Australian Government
Australian Taxation Office

Digital Service Provider (DSP) Operational Framework Review

Operational Framework Review Focus Group – Supply Chain & Payload Encryption

Presented by Diana Porter & Jarrod Wellings

17 November 2020

Overview

Re-cap of 2017 consultation outcomes

2017 supply chain and encryption focus group established principles and outcomes, with controls implemented in 2018.

Encryption 2017 micro focus group consultation

Principles established

- Encryption in transit to be implemented over public or shared network using an ASD approved algorithm.
- Encryption at rest to be applied using ASD approved algorithm or protocol.
- Cryptographic Message Syntax(CMS) to form basis of solution.
- AS4 flexibility of use limited as payload tied to message.
- CMS supports both open source and proprietary libraries.
- Payload encryption maintains integrity between parties via digital signatures.
- Encryption mechanism should be payload and messaging agnostic.

Outcomes from the focus group

Technology exists to support the immediate implementation of:

- Encryption in transit using ASD approved algorithm over public or shared network infrastructure.
- Encryption at rest to be applied at either full-disk, container, application or database level encryption using ASD approved algorithm or protocol.
- New technology solutions are required to support payload encryption.

Supply Chain 2017 micro focus group consultation

Principles established

- Technical solution will seek to balance need for risk mitigation against need for operational effectiveness.
- DSP reads, routes or modifies any sensitive data message must be annotated with DSP's identity and functional role(s) in supply chain.
- DSPs are not responsible for information after it has been securely delivered to an authenticated and authorised customer.
- Supply chain is part of a broader suite of controls, which includes encryption, monitoring, certification of providers.
- Supply chain visibility won't be required where payload level encryption is used.

Outcomes from the focus group

Timelines for design and implementation of these new technology solutions have not yet been developed. Interim solution established and defined functional roles within the supply chain.

Data Collection: Party responsible for the acquisition of data through user interface interaction or APIs.

Data Validation: Party responsible for the verification of data types, structures, formats and/or data values.

Data Integrator: Party responsible for combining data from multiple sources for use.

Data Analysis & Extraction: Party responsible for performing analysis on data to extract a data sub-set or additional derived/calculated data.

Data Transformation: Party responsible for change syntactic representation of data

Data Provider: Party responsible for the payload (which maybe encrypted).

Data Transmitter: Party responsible for the message with the payload (e.g. ebMS3/AS4 transmission).

What are we trying to achieve

There are 2 opportunities to improve ATOs integrity of transactions over our gateways.

1 **Supply Chain Visibility**

Explore compensating controls throughout the supply chain.

2 **Payload Encryption**

Investigate technical solutions and adoption methodology for payload encryption.

1 Supply Chain

What is the current business solution for supply chain visibility

This control seeks to identify entities and annotate their functional roles involved in the transmission of information from the system which generates the payload through to the ATO. This requirement is only relevant when your product or service does not directly connect to the ATO and the payload is not encrypted.

The functional roles within a supply chain are defined as:

- Data Collector: Party responsible for the acquisition of data through user interface interaction or APIs
- Data Validator: Party responsible for the verification of data types, structures, formats and/or data values
- Data Integrator: Party responsible for combining data from multiple sources for use
- Data Analysis and Extraction: Party responsible for performing analysis on data to extract a data sub-set or additional derived/calculated data
- Data Transformer: Party responsible for change syntactic representation of data
- Data Provider: Party responsible for the payload (which may be encrypted)
- Data Transmitter: Party responsible for the message with the payload. (e.g. ebMS3/AS4 transmission).

Evidence requirements

Until a supply chain visibility solution is available, DSPs are required to provide the business details of the participants in the supply chain including:

- Entity name
- ABN
- Service provider role or function

Has this control been effective?

What does the end-to-end supply chain look like

Systems and processes of Authentication & Authorisation (Auth) ♦

Indicator of end user or system driven Auth

User Name and Password	Multi-Factor Authentication	Single Sign On (federated token)
Access Manager	Relationship Authorisation Manager	Business Authentication Manager
Machine to Machine Credential	myGovID Credential	myGov Credential
Cross Entity Authorisation	Cloud Authentication & Authorisation	Whitelisting

