Trust Coordination for Research Collaboration in the EOSC era

Contents

The European Open Science Cloud (EOSC) enters a next phase of integration and consolidation with the establishment of a common service portal listing underpinning services that enable distributed resources in the areas of computation, data, open access, and above-the-net collaboration services. More than ever before, composition of services within the EOSC ecosystem will create mutual dependencies between service providers – in terms of not only quality management, provisioning, accounting and settlement, but specifically also in managing the integrity, resilience, availability, and trust in the composition of services and their use. Trust management is enabled by establishing and maintaining essential capabilities providing the appropriate level of integrity, resilience, availability, and confidentiality of the involved services and data.

The existing e-Infrastructures that are anticipated to be part of the EOSC each provide their own capabilities in terms of trust and identity management, integrity protection and risk management, as well as capabilities to support business continuity and disaster recovery in case of security incidents. Many of these activities are anchored in existing, cross-infrastructure, coordination groups such as the WISE (Wise Information Security for E-infrastructures) community (wise-community.org), the Interoperable Global Trust Federation IGTF (igtf.net), the Special Interest Group on Information Security Management SIG-ISM (wiki.geant.org/display/SIGISM), and the AARC Engagement Group for Infrastructures AEGIS (aarc-community.org). Jointly, the e-Infrastructures also support and further the work of the research-community centric Federated Identity Management for Research FIM4R group (fim4r.org). There are also specific trust, collaboration management, and security services that are jointly managed by multiple e-Infrastructures for the benefit of (but in many cases not exclusively) the European research and collaboration community as a whole. These include for instance the glue between the EOSC AAI suite of services that each implement the AARC Blueprint Architecture (eduTEAMS, EGI CheckIn, Indigo IAM, and B2ACCESS) and components such as the RCauth.eu credential translation bridge service. But also a Security Policy Group addressing joint risk

assessment, and trust and security training activities, for the core and edge services alike, that consider the interdependency of services in the EOSC ecosystem.

Complementing these cross-infrastructure groups there are trust and integrity coordination activities closely linked to the operational infrastructure they support. Such infrastructure-specific activities include response and forensics capabilities to maintain and restore integrity of services (such as the EGI CSIRT group and the eduGAIN Security Capability), vulnerability monitoring and control, and topical vulnerability assessment. By their nature, such infrastructure-bound core services need a thorough understanding of the operational model not only of the infrastructure federation in which they operate, but also of the services that constitute this infrastructure and their operational coherency.

At the edges of each of these categories there is necessarily a complementarity, e.g. in vulnerability monitoring and risk assessment, to ensure that EOSC-wide integrity and service-specific implementation measures connect seamlessly. Yet in broad terms, there is usually a 'natural' classification alongside which a necessary activity can be grouped: underpinning the security across service providers within the EOSC ecosystem as a whole to enable secure composition of services and resources from different providers; or specifically linked to e-infrastructure operators to allow them to open up their services to trusted researchers without unduly increasing their risk.

Trust and integrity services for the consolidated ecosystem

Considerations for the integration of the research infrastructures through the EOSC Portal

Organisations join a dynamic EOSC ecosystem, where service providers emerge, build up composite services, offer their services both to each other and to end-users, and have a natural focus on the functionality offered, including innovations that improve this functionality. Information Security Management (ISM) as well as access management and traceability do not necessarily follow functional innovation, yet are key elements to instil trust in the service for end-users, ensure availability, ease the composition of services, and enable service providers to manage risks. Composition of services between service providers specifically incurs changes in risk profile, usually increasing risk by delegating responsibilities to other parties in the ecosystem over which there is reduced organisational control.

In order to make the EOSC ecosystem trustworthy and secure, and ensure availability, a service provider must do no harm to the interests or assets of users, or – whether on its own or through its interaction with other providers - expose other service providers in the EOSC ecosystem to an enlarged risk as a result of them participating in the EOSC.

With respect to its users, services should be transparent towards the EOSC regarding their ISM maturity, and implement standards and community best practices commensurate with the purpose of the service and the personal and research data processed therein.

