CoSign Mobile App

Version 7.5

Administrator Guide

Notice

This manual contains information that is proprietary to ARX (Algorithmic Research) Ltd. No part of this manual may be reproduced in any form whatsoever without prior written approval by ARX (Algorithmic Research) Ltd.

ARX (Algorithmic Research) Ltd. reserves the right to revise this publication and make any changes without obligation to notify any person of such revisions and changes.

For further information, contact ARX (Algorithmic Research) Ltd.

Trademarks

CoSign Central Enterprise, CoSign Central FIPS, CoSign Web App, MiniKey, and CryptoKit are trademarks of ARX (Algorithmic Research) Ltd. Other names are trademarks or registered trademarks of respective owners and are used solely for identification purposes.

ARX (Algorithmic Research) Ltd, Tel. 1-866-EASY-PKI (327-9754) Site: www.arx.com

CoSign Mobile App – Admin Guide
Pub. Date 10.15
Pub. No. CSN.WBAPP.INS.USR V7.5.10.15

Table of Contents

Chapter 1: Overview

Over the last four decades, the biggest challenge of IT departments in many organizations was moving to a paperless work environment. Seemingly, there was tremendous success in this regard. Today, most transactions in the business world are performed electronically:

- Documents are written using word processing programs.
- Messages are sent via email.
- Inventories and purchases are tracked using Enterprise Resource Planning (ERP) systems.
- Medical information is stored in Electronic Medical Record (EMR) systems.

Although these transactions are performed in a paperless environment, organizations have still not managed to find an easy way to get rid of the paper used for data authentication (signing the authenticity of the data). Today, although organizations have invested large amounts of funds and other resources in creating paperless environments, their workers are still printing every transaction, signing it, and saving the printed copy. These organizations require a digital method for data authentication.

By moving to a viable electronic data authentication system, organizations can reduce their printing, archiving, shipping, and handling costs. In addition, better and more competitive customer service can often be provided.

Requirements for Data Authentication Systems

A viable data authentication system must meet the following specifications:

- Security – The system must ensure that no one other than the data creator can tamper with or change the data in any way.
- Third-party validation – The system must enable any third party to validate the authenticity of the data. If a dispute arises between the parties (the data creator and recipient), any third party must be able to validate the data authenticity in order to settle the dispute.
- System independence – Data authentication must be independent of the system that created the data. Users must be able to validate the authenticity of the data using a known standard that is independent of any specific system.
- Validation over time – Users must be able to validate data authenticity at any point in time. Authenticity cannot expire at any point.

Currently, the only data authentication method known to support all of these requirements is the Public Key Infrastructure (PKI) method of authenticating data, simply called “digital signatures”.

Introduction to CoSign

CoSign is a PKI-based, off-the-shelf digital-signature solution that can be integrated with a wide range of applications. In this way, CoSign enables organizations to embed digital signatures in various documents, forms, and transactions. CoSign is a turnkey, hardware-based solution that is easily and quickly deployed in the network and provides cost-effective digital-signature capabilities for the organization.

CoSign includes all the components needed for PKI-based digital-signature deployment. You do not need to install any other device or integrate any other component for the system to work.

Environments Supported by CoSign

CoSign integrates with leading user management systems, including Microsoft Active Directory and a variety of LDAP (Lightweight Directory Access Protocol) based directories, such as IBM Tivoli. This integration ensures no overhead in managing the digital-signature system and signature credentials (i.e., the private keys that are needed in a PKI environment), solving one of the main problems of legacy digital-signature systems. System managers, network managers, and end-users can continue to use the IT infrastructure in the same manner as before CoSign was installed.

CoSign stores the signature credentials in a secure server, ensuring that the signer has exclusive access to his or her signature credentials, while still maintaining a centrally managed solution. This is necessary in order to fulfill the security requirement of the data authentication system.

Another option is to use the CoSign Cloud service. An organization can register its users to the service and thus enable them to digitally sign content without having to deploy the CoSign appliance on the organizational premises.

Applications that Work with CoSign

An increasing number of applications can work with CoSign as their digital-signature layer without needing any further integration, including:

- Microsoft Office 2007/2010/2013 (Word and Excel)
- Microsoft InfoPath 2007/2010/2013
- Adobe Acrobat

- Microsoft SharePoint 2007/2010/2013
- XML
- TIFF files
- Word Perfect
- Microsoft Outlook and Outlook Express
- Adobe Server forms (for signing web forms)
- AutoCAD
- Lotus Notes
- Microsoft BizTalk
- FileNet eForms
- Verity Liquid Office
- ERP systems (e.g., SAP)
- OpenText
- Oracle
- Crystal Reports
- Web applications
- Any application that has a *print* option can use CoSign to generate a PDF file and sign it.
- For information on using CoSign with other applications, contact ARX technical support.

CoSign Components

CoSign includes the following components:

- **CoSign appliance** – The CoSign appliance hardware and software, connected to the organization's network.
- **Client** – The CoSign Client software, installed on the users' computers.
- **Administrator** – The CoSign Administrative software that includes the CoSign Microsoft Management Console (MMC) snap-in, installed on the administrative computer.
- **CoSign Connector for SharePoint** – This connector enables adding digital signature functionality to documents managed by Microsoft SharePoint, or using digital signatures within any workflow procedure that is based on Microsoft SharePoint.

- **CoSign Web App** – This application is deployed in the Microsoft Web Server of the organization and enables users to sign documents without installing any client component. CoSign Web App can use either the local CoSign appliance or the CoSign Cloud environment for performing digital signature operations. Applications can interact with the CoSign Web App and add a digital signature to documents using a web based interface.
- **CoSign Mobile App –** This mobile application, which can be installed on Android-based devices or Apple iOS devices, enable users to sign documents using their mobile devices.
  The mobile devices interface directly with the CoSign appliance via a CoSign RESTful interface.
  The CoSign Mobile App can interface with either the CoSign Cloud, the organizational CoSign appliance, or CoSign's Trial system.
- **CoSign Cloud** – A CoSign Cloud-based application that provides digital signature services to users who register for the services. The CoSign Cloud supports single users as well as groups of users.
- **CoSign Signature APIs** – Developers can use local and network APIs to integrate their applications with CoSign Central appliances and the CoSign Cloud service.

