January 2019

Xerox® App Gallery 5.1
Information Assurance Disclosure

BR18116

Contents

Introduction 2
Purpose 2
Target Audience 3
Glossary 3
Disclaimer 3
System Workflows 5
Account Creation Workflows: 5
Web Portal Gallery Account Creation and Activation Workflow 5
Gallery App Gallery Account Creation and Activation 5
Channel Partner Account Creation and Activation Workflow 6
Developer Account Creation and Activation Workflow 6
Customer Account Creation and Activation Workflow 7
App Creation Workflows: 8
Create ConnectKey Info App Workflow 8
Create ConnectKey Scan Apps Workflow 8
Create ConnectKey Print Apps Workflow 9
Browse the App Gallery Workflows 10
Browse App Gallery from Web Portal 10
Browse App Gallery from Device 10
Purchase and Installation Workflows: 11
Free App Installation Workflow 11
Trial Installation Workflow 11
Purchase Workflow – Per Device 12
Purchase workflow – Unlimited Devices 13
App Entitlement Check workflow 14
App Usage Reporting and Entitlement Check workflow 14
Configure App Workflow 15
Download App Workflow 16
Security Description 17
Microsoft Azure Cloud Computing Platform and Services 18
Microsoft Azure Security Highlights 18
Xerox® App Gallery Network Protocols and Port Numbers Diagram 19
Individual System Components 20
Web Browser 20
Xerox® App Gallery 21
Office365 Exchange 22
2Checkout Service 22
Payment Processors 23

Devices ... 23
Xerox® App Gallery App ... 23
Developer App ... 24
App Wrapper ... 24
Cloud Repository Designer Apps ... 24
Xerox® Cloud Repository Middleware ... 25
Xerox Document Conversion ... 26
Customer Repository Designer Apps ... 26
Customer Repository Server ... 26
Communication between System Components ... 27
Web Browser and the App Gallery ... 27
Web Browser Extensions and Devices ... 27
App Gallery and Office365 Exchange ... 27
App Gallery App and App Gallery ... 27
App Gallery and Cloud Repository Middleware ... 28
Cloud Repository Designer Apps and Cloud Resident Repositories ... 28
Middleware Azure Cloud Service and the Middleware Azure Cloud Storage ... 29
Customer Repository Designer App and Customer Repository Server ... 29
Middleware Azure Cloud Service and Xerox Document Conversion ... 29
App Wrapper and App Gallery ... 29
App Gallery and the 2Checkout system ... 29
2Checkout system and Payment Processors ... 30
Software Updates ... 31
Xerox® App Gallery – Web Application ... 31
Xerox® App Gallery App ... 31
Browser Add-In/Extension ... 31
Xerox® Cloud Repository Middleware ... 32
PII Data Management ... 33
Personal Data Maintained by the Xerox App Gallery: ... 33
Personal Data Maintained by the e-commerce provider: ... 33
App Gallery 5.x Territorial Map ... 34
App Gallery 5.x PII dataflow ... 35
The Role of Xerox® ... 36
Response to known vulnerabilities ... 36

Introduction

The Xerox® App Gallery is a:

1. Marketplace that allows Gallery users to browse Xerox® ConnectKey® device Apps and purchase and/or install the Apps on the devices themselves.
2. Xerox® workflow solution that allows the creation of Xerox® ConnectKey® device Apps, by Channel Partners, and the placement of the Apps on the devices themselves. There are several App types:
    a. Information,
    b. Scan To E-Mail,
    c. Scan To Multiple Destinations,
    d. Scan To Office 365 SharePoint Online,
    e. Scan To Dropbox,
    f. Scan To OneDrive,
    g. Scan to Box,
    h. Scan to GoogleDrive,
    i. Print From URL,
    j. Print From Office 365 SharePoint Online,
    k. Print From Dropbox,
    l. Print From OneDrive,
    m. Print From Box, and
    n. Print From GoogleDrive

Purpose

The purpose of this document is to disclose information for the Xerox® App Gallery with respect to system security. System Security, for this paper, is defined as follows:

1. How user information is stored and transmitted
2. How the product behaves in a networked environment
3. How the product may be accessed, both locally and remotely
4. How applications are purchased

NOTE: The customer must be responsible for the security of their network and the Xerox® App Gallery product 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 Xerox® App Gallery relative to Information Assurance (IA).

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

Target Audience

The target audience for this document is Xerox field personnel and customers concerned with IT security.

Glossary

Term	Definition
App Developer	The person or organization that creates ConnectKey Apps
CK Apps	ConnectKey Apps – An Application (App) executing on the Device
Content	The digital representation of a scanned document. Or the Digital representation of a document to be printed.
Configuration Data	Name:Value pairs consisting of Names defined by the App Developer; and Values supplied by the gallery user prior to App installation on the Device.
Data Subject	Any person whose personal data is being collected, held or processed.
Device	A Multifunction Device (MFD)
Designer App	A set of pre-defined Apps which may be customized by using the "My Apps / Create App" feature of the App Gallery
Developer App	An app created by the App Developer to implement a particular feature or function utilizing Device capabilities
Downloaded Weblet	A gallery-created weblet that has been downloaded by the gallery user - typically to media. The gallery user then employs non-gallery methods to install the weblet on a Device. The gallery knows nothing of this installation.
e-commerce provider	2Checkout Inc. https://www.2checkout.com/ which acts as Merchant of Record for Xerox App Gallery e-commerce transactions.
GPDR	The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU).
Payment Processor	A business that initiates Credit Card transactions on behalf of the e-commerce provider.
Personal Data	Any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.
PII	Personally Identifiable Information
Weblet	Another term for ConnectKey Apps
XAG	Xerox® App Gallery

Disclaimer

This document does not disclose the information security arrangements of non-Xerox systems with which the App Gallery interacts. Examples of such systems include 2Checkout and Azure. Nor does this document disclose interactions these systems may have with other systems, such as Payment Processors. The responsibility for disclosing the security arrangements of non-Xerox systems lies with the providers of these non-Xerox systems.

The information in this document is accurate to the best knowledge of the authors; and is provided without warranty of any kind. In no event shall Xerox Corporation be liable for any damages whatsoever as a result of user's use or disregard of the information provided in this document which includes direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox Corporation has been advised of the possibility of such damages.

System Workflows

Account Creation Workflows:

Web Portal Gallery Account Creation and Activation Workflow

Step 1: User connects to the Xerox® App Gallery login web page.

Step 2: User selects option to create a Xerox® App Gallery account.

Step 3: User enters required information to create an account and submits the request.

Step 4: Xerox® App Gallery creates and activates account

Step 5: User is then logged into the account.

Gallery App Gallery Account Creation and Activation

Step 1: User starts the Xerox® App Gallery App on a Device.

Step 2: User selects option to create a Xerox® App Gallery account.

