Xerox® Audio Documents App

Information Assurance Disclosure

BR25391
Document Version: 1.0 (September 2018).

Preface

Xerox® Audio Documents App (AD) is a workflow solution that converts paper documents to spoken word audio files. Converting documents to MP3 files is easy and convenient from Xerox® MFP devices without the need of a computer, servers, and 3rd party scan equipment. This reduces time and cost while ensuring privacy and security.

1. Purpose

The purpose of the Information Assurance Disclosure (IAD) is to disclose information for AD with respect to device security. Device security, in this context, is defined as to 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 the Xerox® AD 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 the Xerox® AD does not establish security for network environments where MFPs are installed.

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

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

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.

Contents

1. Purpose i
2. Target Audience i
3. Disclaimer i

1. Description and Details 1-1

Overview 1-1
App Hosting 1-1
App Start Up 1-1
Scanning 1-1
Document Conversion 1-2
Email Notification 1-2
MP3 Retrieval 1-3
MP3 Expiration 1-3

2. Security 2-4

App Hosting 2-4
Zamzar Web Service 2-4
Secure Web Communications 2-4
Encryption 2-4
App Data 2-4

3. Privacy 3-5

Device Browser Cookies 3-5

4. Ports 4-6

App 4-6

5. Diagrams 5-7

Architecture 5-7
Workflow 5-7

6. Appendix: Zamzar Information Security 6-1

Physical Security 6-1
Data Transfer Integrity 6-1
Data at Rest 6-1
Password Encryption 6-2

Firewalls 6-2
Operational Access Controls 6-2
Software Updates 6-2
Process Isolation 6-3
GDPR compliance 6-3
External accreditation 6-3
Bug bounty program 6-3

1. Description and Details

Overview

The Xerox® AD app provides a single workflow.

- Scan a document

Completing the workflow involves a combination of the following aspects described in detail below.

- App Hosting
- App Start Up
- Scanning
- Document Conversion
- Email Notification
- MP3 Retrieval
- MP3 Expiration

App Hosting

The Xerox® AD app is a ConnectKey App / EIP web application registered on a device and executes its functionality in the cloud.

All data communications in and out of the device and cloud components are encrypted over HTTPS using TLS 1.2.

App Start Up

During start-up of the AD app, the EIP browser runs the CK App HTML and JavaScript hosted on the device which fetches the App UI content from AD app endpoints hosted in the Azure App Service. The main page initialization script executes local HTTP calls to web services in order to obtain relevant details associated with the device and its capabilities.

The following app data is stored on the device, in browser storage, until the App is uninstalled from the device.

- Device serial number
- Device network MAC address
- Device Type indicator

Scanning

Scanned documents are securely transmitted to the Azure App Service using HTTPS TLS 1.2 from the device to the AD app and delivered in process, as a pass through, to Zamzar's text-to-speech web service for conversion processing. This workflow is executed multiple times per hour.

The following app data is stored in-process, in the Azure App Service, until the session terminates or is refreshed after expiring:

- System access token for Zamzar web service requests

The following app data is stored in the Azure App Database until periodic deletion is required.

- Device serial number
- Device network MAC address
- AD Job identifier
- Base64 encoded PDF file name
- Encrypted email address
- Number of pages scanned
- Page size per page
- Job cost in scan pages

Document Conversion

The AD app scans a document and transforms the image set into a searchable PDF that is sent to an AD app endpoint for conversion processing.

The following app data is stored in-process, in the Azure App Service, until the session terminates.

- System access token for Zamzar web service requests
- Searchable PDF

A PDF file representing the document scanned is securely delivered to Zamzar over HTTPS and is deleted after the conversion process is completed.

The following app data is stored in the Azure App Database, until periodic deletion is required.

- Zamzar Job identifier
- Zamzar conversion request failure response body (if applicable)

The MP3 file received from Zamzar is persisted to Azure File Storage. The file that is stored will later be removed after 48 hours have elapsed since the point in time the file was received.

Email Notification

When the document conversion step completes successfully, a success email notification is sent to the recipient provided by the user.

The following app data is stored in-process, in the Azure App Service, until the session terminates.

- Job cost in scan pages
- Email address
- PDF file name
- Email envelope and message

When the document conversion step is unsuccessful, a failure notification email is sent to the recipient provided by the user.

The following app data is stored in-process, in the Azure App Service, until the session terminates.

- AD Job identifier
- Email address
- PDF file name
- Email envelope and message

MP3 Retrieval

When the user receives the success email and activates the download link, the AD app securely transmits the MP3 file over HTTPS.

