AARC Authentication and Authorisation for Research and Collaboration

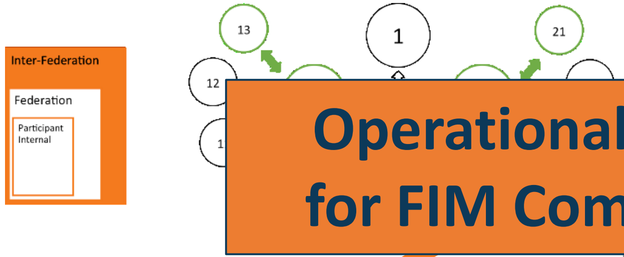
Beyond the finish onwards to the policy horizon

Consolidating policy and best practice activities from NA3

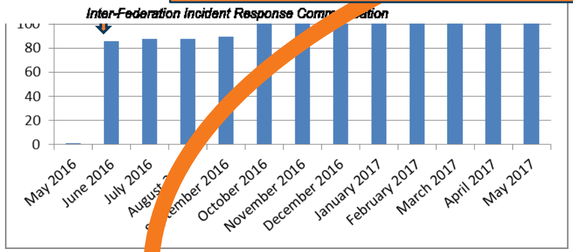
David Groep
NA3 coordinatior
Nikhef

AARC2AHM5 meeting Abingdon
March 2019

How can policy help you ease collaboration?



Operational Security for FIM Communities



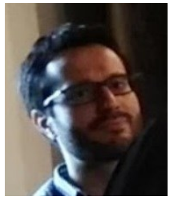
SIRTFI
Security Incident Response Trust Framework for Federated Identity

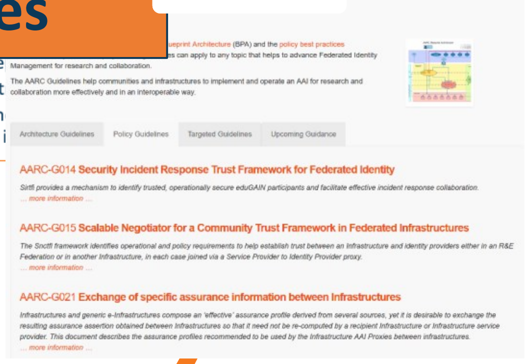
Snctfi

GDPR-style Code of Conduct – a new way?

- Global sharing in controlled communities appears attractive
- Uncertainly about requirements (governing body) and timing (> Mar 2018) are not helpful for adoption today … just yet
- Ongoi… …k: text needs to allow for (community) attribute authori…
- Note that this is not formally BCR, so requires acce…
- Collaborations (e.g. based around Snctfi) with cont…
- "Say what you do, and do as you say" – transparen… is our real benefit towards the person whose data i…

supporting policies for Infrastructures





…ueprint Architecture (BPA) and the policy best practices …es can apply to any topic that helps to advance Federated Identity Management for research and collaboration.

The AARC Guidelines help communities and infrastructures to implement and operate an AAI for research and collaboration more effectively and in an interoperable way.

AARC-G014 Security Incident Response Trust Framework for Federated Identity

Sirtfi provides a mechanism to identify trusted, operationally secure eduGAIN participants and facilitate effective incident response collaboration.

… more information …

AARC-G015 Scalable Negotiator for a Community Trust Framework in Federated Infrastructures

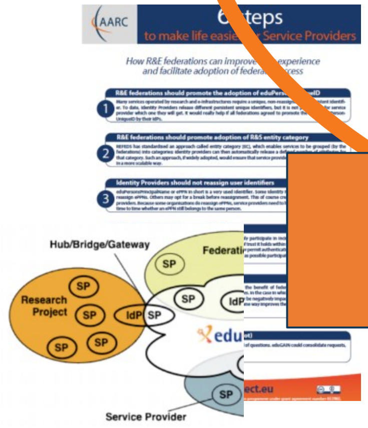
The Snctfi framework identifies operational and policy requirements to help establish trust between an Infrastructure and identity providers either in an R&E Federation or in another Infrastructure, in each case joined via a Service Provider to Identity Provider proxy.

… more information …

AARC-G021 Exchange of specific assurance information between Infrastructures

Infrastructures and generic e-Infrastructures compose an 'effective' assurance profile derived from several sources, yet it is desirable to exchange the resulting assurance assertion obtained between Infrastructures so that it need not be re-computed by a recipient Infrastructure or Infrastructure service provider. This document describes the assurance profiles recommended to be used by the Infrastructure AAI Proxies between infrastructures.

… more information …


AARC
6 steps
to make life easie… …Service Providers
How R&E federations can improve … experience and facilitate adoption of federa… …ess
1
R&E federations should promote the adoption of eduPers… …ID
2
R&E federations should promote adoption of R&S entity category
3
Identity Providers should not reassign user identifiers
Hub/Bridge/Gateway
Federat…
Research Project
SP
IdP
edu…
…ect.eu
Service Provider

3 Community Operations Security Policy

engagement and coordination

2. The Community shall provide and maintain, in a repository designat… *Infrastructure, accurate contact information as specified by the Infrastructure.*

AARC

…a Community …lerated

…s Kanellopoulos (GÉANT), …son (STFC), Stefan Paetow …RIS-CNRS), Mischa Salle …ERN), Uros Stevanovic (KIT) and Gerben Venekamp

AARC - Version 1.0 - 26 Apr 2017

e-mail: david.kelsey@stfc.ac.uk

Abstract: This paper identifies operational and policy requirements to help establish trust between an Infrastructure and identity providers either in an R&E Federation or in another Infrastructure, in each case joined via a Service Provider to Identity Provider proxy.

Audience: This document is intended for use by the personnel responsible for the management, operation and security of an Infrastructure and those wishing to assess its trustworthiness.

'low-risk' use cas…
few unalienable e… by research and c… services
Baseline Assura…
1. known ind…
2. Persistent identifiers
3. Documented vetting
4. Password auth…
…assessment
'Kantara LoA2', 'eIDAS low', or 'IGTF BIRCH'
2. Good entropy passwords
3. Affiliation freshness better than 1 month
'eIDAS substantial', 'Kantara LoA3'
2. Multi-factor authenticator

support for Researchers & Community

1 ACCEPTABLE USE POLICY AND CONDITIONS OF USE

This …licy is effective from 10/10… …ersion of this do… …curity Policy [R… …cuments in the s…

…od and will abid…

…work, or transr… …of use as define…

2. You shall provide appropr… …rt or citation fo… resources/services provided as required by the body or bodies granting you… …the resources/services for any purpose that is unlawful… …mvent any administrative or security controls. …tellectual property and confidentiality agreements. …our access credentials (e.g. private keys or passwords). …our registered information correct and up to date. …tely report any known or suspected security breach…

Value	Cappuccino	Espresso
$PREFIX$/ID/unique	X	X
$PREFIX$/ID/no-eppn-reassign		
$PREFIX$/ID/eppn-reassign-1yr		
$PREFIX$/IAP/local-enterprise	X	X
$PREFIX$/IAP/assumed	X	X
$PREFIX$/IAP/verified		X
$PREFIX$/AAP/good-entropy	X	
$PREFIX$/AAP/multi-factor		X
$PREFIX$/ATP/ePA-1m	X	X

Responding to incidents – sharing relevant information

- Sirtfi take-up at proper organizational level

Beyond basic Sirtfi

- federation-level engagement in process
- *Sirtfi+* registry broadens global base
- engagement in trust groups valuable for federated collective response

