Pittsburgh Supercomputing Center MyProxy Certificate Authority Short Lived Credential Service (PSC MyProxy CA)

Certificate Policy and Certification Practice Statement Version 1.8

Pittsburgh Supercomputing Center
300 South Craig St
Pittsburgh, PA 15213

9 December 2020 11:30 EDT (GMT -4:00)

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Overview

This document (hereafter "Policy") defines the Certificate Policy and Certification Practice Statement (CP/CPS) for the Pittsburgh Supercomputing Center (PSC) MyProxy Certificate Authority (PSC MyProxy CA) short-lived credential service (SLCS). This Policy is structured as specified in the Internet Engineering Task Force (IETF) document "RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" [Chokani et al, November 2003].

The PSC MyProxy CA provides short-lived X.509 credentials (keys and certificates with a lifetime up to 168 hours) to authorized and authenticated XSEDE users, for use in user authentication to XSEDE[1] resources. The PSC MyProxy CA operates as an independent SLCS to provide a second SLCS for the same XSEDE community served by the TAGPMA-accredited NCSA SLCS. XSEDE clients and services configured to use the NCSA SLCS as their default SLCS may use the PSC MyProxy CA as an alternate source for short-lived X.509 certificates if the NCSA SLCS is unavailable. This CP/CPS specifies minimum requirements for issuance and management of user credentials provided by the PSC MyProxy CA and for operation and security of the PSC MyProxy CA..

The PSC MyProxy CA is an online, MyProxy CA[2] short-lived credential service (SLCS) for authorized and authenticated XSEDE users, operated on secured hosts located in the PSC production high performance computing (HPC) systems facility.

Figure 1 illustrates the architecture of the PSC MyProxy CA. The PSC MyProxy CA is integrated with the XSEDE Central Database (XDCDB) and Kerberos authentication service for identity management. The XSEDE accounting process enrolls users in the user database, creates a TERAGRID.ORG[3] Kerberos principal for them, and assigns them a distinguished name (DN). User DNs for NCSA SLCS-issued certificates are differentiated from those for PSC MyProxy CA-issued certificates by their Organization (O=) field.

To obtain credentials, PSC MyProxy CA subscribers run MyProxy client software on the host where their credentials are to be stored. The MyProxy client software generates the subscriber's private key locally, authenticates the user to the PSC MyProxy CA via Kerberos, submits a signed certificate request to the PSC MyProxy CA, and, if the request is approved, receives a signed certificate back from the PSC MyProxy CA.

The PSC MyProxy CA consults data retrieved from the XSEDE Central Database to determine the distinguished name (DN) that corresponds to the user's authenticated TERAGRID.ORG Kerberos identity and issues a certificate with the appropriate DN accordingly.

Further policy and implementation details are provided throughout this document.

---

[1] XSEDE is a distributed cyberinfrastructure project sponsored by the U.S. National Science Foundation (NSF). XSEDE links computation resources at several partner sites located across the U.S., including Indiana University, the National Center for Supercomputing Applications (NCSA), the National Institute for Computational Sciences (NICS), Pittsburgh Supercomputing Center (PSC), Purdue University, San Diego Supercomputer Center (SDSC), Texas Advanced Computing Center (TACC), the National Center for Atmospheric Research (NCAR), and University of Tennessee Knoxville. http://www.xsede.org

[2] MyProxy CA: MyProxy Credential Management System Certificate Authority. National Center for Supercomputing Applications, ©2000-2009 Board of Trustees of the University of Illinois. http://grid.ncsa.illinois.edu/myproxy/ca/

[3] The U.S. National Science Foundation (NSF) XSEDE projects were preceded by similar NSF cyberinfrastructure projects called TeraGrid. The original TERAGRID.ORG Kerberos realm was retained in the follow-on XSEDE projects and remains in use for XSEDE user principals.

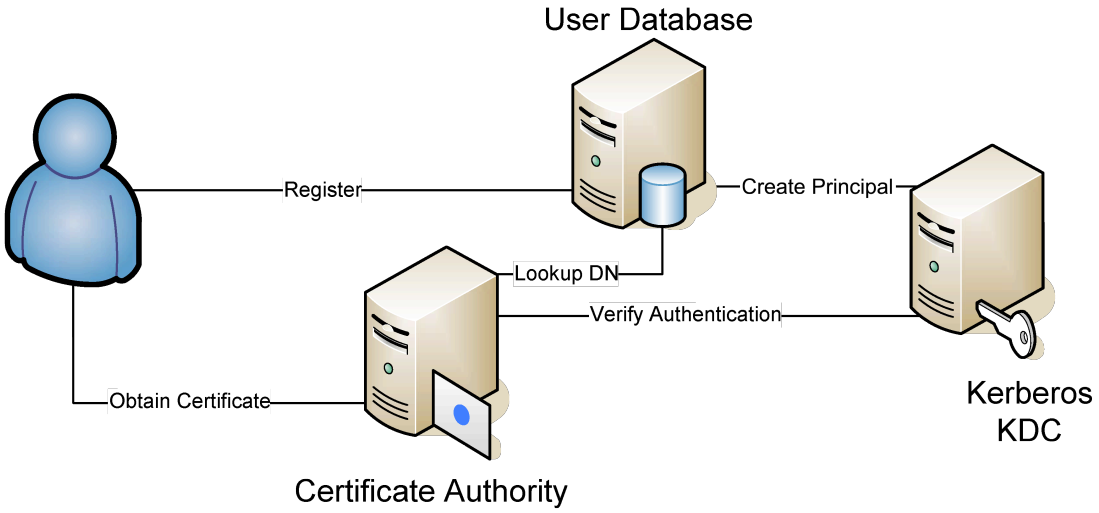

Figure 1: PSC MyProxy CA functional Architecture

1.2 Document Name and Identification

Title:	“Pittsburgh Supercomputing Center MyProxy Certificate Authority Short-Lived Credential Service (PSC MyProxy CA) Certificate Policy and Certification Practice Statement”
URL:	http://ca.psc.edu/psc-myproxy-ca/
Version:	1.7
Revision Date:	9 December 2020 11:30 Eastern Daylight Time (GMT -4:00)
OID:	1.3.6.1.4.1.26703.99.7512.1.1.1.8 { iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) Pittsburgh Supercomputing Center(26703) CA(99) MyProxy CA(7512) SLCS(1) CP/CPS(1) Major Revision(1) Minor Revision(8) }

1.3 PKI Participants

1.3.1 Certification Authorities

This Policy applies to the PSC MyProxy CA. The PSC MyProxy CA's certificate is signed only by the PSC MyProxy CA itself. The PSC MyProxy CA will otherwise only sign end entity certificates. No CAs are subordinate to the PSC MyProxy CA.

1.3.2 Registration Authorities

XSEDE users apply for access to XSEDE resources via the XSEDE User Portal (XUP), backed by a centralized allocations and account management system operated by XSEDE Enterprise Services. XSEDE Allocations staff at NCSA enroll users into the XSEDE Central Database (XDCDB) according to the enrollment process described in Section 4.1.2, create accounts in the TERAGRID.ORG Kerberos realm for new users, and assign distinguished names to new users according to Section 3.1. The NCSA SLCS and PSC MyProxy CA retrieve data from the XDCDB to map authenticated users to the correct X.509 distinguished name (DN), and issue X.509 certificates accordingly. XSEDE allocations group staff thereby serve as the registration authority for both the NCSA SLCS and the PSC MyProxy CA.

1.3.3 Subscribers (End Entities)

XSEDE users include XSEDE staff and all authorized users with active XSEDE project allocations on XSEDE production Service Provider (SP) resources, as recorded in the XDCDB. The PSC MyProxy CA will provide X.509 credentials to users successfully authenticated in the TERAGRID.ORG realm via the XSEDE Kerberos service. These credentials are issued with a PSC distinguished name (see section 3.1.4) specific to the authenticated XSEDE user and with a unique serial number. Credentials issued by the PSC MyProxy CA may be used for authentication, encryption, and digital signing by the authenticated XSEDE user.

1.3.4 Relying Parties

PSC places no restrictions on who may accept PSC MyProxy CA certificates.

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The PSC MyProxy CA issues X.509 credentials to XSEDE users for the purpose of authentication to XSEDE production systems and services that support Grid Security Infrastructure (GSI)[4] and/or SSL/TLS authentication. These include XSEDE web portals, high-performance computing (HPC) systems, storage resources, job submission services and data transfer services.

