INFORMATION TECHNOLOGY SERVICES
George Mason University

Digital Certification Service Process

Version 1.4

PROCESS INFORMATION	
This table should be completed by the responsible office and IT Risk & Compliance, as it provides general information about the process.	
RESPONSIBLE OFFICES	ITS Enterprise Applications – Web Applications/Services
RELATED DOCUMENTS	Responsible Use of Computing (University Policy # 1301)
REFERENCE DOCUMENTS	
DOCUMENT CONTROL NUMBER	ITS. EA-PRS005
PURPOSE	This document is for George Mason University faculty and staff requesting a digital certificate. Any third-party needing a George Mason-affiliated security certificate must have their request sponsored and made by university faculty and staff, who will be responsible for overseeing the system or application being implemented.
LAST REVIEWED DATE	11/20/2024

NOTE TO ALL USERS

REVISION HISTORY

VERSION	DATE	ORGANIZATION/AUTHOR	DESCRIPTION OF CHANGES
1.0	1/16/2019	ITPP	Initial Release
1.1	4/14/2020	ITS EIS	Annual review with minor revisions – corrected policy name and standard name and reformatted using the current template
1.2	8/30/2021	ITS EIS	Annual review with minor revision – updated the number of years that server digital certificates are valid
1.3	11/15/2023	ITS EA – Web Applications/Services	Annual review with minor revisions – reformatted using the current template, updated the DCN as a result of re-organization; updated the Timetable for Review section per new process; and revised for correctness
1.4	11/20/2024	ITS EA – Web Applications/Services	Annual review with minor revisions; Updated document using the new

VERSION	DATE	ORGANIZATION/AUTHOR	DESCRIPTION OF CHANGES
			George Mason University logo, colors and editorial specifications.

PROCESS SCOPE

*Describe the overall scope of the process. It is **concerned primarily with controlling who, what, or when this process is applicable.** Please consider this a high-level summary.*

The process…

Digital certificates ensure both the identity and secure encryption of a website, individual, organization, device, user, or server.

The process is applicable when:

This process applies when Mason faculty and Staff are requesting a digital certificate for themselves or on behalf of a third-party or third-party vendor.

PROCESS INPUTS & OUTPUTS

Process Inputs

When there's a need for a digital certificate by George Mason faculty, staff, and third-party vendors affiliated with official university business.

Process Outputs

1. Certificate Signing Request (CSR)
2. Service Request (SR) in the ITSM tool
3. Email from Certificate Manager (CM) with a link for the certificate

DEFINITIONS

ACRONYM/TERM	DEFINITION
CM	Certificate Manager
CN	Canonical Name
CSR	Certificate Signing Request
SR	Service Request

ROLES AND RESPONSIBILITIES

Role	Responsibilities
Customer (Mason Faculty and Staff)	▪ <*For initial request*> Creates Certificate Signing Request (CSR) and completes a Service Request (SR) in the ITSM tool ▪ <*For canceling existing certificate*> Fills out a SR in the ITSM tool ▪ <*For modifying or adding domain names of existing certificates*> Fills out an SR in the ITSM tool. Provides a new CSR for any certficate changes. ▪ <*For renewal of expiring certificate*> Completes an SR in the ITSM tool ▪ Downloads and installs digital certificate(s)
Registrar (ITS staff appointed by the Chief Information Officer)	▪ <*For initial request*> Copies Customer's CSR onto the Certificate Manager (CM) and then approves Customer's digital certificate request ▪ <*For canceling existing certificate*> Revokes existing digital certificate ▪ <*For modifying domain names of existing certificate*> Replaces the existing CSR with the updated CSR and generates a new digital certificate. ▪ <*For renewal of expiring certificate*> Renews the certificate in CM with existing CSR/parameters, unless customer requests changes to the certificate and provides new CSR.
Certificate Manager (CM)	▪ Completes the digital certificate signing procedures ▪ Sends email to both Customer and Registrar with link to digital certificate(s)

FLOWCHARTS

Provide an image of a Visio diagram to show process steps.

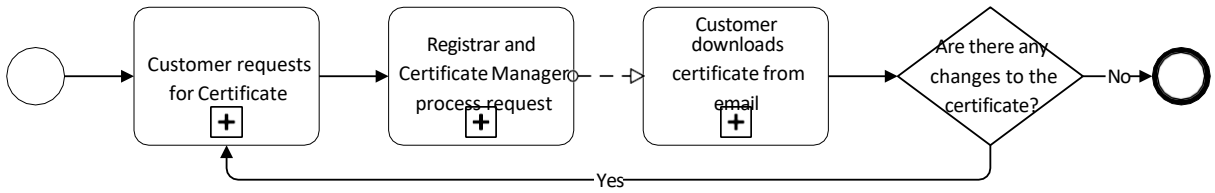
George Mason University (Mason), as an Internet2 member, subscribes to the digital certificate service offered by Internet2. This service allows Mason to issue server, website, and personal digital certificates. A workflow and request process has been created within the ITSM tool to allow customers to request new or change existing digital certificates.

