

Securing and Encrypting Network Traffic with z/OS Communications Server and Policy Agent

Security Workshop

Comparison of IPsec, AT-TLS, and SSH FTP Traffic



IBM Washington System Center
IBM Technical Sales Support

Trademarks

- **The following are Registered Trademarks of the International Business Machines Corporation in the United States and/or other countries.**
 - IBM
 - z/OS
 - **The following are trademarks or registered trademarks of other companies.**
 - Microsoft is a registered trademark of Microsoft Corporation in the United States and other countries.
 - All other products may be trademarks or registered trademarks of their respective companies.
 - Refer to www.ibm.com/legal for further legal information.
-
- OSA-Express Features
 - There are many different types of OSA-Express features. In this document where OSA is mentioned it refers to an OSA port on any of the OSA-Express features unless a specific OSA-Express feature is mentioned.

Agenda

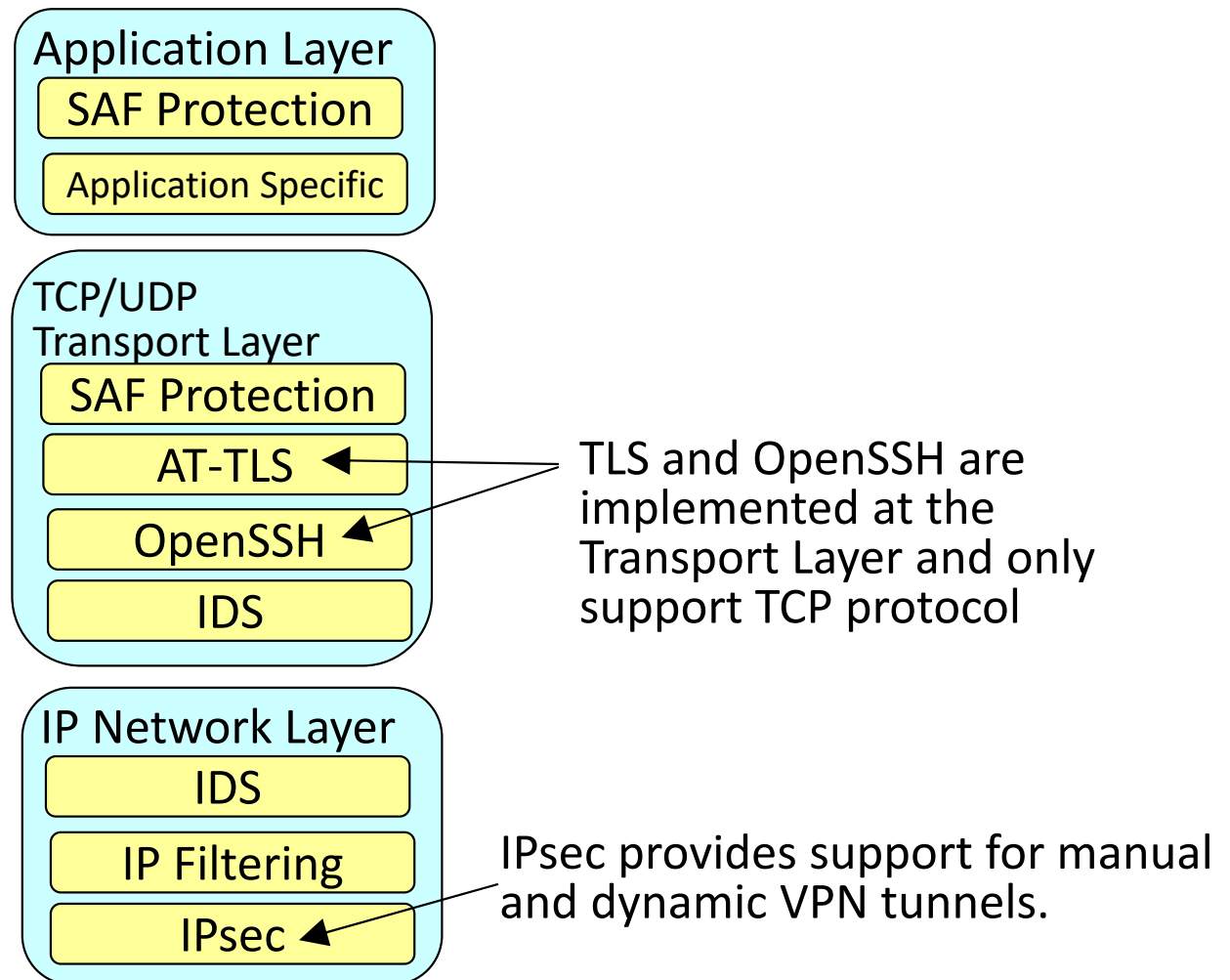
- Standard protocols: IPsec, TLS, and OpenSSH
- What does it mean to "secure" or "protect" a file transfer?
- Ambiguous Acronyms: What Does Secured FTP Mean?
- Protocol Comparison: Transferring Files Securely with TCP/IP
- Comparison of Offload and Cryptographic Hardware Usage by SSL/TLS, IPsec, SSH

Standard protocols: IPsec, TLS, and OpenSSH



Protocol Stack View of TCP/IP Security Features

- IPsec, TLS, and OpenSSH (Open Secure Shell) are all standard protocols that can be used to provide encryption of “Data in Transit”.
- The same protocol must be used on both sides of the connection.
- AT-TLS is just the name for the TLS implementation using Policy Agent. It adheres to the TLS standard and therefore can connect to any partner adhering to the TLS standard protocol.