Step 3: User enters required information to create an account and submits the request.

Step 4: Xerox® App Gallery creates and activates account

Step 5: User is then logged into the account.

Channel Partner Account Creation and Activation Workflow

Step 1: Account user logs into Xerox® App Gallery with an Admin or OPCO account.

Step 2: User selects option to create a Channel Partner account by invitation.

Step 3: User enters Channel Partner e-mail, first name, last name and company name.

Step 4: Invitation e-mail is sent and Channel Partner account is created.

Step 5: Channel Partner receives e-mail with link to activate the Channel Partner account.

Step 6: Channel Partner clicks on the link in the e-mail to complete account creation.

Step 7: User enters remaining required information to complete account creation.

Step 8: Xerox® App Gallery activates account.

Step 9: User is then logged into the account.

Developer Account Creation and Activation Workflow

Step 1: User connects to the developer specific Xerox® App Gallery login web page.

Step 2: User selects option to create a Xerox® App Gallery developer account.

Step 3: User enters required information to create a developer account and submits the request.

Step 4: Xerox® App Gallery creates and activates the developer account

Step 5: User is then logged into the developer account.

Customer Account Creation and Activation Workflow

Step 1: Channel Partner connects to the Xerox® App Gallery login web page.

Step 2: Channel Partner selects option to create a customer account by invitation.

Step 3: Channel Partner enters customer e-mail.

Step 4: Invitation e-mail is sent to the supplied e-mail address.

Step 5: Customer receives e-mail with link to complete account creation.

Step 6: User enters remaining required information to complete account creation.

Step 7: Xerox® App Gallery activates account.

Step 8: User is then logged into the account.

App Creation Workflows:

Create ConnectKey Info App Workflow

Step 1: Channel Partner logs in to Xerox® App Gallery.

Step 2: Channel Partner selects the option to create a new application.

Step 3: Channel Partner selects Xerox® ConnectKey® Info App as the type of app to create.

Step 4: Channel Partner enters the information required and selects the layout of app and customizes the app to meet user's needs.

Step 5: Channel Partner selects Done and app is added to list of apps available from their account.

Create ConnectKey Scan Apps Workflow

Step 1: Channel Partner logs into Xerox® App Gallery.

Step 2: Channel Partner selects the option to create a new application

Step 3: Channel Partner selects to create a Xerox® ConnectKey® Scan App type (i.e. e-mail, multi-destination, Office 365 SharePoint online, etc.).

Step 4: Channel Partner selects if a destination can be entered or if a default value is displayed.

Step 5: Channel Partner sets which scan options will be displayed.

Step 6: Channel Partner enters the information required and sets up layout of the app and customizes the app to meet Channel Partner's needs.

Step 7: Channel Partner selects Done and the app is added to list of apps available from their account.

Create ConnectKey Print Apps Workflow

Step 1: Channel Partner logs into Xerox® App Gallery.

Step 2: Channel Partner selects the option to create a new application

Step 3: Channel Partner selects to create a Xerox® ConnectKey® Print App type. (i.e. from url, Office 365 SharePoint online. Dropbox, etc.)

Step 4: Channel Partner sets print options.

Step 5: Channel Partner sets up layout of the app and customizes the app to meet the Channel Partner's needs.

Step 6: Channel Partner selects Done and the app is added to list of apps available from their account.

Browse the App Gallery Workflows

Browse App Gallery from Web Portal

Step 1: User logs in to Xerox® App Gallery.

Step 2: User selects the All Apps tab.

Step 3: User can browse through the apps in the app gallery.

Step 4: User can select an app and view detailed information.

Step 5: User will see the detailed information for the app including description, restrictions, screenshots and legal disclosures.

Browse App Gallery from Device

Step 1: User starts the Xerox® App Gallery App on a Device.

Step 2: User selects the All Apps tab.

Step 3: User can browse through the apps in the app gallery.

Step 4: User can select an app and view detailed information.

Step 5: User will see the detailed information for the app including description, restrictions, screenshots and legal disclosures.

Purchase and Installation Workflows:

Free App Installation Workflow

Step 1: User logs into Xerox® App Gallery.

Step 2: User navigates to the App Details for the app they want to install and clicks on the "Install" button.

Step 3: User selects the devices where the app is to be installed and selects install.

Step 4: Xerox® App Gallery installs the app to the selected devices.

Step 5: If the app is a cloud repository app, the app and devices are registered with the cloud middleware.

Trial Installation Workflow

Step 1: User logs into Xerox® App Gallery.

Step 2: User clicks on the "Try It" button in the Gallery's My App/ App Details View.

Step 3: User selects the Devices where the App is to be installed for the Trial.

Step 4: Xerox® App Gallery installs the app to the selected devices.

Purchase Workflow – Per Device

Step 1: User logs into Xerox® App Gallery.

Step 2: User clicks on the Buy/Subscribe button in the Gallery's My App/ App Details View.

Step 3: User selects the desired Price Option. (This step is omitted for Apps with only a single Price Option).

Step 4: User selects the Devices for which the App is being purchased.

Step 5: App Gallery initiates a purchase transaction with the 2Checkout system.

Step 6: User Confirms purchase by clicking the "Place Order" button in the 2Checkout shopping cart. For first-time purchases, 2Checkout will request personal information including: email address, physical address, Credit Card Information.

Step 7: 2Checkout processes the order by debiting the User's credit card account. This involves transactions with various payment processors located throughout the world.

Step 8: 2Checkout presents a "Thank You" page to the user.

Step 9: User presses the Done button on the "Thank You" page.

Step 10: Xerox® App Gallery installs the app to the selected devices.

Purchase workflow – Unlimited Devices

Step 1: User logs into Xerox® App Gallery.

Step 2: User clicks on the Buy/Subscribe button in the Gallery's My App/ App Details View.

Step 3: User selects the desired Price Option. (This step is omitted for Apps with only a single Price Option.)

Step 4: App Gallery initiates a purchase transaction with the 2Checkout system.

Step 5: User Confirms purchase by clicking the "Place Order" button in the 2Checkout shopping cart. For first-time purchases, 2Checkout will request personal information including: email address, physical address, Credit Card Information.

Step 6: 2Checkout processes the order by debiting the User's credit card account. This involves transactions with various payment processors located throughout the world.

Step 7: 2Checkout presents a "Thank You" page to the user.

Step 8: User presses the Done button on the "Thank You" page.

Step 9: App Gallery presents a list of Devices for the user to select for installation.

Step 10: User selects the Devices where the App is to be installed.

Step 11: Xerox® App Gallery installs the app to the selected devices.

App Entitlement Check workflow

Step 1: User launches the App at the Device

Step 2: App Wrapper checks with App Gallery for entitlement to execute the App.

Step 3: If App Gallery entitlement check passes, the App is allowed to execute on the Device.

