GINA Implementation in the RSA® Authentication Agent 6.1 for Microsoft® Windows®

TECHNOLOGY BACKGROUNDER

RSA SecurID® for Microsoft® Windows® is an authentication solution that proves the identity of users before allowing access to the Microsoft Windows environment. This product enables customers to use the RSA SecurID solution to authenticate Microsoft operating system users, whether they are online and connected to the corporate network or offline and logging on to their desktops or laptops remotely, e.g., at a hotel or on an airplane.

The solution provides stronger security than passwords; provides a consistent, simple method for users to sign on to the Windows environment; eliminates the need for password change policies and provides an audit log of all authentication events.

I. RSA SECURITY AND MICROSOFT RELATIONSHIP

RSA SecurID for Microsoft Windows was developed in close cooperation with Microsoft Corporation to ensure secure and seamless integration on the desktop. RSA Security is a Microsoft Gold Certified Managed Partner in the Microsoft/ Global ISV community. In addition, RSA Security is a member of Microsoft's security competency program. Microsoft and RSA Security have an agreement in place to work together to provide support for SecurID for Microsoft Windows customers.

The RSA Authentication Agent for Microsoft Windows 6.1 has been independently tested and found to meet the criteria for the Certified for Windows 2000 Server and Advanced Server and Upgraded for Windows 2003 Standard and Windows 2003 Enterprise. This product has also completed the testing to receive the "Designed for Windows XP" logo, the designation for software certification for the XP O/S.

As a Microsoft Gold Certified Partner, RSA receives early releases of service packs and new products to test for interoperability. RSA Security tests interoperability with the new Microsoft release to ensure that RSA SecurID for Microsoft Windows is compatible with the latest relevant Windows revisions.

RSA Security's policy is to test Microsoft XP, Microsoft Windows 2000 and 2003 client software with Microsoft fixes, security packages and service packs for compatibility with RSA SecurID for Microsoft Windows before these Microsoft updates are released.

In addition, RSA Security and Microsoft jointly support this product. Support calls to Microsoft will be answered and the issues directed to Microsoft or RSA Security as appropriate.

II. GRAPHICAL IDENTIFICATION AND AUTHENTICATION (GINA)

GINA is a generic acronym for the Graphical Identification and Authentication, the subsystem that handles the logon presentation to the user. The Microsoft GINA is represented by the logon screen that pops up on the PC when the user presses Ctrl+Alt+Delete.

Windows 2000 and XP rely on a GINA DLL for Graphical Identification and Authentication. The Microsoft GINA DLL is called MSGINA.DLL.

User Experience

When Microsoft Windows users start their desktop, users are prompted to press Ctrl+Alt+Delete to begin the logon process. The Windows operating system then displays a logon screen that asks users to enter their user name and password. Once users respond, the Windows operating system takes the information and authenticates users before granting access to the Windows operating environment.

With the RSA SecurID for Microsoft Windows solution, upon pressing Ctrl+Alt+Delete, users will be prompted for their user name and passcode. This passcode consists of the user's PIN (something the user knows) followed by the unique token code displayed on the user's RSA SecurID authenticator at that time (something the user has).

The combined user ID and passcode information is then passed on to the RSA Authentication Manager software, which confirms that users have presented the proper passcode before granting or denying access to the Windows desktop and/or domain.

The offline user experience is consistent and looks the same from the user's perspective. RSA Authentication Agent 6.1 for Microsoft Windows implements the RSA GINA API to protect desktop logons. The RSA Authentication Agent GINA does not replace Microsoft's GINA. Instead, the RSA GINA is tightly integrated with Microsoft GINA and relies on it to handle all of the internal Windows authentication tasks.

GINA Chaining

In addition to the RSA Authentication Agent GINA, there are also other third party GINA DLLs including NWGINA.DLL (Novell NetWare Client) and AWGINA.DLL (pcAnywhere). Some applications (such as those listed above) require their own GINA DLL, but Windows can only load one GINA DLL. The solution to this problem is to have GINA DLLs loading and calling one another in a "chain". The RSA SecurID for Microsoft Windows solution will support GINA chaining, but the RSA GINA must be installed as the last in the chain.

Kerberos Tickets

The RSA Security components do not issue or verify Kerberos tickets. Rather, the RSA Security components provide the Windows password to the end user's Microsoft GINA When online, the Microsoft GINA will authenticate against a domain controller and receive a Kerberos Ticket. When offline, the GINA will check the Windows password against Microsoft's cached credential store and generate an offline Kerberos Ticket. On reconnection to the network, and depending on how the domain controller is configured, the user's cached credential is used to acquire the Kerberos tickets.