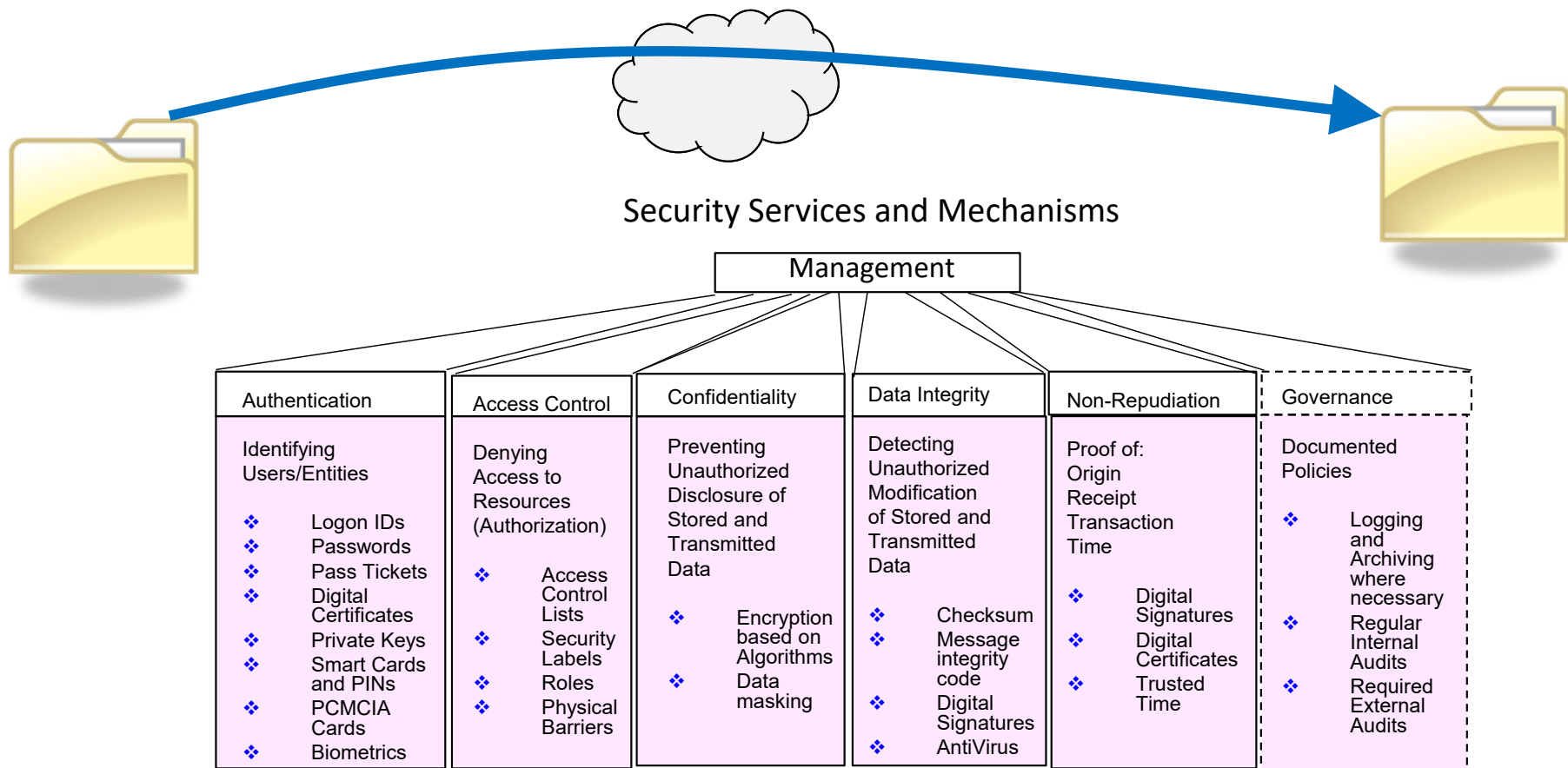


What does it mean to “secure” or “protect” a file transfer?



Protection and Security Services for Transferring a File

1. Authenticate the sender and/or recipient.
2. Keep the data confidential through encryption or masking.
3. Verify the data has not been changed in flight.
4. Verify that the sender is the legitimate owner of the identity he has assumed.



International Standard ISO 7498-2, "Security Architecture"

