

Acceptable Authentication Assurance

Peter Solagna

EGI Foundation



www.egi.eu

This work by EGI.eu is licensed under a
[Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Current Acceptable Assurance

- Current policy:
 - <https://documents.egi.eu/document/83>
- Requirements
 - CA accredited to the IGTF Classic Authentication Profile
 - CA accredited to the IGTF Short Lived Credential Service (SLCS) Profile
 - CA accredited to the IGTF Member Integrated Credential Services (MICS) Profile

The Classic profile

- <https://www.igtf.net/ap/classic/>
- Traditional credential authorities issue long-term credentials users who will possess and control their key pair
- These authorities act as an independent trusted third party for both subscribers and relying parties within the infrastructure.
- The identity of the subscribers is vetted through a face-to-face or equivalent process.

New Acceptable Assurance

- The policy has been updated to be less Grid-centric and less X.509 centric
- The assurance level is a combination of:
 - Issuing Authority
 - IT Infrastructure registration service
 - VO registration service
 - VOs user verification can increase the level of assurance provided by the credentials

New assurance profiles accepted

- IGTF Assurance Profile ASPEN (MICS)
- IGTF Assurance Profile BIRCH (SLCS)
- IGTF Assurance Profile CEDAR (Classic)
- **IGTF Assurance Profile DOGWOOD (IOTA)**
 - The CA assures: unique, non-re-assigned identities
 - The CA is not required to collect more data than are necessary for fulfilling the uniqueness requirements
 - Credentials issued by authorities under this profile may not provide sufficient information to independently trace individual subscribers
 - Should be used in conjunction with complementary vetting

New policy applied to the EGI AAI

- EGI AAI is connected to an online CA for the provisioning of X509 certificates
- Users will be able to access X509 credentials through EGI AAI
 - The AAI services will allow only the users with a minimum set of attributes available to access the online CA
- Accessing the HTC and Fedcloud resources with certificates provided by the online-CA will be conditioned by VO Membership
 - The user must have an X509 certificate and (if the credentials are released by the online CA) **be member of a VO that provides additional user vetting**
- A new release of LCMAPS supporting the VO-specific LoA be available in the next UMD release

Timeline for approval

- Please, provide feedback about the new policy by the end of August
- The new version, if necessary, will be circulated at the beginning of September
- Tentative date for approval:
 - September OMB (September 15th)
 - The security policy is a prerequisite to roll in production all the EGI AAI services including the online CA support

Thank you for your attention.

Questions?



www.egi.eu

This work by EGI.eu is licensed under a
[Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).