Xerox® Mobile Print Cloud

Information Assurance Disclosure

Software Version 3.1

March 2016

702P03595

BR14700

Content

1 Introduction

A Xerox Workflow Solution that connects a mobile workforce to new productive ways of printing. Printing is easy and convenient from a mobile device without needing drivers and cables.

1.1 Purpose

The purpose of this document is to disclose information for the Xerox® Mobile Print Cloud with respect to system security. System Security, for this paper, is defined as follows:

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

Please note that the customer is responsible for the security of their network. The Xerox® Mobile Print Cloud product 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 Print Cloud relative to Information Assurance (IA).

This document does NOT provide tutorial level information about security, connectivity, Print Definition Languages (PDLs), or Xerox® Mobile Print Cloud 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.

1.3 Disclaimer

The information in this document is accurate to the best knowledge of the authors, and is provided without warranty of any kind. In no event shall Xerox Corporation be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this document including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox Corporation has been advised of the possibility of such damages

2 System Workflows

The workflow of mobile printing is quite simple. A user using a mobile device such as a smart phone, tablet, or laptop sends a document to the Xerox® Mobile Print Cloud. Depending on the submission method, the job is either printed without any further user action or the user manually releases the job to print.

There are several methods for a mobile user to submit or release a job to print. The Submission method is technically decoupled from the release method. However, certain submission/release pairs make more sense than other pairs.

Submission methods:

1. E-mail
2. Print Portal Application (i.e., an App on a mobile device)

Release methods:

1. Printing device UI (via EIP)
2. Print Portal Application (i.e., an App on a mobile device)

Combined methods

(i.e., job will print without any explicit user action after submission):

1. E-mail
2. Print Portal App (i.e., an App on a mobile device)
3. Web Portal (web browser interface to Xerox Mobile Print Cloud)

The common link between all submission and release methods is the Xerox® Mobile Print Cloud Solution. Documents are stored in the cloud until they are deleted or until an administrative time-out has passed.

Subsequent sections will detail the methods of submission and release using Xerox® Mobile Print Cloud.

2.1 Submission Methods

2.1.1 Email Submission Workflow

Step 1

The user selects a document to print and creates an email with that document as an attachment. The user sends the email to the Xerox® Mobile Print Cloud email address

Step 2

The Mobile Print Cloud Solution receives the incoming email submissions. The documents are held in the Mobile Print Cloud Solution for later release at the Xerox MFP.

Step 3

The Mobile Print Cloud Solution sends the user a response email letting them know that their document was accepted.

2.1.2 Mobile Print Portal Application Submission Workflow

Step 1

The user selects, and then opens a document to upload with the Xerox® Mobile Print Portal application. Using the Mobile Print Portal Application the user selects the upload option.

Step 2

The document is uploaded to the Xerox® Mobile Print Cloud Solution.

2.2 Release Methods

2.2.1 Print Device UI Release Workflow

Step 1

The user enters their credentials at the MFP, selects which documents to print, and the required print options (duplex, stapling, number of copies and B & W or color). The user then selects Print.

Hosted on Microsoft Azure Platform

Step 2

The Mobile Print Cloud Solution processes the original file, converting it to a print-ready document. If accounting information is required and the user has cached data for the printer or print queue, the system automatically supplies the cached data. The Xerox® Mobile Print Solution routes the print-ready document to the MFP.

Step 3

The Xerox® Mobile Print Cloud Agent retrieves the print-ready document.

Step 4

The user receives their printed document.

2.2.2 Print Portal Application Release Workflow

Step 1

The user opens the Xerox® Mobile Print Portal application. They then select the uploaded document from within the App and select the required print options (e.g. duplex, stapling, and number of copies and B & W or color). The user then selects Print.

Hosted on Microsoft Azure Platform

Step 2

The Xerox® Mobile Print Cloud Solution converts the original document to a print ready format and routes it to the selected printer.

Step 3

The Xerox® Mobile Print Cloud Agent retrieves the print-ready document.

Step 4

User receives their printed document.

2.3 Combined Methods

2.3.1 Mobile Application User Workflow

Step 1

The user selects, and then opens the document to print with the Xerox® Mobile Print Portal application. Using the Mobile application the user selects the desired printer or print queue and print options. The user supplies a Secure Print passcode and/or accounting information, if required, then selects Print.

Hosted on Microsoft Azure Platform

Step 2

The document is uploaded to the Xerox® Mobile Print Cloud service for conversion to a print-ready document.

Step 3

The Xerox® Mobile Print Cloud Agent retrieves the print-ready document.

Step 4

The Xerox® Mobile Print Cloud Agent routes the print-ready document to the selected printer or print queue.

Step 5

If Secure Print is required on the printer, the user enters the passcode to release the document for printing. The user collects the printed document.

2.3.2 Email User Workflow

Step 1

The user selects a document to print and forwards it to the Xerox® Mobile Print Cloud email address.

Email workflow to the Cloud (not a specific printer) is not available for unregistered users. Unregistered users may only access printers configured to accept anonymous email printing.

Hosted on Microsoft Azure Platform

Step 2

The Xerox® Mobile Print Cloud solution receives incoming email submissions. The documents are imported to the Xerox® Mobile Print Cloud service for conversion and printing. Depending on the email address sent to, the documents are delivered to the specified printer or print queue, or held in the Xerox® Mobile Print Cloud service for later release via the Xerox® Mobile Print Portal application. If accounting information is required and the user has cached data for the printer or print queue, the system automatically supplies the cached data.