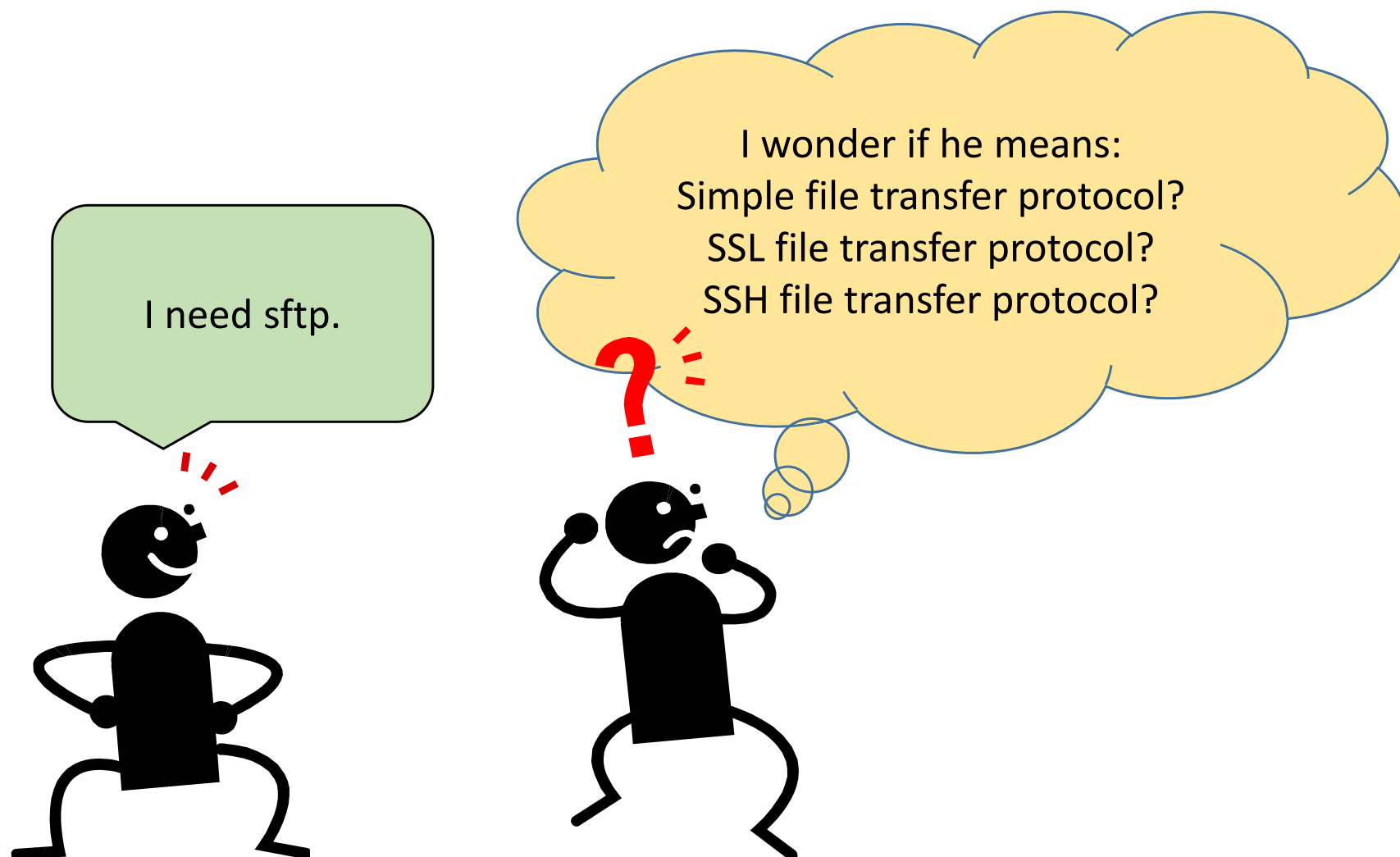
Ambiguous Acronyms: What Does Secured FTP Mean?



The Acronyms --- Confusion

Acronym	Meaning	RFC	Function
SFTP	Simple File Transfer Protocol	913	File Transfer - TCP Port 115
TFTP	Trivial File Transfer Protocol	1350	File Transfer - UDP Port 69
SCP	Secure Copy Program	BSD Remote Copy Protocol	Secure File Transfer over SSH - TCP Port 22
FTP	File Transfer Protocol	959 & 2428	File Transfer - TCP Ports 20 & 21
SFTP	SSL File Transfer Protocol	959, 2428 & 4217	Secure File Transfer – TCP Ports 20 & 21
FTPS	File Transfer Protocol Secure or File Transfer Protocol SSL	959, 2228 & 4217	Secure File Transfer – TCP Ports 20 & 21
ftpd & ftpdns	file transfer protocol daemon & file transfer protocol new server	959, 2228 & 4217	File Transfer Unix processes for FTP Server and forked task for client log in – TCP Ports 20 & 21
SFTP & FTP over SSH	SSH File Transfer Protocol or File Transfer Protocol over SSH	959, 2428 & 4251	Secure File Transfer - TCP Port 22
SSH	Secured Shell	4251	Secure Tunnel for communication
sftp & sftpd	secure file transfer protocol client & daemon	959, 2428 & 4251	Secure File Transfer server and listener - TCP Port 22
MFTP	Managed File Transfer Protocol	Proprietary	File Transfer with automated recovery

The Acronyms --- Confusion



Solution

- Don't use terms or acronyms:
 - Secured FTP
 - SFTP or sftp
- Ask what they mean when someone else uses them...
 - What technology is being used to secure the File Transfer?
 - SSH
 - SSL, TLS, AT-TLS
 - VPN (IPsec Virtual Private Network)
 - Proprietary coding
 - Other
 - What Security Service is required?
 - Authentication
 - Access Control
 - Confidentiality (Encryption, Data Masking)
 - Data Integrity Preservation
 - Non-repudiation
 - Recovery/Restart Capability
 - What platforms are involved?
 - What types of files need to be transferred?
 - File Organization: Record (MVS), Stream, VSAM, DB2, etc.
 - Is FIPS 140 required?
 - Other?

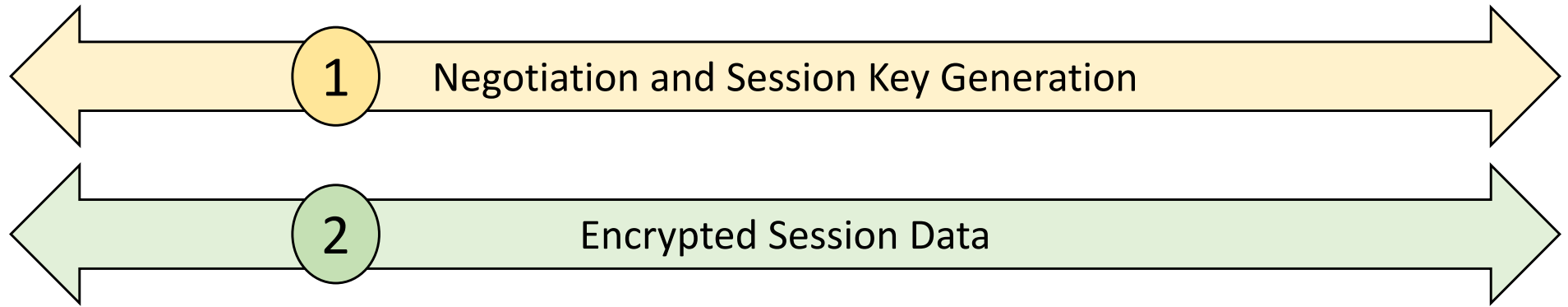
Protocol Comparison: Transferring Files Securely with TCP/IP

Note:

Secure File Transfer is only one aspect for File Transfer Protocols. Certain file transfer protocols have application extensions for security that we do not cover here. Please consult the IP Configuration Reference or other presentations on Security in FTP.



