USARelativity and USASync Request Form

USAO POC:

- All boxes highlighted in RED are required for Federal Employees. All State and Local, or non-federal employees who do not possess a federal background investigation (BI) as part of a task force must provide Full Name, Date of Birth and Social Security Number for an NCIC record check to waive the federal BI requirement.
- Pages 2 through 5 are the Rules of Behavior for the U.S. Attorney's and USASync
- Pages 6 through 12 are instructions to export your PIV/CAC .p7b certificate

First Name:

Middle Name: (Enter NMN if no middle name) No initials, need full middle name

Last Name:

Email:

Phone Number: ● Desk ○ Cell

Access Request: ☑ USARelativity

☑ USASync

SSN:

Birth Date:

Agency:

Agency holding Investigation Record *

Background Investigation Type * Tier 1 (NAC)

Completion Date:

Adjudication Date:

Reciprocity Date:

Rejection Date:

* Check with your local security manager or HR staff. They will be able to help with any information you don't know.

UNITED STATES ATTORNEYS'
INFORMATION SYSTEMS RULES OF BEHAVIOR

Access to United States Attorney information systems, and the sensitive law enforcement and other official information they contain, is governed by USAP 3-16.200.003, Network Account Security Management, which requires all users to read and sign these Rules of Behavior (RoB) prior to access. To ensure that all users are aware of periodic RoB revisions, annual recertification will be part of each year's Computer Security Awareness Training.

A. Classification Usage

1. These rules apply to United States Attorneys' information systems used for storing, processing, and transmitting information designated **LIMITED OFFICIAL USE.** Such systems **must not** be used to store, process, or transmit information that has been identified as Top Secret, Secret, or Confidential in accordance with Executive Order 13526, "Classified National Security Information" (December 9, 2009).

B. User ID and Password Management

1. Do not disclose your unique User ID or password under any conditions. You are individually responsible and accountable for protecting your unique User ID and password.
2. Do not write passwords in any form, either electronically (e.g., login scripts) or hardcopy.
3. Do not share your User ID and password. They are individual credentials that are used to establish a single session that is solely under your control and for which you are accountable.
4. Do not establish a session under your ID and password for another user.
5. Once your account has been successfully initialized using an administrator-provided password, immediately change the password.
6. If your password has been compromised, or is suspected of being compromised, change it immediately and report the incident to your Systems Manager and District Officer Security Manager.

C. Computer Hardware

1. Protect Government-owned computer hardware from incidents such as damage, theft, abuse, loss, and unauthorized use, and report any such incidents or suspected incidents to the District Officer Security Manager and Systems Manager.
2. Obtain a property pass if computer hardware has to be removed from USAO or EOUSA premises, except for permanently assigned laptops, portable hard drives, smartphones, and other Government-furnished devices (e.g., iPads).
3. Computer hardware shall not be removed from USAO or EOUSA premises for unofficial purposes.
4. Do not use computer hardware for which you have not been specifically authorized.
5. Hardware maintenance or configuration changes shall only be performed by authorized personnel.
6. Do not connect or use any unauthorized devices with Government-owned computer hardware.

7. Government-owned computer hardware must be handled as carry-on luggage when using airlines, trains or any other common carriers. Do not check in Government-owned computer hardware on any common carriers.
8. Do not leave Government-owned computer hardware unattended in vehicles or in locations that are susceptible to theft. Store Government-owned computer hardware that is not in use in a secure location.
9. Loss or theft of a DOJ laptop, smartphone, removable media (e.g., "thumb" drives), and other Government-furnished devices shall be reported immediately to the District Officer Security Manager and EOUSA Assistant Director for Information Systems Security.

D. Reporting of Security Breaches

1. Report any actual or suspected security violations, incidents, vandalism or vulnerabilities to the District Officer Security Manager and Systems Manager.

E. Work at Home and Other Remote Users

1. Personally-owned (non-governmental) hardware and software may not be used for work purposes, except that users of Government-furnished remote access devices (e.g., RSA Tokens and https://usaremote.justice.gov) may use non-governmental Internet connections to establish remote connections.
2. All of the on-site safeguards for handling SBU information apply to off-site work.
3. Remote access may not be used for purposes other than official business.

F. Computer Software

1. Software Copyright Laws and Licensing Agreements must be honored both for computer programs and documentation.
2. End-users shall not install software on Government-owned computer systems. For ad-hoc software needs, contact your Systems Manager.

