NASA/MSFC PKI CERTIFICATE - KEY RECOVERY 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.

1. REQUIREMENT

a. Key Recovery Request Made By:

b. ☐ User c. ☐ Administration/Management (Non-Consent of User)

d. User Reason for Request:

e. Reason for Non-Consenting Request:

f. Detailed Reason for Request and/or Need to Access User's Files (Use continuation sheet if needed):

2. CERTIFICATE USER INFORMATION

a. User Name (Last, First, MI):

b. Phone Number (include area code):

c. Badge Number:

d. Mail Code:

e. Organization:

f. E-mail Address:

g. Contract New Expiration Date:

3. REQUESTOR (NON-CONSENTING REQUESTS)

a. Requestor (Name, Title or Function):

b. Organization:

c. Mail Code:

d. Badge Number:

e. E-mail Address:

f. Phone Number (include area code):

g. If request is user-non-consenting, give name(s) of personnel authorized to view/access files and to be responsible for their control and/or subsequent viewing by other parties (name/title, organization, phone number - use continuation sheet, if needed):

h. Required File Access: ☐ Approval to Access/View all files OR ☐ Access/View Specific Files or File Names (Describe - Use continuation sheet, if needed):

i. Disclose Action to User: ☐ Yes ☐ No Other Disclosure Instructions (Describe - Use continuation sheet, if needed):

j. Requestor Approval Signature/Date:

4. USER ORGANIZATION MANAGEMENT NOTIFICATION / APPROVAL

a. Organization and Mail Code:

b. Legal Name (Last, First, MI) and Official Title:

c. Phone Number (include area code):

d. Signature/Date:

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

a. Organization and Mail Code:

b. Legal Name (Last, First, MI) and Official Title:

c. Phone Number (include area code):

d. Signature/Date:

6. IT SECURITY MANAGER NOTIFICATION / APPROVAL

a. Name:

b. Signature/Date:

7. RA ACTION

a. Date Received:

b. Date of Action:

c. User Account Name:

d. Date IT Security Manager Notified (As Applicable):

e. RA Signature/Date:

f. RA Signature/Date:

8. COMMENTS AND NOTES

* Explain Actions and Notifications - Use continuation sheet, if needed:

WHAT YOU NEED TO KNOW ABOUT KEY RECOVERY

Key Recovery Process: The Key Recovery process is used to revise a User's profile data and reassign new key pairs for accessing previously encrypted data. The Users current key pairs are disabled. The Key Recovery process may be invoked for security or legal reasons, Certificate Revocations or Suspensions, as well as for business continuity purposes to recover and view previously encrypted data.

Who May Request: Key Recovery actions may be initiated by:

- End Users
- User's Management
- MSFC IT Security Manager
- Law Enforcement Agencies/Court Orders
- Other Requestors with justifiable need or security concerns

User Requests for Key Recovery: Some examples for User requested Key Recovery include but are not necessarily limited to the reasons below. To protect against unauthorized requests, Users should personally submit written, signed requests and validate their Identity upon submittal.

- User forgets Password
- User loses or damages a PKI profile file
- User loses or damages a security token (PCMCIA card)
- User suspects keys have been compromised
- User accidentally compromises his/her keys
- User key expired due to lack of use or expiration date (contractors)

An immediate report of any key compromise situation must be filed with the PKI RA giving the circumstances of the compromise. The PKI RA will suspend accessibility to a User's files. If the compromise is accidental on the part of the User, no further notification is required but the User should follow up with submission of a written Key Recovery Request. Access will be renewed with reassignment of new key pairs through the Key Recovery process.

Key Recovery without User Consent: Key Recovery actions may be initiated without a User's consent for investigative or business continuity purposes. Actions may or may not be disclosed to the User. Examples for Key Recovery without User consent include but are not necessarily limited to:

- User leaves the organization and management needs to recover and decrypt files for business continuity
- User's actions are in question by Center IT Security Manager and User's files need to be reviewed
- User's actions are in question by an external law enforcement agency and User's files need to be reviewed

To protect Users from unauthorized access to their files, all requests for Key Recovery submitted without the User's consent must be approved through a formal and official written notification and approval process. In certain situations, a Court Order for Key Recovery will constitute written approval. Key Recovery actions must be performed and witnessed by two certified RA personnel.