General Architecture of Encryption Flow



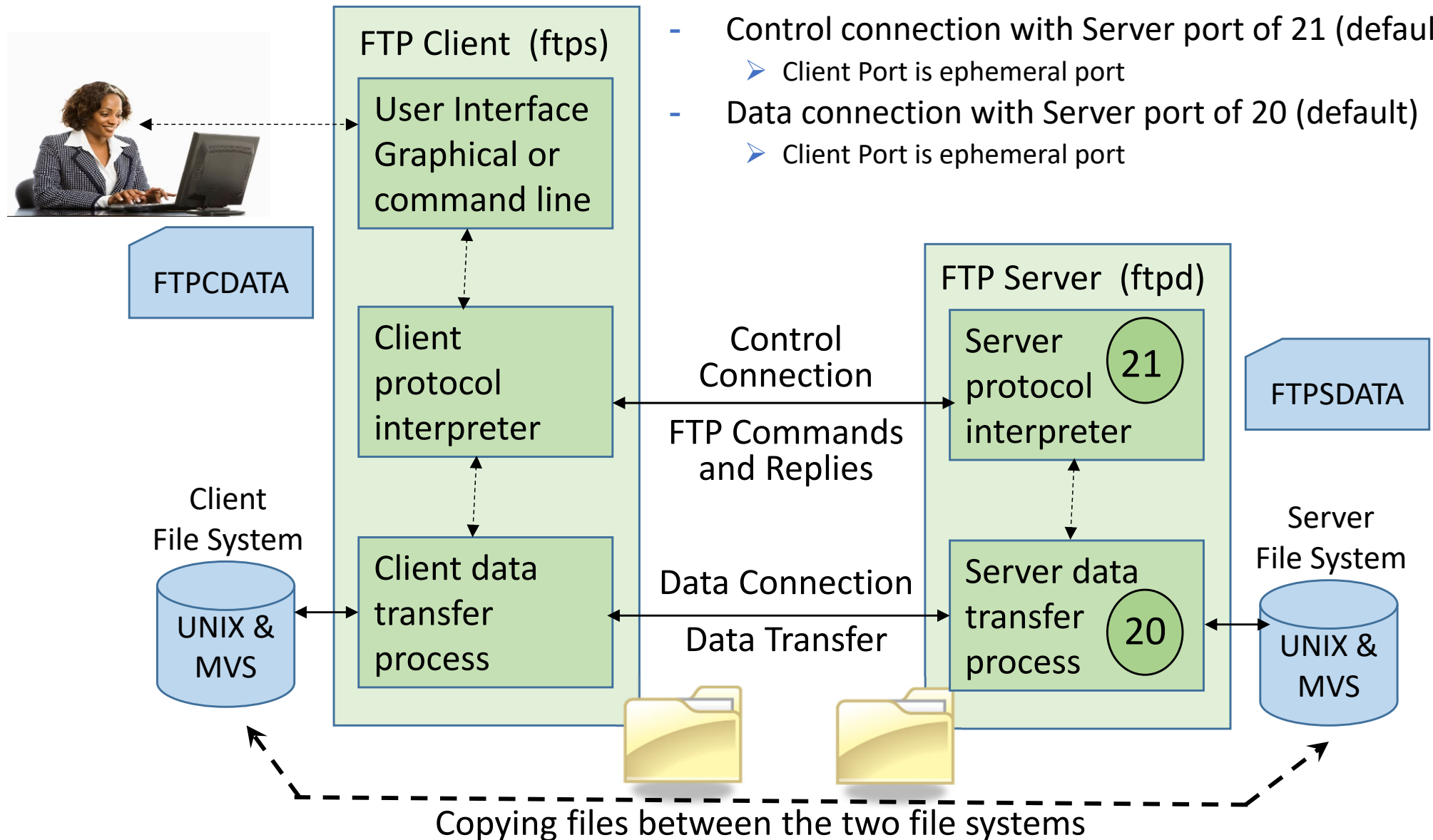
Encryption Flow	What Happens	SSL/TLS Terminology	IPsec Terminology	OpenSSH Terminology
Stage 1 Asymmetric Algorithms	Negotiation of Secure Connection: Authentication and Generation of and encrypted Transmit of Session Key	Handshake Layer	Phase I Phase II	No official terminology; just negotiation stage
Stage 2 Symmetric Algorithms	Encryption and Decryption of Data Payload (Session Data)	Record Layer	Phase II Tunnel	No official terminology, just data transfer stage

- Essentially all these security protocols use the same basic architecture:

