RCauth CA

A Research and Collaboration Authentication CA Service for Europe

RCauth ICA CP/CPS

version 2 (v04.04-20200710)

Document Revision Information

Document Identifier	1.3.6.1.4.1.10434.4.2.8.1.2
Document Version	v04.04-20200710 (CP/CPS version 2)
Last Modified	2020-07-10
Last Edited By	David Groep

Table of Contents

Document Revision History

Version	Date	Comments
1.0	*May 9th, 2016*	*Initial version (accredited)*
1.0.2	*Jan 22nd, 2017*	*Updated description of USR generation, mapping the plus-sign to a hyphen-minus sign since the plus-sign is reserved in RFC2253*
1.0.3	*May 22nd, 2017*	*Non-normative operational change in rendering of non-Latin1 characters, limiting amount of non-transliterated glyphs.*
2.0	*January 2019*	*Reflected changed management of RCauth to dedicated PMA under terms of Governance Model and adapt to support multiple issuing instances of the RCauth ICA.* *The RCauth.eu service is no longer a Pilot service (although the subject name of the RCauth.eu ICA will remain unchanged)* *Clarification of terms and roles (specifically those of Administrators and Operators) in view of the role of the PMA.* *Changes to privacy notice clarifying right to complain under GDPR.* *Reflected insourcing of off-site backup at the Nikhef instance (dislocation now logically within the Nikhef organisation itself).* *Added operational and site security sections for all operating partners.* *Listed all operational partners: Nikhef, STFC, GRNET.* *Corrected multiple minor inconsistencies.*
	March 2019	*Incorporated configuration draft for RAL (UKRI-STFC)*
	July 2020	*Incorporated configuration description for GRNET*

1 INTRODUCTION

1.1 OVERVIEW

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.

This Certificate Policy and Certification Practice Statement is pertinent to the (white-label) Research and Collaboration Authentication Issuing CA ("RCauth ICA"), operated under the Authority of the RCauth Policy Management Authority. It is a subordinate CA of the DutchGrid (DCA) Root CA, to whose policies this Issuing CA adheres.

The DCA Service operates a set of PKI X.509 certification authorities (CAs), including self-signed issuing CAs (e.g. the DutchGrid and Nikhef Medium-Security X.509 Certification Authority), a Root CA that only certifies subordinate CAs, and a set of subordinate issuing CAs (ICAs).

The RCauth ICA issues certificates to end-entities based on a successful authentication to a Federated Identity Management System (FIMS) operated by an eligible Registration Authority – typically a FIMS Identity Provider (IdP) operated by an academic or research organisation. The certificates issued by the RCauth ICA are valid for a period of at most 13 months, but will be as short as 1Ms when certificates are requested by a credential management system (user agent) that stores credentials in activated form.

CP and CPS incorporate the requirements of RFC 3647 and of the Authentication Profile for Identifier-Only Trust Assurance with Secured Infrastructure version 1.0 of the European Grid Authentication Policy Management Authority.

1.2 DOCUMENT NAME AND IDENTIFICATION

This is the RCauth ICA Certificate Policy and Practice Statement. It is generally identified by urn:oid:1.3.6.1.4.1.10434.4.2.8.1.2. This version is specifically identified as urn:oid:1.3.6.1.4.1.10434.4.2.8.1.2.0.

The document shall be referenced as the "RCauth ICA CP/CPS".

The "Research and Collaboration Authentication Pilot Issuing G1 CA" (2016 edition) shall be referenced as the "RCauth ICA" (G1).

1.3 PKI PARTICIPANTS

1.3.1 Certification Authorities

The RCauth ICA is an on-line CA that issues certificates to end-entities involved in research and collaborative use cases across research infrastructures and e-Infrastructures.

The CA is operated by a consortium (the Operating Partners) that is collectively managed as a single coherent and non-severable whole by the RCauth.eu Policy Management Authority (PMA) established by the RCauth.eu Governance Board under the terms of the Governance Model[1].

The Operating Partners each operate a geographically distinct and separate on-line CA instance, interconnected with a secure private link as described in section 6, coherently issuing end-entity certificates that meet all policy criteria at the collective level. Although each issuing instance may be registered with a different Federated Identity Management System and can autonomously authenticate and determine eligibility of its subscribers and end-entities, any issuance is subject to the common criteria, and issuance state (such as the assignment of unique serial numbers amongst all certificates issued) is maintained coherently between all instances.

The issuing instances shall be coordinated by the Operations Coordination Team established by the Governance Model under authority of the PMA, and shall be located at:

- Nikhef, Amsterdam, The Netherlands ("Nikhef")
- UKRI-STFC Rutherford Appleton Laboratory, Didcot, Oxfordshire, UK ("RAL")
- National Infrastructures for Research and Technology GRNET, Athens, Greece ("GRNET")

The Operating Partners shall each designate an Administrator responsible to the PMA for the operation of their issuing instance, one or more Operators responsible for the Service, and one representative to the Operations Coordination Team. A single person may hold one or more of these roles; specifically, the Administrator may be (but is not necessarily) the representative on the Operations Coordination Team.

1.3.2 Registration Authorities

The RCauth ICA delegates all the registration authority operations to the organisations that are responsible for its eligible identity providers connected through the Federated Identity Management System (FIMS). Thus, the organisations operating such identity providers are effectively the Registration Authorities (RAs) of the RCauth ICA. In particular, it uses as a source of authenticators the ensemble of identity providers in eduGAIN, limiting it to entities in eduGAIN that meet the policy requirements of this CA.

The FIMS may include specifically identified providers of authenticated identity (IdPs), as well as federations of entities that convey – directly or indirectly – trust in a collection of IdPs and provide a technical means to convey authentication and attributes or to assert a way of validating the correctness of the authentication and attributes received from the IdP.

Where the CA itself connects to a FIMS that relays information in-line regarding third-party IdPs and other FIMS, it will verify that the policies of such a FIMS are compliant with the requirements of this CP/CPS on all relevant aspects.

With respect to the IdPs directly connected to the SURFconext FIMS to which also this CA is connected, the FIMS policies are adequate since the organisations responsible for the IdPs within SURFconext, having signed Annex IX to the SURFnet contract, are deemed to have entered into an implicit agreement with the RCauth ICA, since the RCauth ICA is itself a Service Provider within SURFconext.

Organisations operating IdPs within eduGAIN but outside SURFconext, by both asserting compliance with Sirtfi[2] and REFEDS R&S[3] section 6, by asserting a non-reassigned identifier, and by permitting attribute release to the RCauth ICA Service, are deemed to have entered materially into an agreement with the CA in that Sirtfi compliance implies meeting the requirements on traceability of credentials in a cooperative way, and by meeting the uniqueness requirements through adherence to R&S.

[1] https://rcauth.eu/governance

[2] https://refeds.org/SIRTFI

[3] https://refeds.org/category/research-and-scholarship

Other organisations operating IdPs, either directly or through and by virtue of their federation implementing binding policies materially equivalent to Annex IX of the SURFnet contract, may conclude specific agreements directly with the CA in order to become eligible registration authorities as subsequently specified in section 3.2. Such IdPs may also be run on behalf of communities and (research) infrastructures.

1.3.3 End Entities

The RCauth ICA shall only issue certificates to human users that are affiliated with an eligible Registration Authority as stipulated in section 1.3.2. The IdP of the RA may further restrict the set of end-entities affiliated with the RA according to its own eligibility policies.

By authenticating end-entities, the RA asserts that the data provided for the end-entity is correct and valid at time of issuing the assertion, and that the requirements on uniqueness and traceability are met.

1.3.4 Relying Parties

Relying parties are individuals or organizations using the certificates to verify the identity of end-entities signed by the RCauth ICA. This CP/CPS does not limit the community of relying parties.

1.3.5 Other participants

Where software agents and credential repositories are used by applicants, and where such repositories are used in a way where they have to establish a relationship with the RCauth ICA, the CA shall recognise such repositories as trust participants.

The RCauth.eu PMA is an element of the governance structure as described in the RCauth.eu Governance Model Document: https://rcauth.eu/governance.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Usage

Certificates issued by this CA are intended to be used in compliance with this CP/CPS.

The certificates issued by the RCauth ICA are not appropriate for any application other than for science, research, and innovation, and then for the purpose of (cross-organisational) distributed resource access, solely in the context of academic, research and similar, not-commercially competitive, applications.

The RCauth ICA certificates are primarily intended for the practitioners of scientific research that are supported, enabled by or work in collaboration with ICT infrastructures for research, and for ancillary, collaborating, and affiliated projects, infrastructures, communities and endeavours, appropriately taking into account the global nature of research and collaboration.

1.4.2 Prohibited Certificate Usage

Certificates shall be used exclusive in compliance with this CP/CPS – other use is prohibited.

Certificates must not be used for unlawful purposes, and must not be used in any way that could harm, be defamatory, cause injury, or be detrimental to the reputation, safe operation or good standing of the RCauth ICA, the DCA Service, the RCauth.eu Operating Partners, members of its governance bodies, Nikhef or its partners and personnel, or SURF, or if the use would result in liability (financial or otherwise) of any of the Operating Partners and members of the RCauth.eu governance bodies, or any individual involved in the operation of the Service.

1.5 POLICY ADMINISTRATION

1.5.1 Organization administering the document

This document is administered by the RCauth.eu Policy Management Authority (PMA) as established under the terms of the Governance Model. The Organisation contact details are:

RCauth PMA c/o Nikhef

Science Park 105, NL 1098 XG Amsterdam, The Netherlands

Phone: +31 20 592 2000, Fax: +31 20 592 5155

Email: pma@rcauth.eu

The Administrators report to the Policy Management Authority of the RCauth ICA.

1.5.2 Contact person

The RCauth ICA is operated under the responsibility of the Operational Coordination Team:

RCauth Operational Coordination Team

operations@rcauth.eu

The responsible Adminstrators of the RCauth ICA are the members of the PMA as listed in the Governance Model document, which may be found at

http://rcauth.eu/governance

1.5.3 Person determining CPS suitability for the policy

This document contains both the Certificate Policy and the applicable Certification Practice Statement, hence the CPS suitability determination is part of the CP/CPS approval process of the RCauth.eu PMA as well as that of any higher-level CA's PMA.

1.5.4 CPS approval procedures

Changes to the Certificate Policy and the Certification Practice Statements are approved by the PMA, having consulted with relevant accreditation and representative stakeholder bodies. For IGTF IOTA AP compliance this is handled by the EUGridPMA.

1.5.5 Modification of the CP/CPS

Modifications of the CP/CPS may be done any time. Changes will take affect after 14 days following its adoption by the PMA in accordance with section 1.5.4, and having been published.

If material changes of referenced policies and schemata i.e. REFEDS R&S, Sirtfi, SURF Annex IX, eduGAIN Declaration, or REFEDS “MACE-dir” occur that effect the core requirements that the ICA has in these, this CP/CPS will be modified.

1.6 DEFINITIONS AND ACRONYMS

Conventional PKI definitions apply. The following terms are specific to this document:

RCauth ICA	The first generation issuing CA for end-entities that is established under this policy and to which this document pertains
Service	The ensemble of services and CAs offered by the DCA or the RCauth.eu ICA
RCauth.eu PMA	The body responsible for the management of policy and adjuration of issues related thereto with respect to the RCauth ICA, and 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.
Administrators	The individuals at the Operating Partners responsible for the technical deployment and implementation of the Service and for ensuring its continued compliance with the Policy and documented Practices and with the PMA decisions
Operators	The individuals at the Operating Partners that can issue certificate and publish updated revocation information for the specific CA for which they have been granted an operational privilege.
DCA	DutchGrid and Nikhef Certification Authority
DCA Root	The self-signed off-line root certification authority of the DCA
FIMS	Federated Identity Management System: the system or hierarchy of systems through which applicant authenticate to the CA
IdP	Identity Provider that is part of or connected to a FIMS and which acts as a source of authentication and applicant attributes
SURFconext	The FIMS collective service through which the CA connects to FIMS IdPs, including to eduGAIN IdPs, in the Netherlands
eduGAIN	The constituency of Identity Federations primarily engaged in research and education and the service provided to them that enables them to inter-federate.
Operating Partners	Those organisations that operate and maintain (part of) the RCauth.eu ICA infrastructure and that are therefore represented in the Operations Management Team.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The RCauth ICA shall publish its own certificate and its policies, a reference to its issuing and cross-signed authorities, and ancillary public document in an on-line accessible repository at

https://www.rcauth.eu/

The RCauth ICA shall publish revocation lists at

http://crl.rcauth.eu/pilot/g1/crl/crl.crl

and as listed in the repository indicated above.

