Whole-of-government Relationship and Authorisation Management Solution

Prepared by:

Trusted Digital Identity Framework project team
Digital Transformation Office
Department of the Prime Minister and Cabinet

Version 0.2 – 18 May 2015

Unclassified

High level overview

INTENT

Implement a whole-of-government authorisation model linked to myGov and the ABR by June 2016, allowing users to nominate others to act on their behalf when interacting across government services (e.g. power of attorney, 'universal' delegations, roles).

DESCRIPTION

This recommendation is for the creation of a whole-of-government Relationship and Authorisation Manager (RAM) solution. Agency on-boarding to this solution will be a subsequent phase. The proposed solution builds upon existing VANguard & myGov authentication systems by allowing access control to be based upon relationships between identities and recording related delegation of functional access. The solution will record relationships specific to access management (regardless of entity type). Agencies will continue to manage the relationships intrinsic to their domain, thus requiring the RAM solution to query those agencies via attribute queries.

CONTEXT

- Identity solutions for Business & Individuals is currently disjoint, making it difficult to provide a seamless experience.
- Agencies have siloed authorisations solutions with legislative & policy barriers to sharing.
- Some agencies assume AUSkey holder has permissions for all agency functions.
- Some transaction require parties to impersonate others.
- Some organisations don't trust their own management of their AUSKey credentials
- Power of Attorney has "legacy" complexities that are not present with nominations from one customer to another

CONSTRAINTS

- A separate interim solution will be provided by Sept 2015 for "individuals in business" to connect ABN to MyGov. This solution will provide the long term solution.
- Need WofG Authorisation solution by June 2016.
- Privacy of individuals & confidentiality of businesses must be preserved.

ADDITIONAL DESIGN CONSIDERATIONS

- Need to recognise industry players (Facebook, Google) are evolving standards based solutions, e.g. OIDC.
- Consider privacy principles around consent and sharing
- Need to consider external systems, processes and environments
- Need to ensure operates in wholesale and retail contexts
- Authentication & Authorisation capability should be consistent across channels
- Authorisation process needs to be simple and information kept current
- Will record relationships & authorisations between any entity type (Individual, Organisation, Device).
- Will leverage existing stores for attribute based queries (where possible)
- Ensure credentials are not automatically elevated
- Need to separate identity level & credential level.
- Trusted 3rd parties may create relationships
- Subject of relationship may not have a credential

KEY STAKEHOLDERS

Department of Human Services
Australian Taxation Office
Department of Industry
and rest of govt. who needs it!!

Lead Agency –ATO

DEPENDENCIES

- Strengthening of Digital Credential (by December 15)
- myGov & VANguard integration
- Agencies will need to modify their systems to be aware of this solution
- Development of Identity Framework
- Adoption requires standardisation of policies & processes for sharing info

ASSUMPTIONS

- The strength of a credential may need to be validated by parties delegating authorisations to it.
- No assumption is required around strength of identity, however, Parties will need to undergo some process to determine if they trust the identity of the delegate.
- Identities and/ or Credentials may be offered by flexible set of accredited 3rd party Identity Providers. RAM should be unaware of Credentials and just use a "link id" supplied by the Identity Hub.
- The WofG Authorisation capability will offer UIs that allows:
  - Customers to create relationships, grant/ request authorisations
  - Agencies staff (e.g. Customer Service Reps) & other trusted 3rd parties (e.g. Tax Agents) to view and create relationships/ authorisations
- To reduce cost of adoption and hence facilitate update (by agencies & 3rd party software developers) the solution will be based on a well accepted standards backed with multiple open source implementations (maybe OpenId Connect).
- The WofG Authorisation capability will offer "common" authorisation & relationship functions (sensitive to context). Complex/ esoteric authorisations will remain with agencies.
- Agencies may seek to internally consume ("dog-food") the authorisations by using it to manage their internal authorisations and delegations.
- All authorisations are established in a context (Parties/ Functionality/ Parties Role & Persona) and have a known end-date (upon which may need to be periodically re-validated). Authorisations may require additional attributes which may result in a step-up in authentication from by transacting party.
- Some relationships automatically create authorisations , e.g. the appointment of a tax agent gives a authorisation to certain tax functions; appointment of doctor gives authorisation to eHealth record. (Nomination v.s. Legal Instrument)
- For some relationships, e.g. Powers of Attorney, there is no "Source of Truth". Currently agencies have their own business processes for verifying & recording such relationship. Also, the actual authorisations granted due to this relationship may be highly contextual (based on jurisdiction & business service).
  - In future state RAM will become a repository in which agencies or delegators may record such authorisation based relationships, together with claims that agency or delegator is able make about that relationship, e.g. Power of Attorney document sighted by non-technical contact centre staff. Over time agencies will need to re-engineer their business processes to exploit the RAM relationships (and the degree of confidence behind that record). Currently there exists obstacles to sharing this info.
- Delegations may be granted to a business and then sub-delegated to a person

CUSTOMERS

Following is an outline of what we know about the potential initial use of a whole-of-government voice authorisation capability:

Australian Taxation Office

Individuals: Aside from Tax Agents (see right), Power of Attorney would be the principle use by individuals. Currently this is only supported by a note of the name.

Business: ATO currently has the Access Manager system for recording authorisations from one AUSKey to another. At the moment Access Manager does not support myGov credentials for businesses.

Tax Practitioners: Tax Agent to their customer's links are recorded in the ATO's Client Register as Client Links. 75% (ish) of tax returns are lodged by Tax Agent's on their customer's behalf. ATO's Access Manager examines Client Links to validate a transaction. Authorisation rules are complex, links to Income Tax role give "god access", links to other roles are limited to the data associated with that role.

Department of Human Services

Centrelink has existing system support for an "Auth Rep" model. It is anticipated that there is a need for approximately 1 million Auth Rep relationships. None of the other master programs have a sufficiently mature system support, the quantified demand for this need is not well understood.

BENEFITS FOR CUSTOMERS

- Faster and easier to establish delegations
- Able to reuse existing WofG credentials – which make those credentials more valuable and worth having
- Greater security of information
  - Provides confidence that only delegated entities are accessing services on customers behalf
  - Avoids the need for delegate to impersonate the end customer
- Easier to move between channels and roles/authorisations
- Easier to tailor the user experience to the Role/Personas (security trimming/ personalisation)
- Ultimately, as part of a whole-of-government service offering it will be easier to do a cluster of tasks across multiple agencies