CoSign Guides

CoSign documentation includes the following guides:

- *CoSign Administrator Guide* – Provides all the information necessary for an administrator to install and manage the CoSign appliance in the various environments in which CoSign can operate.
- *CoSign User Guide* – Provides all the information necessary for an end user to use CoSign. Includes information about special add-ins for various applications such as Microsoft Office.
- *CoSign Connector for SharePoint User Guide* – Provides all the information necessary for implementing and using the CoSign Connector for SharePoint.
- *CoSign Web App User Guide* – Provides all the information necessary for deploying CoSign Web App in the organization's environment.
- *CoSign Signature APIs Developer's Guide* – Provides all the information necessary for a developer to integrate their application with CoSign.
- *CoSign Mobile App Administrator Guide* – Provides all the information necessary for deploying the CoSign Mobile app.

Intended Audience

This guide is intended for administrators wishing to deploy the CoSign Mobile app. It is assumed that readers have prior knowledge of CoSign.

Organization of this Guide

This guide is organized as follows:

- *Chapter 1: Overview* – Provides an overview and introduction to CoSign.
- *Chapter 2: Introduction to the CoSign Mobile* App – Provides an introduction to the CoSign Mobile app.

- *Chapter 3: Installing and Setting up the CoSign Mobile* App – Describes how an end user installs and sets up the CoSign Mobile app.
- *Chapter 4: Using the CoSign Mobile App for Signing and Validating* Documents – Describes how an end user signs a document, validates a signature, and manages end-user signatures and settings.
- *Chapter 5: Deployment Issues in CoSign Central Environment* – Describes how administrators can enable end-users to operate their CoSign Mobile app using the organizational CoSign appliance.
- *Appendix A: Supported Devices* – Lists the devices supported by the CoSign Mobile app.
- *Appendix B: End User License Agreement* – Displays the CoSign Mobile app software license agreement.

Chapter 2: Introduction to the CoSign Mobile App

About the CoSign Mobile App

Using the CoSign Mobile app, users can digitally sign and validate documents using their mobile devices.

The CoSign Mobile app supports the following document types:

- PDF files.

Note:

- The PDF file must be no larger than 30 MB.
- Password-protected PDF files are not supported yet.

The CoSign Mobile app is supported both by iOS and by Android devices. For a full list of supported OS versions, refer to Supported Devices.

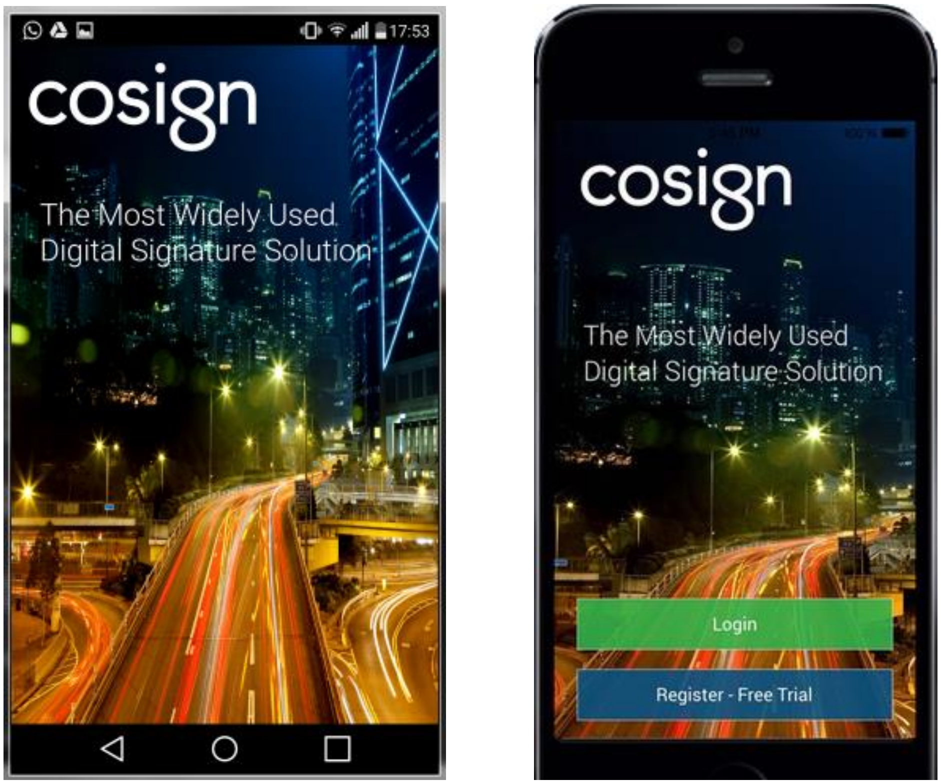


Figure 1 CoSign Mobile App (left - Android; Right – iOS)

Note: For the sake of convenience, most of the screens appearing in this guide are Android screens, but similar functionality is offered in iOS devices.

Chapter 3: Installing and Setting up the CoSign Mobile App

CoSign Mobile App End-user Installation

The CoSign Mobile app can be deployed on Apple devices (such as iPhone, iPAD) or Android devices (such as Samsung Galaxy, Nexus, etc.).

Downloading from the App Store (iOS)

To download from the App Store:

- Go to the following link: https://itunes.apple.com/us/app/cosign-secure-digital-signing/id932750932?ls=1&mt=8
- Or scan the bar code on the right:

Downloading from Google Play (Android)

To download from Google Play:

- Go to the following link: https://play.google.com/store/apps/details?id=com.arx.cosignapp
- Or scan the bar code on the right:

CoSign Mobile App Initial End-user Setup

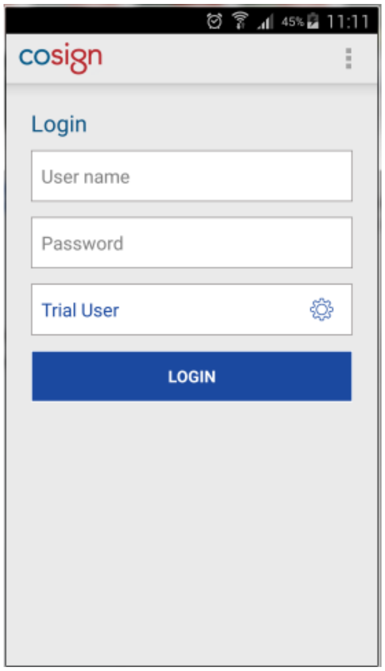
During initial login, the end user specifies which of the following CoSign environments to use by default for the signature signing and verifying operations:

- CoSign Trial
- CoSign Cloud
- CoSign Central - A specific CoSign Appliance that is installed in the organization or at a specific service provider.