Step 4: If the App Gallery entitlement check fails, the user is informed that the app is no longer entitled to execute because 1)Trial has Expired, 2) Subscription has expired, or 3) Development period has expired.

App Usage Reporting and Entitlement Check workflow

Step 1: User launches the App at the Device

Step 2: App Wrapper checks with App Gallery for entitlement to execute, as described in the "App Entitlement Check Workflow" section.

Step 3: User performs an App function (i.e. Scan, Print, etc.)

Step 4: Apps defined with a Usage Based licensing model, report the usage consumed by the App function to the App Gallery.

Step 5: App rechecks with App Gallery for continued entitlement to execute. App behaves as designed by the App Developer when there is no longer entitlement.

Configure App Workflow

Step 1: User logs into Xerox® App Gallery.

Step 2: Authorized user selects the App's "configure" option.

Step 3: Authorized user supplies "Values" for each of the configuration elements defined by the App Developer.

Step 4: Authorized user saves the Configuration Data to the App Gallery.

Step 5: Authorized user elects to Install / Download the App.

Step 6: App Gallery creates a weblet that includes the current Configuration Data.

Step 7: App Gallery Installs / Downloads the weblet.

Step 8: User launches the App at the Device

Step 9: App extracts the Configuration Data from the weblet and honors it during App execution.

Download App Workflow

Step 1: User logs into Xerox® App Gallery.

Step 2: Authorized user selects the option to Download a weblet.

Step 3: App Gallery creates a weblet that includes the current Configuration Data

Step 4: App Gallery downloads the weblet to the user's browser.

Step 5: Gallery user installs the App weblet on devices using media.

Note: once the weblet has been downloaded, the weblet is outside the sphere of gallery interest and control. The App Gallery has no knowledge of the Devices a downloaded weblet may be installed on, what version downloaded weblet is installed on a Device, or what Configuration downloaded weblet is installed on a Device.

Security Description

The security considerations are as follows:

1. The security of the Xerox® App Gallery hosted in Microsoft Azure
2. The security of the apps created by the Xerox® App Gallery
3. The security of the user account information required by the Xerox® App Gallery system
4. The security of the customer account information required by the 2Checkout system.
5. The security of the customer credit card information required by the Payment Processor.
6. The security of the devices registered within the system by the user
7. The security of configuration data stored in the Xerox® App Gallery and used by Apps.

Information travels through multiple system components over a combination of wired and wireless networks. All use normal, industry-standard technologies and built-in security capabilities. These capabilities do need to be enabled, and the choice of which are used at each point in the system varies. This section captures the security considerations of Xerox® App Gallery in the areas shown below:

1) Microsoft Azure Cloud Computing Platform and Services
2) Protocols and Port numbers used by the system
3) Individual system components
4) Communication between system components

Microsoft Azure Cloud Computing Platform and Services

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.

Microsoft Azure Security Highlights

These Security highlights are relevant to the App Gallery system.

General Azure security

- Azure Security Center
- Azure Key Vault
- Log Analytics

Storage security

- Azure Storage Service Encryption
- Azure Storage Account Keys
- Azure Storage Analytics

Database security

- Azure SQL Firewall
- Azure SQL Connection Encryption
- Azure SQL Always Encryption
- Azure SQL Transparent Data Encryption
- Azure SQL Database Auditing

Identity and access management

- Azure Role Based Access Control
- Azure Active Directory
- Azure Active Directory Domain Services
- Azure Multi-Factor Authentication

Networking

- Network Security Groups
- Azure Traffic Manager

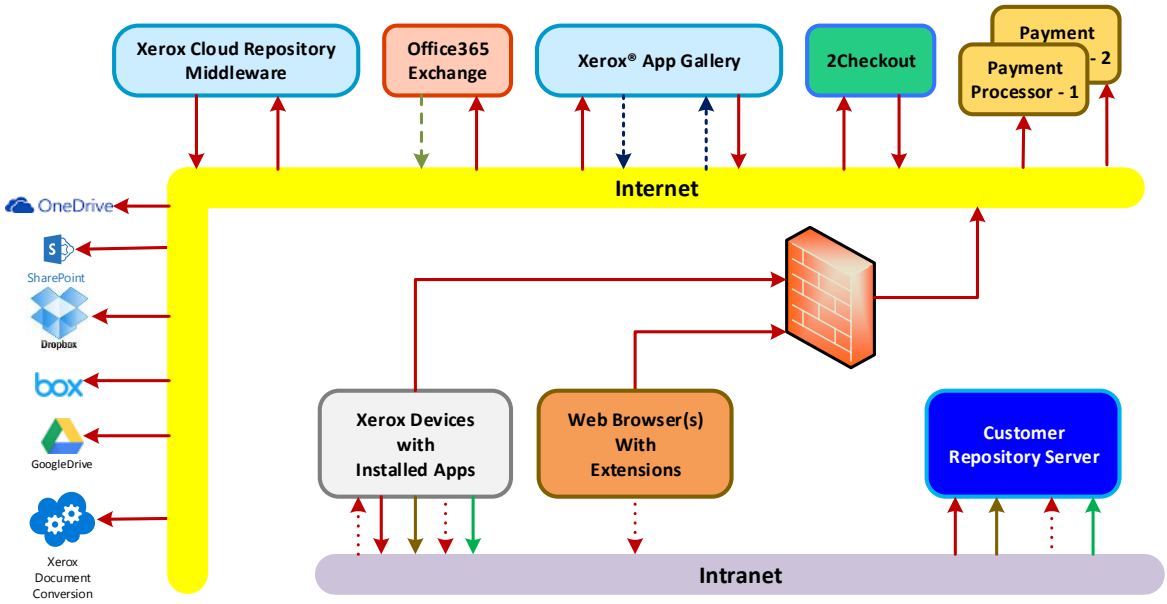
Please visit the Microsoft Azure Security web site for more information:
https://www.microsoft.com/en-us/trustcenter/security/azure-security