If secure printing is required on the printer, an email containing an auto-generated passcode is sent to the user.

Step 3

The Xerox® Mobile Print Cloud Agent retrieves the print-ready document.

Step 4

The Xerox® Mobile Print Cloud Agent routes the print-ready document to the selected printer or print queue.

Step 5

If Secure Print is required on the printer, the user enters the passcode to release the document for printing. The user collects the printed document.

2.3.3 Web Portal User Workflow

Step 1

The user logs in to the Xerox® Mobile Print Cloud Website. Then browses their PC for a document to print, selects a printer or print queue and print options, and then prints the document. The user supplies a Secure Print passcode and/or accounting information, if required, then selects Print.

Hosted on Microsoft Azure Platform

Step 2

The Xerox® Mobile Print Cloud service uploads the document for conversion and printing.

Step 3

The Xerox® Mobile Print Cloud Agent retrieves the print-ready document.

Step 4

The Xerox® Mobile Print Cloud Agent routes the print-ready document to the selected printer or print queue.

Step 5

If Secure Print is required on the printer, the user enters the passcode to release the document for printing. The user collects the printed document.

2.4 Administrator Workflow

Step 1

The customer administrator logs in to the Xerox® Mobile Print Cloud Website. Administrators can configure account behaviors and manage users, agents and printers.

Hosted on Microsoft Azure Platform

Administrator Functions

- Manage Account Settings
- Manage Agents
- Manage Printers and Print Queues
- Manage Users
- Manage Licenses
- Manage Accounting
- Manage LDAP Authentication
- Manage Public Print
- View History

(This page left intentionally blank.)

3 Security Description

The security considerations are three-fold:

1. The security of the user's documents during transport and storage
2. The security of the customer and end user account information required by the Xerox® Mobile Print Cloud system
3. The security of the printers and print queues enabled within the system by the customer

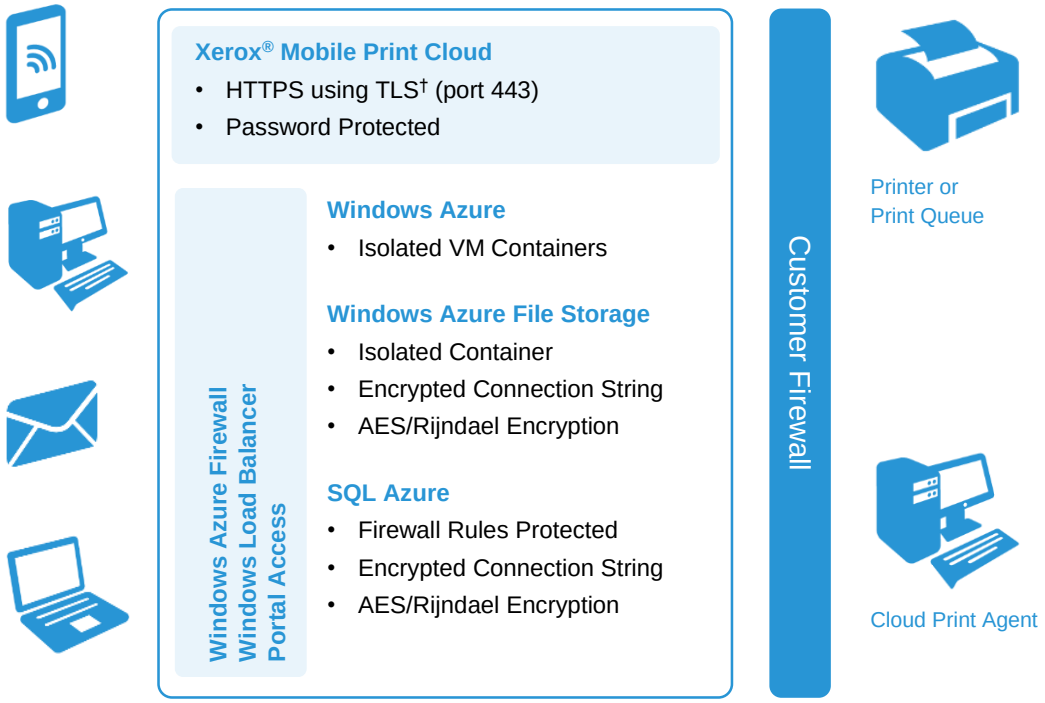
Documents and information travel through multiple system components over a combination of cellular, wired and wireless networks. All use normal, industry standard technologies and built-in security capabilities. Of course these capabilities need to be enabled, and the choice of which are used at each point in the system varies. This section captures the security considerations of Xerox® Mobile Print Cloud in the following areas:

1. Protocols and Port numbers used by the system
2. Individual system components
    a. Xerox® Mobile Print Portal – Mobile Application
    b. Xerox® Mobile Cloud Print Service
        Microsoft® Windows Azure Platform Specific
        Microsoft® Windows SQL Azure Database Specific
        Xerox Mobile Cloud Print Service Specific
    c. Xerox® Mobile Print Cloud Agent
    d. Xerox® Mobile Print Cloud – User Web Pages
    e. Xerox® Mobile Print Cloud – Customer Administrator Web Pages
    f. Printer / Print Queue
    g. Xerox® Mobile Print Cloud EIP App / Xerox® Mobile Print Cloud ConnectKey App

