National Aeronautics and Space Administration

WHAT TYPE OF DATA CAN YOU CAN SHARE IN O365 AND WHERE YOU CAN SHARE IT?

Office of the Chief Information Officer

www.nasa.gov

Contents

Office 365 Help: Guidance on Data 3
What types of information can NASA users store within the O365 Tools? 3
Compliance Quick Reference: 3
Agency Documentation References: 3
ITAR, SBU, PII, EAR: Where Does it Go? 4
SBU Data: How do I store it responsibly? 4
If I have a SharePoint Online site, but have several sensitive SBU documents and don't want to PKI encrypt my data, what can I do? 6
Examples 6
ITAR 6
EAR 7
Sensitive PII 7
Appendix A: EXCHANGING ENCRYPTED EMAILS WITH NON-NASA PERSONNEL 8
Appendix B: Encrypting Individual Files on Mac 9
Appendix C: Encrypting files on Windows 10

Office 365 Help: Guidance on Data

What types of information can NASA users store within the O365 Tools?

NASA policy requires SBU information types with additional regulatory controls, such as sensitive PII, ITAR, and EAR, to be manually PKI-encrypted prior to being uploaded or saved to O365 services, including Teams, SharePoint Online and OneDrive. NASA policy allows other information types of SBU to be to be used with O365 services without manual PKI encryption. SBU information must still be maintained securely, clearly labeled as SBU, and may only be stored or manipulated with Agency managed devices, services and applications.

Agency approved encryption solutions must be used when any SBU information is included in the email body or file attachment(s). The requirement for encryption is applicable to all emails that include SBU information.

Compliance Quick Reference:

Email	Action Required
All Sensitive but Unclassified (SBU)	Encrypt Information
SBU - Export Controlled	Encrypt Information
SBU - Sensitive-PII	Encrypt Information
Other Office 365 Services (SharePoint, OneDrive, Teams)	
All Other Sensitive but Unclassified (SBU)	OK To Store Directly on O365
SBU - Export Controlled	PKI Encrypt Information
SBU - Sensitive-PII	PKI Encrypt Information

Agency Documentation References:

NASA's SBU handling requirements are stated in NPR 1600.1A
NASA's SBU handling requirement are stated in policy NID 1600.55, Sensitive But Unclassified (SBU) Controlled Information, Section 5.24.4.5. Additional handling requirements are included in NPD 1382.17J, NASA Privacy Policy, and NPR 2190.1, NASA Export Control Program.

ESD Knowledge Article Reference #KB0015730

ITAR, SBU, PII, EAR: Where Does it Go?

O365 offers so many awesome tools, and you want to get started collaborating with your team right away... but you are concerned about what type of data you can share and where you can share it. Don't fear - We are here to help!

First, here is a list of data types you want to consider:

- SBU (Sensitive but Unclassified)
- Sensitive PII (Personally Identifiable Information)
- ITAR (International Traffic in Arms Regulations)
- EAR (Export Administration Regulations)

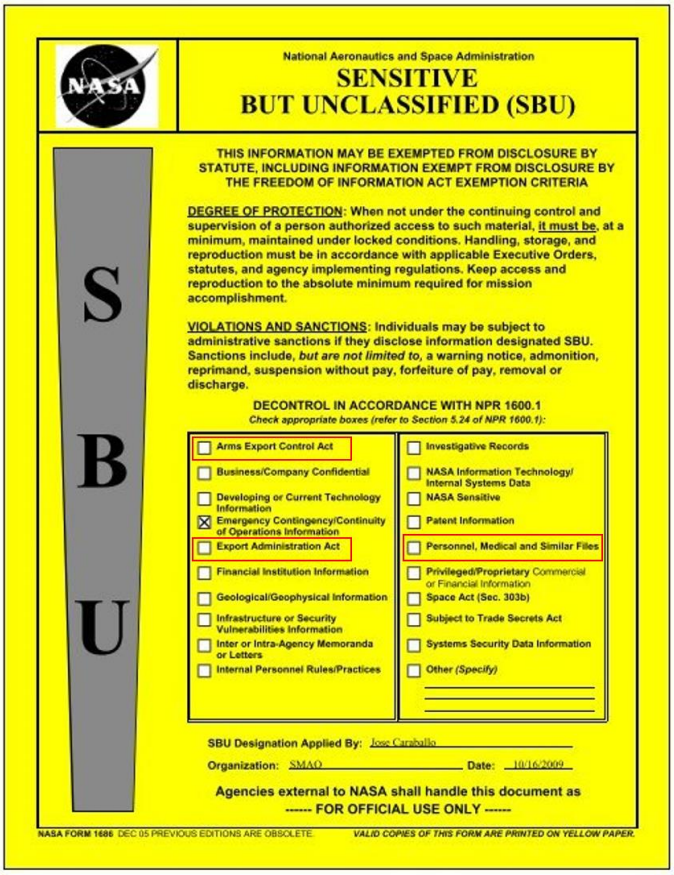
Sensitive PII, ITAR and EAR are all types of SBU data. Some SBU data types, such as these, have additional regulatory controls and therefore should be addressed.

SBU Data: How do I store it responsibly?

What is SBU Data? Can I get a Definition?

> *"The Computer Security Act of 1987, Public Law 100-235, defines 'sensitive information' as 'any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act) but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy.' The purposes of the Computer Security Act included developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems and establishing security plans by all operators of Federal computer systems that contain sensitive information."*

What Type of Data Can You Can Share and Where You Can Share It?