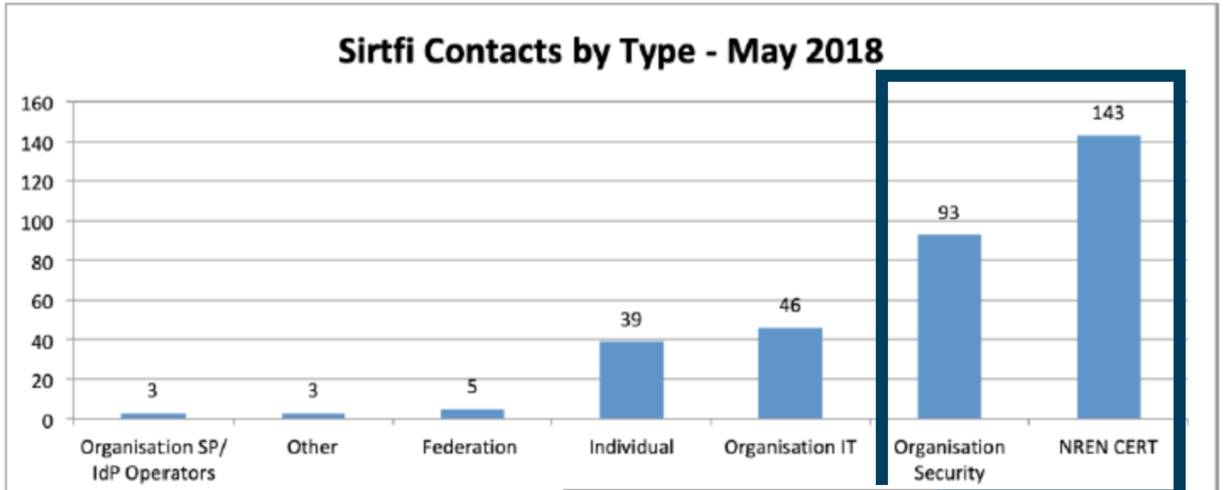
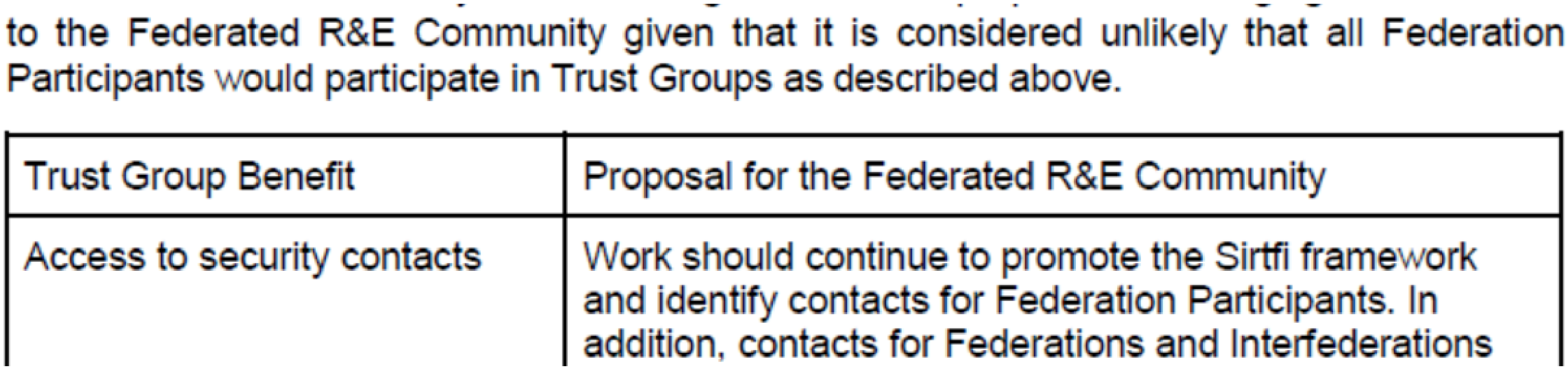
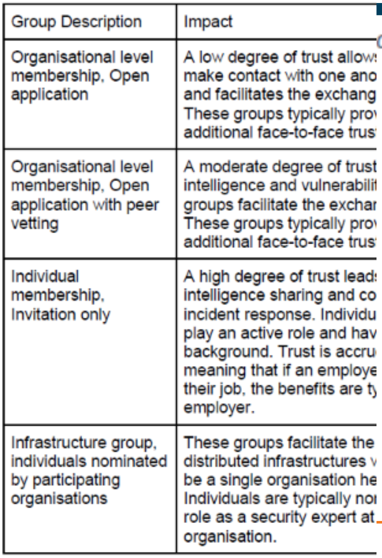


Figure 2: Sirtfi contacts as listed in the edu d by contact type.



to the Federated R&E Community given that it is considered unlikely that all Federation Participants would participate in Trust Groups as described above.

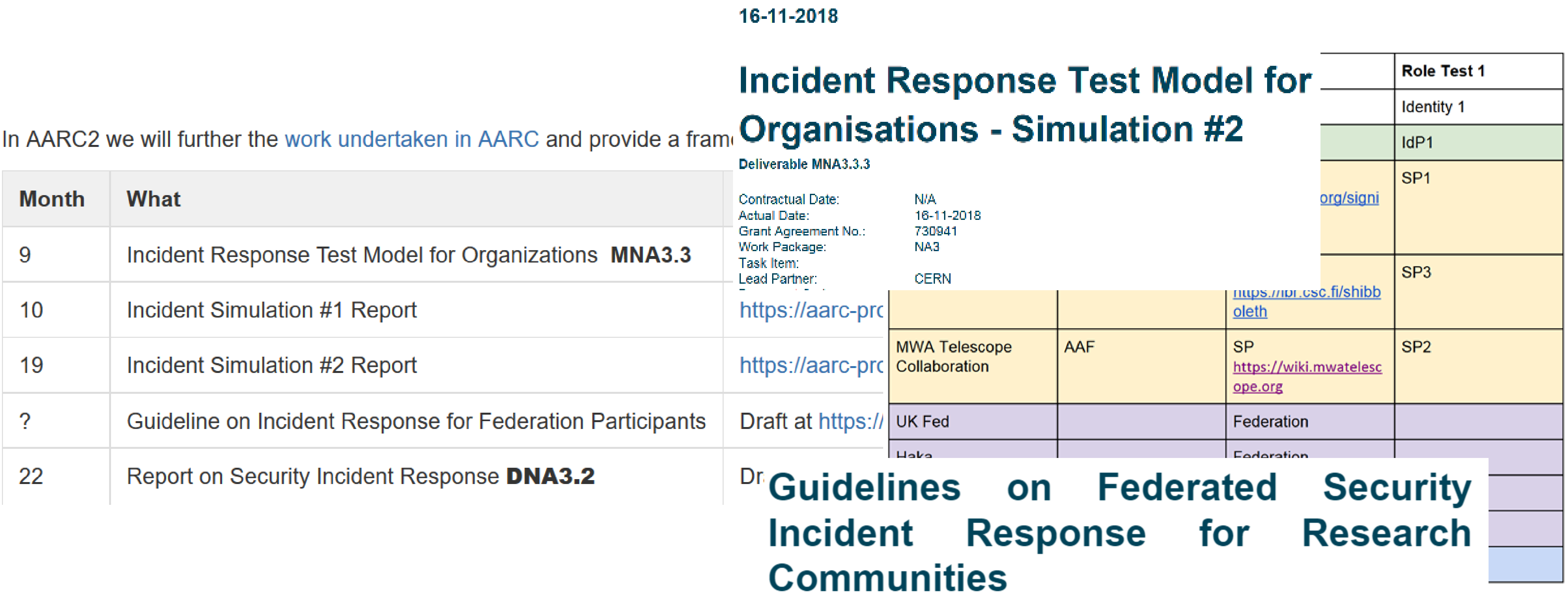
Trust Group Benefit	Proposal for the Federated R&E Community
Access to security contacts	Work should continue to promote the Sirtfi framework and identify contacts for Federation Participants. In addition, contacts for Federations and Interfederations



Group Description	Impact
Organisational level membership, Open application	A low degree of trust allow make contact with one ano and facilitates the exchang These groups typically prov additional face-to-face trus
Organisational level membership, Open application with peer vetting	A moderate degree of trust intelligence and vulnerabilit groups facilitate the exchar These groups typically prov additional face-to-face trus
Individual membership, Invitation only	A high degree of trust lead intelligence sharing and co incident response. Individu play an active role and hav background. Trust is accru meaning that if an employe their job, the benefits are ty employer.
Infrastructure group, individuals nominated by participating organisations	These groups facilitate the distributed infrastructures v be a single organisation he Individuals are typically no role as a security expert at organisation.

from DNA3.2 *Report on Security Incident Response and Cybersecurity in Federated Authentication Scenarios*

… the rest we test …



In AARC2 we will further the work undertaken in AARC and provide a fram

Month	What	
9	Incident Response Test Model for Organizations **MNA3.3**	
10	Incident Simulation #1 Report	https://aarc-prc
19	Incident Simulation #2 Report	https://aarc-prc
?	Guideline on Incident Response for Federation Participants	Draft at https://
22	Report on Security Incident Response **DNA3.2**	Dr

16-11-2018

Incident Response Test Model for Organisations - Simulation #2

Deliverable MNA3.3.3

Contractual Date:	N/A
Actual Date:	16-11-2018
Grant Agreement No.:	730941
Work Package:	NA3
Task Item:	
Lead Partner:	CERN

