Barron McCann Technology
X-Kryptor

RSA SecurID Ready Implementation Guide

Last Modified: December 10, 2008

Partner Information

Product Information	
Partner Name	Barron McCann Technology Ltd
Web Site	http://www.bemac.com
Product Name	X-Kryptor
Version & Platform	Lite/25/100
Product Description	X-Kryptor Secure Client technology enables you to build secure remote access solutions using common, easily available and inexpensive ISP services. X-Kryptor Secure Clients add a layer of strong encryption to common mobile communications devices and are compatible with most desktop and mobile operating systems. It integrates with broadband, ADSL, wireless LAN (Wi-Fi), satellite, microwave, 3G / GPRS, so you can securely connect not just your geographically distant offices, but your home-based and mobile workers too. X-Kryptor combines RSA SecurID authentication to provide high-level, cost-effective security for sensitive data over your local or wide-area networks.
Product Category	Virtual Private Networks

BeMac
Products from Barron McCann

Solution Summary

The X-Kryptor VPN system may optionally be supplied with additional RSA SecurID Authentication Agent software.

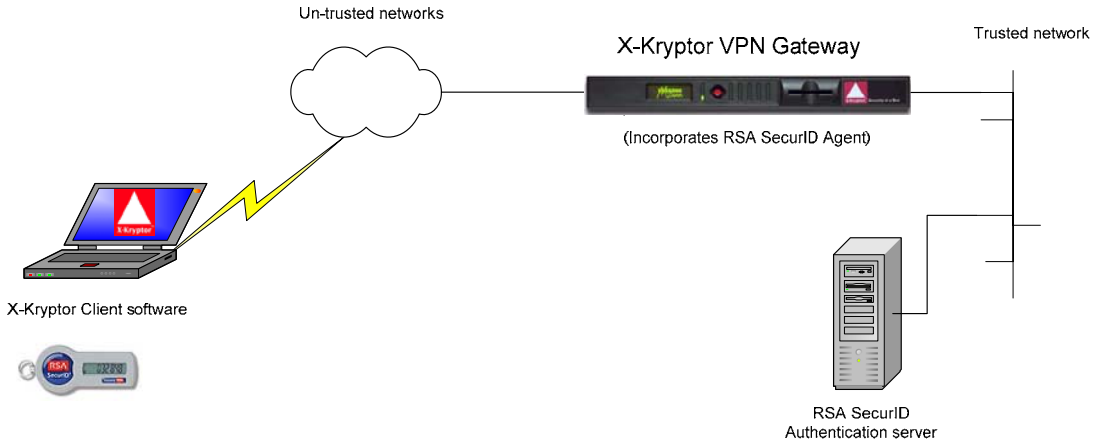
The X-Kryptor VPN system is certified in the UK by CESG. This certification is based upon the cryptographic strength of the product. The RSA SecurID Authentication Agent components provide the addition of a robust method of user authentication. It is not in itself part of the certification process.

Central to the X-Kryptor VPN system is one or more physical appliances known as Gateways. The RSA SecurID Authentication Agent forms part of the supplied X-Kryptor Gateway software. X-Kryptor Client software is installed on Microsoft Windows platforms and provides the VPN endpoint. The installed X-Kryptor Client incorporates RSA SecurID Authentication dialogue screens.

Operationally, the X-Kryptor VPN connection is established and users prompted for their RSA SecurID login credentials. Until a user has successfully authenticated, no data will pass beyond the VPN connection. A system tray icon is used to display the authentication status.

The integration of the RSA SecurID Authentication Manager system thus provides a robust and positive method of user authentication.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication
List Library Version Used	N/A
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	N/A
RSA Authentication Agent Host Type	Communication Server (v6.1.2 or earlier); Net OS (v7.1 or later).
RSA SecurID User Specification	All Users
RSA SecurID Protection of Administrative Users	Yes
RSA Software Token and RSA SecurID 800 Automation	No



System Architecture

Product Requirements

Partner Product Requirements: X-Kryptor VPN system	
Commercial version	All versions
UK CAPS Approved at Baseline	Upon request, requires risk assessment approval

Operating System	
Platform	**Required Patches**
Microsoft Windows 2000 Professional	SP4
Microsoft Windows XP Professional	SP2

Agent Host Configuration

To facilitate communication between the X-Kryptor Gateway and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the X-Kryptor Gateway within its database and contains information about communication and encryption.

To create the Agent Host record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces

When adding the Agent Host Record, you should configure the X-Kryptor as either a Communications Agent (v6.1) or NetOS Agent (v7.1) This setting is used by the RSA Authentication Manager to determine how communication with the X-Kryptor will occur.

Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.

Please refer to the appropriate RSA Security documentation for additional information about creating, modifying and managing Agent Host records.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	Not required. The IP addresses of Authentication Manager servers are entered directly into the X-Kryptor Gateway configuration.
Node Secret	Retained in the X-Kryptor Gateway non-volatile memory. Access the X-Kryptor Gateway configuration menu to remove.