National Aeronautics and Space Administration

SENSITIVE BUT UNCLASSIFIED (SBU)

S B U

THIS INFORMATION MAY BE EXEMPTED FROM DISCLOSURE BY STATUTE, INCLUDING INFORMATION EXEMPT FROM DISCLOSURE BY THE FREEDOM OF INFORMATION ACT EXEMPTION CRITERIA

DEGREE OF PROTECTION: When not under the continuing control and supervision of a person authorized access to such material, it must be, at a minimum, maintained under locked conditions. Handling, storage, and reproduction must be in accordance with applicable Executive Orders, statutes, and agency implementing regulations. Keep access and reproduction to the absolute minimum required for mission accomplishment.

VIOLATIONS AND SANCTIONS: Individuals may be subject to administrative sanctions if they disclose information designated SBU. Sanctions include, *but are not limited to*, a warning notice, admonition, reprimand, suspension without pay, forfeiture of pay, removal or discharge.

DECONTROL IN ACCORDANCE WITH NPR 1600.1

Check appropriate boxes (refer to Section 5.24 of NPR 1600.1):

- ☐ Arms Export Control Act
- ☐ Business/Company Confidential
- ☐ Developing or Current Technology Information
- ☒ Emergency Contingency/Continuity of Operations Information
- ☐ Export Administration Act
- ☐ Financial Institution Information
- ☐ Geological/Geophysical Information
- ☐ Infrastructure or Security Vulnerabilities Information
- ☐ Inter or Intra-Agency Memoranda or Letters
- ☐ Internal Personnel Rules/Practices
- ☐ Investigative Records
- ☐ NASA Information Technology/ Internal Systems Data
- ☐ NASA Sensitive
- ☐ Patent Information
- ☐ Personnel, Medical and Similar Files
- ☐ Privileged/Proprietary Commercial or Financial Information
- ☐ Space Act (Sec. 303b)
- ☐ Subject to Trade Secrets Act
- ☐ Systems Security Data Information
- ☐ Other *(Specify)*

SBU Designation Applied By: Jose Caraballo

Organization: SMAO Date: 10/16/2009

Agencies external to NASA shall handle this document as

------ FOR OFFICIAL USE ONLY ------

NASA FORM 1686 DEC 05 PREVIOUS EDITIONS ARE OBSOLETE. *VALID COPIES OF THIS FORM ARE PRINTED ON YELLOW PAPER.*

When saving data in O365, products such as SharePoint Online, Teams, Planner, Forms and OneDrive, first ask yourself what kind of data you are saving. If it is Sensitive PII, ITAR or EAR data, you are required to PKI Encrypt the data before you upload or save it within O365. All other SBU data is okay to store directly on O365! You should keep this in mind when you are backing up your NASA computer. You can accidently push restricted data to the cloud if your backup your computer to OneDrive. This is a Data Spillage and will notify SOC so pay attention to what you're backing up and where.

When you need to Email any SBU data you must encrypt the information first and note SBU in the email subject line. If you need a refresher on how to do that, check out your annual NASA IT Security Training in SATERN.

It is important to remember that anytime you store SBU Data, it must be marked as SBU so that individuals having access to the SBU information are aware of its sensitivity and protection requirements and stay in compliance with NPR 1600.1A

This guidance applies to all data within O365 regardless of the specific tool you are using.

If I have a SharePoint Online site, but have several sensitive SBU documents and don't want to PKI encrypt my data, what can I do?

If your site contains several SBU documents that require additional regulatory controls, you may consider having an on-prem page dedicated to storing your sensitive information. This page would be a link to your SharePoint Online page or a tab within Teams to make navigation seamless. Because those files are stored on-prem, they do not need to be encrypted.

*Each center's SharePoint On-Prem configuration differs and you should ensure that your center's storage supports those SBU types prior to storing them without encryption.

Another option to consider is "Box", a cloud management platform. "Box" enables users to collaborate on all types of files, store data and is rated for ITAR, EAR and Sensitive PII.

If you do not want to use SharePoint on-prem or "Box" for these documents, be sure to follow encryption governance.

Examples

ITAR

ITAR regulates the export of defense articles and services with the objective to keep materials out of the hands of foreign nationals. These regulations apply for both government contractors and subcontractors, and the articles and services covered by these regulations are outlined in the United States Munitions List (USML).

For some not so in-depth possible examples of ITAR data, see below:

- DDTC license applications
- certain algorithms
- electronic export information filings
- destination declarations
- delivery verifications
- applications for registration
- purchase orders
- foreign import certificates
- bills-of-lading
- non-transfer and use certificates
- shipping documents that contains information relevant to the export of a defense article

What Type of Data Can You Can Share and Where You Can Share It?

EAR

EAR covers the commercial component of product and data import and export. It applies to dual-use items, which are available both for commercial sales and government use, like Aerospace and Propulsion data or Information Security.

Items subject to EAR are enumerated on the Commercial Control List (CCL) in a few categories of products or services:

- Navigation and Avionics
- Aerospace and Propulsion
- Information Security
- Telecommunications
- Materials Processing

Sensitive PII

Sensitive Personal Identifying Information (PII) is defined as information that if lost, compromised, or disclosed could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. In general terms, it is any information that could be used by criminals to conduct identity theft, blackmail, stalking, or other crimes against an individual. Federal and State laws dictate how this information must be stored, transmitted, and processed. For more information on PII and Sensitive PII check out this link.