G. Property

1. An employee has a duty to protect and conserve Government property and shall not use such property, or allow its use, for other than authorized purposes (5 C.F.R. §2635.704). Government property includes, but is not limited to, DOJ-issued hardware and software.
2. Do not use Government property for personal commercial gain or to promote personal causes or in an attempt to influence legislation or elections.

H. Communications and Usage

1. Do not transmit SBU or other sensitive information, or copyrighted documents over the Internet unless encrypted.
2. Do not send or auto-forward electronic mail over the Internet unless encrypted.
3. Do not utilize nongovernmental Voice-Over-IP websites (e.g., Skype).
4. Abide by the Standards of Ethical Conduct for Employees of the Executive Branch.
5. Political activity, commercial activity (e.g., conducting a business), unlawful activity, and inappropriate conduct are prohibited.
6. Any personal use must be on personal time, have a negligible cost to the government, and be of reasonable duration.

7. Obtaining, viewing, or transmitting sexually-explicit material is prohibited except for official law enforcement purposes.
8. Do not forward chain letters, jokes, or other inappropriate content.

I. Confidentiality

1. Do not use or attempt to access data for which you have not been authorized.
2. Information that you are authorized to retrieve from information systems is for your use only, and not to be shared.
3. Ensure that sensitive information sent to a fax or printer is handled securely and labeled appropriately (e.g., use a fax cover sheet that indicates the classification and sensitivity of the information, contact information for recipient and sender, and instructions to the recipient if the information is received in error).

J. Integrity

1. Do not introduce unauthorized, inaccurate or false information into information systems.
2. Do not use system privileges to misuse or exploit information in information systems.
3. Do not alter files improperly. If files appear to be altered improperly or are missing, notify your Systems Manager and District Officer Security Manager.

K. Availability

1. Do not eat, drink, smoke, or store combustible materials near a computer or electronic media.
2. In the event of a crash or system outage, check that critical files are available and have not been altered. If files are missing or appear to be altered, notify your Systems Manager and District Officer Security Manager.

L. Hardware and Software Support

1. Do not attempt to perform hardware or software support activities. Contact your Systems Manager and use District procedures for hardware and software support.

M. Additional Provisions for Privileged Users

1. Use non-privileged accounts by default. **Use your privileged accounts only in the performance of official duties and only as necessary to complete assigned tasks.**
2. Do not make unauthorized changes to systems.
3. Do not deploy patches, updates, or upgrades except as authorized via Technical Bulletin or Security Bulletin. Do execute bulletins in accordance with deadlines.
4. Browsing the web, accessing email, or accessing any other Internet resource with a privileged account is prohibited.

I acknowledge that I have read the above Rules of Behavior and understand my responsibilities and agree to comply with the Rules delineated herein. I acknowledge that any violation of these Rules may be cause for disciplinary actions.

Signature: ____________________________________ Date: _____________

Printed Name: ____________________________________

USASYNC RULES OF BEHAVIOR & TERMS OF SERVICE

USAsync is a United States Department of Justice system designed to enable the Department of Justice to better collaborate with authorized, non-adverse members of a federal case team.

Access to USAsync is restricted to authorized users. All authorized users must be sponsored by an authorized Department of Justice employee. No one may access the USAsync system without first accepting these Rules of Behavior and Terms of Service, which supplement and do not supersede any/all other applicable laws, regulations, and policies governing the use of official Government systems such as this.

System Access and Security: Only authorized users may access and use USAsync. You are individually responsible and accountable for protecting your user credentials. Do not disclose or share your user credentials under any conditions. They are individual credentials that are used to establish a single session that is solely under your control and for which you are accountable. Do not establish a session under your user credentials for another user. If your user credentials have been compromised, or are suspected of being compromised, report the incident to the Department of Justice employee who sponsored your access immediately. No one may access, or attempt to access, areas of USAsync not approved for the user. Access to, and use of, USAsync is subject to audit logging for intrusion/malware detection and security/compliance purposes.

Classification Usage: USAsync is to be used to store, process, and/or transmit information designated LIMITED OFFICIAL USE. USAsync must **not** be used to store, process, or transmit information that has been identified as Top Secret, Secret, or Confidential in accordance with Executive Order 13526, "Classified National Security Information" (December 9, 2009).

Data Privacy: Some data in USAsync may be subject to statutory, regulatory, or court-imposed privacy and/or data-handling conditions, such as protective orders, stipulations, grand jury secrecy rules, and the like. By using USAsync, you agree to protect the privacy of such data and limit its further dissemination in accordance with law.

