

Mobile Digital Signature (MDS) Application

HELP GUIDE

Version 4.0.1

Contents

About

[MDS Application Limitations](#)

Getting Started

[Launching the MDS Application](#)

[Opening a PDF with the MDS icon](#)

[Opening PDFs through an email application or web browser](#)

Using the Application

[Digital Signatures](#)



[Removing Unsigned Custom Signatures Fields](#)[Continue Signing](#)[Signature Verification](#)[Invalid Signatures](#)[Removing Signatures](#)[Viewing Digital Certificate Properties](#)[Edit](#) [Share](#) [Help Guide](#) [Close PDF](#) 

About

Digital signatures can be used for many types of documents where traditional hand-written signatures have been used in the past. The sole existence of a digital signature is not enough assurance that a document is what it appears to be. For a recipient to fully trust an electronic document, they must be able to verify that:

- The document has not been altered
- The document came from someone they trust

Electronic Signatures are the equivalent of a hand-written signature that has been digitized. Electronic signatures are popular because they are easy to use (ex. created using a finger or mouse) however they are not equivalent to digital signatures.

Digital Signatures are quite different from Electronic signatures as they are more trustworthy because they verify the identity of the person who signed and that the signature is valid. In contrast to paper-based (hand-written) signatures, digital signatures offer higher levels of fidelity and integrity. Digital signatures verify and assure the following:

- The document is authentic and comes from a verified source
- The document has not been tampered with since being digitally signed as the signature would be displayed as invalid if changes were made
- The identity of the signer has been verified by a trusted entity or organization (by a trusted Certificate Authority (CA))

Digital signatures in Portable Document Format (PDF) documents address these needs by providing a way to authenticate digital data based on public key cryptography. This document describes how digital signatures can be placed on or validated within a PDF document by using the Mobile Digital Signature (MDS) application.

The Mobile Digital Signature (MDS) application allows users to apply digital signatures to PDFs from mobile devices on both the Apple iOS and Android platforms using the Purebred derived DoD issued digital certificate on the DoD Mobility Unclassified Capability (DMUC) device.

The following limitations should be noted as you utilize the MDS Application:

- The MDS Application will only support PDF documents that are fillable, containing predefined digital signature blocks, using X.509 based digital signing certificates, and will interact with PDF documents whose document security permission settings authorize it.
- The MDS Application will not create PDF documents.
- The MDS application will not identify or validate hand-written or electronic signatures.
- The MDS Application will only utilize X.509 based digital signing certificates that are accessible from within the mobile device upon which it is installed.
- The MDS Application will rely on external Certificate Authorities to provide a revocation status for an issued certificate.
- The MDS Application will rely on an Internet connection to perform a CRL check.
- The MDS Application cannot store the information related to any PDF documents and as such you must rely on external applications or storage.

Getting Started

This section explains how to launch the MDS Application from an Android device.

LAUNCHING THE MDS APPLICATION

Users launch the MDS Application via two methods:



- 1) Select the MDS icon on an Android device. This will bring you to the MDS Application's welcome screen.

- a. At the MDS Application's welcome screen, users select  to open files stored locally on the device or in cloud storage (i.e. Google Drive, OneDrive, Dropbox, etc.).
 - i. Once a PDF file has been selected, the file will be opened to the MDS Application's main screen to allow the user to use all the features of the MDS Application.
- b. Select the  (Exit) icon
 - i. Selecting this icon will close the MDS Application
- c. Select the  (Help Guide) icon
 - i. Selecting this icon will open the help guide

- 2) Open a PDF through a PDF viewing application (if installed) and share (export) the PDF with the MDS Application. This will open the MDS Application and the PDF that was shared.
 - a. Alternatively, save a PDF received from an email to either the internal storage on the device or a cloud storage service. Then follow method #1 (above) to open the PDF.



OPENING A PDF WITH THE MDS ICON

Once the MDS Application opens to the welcome screen, users can access PDFs that are stored locally on the device or in cloud storage (i.e. Google Drive, OneDrive, Dropbox, etc.) by selecting the  icon.

- Digitally sign the PDF in predefined signature blocks
- Determine the validity of existing digital signatures on the PDF
- Edit the fields in fillable PDF
- Save PDF locally on the mobile device or on a cloud storage media
- Share and export the PDF using multiple applications that are enabled on the device such as email, cloud storage applications or text messaging
- Open new PDF documents
- View the MDS help guide
- Close the MDS Application

OPENING PDFS THROUGH AN EMAIL APPLICATION OR WEB BROWSER

PDF attachments will either have to be saved to the local device or a cloud storage application; from which the MDS Application is able to open. Alternatively, a 3rd party PDF viewer application with the ability to share to other applications will be able to export a PDF into the MDS Application. The MDS Application will allow users to perform the following:

- Digitally sign the PDF in predefined signature blocks
- Determine the validity of existing digital signatures on the PDF
- Edit the fields in fillable PDF
- Save PDF locally on the mobile device or on a cloud storage media
- Share and export the PDF using multiple applications that are enabled on the device such as email, cloud storage applications or text messaging
- Open new PDF documents
- View the MDS help guide
- Close the MDS Application

Using the Application

This section explains the navigation ribbon icons of the MDS Application.

DIGITAL SIGNATURES

The MDS Application identifies all areas of the PDF that have predefined digital signature blocks that will accept a digital signature. Selecting the  icon brings a right-side menu that lists all signature block areas of the PDF that can accept a digital signature.

Signing

After selecting the  icon on the navigation ribbon, the list of digital signature block areas of the PDF that can be signed will appear on a right-side menu. Follow the steps below (1-2) to successfully sign a PDF.

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT
 Executive Order 13495, 9397, and Public Law 94-474, the Computer Fraud and Abuse Act.
PRINCIPAL PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DOD) systems and information. **NOTE:** Records may be maintained in both electronic and/or paper form.

ROUTINE USES: Disclosures of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

DISCLOSURE: None.

TYPE OF REQUEST: AUTHORIZED MODIFICATION DEACTIVATE USER ID: _____ DATE (YYYYMMDD): 20110107

SYSTEM NAME (Platform or Application): Defense Civilian Personnel Data System (DCPDS) **LOCATION (Physical Location of System):** NGB-San Antonio, TX

PART I - (To be completed by Requestor)

1. NAME (Last, First, Middle Initial)	2. ORGANIZATION
3. OFFICE SYMBOL/DEPARTMENT	4. PHONE (DOD or Commercial)
5. OFFICIAL E-MAIL ADDRESS	6. JOB TITLE AND GRADE/RANK
7. OFFICIAL MAILING ADDRESS	8. CITIZENSHIP <input type="checkbox"/> US <input type="checkbox"/> FN <input type="checkbox"/> OTHER <input type="checkbox"/> MILITARY <input type="checkbox"/> CIVILIAN <input type="checkbox"/> CONTRACTOR

10. I/A TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.)
 I have completed Annual Information Awareness Training. DATE (YYYYMMDD): _____

11. USER SIGNATURE: _____ 12. DATE (YYYYMMDD): _____

PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (Individual is a contractor - provide company name, contract number, and date of contract expiration in Block 1E.)

13. JUSTIFICATION FOR ACCESS
 Defense Civilian Personnel Data System (DCPDS) Supervisor/Manager permission responsibility to input and coordinate electronic Request for Personnel Access (RPA) to DCPDS.

14. TYPE OF ACCESS REQUIRED: AUTHORIZED PRIVILEGED

15. USER REQUIRES ACCESS TO: UNCLASSIFIED CLASSIFIED (Specify category) OTHER

16. VERIFICATION OF NEED TO KNOW
 I certify that this user requires access as requested. Yes. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.) 20110107

17. SUPERVISOR'S NAME (Print Name) _____ 18. SUPERVISOR'S SIGNATURE _____ 19. DATE (YYYYMMDD) _____

20. SUPERVISOR'S ORGANIZATION/DEPARTMENT _____ 20a. SUPERVISOR'S E-MAIL ADDRESS _____ 20b. PHONE NUMBER _____

21. SIGNATURE OF INFORMATION OWNER/OPR _____ 21a. PHONE NUMBER (608) 242-3713 _____ 21b. DATE (YYYYMMDD) 20110107

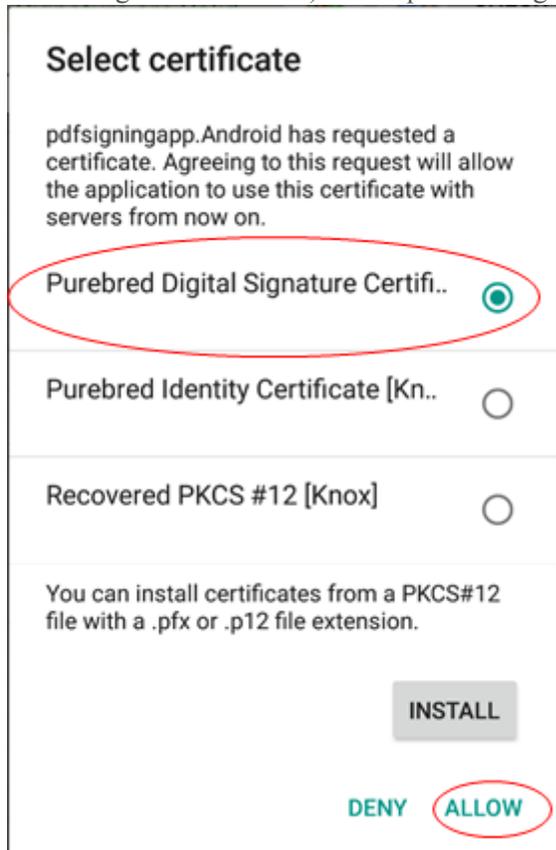
22. SIGNATURE OF IAD OR APPOINTEE _____ 22a. ORGANIZATION/DEPARTMENT WJ JF1QJ1 IS _____ 24. PHONE NUMBER (608) 242-3713 _____ 25. DATE (YYYYMMDD) 20110107

DD FORM 2875, AUG 2009 PREVIOUS EDITION IS OBSOLETE. Admin Professional 8.3



SYSTEM AUTHORIZATION	
AUTHORITY: Executive Order 10450, 9367, and Public Law 96-354	Field Name: Page1 usersign - Unsigned
PRINCIPAL PURPOSE: To record names, signatures, and other identifiable access to Department of Defense (DOD) system and/or paper form.	<input checked="" type="checkbox"/>
ROUTINE USES: None	Field Name: Page1 supvsign - Unsigned
DISCLOSURE: Disclosure of this information is voluntary; however, consent is required for processing of this request.	<input checked="" type="checkbox"/>
TYPE OF REQUEST: <input type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATE <input checked="" type="checkbox"/> USER1	
SYSTEM NAME (Platform or Application): IPERMS	
PART 1 (To be completed by Requestor)	Field Name: Page1 ownersign - Unsigned
1. NAME (Last, First, Middle Initial)	2. YR
SOLDIER, JOE I	YO
3. OFFICE SYMBOL/DEPARTMENT	4. T
YOUR PARENT UIC	
5. OFFICIAL EMAIL ADDRESS	6. 2
YOUR ENTERPRISE EMAIL ADDRESS ONLY	YO
7. OFFICIAL MAILING ADDRESS	8. 3
YOUR OFFICIAL WORK ADDRESS	
10. TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS <input type="checkbox"/> I have completed Annual Information Awareness Training.	Field Name: Page2 sec mgr sign - Unsigned
11. USER SIGNATURE	<input checked="" type="checkbox"/>
USER DIGITAL SIGNATURE	<input checked="" type="checkbox"/>
PART 2 - ENDORSEMENT OF ACCESS BY INFORMATION OWNER US (contactor - provide company name, contract number, and date of contract)	Field Name: Page2 procsign - Unsigned
22. AUTHORIZATION FOR ACCESS: THE BELOW MUST BE ON YOUR DD 2875 ACCEPTABLE USE STA: Personally Identifiable Information (PII) contained in IPERMS is not for public use and can be made available to management agents on official need other than official duty purposes are violations of the Privacy Act which is unauthorized use or viewing of their records can result in a suspension in a violation of access and can result in the removal of IPERMS access. E a. Viewing or downloading a Soldier's AMIBIK without a mission req. b. Accessing PII for the purpose of identity theft or other extantial misa	Field Name: Page2 revalsign - Unsigned

1. Select the corresponding  icon of the part of the PDF to be digitally signed.
2. Select 'Purebred Digital Signature Certificate' from the list of certificates and then select 'ALLOW' (located at the bottom right of the screen) to complete the signing of the PDF.



Once the PDF has been successfully signed, the message 'All digital signatures are valid' will appear below the navigation ribbon.



Adding Custom Signature Fields



Digital Signature Functions

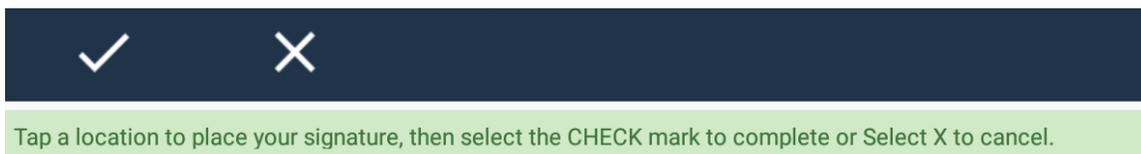
CLOSE **CREATE SIGNATURE**

Signature Title

Signature Size

PLACE SIGNATURE

1. Enter the name of the new custom signature field under ‘Signature Title’.
 - a. Note: A unique name must be used for each new custom signature field. Entering a duplicate name will replace the pre-existing custom signature field.
2. Select a size of the new custom signature field based on the user’s desired preference. The sizes range from the following:
 - a. Small
 - b. Medium
 - c. Large
3. Select ‘Place Signature’ once the size of the new custom signature field has been selected, the user will be taken back to the PDF to place the location of the signature.
4. Tap the area of the PDF that the new custom signature will be placed.
 - a. Note: the user can use his/her finger to scroll up/down the PDF and to find the location to place the signature.
5. Select the CHECK MARK as shown below in the navigation ribbon to confirm the placement of the new custom signature. Select X to cancel this function.



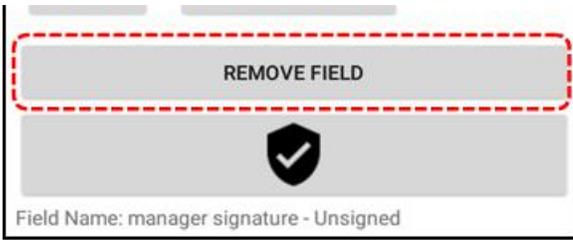
Upon completion, a gray box with the text ‘SIGN HERE’ will appear in the selected location.



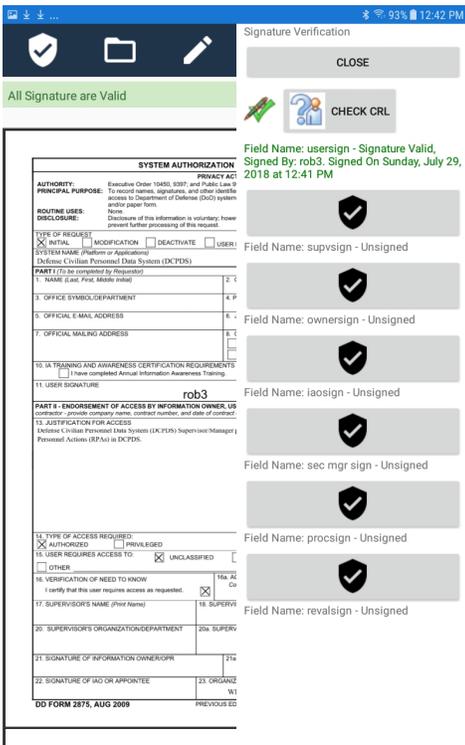
Once the new custom signature field has been added, the user may sign it using the steps in the ‘Signing’ section of this help guide. Alternatively, the user may send the unsigned document with the new custom signature field to another user to sign.

Removing Unsigned Custom Signatures Fields

After selecting the  icon on the navigation ribbon, select ‘REMOVE FIELD’ on a right-side menu for the appropriate custom signature field. This will remove the custom signature field from the PDF.



Continue Signing



To continue signing other areas of the PDF, select the  icon and complete steps 1-2 from the previous section for each additional digital signature.

Once a signature field has been signed, it will appear with  and the metadata of the digital signature (see image to the right). In addition, it will provide the user the option to conduct a Certificate Revocation List (CRL) check on the digital signature.

Signature Verification



To perform a Certificate Revocation List (CRL) check on a signature, select the

 icon from the navigation ribbon to bring up the right-side menu that lists all areas of the PDF that can accept a digital signature.

Next, select 'Check CRL' to validate a signature. If a signature is valid, 'CRL Check: SUCCESS' will appear below the navigation ribbon.

Note:



- If a document does not have a digital signature field, when the user selects the  icon, the right-side menu will display the message 'No Signatures available in this document?'. 
- CRL checks fail on self-signed certificates as they are inherently considered untrustworthy as they are directly trusted as a trust anchor.

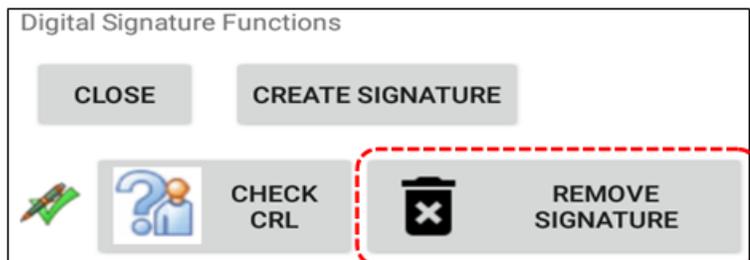
Invalid Signatures

If the MDS Application detects an invalid signature on the PDF due to an expired or revoked certificate, the message 'Signature problems exist' will be displayed on the navigation ribbon. If the user selects the 'sign' icon, the right-side menu will appear, and the invalid signature will not have  nor will the user be able to conduct a CRL check on the signature.



Removing Signatures

After selecting the  icon on the navigation ribbon, select 'REMOVE SIGNATURE' on a right-side menu for the appropriate signature field. This will remove the signature and reset the signature field.



Note: This feature will only work on signatures applied during the current session. Any PDFs signed in a prior session or by another user cannot be removed.

Viewing Digital Certificate Properties

MDS allows users to view the X.509 digital certificate properties for all digital signatures that are placed on a document being viewed. To use this function, open the Digital Signature Function menu and select 'More Details' for the corresponding digital signature.








Field Name: Page1 usersign - Signature Valid, Signed By: rob3. Signed On 12/23/2018 07:41:53-05:00

Selecting ‘More Details’ will provide the properties for the digital certificate that was used to make the digital signature that is represented on the document. The following scrollable screen is displayed when ‘More Details’ is selected and provides various details for the digital certificate used to make the digital signature.

Digital Signature Functions




All digital signatures are valid





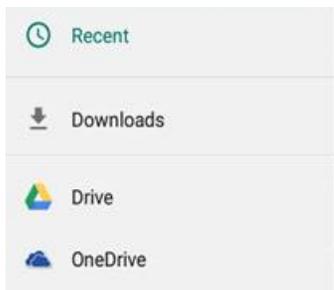

Certificate Details CLOSE

Version	3
Signature algorithm	sha256RSA (1.2.840.113549.1.1.1)
Subject	E=rob@rob.com, O=myorg, CN=rob3
Issuer	E=rob@rob.com, O=myorg, CN=rob3
Serial number	00A5A05285D4F3A2C4D 50A890B092B4C74
Validity Starts	5/29/2018 5:30:41 PM
Validity Ends	5/29/2019 5:32:21 PM
Key usage	EncipherOnly, CrlSign, KeyCertSign, DataEncipherment, KeyEncipherment, DigitalSignature
CRL distribution points	
SHA1 Digest	2B65FB5E1334A6F820CF A35AE7E0BEE8D2F8E995
MD5 Digest	1F5A593BD34110DDA83 51909FB38DBC5
X.509 data	308203773082025FA003 020102021100A5A05285 D4F3A2C4D50A890B092 B4C74300D06092A86488 6F70D01010B0500303B3 10D300B06035504030C0 4726F6233310E300C060

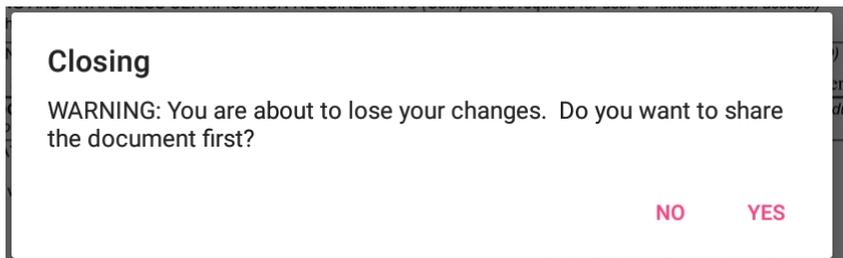
Select ‘Close’ to return to the previous screen.

Open folder 

Selecting the  icon allows users to access PDFs stored locally on the device or in cloud storage (i.e. Google Drive, OneDrive, Dropbox, etc.).



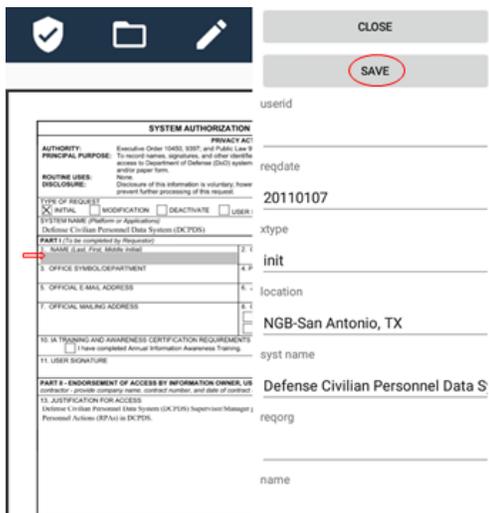
Note that MDS will prompt you to SHARE the document that is currently opened within the application if you select the OPEN function, this is to prevent loss of any modifications that have been made to the current document as the application does not save documents.