If the domain controller is configured to force a re-authentication, then the Windows password will be supplied to the domain controller for generation of the ticket.

III. SUPPORT FOR THIRD PARTY GINAS

Because RSA GINA does not replace Microsoft GINA, third-party products that capture the Microsoft Windows password as it is passed into Microsoft GINA, still work. Again, because RSA GINA delegates tasks to Microsoft GINA, RSA GINA must be the last GINA in the GINA chain (if one exists).

Some software vendors implement their GINAs as chaining GINAs. This means that after a GINA finishes executing its authentication tasks, it can pass authority to another GINA down the GINA chain. Note that there is no standard method by which one GINA can chain to another GINA. Microsoft only defines a method for a single GINA to replace the Microsoft GINA. Third party GINA vendors like RSA Security cooperate with each other to ensure that their GINAs can work together.

Chaining GINAs can pass authority to the RSA GINA provided that the chaining GINAs have documented support for GINA chaining, and that the RSA GINA is the last in the GINA chain.

RSA Authentication Agent 6.1 for Microsoft Windows directly supports some chaining GINAs by registering the RSA GINA correctly with the third party GINA during RSA Authentication Agent installation. RSA Authentication Agent indirectly supports other chaining GINAs by enabling you to manually configure your registry to enable the third-party GINAs to chain to RSA GINA.

Directly Supported GINAs

Directly supported GINAs are ones that the RSA Authentication Agent installer correctly registers with so it can chain to the RSA GINA. RSA Authentication Agent 6.1 for Windows directly supports the following third-party chaining GINAs:

- Check Point VPN SecurRemote/SecureClient (Ckpginashim)
- Cisco VPN client (Csgina)
- Citrix Metaframe (Ctxgina)
- Symantec pcAnywhere (Awgina)
- Funk Odyssey WLAN client
- Nortel VPN client

If these products are on your system, when you install RSA Authentication Agent 6.1 for Microsoft Windows, the RSA Authentication Agent installer places RSA GINA in the correct location for the third party GINA. For more information, see "Installing the RSA Authentication Agent GINA" on page 136 of the documentation in the RSA Authentication Agent 6.1 for Windows Installation and Administration Guide.[1]

Integration with the Novell Client

The RSA GINA does not "chain" to the Novell GINA. Instead, it integrates with the Novell Client for specific use cases. The Novell Client handles logon to the Novell Network, and the RSA GINA uses Novell Client APIs to change the Novell password when necessary. This feature must be enabled using the control panel.

When the RSA GINA is installed, the Novell GINA is not loaded.* Instead, the Novell Client registers itself as a Credential Manager.[2] The Novell client is notified of all logons, and if the user's Windows password is the same as the Novell password, the user is logged in to Novell automatically. Credential Managers do not require any action on the part of RSA SecurID for Windows to work properly and is a supported part of the Windows operating systems.

For those deployments that require synchronization of the Windows and Novell passwords and had been depending on the Novell GINA to perform that synchronization, the RSA GINA is being enhanced to inform the Novell Client of the user's new password, allowing those two passwords to remain synchronized. The RSA GINA allows the Microsoft GINA to perform the Windows password change but also

[1] RSA ACE/Agent and RSA ACE/Server were renamed in 2004 as RSA Authentication Agent and RSA Authentication Manager, respectively. Some documentation may retain the old nomenclature

[2] See http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secauthn/security/credential_management_api.asp.

intercepts the password change notification being sent to network providers. When it does, it loads the Novell Client's netwin32.dll and calls its NWDSChangeObjectPassword() function. This tells the Novell Client about the new password and allows it to keep the password synchronized in NDS.

In addition, the RSA GINA understands the ten most common error codes returned from the Novell Client should a non-successful password change occur (e.g., "User does not exist in the Novell directory"). The messages were provided by Novell. These errors are reported to users that encounter them to inform them of the problem. If an error occurs for which no error message is defined, the RSA GINA displays the error mnemonic provided by Novell in their integration "header" files.

Indirectly Supported GINAs.

Indirectly supported GINAs are ones that can co-exist with the RSA Authentication Agent, but are not configured to chain to the RSA GINA by the Agent installer. You can use RSA Agent 6.1 for Windows with third-party chaining GINAs that are not directly supported by manually configuring your registry to enable chaining to the RSA GINA. For registry keys and values, see the section "Manually Configuring GINA Chaining" in the documentation "RSA Authentication Agent 6.1 for Windows Installation and Administration Guide".

