Information Assurance Disclosure of Xerox® Connect App for Remark Test Grading

1. Introduction

Xerox® Connect App for Remark Test Grading (TG) is a workflow solution that connects Xerox® Multifunction Printers (MFP) to the Gravic Remark Test Grading Cloud. Print, grading, and viewing results of tests is easy and convenient from Xerox® MFP devices without the need of a computer, servers, 3rd party scan equipment, or manual processing of test and results. This reduces time and cost with ensuring privacy and security.

1.1. Purpose

The purpose of the Information Assurance Disclosure (IAD) is to disclose information for TG 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® TG 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® TG 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 TG relative to Information Assurance (IA).

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

It is assumed that the reader is familiar with the TG app; as such, some user actions are not described in detail.

1.3. 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.

2. Description and Details

2.1. Overview

The Xerox® TG app provides three primary workflows:

- Print Tests
- Grade Tests
- Review & Print/Email results

Each workflow facilitates a combination of the steps:

- App hosting
- Authentication
- Selection
- Scanning
- Printing
- Emailing
- SNMP & device webservice calls

2.2 App Hosting

The Xerox® TG app consists of two key components, the device app and the API. The device app is a ConnectKey / EIP webapp and the API is a REST API, both are served by webservers in the cloud.

2.3. Authentication

Authentication consists of 2 key steps.

User creation: A new user is required to link/connect their Gravic Remark Cloud (GRC) account to the device. Adding themselves requests their username and password. These values are passed through the Xerox® TG Application Programming Interface (TG-API) and forwarded onto the Remark Cloud API (RC-API). An OAuth login token is returned to the device which is used for further interactions. At this time, the user is prompted for a PIN to facilitate convenient login.

The user's token, along with their name as it appears in the GRC and email address (to ensure no duplicate entries) is stored on the Xerox® device in the TG app's local storage.

User login: Once a user has linked their account to the TG app, they can select themselves off the user list and key in their chosen PIN. Once validated, the TG app will refresh the stored token, via TG-API and subsequently RC-API, allowing the user the ability to use the app for the given session.

The token is updated on the local device once refreshed.

2.4. Selection

At various steps in the application the user may be prompted to make selections, these include Class, Tests, Students, and Reports. These lists are dynamic and driven by API calls to the TG-API with the user's OAuth token.

2.5. Scanning

When scanning tests for grading, documents are scanned and submitted to the TG-API. Due to the nature of the Xerox® EIP scanning workflow design, the users OAuth token is temporary persisted (encrypted) in the TG-API database. As the scan is received by the TG-API it is forwarded onto the RC-API along with the temporarily persisted OAuth token. Once the scan process is complete this token is deleted from the database. If the scan process is interrupted, the token value will be removed by the TG-API privacy workflow which removes old records. This workflow is executed multiple times per hour.

2.6. Printing

When printing tests or reports, the request is sent to the TG-API along with the user's OAuth token. These values are forwarded to the RC-API and the relevant reports are generated. These reports are sent back to the TG-API where they are temporarily persisted. A TG-API URL link to these reports is sent to the Xerox® device for use with Pull-Print. These URLs are short live and removed upon expiry.

2.7. Emailing

In conjunction with printing, the user can choose to email reports to themselves or to students. In both cases the request to email is sent to the TG-API along with the OAuth token and this request is forwarded to the RC-API. During this workflow the RC-API manages the email process and at not time does the TG-API store any user or report details.

2.8. SNMP & Device Webservice Calls

During standard usage of the TG app, local calls to SNMP are initiated to pull relevant details such as device language and paper size preferences. The initiation of scan, print, and the usage of internal graphical components are handled though these local webservice calls

3. Security

3.1. Hosting

The Xerox® TG-API and the TG EIP app 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

3.2. Secure Web Communications

All web communications between servers and Xerox® devices are encrypted using HTTP Secure (https).

3.3. Encryption

When required, the user's OAuth token is persisted on the device and in the cloud (temporarily). While at rest, this token is salted and encrypted using AES-256. Token encryption and decryption is done on the server. The Xerox® device has no internal means to decrypt this value.

3.4. Data

It should be noted that report data is temporarily stored in our Test Grading service while scans and student grades are forwarded to Gravic and stored / handled by them. Moreover, scans of tests are sent and passed through to Gravic while class, test and student lists, along with result information is pulled for display on the Xerox® device (this is not persisted anywhere). Reports are pulled for printing."

4. Ports

4.1. App & API

The Xerox® TG app and TG-API require that the device is able to communicate over port 443 outside the client's network.