Networks of Software Products

IMPLICATIONS FOR SBR AUTHENTICATION, AUTHORISATION AND CERTIFICATION

Purpose & Scope

Purpose

To recommend an authorisation and relationship model that encompasses all the software products that share functions and capabilities in exchanging data between users and government agencies via SBR; using the interrelationships between the authentication, authorisation, and certification processes.

Scope

- Identify the parties involved in the exchange of data between end users and government agencies,
- Outline how relationships between each party are managed,
- Define the roles and responsibilities of each party involved,
- Identify the issues that exist with the current approach for authentication, authorisation and certification.
- Recommend an approach to manage the issues.

The Problem

The current authentication, authorisation and certification solutions implemented for SBR have revealed the following problems:

1. The approach only caters for linear relationships from end users of business management software to government agencies.

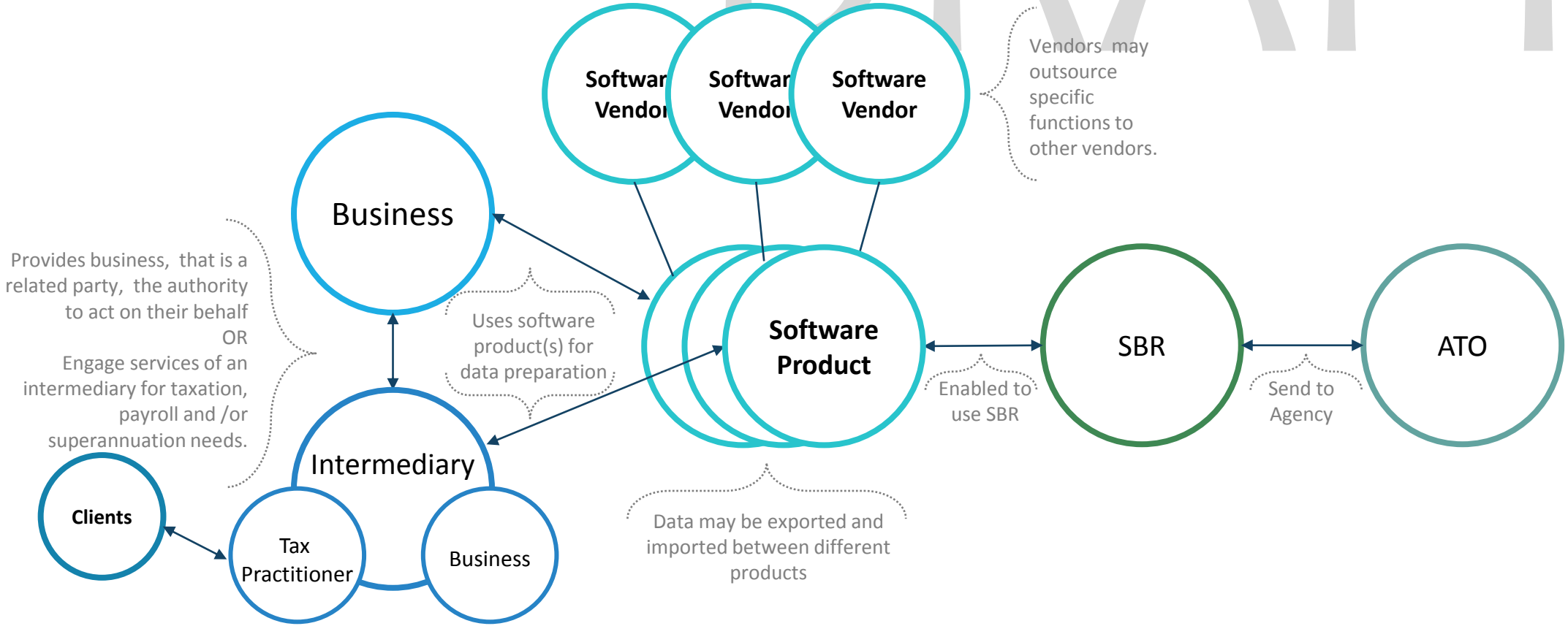
2. The linear approach consequently breaches commercial in-confidence agreements between software vendors in their service offerings.

Expectations of audience

This presentation is intended for an audience with the knowledge and understanding of all the following dependencies in communicating electronically with SBR and the ATO:

- *Tax practitioner and tax payer declarations,*
- *AUSkey; and use of Administrator, Standard and Device AUSkeys.*
- *ATO Access Manager; for managing:*
  - *business and tax practitioner appointments and relationships,*
  - *functional permissions in lodging via SBR*
  - *Cloud software provider appointments*
- *The current 'Cloud Authentication and Authorisation' model in SBR*
- *The current SBR self certification process; involving conformance testing and whitelisting.*
- *(High level understanding of) The ebMS 3.0 / AS4 standard implemented in SBR for SuperStream and PLS.*

Parties involved in the exchange of data…



Managing relationships between parties

Declaration

Tax practitioners must have a signed declaration from their **clients** to act on their behalf.

Tax payer declarations confirming the accuracy of the data being submitted.

Commercial Licence Agreement

A licence outlining services offered between **software vendors** , where one party is the service provider and the other is the service receiver.

Authentication

Identifies the party submitting data to the agency. The party may be either a **business** *or* **Tax Practitioner** *or* **software vendor** .

Authorisation

Verifies lodging party has access to functions/ services;

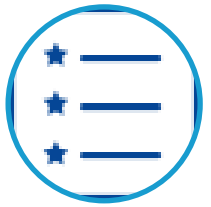
and

Verifies organisational relationships between **businesses**, **tax practitioners** and/or **software vendors**.