Xerox® App Gallery Network Protocols and Port Numbers Diagram

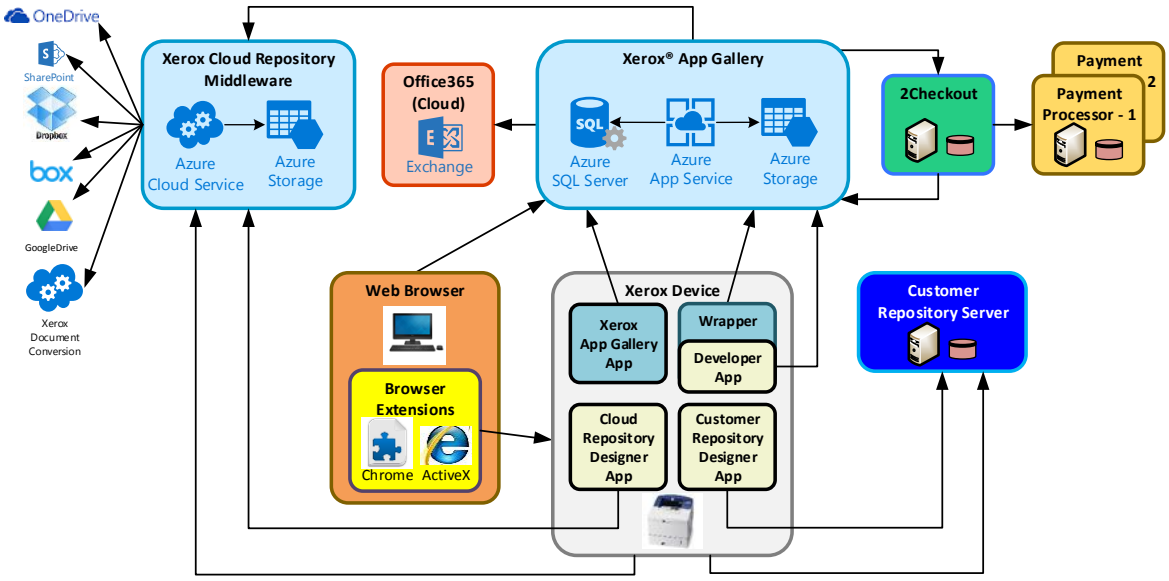
This Table and diagram shows the protocols used in the system. Port numbers are not configurable.

The Firewall only requires port 443 to be open for outbound communications. No inbound ports need to be opened for the system to function.

Arrow	Protocol	Port
→	HTTPS	443
- - →	SMTP	25
- - →	TCP	1433
→	FTP	21
→	SMB	445
····→	HTTP	80



Individual System Components



Web Browser

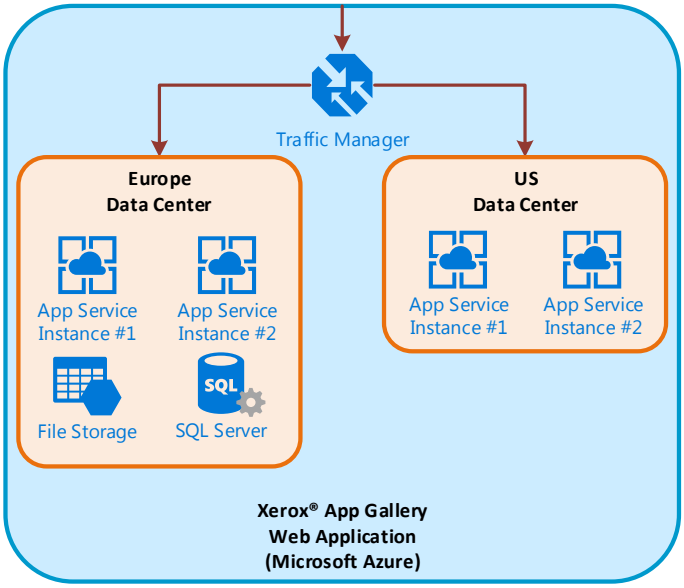
Access to the Xerox® App Gallery is allowed through the following list of supported Web Browsers: Microsoft Internet Explorer v11.0 or higher and Google Chrome v60.0 or higher.

Browser Extensions

In addition, each supported browser requires the installation of a Browser Add-On/Extension. The Browser Add-On/Extension is required to access the Xerox Device for adding/removing devices in a user's account as well as the install/update/uninstall of Apps. The Microsoft Internet Explorer Browser uses an ActiveX control. The Google Chrome Browser uses a standard Chrome Extension. The ActiveX control is hosted in the App Gallery web portal for download and installation by the IE Browser. The Chrome Extension is hosted in Google's Chrome web store for download and installation by the Chrome Browser.

Xerox® App Gallery

The Xerox® App Gallery is a web application hosted in the Microsoft Azure Cloud Computing Platform. The web application consists of web pages (Azure App Service), file storage (Azure Storage) and a database (Azure SQL Server). Instances of the web pages are hosted in two different Azure data centers, while the file storage and database are hosted in a single Azure data center. The Azure data centers used by the App Gallery are located in the European Union and the United States. Azure "Traffic Manager" routes incoming requests to an instance, running in an Azure data center, based on the lowest network latency.



Azure App Services

The web pages, for the Xerox® App Gallery, are deployed in a Microsoft Azure App Service. All web pages are accessed via HTTPS from a Web Browser. All communications to and from the Xerox® App Gallery App Service are over HTTPS. Data is transmitted securely and is protected by TLS security for both upload and download. The minimum TLS version used is 1.2.

Xerox® App Gallery users must authenticate with the Xerox® App Gallery Service to access the web pages that contain personal information. Authentication with the Xerox® App Gallery Service requires the entry of an email address and password known by the system. Passwords are required to be a minimum of 8 characters and contain at least one character that meets 3 out of 4 of the following character restrictions: Upper Case Alpha, Lower Case Alpha, Numeric, Punctuation.

Once authenticated, the user can view and modify:

1. Account profile
2. All apps created by the user through the App Gallery system
3. All app configuration data created by the user through the App Gallery system
4. All devices registered by the user in the App Gallery system

Non-authenticated users may access the non-restricted Xerox® App Gallery web pages. This includes viewing:

1. All Publicly available Apps

2. Details for a Publicly available App

Azure SQL Server

Azure SQL server stores and protects the data used by the Xerox® App Gallery. Both "Advanced Threat Protection" and "Transparent data encryption" are enabled. In addition, the database is encrypted. Communications to the Azure SQL Server are only by the Azure App Services using TCP over Port 1433.

Azure Cloud Storage

Azure Cloud Storage contains a file repository used by the App Gallery. Access requires an Account Name and Access Key, which are securely stored in the configuration for each Azure App Service deployment. Only authorized Xerox IT personnel have access to these keys via Microsoft's Azure Management Portal.

Office365 Exchange

The solution provides for an Office 365 Exchange email service, hosted by Microsoft. The email service sends Xerox® App Gallery email notices to Gallery Account owners using SMTP.

2Checkout Service

Xerox has partnered with 2Checkout, formerly known as Avangate Inc., (https://www.2checkout.com/) to act as Merchant of Record for Xerox® App Gallery e-commerce transactions. The 2Checkout platform provides the e-commerce solution with a scalable multi-tenant SaaS eCommerce, payments and subscription management capability:

- PCI (Payment Card Industry Data Security Standard) compliance
- Security Certifications
- International Banking relationships
- Tax and VAT compliance
- Fraud and Risk management

This partnership allows App licenses to be sold in gallery-supported countries world-wide.

The e-commerce provider maintains an account for each it's 'customers' (i.e. Gallery users who make App purchases.) The customer account contains user data such as the customer's email address, company, and physical address. 2Checkout maintains a history of the customers' Credit Card transactions; and maintains Credit Card information on file as a convenience to the customer.

