

Xerox

SMart eSolutions

Security White Paper

Xerox SMart eSolutions White Paper

Network and data security is one of the many challenges that businesses face on a daily basis. Recognizing this, Xerox Corporation continues to engineer and design all of our products to ensure the highest level of security possible.

This White Paper provides additional background on SMart eSolutions capabilities, and specifically focuses on the security aspects of Xerox SMart eSolutions - with the goal of ensuring that Xerox customers understand and feel confident how SMart eSolutions functions are performed and that machine data is transmitted to Xerox in a secure, accurate and auditable manner.

Xerox recommends that customers read this document in its entirety and take appropriate actions consistent with your information technology security policies and practices. Customers have many issues to consider in developing and deploying a security policy within their organization. Since these requirements will vary from customer to customer, the customer has the final responsibility for any and all implementations, re-installations and testing of security configurations, patches and modifications.

NOTICE: DISCLAIMER

THIS INFORMATION IS PROVIDED FOR INFORMATION PURPOSES ONLY. XEROX CORPORATION MAKES NO CLAIMS, PROMISES OR GUARANTEES ABOUT THE ACCURACY, COMPLETENESS, OR ADEQUACY OF THE INFORMATION CONTAINED IN THIS WHITE PAPER AND DISCLAIMS ALL LIABILITY CONCERNING THE INFORMATION AND/OR THE CONSEQUENCES OF ACTING ON ANY SUCH INFORMATION. PERFORMANCE OF THE PRODUCTS REFERENCED HEREIN IS EXCLUSIVELY SUBJECT TO THE APPLICABLE XEROX CORPORATION TERMS AND CONDITIONS OF SALE, LICENSE AND/OR LEASE. NOTHING STATED IN THIS WHITE PAPER CONSTITUTES THE ESTABLISHMENT OF ANY ADDITIONAL AGREEMENT OR BINDING OBLIGATIONS BETWEEN XEROX CORPORATION AND ANY THIRD PARTY.

Xerox SMart eSolutions Overview

Xerox SMart eSolutions capabilities are based on a technology platform that provides a flexible end-to-end system for connecting products to the Xerox infrastructure which administers our post-sale offerings.

The diagram shown in Figure 1 emphasizes the three main architectural elements of the system, which are located at the vertices of the triangle. These three elements work together in a seamless manner to enable a rich variety of remote services and to provide for additional services to be added in the future.

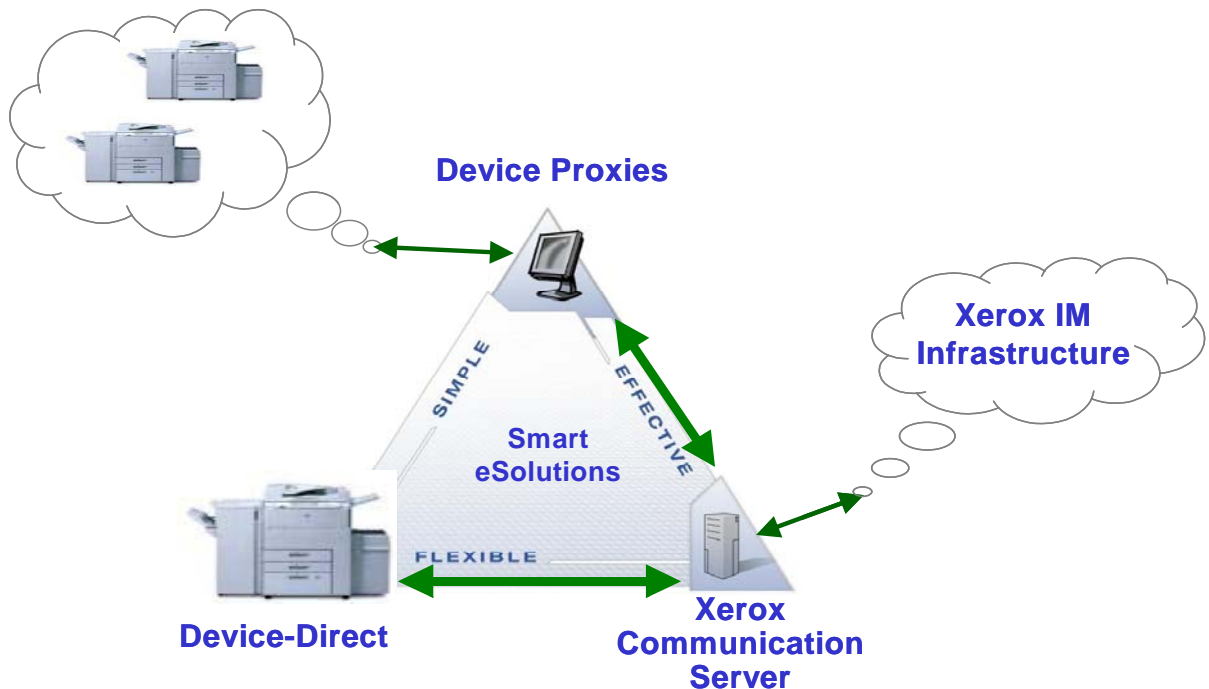


Figure 1: Major components of the Xerox SMart eSolutions architecture

At the lower left corner of the triangle are devices with the SMart eSolutions client software module embedded in them to provide the client-side infrastructure that enables secure transactions back to Xerox.

