Security Guide

Xerox® Note Converter App

xerox™

Document Version: 2.0 (October 2023).

Contents

1. Introduction

Purpose

The purpose of the Security Guide is to disclose information for Xerox® Apps 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 the Xerox® Apps 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® Apps do not establish security for any network environment.

This document does not provide tutorial level information about security, connectivity or Xerox® 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

The Xerox® Note Converter App is a simple document conversion solution for your Xerox® device that assists the user with converting a handwritten document into digital files, which are delivered via an email message sent to the provided recipient.

The app supports the following workflow:

- Convert a paper handwritten document into a text editable file format

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

- App Hosting
- Device Authorization
- App Startup
- Scan and convert a paper document
- View the editable result file

APP HOSTING

The Xerox® Note Converter App depends heavily on cloud hosted components. A brief description of each can be found below.

Xerox® Note Converter App

The Xerox® App consists of two key components, the device weblet and the cloud-hosted web service. The device weblet is a Xerox® App that enables the following behavior on a Xerox® Device:

- Presents the user with an application UI that executes functionality in the cloud.
- Interfaces with the EIP API, which delegates work, such as performing the device scan operation.

The weblet communicates with the cloud-hosted web service, which executes the business logic for the App.

Google Cloud Vision API

The solution depends on the Google Cloud Vision API to convert digitized handwritten documents into document files that are editable. All requests are made over HTTPS.

Xerox Extensible Interface Platform®

During standard usage of the Xerox® App, calls to the device-hosted web services are used to initiate and monitor scan functions and to pull relevant details related to device properties and capabilities.

COMPONENTS

MFD with Xerox® Note Converter App – a Xerox® ConnectKey® App

This is an EIP capable device that can print, scan and execute ConnectKey Apps installed from the Xerox® App Gallery. In this case, the device has the Xerox® Note Converter App installed.

Xerox® Note Converter App Service – UI & App API

The UI and App API are hosted on the Microsoft Azure Cloud System. The UI aspect produces resources rendered by the embedded EIP browser. The App API is a service, which orchestrates downstream document conversion and delivery.

Xerox® Support Assistant App Service – Support Assistant API (SA-API)

The SA-API aspect is hosted on the Microsoft Azure Cloud System. This aspect provides the business logic service and communicates with the Xerox Integration Service middleware component.

Xerox App Gallery

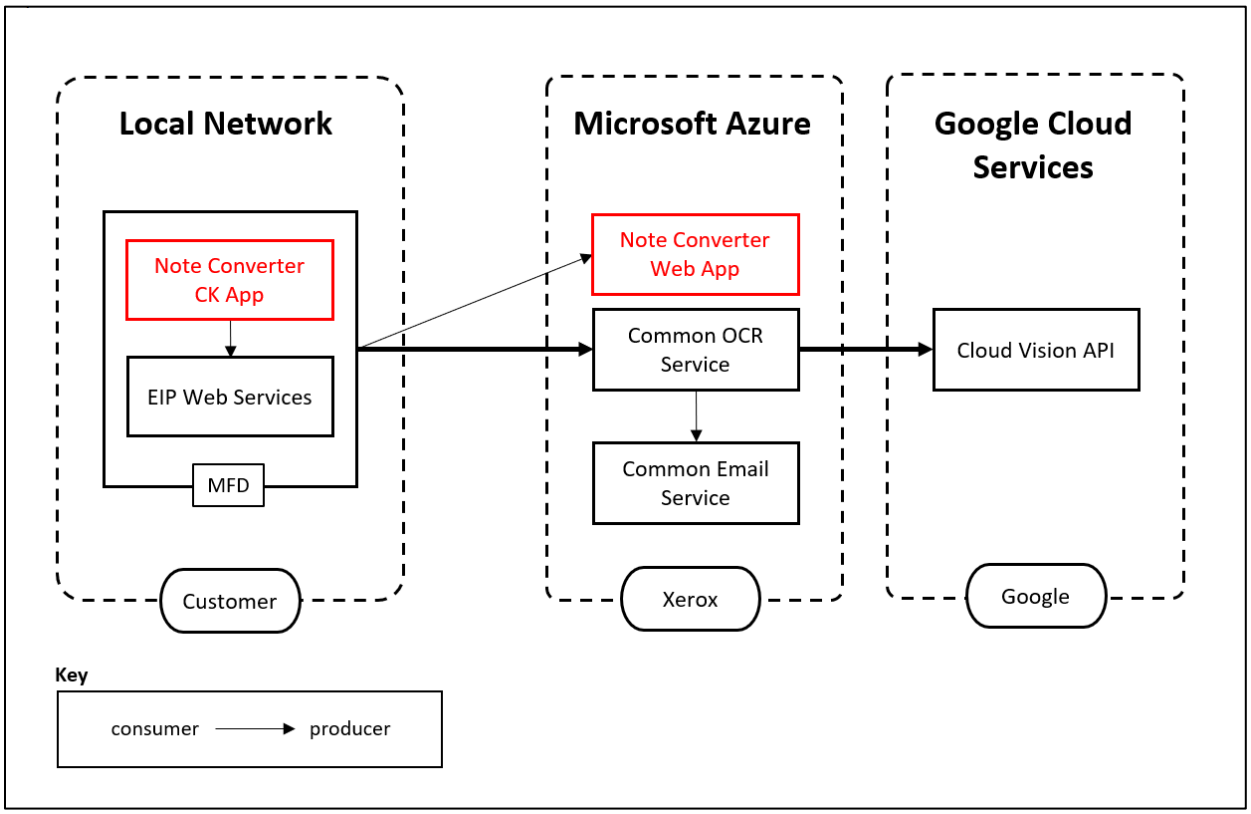
The App Gallery component is a web application, with services, hosted on the Microsoft Azure Cloud System. The App Gallery is accessed to ensure the App is entitled to run and is used when upgrading the App whenever the auto-update conditions apply.