The 2Checkout Service is accessed via 40+ globally distributed proxies hosted by a 3rd party service provider, providing DDoS mitigation, load balancing, failover, and security services.

- There are two 2Checkout Datacenters located within the European Union:
  - Eastern Europe
  - Western Europe
- One 2Checkout Datacenter is located within North America
  - Eastern United States

- 2Checkout utilizes one Cloud storage provider for offsite storage of data backups, protected using industry standard strong encryption.
- 2Checkout utilizes multiple payment networks located in North America, Asia, and the European Union

For a 2Checkout GDPR statement go to: https://www.2checkout.com/policies/gdpr-compliance-statement . For further IAD concerning 2Checkout, contact: http://www.avangate.com/legal.php.

Payment Processors

2Checkout interacts with several different Payment Processors to debit customer (i.e. App Gallery user) credit card accounts. Payment Processors are located in various geographies, and specialize in transactions denominated in one or more currencies. The Xerox App Gallery has no direct interaction with Payment Processors. For further IAD concerning 2Checkout and its interactions with Payment Processors, contact: http://www.avangate.com/legal.php.

Devices

Xerox® devices have a variety of security features that can be employed to increase security. Availability of these features depends based on model. It is the customer's responsibility to understand and implement appropriate controls for devices behavior.

Some examples are as follows:

1. Xerox Image Overwrite electronically shreds information stored on the hard drive of devices as part of the routine job process.
2. Data Encryption uses state of the art encryption technology on data stored within the device as well as for data in motion in and out of the device.

For more information about the above examples as well as for other device security related technologies please see http://www.xerox.com/information-security/product-security.

The Xerox® App Gallery supports Xerox® ConnectKey, AltaLink and VersaLink devices. It is the customer's responsibility to understand the security features of these Xerox® devices, which are used in the Xerox® App Gallery system.

Xerox® App Gallery App

The Xerox® App Gallery App is an application that comes pre-installed on Xerox devices. The purpose of the App is to provide allow access to the Xerox App gallery at the device. The App allows users, at the device, to Browse the Apps available in the Gallery, login to their account and install/upgrade one or more Apps. Users login to their account by supplying their email address and password. Users can also create a Gallery account if one was not created using the Xerox® App Gallery web application.

When a user with device admin privileges executes the App at the device and logs into their Gallery account, the App will give the user the option to have the credentials "remembered" at the device. If the user chooses to have the credentials "remembered", then any user who executes the Gallery App will automatically be logged into the Account. A user with device admin privileges also has the option to "clear" the "remembered" credentials from the device. The admin credentials are stored in the device browser's internal storage and can only be retrieved by the Xerox® App Gallery App.

Developer App

Xerox® App Gallery allows developers to generate Apps that can be purchased and/or installed on Xerox devices. Developer Apps utilize Xerox's EIP SDK to interface with the device to perform specific functions like printing and scanning.

In XAG 5.0, Developer Apps can also utilize the XAG ecommerce API when an App, that requires the purchase of a usage subscription, needs to report the usage consumed during the App execution.

In XAG 5.1, App Developers may define configuration elements for their Developer Apps. Configuration elements consist of Names defined by the App Developer; and Values supplied by the gallery user. Configuration data is stored by the App Gallery and used by the gallery when creating the weblet for Download/Installation. Configuration data is stored AES-encrypted in the weblet. At runtime, the App uses a gallery-supplied method to decrypt and extract configuration data from the weblet.

App Wrapper

As part of the process of uploading a new Developer App, the XAG 5.x system wraps the App. At runtime, the Wrapper performs an initial entitlement check with the App Gallery to determine if the App is entitled to run on the Device. If not entitled, the App will be prohibited from running. All 5.x Apps are wrapped prior to Publication. Once an App is Published to the Gallery, only Apps that require purchase are wrapped.

Apps that were uploaded prior to XAG 5.x are not wrapped and therefore do not interact with the App Gallery. However, the App Developer may publish a new Version of such an app that includes e-commerce features; in which case the XAG 5.x system will wrap the new App version.

Cloud Repository Designer Apps

Xerox® App Gallery currently generates applications that interface with multiple commercial cloud resident repositories. These apps allow users to scan documents to a supported cloud repository or print documents from a supported repository.

Office 365 SharePoint Online – this cloud repository requires users to have an account with them. The Xerox® App Gallery app requires the user to provide proper/valid credentials in order to gain access to the cloud repository. The credentials for Office 365 include a user ID and e-mail address which contains the Office 365 domain the user has permission to access. A password is also part of the credentials. With valid credentials, the Xerox® App Gallery app can browse the repository main site or team site, the libraries contained within and the folders in the libraries. The Xerox® App Gallery can generate an app to scan to Office 365 and an app to print from Office 365.

DropBox - this cloud repository requires users to have an account with them. It supports OAuth 2.0 authentication. The DropBox repository requires the user to provide proper/valid credentials in order to gain access to the cloud repository. The credentials for DropBox include a user ID which is the user's e-mail address and a password. With valid credentials, the Box repository asks for the user to give permission for the app to access the repository. Once given, the Xerox® App Gallery app can browse the repository's folders. The Xerox® App Gallery can generate and app to scan to DropBox and an app to print from DropBox.

Box - this cloud repository requires users to have an account with them. It supports OAuth 2.0 authentication. The Box repository requires the user to provide proper/valid credentials in order to gain access to the cloud repository. The credentials for Box include a user ID which

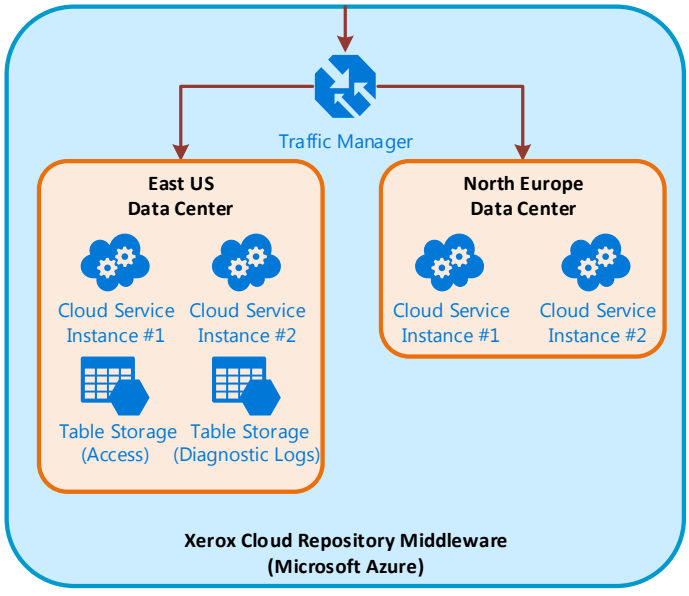
is the user's e-mail address and a password. With valid credentials, the Box repository asks for the user to give permission for the app to access the repository. Once given, the Xerox® App Gallery app can browse the repository's folders. The Xerox® App Gallery can generate an app to scan to Box and an app to print from Box.