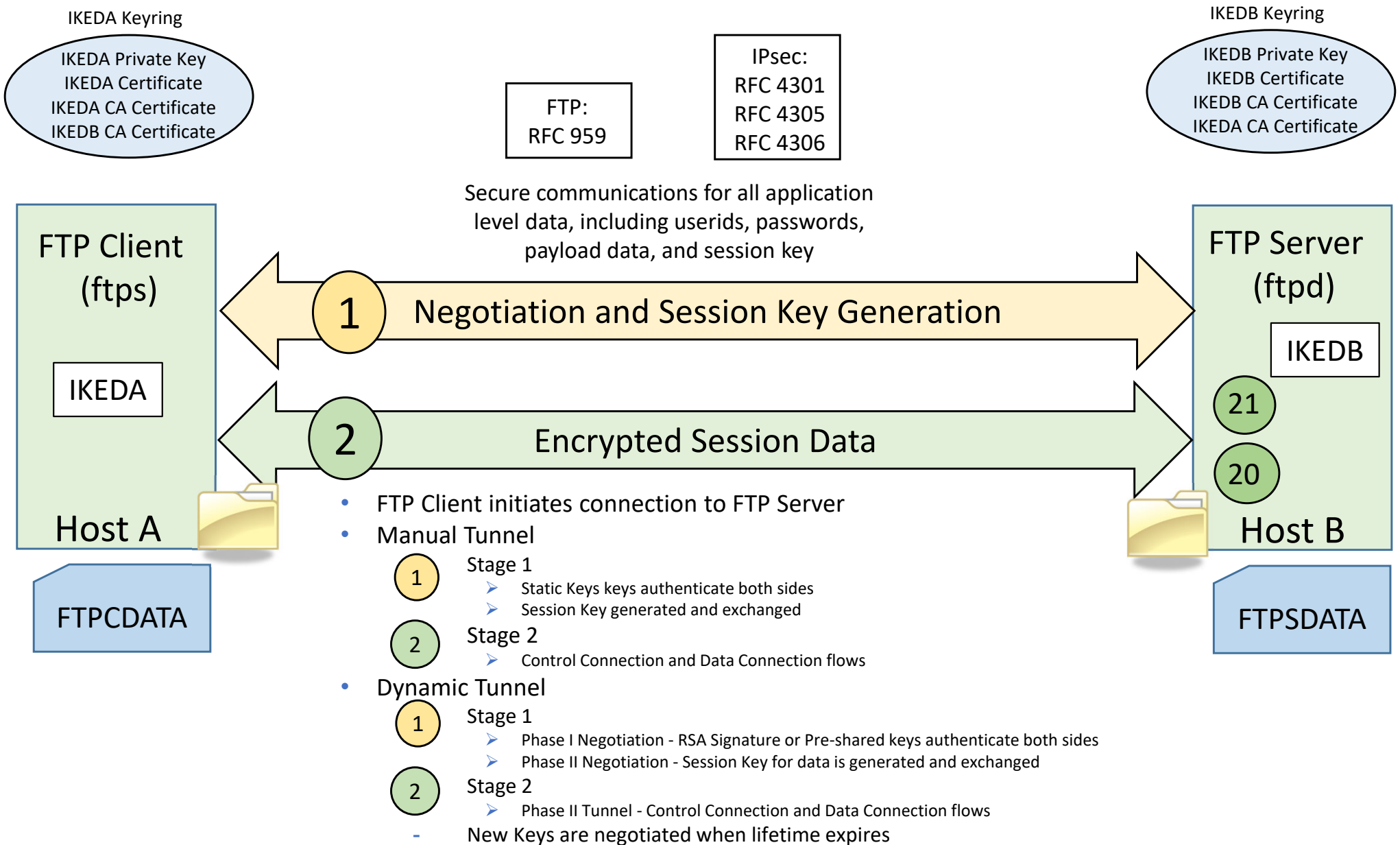
- 1 Authenticate the partner; generate a symmetric key
 - Encrypt symmetric key with asymmetric algorithm and send
- 2 Encrypt session data with symmetric ("Session") key and transmit session data

File Transfer Protocol (FTP) (RFC 959)

