POLICY ON ACCEPTABLE AUTHENTICATION ASSURANCE

Document identifier	EGI-SPG-AuthNAssurance-V1.0
Document Link	https://documents.egi.eu/document/2930
Last Modified	06/01/2017
Version	1.0
Policy Group Acronym	SPG
Policy Group Name	Security Policy Group
Contact Person	David Kelsey/STFC
Document Type	Policy
Document Status	Draft
Approved by	Body who approved the doc
Approved Date	DD/MM/YYYY

TABLE OF CONTENTS

COPYRIGHT NOTICE

AUTHORS LIST

	Name	Partner/Activity/ Organisation/Function	Date
From	David Groep David Kelsey	Nikhef/SPG STFC/SPG	22/10/2016

DELIVERY SLIP

	Body	***Date***
Reviewed by:	Reviewed by EGI OMB in July 2016 and approved by EGI OMB in Sep 2016	28/07/2016 & 15/09/2016
Reviewed by:		
Reviewed by:		
Approved by:		

DOCUMENT LOG

Issue	***Date***	***Comment***	***Author/Partner***
v1	23/07/2016	New security policy replacing old policy "Approval of Certification Authorities"	David Groep /Nikhef

TERMINOLOGY

A complete project glossary is provided at the following page: http://www.egi.eu/about/glossary/

APPLICATION AREA

This document is a formal EGI.eu policy or procedure applicable to all participants and associate participants, beneficiaries and Joint Research Unit members, as well as its collaborating projects.

POLICY/PROCEDURE AMENDMENT PROCEDURE

Reviews and amendments should be done in accordance with the EGI.eu "Policy Development Process" (https://documents.egi.eu/document/169).

This policy is effective from <DATE> and replaces the earlier policy "Approval of Certification Authorities" [R1]. This policy is one of a set of documents that together define the Security Policy [R2]. This individual document must be considered in conjunction with all the policy documents in the set. All terms are defined in the Glossary [R3].

1 INTRODUCTION

In order to protect its assets, the e-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 long term nature of data stored within the e-Infrastructure and the heterogeneous authentication and identification capabilities provided by the Virtual Organisations (VOs) in verifying user data.

2 INTEROPERABLE GLOBAL TRUST FEDERATION (IGTF)

The e-Infrastructure endorses the work of the Interoperable Global Trust Federation (IGTF) [R4] as a body to establish common policies and guidelines that help establish interoperable, global trust relations between providers of e-Infrastructures and cyber-infrastructures, identity providers, and other qualified relying parties, for the definition of authentication assurance profiles, operational requirements for authentication services, and the accreditation of Issuing Authorities. The e-Infrastructure MAY participate in the accreditation standards process of the IGTF through formal membership of the IGTF member Policy Management Authorities.

3 DEFINITION OF APPROVED AUTHENTICATION ASSURANCE SOURCES

Authentication and identification is considered adequate if the combined assurance level provided by the Issuing Authority, the e-Infrastructure registration service, and the VO registration service, for each User authorised to access Services, meets or exceeds the requirements of the following approved IGTF authentication assurance profiles [R5]:

a) IGTF Assurance Profile ASPEN (urn:oid:1.2.840.113612.5.2.5.1)
b) IGTF Assurance Profile BIRCH (urn:oid:1.2.840.113612.5.2.5.2)
c) IGTF Assurance Profile CEDAR (urn:oid:1.2.840.113612.5.2.5.3)

Unless either the VO or e-infrastructure registration service can demonstrate that - for the Users it authorises to use Services - it meets one of the approved assurance profiles, the IGTF accredited issuing authority MUST provide this level of assurance.

If either the specific VO registration service or the e-Infrastructure registration service meets or exceeds the approved authentication assurance profiles, an IGTF accredited Issuing Authority meeting the IGTF Assurance Profile DOGWOOD (urn:oid:1.2.840.113612.5.2.5.4) is considered adequate when used solely in combination with said VO or e-Infrastructure registration service[1].

For credentials issued in the form of PKI certificates, the e-Infrastructure requires compliance with the IGTF PKI Technology Guidelines [R6].

The e-Infrastructure management MAY incidentally approve other Issuing Authorities. These SHOULD normally be temporary, pending IGTF accreditation. Credentials issued by authorities other than those listed above are not approved.

4 OPERATIONAL MATTERS

The e-Infrastructure deployment team SHALL maintain its own repository containing the trust anchors of all approved Issuing Authorities (see section 3), synchronised promptly with each IGTF trust anchor release. All e-Infrastructure resources SHOULD promptly install the full list of approved trust anchors from the repository as packaged, updated and announced from time to time by the deployment team. Decisions not to install or to subsequently remove a trust anchor from an approved Issuing Authority MUST be communicated immediately to the e-Infrastructure Security Officer. Individual resources MAY deploy other non-approved trust anchors for their own local use, providing this is allowed by their local policy and that they take care of the potential problems arising from e.g. non-uniqueness of user subject names.

5 MORE-SPECIFIC POLICIES

For specific cases, a risk evaluation and assessment having been completed, different authentication assurance policies may apply. The e-Infrastructure shall maintain a registry of such specific policies and their area of applicability.

[1] In the PKI Technology Rendering, the e-Infrastructure thus approves the IGTF SLCS, MICS, and Classic APs for general use, and the IGTF IOTA AP for use in combination with VO or e-Infrastructure registration services that themselves meet the IGTF ASPEN, BIRCH or CEDAR assurance profiles.

6 REFERENCES

R 1	(Old version) Policy. Approval of Certification Authorities. https://documents.egi.eu/document/83
R 2	Approved EGI Security Policies. https://wiki.egi.eu/wiki/SPG:Documents
R 3	EGI Glossary. https://wiki.egi.eu/wiki/Glossary_V1 SPG Security Policy Glossary of Terms. https://documents.egi.eu/document/71
R 4	Interoperable Global Trust Foundation (IGTF). http://www.igtf.net/
R 5	IGTF Levels of Authentication Assurance. https://www.igtf.net/ap/authn-assurance/
R 6	IGTF PKI Technology Guidelines https://www.igtf.net/guidelines/pkitech/