Google Drive - this cloud repository requires users to have an account with them. It supports OAuth 2.0 authentication. The Google Drive repository requires the user to provide proper/valid credentials in order to gain access to the cloud repository. The credentials for Google Drive include a user ID which is the user's e-mail address and a password. With valid credentials, the Google Drive repository asks for the user to give permission for the app to access the repository. Once given, the Xerox® App Gallery app can browse the repository's folders. The Xerox® App Gallery can generate an app to scan to Google Drive and an app to print from Google Drive.

OneDrive - this cloud repository requires users to have an account with them. There are two account types, personal and business. Personal accounts support OAuth 2.0 authentication. The OneDrive repository requires the user to provide proper/valid credentials in order to gain access to the cloud repository. The credentials for OneDrive include a user ID which is the user's e-mail address and a password. With valid credentials, the OneDrive repository asks for the user to give permission for the app to access the repository. Once given, the Xerox® App Gallery app can browse the repository's folders. For business accounts, the user must provide a user id and password, which the app uses to authenticate the user. The Xerox® App Gallery can generate an app to scan to OneDrive and an app to print from OneDrive.

Xerox® Cloud Repository Middleware

The Xerox® Cloud Repository Middleware is a web application hosted in the Microsoft Azure Cloud Computing Platform. The web application consists of Web Service API's (Azure Cloud Service) and table storage (Azure Storage). Instances of the Azure Cloud Service are hosted in two different Azure data centers, while the Azure Table Storage is hosted in a single Azure data center. The Azure data centers used by the Cloud Repository Middleware are located in the European Union and the United States. Azure "Traffic Manager" routes incoming requests to an instance, running in an Azure data center, based on the lowest network latency.



Azure Cloud Service

The Azure Cloud Service, in the Cloud Repository Middleware, contains the Web Service APIs used to interface with the supported Cloud Resident Repositories and Xerox Document Conversion.

Azure Cloud Storage

The Azure Storage Tables, in the Cloud Repository Middleware, are used to store the list of authorized apps and devices that can access the Cloud Repository Middleware API. Azure Storage is also used to store diagnostic logs generated by the Azure Cloud Service. Access requires an Account Name and Access Key, which are stored and encrypted in each Azure Cloud Service instance.

Xerox Document Conversion

Xerox® Document Conversion is a service to convert non-print ready documents to a print ready a format. The service is hosted in an Azure VM Server. It is utilized for print jobs generated from the Xerox® App Gallery print apps for the third party cloud repositories.

Customer Repository Designer Apps

Xerox® App Gallery currently generates applications that interface with a customer hosted repository server using a variety of supported protocols. These generated apps can scan documents using FTP or SMB as well as print documents using HTTP/HTTPS.

Customer Repository Server

This server is configured and controlled by Xerox customers. It is the customer's responsibility to secure access to the server. A Customer Repository Server can be configured to allow for FTP, SMB and HTTP/HTTPS communications to allow for scanning and printing of documents.

Communication between System Components

Web Browser and the App Gallery

App Gallery software executing on Azure servers uses the HTTPS protocol for all communication with App Gallery Web Pages. The minimum TLS version used is 1.2. The protocol establishes an HTTPS secure connection with the App Gallery Service, which relies on the web page OS to validate the security certificate as part of creation of the TLS connection. The TLS certificate is issued by Comodo (a trusted certificate authority) and ensures that the App Gallery webserver is in communication with the user's web browser, and no third party can pretend to be that webserver or intercept traffic between the web browser and the webserver.

The App Gallery requires users to authenticate before they can access features involving personal information. Basic authentication is performed with the Xerox® App Gallery that transmits username and password information over the HTTPS protocol.

Once authentication is complete, data is passed between the Xerox® App Gallery executing on Azure servers and the Xerox® App Gallery Web Pages, to enable the features of the service within the Xerox® App Gallery. This includes all data for apps, information for registered devices, and user data. App Gallery users are only able to access apps they created or purchased; and MFDs to which they have been granted access, and registered.

Web Browser Extensions and Devices

The Xerox® App Gallery web browser extensions use SOAP messages, transmitted using the HTTP protocol on port 80, to find and add devices to a user's account. To add a device, a user must provide device administrator credentials and the SNMPv2 read/write community name string. The credentials and community string are securely stored as part of the device record in Xerox® App Gallery database.

The Xerox® App Gallery web browser extensions also use SOAP messages, transmitted using the HTTP protocol on port 80, to communicate with devices in order to accomplish app installation and uninstallation. The WSSE standard for SOAP messages is used to transmit nonce-protected hashes of device administrator credentials to the device to provide authorization.

App Gallery and Office365 Exchange

The Xerox® App Gallery communicates with Office365 Exchange to send emails using Microsoft's Exchange Web Service interface. This communication is done via HTTPS and the data is transmitted securely and is protected by TLS security. The minimum TLS version used is 1.2.

App Gallery App and App Gallery

The Xerox® App Gallery App, running on a device, communicates with the Xerox® App Gallery using HTTPS. Data is transmitted securely and is protected by TLS security. The minimum TLS version used is 1.2.

App Gallery App and Device

The Xerox® App Gallery App, running on a device, communicates with the device to get a list of apps currently installed on the device and to install/upgrade apps on the device. The communication is via HTTPS and data is transmitted securely and is protected by TLS security. The minimum TLS version used is 1.2.

App Gallery and Cloud Repository Middleware

The Xerox® App Gallery communicates with the Cloud Repository Middleware when a cloud repository app is installed on one or more devices. Xerox® App Gallery registers the App and the Device Serial Numbers, where the App is being installed. This communication is done using a web service calls via HTTPS and the data is transmitted securely and is protected by TLS security. The minimum TLS version used is 1.2.

Cloud Repository Designer Apps and Cloud Resident Repositories

The Cloud Repository Middleware facilitates communication between the Xerox® App Gallery Cloud Repository Apps and the Cloud Resident Repositories. This section describes the communication that occur between the Cloud Repository Designer Apps and the Cloud Repository Middleware as well as the communications between the Cloud Repository Middleware and the Cloud Resident Repositories.

Cloud Repository Designer App and Xerox Cloud Repository Middleware

At launch, the app must get an authentication/session token from the Cloud Repository Middleware Service in order to be given permission to access the cloud repository thru the Cloud Repository Middleware Service. The app requests the authentication/session token by transmission of the device serial number and the app id. The token is used for that session of the app. The app can then authenticate with the Cloud Resident Repository and then browse for folders and files. For Cloud Repository Designer Apps that do NOT use OAuth 2.0 for authentication, the app encrypts any user credentials sent to the Cloud Repository Middleware service as a URL query parameter.