3. Communication between system components
    a. Communication between Xerox® Mobile Print Portal Mobile Application and Xerox® Mobile Print Cloud Service
    b. Communication between Mobile Device and Email Server
    c. Communication between Email Server and Xerox® Mobile Print Cloud Service
    d. Communication between Xerox® Mobile Print Cloud Service and Xerox® Mobile Print Cloud Agent
    e. Communication between Xerox® Mobile Print Cloud Agent and Printer or Print Queue
    f. Communication between Xerox® Mobile Print Cloud Service and Xerox® Mobile Print Public Print Service
    g. Communication between Xerox® Mobile Print Public Print Service and a Third Party Public Print Provider
    h. Communication between Xerox® Mobile Print Cloud EIP App and the Xerox® Mobile Print Cloud Service.

3.1 Xerox® Mobile Print Cloud Network Protocols and Port Numbers Diagram

This diagram shows the protocols and typical port numbers used in the system.



Print Cloud Agent Requirements and Functions	
• TCP Print 9100 (Admin settable)	• Behind Customer Firewall (if applicable)
• SNMP Port 161	• Initiates all Communications
• IPP Port 631	• Receives Job Data
• HTTPS using TLS† (port 443)	• Sends Device Data
• LPR Print 515 (Admin settable)	• Connection to LDAP
• LDAP Port 389	• Receive Print Job Data

Print Cloud @PrintByXerox App Requirements and Functions	
• HTTPS using TLS† (port 443) to Internet	• Initiates Print Conversion Requests
	• Initiates Pull-Print Request to Printer

† *Note: The use of SSLv2 and v3 has been deprecated due to security issues. The Xerox Mobile Print Cloud server uses TLS as the encryption scheme for HTTPS communication.*

3.2 Xerox Mobile Print Cloud Endpoint Table

The following endpoints, given in FQDN format, are accessed by various components of the XMPC solution that reside inside a customer's network. The customer must ensure that these components have access to the internet and in particular these specific endpoints, in order for this solution to work properly. All endpoints are accessed via HTTPS using TLS (port 443).

Component	Endpoint FQDN
Xerox Mobile Print Cloud Agent	• https://xmpcws.services.xerox.com • https://xcpagentservicebus.servicebus.windows.net • https://xcpagentservicebus01.servicebus.windows.net • https://xcpagentservicebus02.servicebus.windows.net • https://xcpagentservicebus03.servicebus.windows.net : • https://xcpagentservicebus10.servicebus.windows.net
Xerox Mobile Print Cloud EIP App – Printer App	• https://xmpceip.services.xerox.com • https://xccsts.services.xerox.com • https://xmpcws.services.xerox.com
Xerox Mobile Print Portal – Mobile App	• https://xccsts.services.xerox.com • https://xmpcws.services.xerox.com • https://publicprintapi.services.xerox.com
Xerox Mobile Print Cloud – Customer Web Pages	• https://xmpc.services.xerox.com

3.3 Individual System Components

3.3.1 Xerox® Mobile Print Portal - Mobile Application

The Xerox® Mobile Print Portal Mobile Application is the main user interface to the Xerox Mobile Print Cloud system.

The application requires users to authenticate with the Xerox® Mobile Print Cloud Service before using the application. Once authenticated, the user's credentials and authentication token are stored in the application until they log out (Please refer to the section titled "Communication between Xerox® Mobile Print Cloud Mobile Application and Xerox® Mobile Print Cloud Service" for more information about authentication and communications related security information).

Users can access their print jobs for preview and printing, locate printers and print queues but only access documents they submitted and printers or print queue to which they have been granted access. The Mobile Print Cloud Mobile Application also provides the ability to unlock a printer whose authentication is being managed by Xerox® Mobile Print Cloud.

The Xerox® Mobile Print Portal Mobile Application does not provide the capability to remotely wipe the mobile device.

It is ultimately the user's responsibility to secure their mobile device. Users can enable device level passwords and manage physical access to the device. If the mobile device is lost or stolen, the user can access the webpage to change their password making the device unable to access the Xerox® Mobile Print Cloud system.

Of special note for iOS 7.0 users. The Print Portal Mobile application uses DNS-SD (Service Discovery) and IPPS to locate printers on the local subnet. There is a bug in iOS 7.0.x which prevents the Xerox Print Portal services from being discovered and displayed in the printer list of iOS. This issue does not exist in iOS 6.0.x, and it has been fixed in iOS 7.1. It is recommended that all users with an iOS device upgrade to the latest version.

3.3.2 Xerox® Mobile Print Cloud Service

The Xerox® Mobile Print Cloud Service runs in the Microsoft® Windows Azure Platform and utilizes the SQL Azure Database for storage. There are five considerations for security based on this architecture as follows:

1. Windows Azure Platform specific security information
2. SQL Azure Database specific security information
3. Xerox® Mobile Print Cloud Service specific security
4. Xerox® Mobile Print Cloud EIP App specific security
5. Xerox® Mobile Print Cloud Service Virtual Machines

Each consideration is covered below.