The desired future experience: selected user pathways

User Pathways

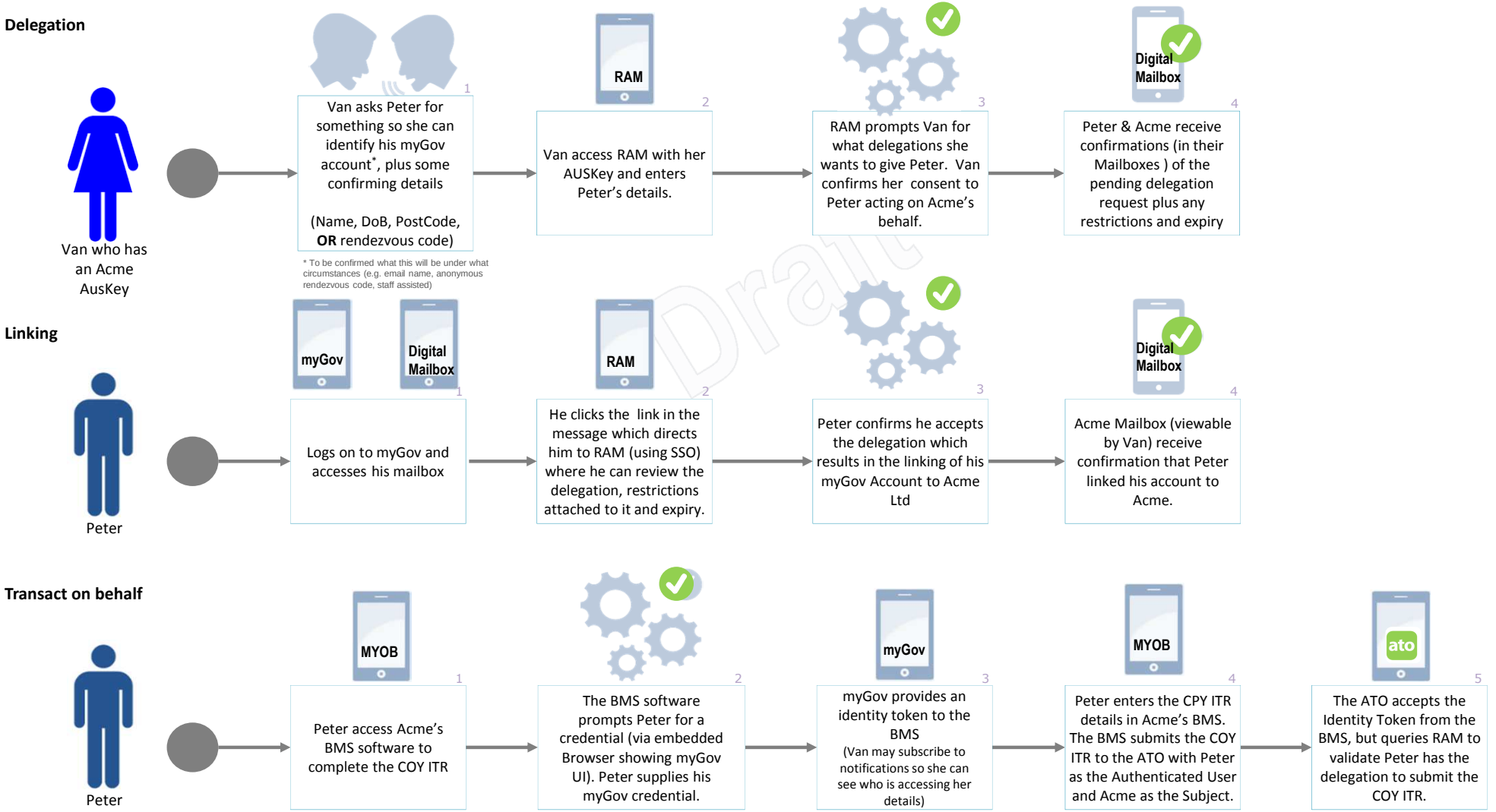
The following six slides illustrate at a very high level selected scenarios. These slides illustrate the pathway from the user's perspective. The information flows between systems are shown later. The selected scenarios are:

- **Business Scenario**: showing an employer/ business owner setting up an employee to act for the business
- **Individual Scenario**: showing a couple setting up permissions for the other partner to act on their behalf
- **Trusted Party Scenario**: showing a tax agent establishing authority to view one of their customer's details
- **Third Party delegator scenario**: showing an authorised government official setting up a delegations
- **Two complex scenarios**:
  - The same third party delegator but where one of the parties doesn't have all the necessary digital identities
  - A merge scenario - someone with multiple credentials only wants to manage their relationships once across all credentials.

The desired future experience: selected user pathways

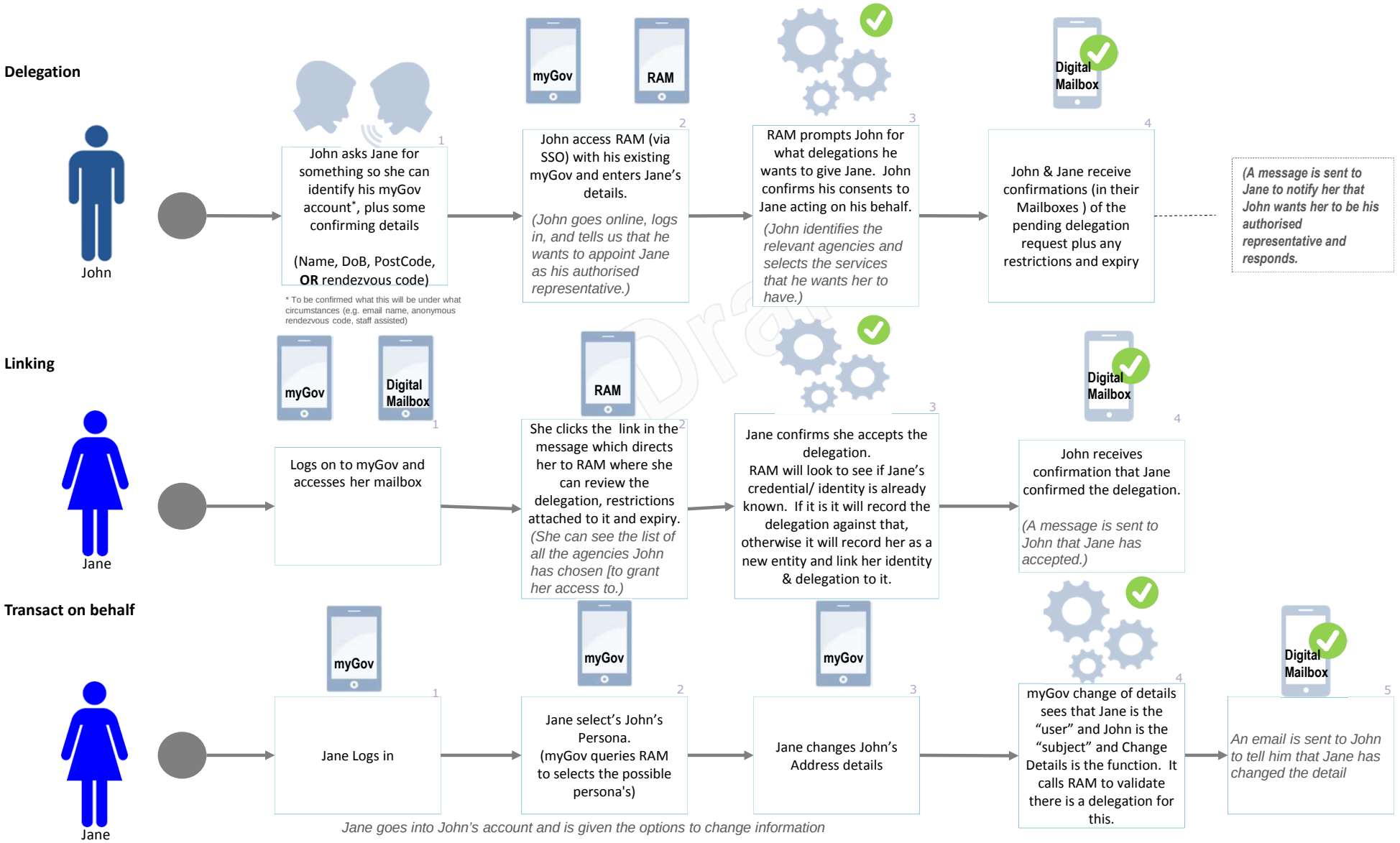
Business Scenario: A business customer (Van who owns for Acme Ltd) chooses to give an employee (Peter) delegation (via his myGov credential) so he can submit the Acme's Company ITR.

The below scenario is for illustrative purposes only and assumes the following pre-condition; that Van has an Acme AUSkey and Peter has a myGov account linked to some service that will allow RAM to validate his Name, DoB & Postcode.



