Software Version 2.1.01
Version 1.0

Xerox® Mobile Link App

Information Assurance Disclosure

Contents

1. Introduction

Xerox® Mobile Link Solution is a Workflow Solution that connects a corporation mobile workforce to new productive ways of scanning. Scanning is easy and convenient from any mobile device without needing standard drivers and cables.

1.1. Purpose

The purpose of the IAD is to disclose information for the Xerox® Mobile Link Solution with respect to device security. Device security, in this context, is defined as follows:

1. How scan jobs are received, accessed, and transmitted.
2. How data is stored and transmitted.
3. How the product behaves in a networked environment.
4. How the product may be accessed, both locally and remotely.

This document describes design, functions, and features of the Xerox® Mobile Link Solution relative to Information Assurance (IA).Please note that the customer is responsible for the security of their network and the Xerox® Mobile Link Solution does not establish security for any network environment.

The purpose of this document is to inform Xerox customers of the design, functions, and features of the Xerox® Mobile Link Solution relative to Information Assurance (IA).

This document does not provide tutorial level information about security, connectivity or Xerox® Mobile Link Solution features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these types of topics.

1.2. Target Audience

The target audience for this document is Xerox field personnel and customers concerned with IT security.

It is assumed that the reader is familiar with the Xerox® Mobile Link Solution; as such, some user actions are not described in detail.

1.3. Disclaimer

The content of this document is provided for information purposes only. Performance of the products referenced herein is exclusively subject to the applicable Xerox Corporation terms and conditions of sale and/or lease. Nothing stated in this document constitutes the establishment of any additional agreement or binding obligations between Xerox Corporation and any third party.

2. Product Description

The workflow of Xerox® Mobile Link scanning is quite simple. A user using a mobile device, such as a smart phone or tablet, scans a document from a Xerox MFP to the mobile device. Once scanned, the document is stored on the mobile device, sent to email or a cloud repository, faxed, sent to a printer or any combination of up to four of these options without any further user action required.

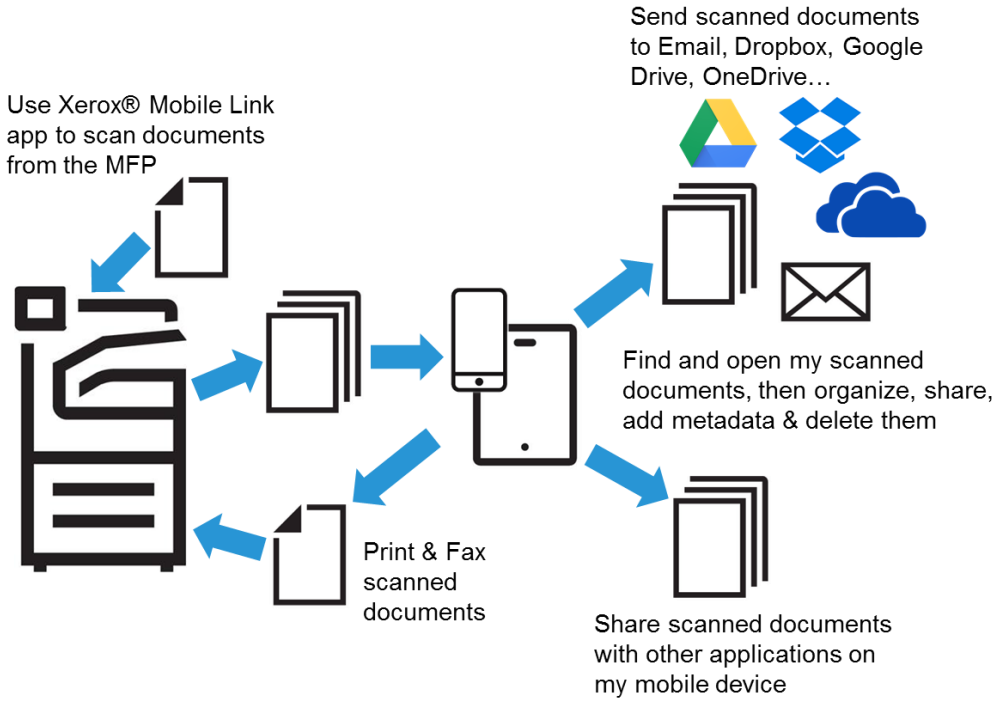

Figure 2.1-1: High Level Document Flow

2.2. Component Diagram

The architecture of the Xerox® Mobile Link app incorporates technical controls to eliminate, where possible, information security risk from all information assets including software components, connected system components, and information owners. The Xerox® Mobile Link Architecture illustrates the relationship between the Xerox® Mobile Link app and these other system components.

