RSA SecurID Quick Reference Card

RSA SecurID Solution Summary

The RSA SecurID system identifies and authenticates authorized users at designated access points and denies unauthorized access attempts.

RSA SecurID authenticators help organizations protect private information and assure the identities of users, devices, and applications exchanging that information. They are designed to fit seamlessly into the existing business infrastructures of over 30,000+ organizations worldwide. With over 25 years of outstanding performance and innovation, the RSA SecurID solution remains an industry standard for organizations that want to protect key business data assets. RSA SecurID authenticators provide organizations with:

- Strong network security
- Reliable authentication
- Convenient solutions for users
- A choice of form factors and options

Each RSA SecurID authenticator has a unique symmetric key that is combined with a proven algorithm to generate a one-time password (OTP) every 60 seconds. Patented technology synchronizes each authenticator with the security server, ensuring a high level of security. The OTP is coupled with the user's personal identification number (PIN) to create a combination that is nearly impossible to be hacked. This protection is imperative when there is a risk of exposing critical information.

The RSA SecurID 700 used at BNY Mellon is a small fob that can be easily carried in the user's pocket or on a key ring.

Using the RSA SecurID

When the user attempts to access a protected entity, like a Virtual Private Network (VPN) or a secure portal, they are prompted for their user ID and passcode. The passcode is a combination of their PIN the OTP currently displayed on the token.

The user ID and passcode are transmitted to the RSA Authentication Manager Agent and verified by the RSA Authentication Manager software, the system's authentication engine. The software checks the passcode to ensure it is correct before issuing instructions to the system to either allow or deny access to the user.

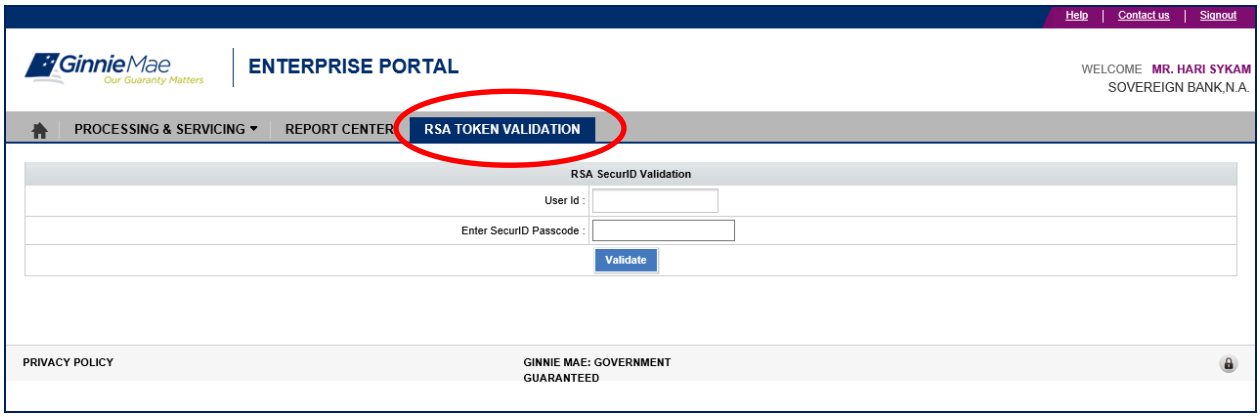
Once the user is authenticated, access is allowed and the user may access the protected resources.