By accepting these USAsync Rules of Behavior and Terms of Service, you acknowledge that:

- You have read and understand the foregoing terms and conditions of the USAsync system;

- You consent to, and will comply with, these Rules of Behavior and Terms of Service freely and voluntarily;

- Any violation of these USAsync Rules of Behavior and Terms of Service may be cause for revocation of USAsync access; and

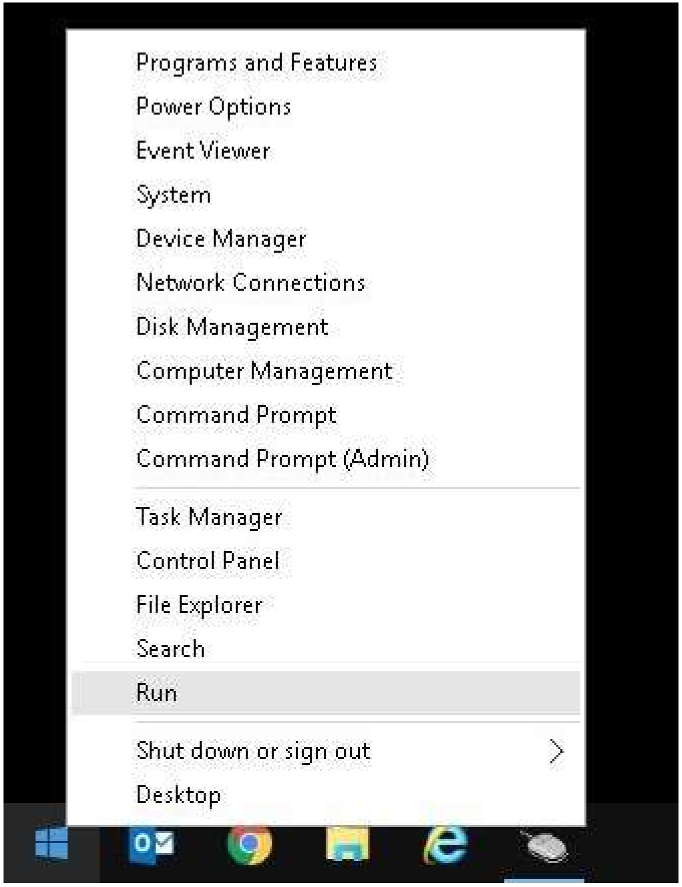
- Misuse of the USAsync system may result in disciplinary action, civil penalties, and/or criminal prosecution.

By signing below, you acknowledge that you have read and consent to the foregoing USAsync Rules of Behavior and Terms of Service.

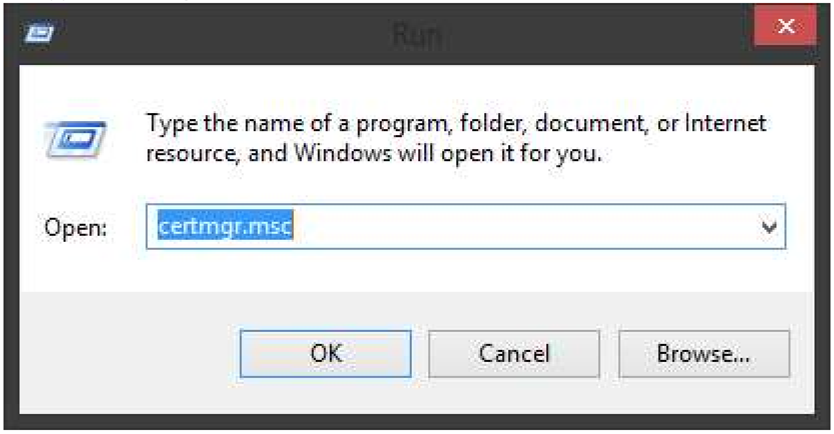
Signed: ___________________________________ Date:_______________________________

Certificate Export Process

1. Use the Right mouse button to click on their Start button, and select Run from the pop-up menu.



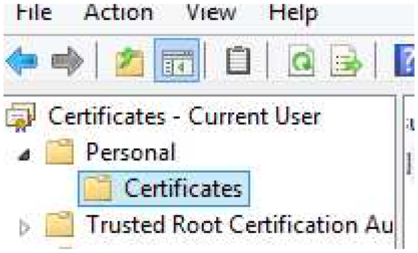
2. Type “certmgr.msc” in the text box and click “Run”