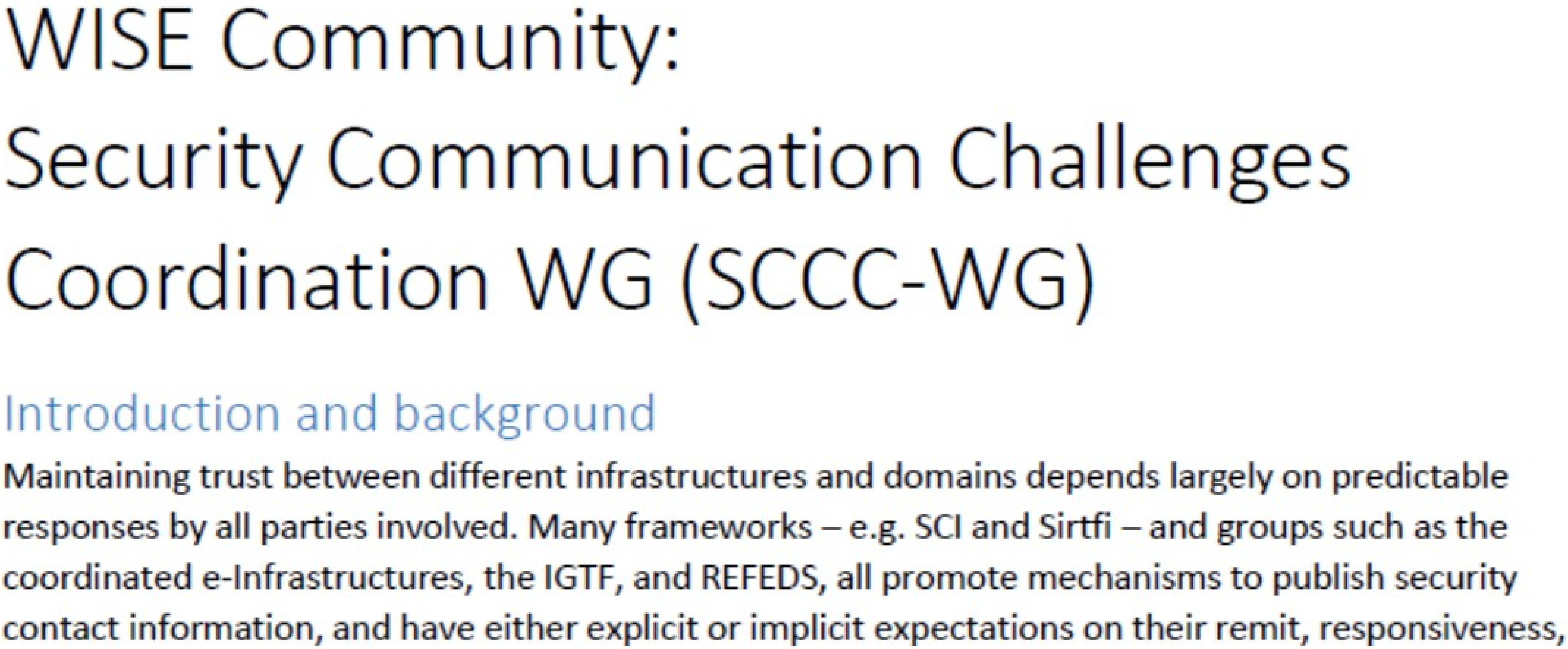
			Role Test 1
			Identity 1
			IdP1
		org/signi	SP1
		https://ibr.csc.fi/shibboleth	SP3
MWA Telescope Collaboration	AAF	SP https://wiki.mwatelescope.org	SP2
UK Fed		Federation	
Haka		Federation	

Guidelines on Federated Security Incident Response for Research Communities

'AARC-G051', maybe ?

https://wiki.geant.org/display/AARC/AARC2+NA3+Task+1+-++Overview

WISE SCCC WG



WISE Community: Security Communication Challenges Coordination WG (SCCC-WG)

Introduction and background

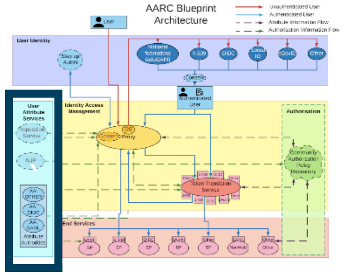
Maintaining trust between different infrastructures and domains depends largely on predictable responses by all parties involved. Many frameworks – e.g. SCI and Sirtfi – and groups such as the coordinated e-Infrastructures, the IGTF, and REFEDS, all promote mechanisms to publish security contact information, and have either explicit or implicit expectations on their remit, responsiveness,

https://wise-community.org/events/ https://eventr.geant.org/events/3044

Attribute Authority Operations and ‘MMS assessment’

3. Operational Guidelines
3.1. Naming
3.2. Attribute Management and Attribute Release
3.3. Attribute Assertions
3.4. Operational requirements
3.4.1. Key Management
3.4.2. Network Configuration
3.5. Site Security
3.6. Metadata publication
3.7. Assessments and auditability
3.8. Privacy and confidentiality
3.9. Compromise and disaster recovery
4. Relying Party obligations

Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements



3.3. Attribute Assertions

Publication Date 2018-11-22
Authors: David Groep;David Kelsey;Hannah Short;Mischa Sallé;Uros Stevanovic;Stefan Paetow;Maarten Kremers

Document Code: AARC-G048

1. Assertions provided by an AA must be integrity-protected. They must be signed by the identified AA, or be transmitted over an integrity-protected channel where the server has been authenticated, and preferably both.

Push model
Where the protocol supports it, enable protection also of the messages conveyed over the established channel. Good examples: SAML Attribute Query should enable message signing and use TLS.

Pull model
As a good example: LDAP should enable TLS protection of the channel

https://aarc-project.eu/guidelines/aarc-g048/
https://www.eugridpma.org/guidelines/aaops/

Traceability in Multi-Domain Service Provider Environments (“D3.2”)

All what we have, and what we ‘lump in’ here (since it has nowhere else to go)

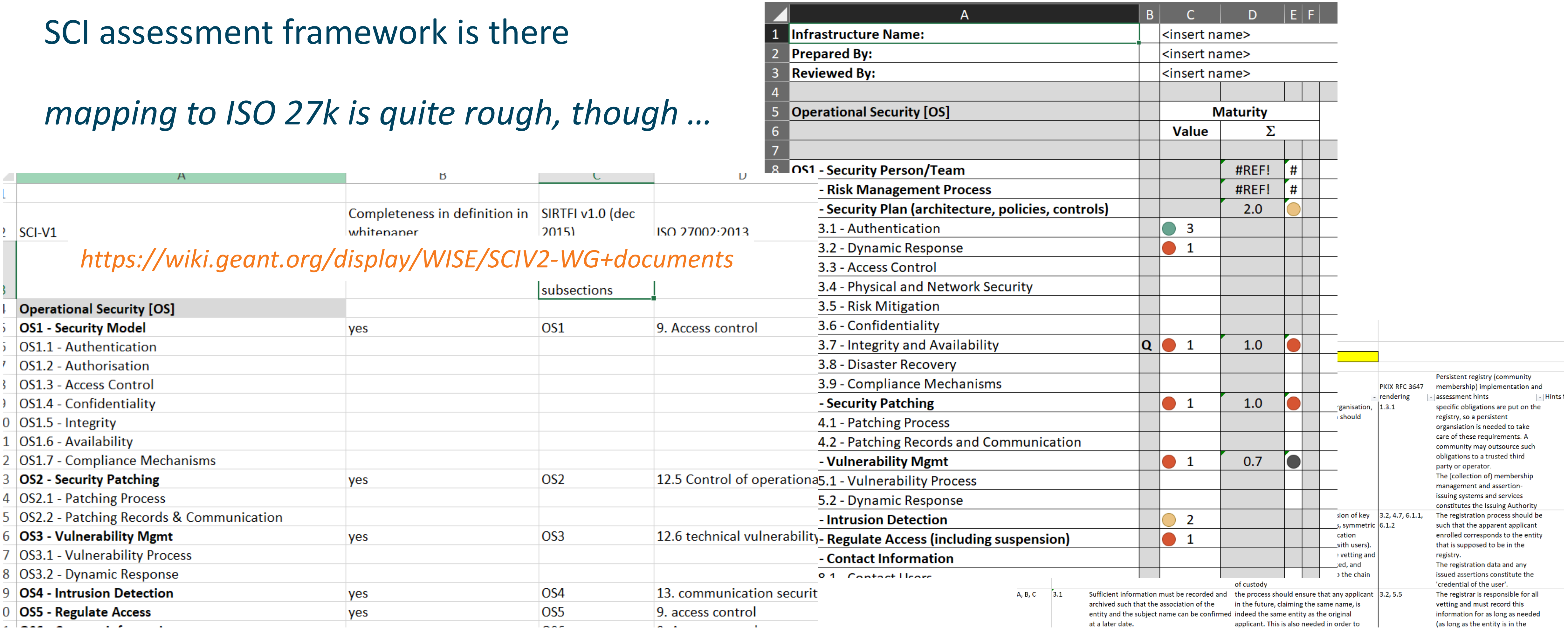
- SCI v2 and the assessment methodology
- Managing the proxy: data minimization, why the proxy can release attributes and still be data-minimalistic (“Interest of users to reduce the release of personal, as well as the potential risks for the users info vs. the need of resources to have proper accounting and security”)
- Policy Development Kit – how to help infrastructures meet their requirements on traceability and much more

should G021 (“exchange of assurance information *between infrastructures*”) go here as well?

