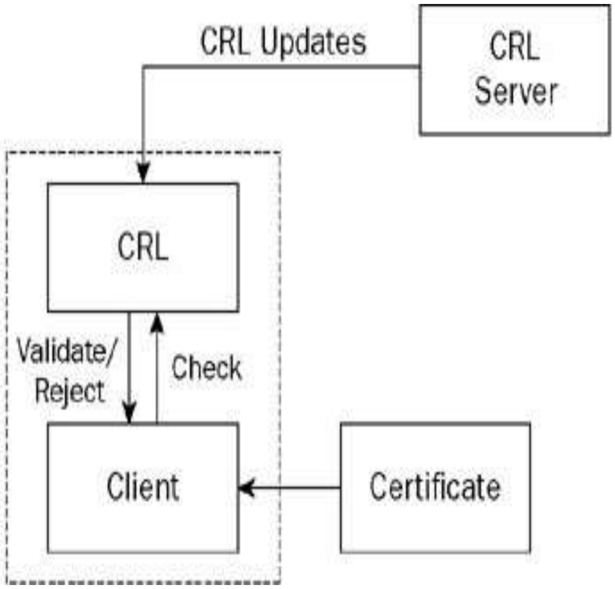


Fig.(5) **Verify the certificate through CRL [10].**

OCSP protocol differs from CRL protocol in the following way:

1.OCSP is used to instantly verify the validity of certificates, while CRL requires uploading a complete list of revoked and withdrawn certificates.

2.CRL contains a list of all revoked and withdrawn certificates, while OCSP is used to verify the validity of a specific certificate only.

3.The CRL is updated periodically, while the OCSP is used to verify the validity of the certificate in real time.

Comparison between the concepts of Keystore and Truststore [4]:

• ***Truststore concep****t*: All systems that use digital certificates have a default list contains a private certificates of the approved authorities called trusted Root certificates, the place where these trusted certificates are stored is called the truststore.

• ***KeyStore concept*****:** It is a file that contains the private keys and the digital certificates used in encryption and authentication processes. Keystore is used to store private keys that are used to sign or encrypt messages or to authenticate communications. Table (1) shows a comparison between each of the previous two concepts.

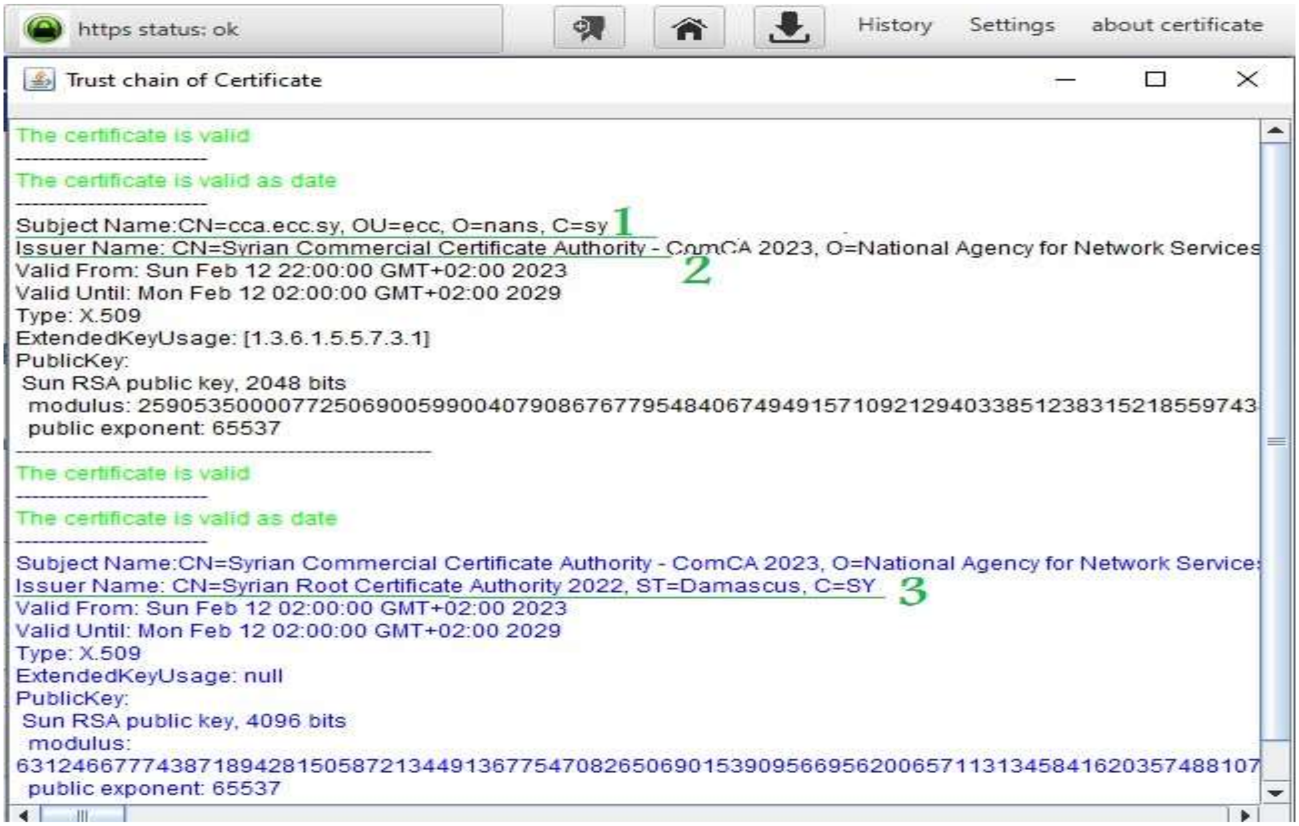
Table (1): Comparison between Truststore and KeyStore