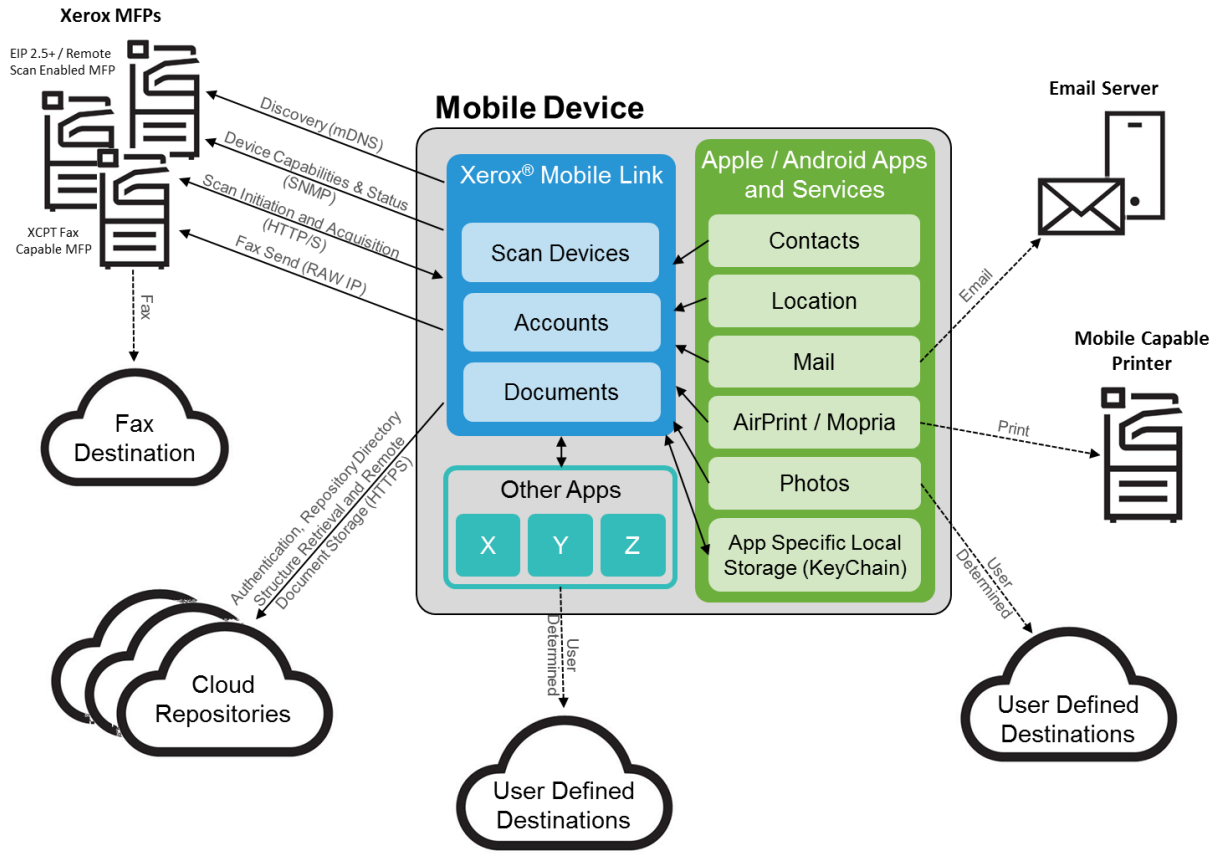

Figure 2.2-1: Component Diagram

2.3. Description of System Components

Component	Description
Mobile User	End user using an iOS or Android device with the Xerox® Mobile Link App.
Xerox® Mobile Link App	Mobile Phone application that allows the user to find printers, initiate scan jobs and receive and transmit the scan output images.
Mobile Link Local Storage	Local storage on the mobile device allocated to the Mobile Link App. Includes: • Multi-function Device List • Email and Fax Accounts • Scanned Documents • Cloud Repository Accounts
OS Provided Services and Data Stores	Mobile Link makes use of: Contacts, Location, Camera and Photos on the mobile device. Permission must be granted by the user to use these services.
Other Apps	The Mobile Link App can import and export documents with/from other apps that are registered to handle documents output by Mobile Link.
Xerox Multi-Function Device	A Xerox device capable of performing remote scans. May also be used for print submission and faxing.
Email Server	Email Service(s) configured for use on the user's mobile phone.
Printer	Printer used for printing any previously stored job. Must support AirPrint, Mopria or other Print Service supported by the mobile device OS.

Table 2.3-1: System Components

3. System Architecture

3.1. Sub-Systems

3.1.1. Xerox® Mobile Link App

3.1.1.1. Memory Information (SoV)

Volatile Memory				
Type (SRAM, DRAM, etc.)	**Size**	**User Modifiable (Y/N)**	**Function or Use**	**Process to Clear:**
RAM	Varies	Y	Executable code, temporary storage	Power Off; Process Cleanup

Table 3.1.1-1: Xerox® Mobile Link Volatile Memory

Non-Volatile Solid State Memory				
Type (Flash, EEPROM, etc.)	**Size**	**User Modifiable (Y/N)**	**Function or Use**	**Process to Clear:**
Mobile Phone Storage	N/A	N	Images, Configuration and App Content	Deletion of App to remove Configuration and App Content. Images are manage using the phone's native apps.

Table 3.1.1-2: Xerox® Mobile Link Non-Volatile Memory

4. System Interaction

4.1. System Components

4.1.1. Xerox® Mobile Link App – Mobile Application

The Xerox® Mobile Link app is the foundational component of the Xerox® Mobile Link Scan Solution used to manage the system's behavior and user's interaction within the system from document scan to store. Xerox® Mobile Link app is an iOS / Android application running on an Apple or Android phone or tablet. Access to the Xerox® Mobile Link app will be controlled by the mobile devices authentication mechanism.