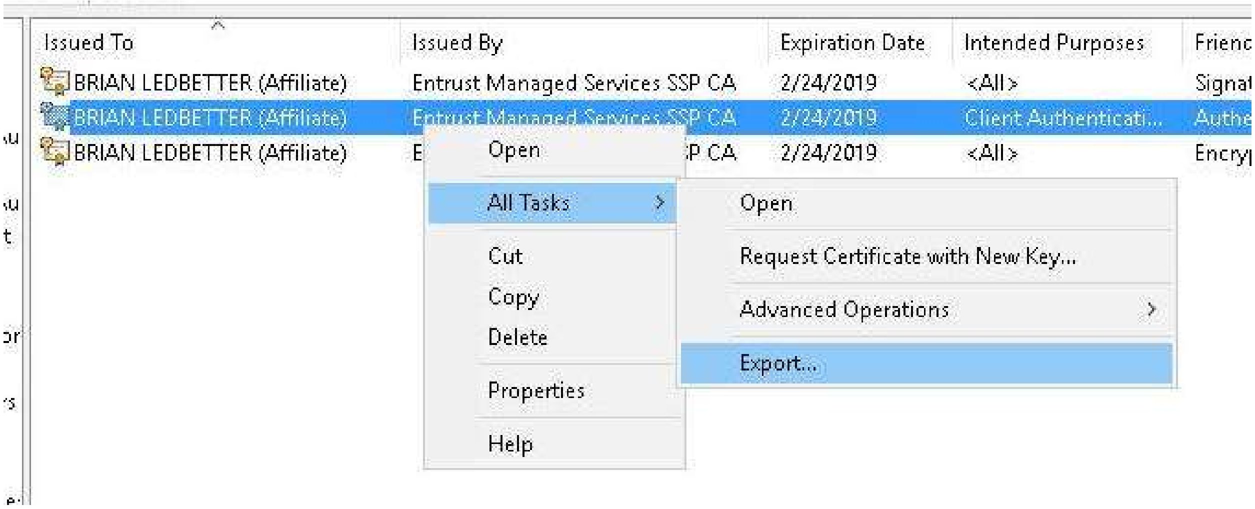
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: certmgr.msc