Service policies: helping peer-reviewed self-assessment in SCI and more

SCI assessment framework is there

mapping to ISO 27k is quite rough, though …



A	B	C	D
SCI-V1	Completeness in definition in whitepaper	SIRTFI v1.0 (dec 2015)	ISO 27002:2013
		subsections	
Operational Security [OS]			
OS1 - Security Model	yes	OS1	9. Access control
OS1.1 - Authentication			
OS1.2 - Authorisation			
OS1.3 - Access Control			
OS1.4 - Confidentiality			
OS1.5 - Integrity			
OS1.6 - Availability			
OS1.7 - Compliance Mechanisms			
OS2 - Security Patching	yes	OS2	12.5 Control of operationa
OS2.1 - Patching Process			
OS2.2 - Patching Records & Communication			
OS3 - Vulnerability Mgmt	yes	OS3	12.6 technical vulnerability
OS3.1 - Vulnerability Process			
OS3.2 - Dynamic Response			
OS4 - Intrusion Detection	yes	OS4	13. communication securit
OS5 - Regulate Access	yes	OS5	9. access control

https://wiki.geant.org/display/WISE/SCIV2-WG+documents

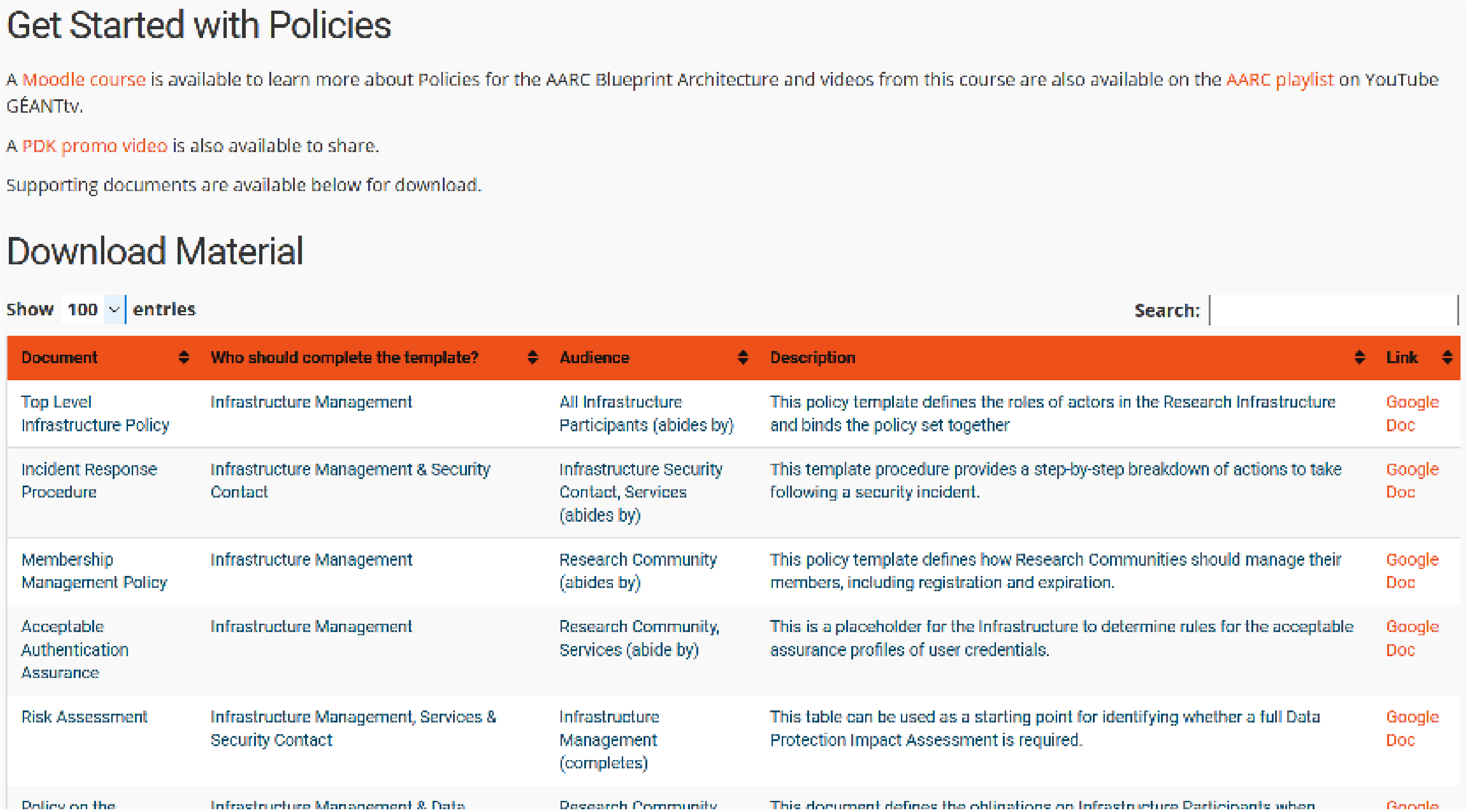
	A	B	C	D	E	F
1	**Infrastructure Name:**		<insert name>			
2	**Prepared By:**		<insert name>			
3	**Reviewed By:**		<insert name>			
4						
5	**Operational Security [OS]**		**Maturity**			
6			**Value**	**Σ**		
7						
8	**OS1 - Security Person/Team**			#REF!	#	
	- Risk Management Process			#REF!	#	
	- Security Plan (architecture, policies, controls)			2.0	●	
	3.1 - Authentication		● 3			
	3.2 - Dynamic Response		● 1			
	3.3 - Access Control					
	3.4 - Physical and Network Security					
	3.5 - Risk Mitigation					
	3.6 - Confidentiality					
	3.7 - Integrity and Availability	**Q**	● 1	1.0	●	
	3.8 - Disaster Recovery					
	3.9 - Compliance Mechanisms					
	- Security Patching		● 1	1.0	●	
	4.1 - Patching Process					
	4.2 - Patching Records and Communication					
	- Vulnerability Mgmt		● 1	0.7	●	
	5.1 - Vulnerability Process					
	5.2 - Dynamic Response					
	- Intrusion Detection		● 2			
	- Regulate Access (including suspension)		● 1			
	- Contact Information					
	8.1 - Contact Users					

				PKIX RFC 3647 rendering	Persistent registry (community membership) implementation and assessment hints	Hints f
			rganisation, should	1.3.1	specific obligations are put on the registry, so a persistent organsiation is needed to take care of these requirements. A community may outsource such obligations to a trusted third party or operator. The (collection of) membership management and assertion-issuing systems and services constitutes the Issuing Authority	
			sion of key s, symmetric cation vith users). vetting and ed, and the chain of custody	3.2, 4.7, 6.1.1, 6.1.2	The registration process should be such that the apparent applicant enrolled corresponds to the entity that is supposed to be in the registry. The registration data and any issued assertions constitute the 'credential of the user'.	
A, B, C	3.1	Sufficient information must be recorded and archived such that the association of the entity and the subject name can be confirmed at a later date.	the process should ensure that any applicant in the future, claiming the same name, is indeed the same entity as the original applicant. This is also needed in order to	3.2, 5.5	The registrar is responsible for all vetting and must record this information for as long as needed (as long as the entity is in the	

http://wise-community.org/sci/ https://wiki.eugridpma.org/Main/AssuranceAssessment

Policy Development Kit

introduction video – training – 9 reference templates – continuous improvement



Get Started with Policies

A Moodle course is available to learn more about Policies for the AARC Blueprint Architecture and videos from this course are also available on the AARC playlist on YouTube GÉANTtv.

A PDK promo video is also available to share.

Supporting documents are available below for download.

Download Material

Show 100 entries Search:

Document	Who should complete the template?	Audience	Description	Link
Top Level Infrastructure Policy	Infrastructure Management	All Infrastructure Participants (abides by)	This policy template defines the roles of actors in the Research Infrastructure and binds the policy set together	Google Doc
Incident Response Procedure	Infrastructure Management & Security Contact	Infrastructure Security Contact, Services (abides by)	This template procedure provides a step-by-step breakdown of actions to take following a security incident.	Google Doc
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.	Google Doc
Acceptable Authentication Assurance	Infrastructure Management	Research Community, Services (abide by)	This is a placeholder for the Infrastructure to determine rules for the acceptable assurance profiles of user credentials.	Google Doc
Risk Assessment	Infrastructure Management, Services & Security Contact	Infrastructure Management (completes)	This table can be used as a starting point for identifying whether a full Data Protection Impact Assessment is required.	Google Doc
Policy on the	Infrastructure Management & Data	Research Community	This document defines the obligations on Infrastructure Participants when	Google

https://aarc-project.eu/policies/policy-development-kit/

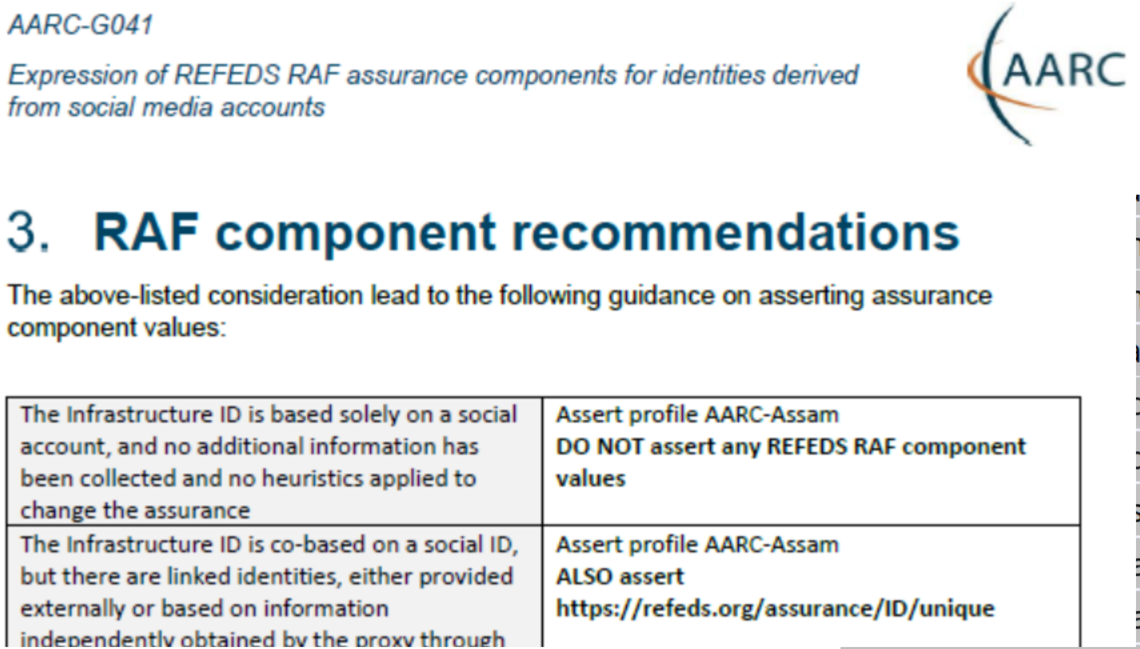
Supporting e-Researchers and communities (“D3.4”)