The instructions for end-user initial setup are as follows:

Launch the CoSign Mobile app CoSign.

The following Login screen appears, with the **CoSign Trial** option selected by default.



Login

User name

Password

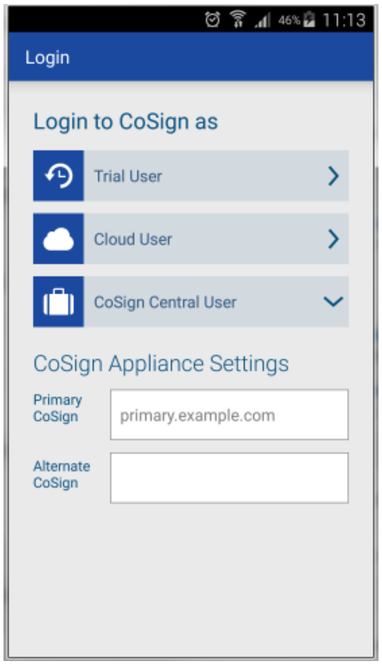
Trial User

Figure 2 CoSign Mobile App Initial Login screen

If CoSign Trial is the desired environment, enter your **User name** and **Password**, and press **Login**.

If the desired environment is CoSign Cloud or CoSign Central:

a. Click the cogwheel icon ⚙ adjacent to **Trial User** (see Figure 2). The following screen appears.



Primary CoSign: primary.example.com

Alternate CoSign:

Figure 3 Selecting the Default CoSign Environment

b. If the desired environment is CoSign Cloud, select **Cloud User**. The Login screen appears (see Figure 4), displaying the **Cloud User** option. Enter the **User Name** and **Password**, and press **Login**.

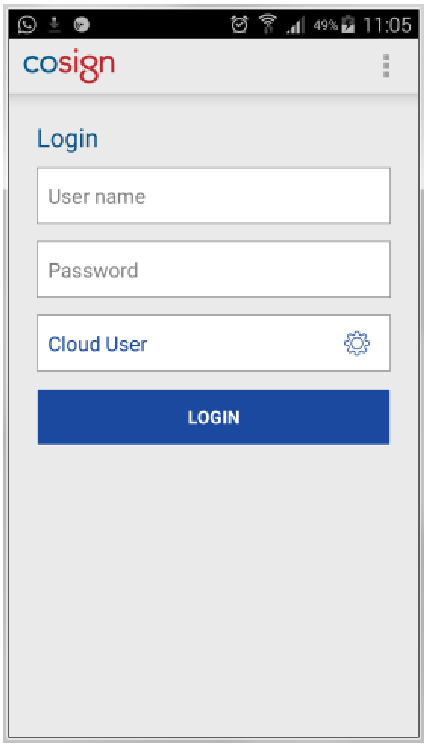


Figure 4 Login screen for CoSign Cloud Environment

c. If the desired environment is CoSign Central, press **CoSign Central User** (see Figure 3), and specify the DNS name of the primary CoSign appliance and the DNS name of the alternate CoSign appliance.

The CoSign Mobile app attempts to connect to the primary and alternate appliances. Upon success, the Login screen appears, with the CoSign Central User option selected. Enter the **User Name** and **Password**, and press **Login**.

Note that if CoSign is deployed in an Active Directory environment, you must enter in the **User name** field your Active Directory User ID and domain in the following email format: <Active Directory user ID>@<domain name>.

Changing the Default CoSign Environment

The end-user can change the default CoSign environment at any time.

To do so, the end-user must perform the following:

1. Logout from the CoSign Mobile app by accessing the CoSign Mobile app drawers menu, and selecting **Logout**.

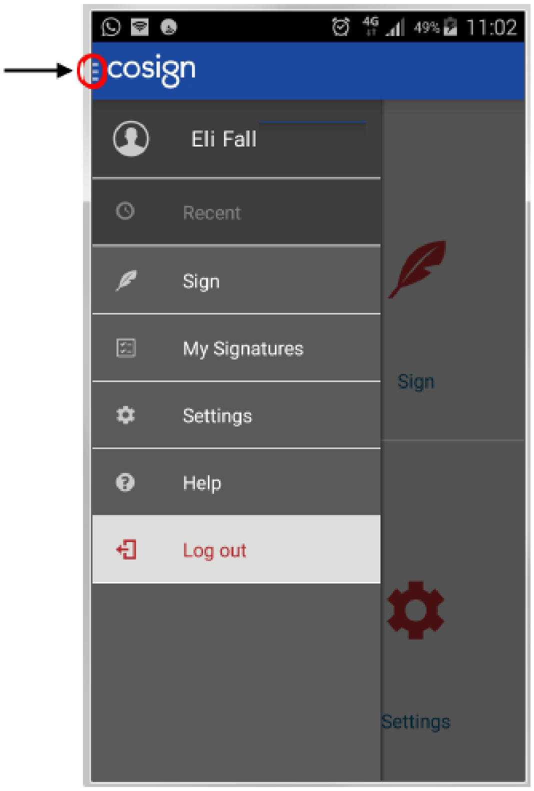


Figure 5 CoSign Mobile App Menu

2. Launch the CoSign Mobile app.

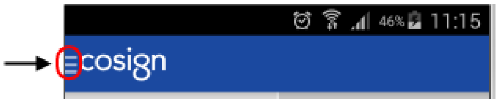
3. In the Login page that appears, follow the procedure described in *CoSign Mobile App Initial End-user Setup*.

Chapter 4: Using the CoSign Mobile App for Signing and Validating Documents

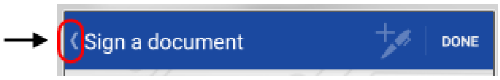
Accessing the Main Options

To access the CoSign Mobile app main options, the end user should do as follows:

1. In the CoSign Mobile app, press the drawers icon at the top of the screen.



> ***Note***: If the drawers icon is not visible press the Back button until the drawers icon is visible



The CoSign Mobile app menu appears.