There are four types of digital certificates: single domain, multi-domain, wildcard, and personal. Single domain is the default digital certificate type, and valid for a website or server known by a single name. A multi-domain digital certificate is issued to a website or server that will be known by many different names. All of the

domain names must either end in ".gmu.edu" or have been defined within the Certificate Manager (CM) web-based interface as delegated to Mason. A domain validation process has been established by the vendor to prove that Mason has control over a domain name or to delegate certificate management of a gmu.edu domain to a third-party. A wildcard digital certificate is valid for all systems under a specific sub-domain. It is not necessary to specify which systems reside within the subdomain. For security reasons, a wildcard digital certificate for the top-level gmu.edu domain will only be issued by approval of the IT Security Office to a trusted ITS-managed server. Personal digital certificates are used to digitally sign email and, optionally, encrypt the body of the email message. These certificates are available but are not in general use because ITS has not yet developed a formal process that includes identity proofing. At present, personal digital certificates are limited in scope to Information Technology Services (ITS) and selected university staff.

Server digital certificates are valid for 1 year and must be renewed on an annual basis. Personal digital certificates are valid for one year only.

Requestors are responsible for complying with minimum key sizes when requesting certificates. For all server and website digital certificates, the Canonical Name (CN) must be a Fully Qualified Domain Name (FQDN). Internet Protocol (IP) addresses and internal domain names (.local) are not acceptable.



HIGH-LEVEL PROCESS OR STEP

PROCESS/STEP DESCRIPTION	Responsible Group	Output(s)
Requesting Certificate		
1. The customer initiates the request by creating a Certificate Signing Request (CSR) and completing a Service Request (SR) in the IT Service Management (ITSM) tool. Customers must comply with minimum key sizes when requesting digital certificates. 2. If the customer is requesting server and website digital certificates, the CN must be a FQDN. IP addresses and internal domain names (.local) are not acceptable. 3. Upon notification by the ITSM tool, a registrar will take responsibility for the request.	Customer	CSR and SR
Processing Certificate Request		
1. Using the Certificate Manager (CM) service, the registrar copies over the CSR and completes the remaining fields needed for requesting a digital certificate. 2. The registrar issues the cert and notes the ITSM ticket number in comments of the certificate.	Registrar, CM	An email containing the link to the certificate

3. The CM completes all the certificate signing procedures. 4. The CM sends an email to both the registrar and the customer that contains the links for the digital certificate(s).		
Downloading and Installing Certificate(s)		
1. For Server Certificates, the customer will download and install the server certificate and, if necessary, any intermediate and root certificates. 2. For Personal Certificates, the customer will download the certificate and add it to the appropriate application such as an Outlook client.	Customer	Installed certificate
Making Changes to Existing Certificate(s)		
1. If a customer is using a multi-domain digital certificate and requires that changes be made to the domain names listed, he/she requests the ITSM tool by supplying a new CSR. The registrar replaces the existing CSR with the updated CSR and generates a new digital certificate. The issue and expiration dates remain unchanged from the original request. 2. If a customer no longer requires his/her digital certificate to be valid or if the private key has been compromised, a request to revoke/cancel the existing certificate can be made in the ITSM tool. The registrar uses the revoke certificate functionality to revoke the certificate. Once revoked, a digital certificate cannot be made valid again. A new digital certificate request can be made using the same name. 3. When a digital certificate comes within 30 days of expiration, the customer receives a daily email alerting him/her of pending expiration. The notices continue until the expiration date (even if the certificate is renewed). A renewal request is made via the ITSM tool. During renewal, the CSR for the previous request can be used unless the customer requires the use of a new CSR.	Customer	CSR

ARTIFACTS

ARTIFACT	PURPOSE
Certificate Signing Request (CSR)	The CSR is a standardized way to send the issuing Certificate Authority (CA) your public key, which is paired with a secret private key on the server, and provides relevant information about the requester.
Service Request	A Service Request is a request for information, advice, or access to a service. Some examples are a request to reset a password, obtain software, or install a new workstation.
Email from CM with a link for the certificate	This email is sent by the Certificate Manager to the customer and registrar with a link to the certificate.

TIMETABLE FOR REVIEW

This process will be reviewed every 2 years at a minimum.

APPROVALS

ROLE	NAME & ORGANIZATION	SIGNATURE	DATE
IT EA Web Applications/Services Team Lead	Kate Orf	Signed by: Katherine L Orf 0377E4CB574747B...	11/21/2024