Some examples of sensitive PII:

- Social Security Numbers
- Bank Account Numbers
- Passport Information
- Healthcare related information
- Medical information
- Drivers license and State ID information
- Biometric identifiers

Appendix A: EXCHANGING ENCRYPTED EMAILS WITH NON-NASA PERSONNEL

EXCHANGING ENCRYPTED EMAILS WITH NON-NASA PERSONNEL

CREATED BY: NASA PKI TEAM

TABLE OF CONTENTS

What is required to exchange encrypted email with outside personnel? 1

How to recognize an encryption certificate 1

Exchange digitally signed emails 1

Download certificate from an external ldap directory server 2

Export and exchange certificates manually via email 2

Exchange certificate using a cd-rom, a secure ftp site or a private email 3

WHAT IS REQUIRED TO EXCHANGE ENCRYPTED EMAIL WITH OUTSIDE PERSONNEL?

When dealing with people outside of NASA community, you may have to exchange emails securely. For doing this, you must have access to their encryption certificate and vice versa. There are a few ways of obtaining the encryption certificate of the other party. Depending on your center and agency security policies about email exchange, you will have to choose the best method that suits you.

HOW TO RECOGNIZE AN ENCRYPTION CERTIFICATE

1. Open a certificate for a user.
2. On the **Details** tab of the certificate window, make sure to select **<ALL>** in the **Show** dropdown box.
3. On the same tab, go to fields section in the middle and scroll down to find and select **Key Usage**.
4. Below in the text area, the key usage should read "**Key Encipherment (20)**" if this is an encryption certificate.
5. Also, if you see a R**evocation Status** tab in the certificate viewer, select it and make sure the revocation status is **OK**.

EXCHANGE DIGITALLY SIGNED EMAILS

1. Request a digitally signed message from the intended recipient. Outlook should attach the necessary encryption certificate to that signed message.

2. When you receive the signed message, open it.
3. Right-click the person's name in the **From**: field.
4. Select **Add to Outlook Contacts**.
5. Click the Certificates button in the Contacts menu tab, and verify an encryption certificate was found in the digitally signed message. If there is no certificate listed, you will need to verify with the person that their email desktop client is set to send encryption certificates with digitally signed messages, and resend the message. Ifyou are still unable to see a certificate, you will need to move to one of the two remaining options.
6. Click the **Save & Close** button.
1. Note: if you already had an Outlook contact with the same email address, Outlook may ask if you want to update the existing contact
7. You should be able to encrypt email to this person now.

DOWNLOAD CERTIFICATE FROM AN EXTERNAL LDAP DIRECTORY SERVER

Some certificate authorities may have a directory server that would allow external users to search for and download certificates. The availability of this service would depend on the particular certificate authority that issued the person's encryption certificate. This information would have to be provided to you from the person you are trying to exchange encrypted email with.

Personnel outside NASA can access LDAP directory of NASA at **pubdir.nasa.gov port 389** and can go to the following searchbase to look for a NASA user's encryption certificate

OU = People, OU = NASA, O = U.S. Government, C = US

EXPORT AND EXCHANGE CERTIFICATES MANUALLY VIA EMAIL

This option requires actions to be taken by both the sender and the intended recipient of the encrypted email messages.

Recipient of the email provides his/her encryption certificate to the sender of the email as follows:

1. Open Internet Explorer.
2. Click on **Tools** from the menu.
3. Click on **Internet Options**.
4. Click on the **Content** tab.
5. Click on the **Certificates** button.
6. Select your encryption certificate within the list of Personal certificates.
    a. Expand the **Friendly Name** column
    b. Select the one that indicates "encryption certificate"
    c. If you are uncertain, you may need to ask your computer support staff.
7. With your encryption certificate selected, click the **Export** button.
8. Click Next in the Certificate Export Wizard.
9. Ensure **No, do not export the private key** is selected, and click **Next**
10. Select the **DER encoded binary X509 format**, and dick Next.
    a. If the above does not work, export as a base-64 encoded cert.

11. Chose a file name and location for the file, and click **Next**.
12. Review the settings, and click **Finish**.
13. Go to the folder where the certificate file was saved, and rename it from a .CER extension, to a .TXT extension. This is required so that when the file is emailed (next step) it will not be stripped out by the email gateway servers.
14. Send the renamed certificate file via email to the sender. Note: this file represents the public key of your encryption certificate, so there are no security concerns for sending this in plain text.

Sender of the email receives the encryption certificate from the recipient and imports it into his/her Outlook contacts as follows:

1. When the recipient's email arrives, save the attached .TXT to your hard drive.
2. Rename the .TXT file back to .CER.
3. If you haven't already done so, create an Outlook Contact card with the recipient's name and email address.
4. In the **Outlook Contact** window, look for the **Certificates** button.
5. Click the **Import** button.
6. Navigate to the **.CER** file that you received from the recipient, and click **Open**.
7. The Certificate name should now appear in the Certificates list.
8. Highlight the certificate, and press the **Properties** button.
9. If the certificate information on the **General** tab indicates there is a problem validating the certificate [as shown by a yellow exclamation point or red 'x' on the certificate icon), continue the steps below. Otherwise, click **OK** and skip to step 10.
    a. Click the **Trust** tab.
    b. Select **Explicitly Trust this certificate**, and press **OK**.
10. Click **Save & Close**.
11. You should now be able to send an encrypted message to the recipient.