The Xerox® Mobile Link app has three primary functions.

- First, the app is responsible for providing the user with methods of discovering EIP-enabled Xerox MFPs within the customer's network, determining the printer capabilities, and relaying that information to the Xerox® Mobile Link app.
- Second, the Xerox® Mobile Link app is responsible for acquiring scanned images from these devices.
- Third, the app distributes these images to local folders, cloud repositories, printers, email users and fax recipients.

The Xerox® Mobile Link app user interface is available to all users who can log on to the mobile device. It displays the scan devices, cloud repositories and selected remote folders (but not credentials), fax numbers, and contact information added to Mobile Link by the user.

4.1.2. Xerox® Mobile Link Local Storage

The following data is stored in the Mobile Link app's assigned storage space on the mobile device. This is typical of all mobile apps. Other apps do not have access to this same space on the mobile device. The collection of stored information includes:

- Scan Device List (i.e. the Multi-Function Devices)
- Email and Fax Account Lists created within Mobile Link
- Documents routed to Mobile Link local folders
- Cloud Repository Authorization and Access information

The Mobile Link app uses the iOS / Android approved methods to encrypt and secure information stored on the device.

- If the mobile device is password protected by the user, then the Mobile Link data is encrypted and secure.
- [iOS Only] If the mobile device is NOT password protected by the user, then the Mobile Link data is NOT encrypted and can be easily accessed by connecting the

mobile device to a PC and browsing the files in a file browser. In fact, all documents from all apps using this security model are vulnerable in the same manner.

The users Scan Device List can be shared via e-mail between two devices running the Xerox® Mobile Link App. The names and IP addresses of the devices will appear in plaint text in the email attachment in a Xerox proprietary format.

4.1.2.1. Mobile Link E-mail and Fax Accounts

Mobile Link E-mail and Fax Accounts are created by the user within the app for use in One Touch Workflows. The details of these accounts are stored in the Xerox® Mobile Link assigned space and encrypted or not based on the protection set up by the user, as noted above.