Manually Configuring GINA Chaining

You can manually configure your registry to enable chaining with indirectly supported third-party GINAs. You can also edit the registry to repair the GINA chain if the RSA Authentication Agent or the third-party GINA installer creates a configuration that renders either the RSA GINA or the third-party GINA inoperable.

Unsupported GINAs

Some vendors implement GINAs as replacement GINAs. This means that the replacement GINA does not use the Microsoft GINA and does not pass through to another GINA. The RSA GINA cannot coexist with replacement GINAs. To use RSA Authentication Agent 6.1 for Windows on a system that has a third-party replacement GINA, you must replace the third-party GINA with RSA GINA. For more information, see the documentation "Installing the RSA Authentication Agent GINA"

Important: RSA Security recommends uninstalling the third-party GINA software instead of replacing the third-party GINA with RSA GINA when you install the RSA Authentication Agent. Uninstalling the third-party replacement GINA software after you install RSA GINA may prevent RSA GINA from functioning. If you plan to install unsupported third-party GINA software, RSA Security recommends uninstalling the RSA Authentication Agent first.

Installing the RSA Authentication Agent GINA

If there are no previously installed third-party GINAs on the system, the RSA Authentication Agent 6.1 for Windows installer registers the RSA GINA as the official GINA on the Windows system. If a supported third-party GINA is already installed on the system, the Agent installer configures the GINA to chain, or pass authority, to RSA GINA. The third-party GINA remains the official GINA on the Microsoft Windows system. If an unsupported third-party GINA is already installed on the system, the RSA Authentication Agent installer warns you about it and prompts you to either abort the installation or replace the third-party GINA's registration with the RSA GINA. (The third party software is not removed.)

If you choose to abort the installation, the RSA GINA is not installed and no change is made to the system. If you choose to replace the current GINA with RSA GINA, the installer unregisters the third-party GINA and registers RSA GINA as the official GINA on the Microsoft Windows system. Any functionality from the third-party GINA that is replaced by RSA GINA is lost.

Note: Although the RSA Authentication Agent gives you the option of replacing the third-party GINA, RSA Security recommends that you uninstall the third-party GINA before you install RSA Authentication Agent. If you attempt to install a third-party GINA after RSA GINA has been installed, the behavior of RSA GINA depends on whether the third-party GINA installer can correctly chain to RSA GINA.

SUMMARY

The RSA SecurID for Microsoft Windows solution provides a convenient and consistent authentication experience, encouraging adoption. It is easy to implement and manage and designed to be compatible with the Microsoft Windows GINA architecture, not replace it. SecurID for Windows also allows for the support of other popular security application software GINAs such as Citrix, Cisco, Check Point, Funk and Nortel—as long as the SecurID for Windows is the last GINA in the chain.

GINA INTEROPERABILITY

PRODUCT GINA	STATUS	COMMENT
Check Point SecureRemote / Secure client	Directly supported	
Cisco VPN client	Directly supported	
Citrix MetaFrame	Citrix ICA client fully supported	To log on to Citrix Metaframe Presentation Server with RSA SecurID, requires user ID, RSA SecurID passcode and domain.
Symantec pcAnywhere	Directly supported	
Funk Odyssey WLAN client	Directly supported	
Nortel VPN client	Directly supported	
RSA Sign-On Manager 4.1	Directly supported	
RSA Authentication Utility 1.0 RSA SID800 authenticator	Directly supported	
Novell	Password update and error message integration may be enabled through the control panel	The RSA GINA integrates with the Novel client in order to keep the Windows and Novell passwords synchronized.

ABOUT RSA SECURITY

RSA Security is the expert in protecting online identities and digital assets. The inventor of core security technologies for the Internet, the company leads the way in strong authentication and encryption, bringing trust to millions of user identities and the transactions that they perform. RSA Security's portfolio of award-winning identity & access management solutions helps businesses to establish who's who online—and what they can do.

With a strong reputation built on a 20-year history of ingenuity, leadership and proven technologies, we serve more than 18,000 customers around the globe and interoperate with more than 1,000 technology and integration partners. For more information, please visit www.rsasecurity.com

GINA TB 0905

RSA SECURITY®

RSA Security Inc.
www.rsasecurity.com

RSA Security Ireland Limited
www.rsasecurity.ie