The desired future experience: selected user pathways

Individual Scenario: *A couple forms a relationship and makes a decision that they want to appoint the other person as their representative.*
John goes online, logs in, and tells us that he wants to appoint Jane as his authorised representative.



The desired future experience: selected user pathways

Trusted Party Scenario: *Shane is a small business owner and uses tax agents. He feels his existing tax agent is overcharging so he decides to go to a new tax agent H&R Square. At H&R Square he is met by Peter, a qualified tax agent.*

Delegation

1

Shane meets Peter at the H&R Square offices so Peter can doe his "tax agent thing".

Peter wishes to view Shane's personal & business prefill information, so asks Shane for his myGov ID & ABN so he can set up a relationship. When Shane booked the appointment the H&R Receptionist informed him it would be useful if he could bring his myGov details.

Shane says he doesn't use myGov. Peter offers to assist Shane to set up an account, but Shane declines as he has no intention to interact online, that is what he is paying Peter for.

Peter says it is OK that he doesn't have a myGov credential, but in order for him to act on Shane's behalf he will need to hook into a digital identity. Shane says he is OK using his email address with a digital id, as long as he doesn't need to do anything himself.

2

Peter logs onto the RAM UI and creates two sets of relationships between H&R Square and Shane as well as H&R Square and Shane's business. Peter can use the RAM UI and act on behalf of H&R Square due to a relationship he has to his employer. *(Peter prefers the RAM UI over his practice management UI.)*

Setting up the relationship to Shane's business is easy as Peter can look-up and enter the ABN.

Creating the relationship to Shane is not so easy as Shane has declined to participate in setting up a myGov Account. So Peter creates a "dummy relationship" and enters Shane's TFN.

"Whole Customer Tax Agent" relationship are defined to have a cardinality of 1 for the customer, therefore these new relationships end-date the existing relationships.

3

RAM interrogates the dummy relationship(s) and initiates message to the (myGov) Identity Hub to obtain a RAM Link Id for Shane. This messages will have a context for when the reply is received.

[Note: this needs to be tested with myGov as it is may be perceived that the customer has lost discretion about what myGov links are created.]

4

Shane & Peter receive confirmations (in their Mailboxes) of the approved delegation. Shane has no intention of ever login on to his mailbox. Peter will be able to use this relationship regardless of channel (i.e. he can use this authorisation in agency's call centre to talk about Shane's affairs).

(Little does he know that in 18 months time he uses his email address to recover his myGov username to accesses his mailbox to retrieve NoA info after Peter skips the country. He discovers self-preparing a more delightful experience.)
[Note: is it OK sending this to Shane's mailbox knowing he doesn't have a credential for it?]

Transact on behalf

1

Peter use his SBR enabled practice management software to view Shane's prefill info and prepare Shane's personal & business ITRs. Peter authenticates to H&R Square's cloud based practise management software using that software's proprietary solution. When Peter submits the "prefill" request, the cloud software authenticates itself using a device AUSKey. H&R Square have set up a relationship between it and the cloud based practice management software business. Peter sets up a relationship between H&R $quare and Shane & Shane's Business.

2

When Peter is satisfied with his work he Lodges Shane's personal & business ITRs.

This scenario illustrates where the subject doesn't have a credential recognised by RAM. In this scenario, the subject would be capable of having a credential, but is choosing not to have one. A very similar scenarios exists where due to some limitation (e.g. an older person who is uncomfortable with digital channels) the subject is unable to obtain a credential. How will the subject provide their consent? Possible answers are they visit a shopfront, interact via a call centre, etc. in order to provide consent. This is not an ideal situation the interactions will occur outside the digital channel

The desired future experience: selected user pathways

Third Party Delegator Scenario: *John's widowed mother, Ita, had a stroke and is left in a nursing home unable to make her own decisions. John obtains appropriate powers of attorney though relevant processes. John wishes to update Ita's aged benefit details. John & Ita each have myGov Account. John knows the details for both. Ita has two myGov Accounts, one linked to ATO, Centrelink & Yass Council, the other linked to Medicare.*

Delegation

Legally Authorised Person

Note: It is aspirational that the creation of relationships in RAM would be an integral part of the natural system which establishes the Power of Attorney. It is unlikely that in the near future this process will be re-engineered for this to occur. Therefore, as a stepping stone to achieving this outcome, it is more likely that the documents will be uploaded to some participating agency using that agencies existing document upload workflow systems (or even worse customers may visit shopfronts with the documents). Staff within that agency will view the (uploaded) documents and create the relationships as required. Essentially it is the same user pathway, but with the addition of a workflow step at the beginning to get the documents to the trusted delegator.

1. A "legally authorised person" asks John for something so she can identify his & Ita's myGov account(s)*, plus some confirming details

   (Name, DoB, PostCode, **OR** rendezvous code)

   * To be confirmed what this will be under what circumstances (e.g. email name, anonymous rendezvous code, staff assisted)

2. myGov RAM — A "legally authorised person" logs on to RAM and enters John's & Ita's myGov Ids (plus confirming details)

   This step is repeated for each of Ita's myGov Accounts that are linked to services covered by the PoA.

3. The "legally authorised person" reviews the relevant documents to determine what delegations she needs to give John. She enters these delegations into RAM.

   Again this may need to be repeated for multiple myGov A/cs

4. Digital Mailbox — John &Ita receive confirmations (in their Mailboxes) of the delegation request plus any restrictions and expiry. This delegation is active as the "legally authorised person" has the authority to create relationships.

A confirmation message is sent to Ita's myGov Inbox. This message will not need to be actioned. Given Ita is incapacitated she will probably never see this. John may be monitoring Ita's inbox on her behalf.

Linking

John

1. myGov Digital Mailbox — Logs on to myGov. myGov queries RAM to select the possible myGov Accounts he can select. It defaults to his own account. He accesses his mailbox and reviews the message from RAM.
2. RAM — He clicks the link in the message which directs him to RAM where he can see the delegation & restrictions attached to it. He checks that the delegations & restrictions match his expectations.
3. myGov — John select's Ita's first myGov Account.

   In this scenario Ita has two accounts– one linked to ATO, Council & Centrelink plus another linked to Medicare.)
4. myGov ATO Yass Council Centrelink — John checks the links worked by navigating in turn to ATO, Centrelink & relevant local council portal. He doesn't need to re-logon as myGov provides Single Sign On.

   John didn't need to accept these delegations as 1) he initiated the process through an official process, 2) based on that process the legally authorised person had the authority to create the links.
5. myGov — John returns to myGov, selects Ita's second myGov account(the one linked to Medicare.)
6. Medicare — John checks he can access Ita's Medicare details.

Transact on behalf

John

1. myGov — John Logs in
2. myGov — John select's one of Ita's Account. (myGov queries RAM to selects the possible persona's)
3. Centrelink — John changes Ita's Aged Benefit details
4. Centrelink — The Centrelink change of circumstances function sees that John is the "user" and Ita is the "subject" and "Age Benefit Update" is the function. It calls RAM to validate there is a delegation for this.
5. Digital Mailbox — *An email is sent to Ita to tell her that John has changed the detail. Ita still will never see this email.*

The desired future experience: selected user pathways

Complex Scenario 1: *John's widowed mother, Ita, had a stroke and is left in a nursing home unable to make her own decisions. John obtains appropriate powers of attorney though relevant processes. Ita didn't anticipate her infirmity and so didn't tell John her digital identities she used for Medicare & Centrelink, also, she never linked her identity to the ATO. Thus John's life is more complicated.*

Delegation

Legally Authorised Person

Note: It is aspirational that the creation of relationships in RAM would be an integral part of the natural system which establishes the Power of Attorney. It is unlikely that in the near future this process will be re-engineered for this to occur. Therefore, as a stepping stone to achieving this outcome, it is more likely that the documents will be uploaded to some participating agency using that agencies existing document upload workflow systems (or even worse customers may visit shopfronts with the documents). Staff within that agency will view the (uploaded) documents and create the relationships as required. Essentially it is the same user pathway, but with the addition of a workflow step at the beginning to get the documents to the trusted delegator.