1.4.2 Prohibited Certificate Uses

Other uses of PSC MyProxy CA certificates are not prohibited, but neither are they endorsed, approved, nor supported by PSC.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This Policy is administered by the Pittsburgh Supercomputing Center, 300 South Craig Street, Pittsburgh, PA 15213, U.S.A.

1.5.2 Contact Person

The primary contact for this Policy and matters relating to the PSC MyProxy CA is the PSC Information Security Officer:

Derek K. Simmel <dsimmel@psc.edu>
Senior Information Security Officer
Pittsburgh Supercomputing Center
300 South Craig St
Pittsburgh, PA 15213, U.S.A.
+1 (412) 268-4960

After hours contact information:
PSC Hotline: +1 (412) 268-6350

Security issues should be reported to the PSC Hotline or vie e-mail to: <security@psc.edu>
Inquiries regarding CA operations and certificates issued by the PSC PKI: <ca-admin@psc.edu>
Other non-emergency inquiries: <remarks@psc.edu>

Registration Authority and XSEDE user inquiries may be directed to:
XSEDE Help Desk: +1 (866) 907-2383
or via e-mail to: <help@xsede.org>

1.5.3 Person Determining CPS Suitability for the Policy

The PSC Information Security Officer is the designated authority with responsibility for determining CPS suitability for the Policy.

[4] Grid Security Infrastructure (GSI). http://www.globus.org/security/overview.html

1.5.4 CPS approval procedures

The PSC Information Security Officer determines CPS approval procedures in keeping with requirements of accrediting policy management authorities (PMAs) recognized by PSC and relying parties (e.g., TAGPMA).

1.6 Definitions and Acronyms

1.6.1 Definitions

This Policy makes use of the following terms and concepts. For terms defined in IETF RFC 3647, the definitions are included here verbatim:

Activation Data – Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually-held key share).

Authentication – The process of establishing that individuals, organizations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual or organization. This corresponds to the second process involved with identification, as shown in the definition of "identification" below. Authentication can also refer to a security service that provides assurances that individuals, organizations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organization, or device. Thus, it is said that a digital signature of a message authenticates the message's sender.

Certificate – (see *Digital Certificate* below).

Certificate Authority (CA) – A service established to digitally sign public digital keys, producing signed digital certificates. Relying parties trust the CA to sign the public digital key of end entities (users, systems, services, etc) only after the CA's registration authority has authenticated certificate requests by end-entities and has verified that applicants and requests meet policy requirements for certificate issuance by the CA.

CA-certificate – A certificate for one CA's public key issued by another CA.

Certificate policy (CP) – A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range.

Certification Path – An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

Certification Practice Statement (CPS) – A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.

CPS Summary (or *CPS Abstract*) – A subset of the provisions of a complete CPS that is made public by a CA.

Credential – A digital certificate and associated private digital key used in authentication transactions to establish the identity of end entities.

Digital Certificate – A uniquely defined data structure containing a digital public key and digital signatures of the digital public key provided by certificate authorities.

Digital Signature – A unique cryptographic checksum calculated for a data structure, which is then encrypted using a private digital key. In the case of digital certificates issued by a CA, the data structure includes an end entity's public key and other data to assure the uniqueness of the resulting digital signature (e.g., timestamp, serial number, attributes, etc.). The CA's private digital

key is used to encrypt the cryptographic checksum. Relying parties then use the CA's corresponding public digital key (contained in the CA-certificate) to decrypt the checksum and verify the digital certificate's contents.

End Entity – a unique user, system, or service whose identity or authenticity can be validated via trusted means.

GRID-SEC - A private consortium of information security professionals world-wide, focused on coordinated response to cross-grid security incidents. http://grid-sec.web.cern.ch/grid-sec/Site/GRID-SEC.html

Identification – The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization. In the context of a PKI, identification refers to two processes:

1. Establishing that a given name of an individual or organization corresponds to a real-world identity of an individual or organization, and
2. Establishing that an individual or organization applying for or seeking access to something under that name is, in fact, the named individual or organization. A person seeking identification may be a certificate applicant, an applicant for employment in a trusted position within a PKI participant, or a person seeking access to a network or software application, such as a CA administrator seeking access to CA systems.

Issuing Certification Authority (issuing CA) – In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject certification authority).

Kerberos – "a secure, single-sign-on, trusted third party, mutual authentication service" [Garman, P.6]. Kerberos is a network authentication protocol developed at the Massachusetts Institute of Technology (MIT), designed to provide strong authentication for client/server applications by using symmetric (i.e., secret-key) cryptography [http://web.mit.edu/kerberos/]. The Kerberos Network Authentication Service (version 5, current as of this document) is described in IETF RFC 4120 (http://www.ietf.org/rfc/rfc4120.txt). Implementations of Kerberos version 5 are available from MIT (http://web.mit.edu/kerberos/) and from Heimdal (www.h5l.org).

Kerberos Key Distribution Center (KDC) – A KDC contains Kerberos principals and their associated secret-key passwords. A Kerberos realm must have at least one primary KDC, and may have additional secondary KDCs distributed throughout the network. Principals and their passwords are automatically and securely replicated among all KDCs participating in a Kerberos Realm. A KDC provides two services:

1. *Authentication Service* (AS): When a client (as identified by its principal) wishes to authenticate via Kerberos, it must first contact the Authentication Service to obtain a Ticket Granting Ticket (TGT). The AS generates and encrypts a TGT using the client's password and returns it to the client. Since only the authentic client should know the correct password, it can decrypt the TGT correctly. All subsequent requests for services by the client are submitted using the TGT. The TGT has short-term validity and contains an encrypted session key used for subsequent, secured interactions by the user with the KDC's Ticket Granting Service. This enables single-sign-on: a client who is a user can use the TGT to authenticate to services without having to re-enter his/her password.
2. *Ticket Granting Service* (TGS): Clients authenticate to services by submitting a request to the Ticket Granting Service along with their TGT. The TGS decrypts the TGT to check its validity..It then generates a new private session key, to be shared between the client and the service. The private session key is encrypted in a service ticket using the service's password. The TGS responds to the client by sending it the service ticket together with another copy of the private session key, all encrypted using the client's password. The client then decrypts the private session key and the service ticket. The client then contacts the service, supplying the encrypted service ticket. The service decrypts the service ticket to authenticate the client and to extract the private session key. Thereafter

the client and service establish secure communications using their mutually shared, private session key.

Kerberos Principal – a unique name identifying a user, host, device, or service participating in a Kerberos Realm.

Kerberos Realm – a name, representing a single administrative domain, for a collection of users, hosts, devices, and services, managed together for authentication purposes.

Legal Name (of user end entities) – The user's name as it appears on official government-issued identity credentials, e.g. passport, driver's license, birth certificate.

Participant – An individual or organization that plays a role within a given PKI as a subscriber, relying party, CA, RA, certificate manufacturing authority, repository service provider, or similar entity.

PKI Disclosure Statement (PDS) – An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS.

Policy Qualifier – Policy-dependent information that may accompany a CP identifier in an X.509 certificate. Such information can include a pointer to the URL of the applicable CPS or relying party agreement. It may also include text (or number causing the appearance of text) that contains terms of the use of the certificate or other legal information.

Private Digital Key (or *Private Key*) – A sequence of bits (typically generated via pseudo-random calculations) to be used privately by the key holder as a digital encryption and decryption key. The key holder must store and use the private key securely to prevent disclosure to unauthorized users. In public key cryptography procedures, the private key is generated together with a corresponding public key; data encrypted with the private key can only be correctly decrypted using the corresponding public key – this assures authenticity of the encrypting source and enables digital signatures and nonrepudiation; data encrypted with the public key can only be decrypted using the corresponding private key – this assures secrecy of data encrypted by the source and transmitted to the private key holder, which facilitates secure communications including private e-mail.

Public Digital Key (or *Public Key*) – A sequence of bits (typically generated via cryptographic calculations) generated as a complementary key for a corresponding private digital key. The public key is not secret and may be distributed publicly. The public key is used in public cryptography procedures to encrypt data that can only be decrypted correctly using the corresponding private key, and visa versa; the public key can only correctly decrypt data encrypted using the corresponding private key. Digital certificates contain a public key, digitally signed by one or more CAs, which serve to bind the public key to the identity of a specific end entity.

Registration Authority (RA) – An entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by subscribers to renew or re-key their certificates. RAs, however, do not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA). [Note: The term Local Registration Authority (LRA) is sometimes used in other documents for the same concept.]