All what we have, and what we ‘lump in’ here (since it has nowhere else to go)

- Assurance
- Acceptable use policy and guidance
- FIM4R

Assurance – standard profiles and ‘untangling spaghetti’

- REFEDS RAF profiles (feasible assurance from all over R&E federations – as far as we can!)
- inter-infrastructure profiles and relying-party oriented profiles (IGTF BIRCH, DOGWOOD)
- how to express social media assurance, for citizen science and in support of account linking



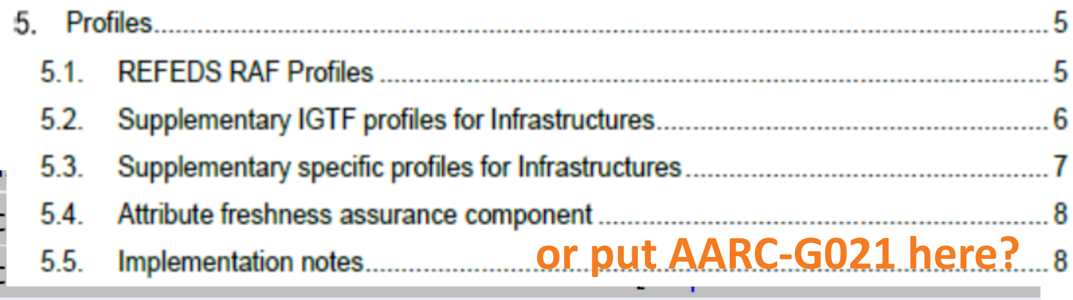
AARC-G041

Expression of REFEDS RAF assurance components for identities derived from social media accounts

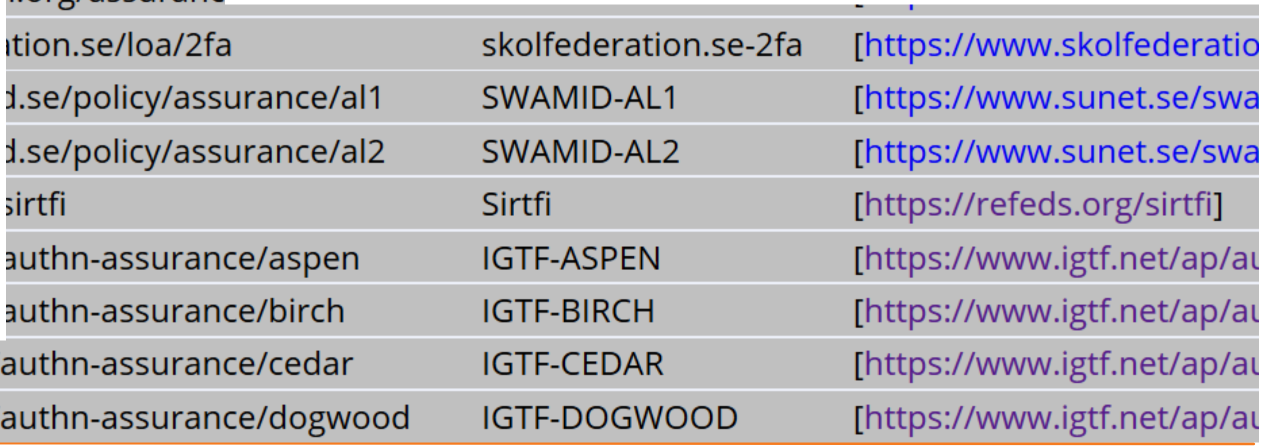
3. RAF component recommendations

The above-listed consideration lead to the following guidance on asserting assurance component values:

The Infrastructure ID is based solely on a social account, and no additional information has been collected and no heuristics applied to change the assurance	Assert profile AARC-Assam **DO NOT assert any REFEDS RAF component values**
The Infrastructure ID is co-based on a social ID, but there are linked identities, either provided externally or based on information independently obtained by the proxy through	Assert profile AARC-Assam **ALSO assert** **https://refeds.org/assurance/ID/unique**



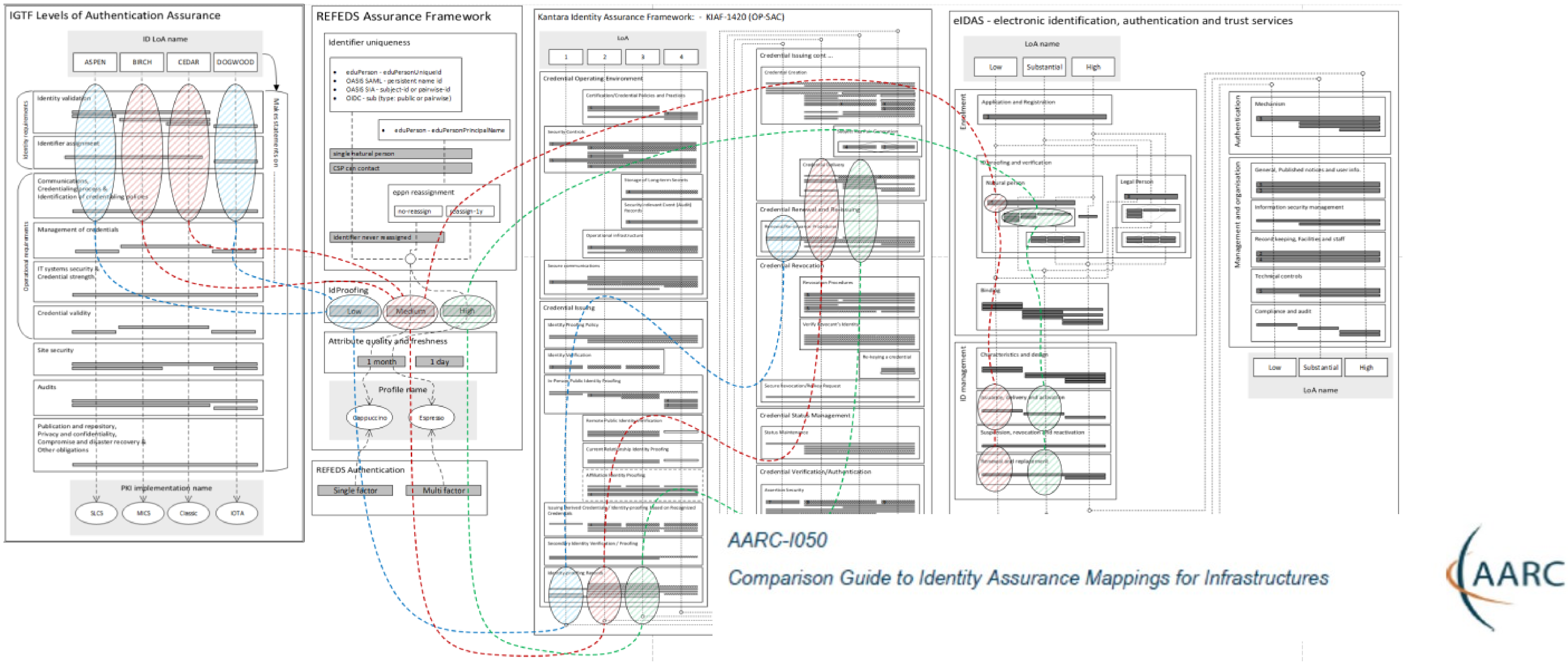
or put AARC-G021 here?



n.org/assuranc		
n.org/assuranc		
ation.se/loa/2fa	skolfederation.se-2fa	[https://www.skolfederatio
d.se/policy/assurance/al1	SWAMID-AL1	[https://www.sunet.se/swa
d.se/policy/assurance/al2	SWAMID-AL2	[https://www.sunet.se/swa
sirtfi	Sirtfi	[https://refeds.org/sirtfi]
authn-assurance/aspen	IGTF-ASPEN	[https://www.igtf.net/ap/au
authn-assurance/birch	IGTF-BIRCH	[https://www.igtf.net/ap/au
https://igtf.net/ap/authn-assurance/cedar	IGTF-CEDAR	[https://www.igtf.net/ap/au
https://igtf.net/ap/authn-assurance/dogwood	IGTF-DOGWOOD	[https://www.igtf.net/ap/au

https://www.iana.org/assignments/loa-profiles/

Untangling Assurance Spaghetti:
Comparison Guide to Identity Assurance Mappings for Infrastructures