SBR Certification

Certified **software products** that meet conformance testing requirements for functions/services offered.

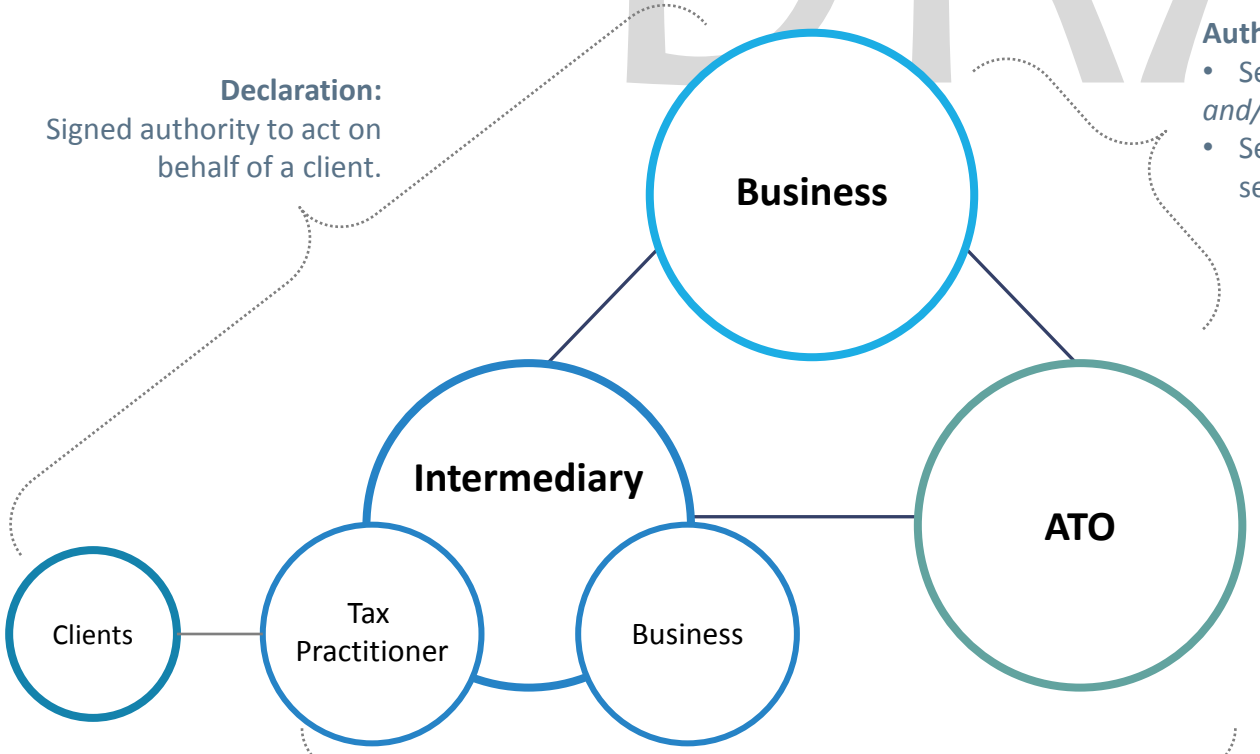
Includes conformance of message format *and* ebMS 3.0/AS4.



SBR Whitelist

Software Product and version is whitelisted per services offered, once successfully certified.

Managing business relationships



Declaration:
Signed authority to act on behalf of a client.

Authorisation:
- Setup business appointments,

and/ or
- Set up permission to access SBR services

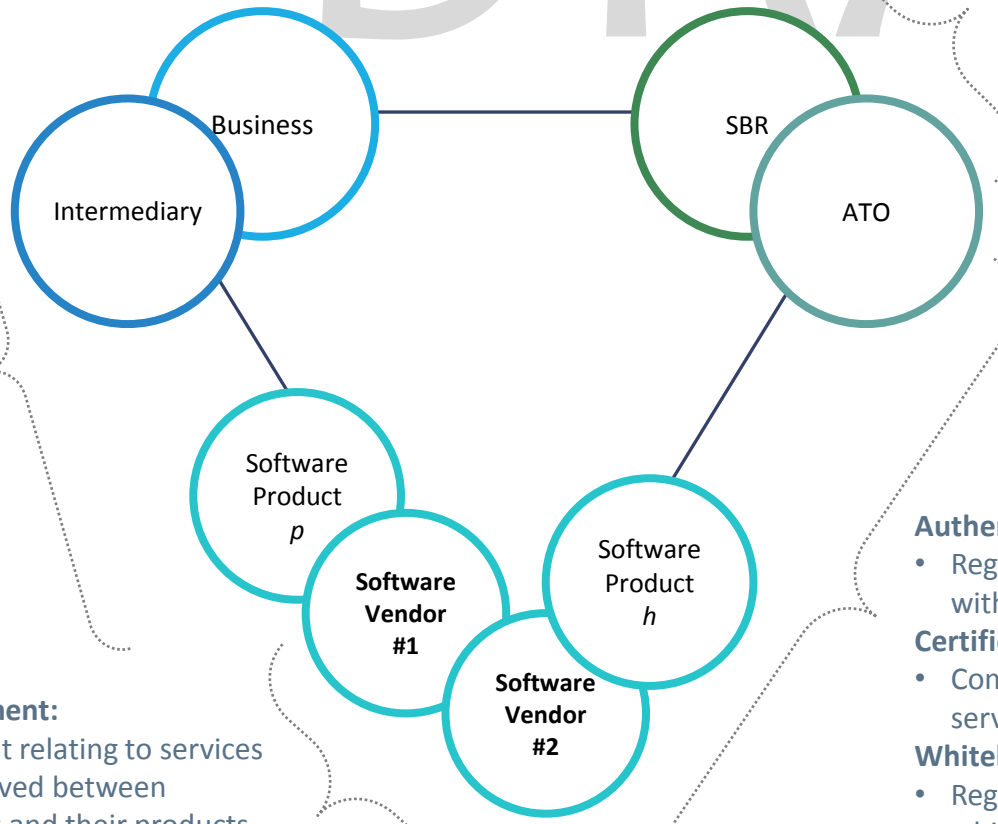
Authentication:
- Identify the lodger of data

