



BDA Modernisation Secure File Transfer Protocol (SFTP) Guidance Note

As part of the BDA Modernisation Programme, the JSE is enhancing the security of the current File Transfer Protocol (FTP) by transitioning from user id/password authentication to **Secure File Transfer Protocol (SFTP) using SSH public-key authentication**. User ID and password credentials will no longer be feasible and instead authentication in the modernised solution will be performed using public and private key pairs. This approach is widely adopted and provides stronger security, improved automation support and reduced operational risk.

Each client will be required to generate an SSH key pair and provide their public key to the JSE during the onboarding process. When connecting to the JSE SFTP service, the client's SFTP application uses the associated private key to generate a digital signature. The JSE SFTP server validates this signature against the registered public key and, if successful, authenticates the user and establishes the connection.

The high-level process will be as follows: (see supporting diagrams in [Annexure A](#))

1. Each SFTP user will generate a SSH public/private key pair.
2. The prescribed key standard is **RSA-4096 with SHA-256 signing**.
3. The key pair may be generated using suitable SSH key-generation software.
 - a. For Windows users, this may include **PuTTYgen** or the ssh-keygen command-line tool where available.
 - b. For Linux or macOS users, this can be done using the standard ssh-keygen utility.
4. Two files will be created: a **private key** and a **public key**.
5. The **private key** must remain securely within your organisation and must never be shared with anyone.
6. The **public key** will be provided to the JSE and registered against the relevant SFTP user account. Unlike the private key, the public key is not confidential and may be shared with the JSE for authentication purposes.
7. When your system connects to the JSE SFTP service, it will use the private key to prove its identity. The JSE will validate that identity using the registered public key.
8. Once authentication is successful, the SFTP user will be granted access to the authorised input and output directory folders and files, assigned to the SFTP account.
9. Existing BDA file upload and download permissions will be migrated separately.

Example key-generation commands are shown below for reference:

Windows:

```
ssh-keygen -t rsa -b 4096 -f C:\Users\<username>\.ssh\sftp_key
```

Linux / macOS:

```
ssh-keygen -t rsa -b 4096 -f ~/.ssh/sftp_key -C "broker@company.com"
```

Please note: these commands are provided as examples only. If your organisation already uses an approved enterprise SSH key-management tool or managed file-transfer platform, you may use your approved internal tooling, provided it can generate a compatible RSA-4096 SSH key pair.

Required Client Action:

To support onboarding planning, the JSE requests that clients review the proposed authentication process and confirm whether your organisation can support:

1. Generating SSH public/private key pairs.
2. Using PuTTYgen, ssh-keygen, or your equivalent key-generation tool.
3. Securely storing and protecting the private keys within your environment.
4. Providing public keys to the JSE for registration.
5. Configuring your SFTP client, scheduler, or automated process to use private-key authentication.

Please advise of any challenges, constraints, impacts, or support requirements that may affect your readiness to adopt this authentication method.

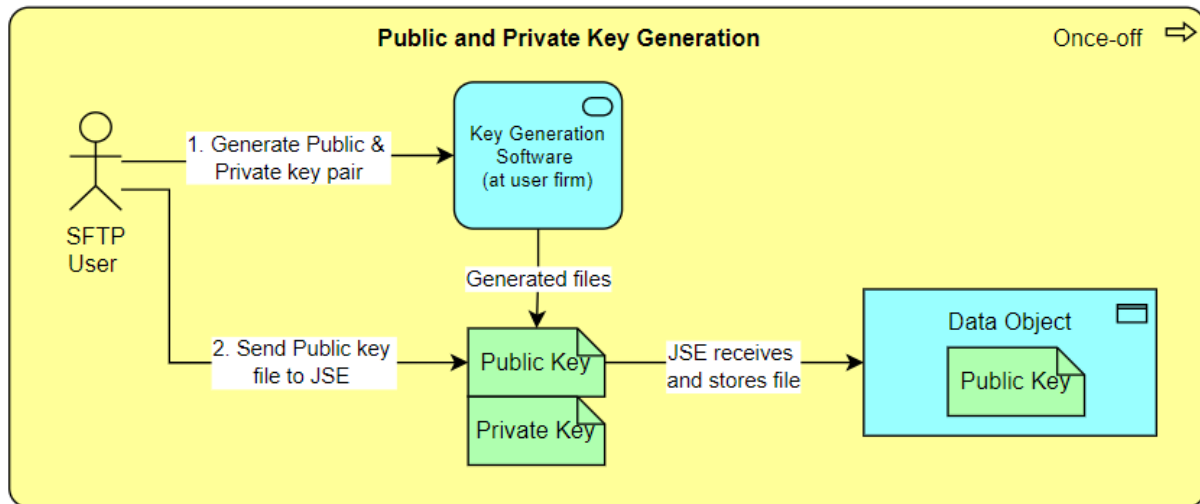
We kindly request that feedback be submitted via email by close of business on **22 July 2026**.

Further details regarding onboarding, public key submission, connectivity testing and implementation timelines will be shared in due course.

Should you have any questions or require assistance, please contact the BDA Modernisation team via your JSE Relationship Manager or the project mailbox at BDAM@jse.co.za.

Annexure A – Supporting diagrams

a. Private and Public Key Generation



b. User Connection Process