3. In the left hand side of the Certificate Manager window, browse to Personal > Certificates.

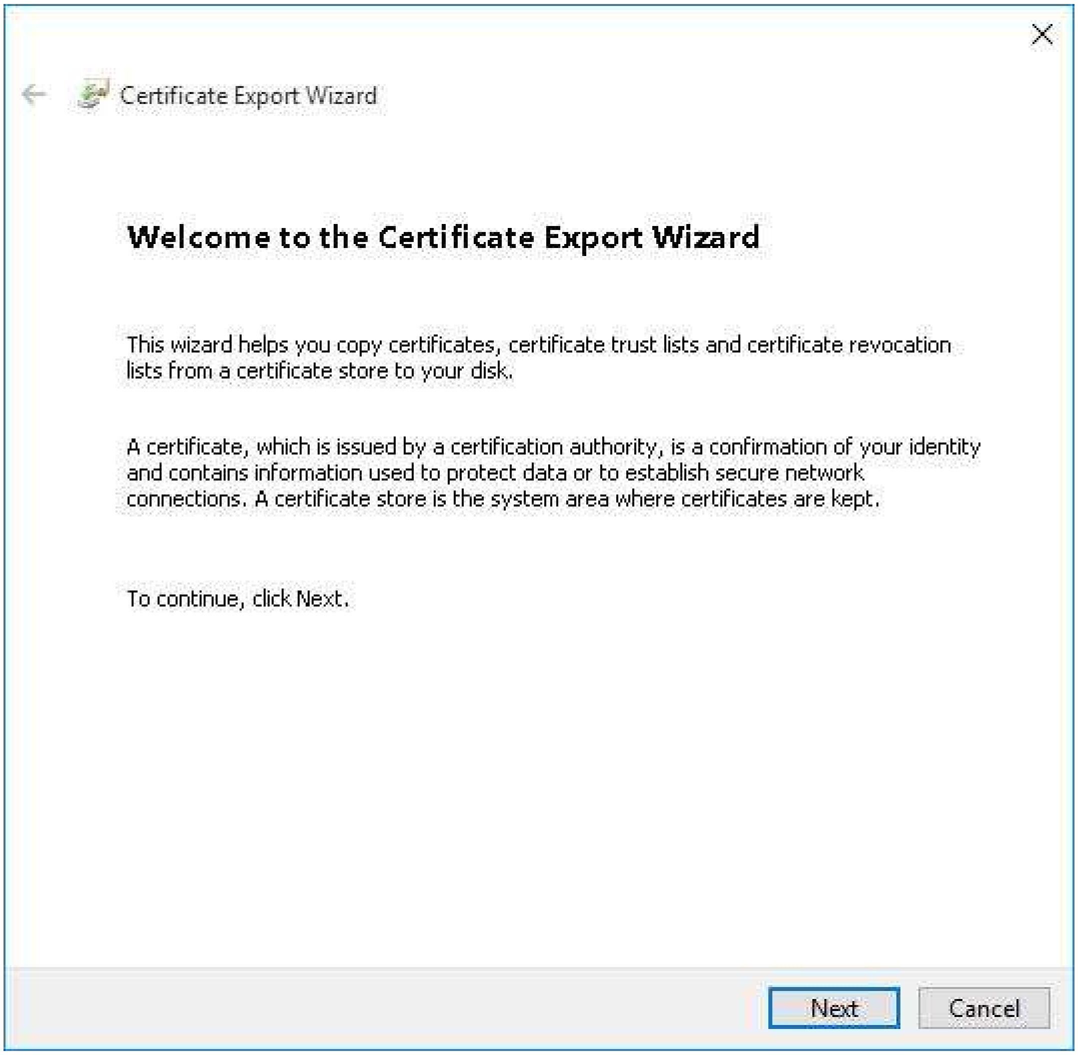


4. Right-click on one of the certificates that are listed here that has the user’s name in it. From the popup menu, select All Tasks > Export to start Certificate Export Wizard. (The “Intended Purposes” field should read “Client Authentication.”)



Issued To	Issued By	Expiration Date	Intended Purposes	Frienc
BRIAN LEDBETTER (Affiliate)	Entrust Managed Services SSP CA	2/24/2019	<All>	Signat
BRIAN LEDBETTER (Affiliate)	Entrust Managed Services SSP CA	2/24/2019	Client Authenticati...	Authe
BRIAN LEDBETTER (Affiliate)	E P CA	2/24/2019	<All>	Encry

5. Walk through the wizard steps. Importantly, select “No, do not export the private key” (if presented the option), and for the format select both “xxx” and “Include all certificates in the path.”