Authorisation:
- Verify the relationship between lodger and business (if applicable)

Declaration:
- Confirm accuracy of data supplied

Authorisation:
- Set up permission to access SBR services

Managing technical relationships



Authentication:
- Identify the sender of data (software vendor or business or intermediary)

Authorisation:
- Verify the relationship between lodger and software product (if applicable)

Authentication:
- Setup AUSkey to authenticate submission of data

or
- Appoint software product as Cloud Software provider with ATO

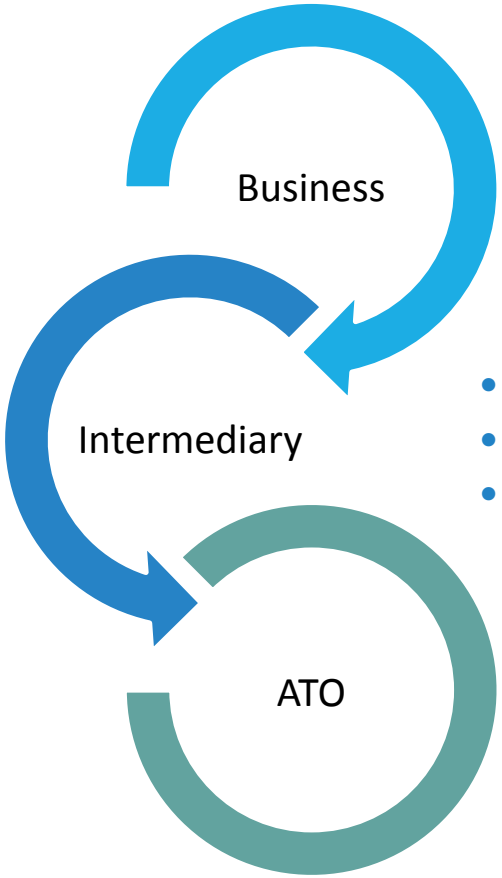
Commercial agreement:
- Signed agreement relating to services offered and received between software vendors and their products.

Authentication:
- Register as a cloud software provider with the Software Vendor's AUSkey

Certification:
- Complete conformance testing for all services offered

Whitelisting
- Register product and version for whitelisting against certified services.

Legal responsibility for supplying data

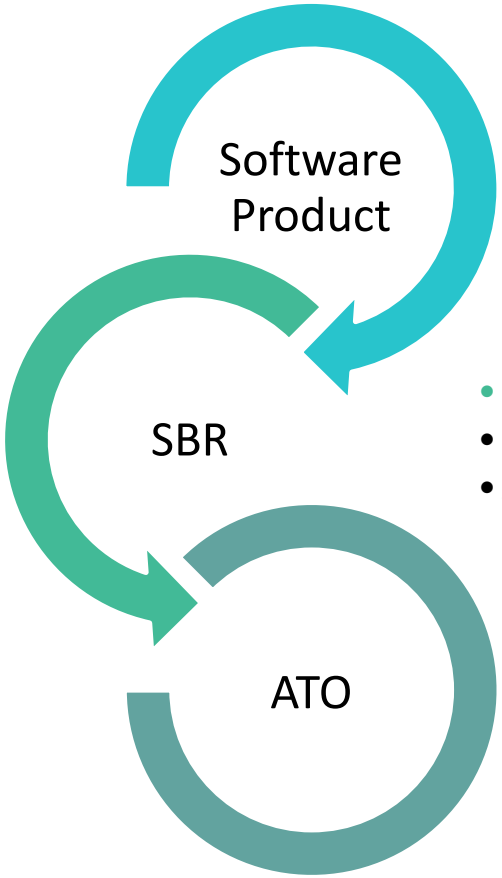


- **Owns** business data
- **Collate** and **prepare** data to meet reporting obligation
- **Endorse** or **declare** accuracy of data being submitted
- **Submit** reporting obligation (or engage services of an intermediary)

- **Collate** and **prepare** data to meet reporting obligation from **client**
- **Declare** accuracy of data being submitted
- **Submit** reporting obligation on behalf of client

- **Receive** and **process** financial information
- Acknowledge receipt of information

