RCauth.eu

A Research and Collaboration Authentication PKIX Service for Europe

RCauth.eu Governance Model

version v02-20180110

Document Revision Information

Document Identifier	1.3.6.1.4.1.10434.4.2.8.2.1.1
Document Version	v02-20180110 (DRAFT)
Last Modified	2018-01-10
Last Edited By	David Groep

Table of Contents

1 INTRODUCTION **3**
1.1 STAKEHOLDERS 3
1.2 MISSION 3
1.3 PRINCIPLES AND VALUES 3
1.4 MANAGEMENT GUIDANCE 5
1.5 NAMES AND BRANDS 5
1.6 BODIES AND THEIR RESPONSIBILITIES 5
1.7 ESTABLISHMENT AND GOVERNANCE BYLAWS 6
2 GOVERNANCE BOARD **7**
3 POLICY MANAGEMENT AUTHORITY **8**
4 OPERATIONAL MANAGEMENT **9**
5 REFERENCES **10**

Document Revision History

Version	Date	Comments
0.1	*2017-11-13*	*For consultation with AARC PMT and policy leads*
0.2	*2018-01-10*	*Clarified language and moved responsibility description*

1 INTRODUCTION

The RCauth.eu service is a token translation service (TTS) that can on-the-fly identify entities based on federated credentials and issue to them PKIX credentials in real-time, focussing on converting SAML-to-PKIX. It is based on the results of the AARC (AARC Consortium, 2015) Pilot to introduce CILogon (Basney, Fleury, & Gaynor, 2014) like capabilities for European Infrastructures. The AARC pilot system comprises several components, as discussed in its sustainability model study (Groep, 2016). The Delegation Service is identified in the model study as a single component that would particularly benefit from having just a single instance for Europe, serving all relying parties equally in an open, collaborative, and non-discriminatory fashion. In particular, it should be open to all Research Infrastructures (both pan-European and otherwise) and the generic e-Infrastructures that would be accepting and relying on the credentials emanating from the RCauth.eu token translation service.

1.1 Stakeholders

The RCauth.eu service recognises as Qualified Stakeholders those Research Infrastructures, user communities, and users that use RCauth.eu credentials for their acceptable usage, and (generic) e-Infrastructures and others that rely on the credentials issued by RCauth.eu to address (part of) the risk involved with providing service to qualified holders to RCauth.eu credentials and that contribute in material or non-material ways to the continuity of the service (Qualified Relying Parties).

1.2 Mission

The mission of RCauth.eu is to enable publicly (co-)funded research collaboration for Research and e-Infrastructures based in Europe, by providing trustworthy PKI authentication and credential translation services to end-users, and trust services to relying parties, based on externally sourced federated identity management in its broadest sense, regardless of technology, nationality, or organisational affiliation.

1.3 Principles and Values

The RCauth.eu service implements the scalable policy negotiation principles of AARC through adherence to the following principles of trust:

- RCauth.eu shall always primarily consider benefit to the research and innovation capabilities of global, cross-national, and national Research and e-Infrastructures in all decisions made in governance, management, and implementation, whilst taking due regard of practicality and of appropriate representation by its stakeholders, and with consideration to the global research and innovation ecosystem. *In all decisions they make, Qualified Stakeholders, the Stakeholders that materially contribute to the service, its subscribers, and its Qualified Relying Parties are to take due consideration of also those other individuals, organisations, and infrastructures outside their own group, in order to fully implement the Mission of the service.*
- The service must be accessible to any qualified person that has a federated identity, or can be provided with an appropriate federated identity by an Infrastructure. No costs shall be charged to qualified subscribers or to relying

parties for access to the service, and cost shall be no barrier to supporting qualified subscribers. *The service should be obtainable for any organization, regardless of the (European) country in which they are based, and regardless of business model considerations by the country, national research network or e-Infrastructure organisation, or (national) bodies where the home organization (or person) is based. Insofar as global research can be considered related in some manner to a European entity, it should be accessible to researchers world-wide. It should be possible to join the service as an identity provider independent of whether there is a national identity federation, whether a national identity federation has joined or not joined an inter-federation scheme such as eduGAIN – within reasonable limits of available effort on behalf of the RCauth.eu service. In particular, Research and e-Infrastructures must be able to join as identity providers of last resort. Reliance information, including credential status information, shall always be provided at no cost to relying parties, regardless of their location, organisational form, or relationship with the service.*

