

NASA/MSFC PKI CERTIFICATE REVOCATION AND SUSPENSION/DISABLING REQUEST

This form must be filled out completely. Please read and follow all instructions. Any form lacking information will be disregarded. Misuse of PKI processes may constitute grounds for termination of privileges, administrative action, and/or civil or criminal prosecution. If the user account is no longer required, select the "Delete" user account from the pop-up menu under 1a. "Action Requested" and complete Section 2, "Certificate User Information."

1. REQUIREMENT

a. Request Date:	b. Action Requested:
------------------	----------------------

c. Detailed Reason for Request (Use continuation block on page 2, if needed):

d. Period of Suspension/Disabling (As Applicable): From: _____ To: _____

e. Requestor (Name, Title or Function):	f. Organization:	g. Mail Code:
---	------------------	---------------

h. Badge Number:	i. E-mail Address:
------------------	--------------------

j. Phone Number (include area code):	k. Requestor Approval Signature/Date:
--------------------------------------	---------------------------------------

2. CERTIFICATE USER INFORMATION

a. User Name (Last, First, MI):	b. NASA Center:	c. Building and Room Number:
---------------------------------	-----------------	------------------------------

d. Badge Number:	e. E-mail Address:
------------------	--------------------

f. Organization:	g. Mail Code:	h. Phone Number (include area code):
------------------	---------------	--------------------------------------

3. USER ORGANIZATION MANAGEMENT NOTIFICATION / APPROVAL

a. Legal Name (Last, First, MI) and Official Title:	b. Organization:	c. Mail Code:
---	------------------	---------------

c. Phone Number (include area code):	e. E-mail Address:	d. Signature/Date:
--------------------------------------	--------------------	--------------------

4. COTR / TECHNICAL MONITOR NOTIFICATION / APPROVAL (FOR CONTRACTORS ONLY)

a. Legal Name (Last, First, MI) and Official Title:	b. Organization:	c. Mail Code:
---	------------------	---------------

d. Phone Number (include area code):	e. E-mail Address:	f. Signature/Date:
--------------------------------------	--------------------	--------------------

5. RA ACTION

a. Date Received:	b. Date of Action:	c. Action Taken:
-------------------	--------------------	------------------

d. User Account Name:	e. Validity Period:
	From: _____ To: _____

e. RA Signature/Date:	d. Date IT Security Manager Notified (As Applicable):
-----------------------	---

6. COMMENTS AND NOTES

* Explain Actions and Notifications (Use continuation block on page 2, if needed):

**NASA/MSFC PKI CERTIFICATE REVOCATION AND SUSPENSION/DISABLING REQUEST
(Continuation Sheet)**

Requestor Name:

User Name:

Request Date:

1c. DETAILED REASON FOR REQUEST (Continued)

Requestor / User Signature/Date:

6. COMMENTS AND NOTES (Continued)

IT Security Manager Signature/Date:

RA Signature/Date:

RA Signature/Date:

NASA/MSFC PKI CERTIFICATE REVOCATION AND SUSPENSION/DISABLING REQUEST INSTRUCTIONS

1. Requestor: Read "What You Need to Know About Certificate Revocation and Suspension" below. Notify MSFC PKI RA by phone (544-5205) of serious incident and immediate revocation requirement (e.g., Key compromise, suspected compromise, dismissal for cause) as appropriate. Notify the user's management if an immediate revocation action has been requested. Follow up with submittal of Revocation and Suspension/Disabling Request form as required by circumstances of event.
2. Requestor/User: Complete Section 1, "Requirement", of the request form; digitally sign as the requestor. Indicate type of action requested (e.g., suspend/disable for temporary requirements; revoke if serious incident; delete if no longer needed). Provide detailed reason for action. Indicate period of suspension/disabling as applicable. Note: someone other than the Certificate owner may be the requestor for the process. Note: Put cursor over signature block for instructions on how to digitally sign.
3. Requestor/User: Complete Section 2, "Certificate User Information", providing user information. Submit form to User Management for notification/approval and digital signature. Note: someone other than the Certificate owner may be the requestor for the process and may not have all the user information. If not the User, Requestors should provide as much information as possible.
4. User Management: Complete Section 3, "User Organization Management Notification/Approval" and digitally sign.
Contractor: Submit form to COTR or Technical Monitor for notification/approval and signature.
NASA Manager: Go to Step 6.
5. COTR or Technical Monitor: Complete Section 4, "COTR/Technical Monitor Notification/Approval" and sign.
6. Submit form via email to: pkira@msfc.nasa.gov and wait for a response from the RA.
7. RA: Complete Section V and sign. Indicate Action Taken and Date of Action; disable/suspend or revoke certificate per direction, and record event in logbook. Indicate period of suspension as applicable. Indicate date MSFC IT Security Manager notified of immediate revocation actions.
8. RA: Notify Requestor (and/or User) as appropriate to circumstances and/or per MSFC IT Security Manager direction of action taken by secure method.
9. Requestor/User: Receive notification of action taken via sealed envelope or other secure method.

WHAT YOU NEED TO KNOW ABOUT CERTIFICATE REVOCATION OR SUSPENSION

Revocation: Certificates will be revoked when the certificate is no longer trusted for any reason. This includes encryption and/or verification certificates for **end users**, RA Administrators, and PKI Security Officers. Loss of trust includes but is not limited to:

1. Dismissal or suspension for cause
2. Compromise/suspected compromise of private key and/or user password and profile
3. Change in requestor's/user's role (e.g., organizational change between Centers) or permissions
4. Termination of employment
5. Failure of requestor/user to meet specified obligations under the NPG and relevant policies

Note 1: Key compromise, suspected compromise or dismissal for cause is provocation for immediate revocation of user access. These events are classified as security incidents and will be handled in accordance with MSFC Security Incident/Investigative procedures. Reports of incidents of key compromise, suspected compromise, or dismissal for cause MUST be placed within 1 hour of the detection of the compromise or suspected compromise. To report such cases or incidents, phone (544-5205) MSFC PKI RA.

Note 2: Requests for revocation for other reasons MUST be placed within 24 hours of the change.

WHAT YOU NEED TO KNOW ABOUT CERTIFICATE REVOCATION OR SUSPENSION (Continued)

Reinstatement of Revoked Privileges: Reinstatement of revoked certificates is permitted only under specific circumstances. Re-application with administrative review and determination will be required. Reinstatements may be permitted for the following situations:

- o Organizational changes within NASA which result in Distinguished Name changes affecting several employees.
- o Revocations not the result of a key compromise and the user is temporarily unavailable to present him/herself in person.

Suspension/Disabling: Certificates may be suspended and disabled for such circumstances as when a user goes on leave or is no longer a part of the domain. Disabled user accounts may be **reinstated** at a later time. Re-application is required to re-enable. Notification to Suspend/Disable a user certificate **MUST** be made as soon as the requirement is known or within 14 hours of identification of the requirement or change.

Who May Request: Revocation or suspension/disabling of an end-entity's certificate may be requested by:

- o Requestor/End Users
- o RA Administrator
- o User's Management
- o MSFC IT Security Manager

Accidental Key Compromise: An immediate report of any key compromise situation must be filed with the PKI RA giving the circumstances of the compromise, See Note 1 (Page 1 of Instructions). If the compromise is accidental on the part of the user/requestor, no further notification action is required. The RA will rescind access. A request for Key Recovery will be required to regain access.