June 2018

TABLE OF CONTENTS

1. Agreement Sign off

I, as part of the TechCARE Agreement, have read the below documentation and been informed about the content, requirements, and expectations of the agreement. I have received a copy of the agreement and agree to abide by the guidelines as a condition of my engagement with AUB.

Policy Name: _____

Institution Representative Signature: _____

Representative Printed Name: _____

Receipt By: _____

Date: _____

2. Purpose

A digital certificate is a type of signature which identifies a server,a website or a document to verify its publisher.

The purpose of this agreement is to identify the appropriate use of digital certificates provided through the TechCARE Digital Certificate Service, and to describe the Service Level Agreement (SLA) between AUB IT and other institutions who are part of the TechCARE agreement.

3. Definitions

SSL (Secure Sockets Layer) is the protocol that creates a secure, encrypted connection between two parties and ensures integrity of data in transit.

HTTPS: A combination of the Hypertext Transfer Protocol (HTTP) with the SSL/TLS protocol to provide encryption and secure identification of the server.

Private Key Management: SSL certificates have a key pair, a public and a private key. These keys work together to establish the encrypted connection

Certificate Authority (CA): Digital certificates depend on trust and are issued by certificate authorities. The CA assure the user that the certificates they provide are valid and reliable. DigiCert is the current CA used by the TechCARE Digital Certiciate Service

Certificate Signing Request (CSR): The Certificate Signing Request is a block of encoded text that is given to a Certificate Authority when applying for an SSL Certificate. It is generated on the server where the certificate will be installed and contains information that will be included in the certificate such as the organization name, common name (domain name), location, and country.

4. Service Description & SLA

GÉANT, with whom TechCARE is a partner, chooses DigiCert as its official Certification Authority, which entitles TechCARE members to unlimited number of digital certificates (currently SSL/X.509, and email certificates only).

4.1 Service Cost

The cost of this service are included as part of the Base Services charge in the TechCARE agreement.

4.2 How to request DigiCert-AUB account

The requester, representing the TechCARE member institution, requests AUB-DigiCert account by sending an email to certificate.requester@aub.edu.lb. Refer to the "SSL digital Certificate SOP" document for required details.).

Commented [SEH1]: Romy is confirming this

4.3 Service Assumption

i. Details of this service and its related information is clearly documented in the AUB IT Service Catalog (xxxxxx) . The service catalog is continually updated to provide the latest service information regarding details of the offering, how to request services, how to get help for services.
ii. Outages to this service are communicated and documented to all stakeholders via emails to the registered representative.
iii. Services are provided in adherence to digital certificate agreement.

Commented [SEH2]: Romy is working on this with omar

4.4 . Responsibilities

4.1 AUB IT general responsibilities

AUB IT will be responsible for the liaison with cloud PKI infrastructure provider, processes and monitoring tools necessary for the Digital Certificate Service and to:

- Document the service in the AUB IT service catalog
- Meet response times associated with this SLA as documented below
- Maintaining the certificate subscription with GEANT.
- Act as liaison between certificate custodian and certificate authority
- Manage the certificate portal configuration
- Create accounts and divisions and reset passwords for certificate custodians' accounts (in case of reset action problem)
- Provide technical assistance related to the certificate service
- Perform an annual audit and validation of custodians' certificate accounts
- Train the certificate custodians when needed

4.2 TechCARE Member Institution Responsibilities

- Every institution must assign a certificate custodian who has administrative control over ordering, approving, renewing, and revoking their institution/group/department's certificates and creating new users in their division.

- Once assigned, the certificate custodian must inform AUB IT in order to create an institution account for the certificate custodian.
- The certificate custodian send all requests for additions or changes to the service to certificate.requester@aub.edu.lb
- The certificate custodian should attend any required training
- The institution is responsible to ensure that the issued certificates are utilized according to the

4.5 Hours of Coverage

4.5.1 Hours of Coverage

AUB will respond to requests within during business hours from Monday through Friday from 8 AM to 5 PM excluding AUB holidays (refer to AUB calendar).

4.5.2 Response Time

Certificates are issued within 3-5 business days from the time of submission of a completed request.

5. Acceptable Use

Server Certificates are used to secure and encrypt the connection between parties and ensure the integrity of data in transit.

AUB provides digital certificate through the TechCARE service with considerations and restrictions:

a. Standard SSL Certificate: used to secure a single-domain and establishes a traditional secure connection between two parties.

b. Extended Validation (EV) SSL Certificate: used to secure a single-domain and shows visitors the website is a safe place to enter their sensitive data because of the branded green address bar in the link.

c. Wildcard Certificates: allow web-hosts to secure unlimited sub-domains of a domain name on a single certificate; this type of certificate should not be used unless technical requirements force its use.

d. Alternative Name (SAN) and Unified Communication Certificates (UCC): Where technically feasible, SAN or UCC certificates should be used instead of wildcard certificates,. An UCC certificate allows securing a primary domain name and many Subject Alternative Names (SANs) in a single certificate.

e. Self-Signed certificate: A Self-signed certificate does not use the chain of trust used by standard SSL certificate (issued by institution). This kind of certificate is recommended for use only on systems without confidential data and only whenever there are technical or vendor requirements to do so.

f. Email certificate: Email certificates are use to digitally sign and/or encrypt user email to verify the sender and prevent tampering of email messages.

g. Certificate Status Change:

   a. The certificate custodian must renew or replace existing certificates before expiration to avoid business operations interruption based on certificate owner's requests.

   b. Certificate custodians must revoke certificates when one of the following occur:

      i. A private key has been compromised
      ii. The service is being retired or decommissioned
      iii. When the private key is no longer in use.
      iv. When an employee who has access to private keys leaves the organization, private keys and associated certificates must be revoked and replaced by new ones where feasible.

h. Certificate Protection

   i. Private keys are considered confidential data and as such the server administrator must protect the private keys.
   ii. Certificate administrators may not install the same private key on multiple hosts, except for clustered and load-balanced services.
   iii. The same private key and certificate should only be used by the service for which the certificate was ordered to reduce the risk of compromise across multiple data sets.

6. Applicability

This agreement applies to managers, administrators and/or technical staff from institutions who are responsible for systems, applications, and sites that needs SSL as any part of a PKI framework or to end users who need to digitally sign and encrypt their emails.

7. Compliance

Violations of the agreement may result in termination of this service agreement.

8. Authoring History

Revision	Date (DD-MM-YYYY)	Author	Reason for Changes
1	May 2016	Suzanne Elhorr	Document Draft
1.5	January 2017	Suzanne Elhorr	Document V1.5
2	17 November 2017	Suzanne Elhorr	Updated Document
2.5	2 January 2018	Suzanne Elhorr	Updated Agreement
2.6	25 January 2018	Suzanne Elhorr	Updated Agreement
2.7	February 8 2018	Suzanne Elhorr	Updated Agreement
3	12 June, 2018	Suzanne Elhorr	Reflect CIO's comments
3.1	9 July 2018	Suzanne Elhorr	Final Version