With respect to its peer service providers and e-Infrastructure consortia, interaction the service has with those participants clearly must comply with the minimum requirements defined by such underpinning peer services and infrastructures, in addition to meeting their local policy requirements and stated service level. Just as important, however, is their own (self) assessment in terms of the risk change induced in the ecosystem: requirements on traceability, access management and accountability, and operational security cooperation that a peer service provider or infrastructure would customarily apply to its own end-users now become their responsibility. The principle of least privilege must apply, as well as transparency as to how the trust and traceability requirements of partner services are met – following the models of WISE SCI and the Snctfi framework.

The basic premise should be ‘do no harm to your users nor to your peer and underpinning services’.

One of the roles of EOSC is to mediate trust establishment between participating services/users and to help maintain it. In order to attain this, the EOSC will need to provide functions to manage risks, monitor and handle any breaches of operational policies (security incidents), as described here. Based on existing capabilities EOSC will contribute to establishment of trustworthy ecosystem, both on the technology level (AAI, credentials conversions), on the operational level, and on policies.

Collaborative risk management for service composition

The EOSC Portal intentionally brings together services from a wide range of providers that have varying levels of Information Security Management (ISM) maturity. Although all services are ‘production-ready’ and valuable to the EOSC user community, ISM-specific risks may play out differently depending on the sensitivity of the (personal or IPR) data, the amount of data processed, and the impact of incidents on the other services. To enable a true end-to-end risk assessment, either by the data owner or a provider of composite services, requires insight into the ISM maturity as well as operational capabilities of all service providers in the EOSC Portal. The WISE Security for Collaborating Infrastructures (SCIv2) model, which was endorsed by all major infrastructures now

participating in the EOSC, identifies a multi-tier approach to maturity, in which peer review ("reviewed by a collaborating Infrastructure") based on a self-assessment enables a scalable approach to trust that is applicable to the dynamic and research-oriented EOSC ecosystem.

Actions:

- Risk assessment framework for EOSC services (based on WISE SCI)
- Formalised peer reviewed maturity model and mechanisms

Coherency of trust management and implementation measures across the EOSC core services

The ecosystem brings together communities and services from a wide range of stakeholders that will have to establish a basic mutual operational trust in order to interoperate. Interaction between them needs to preserve the risk appetite of the participants involved, so trust should be transparent, comparably formulated, and address existing and emergent usage patterns driven by the user communities. Given that much of the risk is ultimately absorbed by the service providers, shared policies and best-practice implementation patterns will help providing collective services – since if many providers and infrastructures share common practices, research communities can move and compose services without much friction.

The overall aim of the policy and best practice activity is to minimize the number of divergent AAI policies and empower identity providers, service providers and user communities to identify interoperable policies for the open science vision. Aiming at limiting divergence, coherence can be improved by sharing practices and by reflecting collectively on potential implementation measures, address alignment for communities and infrastructures even if structured differently. A 'trust information security alignment' group is needed to identify and reach consensus on which elements are essential - and what level of information assurance is provided.

Such an alignment group can recommend common trust and information security practices, support major stakeholders in maintaining trust between service providers and between infrastructures and communities, and coordinate assurance profiles and operational trust capabilities across the stakeholders in the ecosystem.

Actions:

- Evolve trust availability and security policies to address communities' needs and the requirements of heterogeneous service providers
- Act as reference expert group on cross-service risk acceptance
- Draft implementation measures in response to EOSC portal evolution, describe the implementation measures that will implement this evolution.
- Provide trustworthy sources for trust anchors matching a limited number of common EOSC assurance profile requirements and protocols.

Fostering trusted services

Services in the ecosystem come with varying scopes and maturity levels, yet taken together constitute a single powerful system with many mutual dependencies. The providers comprising this system should be able to leverage expert support in addressing the collective challenges that face them through their participation in the EOSC ecosystem. This means gaining the ability to effectively communicate on trust and integrity issues; augment the maturity level of service providers in terms of trust management, resilience, incident remediation, and investigation capability; and to exercise these elements periodically so that all stakeholders are able to react as and when needed.