1 A "legally authorised person" asks John for something so she can identify his & Ita's myGov account(s)*, plus some confirming details . John provides his details, but cannot provide Ita's.

(Name, DoB, PostCode, **OR** rendezvous code)

* To be confirmed what this will be under what circumstances (e.g. email name, anonymous rendezvous code, staff assisted)

2 A "legally authorised person" accesses RAM and enters Johns myGov Account (plus confirming details). As John can't provide Ita's myGov details the "legally authorised person" creates a "dummy" relationship(s) and then enters Ita's known agency Identifiers (CRN, TFN, M/C #) against these dummy relationship(s).

3 The "legally authorised person" reviews the relevant documents to determine what delegations she needs to give John. She enters these delegations into RAM against the dummy relationship(s).

4 RAM interrogates the dummy relationship(s) and orchestrates a message between Agencies & myGov. myGov will respond to RAM with an appropriate RAM Link id(s). This will allow the relationship(s) to be created. For the purpose of making this scenario complicated, let's say ATO couldn't definitively identify Ita's record using the supplied details.

5 John (& Ita) will receive notification from RAM indicating relationships have been created enabling Centrelink & Medicare but not the ATO.

Linking

John

1 John rings the ATO call centre. He uses his voice bio to authenticate himself. He then explains his problem. The CSR explains Ita 's myGov Account is not linked to the ATO. The CSR could generate a link to a new myGov A/c, but if John wants to reuse Ita's existing A/c (and keep her Mailbox history) he will need to do the linking. John opts to link Ita's A/c himself.

2 The CSR uses the RAM Agency UI to review John's dummy links set up by the legally authorised person. The CSR see the "dummy" link with Ita's TFN. The CSR can resolve the multi-match

The CSR generates a link code for John to use to link Ita to ATO.

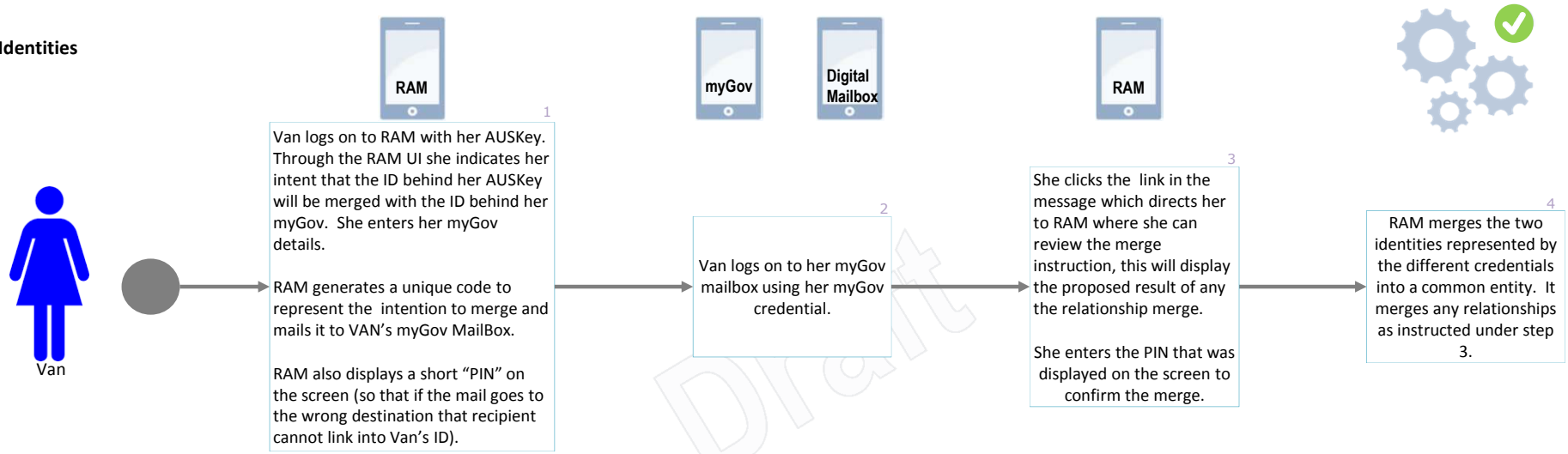
3 John logs on to myGov and selects Ita's Persona. This can be done because of the successful link to Medicare/ Centrelink.
John uses the link code to establish PORO against Ita's ATO record.

4 John returns to RAM and requests it to repeat the interrogation of the dummy record. It sees the ATO is outstanding, sends the message to myGov & ATO. The processes from step 4 onwards are repeated for the ATO link id.

The desired future experience: selected user pathways

Complex Scenario 2: A business customer (Van who owns for Acme Ltd, we met her in an earlier scenario) has decided connect her myGov to her ABN. She doesn't want to maintain her relationships twice under each of these separate identities/ credentials, thus she chooses to "merge" these identities together.

Merge Identities



Terminology

Delegate: entity who will be transacting with government on someone else's behalf. To do so they will need to have been granted authorisation. a.k.a User

Subject: the entity which is the focus of a transaction/ interaction.

Delegator: entity who grants authorisations to other entities to interact/ transact on behalf of a Subject. Examples include:

- Businesses with employees
- Businesses or Individuals with professional representatives, e.g. lawyers, tax agents, doctors. These professional representatives may be businesses or individuals.
- Individuals with relatives who are unable to transaction on their own behalf (say infirmed or travelling or simply due to inconvenience)

Typically the delegator will be the subject customer (or an existing delegate of the subject). However, it may be: a court determining a person is incompetent, it may be another employee who has been given delegation authority, it may be a member of a trusted group (e.g. doctor or tax agent) who is trusted to delegate specific authorisations to themselves.

Registration Authority (RA): a known & accredited organisation/system which is trusted to provide identity information about entities.

Credential: Data presented as evidence of the right to use an identity or other resources.

Credential Service Provider (CSP): an organisation which provides a credential –based on an identity from an RA. Some organisations will do both: Registration Authority (RA) & Credential Security Provider (CSP) functions.

