Issued October 15th, 2012

Security White Paper
for
GlobalScan NX Version 2.1
Appendix
- Encryption -

Solution Support Department
Service and Support Center
Global Marketing Group
Ricoh Company, Ltd.

Document version: 1.0

Notice:
This document may not be reproduced or distributed in whole or in part, for any purpose or in any fashion without the prior written consent of Ricoh Company Limited. Ricoh Company Limited retains the sole discretion to grant or deny consent to any person or party.

All product names or product illustrations, including desktop images, used in this document are trademarks, registered trademarks or the property of their respective companies. They are used throughout this book in an informational or editorial fashion only. Ricoh Company, Ltd. does not grant or intend to grant hereby any right to such trademarks or property to any third parties. The use of any trade name or web site is not intended to convey endorsement or any other affiliation with Ricoh products.

Although best efforts were made to prepare this document, Ricoh Company Limited makes no representation or warranties of any kind with regards to the completeness or accuracy of the contents and accepts no liability of any kind including but not limited to performance, merchantability, fitness for any particular purpose, or any losses or damages of any kind caused or alleged to be caused directly or indirectly from this document.

Document version history:

Version	Date of Issue	Revision
1.0	October, 2012	1st Release

1 Overview

1.1 Summary

This document describes the encryption methods and processes used by GlobalScan NX. This document is an appendix to “Security White Paper for GlobalScan NX”.
Widespread knowledge of the encryption methods used by GlobalScan NX increases the chances of a security risk. Therefore, the contents of this document should be tightly controlled. Distribution should be limited to the smallest number of people possible, with careful consideration given to whether or not the requesting individual really needs to read this or the parent document.
There are separate chapters for GlobalScan NX Server Edition and Serverless Edition. Each chapter covers the details of encryption processing according to the differences in capabilities and workflow of the two editions of GlobalScan NX.

1.2 Glossary

Administration Tool

The “Administration Tool” is the web browser-based Flash application used to manage GlobalScan NX’s settings.

Subject

“Subject” is the Java class in which user credentials, Kerberos tickets, and other information is stored after encryption.

User Credentials

This term includes all user account authentication information, such as “Account Name”, “Password”, and “Domain Name” and so on. The term “password” is only used when specifically referring to a password issue.

Utility PC/Server PC

A Utility PC is the PC where GSNX Serverless Edition is installed. A Server PC is where GSNX Server Edition is installed.

1.3 Encryption Systems

GlobalScan NX primarily uses 2 types of encryption systems, RSA and Blowfish.

RSA Encryption (1024-bit key)

RSA is an asymmetric key cryptosystem (public key/private key). Due to the data size limits and slow speed of this algorithm, GlobalScan NX usually only uses RSA to encrypt the Blowfish key (both Server and Serverless Edition, see below) and the “Subject” (Server Edition only, described later).

Blowfish Encryption (128-bit)

Blowfish is high-speed block cipher used for information encryption. This algorithm uses a free license and is widely used (ex: SSH protocol). GlobalScan NX encrypts information with this algorithm and then uses RSA encryption to exchange the keys.

2 Serverless Edition

2.1 Login to the AdminTool

When a user logs in to the AdminTool, user credentials are encrypted using the following procedure and transferred to the Utility PC.

AdminTool	Utility PC
	1. Creates the RSA keys. ** Only the 1st time the system is started.*
2. Requests the Utility PC's public key. 3. Creates the Blowfish key (single-use). 4. User Credentials are encrypted using the Blowfish key. 5. Blowfish key is encrypted using the Utility PC's public key. 6. Transfer the data from steps 4 and 5 with the request.	
	7. The Blowfish key is decrypted using the private key. 8. The User Credentials are decrypted using the Blowfish key. 9. The decrypted credentials are passed to the authentication system to verify the user. If authentication succeeds, the user is logged in.

2.2 Encryption of Settings (Profile) Data

This section describes the process used to encrypt settings (Profile) data.

[Background]
Settings (Profile, etc.) need to be distributed to one or more MFPs. If different keys are used for each MFP, distribution times significantly increase. Therefore, GlobalScan NX stores the pre-encrypted settings on the Utility PC and then distributes the settings to any MFPs along with the key.

Encryption is performed by the AdminTool. Then the encrypted data is transferred to the Utility PC and stored there. The Blowfish key used for this encryption is created by the Utility PC.

After logging in to the AdminTool, the AdminTool gets the Blowfish key from the Utility PC. The AdminTool then creates a single-use RSA key. Next the AdminTool sends the Public Key to the Utility PC. The Utility PC encrypts the Blowfish key using the Public Key and sends it to the AdminTool. Finally, the AdminTool decrypts the Blowfish key using the private key and encrypts the settings data for storage.