Actions:

- Security Communications exercises across EOSC service providers and infrastructures
- Development of trust and operational security maturity training
- Advanced forensics training for providers in order to maintain integrity of the EOSC ecosystem
- Development of best practice and guidance for secure service alignment
- *Optionally* training for trust maturity development and secure joining

Trust and response posture & resolution capabilities

The growth and inter-connection of federations and research infrastructures has created new vectors of attack that expose the EOSC to cybersecurity risks. Compromised identities can provide access to a multitude of services across the ecosystem and across service providers and infrastructures. Since a centrally coordinated incident response capability within the EOSC community does not - and cannot - exist, participants must collaborate to mitigate the risk of future incidents, yet the maturity of security operations across the service providers is variable, and often unknown to the peers and users. Frameworks such as Sirtfi - developed in a global collaboration and supported by AARC - recommends core practices, and provides information that can support all participants to become 'effective actors' in maintaining the cybersecurity cyber-security posture.

Resolving those incidents that do happen, similarly requires close coordination between a potentially large number of affected communities and services. As incidents by definition are not limited to just one participant, their mitigation, containment, and ultimate resolution requires a collective response that spans the various areas of service offerings, all users, and service providers

Actions:

- Exchange and liaison in operational security response to cyber security events
- Global interoperability of trusted response teams
- Cooperation with peer infrastructures from both the research infrastructures and commercial service providers, including specific collaboration with eduGAIN and GEANT *optionally including* emergency response capabilities to ensure secure, reliable and traceable resolution of incidents that affect the functional abilities of the EOSC ecosystem as a whole

Trust and collaboration operational (AAI supporting) services

Establishing the trust infrastructure requires *coherent organisation of credentials* (at several assurance levels matching the service infrastructure risk profiles), alignment of *credential acceptance* across the infrastructures, and an *Authentication and Authorization infrastructure* (AAI) supporting the access management to service can profitably be based on the AARC Blueprint Architecture (BPA) and leverage industry-standard protocols and interoperability profiles.

The underlying requirements on the AAI are well understood qualities: *access coherency* (a common way to allow delivery of collective services), *collective access* to services (e.g. by brokering through science gateways or in service composition), and *delegation of capabilities* (so that agents and services can act on behalf of a researcher and community without exposing the user to undue risks).

The Community and infrastructure AAI must be aligned with industry standards (from the IETF, OASIS/W3C, and the OpenID Forum) and engaged in the evolution of the AA mechanisms to ensure continued interoperability with service providers and the e-Infrastructures, including global providers. Alignment with the ESFRI clusters that share those requirements will enable re-use of both technology as well as integration with operational (AAI proxy) services.

The AARC 'Community-first' BPA model will need to evolve to support a wide mash-up of proxies and provider infrastructures that are to characterise the open EOSC ecosystem. Communities by themselves emerge as service providers towards their peers, resulting in composite, hierarchical, service offerings. The access control underpinning such composite services by itself creates recursive dependencies in the AAI layer that will grow beyond the current 'community-first' BPA model – a development that will be of paramount importance as open and FAIR data will be combined across research verticals, whilst preserving the necessary confidentiality of e.g. personal, privacy-sensitive data.

Actions:

- Evolution and deployment of a mesh of AAI services aligned with the AARC Blueprint Architecture (BPA), supporting national-level gateways, those of the generic pan-European e-Infrastructures, and domain specific and global proxies.
- Risk-aligned assurance mapping services to allow researchers to translate tokens operative in global and domain verticals, such as RCauth.eu, and CILogon at the global level, cross-service integration of non-academic IDs (including eIDAS as well as social ID), and supporting token translation services. Since the requisite trust fabric, by necessity spans all infrastructures, such components are most logically placed as a logically-single (if distributed) entity for the EOSC.
- Evolution of community and group management standards, specifically enabling cross-domain use of generic services (most likely based on capabilities and hierarchical AAI proxy composition)
- *Supplementary topics and activities can be envisioned in this area, in alignment with the AAI in the EOSC Architecture*

Trust and integrity for the distributed resource Infrastructures

Considerations for the increased service offerings in the EOSC ecosystem

Each infrastructure delivering research-enabling services should include both mechanisms that ensure integrity, availability, and trust for the services offered to the EOSC, as well as integrate with the activities of the EOSC ecosystem at this level. This comprises policies and implementation measures specifically attuned to the type of services offered by the infrastructure to the EOSC portal, as well as technical mechanisms and operational controls to identify, contain, mitigate and resolve incidents impacting security and availability in line with service provider and EOSC Portal requirements. For example, ensuring that a service does not adversely impact the risk of peer services and users of the infrastructure is most efficiently performed at the Infrastructure level when multiple providers offer services in a similar manner using similar technology.