Governing controls across the supply chain

IT Information security management frameworks

SSAM	APRA CPS 234	DSP Operational Framework	Gateway standards	Tax agent charter

Legislative controls

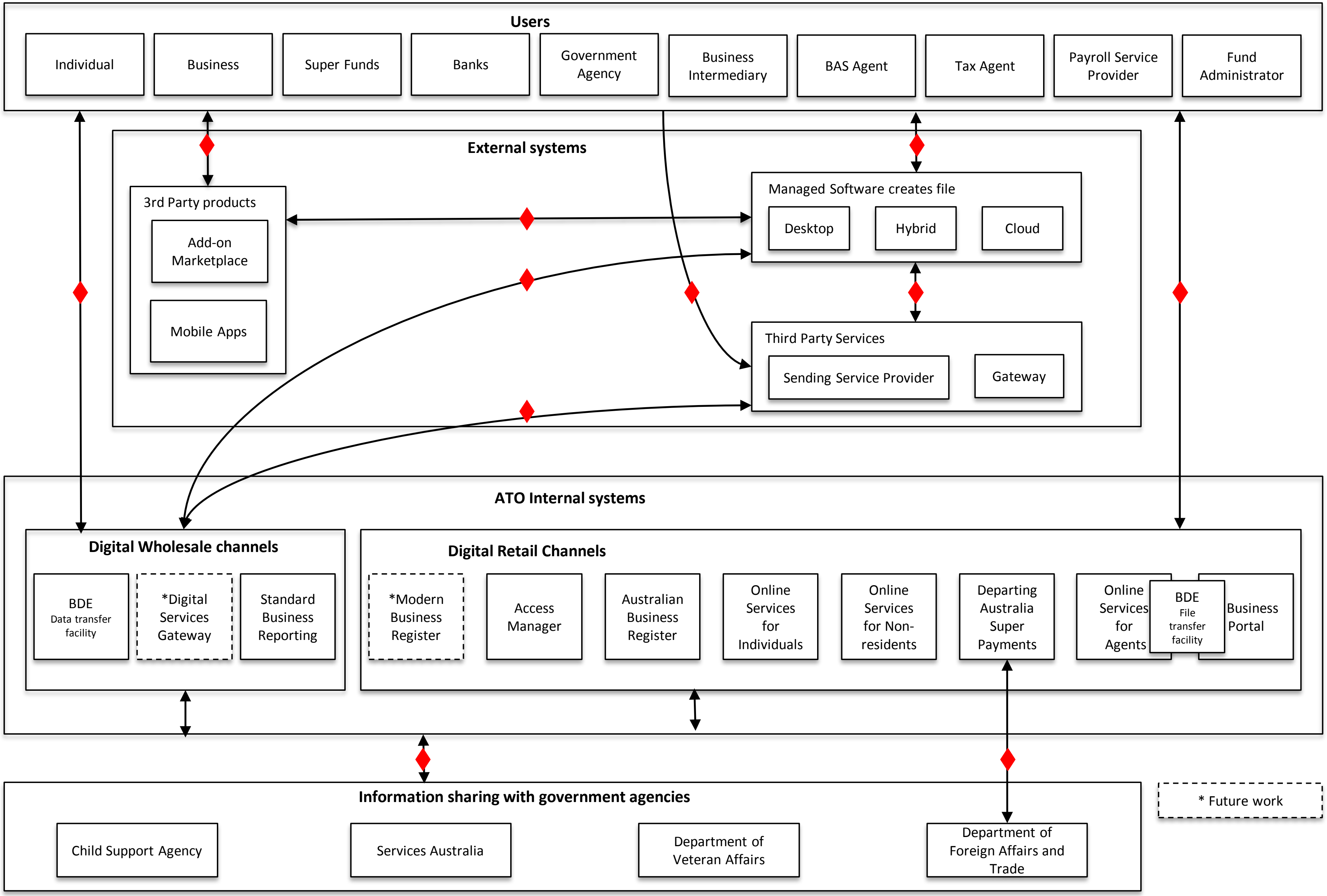
Privacy Act	Tax Administration Act	National Archives Act	Tax Agent Services Act

Anti Money Laundering and Counter Terrorism Financing Act

Superannuation Industry Supervision Act

Technical and non-technical controls

Personnel Security	Data Hosting	Encryption at Rest	Audit Logging
Encryption in Transit (TLS1.2)	KYC	Security Monitoring	Supply Chain



Users

Individual | Business | Super Funds | Banks | Government Agency | Business Intermediary | BAS Agent | Tax Agent | Payroll Service Provider | Fund Administrator