2.2 PUBLICATION OF CA INFORMATION

The RCauth ICA shall make the following publicly available on the relevant on-line repositories:

1. The RCauth ICA's certificate in at least DER encoding, and with a textual representation thereof
2. A DER-formatted CRL
3. A copy of this CP/CPS document and of any previous versions pertaining to valid issued certificates.
4. A copy of its Governance Model document
5. A reference to its superior issuing CA(s)

2.3 TIME OR FREQUENCY OF PUBLICATION

Changes to the materials contained in the repository shall be published promptly.

The CRL will be published promptly after each revocation, and at least once every 24 hours.

2.4 ACCESS CONTROLS ON REPOSITORIES

The RCauth ICA imposes no access control restrictions for read access to the published information including policy, certificate, issued certificates and CRLs. Excluding reasonable scheduled maintenance or unforeseen failures, the repository will be available on a continuous basis.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

The RCauth ICA assigns subjectName in each of its issued certificates as non-empty X.501 distinguished names (DNs). Each assigned subjectName identifies a single entity and shall never be re-assigned to any other entity.

The issuerName in the issued certificates shall be set to the name of the RCauth ICA, which is represented as a non-empty X.501 DN.

The subjectName shall be structured as a sequence of RDNs that starts with a determined prefix "/DC=eu/DC=rcauth/DC=rcauth-clients", followed by an organisation (O) RDN, followed by a commonName (CN) RDN. The value of these is set as specified in section 3.1.2.

3.1.2 Need For Names to be Meaningful

The subjectName will represent the end-entity CA in a clear manner, taking into account the structure of the FIMS on which it relies. Each subjectName of an end-entity certificate will contain an organisation name as organisation name (O) attribute and a common name as CN-attribute.

The CN attribute will identity the individual applicant and contain a unique identifier constructed by the CA that will be unique and non-reassigned across all certificates issued by the RCauth ICA. The organisation name (O) is not essential to providing the uniqueness properties of the subject name, but solely identifies the FIMS IdP used to authenticate the applicant.

The length of the attribute values for the CN and O attributes are limited to 64 characters (code points). Where necessary, elements and element fragments will be uniquely shortened by taking the first 16 characters of the base-64 encoded binary representation of the SHA-256 hash of the value, with any SOLIDUS ("/") and PLUS ("+") characters replaced by HYPHEN-MINUS ("-") characters[4]. This method is hereafter referenced as the Unique Shortened Representation (USR).

The organisation name (O) attribute will indicate which FIMS IdP originated the identified applicant. It will do that based on automated data and meta-data supplied through the FIMS in the following order of preference:

1. The value of the schacHomeOrganisation attribute (oid 1.3.6.1.4.1.25178.1.2.9)
2. The organisationDisplayName as contained in either an attribute or the relevant FIMS meta-datadistribution
3. If the IdP entity ID is a URL: the domain name element of the entityID.
4. If the IdP entity ID is a URN: the entityID

If the organisation name is longer than 61 characters, only the first 61 characters will be used, followed by 3 FULL-STOP (".") characters. The mapping between the truncated and the full organisation name will be recorded by the CA.

The CA will record the mapping between the IdP entityID, the scope, the organisationDisplayName if present, and the value of the organisation (O) attribute in the name.

The commonName (CN) will contain the name of the applicant as asserted, vetted, and authenticated by the FIMS IdP. It is a representation of the applicant's asserted name. It is formed in order of preference as:

1. The value of the displayName attribute from the IdP

[4] This mapping leaves 96 bits of entropy of the hash and a collision probability of 1 in 10^{28}.

2. The value of the givenName attribute, followed by a space, followed by the value of the sn attribute from the IdP
3. The value of the commonName (cn) attribute from the IdP

When the applicant name so constructed contains characters outside the set of PrintableString, these characters shall be minimally-casted to their closest PrintableString equivalent or – when such is impractical because no single-character mapping exists – shall be replaced by the upper-case character "X".

When the applicant name so constructed is longer than 40 characters, it will be truncated after 40 characters and three FULL STOP (".") characters will be appended to it.

A white space (" ") plus a uniqueness-ensuring element will be appended to the commonName part constructed above. The uniqueness-ensuring element will be the USR of a uniqueness identifier provided by the FIMS IdP. As the FIMS uniqueness identifier shall be used, in order of preference:

1. The value of the eduPersonUniqueID attribute (scoped) from the IdP
2. The value of the eduPersonPrincipalName (scoped) attribute from the IdP
3. The value of the eduPersonTargetedID value as constructed by federation software out of solely the IdP entityID and the IdP-local opaque value (the IdP entityID concatenated with an exclamation mark followed by the IdP-local opaque value)

The mapping between the constructed USR and the full attribute value is recorded by the CA. The scope stated in the scoped attribute values will be verified against the permitted scopes in the registered meta-data for the IdP.

If it is needed to ensure uniqueness of the commonName element, as determined by the CA heuristics[5], a white space followed by a decimal integer sequence number of at most 3 positions will be appended by the CA. This sequence number will be recorded by the CA. Determination of uniqueness will take into account name construction across all instances of the issuing CA: assignment of the sequence number shall be transactionally protected against duplication.

The subjectAlternativeName may contain zero or more rfc822Name attributes, which – when present – will contain the values of the mail attribute as provided by the FIMS IdP. When mail addresses are provided by the IdP, they will always be included in the subjectAltName.

3.1.3 Anonymity Or Pseudonymity of Subscribers

The RCauth ICA will not issue anonymous certificates. The common name of the applicant as asserted, vetted and authenticated by the FIMS IdP is not considered a pseudonym. When represented in the commonName of the certificate subjectName, the name of the applicant may be mapped to consist of solely of printable characters as per section 3.1.2, and the USR of the identifier added, causing it to become pseudonymous.

3.1.4 Rules for Interpreting Various Name Forms

Names will use the PrintableString sub-set encoding and will contain only upper- and lower-case characters, numerals, space, dash, dot, plus, and (round) brackets. These should be interpreted as per the encoding used.

3.1.5 Uniqueness of Names

The subjectName shall be unique and – once assigned to an entity – will not be re-assigned to any other entity. The CA uses both upstream federation policy as well as local controls to ensure

[5] The CA heuristics will determine that the constructed identifier is insufficient to provide uniqueness if the value of any of the other – ancillary – attributes ePTUID, ePPN, ePTID, displayName, givenName, sn, or commonName changes.

uniqueness. Unless the identity of the applicant can be re-associated with a formerly vetted identity, the CA will add a unique incremental serial number at the end of the commonName RDN component of the subjectName as described in section 3.1.2.

An identity will only be re-associated when entityID of the FIMS IdP is the same, and all of the attributes value of the set (eduPersonUniqueID, eduPersonTargetedID, eduPersonPrincipal-Name, displayName, givenName, sn, commonName) that have been provided on the initial authentication for this entity have remained unchanged.

If elements of this attribute set are missing on first identification, they are not considered in the uniqueness determination for subsequent re-association.

For multi-valued attributes, the first value of the lexically sorted list of attribute values is used.

To determine identity of the attribute set, for each assigned subjectName the CA will record:

- the one-way non-salted cryptographically secure SHA-256 digest of the commonName as constructed as per section 3.1.2, omitting the sequence number
- the sequence number, being either NULL or the sequence number added as per the rules of section 3.1.2
- the salted one-way cryptographically secure SHA-256 digest of the concatenation of all values of the attributes provided as by the IdP from the ordered list of displayName, givenName, sn, commonName, and mail (values of multi-valued attributes are pre-sorted based on their binary representation before concatenation).
- the set of attributes used to compose the uniqueness digest indicated above

This table of record will be used to assign the necessary sequence numbers to ensure uniqueness as per the rules in section 3.1.2. Sequence numbers are monotonically increasing integers. This table of record is kept for the entire duration of the service and does not contain personally identifiable data.

3.1.6 Recognition, Authentication and Role of Trademarks

Where this is known to the Service, brands and trademarks recognised in the Benelux will not be used without appropriate authentication of the entity named, and will be assigned only to or with endorsement of the recognised brand and trademark holder, or where reasonable expectation exists that such an assignment will meet with consent of the brand or trademark holder.

The release of attributes by or on behalf of the IdP of an organisation is interpreted as acceptance to use the name of the organisation in the issued certificate.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

The requester must prove possession of the private key which corresponds to the public key in the certificate request. This is done through the submission of a digitally signed PKCS #10 request.

Possession of the private key is defined as having generated, stored, and managed the key in compliance with the Private Key Protection Guidelines[6]. It may thus be that the key pair has been generated by the specific intent of the user and on behalf of the user by a third party subject to those Guidelines.

3.2.2 Authentication of Organization Identity

The RCauth ICA issues certificates to applicants that have been authenticated through FIMS IdPs. Only FIMS IdPs that have been securely authenticated are trusted by the CA, and only assertions

[6] http://www.eugridpma.org/guidelines/pkp/

that are properly signed by the FIMS are accepted. The CA will reject and log assertions that are not properly signed. Signature verification can take place by the CA software, by the FIMS proxy to which the CA is connected, or by both. It will be based on reliably published information regarding the signing key in trusted sources, including SURFconext and eduGAIN meta-data publications.

The FIMS policy describes which organisations are eligible to participate in the FIMS service and how they are authenticated. All IdPs within the constituency of SURFconext are authenticated and subject to the SURFconext usage agreement (SURFnet contract Annex IX).

IdPs outside SURFnet but within eduGAIN are subject to their federation policy, with the federation itself being subject to the eduGAIN Policy Declaration[7]. The CA will not knowingly rely on authentication by IdPs that provide inaccurate or fraudulent information, including the misuse of attribute assertions in violation of their specification.

Other IdPs, when granted trust by the CA to authenticate organisations and/or individuals, will explicitly agree to comply with all relevant provisions of this CP/CPS.

The Organisation is identified based on the entityID as presented in the signed assertion. Publication of the entity in trusted SAML meta-data, or by means of a trusted assertion of an organisational identifier, including but not limited to the schacHomeOrganization attribute by the FIMS, is considered sufficient authentication.

3.2.3 Authentication of Individual Identity

All authentication of individual identity is bound to an act of organisational identity authentication.

Organisations of connected FIMS IdPs, who act as registration authorities, vet applicant identities in accordance with the documented procedures:

- for SURFconext entities as described in Annex IX[8] of their SURFnet contract
- for entities in eduGAIN that are not in SURFconext: as described by their federation operator, which is itself subject to the eduGAIN Policy Declaration
- for all other IdPs it shall be based on an act of identity verification sufficient to ensure that for each entity where a unique identifier is asserted, this unique identifier will never be re-assigned to another entity. Such uniqueness should be guaranteed by auditable means. Such IdPs shall also assert a displayName, commonName, or a givenName together with an *sn* attribute for which the value is set by the IdP itself to a value corresponding to the name of the validated entity, and which cannot reasonably be modified by the applicant at will. These IdPs will assert one or more of eduPersonUniqueID, eduPersonPrincipalName, or eduPersonTargetedID and ensure non-reassignment of at least one of the asserted attributes.

The RCauth ICA will only accept authentication assertions when the IdP:

- is a SURFconext participant; or
- is in eduGAIN and eduGAIN and/or its federation asserts compliance with the REFEDS R&S[9], and the IdP has asserted publicly or to the CA explicitly its compliance with Sirtfi[10] - minimally at version 1.0; or
- is in a federation which has declared to the CA to have internal policies with respect to authenticating entities, traceability and security incident response, applicable to all its

[7] services.geant.net/edugain/Resources/

[8] http://www.rcauth.eu/policy/Template_Bijlage_IX_Lidmaatschap_SURF-Federatie.pdf

[9] https://refeds.org/category/research-and-scholarship

[10] https://refeds.org/SIRTFI

IdPs, that are materially equivalent to those in SURFconext, or to those inferred by REFEDS R&S and in accordance with Sirtfi; or

- is registered directly with the RCauth CA (with meta-data registered by eduGAIN, in RE:EP[11], or provided to the CA by other trusted means), and the organisation has asserted its compliance with the Sirtfi requirements and the non-reassignment and attribute release qualities for REFEDS R&S;

and releases the attribute from eduPersonUniqueID, eduPersonPrincipalName and eduPersonTargetedID which is never re-assigned, and at least one of the displayName, commonName, or givenName together with sn attributes for this entity.