AdminTool	Utility PC
	1. Creates a permanent Blowfish key. ** Only the 1st time the system is started.*
2. Creates a RSA Key on demand. ** Per session* 3. Transfers the RSA public key to the Utility PC.	
	4. Encrypts the Blowfish key using the RSA public key. 5. Transfers the encrypted Blowfish key to the AdminTool.
6. Decrypts the Blowfish key using the private RSA key. 7. The administrator creates settings data using the AdminTool. 8. The Blowfish key is used to encrypt the settings. 9. The encrypted settings are transferred to the Utility PC.	
	10. The settings are stored in the encrypted format.

2.3 SDK application self-synchronization

When device registration and profile synchronization is triggered from the device, user credentials are encrypted using the following procedure and transferred to the Utility PC.

Device (SDK application)	Utility PC
	1. Creates the RSA keys. ** Only the 1st time the system is started.*
2. Requests the Utility PC's public key. 3. Creates the Blowfish key (single-use). 4. User Credentials are encrypted using the Blowfish key. 5. Blowfish key is encrypted using the Utility PC's public key. 6. Transfer the data from steps 4 and 5 with the request.	
	7. The Blowfish key is decrypted using the private key. 8. The User Credentials are decrypted using the Blowfish key. 9. The decrypted credentials are passed to the authentication system to verify the device. If authentication succeeds, the synchronization is performed.

2.4 What data is encrypted?

As described in section 2.2, much of the settings data is saved in an encrypted format before being transmitted to a device. This means that even if SSL communication is not used, there is some protection for confidential information.

The following information is included in the stored encrypted data:

- AdminTool System Settings **(Note 1)**
  General Settings
  Authentication Profiles
  Administrator Settings
  Job Settings
  System Log Settings

- Service/Filter User Credentials
  ** Such as POP account information, LDAP server access account information, etc.*

- Backup Data (not sent to a device)

Note 1: All the information is encrypted during transmission. When the data is stored, only the User Credentials are encrypted.

To protect any data not listed above, SSL communication should be used in addition to increasing security on the Utility PC (hardware lockouts, HDD encryption, etc.).

2.5 Distribution of Settings to MFPs

The MFPs will work as GSNX Serverless Edition once settings data is sent from the Utility PC to the MFPs. After that, the Utility PC will not be used again until settings need to be changed.

As described in 2.2, the Utility PC stores the encrypted settings and distributes them to MFPs with the decryption key in order to avoid any performance problems at the time of distribution.

Use of SSL communication is recommended in order to more strongly protect the encrypted data, as well as the data fields which are not included in the encrypted archive.

2.6 Project Authentication, Job Data

See the explanation in the Server Edition Chapter, section 3.2 and 3.3.

3 Server Edition

The differences between the Serverless Edition and the Server Edition are described in this chapter.

3.1 Distribution of Settings to MFPs

Most settings are distributed dynamically to the MFPs. In other words, settings are saved only on the Server PC and no information is saved in the MFPs' HDD.

The MFP is only passed information related to the LCD panel display (UI). As the transferred information does not include any User Credentials or settings information, the data does not need to be encrypted.

3.2 Projects with Authentication

When using a project with authentication, users must login to GSNX using the MFP's LCD panel.

[Ref.]
The AdminTool is designed as a stateless server, and therefore the login process must be done every time communication is initiated with the Utility PC/Server PC.

After logging in using the LCD panel, the data group called "Subject" is sent to the MFP as the result and is used until logout. The "Subject" data includes the User Credentials. However, this data is encrypted using the Server PC's public key. Since the MFP does not possess the Server PC's private key, it is impossible to decrypt this data on the MFP side.

3.3 Job Data

Job Data (ex: scanned image, Subject) is transferred to the Server PC and the delivery process is initiated on the Server PC. Job data is temporarily queued on the HDD, and the Subject is serialized onto the file after encryption.

As private key exists on the Server PC in which the jobs are queued, it is possible to decrypt the data if the PC is not protected physically.

3.4 Load balancing and secondary server

As described above, the Subject can be decrypted only on the Server in which the subject was encrypted.
As the RSA keys are different on each Server PC, there is a problem if the encrypting PC and the PC processing the job are different. Therefore, a method is needed to exchange the Subject between PCs. However, this method is not explained here as it is beyond the scope of this document.

4 Other Information

4.1 Data Structure

4.1.1 Backup Data

Password-based encryption (implemented as a part of the Java SDK) is applied to the whole file. An empty password is used if a user does not set a password.

4.1.2 Export Profile Data

The selected data will be encrypted by the method described in Chapter 2.

4.2 Connecting with an External System

The security methods used in connections between GlobalScan NX plug-ins and an external system are dependent on the network protocol which is used by the plug-in. Description of each plug-in is considered to be outside the scope of this document.

4.3 FAQ

Q. Where and how is the encrypted key saved?
A. Such information cannot be disclosed.