

PLEASE NOTE: THIS POLICY IS A DRAFT AND SUBJECT TO REVISION

05. Acceptable Authentication Assurance Policy

This policy is effective from 20 January 2025.

INTRODUCTION

To protect its assets, the Infrastructure needs to authenticate, identify, and trace Users granted access to its Services. The authentication and identification must be sufficient to meet the requirements of the Security Policy and any ancillary Specific Policies, bearing in mind the nature of data stored within the Infrastructure and the heterogeneous authentication options.

DEFINITION OF APPROVED AUTHENTICATION ASSURANCE SOURCES

CILogon is the platform with which CADRE authenticates users.

See the CILogon details of [What level of assurance does CILogon support?](#) for CILogon's Level of Assurance.

Assurance Profile for CADRE:

1. Should identifiers be unique, personal and traceable? YES
2. Should identifiers be unique across the infrastructure? YES
3. How fresh do attributes need to be? 1 month
4. What kind of ID proofing is required? Low (self-asserted)
5. Is MFA required? SFA currently required

OPERATIONAL MATTERS

Authentication Assurance will be propagated with the user's authentication token for relying services to include in Authorisation decisions.



Only users conforming to one of the approved authentication assurance profiles shall be granted access to the Infrastructure.

Policy Development Kit

Acceptable Authentication Assurance Policy

© Owned by the authors and made available under license:

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Other Sources / Attribution / Acknowledgements: SClv2 from the WISE Community, used under CC BY-NC-SA 4.0. EGI e-Infrastructure Security Policy EGI-SPG-SecurityPolicy-V2, used under CC BY-NC-SA 4.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).



Policy Development Kit was reviewed by the AAF Trust and Identity Pathfinder Policy Working Group, by and for Australian national research infrastructure, enabled by NCRIS.