The RCauth ICA will record sufficient information to ensure that it can trace each validation to an identified IdP, and can provide one or more identifying attributes asserted by the IdP that will enable the IdP to uniquely refer to an entity that performed the authentication.

Authenticated information included in the issued certificates shall be the applicant name as constructed according to section 3.1.1, the unique identifier constructed according to section 3.1.1, and – only when provided by the IdP – the rfc822mail address. This information shall be in accordance with the assertions given by the IdP.

3.2.4 Non-verified Subscriber Information

Other than the authentication described above, the CA does not check, and makes no assertions, about the subscriber's data in the certificate. In particular, the CA does not check and makes assertion that the subscriber is trustworthy, is acting in good faith at any particular time, or is a capable user.

3.2.5 Validation of Authority

The possession of a valid authentication assertion issued by an eligible FIMS IdP entitles the applicant to request certificates from the CA. A certificate is subsequently issued based on this assertion, unless

- the request does not meet the requirements of the CA as stated in this CP/CPS
- the applicant has been discretionarily banned from using the CA service
- the IdP (or the federation via which it has registered with eduGAIN) has been banned from using the CA service for failing to meet the requirements put upon a Registration Authority
- the IdP or the federation via which it has registered with eduGAIN has been discretionarily banned from using the service.

The Operations Team having been consulted, the PMA is authoritative for any discretionary bans. Such bans are usually put in place in order to ensure compliance with certificate usage as defined in section 1.4. When an IdP is banned from the service, it is no longer considered a valid authority to issue assertions and may no longer act as a Registration Authority.

3.2.6 Criteria for Inter-operation

No stipulation.

3.3 IDENTIFICATION AND AUTHENTICATION OF RE-KEY REQUESTS

[11] http://reep.refeds.org/

3.3.1 Identification and Authentication for Routine re-Key

Re-key is not supported. All applications are processed as a new request according to the stipulations in section 3.2

3.3.2 Identification and Authentication for re-Key after Revocation

Re-key is not supported. All applications are processed as a new request according to the stipulations in section 3.2

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Anyone can make certificate revocation requests to the RCauth ICA, in-person, by email, or by phone. A revocation request will be authenticated, unless the request is made directly by the PMA or the Administrators of the Service named in section 1, or the revocation request contains a proof of key compromise or other reasons listed on section 4.9.1.

Revocation requests received from Registration Authorities must be authenticated and will pertain only to certificates that have been issued based on assertions issued by themselves. IdPs will be contacted through the security contact meta-data when available. Otherwise, the CA will contact the Registration Authorities via a trusted out-of-band means to verify the request.

In all other cases, authentication can be via a digitally signed message with a non-expired and not previously revoked certificate issued under this Policy, or by means of in-person or videoconference supported verification of a government-issued photo ID document.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Who Can Submit a Certificate Application

Any person authenticated via a FIMS IdPs of an eligible Registration Authority, for whom the attributes required to determine name uniqueness as per section 3.1.5 and for whom the applicant name can be constructed as per section 3.1.2, and from whom the assertion issued by the IdP indicates that the applicant is eligible to use the CA service, is permitted to submit a certificate application.

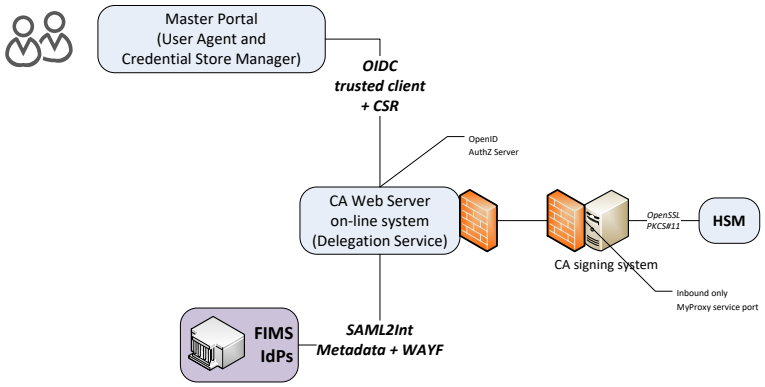
The certificate application can be made:

- Directly by the applicant by authenticating through its IdP to the CA service
- A trusted third party software agent or system on behalf of the user, only as a result of an explicit request initiated by the applicant, and where such a system is a permissible appropriate system compliant with the requirements of the IGTF Private Key Protection Guidelines version 1.2 or above[12]

4.1.2 Enrollment Process and Responsibilities

Subscribers obtain a certificate from the CA via an on-line transaction. All network communication occurs over encrypted HTTPS connections, with server identity verification according to RFC 2818 and identification of all clients.

The subscriber, or a third party system on behalf of the subscriber, generates an RSA key pair. First, the subscriber (i.e., software running on the subscriber's behalf) opens a connection to the CA web service through the OpenID Connect Protocol. Through this the subscriber (i.e., software running on the subscriber's behalf) generates an RSA key pair of at least 2048 bits strength and submits a certificate request containing the RSA public key to the CA web service.



The CA web service then authenticates the subscriber according to the OASIS standard SAML Web Browser Single Sign On (SSO) protocols (SAML2Int), i.e., the CA web service redirects the subscriber's web browser to his or her IdP, where the subscriber authenticates, and then the identity provider redirects the subscriber's web browser back to the CA web service, delivering a signed, time-limited SAML authentication assertion issued by the IdP to the CA web service. This establishes a trusted, secured, and identified connection between the CA web service and the subscriber or subscriber agent system.

[12] https://www.eugridpma.org/guidelines/pkp/

Finally, if the CA approves the request (according to Section 4.2.2), the CA web service returns a signed X.509 certificate containing the public key, the subject distinguished name, and other validated alternative names, to the subscriber. Otherwise, if the CA rejects the request (i.e., any of the conditions in Section 4.2.2 are unmet), the CA web service will not return a signed certificate but will instead return an error message to the subscriber.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

The CA will validate all assertions sent by IdPs by checking their signature and validating it using trusted SAML meta-data sources. Trusted meta-data sources include the signed data originating from SURFconext, signed data originating from the eduGAIN meta-data service, and validation certificates directly supplied via trusted and integrity-protected means (or in person) to the PMA and distributed to the Administrators.

4.2.2 Approval or Rejection of Certificate Applications

The CA approves certificate applications if all of the following criteria are met:

- The subscriber submits the certificate application in a SAML authenticated and TLS secured web session.
- The digital signature on the SAML assertion is valid and corresponds to the identity provider's public key in a trusted meta-data source as specified in section 4.2.1.
- The SAML assertion contains the attributes required for constructing the certificate subject (see section 3.1.1).

The certificate signing request supplied by the applicant must be digitally signed by the private key associated with the 2048 bit RSA public key in the request (see section 3.2.1).

Otherwise, the certificate application will be rejected.

4.2.3 Time to Process Certificate Applications

Certificate applications are processed automatically. Approved applications result in automatic certificate issuance, which will be processed without undue delay. There is however no guaranteed time period within which a certificate application will be processed.

Non-approved applications are automatically rejected.

All certificate applications (approved and non-approved) are logged.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions during Certificate Issuance

Upon approval of a certificate application, the CA assigns an X.500 distinguished name to the applicant based on the identifying information in the authentication assertion (see section 3.1) and issues a signed X.509 certificate containing the applicant's public key and subject distinguished name.

The CA signing system to which the HSM is connected will log the signing operation.

The CA signing system to which the HSM is connected will not sign certificates if the key pair has been used previously for another certificate.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The CA delivers the issued certificate to the subscriber through the software process the applicant used to apply for the certificate.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

Certificate acceptance by the applicant is assumed. To reject an issued certificate, the subscriber should submit a revocation request according to section 4.9.

4.4.2 Publication of the Certificate by the CA

The RCauth ICA does not publish issued certificates.

4.4.3 Notification of Certificate Issuance by the CA to other Entities

The RCauth ICA does not notify any other entity.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers must protect their private keys according to the latest approved version of the Guidelines on Private Key Protection[13].

Subscribers must not use their RCauth ICA certificate if they engage in activities incompatible with the scope, purpose and policy as described in this document, or if the use of their RCauth ICA certificate would in any way harm, be defamatory, cause injury, or be detrimental to the reputation, safe operation or good standing of the RCauth ICA or the Service, or if the use would result in liability (financial or otherwise) of any of the the Operating Partners, of Nikhef, SURF, or any individual involved in the operation of the Service.

Subscribers must request revocation of their certificate within one business day if the private key pertaining to the certificate is known or suspected to be compromised or lost, or if the data in the certificate is no longer valid.

4.5.2 Relying Party Public Key and Certificate Usage

The RCauth ICA public key and certificate shall be used by relying parties only in accordance with this CP/CPS, only for as long as it is valid, and only after having checked its revocation status.

Relying parties may not use a certificate of the RCauth ICA if such use would in any way harm, be defamatory, cause injury, or be detrimental to the reputation, safe operation or good standing of the RCauth ICA or the Service, or if the use would result in liability (financial or otherwise) of the Operating Partners, Nikhef, SURF, or any individual involved in the operation of the Service.

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstances for Certificate Renewal

Certificate renewal is not supported.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

[13] https://www.eugridpma.org/guidelines/pkp/

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate Issuance by the CA to other Entities

Not applicable.

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstance for Certificate Re-key

Certificate re-keying is not supported.

4.7.2 Who May Request Certification of a New Public Key

Not applicable.

4.7.3 Processing Certificate Re-keying Requests

Not applicable.

4.7.4 Notification of new Certificate Issuance to Subscriber

Not applicable.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Not applicable.

4.7.6 Publication of the Re-keyed Certificate by the CA

Not applicable.

4.7.7 Notification of Certificate Issuance by the CA to other Entities

Not applicable.

4.8 CERTIFICATE MODIFICATION

4.8.1 Circumstances for Certificate Modification

Certificate modification is not supported.

4.8.2 Who May Request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

A certificate will be revoked in the following circumstances:

1. The subscriber does not comply with this policy.
2. The system through which the subscriber has submitted the certificate signing request is known to be compromised or non-compliant with the Private Key Protection Guidelines.
3. The private key is lost or suspected to be compromised.
4. The information in the certificate is wrong or inaccurate.
5. The service that manages the credential has been discontinued.
6. At the request of the subscriber, or at the request of anyone able to present the private key pertaining to the issued certificate.

4.9.2 Who Can Request Revocation

Any certificate holder, subscriber, or IdP that gains knowledge of the occurrence of any of the circumstances 1 through 5 for revocation as listed in section 4.9.1 must request revocation of the pertinent certificate.

Any entity which can prove or gains knowledge of the occurrence of any of the circumstances 1 through 5 for revocation as listed in section 4.9.1 should request revocation of the pertinent certificate.

4.9.3 Procedure for Revocation Request

The entity requesting revocation of a certificate shall submit their revocation request to the RCauth ICA Administrators by electronic mail to <**revocation@rcauth.eu**>, or by using the contacts in section 1.5.1.

Upon receipt of a revocation request, the RCauth ICA shall:

1. Verify the circumstances for revocation
2. Verify the identity of the revocation requester in accordance with section 3.4

If one or more of the conditions specified in section 4.9.1 are met, the RCauth ICA shall then revoke the certificate.

4.9.4 Revocation Request Grace Period

Any party that becomes aware of circumstances for revocation should request a revocation as soon as possible but not later than within one business day.

4.9.5 Time within which CA must Process the Revocation Request

All reasonable requests for revocation shall be acted upon promptly, without undue delay, and with appropriate urgency. Once the request has been validated, the RCauth ICA shall revoke the certificate forthwith, and publish updated revocation information.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying parties may rely on a certificate only as long as that certificate has not been included in a published certificate revocation list.

Relying parties should check freshness of their revocation data as often as relevant, based on their own risk assessment. In absence of specific risks we recommend to download CRL data not more frequently than once every 60 minutes.