The connection to Xerox and our back-office processes is shown at the lower right corner of the triangle. SMart eSolutions clients connect to Xerox through a common connectivity server referred to as the *Xerox Communication Server*.

At the top of the triangle are device proxies. These proxies enable Xerox devices to communicate to the *Xerox Communication Server* through a single point. This provides the customer with the capability to consolidate data communication through a reduced number of Production Systems and Office products. This document refers to both direct and proxy clients generically as *SMart eSolutions Clients*.

Xerox SMart eSolutions Design Goals for Security

Xerox views network security as a key requirement of the overall SMart eSolutions architecture. The security related goals were derived from the following sources:

1. Xerox Customer Service and Support Organizations across the world.
2. Inputs and feedback from extensive Voice of the Customer studies conducted by the Xerox Innovation Group (XIG). These studies were focused on determining customer preferences and their remote services needs.
3. Security guidelines published by the Xerox Information Management (XIM) organization.
4. Various (internal Xerox) business group customer advocates.

Xerox SMart eSolutions include capabilities designed to address the following concerns about security:

1. **Identification and Authentication.** The process of uniquely and reliably identifying a device.
2. **Authorization.** The process of granting the device remote access services based on our customer's security needs and product acquisition decisions.
3. **Data Integrity.** The ability to verify that data has not been subjected to unauthorized modification.
4. **Audit Capabilities.** The ability to track all communication between it and Xerox, allowing the customer to monitor the number and types of communication.
5. **Customer Confidentiality.** The prevention of access to unauthorized parties by making use of encryption techniques (i.e. https).

Within the end-to-end SMart eSolutions system, the system design goals respond to network security concerns in two main categories.

Customer Network Environment

The first category is security concerns related to the connection of the client software to the end-user's network and to the transmission of data across the Internet to Xerox. Xerox SMart eSolutions incorporate the following controls:

- The customer must authorize communications between the device and Xerox .
- Communications from the device shall not include information that indicates the identity of the customer or customer's employees
- The *SMart eSolutions Client* allows a one-way connection from the device to Xerox. It is not possible to use this connection to access the customer's network or data beyond what is pushed to Xerox by the customer.

- The integrity and authentication of any information (data or code) downloaded by the *SMart eSolutions Client* is verified prior to installation.

Transaction Security

The second category is the network security concerns related to the exchange of information between the customer and Xerox in executing transactions. The following controls have been established:

- The *Xerox Communication Server* and the *SMart eSolutions Clients* mutually authenticate themselves.
- All transaction content between the *SMart eSolutions Client* and the *Xerox Communication Server* is auditable by both the customer and Xerox.
 - a. A viewable transaction log gives end-users the ability to audit the information shared with Xerox.

The *Xerox Communication Server* currently logs all incoming and outgoing transactions.

Xerox Smart eSolutions Technology Architecture

Figure 2 depicts a high-level view of an end-to-end SMart eSolutions architecture. It highlights communication flow between the *Smart eSolutions Client* (direct-device and/or proxy-host) and the *Xerox Communication Server*. As shown in the diagram, *Smart eSolutions Clients* are embedded either in Xerox devices or in a hosted application (e.g. CentreWare™ Web). The clients are configured to connect and send messages to the *Xerox Communication Server*.