Twilio SendGrid® Email API

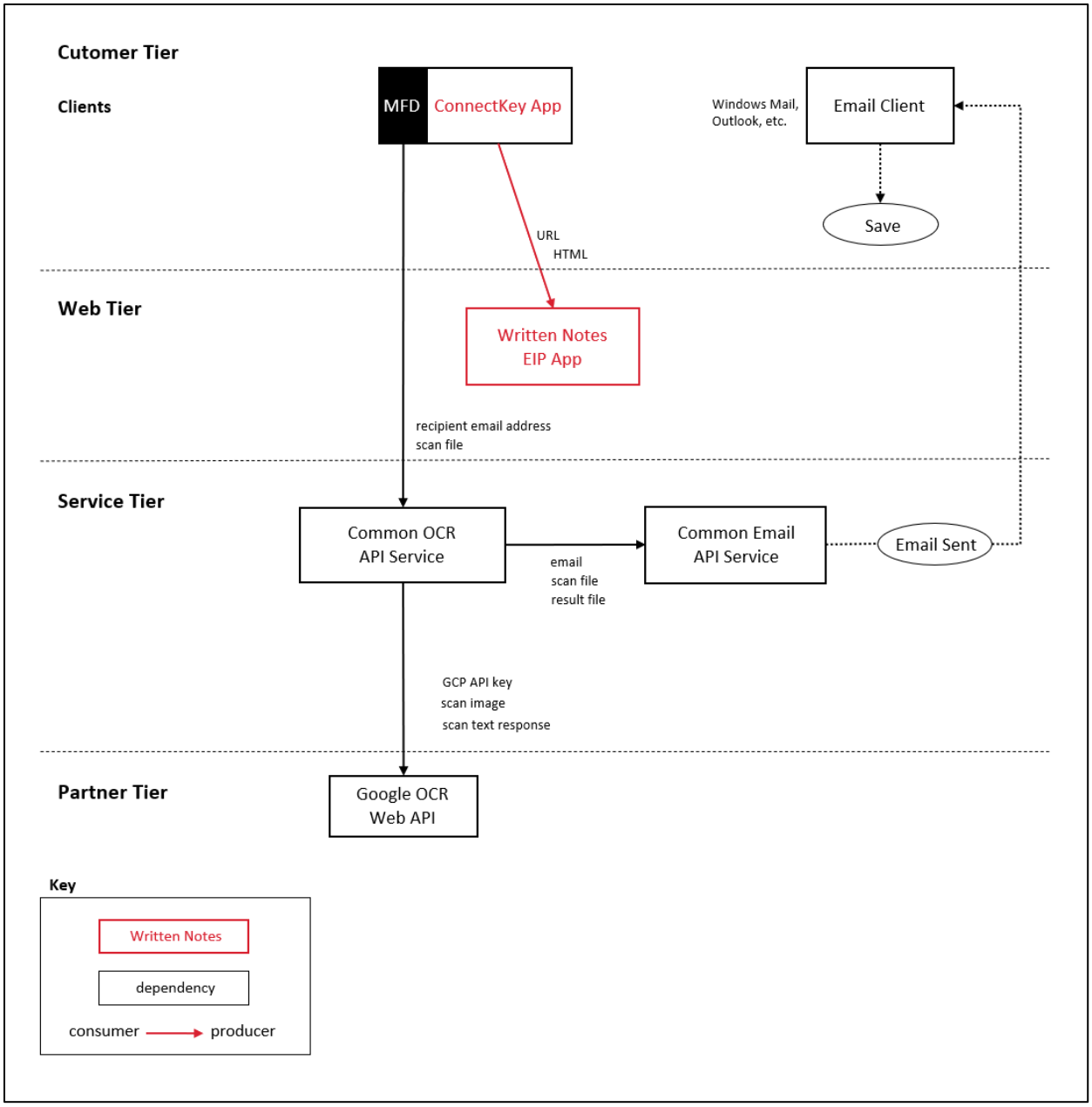
The SendGrid Email API is a cloud API service produced by Twilio. The SendGrid Email API is used to deliver the scan workflow result email to the user specified recipient.

Diagrams

ARCHITECTURE DIAGRAM



DATA FLOW DIAGRAM



Workflows

DEVICE AUTHORIZATION

Prior to app startup, the Xerox® Note Converter App verifies the device is authorized to run the app.