- The service shall meet assurance requirements commonly agreed amongst the European Research Infrastructures and e-Infrastructures, and proactively engage in developing standards and accreditations that support the Mission of the service.
- Wherever possible it leverages inter-federation (eduGAIN) and the relevant trust marks and brands (Entity Categories) and assurance profiles. Yet the service shall allow for exceptions and explicit trust relationships where this aim would conflict with the primary aim of ubiquitous availability. *For example, the REFEDS R&S category combined with the Sirtfi incident response scheme combined meet current commonly agreed assurance requirements. Yet in absence of a federation or identity provider asserting or being able to assert these qualities technically, a materially equivalent commitment may be used in lieu of such an entity category tag – permitting the service to break the 'adoption barrier' and serve its primary aim of ubiquitous service – as long as this commitment is substantiated, scoped, and open to external assessment (i.e. considered by the RCauth.eu policy management authority).*
- The RCauth.eu service operation should not inadvertently take on liability or risks that are beyond its domain of authority or influence, and its Qualified Relying Parties shall acknowledge that the service is a collaborative effort based on peer review and on appropriate assessments that will always be publicly documented. *For example the service may in good faith rely on an entire global inter-federation as well as many other entities, yet it should not assume full liability for everything emanating from such domain, as no service operators can subsume such risk to operate the proxy service. Identity sources must be willing and able to absorb the risk for any incidents originating there without compromising the trust given to the service itself by its Qualified Relying Parties (Infrastructures). Since the Infrastructures (being direct stakeholders) are inherently motivated to collaborate, a peer-review, transparent and assessable policy model will suffice to maintain such trust – the more so since most stakeholders are directly represented as relying parties in the IGTF peer review process and assessments.*
- Wherever transparency does not compromise trust relationships with subscribers, Qualified Relying Parties, or accrediting bodies, the proceedings of the RCauth.eu service shall be open, and its positions taken towards its peer and accreditation bodies be openly discussed.

1.4 Management Guidance

The RCauth.eu service management shall ensure that the service:

- provides appropriate availability and reliability for the research services it supports
- documents all its policies and processes in a Certificate Policy (CP) and in a Certificate Practice Statement (CPS) in accordance with international and internet standards
- maintains accreditation at the relevant assurance levels with the Interoperable Global Trust Federation IGTF through participation in the EUGridPMA and other relevant standardisation bodies
- is compliant with applicable national and international legislation
- provides at least IGTF-DOGWOOD level assurance credentials to its subscribers
- is operated as a single collective entity with respect to its policy, practices, trust anchor materials, operational security, and business continuity and disaster recovery process
- interconnects with the eduGAIN interfederation service and provides suitable and state-of-the-art discovery and filtering-proxy capabilities
- provides and implements a process for connecting with and recognising credentials from other federated identity management systems that support the mission of the service
- provides and implements a process for assessing the consistency of its operational partners with respect to management of key material, access credentials, site and systems security, and any other aspects that impact trust and reliability
- provides and implements processes for key material roll-over, expiration, and introduction of new key material and trust anchors in support of the service

1.5 Names and brands

The RCauth.eu brand and domain name shall be managed by Nikhef on behalf of the consortium of Qualified Stakeholders and the Governance Board in support of the mission of the RCauth.eu service and in accordance with its principles and values. If Nikhef is no longer able or willing to maintain such registrations and domain name management, the Governance Board shall unanimously decide on a new legal entity to take on management of the brand and domain name. In absence of such a decision, Nikhef shall have the obligation to main only such registrations that are necessary to permit such a decision to be deferred.

1.6 Bodies and their Responsibilities

The RCauth.eu governance structure shall consist of

- a Board of stakeholders comprising representatives for the stakeholders of the service that materially contribute to the sustenance of the service;
- a Policy Management Authority (PMA), consisting of individual policy and identity experts from the stakeholder community, to which the Board entrusts an independent responsibility to manage the trust and operational policies;
- an Operational Management Team consisting of representatives of all partners that collective provide the RCauth.eu service which, under the authority of the

PMA, is responsible for the continued operational availability and operational compliance.

1.7 Establishment and governance bylaws

The Governance of RCauth.eu and the terms of reference for the Governance Board and the Policy Management Authority (PMA) shall be maintained by the Governance board. Changes to the terms of reference and the Governance bylaws shall be taken through unanimous decisions, having heard and taken into consideration the position of the Qualified Stakeholders in its widest sense.