IGTF Levels of Authentication Assurance
ID LoA name
ASPEN
BIRCH
CEDAR
DOGWOOD
Identity requirements
Identity validation
Identifier assignment
Communications, Credentialing process & Identification of credentialing policies
Operational requirements
Management of credentials
IT systems security & Credential strength
Credential validity
Site security
Audits
Publication and repository, Privacy and confidentiality, Compromise and disaster recovery & Other obligations
Makes statements on
PKI implementation name
SLCS
MICS
Classic
IOTA
REFEDS Assurance Framework
Identifier uniqueness
eduPerson - eduPersonUniqueId
OASIS SAML - persistent name id
OASIS SIA - subject-id or pairwise-id
OIDC - sub (type: public or pairwise)
eduPerson - eduPersonPrincipalName
single natural person
CSP can contact
eppn reassignment
no-reassign
reassign-1y
identifier never reassigned
IdProofing
Low
Medium
High
Attribute quality and freshness
1 month
1 day
Profile name
Cappuccino
Espresso
REFEDS Authentication
Single factor
Multi factor
Kantara Identity Assurance Framework: - KIAF-1420 (OP-SAC)
LoA
1
2
3
4
Credential Operating Environment
Certification/Credential Policies and Practices
Security Controls
Storage of Long-term Secrets
Security-relevant Event (Audit) Records
Operational Infrastructure
Secure communications
Credential Issuing
Identity Proofing Policy
Identity Verification
In-Person Public Identity Proofing
Remote Public Identity Verification
Current Relationship Identity Proofing
Affiliation Identity Proofing
Issuing Derived Credentials / Identity-proofing based on Recognized Credentials
Secondary Identity Verification / Proofing
Identity-proofing Records
Credential Issuing cont ...
Credential Creation
Subject Key Pair Generation
Credential Delivery
Credential Renewal and Re-issuing
Renewal/Re-issuance Procedures
Credential Revocation
Revocation Procedures
Verify Revocant's Identity
Re-keying a credential
Secure Revocation/Status Request
Credential Status Management
Status Maintenance
Credential Verification/Authentication
Assertion Security
eIDAS - electronic identification, authentication and trust services
LoA name
Low
Substantial
High
Enrolment
Application and Registration
ID proofing and verification
Natural person
Legal Person
Binding
ID management
Characteristics and design
Issuance, delivery and activation
Suspension, revocation and reactivation
Renewal and replacement
Authentication
Mechanism
Management and organisation
General, Published notices and user info.
Information security management
Record keeping, Facilities and staff
Technical controls
Compliance and audit
Low
Substantial
High
LoA name

AARC-I050

Comparison Guide to Identity Assurance Mappings for Infrastructures

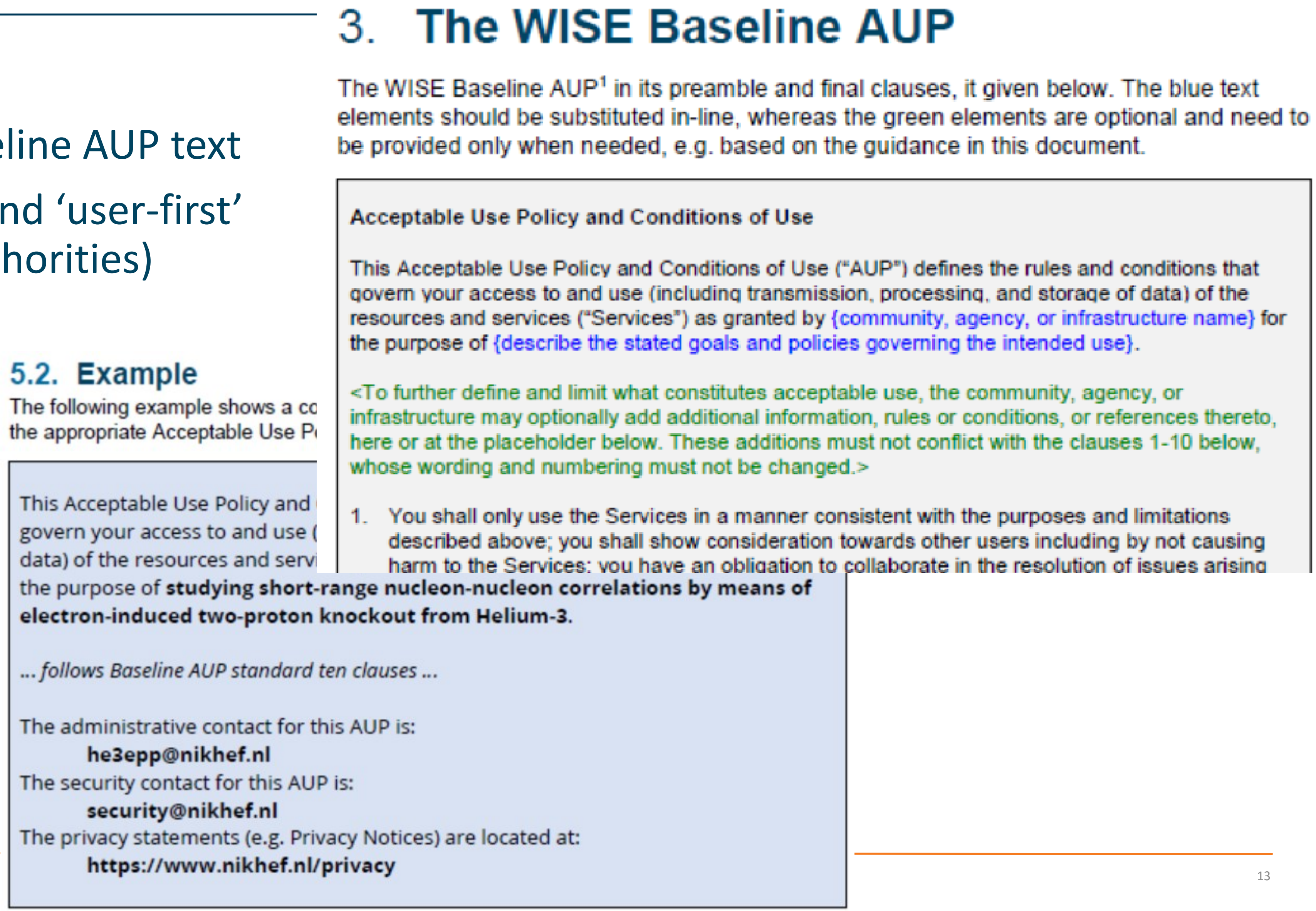
https://aarc-project.eu/guidelines/aarc-i050/

WISE Baseline AUP – and how to apply it for your Infrastructure

AARC-I044

- Includes the final WISE Baseline AUP text
- for both 'community-first' and 'user-first' MMS services (attribute authorities)
- examples make it concrete

Quick take-up by e-Infras (both global and national)



3. The WISE Baseline AUP

The WISE Baseline AUP[1] in its preamble and final clauses, it given below. The blue text elements should be substituted in-line, whereas the green elements are optional and need to be provided only when needed, e.g. based on the guidance in this document.

Acceptable Use Policy and Conditions of Use

This Acceptable Use Policy and Conditions of Use ("AUP") defines the rules and conditions that govern your access to and use (including transmission, processing, and storage of data) of the resources and services ("Services") as granted by {community, agency, or infrastructure name} for the purpose of {describe the stated goals and policies governing the intended use}.

<To further define and limit what constitutes acceptable use, the community, agency, or infrastructure may optionally add additional information, rules or conditions, or references thereto, here or at the placeholder below. These additions must not conflict with the clauses 1-10 below, whose wording and numbering must not be changed.>

1. You shall only use the Services in a manner consistent with the purposes and limitations described above; you shall show consideration towards other users including by not causing harm to the Services; you have an obligation to collaborate in the resolution of issues arising

5.2. Example

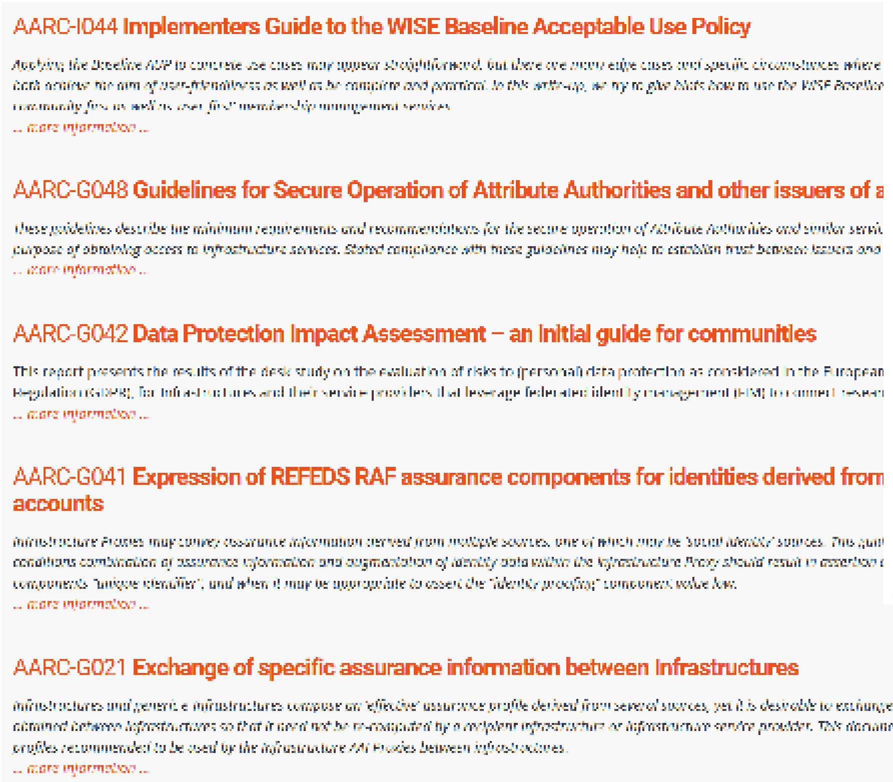
The following example shows a co
the appropriate Acceptable Use P

This Acceptable Use Policy and
govern your access to and use (
data) of the resources and servi
the purpose of **studying short-range nucleon-nucleon correlations by means of electron-induced two-proton knockout from Helium-3.**

... follows Baseline AUP standard ten clauses ...

