RSA SECURID TOKENS

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.

RSA SecurID 700

The RSA SecurID 700 is a small key fob that connects easily to any key ring and fits into a user's pocket or small carrying case. Its display includes a countdown timer until the next token code is displayed, as well as the token code itself in an easy to read window. For more information about RSA SecurID tokens refer to https://www.rsa.com/content/dam/en/data-sheet/rsa-securid-hardware-tokens.pdf .

CONFIRM ABILITY TO SUBMIT IN GINNIENET

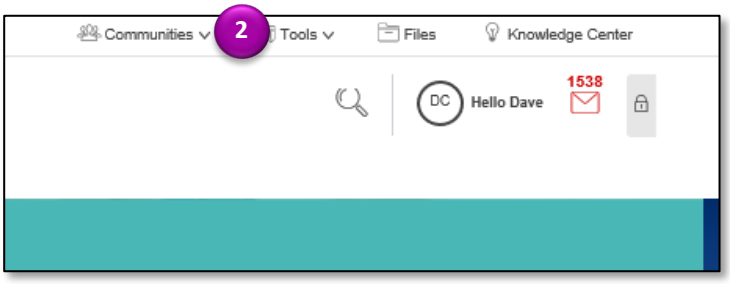
In order to submit data in GinnieNET, the user must first have the following:

1. Be listed on HUD Form 11702
2. Have a GinnieNET login and password
3. Have a GinnieNET role assigned
4. Have a GMEP Login and Password
5. Have SecurID Token Role Assigned in GMEP
6. Have "Authorized GinnieNET Signer" role assigned in GMEP
7. Have an active SecurID Token
8. Ensure that the "Verify Role Assignment" check in GMEP has been completed by the user or the Security Officer

If the user has completed Steps 1-8 above, then the user may continue to the following process.

ACCESS GINNIE*NET*

1. Log in to MyGinnieMae via https://my.ginniemae.gov.
2. Select the **Tools** dropdown at the top of the Dashboard.
3. Select **Ginnie*Net*** under Applications.



The Ginnie*NET* on the Web Main Menu will display.

HOST COMMUNICATIONS

4. Select the **Host Communications** link on the Ginnie*NET* Main Menu.
5. Select one of the available menu options,

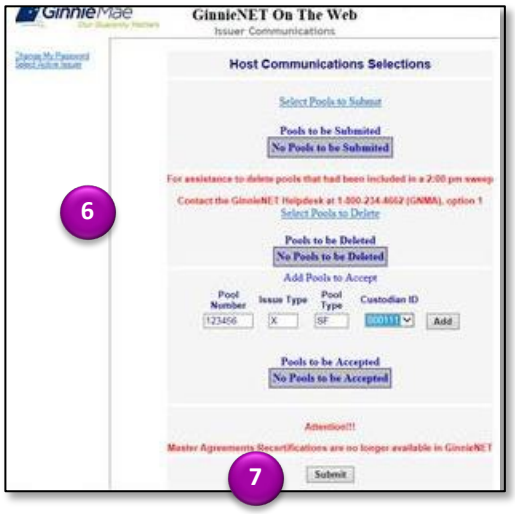
NOTE: Issuers will have the following menu options to choose from:

- Issuer Communications
- Investor Reporting Communications
- Certifications Communications
- HMBS Investor Communications
- HMBS Investor Reporting Communications
- HMBS Certifications Communications

NOTE: Document Custodians will have the following menu options to choose from:

- Custodian Communications
- Certification Communications
- HMBS Custodian Communications

6. Complete the tasks for the selected option.
7. Select **Submit**.

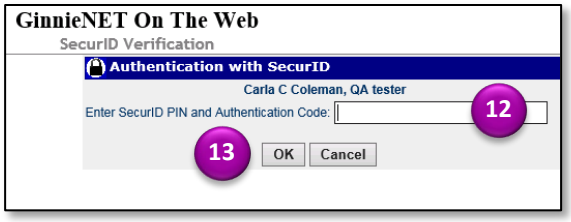


SUBMISSION PROCESS

8. Enter your Title.
9. Select OK.

10. Enter your GMEP ID and Password.
11. Select OK.

12. Enter your 10-digit ID consisting of your 4-digit PIN followed by the SecurID Token Authentication Code displayed on your token.
13. Select OK.



A “Success” or “Failure” login message will display. For unsuccessful login, retry or contact the SecurID Assistance Client Assistance Center at: 800-332-4550 (Option 8).