EXCHANGE CERTIFICATE USING A CD-ROM, A SECURE FTP SITE OR A PRIVATE EMAIL

If none of the above methods are useful due to restrictions of security policy at your NASA center, you will have to export and exchange your and their encryption certificates using a CD-ROM, a secure FTP server or an external personal email (e.g. gmail).

Refer to "**Export and exchange certificates manually via email**" section above for how to export your encryption certificate to a file.

Once you receive the other user's encryption certificate, you can then import it into your machine store as follows:

1. Once you obtain the other party's encryption certificate as a file, save it to your hard drive and rename the extension of that file to **.CER**
2. Open Windows Explorer and double click the .CER file.
3. The certificate window opens showing that user's certificate. On the General tab, click the **Install Certificate** button.
4. Certificate Import Wizard window opens. Click **Next**.
5. Select the **Place all certificates in the following store** radio button and click **Browse** button.
6. The Select Certificate Store window opens. Scroll down and highlight the **Trusted People** store and click **OK**.

7. Click **Next** on the Certificate Import Wizard.
8. The final page of the Certificate Import Wizard displays. Click **Finish** button.

Now, you should have the other user's encryption certificate in your machine. Outlook should be able to find it when you try to send an encrypted email to them.

Appendix B: Encrypting Individual Files on Mac

Job Aid

Entrust SDM 8.2 for macOS - Encrypting Individual Files

Last update: 12/07/18

Encrypted File Protection with PIV & ASB support is available for macOS

Entrust SDM 8.2 for macOS now supports decryption leveraging the encryption keys on the NASA PIV & Agency Smart Badges (ASB), as well as legacy EPF support. Entrust SDM 8.2 may be used to encrypt SBU Data to one's self and or others. See *NID 1600.55* for more information on NASA's Policy on *Sensitive But Unclassified (SBU) Controlled Information.*

Operating system support

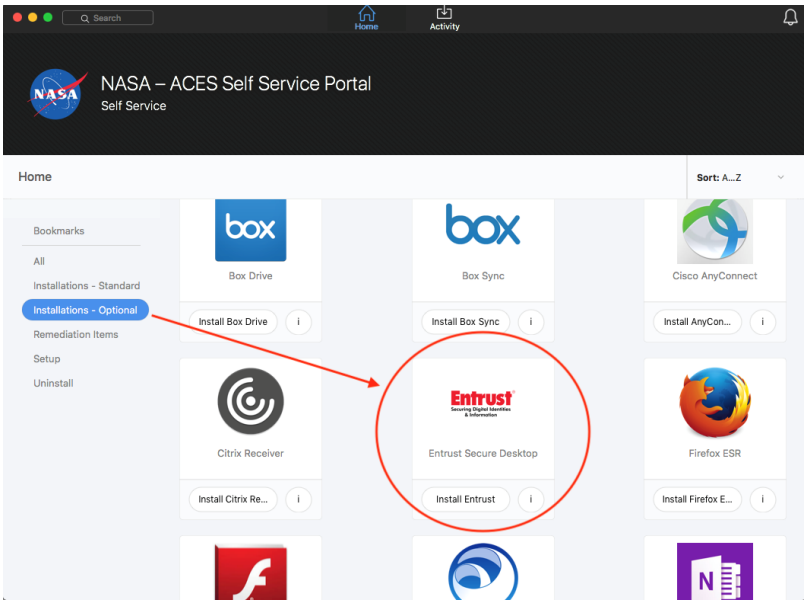
- macOS 10.12 through 10.14 supports Entrust SDM 8.2
- Legacy versions of Mac OS X, 10.11 and below, are not supported

Compatibility

The Entrust encrypted file format is compatible with both macOS SDM 8.2 users and all Windows Entrust ESP users. The file type is a standard P7M S/MIME format.

Obtaining and Installing Entrust SDM

- NEST/ACES Mac users can use the "Self Service" application in the Applications folder. Once launched, chose "Installations – Optional" from the left side, then find the Entrust item and choose "Install Entrust"



- Non-NEST/ACES Mac users will need to work with their Service Provider or system admin to get the Entrust SDM 8.2 client installed. The installer can be downloaded from https://pki.nasa.gov from the "Entrust Software SDM 8 for Mac" section of the right-hand side "PKI User Support" menu.