The administrative contact for this AUP is:
he3epp@nikhef.nl
The security contact for this AUP is:
security@nikhef.nl
The privacy statements (e.g. Privacy Notices) are located at:
https://www.nikhef.nl/privacy

Our collective wisdom from AARC2



AARC-I044 Implementers Guide to the WISE Baseline Acceptable Use Policy

Applying the Baseline AUP to concrete use cases may appear straightforward, but there are many edge cases and specific circumstances where both achieve the aim of user-friendliness as well as be complete and practical. In this write-up, we try to give hints how to use the WISE Baseline community first as well as user first membership management services.

... more information ...

AARC-G048 Guidelines for Secure Operation of Attribute Authorities and other issuers of a

These guidelines describe the minimum requirements and recommendations for the secure operation of Attribute Authorities and similar servic purpose of obtaining access to infrastructure services. Stated compliance with these guidelines may help to establish trust between issuers and

... more information ...

AARC-G042 Data Protection Impact Assessment – an initial guide for communities

This report presents the results of the desk study on the evaluation of risks to (personal) data protection as considered in the European Regulation (GDPR), for Infrastructures and their service providers that leverage federated identity management (FIM) to connect researc

... more information ...

AARC-G041 Expression of REFEDS RAF assurance components for identities derived from accounts

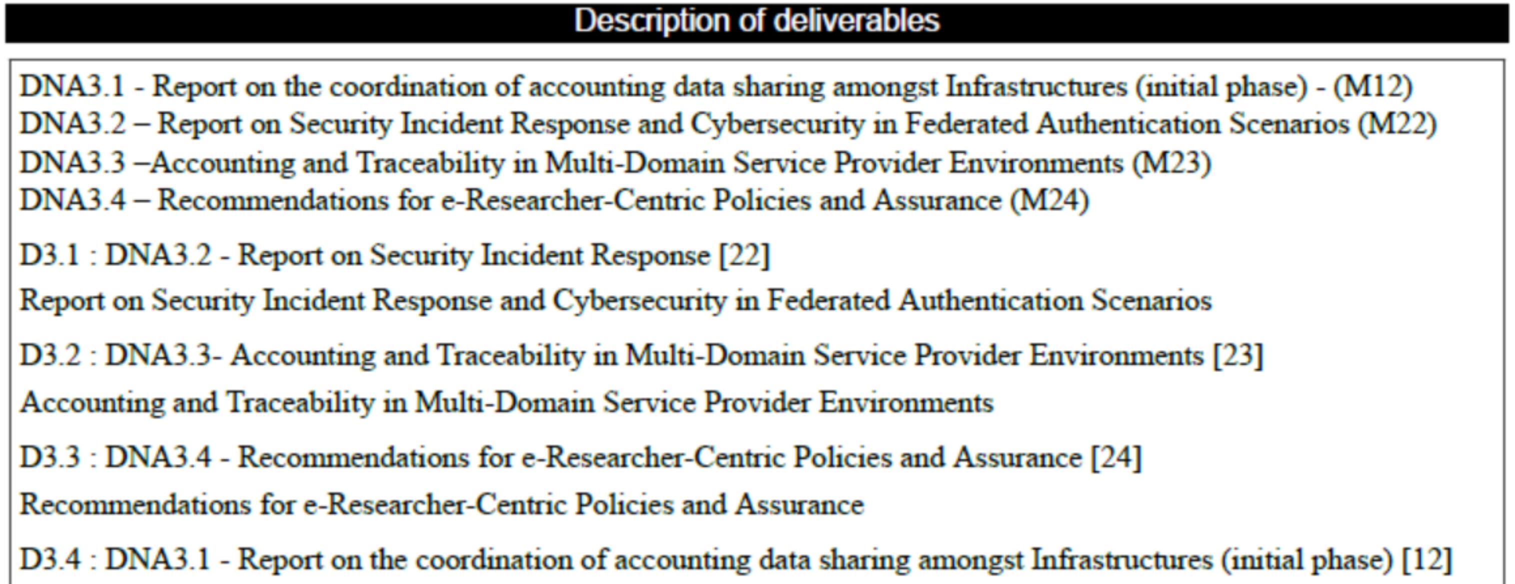
Infrastructure Proxies may convey assurance information derived from multiple sources, one of which may be 'social identity' sources. This guid conditions combination of assurance information and augmentation of identity data within the Infrastructure Proxy should result in assertion c components "unique identifier", and when it may be appropriate to assert the "identity proofing" component value low.

... more information ...

AARC-G021 Exchange of specific assurance information between Infrastructures

Infrastructures and generic e-Infrastructures compose an 'effective' assurance profile derived from several sources, yet it is desirable to exchange the resulting assurance assertion obtained between Infrastructures so that it need not be re-computed by a recipient infrastructure or Infrastructure service provider. This document describes the assurance profiles recommended to be used by the Infrastructure AAI Proxies between infrastructures.

... more information ...



Description of deliverables

DNA3.1 - Report on the coordination of accounting data sharing amongst Infrastructures (initial phase) - (M12)
DNA3.2 – Report on Security Incident Response and Cybersecurity in Federated Authentication Scenarios (M22)
DNA3.3 –Accounting and Traceability in Multi-Domain Service Provider Environments (M23)
DNA3.4 – Recommendations for e-Researcher-Centric Policies and Assurance (M24)

D3.1 : DNA3.2 - Report on Security Incident Response [22]

Report on Security Incident Response and Cybersecurity in Federated Authentication Scenarios

D3.2 : DNA3.3- Accounting and Traceability in Multi-Domain Service Provider Environments [23]

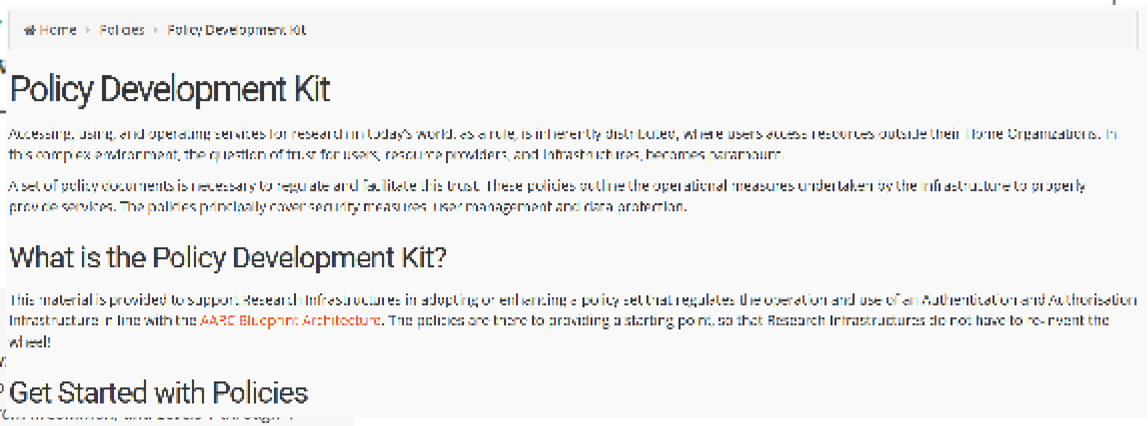
Accounting and Traceability in Multi-Domain Service Provider Environments

D3.3 : DNA3.4 - Recommendations for e-Researcher-Centric Policies and Assurance [24]

Recommendations for e-Researcher-Centric Policies and Assurance

D3.4 : DNA3.1 - Report on the coordination of accounting data sharing amongst Infrastructures (initial phase) [12]

This document assess privacy
ensure smooth and secure serv



Policy Development Kit

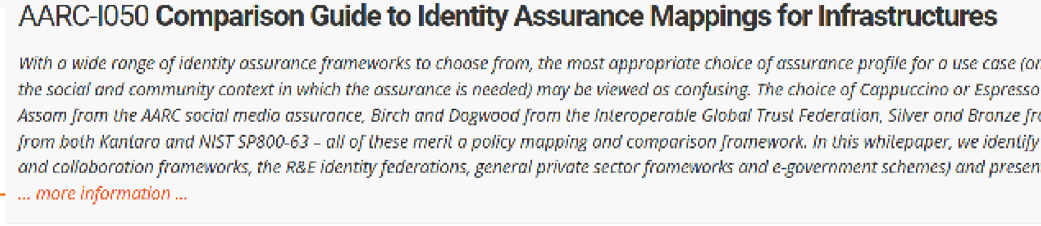
Accessing, using, and operating services for research in today's world, as a rule, is inherently distributed, where users access resources outside their Home Organizations. In this complex environment, the question of trust for users, resource providers, and Infrastructures, becomes paramount.

