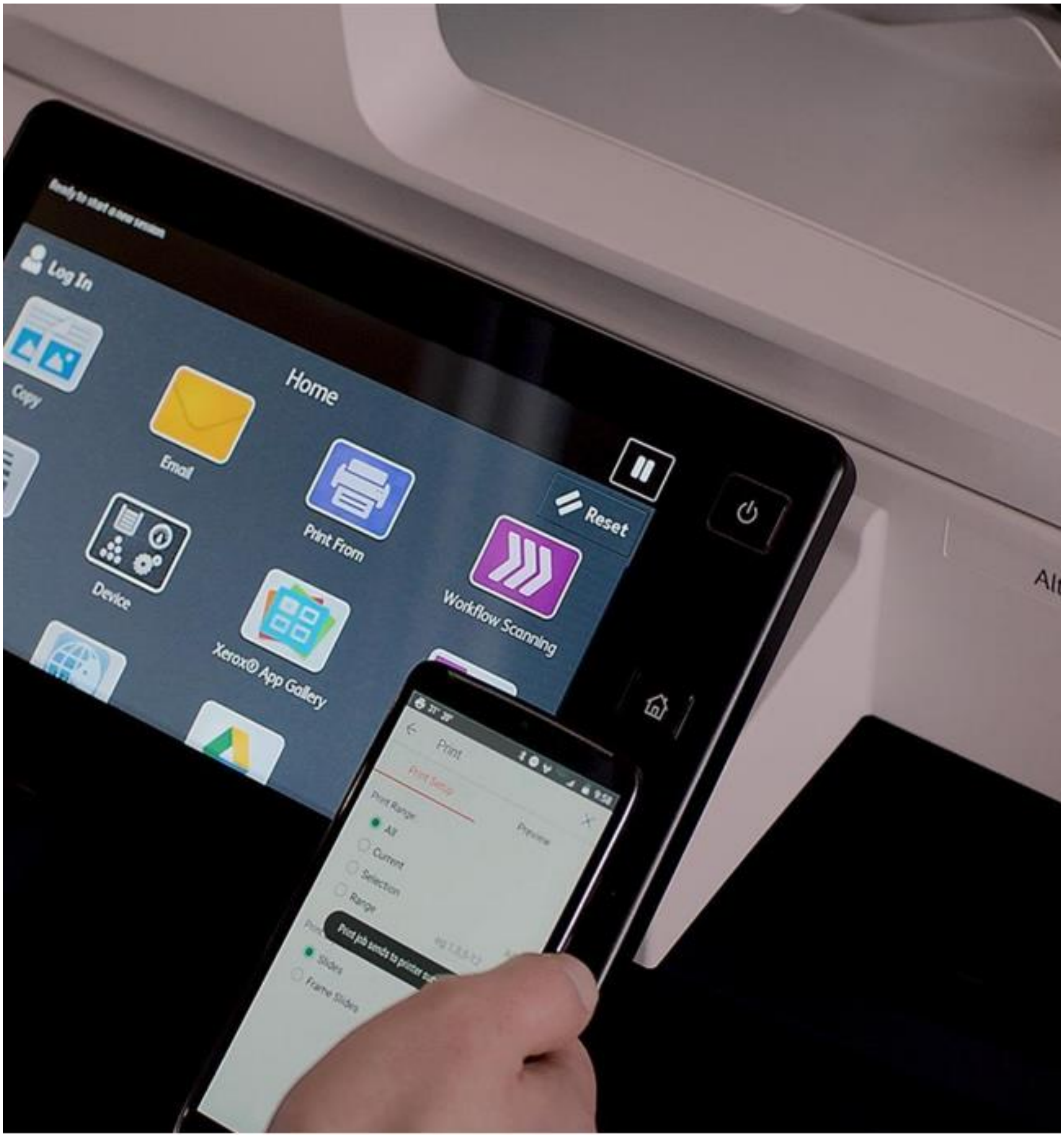
Security Guide

Xerox® Touchless Access App



Document Version: 1.0 (July 2020).

Contents

1. Introduction

Purpose

Xerox® Touchless Access App helps keep your employees safe by reducing the need to touch shared multifunction devices. The App enables users to access printing, scanning, and copying services via their mobile devices.

Xerox® Touchless Access App works via the cloud, removing the need for your mobile device to connect to your organization's local network, and maintaining the security you expect from Xerox.