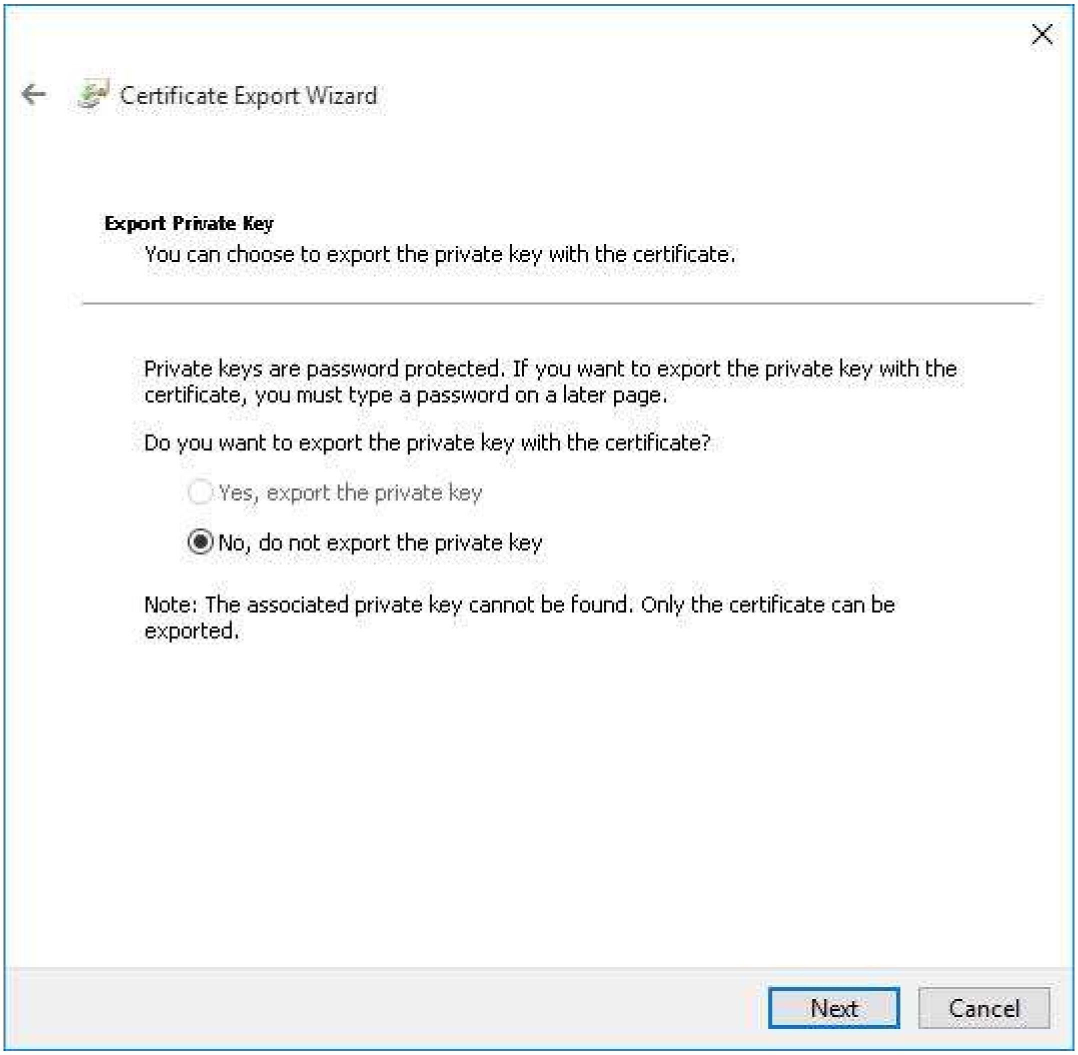


Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.



Export Private Key

You can choose to export the private key with the certificate.

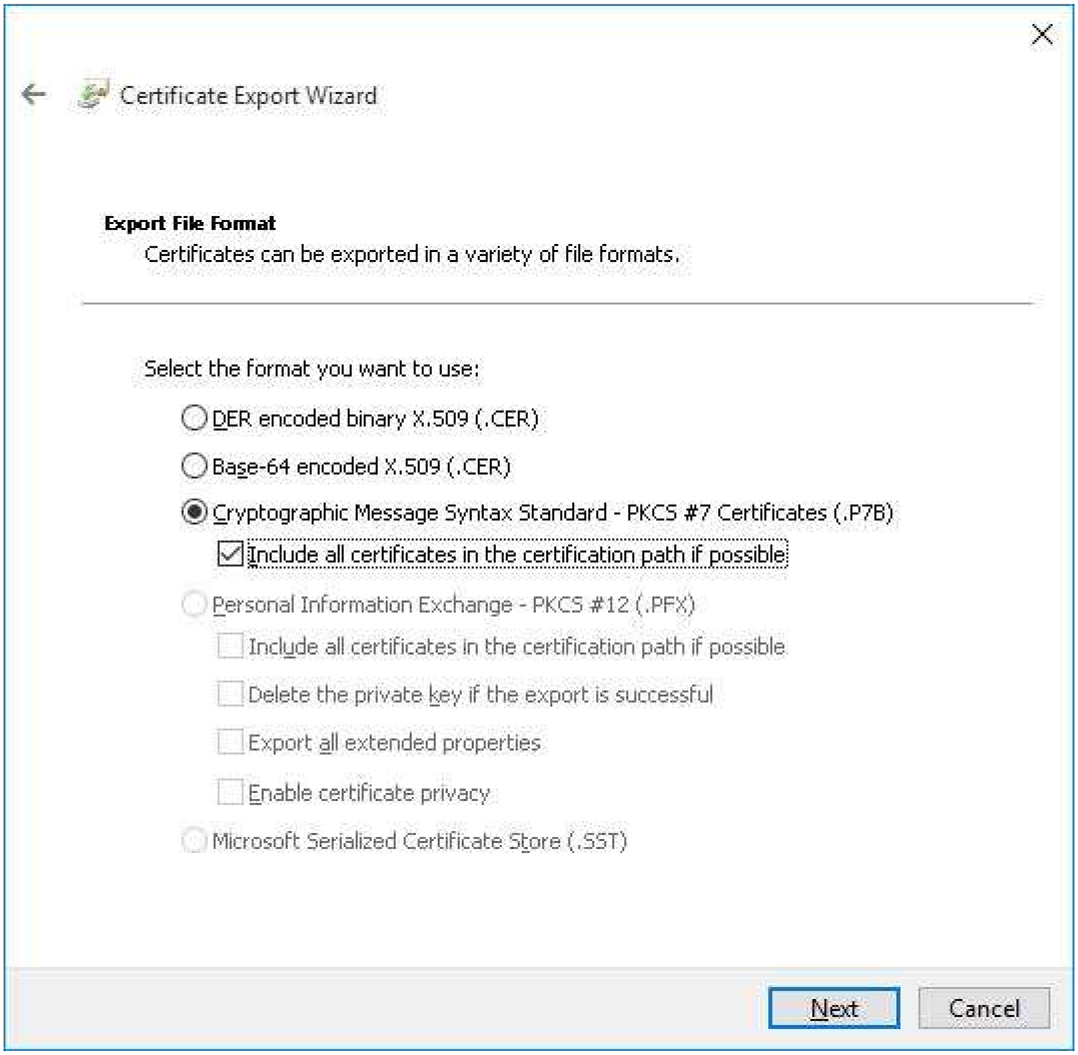
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key