External systems

3rd Party products: Add-on Marketplace; Mobile Apps

Managed Software creates file: Desktop; Hybrid; Cloud

Third Party Services: Sending Service Provider; Gateway

ATO Internal systems

Digital Wholesale channels: BDE Data transfer facility; *Digital Services Gateway; Standard Business Reporting

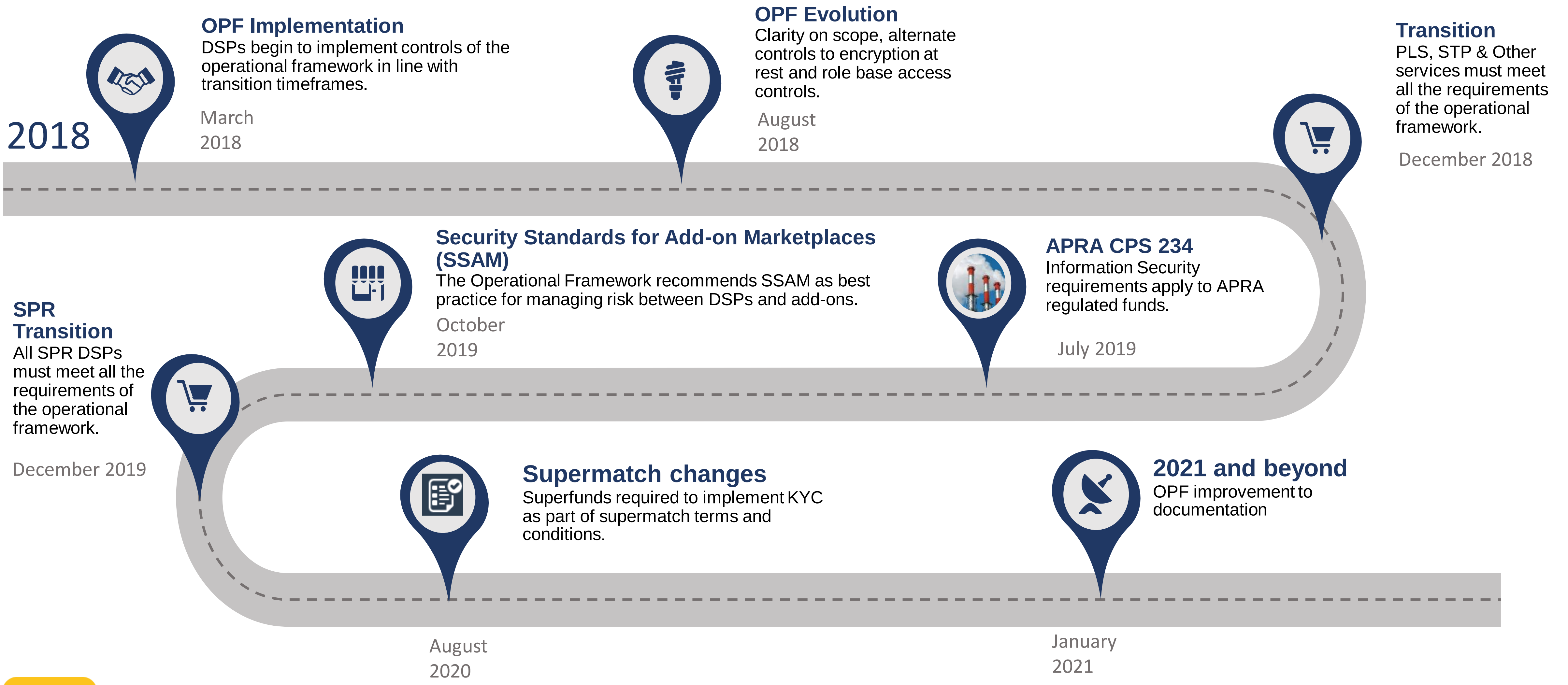
Digital Retail Channels: *Modern Business Register; Access Manager; Australian Business Register; Online Services for Individuals; Online Services for Non-residents; Departing Australia Super Payments; Online Services for Agents; BDE File transfer facility; Business Portal

Information sharing with government agencies

Child Support Agency | Services Australia | Department of Veteran Affairs | Department of Foreign Affairs and Trade

* Future work

How the supply chain has matured over time



2018

OPF Implementation
DSPs begin to implement controls of the operational framework in line with transition timeframes.

March 2018

OPF Evolution
Clarity on scope, alternate controls to encryption at rest and role base access controls.

August 2018

Transition
PLS, STP & Other services must meet all the requirements of the operational framework.

December 2018

APRA CPS 234
Information Security requirements apply to APRA regulated funds.