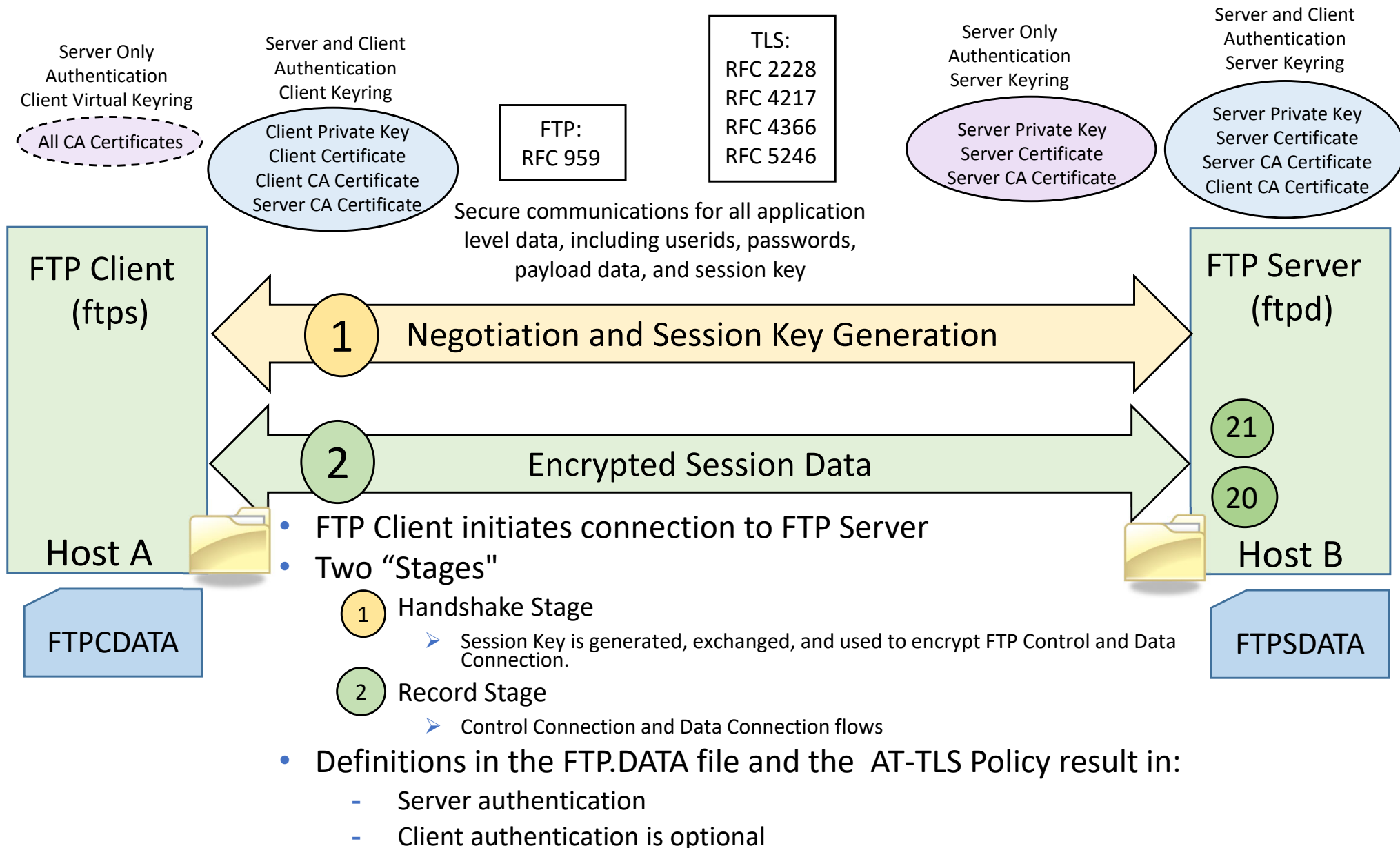
- An FTP session uses two TCP connections:
 - Control connection with Server port of 21 (default)
 - Client Port is ephemeral port
 - Data connection with Server port of 20 (default)
 - Client Port is ephemeral port



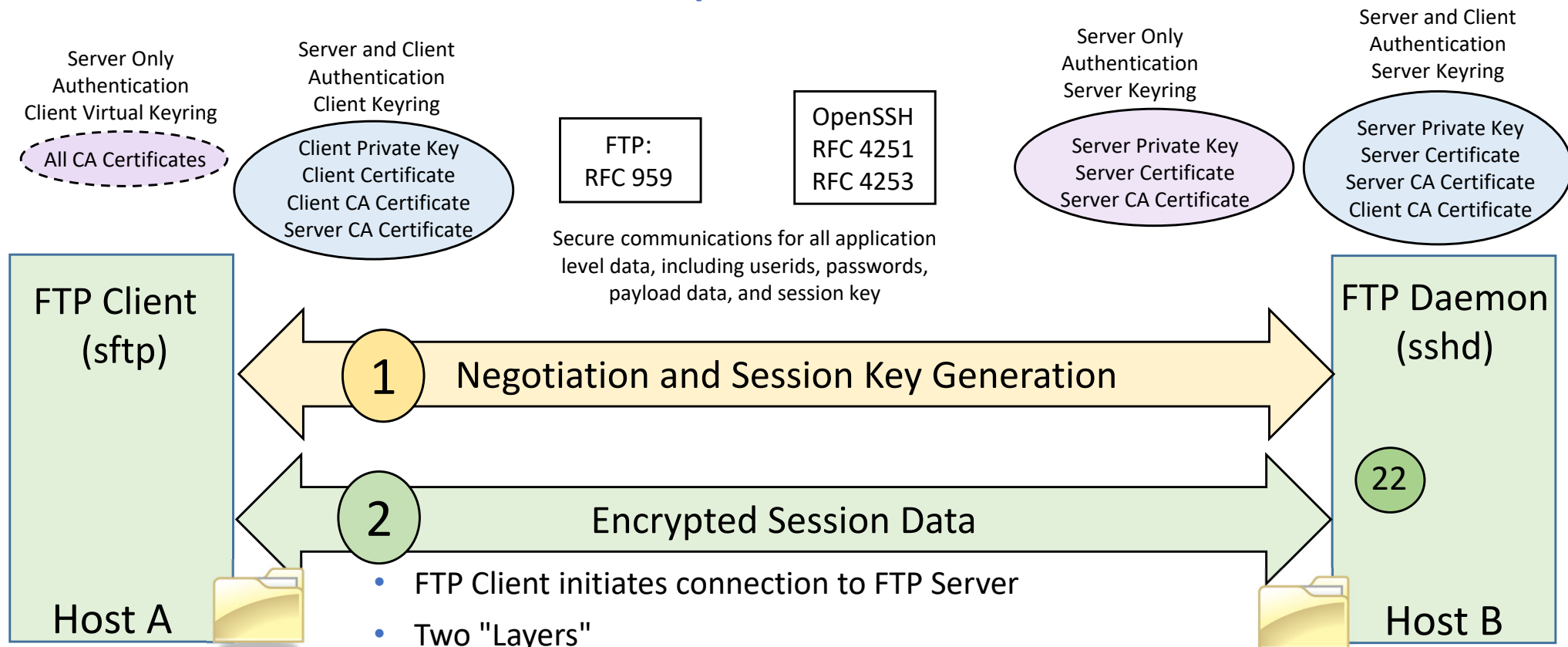
Secure FTP with IPsec



Secure FTP with TLS (and SSL and AT-TLS)