4.9.7 CRL Issuance Frequency

The RCauth ICA shall issue a CRL at least once every day and immediately after a certificate revocation.

4.9.8 Maximum Latency for CRLs

Following a revocation, a new CRL will be issued forthwith and posted in the public repository within one hour.

4.9.9 On-line Revocation/Status Checking Availability

The RCauth ICA does not operate a production OCSP service.

4.9.10 On-line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

There are no other forms of revocation advertisement available.

4.9.12 Special Requirements Re-key Compromise

No stipulation.

4.9.13 Circumstances for Suspension

Suspension of certificates is not supported.

4.9.14 Who can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

The RCauth ICA shall publish a full RFC 5280 compliance X.509 v2 CRL in the on-line repository stated in section 2.1.

4.10.2 Service Availability

The on-line repository containing the CRL is provided with an intended continuous availability.

4.10.3 Optional Features

None.

4.11 END OF SUBSCRIPTION

A subscriber may end subscription to the CA services by requesting revocation of all certificates issued to the subscriber or by allowing all certificates issued to the subscriber to expire without requesting any new certificates.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

The RCauth ICA does not provide a key escrow service.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

The RCauth ICA is operated as a coherent single entity in three distinct physical locations: at Nikhef in Amsterdam, The Netherlands; at RAL in Didcot, Oxfordshire, UK; and at GRNET in Athens, Greece. Each of these operating locations has specific facility, management, and operational controls that are described separately in this section.

5.1 PHYSICAL CONTROLS

The RCauth CA service consists of three principal components – the repository service, the CA web server (delegation server), and the CA signing machines.

Nikhef

Besides the CA systems, two secondary back-up related services exist: a disk-based backup service at Nikhef and a secondary off-site backup at a Nikhef collaboration member organisation under confidentiality requirements.

All CA web server systems are located in a dedicate secured cabinet inside the Nikhef data centre mentioned before, the Nikhef backup server is located in the same data centre in a different cabinet, and the off-site backup solution is located in two geographically distinct locations in a different secured data centre, with at least one of the tape robots in a vault with self-closing doors.

RAL

The signing key is installed on at least one FIPS140-2 HSM running in L3 mode, but with the key essentially permanently activated. The HSM may host other keys requiring a similar level of protection. All HSMs in operation are housed in a secured rack inside the data centre.

GRNET

Both the CA web server and the CA signing machine are housed in a secure cabinet inside GRNET's data centre located at the Greek Ministry of Education, Research and Religious Affairs in Athens. The GRNET backup server is located in a different data centre within the same building.

5.1.1 Site Location and Construction

Nikhef

The RCauth ICA is located at Nikhef, Watergraafsmeer, Amsterdam, in a data centre location dedicated to Nikhef and Nikhef-operated ICT services. The data centre is located on the 2nd floor of the building. Both the CA web server ('delegation server'), the CA signing system (to which the HSM is connected), and the CA repository server are within this data centre.

RAL

UKRI-STFC hosts the RCauth CA at Rutherford Appleton Laboratory, in a data centre with suitable physical controls, and with physically separate primary and backup connection to JANET.

GRNET

The RCauth ICA is located at the Greek Ministry of Education, Research and Religious Affairs, Marousi, Athens, in a data centre dedicated to GRNET and GRNET-operated ICT services. The data centre is located on the basement of the building. Both the CA web server ('delegation server') and the CA signing system (to which the HSM is connected) are within this data centre. The GRNET backup server is located in a different data centre within the same building.

5.1.2 Physical Access

Nikhef

The Nikhef data centre is a locked room that uses DESfire RFID access cards issued to named individuals. Access to the data centre is restricted to authorized personnel, access is logged, and the logs periodically reviewed. Within this locked room, a CA-services dedicated pad-locked cabinet contains the CA web server (delegation server), the CA signing machine with the attached HSM, and the security services hosting environment that runs the CA on-line repository service. The cabinet has a padlock mechanism protecting the two doors the combination of which is only known to local Administrator and Operators. The backup keys for the cabinet are controlled by the Administrator.

The CA signing machine with the attached HSM is located in a locked drawer inside this cabinet.

RAL

Access to the data centre is granted only to authorised personnel, based on individual RFID cards and monitored by CCTV. Access to the CA hardware within the data centre requires an additional set of physical keys.

GRNET

GRNET's data centres is restricted to authorised personnel based on RFID cards issued to named individuals (ISO 9001 Certified). Access is logged and the logs are periodically reviewed. Each data centre is constantly being monitored by Dome Cameras whose feed is being recorded to a dedicated surveillance system. A locked cabinet within the data centre houses the CA web server (delegation server) and the CA signing machine to which the HSM is connected. The cabinet keys are available only to local Administrator and Operators.

5.1.3 Power and Air Conditioning

Nikhef

All CA systems are connected to a no-break UPS system with a capacity sufficient to power both the systems and to provide the requisite cooling. The UPS battery system is backed by two redundant diesel generators and the fuel supply is monitored and kept at a level adequate to run for at least 48 hours without need for refuelling. The systems are tested monthly. Power and air conditioning systems are monitored 24x7 with a 15-minute response time.

Both the CA web server and the security systems hosting cluster running the CA on-line repository are connected to independent power feeds. The CA signing machine is connected to a single power feed.

RAL

The data centre has both UPS and generator power, but the services supporting the HSMs are only on the generator backup.

GRNET

The whole data centre is connected to three GALAXY 7000 500KVA UPS systems with sufficient capacity to power both the systems and the necessary cooling. The UPS system is backed by a redundant diesel generator and the fuel supply is monitored and kept at a level adequate to run for at least 48 hours without need for refuelling. The systems are tested periodically. Power and air conditioning systems are monitored 24x7 with a 15-minute response time.

5.1.4 Both the CA web server and the CA signing machine have N+1 redundant power supplies .Water Exposures

Nikhef

All CA systems are above sea level. Installations that contain water near the CA systems are periodically tested for pressure bearing capabilities. The data centre is equipped with moisture sensors and monitored continuously. Fire suppression systems do not use water.

RAL

The data centre is currently wholly air cooled, and is not located in an area at risk of flooding.

GRNET

The data centre housing the CA systems is located in a building that poses little or no risk of flooding.

5.1.5 Fire Prevention and Protection

Nikhef

The data centre is equipped with an inert-gas fire extinguishing system and has appropriate smoke-sensitive detectors. Automatic notifications are sent in case of fire detection. Systems are tested at least quarterly.

RAL

The data centre is continuously monitored for smoke and fire, and with a fire suppression system on automatic whenever operations staff are absent.

GRNET

The data centre is equipped with an inert-gas fire extinguishing system and has appropriate smoke-sensitive detectors. Automatic notifications are sent in case of fire detection. Systems are tested at least quarterly.

5.1.6 Media Storage

All backup media containing the private key material of the RCauth ICA are kept in the locked safe near the off-line machine. Copies of private key material are also kept exclusively in locked safes under the control of the Administrator, and to which Operators are granted access.

All other media, except for transfer media, of the RCauth ICA are kept inside the locked cabinets. Transfer media are either kept in the locked cabinet or kept under the control of the Administrator.

Neither the CA signing system, nor any on-line back-up systems and tape replicas contain any private key material. Private key material in the data centre is kept exclusively inside the HSM.

Media for storage during key transfer

Media that are used to transfer the private key do not themselves hold any part of the private key except when encrypted using at least two independent one-time-pads. The exchange of one-time pads and any so-encrypted private key is done over different transport modalities and separated in time and space.

5.1.7 Waste Disposal

Waste carrying potential confidential information is physically destroyed before being trashed.

5.1.8 Off-site backup

Nikhef

The off-site backup copy of the encrypted private key of the RCauth ICA is kept off-site in a safe under the direct personal control of an Administrator.

Other, non-sensitive, material of the RCauth ICA, including the state of the CA, index files, and related material of the CA systems are regularly backed up to distinct locations within and outside the building and physically distant from the originals.

The on-line repository system is backed-up on a primary backup on-site system at Nikhef which is itself back-up daily to a secondary redundant off-site backup at a Nikhef collaboration member organisation under confidentiality requirements.

RAL

RAL will implement an offline (but not off-site) backup, using a safe that is owned and controlled by the organisational unit that operates the CA. The safe is bolted to the floor. The organisational roles and their process for recovering the key from backup is documented.

GRNET

The off-site backup copy of the encrypted private key of the RCauth ICA is kept off-site in a safe under the direct personal control of an Administrator.

Other, non-sensitive, material of the RCauth ICA, including the state of the CA, index files, and related material of the CA systems are regularly backed up to distinct locations within and outside the building and physically distant from the originals.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

All roles related to the issuance operation of the RCauth ICA shall be performed by the Service Administrators or Operators under authority of the PMA. Operators may be assigned to operate just a single issuing instance of the CA. They shall be permanent employees of the Operating Partner organisation (as conventionally defined according to the employment conditions of the organisation).

5.2.2 Number of Persons Required per Task

The Administrators and Operators are permitted to act singly, unless elsewhere in this Policy a specific action is required to be performed in the presence of witnesses or another Administrator or Operator.

5.2.3 Identification and Authentication for Each Role

CA operators authenticate by individual password or private key. When any person leaves the role of CA operator, his or her access to CA systems will be immediately revoked (i.e., system accounts removed or disabled).

5.2.4 Roles Requiring Separation of Duties

No stipulation.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

RCauth ICA Administrators shall all be personnel with a sound understanding of PKI, its implementation, and its trust implications. They are experienced in operating CA infrastructures and are knowledgeable about this document and the requirements stipulated herein. The

Operators shall all be personnel with a proper understanding of PKI, and trained in following the operational procedures implementing this CP/CPS.

Beyond being employees in good standing, there are no specific clearance requirements.

5.3.2 Background Check Procedures

The background of each additional Administrator shall be assessed by his or her peers and by the PMA.

5.3.3 Training Requirements

The Administrators will ensure both they and Operators are capable of fulfilling their tasks and understand their responsibilities with regards to this CP/CPS.

5.3.4 Retraining Frequency and Requirements

No stipulation.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

If an unauthorized action is observed, the Service Administrators will take appropriate measures to prevent re-occurrence, may revoke any privileges, and will correct any inappropriate results. Other sanctions are possible as specified in the terms of employment.

5.3.7 Independent Contractor Requirements

The RCauth ICA shall not employ contractors for its primary service operation. However, it does rely on vendors to supply hardware, software, and other (physical) infrastructure. It will obtain such supplies in a way that does not knowingly expose the RCauth ICA to security compromises. The CA uses the off-site backup at a Nikhef collaboration member organisation under confidentiality requirements for all operational data, except for the private key of the CA and the long-term data archive of personal data.

5.3.8 Documentation Supplied to Personnel

The RCauth ICA Administrators and any operators are given a copy of this document as well as any ancillary documentation.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

The following events will be recorded by the RCauth ICA:

- System boots and shutdowns of the CA signing machine and the CA web server (delegation server) machine
- Certificate application, issuance and revocation
- Activation and deactivation of the CAs signing key and of the HSM

Key pair generation is recorded as part of the key generation ceremony. The key generation ceremony shall be in the presence of qualified witnesses, and be recorded on both paper and visual media.

5.4.2 Frequency of Processing Log

Audit logs will be analysed

- during annual audits

- whenever an incident occurs or is suspected

5.4.3 Retention Period for Audit Log

System audit logs are retained for at least three years after the certificate pertaining to the log entry has expired or has been revoked. After a period 6 months following certificate expiration or revocation, the logs are archived and those log elements containing personal data may only be used for dispute resolution purposes.

Authentication audit logs that contain personal data as meant in the SURFconext Privacy Policy and the Dutch Data Protection Act (WBP) shall be kept in accordance with the Privacy Plan (section 9.4.1.8).

Neither the unique identifier supplied in the authentication assertion (eduPersonUniqueID and/or eduPersonPrincipalName, and/or eduPersonTargetedID) nor the entity ID of the IdP shall be considered personal data. Anonymised data, being one-way secure digests of personal data, shall not be considered personal data. Both will therefore be logged for the duration of the system audit log retention period (three years).

Audit logs are retained on the CA systems and on backup systems.

5.4.4 Protection of Audit Log

The audit logs are stored in the CA and disk back-up systems to which only designated Nikhef personnel have access. Off-site backups are stored in a trusted location where confidentiality is agreed by contract.