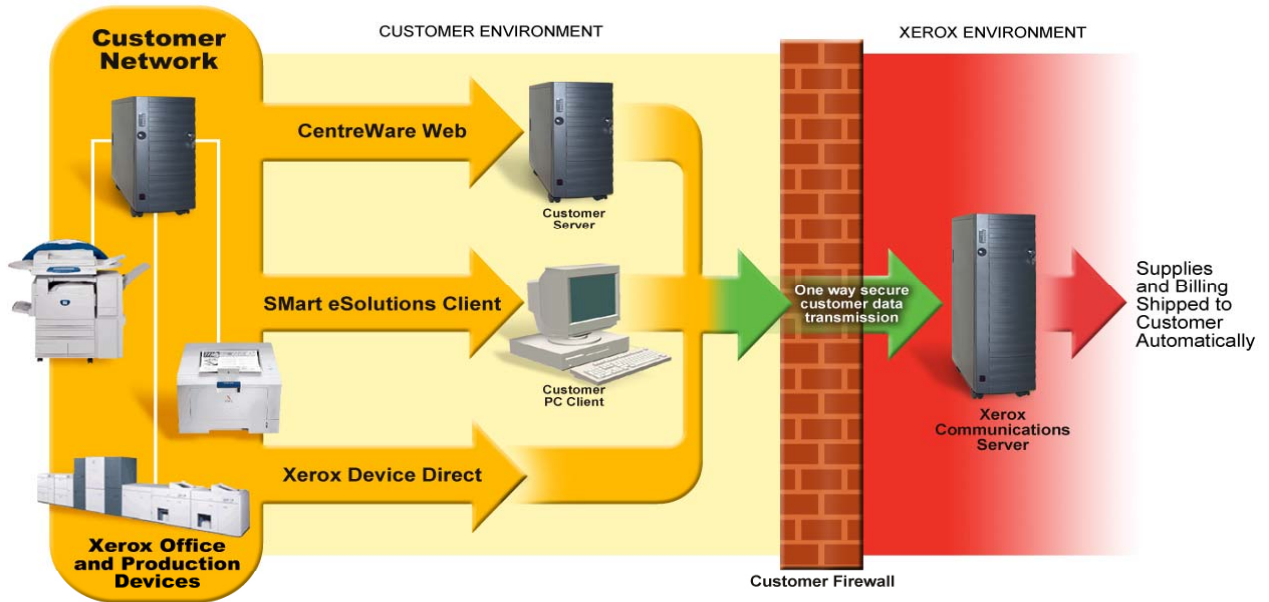


Figure 2: Xerox SMart eSolutions data communications

Xerox SMart eSolutions use industry standard web services protocols for all communications between *SMart eSolutions Clients* and the *Xerox Communication Server* (Figure 3). Web services are accessed via the secured-socket HTTP (HTTPS) that is common to web browsers and web servers. Use of web services as the underlying mechanism for all SMart eSolutions transactions ensures both interoperability and compatibility with firewalls.

Web Services
SOAP
XML
HTTPS
SSL
TCP

Figure 3: Web services protocol stack

- By using HTTP, web services can also take advantage of the Secure Socket Layer (SSL) protocol for security and HTTPS connection management capabilities in order to prevent customer data from being broadcasted over the open Internet.
- A *proxy* server is commonly used in network environments to provide a firewall system between the end-user network and the Internet. Most firewalls/proxies are configured to block requests on all but a few network *ports*. Firewalls, however, usually allow traffic on port 80 for HTTP and 443 (secured HTTP or HTTPS) so browsers can access the Internet. By using HTTP or HTTPS over standard ports, *SMart eSolutions Clients* are able to communicate through firewalls. The *SMart eSolutions Clients* act like any web browser (over standard ports) requiring no "holes in the customer firewall" or changes to other equipment at the customer site. *SMart eSolutions Clients* support the 128 bit SSL encryption
- As shown in Figure 2, *SMart eSolutions Clients* initiate all interactions between themselves and the *Xerox Communication Server*.
- To achieve the effect of 2-way connectivity the *SMart eSolutions Clients* periodically “check-in” with the *Xerox Communication Server* to receive any “instructions” for them. This check is infrequent and very lightweight, avoiding congestion of the customer intranet.
- The *Xerox Communication Server* digitally signs all software downloaded by the *SMart eSolutions Client*. The customer benefits from this software integrity because it addresses the following issues:
 - Content Source: this feature certifies that the software really comes from Xerox.
 - Content Integrity: this feature confirms that the software has not been altered or corrupted since it was signed.

Frequently Asked Questions

Listed below is a set of FAQs helpful for an end-user of Xerox SMart eSolutions from Xerox.

1. *Will enabling a Xerox SMart eSolutions Client make my network more susceptible to viruses or hacker attacks?*

No. Customers make no changes to their own security infrastructure, hence no additional ports need to be opened up the customer's firewall. Xerox SMart eSolutions only communicate to a specific secure server at Xerox and services are designed specifically to prevent unauthorized data transfers. The secure server at Xerox is regularly scanned for viruses using the latest tools.

2. *How do I know that Xerox is not accessing my company's private data off the machine disk?*

You may examine the data sent back to Xerox by using the device User Interface to view the transaction details. SMart eSolutions features only access machine related data, and not customer images or other customer data. Customer Job Data is specifically provided only at customer discretion and in concert with problem diagnostics.

3. *How can I be sure that the device data is going to Xerox only?*

The secure transmittal process uses HTTPS and VeriSign signed certificates to ensure and verify that the device is sending to Xerox. In addition, all transmission data is sent over a Secure Socket Layer (SSL) connection using 128-bit encryption, which only Xerox has the key to decipher.

4. *Will my machine interact with or receive information from "non-Xerox" systems?*

No. The device always initiates the remote services transfer activity and sets up a Xerox-only, non-intrusive communication path. The device always checks the authentication of who it is communicating with by validating the Verisign Certificate.

5. *What is this data used for?*

Currently this data is used for one of two purposes:

- 1) Billing – Billing information is sent up with each data push allowing Xerox to produce accurate and timely customer invoices.
- 2) Supplies Replenishment – Meter and toner usage information is sent up to enable Xerox to better meet the toner needs of your equipment by insuring that you have the right amount of toner on hand at all times.

In summary, Xerox is responsive to the security concerns of our customers. Xerox SMart eSolutions will not make networks more susceptible to viruses. SMart eSolutions transactions always originate from the device, based on authorizations made by the customer. Services can only communicate with a secure server at Xerox that conforms to the stringent requirements of the internal Xerox Corporation information management infrastructure. Customers do not need to make any changes to Internet firewalls, proxy servers, or other security infrastructure.