Note: The associated private key cannot be found. Only the certificate can be exported.



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

● Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

☑ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

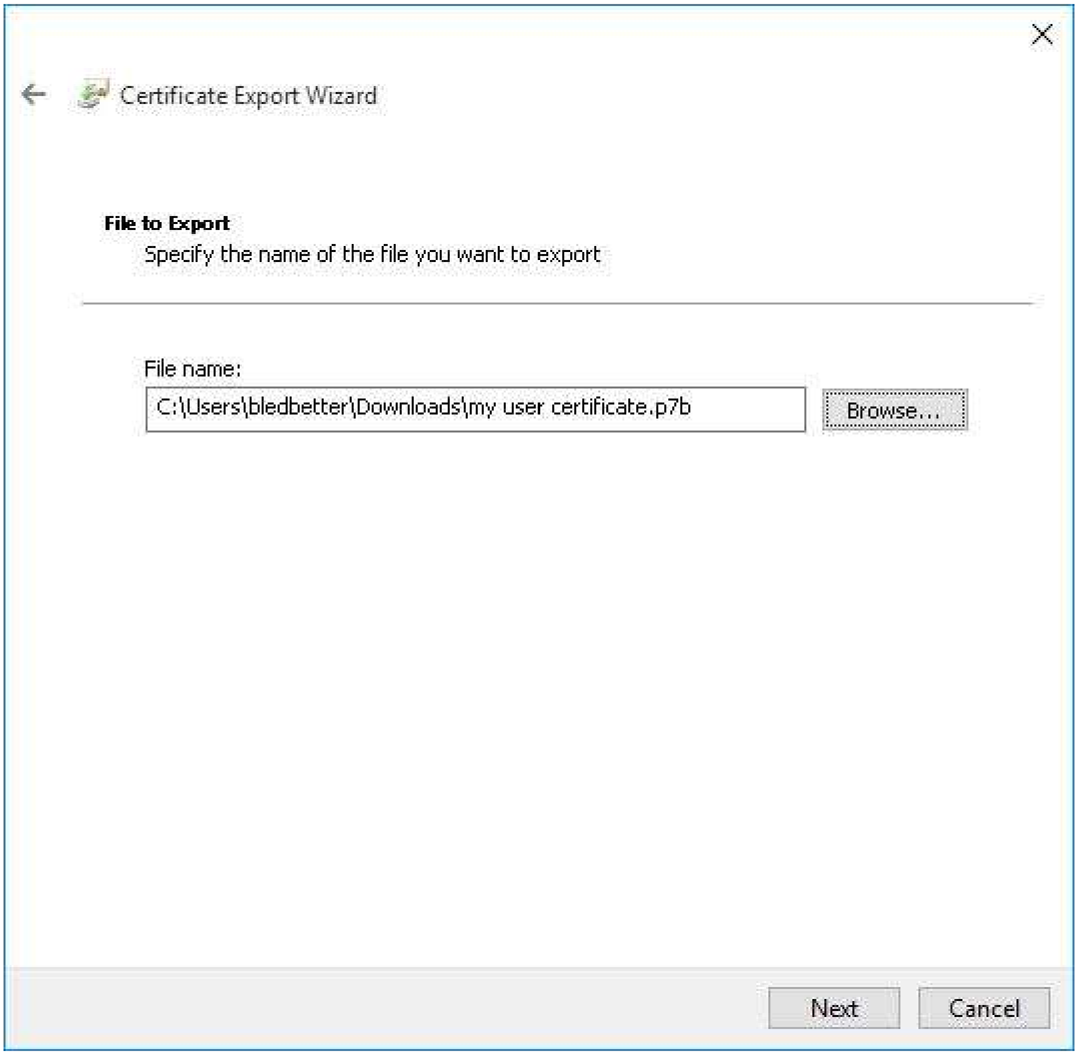
□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