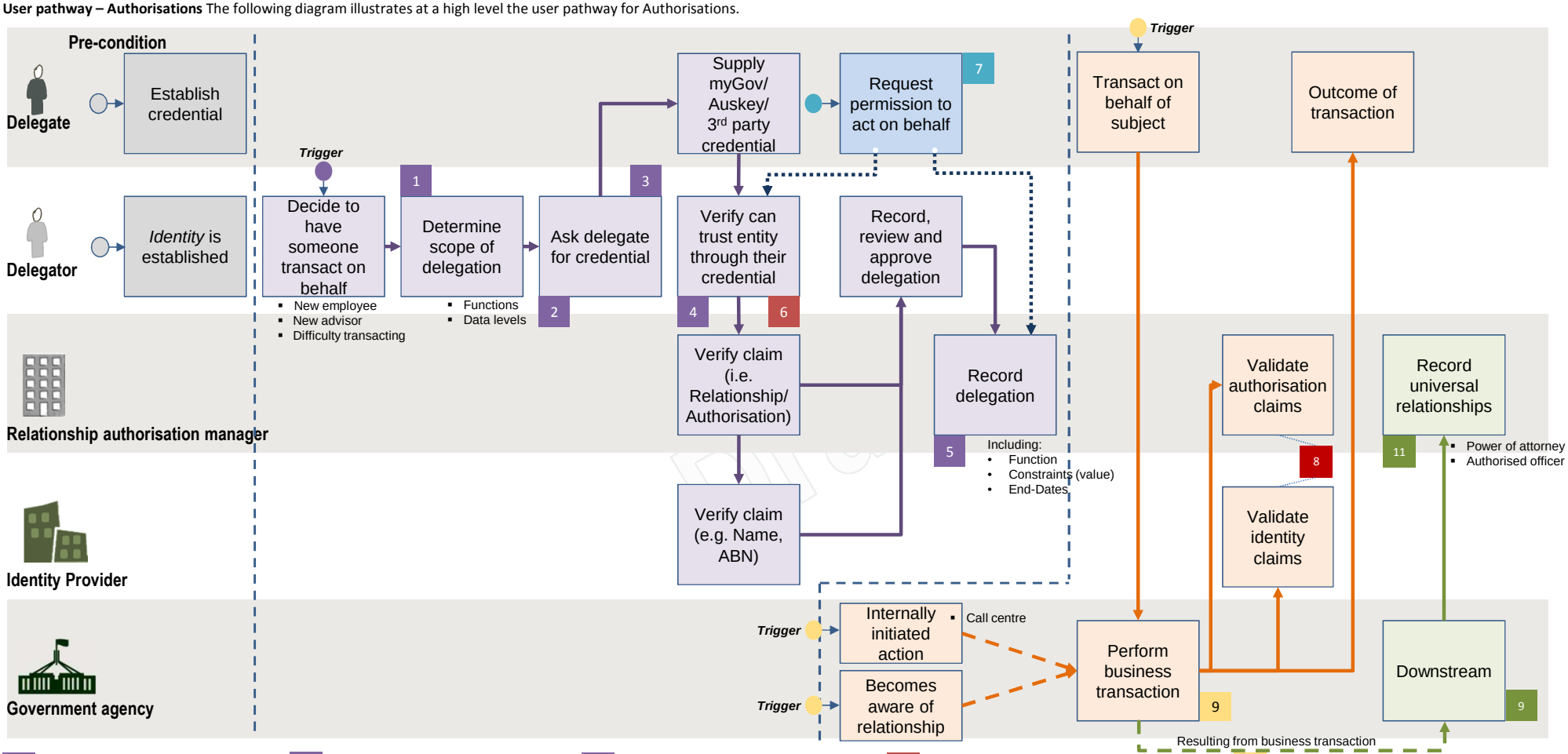
Single Sign On (SSO): This is the ability to sign-on (log on) to one site (e.g. myGov) and then allow the user to interact at another site (e.g. RAM) based on the subsequent sites having a relationship and trusting information supplied from the first site.

Business Management Software (BMS): It is common for businesses to use software products (such as accountancy software) to transact with government. This is also sometimes generically referred to as wholesale services (as opposed to a Portal or Government App which is considered a retail offering).

High level process map

Relationship and authorisation Management - User Pathways

User pathway – Authorisations The following diagram illustrates at a high level the user pathway for Authorisations.



1 The delegator will need to decide what functions they wish to have done by someone else. They will also need to decide what limits to that function (only on certain topics, only for transactions below certain value).

2 In order to be able to operate digitally the Delegator will need a credential

5 All relationships/ authorisations have an end-date

3 In order to grant the delegation the delegator must know who to give that delegation to. It could be as simple as asking the (to be) delegate for their myGov user name/ AUSKey distinguished name for subsequent selection when using a RAM User Interface. It may also require capturing additional claims from the (to be) delegate, e.g. the ABN of the Tax Practice they (claim to) work for.

4 How can the Delegator know to trust this credential (and hence the underlying entity)? It may be necessary to insist upon certain claims to be associated with the credential, e.g.

- the delegate works for an ABN
- The delegate has the expected name, DoB & Postcode or other shared secret
- it is secured by a second authentication factor such as One Time Password

This is going to take community education.(e.g. only trust validated ids)

6 How do we avoid this becoming a phishing mechanism.

7 Not all subjects will have the capability or willingness to operate digitally. Some of these will need to go down the digital assistance path. Others will be helped out by the delegate being trusted to grant authorisation to themselves.

8 These solution will become a honey-pot for attack.

9 When performing any non-self-service business function, in addition to validating the identity, the Agency will need to check any authorisations claims.
Contacts through call centres is an example of this.

9 A downstream outcome of a business transaction may be to record a relationship in the WofG Solution.

11 Relationships will be either nominations or legal instrument.. Bus Processes will need to be modified to allow WofG Usage.

High level data/information flow

The following slides expand upon the high level user pathways shown above to begin to describe how the various systems collaborate to support the user pathway. The selected scenarios are:

1. An Employer using VANguard to link an Employee using myGov
2. An Employee using myGov accessing focused business functionality
3. One partner in a relationship linking to the other partner
4. One partner in a relationship Acting on behalf of the other partner
5. A trusted tax agent setting up relationship to their customer
6. A tax agent using the relationship to view customer details
7. A trusted government official setting up relationship/ authorisation between two individuals
8. A carer using a 3rd party established relationship/ authorisation to act on behalf of another
9. Same as 7 but with the extra complexity of missing identities

High level data/information flow

Flow 1 - *Link an Employee via myGov*

1. *An existing representative of a business (Van) uses RAM to create a relationship to an employee's myGov A/c (Peter)*
2. *The employee (Peter) logs on to myGov and then uses Mailbox/ RAM functions to accept relationship.*

Linking – Employee via myGov (note: this is not self-service) – June '16

VANguard

Employer (VAN)

Login

VANguard supplies a RAM Link Id (ABN + Person ID)

Core RAM

Verify Van can act-on-behalf of Acme

Create Relationship/ Authorisation

Consent to links

Activate Link

Core Mailbox

myGov supplies a RAM Link Id for Peter based on info Van enters into RAM

Message advising new Relationship/ Authorisation

employer

Message advising new Relationship/ Authorisation

employee

Read message & follow links

Obtain RAM Link Id for Peter

Logon

Employee (Peter)

Some Agency

Retrieve attributes relevant to relationship type being created

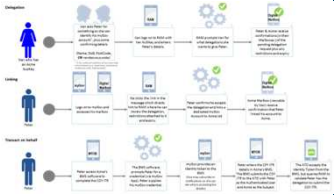
RAM will need to be configurable to only allow certain types of relationships to be created if some attributes exists (e.g. delegate is a doctor) or doesn't exist (e.g. delegator doesn't have an administrative court order declaring unable to manage own affairs). RAM will need to access "truth stores" held in other agencies to determine these attributes.