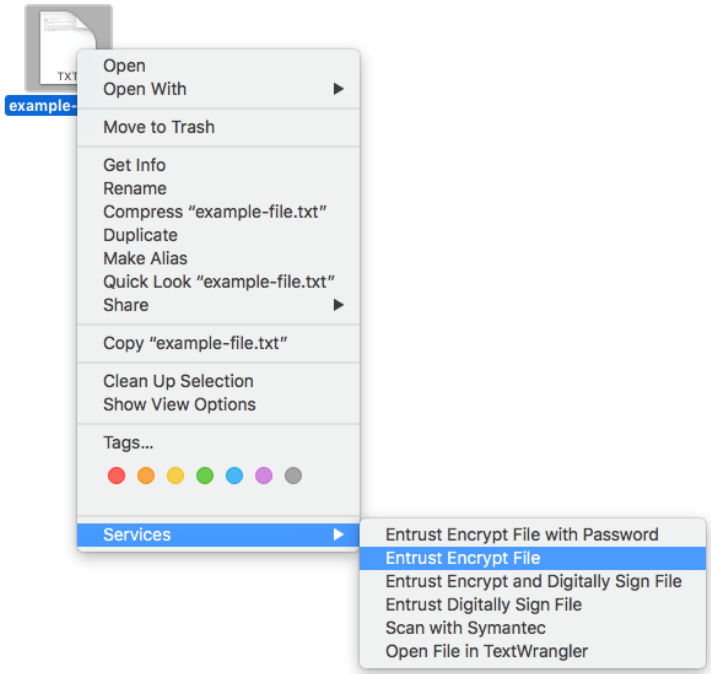
Job Aid

Entrust SDM 8.2 for macOS - Encrypting Individual Files

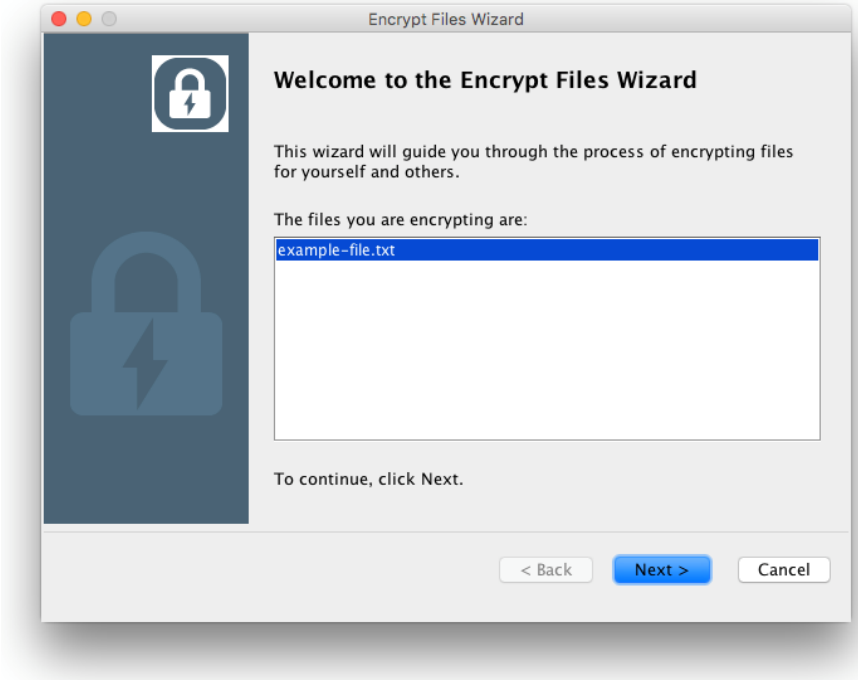
Last update: 12/07/18

How to Encrypt a file with Entrust SDM 8.2

1. Right-click or Control-click the file. Select “Services”, then “Entrust Encrypt File”



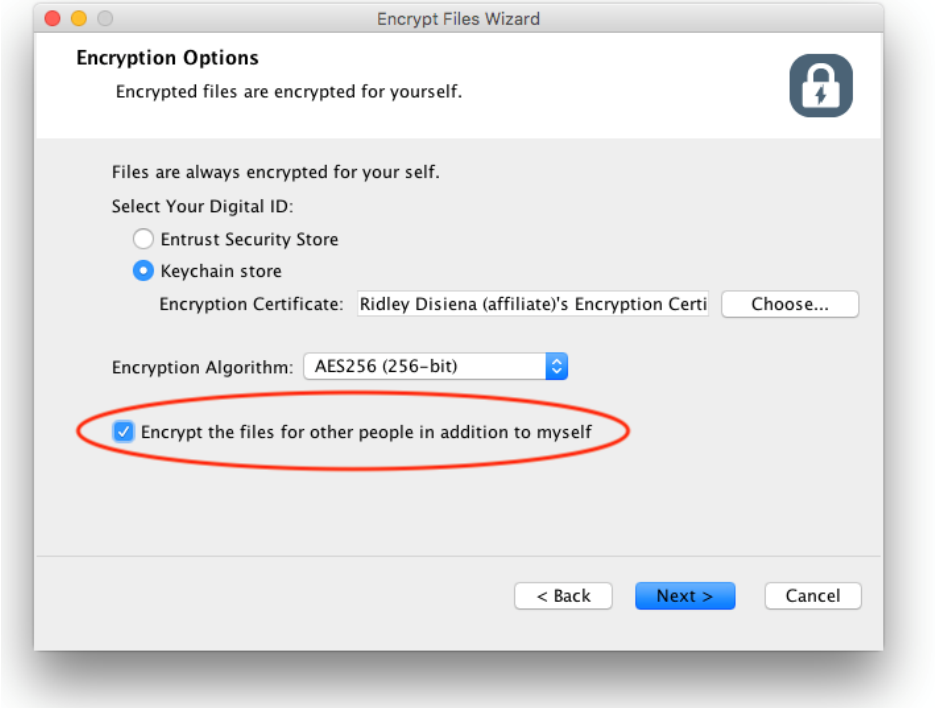
2. Click “Next” on the Encrypt Files Wizard