		Keystore	**Truststore**
1	**The purpose:**	It is used on the server side to store the private key and the private identity certificate for the Verification process and is used only when the server operates in SSL mode.	It is used on the client side (browser) to store trusted certificates granted by /CA/, and this storage is used to verify the certificate provided by the server when using an SSL connection.
2	**In the SSL handshake phase:**	Keystore's job is to provide credentials information.	Truststore's job is to verify credentials information.
3	**The Library used in Java**	Use Key manager library	Use Trustmanager library
4	**Define path in Java**	Djavax.net.ssl.keystore	Djava.net.ssl.truststore
5	**Get password**	Djavax.net.ssl.keystore password	Djavax.net.ssl.truststore password
6	**Contain the host's private key:**	It contains one private key for the host.	It does not contain any private keys.
7	**Create and remove a list of certificates**	This can be done through the Keytool tool.	This can be done through the Keytool tool.
8	**Accessibility:**	It can only be accessed by those who have the right to manage the Host.	Almost all SSL clients have access to the Truststore.

How to test whether the browser is working properly:

In cooperation with the Digital Certification Center of the National Authority for Information Technology Services within the Ministry of Communications and Technology, an experimental website was developed (https://tools.ecc.sy) on the Internet, embedded with a generated and nationally certified certificate, and its operation was tested on three well-known browsers (MicrosoftEdge ،Google Chrome ،Mozilla firefox), These browsers were unable to run it due to the existence of the Syrian certificate, which is not trusted by them due to sanctions.

The website was tested using the browser that was built and it worked. After running the experimental site on the national browser, the connection was tested if it is secure (encrypted) using the programming code which is custom of testing Https connection. In addition to testing the reliability of the certificate through the browser's trust store, note that the success of the secure connection is shown by the appearance of a closed lock symbol and writing (Https status: ok) next to the address field within the browser. You can view the certificate for the experimental site described in paragraph 1 above and view the certifying parties (certificate authorities) for this certificate (chain of trust), in Figure (6).



```
The certificate is valid
------------------------
The certificate is valid as date
------------------------
Subject Name:CN=cca.ecc.sy, OU=ecc, O=nans, C=sy
Issuer Name: CN=Syrian Commercial Certificate Authority - ComCA 2023, O=National Agency for Network Services
Valid From: Sun Feb 12 22:00:00 GMT+02:00 2023
Valid Until: Mon Feb 12 02:00:00 GMT+02:00 2029
Type: X.509
ExtendedKeyUsage: [1.3.6.1.5.5.7.3.1]
PublicKey:
 Sun RSA public key, 2048 bits
  modulus: 25905350000772506900599004079086767795484067494915710921294033851238315218559743
  public exponent: 65537
--------------------------------------------------
The certificate is valid
------------------------
The certificate is valid as date
------------------------
Subject Name:CN=Syrian Commercial Certificate Authority - ComCA 2023, O=National Agency for Network Service
Issuer Name: CN=Syrian Root Certificate Authority 2022, ST=Damascus, C=SY
Valid From: Sun Feb 12 02:00:00 GMT+02:00 2023
Valid Until: Mon Feb 12 02:00:00 GMT+02:00 2029
Type: X.509
ExtendedKeyUsage: null
PublicKey:
 Sun RSA public key, 4096 bits
  modulus:
63124667774387189428150587213449136775470826506901539095669562006571131345841620357488107
  public exponent: 65537
```

Fig.(6) **A series of certificates (chain of trust), starting from the certificate for the experimental site, all the way to the national Syrian root certificate**

The previous figure shows that issuer name shown by the number (3) has certified the issuer name shown by the number (2), which in turn has certified the certificate for the experimental site on the Internet shown in number (1). The issuer name (certification authority) shown in the number (1) represents the national Syrian root certificate and is embedded in the browser's trust store.