All communication is done via HTTPS and the data is transmitted securely and is protected by TLS security. The minimum TLS version used is 1.2. Xerox® App Gallery supplies a link to a Certificate Authority root certificate for validation with Cloud Repository Middleware service. It is the responsibility of the customer to install the certificate on their devices and to enable server certificate validation on the devices.

Based on the type of app, either a print or scan job is initiated with the device. Once the job has been submitted, the device communicates with the Xerox Cloud Repository Middleware (See the section **Device and Xerox Cloud Repository Middleware** for details).

Device and Xerox Cloud Repository Middleware

The Scan and Print jobs submitted to a device communicate with the Cloud Repository Middleware via HTTPS and the data is transmitted securely and is protected by TLS security for both Upload and Download of documents. The minimum TLS version used is 1.2. All web service calls by the device, to the Cloud Repository Middleware, use the same authentication/session token acquired by the Cloud Repository Designer App.

Cloud Repository Middleware and Cloud Resident Repositories

The Cloud Repository Middleware routes incoming requests to the Cloud Resident Repository specified in the request (i.e. GoogleDrive, Dropbox, etc.). The Cloud Repository Middleware will decrypt any credentials before using them to access a Cloud Resident Repository.

The Cloud Repository Middleware uses a published API to communicate with each of the supported Cloud Resident Repositories. All communication is via HTTPS and the data is transmitted securely and is protected by TLS security. The minimum TLS version used is 1.2.

Middleware Azure Cloud Service and the Middleware Azure Cloud Storage

The Middleware Azure Cloud Service communicates with the Middleware Azure Cloud Storage via HTTPS and the data is transmitted securely and is protected by TLS security. The minimum TLS version used is 1.2. Cloud Repository Middleware Service does a look up for a device serial number and app id pair in the Cloud Repository Middleware's Azure Cloud Storage when an app requests an authentication/session token.

Customer Repository Designer App and Customer Repository Server

The Xerox® App Gallery does not guarantee secure communications for the Print From URL app and the Scan to Multi-Destination app with the Customer Repository Server. It is the responsibility of the customer to install certificates on the device and repository server which would ensure secure communication.

Middleware Azure Cloud Service and Xerox Document Conversion

The Middleware Azure Cloud Service communicates with the Azure VM Document Conversion Engine via HTTPS and is protected by TLS security. The minimum TLS version used is 1.2.

App Wrapper and App Gallery

Communication between the App Wrapper executing on the Device and the App Gallery software is via the Xerox e-commerce API. The communication is over HTTPS - and is hashed; but not encrypted. Hashing problems are detected at the receiving end, so that data tampering will be detected. The usage reported via the e-commerce API is not considered to be personal data; and is therefore not further encrypted.

App Gallery and the 2Checkout system

Communication between the Xerox App Gallery and the 2Checkout system is via the 2Checkout API 4.0 defined at: https://knowledgecenter.avangate.com/Integration/01JSON-RPC_API. Communication involves passing user data between the two systems. The user data includes user email address, company, and physical address. NOTE: user physical address is stored by the Gallery while a transaction is in progress; but is not permanently stored in the App Gallery database. Once the transaction has completed, the user physical address is permanently stored in the 2Checkout system. The following user Credit Card information is exchanged between the two systems: 1)last 4 digits, 2)expiration date, 3)card vendor.

The App Gallery utilizes the same URLs (described below) regardless of the Gallery User's country. This means that the physical locale of data processing and storage are the responsibility of the 2Checkout system for GDPR purposes.

Instant Payment Notification

When the details of an order change, the 2Checkout server will send to a predefined App Gallery URL an HTTP POST which encapsulates a data structure containing the information about the modified order. That information will be assigned a signature for authentication. The signature is realized using an HMAC_MD5 signature and a common secret key established between 2Checkout and the Xerox App Gallery. The HMAC algorithm is applied to all data sent. RFC 2104).

License Change Notification

When the details of a license change, the 2Checkout server will send to a predefined App Gallery URL an HTTP POST which encapsulates a data structure containing the information about the modified license. That information will be assigned a signature for authentication. The signature is realized using an HMAC_MD5 signature and a common secret key established between 2Checkout and the Xerox App Gallery. The HMAC algorithm is applied to all data sent. RFC 2104).

Buy/Renew Link

The App Gallery issues requests to 2Checkout on behalf of the Gallery user to Purchase or Renew a subscription in the 2Checkout system. Communication is via secure HTTP using a common secret key established between 2Checkout and the Xerox App Gallery.

2Checkout system and Payment Processors

For information on the interface between 2Checkout and the Payment Processors, contact 2Checkout at http://www.avangate.com/legal.php.

Software Updates

Xerox® App Gallery – Web Application

Xerox® App Gallery is a web application hosted in Microsoft's Azure Cloud Computing Platform. All updates to Xerox® App Gallery are strictly controlled by authorized Xerox IT personnel. When updates to the application are deployed, users connecting to the web site through their web browser will be accessing the most up-to-date release.

Xerox® App Gallery App

The Xerox® App Gallery App consists of both a device side component and a server side component. The two components have different methods for update and are described below.

Device Side Component - Weblet

The device side component is updated through the publication of a new version in the Xerox App Gallery. When a new version of an App is published, users are made aware of the update in both the App Gallery App and the App Gallery Web Application. Users must choose whether or not to install the update.

Apps in the Gallery are installed as a "weblet" which is digitally signed and encrypted. Encryption is only performed for devices that support the weblet encryption feature. The device will not install a weblet that has been tampered with and/or have an invalid digital signature.

After installation of an updated version, the update runs whenever a user starts the App Gallery App on a device.

Server Side Component – Web Application

Updates to the Gallery App server side component require an update to the Xerox® App Gallery web application (See the section above for details).

After the deployment of the updated server side component, the update runs whenever a user starts the App Gallery App on a device.

Browser Add-In/Extension

Internet Explorer ActiveX Control

Updates to the Internet Explorer ActiveX Control require an update to the Xerox® App Gallery web application (See the section above for details).

When the new version has been deployed, users, accessing the Xerox® App Gallery with the IE Browser, will be informed of the update and asked to confirm the installation. Once the updated Add-In is installed, the new version will be utilized.

Google Chrome Extension

Updates to the Google Chrome extension, for the Xerox® App Gallery, are hosted in the Google Chrome Web Store. All updates to the Chrome Extension are strictly controlled by authorized Xerox personnel.

When a new version has been released to the Google Chrome Web Store, users, accessing the Xerox® App Gallery with the Google Chrome Browser, will be informed of the update and asked to confirm the installation. Once the updated Extension is installed, the new version will be utilized.