5.4.5 Audit Log Backup Procedures

All audit logs are backed-up according to section 5.1.8.

5.4.6 Audit Collection System (internal vs. external)

All audit logs collected by the the RCauth ICA are internal.

5.4.7 Notification to Event-causing Subject

The RCauth ICA is neither required to nor prevented from notifying event-causing subjects.

5.4.8 Vulnerability assessments

Vulnerability of the audit logs are assessed during periodic self-audits and whenever a change to section 5.4 of this CP/CPS is considered.

Vulnerabilities in the CA software and the operating system used are traced and promptly and appropriately acted upon.

5.5 RECORDS ARCHIVAL

5.5.1 Types of records archived

The RCauth ICA will archive the following data:

- All certificate application data, issued certificates, and CRLs
- Operations on the CA systems, including startup, reboot, and login actions
- Events generated by the CA software and significant operator actions
- Any documentary evidence and witness reports of key generation ceremonies, key transfer and certificate acceptance

5.5.2 Retention Period for Archive

Records that do not contain personal data will be kept for at least three years following the expiration or revocation of the certificates to which they pertain. Records ensuring non-reassignment of identifiers are kept for the duration of the RCauth service.

Records that contain personal data as identified in section 5.4.3 will be archived as per the retention periods listed in the Privacy Plan (section 9.4.1.8). Archived records with personally identifiable information have an exclusive archival purpose and may only be used for dispute resolution.

5.5.3 Protection of Archive

Archive are stored on-line and protected like audit logs as per section 5.4.4.

5.5.4 Archive Backup Procedures

As per section 5.1.8.

5.5.5 Requirements for Time-stamping of Records

Records on on-line systems will be timestamped using a clock frequently using the ntp protocol from trusted time sources operated by Nikhef, SURFnet, and/or a distributed NTP pool.

5.5.6 Archive Collection System (internal or external)

All archives are collected internally or are stored on services under contract of Nikhef.

5.5.7 Procedures to Obtain and Verify Archive Information

Information from the archive may be inspected by auditors. In addition, subscribers or third parties may request the RCauth ICA for permission to inspect or obtain information from the archives if such – at the discretion of the RCauth ICA or if required by law – is pertinent to the proper operation and trust or compliance of the RCauth ICA. The Service may require prior compensation for reasonable costs associated with such requests.

At all times, individuals shall have the right to inspect, and in case of omissions, errors or inconsistencies, have the right to amend and correct data regarding themselves.

5.6 KEY CHANGEOVER

The RCauth ICA key pair shall be changed once the maximum validity period of 20 years expires or when the cryptographic data on which it is based is no longer considered appropriate to protect the certificates it issues. It may change key material at any time prior to these conditions.

If the RCauth ICA key changes, the overlap between the old and the new key pair shall be more than 400 days unless all certificates signed by the old key have expired or have been revoked. From the time of the key changeover, only the new key will be used to sign certificates.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

In the event of an incident which compromises the integrity of the RCauth ICA, the personnel shall – in coordination with the Nikhef CSIRT – initiate an incident analysis immediately. Further steps to be undertaken will depend on the outcome of the analysis.

The Service will collaborate with registration authorities, representative groups of registration authorities, qualified relying parties, and computer security incident response teams of any bodies to which it has been accredited.

5.7.2 Computing Resources, Software, and/or Data are corrupted

The Operators will take all reasonable precautions to enable recovery. In order to be able to resume operation, the following measures are implemented:

- All CA software shall be backed-up after a new release of any of its components is installed.
- All data files of the CA signing server[14] shall be backed-up daily to the CA web server on-line system – from which further backups are taken.

If any part of the running system is corrupted, functioning replacement hardware shall be loaded with the latest state of the software and data backed-up and estimated to be uncorrupted. If necessary, the HSM will be loaded with the CA key pair from the secure backup media. Unless in the exceptional case that all copies of the RCauth ICA private key have been destroyed or lost, and as long as these are not compromised, the operation shall be re-established as soon as possible. This will not constitute a need to revoke any issued certificates.

Subscribers must not assume that the service is available to them at any time, and must not expect that the data stored about them in the service will persist beyond the authentication transaction. The ability of a specific subscriber to obtain certificates from the RCauth ICA with the same subject name must not be assumed by a subscriber. Removal of data about a subscriber, either explicitly or as a result of data corruption, is a regular event and will not be considered as having a serious impact on the subscriber.

5.7.3 Entity Private Key Compromise Procedures

In the event of private key compromise of its own key, the RCauth ICA shall immediately cease issuing certificates, revoke any issued certificates, and request revocation of any cross-signed certificates. It shall also forthwith inform all bodies to which it has been accredited, and post a notice for applicants and subscribers on the public repository. Current subscribers for whom it has individual contact information will be contacted using their recorded communications means.

Circumstances that led to the compromise will then be fixed and eliminated, and these remedial actions documented. A new key and certificate for the CA may then be re-created and operations restarted with a certificate based on a new key pair.

In case a key of a subscriber certificate has been compromised, the RCauth ICA will revoke the corresponding certificate and will not accept new certificate applications from this entity until the incident has been satisfactorily closed.

5.7.4 Business Continuity Capabilities after a Disaster

Following a disaster, the Administrators and/or the PMA will – as soon as reasonably practical – assess the extent of the disaster and its impact on the operational of the Service. Having established that no compromise has occurred and that sufficient elements are available to recover from the disaster, it shall proceed to re-establish operations, if so needed from back-up media.

When it is deemed likely that the disaster will result in long-term outage for a period over 30 days, the Operators may opt to suspend operations by informing its subscribers and any bodies to which it has been accredited.

[14] This does – by design – not include the private key which is solely inside the HSM.

5.8 CA or RA TERMINATION

Upon termination of service of the RCauth ICA, the PMA will

1. Inform any bodies to which it has been accredited
2. Announce termination on RCauth repository website and on the service site.
3. Terminate the issuance and distribution of certificates and CRLs following a reasonable grace period.
4. Archive all relevant information in accordance with section 5.5
5. Revoke all certificates.
6. Notify relevant security contacts.
7. Destroy all copies of private keys.
8. Notify as widely as possible the end of the service.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

The RCauth ICA shall generate and store its private keys both on off-line media and in an FIPS 140-2 level 3 compliant token into which it will be imported in a secure manner. The private key will never be present in an on-line system except when protected inside the HSM.

After generation, off-line media with private keys are stored in safes in accordance with section 5.1.

The RCauth ICA key pair generation shall be performed on an off-line system, using a recent trustworthy version of the OpenSSL software which has been verified for integrity with its source. The generation will be witnessed by experts knowledgeable about PKI, and they shall witness that the private key pair material is stored on removable media and not further distributed beyond the reach of the Administrators and the Operators of the RCauth ICA. The Administrators may transport the generated the private key and any other RCauth ICA materials without further supervision to a safe at a geographically separate location having been so authorized by the PMA. The RCauth ICA shall not proceed to include its certificate in external trust anchor distributions until the generating Administrator (Nikhef) confirms that the private key material has been deposited in said safe.

The key pair, alongside the RCauth ICA certificate signed by its higher-level Root CA, will also be exported in PKCS#12 format on dedicated USB media for import into the HSM module. The import onto the HSM module will be done, in the presence of qualified witnesses, by the RCauth CA Operator on the dedicated machine that has not been previously connected to the public internet.

End-entity private keys are generated by the applicant or by a software agent on a third-party system at the request of the applicant in accordance with the Guidelines on Private Key Protection. The RCauth ICA does not generate key pairs for its subscribers.

6.1.2 Private Key Delivery to Subscriber

The RCauth ICA does not generate key pairs for its subscribers.

6.1.3 Public Key Delivery to Certificate Issuer

The subscriber's public key is delivered to the CA in the form of a PKCS#10 request, bound to the act of identification through a SAML authenticated TLS session according to the process described in section 4.1.

6.1.4 CA Public Key Delivery to Relying Parties

The public keys of the RCauth ICA can be downloaded in the form of an X.509 certificate from the online repository. The CA certificate may be redistributed under the terms of the Creative Commons CC-BY-4.0 license by any other entity, including bodies to which the CA has been accredited.

6.1.5 Key sizes

The signing key of the RCauth ICA shall be an RSA key and shall be 2048 bits long. The key pair of the applicant shall be an RSA key and shall be at least 2048 bits long.

6.1.6 Public Key Parameters Generation and Quality Checking

The RCauth ICA will refuse to certify public keys not matching the quality requirements stated in section 6.1.5.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The key of the RCauth ICA may be used for certificate signing and for CRL signing. The keys of end-entities may be used for Digital Signatures, Key Encipherment, and Data Encipherment.

6.2 PRIVATE KEY PROTECTIONS AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

The RCauth ICA stores its private keys on off-line media in controlled locations (safes), and in a cryptographic hardware security module certified at FIPS 140-2 level 3, operated using role-based authentication and with the key being imported into it in a controlled way.

6.2.2 Private Key (n out of m) Multi-person Control

There is no requirement for any role to be performed in the presence of more than one person.

6.2.3 Private Key Escrow

The RCauth ICA does not escrow any keys.

6.2.4 Private Key Backup

The RCauth ICA private key is backed up in encrypted form on multiple removable media, stored in safe boxes in geographically separated locations.

The pass phrase of the encrypted private key is stored in a sealed envelope in another location, separate from the encrypted private keys, under the control of an Administrator.

6.2.5 Private Key Archival

The private key is not archived beyond its active use period or post the termination of the CA, and only according the backup and use conditions detailed above.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The RCauth ICA operators transfer the encrypted CA private keys from off-line media into the cryptographic hardware security modules during the key pair generation ceremony (section 6.1.1) or in the case that a new cryptographic hardware security module is added to the CA system. Private keys are never transferred from a cryptographic module.

The private key may be transferred between Operating Partners under the control of each of the Administrators whilst not being in a cryptographic module, as long as no compromise of a single transport action would endanger the confidentiality of the private key. Different transport modalities for each fragment shall be chosen. Any key transport protocol shall be documented and be subject to scrutiny by pertinent accreditation bodies.

6.2.7 Private Key Storage on Cryptographic Module

The RCauth ICA stores private keys on cryptographic modules in non-exportable form.

6.2.8 Method of Activating Private Key

The private key of the RCauth ICA inside the HSM is activated by a passphrase of at least 15 elements. On system startup, a CA Operator must enter the activation data by hand on the

console of the CA signing system, after which this activation data will be cached in an isolated user process (the HSM access interface software) to which other signing system processes refer during signing operations.

Keys are effectively activated for as long as the process containing the activation data is operative. When access to the activation data is lost, the activation data can only be re-entered on the console by a CA Operator.

Activation data can only be entered on the physical console, since remote interactive access to the signing system is prevented by network firewall rules.

6.2.9 Method of Deactivating Private Key

The private key is de-activated by unplugging the cryptographic module from the system, by powering down the system, or by terminating the HSM access interface software (thereby loosing access to the activation data).

6.2.10 Method of Destroying Private Key

Following termination of CA operations, all copies of the private key will be securely destroyed according to then-current best practice for the destruction of sensitive materials.

The private key contained in the cryptographic modules will be destroyed by re-initializing the module.

When an Operating Partner intends to withdraw from the Service, it shall inform both the PMA and its peers of its intention to do so. At that point

- the PMA shall assess the operational integrity of the Operating Partner;
- the PMA shall ascertain the location of all copies of the private key of the RCauth ICA, including those held in HSM cryptographic modules;
- the Administrators of the peer service, so directed by the PMA, shall implement the technical measures sufficient to continue the service using on the remaining Operating Partners;
- the Operating Partner shall, under appropriate supervision of the PMA, demonstrate the destruction of all copies of the private key of the RCauth ICA;
- the Operating Partner shall transfer, in machine-readable form, all audit and logging material to another Operating Partner designated by the PMA;
- the Operating Partner shall relinquish all trust material and all the rights and privileges on software and the use of the RCauth name and trademarks that emanate from the fact of being an Operating Partner.

An Operating Partner is not permitted to withdraw from the control of the PMA until all of the above conditions have been met, and the Operating Partner shall comply with all reasonable requests from the PMA with regard to on-site inspections and the provisioning of pertinent information. The PMA will relieve the Operating Partner from its responsibilities once the above conditions have been met.

