How to Create DSA Keys for IPSO

4 August 2014
How To Create DSA 2048 key pairs

Objective

This document outlines the steps needed to generate DSA 2048 byte key pairs to be used for authentication.

Details

Supported OS

- IPSO 6.2 GA083 (MR4)

Supported Appliances

- All IP Appliances that support IPSO 6.2

Before You Start

Related Documentation, Assumed Knowledge and Prerequisites

- Digital Signature Algorithm at Wikipedia: http://en.wikipedia.org/wiki/Digital_Signature_Algorithm
- Public Key Authentication at Wikipedia: http://en.wikipedia.org/wiki/Public-key_encryption
- Local users have already been defined in the IPSO environment
- WinSCP and PuTTY are installed on Windows environment
- Access to Linux environment (optional)

Warnings and Environmental Impact

- None
Generating the key pairs

In this exercise, we will generate keys for a user named “Joe Smith”. Joe’s login name is `jsmith`

To generate the DSA private key using `openssl`:
1. Log in to IPSO system through the console or SSH as `jsmith`.
2. Use this command to generate the private key:
   
   ```bash
   openssl dsaparam -genkey 2048 | openssl dsa -out privatekey
   ```
3. Change the permissions so that only Joe Smith can use the private key file:
   
   ```bash
   chmod 700 privatekey
   ```

To generate the DSA public key using `ssh-keygen`:
1. Use this command to generate the public key:
   
   ```bash
   ssh-keygen -y -f privatekey > publickey
   ```
2. The resulting key is in OpenSSH format.
Storing the public key in IPSO

To use these key pairs, the public key must be stored in IPSO.

To add the public key to Voyager's Authorized Key Pairs:
1. Log in to IPSO's Voyager.
2. Navigate to **Security and Access > SSH (Secure Shell) > SSH Authorized Keys**

3. On the console (or SSH session), see the contents of the public key:
   ```
cat publickey
   ``
   The contents look like this : (truncated for space)
   ```
   ssh-dss AAAAB3NzaC1kc3MAAAEBAOv/5DPgLHWuueFYgktp1v1HmjF6y.....
   ```
4. Copy the entire text, excluding the “ssh-dss” segment.
5. In Voyager, on the **SSH Authorized Key Configuration page**, select the user in the **Add a New Authorized DSA Version 2 Key**.
7. The public key is in OpenSSH format. Paste the text from Step 5 in the **Key in OpenSSH format** textbox.

**SSH Authorized Key Configuration**

<table>
<thead>
<tr>
<th>User</th>
<th>Type</th>
<th>Key</th>
<th>Comment</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Entry</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Add a New Authorized RSA Version 1 Key**

- **Username**: jsmith
- **Key in OpenSSH format**: 6vJIn6e2Vx/z3hBakW0hB
- **Key in SSH-2 format**: 8v.Jd6e2Vx/z3hBakW0hB
- **Comment (optional)**:  

(RSA key settings have no effect in the current configuration because protocol version 1 is disabled.)

8. Click **Save**.

**SSH Authorized Key Configuration**

---
Success.
---

Save successful.

**View/Delete Per-User Authorized Keys**

<table>
<thead>
<tr>
<th>User</th>
<th>Type</th>
<th>Key</th>
<th>Comment</th>
<th>Delete</th>
</tr>
</thead>
</table>
| jsmith | DSA | AAAAB3NzaC1kc3MAAAADwAgEA0/v5DPgLHNumYFgktpTiv1HmjF6yiz0I90ZBpy/3mkJnKtH6dRnThG0wJ50HnJTv7E2d0kS1J7Y6Lx6I99yZ/6g+ZWC8pVcFKmkfPfIH8j1jFr91CyB3jg9F22U1YSanb20HItp2YkgybYjpBLY1tTylFqHMY44a7j3+6YzWHOesuRyA4hKDVm5VIM7pawstc2M2q7P7r2mxM6e7UU799zDFWDAI91vqU93Cfegnt6LL2BKrCQ37EzEqxi4vRwizdU22aMDJO1UkU61hmv147rEI16J8iwP3kFh4pRQU75jG8Hj4HuGU3f97AI14orinx89Q7hpufUAAAAAwKr0cFlaLAsibayqP1C5K6jV/7SAAAB AQDFTkIa5didi3d0r0GjOkqaMQq1gktTqv9461aCth+3BFp8eI8dpwmxmxyQDlE1+uusnZX+GIDBdNtB7mB7qu3M1vjjyCenmunYzKQ67qAnV99yFpM3Vp88z0s0g0U9Kkb0urpETy/1EtY5dRMHveB2ynwV/MqBpCTvTI4q0nUS6ak62hG6lUyWspCccKNigmiC9j10V7veCmXwbiuikEMc+Df7bfJRQnZ2D0J7wcfTVLk4ZSbNnycy1pP6uFvIDomQz2BaW8i/v0+i+1J+T/5u9acDU/naHs9  

9. The public key is now stored in IPSO.
Completing the Procedure

To enable Joe Smith to use the DSA authorized keys for SSH, we must configure an SSH client to use the key pair. In this exercise, we configure PuTTY for Windows and SSH on Linux.

Note: PuTTY uses a proprietary key file so we must use PuTTYgen to convert the private key into PuTTY’s format.

To convert the private key into PuTTY’s format:

1. Use WinSCP to download the private key file from the IPSO appliance to a folder on the Windows machine.
2. Start the PuTTYgen application.
3. From the File menu, Load private key.
4. Browse to the private key from the IPSO appliance and open.
5. In the bottom right corner, select SSH-2 DSA.
6. Enter 2048 for Number of bits in a generated key.
7. Click Save private key.
8. Answer yes to the question (no passphrase was used to generate the keys originally).
9. Save the file in the same location as the IPSO private key.
10. Start PuTTY.
11. Configure the IP address for the IPSO appliance.
12. Navigate to **Connection > SSH > Auth**

13. Click **Browse** and open the private key generated in Step 7.

14. Click **Open**.

15. A PuTTY Security Alert opens. In this window you can see the dss key fingerprint.

   To validate the fingerprint:

   IP290[jsmith]> **ssh-keyscan -t dsa localhost > hostkey-dsa.pub**
   # localhost SSH-2.0-OpenSSH_4.5p1 FreeBSD-20061110
   IP290[jsmith]> **ssh-keygen -lf hostkey-dsa.pub**
16. The fingerprint can be trusted the next time you connect through PuTTY.

To configure the Linux based SSH client to use the private key:
1. Place a copy of the private key on the Linux host.
2. Change the permissions of the private key to make it more secure.
3. Open SSH session with the following syntax:
   ```
   ssh -i /path/to/privatekey jsmith@ipso_host
   ```
4. Verify the fingerprint and answer yes.

Verifying the Procedure

The procedure is successful if there are no issues connecting with SSH to the IPSO appliance using the DSA keys.