Operational Framework: Multi-factor Authentication

Digital Service Providers – paper for discussion

Version 1.0 DRAFT for Consultation
Operational Framework - Multi-factor Authentication

Engagement plan and intent:

**Further Develop** an understanding of the key outcomes of the working group (Identity (incl enrolment), credential strength and the timeframes for implementation)

**Develop** and finalise the Multi-Factor Authentication patterns and use cases

**Agree** and finalise position including minimum standards and timeframes

<table>
<thead>
<tr>
<th>Date</th>
<th>Multi-factor Authentication (Focus group)</th>
<th>Broader - Operational Framework Working Group</th>
</tr>
</thead>
</table>
| Wednesday 9th August 2017  | Initial focus group:  
  - What is identity authentication and authorisation (multi-factor)  
  - Know your customer  | Information session - overview of what we need to achieve                                           |
| Wednesday 23rd August 2017  | Monday 28th August 2017:  
  - ATO to issue papers  
  - Focus group to review in readiness for meeting on 31 August 2017                             |                                                                                                                                               |
| Thursday 31st August 2017   | Focus group: use case patterns  
  - ATO - 4 use case patterns  
  - Other considerations  
  - Group to agree on multi factor credential standards                                             |                                                                                                                                               |
| Thursday 7th September 2017 | Focus group:  
  - Discuss and identify timeframe  
  - Finalise requirement for remaining meeting/s (if required)                                      |                                                                                                                                               |
Multi-Factor Authentication - Patterns

The following patterns were established during the initial workshop as the key, high-level end-to-end process/s that are covered by the requirements for Multi-Factor Authentication.

1. As a DSP I am consuming identity, authentication and authorisation solutions as a service.
2. As a DSP I am accredited to provide identity, authentication and authorisation solutions as a service.
3. As a DSP I am providing a multi factor authentication in my software, and my customer is providing me with the authority to transmit.
4. Machine to machine – machine automatically transacting/exchanging data with government or business system)

The patterns will be further explored as part of the next workshop, and the following pages cover use cases for the patterns to show the process from the customer lense.
Use case one - future state experience

Business software purchase (Business owner purchasing a licensed software product from a vendor)

1. The vendor’s online check out process directs me to the identity exchange to authenticate.

2. As I have verified my identity with Government before I use my preferred credential to authenticate with the vendor.

3. The identity exchange prompts me to consent to the release of personal details from my enrolled identity, for vendor purchase process (this includes authorisation attributes).

4. I consent to release the information, my identity is then passed to the vendor in a verified state with the successful authentication result.

5. The vendor’s check out process pre-fills the license registration and account creation for the sale of the software.

6. The check out process is completed and the registered software is ready for use. (Optional). For cloud enabled products, the vendor can automatically create a CAA relationship for the new client.

Based the authorisation attributes received the DSP can determine which ABN entities this license can be set up for.
Use case two - future state experience

Employee accessing software (Authorised employee accessing their employer’s software to prepare and submit the BAS)

1. The software directs me to the identity exchange to authenticate
2. I have verified my identity with Government before and already have a credential. I can choose to use my DSP’s credential offering as my preference for authenticating
3. My identity is verified and the successful authentication result is passed into my software from the exchange (this includes authorisation attributes)
4. I am now in an authenticated session in my employer’s software
5. Based on my authorisations, I prepare and submit the BAS to the ATO via software on behalf of the business I represent

Access can be controlled in software based on authorisation attributes received
Use case three - future state experience

CAA set up & lodgement (Existing user sets up a CAA notification and submits a BAS lodgement via cloud software)

1. I am directed to the identity exchange to establish an identity or authenticate with an existing identity
2. As I have verified my identity with Government before, I use my preferred credential to authenticate
3. Based on my existing relationship to the business I am authorised to represent, I set up a CAA notification in RAM by providing the details my cloud provider has given me
4. I access cloud software by authenticating with the credential I created with my cloud provider
5. Based on my software permissions, I prepare and submit a BAS to the ATO via software on behalf of the business I represent
6. RAM confirms that the appropriate CAA relationship exists between the business I represent and my nominated cloud provider
7. Once the CAA check is completed the lodgement is accepted by the ATO
Use case four - future state experience

Machine 2 Machine (Machine set up to automatically transact/exchange data with government or business system)

1. As I have verified my identity with Government before I use my preferred credential to authenticate
2. Once authenticated the software administrator downloads or exports a PKI credential onto the machine/server and authorises a M2M scheduled transaction
3. The initiating machine software automatically schedules a data (pull/push) request with another system and broadcasts its embedded credential, along with the transaction request
4. The broadcast is routed through the identity exchange where the credential is authenticated
5. The verified and signed transaction is now released by the initiating machine software to the receiving machine
6. The receiving machine (B2G or B2B) receives the verified transaction and processes the pull or push request
7. The data involved in the transaction is either released back to the initiating machine (pull) or processed and stored (push)

For this scenario the assumption is that the business/client has already completed the software set up process of CAA notification if operating a cloud enabled product

For all B2G machine transactions, a relationship authorisation check will need to be performed

UNCLASSIFIED – Operational Framework, Multi-factor authentication
For further discussion in the workshop

Know your customer

The working group has agreed that we need to harden the security in the ecosystem, particularly at the front end.

Part of which, we will be strengthening the ‘Know Your Customer’ capability. This will be covered as part of the workshop.

Level of Assurance (LOA) 3

Users of digital government services need to be able to sign in securely and conveniently to access services and records, and be confident that their data is secure and their privacy protected. Government also needs to be confident that users are who they say they are. Identity assurance is a means of delivering the required confidence to both users and government.

Based on current standards, the ATO is looking to support identity and authentication solution to achieve an overall assurance level 3 (based on NeAF and National Identity Proofing standards.)*

The ATO currently only accepts multifactor credentials equivalent to NeAF Level 3 for individual and business portal services (e.g. AUSkey and myGov +SMS verification credential)