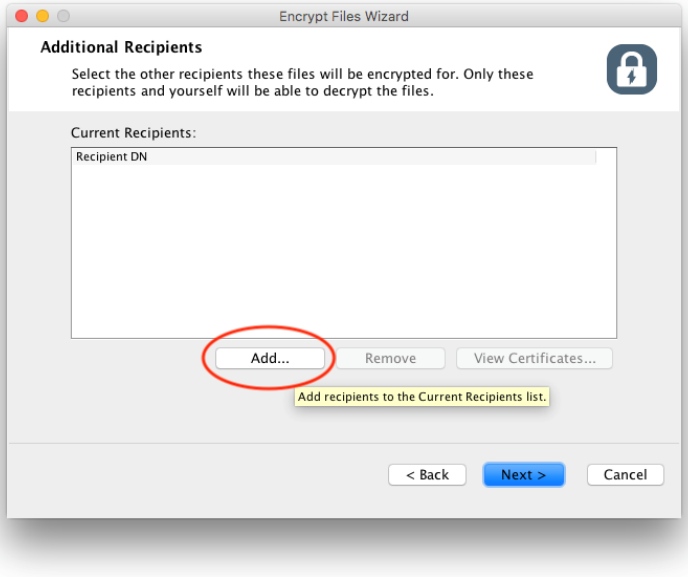
Entrust SDM 8.2 for macOS - Encrypting Individual Files

Last update: 12/07/18

3. If the file is to be encrypted to other people, besides one's self, then be sure to check the "Encrypt files for other people in addition to myself" checkbox. Click "Next". If the Encrypt to others option was not selected, skip to step 8.



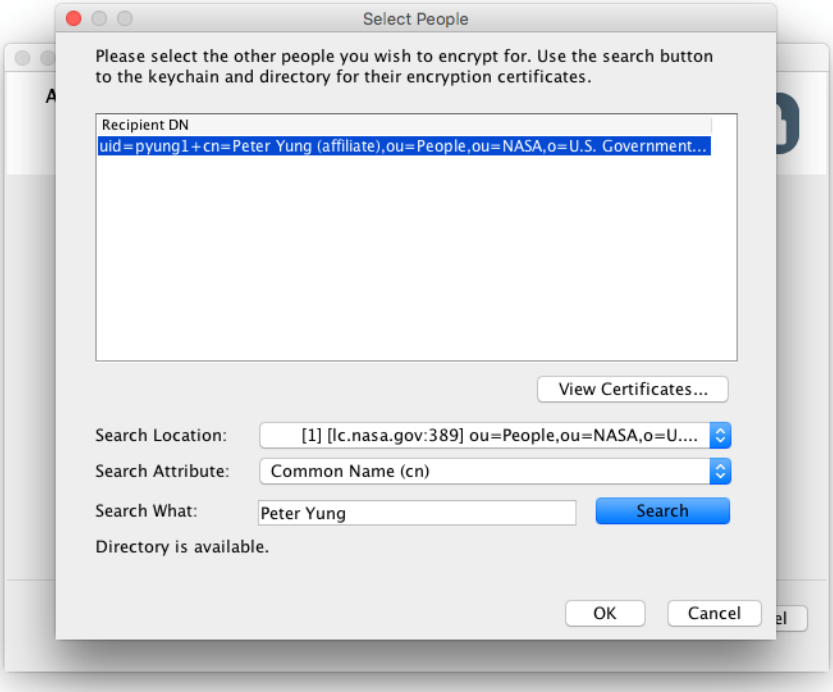
4. If Encrypt to other people was chosen, you will get the Additional Recipients dialog. Choose "Add…" to add recipients.



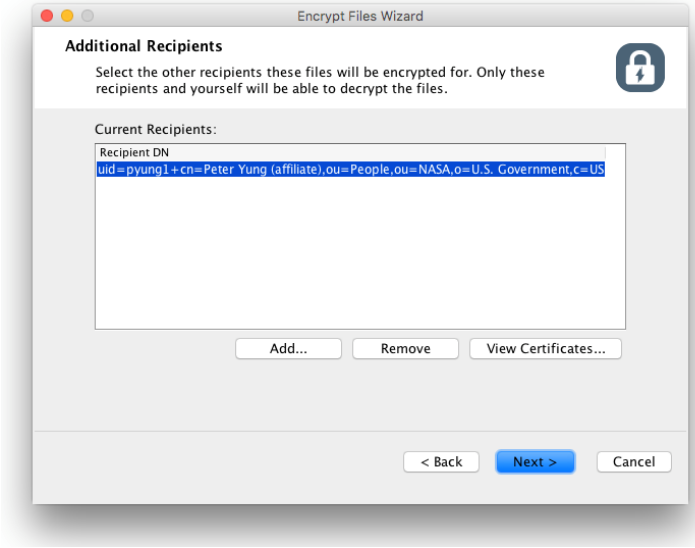
Entrust SDM 8.2 for macOS - Encrypting Individual Files

Last update: 12/07/18

5. To find recipients, you can just use the default Common Name selection and type in the person's first and last name in the "Search What" field, then click search. You may also use just last name and then browse to find the person. Alternatively, other search attributes can be selected instead of Common Name to assist in finding the recipient.