The initial composition of the Governance Board shall be of one representative and one alternate for each of the following five materially-contributing Qualified Stakeholders: *stichting EGI*, *STFC* (*UKRI*) representing the EUDAT collaboration, *vereniging GEANT*, and *Nikhef* (representing stichting NWO-I and cooperatie SURF u.a.). *PRACE ivzw* shall be invited as an observer to the Board for as long they do not yet materially contribute to the service, with a view to become a full member.

The initial composition of the Policy Management Authority shall be: (tba)

2 Governance Board

The Board will be comprised of representatives of those Qualified Stakeholders that contribute materially to the operation or sustenance of the RCauth.eu Service and that subscribe to the mission, principles, and values of the Service as stated in section 1. Each Qualified Stakeholder shall have a lead representative and an alternate on the Board.

The governance board shall be responsible for

- ensuring continued and adequate material support for the service
- ensuring the service fulfils its mission and adheres to its principles and values
- appointing and dismissing Policy Management Authority members based on the recommendations and nominations of the Policy Management Authority
- designate and support the operational management and the operational coordination team without prejudice to the autonomy of each of the materially contributing Qualified Stakeholders
- liaising with current and prospective Qualified Stakeholders to ensure the service meets and continues to meet the needs of its target audience
- rule on all aspects that are not otherwise covered in the mission statement, the principle and values, this Governing Model, the CP and CPS, and that cannot be resolved by the Policy Management Authority

The governance board may decide to terminate the service only by unanimous vote following a one-year consultation period with all Qualified Stakeholders, and then only in accordance with the CP and CPS policies. The Governance Board must positively support proposals by other groups that would be willing to continue the service, if such groups are qualified to operate, maintain, and support the service in the fulfilment of its mission, and based on the principles and values of the service.

3 Policy Management Authority

The RCauth.eu Policy Management Authority (PMA) shall be composed of individuals drawn from the wide community of Qualified Stakeholders who are experts in the field of identity management for research and collaboration, PKI technology and identity bridging.

The PMA shall have at least 3 members. The members of the PMA shall exercise their duty independently and on a personal basis. Personal overlap between members of the PMA and the Governance board is permitted (bearing in mind the terms of reference of the PMA with regards to technical policy development and identity management specialisation).

The PMA members shall be appointed or dismissed by the Governance Board, based on nomination by the current PMA membership. PMA members may step down on their own accord.

The PMA shall be responsible for

- implementing the Management Guidance
- monitoring the operations of the service by the operational team(s) with respect to the Mission and the CP and CPS policies and practices
- ensuring continued accreditation of RCauth.eu to the IGTF and other relevant accreditation bodies
- informing the Governance Board about requisite changes to the CP and CPS policies and practices
- liaising with standardisation and technology groups to improve and evolve the service to further the fulfilment of its mission
- proposing new PMA members to the Governance Board

4 Operational Management

The operational partners providing the RCauth.eu service, so entrusted by the Governance Board and the Policy Management Authority, shall establish an operational coordination team. This team shall be responsible for the day-to-day provisioning of the service, implementing the decisions of and reporting to the Policy Management Authority, resolving issues of availability, reliability, and access to the service, and for the maintenance of any registries so-designated by the Policy Management Authority.

The operational coordination team shall maintain at least:

- records of all places where trust anchor key material is maintained
- a registry of directly-connected federated identity providers, including such documentation submitted by them to assert compliance with the CP and CPS
- a registry of connected credential repository and management systems that are connected as clients to the RCauth.eu delegation service instances, including such documentation submitted by them to assert compliance with the CP and CPS
- any audit records maintained or prepared for assessment by the Policy Management Authority
- a list of Qualified Stakeholders and contact information to the extent to which these have registered themselves to receive information from the RCauth.eu service

The operations team shall pro-actively communicate operational information to connected credential repositories and to those Qualified Stakeholders that have expressed interest in receiving operational communications.

5 References

AARC Consortium. (2015). *AARC Project*. Retrieved 11 07, 2017, from http://aarc-project.eu/

Basney, J., Fleury, T., & Gaynor, J. (2014). CILogon: A Federated X.509 Certification Authority for CyberInfrastructure Logon. *Concurrency and Computation: Practice and Experience, 26*(13), 2225-2239. Retrieved from http://dx.doi.org/10.1002/cpe.3265

Groep, D. (2016). *Models for sustaining the RCauth.eu service.* AARC Project. Retrieved from https://wiki.geant.org/download/attachments/56918657/AARC-sustainability-models-for-RCauth-20160506.pdf