



Chief Information Security Office

Exception Request Form Directions

This document contains the directions for filling out the [NYS-P13-001 Security Exception Form](#). This form should be completed with the assistance of your organization's information security officer (ISO)/designated security representative. If you receive IT services from NYS ITS, please work with your assigned Business Information Security Officer (BISO) to complete the form. If you are part of a local government, school district, or other State Entity and have questions regarding the form, please contact the NYS Chief Information Security Office –Governance and Compliance unit by email for assistance at GCAT@ITS.ny.gov

Please fill out every section. If necessary, insert “N/A” if not applicable.

Section 1: Exception

1.1 Point of Contact Information

This area is to identify who would be the best contact for any questions on the exception request. The ISO/designated security representative is often a good choice; however, it could be others such as a Project Manager, Application/Information/Business Owner, etc.

1.2 Exception Details

Policy Reference:

Please identify from which NYS security policy(s) you are requesting an exception. Please provide the policy reference number(s) and name(s). (<https://its.ny.gov/ciso/policies/security>)

Standard Reference:

Please identify from which NYS security standard(s) you are requesting an exception. Please provide the standard reference number(s) and name(s). (<https://its.ny.gov/ciso/policies/security>)

Proposed End Date:

How long will the exception be required? Remember that exceptions should be used as a temporary measure while a change in technology or procedure is developed that will meet the policy and/or standard. No indefinite exception requests will be allowed.



Agency(s) Impacted:

Which agency(s) is impacted by the non-compliance? (Remember that systems and data can impact multiple agencies.)

System(s) Hardware Impacted (if applicable):

List any systems, servers, databases, endpoints, network equipment, etc. that may be impacted by the granting of this exception. This may also help in identifying the agency(s) that may be impacted.

Will this impact the process, staging, and/or transmission of PPSI?

Yes No

If yes, please provide type(s) of PPSI.

1.3 Exception Request

Background Information:

Please provide sufficient information that will allow the reviewers to have a clear understanding of the system(s) involved with this request, including its purpose, its data, and its platform/architecture.

Reason for Request:

Please describe the specific issue with compliance. Note the specific subsection with the policy or standard listed above. (<https://its.ny.gov/ciso/policies/security>)

1.4 Description/Assessment of Risk

Please describe the risk(s) that will exist as a result of non-compliance. This should be expressed clearly and speak to technical and business risk that will exist for the duration of the exception. It is highly recommended to work with your ISO/designated security representative, or BISO for ITS-served entities, to appropriately determine the risk of non-compliance.

1.5 Compensating Controls (to mitigate risk associated with non-compliance)

Please provide the compensating controls (if any) that have been implemented to lessen the risks that are described in the description/assessment of risk above.

1.6 Corrective Action Plan

This area can have two distinct answers:

- 1. Corrective Action Plan - Please provide the plans and methods that will be employed to eliminate the need for this exception request, with specific details such as project number, major milestones, and estimated completion date.*



2. *Risk Acceptance - Provide an explanation of why compliance is not reasonable or feasible to achieve, and why the agency has chosen to accept the risk. (This may allow for a longer period of time before the exception would expire.)*

Section 2: Requestor Authorizations

(For Adobe Digital Signature, please see directions in [Appendix A](#)) – cc: all signers on email submission

2.1 Information/Business Owner:

Please provide Name, Title, and Signature/digital signature

2.2 Information Security Officer (ISO)/Designated Security Representative:

Please provide Name, Title, and Signature/digital signature

2.3 Chief Information Officer (Agency/Portfolio CIO):

Please provide Name, Title, and Signature/digital signature

2.4 Commissioner/Executive Deputy Commissioner (or equivalent):

Please provide Name, Title, and Signature/digital signature

2.5 Additional comments by any Authorized Signers:

This section provides a place for a signatory to provide any comments they may have in support of, or against, the approval of this request. For example, the ISO/designated security representative may not approve of the exception, even though they are required to sign it prior to submission.

Section 3: Exception Approval/Denial (For CISO Use Only)

Approved Denied

Approved Review Date:

This is the date set by the CISO as to when this exception will need to be reviewed.

Reason for Approval/Denial:

This allows for any comments that the CISO may have regarding the approval/denial of the exception.

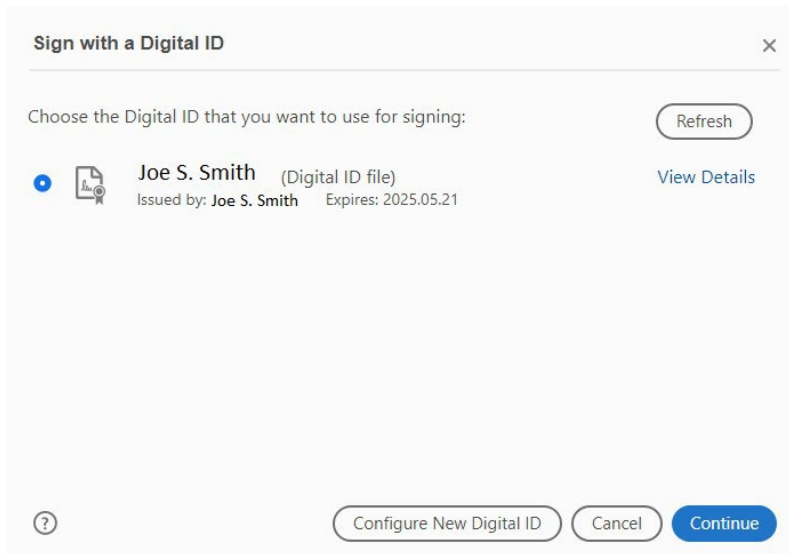
3.1 Chief Information Security Officer or Delegate:

Please provide Name, Title, and Signature/digital signature

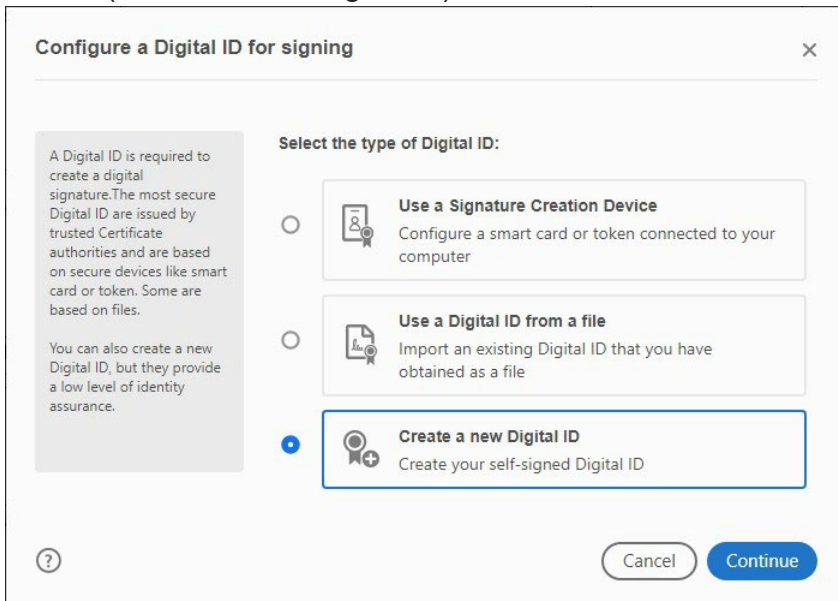


Attachment A – Adobe Acrobat Reader DC Digital Signature Directions

1. Open the Exception form PDF that needs to be Signed.
2. Click on the signature field on the form.
3. The following screen will open: (If you have a signature skip to step 9)
4. To create a new signature, select (Configure new Digital ID) on the bottom, then click continue:



5. Select (Create a new Digital ID) then click continue:





6. Select the Destination (It will show SAVE TO FILE) then click continue:

Select the destination of the new Digital ID

Digital IDs are typically issued by trusted providers that assure the validity of the identity. Self-signed Digital ID may not provide the same level of assurance and may not be accepted in some use cases.

Consult with your recipients if this is an acceptable form of authentication.

- Save to File**
Save the Digital ID to a file in your computer
- Save to Windows Certificate Store**
Save the Digital ID to Windows Certificate Store to be shared with other applications

[?](#) [Back](#) [Continue](#)

7. Fill in the information, then click continue:

Create a self-signed Digital ID

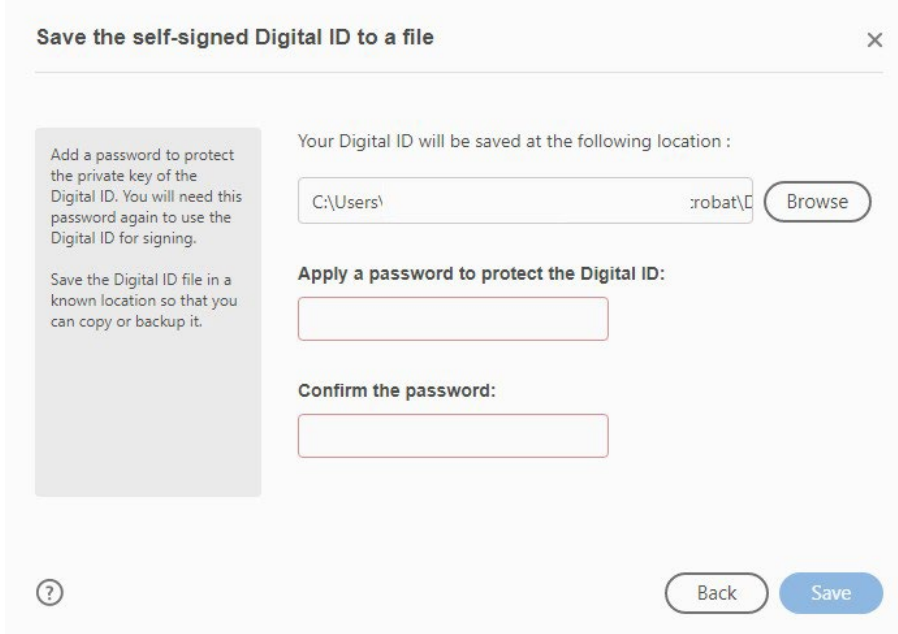
Enter the identity information to be used for creating the self-signed Digital ID.

Digital IDs that are self-signed by individuals do not provide the assurance that the identity information is valid. For this reason they may not be accepted in some use cases.

Name	<input type="text" value="Enter Name..."/>
Organizational Unit	<input type="text" value="Enter Organizational Unit..."/>
Organization Name	<input type="text" value="Enter Organization Name..."/>
Email Address	<input type="text" value="Enter Email..."/>
Country/Region	<input type="text" value="US - UNITED STATES"/>
Key Algorithm	<input type="text" value="2048-bit RSA"/>
Use Digital ID for	<input type="text" value="Digital Signatures"/>

[?](#) [Back](#) [Continue](#)

8. Choose location to save file, and create password, then click save:



Save the self-signed Digital ID to a file [X]

Add a password to protect the private key of the Digital ID. You will need this password again to use the Digital ID for signing.

Save the Digital ID file in a known location so that you can copy or backup it.

Your Digital ID will be saved at the following location :

C:\Users\ .robot\ [Browse]

Apply a password to protect the Digital ID:

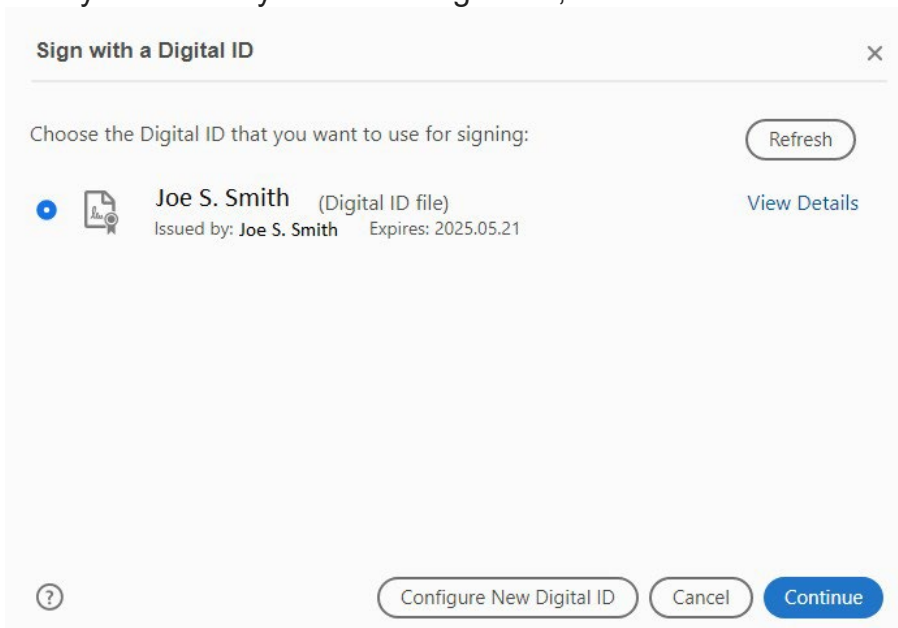
[Text Input]

Confirm the password:

[Text Input]


[?] [Back] [Save]

9. Now you are ready to use the signature, then click continue:



Sign with a Digital ID [X]

Choose the Digital ID that you want to use for signing: [Refresh]

 **Joe S. Smith** (Digital ID file) [View Details](#)
Issued by: Joe S. Smith Expires: 2025.05.21

[?] [Configure New Digital ID] [Cancel] [Continue]



Office of Information Technology Services

10. Make any changes you want and enter your password and click sign:

The screenshot shows a digital signature interface. At the top, there is a dropdown menu for 'Appearance' set to 'Standard Text' and a 'Create' button. Below this is a signature box containing the name 'Joe S. Smith' in large black font, a red digital signature scribble, and the text 'Digitally signed by Joe S. Smith' followed by the date and time 'Date: 2020.05.21 13:20:07 -04'00''. Below the signature box is a link 'View Certificate Details'. Underneath is a section for 'Review document content that may affect signing' with a 'Review' button. At the bottom, there is a password field with asterisks, a 'Back' button, and a blue 'Sign' button.

11. After clicking sign it will prompt you to save the document. Now you can forward the document on to the next person to review and sign.