

# Registration and EOI

## What is registration?

Registration is the process of a user being accepted or provisioned into an identity management or credential issuance system. In the case of those applying for a digital credential, it often involves the collection of information from the individual and from systems they are known to. This allows for the positive identification of the individual ensuring that the integrity of the registration process is maintained by providing a high level of assurance that the individual is who they say they are.

## What is EOI?

Evidence of Identity (EOI) information is the information that an individual presents at registration to prove who they are. The EOI required is dependent on the use and the level of trust required.

In Australia, AGIMO (Australian Government Information Management Office) as part of the Department of Finance and Deregulation offers a framework that Government and Commercial bodies can adhere to if they wish.

The AGIMO proof of identity framework classifies documents as follows:

- Evidence of commencement of identity in Australia
- Linkage between Identity and Person (photo and signature)
- Evidence of Identity Operating in the Community
- Evidence of residential address (if not established by one of the above categories)

This allows for the positive identification of the individual ensuring that the integrity of the registration process is maintained by providing a high level of assurance that the individual is who they say they are.

In many organisations, proof of identity is required as part of the on boarding process. Unfortunately, in most cases this induction process is not integrated with sufficient safeguards in order for it to be used for the credential registration.



## What are the benefits?

Ensuring a high level of rigor in the registration process and requiring high levels of EOI allows a high level of trust to be afforded to the identity and credentials that are created as part of the registration process. This allows for a common understanding of the requirements and rigor of the process that has been undertaken by another party. This in turn allows decisions of trust to be made. An example is deciding if an externally created identity is accepted by an organisation when making system access control decisions, based on the certainty that the correct person is in charge of the correct digital credential.

## If I am known to the organisation, why do I have to prove who I am again?

In many organisations, proof of identity is required as part of the on boarding process. Unfortunately, in most cases this induction process is not integrated with sufficient safeguards in order for it to be used for the credential registration process. It is not necessarily the process that is undertaken at induction that is the issue. The problem often lies with the linkage between the induction or HR solution and the credential issuance system failing to provide sufficient safeguards to prevent the potential for identity fraud. To avoid the potential for a weak induction process or a weak link between this and the credential issuance process, it is often necessary to request EOI information again.

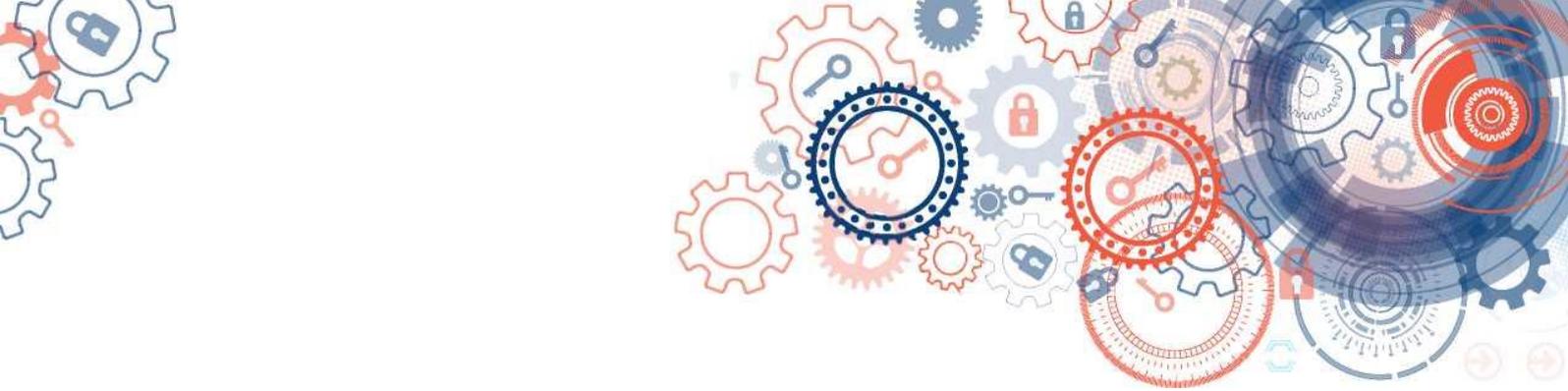
## Are there alternatives to a second registration?

If an organisation does not perceive a threat and the relying parties are happy to accept a lower level of identity assurance, an organisation may use a known customer model. That is that they would accept an individual presenting themselves and use system data as proof of identity.

An alternative approach is to link the on boarding process with the credential registration process. One way this can be done is by the collection of a biometric with the EOI confirmation at induction. This biometric can then be used as a trust or assurance anchor by conducting a biometric confirmation as part of credential registration.

Yet another approach is to use the credential registration process as the front end to other on boarding processes. That is the credential registration process is the first and authoritative source for other systems such as the HR system.





## About Cogito Group

Cogito Group is an award winning Australian owned and operated ICT company specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.



> 54th Australian  
Export Awards  

---

**2016 NATIONAL FINALIST**



**Canberra Office**  
t +61 2 6140 4494  
w [www.cogitogroup.com.au](http://www.cogitogroup.com.au)

**Wellington Office**  
t +64 4909 7580  
w [www.cogitogroup.co.nz](http://www.cogitogroup.co.nz)

 **Cogito Group**