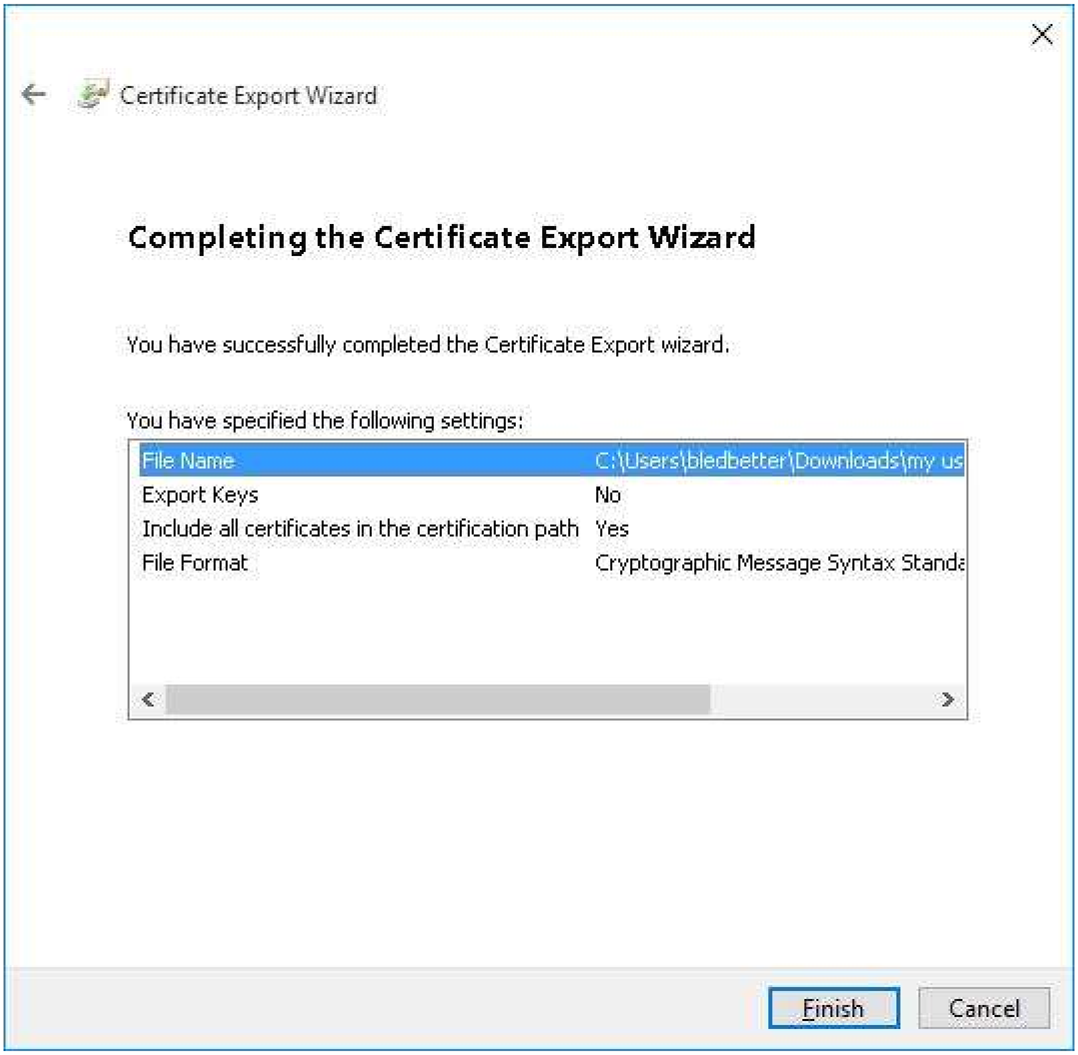


File to Export

Specify the name of the file you want to export

File name:

C:\Users\bledbetter\Downloads\my user certificate.p7b

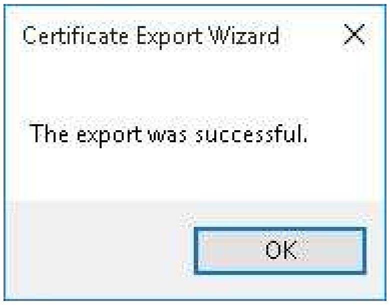


Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\bledbetter\Downloads\my us
Export Keys	No
Include all certificates in the certification path	Yes
File Format	Cryptographic Message Syntax Standa



The export was successful.

6. Save the file to a temporary location such as your downloads folder.

7. Upload .p7b file, along with this form to Secure Upload Link and notify your POC of your completion.