Partner Product Configuration

Before You Begin

This section provides instructions for integrating X-Kryptor with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components. All products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

RSA SecurID Authentication Manager

You should establish a working RSA SecurID Authentication Manager system before implementing the X-Kryptor Gateway Authentication option. You will need to add X-Kryptor as a Communications Server Agent host or a Net OS Agent Host, depending on the version of Authentication Manager.

Authentication Manager Version	Agent Host Type
V6.1.2 and earlier	Communications Server
v7.1 and later	Net OS

The Agent Host configuration requires a resolvable hostname and IP address. Enter this hostname into your DNS table.

X-Kryptor Gateway configuration

The X-Kryptor Gateway software (firmware) was updated in December 2008 to be compatible with RSA SecurID Authentication Manager v7.1. All Firmware versions prior to BMF846-9 (Baseline) and BMF884 (Commercial) use Legacy Agent Hosts settings. Two servers are supported, an Acting Master and Slave. This mode of operation is not supported in Authentication Manager 7.1. The Agent software supports Authentication Manager v7.1 and v6.1. We would advise customers using RSA Authentication Manager prior to v5.2.1 to upgrade to v6.1 or v7.1.

Administrators should be familiar with the operation and configuration of the X-Kryptor system. Once the RSA Authentication option has been defined and saved, all X-Kryptor Clients must incorporate the RSA Agent dialogue software. Thus, for existing X-Kryptor installations, it is essential to replace the XK Client software and to distribute RSA SecurID tokens before implementation.

Please refer to the X-Kryptor RSA Authentication Guide supplied on your product CD for details on parameter settings.

Configuring via the X-Kryptor Management Console

1. Login to the X-Kryptor using the secure password
2. From the System Administration menu select:

```
1. X-Kryptor Name
```

Enter a suitable name. This name will be displayed in the XK Client RSA dialogue screen

```
2. IP and TCP Configuration

    A. Authentication Parameters

        Use the <space bar> to select Authentication Type [RSA SecurID]
```

Latest firmware release

```
Authentication Configuration
1.  Authentication Type                      [RSA SecurID]
2.  Max. Authentication Fails Permitted      [005]
3.  Max. Time for Authentication (minutes)   [005]
4.  Max. Valid Authentication Period (hours) [n/a]
5.  Authentication Master IP Address         [000.000.000.000]***
6.  Authentication Port                      [05500]
7.  LAN A / Local Manager Authentication     [Y]
8.  Local VDU Manager Authentication on Fail [Y]
9.  Authenticate Client Initial NetBIOS      [Y]
10. Authentication Server on LAN B (Client)  [N]
11. Re-Authenticate On IP Address Change     [Y]
12. Re-Authenticate On TCP Connection Fail   [N]

        3. RSA SecurID Authentication Parameters

RSA SecurID Authentication Configuration
1.  ACE Server Version    [5.0 or Higher ]
2.  Encryption Type       [DES]
3.  Clear Node Secret     [N]
4.  Replica 1 IP Address  [000.000.000.000]
5.  Replica 2 IP Address  [000.000.000.000]
6.  Replica 3 IP Address  [000.000.000.000]
7.  Replica 4 IP Address  [000.000.000.000]
8.  Replica 5 IP Address  [000.000.000.000]
9.  Replica 6 IP Address  [000.000.000.000]
10. Replica 7 IP Address  [000.000.000.000]
11. Replica 8 IP Address  [000.000.000.000]
12. Replica 9 IP Address  [000.000.000.000]
13. Replica 10 IP Address [000.000.000.000]
```

Prior firmware releases

```
Authentication Configuration
1.  Authentication Type                      [RSA SecurID]
2.  Max. Authentication Fails Permitted      [005]
3.  Max. Time for Authentication (minutes)   [005]
4.  Max. Valid Authentication Period (hours) [n/a]
5.  Authentication Master IP Address         [000.000.000.000]
6.  Authentication Slave IP Address          [000.000.000.000]
7.  Authentication Port                      [05500]
8.  LAN A / Local Manager Authentication     [Y]
9.  Local VDU Manager Authentication on Fail [Y]
10. Authenticate Client Initial NetBIOS      [Y]
11. Authentication Server on LAN B (Client)  [N]
12. Re-Authenticate On IP Address Change     [Y]
13. Re-Authenticate On TCP Connection Fail   [Y]
```

*** Note the menu changes. The prior firmware release refers to Master and Slave IP addresses. Only the later version is compatible with RSA SecurID Authentication Manager v7.1.

X-Kryptor Client Installation

The X-Kryptor Client is configured and installed with the normal privileges. The X-Kryptor Client installation has no specific RSA SecurID configuration parameters.In normal operation, following the first valid authentication, the node secret is exchanged between the X-Kryptor Gateway and RSA SecurID Authentication Manager.