Technical responsibility for supplying data

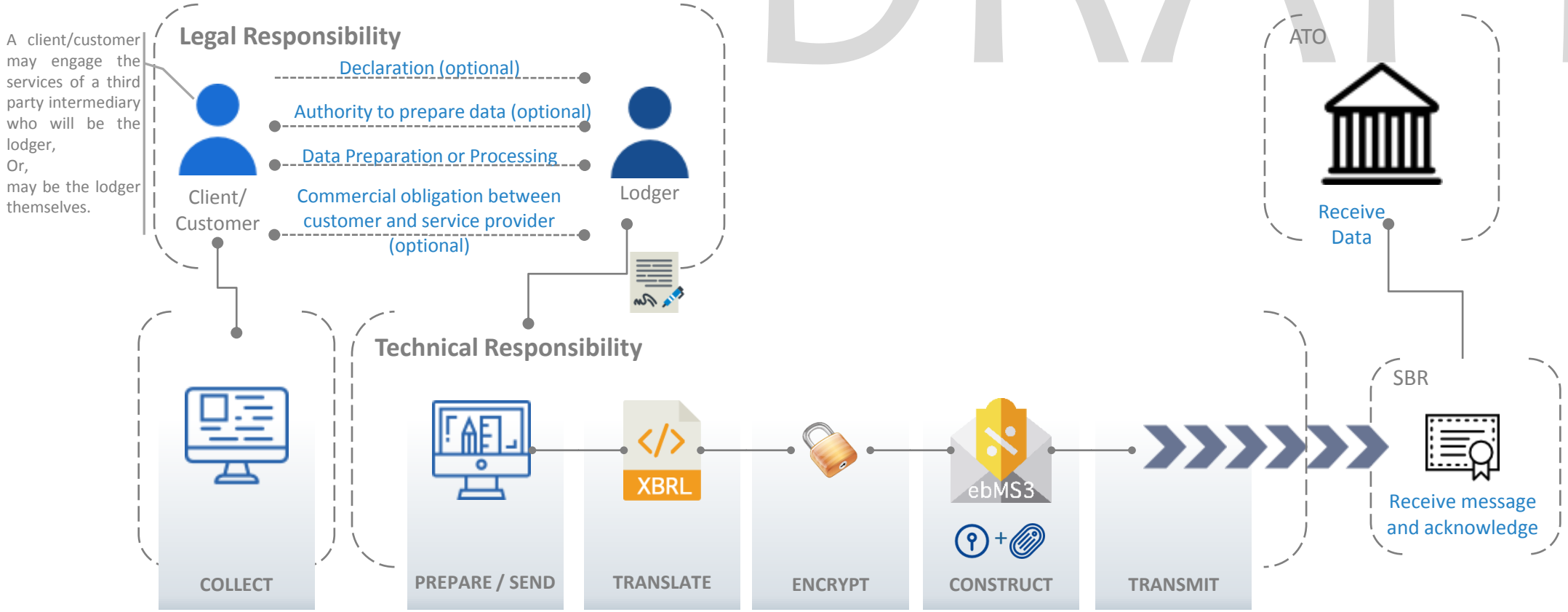


- A **data source**; **Collect** and **collate** data to meet reporting obligation
- **Prepare** and display data report to **declare** for **submission**
- **Translate** data to/from SBR supported message format
- Ensure privacy of data is maintained during transmission, e.g. **encrypt** payload
- **Construct** ebMS message with header and payload
- Securely **transmit** ebMS message to SBR

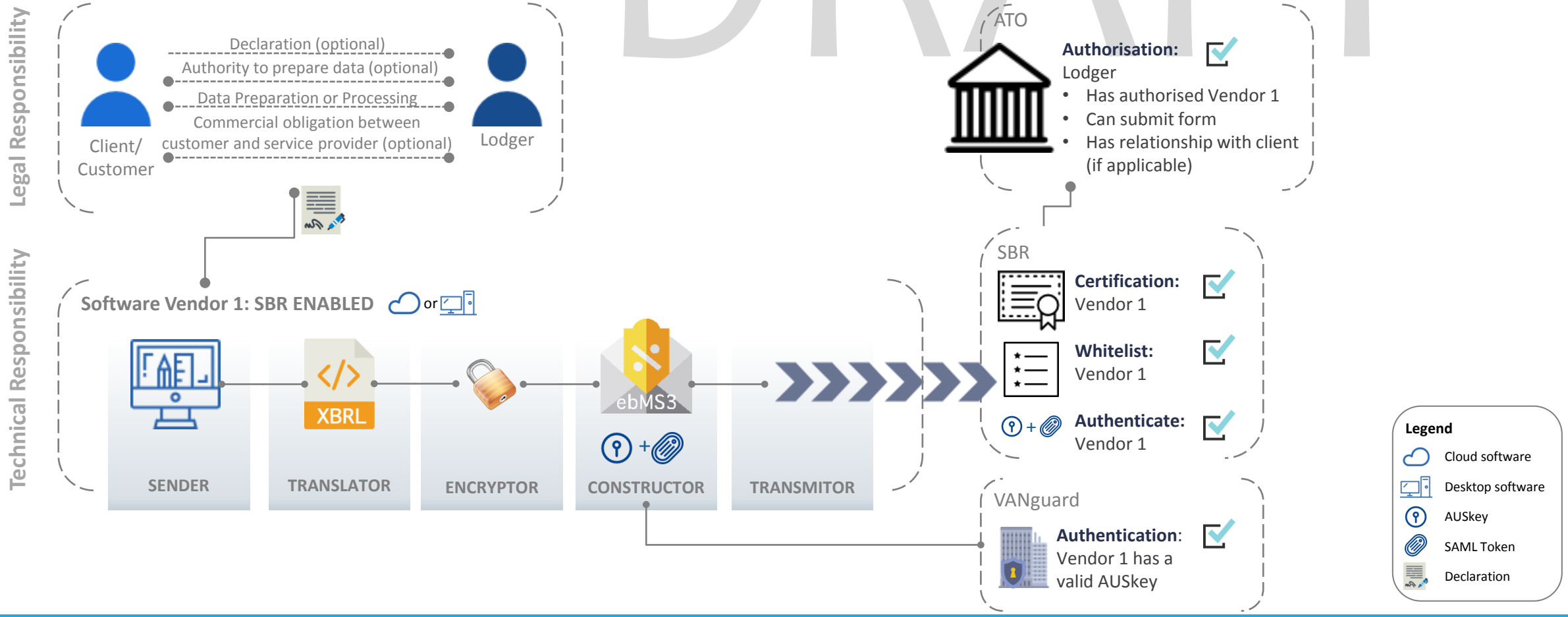
- **Receive** messages from SBR enabled products on behalf of agencies
- Process ebMS header content; Route payloads to agency
- Acknowledge receipt of message