3.3.2.1 Windows Azure Platform Specific

The Windows Azure Platform operates in the Microsoft® Global Foundation Services (GFS) infrastructure, portions of which are ISO27001-certified.

Windows Azure Security Highlights:

- Built-in Identity Management for administrator access
- Dedicated hardware firewall
- Stateful packet inspection technology employed
- Application-layer firewalls
- Hypervisor firewalls
- Host-based firewalls
- SSL termination / load balancing / application layer content switching
- Each deployed hosted service is segmented in its own VLAN, preventing compromised node access

Please visit the Microsoft web site for more information:
http://azure.microsoft.com/blog/2010/08/10/new-windows-azure-security-overview-white-paper-now-available/

Select Windows Azure Security Overview.

3.3.2.2 SQL Azure Database Specific

The application data is stored in a SQL Azure database. This database contains information about the printers, print queues, jobs etc.

SQL Azure is protected by two levels of security. In addition to username and password to access the database, Microsoft protects access to SQL Azure databases by allowing configuration of a whitelist of IP Addresses that can connect to the database.

Only internal Xerox IP Addresses have been configured on the whitelist for this database. Only authorized Xerox personnel have access to this data.

Passwords, Printer MAC Addresses and Printer Serial Numbers are stored in an encrypted format in the database.

3.3.2.3 Xerox® Mobile Print Cloud Service Specific

Original documents and printable documents are stored within Azure Storage. Both the original and printable documents are in an encrypted format.

Access to these documents is only available to the following:

1. The owner of the documents via the Xerox® Mobile Print Portal Mobile Application for preview.
2. Authorized Xerox personnel responsible for deployment and maintenance of the system. Since the documents are encrypted, even the authorized personnel cannot open the document to view its contents.

Each document printed follows a document retention policy which is applied to the document at the time of printing. The document retention policy is either immediate or 7 days. If set to immediate, the document is deleted immediately after printing. If the document retention policy is set to 7 days, the document is removed 7 days after printing. Therefore, documents are stored in the system for a maximum of 7 days.

Accounting information may be stored within the Azure Storage. It is stored in an encrypted format. Accounting information that can be saved is:

1. Default accounting information to be used when printing Welcome Pages to printers and print queues that require accounting information. If the administrator chooses to enter this information, it will be saved within Azure.
2. User accounting information that is entered by the user when they print a job to a printer is identified with having Xerox Network Accounting or Xerox Standard Accounting, or a print queue that is set with server-based accounting. The administrator can configure the software to allow user accounting data to be saved. The default is to not save user accounting data.

All communications to and from the Xerox® Mobile Print Cloud Service are over HTTPS using TLS (SSLv2 and v3) are not used. Documents are always transmitted securely and are protected by TLS security during upload and download.

Certificates used for encryption/decryption of documents are stored in the Windows Azure Certificate store as per Microsoft guidelines. This is a highly secure area protected by Microsoft. Account administrators can only upload certificates to this store. Downloads are not allowed. Only applications running within the same Windows Azure subscription can access the certificate.

3.3.2.4 Xerox® Mobile Print Cloud EIP App Specific

When accessing the Xerox® Mobile Print Cloud EIP App, web pages (HTML, JavaScript, icons, etc.) are served up by the Xerox® Mobile Print Cloud Service. This pathway includes the ability to provide login credentials to view and manage a user's list of jobs, including print job deletion or print initiation. This pathway also includes the ability for a Cloud Admin / System Administrator to manage some of the settings of the printer, including: Printer Enablement, Public Print Enablement, Site and Friendly Name.

All communications between the Xerox® Mobile Print Cloud EIP App and the Xerox® Mobile Print Cloud Service are over HTTPS using TLS. Certificates used for this communication path are stored in the Windows Azure Certificate store as per Microsoft guidelines.

Note: The Xerox® Mobile Print Cloud EIP App does not validate the server certificate when using TLS.

3.3.2.5 Xerox® Mobile Print Cloud Service Virtual Machines

Xerox will monitor vendor security bulletins and products update announcements, and assess what actions are required on the Azure virtual machines. These bulletins and announcements can come from Microsoft and other external vendors, as well as internal partners supplying components used in the product system. Xerox will update the virtual machines to maintain the health and integrity of the product system.

As anti-virus definition files are released more frequently than application and operating system patches, these updates will occur on a more frequent basis. Virtual machines are configured to perform full scans weekly, and update the anti-virus definition files before the full scan.

3.3.3 LDAP/Active Directory Authentication

When Company Authentication Type is enabled for LDAP Authentication, Xerox® Mobile Print Cloud will verify user credentials against Active Directory. The workplace credentials consist of Domain Name, Domain Username and Domain Password.