If the PMA at any point suspects, or is presented with good-faith evidence, that the integrity of the private key has been compromised, it shall proceed by requesting revocation of the RCauth ICA and re-build the trusted infrastructure using a new key pair.

6.2.11 Cryptographic Module Rating

All RCauth ICA cryptographic modules have been certified according to FIPS 140-2 at level 3 or better.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

The RCauth ICA archives all issued certificates for at least three years. No more than 6 months after expiration or revocation of the certificate, the certificate is archived in a long-term archive whose access is limited to dispute resolution purposes.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The RCauth ICA shall have a validity period of 20 years.

The end-entity certificates issued by the RCauth ICA shall have a validity period of no longer than 13 months, and for no longer than the RCauth ICA itself is valid.

End-entity certificates will be valid for no more than 1 million seconds (approximately 11 days) when the user or the agent on behalf of the user is registered or known as being a credential management portal with permanent key activation.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

The RCauth ICA does not generate activation data for its subscribers. Subscribers to the RCauth ICA must generate activation data, or have activation data generated for them, in accordance with the Guidelines on Private Key Protection. If the private key pertaining to the certificate is destroyed within 24 hours of key generation, it need not be protected by activation data beyond a standard operating system protection level.

The RCauth ICA generates activation data for the off-line copies of the private key as a passphrase of at least 15 elements at the time of generation. This activation data is used when importing the key into the HSM, and need not be installed.

The RCauth ICA generates activation data for the cryptographic module on initialisation of the module. This activation data shall have at least 15 elements, and not be installed in an on-line system. The activation data is provided on system initialisation by on-site operator action, and cached only in memory on the signing machine.

6.4.2 Activation Data Protection

Each subscriber is responsible to protect any activation data for its own private key.

The RCauth ICA uses a pass phrase to activate its off-line private key which is

- only ever entered on the off-line machine,
- known exclusively to the Administrators,
- is never stored in the same cabinet or safe as the private key itself,
- may be distributed on paper, in fragments and never in whole – or alternatively using Shamirs Secret Sharing Algorithm, between the Administrators, as long as such fragments are kept in sealed, tamper-evident containers (envelopes), away from the key material, at distinct, widely separated geographical locations (at least 10 km), and in locked cabinets.

The RCauth ICA uses a pass phrase to activate its cryptographic module which is only ever entered by an Administrators or Operator on the signing machine to which the module is connected.

Old activation data is destroyed according to current best practices.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

The RCauth ICA service is a model A[15] on-line CA service consisting of a CA web server on-line system, a back-end CA signing server, and a cryptographic hardware security module.

The FIMS IdPs are not considered part of the CA computer systems.

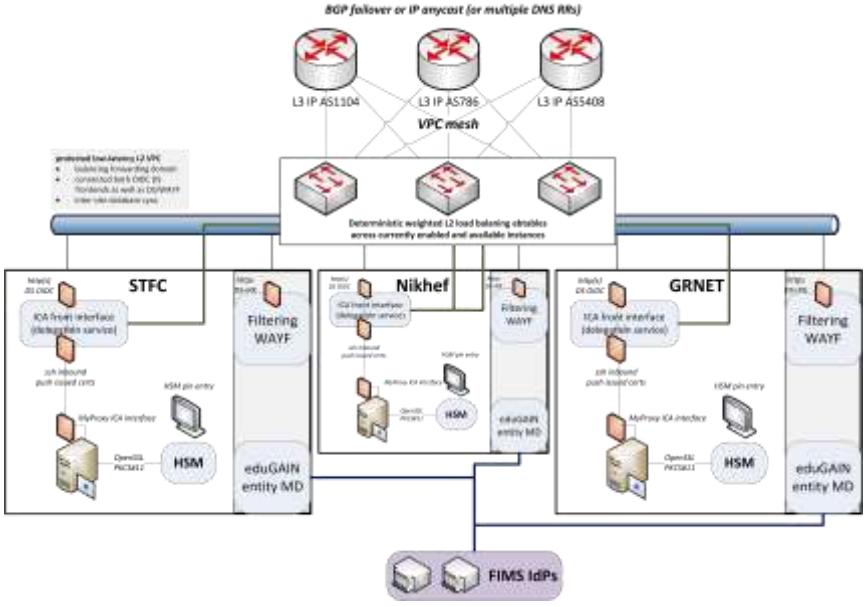
All Operating Partner instances

The **CA web server** on-line system ("Delegation Service") accepts connections on port http (80/tcp) and https (443/tcp) from the internet, serving both the web interface and user authentication consent and where-are-you-from-service and SAML and OpenID Connect protocol flows. It also accepts inbound rsync connections over a trusted network from the back-up service, inbound SSH connections from Service management networks (not shown), rsync connections from the RCauth and CA repository service (to retrieve the CRL for subsequent publication), and inbound connections from the CA signing system for SSH and NTP. The delegation server runs OpenID Connect and SAML software.

The **CA signing system** is exclusively connected to the CA web server using a dedicated physical network link. Both ends of the link have network access control using host-based firewall rules. The CA signing system accepts only inbound MyProxy connections over which approved CSR are sent and certificates returned. The CA web server accepts inbound SSH connections from the signing server, authenticated with a dedicated SSH public-private key pair, over which the CA signing system pushes its generated CRLs, its log files, and its backups to the CA web server. Besides the MyProxy service, there is no inbound network connection possible to the signing system. The management of the signing system is done through a physical console (USB HID+VGA connection).

Collective operations control

The issuing instances are interconnected with dedicated encrypted links. A cluster of high-availability proxy services distributed over all operating partners ensures both load balancing dependent on source internet address (to retain state between invocations by applicants) and has access to all signing instances. The high-availability proxy servers connect three distinct delegation server-signing system combinations.

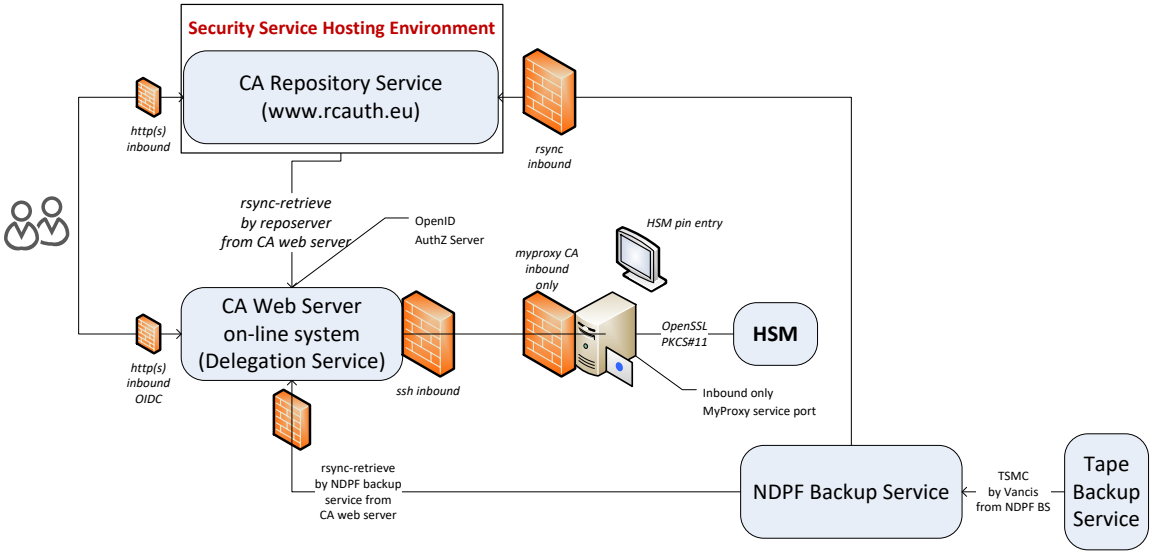


[15] http://wiki.eugridpma.org/Main/GuidelinesForOnLineCAs

For interoperability reasons, all three instances will appear towards identity providers also as a single entity and the stateful mapping amongst these is maintained through the same deterministic load-balancing algorithm.

Nikhef

Ancillary services for the on-line repository and backup are also present. The figure below details the various components and their relationships.



The **hardware cryptographic module** (HSM) is connected to the signing system through a USB port. The HSM interface software process on the signing machine uses the PIN of the HSM – provided in real-time by the CA operator – to activate the HSM over its encrypted USB connection, following which PKCS#11 requests can be sent to it.

The **CA repository service** is hosted in a virtualisation cluster exclusively dedicated to security operations, on a system shared between the RCauth CA and the other on-line repository services. The virtualisation cluster runs a recent version of the Xen virtualisation software in a 2-system cluster. The virtual system images are located exclusively on the cluster and do not use external storage. The CA repository service runs a recent version of an enterprise-classLinux operating system with host-based firewalls, connected to a network segment dedicated to trusted service operations. It accepts inbound http(80/tcp) and https(443/tcp) connections, and SSH connections only from designated Service management networks (not shown), and rsync inbound connections from the back-up service, and from a specific off-site mirror server for its public content. The virtualisation cluster only runs repository services related to operations, and ancillary operations of equal of higher trust status.

The **Nikhef Backup Service** is hosted on a dedicated system, to which only connections inbound from the and Nikhef service management networks are allowed over SSH. It initiates rsync connections to its backup clients.

The **Off-site Backup Service** is run on a trusted secure service to which interactive access is limited to operator personnel. It initiates Tivoli Storage Manager connections to its clients over port 1503/tcp, and only accepts client registration requests from trusted, authenticated, clients.

Systems are located on a monitored and controlled network segment and the systems are actively monitored for intrusions. System access logs are collected on a central log server, to which only Administrators and Nikhef CSIRT personnel have access.

RAL

Describe RAL specific setup.

GRNET

The **hardware cryptographic module** (HSM) is connected to the signing system through a PCI-E bus. The HSM interface software process on the signing machine uses the PIN of the HSM – provided in real-time by the CA operator – to activate the HSM PCI-E card, following which PKCS#11 requests can be sent to it.

The **GRNET Backup Service** is hosted on a dedicated system, to which only connections inbound from the GRNET private management networks are allowed over SSH.

6.5.2 Computer Security Rating

The systems and environment do not have a security rating.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

Necessary systems development will be performed on separate systems. All software developed or assembled will be tested for consistency and defects, and its deployment process documented. Development and operational systems are monitored for consistency with the specification.

6.6.2 Security Management Controls

Security management comprises:

- the self-audit as detaile in section 8.1
- regular review of the security concept as detailed in section 5.4 on assessments
- regular monitoring of events during log analysis as described in section 5.4.2 based on the recorded information.

6.6.3 Life Cycle Security Controls

Security controls will be reviewed during the self-audits and following (suspected) security incidents and updated when necessary.

6.7 NETWORK SECURITY CONTROLS

The Distributed RCauth service components are interconnected by a virtual private circuit on which encrypted traffic is exchanged between the issuing instances. The load-balancing layer (which is depicted in the section on operational controls) is itself distributed across the instances and distributes traffic in a deterministic way across the available issuing instances, where the traffic direction is based on the source internet address of the client so as to ensure consistent issuing state between the filtering WAYF and the delegation server.

Individual web server (and filtering WAYF) instances of the RCauth ICA may be connected directly to a monitored network of its operating partner, in order to provide a backstop capability in case of breakdown of the load balancing layer. In these cases, only a single issuing instance will be connected and be findable through the relevant RCauth.eu domain names.

At each of the operating partner networks, the RCauth ICA signing system is on a dedicated physical network, connected only to the CA Web Server as per the figure in section 6.5.1.

All other CA services are on a network segment dedicated to managed security services that does connect only machines to which specific persons carrying a Nikhef CSIRT, ICT management and security trust role. The network is monitored for intrusions.

All systems are protected by network-switch level and host-level packet filters permitting traffic to only intended ports. Management access to these systems is limited to such network endpoints

that are minimal necessary for Operators to access the system, and will not be possible from outside the operating partner location without further network authentication steps.

6.8 TIME-STAMPING

Time stamping of certificates will be done based on the internal system clock, which is periodically synchronised with external time sources. The CA signing machine synchronises with the CA web server. The CA web server synchronises with stratum-1 NTP time servers operated by Nikhef and periodically synchronised to an external reference.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

End-entity serial number

The end-entity certificates issued by the RCauth ICA can originate at any of the issuing instances of the Operating Partners. To ensure uniqueness of the serial number of the issued certificates, each issuing instance of the RCauth ICA will be assigned a numeric identifier in the range 0 ... 255, which is added to the monotonically increasing serial number of the issuing instance after multiplication of said increasing serial number by a factor 256. The resulting product will be the certificate serial number.