Accordingly, the experimental site's certificate was trusted and approved within the HTTPS protocol. When running a site that does not have a certificate or uses the /http/ protocol, the browser will show that. The success of the TLS protocol was monitored through the Wireshark application, which eavesdrops on the entire network. Also monitor data movement (exchanged in encrypted form) across the network through the Wireshark application.

CONCLUSIONS

By the end of the research, the first Syrian national web browser was completed that includes a trusted certificate store that ensures the operation of the https protocol, and offers a set of solutions to the existing problems due to the international technological ban on our country, Syria, and other countries, which prevents us at Syria from using the Internet or the Intranet in the field of reliable electronic dealing in all sectors on government websites which have the SY extension. This Syrian national web browser allows the use of digital certificates approved, generated and signed by the National Authority for Information Technology Services, which are not trusted internationally due to sanctions. Our web browser is a secure, open-source and it can be portable application that does not require installation [2]. Finally, this browser is useful to All entities in the public and private sectors that need to use digital authentication or need protection and reliability in the operation of their applications. In the first place, it will serve the Ministry of Communications and Technology, the National Authority for Information Technology Services in Syria, which presented the National Digital Authentication Project that faltered due to the international browsers not supporting Syrian digital certificates.

FUTURE WORKS

After achieving the desired objectives of the research, which we have mentioned in the context of this article, we can identify a set of recommendations such as: adding tasks related to privacy and protection to the browser, for example adding a digital signature and adding programming code that links the browser to an application for preventing the use of that application except through this version of the browser. The browser can be used as a secure means of communication by adding programming codes that enable communication and the exchange of files and messages. Finally many features can be added and customized when needed for example, adding monitoring features for monitor all types of sites and adding Advanced security and privacy features.

REFERENCES

1. **Berbecaru D, Lioy A. An Evaluation of X.509 Certificate Revocation and Related Privacy Issues in the Web PKI Ecosystem.IEEE. 27 July 2023; Volume:11: 79156 – 79175.**
2. **MarringtonA, Baggili I, Al Ismail T, AlKaf A. Portable web browser forensics: A forensic examination of the privacy benefits of portable web browsers. IEEE. 07 February 2013.**
3. **Pletinckx S, Nguyen T, Fiebig T, Kruegel C, Vigna G. Certifiably Vulnerable: Using Certificate Transparency Logs for Target Reconnaissance. IEEE. 31 July 2023.**
4. **Tijms A, Keil W, Bais T. Jakarta EE Implementations. Apress. 14 April 2022; 413–474.**
5. **Wang C, Lin J, Li B, Li Q, Wang Q, Zhang X. Analyzing the Browser Security Warnings on HTTPS Errors. IEEE. 15 July 2019.**
6. **Park J, Shin D, Shin D, Lee J, Lee H. Design and Implementation of Web Browser Secure Storage for Web Standard Authentication Based on FIDO. SoICT '19. 04 December 2019; 229–235**
7. **Laperdrix P, Rudametkin W, Baudry B. Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints. IEEE. 18 August 2016.**
8. **Leo C. Singleton, IVJuanRiveraJitendraDeshpandeSridharMullapudi. Redirector for secure web browsing. Citrix Systems Inc. 14 Aug. 2018**
9. **Levi S, Racke-Bodha S, Downey J, Hiltch O. METHOD FOR REGULATING USAGE OF A BROWSER STORE FOR A WEB BROWSER FEATURING TABBED WEB PAGE VIEWING BASED ON BROWSER ACTIVITY. Avast Software s.r.o., praha (CZ). 10 Jul 2018.**
10. **Berkowsky J, Hayajneh T. Security issues with certificate authorities. IEEE. 08 January 2018**

Funding: No Fund

Author Contributions: Supervision: Bassel AlKhatib - Mohamad Ali Mohamad. Writing– original draft: Hosam Kamal Ahmad. Writing – review & editing**:** Bassel AlKhatib, Mohamad Ali Mohamad.

Competing interests: The Authors declare that they have no competing interests.

Data and materials availability: All data are available in the main text.