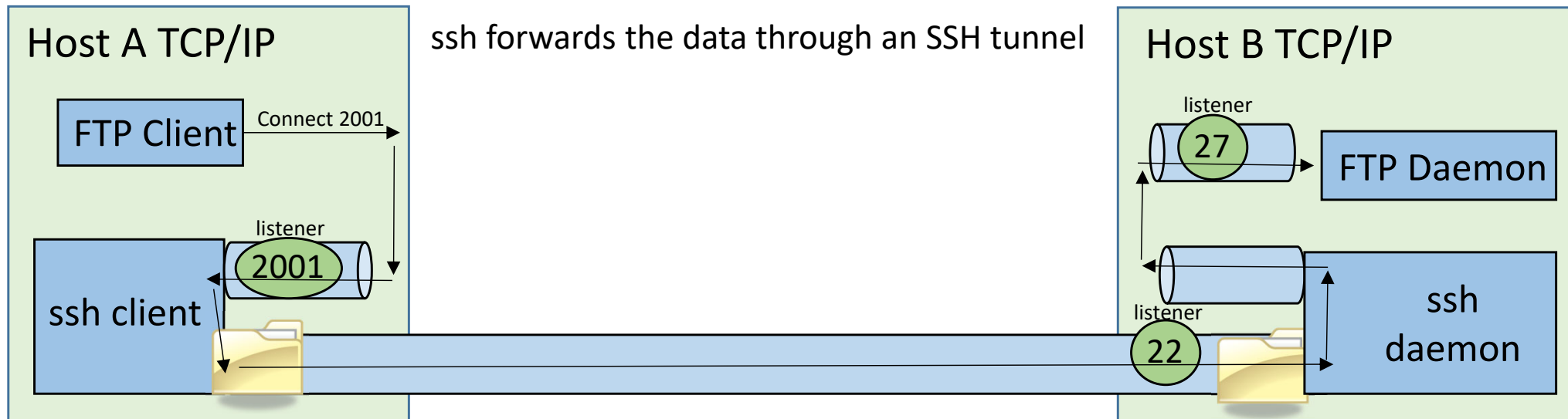
Secure FTP with OpenSSH



- FTP Client initiates connection to FTP Server
- Two "Layers"
 - 1 Handshake Layer
 - Session Key is generated, exchanged, and used to encrypt FTP Control and Data Connection.
 - 2 Record Layer
 - Control Connection and Data Connection flows
- OpenSSH V1R2 supports RACF key rings (for access to CA Certificates only).
 - Prior to V1R2 a unix key generation and management.

OpenSSH does not use X.509 certificates but does use Public / Private key pairs.

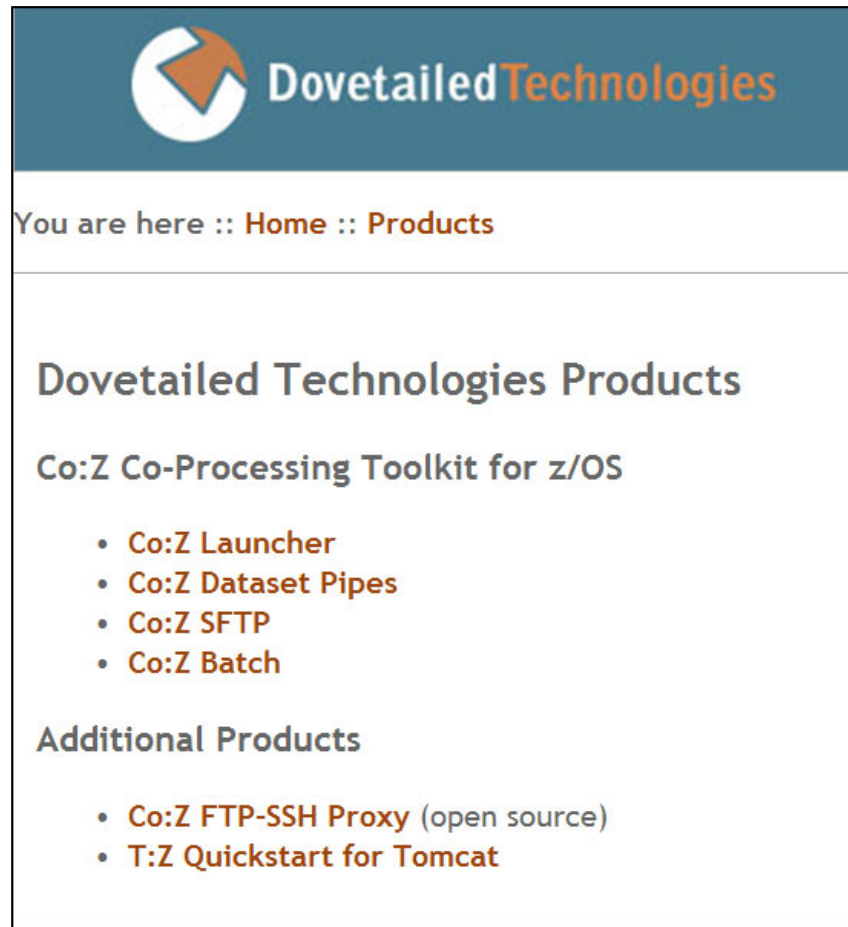
OpenSSH with TCP/IP Port Forwarding



- Encrypts Userid and Password and Data in communication flows
 - Through Port Forwarding or "Tunneling"
- Scenario:
 - Application Client at Port 2001 on Host A
 - Application Server at Port 27 on Host B
 - SSH is configured to support Port Forwarding
 - The SSH client forwards the data through an SSH tunnel to the SSH daemon
 - The SSH daemon delivers the data to the server at Port 27