The following app data is stored in-process, in the Azure App Service, until the session terminates.

- AD Job identifier
- MP3 file

Each link activation increments a download counter stored in the Azure App Database, and the MP3 file download will be permitted when the download limit is not exceeded.

MP3 Expiration

After 48 hours have elapsed since the point in time the file was received, the MP3 file that is stored in Azure File Storage is deleted.

2. Security

App Hosting

The Xerox® AD EIP app is 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

Zamzar Web Service

The Zamzar Web Service system and network security is established and maintained by Zamzar.

All Zamzar web communications are encrypted using TLS 1.2 over HTTPS.

All data is secured when at rest using AES-256 encryption.

For more information concerning Zamzar's information security methods, please see Appendix A: Zamzar Information Security.

Secure Web Communications

All App web communications are encrypted using TLS 1.2 over HTTPS.

Encryption

In addition to securing the web communications, the AD app uses AES-256 encryption to secure the email address associated with the AD job.

All Azure Storage data is secured when at rest using AES-256 encryption.

App Data

The email address and file name provided by the user is stored in the AD app transaction log.

3. Privacy

Device Browser Cookies

The AD app does not store any cookies on the device.

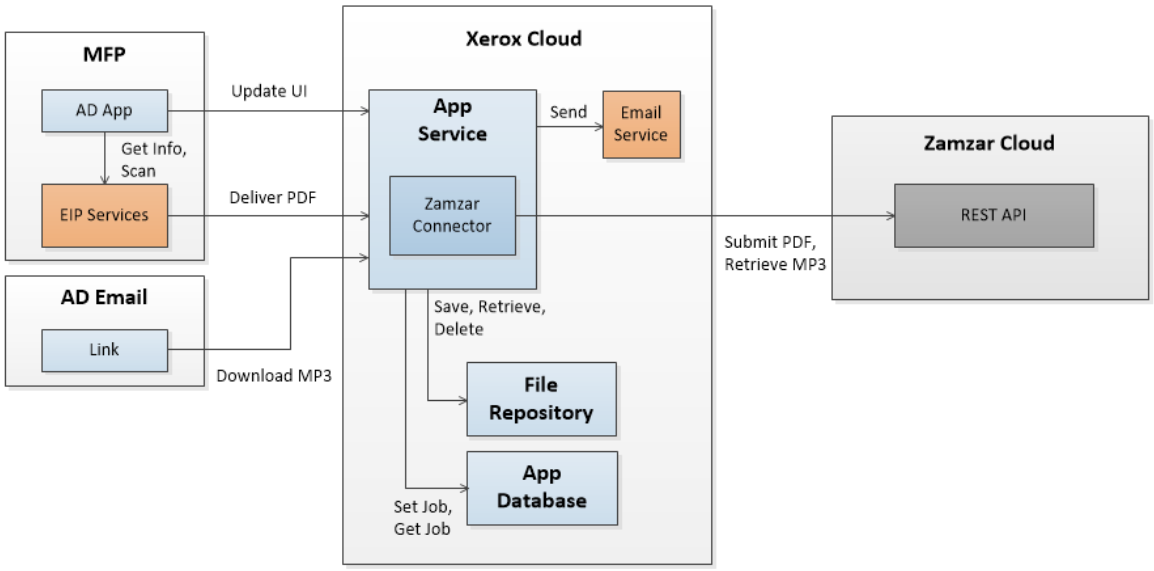
4. Ports

App

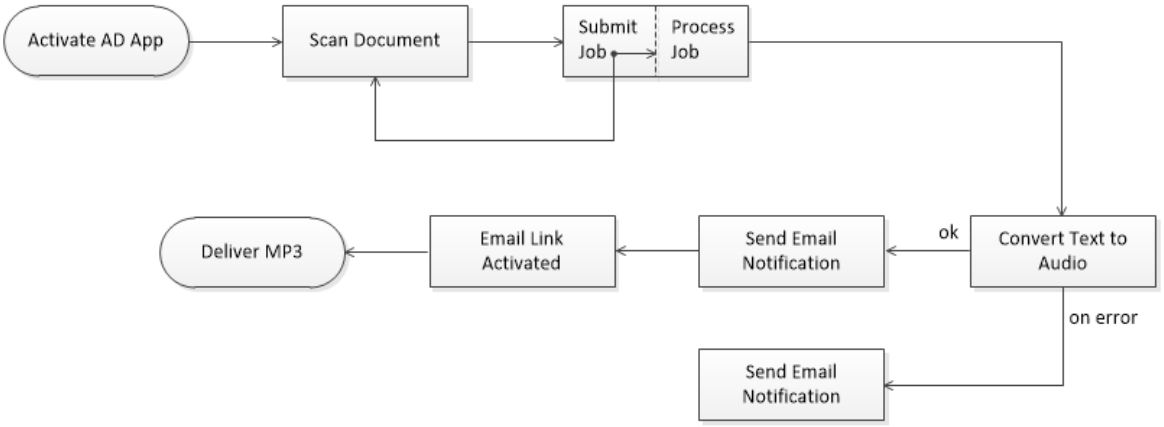
The Xerox® AD app requires the device to have Internet connectivity through HTTPS TCP port 443.