- **Receive** and **process** payload data

A summary flow of data



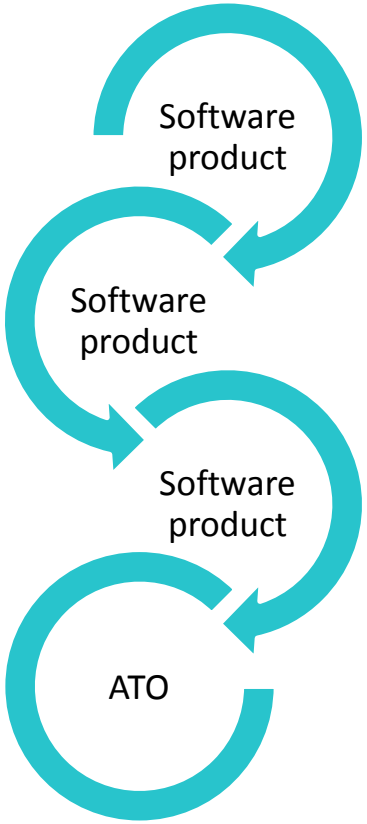
Known Interactions: 1 vendor : SBR



What about multiple vendors : SBR?

THE NETWORK OF SOFTWARE PRODUCTS AND VENDORS

Emerging desire paths



- Software vendors are seeking commercial agreements with other vendors to provide specific functions or capabilities to become SBR enabled.
- Software vendors may choose to provide a specialised service in data preparation and/or processing, or data translation, or data transmission, or a combination of these functions.
  - Through these partnerships, multiple software products, as a collective, can become "SBR enabled".

Roles from Responsibilities

Based on the desire to share services, and the legal and technical responsibilities listed, the following roles have been used to define the steps in the end-to-end exchange of data with a government agency.

How software venders play one or more roles is outlined in the proceeding examples.

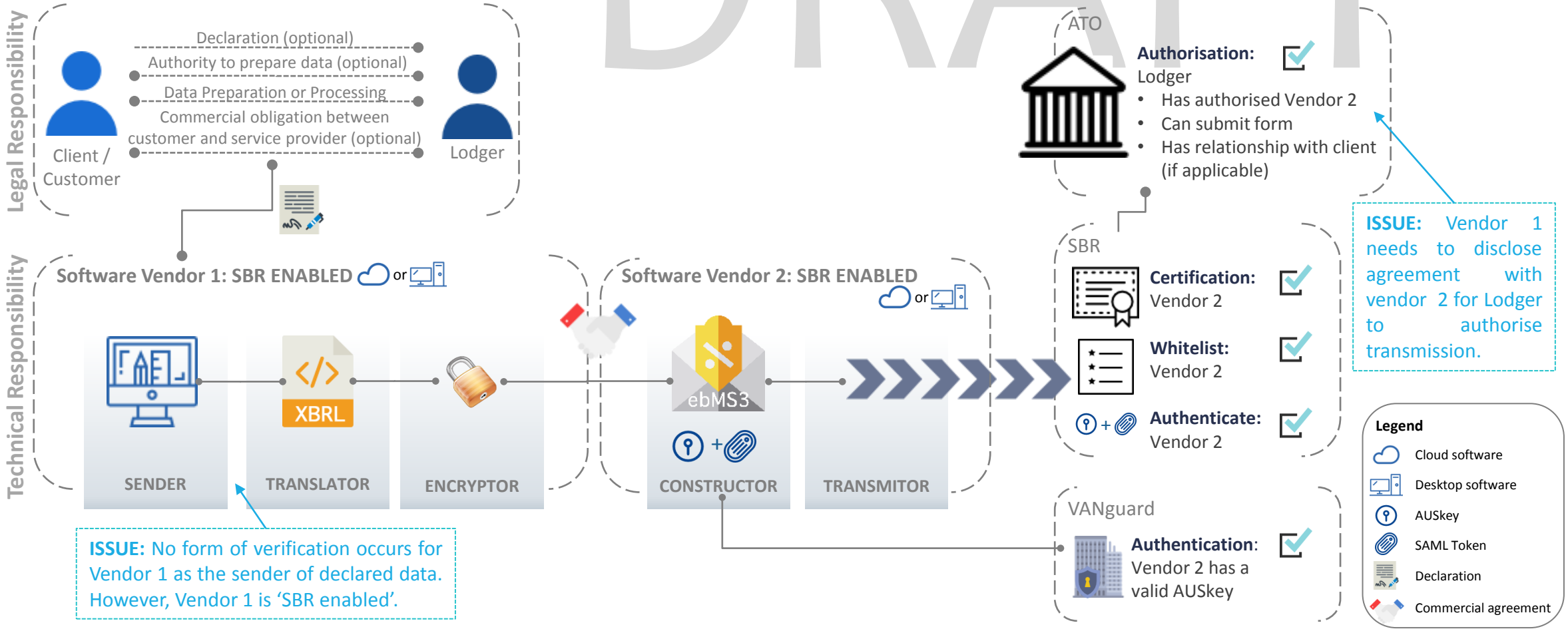
1. **Client / customer**: A business or individual that has engaged the services of an intermediary or service provider to act on their behalf. The client / customer is also the **preparer** of data.
2. **Lodger**: Responsible for ensuring the accuracy of the data being lodged with an agency via SBR. The lodger is also the **preparer** of data and can be an intermediary or the client / customer (e.g. a business).
3. **Sender**: Software product in which the *lodger* has declared the accuracy of the data being lodged. The software product is also a **preparer** of data.
4. **Translator**: Software product responsible for translating data declared for lodgment into an SBR supported format and vice versa.
5. **Encryptor**: Payloads are encrypted for privacy.
6. **Constructor**: Creates the ebMS 3.0 / AS4 header and attaches payload. Also authenticates AUSkey with VANgaurd and attaches AUSkey and SAML signatures to ebMS header.
7. **Transmitter**: Transports ebMS message to/from the agency via SBR.