The purpose of the Security Guide is to disclose information for Xerox® Touchless Access App with respect to device security. Device security, in this context, is defined as how data is stored and transmitted, how the product behaves in a networked environment, and how the product may be accessed, both locally and remotely. This document describes design, functions, and features of Xerox® Touchless Access App relative to Information Assurance (IA) and the protection of customer sensitive information. Please note that the customer is responsible for the security of their network and Xerox® Touchless Access App does not establish security for any network environment.

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

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 apps; as such, some user actions are not described in detail.

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

Overview

Xerox® Touchless Access App consists of three primary workflows. The three workflows are:

- Copy a document
- Print a document
- Scan and email a document

The app and three workflows facilitate a combination of the following steps:

- App components and hosting
- Communication via Kiosk server
- Copy
- Print
- Scan to Email
- Logging
- Cookies

App components and hosting

Xerox® Touchless Access App consists of six key components: the Kiosk server, the mobile web app, the EIP app, the API, the database, and encrypted blob storage. The device app is a ConnectKey®/EIP web app, the mobile web app is a Progressive Web App (PWA), and the API is a REST API.

All six components are hosted in Microsoft Azure and are secured via TLS.

Communication via the kiosk server and database

The kiosk server provides the communications conduit between the PWA and EIP device app. It manages the user sessions and passes APIs between the apps. The PWA and EIP device app must authenticate to the kiosk server to initiate an communication.

The database is used to gather summary app usage statistics. Collected data includes the number of unique devices using the app as well as the number of copy, print and scan jobs initiated by the app across the fleet. App usage is not monitored per individual devices.

Copy

The copy job is local to the Xerox® Device and at no time is the document transmitted off of the device.

Print

A user has the option to remotely print a file from their mobile device. The file(s) a user selects for print are stored in encrypted blob storage for no more than 15 minutes. The PWA cannot talk directly to the EIP app, so blob storage temporarily persists files to enable transfer between the mobile and Xerox® Devices.

The app supports print for the following file types: PDF, PDF/A, JPEG, JPG, TIFF, TIF, and TXT.

Scan to Email

The Scan to Email workflow leverages existing SMTP settings on the Xerox® Device. Users must have email configured and enabled on their device to use the Scan to Email feature.

Logging

Logging is persisted on the server to aid with support and application scaling. Logging is transmitted over TLS and no PII is stored.