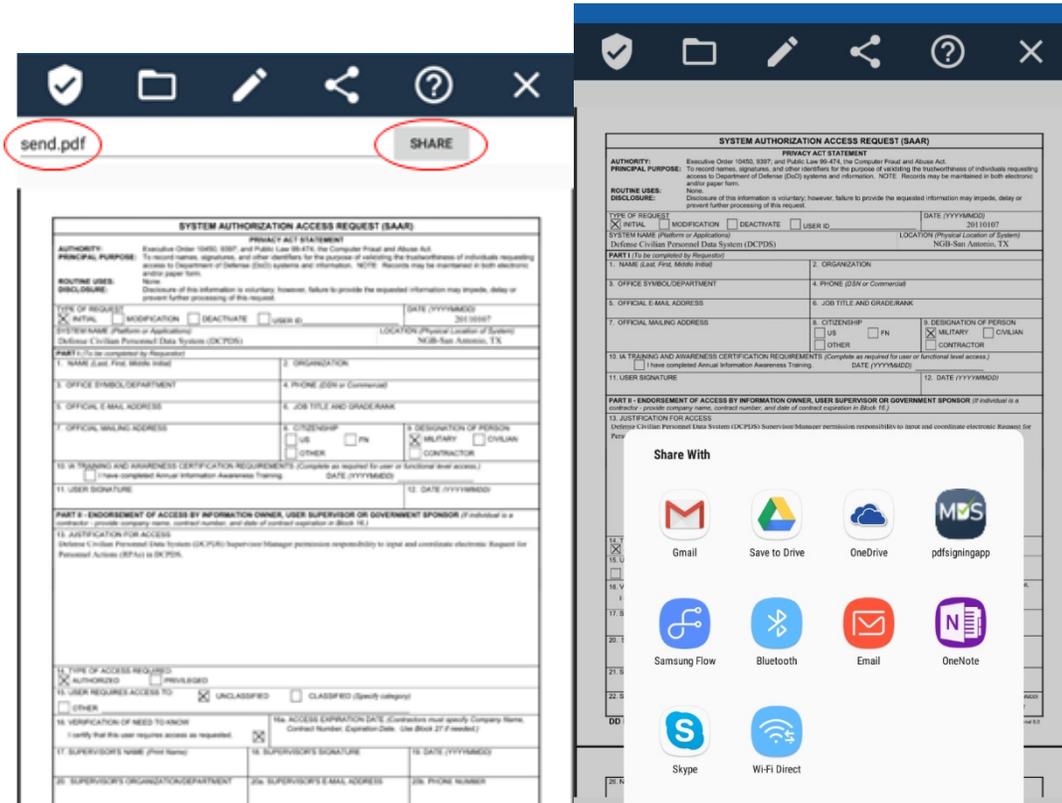
Selecting 'Yes' when prompted will provide the option to SHARE the document. Selecting 'No' will proceed with the OPEN function, thus removing the current document from the application, when another document is selected.



Selecting the  icon allows the user to add text to editable field of the document. Once the user selects the  icon, a right-side menu will appear displaying all editable areas of the PDF. The user can add text to the editable area by selecting the corresponding field on the right-side menu (note: the area being edited will be shaded in grey). Once complete, the user selects 'SAVE' to capture the changes made to the PDF. Note that selecting 'DONE' on the keyboard will also save the changes made; after which you can select 'CLOSE' to return to the unobstructed view of the document.



After selecting the  icon, the user will be prompted with the option to change the name of the PDF file before exporting it. Once the user enters the desired name, then selecting ‘Share’ will bring up the menu of share options.



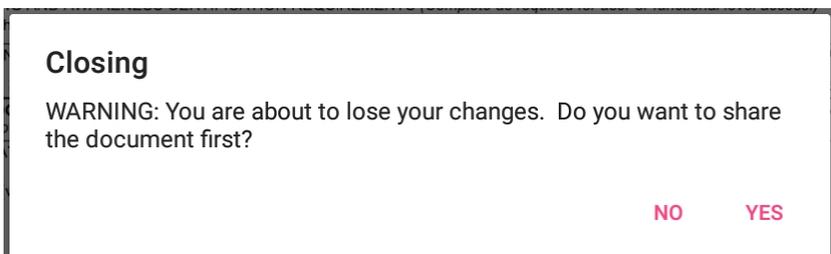
HELP GUIDE

Selecting this icon will open the help guide.

CLOSE PDF

Selecting this icon will close the open PDF and return the user back to the MDS Application’s welcome screen.

Note that MDS will prompt you to SHARE the document that is currently opened within the application if you select the CLOSE function, this is to prevent loss of any modifications that have been made to the current document as the application does not save documents.



Selecting ‘Yes’ when prompted will provide the option to SHARE the document. Selecting ‘No’ will proceed with the CLOSE function, thus removing the current document from the application, when another document is selected.

MDS Android Help Guide

[Click here to see this page in full context](#)

The DoD Mobility User Corner is accessible from this URL:
https://disa.deps.mil/ext/cop/dod_mobility/SitePages/Home.aspx