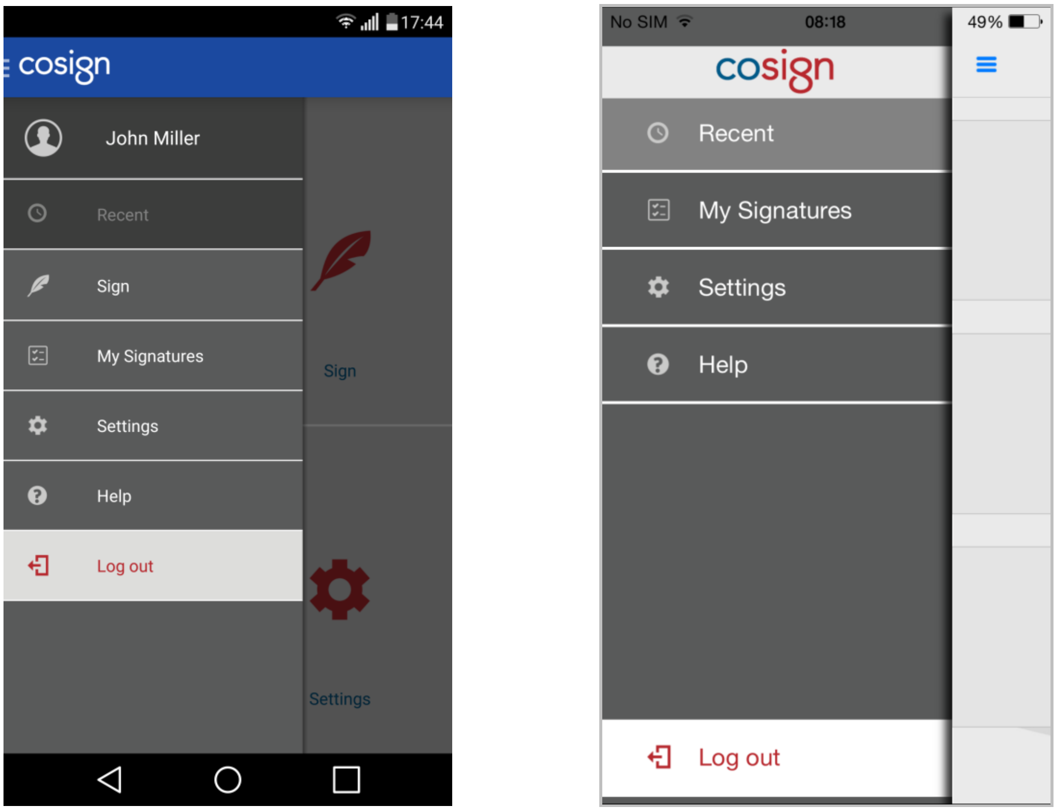


Figure 6 CoSign Mobile App Menu (Left – Android; Right – iOS)

2. You can, if you wish, continue to the main page, as follows:

- In Android deivces, press the name of the user.
- In iOS devices, press the CoSign logo.

The CoSign Mobile app main page appears.

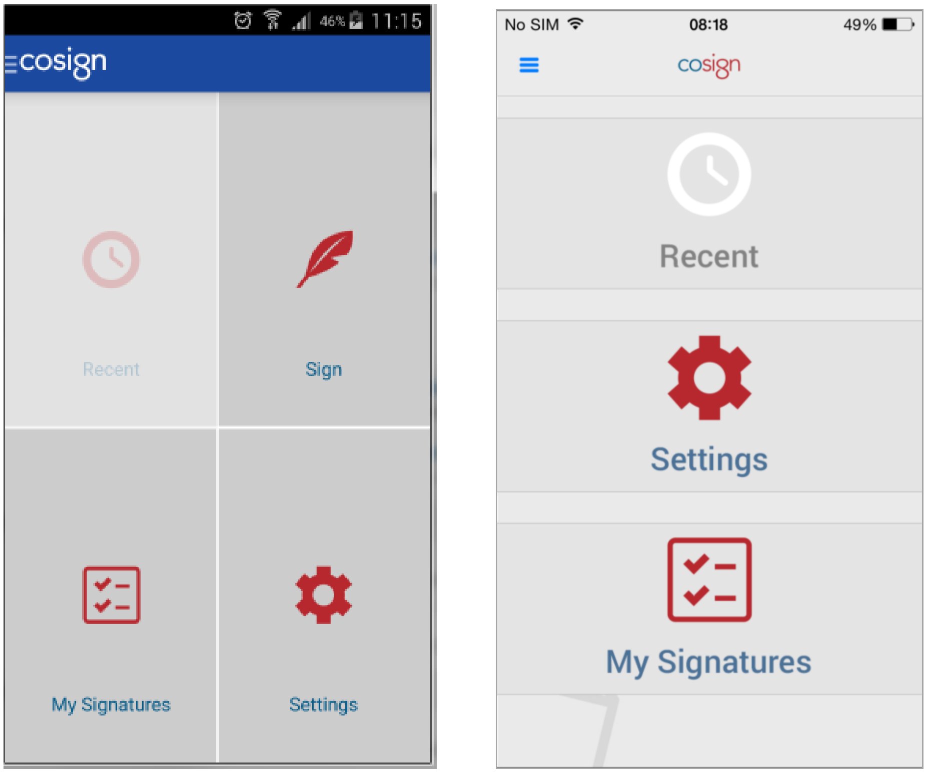


Figure 7 CoSign Mobile App Main Page (left - Android; Right – iOS)

Signing a Document

The end-user signing process is as follows:

1. Open a PDF document.

   Note that the PDF can be attached to an email, loaded locally from the device (relevant only for Android devices), loaded from cloud file storage providers such as Box or Dropbox, or accessed via another application.

2. Select from the menu either **Share** > **CoSign Mobile App** (for Android devices) or **Open In** > **CoSign Mobile App** (for iOS devices).

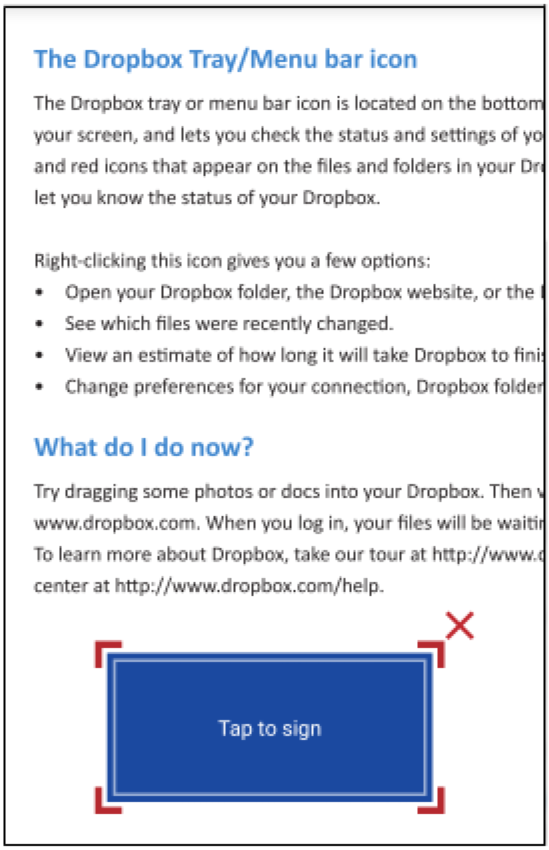
   Or

   For Android devices only – open the drawers menu as described in

   , press **Sign**, and browse to the desired PDF document.