Assumptions

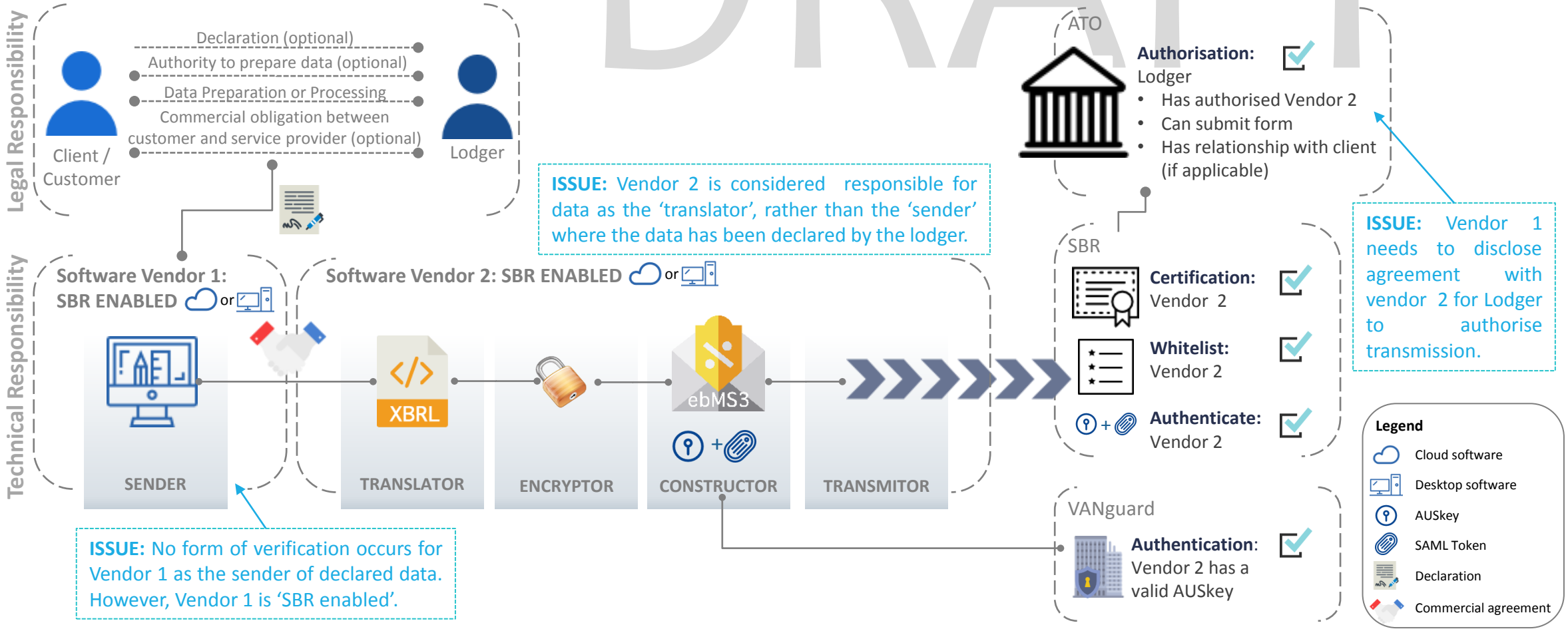
These assumptions apply to the proceeding scenarios and examples:

- *Declarations between client and registered tax practitioner is in place.*
- *Data may be collected from multiple products.*
- *Commercial licences/ agreements between software vendors is in place.*
- *The party defined as the 'constructor' is always required to authenticate with their device AUSkey.*
- *The role 'encryptor' is not currently supported, but has been included to highlight privacy risk,*
- *Future scope: The roles 'translator' and 'encryptor' will be performed by the same vendor.*
- *Where multiple parties are involved in the transmission of data:*
  - *the commercial agreements and integration solutions will manage the retrieval of responses and return transmission to the correct recipient,*
  - *the parties may be in different physical locations,*