Relying Party – A recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.

Relying Party Agreement (RPA) – An agreement between a certification authority and relying party that typically establishes the rights and responsibilities between those parties regarding the verification of digital signatures or other uses of certificates.

Research and Education Networking - Information Sharing and Analysis Center (REN-ISAC). http://www.ren-isac.net/

Set Of Provisions – A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a CP or CPS employing the approach described in this framework.

Subject Certification Authority (subject CA) – In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate (see also Issuing certification authority).

Subscriber – A subject of a certificate who is issued a certificate.

Subscriber Agreement – An agreement between a CA and a subscriber that establishes the right and responsibilities of the parties regarding the issuance and management of certificates.

TeraGrid – The name of the U.S. National Science Foundation national cyberinfrastructure project (2001-2010) prior to its new XSEDE (2011-present) name.

TERAGRID.ORG – The name of the Kerberos authentication realm for the TeraGrid and XSEDE projects. XSEDE user principal names are Kerberos principals in the TERAGRID.ORG realm.

Validation – The process of identification of certificate applicants. "Validation" is a subset of "identification" and refers to identification in the context of establishing the identity of certificate applicants.

XSEDE – XSEDE is a distributed cyberinfrastructure project sponsored by the U.S. National Science Foundation (NSF). XSEDE links computation resources at several partner sites located across the U.S., including Indiana University, the National Center for Supercomputing Applications (NCSA), the National Institute for Computational Sciences (NICS), Pittsburgh Supercomputing Center (PSC), Purdue University, San Diego Supercomputer Center (SDSC), Texas Advanced Computing Center (TACC), the National Center for Atmospheric Research (NCAR), and University of Tennessee Knoxville. http://www.xsede.org

XSEDE User Portal (XUP) – a web portal operated by the XSEDE to provide user support services and documentation to the XSEDE user community.

1.6.2 Acronyms

AS	Authentication Service (Kerberos)
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules (binary file format)
DN	Distinguished Name (a.k.a. certificate Subject)
FIPS	(U.S.) Federal Information Processing Standard
GSI	(Globus) Grid Security Infrastructure
HPC	High Performance Computing
IETF	Internet Engineering Task Force

IGTF	International Grid Trust Federation
IPR	Intellectual Property Right
KDC	Key Distribution Center (Kerberos)
LONI	Louisiana Optical Network Initiative
LRA	Local Registration Authority
NCAR	National Center for Atmospheric Research
NCSA	National Center for Supercomputing Applications
NICS	National Institute for Computational Sciences
NSF	National Science Foundation (United States)
ORNL	Oak Ridge National Laboratory
PDS	PKI Disclosure Statement
PEM	Privacy Enhanced Mail (e-mail-compatible text file format)
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PSC	Pittsburgh Supercomputing Center
RA	Registration Authority
REN-ISAC	Research and Education Networking - Information Sharing and Analysis Center
RFC	Request for Comments (IETF publication)
RPA	Relying Party Agreement
SDSC	San Diego Supercomputer Center
SSH	Secure Shell (protocol, service and client software)
SSL	Secure Sockets Layer (protocol)
SLCS	Short-Lived Certificate Service
SP	Service Provider (XSEDE)
TACC	Texas Advanced Computing Center
TAGPMA	The Americas Grid Policy Management Authority
TGS	Ticket Granting Service (Kerberos)
TGT	Ticket Granting Ticket (Kerberos)
TLS	Transport Layer Security (protocol)
UC/ANL	University of Chicago / Argonne National Laboratory
XDCDB	XSEDE Central Database
XUP	XSEDE User Portal

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The repository for the PSC MyProxy CA is at http://ca,psc.edu/psc-myproxy-ca/

2.2 Publication of Certification Information

The PSC MyProxy CA repository lists contact information for PSC CA operations, and contains:

- The self-signed PEM-formatted CA-certificate
- Current signing policy file for the CA, defining subjects of certificates signed by the CA
- A file containing the URL for the CA's CRL, with a .crl_url file suffix
- Current DER-formatted CRL for the CA, with a .crl file suffix
- Current PEM-formatted CRL for the CA, with a .r0 file suffix
- Public sections of governing policy documents for the CA, including the CA's CP/CPS
- An example user certificate issued by the PSC MyProxy CA

Public announcements issued by the PSC Information Security Officer regarding PSC CAs may also be posted at the repository website.

2.3 Time or Frequency of Publication

New CA certificates will be published immediately upon issue, renewal or replacement.

New CA Certificate Revocation List Uniform Resource Location (CRL URL) files will be published immediately following changes to the URLs for the locations of the corresponding CRL files.

Certificate Revocation Lists (CRLs) for PSC MyProxy CA will be published immediately to the repository upon revocation of a certificate, as well as on a regular basis to assure relying parties regarding the currency of each CRL. The date of issue for each CRL will be recorded in the CRL's *lastUpdate* field, and the CRL's *nextUpdate* field will indicate the maximum validity lifetime of the issued CRL. The maximum validity for PSC CA CRLs will be 14 days, although new CRLs will be issued regularly on a more frequent basis.

The PSC MyProxy CA will generate and publish its CRL daily, and immediately following revocation of any issued certificates.

The signing policy file for the PSC MyProxy CA will be published immediately following any update to the file.

New editions of public sections of governing policy documents (including this Policy) will be published immediately following updates and release for publication by the PSC Information Security Officer.

2.4 Access Controls on Repositories

No restrictions will be placed on access to public documents and data published on the PSC CA repository. 24x7 availability of the PSC CA repository will be maintained on a best effort basis.

PSC grants accrediting PMAs unlimited redistribution of public documents published on the PSC CA repository.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

Subject distinguished names are X.500 names, with component fields defined according to the type of certificate issued.

3.1.2 Need for Names to be Meaningful

Subject DNs for user certificates issued by the PSC MyProxy CA include a “Common Name” (CN=) field defined using the user’s legal name. In the event of name conflicts, an additional number value is permanently assigned and recorded in the XSEDE Central Database and is included in the Common Name field to distinguish between users.

3.1.3 Anonymity or Pseudonymity of Subscribers

Anonymity and Pseudonymity are not supported.

3.1.4 Rules for Interpreting Various Name Forms

All Subject Distinguished Names (DNs) in certificates issued by PSC CAs are defined with the following initial component fields:

- Country C=US
- Organization O=Pittsburgh Supercomputing Center

The PSC MyProxy CA certificate subject DN includes an additional “Common Name” (CN=) field, identifying the CA:

“C=US, O=Pittsburgh Supercomputing Center, CN=PSC MyProxy CA”

Subject DNs for end entity certificates issued to authenticated users by the PSC MyProxy CA are defined as follows:

- Country C=US
- Organization O=Pittsburgh Supercomputing Center
- Common Name CN=*XSEDE User Legal Name [#]*

A XSEDE user’s “Common Name” component field is defined using the user’s legal name field as recorded in the XSEDE Central Database (XDCDB). This field includes a unique number suffix assigned in the event of name conflicts.

Example:

"C=US, O=Pittsburgh Supercomputing Center, CN=Jim Marsteller 2"

3.1.5 Uniqueness of Names

To differentiate certificates issued by PSC CAs in the global namespace, all certificates issued by PSC CAs begin with the following initial component fields:

- Country C=US
- Organization O=Pittsburgh Supercomputing Center

End entity user certificates issued by the PSC MyProxy CA will have a unique subject DN assigned to only one XSEDE user. New certificates with the same subject DN may be issued by the PSC MyProxy CA to the same authenticated user, but never to different users.

Every certificate issued by the PSC MyProxy CA will have a unique serial number that is never reused. The MyProxy service keeps track of the serial number of the most recently issued certificate. For every new certificate issued, the service increments the current serial number and assigns it to the new certificate.

XSEDE users are identified by unique records in the XDCDB and their corresponding Kerberos principals in the TERAGRID.ORG realm. XSEDE Allocations Group procedures and database applications check for name conflicts and ensure that applicable field contents are unique by appending, when required, a unique numeric suffix. Every XSEDE user is assigned a unique TERAGRID.ORG Kerberos principal. The initialization procedure for TERAGRID.ORG Kerberos principals rejects duplicates.

New XSEDE users are required to change their initial TERAGRID.ORG Kerberos password within 30 days. New TERAGRID.ORG Kerberos principals that do not have their initial passwords changed within 30 days are automatically disabled. Affected users must request a new initial password to reinstate their TERAGRID.ORG principal, as described in section 4.1.2.

