Security Guide

Xerox® Translates Service

Document Version: 1.0 (October 2020).

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® Apps 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.

Contents

1. 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 SQL

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

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 TLS version used is 1.2.

The Xerox® App requires the user to provide proper/valid credentials in order to gain access to the application's features. Authenticated users are allowed to access the features and data using HTTPS.

At launch, the apps must get an authentication/session token through the solution's authentication process. The access token acquired is used for that session of the app.

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

User Data Protection

APPLICATION DATA STORED IN THE XEROX® CLOUD

User data related to the categories below are stored in cloud persistent storage.

- Translation Workflow data, including intermediate processing files and output files, for jobs that are processing or pending completion due to required user interaction.
- Logs of completed and cancelled Translation jobs.

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

- A delete occurs when the system detects intermediate processing files exist after a translation job has completed.
- A delete occurs for translated output files, where the user has chosen to have an email sent with a download link, on the 7th day after the output file was created.

LOCAL ENVIRONMENT

Application data transmitted

Application data related to the categories below are transmitted to/from a User's PC.

- Account Login data
- Translation Workflow Input, Output, Control Parameters and Execution Status data

Application data stored on a User's PC

The Xerox® Translates Service Web App stores the authenticated user's "access token" in Browser Internal Storage. The "access token" has limited lifespan of 2 hours.

HTTP Cookies

The Xerox® Translates Service Web App stores a non-tracking, technically necessary data required by Microsoft Azure.

2. Xerox® Translates Service Web App – Product Description

OVERVIEW

This Xerox® solution is a web application run from a compatible web browser on a PC, Tablet or Laptop computer.

Web App

The Xerox® Translates Service Web App provides the ability to translate the language of digital documents for the logged in customer.

Application	What can I do?
Web App	• Login to my account • Translate a document from one language to a different language

Table 1 Web App user benefits

APP HOSTING

The Web App consists completely of cloud hosted components that are accessed via a web browser. A brief description of each can be found below.

Web App

The Web App consists of three key components, the Xerox® Translates Service User Interface, the Xerox® Translates Service Services Interface and the Xerox® Microservice Functions. These components enable the following behavior in a web browser:

1. Provides the user with the application UI that executes functionality in the cloud.
2. Executes Microservice functions, which delegates the language translation work.

Xerox® App Gallery

The App Gallery component is a web application hosted on the Microsoft Azure Cloud System. The App Gallery Component implements the following functions for the Xerox® Translates Service Web App: Authentication.

Xerox® Translation API

The Xerox® Translation API component is a set of translation APIs hosted in the Microsoft Azure Cloud System. Xerox® Translates Service uses the Translation APIs to translate documents into a different language while maintaining the layout and format of the original document.

ABBYY Cloud OCR API

The ABBYY Cloud OCR API component is a partner, cloud hosted Optical Character Recognition (OCR) service.

Microsoft Translator API

The Microsoft Translator API component is a partner, cloud hosted language translation service.

SendGrid API

The SendGrid API component is a partner, cloud hosted email services platform. Xerox® Translates Service uses the SendGrid API to send email when it is specified.

COMPONENTS

Xerox® Translates Service UI

The Xerox® Translates Service UI component is hosted on the Microsoft Azure Cloud System. This component is responsible for hosting the web pages, which are displayed in the User's web browser on their PC.