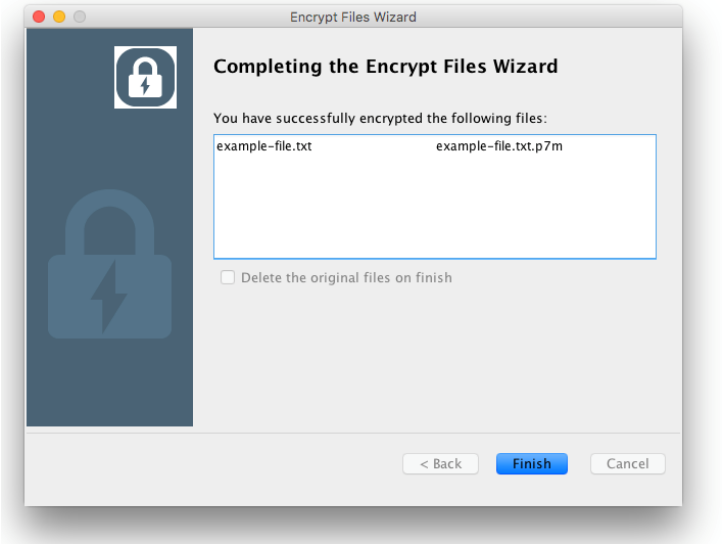
6. Once the recipient is found and selected, click "OK".
7. Then click "Next" if finished adding recipients, or click "Add…" to add more individuals as needed. Clicking "Next" will begin the encryption process.



Entrust SDM 8.2 for macOS - Encrypting Individual Files

Last update: 12/07/18

8. Click “Finish” on the final wizard screen.



9. You will now see the encrypted file placed in the same location as the file that was to be encrypted. The encrypted file shows an icon with a lock display a “.p7m” extension. The non-encrypted cleartext file will remain where it was and it will not be deleted automatically by default.

Appendix C: Encrypting files on Windows

Job Aid

Entrust ESP for Windows - Encrypting Individual Files

Last update: 10/15/19

Encrypted File Protection with PIV & ASB support

Entrust ESP for Windows supports decryption leveraging the encryption keys on the NASA PIV & Agency Smart Badges (ASB), as well as legacy EPF support. Entrust ESP may be used to encrypt SBU Data to one's self and or others. See *NID 1600.55* for more information on NASA's Policy on *Sensitive But Unclassified (SBU) Controlled Information.*

Operating system support

- Windows 10 support with Entrust ESP 10 - NASA PKI Version 10.0.3
- Windows 7 support with Entrust ESP 9.3 - NASA PKI Version 9.3.3

Compatibility

The Entrust encrypted file format is compatible with both Windows Entrust ESP users and macOS Entrust SDM users. The file type is a standard P7M S/MIME format.

Obtaining and Installing Entrust ESP for Windows

- NEST/ACES systems will have the latest version of NASA PKI version of Entrust ESP already installed on the system as part of the standard load.
- Non-NEST/ACES Mac users will need to work with their Service Provider or system admin to get the Entrust client installed if it is not already installed. The installer can be downloaded from https://pki.nasa.gov from the "ESP Installers" section of the right-hand side "PKI User Support" menu.

How to Encrypt a file with Entrust ESP

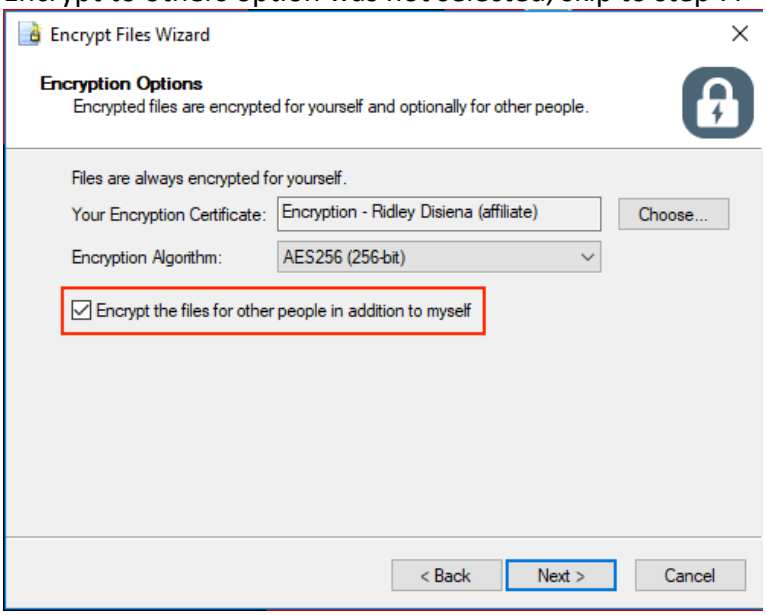
1. Right-click the file then select "Encrypt File" from the menu

