FTPS vs. SFTP: Understanding the difference

	FTPS	SFTP
Connection Security	**via SSL/TLS**	**via SSH channel**
Security	Server authentication is verified using a public key intrastructure. Client authentication can also be performed using usernames and passwords or client certificate verification.	Server authentication is typically achieved by securely distributing the server's public key to clients ahead Of time. Clients can be authenticated using usernames and passwords, or public key authentication.
Adoption	Most commonly used, primarily due to its ubiquitous legacy.	More common in more recent devices and software.
Connections Required	At least 2: one port to issue commands and a separate data port for each and every directory listing or file transfer.	Only 1 is required (commands and data use the same connection).
File & Directory Listings & Operations	More rudimentary and not uniform. For example, there is no universal way to get/change file or directory attributes.	Operates via uniform directory listing and documented standards.
Algorithms	Asymmetric, symmetric, and key exchange.	Asymmetric, symmetric, and key exchange.
Authentication	Performed via x.509 certificates (which contain a public key and some ownership information along with a private key).	Performed via SSH keys (which only provide a public key and do not normally confirm ownership information).
Server Requirements	Requires a server x.509 certificate and private key.	Most SSH server installations will include SFTP support (or Open SSH can be used).

Redwood