There shall be no more than 255 issuing instances of the RCauth ICA.

7.1.1 Version Number(s)

All certificates shall be issued as X.509 version 3 certificates.

7.1.2 Certificate Extensions

The certificate of the RCauth ICA shall have the following extensions:

Basic Constraints	Critical, CA:True
Key Usage	Critical, Certificate Sign, CRL Sign
Subject Key Identifier	keyid:*identifier*
Certificate Policies	Policy: 1.3.6.1.3.1.10434.4.2.7.1.1

The certificates issued to subscribers shall have the following extensions:

Basic Constraints	Critical, CA:False
Key Usage	Critical, Digital Signature, Key Encipherment, Data Encipherment
extendedKeyUsage	TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)
Subject Key Identifier	*The keyID identifier of the subscribers public key*
Authority Key Identifier	keyid:*identifier*
CRL Distribution Points	Full Name: URI: http://crl.rcauth.eu/pilot/g1/crl/crl.crl
Certificate Policies	Policy: 1.3.6.1.3.1.10434.4.2.8.1.2, Policy: 1.2.840.113612.5.2.2.6
Subject alternative name	email:*rfc822mail address(es) of the subscriber* [optional]

where the *identifier* shall be composed of the 160-bit SHA-1 hash of the value of the BIT STRING containing the pertinent public key (excluding the tag, length, and number of unused bits) as per option 1 of section 4.2.1.2 of RFC 5280.

The policy OID 1.2.840.113612.5.2.2.6 is asserted subject to continued accreditation by the IGTF of the CA and will be included for as long as the RCauth ICA is accredited according to the IGTF Identifier-Only Trust Assurance with Secured Infrastructure (IOTA) Authentication Profile.

7.1.3 Algorithm Object Identifiers

The appropriate object identifiers shall be included in the certificates.

For the RCauth ICA, these shall be id-sha256 (1.3.14.3.2.26), rsaEncryption (1.2.840.113549.1.1.1), and sha256WithRSAEncryption (1.2.840.113549.1.1.5).

7.1.4 Name Forms

The issuer names of the RCauth ICA shall be comprised of the sequence of sets of size one in the following order

domainComponent (DC)	IA5String	eu
domainComponent (DC)	IA5String	rcauth
organisationName (O)	PrintableString	Certification Authorities
commonName (CN)	PrintableString	Research and Collaboration Authentication Pilot CA G1

The subject names in certificates issued by the RCauth ICA shall be the sequence of sets of size one comprising in order

domainComponent (DC)	IA5String	eu
domainComponent (DC)	IA5String	rcauth
domainComponent (DC)	IA5String	rcauth-clients
organisationName (O)	UTF8String[16]	*Representation of the FIMS IdP name per section 3.1*
commonName (CN)	UTF8String	*Representation of the subscriber name and unique identifier per section 3.1*

7.1.5 Name Constraints

The RCauth ICA does not include name constraints in its issued certificates.

7.1.6 Certificate Policy Object Identifier

Issued certificates will contain the certificate policy object identifier of the RCauth ICA policy under which they are issued.

7.1.7 Usage of Policy Constraints extension

The RCauth ICA does not include a policy constraints extension.

7.1.8 Policy Qualifiers Syntax and Semantics

The RCauth ICA does not include a policy qualifier.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The RCauth ICA does not include a critical policy extension.

7.2 CRL PROFILE

The CRL nextUpdate (expiration) date shall be 30 days after the issuing date.

7.2.1 Version Number(s)

The RCauth ICA issues X.509 version 2 CRLs compliant with RFC5280.

7.2.2 CRL and CRL Entry Extensions

The RCauth ICA issues CRLs using the SHA-256-with-RSA-encryption signature algorithm. It includes the CRL number extension, which will be monotonically increasing.

[16] Out of the permissible character set of UTF8String, only the PrintableString subset will be used.

7.3 OCSP PROFILE

The RCauth ICA does not operate an authoritative OCSP service.

7.3.1 Version Number(s)

Not applicable.

7.3.2 OCSP Extensions

Not applicable.

8 COMPLIANCE, AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

The RCauth ICA will ensure that all its procedures and processes are carried out in compliance with the provisions of this CP/CPS. To this end, it shall at least once a year perform a self-assessment to check the compliance of the operation with the CP/CPS document in effect, and effectuate a review of staff.

The RCauth ICA accepts to be audited by qualified external peers, by bodies to which it has been accredited, and by qualified relying parties in order to verify its compliance with the rules and procedures prescribed herein. Any costs associated with such audit must be covered by the requesting party.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The assessor must be a knowledge expert in the domain of assessing public key infrastructures for research and scholarly purposes.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

No stipulations.

8.4 TOPICS COVERED BY ASSESSMENT

An audit may verify that the services provided by the CA comply with the version of the CP/CPS currently in force.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

In the event of a deficiency, the PMA will communicate the steps that will be taken to remedy the deficiency, including relevant time lines. If a discovered deficiency has direct consequences on the reliability of the certification process, or if certificates are likely to have been affected by the deficiency they will be revoked with immediate effect.

8.6 COMMUNICATION OF RESULTS

Results on any assessment are maintained in confidence between the assessor, the audit requesting party or parties, and the Service. Results will be disclosed to any bodies to which the RCauth ICA has been accredited. Results may be disclosed to other parties when so agreed to by the PMA.

Revocation of certificates that is an effect of an identified deficiency are communicated via the Certificate Revocation List.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

No fees are charged for certificate issuance or revocation.

9.1.2 Certificate Access Fees

No fees are charged for access to certificates.

9.1.3 Revocation or Status Information Access Fees

No fees are charged for access to certificate status information or CRLs.

9.1.4 Fees for Other Services

A reasonable reimbursement of costs may be charged for other services.

9.1.5 Refund Policy

There shall be no refunds.

9.2 FINANCIAL RESPONSIBILITY

Nikhef does not accept any financial responsibility for the use or failure to use any of the certification services, or of any information provided by, on behalf of, or by way of the Service.

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-entities

Neither the PMA, not the Operating Partners, not the Governance Board as such provide any insurance or warranty for end-entities, of whatever type. Reliance on Service material and services is at your own sole risk.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

The RCauth ICA, in its validation of individual and organisational identity, will collect personal data about subscribers. This data collection is subject to the Dutch Personal Data Protection Act (Wet bescherming persoonsgegevens). The subscriber acknowledges that the stated data is being processed according to the Privacy Plan described in section 9.4.1.

Apart from the published certificate revocation lists, the information on the on-line repository, and the fact of authentication as described in section 9.4.3, the RCauth ICA considers all data confidential.

9.3.2 Information not within the Scope of Confidential Information

Information included in and derived from CRLs and the published certificate revocation lists, the information on the on-line repository, and the fact of authentication as described in section 9.4.3 shall not be considered confidential.

9.3.3 Responsibility to Protect Confidential Information

The Service shall not disclose confidential information unless so specified in this policy (to auditors and assessors), unless it be to the PMA or to Administrators and Operators, and then only as necessary for the performance of their tasks, or unless required to by law or regulation applicable to an Operating Partner.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

The Service will keep a minimal amount of personal information, compatible with the goals of the service.

9.4.1.1 Goal of the information processing

The goal of the RCauth ICA data processing is to provide a service that issues unique, long-term, non-reassigned identity assertions to its subscribers and their explicitly authorized (software) agents for the purpose of access control to and secure operation and management of academic and research distributed digital infrastructures.

All personal data processed by the RCauth ICA is a result of an explicit, user-initiated action, to which the user is a conscious and informed participant.

Besides this processing for delivering the certificate service, the Service will store user information in log files and audit archives. These logs and audit records are used solely for administrative, operational, monitoring, security, and dispute resolution purposes of the RCauth ICA service. It may be shared for security incident response purposes with other authorised participants in the academic and research distributed digital infrastructures via secured mechanisms, only for the same purposes and only as far as necessary to provide the incident response capability.

9.4.1.2 User information and legal basis

The processing of personal data is based on the legal grounds “performance of contract” (for data described here as needed for initial issuance) and on “legitimate interests” (to enable the RCauth ICA to protects its systems, to enable the trust infrastructure enabled by the CA, and to enable participation in information security incident response resolution). The processing is thus not based on “consent”.

Before authenticating the applicant, the service will inform the user regarding the goal of the service and give the applicant the choice to continue or abort the authentication. The information will describe the types of personal data that will be processed, the fact that this information may be shared with other authorised participants as stated in section 9.4.1.1, and contain a reference to this CP/CPS and the Privacy Plan contained therein.

The user will be informed when a certificate is requested, and can at that point object to the processing of the data. By continuing the certificate request process, the user agrees to the processing for the goals stated under section 9.4.1.1. This attribute release agreement may be remembered across sessions, and this agreement can be withdrawn by the user discretionarily.

9.4.1.3 What information will be processed and stored

The following information will be processed:

- The name (display name, common name, and given name and surname) of the user
- An administrative number provided by the IdP used to identify the applicant (eduPersonUniqueID, eduPersonPrincipalName, or eduPersonTargetedID)
- A business electronic mail address of the user
- The professional affiliation of the user, for the purpose of embedding it in the certificate and for the security logs and audit records
- Any specific entitlements and authentication assurance level information provided that enable the certificate issuance to proceed

The following information will be stored:

- The issued certificates, containing the name of the user, the IdP administrative number or an rendering thereof, and the affiliation
- In the security audit logs, the certificate subject name including the information listed above, together with the affiliation (IdP entity identifier) and the full IdP administrative number

The following anonymous information derived from the personal data will be stored:

- In a long-term persistent database a one-way cryptographically non-salted secure digest of the certificate subject user elements – to ensure non-reassignment of identifiers
- In a long-term persistent database a salted one-way cryptographically secure digest of the concatenation of all values of the attributes provided as by the IdP from the ordered list of displayName, givenName, sn, commonName, mail

9.4.1.4 Where will the information be processed

The information is processed by the Service at all its operating locations: Nikhef, Amsterdam, The Netherlands; Didcot, UK; and Athens, Greece - according to the conditions stated in section 5.1. Backups of data are stored under a confidentiality agreement by the contracted backup service provider.

9.4.1.5 Who may receive the information

The information is received and processed by the RCauth ICA service, by the Administrators and Operators responsible for this service, and where necessary by the PMA and by auditors.

Certificates and certificate information may be disclosed, after explicit approval by the user, to software agents and services that act on behalf of the user, and that have registered with the RCauth ICA service[17].

Having been so informed and the user having so accepted during the certificate application, the name and contact information consisting of the organisational affiliation (the IdP name) may be shared for security incident response purposes with other authorised participants in the academic and research distributed digital infrastructures via secured mechanisms, only for the same purpose, and only as far as necessary to provide the incident response capability.

Information may be shared with law enforcement by each of the Operating Partners of the RCauth Service when so required by local applicable law.

9.4.1.6 User information and transparency

The user is informed about his or her data that is processed by the service via this privacy policy, a link to which will be presented to the user each time a certificate is requested, and a link to which will be posted on the RCauth public repository.

For more information the user is referred to this comprehensive policy and practice statement at https://www.rcauth.eu/policy/.

Users can request access to information regarding all their data at any time, and all reasonable requests to correct and/or amend the data will be processed promptly. Due to the nature of the

[17] Any such software agents are pre-registered as trusted credential management systems with the RCauth ICA service.

service, the RCauth service has a legitimate interest in recording the information recorded as per section 3.2.3 for as long as the certificate is valid plus the audit log retention period.

9.4.1.7 Protection of personal data

The personal data is protected in accordance with this CP/CPS, specifically sections 5.1 and 5.2.