The decision to perform a Key Recovery without a User's consent should be made with discretion by the Requestor in consideration of the particular circumstances. When a User discovers a change in accessibility, the PKI RA may be contacted for assistance. Requestors should assess the impact of disclosure to the User and depending upon circumstances may choose not to perform a Key Recovery. Security issues and concerns should be reported to and coordinated with the IT Security Manager for determination of course of action appropriate. In choosing Key Recovery, Requestors must provide instructions on whether or not the Key Recovery action is to be disclosed and what specific information may or may not be provided to the User.

KEY RECOVERY REQUEST INSTRUCTIONS

1. Requestor/User: Read "What You Need to Know About Key Recovery" section (above).

2. Requestor/User: Complete Section 1, "Requirement". Indicate who is making request. Select reason from pop-up menu and provide detailed reason for action. If the request reason is a suspected Key Compromise, see NOTE* (next page) and follow procedure for incident reporting.

3. Requestor/User: **Complete Section 2, "User Information". User go to Step 9.** If you are recovering for yourself, you do not need management approval. If the Requestor is someone other than the Certificate User and the request is being submitted without the users knowledge, go to Step 4.

KEY RECOVERY REQUEST INSTRUCTIONS (Continued)

4. Requestor: Contact the MSFC IT Security Manager (544-4373) to determine course of action. If proceeding, complete Section 3, "Requestor (Non-Consenting Requests)" and digitally sign. Identify the person(s) to be responsible for viewing and controlling recovered files. Identify files to be viewed (all or specific). Provide instruction as to whom disclosure of the Key Recovery action should be made and what information is to be provided. Submit form to User's management for notification and approval of requested action. If applicable, Requestor's may supply a diskette containing the Users files to be viewed during the scheduled Key Recovery. (Note: Place cursor over signature block for instructions on how to digitally sign.)

5. User Management: Complete Section 4, "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 7.

6. COTR or Technical Monitor: Complete Section 5, "COTR/Technical Monitor Notification" and digitally sign.

7. Submit form to: NASA/MSFC IT Security Manager, Steve.R.Jones@msfc.nasa.gov.

8. IT Security Manager: Validate requirement and digitally sign approval in Section 6, "IT Security Manager Notification/Approval". Provide explanatory comments on notifications and actions in Section 8, "Comments and Notes".

9. Submit form to: **PKIRA@msfc.nasa.gov** with the subject "recover - user name" and wait for response from the RA.

10. User: The RA will notify User of Key Recovery approval/rejection by phone, and request that User pick up new account information in person. The User will present in person to the RA at building 4312 the original Key Recovery Request. Verify identity by showing MSFC badge upon delivery. Acknowledge receipt of new account information.

11. Requestor: Supply list or diskette of files to be reviewed. Present in person to RA at building 4312. Verify identity by show of MSFC Badge.

*NOTE: 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 or e-mail the IT Security Manager detailing reasons and circumstances or phone the designated MSFC PKI RA at 544-3623. Follow up with submission of approved Revocation and/or Key Recovery request form. The IT Security Manager will validate immediate requirements and coordinate revocation and key recovery requirements with PKI RA.

I acknowledge and declare that, prior to applying for, accepting or using the NASA Public Key Certificate, I have read and accepted the conditions in the NASA PKI Subscriber Agreement (which is available on the Internet at http://nasaca.nasa.gov/docs.html **. I am aware that the X.509 Certificate Policy for NASA PKI and the NASA Certification Authority Certification Practice Statement are available on the Internet at http://nasaca.nasa.gov/docs.html and I accept the subscriber obligations and responsibilities contained therein as summarized in the NASA PKI Subscriber Agreement. I hereby certify that the information provided by me is true and correct to the best of my knowledge and belief.**

I certify that I am the individual described in the attached NASA/MSFC PKI Certificate Application and acknowledge receipt of the corresponding Registration Number and Authorization Code for my PKI Certificate.

User Approval Signature/Date: