Memo

To	All participants
From	Market Administrator
Date	17 December 2013
Subject	Migration of registry FTP interactions to SFTP

For your information and action

As you should be aware, the Authority has been modernising and updating the communication channels between participants and the registry. Web services and the EIEP Exchange hub using Secure File Transfer Protocol (SFTP) are already fully operational and in use by many participants.

However, for the majority of the data interactions with the registry - switching, metering, distributor updates, notifications and other data updates, most participants use File transfer Protocol (FTP) to send and receive comma separated value (CSV) files.

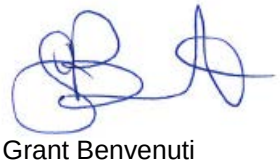
In 2010, the Authority released a consultation paper on shifting these data interactions to a more secure type of transmission channel. After submissions were reviewed, the Authority agreed to implement Secure File Transfer Protocol (SFTP).

Over the past two years, the Authority has been encouraging use of SFTP. Some existing participants have already transferred their transmission channel to SFTP, and in November 2013 FTP was closed to new participants. To ensure the integrity of file transfers between participants and the registry, the Authority will be closing FTP to all existing participants from 31 December 2014

Action required

All participants will need to migrate their registry data files to SFTP by **31 December 2014**. The Authority strongly encourages you to migrate earlier than this, preferably in the first half of 2014.

For further information and assistance with converting to SFTP please contact the Registry Manager at registry.engineer@jadeworld.com



Grant Benvenuti
Manager Market Operations
Email marketoperations@ea.govt.nz , grant.benvenuti@ea.govt.nz
DDI: 04 460 8849

Appendix A – More information on SFTP

Enhancing Data Transmission Security

In today's security conscious landscape and with recent high profile security breaches, protecting information and data has never been more crucial. Data transfer across the Internet provides an obvious attack vector for private data to be compromised. As a result, due care and best practice standards should be used to eliminate these risks.

Most industry participants currently use File Transfer Protocol (FTP) to send updates and report requests into the Registry system and to receive reports and notifications back. FTP has been around since the early days of the Internet as a standard means for transferring files between a client computer and a server. However, due to its un-encrypted nature it is not considered highly secure and is now being rapidly replaced in the Internet world by Secure File Transfer Protocol (SFTP)

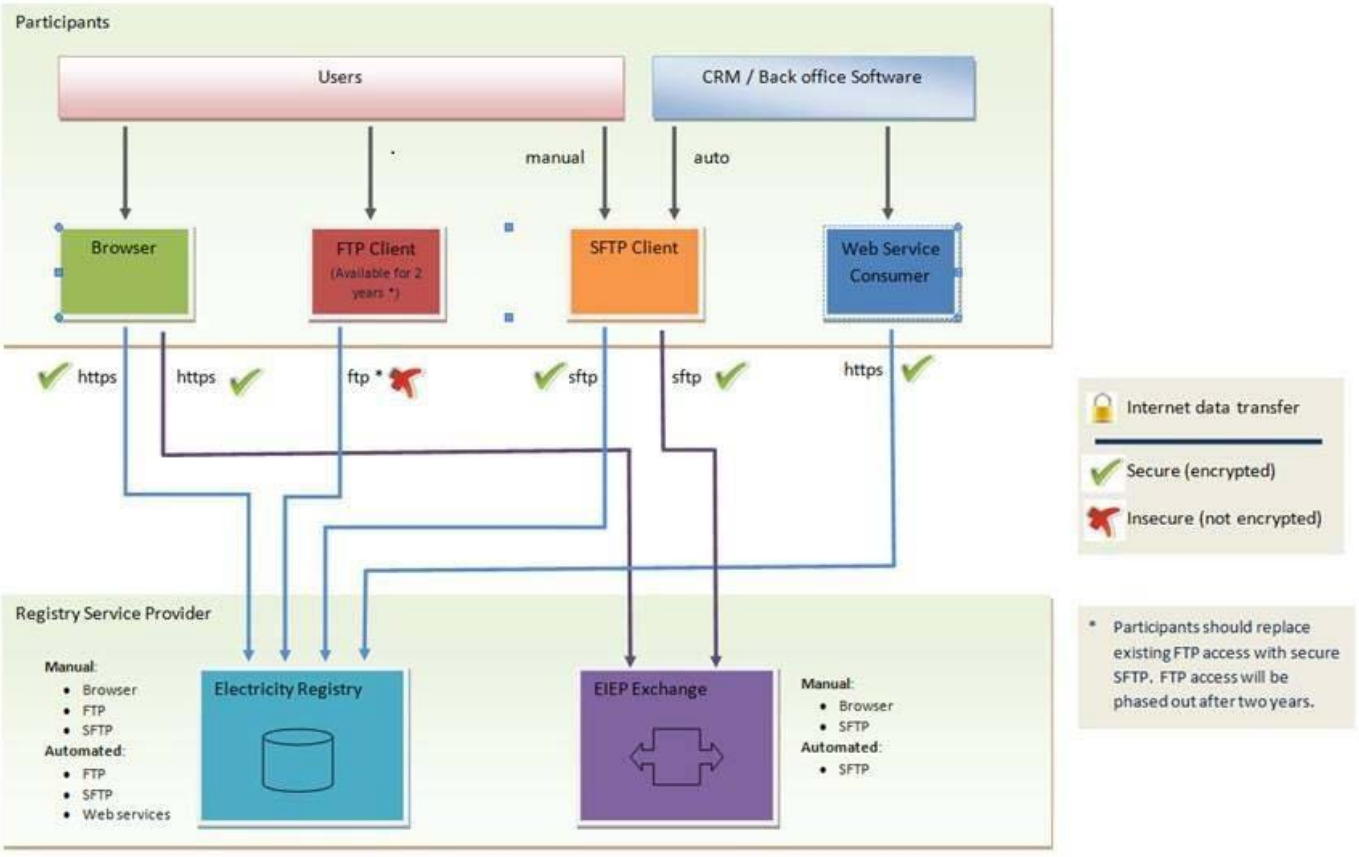
SFTP has been available as an option to industry participants for file transfer since early 2012. However, its uptake has been slow. Although the Registry has committed to continuing to provide FTP access until end 2014, we highly recommend that participants switch to SFTP as soon as possible to ensure that their data exchanges are fully secured.

For further information and assistance with converting to SFTP please contact the Registry Manager at registry.engineer@jadeworld.com

FTP is inherently insecure as it does not encrypt either the data or the commands that are being sent between the client and server. All data is sent "in the clear" including usernames and passwords. This makes it very easy for the credentials or the files being sent to be intercepted and compromised.

For the technically minded, SFTP uses the SSH secure shell protocol to establish a single secure and encrypted channel between client and server over which all data is sent. The server is authenticated during the initial session negotiation and all credentials are encrypted prior to transmission. Data is fully encrypted using robust algorithms such as AES and transmitted over the secure channel established between the client and the server. Data integrity algorithms protect the content of the transmission and prevent modification of the data.

The following diagram shows the information flow through the various access channels and highlights the insecure FTP interface



A comparison of FTP and SFTP File Transfer Protocols

Category	FTP	SFTP
Transmission of data	Data is transmitted in clear text, allowing an attacker to eavesdrop on the network and intercept the communication's content	Data is fully encrypted using robust algorithms such as AES and transmitted over a secure channel established between the client and the server. Attackers eavesdropping on the network will only be seeing encrypted traffic.
Client authentication	Credentials are transmitted in clear text over the network and could be obtained by an attacker using a network sniffer. Authentication is through usernames and passwords only.	Credentials are fully encrypted and use different mechanisms to guarantee protection of the encryption shared secret (the key being used for encrypting and decrypting the data stream) Authentication mechanisms include user names and passwords, public and private keys, digital certificates, Kerberos ticket.
Server authentication	No server authentication, attacker could impersonate the server without being noticed.	Server authenticates during initial negotiation with the client by sending its public key.
Data Integrity	No data integrity mechanism allowing attackers to compromise and alter data without being noticed.	Data integrity algorithms that allow both clients and server to protect the content of the transmission and prevent modification of the data.