3. You can Sign existing empty signature fields in the document, and/or Create and Sign new signature fields in the document.

    - To create a new digital signature field, long-tap the desired area in the document or uses the toolbar's "plus" icon. You can edit the location, size and shape of the signature field (as indicated by the red handles).



The Dropbox Tray/Menu bar icon

The Dropbox tray or menu bar icon is located on the bottom your screen, and lets you check the status and settings of yo and red icons that appear on the files and folders in your Dr let you know the status of your Dropbox.

Right-clicking this icon gives you a few options:

- Open your Dropbox folder, the Dropbox website, or the
- See which files were recently changed.
- View an estimate of how long it will take Dropbox to fini
- Change preferences for your connection, Dropbox folder

What do I do now?

Try dragging some photos or docs into your Dropbox. Then www.dropbox.com. When you log in, your files will be waiti To learn more about Dropbox, take our tour at http://www. center at http://www.dropbox.com/help.

Figure 8 Creating a New Signature Field

- To sign an existing field, tap it once. Note that the field's location, size and shape and are fixed (as indicated by the blue handles).

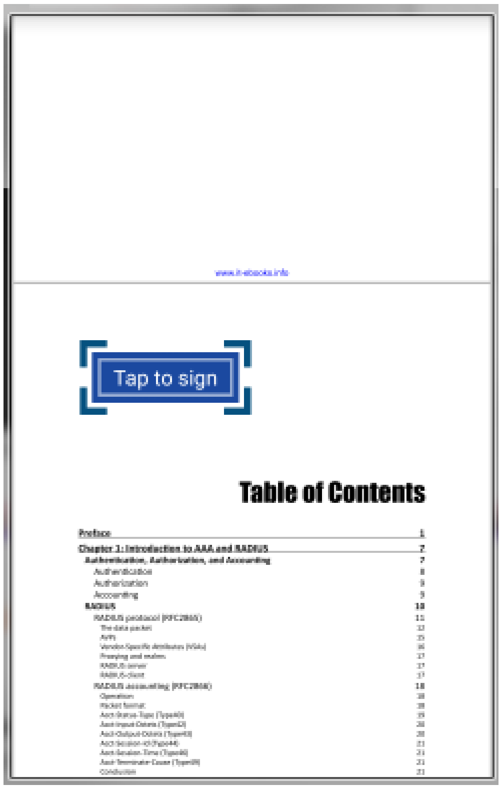
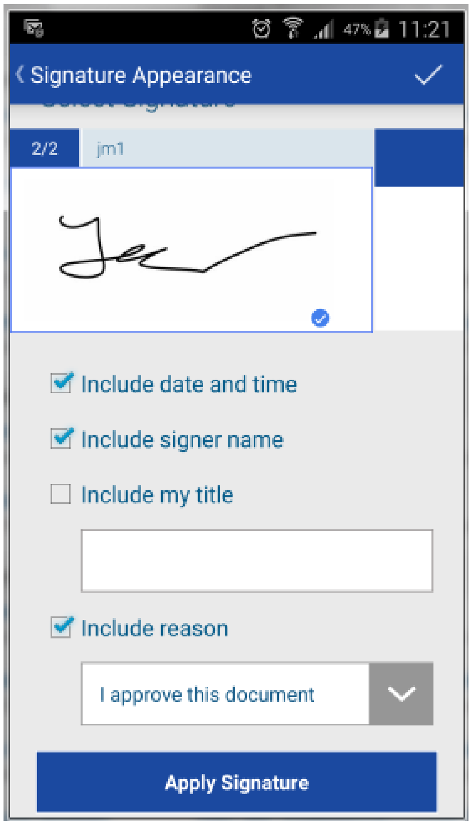


Table of Contents

Figure 9 Signing an Existing Signature Field

4. The app collects additional information from you, and accesses your account via the RESTful HTTPS protocol.



☑ Include date and time

☑ Include signer name

□ Include my title

☑ Include reason

I approve this document

Figure 10 Signature Information

5. Click Apply Signature.

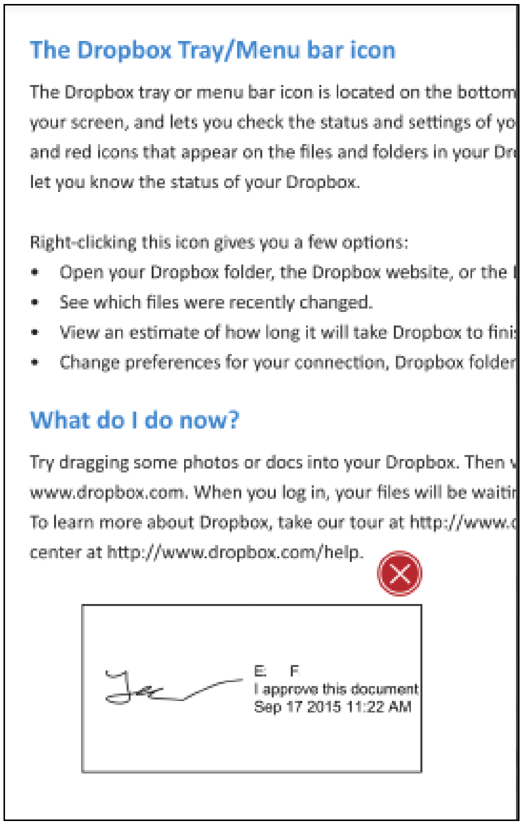
6. The PDF is signed digitally as follows:

   a. The Cosign Mobile app uploads the entire PDF document to the CoSign appliance.

   b. The document is digitally signed inside the CoSign appliance,

   c. The digital signature is sent back to the Cosign Mobile app.

The signature is displayed in the mobile device.



