Aayu TECHNOLOGIES

SECURE FILE TRANSFER PROTOCOLS

AS2 vs AS3 vs AS4

Three Applicability Statement protocols move business-critical data safely between trading partners. They differ in how they transport files, how they secure them, and where they fit. Here's how to tell them apart.

THE PROTOCOLS AT A GLANCE

One family, three transports

AS2

MOST ADOPTED

Applicability Statement 2 - late 1990s

TRANSPORT
HTTP / HTTPS

ENCRYPTION
S/MIME

- Securely sends almost any file type
- Encryption and digital signatures
- MDN receipts confirms delivery
- Heavy use in retail, healthcare & logistics

AS3

FTP-BASED

Applicability Statement 3

TRANSPORT
FTP / SFTP

ENCRYPTION
S/MIME + transport layer

- Handles batch & large file transfers
- Encryption and digital signatures
- No constant direct connection needed
- No built-in MDN confirmation

AS4

NEWEST

Applicability Statement 4 - ebMS

TRANSPORT
Web Services / SOAP

ENCRYPTION
WS-Security

- Web services-based architecture
- Message-level WS-Security controls
- Asynchronous reliable messaging
- Built for cloud & SOA environments

SIDE BY SIDE

Feature Comparison

CAPABILITY	AS2	AS3	AS4
Transport	HTTP / HTTPS	FTP /SFTP	Web Services / SOAP
Encryption	S/MIME	S/MIME + FTP/SFTP layer	WS-Security (message level)
Digital signatures	✓ Yes	✓ Yes	✓ Yes
MDN receipts	✓ Built in	✗ None	✓ Reliable messaging
Asynchronous messaging	Async MDNs	Connection-independent	✓ Native, queued
Batch / large files	Per-message	✓ Strong	Supported
Encryption at rest	In transit	Depends on layer	✓ In transit & at rest
Adoption	Very high	Low / niche	Growing (cloud, ED)
Best for	EDI & compliance	Existing FTP workflows	Modern web & cloud

SECURITY & ENCRYPTION

Same goal, three approaches

AS2

S/MIME encryption

Encrypts payloads with a long, proven track record. Digital signature add confidentiality, integrity, and non-repudiation in transit.

AS3

Encryption + FTP/SFTP

Support encryption and signatures, but much of its security rides on the underlying FTP or SFTP layer - risk grows if configs aren't carefully managed.

AS4

WS-Security, message level

Protects SOAP messages end-to-end even when stored, queued, or routed through intermediaries. Data stays protected in transit and at rest.

For organizations with strict regulatory or compliance requirements, **AS4 often provides the highest level of assurance** - making it the most robust option when encryption and data protection are top priorities.

DECISION GUIDE

Choosing the right protocol

AS2
Proven standard

Pick AS2 for EDI & compliance-driven exchange

Ideal when you need a widely adopted, audit-ready protocol - the default for retail, healthcare, and ligistics trading partners.

AS3
FTP-native

Pick AS3 when FTP/SFTP is already embedded

Works well if your infrastructure depends heavily on FTP or SFTP and you need batch transfers of large data volumes.

AS4
Modern & flexible

Pick AS4 for modern web & cloud integration

Best for the businesses wanting a flexible solution that integrates easily with web services, APIs and cloud platforms - with the strongest security.

FINAL THOUGHTS

The right protocol makes a real difference in security, reliability, and efficiency.

Looking to implement or upgrade your security file transfer solution? Reach out to find the right AS2, AS3, or AS4 approach for your business.