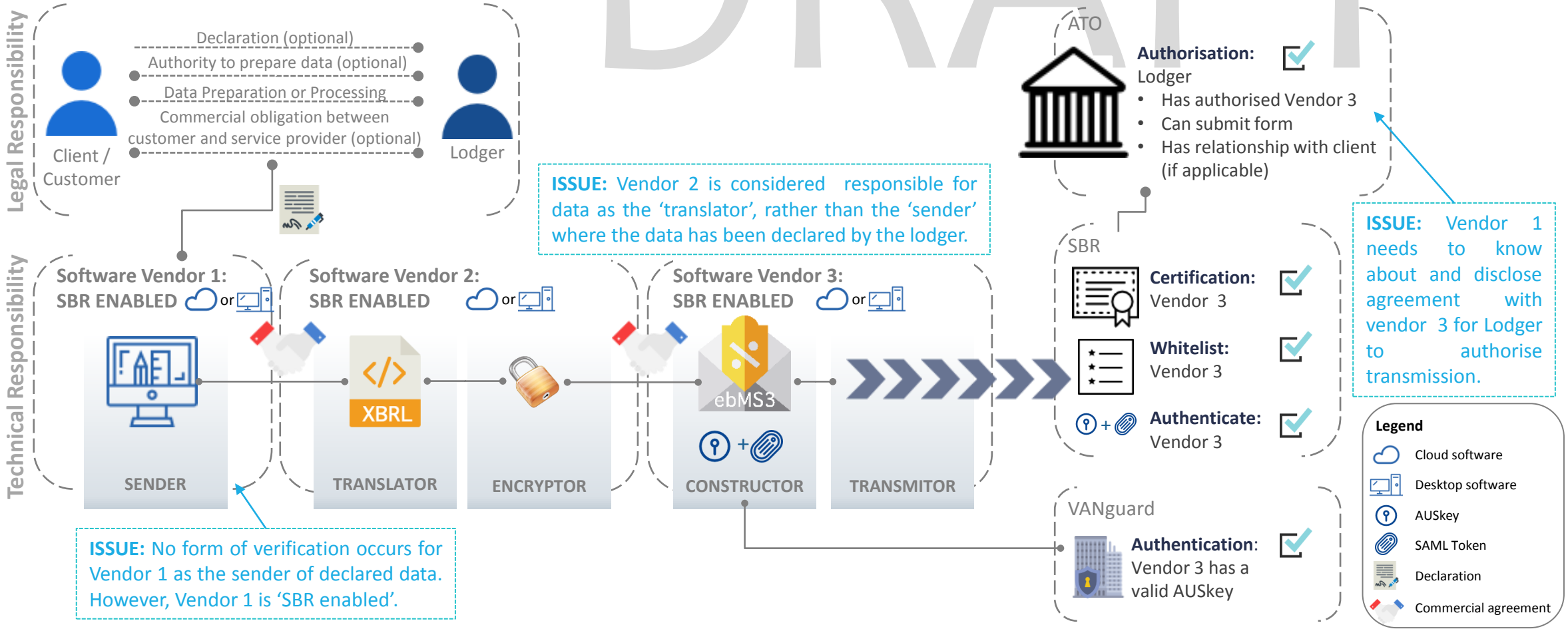
Current State Example 1: 2 vendors, 2 products



Current State Example 2: 2 vendors, 2 products



Current State Example 3: 3 vendors, 3 products



Risks with the current approach

- **Privacy**: data being transferred between multiple parties, possibly in different physical locations, is at risk from identity theft, tampering, and fraud.
- **Technical audit trail**: potentially unable to identify the point where faults occur when multiple products are involved.
- **Authorisation:** *Cloud authentication and authorisation*: the current model only verifies the relationship between lodger and the cloud software provider. It does not include the capability for lodgers to assign or limit software providers to specific services.
  - I.e. once appointed, cloud software providers have authority to transmit all services on behalf of the lodger.
  - When coupled with the above risks, creates another avenue for tampering and fraud.

Recommendation: Mask the commercial agreements between vendors

CREATE APPOINTMENTS BETWEEN SOFTWARE PRODUCTS AND VENDORS

Delegate granular permissions based on roles

A business or tax practitioner assigns permissions to AUSkey holders limiting the service *and* action they can perform when interacting with SBR.

For example, an AUSkey holder can *view* and *prepare* Non-Individual Tax Returns (NITR), but not *lodge* NITR.