Specifically the data is exclusively processed on

- The CA front-end web server, which is maintained at a high level of security and behind a double firewall both at the edge of the network and on the system itself, and where the software is maintained in accordance with best practices for vulnerability management and patching. It will run a minimal set of services. Access is via secure, encrypted and authenticated means only, and only from selected networks to which service personnel have access.
  This system is contained in a dedicated locked cabinet in a secure data centre to which access is individually controlled.
- The on-site disk back service, which is only accessible over a network from designated systems within Nikhef designated for secure system management operations, or through a VPN tunnel to which users authenticate with individual credentials, and to which only specifically authorized systems management personnel of Nikhef and the service have access.
  This system is contained in a secure data centre to which access is individually controlled.
- The off-site redundant tape backup service, which is managed under contract in the Netherlands, to which only authorized service personnel have access, and which is located in a vault inside a secure data centre where access is individually controlled.

All software is kept up to date and vulnerabilities in the software are patched promptly. Databases containing personal data are not accessible from outside the system.

The specific data protection measures are disclosed and discussed with accrediting bodies and qualified relying parties. Incidents involving personal data shall be pro-actively disclosed with the active users of the service, based on the communications information available at that time.

9.4.1.8 Information retention periods

The information that is stored will be retained for the following periods:

- issued certificates, including the information contained therein – name of the user, the IdP-provided administrative number, and the users affiliation (organisation name) – for a period of 6 months after the end of the validity period of the issued certificate, i.e. in total 19 months.
- the subject name and the non-shortened versions of the affiliation (IdP entity identifier, home organisation name) and the full IdP administrative number for 19 months after the initial authentication transaction has completed, i.e. 6 months after the issued certificate has expired.

After this period, the information will be archived in a separate long-term archive. The information in the long-term archive will be kept for a period of 3 years after the issuance of the certificate. The information in the archive is accessible only to the Administrators and will be used exclusively for dispute resolution purposes.

In separate security audit logs will be recorded the attributes[18] used to construct and issue the certificate – the displayName, commonName, givenName, sn, mail, eP(Scoped)Affiliation, ePPN, ePTID, ePUID, ePEntitlement, ePAssurance, the SAML NameID and the SAML AuthenticationContextClassReference as provided by the IdP to the service – for a period of 6 months. This information is not further archived.

[18] For attribute naming we refer to the inetOrgPerson schema definition of RFC 2798, the eduPerson 2013 definition by MACE-Dir, and the OASIS SAML 2.0 specification.

The one-way cryptographically non-salted secure digest of the certificate subject user elements is not personal information and will be recorded in the database until 3 years after the RCauth service has ceased operation.

The salted one-way cryptographically secure digest of the concatenation of all values of the attributes provided as by the IdP from the ordered list of displayName, givenName, sn, commonName, mail is not personal information and will be recorded in the database until 3 years after the RCauth service has ceased operation.

In addition to the above, backups of all data are stored – under confidentiality agreements and only for the purpose of security investigations and data recovery– for a period of 90 days.

9.4.1.9 Concerns and complaints

By law, you have certain rights over your personal data that we hold: to receive a copy of the data, to ask us to correct any errors, or to delete it once we no longer need it. To contact us regarding those rights, or anything else in this privacy notice, please write to the RCauth PMA at pma@rcauth.eu. If you do not feel we've dealt with your request appropriately, you can appeal to the data protection authority the country in which the Operating Partner is based. We refer your to the EDPB web site at https://edpb.europa.eu/about-edpb/board/members_en for contact information.

9.4.2 Information Treated as Private

Any information not explicitly made public is treated as private information. The Service protects private information using appropriate safeguards and an appropriate degree of care.

9.4.3 Information not Deemed Private

The following information collected by the RCauth ICA is deemed not to be private:

- To authenticate users with the FIMS IdPs, the RCauth service needs to redirect applicant to the IdP. The applicant, having authenticated to its own IdP, provides the RCauth service with a token to retrieve user attributes from the IdP. By retrieving attributes from the IdP, the RCauth service will disclose that the user proceeds with an authentication transation. This fact is thus implicitly released to the IdP, and this information, while confidential, will be shared with the IdP
- The contents of CRLs are not considered private information

9.4.4 Responsibility to Protect Private Information

The Service is responsible for protecting private information as stipulated in this policy.

9.4.5 Notice and Consent to Use Private Information

The processing of private information is based on the GDPR legal grounds “performance of contract” (for issuance) and “legitimate interest” (for ensuring secure, stable, and trustworthy operation of the Service and where necessary its relying parties and peers). It is not based on consent of the user.

Whenever private information is leaked or destroyed in a way that significantly impacts a person, it will be so communicated to the person involved, as long as the CA has a means of contacting the person involved.

Unless already prescribed by law, any intent of novel use of private information will be communicated to the impacted person without undue delay. No such novel use is foreseen.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The Service and/or an Operating Partner may be forced to disclose confidential information to law enforcement agencies in the country or countries in which they are established.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 INTELLECTUAL PROPERTY RIGHTS

The Service does not claim Intellectual Property Rights on issued certificates or CRLs.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA Representations and Warranties

Except as stated in this CP/CPS or in a separate agreement with the Service Governance bodies, nor any of the governance bodies, nor any of its members, not the Operating Partners and any of their personnel, not Administrators nor Operators make any representations regarding their services.

The Service represents to the extent specified in this CP/CPS that it

- complies with this CP/CPS;
- the certificates issued by the RCauth ICA will be issued solely in compliance with this CP/CPS;
- it will maintain an on-line accessible repository containing the published information with an intended continuous availability.

9.6.2 RA Representations and Warranties

The RCauth ICA PMA and the Administrators, being responsible for the acceptance of RAs, represent that the RA will act in accordance with the provisions in this CP/CPS to the best of their knowledge.

By performing a successful authentication and by releasing a signed statement of attributes regarding the applicant, the RA – represented by its FIMS IdP – represents that the data provided substantially corresponds to its current best knowledge of the value of the released attributes, and that the authenticator of the applicant – at the time of authentication, is not known to be compromised and that the applicant is not in violation of any acceptable use policies imposed by the RA upon its users.

The RA represents that the authenticated applicant has been identified and is known to the RA, and that – based on the unique identifier provided by the IdP to the CA service – the RA has a means to link the act of authentication to that authenticated specific applicant.

The RA represents that any FIMS systems and networks used to authenticate applicants and interact with the RCauth ICA service are adequately protected and configured to provide an operational security capability suitable for identity management, aligned with the Operational Security capabilities specified in Sirtfi.

The RA warrants that it will only indicate compliance with the REFEDS R&S specification and with the Sirtfi framework if the RA is capable of fulfilling respectively the R&S and Sirtfi requirements, and – if the IdP is registered in eduGAIN and releases attributes to the CA service – that it will abide by the policies of the registering federation (eduGAIN registrar).

9.6.3 Subscriber Representations and Warranties

Subscribers are responsible for any representations and warranties made by them to the Service, their relying parties, and any other third parties, and for any actions that use the private key of the subscriber, regardless whether such use was authorized, for as long as the certificate is valid and for as long as a CRL containing the certificate's revocation information has not been published.

The subscriber represents to the Service and third parties that he or she will act in accordance with all the provisions in this CP/CPS document; inform without undue delay the RCauth ICA of any material changes that pertain to the certificate or the information contained therein; use the certificate only for lawful purposes; will cease using the certificate if so instructed by the RCauth ICA; and has taken notice of and consented to the Privacy Policy as detailed in section 9.4.1.

Subscribers represent and warrant that certificates are only used for purposes compatible with section 1.4.

9.6.4 Relying Party Representations and Warranties

Each relying party represents that, before relying on any certificate of the RCauth ICA, it shall have read, understood, and act in compliance with this CP/CPS, that it has appropriate knowledge of PKI and appropriate technical implementations to validate certificates issued by the RCauth ICA, and that it shall have obtained the up-to-date certificate status information as published by the RCauth ICA and act in accordance therewith.

Each relying party shall represent that it bear the sole responsibility for reliance on any certificate issued by the RCauth ICA, any such reliance is at its own risk, and that it has thereto executed an appropriate risk assessment.

9.6.5 Representations and Warranties of Other Participants

Software agents and credential repositories may be used by applicants, in such a way that these repositories have to establish a relationship with the RCauth ICA. Where such a relationship is established, the CA will consider such relationships based on compliance with the Private Key Protection Guidelines[19] and the current best practice with regard to the operation of Trusted Credential Stores[20]

9.7 DISCLAIMERS OF WARRANTIES

All certificates and any related materials, software, publications, and service are provided 'as-is' and 'as available', without any warranties. To the maximum extent permitted by law, the Service, Nikhef, Nikhef partners, Nikhef personnel, SURF, and all others involved in the Service disclaim all express and implies warranties and liabilities, including all warranties of merchantability, fitness for a particular purpose, and non-infringement. Neither the Service, Nikhef, Nikhef partners, Nikhef personnel, SURF, not any others involved in the Service warrant that any service, product, certificate or other artefact will meet any expectations or that access to certificates will be timely or error-free, or that it is available at any time. The RCauth ICA and the Service may discontinue any service at any time.

9.8 LIMITATIONS OF LIABILITY

The Service, Nikhef, Nikhef partners, Nikhef personnel, SURF, and all others involved in the Service decline any liability for damages incurred by any subscriber, registration authority, relying party, or third party relying on the certificates or information issued or published by the RCauth ICA or Service. It also declines any liability for damages arising from the non-issuance of a requested certificate, or for the revocation of a certificate even when initiated directly by the RCauth ICA.

[19] https://www.eugridpma.org/guidelines/pkp/

[20] http://wiki.eugridpma.org/Main/CredStoreOperationsGuideline

9.9 INDEMNITIES

To the extent permitted by law, each subscriber and relying party shall indemnify the Service, Nikhef, Nikhef partners, SURF, and all others involved in the Service, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the subscriber's or relying party's (i) breach of this CP/CPS, or applicable law; (ii) unreasonable reliance on a certificate; or (iii) failure to check the certificate's status prior to use.

9.10 TERM AND TERMINATION

9.10.1 Term

This CP/CPS and any amendments are effective when published in the on-line repository as per the date there stated, and will remain in effect until replaced with a newer version or withdrawn.

9.10.2 Termination

This CP/CPS will remain in effect until replaced with a newer version or withdrawn.

9.10.3 Effect of Termination and Survival

Its text shall remain available for at least 5 years after the last certificate issued under this CP/CPS expires or is revoked.

All conditions related to retention of data and audit logs, and all conditions related to the protection of personal information will survive the termination of the RCauth ICA.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Individuals can communicate with the RCauth ICA using the information provided in section 2.2.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

This CP/CPS is reviewed annually at the time of the self-audit. Amendments are made by posting an updated version of the CP/CPS to the online repository.

9.12.2 Notification Mechanism and Period

The Service will post changes to this CP/CPS in its on-line repository. It will inform any bodies to which it has been accredited and that request prior notification for changes to the CP/CPS in a timely fashion but at least two weeks before the new CP/CPS becomes effective.

9.12.3 Circumstances Under which OID Must be Changed

Material changes to the CP/CPS, such as to be determined by the Service Manager, will cause the OID to change.

9.13 DISPUTE RESOLUTION PROVISIONS

Parties are required to notify and communicate with the PMA and with the Administrators of the Service and attempt to resolve disputes directly, before resorting to any dispute resolution mechanism.

9.14 GOVERNING LAW

The interpretation, construction, and validity of this policy shall be governed by the laws of the Kingdom of the Netherlands.

9.15 COMPLIANCE WITH APPLICABLE LAW

This CP/CPS is subject to all applicable laws and regulations.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire agreement

This CP/CPS constitutes the entire agreement between the Service RCauth ICA and any other party, unless a more specific agreement is in place. If such an agreement has provisions that differ from this CP/CPS, the more specific agreement takes precedence, but only with respect to that party. No others may rely on such a more specific agreement, or bring action to enforce such agreement.

9.16.2 Assignment

Any entities operating under this CP/CPS may not re-assign their rights or obligations without consent of the Service Managers.

9.16.3 Severability

If any provision of this CP/CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of this CP/CPS will remain valid and enforceable. Each provision of this CP/CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

The Service, Nikhef, Nikhef partners, Nikhef personnel, SURF, and all others involved in the Service may seek indemnification and attorney's fees from a party for any damages, losses, or expenses related to that party's conduct.

9.16.5 Force Majeure

The Service is not liable for any delay or failure to perform an obligation under this CP/CPS to the extent that the delay or failure is caused by an occurrence beyond the Service' or Nikhef's reasonable control.

9.17 OTHER PROVISIONS

No stipulation.