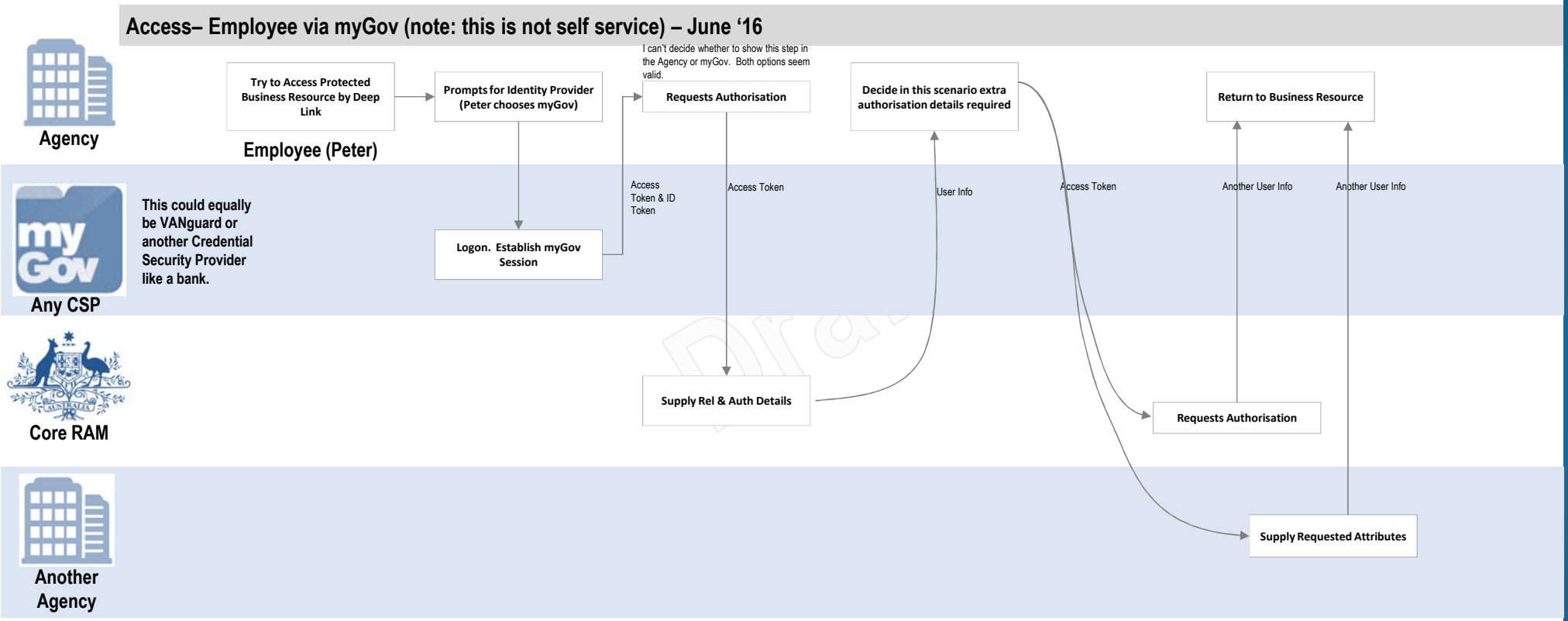
Respond to establishment of new Relationship/ Authorisation

High level data/information flow

Flow 2 - *An Employee (Peter) logs on via myGov to transact on behalf of a business*

1. *An employee lands in an agency service (after a google search) which forwards to myGov for logon*
2. *The employee logs on using myGov which uses RAM to inform the Agency the employee can represent the business*
3. *The Agency may make additional calls to RAM for more details about the relationship should the business function need that additional info*





High level data/information flow

Flow 3 - *John & Jane form a relationship and John delegates management of his Govt. functions to Jane*

1. *John access RAM through myGov and creates a delegation to Jane*
2. *Jane logs on to myGov and then uses Mailbox/ RAM functions to accept relationship.*

Linking – Partner grants access via myGov/ RAM – June '16

Core RAM

Specifying: Who, What (type of relationship/ authorisation), Restrictions (functions, limits {when, limits}), Expiry

Create Relationship/ Authorisation

If RAM has never seen John before it will have to create him as an entity within the system.

If RAM has never seen Jane before it will have to create her as an entity within the system.

Consent to links

Activate Link

myGov ensures individual customers do not have a common identifier across all agencies. Thus RAM is going to need honour a preference from the customer whether they wish the relationships created to apply to all agencies or not.

Core MailBox

Message advising new Relationship/ Authorisation *(Maybe this isn't needed as John could just read what is on the screen in front of him)*

John

Message advising new Relationship/ Authorisation

Jane

Read message & follow links

myGov

Login

John

Logon

Jane

Some Agency

Retrieve attributes relevant to relationship type being created

RAM will need to be configurable to only allow certain types of relationships to be created if some attributes exists (e.g. delegate is a doctor) or doesn't exist (e.g. delegator doesn't have an administrative court order declaring unable to manage own affairs). RAM will need to access "truth stores" held in other agencies to determine these attributes.

Respond to establishment of new Relationship/ Authorisation

High level data/information flow

Flow 4 - *A partner (Jane) in a relationship logs on via myGov to transact on behalf of their "spouse"*

1. *A partner starts in an agency service which forwards to myGov for logon*
2. *The partner logs on using myGov which uses RAM to inform the Agency the partner can represent their spouse*
3. *The agency may make additional calls to RA for more details about the relationship.*

Access– Change of Circumstances for Spouse via myGov – June '16

Agency

Jane follows a link within a "member service" to a function that requires logon (e.g. records change of circumstances)

System asks Jane who she is going to log on with. Jane selects myGov

Jane indicates the change of circumstances transaction is not for herself but for her partner John

Agency transaction decide in this scenario extra authorisation details required

Because Jane chose to back-date the transaction beyond a year, Agency business rules require a check to see if the "update" authorisation was in place a year ago.

Also, because John is X (lets say foreign national on a 245 visa), and because Jane is updating value Y (lets say the address from rural to metropolitan), agency business rules require confirming attribute Z (lets say Visa Conditions allows work in metropolitan location) from another agency (let's say Immigration).

Apply the change of circumstance transaction

myGov

This could equally be another Identity Provider like a bank.

Logs on. Establish myGov Session

I can't decide whether to show this step in the Agency or myGov. Both options seem valid.

Requests known Authorisation

JWT to establish Agency Session

Return to Agency with Access & ID Token

Access Token

Another User Info Payload

Another User Info Payload

Core RAM

Supply Rel & Auth Details

This might return the known information about Jane that she has a spouse John (thus allowing her to view some of John's details)

Requests Extra Authorisation Details

Another Agency

Supply Requested Attributes

Assume this other agency already has John's consent to supply this detail.

High level data/information flow

Flow 5 - *Shane is a small business owner and uses a tax agent. He feels his existing tax agent is overcharging so he decides to go to a new tax agent H&R Square. At H&R Square he is met by Peter, a qualified tax agent.*

Delegation – Peter (Tax Agent) sets up relationship. – June '16

Core RAM

Specifying: Who, What (type of relationship/ authorisation), Restrictions (functions, limits {when, limits}), Expiry

Create "Dummy" Relationship/ Authorisation

Peter is establishing a link between H&R Square and Shane & Shane's Business.

Peter can act-on-behalf of H&R Square to create relationships due to a recorded relationship in RAM between Peter & H&R Square.

Peter can link to Shane's business using its ABN as it is public.

Shane is a bit of a luddite and reject's Peter's offer to assist create a myGov Account. Peter creates a "dummy" relationship using a known Agency Identifiers – TFN – in this case as Peter is a TAX agent. The TFN is not stored in RAM, but just used in messages between systems.

Get Shane's RAM Link Id

RAM interrogates the dummy relationship(s) and initiates message to the myGov Identity Hub to obtain a RAM Link Id for Shane. This messages will have a context for when the reply is received.

Activate Dummy Relationship

As Peter is a Tax Agent, he is trusted to create this kind of relationship, hence RAM turns the dummy relationship into an "active relationship" using the supplied RAM Link Id. RAM had no permanent use for the TFN so it never stored it outside of messages. Thus the TNF is forgotten.

Core Mailbox

Message advising new Relationship/ Authorisation

Message advising new Relationship/ Authorisation

This could equally be another Identity Provider like a bank.