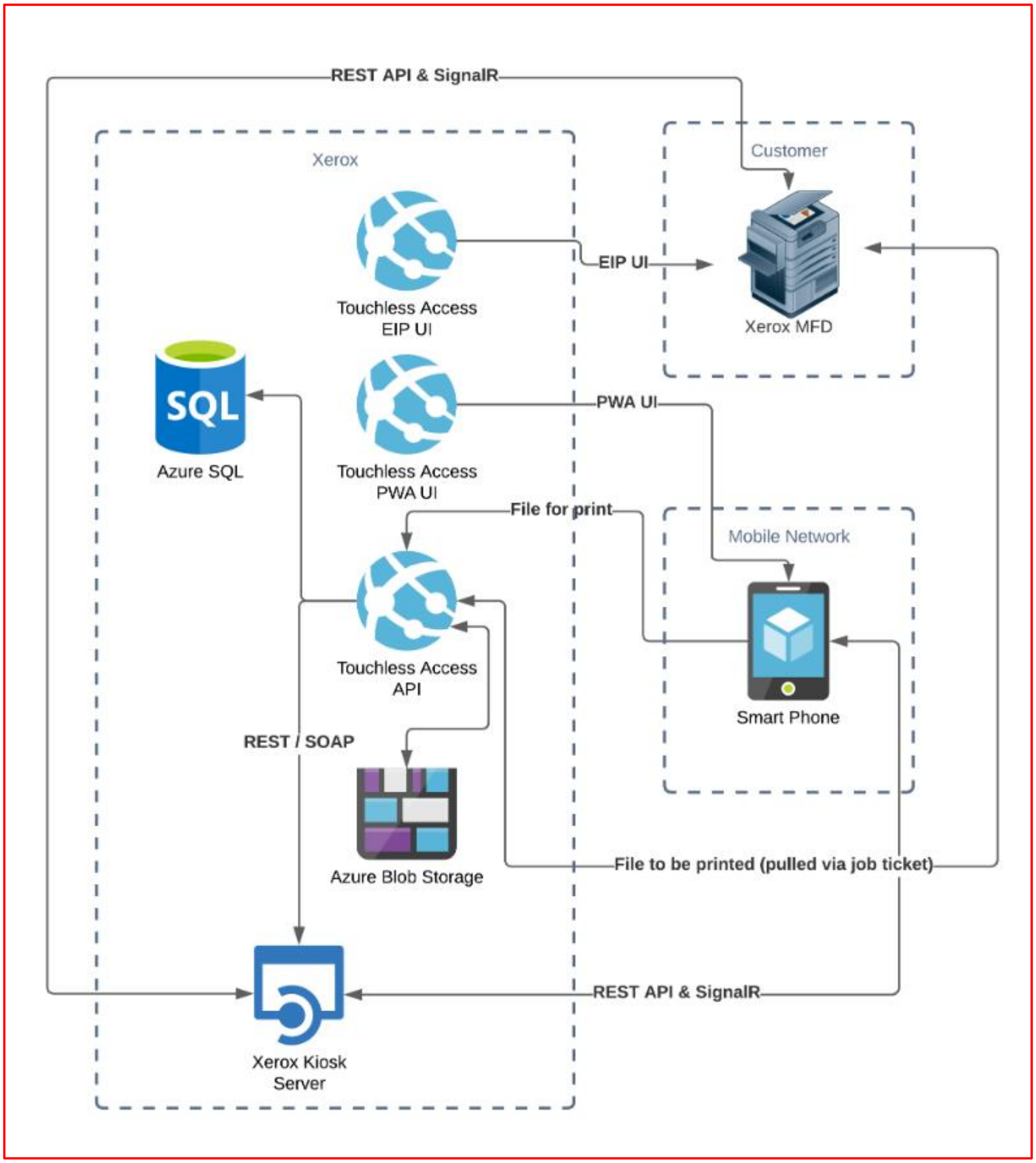
Cookies

If the user chooses to persist their email address for convenience, the PWA stores the email address in a cookie. This cookie will expire after 365 days. No information besides the email address is collected. The user must accept this in a PWA popup.

Architecture and Workflows

Architecture Diagram

Below is a diagram that outlines what's being transmitted between each service:



3. User Data Protection

User Data Protection within the Product

The Xerox® Touchless Access PWA, EIP app, API, database, and encrypted blob storage are hosted on the Microsoft Azure Network. Microsoft's Azure data center operations feature comprehensive information security policies and processes using standardized industry control frameworks, including ISO 27001, SOC 1, and SOC 2.

For a full description, please follow the link: https://docs.microsoft.com/en-us/azure/security/azure-network-security.

For more information regarding user data protection provided by the Xerox® Multifunction Device, please reference your specific model's Security Guide.

User Data at Rest

Data Persistence

Files selected for print are temporarily persisted in encrypted blob storage for a maximum of 15 minutes. The file is not accessible from anything other than the server-side code. As stated above, the PWA cannot talk directly to the EIP app, so blob storage temporarily persists files to enable transfer between the mobile and Xerox® Devices.

Azure blob storage is encrypted using 256-bit AES encryption, and is FIPS 140-2 compliant.

The API also persists the session and device ID in the database using a 1-way hash function. These values do not contain any PII.

User Data in Transit

Secure Network Communications

The Xerox® Touchless Access EIP app and API require that the device can communicate over port 443 outside the client's network. All communication between all aspects of the application, including, but not limited to the PWA, EIP app, API, database, encrypted blob storage, and Kiosk server are encrypted using HTTP Secure (TLS).

4. Additional Information and Resources

Security Xerox

Xerox maintains an evergreen public web page that contains the latest security information pertaining to its products. Please see https://www.xerox.com/security.

Responses to Known Vulnerabilities

Xerox has created a document which details the Xerox Vulnerability Management and Disclosure Policy used in the discovery and remediation of vulnerabilities in Xerox® Software and Hardware. It can be downloaded from this page: https://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html.

Additional Resources

Security Resource	URL
Frequently Asked Security Questions	https://www.xerox.com/en-us/information-security/frequently-asked-questions
Bulletins, Advisories, and Security Updates	https://www.xerox.com/security
Security News Archive	https://security.business.xerox.com/en-us/news/

Table 1 Security Resources