The Dropbox Tray/Menu bar icon

The Dropbox tray or menu bar icon is located on the bottom
your screen, and lets you check the status and settings of yo
and red icons that appear on the files and folders in your Dr
let you know the status of your Dropbox.

Right-clicking this icon gives you a few options:

- Open your Dropbox folder, the Dropbox website, or the
- See which files were recently changed.
- View an estimate of how long it will take Dropbox to fini
- Change preferences for your connection, Dropbox folder

What do I do now?

Try dragging some photos or docs into your Dropbox. Then
www.dropbox.com. When you log in, your files will be waiti
To learn more about Dropbox, take our tour at http://www.
center at http://www.dropbox.com/help.

E F
I approve this document
Sep 17 2015 11:22 AM

Figure 11 Example of a Signed Document

7. After finalizing the signature operation, you can either send the signed PDF using email or keep the signed file in the cloud storage system.
In an Android device, the file can be kept in the user's local device.

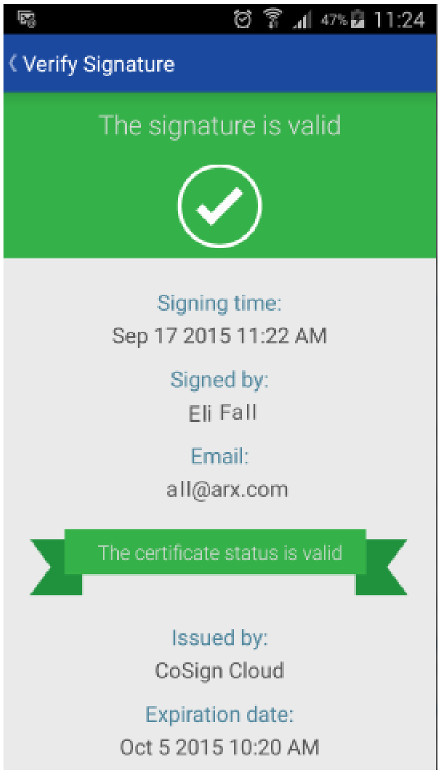
Validating an Existing Signature

A user can validate existing signatures in a signed PDF document.

To do so, the user should perform the following:

- Open a signed PDF, and press the signature (see Figure 11).

If the signature is valid, a screen similar to the following appears:



The signature is valid

Signing time:
Sep 17 2015 11:22 AM

Signed by:
Eli Fall

Email:
all@arx.com

The certificate status is valid

Issued by:
CoSign Cloud

Expiration date:
Oct 5 2015 10:20 AM

Figure 12 Valid Signature Indication

Managing Graphical Signatures and User Settings

An end-user can also manage his/her graphical signatures and other user settings. To do so:

1. Access the CoSign Mobile app main menu, as described in

2. :

To manage user signatures, press **My Signatures**. The My Signatures screen appears.

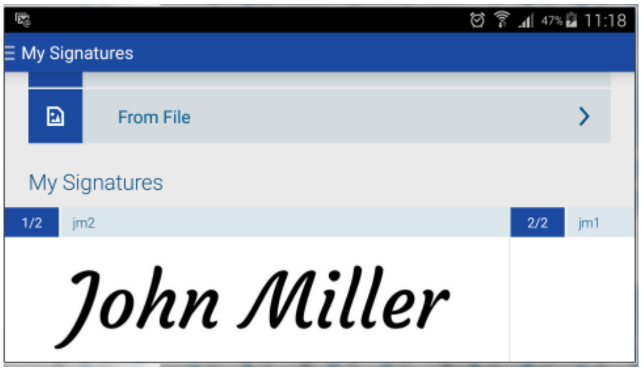
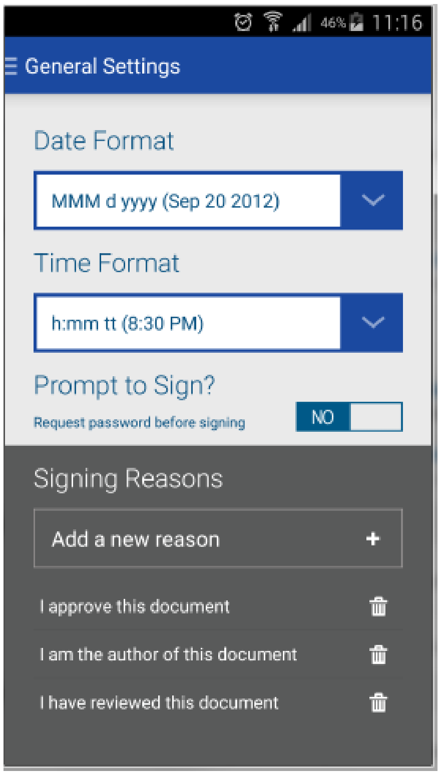


Figure 13 Managing User Signatures

3. To set user settings, press **Settings**. The General Settings screen appears.



General Settings

Date Format

MMM d yyyy (Sep 20 2012)

Time Format

h:mm tt (8:30 PM)

Prompt to Sign?

Request password before signing

NO

Signing Reasons

Add a new reason +

I approve this document

I am the author of this document

I have reviewed this document

Figure 14 Managing General Settings

Chapter 5: Deployment Issues in CoSign Central Environment

This chapter describes how administrators can enable end-users to operate their CoSign Mobile app using the organizational CoSign appliance.

Enabling the CoSign RESTful Service

The CoSign Mobile app interfaces with the CoSign appliance for a variety of operations such as digital signature operation, retrieval of the end user's graphical signatures, etc.

The interface is based on *CoSign Signature* – CoSign's RESTful web network API. This interface is described in detail in the *CoSign Signature* section of the *CoSign Signature APIs Developer's Guide*.

To enable the CoSign RESTful service, you must set the **RESTful Web Services Support** system parameter to **True**, as explained in the *Changing CoSign System Parameters* section in chapter 5 of the *CoSign Administrator Guide.*

Note: The minimal CoSign version that supports the RESTful API is CoSign v7.4.

Enabling Network Connectivity

CoSign's RESTful web network API is based on the HTTPS protocol (HTTP over TLS/SSL security channel) on port 8081.

To ensure connectivity between the mobile device and the organizational CoSign appliance, pay special attention to the following:

- Make sure the routing definitions enable TCP/IP connectivity.
- Make sure all firewalls between the users' mobile devices and the CoSign Appliance allow HTTPS communication between the mobile devices and the CoSign appliance on port 8081.
- Make sure the CoSign Appliance has a DNS name such as CoSign.company.com. Note that this name will also appear as the Common Name in the TLS/SSL server certificate, discussed in the following section.