Login via accredited CSP

Tax Agent (Peter)

Send message to ATO to find ATO Link Id

Use ATO Link Id to find RAM Link Id

myGov creates an a/c for Shane with profile info supplied by ATO.

It returns a link it to ATO and a RAM Link Id to RAM (supplying the context info provided to it from RAM via the ATO).

ATO will look up its records and finds no Link Id against the Shan's Record.

ATO sends a message to myGov to create a new myGov Account and forward a RAM Link Id back to RAM.

Use TFN to find ATO Link Id

Retrieve attributes relevant to relationship type being created

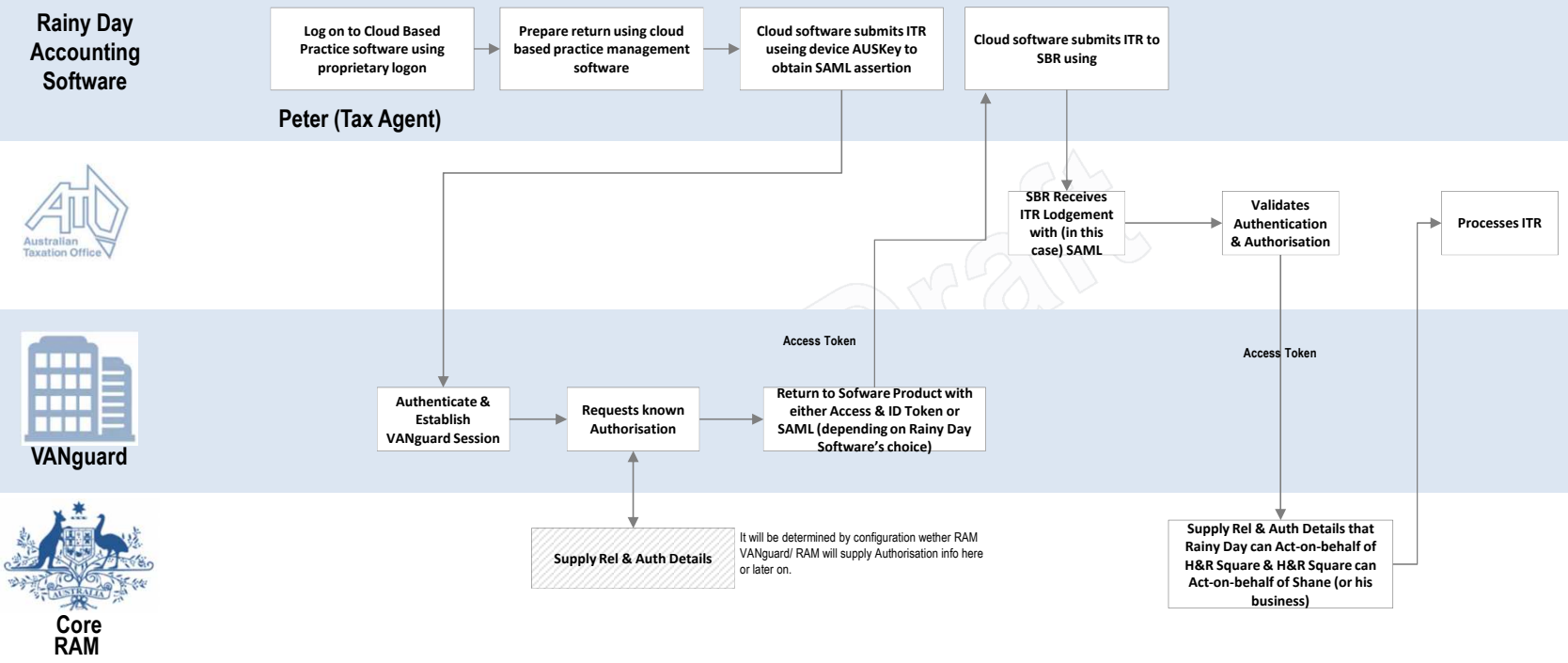
Respond to establishment of new Relationship/ Authorisation

RAM will need to be configurable to only allow certain types of relationships to be created if some attributes exists (e.g. delegate is a doctor) or doesn't exist (e.g. delegator doesn't have an administrative court order declaring unable to manage own affairs). RAM will need to access "truth stores" held in other agencies to determine these attributes.

High level data/information flow

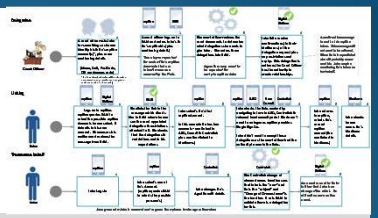
Flow 6 - *Shane is a small business owner and uses a tax agents. He feels his existing tax agent is overcharging so he decides to go to a new tax agent H&R Square. At H&R Square he is met by Peter, a qualified tax agent.*