Dovetail Technologies and Co:Z FTP

<http://dovetail.com>



- The Co:Z Co-Processing Toolkit for z/OS includes Co:Z SFTP - a port of the OpenSSH (v5.0p1) sftp-server subsystem and sftp command (renamed as cozsftp). Extensive enhancements have been made to support z/OS facilities such as MVS datasets and spool files.

z/OS OpenSSH

- z/OS OpenSSH is part of z/OS base in Unix System Services
 - Starting in z/OS V2.2
 - z/OS OpenSSH User's Guide, SC27-6806
- OpenSSH was part of IBM Ported Tools for z/OS
 - Prior to z/OS V2.2
 - IBM Ported Tools for z/OS User's Guide (SA22-7985-06)
 - OpenSSH User's Guide (SA23-2246-02)
- The Internet Engineering Task Force (<http://www.ietf.org/>)
- Four main SECSH internet drafts are:
 - SSH Transport Layer Protocol
 - draft-ietf-secsh-transport-17.txt
 - SSH Authentication Protocol
 - draft-ietf-secsh-userauth-20.txt
 - SSH Protocol Architecture
 - draft-ietf-secsh-architecture-15.5.txt
 - SSH File Transfer Protocol
 - draft-ietf-secsh-filexfer-05.txt

Managed FTP Applications

- Many alternatives for transferring files over the internet:
 - FTP without Encryption
 - FTP with TLS implemented in the application
 - FTP with AT-TLS
 - FTP over IPsec Tunnel
 - FTP over OpenSSH
 - FTP over OpenSSH with Port Forwarding
- Some of these options have manually triggered recovery/restart capabilities
 - Others (OpenSSH) do not
- Managed File Transfer Applications
 - Provide automatic recovery/restart
 - Examples:
 - Tivoli Storage Manager (formerly known as ADSM)
 - Sterling DB2 Connect and Connect Direct (formerly Network Data Mover - NDM)
 - Connect Direct can call System SSL directly and can offload System SSL and some compression operations to zIIP
 - MQ Series File Transfer Enhanced (MQ FTE)
 - and many more

MQ File Transfer Edition (FTE)

- FMID 5655-U80
- Popular Managed FTP product
- Provides Reliable Transfer
 - Binary
 - DB2
 - Microsoft Products
 - MVS files
 - Open Database Connectivity (ODBC)
 - Oracle Informix
 - SQL
 - Sybase
 - Text
 - Unix files
 - VSAM
- and Optional Security with TLS

Summary

Support	IPsec	TLS	OpenSSH
IETF Standard	Yes	Yes	Yes
MVS Datasets	Yes	Yes	No
Unix Files	Yes	Yes	Yes
Server Authentication	Required	Required	Required
Client Authentication	Required	Optional	Optional
System SSL	Yes	Yes	OpenSSL instead
CPACF	Yes	Yes	Yes
Crypto Cards	Authentication Only	Authentication Only	Random Number Generation (RNG) Only
TCP Protocol	Yes	Yes	Yes
UDP Protocol, etc.	Yes	No	No
FIPS 140	Yes	Yes	Yes

Comparison of Offload and Cryptographic Hardware Usage by TLS, IPsec, SSH

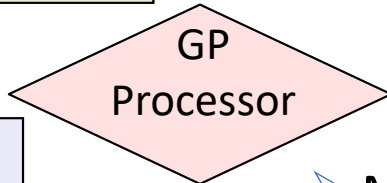


- Two Stages

Cryptographic Cards
(Accelerator or Coprocessor)

CPACF

Software



- Phase 1 Negotiation / Key Generation

- Dynamic Tunnels IPsec IKED Phases 1 and 2

- Authenticates Partners and generates SA Keys

- Uses ICSF or Crypto Card if available
Accelerator Card (Clear Key Mode)
Coprocessor Card (Secure Key Mode)

- Manual (Static) Tunnels

- Uses prior agreement instead of dynamic negotiation

- Phase 2 Data Tunnel

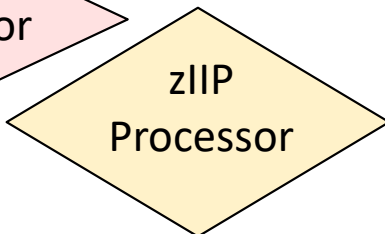
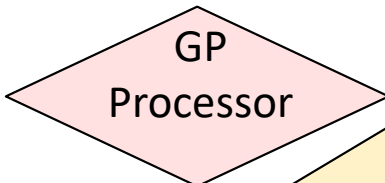
- Dynamic or Manual Tunnels

- Encrypts/Decrypts data

- Uses CPACF (clear key only) if available

CPACF

Software



- Two Stages

- Phase 1 Negotiation / Key Generation

- Handshake Layer

- Authenticates Server (and Optionally Client) and generates Session Key

- Uses ICSF or Crypto Card if available
 - Accelerator Card (Clear Key Mode)
 - Coprocessor Card (Secure Key Mode)

Cryptographic
Cards
(Accelerator or
Coprocessor)

CPACF

Software

GP
Processor

- Phase 2

- Record Layer

- Encrypts/Decrypts data

- Uses CPACF (clear key only) if available

CPACF

Software

GP
Processor

OpenSSH Use of Cryptographic Hardware

Cipher	Available Hardware	
	CPACF only	CPACF & Coprocessor
RNG (Random Number Generation)	In software	In Coprocessor
RSA	In software	In software
DSA	In software	In software

- RSA, DSA
 - for Authentication of peer
 - for Generation of Session Key and Digital Signature
- RNG
 - OpenSSH on z accesses the hardware Coprocessor only during the Random Number Generation (RNG) that is used in the process of generating the symmetric key which will be used during the data transfer stage of SSH.

End of Topic