If network connectivity is established between the mobile device and the CoSign appliance, any usages of VPNs, proxies, etc. should work.

Obtaining and Uploading a RESTful TLS/SSL Server Key and Certificate

CoSign's RESTful interface is shipped with a default key that can be used only for limited demo purposes. To use CoSign's RESTful interface in production:

1. Contact a well-known and World Wide Verifiable Certificate Authority that can issue a TLS/SSL server certificate.

   Note that as part of the TLS/SSL secured session, the mobile device communicates with the CoSign appliance for the purpose of creating a secure channel using the TLS/SSL protocol. The mobile device's operating system inspects the TLS/SSL server certificate and if it is valid, the mobile device establishes a secure session.
   One of the important validations performed by the mobile device is ensuring that the TLS/SSL server certificate was given by a trusted CA which appears in the mobile device's trust store. It is therefore important to get a certificate from a recognized and well known Certificate Authority.

   The output of the process is a file in PKCS#12 format that includes both the TLS/SSL server key and a certificate. This file is secured by a password.

Upload the TLS/SSL server key and certificate file as described in the *Uploading an SSL Certificate* section in chapter 5 of the *CoSign Administrator Guide*.

> **Note:**
>
> There may be cases where a user is required to upload the certificates chain of all certificates representing the hierarchy of CAs between the ROOT CA certificate and the RESTful TLS/SSL Server certificate.
> Please contact ARX for help if you need to upload the certificate chain to your CoSign appliance.
>
> To do so, follow the instructions in the *Renewing the subordinate CA Certificate* section in chapter 5 of the *CoSign Administrator Guide*.
> Essentially, the user should use the > > option in the ARX CoSign Appliance Management window to load each of the intermediate certificates in the chain.
>
> In some rare cases, a user may be required to upload the ROOT CA certificate. Again, use the > > option in the ARX CoSign Appliance Management window to upload the ROOT certificate.

Performance Consideration

As part of the signing process, the entire PDF document is compressed by the CoSign Mobile app and sent to the CoSign Appliance for the purpose of digital signature operation. The reply from the appliance contains only the digital signature, which the CoSign Mobile app applies to the entire document.

Note that the compression action may cause performance issues when signing very large documents.

Special Configurations of the CoSign Appliance

Any special configuration of the CoSign Appliance affects also the CoSign Mobile app.
For example, if extended authentication is required for every digital signature operation (that is, the **Prompt For Sign** system parameter is set to **True**), then the CoSign Mobile app will accordingly require the end user to provide an extended password for any digital signature operation.

Appendix A: Supported Devices

The following table lists the devices supported by the CoSign Mobile app.

Device	OS Version
Nexus 5	4.4.2/5.0.1
iPhone 5	7.1.1/7.1.2/8.1
iPhone 5S	7.1.1/7.1.2/8.1
Nexus 7	4.4.4
iPad Air	7.1.2/8.1.2
Nexus 10	4.4.4
Samsung Tab 2	4.1.2
Samsung Note 3	4.4.2
Samsung Galaxy S3	4.3
Samsung Galaxy S4	4.4.2
Samsung Galaxy S5	4.4.2
Samsung SM-T325	4.4.2
iPad Mini	7.1
Samsung Galaxy S4 mini	4.2.2
LG G3	4.4.2
IPAD Air Cell	8.1
SONY XPERIA Z2 Tablet (Cell)	4.4.2
iPhone 6	8.1.2
iPhone 6 Plus	8.1.2

Appendix B: End User License Agreement

COSIGN® MOBILE APP

SOFTWARE LICENSE AGREEMENT

NOTICE TO USER: This Software License Agreement ("Agreement') is a legal agreement between you and ARX, Inc. regarding use of the Software (defined below) that accompanies this Agreement. BEFORE YOU INSTALL OR USE THE SOFTWARE, CAREFULLY READ THE TERMS OF THIS AGREEMENT. BY CLICKING THE "ACCEPT" BUTTON IN THE INSTALLER, INSTALLING OR USING THE SOFTWARE, YOU ARE AGREEING TO BE BOUND BY, AND ARE BECOMING A PARTY TO, THIS AGREEMENT, INCLUDING THOSE TERMS THAT APPLY TO THIRD PARTY SOFTWARE, IF ANY, THAT ACCOMPANY THIS SOFTWARE. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, (i) DO NOT INSTALL OR USE THIS SOFTWARE, AND (ii) DESTROY OR DELETE ALL COPIES IN YOUR POSSESSION, IF ANY. THIS AGREEMENT IS ENFORCEABLE AGAINST YOU AND ANY LEGAL ENTITY ON WHOSE BEHALF IT IS USED.

ARX permits you to use the Software only in accordance with the terms of this Agreement.

1. Software. "Software" means all of the contents of the files, including, but not limited to, related explanatory written materials or files (“Documentation”), which are delivered during the installation process that is contemporaneous with your acceptance of this Agreement, and all future updates to these files. The term “Software” also includes any software licensed by ARX from third parties for distribution under this Agreement (“Third Party Software”).

2. Software License. This is a license and not a sale of the Software. For the duration of the Term, ARX grants to you a personal, revocable, non-exclusive, non-transferable, limited copyright license to install and use the Software solely in connection with the ARX CoSign Cloud service (the “Service”), in accordance with the Service’s terms and conditions which are located at https://cloud.arx.com and ARX CoSign Central solutions, including any trials of these products and services (collectively the “CoSign Solutions”).

3. Intellectual Property Ownership, Copyright Protection. ARX and its licensors have exclusive ownership of all right, title and interest in the Software, and all intellectual property incorporated therein and any authorized copies that you make. The Software’s structure, organization and code are the valuable trade secrets and confidential information of ARX and its licensors. The Software is protected by law, including, without limitation, the copyright laws of the United States and other countries, and by international treaty provisions. Except as expressly stated herein, this Agreement does not grant you any intellectual property rights in the Software, or any component thereof, and all rights not expressly granted are reserved by ARX and its Licensors. If you are acting on behalf of a business, organization or entity of any kind, you agree that you will, within 30 days of a

request by ARX's representative, fully document and certify that your use of the Software complies with this Agreement.