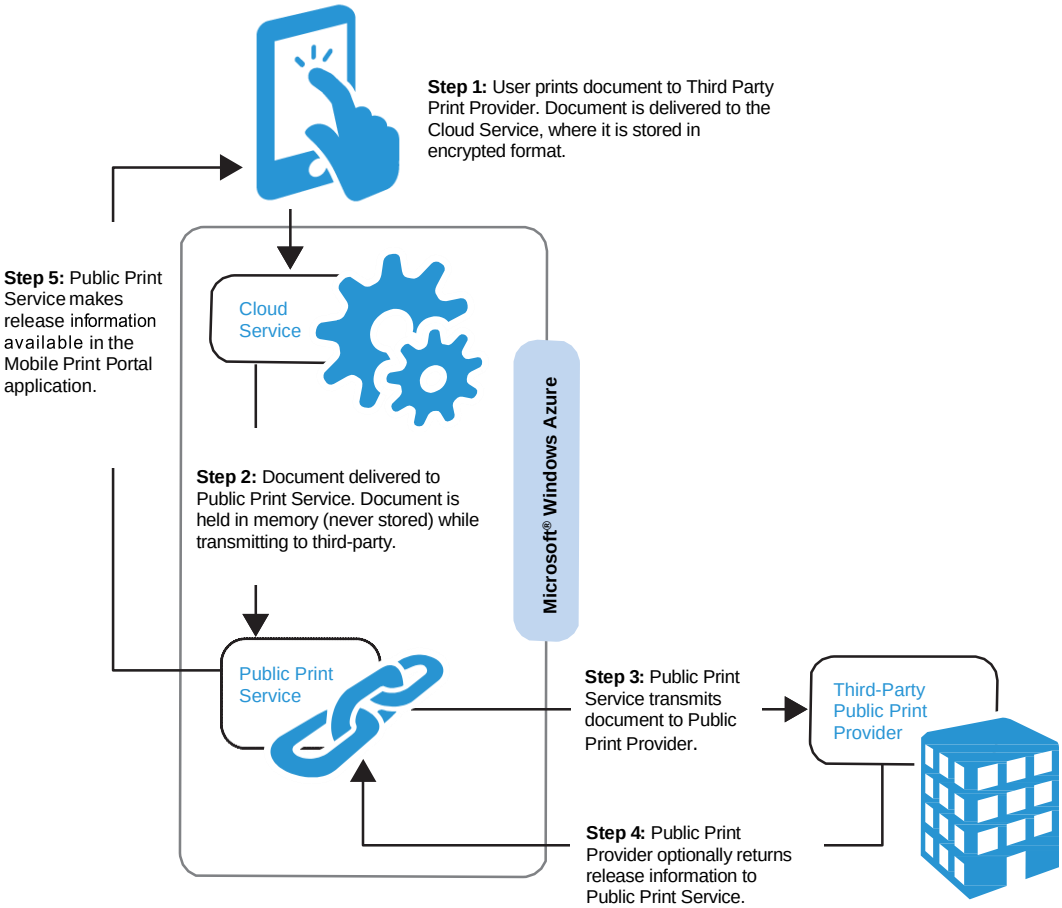
Workplace Credentials are not stored on the Agent computer or in the Cloud database. The Print Portal App stores the Workplace Credentials encrypted on the mobile device. Xerox® Mobile Print Cloud agent will query Active Directory for available domains.

In order to communicate with Active Directory, Xerox® Mobile Print Cloud uses the Active Directory Services Interfaces (ADSI) technology that is available in all Windows Operating Systems supported by Xerox® Mobile Print Cloud. The communication with the Active Directory servers occurs via the standard LDAP port 389. Communication is secured via SASL bind usually using the GSSAPI mechanism.

The Xerox® Mobile Print Cloud Agent retrieves and stores a list of available active directory domains based on the context of the logged in user on the Agent computer.

3.3.4 Third Party Public Print Provider

This diagram shows the flow between Xerox® Mobile Print Cloud components and a third party public print provider. All communications are over HTTPS using TLS.



Xerox® Mobile Print Cloud, when configured to do so, offers the capability to a user of printing to a third party public print provider from the Xerox® Mobile Print Portal application. These third party networks provide access to printers at hotels, airport lounges and other public locations.

When printing to a third party public print provider, the user is alerted that they are sending their document outside of the Xerox® Mobile Print Cloud Service. Each document printed to a third party public print provider is stored within Azure Storage. It follows a 7-day document retention policy, which is applied to the document at the time of printing. The original document is stored within Azure Storage in an encrypted format.

Access to these documents is only available to the following:

1. The owner of the documents via the Xerox® Mobile Print Portal Mobile application for preview.
2. Authorized Xerox personnel responsible for deployment and maintenance of the system. Since the documents are encrypted, even the authorized personnel cannot open the document to view its contents.

Original documents printed to a third party print provider are delivered to the Xerox® Mobile Print Public Print Service, which is co-located with the Xerox® Mobile Print Cloud Service in Microsoft® Windows Azure.

Original documents are transmitted from the Xerox® Mobile Print Public Print Service to the third party public print provider in a secure manner. All communications to and from the Xerox® Mobile Print Public Print Service are over HTTPS over TLS. Documents are always transmitted securely and are protected by TLS security during transmission to the third party public print provider.

The third party public print provider may respond with a release code or other information the user would need to retrieve their printed output. It is delivered securely over HTTPS. This information is available via the Xerox® Mobile Print Portal application only by the user who printed the document.

Xerox maintains the security and integrity of the document up until the point that it is transmitted to the third party. Xerox cannot assume responsibility for the security of any content of the document that is transferred.

3.3.5 Xerox® Mobile Print Cloud Agent

The Xerox® Mobile Print Cloud Agent has five primary functions.

