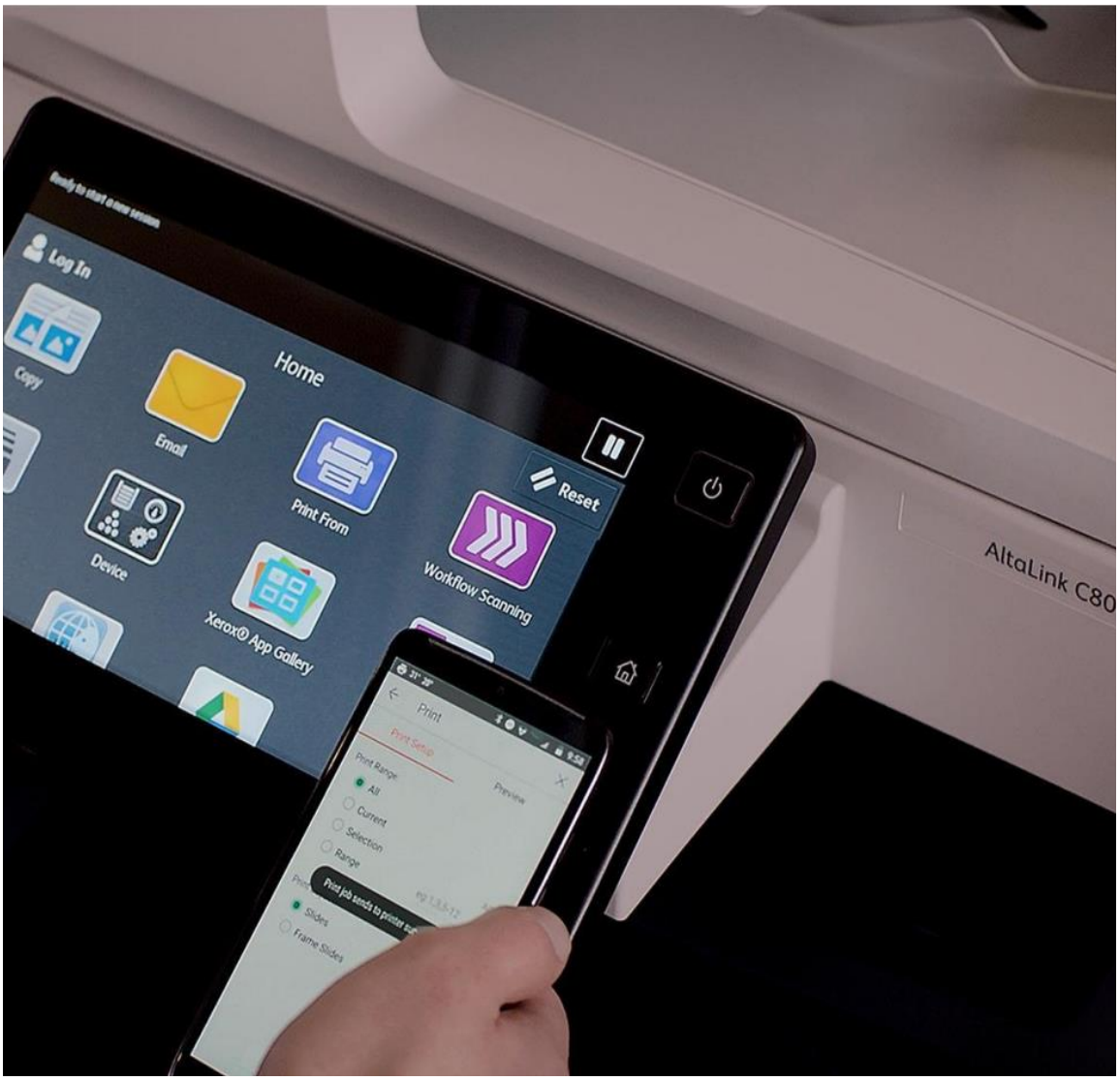
Xerox Security Guide

Xerox® ID Checker App



xerox™

Document Version: 1.0 (July 2020).

Contents

1. Introduction

Purpose

Xerox® ID Checker is a Xerox® Gallery App that allows users to quickly scan and verify a selection of identification documents, including passports and driver's licenses[1], right on a Xerox® device. Xerox® ID Checker utilizes state of the art technology to automatically read and process dozens of fields and characteristics to confirm whether an ID is valid or not. Once the ID has been verified, users can print or email themselves a certificate (PDF), which displays the authenticity score, scan images, and document data of the processed ID. The user can also email themselves the scanned ID images or generated JSON data file.

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

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

[1] The list of available IDs depends on the country. Please see the Customer Support Forum for a full list of supported countries and available ID types.

2. Product Description

Overview

Xerox® ID Checker consists of two primary workflows. The two workflows are:

- Scan a single-sided ID
- Scan a double-sided ID

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

- App Hosting
- Scanning
- ID Verification
- Email
- Printing
- SNMP & Device Webservice Calls

App Hosting

Xerox® ID Checker consists of three key components: the device app, the API, and the associated database. The device app is a Xerox® ConnectKey App/EIP web app and the API is a REST API.