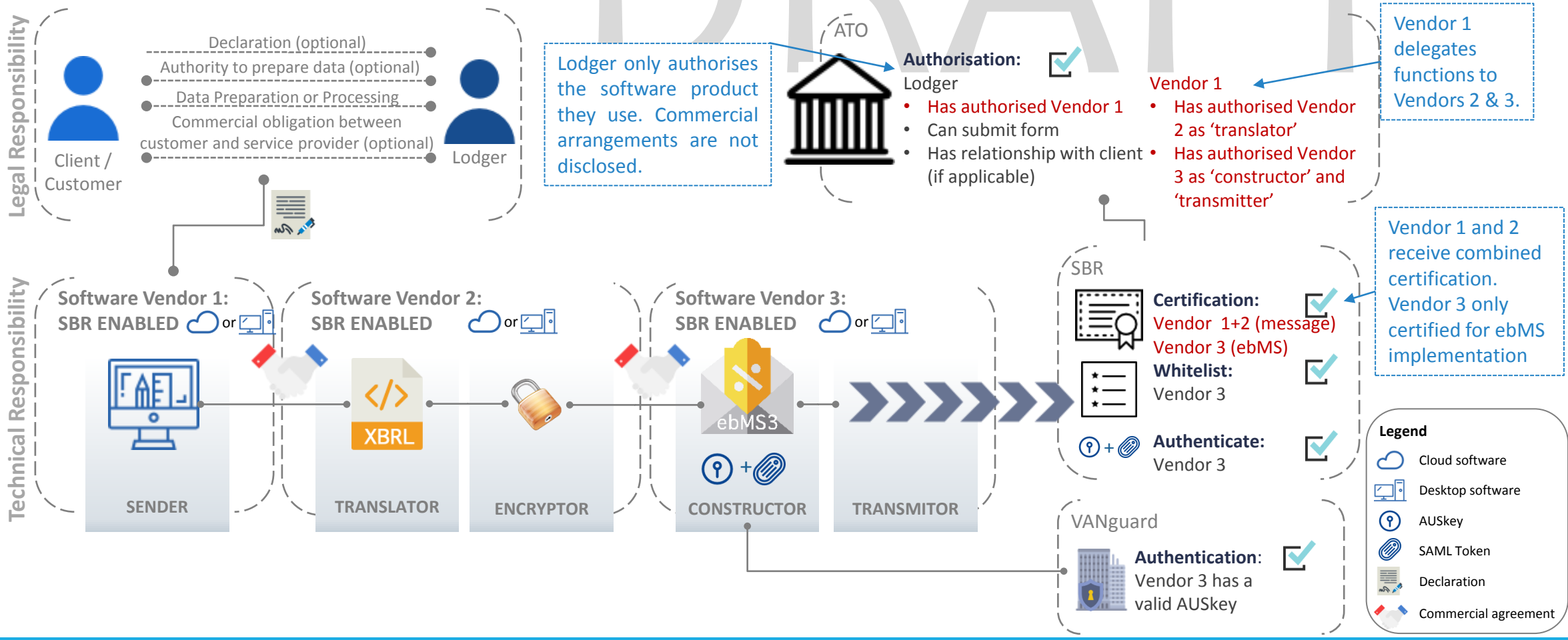
The same concept can be applied to software vendors – the ability for vendors to authorise how their integration partners acted on their behalf when interacting with SBR and the ATO?

- Where permissions are based on the roles mentioned in previous slides, and assigned to vendors who provide the equivalent service,
- This relationship can then be used to streamline the certification and whitelisting requirements to align with the roles performed by each vendor.
  - For example: The 'translator' role will only be required to conformance test against the message format

Authorisation between software products and vendors

Role	Function	Authentication	Authorisation	Certification	Whitelist
'Sender'	Final source of data collation for submission. Lodger declares accuracy of data being supplied from sender.	Identity of 'sender' managed through authorisation, and certification.	Authorised by lodger as a Cloud Software provider	Joint conformance testing with 'Translator' for generation of SBR formatted messaging and handling of responses	N/A
'Translator' + 'Encryptor'	Generate SBR formatted message. Encrypt message before further transmission.	Identity of 'translator' managed through authorisation, and certification.	Authorised by 'Sender' as a 'Translator'	Joint conformance testing with 'Translator' for generation of SBR formatted messaging and handling of responses	N/A
'Constructor'	Construct ebMS 3 / AS4 message	Authenticate Device AUSkey.	Authorised by 'Sender' *or* 'Translator' as the 'Constructor'.	Joint conformance testing with 'Transmitter' for ebMS message transmission and retrieval of responses.	Joint whitelisting with 'Transmitter'
'Transmitter'	Transmit message to target party. Transmit responses to initiating party.	Identity of 'Transmitter' managed through authorisation, certification, and whitelisting.	Authorised by 'Sender' *or* 'Translator' or 'Constructor' as a 'transmitter'.	Joint conformance testing with 'Transmitter' for ebMS message transmission and retrieval of responses.	Joint whitelisting with 'Constructor'

New Scenario 3: 3 vendors, 3 products



Request for comment

ABSIA want to hear your feedback on the topic of authentication, authorisation and certification as an interrelated process.

- Has your industry, and commercial arrangements been captured?
- Are there other risks and issues not yet captured?
- Do you have more suggestions for the recommendation?

Send your comments and feedback to info@absia.asn.au

or start a discussion at forum.absia.asn.au

Resources for more information

- Declarations
  - ww.ato.gov.au/tax-professionals/prepare-and-lodge/managing-your-lodgment-program/client-declarations-and-lodgment-online/
  - ww.sbr.gov.au/__data/assets/file/0014/43511/ATO-Taxpayer-Declaration-Guide.docx
- Authentication
  - www.abr.gov.au/auskey
- Authorisation
  - www.ato.gov.au/General/Online-services/In-detail/Using-Access-Manager/Using-Access-Manager/
  - www.ato.gov.au/General/Online-services/In-detail/Using-Access-Manager/Access-Manager-permissions-for-ATO-and-ABR-online-services/
- Cloud authentication and authorisation
  - softwaredevelopers.ato.gov.au/Cloud_Software_Authentication_and_Authorisation/FAQ
- SBR Certification and Whitelist
  - www.sbr.gov.au/__data/assets/pdf_file/0012/2451/20110411-sbr-self-certification-testing-guide.pdf
- SBR implementation of ebMS 3 / AS4
  - www.sbr.gov.au/software-developers/developer-tools/new-form-pages/ebms-webservice

About ABSIA

The Australian Business Software Industry Association (ABSIA), a Not for Profit Association, was formed in April 2014 to fill a void where an Australian Software Industry peak body should exist. ABSIA

- provide technology thought leadership,
- represent stakeholder opinion,
- help shape technology policies, and
- establish new technology standards.

Our membership currently includes software developers and business service providers from the superannuation, accounting, pay-roll and tax software industry. Our members benefit from collective representation and are a key source of knowledge for government initiatives.

ABSIA members