User account records may be deactivated but are not deleted from the XDCDB. User account records in the XDCDB are never reassigned to different users. TERAGRID.ORG Kerberos user principals are never reassigned to different users.

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulation.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Certificate requests must be digitally signed using the private key.

3.2.2 Authentication of Organization Identity

Users are identified as *XSEDE users* by their records in the XSEDE Central Database (XDCDB), and assignment of a unique principal in the TERAGRID.ORG Kerberos realm. Users obtain records in the XDCDB as described in section 4.1.2. Users employ their TERAGRID.ORG Kerberos principal and associated private password to authenticate themselves to XSEDE systems and services.

3.2.3 Authentication of Individual Identity

XSEDE users employ a MyProxy client to generate a private key and to submit a certificate request (signed using the private key) to the PSC MyProxy CA. Users must provide their TERAGRID.ORG Kerberos principal to identify themselves to the PSC MyProxy CA. The PSC MyProxy CA authenticates users submitting certificate requests via Kerberos. XSEDE users are prompted by the MyProxy client to enter their TERAGRID.ORG Kerberos password, which is used to decrypt a Kerberos ticket retrieved from a TERAGRID.ORG Kerberos Key Distribution

Center (KDC). Successful decryption of the Kerberos ticket serves as proof of the correct password entered by the user.

The Kerberos authentication infrastructure for TERAGRID.ORG is distributed among several participating XSEDE Service Provider (SP) sites. XSEDE SP sites are connected to the XSEDE network and provide high performance computation (HPC), storage, networking, security, and web resources to XSEDE. The primary TERAGRID.ORG KDC is operated and administered by NCSA. PSC operates and administers a secondary KDC for the TERAGRID.ORG Kerberos realm. The PSC TERAGRID.ORG KDC is physically maintained in the same facility as the PSC MyProxy CA, as described in Section 6.5.

The Kerberos authentication infrastructure only provides data to users and services (in this case the PSC MyProxy CA) necessary to perform authentication tasks. Authentication processing and resulting user authorization decisions are executed by the MyProxy service (PSC MyProxy CA) to which the user has submitted a certificate request (via their MyProxy client). Traceability of approved and denied certificate requests thereby lies in the MyProxy service transaction logs.

Upon successful authentication, the PSC MyProxy CA maps the user's TERAGRID.ORG principal to a unique certificate subject DN that is based on a unique “common name” assigned to the user in the XDCDB.

The NCSA SLCS and PSC MyProxy CA use the same XSEDE-maintained Kerberos service to authenticate user requests. The NCSA SLCS and PSC MyProxy CA separately retrieve data from the XDCDB to map the correct distinguished name (DN) for short-term X.509 certificates issued to authenticated requesters. Queries to the XDCDB are executed via SSL-encrypted sessions. DNs for certificates issued by the NCSA SLCS are differentiated from those issued by the PSC MyProxy CA by their Organization (O=) fields, as described in section 3.1.

If traceability to a user is lost, i.e., PSC is unable to contact a user based on the data associated with that user in the XDCDB, then the user's TERAGRID.ORG user principal will be disabled via XSEDE security procedures to prevent further attempts to obtain certificates issued by the PSC MyProxy CA. Disabling the user's TERAGRID.ORG principal also prevents its use for authentication by the user to other XSEDE services.

3.2.4 Non-Verified Subscriber Information

Subscriber name, organization affiliation, phone number and postal address are verified by the XSEDE Allocations staff upon creation of the subscriber’s user record in the XDCDB and their TERAGRID.ORG Kerberos user principal. Other subscriber information is not verified.

3.2.5 Validation of Authority

Users with an active XSEDE project resource allocation are permitted to use MyProxy clients together with their TERAGRID.ORG user principal and password to obtain a certificate from the PSC MyProxy CA. XSEDE users requesting credentials from the PSC MyProxy CA must authenticate successfully via Kerberos (using their TERAGRID.ORG user principal and password) as the user identified in the certificate to be issued.

3.2.6 Criteria for Interoperation

The PSC PKI is intended to interoperate with other CAs within XSEDE and the International Grid Trust Federation (IGTF).

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

The PSC MyProxy CA certificate will not be re-keyed. Circumstances warranting replacement of the PSC MyProxy CA key will be treated as a Key Changeover, as described in section 5.6.

End-entity certificates issued by the PSC MyProxy CA are not re-keyed. Subscribers must request a new certificate as described in section 3.2.3

3.3.2 Identification and Authentication for Re-Key after Revocation

The PSC MyProxy CA certificate will not be re-keyed after revocation.

End-entity certificates will not be re-keyed after revocation.

3.4 Identification and Authentication for Revocation Request

Revocation of certificates issued by PSC CAs will only be initiated and executed by PSC security staff under direct supervision of the PSC Information Security Officer.

Users may request revocation by contacting the PSC Hotline at +1 (412) 268-6350 or via e-mail at security@psc.edu.

PSC Information Security Operations may revoke a certificate if evidence of compromise or exposure of the private key is received.

PSC Information Security Operations will verify the authenticity of revocation requests by checking digital signatures on the request or by telephone to the requester’s registered phone number.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can Submit a Certificate Application

A XSEDE user with an active XSEDE project allocation in the XDCDB, and thereby an active Kerberos principal in the TERAGRID.ORG realm, may request a certificate from the PSC MyProxy CA.

4.1.2 Enrollment Process and Responsibilities

XSEDE Allocations staff serve as registration authorities for both the NCSA SLCS and the PSC MyProxy CA. They enroll users in the XSEDE Central Database (XDCDB) according to the following enrollment process:

To receive an entry in the XDCDB, a user must satisfy one of the following conditions:

- Be an XSEDE staff member authorized for access in an XSEDE project allocation.
- Be an XSEDE project Principal Investigator (PI) with an allocation on XSEDE computational resources approved through a U.S. National Science Foundation (NSF)-approved peer review process.
- Have an XSEDE project account requested on their behalf by an existing XSEDE project PI using that PI's XSEDE project allocation.

Identity vetting of XSEDE staff members is performed in person as part of the hiring process at XSEDE service provider sites.

XSEDE is funded by the U.S. National Science Foundation (NSF). Identity vetting for PIs is performed via peer review. PIs submit proposals for XSEDE allocations to the XSEDE Resource Allocations Committee (XRAC), which evaluates applications according to specific criteria. The application process is described at https://www.xsede.org/for-users/getting-started/. XSEDE allocations information and policies are described at https://portal.xsede.org/allocations/policies.

XSEDE project allocations are awarded to PIs in terms of service units to be spent on specific XSEDE resources matched to the needs identified in their proposals. Allocations are typically awarded for one year. PIs can submit renewal or supplemental proposals to the XRAC to extend their allocation.

PIs are required by policy not to share their XSEDE accounts with others. Instead, they use the Add User Form on the XSEDE User Portal to request accounts for their project members. PIs can also use this form to remove project members. Access to this form requires authentication via Kerberos username and password. Additional Multi-factor authentication may also be required. PIs submit name, telephone, and address information for the users on their project. For users on multiple projects, each project PI must complete the required information separately for each user to request the user to have access to that PI's allocated project resources. The PI is notified by e-mail whenever a user is added to their project.

All XSEDE users are required to sign and return a copy of the XSEDE Acceptable Use Policy, acknowledging their acceptance of XSEDE user policy requirements. The XSEDE User Responsibility Form educates users about secure and appropriate computing practices, and specifies XSEDE user responsibilities. The XSEDE Acceptable User Policy is described at https://www.xsede.org/ecosystem/operations/usagepolicy.

When a user no longer has any active XSEDE projects, the user's Kerberos principal may be disabled. Users' Kerberos principals may also be disabled for inactivity. Disabled Kerberos principals are not reassigned to other users. Inactive XDCDB user records are kept indefinitely for regulatory reporting purposes and to prevent reassignment to different users.

New XSEDE users' initial TERAGRID.ORG Kerberos passwords are set using the XSEDE User Portal password reset webpage at https://portal.xsede.org/login/reset-password. Users must correctly identify their TERAGRID.ORG principal name and the e-mail address associated with their account to receive instructions and a unique link for password reset. Users may also enroll in XSEDE's multifactor authentication service for additional account protection.