Scanning

When a user scans a single or double-sided ID, the scan images are submitted to the ID verification API for processing. When processing is complete, the verification results are returned. The scan images are temporarily persisted while in transit to/from the ID verification API.

ID Verification

The first step in the ID verification workflow(s) is choosing a country and ID type. The most recently used countries are always at the top of the list and are stored in the device's local storage. Once a country and ID type are selected, the user can scan the front-side, or front-side *and* back-side of an ID and submit the scan image(s) to the ID verification API for processing. The scan images (JPEG) are temporarily persisted in Azure Blob storage for a maximum of 15 minutes, while in transit to/from the API.

The ID's characteristics and attributes are checked by the API to determine whether they are valid or not. If any of the checks fail, the ID is considered invalid.

Once processing is complete, the API returns a list of results in the form of a JSON file, as well as a PDF certificate that displays the authenticity score, scan images, and document data of the processed ID.

Email

Near the end of the ID verification workflow, the user has the option to email the following:

- A certificate that's generated by the ID verification API for valid *and* invalid certificates
- A JSON file that summarizes an ID's attributes, confidence scores, and more
- The JPEG image(s) of the scanned valid, expired, or fake ID. These images could contain PII

The user can send all three options as email attachments or secure Azure links in the body of the emails. If the user chooses attachment, the file is stored in Azure Blob storage for a maximum of 15 minutes. If the user chooses to send the files as secure links, the files are stored for 7 days.

The email addresses that the user enters in the app are stored in the device's local storage.

To email an ID's JSON file, the user must enable the option in the app. The page to enable or disable the option is locked behind a password. The password is set upon install in the Xerox App Gallery. It's hashed in the shell app using salted SHA1. The salt is 32 characters long. The frontend validates the hash to authenticate and verify the user.

All emails come from noreply@xeroxidchecker.com.

Printing

A user has the option to print the generated PDF certificate for valid or invalid IDs on all supported devices.

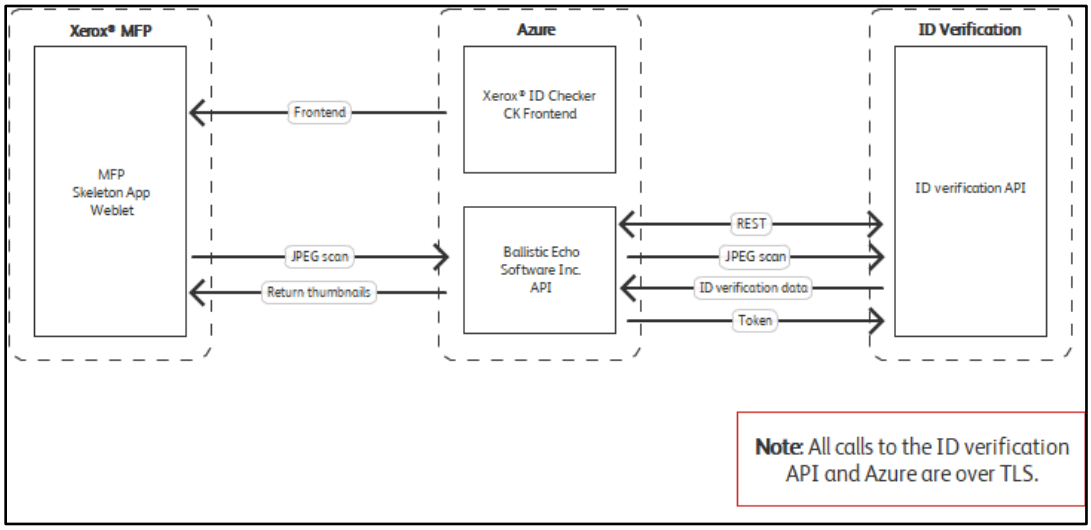
SNMP & Device Webservice Calls

During standard usage of Xerox® ID Checker, local calls to SNMP are initiated to pull relevant details such as device language. The initiation of scan and the usage of internal graphical components are also handled through these local web service calls.

Architecture and Workflows

Architecture Diagram

Below is a diagram that outlines what data is being processed and transmitted between each service:



3. User Data Protection

User Data Protection within the Product

The Xerox® ID Checker API and 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

User Data in Transit

Secure Network Communications

Xerox® ID Checker and the API require that the device can communicate over port 443 outside the client's network. All web communications between the APIs and Xerox® Devices are encrypted using HTTP Secure (TLS).

Images of the scanned documents are temporarily persisted in Azure Blob storage (raw image, thumbnails, etc.) for a maximum of 15 minutes, while in transit to/from the ID verification API. The raw image is not accessible from anything other than the server-side code.

If the user chooses to send the generated certificate, JSON results file, or scan images as email attachments, they are stored in Azure Blob storage for a maximum of 15 minutes, as stated above. If the user chooses to send them as secure Azure links in the body of the email, they are stored for 7 days. That way, users have up to 7 days to open the link and retrieve the file(s).

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