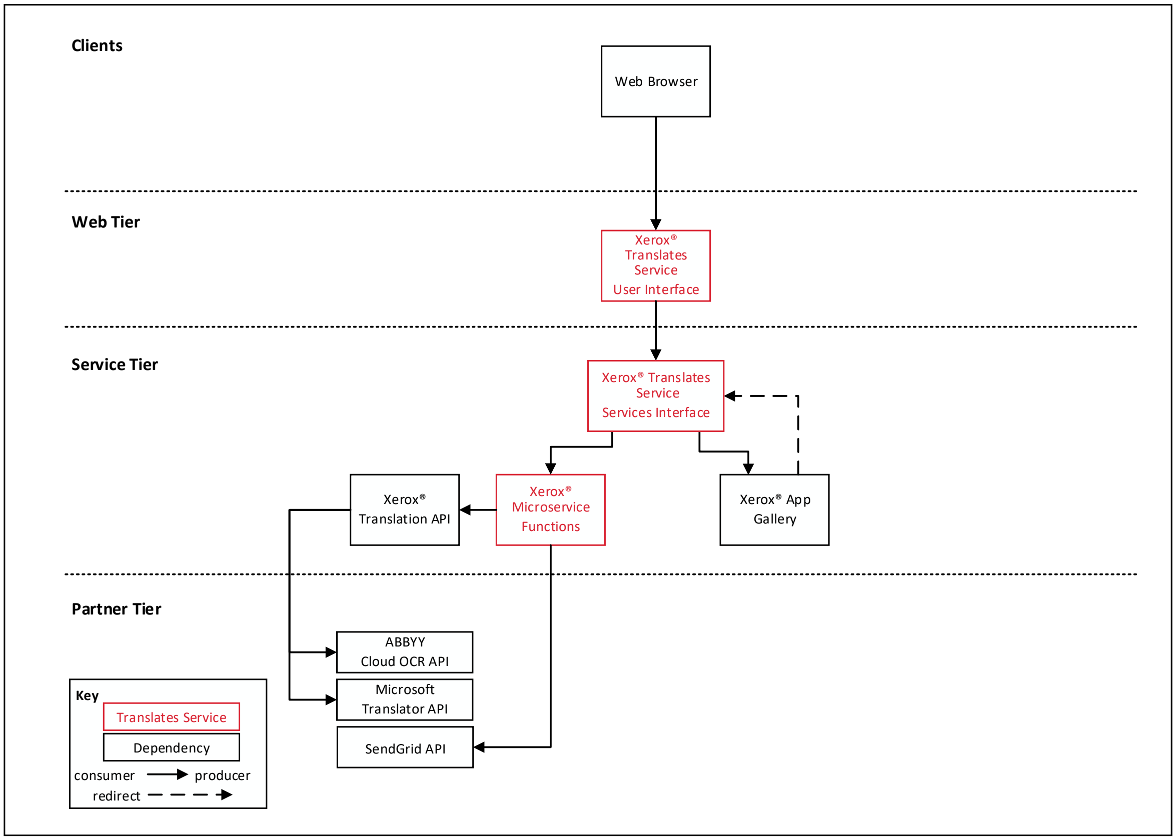
Xerox® Translates Service Services Interface

The Xerox® Translates Service Services Interface component is hosted on the Microsoft Azure Cloud System. The component provides the business logic services for the application.

Xerox® Microservice Functions

The Microservice Functions component is a set of Microsoft Azure Functions hosted on the Microsoft Azure Cloud System. The various microservice functions interface with a host of 3rd Party APIs to perform specific operations like Language Translation and Email.

Architecture Diagram



Workflows

Execute Translation workflow

Step 1: User enters the Xerox® Translates Service URL in a web browser on their PC/Laptop/Tablet.

Step 2: User selects the “Log In” button and enters their account username and password.

Step 3: The Web App displays the Translation workflow.

Step 4: User opens the Translation workflow.

Step 5: User navigates to and selects the input file for translation.

Step 6: User selects the language of the input file, the output filename, and the language in which to translate for the output file.

Step 7: User defines the settings for where to put the translated output file. (Email or Save to Local File).

Step 8: User selects Run button to start the execution of the Translation workflow.

Step 9A: If Email was defined as the output setting, then an email is sent to the specified recipients with a link to download the translated output file.

Step 9B: If Save to Local File was defined as the output setting, then the translated output file is saved to the specified location.

3. 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 2 Additional Resources