New TERAGRID.ORG principals that do not have their initial passwords changed within 30 days are automatically disabled. Users whose accounts have been disabled must contact the XSEDE Help Desk to have their TERAGRID.ORG principal reinstated.

XSEDE users can reset their password via the XSEDE User Portal password reset webpage, which authenticates the request via e-mail to the user's registered e-mail address.

Each user is assigned a unique username used as their Kerberos principal as described in 3.1.5.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

PSC MyProxy CA services authenticate certificate requests as described in Section 3.2.3.

4.2.2 Approval or Rejection of Certificate Applications

Certificate requests submitted by XSEDE users who have successfully authenticated via Kerberos will be approved.

4.2.3 Time to Process Certificate Applications

Certificate applications are processed automatically. Approved applications result in automatic certificate issuance. Non-approved applications are automatically rejected. All certificate application attempts are logged.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Authenticated certificate requests submitted to the PSC MyProxy CA are logged, signed by the PSC MyProxy CA and returned. Upon failed authentication of the subscriber or failed validation of a certificate request, the failed attempt is logged and an error is returned.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Users are notified automatically of certificate delivery by the MyProxy client software they use to submit the certificate request to the PSC MyProxy CA.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Subscribers accept responsibility for delivered certificates, and accept certificates upon receipt.

4.4.2 Publication of the Certificate by the CA

End entity certificates are not published.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No notifications of certificate issuance to other entities will be made.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers must safeguard the private key corresponding to certificates issued to them by the PSC MyProxy CA against compromise, exposure to access by others, and unintended disclosure.

Subscribers must:

- Not make copies of private keys.
- Not share private keys with others.
- Not transmit private keys between systems or storage.
- Not store private keys in areas accessible to others, including networked filesystems.
- Operate MyProxy client software safely to prevent disclosure of private keys that are generated. This includes using appropriate environment variables and client parameters with arguments to direct the client software to write private keys to private file storage area, with access controls set to permit only the subscriber to access the file containing the private key.
- Observe restrictions on private key and certificate use.
- Immediately notify PSC regarding any event in which the private key may have been exposed to others.

These responsibilities are explained to subscribers in this Policy and in the XSEDE Acceptable Use Policy that they are required to read and affirm with a personally signed acknowledgement form returned via postal mail to the registration authority.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties should:

- Observe and remain up to date regarding the provisions detailed in this Policy.
- Verify all certificate signatures in the signature chain.
- Verify self-signed CA certificates (e.g. PSC MyProxy CA) to their own satisfaction by out-of-band means.
- Obtain and check current CRLs for all CAs in the signature chain before accepting a certificate.

- Observe restrictions on private key and certificate use.
- Not assume authorization of an end entity for any purpose based on possession of a certificate issued by the PSC MyProxy CA or its corresponding private key.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

The PSC MyProxy CA certificate will be renewed if operation of the CA is supported beyond the current expiration date/time of the certificate, and the current date is within one month of the expiration date/time of the certificate.

End-entity certificates issued by the PSC MyProxy CA are not renewed. Subscribers must generate a new key and request a new certificate as described in section 3.2.3.

4.6.2 Who May Request Renewal

Renewal of the PSC MyProxy CA certificate may be requested by the PSC Information Security Officer.

No-one may request renewal of an end-entity certificate issued by the PSC MyProxy CA.

4.6.3 Processing Certificate Renewal Requests

Renewal for the PSC MyProxy CA certificate will be processed as specified by PSC security procedures by authorized PSC security personnel designated by the PSC Information Security Officer.

Certificate renewal requests for end-entity certificates issued by the PSC MyProxy CA are not processed.

4.6.4 Notification of New Certificate Issuance to Subscriber

Subscribers requesting a new certificate are notified as described in Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not Applicable for end-entity certificates. Relying parties accept a renewed PSC MyProxy CA certificate by downloading it from the CA repository specified in section 2.1.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable for end-entity certificates. A renewed certificate for the PSC MyProxy CA will be published to the CA repository specified in section 2.1.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable for end-entity certificates. No notification of certificiate renewal will be made beyond notes published on the CA repository website specified in section 2.1.

4.7 Certificate Re-Key

The PSC MyProxy CA certificate will not be re-keyed.

End-entity certificates issued by the PSC MyProxy CA will not re-keyed. Subscribers must generate a new key and request a new certificate as described in section 3.2.3.

4.7.1 Circumstances for Certificate Re-key

None.

4.7.2 Who May Request Certification of a New Public Key

No-one.

4.7.3 Processing Certificate Re-Keying Requests

Certificate re-keying requests are not processed.

4.7.4 Notification of New Certificate Issuance to Subscriber

Subscribers requesting a new certificate are notified as described in Section 4.3.2.

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

See Section 4.4.3.

4.8 Certificate Modification

Certificates issued by the PSC MyProxy CA will not be modified.

4.8.1 Circumstances for Certificate Modification

None.

4.8.2 Who May Request Certificate Modification

No-one.

4.8.3 Processing Certificate Modification Requests

Certificate modification requests are not processed.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of a 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

Certificates issued by the PSC MyProxy CA will be revoked in any of the following circumstances:

- The private key is suspected or reported to be lost or exposed.
- The information in the certificate is believed to be, or has become inaccurate.
- The certificate is reported to be no longer needed, e g., as requested by the subscriber.
- Traceability of a certificate to the subscriber is lost, i.e., PSC is unable to contact the user based on data associated with the user in the XDCDB. In this event, the user's TERAGRID.ORG user principal will also be disabled via XSEDE security procedures. Disabling the user's TERAGRID.ORG user principal will prevent further attempts to obtain certificates issued by the PSC MyProxy CA.

4.9.2 Who can Request Revocation

PSC Information Security Operations personnel may request revocation of any certificate issued by the PSC MyProxy CA.

The original subscriber for a certificate may request its revocation.

Entities other than the subscriber who suspect that the private key associated with a certificate issued by the PSC PKI may be compromised should contact PSC Information Security Operations via the PSC Hotline at +1 (412) 268-6350 or via e-mail at security@psc.edu.

4.9.3 Procedure for Revocation Request

Requests for revocation should be made by email to ca-admin@psc.edu or security@psc.edu, or by phone to the PSC Hotline at +1 (412) 268-6350. Requests will be authenticated as described in Section 3.4.

Authorized PSC security personnel designated by the PSC Information Security Officer will process certificate revocations as specified in PSC security procedures.

4.9.4 Revocation Request Grace Period

No constraints.

4.9.5 Time Within which CA Must Process the Revocation Request

Revocation requests will be processed within one working day of the request being received.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying parties are advised to obtain and consult a valid CRL from http://ca.psc.edu/psc-myproxy-ca/

4.9.7 CRL Issuance Frequency (if applicable)

A new CRL for the PSC MyProxy CA will be issued daily and whenever a certificate issued by it is revoked.

4.9.8 Maximum Latency for CRLs (if applicable)

The maximum latency between the generation of CRLs for the PSC MyProxy CA and posting of the CRLs to the repository at http://ca.psc.edu/psc-myproxy-ca/ will be one day.

4.9.9 On-Line Revocation/Status Checking Availability

Other than the published CRL, no on-line certificate status checking is available.

4.9.10 On-Line Revocation Checking Requirements

None.

4.9.11 Other Forms of Revocation Advertisements Available

None.

4.9.12 Special Requirements Re-Key Compromise

None.

4.9.13 Circumstances for Suspension

Certificates issued by the PSC MyProxy CA will not suspended. Any circumstances warranting suspension of a certificate will be processed as a revocation request and processed as described in section 4.9.3.

4.9.14 Who can Request Suspension

No-one.

4.9.15 Procedure for Suspension Request

Suspensions are processed as certificate revocation requests. Revoked certificates will not be reinstated. Subscribers must generate a new key and request certificates as described in section 3.2.3.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

Other than the published CRL, no on-line certificate status checking is available.

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

No stipulation.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

Subscribers may end their subscription by requesting revocation of any remaining, valid certificates and retirement of their TERAGRID.ORG Kerberos user principal.

4.12 Key Escrow and Recovery

No key escrow is performed.

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Site Location and Construction

The PSC MyProxy CA hardware is located in the PSC HPC machine room at 4350 Northern Pike in Monroeville, PA 15146, U.S.A.