Node Secret

Upon the first successful user Authentication using the X-Kryptor Client, the RSA SecurID Authentication Manager will set an agent node secret. The node secret will be sent to and stored in the X-Kryptor Gateway. Should the X-Kryptor be replaced, then the node secret must be cleared within the agent configuration screen.

X-Kryptor Client Authentication

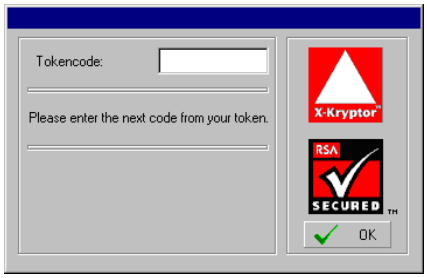
The X-Kryptor Client has additional software to prompt the user to enter their RSA login credentials.

The following screens may be shown:-

Authentication screen

New PIN request

Confirm new PIN



Next Token mode

Certification Checklist For RSA Authentication Manager v6.x

Date Tested: 12/11/2008

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.1	Windows
xKryptor	100	N/A

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	✓	Force Authentication After New PIN	N/A
System Generated PIN	✓	System Generated PIN	N/A
User Defined (4-8 Alphanumeric)	✓	User Defined (4-8 Alphanumeric)	N/A
User Defined (5-7 Numeric)	✓	User Defined (5-7 Numeric)	N/A
User Selectable	✓	User Selectable	N/A
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	N/A
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	N/A
Passcode			
16 Digit Passcode	N/A	16 Digit Passcode	N/A
4 Digit Password	✓	4 Digit Password	N/A
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	N/A
Name Locking Enabled	✓	Name Locking Enabled	
No RSA Authentication Manager	✓	No RSA Authentication Manager	N/A
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SecurID 800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
Credential Functionality			
Determine Cached Credential State	N/A	Determine Cached Credential State	
Set Credential	N/A	Set Credential	
Retrieve Credential	N/A	Retrieve Credential	

JGS / PAR

✓ = Pass ✗ = Fail N/A = Non-Available Function

Certification Checklist For RSA Authentication Manager 7.x

Date Tested: 12/11/2008

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1	Windows
xKryptor	100	N/A

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	✓	Force Authentication After New PIN	N/A
System Generated PIN	✓	System Generated PIN	N/A
User Defined (4-8 Alphanumeric)	✓	User Defined (4-8 Alphanumeric)	N/A
User Defined (5-7 Numeric)	✓	User Defined (5-7 Numeric)	N/A
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	N/A
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	N/A
Deny Numeric PIN	✓	Deny Numeric PIN	N/A
PIN Reuse	✓	PIN Reuse	N/A
Passcode			
16 Digit Passcode	N/A	16 Digit Passcode	N/A
4 Digit Fixed Passcode	✓	4 Digit Fixed Passcode	N/A
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	N/A
No RSA Authentication Manager	✓	No RSA Authentication Manager	N/A
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SecurID 800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A

JGS / PAR

✓ = Pass ✗ = Fail N/A = Non-Available Function

Appendix

Location of Node Secret

The node secret will be stored in the X-Kryptor Gateway. See X-Kryptor documentation for details.

X-Kryptor Client Registry values

After the user has successfully authenticated using their RSA login credentials, a digital certificate is generated by the X-Kryptor Gateway and passed to the X-Kryptor Client. This X.500 certificate indicates that the user has already successfully authenticated the VPN to the X-Kryptor Gateway.

The X-Kryptor Client has some registry key values that affect the behavior with regard to the storage of the X.500 certificate. For instance, when the user logs off, what happens to the VPN connection? Does the VPN immediately close or remain open long enough for a Roaming Profile and/or Briefcase folders to be copied back to the Network Share?

HKEY_LOCAL_MACHINE\SOFTWARE\Barron McCann\XGntr\

Value Name	Type	Action
logoffAction	REG_SZ	i) If set to 'none' then any held certificates will not be lost on a user logoff, incoming challenges will be responded to. ii) If set to 'no refuse' then any held certificates will be lost but incoming challenges will be responded to immediately iii) Set to 'refuse' will result in any certificates being lost and any incoming challenges being reset until the GINA flags Xgntr to resume or Xgntr timesout. This will only occur if a GINA is currently in use. Otherwise incoming connections are never refused. iv) If set to "delay" then the certificate is retained for the period specified in retainDelay v) Any other setting will result in any certificates being lost and any incoming challenges being reset until GINA flags Xgntr to resume or Xgntr's timeout. This will only occur if a GINA is currently in use. If GINA not in use then incoming connections are never refused. Options : none, no refuse, refuse, delay Default: delay
RetainDelay	REG_DWORD	Time in seconds to retain certificate if logoffAction is set to "delay" Default: 5 seconds

Known Issues

At the time of certification, the integration was not capable of accepting 16-digit passcodes (an 8-digit PIN and an 8-digit tokencode). Barron McCann is currently addressing this limitation. They are expected to resolve the issue in early 2009. At that time, Partner Engineering will verify the solution and update this guide.