July 2019

Security Standards for Add-on Marketplaces (SSAM)
The Operational Framework recommends SSAM as best practice for managing risk between DSPs and add-ons.

October 2019

SPR Transition
All SPR DSPs must meet all the requirements of the operational framework.

December 2019

Supermatch changes
Superfunds required to implement KYC as part of supermatch terms and conditions.

August 2020

2021 and beyond
OPF improvement to documentation

January 2021

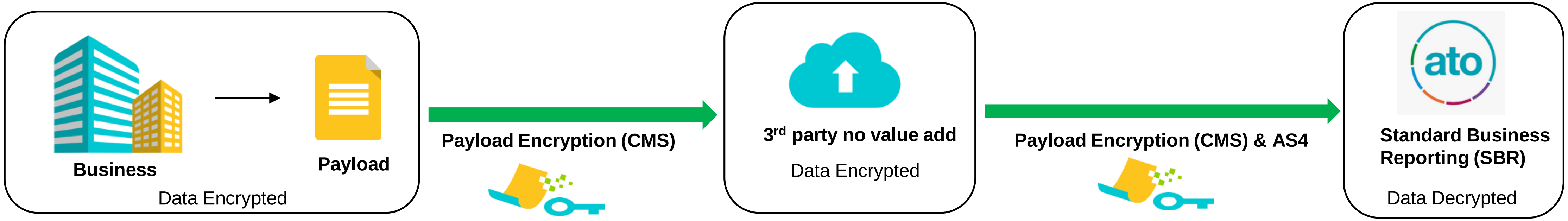
Final thoughts and feedback

2 Payload Encryption

What could payload encryption look like

End-to-end encryption (**E2EE**) is a system of communication where only the communicating users can read the messages. End-to-end encryption is intended to prevent data being read or secretly modified, other than by the true sender and recipient(s). The messages are encrypted by the sender, but the third party does not have a means to decrypt them, and stores them encrypted. The recipients retrieve the encrypted data and decrypts it themselves.

Example of E2EE in place - direct connect



Business

Payload

Data Encrypted

Payload Encryption (CMS)

3rd party no value add

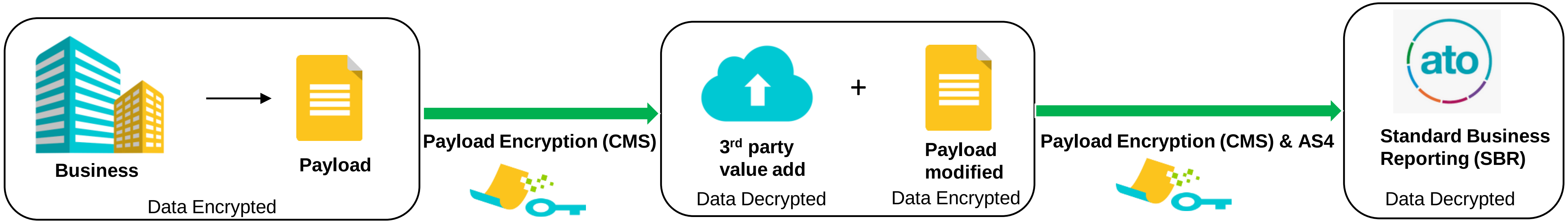
Data Encrypted

Payload Encryption (CMS) & AS4

Standard Business Reporting (SBR)

Data Decrypted

Example of E2EE in place - indirect connect



Business

Payload

Data Encrypted

Payload Encryption (CMS)

3rd party value add

Data Decrypted

+

Payload modified

Data Encrypted

Payload Encryption (CMS) & AS4

Standard Business Reporting (SBR)

Data Decrypted

Benefits, barriers and current risk mitigation in relation to payload encryption

Specific benefits of implementing payload encryption

Data Integrity

Rogue insider

Man in the middle attack

Barriers to implementing payload encryption

Costs of implementation

Where in supply chain to implement

Timing of implementation

Specific controls that mitigate risk of not implementing payload encryption

Encryption at Rest

Personnel Security

Encryption in Transit

Open Discussion

In Summary

- Does our business solution for supply chain been need to be changed?
- Is the risk being managed sufficiently through the supply chain?
- Do we need payload encryption?
- Do we agree that timeframes for, if and when we implemented payload encryption would involve:
    - Risk based decisions
    - Consideration to implement across the supply chain,
    - Utilisation of cryptographic message syntax (CMS)

Next steps