A set of policy documents is necessary to regulate and facilitate this trust. These policies outline the operational measures undertaken by the infrastructure to properly provide services. The policies principally cover security measures, user management and data protection.

What is the Policy Development Kit?

This material is provided to support Research Infrastructures in adopting or enhancing a policy set that regulates the operation and use of an Authentication and Authorisation Infrastructure in line with the AARC Blueprint Architecture. The policies are there to providing a starting point, so that Research Infrastructures do not have to re-invent the wheel!

Get Started with Policies



AARC-I050 Comparison Guide to Identity Assurance Mappings for Infrastructures

With a wide range of identity assurance frameworks to choose from, the most appropriate choice of assurance profile for a use case (or the social and community context in which the assurance is needed) may be viewed as confusing. The choice of Cappuccino or Espresso Assam from the AARC social media assurance, Birch and Dogwood from the Interoperable Global Trust Federation, Silver and Bronze fr… from both Kantara and NIST SP800-63 – all of these merit a policy mapping and comparison framework. In this whitepaper, we identify the implicit trust assumptions (in research and collaboration frameworks, the R&E identity federations, general private sector frameworks and e-government schemes) and present a way of comparing these frameworks.

... more information ...

plus all our AARC1 wisdom!

and the AARC-G051 incident response process draft?

Since Milano – our final 6 months

OpSec	**Attribute authority operations** practice … also for Infra proxies	✓
	Trust groups and the exchange of (account) compromise information: ***beyond Sirtfi***	✓
Infra-centric	traceability and accounting data-collection policy framework based on **SCI, providing self-assessment methodology** and comparison matrix for infrastructure services	✓
	information obtained **from the proxy** good enough for data protection, security, &c	✓
Researcher-centric	**Baseline AUP** with major Infrastructures (EGI, EUDAT, PRACE, XSEDE) and communiti	✓
	Deployment of **assurance guidelines** and assess high-assurance use cases (BBMRI)	✓
Engagement	Evolve **Policy Development Kit** and a simpler top-level security policy with a community ‘assessment method’ or ‘guide’ to the adoption of appropriate policy	✓
	Support communities and use cases in policy interpretation through Guidelines	✓

Some loose ends

For the **“service-centric” work** a final touch is needed on how to apply the frameworks and help interoperability

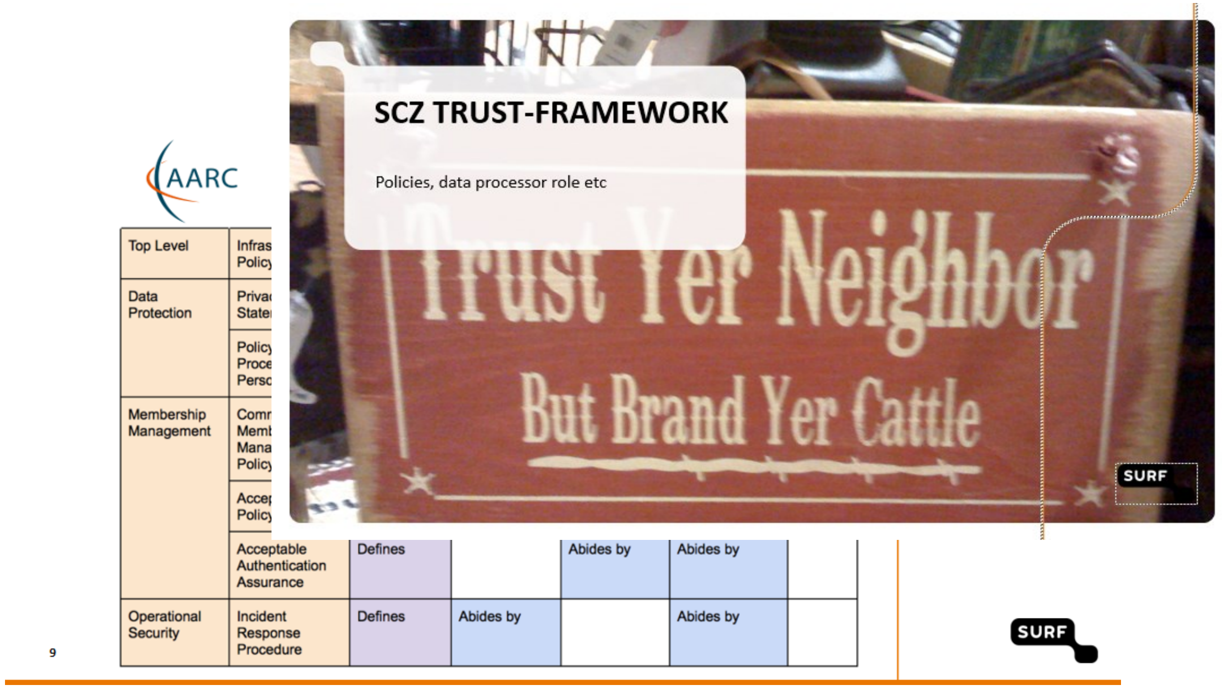
- Assessment methodology for SCI – and how is peer-reviewed self-assessment better then pushing everyone through ISO27k
- How to apply data minimization in attribute release from the membership services

For **Assurance**

- Do our high-assurance in REFEDS (“Espresso”) actually meet the target community need?
- Do we need to update G021 (“Exchange of specific assurance information between Infrastructures”), which is also on Zenodo, before we close?

Incident Response: we should publish draft response procedure before the end (as ‘G051’)?

Adoption – how to promote that for ourselves and the review?



SCZ TRUST-FRAMEWORK

Policies, data processor role etc

Top Level	Infras Policy					
Data Protection	Privac Stater					
	Policy Proce Perso					
Membership Management	Comr Memb Mana Policy					
	Accep Policy					
	Acceptable Authentication Assurance	Defines		Abides by	Abides by	
Operational Security	Incident Response Procedure	Defines	Abides by		Abides by	

9

Policy Development Kit showing up without me prompting in a Dutch collaborative science presentation …

And much more (do we want a list?):

- PDK adoption: by HDF, WLCG
- MMS services adopting AUP
- LSAAI R&S+DPCoCo
- EOSC-HUB and WLCG policy framework revision
- AUP by many (even by a FH)
- FIM4R impact
- …

Beyond AARC – how can the good work continue and thrive?

- EOSC-HUB: mainly WP4.4 “ISM”, WP5.1 “AAI”, and WP13 “Virtual Access” for RCauth
- GN4-3: T5.1.4 – eduGAIN security operations and readiness
- GN4-3: T5.4 – enabling communities

Without specific funding but *endorsed by funded infrastructures & projects*:

- IGTF
- Collaboration Agreement GN4-* and EOSC-HUB
- WISE
- AEGIS
- REFEDS
- FIM4R

Complementary sources: national e-Infrastructures, domain funding, ESFRIs and EOSC projects

Finding a home – some proposals

Sirtfi

- already in a REFEDS WG (Sirtfi+)
- ‘response model’ to the extent it involves federations can go here as well
- actual incident response plus readiness challenges *on federated ID side* go with new eduGAIN security capability

Communications challenges for security that involve also the Infrastructures

- WISE, specifically the new SCCC WG
- needs some love and care from all Infrastructures

Infrastructure-specific challenges remain infrastructure, but coordinated through SCCC

- like the IGTF RAT CC

Finding a home – some proposals

SCI Assessment

- WISE SCI WG, with assessment in the IGTF
- support through EOSC-HUB WP4.4 and GN4-3T5.4
- but obviously also from PRACE, XSEDE, GridPP, SURF, &c

Assurance Profiles – from federations to Infrastructures, and between R/E infrastructures

- the ‘feasible’ assurance and alignment with IdPs and federations belongs in REFEDS RAF
- assurance requirements of, and exchange of assurance between, infrastructures: in IGTF

AUP and Terms of Use

- the home is WISE SCI, but it needs care and nourishment from EOSCHUB and GN4-3
- extends beyond just WP4.4/T5.4 and involves e.g. also eduTEAMS, CheckIn, B2ACCESS

Finding a home – some proposals

Data Protection and GDPR – service centric policy support

- we should lean heavily on AndrewC and the TF-DPR, but more is needed
- risk-assessment methodology for infrastructures and communities
- consultancy role for new communities to enable use of the infrastructures -> mailing list?
- joint GN4-3 + EOSC-HUB + WLCG effort, homed (for lack of anything else) in AEGIS?

Tuning the policy development kit

- the WISE SCI WG can coordinate, but the effort should come from somewhere
- again GN4-3 + EOSC-HUB (EGI, EUDAT) seem the natural choice, with input from PRACE
- other sources have been very successful as well: HDF, GridPP, SURF

For the rest and new things needed, leverage GN-EOSCH collaboration agreement & AEGIS?

- one-on-one consulting with communities highly appreciated also beyond AEGIS,
  but must be and be seen as neutral (maybe a FIM4R or WISE WG? or RDA?)

From now on …

- Coherency of vision and an umbrella for Collaborative policy work will be more challenging
- Exploit personal overlap in the various groups (and cross-membership of lists)
- Provide a forum for cross-fertilization through continued joint workshops

Thank you
Any Questions?

davidg@nikhef.nl

AARC

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agre