5.1.2 Physical Access

Access to the PSC machine room at WEC is strictly limited to authorized PSC personnel, WEC site security officers, and authorized PSC HPC systems vendor contractors. Entry to the WEC PSC machine room requires two-factor authentication via Photo-ID keycard and corresponding PIN entry, unique to each authorized individual. All entries to and departures from the PSC WEC machine room are logged by on-site security. The PSC machine room is monitored 24x7 by on-site security officers via video surveillance and frequent building patrols. Patrol routes and progress are logged with station check-ins.

The PSC machine room facilty is not open to the general public. Entry to the building requires a photo-ID keycard or pre-authorized visitor pass that must be presented upon entry to and exit from the building at every entrance. The main entrance is staffed by on-site security 24x7. On-security personnel staff the delivery entrance/loading dock during business hours. All doors except the main entrance are locked during non-business hours and require keycard/PIN for entry. All entrances are monitored with video surveillance. All entries and departures are logged.

5.1.3 Power and Air Conditioning

Power to the PSC machine room is supplied via two independent feeds from regional electric utilities. On-site commercial UPS facilities and backup diesel generators assure power to all critical systems. Power delivery systems are continuously monitored and logged, with support for event reporting via telephone paging.

Industrial air conditioning systems within the PSC machine room assure continuous temperature and humidity regulation. Air conditioning systems are continuously monitored and logged, with support for event reporting via telephone paging.

5.1.4 Water Exposures

The PSC machine room facility is physically located on a hill and is not exposed to environmental flood risk. Monitoring infrastructure built into the PSC machine room automatically alerts on-site security to water risks detected in the machine room.

5.1.5 Fire Prevention and Protection

Standard industrial fire detection, alarms and suppression facilities protect the PSC machine room facility. The PSC machine room has industry-standard fire detection, alarms and suppression systems appropriate to large-scale HPC computing facilities.

5.1.6 Media Storage

Media containing sensitive information are stored in the PSC security physical safes in the secured PSC machine room area and at the PSC main offices.

5.1.7 Waste Disposal

Custodial staff servicing the PSC machine room are specifically authorized for entry to the facility and are monitored during performance of their duties.

5.1.8 Off-Site Backup

Audit logs are archived automatically to a secondary storage facility in the PSC main office building at 300 South Craig Street in Pittsburgh, PA. The PSC main office building is located 11 miles from the PSC machine room facility at 4350 Northern Pike in Monroeville, PA, where the PSC MyProxy CA hardware is located.

5.2 Procedural Controls

All persons with access to the systems hosting the PSC MyProxy CA will be full-time PSC employees. Personnel will be PSC Operations staff, PSC Security Operations staff, and PSC Systems Administration staff.

When any person with access to the PSC MyProxy CA systems leaves PSC or their administrative role, their access will be revoked and any relevant passwords and access control keys changed.

PSC will perform an operational audit of the CA staff at least once per year. A list of CA and site identity management personnel will be maintained and verified at least once per year.

5.2.1 Trusted Roles

The PSC Information Security Officer is designated responsibility and authority for managing procedural controls associated with the PSC MyProxy CA.

5.2.2 Number of Persons Required per Task

Individual PSC security personnel may perform assigned duties independently. However, at least two authorized PSC security personnel must have the knowledge, skills, access to necessary controls and means to administer the PSC MyProxy CA.

5.2.3 Identification and Authentication for Each Role

Roles are designated and authorized to PSC security personnel directly by the PSC Information Security Officer.

5.2.4 Roles Requiring Separation of Duties

No stipulation.

5.3 Personnel Controls

Operators of the PSC MyProxy CA will be qualified, authorized, full-time PSC security staff system administrators, working under the direction of the PSC Information Security Officer.

5.3.1 Qualifications, Experience, and Clearance Requirements

PSC Information Security staff include members holding industry-standard security certifications, as well as significant experience in deploying, operating, administering and monitoring security technologies and procedures. PSC Information Security staff are also experienced in security incident handling and response. PSC Information Security staff participate in the XSEDE security working group and incident response teams, as well as Grid-SEC and REN-ISAC.

PSC staff requiring access to classified materials maintain clearances necessary for such access.

5.3.2 Background Check Procedures

Background checks of PSC personnel are performed by Carnegie Mellon University Human Resources and official clearance-granting agencies as needed upon employment and changes in employment status.

5.3.3 Training Requirements

The PSC Information Security Officer maintains training requirements for PSC security staff. PSC personnel authorized to perform PSC CA administrative tasks will be trained as needed to perform their duties correctly as specified by PSC policies and procedures.

5.3.4 Retraining Frequency and Requirements

PSC conducts mandatory, annual training seminars regarding security policies and procedures for all PSC personnel. PSC security personnel authorized to perform PSC CA administration are retrained as needed under the direction of the PSC Information Security Officer.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Unauthorized actions may result in disciplinary action and criminal prosecution.

5.3.7 Independent Contractor Requirements

Independent contractors are not authorized to access PSC PKI infrastructure. All PSC PKI administrative roles and responsibilities are assigned to authorized, full-time PSC personnel.

5.3.8 Documentation Supplied to Personnel

Documentation regarding PSC policies and procedures for appropriate use of PSC PKI client interfaces are made available to all PSC personnel. Documentation regarding PSC policies and procedures for secure administration of PSC PKI systems and data are provided to authorized PSC security personnel.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

The following items will be logged and archived:

- System and software service events
- Login / Logout
- MyProxy service logs, including
- IP address of host from which a certificate request was initiated
- client user TERAGRID.ORG user principal and authentication results
- certificate request arguments (public key hash, certificate lifetime)
- issued certificate DN, lifetime, and serial number
- Certificate requests
- Certificate issuance
- Certificate revocations
- Issued CRLs
- Attempted and successful accesses to the systems hosting the PSC MyProxy CA, and reboots of those systems

The XSEDE Central Database (XDCDB) maintains contact information for all subscribers. Traceability of issued certificates to end users is established by examination of certificates, search for matching records in the MyProxy service logs, and queries to the XDCDB as needed to retrieve detailed user contact information.

5.4.2 Frequency of Processing Log

Logs are updated continuously on both local systems and site loghosts. Logs are rotated and archived daily.

5.4.3 Retention Period for Audit Log

Audit logs are archived for a minimum of three years.

5.4.4 Protection of Audit Log

Events are recorded in real-time via syslog to the local system and to PSC's central syslog collector service, which provides an independent, protected log collection point that is physically and logically separated from CA systems. Access to the syslog collector service is restricted to PSC information security operations staff.

5.4.5 Audit Log Backup Procedures

See section 5.1.8.

5.4.6 Audit Collection System (Internal vs. External)

Audit logs are stored on the local system, on PSC's central syslog collector service, and in off-site backups (see Section 5.1.8). In all cases the logs are maintained internally on PSC systems, under the supervision of PSC security staff, in PSC-controlled facilities.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

PSC Information Security infrastructure includes automated, active probing systems designed to identify vulnerabilities in all PSC hosts. Results are reported directly to the PSC Information Security Officer and PSC security staff assigned to intrusion prevention and response responsibilities. Vulnerability probe results are reviewed immediately in the case of high-risk vulnerabilities, and at least weekly for all vulnerability probe results.

5.5 Records Archival

5.5.1 Types of Records Archived

System logs record all system and software service events, including login/logout/reboot of the issuing machine. The PSC MyProxy CA records and archives all requests for certificates, all issued certificates, all revocation requests, and all issued CRLs.

5.5.2 Retention Period for Archive

Records will be kept for at least 3 years.

5.5.3 Protection of Archive

Access controls for archived files restrict access to authorized PSC security staff.

5.5.4 Archive Backup Procedures

Automated backup procedures transfer archive logs to PSC's production hierarchical storage management (HSM) system on a daily schedule.

5.5.5 Requirements for Time-Stamping of Records

All PSC production systems synchronize time via secured Network Time Protocol (NTP) services. Log records are time-stamped accordingly within log files. Original (last modification) time-stamps for log files are retained in archived copies.

5.5.6 Archive Collection System (Internal or External)

The archive collection system is internal to PSC.

5.5.7 Procedures to Obtain and Verify Archive Information

Authorized PSC security staff retrieve copies of archived logs from site loghosts using standard file transfer clients. All file transfers require successful user authentication and file access permissions, and are logged.

5.6 Key Changeover

Best effort will be made to notify relying parties of any key changes for the PSC MyProxy CA. Unless a security event requires immediate revocation and replacement of the PSC MyProxy CA key, an overlap in the availability of the old and new CA key and certificates will be at least as long as the maximum lifetime for a user-issued short-lived certificate from the PSC MyProxy CA.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

PSC Information Security Operations staff will handle all security incidents as they deem appropriate, in consultation with XSEDE security incident handling and response personnel.