1. The agent is responsible for discovering printers within the customer's network, determining the printer capabilities, and relaying that information to the Xerox® Mobile Print Cloud Service.
2. The Xerox® Mobile Print Cloud Agent is responsible for routing print jobs to target printers and print queues.
3. The Agent is responsible for performing any printer configuration. This includes the following feature areas:
    a. Cardless Authentication - The agent will make SNMP queries and modifications to the following device settings: enable/disable for Cardless Authentication, Blocking Screen strings, Alternate Login, and Service Locking.
    b. Xerox® Mobile Print Cloud EIP App - The agent will register the Xerox® Mobile Print Cloud EIP App on the printer.
4. The Agent will implement the EIP Cardless Authentication, acting as the authentication server, which allows users to authenticate their identity and unlock the printer.
5. The Agent is responsible for domain authentication lookups of users.

The Xerox® Mobile Print Cloud Agent is installed on a PC. The installing user must have administrator privileges since the Xerox® Mobile Print Cloud Agent software is installed as a Windows service. The Xerox® Mobile Print Cloud Agent cannot be connected to the Xerox® Mobile Print Cloud Service unless the Xerox® Mobile Print Cloud Service has been configured to accept the agent.

The Xerox® Mobile Print Cloud Agent user interface is available to all users who can log on to the agent PC. It displays the printers discovered by the agent and print queues served by the agent. It allows only the proxy server address for that agent to be changed. It does not present any user or customer specific information.

If the Agent Proxy setting is configured by a user, the Agent will in turn set the system level proxy of the PC on which the Agent is running. The system level proxy settings would then be usable by other applications running on the same PC.

A local database is maintained on the Xerox® Mobile Print Cloud Agent PC. This database stores printer discovery settings and printer information for each printer discovered, and print queue information as entered by the administrator. Access to the database is restricted to user's who have permission to log into the agent PC.

The Xerox® Mobile Print Cloud Agent installs by default in the following location:

- Program Files(x86) > Xerox > Mobile Print Cloud Agent

Access to this folder and sub-folders is limited to users logged on to the agent PC. It contains the agent executable file, its database, and language libraries.

By default, agents are set to upgrade automatically when a new version of the agent software is available. Agents connect to the Xerox® Mobile Print Cloud Service and, if a newer version is available, it is automatically downloaded over HTTPS using TLS and installed. The administrator can disable this feature.

Threats include physical damage to the system, attacks over the network, as well as damage caused by viruses. The goal is to minimize the security risks as much as possible, and have policies in place to detect and reduce the negative impact of a

security incident. Examples of things that can be done to reduce risks include proper use of logins and passwords, restricting network access, applying security related operating system updates, and the use of virus detection software.

The customer is ultimately responsible for securing their environment to meet their specific security needs. Depending on the customer needs, the customer can increase security by installing a firewall, and/or physically securing the hardware to a limited access area. The customer, depending on their needs, should use tools to monitor and log physical and network access to the Xerox® Mobile Print Cloud Agent hardware and software to determine if and when a security incident has occurred. The customer should also back-up their data to ensure that it may be recovered in case of deletion or corruption.

Please refer to the section titled “Communication between Xerox® Mobile Print Cloud Service and Xerox® Mobile Print Cloud Agent” and the section titled “Communication between Xerox® Mobile Print Cloud Agent and Printer” for more information about authentication and communications related security information.

3.3.6 Xerox® Mobile Print Cloud - User Web Pages

All user web pages are accessed using HTTPS over TLS from a browser.

Xerox® Mobile Print Cloud customer account users have to authentication with the Xerox® Mobile Print Cloud Service to access the user web pages. Once authenticated the user can view:

1. All printers enabled by the customer account administrator inclusive of printer name, printer location, and the printer’s direct email submission email address.
2. Only jobs submitted by the user inclusive of document names, date of completion, and printer name of printer used to print the job.

3.3.7 Xerox® Mobile Print Cloud - Customer Administrator Web Pages

All user customer administrator web pages are accessed using HTTPS over TLS from a browser.

Xerox® Mobile Print Cloud customer account administrators have to authenticate with the Xerox® Mobile Print Cloud Service to access the administrator user web pages. Once authenticated the administrator user can view everything that users can in addition to the following:

1. Users associated with their customer account via a listing that includes email addresses.
2. All jobs processed for the account inclusive of document names, date of completion, email address of user that submitted the document, and printer name of printer used to print the job. This includes documents submitted by users who are not members of the customer account, but have seen and printed to one of the account printers.
3. Licensing information that includes license activation keys and associated serial numbers. Once a license is installed for a customer account, the license activation keys and associated serial numbers cannot be re-used to install in other customer accounts.
4. IP addresses for all printers discovered by the customer account's Xerox® Mobile Print Cloud Agents. For each printer, the administrator can view and manage the enablement for Xerox® Mobile Print Cloud, as well as the enablement for Cardless Authentication and whether the printer has the Xerox® Mobile Print Cloud EIP App installed.
5. The addresses of sites where printers are located.
6. Xerox® Mobile Print Cloud Agents that have been created and registered with the customer account. This includes the agents Activation Codes which are tied to the customer account and cannot be used to register a Xerox® Mobile Print Cloud agent in another customer account. This information is displayed for the customer account administrators only. It is the responsibility of the administrator in sharing Activation Codes with others.

3.3.8 Server-Based Print Queues

For a server that hosts print queues used by Xerox® Mobile Print Cloud, nothing special is required. To minimize security risks, leverage any security features of print control software. Incorporate standard security measures, apply security related operating system updates, use anti-virus software and add hard disk encryption.