Entrust ESP for Windows - Encrypting Individual Files

Last update: 10/15/19

2. Click “Next” on the Encrypt Files Wizard

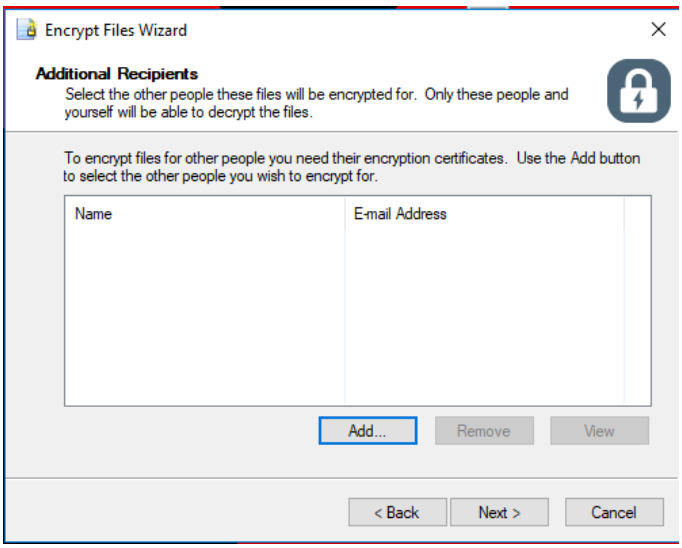
3. If the file is to be encrypted to other people, besides one’s self, then be sure to check the “Encrypt files for other people in addition to myself” checkbox. Click “Next”. If the Encrypt to others option was not selected, skip to step 7.



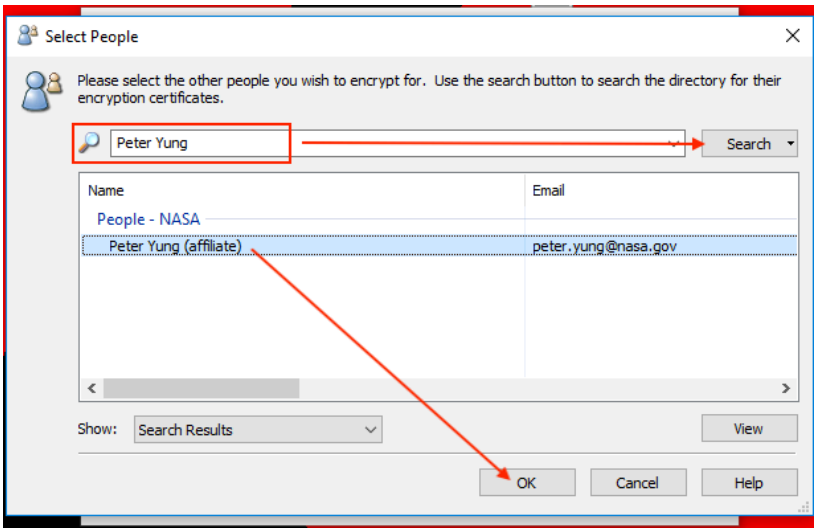
Entrust ESP for Windows - Encrypting Individual Files

Last update: 10/15/19

4. If Encrypt to other people was chosen, you will get the Select People dialog. Choose "Add…" to add recipients.



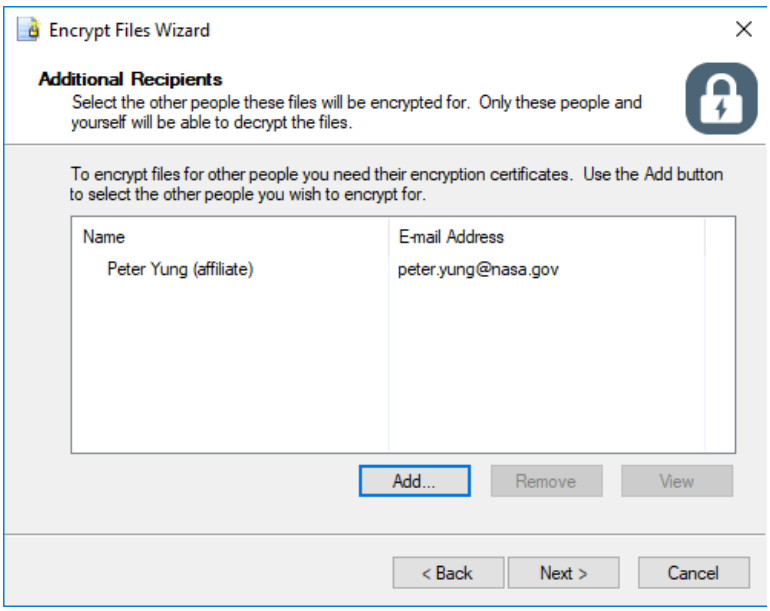
5. To find recipients, you can just type in the person's first and or last name in the search field, with the magnifying glass, then click search. If there is more than one result you may have to scroll through the results and select the correct identity. Alternatively, you may search for the individual by using their email address. Once the recipient is found and selected, click "OK".



Entrust ESP for Windows - Encrypting Individual Files

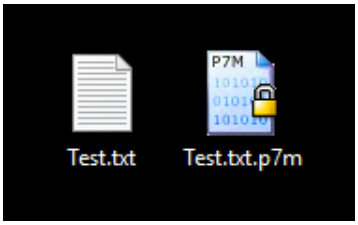
Last update: 10/15/19

6. Then click “Next” if finished adding recipients or click “Add…” to add more individuals as needed. Clicking “Next” will begin the encryption process.



7. On the final step you may choose to keep only the encrypted version of the file, by checking the checkbox "Delete the original files on finish". Alternatively, by default, that option is not checked, which will leave you with both the original unencrypted file and the encrypted version of the file. Click “Finish” once you have made that choice.

Entrust ESP for Windows - Encrypting Individual Files

Last update: 10/15/19

8. You will now see the encrypted file placed in the same folder location as the file that was encrypted. The encrypted file shows an icon with a lock display a ".p7m" extension.