Xerox® Cloud Repository Middleware

Xerox® Cloud Repository Middleware is a web application hosted in Microsoft's Azure Cloud Computing Platform. All updates to Xerox® Cloud Repository Middleware are strictly controlled by authorized Xerox IT personnel. When updates to the application are deployed, users connecting to the Cloud Repository Middleware using either a Designer App or Developer App will be accessing the most up-to-date release.

PII Data Management

In Scope for this document:

- Personal Data acquired and maintained by the Xerox App Gallery
- Personal Data acquired by the App Gallery App (hosted on the Device)
- Personal Data *acquired* by the XAG e-commerce provider.

Out of Scope for this document:

- Personal Data *maintained* by the XAG e-commerce provider. See the 2Checkout GDPR Compliance Statement at: https://www.2checkout.com/policies/gdpr-compliance-statement .
- Personal Data supplied by the e-commerce provider to Payment Processors to transact the payment
- Personal Data acquired and maintained by **Developer Apps** hosted by the App Gallery. See the Privacy Policy for each App, which is accessible from the App Gallery.
- Personal Data acquired and maintained by **Designer Apps** hosted by the App Gallery.
- Personal Data appearing in content acquired by any App.

Personal Data Maintained by the Xerox App Gallery:

- Email address (which then becomes the Gallery Account login)
- Gallery Account Password
- FirstName, LastName
- Company (channel partner accounts only)
- Country

Note: The Xerox App Gallery maintains configuration data for configurable apps at the Account level. The Names for each Configuration Element are supplied by the App Developer; and the Values are supplied by the gallery user. Personal Data may be stored in Configuration Data.

Personal Data Maintained by the e-commerce provider:

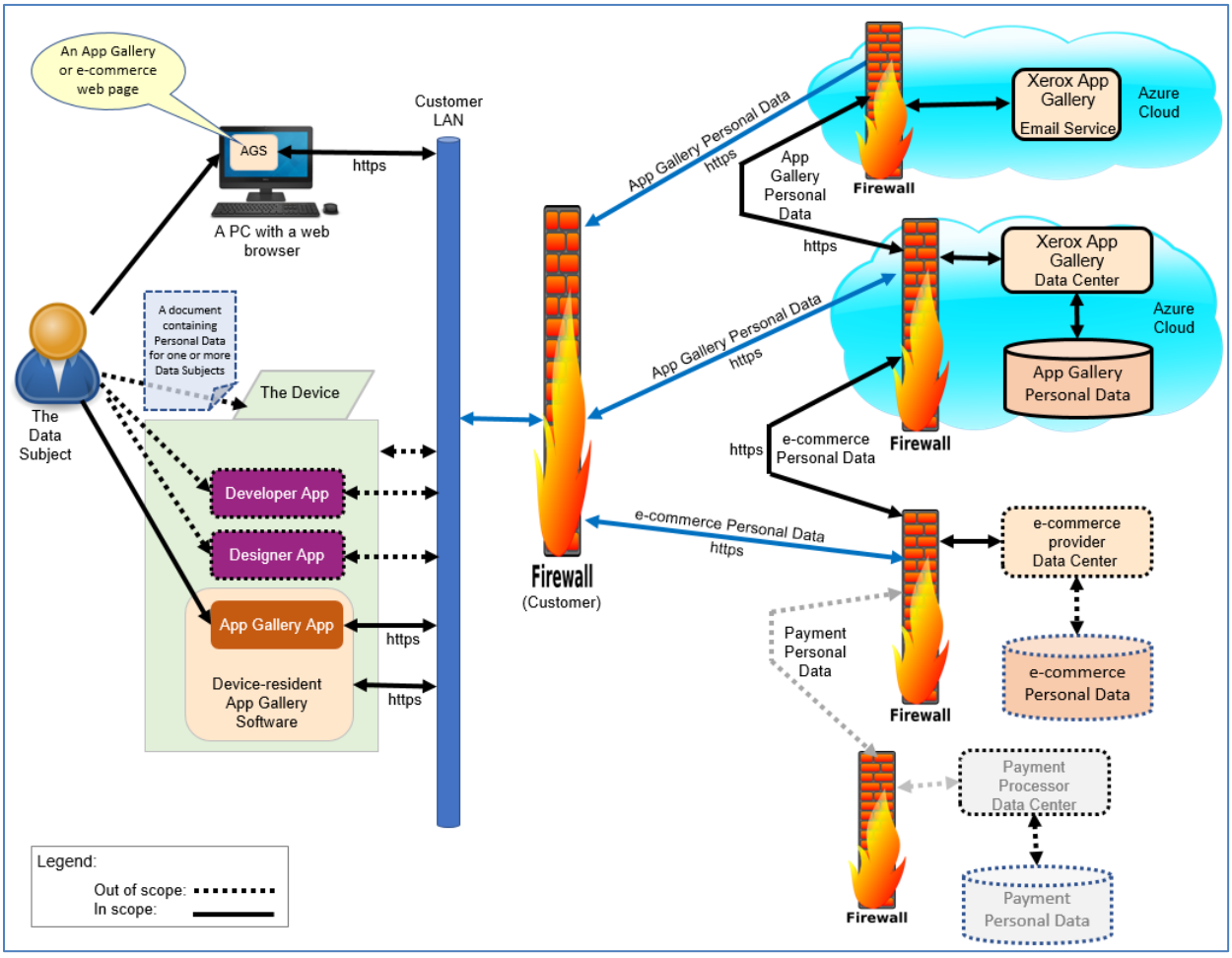
Note: The Xerox App Gallery acts as a passthrough for e-commerce Personal Data for the duration of the e-commerce purchase session. The Xerox App Gallery does not persistently store this Personal Data.

- Email address (which is identical to the Gallery Account email address)
- Full Name
- City, State, Zip/Postal Code, Country
- Credit Card Details for one or more cards, each of which includes:
    - Card Number
    - Card expiration Month and Year
    - CVV2 / CVC2 Code
    - Cardholder Name

App Gallery 5.x Territorial Map

Note1: **Devices** (which host Apps) may be located anywhere in the world (except embargoed countries).
Note2: The **App Gallery** is accessible via browser from anywhere in the world (except countries blocking the App Gallery

App Gallery 5.x PII dataflow



The Role of Xerox®

Xerox® strives to provide the most secure software product possible based on the information and technologies available while maintaining the product performance, value, functionality, and productivity.

Xerox® will:

- Run industry standard security diagnostics tests in development to determine vulnerabilities. If found, the vulnerabilities will either be fixed, minimized, or documented
- Monitor, notify, and supply necessary security patches provided by third party software vendors used with the App Gallery software.

Response to known vulnerabilities

Xerox maintains a website, https://www.xerox.com/security with up to date security vulnerability status, white papers, Common Criteria Certification, Intel Security McAfee information, and a portal to submit security questions to Xerox.