The customer is ultimately responsible for securing their environment to meet their specific security needs. Depending on the customer needs, the customer can increase security by installing a firewall, and/or physically securing the hardware to a limited access area. The customer should back up their data to ensure that it may be recovered in case of deletion or corruption.

3.3.9 Printer

Xerox printers have a variety of security features that can be employed to increase security. Availability of these features will vary depending on model. It is the customer's responsibility to understand and implement appropriate controls for printer behavior.

Xerox Secure Print allows you to control the print timing of your documents. When using Secure Print during print job submission, users enter a passcode, and then must enter the same passcode to retrieve the job at the printer.

Users may choose to use Secure Print with Secure Print enabled printers, or the administrator may configure their Mobile Print Cloud account to require that Secure Print be used for all jobs sent via Mobile Print Cloud to that printer.

Secure Print passcodes are never stored on the mobile App or in the Mobile Print Cloud Service. They are transferred securely over SSL. Passcodes are never stored externally to the job on the printer.

Passcodes are numeric and conform to the requirements of the printer model. Auto-generated passcodes are a minimum of six digits for all printers whose maximum is at least six digits.

Additional security can be enforced at the printer if the printer is EIP Capable and/or supports the EIP Convenience Authentication API. For those printers which support this capability, the Xerox® Mobile Print Cloud Service provides the capability to lock the printer's local user interface, and require the user to authenticate themselves at the printer in order to gain access to any of the services / features of the printer. There are two ways in which a user can authenticate themselves:

1. The user may supply their Xerox® Mobile Print Cloud user credentials (username / password or LDAP credentials depending upon the Company/Account configuration) at the printer.
2. The user may use the Xerox® Print Portal App, by supplying the 4-character code found on the local user interface of the machine into the Print Portal App. This will identify the printer in the App and the user can confirm that they wish to unlock the device.

In either of the above scenarios, upon supplying valid credentials or making the unlock request, the printer will remove the blocking screen and the user will have access to the services / features of the printer. If the printer is an EIP capable device and the Xerox® Mobile Print Cloud EIP App is installed, then the user may select the App and view their list of jobs without providing additional login credentials for the app.

For information on the security of a job while it is stored on the printer, refer to your printer's documentation.

Other examples of printer security features are as follows:

1. Xerox Image Overwrite electronically shreds information stored on the hard drive of devices as part of routine job processing.
2. Data Encryption uses state of the art encryption technology on data stored within the device as well as for data in motion in and out of the device.

For more information about the above examples as well as for other printer security-related technologies please see http://www.xerox.com/information-security/product-security.

The Xerox® Mobile Print Cloud Service supports printers from a variety of manufacturers. It is the customer's responsibility to understand the security features of any non-Xerox printers configured for use in the system.

3.3.9.1 Xerox® Mobile Print Cloud EIP App

Devices which are EIP capable have the ability to support the Xerox® Mobile Print Cloud EIP App. This App allows users to log into their Cloud account, view and manage their print jobs. There are two methods of adding / using the Xerox® Mobile Print Cloud application with EIP:

1. ConnectKey App – sometimes referred to as a weblet. This form of App is installed by the customer, typically a system administrator.
2. Xerox Mobile Print Cloud Agent – The Agent install the EIP App directly on the printer based on configuration settings made using the Xerox® Mobile Print Cloud Web Portal.

There are three modes of execution for the Xerox® Mobile Print Cloud EIP App. The first of which is the unlicensed mode. This mode is only supported with the ConnectKey App, and the user is limited to the basic workflow of email submission and EIP print release. When using this mode, there is no Agent installed on the customer's network. Print jobs are transferred to the printer via HTTPS over TLS using port 443.

The second mode of execution for the EIP App is a licensed mode, without an Agent. This mode is only supported with the ConnectKey App. In this mode, the user has access to most of the features of Xerox® Mobile Print Cloud, including use of the Print Portal App. Print jobs are transferred to the printer via HTTPS over TLS using port 443.

The third mode of execution for the EIP App is the traditional Mobile Print Cloud environment, with a license and one or more Agents. The Agent will install EIP in this mode, using the EIP Registration API, which is done using HTTP/HTTPS. Print jobs are received via the Agent using LPR (port 515) or Raw IP (port 9100).

3.4 Communication Between System Components

3.4.1 Communication Between Xerox® Mobile Print Portal Mobile Application and Xerox® Mobile Print Cloud Service

The Xerox® Mobile Print Portal Mobile Application uses the HTTPS over TLS protocol for all communication with the Xerox® Mobile Print Cloud Service. It establishes an HTTPS secure connection with the Xerox® Mobile Print Cloud Service relying on the mobile device operating system to validate the security certificate as part of establishing the SSL connection. The SSL certificate is issued by Comodo (a trusted certificate authority) and ensures that the application has been verified and validated.

The Xerox® Mobile Print Portal Mobile Application requires users to authenticate before using any of its features. Basic authentication is performed with the Xerox® Mobile Print Portal Mobile Application providing username and password information over the HTTPS protocol (using TLS).