GMEP RSA SecurID Token Authentication Validation

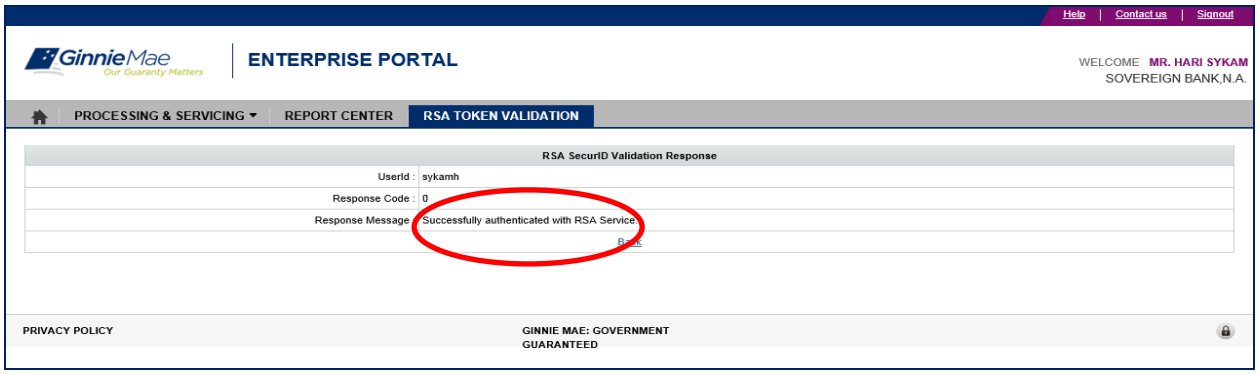
1. Log in to the GMEP Portal (www.eginniemae.net) and click on the **RSA Token Validation** tab and enter **User ID** (not case sensitive) and **Passcode**.

Note: The Passcode is your 4-digit PIN followed by your 6-digit Tokencode (the 6 digits displayed on your RSA SecurID token). When entering your Passcode, ensure that there are no spaces between your 4-digit PIN and your 6-digit Tokencode.

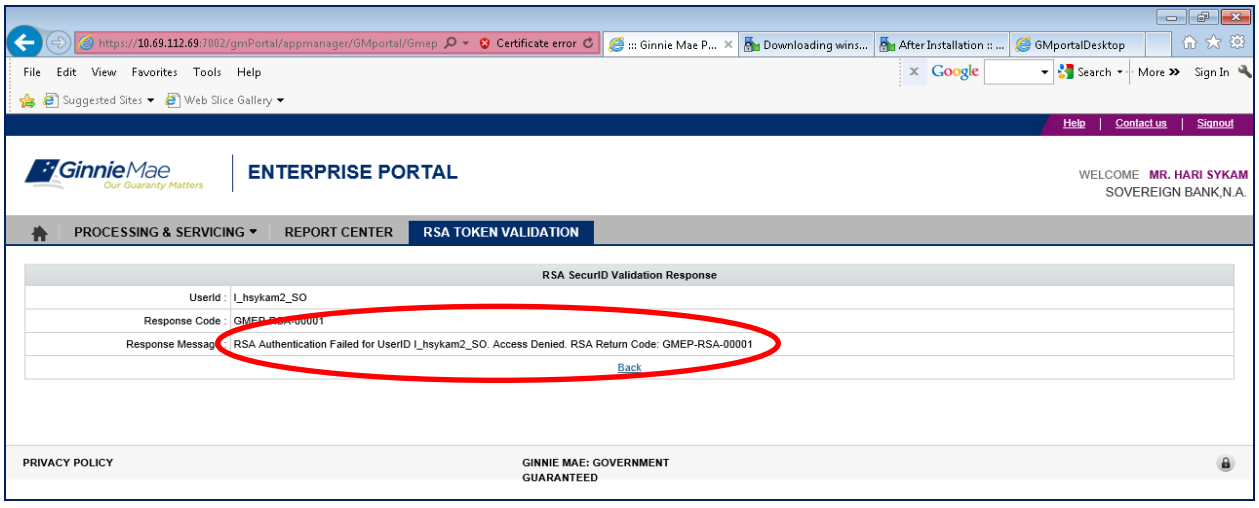
Example: If your User ID is ABC123, then enter ABC123 in the **User ID** field. If your 4 Digit PIN is 9876 and the 6 Digit Numbers that is currently being displayed on the RSA SecurID Token is 289437, then enter 9876289437 in the Enter SecurID Passcode field.



A **Valid Authentication** will display the following response message:
Successfully authenticated with RSA service.



An **Invalid Authentication** will display the following response message:
RSA Authentication failed for USER <USER NAME><RSA RETURN CODE>.



If you receive an invalid authentication, repeat the log in process and ensure that information is entered correctly.

If you still have issues with authentication being invalid, contact RSA SecurID Token Activation Line at 1-800-332-4550 (option 8).