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

The PSC MyProxy CA implementation and operations are designed to provide continuity of operation through scheduled maintenance periods and through failures of hardware, software or storage resources. Under normal conditions, data backup and system restoration procedures are designed to permit failed/corrupted systems to be reconstituted within one business day.

5.7.3 Entity Private Key Compromise Procedures

Any private key compromise will result in immediate revocation of the associated certificate and publication of an updated CRL. The associated subscriber's TERAGRID.ORG Kerberos user principal will also be immediately disabled via XSEDE security procedures.

5.7.4 Business Continuity Capabilities after a Disaster

PSC maintains a disaster recovery and business continuity plan with specific procedures for handling essential and security-sensitive functions. PSC maintains secure, geographically separated production computing facilities to which essential and security-sensitive functions may be securely relocated in the event of a disaster.

5.8 CA or RA Termination

Upon termination, the PSC Information Security Officer will direct authorized PSC security and administrative staff to conduct PSC's secure retirement procedure for all systems, software and data resources associated with the CA.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The PSC MyProxy CA does not generate any private keys except its own.

Subscriber private keys will be generated by MyProxy client software, operated by the subscriber. As described in section 4.5.1, subscribers must operate MyProxy client software in a manner that protects generated keys against disclosure. Selection of storage location and file system access controls must be applied appropriately to protect the stored private key against disclosure.

6.1.2 Private Key Delivery to Subscriber

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys are delivered directly to the MyProxy service by the MyProxy client with Kerberos authentication and integrity protection.

6.1.4 CA Public Key Delivery to Relying Parties

The public key of the PSC MyProxy CA will be available at http://ca.psc.edu/psc-myproxy-ca/ in addition to distribution points of accrediting PMAs.

6.1.5 Key Sizes

The CA private key is 2048 bits in length. Public RSA keys shorter than 2048 bits will not be signed.

6.1.6 Public Key Parameters Generation and Quality Checking

No stipulation.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

The PSC MyProxy CA does not enforce key usage restrictions by any means beyond the X.509v3 extensions in the certificates it issues. The certificate extensions are specified in Section 7.1.2.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The PSC MyProxy CA uses FIPS 140 level 3 Hardware Security Modules for storage of its private key.

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

No stipulation.

6.2.3 Private Key Escrow

PSC MyProxy CA private keys are not escrowed.

6.2.4 Private Key Backup

The PSC MyProxy CA private key is replicated on two identical cryptographic modules on two separate but identical hosts in the PSC machine room to provide for failure protection. The replication procedure requires import of the private key from encrypted media into each cryptographic module. Once on the cryptographic modules, the private key is not exportable in any form. The private key on encrypted media is retained in the PSC Security safe after import has been completed (See Section 6.2.5). If a system hosting one CA should fail, the other system takes over CA operations automatically until the other can be rebuilt or replaced.

6.2.5 Private Key Archival

PSC MyProxy CA private keys are not archived, except on the single original encrypted media retained in the PSC Security safe. Only authorized PSC Security staff have access to this safe, and each authorized staff member uses their own PIN to enter the safe. All safe entries are logged.

6.2.6 Private Key Transfer into or from a Cryptographic Module

PSC MyProxy CA private keys will initially be replicated on two identical cryptographic storage modules in a secure manner. After that point they are not exportable from the cryptographic modules. The private key is never stored nor exported in plain text form.

6.2.7 Private Key Storage on Cryptographic Module

The PSC MyProxy CA private key is stored on cryptographic modules meeting FIPS 140 level 3, operated in FIPS 140 level 2 mode.

6.2.8 Method of Activating Private Key

The private key is activated automatically at CA startup to allow immediate PSC MyProxy CA operation.

6.2.9 Method of Deactivating Private Key

HSM utilities on the server support deactivation of the PSC MyProxy CA private key.

6.2.10 Method of Destroying Private Key

The HSM Security Officer can reinitialize the HSM to destroy the private key.

6.2.11 Cryptographic Module Rating

The hardware security modules meet FIPS 140 level 3.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

No stipulation.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The certificate for the PSC MyProxy CA will have a lifetime of up to 10 years.

PSC MyProxy CA-issued end-entity certificates will have a lifetime of not more than 168 hours (1 week).

6.4 Activation Data

The PSC MyProxy CA private key is activated automatically at CA startup time.

6.4.1 Activation Data Generation and Installation

Activation data is generated using the operator interface of the cryptographic module and stored on the local CA server filesystem.

6.4.2 Activation Data Protection

Activation data is readable only by the root account on the local CA server filesystem.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

The PSC MyProxy CA software runs on dedicated hosts, running only the MyProxy CA service software and the minimum essential operating system services required to support and secure the MyProxy CA service. No other services are enabled.

The PSC MyProxy CA hosts are physically secured in a locked security rack located in PSC's production HPC computing facility. Only authorized PSC Security staff have access to the physical safe containing the keys required to open the locked security rack.

The PSC MyProxy CA servers' network is protected by a dedicated hardware firewall. The servers also run an operating system firewall to further restrict access behind the network firewall. The servers are monitored via both host-based and network-based intrusion detection systems. Login access requires multi-factor authentication. Access is permitted only for PSC Security administrative personnel authorized to access the system for its operation and maintenance.

Kerberos Key Distribution Center (KDC) servers operated at PSC for Kerberos user authentication services are similarly secured and also located in the locked security rack. All servers are monitored via both host-based and network-based intrusion detection systems, and login access requires multi-factor authentication.

6.5.1 Specific Computer Security Technical Requirements

No stipulation.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

No stipulation.

6.6.2 Security Management Controls

PSC uses regression testing methods to verify correct operation and security of systems following updates to operating systems, service software, and configuration changes. PSC also operates automated vulnerability probing and detection infrastructure to detect and alert PSC security personnel to system and service vulnerabilities. See Section 5.4.8.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

Network security controls (software and hardware firewalls) allow inbound connections only for certificate requests and download of CA certificates and CRLs from hosts outside PSC's network.

6.8 Time-Stamping

All PSC production systems synchronize time via secured Network Time Protocol (NTP) services. Log records are time-stamped accordingly within log files. Original (last modification) time-stamps for log files are retained in archived copies.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

End-entity certificates will be X509v3, compliant with RFC 5280.

7.1.1 Version Number(s)

The version number will have a value of 0x2 indicating a Version 3 certificate.

7.1.2 Certificate Extensions

For the CA certificate:

- X509v3 Basic Constraints: critical
  - CA:TRUE
- X509v3 Key Usage: critical
  - Certificate Sign, CRL Sign
- X509v3 Subject Key Identifier
  - 23:92:D8:E7:79:6C:35:52:5F:50:12:17:09:B9:20:9B:F2:97:63:08
- X509v3 Subject Alternative Name
  - email:ca-admin@psc.edu
- X509v3 Authority Key Identifier
  - Keyid:23:92:D8:E7:79:6C:35:52:5F:50:12:17:09:B9:20:9B:F2:97:63:08

For user certificates:

- X509v3 Basic Constraints: critical
  - CA:FALSE
- X509v3 Key Usage: critical
  - Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
- X509v3 Subject Key Identifier
- X509v3 Authority Key Identifier
- X509v3 Certificate Policies:
  - Policy: 1.3.6.1.4.1.26703.99.7512.1.1.1 (This Policy)
  - Policy: 1.2.840.113612.5.2.2.3 (Short-Lived Credential Services)
  - Policy: 1.2.840.113612.5.2.3.2.1 (Identity Vetting by a Trusted Third Party)
- X509v3 CRL Distribution Points:
  - URI:http://ca.psc.edu/psc-myproxy-ca/crl/4b2783ac.crl (PSC MyProxy CA CRL, DER)

7.1.3 Algorithm Object Identifiers

- Hash Function: id-sha1 1.3.14.3.2.26
- RSA Encryption: rsaEncryption 1.2.840.113549.1.1.1
- Signature Algorithm: sha1WithRSAEncryption 1.2.840.113549.1.1.5

7.1.4 Name Forms

All certificates will have the following name form:

C=US, O=Pittsburgh Supercomputing Center, CN=*user name*

Where:

user name is a unique proper name for the subscriber, which may have appended digits to disambiguate.