Once authentication is complete, data is passed between the Xerox® Mobile Print Portal Mobile Application and the Xerox® Mobile Print Cloud Service to enable the features of the service within the Xerox® Mobile Print Portal Mobile Application. This includes all data for previewing and printing jobs, location of printers, and user location data as determined by the mobile device. Users are only able to access documents they submitted and printers to which they have been granted access.

Users should consult their network provider on best practices for securing their 3G/4G communications on their mobile devices.

3.4.2 Communication Between Mobile Device and Email Server

Emails submitted to the Xerox® Mobile Print Cloud Service 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 to the Xerox® Mobile Print Cloud Service. It is the user's responsibility to ensure appropriate email security controls are in place.

Emails generated by the Xerox® Mobile Print Cloud Service typically contain temporary user passwords and system messages.

3.4.3 Communication Between Email Server and Xerox® Mobile Print Cloud Service

Emails are processed and consumed immediately upon receipt by the Xerox® Mobile Print Cloud service. Emails are not stored in any repository or inbox.

3.4.4 Communication Between Xerox® Mobile Print Cloud Service and Xerox® Mobile Print Cloud Agent

The Xerox® Mobile Print Cloud Agent uses the HTTPS protocol over TLS for all communication with the Xerox® Mobile Print Cloud Service. It establishes an HTTPS over TLS secure connection with the Xerox® Mobile Print Cloud Service relying on the PC's operating system to validate the security certificate as part of establishing the SSL connection.

After successful installation of the Xerox® Mobile Print Cloud Agent software, it will attempt to register itself with the Xerox® Mobile Print Cloud Service. The Xerox® Mobile Print Cloud Agent's registration process provides the Xerox® Mobile Print Cloud Service with the Xerox® Mobile Print Cloud account's administrator credentials, the Xerox® Mobile Print Cloud Agent Activation Code, and a machine hash code. The Xerox® Mobile Print Cloud Service returns a Xerox® Mobile Print Cloud Agent registration identifier to complete the registration process. The Xerox® Mobile Print Cloud account's administrator credentials are only held in memory during the registration process and removed once the registration process is complete.

After successful registration of the Xerox® Mobile Print Cloud Agent, print job data is transmitted between the Xerox® Mobile Print Cloud Service and the Xerox® Mobile Print Cloud Agent in the form of print ready files. This data may exist in memory on the agent PC while it is being spooled to the printer. In addition, data about printers discovered and printer capabilities is transmitted.

If the Cardless Authentication feature is enabled, the Agent will facilitate communications act as a middleman between the printer and the Xerox® Mobile Print Cloud Service, receiving authentication requests from either entity and converting them to the appropriate response and passing that onto the recipient. All such communication is done using HTTPS.

3.4.5 Communication Between Xerox® Mobile Print Cloud Agent and Printer

The Xerox® Mobile Print Cloud Agent uses SNMPv2 to discover printers and printer capabilities. Customers can configure the community name strings for the agent to use if they have configured their printers to use non-default values.

The Xerox® Mobile Print Cloud Agent will route print jobs to the target printer using either Raw Port 9100 or LPR/LPD Port 515. These ports are both configurable.

Customers can further secure the print path by enabling IPSec between their Xerox® Mobile Print Cloud Agent PC and their printers provided the printers support IPSec. When configuring IPsec, ensure that the communication between the Xerox® Mobile Print Cloud Agent and Xerox® Mobile Print Cloud Service does not employ IPsec.

When a printer is enabled, the Agent may register the Xerox® Mobile Print Cloud EIP App, or it may enabled the Cardless Authentication feature based on the printer configuration settings supplied by the administrator. The EIP App will be registered using the EIP Registration API, which requires the printer's administration credentials. The Cardless Authentication feature enabled and configuration is done via SNMP using the SET Community string and administration credentials for the printer.

If the Cardless Authentication feature is enabled, the Xerox® Mobile Print Cloud Agent will play a role in authenticating a user at the printer. The Agent will facilitate communications between the printer and the Xerox® Mobile Print Cloud Service, receiving authentication requests from either entity and converting them to the appropriate response and passing that onto the recipient. All such communication is done using HTTPS.

The Xerox® Mobile Print Cloud Agent may be enabled to support iOS Native printing. When enabled, devices running iOS may locate and send print jobs directly to the Agent. This is done using the IPP protocol using port 631. For further details on this capability, please review the Xerox® Mobile Print Cloud Administration Guide.

3.4.6 Communication Between Xerox® Mobile Print Cloud Agent and Print Queue

Customers identify their print queues to Xerox® Mobile Print Cloud Agent by providing information on the server, port and queue name.

The Xerox® Mobile Print Cloud Agent will route print jobs to the print queue using LPR/LPD Port 515. This port is configurable.

Customers can further secure the print path by enabling IPSec between the Xerox® Mobile Print Cloud Agent PC and the servers. When configuring IPsec, ensure that the communication between the Xerox® Mobile Print Cloud Agent and Xerox® Mobile Print Cloud Service does not employ IPsec.

4 The Role of Xerox

Xerox will strive to provide the most secure software product possible based on the information and technologies available while maintaining the products performance, value, functionality, and productivity.

Xerox will:

- Run industry standard security diagnostics tests during development to determine vulnerabilities.

  If found, the vulnerabilities will either be fixed, minimized, or documented

- Monitor, notify, and supply (when necessary) security patches provided by third party software vendors used with the Mobile Print software.


xerox