The device authorization step interacts with a Xerox® App Gallery API when determining runtime entitlements. When the device is authorized, app start up commences.

APP STARTUP

During startup of the Note Converter App, the EIP browser runs the CK App HTML and JavaScript hosted on the device which fetches the App's UI content using App Service endpoints hosted in the Azure App Service.

The main page initialization script executes local HTTP calls to device EIP web services in order to obtain relevant details associated with the device and its capabilities.

SCAN AND CONVERT A PAPER DOCUMENT

Workflow steps:

1. Provide the workflow recipient's email address.
2. Optionally modify the result file title.
3. Optionally modify the result file type.
4. Optionally change the scan settings.
5. Submit the job using the Scan button.
6. The workflow recipient receives an editable file and a copy of the original scan image.

VIEW THE EDITABLE RESULT FILE

Workflow steps:

1. Open the Note Converter email message received, which is associated with the workflow.
2. Open the document file attachments provided in the email message.
3. The OS will handle the document file content using the application associated with the file extension.

User Data Protection

APPLICATION DATA STORED IN THE XEROX CLOUD

User data related to the categories below are stored in cloud persistent storage until a delete event occurs.

- Session data
- Job data
- Document data

The following activities will trigger a delete event, for cloud files that meet the associated criteria.

- A delete occurs when the system detects intermediate processing files exist after a job has completed.

The balance of data stored in the cloud, that is unrelated to PII, may be stored indefinitely for event reporting purposes.

APPLICATION DATA STORED IN THE TWILIO SENDGRID SERVICE

For detailed information on User Data Protection and Security for the Twilio SendGrid Service, please follow this link: https://www.twilio.com/legal/privacy/

LOCAL ENVIRONMENT

Application data transmitted

Application data related to the categories below are transmitted to/from the Xerox® Device.

- Account data
- Session data
- Job data
- Document data

Application data stored on the Xerox® Device

The Xerox® Note Converter App does not store any customer data on the device.

HTTP Cookies

The Xerox® Note Converter App does not store any cookies on the device.

PII DATA MANAGEMENT

The following personal data is acquired and transmitted by the Xerox® Note Converter App. No personal data is stored and maintained by the Xerox® App.

- Email address

Clearing Device Browser Cache

The Device Browser Cache is cleared when one of the following events occur.

- Device Logout
- Device Timeout
- Double Clear All
- Browser Restart
- Cycling the Browser from Disabled to Enabled

3. Network Information

Protocol, Ports and URLs

The following table lists the protocol, ports and URLs used by the Xerox® Note Converter when executing within a customer's private network. All public connections are outbound to Cloud hosted components.

Protocol	Transport and Port Value	Use	Component	URL
HTTPS using TLS	TCP 443	App UI	EIP browser to Note Converter App UI Interface	wnc-web.services.xerox.com
HTTPS using TLS	TCP 443	App API	EIP scan engine to Note Converter App API Interface	wnc-api.services.xerox.com
HTTPS using TLS	TCP 443	App Configuration	ConnectKey App to App Gallery	appgallery.services.xerox.com
HTTPS using TLS	TCP 443	Subscription Entitlement	ConnectKey App to App Gallery	entitlements-appgallery.services.xerox.com

4. General Security Protection

User Data Protection within the Products

DOCUMENT AND FILE SECURITY

File content is protected during transmission by standard secure network protocols at the channel level. Since document source content may contain Personally Identifiable Information (PII) or other sensitive content, it is the responsibility of the user to handle the digital information in accordance with information protection best practices.

HOSTING - MICROSOFT AZURE

The cloud services are hosted on the Microsoft Azure Network. The Microsoft Azure Cloud Computing Platform operates in the Microsoft® Global Foundation Services (GFS) infrastructure, portions of which are ISO27001-certified. Microsoft has also adopted the new international cloud privacy standard, ISO 27018. Azure safeguards customer data in the cloud and provides support for companies that are bound by extensive regulations regarding the use, transmission, and storage of customer data.

The Apps hosted in the cloud are scalable so that multiple instances may be spun up/down as needed to handle user demand. The service is hosted both in the US and Europe. Users will be routed to the closest server geographically based on server load and network speed.

CLOUD STORAGE – MICROSOFT AZURE

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

For a full description, please follow these links:

Azure Storage

https://azure.microsoft.com/en-us/blog/announcing-default-encryption-for-azure-blobs-files-table-and-queue-storage/

User Data in Transit

SECURE NETWORK COMMUNICATIONS

The web pages and App services that constitute the Xerox® Solutions are deployed to Microsoft Azure App Services. All web pages are accessed via HTTPS from a web browser. All communications are over HTTPS. Data is transmitted securely and is protected by TLS security for both upload and download. The default minimum TLS version used is 1.2.

Xerox App Gallery supplies a link to a Certificate Authority root certificate for validation with the cloud web service. It is the responsibility of the customer to install the certificate on their devices and to enable server certificate validation on the devices.

For more information related to Azure network security, please follow the link:
https://docs.microsoft.com/en-us/azure/security/azure-network-security

5. Additional Information & 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 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 Additional Resources