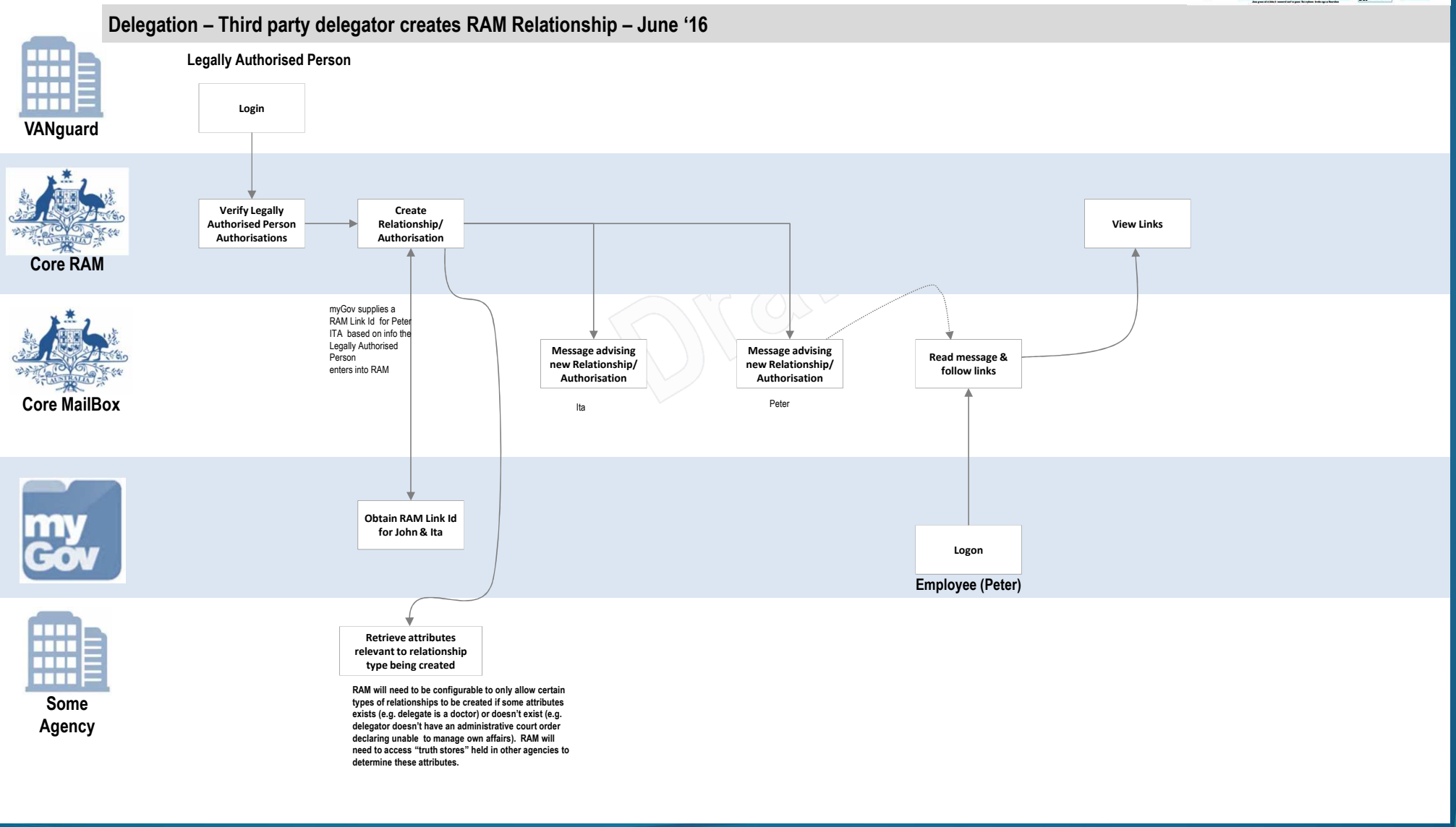
Access– Lodge an ITR – June '16



High level data/information flow

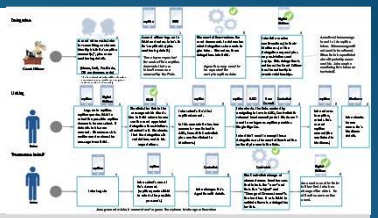
Flow 7 - *John's widowed mother, Ita, had a stroke and is left in a nursing home unable to make her own decisions. John obtains appropriate powers of attorney though relevant processes. John wishes to update Ita's aged benefit details. John & Ita each have myGov Account. John knows the details for both. Ita has two myGov Accounts, one linked to ATO, Centrelink & Yass Council, the other linked to Medicare.*





High level data/information flow

Flow 8 - *John's widowed mother, Ita, had a stroke and is left in a nursing home unable to make her own decisions. John obtains appropriate powers of attorney though relevant processes. John wishes to update Ita's aged benefit details. John & Ita each have myGov Account. John knows the details for both. Ita has two myGov Accounts, one linked to ATO, Centrelink & Yass Council, the other linked to Medicare.*



Access– Peter uses Third Party created delegation to update Ita's Details – June '16

centrelink

John searches google which takes him straight to the Update Age Benefits page in Centrelink

System asks John who he is going to log on with. John selects myGov

System suggests john is Acting on behalf of Ita

Enter & Apply the change of circumstance transaction against Ita's record.

Because prior to logging on John had accessed the Update Aged Benefits function and the system can see that John isn't registered for Aged Benefits, but that he can act on behalf of Ita who is eligible, the system prompts John to Act on behalf of Ita.

myGov

This could equally be another Identity Provider like a bank.

Logs on. Establish myGov Session

Requests known Authorisation

JWT to establish Agency Session

Return to Agency with Access & ID Token

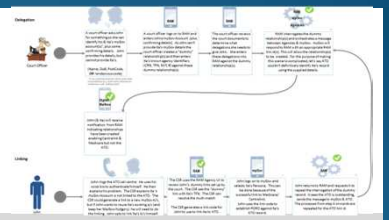
Core RAM

Supply Rel & Auth Details

This might return the known information about John & Ita

High level data/information flow

Flow 9 - *John's widowed mother, Ita, has had a stroke and is left incapacitated in a nursing home. John obtains appropriate powers of attorney though relevant processes.* ***Ita didn't anticipate her infirmity and so didn't tell John her digital identities*** *she used for Medicare & Centrelink, also, she never linked her identity to the ATO. Thus John's life is more complicated.*



Delegation – Third Party Delegator Sets up relationship with unknown myGov IDs. – June '16

VANguard

Core RAM

Core MailBox

myGov

centrelink

Australian Taxation Office

Legally Authorised Person

Login

Specifying: Who, What (type of relationship/ authorisation), Restrictions (functions, limits (when, limits)), Expiry

Create "Dummy" Relationship/ Authorisation

Legally Authorised Person is establishing a link between John & Ita.

As John can't provide Ita's myGov details the Legally Authorised Person creates a "dummy" relationship(s) and then enters Ita's known agency Identifiers (CRN, TFN, M/C #) against these dummy relationship(s).

Get Ita's RAM Link Id

RAM interrogates the dummy relationship(s) and initiates message to the myGov/ agencies to obtain a RAM Link Id for Shane. This messages will have a context for when the reply is received.

Activate Dummy Relationship

As the Legally Authorised Person who initially created the link is a trusted, no confirmation process is needed.

Message advising new Relationship/ Authorisaiton

Get Dummy Record Details

Get Ita's RAM Link Id

Activate Dummy Relationship

Same process as before but now going to ATO.

Get Ita's RAM Link Id

Use Clk Link Id to find RAM Link Id then send to RAM

myGov sends to RAM the RAM Link Id corresponding to the Agency Link ID

John

Login & Switch Context to Ita

Record Link

Use ATO Link Id to find RAM Link Id then send to RAM

Respond to establishment of new Relationship/ Authorisation

Use CRN & Details to find Ita's Clk Link Id

Clk will look up its records and finds a Link Id against the Ita's Record.

Clk sends a message to myGov telling it to send the the corresponding RAM Link Id to RAM

Retrieve attributes relevant to relationship type being created

RAM will need to be configurable to types of relationships to be created if some attributes exists (e.g. delegate is a doctor) or doesn't exist (e.g. delegator doesn't have an administrative court order declaring unable to manage own affairs). RAM will need to access "truth stores" held in other agencies to determine these attributes.

Fail to use TFN & Details to find Ita's ATO Link Id

Look-Up details in RAM

Resolve ID issue & Generate Link Id

PORO Ita's Record with Link Code

Use TFN CRN & Details to find ATO Link Id

John rings CSR

Principles & NFR identified during costing workshop

RAM Principles:

Where a relationship (or access based attribute) exists in some existing "truth store", RAM will leverage it via federation.

The goal is not to replicate data into RAM, as that only introduces complexity, instead the goal would be either:

- for RAM to return a reference (URI) to the relying party so that the relying party can directly query the truth store (in a consistent & standards compliant attribute query fashion) using the "authentication token"; or
- for RAM to perform the query to the truth store, possibly in some "one-off" fashion mutually convenient to RAM and the truth store, and for RAM to return the data to the relying party in a consistent & standards compliant fashion

Where no adequate existing truth store exists for some relationship (or access based attribute), it will set up through RAM

- A store would be viewed inadequate if it was unable to meet the non-functional requirements such as availability, throughput, etc.

Non-Functional Requirements

RAM will be a collection of UI/ Data Store/ Processes (collaborations)

The UI will consist of:

- Customer facing ur for setting up relationships
- Agency facing – particularly for small agencies
- Admin UI

There will be a taxonomy of services (relationships & authorisations) that may be granted. This will be determined as a BAU activity of RAM.

There will be a need to adopt suitable interchange standard(s)

Assume 3 different stds to access truth stores

All authorisations requests & responses will need to be audited.

Availability:

Target availability will be 99.99% (based on myGov)

Response:

- 95% will respond within 0.1 sec from time hits firewall to return to fire wall. This 0.1 may be extended by 0.5 sec for each truth store that needs to be hid.
- 98% will respond within 1 second + 0.5 sec for each truth store
- 99% will respond within 5 secs + 0.5 sec for each truth store

Throughput

- Expected volume metrics after 3 years will be based on the formula
- myGov authentications + VANguard authentications times 5 (i.e. a session is expected on average to need 5 RAM queries)

Volumes

- 25 million (20 million individuals + 5 million non-individuals times 10 relationships times 5 attributes)