Although the individual service providers have their own responsibilities with respect to trust and integrity protection, information security maturity, and operational response, they also have a collective responsibility at the infrastructure level. Since seamless access across services, and the provisioning of collective service components, are their raison d'être in the ecosystem, and they share common threat exposure, a coherent perimeter response is required. Such a collective response and the technical ways to provide that, both pro-actively in monitoring and vulnerability management as well as retroactively in operational incident response, are an integral part of service provisioning. The means required are thus part of the cost of a unit of access to services and infrastructures.

Integrity and vulnerability compliance monitoring

Providers of services to the EOSC ecosystem have an autonomous responsibility to meet their stated trust maturity, where for infrastructures and services that are intended to be generic and re-used for a wide range of composite services and use cases their maturity should be supported by effective integrity and security monitoring. This support individual service providers in assessing their status and capabilities, and provides the infrastructure with the key indicators of maturity at the collective level and a way to support improvement of both the ISM maturity as well as the maturity level of the service providers contributing to the infrastructure.

Actions:

- Operation and evolution of vulnerability identification and assessment tools specific to the services provided in the infrastructure
- Support for service provider self-inspection and assessment, complemented by external probing supported by infrastructure-level expert team, which jointly provide a view of service resilience to integrity threats
- Follow-up for identified threats to service providers by the infrastructure, to support resolution and iterative maturity improvement

Continuity and recovery from incidents

The progressive federation of services and resources will increase the interdependencies between service providers, for any of the service federations involved. Incidents spread more rapidly among service that share common components and users, and containment, forensic analysis, and remediation across similarly-affected service providers requires a central capability that has deep knowledge of the service structure. Products used to provide services are often shared, and systems

architectures comparable – and maintaining a high response readiness level will maintain higher over-all user service availability and trust in the ability to provide more sensitive services.

These teams need to engage with and be trusted by the European and global operational security community, and maintain standing relationships with academic, commercial, and governmental and law enforcement peers. Leveraging technical and policy maturity knowledge of the services in the federation, and the ability to contain and manage threats to the services, will benefit service providers and their research communities alike.

Actions:

- Provisioning of a (TI accredited/certified) incident response team providing emergency security incident response coordination across the infrastructure services
- Provisioning of advanced forensic capabilities to address and mitigate security incidents, limit their spreading, and support restoration of continuity
- Maintain global liaison with academic, industrial, and government/LE peers to provide early/rapid response and advance warning capability and collect and share threat intelligence
- Planning and execution of readiness posture, and map-table crisis management, exercises

Service vulnerability management

The coherency of the service offerings through e-Infrastructures in the EOSC is both an advantage as well as a risk for in terms of service vulnerability. The use of common service components and software eases lateral movement for attackers that exploit the homogeneity of the infrastructure, but it also provides a unique way of accelerating collective response to threats and vulnerabilities that can be assessed once in the context of the service offering, and then such an assessment will be valid across a larger range of service providers. Since this hold in particular within an ensemble of coordinated service offerings (the infrastructure), it naturally aligns with the scope and implementation model of the distributed resource offering.

Actions:

- Assessment of reported and identified vulnerabilities in operational services, and provide specific recommendations to service providers in the infrastructure based on an infrastructure-specific risk assessment

Trusted access mechanisms for infrastructure resources

Actions:

- E-Infrastructure AAI proxies and capability coordination services (aligning shared service properties of the infrastructure services involved)
- User credential management services and token-translation bridges (to support the use of services with common capabilities in the infrastructure in a non-interactive and agent/broker based model)