4.1.2.2. Local Documents

The user can decide to share Mobile Link documents with other apps on the iPad/iPhone using the standard IOS (open in) feature.

4.1.2.3. Cloud Repository Authorization and Access Information

Xerox® Mobile Link supports nine different cloud repositories at the time this document was created. Additional repositories may be added in the future. The supported cloud repositories are Dropbox, Box, Google Drive, OneDrive, OneDrive for Business, Office 365, Evernote, SharePoint and SharePoint Online.

Dropbox – Mobile Link presents the user with a dialog from the dropbox.com site wherein they enter their Dropbox credentials (user name and password). This authentication API then provides the Mobile Link app an authorization token, allowing Mobile Link to access the user's folders and documents.

The authentication token is stored in an encrypted database as part of the app's local data. The user's actual credentials are never captured or stored by the Mobile Link App.

Box – Mobile Link presents the user with a dialog from BOX.com site wherein they enter their box credentials (user name and password). This authentication API then provides the app an ACCESS token, allowing the app to access the user's folders and documents.

The authentication token and refresh token is stored in an encrypted database as part of the app's local data (KeyChain).

The expiration time of 1 hour is stored in DB for access tokens. After 1 hour the access token is expired and using the refresh token a new access token is obtained and store in the Keychain. The user's actual credentials are never captured or stored by Mobile Link.

GoogleDrive - Mobile Link presents the user with a dialog from googledrive.com site wherein they enter their Google credentials (user name and password). This

authentication API then provides the app an ACCESS token, allowing the app to access the user's folders and documents.

The authentication token and refresh token is stored in an encrypted database as part of the app's local data (KeyChain).

The expiration time of 1 hour is stored in DB for access tokens. After 1 hour the access token is expired and using the refresh token a new access token is obtained and store in the Keychain. The user's actual credentials are never captured or stored by Mobile Link.

OneDrive – Mobile Link presents the user with a dialog from OneDrive.com site wherein they enter their OneDrive credentials (user name and password). This authentication API then provides the app an ACCESS token, allowing the app to access the user's folders and documents.

The authentication token and refresh token is stored in an encrypted database as part of the app's local data (Key Chain).

The expiration time of 1 hour is stored in DB for access tokens. After 1 hour the access token is expired and using the refresh token a new access token is obtained and store in the Keychain. The user's actual credentials are never captured or stored by Mobile Link.

OneDrive for Business - Mobile Link presents the user with text fields from our app wherein they enter their OneDrive for Business credentials (user name, password & Base url). This authentication API then provides the app a Security token & Cookies allowing the app to access the user's folders and documents.

The Base URL and Username provided by the user is stored in the Database (CoreData). The password is stored in the Keychain. Once authenticated, the app gets the security token & expiration time (1 Day) which is stored in the DB. The security token is used to retrieve cookies that are used for subsequent requests and it is stored in the DB.

Office 365 – Mobile Link presents the user with text fields from our app wherein they enter their Office 365 for Business credentials (user name, password & Base url). This authentication API then provides the app a Security token & Cookies allowing the app to access the user's folders and documents.

The Base URL and Username provided by the user is stored in Database (CoreData). The password is stored in the Keychain. Once authenticated we get the security token & expiration time (1 Day) which is stored in the DB. The security token is used to retrieve cookies that are used for subsequent requests and it is stored in the DB.

Evernote – Mobile Link presents the user with a dialog from the evernot.com site wherein they enter their Evernote credentials (user name and password). This

authentication API then provides the Mobile Link app an authorization token, allowing Mobile Link to access the user's folders and documents.

The authentication token is stored in an encrypted database as part of the app's local data. The user's actual credentials are never captured or stored by the Mobile Link App.

SharePoint - Mobile Link presents the user with text fields from our app wherein they enter their SharePoint credentials (user name, password & Base url). This authentication API then provides the app a Security token & Cookies allowing the app to access the user's folders and documents.

The Base URL and Username provided by the user is stored in the Database (CoreData). The password is stored in the Keychain. Once authenticated, the app gets the security token & expiration time (1 Day) which is stored in the DB. The security token is used to retrieve cookies that are used for subsequent requests and it is stored in the DB.