5. Diagrams

Architecture



Workflow



6. Appendix: Zamzar Information Security

Zamzar takes the security of customer data extremely seriously, and takes a number of measures to ensure the integrity of that data is not compromised. These measures include, but are not limited to:

Physical Security

Zamzar infrastructure is hosted in data centres provided by Amazon Web Services. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilising video surveillance, intrusion detection systems, and other electronic means.

Authorised staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorised staff.

AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services.

All physical access to data centers by AWS employees is logged and audited routinely.

Data Transfer Integrity

All traffic to and from Zamzar servers is secured by transport level security (TLS) sent over a Secure Socket Layer (SSL), and secured using an AES 256-bit SSL certificate. This ensures that data sent between your systems and ours is encrypted using military grade encryption.

By encrypting the communication, we ensure that no third-party is able to read or tamper with the data that is being exchanged during connections to our servers.

Additionally data sent internally between the constituent parts of the Zamzar application is also secured using TLS/SSL to ensure internal data integrity.

Data at Rest

When storing your files within the Zamzar API we encrypt each file on disk with a unique key employing strong multi-factor encryption using one of the strongest block ciphers

available - 256-bit Advanced Encryption Standard (AES-256). This ensures that data “at rest” on disk is protected in the event that hardware is physically compromised.

Password Encryption

Zamzar API user passwords are stored in our database after being salted and hashed using the Bcrypt encryption algorithm.

Bcrypt is considered to be the current state of the art in password hashing algorithms.

Firewalls

Zamzar enforces network level control for access to infrastructure by using multiple different firewall technologies to ensure that different components of its systems are logically isolated from one another.

This is a “defence in depth” security precaution which helps to ensure that the compromise of one part of the system does not automatically lead to access to other areas.

Operational Access Controls

Zamzar employees require access to production services for operational reasons. We employ multiple authentication mechanisms to ensure that production systems are accessed only by authorised members of staff and are protected from unauthorized access.

Strong passwords, multi-factor authentication devices and whitelisting of specifically allowed IP addresses are all used to ensure a multi-layered approach to operational security.

Software Updates

Zamzar regularly applies software patches to production infrastructure in order to ensure a strong security posture to known software vulnerabilities. Staff also routinely monitor industry mailing lists to stay abreast of breaking vulnerabilities.

We ensure that only vendor-approved updates are installed on our infrastructure by automatically verifying the integrity of all operating system package updates. In each case either a SHA1, SHA2 or MD5 checksum is checked to ensure it matches the vendor-generated value. The integrity of these checksums is ensured as they are signed via GPG by the package maintainers.

Process Isolation

Zamzar uses “software jails” to run selected software components in isolated operating system “jails”. In practice this ensures that any vulnerability exploited in that software cannot be used to pivot into other areas of the operating system or application and exploit other targets since software access to shared O.S. level computing resources is limited to the “jail” in which it runs.

GDPR compliance

Zamzar is compliant with the EU General Data Protection Regulation (GDPR) introduced on 25th May 2018.

External accreditation

Zamzar takes a pro-active approach to security by employing an external company (Trustwave Holdings Inc) to perform monthly security scans of its infrastructure. This helps to ensure that any “blind spots” in Zamzar’s security posture are caught early and gives further confidence in the system.

A copy of Zamzar’s latest successful PCI compliance scan has been sent to Xerox in a separate document.

Bug bounty program

Zamzar operates an informal “bug bounty” program that encourages security researchers to perform limited and authorised testing of the integrity of Zamzar systems.

This pro-active stance to security helps Zamzar’s systems to stay resilient to emergent “real world” security attacks in a way that merely responding to attacks “after the fact” would not. It also exposes the Zamzar team to new classes of security vulnerability at the earliest possible opportunity.