Certificate Retrieval

Instructions

for external customers using

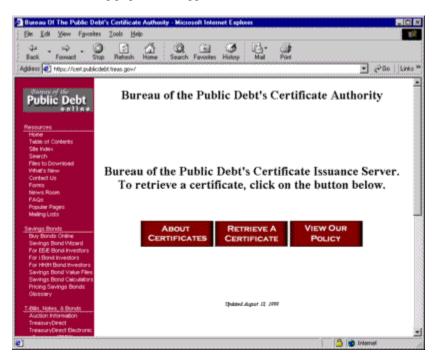
Internet Explorer 4.0.1 on NT 4.0

Updated 12/6/1999

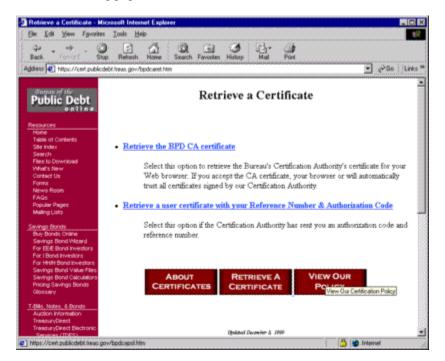
Prepared By: The Internet Services Group

Office of Information Technology Division of Technical Services Distributed Systems Branch

- 1. Ensure that your current configuration of Internet Explorer matches one of the supported browsers in the list of "BPD CA Supported Browsers".
- 2. Point your web browser to : <u>https://cert.publicdebt.treas.gov/</u>
- 3. The following page should appear:



4. Select "**Retrieve a Certificate**". Pending the version of the browser that you are using is supported, you will either receive an error page notifying you that your browser is not supported, or you will see the following page:



- 5. Select "Retrieve the BPD CA certificate".
- 6. Depending if you have ever downloaded a certificate before, a "File Download" dialog may appear asking you to either: a. "Run this program from its current location" or b. "Save this program to disk". Select "Run this program from its current location", then select "OK". The following dialog will appear:

| New Site | Certificate X |
|----------|--|
| | You have been offered a new site certificate to place in your list of trusted issuers. Please select the services for which this certificate will be used. |
| | 🗹 Enable Certificate |
| | Available Usages: |
| | Network client authentication |
| | ✓ Network server authentication |
| | ☑ Secure <u>e</u> -mail |
| | ✓ Software publishing |
| | |
| | View Certificate |

7. Ensure all options are selected and select "OK". The following dialog will appear:

| Root Certificate Store 🔀 | | |
|--------------------------|--|--|
| | Do you want to ADD the following certificate to the Root Store? | |
| <u>•</u> | Subject : Bureau of the Public Debt, Department of the Treasury, U.S. Government, US Issuer : Self Issued | |
| | Time Validity : Wednesday, September 29, 1999 through Sunday, September 29, 2019 Serial Number : 37F27F18 | |
| | Thumbprint (sha1) : 96C49D60 4EBFC598 87C144DC 11CD976E 1CD3A9C7 Thumbprint (md5) : 69C941A7 1817C6ED 360F3C05 7B714670 | |
| | | |
| | <u>Y</u> es | |

- 8. Verify the following information:
 - a. That the Subject (CA) is: "Bureau of the Public Debt, Department of the Treasury, U.S. Government, US".
 - b. That the Issuer (CA) is: "Bureau of the Public Debt, Department of the Treasury, U.S. Government, US".
 - c. That the Thumbprint(shal) is: "96C49D60 4EBFC598 87C144DC 11CD976E 1CD3A9C7"
- 9. Select "**OK**". Select "**Yes**". This will allow your browser to add the BPD CA's Public Key Certificate into your database of trusted certificate authorities. In order for your personal verification certificate to work you must complete this first.

10. You should now be back to the "**Retrieve a Certificate**" page in your web browser. Select "**Retrieve a user certificate with your Reference Number & Authorization Code**". The following web page will appear:

| Internet Explorer Certile Ein Edit View Fyrai | ade Aggüication Form - Microsoft Internet Explorer (2013) |
|--|--|
| Ga and Back Former 1 Addess (2) Hop://cent.public | Sup Refeats Have Search Fercetes Have Mai Fuel |
| Public Debt | ≥ Browser Certificate Retrieval |
| Pessources Flow Flow Search Search Flex to Contents Search Flex to Download What's New Contact Us Forms News Roon PAce Papsal Pages Maling Lists Sarrots Buy Bonts Chine | Please enter the reference number and authorization code that you received from the your Security Administrator. Reference Number : Authorization Code : Submit Request Start Over |
| Savings Bond Ward For ESE Bond Investors For Hold Bond Investors For Hold Bond Investors Savings Bond Value Files Savings Bond Value Files Savings Bond Calculators Pricing Savings Bonds Globbary | Spatned August 12, 1000 |
| T-Bits, Hotes, & Bonds Auction Information TreasuryDirect TreasuryDirect Electronic Come | 🚽 🍙 👘 traenaer |

11. Insert the Reference Number & Authorization code that is printed within your burst pack and select "Submit Request". The following dialog will appear:

| 03644278-e83t | b-11d2-b18a-00a024e7dd97 | × |
|---------------|---|------------------------|
| | Creating a new RSA exchange key! | |
| 议上 | Security level set to Medium Set Sec OK Cancel | urity Level Details |

12. Select "Set Security Level".

| 03644278-e83b-11d2-b1 | 8a-00a024e7dd97 🛛 🗙 |
|-----------------------|---|
| | Choose a security level appropriate for this item contained in your Protected Storage. High Request my permission with a password when this item is to be used. Medium Request my permission when this item is to be used. Low Automatically grant permission to use this item without notification. |
| | < Back. <u>N</u> ext > Cancel |

13. Select "High", then Select "Next".

| 03644278-e83b-11d2-b18a-00a024e7dd97 | | |
|--------------------------------------|--|--|
| | Choose or create a password to protect this item. | |
| aQ, | O Use this password to access this item. Password for: | |
| | <u>C</u> reate a new password for this item. Password for: Babs Jensen | |
| | (example: Tom) Password: | |
| | Confirm: | |
| | < Back <u>F</u> inish Cancel | |

- 14. Insert an identity (Make up a username, do not use the example above), and enter a password. This is the password that protects your certificate's private key. This password will have to be remembered so you can use your certificate, or create new certificates. It is recommended that you create a password at least 8 (Eight) characters long, contains no words from a dictionary. We also recommend that it includes a combination of upper and lowercase characters, numbers, and special characters.
- 15. When you are finished, select "Finish".

| 03644278-e83t | o-11d2-b18a-00a024e7dd97 🛛 🗙 |
|---------------|---|
| | Creating a new RSA exchange key! |
| 1111 AR | Password for Babs Jensen |
| | Security level set to High Set Security Level |
| | OK Cancel <u>D</u> etails |

16. Enter your password and select "**OK**". In about 15 to 30 seconds you should receive a confirmation that you have successfully retrieved your certificate.