4. Restrictions. You will not copy any portion of the Software, except to make a back-up copy that is not installed or used on any device that can run the Software. Any copy of the Software that you make, in whole or in part, must contain the same copyright and other proprietary notices that appear on or in the Software, and the accompanying Documentation. You will not: (a) modify, adapt, merge, translate, or create any derivative works of any portion of the Software; (b) reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of any portion of the Software except to the extent you may be expressly permitted to decompile under applicable law; (c) remove or destroy any copyright notices or other proprietary markings; or (d) rent, lease, sell, loan, sublicense, assign or otherwise transfer your rights in the Software, or authorize all or any portion of the Software to be copied onto another user's computer except as may be expressly permitted herein.

5. Feedback. If you provide any feedback to ARX concerning the functionality or performance of the Software (including identifying potential errors and improvements) ("Feedback"), you hereby assign to ARX all right, title, and interest in and to the Feedback, and ARX is free to use the Feedback without any payment or restriction.

6. Term and Termination. This Agreement will be effective upon installation of the Software, and shall expire on the earlier of: (i) expiration or termination of your license to access and use the CoSign Solutions; or (ii) 90 days from the date of commercial release of any subsequent version of the Software. Notwithstanding anything to the contrary herein, ARX may (at its sole discretion) terminate this license in the event of your failure to comply with any term of this Agreement. ARX's rights and your obligations will survive the termination of this Agreement. Upon termination of this Agreement, if requested by ARX, you will certify in writing to ARX that all copies of the Software, and all portions thereof, have been deleted from any and all computer libraries or storage devices in your possession.

7. No Warranties And Limited Remedy. All components of the Software are provided "AS IS" and without any warranties of any kind whatsoever. ARX does not warrant that use of the Software will be error-free, without defects or malicious code, or that it will meet your requirements. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, ARX DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, NONINFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE. You assume all responsibility for selection of the Software for your intended use. In the event of any claim or objection concerning the Software, your sole and exclusive remedy shall be to discontinue its use and delete all copies in your possession.

8. Limitation Of Liability. ARX and its Licensors shall not be liable to you for any damages, claims or costs of any kind whatsoever, including any consequential, indirect, incidental or exemplary damages, lost profits or any lost savings (collectively "Losses"), even if an ARX representative has been advised at any time of the possibility of such Losses. ARX's aggregate liability, including that of its Licensors, shall be limited to the amount paid by you for the Software, if any. The foregoing limitations and exclusions apply to the extent permitted by applicable law in your jurisdiction and, to the extent they are inconsistent with

such law they shall be deemed amended by the minimum amount necessary to bring them into compliance.

9. Indemnification. You will indemnify, hold harmless, and defend ARX (including all of its officers, employees, directors, subsidiaries, representatives, affiliates, and agents) and ARX's Licensors from and against any damages (including attorneys' fees and expenses), claims, and lawsuits that arise or result from your use of the Software or your breach of this Agreement.

10. Export Rules. You may not export or re-export the Software without (a) the prior written consent of ARX; and (b) complying with applicable export control laws and obtaining all necessary permits and licenses.

11. Governing Law, Jurisdiction and Arbitration. Except for the right of ARX to apply to a court of competent jurisdiction for a temporary restraining order, a preliminary injunction, or other equitable relief to preserve the status quo or prevent irreparable harm, any dispute as to the interpretation, enforcement, breach, or termination of this Agreement will be resolved by binding arbitration in San Francisco, California, in accordance with the California Code of Civil Procedure by one arbitrator appointed in accordance with said Code. The prevailing party will be entitled to receive from the other party its attorneys' fees and costs incurred in any arbitration and all related proceedings. The federal and state courts having jurisdiction over disputes arising in the City of San Francisco, California, shall be the exclusive venue for all other proceedings, and you waive any objection to this venue on the grounds of inconvenience or lack of personal jurisdiction. This Agreement will be governed by and construed in accordance with the substantive laws in force in the State of California as it applies solely to its citizens and without regard to any principles of conflict of laws.

12. Privacy Policy: The Privacy Policy at http://www.arx.com/misc/privacy-policy/ governs any personal information you provide to us. By using this Software you agree to the terms of this Privacy Policy.

13. General Provisions. If any part of this Agreement is found void and unenforceable, it shall be deemed severable and will not affect the validity of the remaining provisions of this Agreement, which shall remain valid and enforceable according to its terms. This Agreement may only be modified by a writing signed by an authorized officer of ARX. Updates may be licensed to you by ARX with additional or different terms. This is the entire agreement between ARX and you relating to the Software, and it supersedes any prior representations, discussions, undertakings, communications or advertising relating to the Software.

14. Notice to U.S. Government End Users. The Software and Documentation are "Commercial Items," as that term is defined at 48 C.F.R.§2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights

as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States.

15. Third Party Software. The Software is distributed with Third Party Software which is governed by the terms of this License. This Third Party Software includes PDF technology powered by the PDFNet Mobile SDK copyright © by PDFTron™ Systems Inc., 2001-2014, and distributed by ARX, Inc. under license. All rights reserved.
    All Third Party Software may be used solely with the Software, and all use of the Third Party Software on a stand-alone basis is strictly prohibited.

SCHEDULE 3.2

List of Open Source Software used by Licensor in development of the PDFTron Software

1. FreeType Project under the "FreeType License": http://freetype.sourceforge.net/license.html (The FreeType License Agreement is specifically located at: http://freetype.sourceforge.net/FTL.TXT)

   The Patent Issues section is located at http://freetype.sourceforge.net/patents.html) which describes patents related to various aspects of font technology. The Software does not rely upon any software code that may infringe on these patents. The Software expressly excludes all modules related to hinting and rendering.

2. LibPNG:http://www.libpng.org/pub/png/src/libpng-LICENSE.txt

3. ZLib: http://www.zlib.net/zliblicense.html

4. LibTiff: http://www.libtiff.org/misc.html

   The Software does not use the LZW algorithm published in LibTiff. Furthermore, the LZW patent has expired as at June 20, 2003 in any event.

5. LibJPEG: http://dev.w3.org/cvsweb/Amaya/libjpeg/README?rev=1.2

6. AGG v.2.4 under the "Anti-Grain Geometry Public License":

   Anti-Grain Geometry - Version 2.4

   Copyright (C) 2002-2004 Maxim Shemanarev (McSeem)

   Permission to copy, use, modify, sell and distribute this software is granted provided this copyright notice appears in all copies. This software is provided "as is" without express or implied warranty,