SharePoint Online - Mobile Link presents the user with text fields from our app wherein they enter their SharePoint Online credentials (user name, password & Base url). This authentication API then provides the app a Security token & Cookies allowing the app to access the user's folders and documents.

The Base URL and Username provided by the user is stored in the Database (CoreData). The password is stored in the Keychain. Once authenticated, the app gets the security token & expiration time (1 Day) which is stored in the DB. The security token is used to retrieve cookies that are used for subsequent requests and it is stored in the DB.

4.1.3. OS-Provided Services/Data Stores

The Xerox® Mobile Link App may acquire data from the following services/data stores provided by the OS on the mobile device:

- Contacts
- Location
- Camera

The Xerox® Mobile Link App may acquire data from and write data to the following services/apps provided by the OS on the mobile device:

- Photos

The user is asked to grant/deny permission to access these services/data stores the first time the Xerox® Mobile Link app needs to use them. The user can change the decision to grant/deny permission through Settings on their mobile device. Access to each of these services/data stores is managed individually.

4.1.4. Interaction with Other Installed Apps

Through the iOS provided Share capability, the Mobile Link app can import (Share In) or export (Share Out) documents with/from other apps that are registered to handle the document types supported by Mobile Link (pdf and jpeg). A similar capability exists in Android. Once imported, docs are stored in the local store as above. Once exported, the security, control and management of that document is dictated by the capabilities of the app to which the document was exported.

4.1.5. Multi-Function Devices and Printers

The Xerox® Mobile Link app can interact with any Xerox Extensible Interface Platform® multi-function device connected to your network. In addition, it can use any AirPrint, Mopria or Xerox Print Service enabled printer which is visible on your network, in order to execute its print capabilities.

Xerox Extensible Interface Platform® (EIP)

Xerox multifunction devices introduce a flexible Xerox proprietary platform called EIP. This platform acts as a secure embedded web service that other applications can leverage to expose functionality and services to the user through the local control panel interface. Xerox® Mobile Link uses this platform to determine device capabilities and status and acquire scan images.

Simple Networking Management Protocol (SNMP)

Xerox multifunction devices could also be discovered through Simple Networking Management Protocol. SNMP exposes data in the form of variables on the managed systems organized in a management information base (MIB) which describe the system status and configuration. Xerox® Mobile Link would query and manipulate these variables to get device information.

Fax Sending

The Mobile Link app uses Xerox MFPs to send faxes as print jobs using a proprietary job ticket header. Jobs are submitted using RAW IP over port 9100.

4.1.6. Mobile User

The mobile user is an end-user attempting to scan a document using the Xerox® Mobile Link app running on a mobile device. It is assumed that the client's security policy and systems have already authorized the user to access and use corporate resources (e.g. network, multi-function device).

4.1.7. Email Server

The Xerox® Mobile Link app will make use of the email client and services configured on the mobile phone in order to send the following using either Contacts designated by the user or Email Addresses specifically added to the Local Storage of the Mobile Link App.

- Scanned Documents
- Shared Devices

5. Logical access, network protocol information.

5.1. Protocols and Ports

The following table shows the protocols and typical port numbers used in the Mobile Link app:

Protocol (Ports)	Protocols / Ports
HTTP (port 80)	Device Discovery, Capabilities and Status; Scan Acquisition (Android)
HTTPS (443)	Cloud Repository Access; Scan Acquisition (iOS)
mDNS (port 5353)	Device Discovery
RAW (port 9100)	Fax Job Submission
SNMP (port 161)	Device Information and Status

Table 5.1-1: Protocols and Ports

The Xerox® Mobile Link app relies on OS-provided and user-managed/installed services to route data for e-mail and print (AirPrint, Mopria, Xerox Print Service, etc.).

Emails submitted from the Xerox® Mobile Link app by a user's mobile device or computer will use the security mechanism defined by the user's email client. User documents are the primary data transmitted via email from the Xerox® Mobile Link app. It is the user's responsibility to ensure appropriate email security controls are in place. Emails generated by the Xerox® Mobile Link app typically contain scanned documents and images.