7.1.5 Name Constraints

All certificates issued by the PSC PKI will have names with the following prefix:

“C=US, O=Pittsburgh Supercomputing Center”

7.1.6 Certificate Policy Object Identifier

1.3.6.1.4.1.26703.99.7512.1.1.1

{ iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) Pittsburgh Supercomputing Center(26703) CA(99) MyProxy CA(7512) SLCS(1) CP/CPS(1) Major Revision(1) }

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

7.2.1 Version Number(s)

The version number will be 0x1 indicating a version 2 CRL.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

7.3 OCSP Profile

OCSP is not supported.

7.3.1 Version Number(s)

No stipulation.

7.3.2 OCSP Extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

PSC MyProxy CA may be audited by other IGTF accredited CAs to verify compliance with the rules and procedures specified in this document. PSC MyProxy CA audit records will be made available to external auditors in the course of their work as auditor

As an XSEDE Service Provider (SP), PSC participates in the highest levels of management within XSEDE, and will continue to do so for the lifetime of the PSC MyProxy CA. PSC has authority to request applicable audit data from XSEDE partner sites (e.g., NCSA) to ensure the integrity of PSC MyProxy CA operations and to support external auditors in the course of their work as auditor. Examples include Registration Authority records and Kerberos KDC configuration files and event logs.

8.1 Frequency or Circumstances of Assessment

No stipulation.

8.2 Identity/Qualifications of Assessor

No stipulation.

8.3 Assessor's Relationship to Assessed Entity

No stipulation.

8.4 Topics Covered by Assessment

No stipulation.

8.5 Actions Taken as a Result of Deficiency

No stipulation.

8.6 Communication of Results

Audit results will be made available to TAGPMA upon request.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

No fees are assessed nor refunds given to subscribers or relying parties by the PSC MyProxy CA.

9.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

No stipulation.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

No financial responsibility is accepted.

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

None.

9.3 Confidentiality of Business Information

The XSEDE Acceptable Use Form (See Section 4.1.2), which all XSEDE users (and thereby potential PSC MyProxy CA subscribers) must read and acknowledge receipt of, defines expectations and responsibilities regarding the handling of sensitive data by XSEDE Resource Providers (including PSC) and by XSEDE Users. The PSC MyProxy CA adheres to these expectations and responsibilities accordingly. No further stipulations are made.

9.3.1 Scope of Confidential Information

No stipulation.

9.3.2 Information Not Within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

No stipulation.

9.4 Privacy of Personal Information

Operations of the PSC MyProxy CA are publicly funded. The limited personal information necessarily gathered for PSC MyProxy CA operations is not private, and must be reported to authorized government funding agencies as required. PSC does not otherwise distribute or share user information.

9.4.1 Privacy Plan

No stipulation.

9.4.2 Information Treated as Private

No stipulation.

9.4.3 Information not Deemed Private

No stipulation.

9.4.4 Responsibility to Protect Private Information

No stipulation.

9.4.5 Notice and Consent to use Private Information

No stipulation.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

No stipulation.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

The PSC MyProxy CA asserts no ownership rights in certificates issued to subscribers.

9.6 Representations and Warranties

The PSC MyProxy CA and its agents make no guarantee about the security or suitability of a service or end-entity that is identified by a PSC certificate. The PSC MyProxy CA is run with a reasonable level of security, but it is provided on a best effort only basis. PSC does not warrant its procedures and will take no responsibility for problems arising from its operation, or for the use made of the certificates it provides.

9.6.1 CA Representations and Warranties

None.

9.6.2 RA Representations and Warranties

None.

9.6.3 Subscriber Representations and Warranties

No stipulation.

9.6.4 Relying Party Representations and Warranties

No stipulation.

9.6.5 Representations and Warranties of other Participants

No stipulation.

9.7 Disclaimers of Warranties

The PSC MyProxy CA denies any financial or any other kind of responsibility for damages or impairments resulting from its operation.

9.8 Limitations of Liability

The PSC MyProxy CA is operated substantially in accordance with PSC's own risk analysis. No liability, explicit or implicit, is accepted.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

This policy becomes effective upon publication to http://ca.psc.edu/psc-myproxy-ca/

9.10.2 Termination

This Policy may be terminated at any time and without prior notice.

9.10.3 Effect of Termination and Survival

No stipulation.

9.11 Individual Notices and Communications with Participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

Major changes to this document will be presented to TAGPMA for approval prior to taking effect.

Approved changes will go into effect upon publication to http://ca.psc.edu/psc-myproxy-ca/

9.12.2 Notification Mechanism and Period

Announcements regarding amendments to this Policy will be posted at http://ca.psc.edu/psc-myproxy-ca/

9.12.3 Circumstances Under Which OID Must be Changed

Any substantial changes to this Policy will incur a change in OID.

9.13 Dispute Resolution Provisions

PSC Information Security Operations will resolve all disputes regarding this Policy.

9.14 Governing Law

Interpretation of this policy is according to the laws of the United States of America and the State of Pennsylvania, where the conforming CA is established.

9.15 Compliance with Applicable Law

No stipulation.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

No stipulation.

10. REFERENCES

Certificate Policy and Practice Statement for the NCSA SLCS, National Center for Supercomputing Applications (NCSA) Version 1.4 (Mon Sep 28 16:27:57 CDT 2009)

IGTF Classic Profile: Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure Version v5.0 (rev 20160510)
https://www.igtf.net/ap/classic/IGTF-AP-classic-5-0.pdf

IGTF One Statement Certificate Policies: Policy on Vetting Identity by a Trusted Third Party
https://www.eugridpma.org/guidelines/1scp/1SCP-vetting-ttp-0.1.pdf

IGTF Short-Lived Credential Service Profile: Authentication Profile for SLCS X.509 Public Key Certification Authorities with secured infrastructure Version v3.0 (rev 20151001)
https://www.igtf.net/ap/slcs/IGTF-AP-SLCS-3.0.pdf

Interoperable Certificate Profile. Open Grid Forum GFD.225, July 2016.
https://www.ogf.org/documents/GFD.225.pdf

FBCA CP: X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), Version 1.0, 18 December 1999
http://www.cio.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf

Garman, J. (2003). **Kerberos: The Definitive Guide**. Sebastopol, CA: O'Reilly & Associates.

MyProxy Credential Management Service: Online credential repository and/or certificate authority developed and maintained at the National Center for Supercomputing Applications (NCSA), Version 5.1, 9 March 2010.
©2000-2010 Board of Trustees of the University of Illinois.
http://grid.ncsa.illinois.edu/myproxy/
MyProxy Certificate Authority details at
http://grid.ncsa.illinois.edu/myproxy/ca/

PKI Assessment Guide: PKI Assessment Guidelines (PAG)
http://www.abanet.org/scitech/ec/isc/pag/pag.html

RFC 3647: S. Chokani and W. Ford, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, RFC 3647, November 2003 [replaces RFC 2527]
http://www.ietf.org/rfc/rfc3647.txt

XSEDE Acceptable Use Policy (AUP): Defines user responsibilities regarding use of XSEDE resources and safekeeping of authentication credentials issued.
https://www.xsede.org/ecosystem/operations/usagepolicy

Webtrust for CAs Assessment Guidelines: AICPA/CICA WebTrust Program for Certification Authorities, Version 1.0, 25 August 2000
http://www.webtrust.org/certauth_fin.htm

11. REVISION HISTORY

This section captures the revision history for the Certificate Policy and Practice Statements of the PSC MyProxy CA.

1.0 Presented at TAGPMA face-to-face meeting at Summit 09 (Banff, Canada), 16-Oct-2009.

1.1 Revised for elaboration and clarification in response to TAGPMA review, 30-Mar-2010.

1.2 Updated Figure 1, and including minor edits and corrections, 6-Apr-2010.

1.3 Corrections and additions in response to TAGPMA review call, 7-Apr-2010.

1.4 Updated Figure 1 and descriptive text to reflect move to self-signed PSC MyProxy CA certificate, 7-Apr-2010.

1.5 Corrections and additions in response to TAGPMA review comments, 10-Apr-2010.

1.6 Corrections in response to TAGPMA review comments, 12-Apr-2010.

1.7 Updates reflecting change in PSC MyProxy CA website URL, and terminology associated with its registration authority organization (TeraGrid -> XSEDE), 08-Dec-2020.

1.8 Removed CRL URLs from CA certificate extensions and PEM CRL URL from user certificate extensions as advised in review comments, 09-Dec-2020.