SecurID Token FAQs

A. General Questions

1. **What is a SecurID Token?**
   A SecurID Token, also known as 'key fob' or SecurID Token (and formerly known as an RSA SecurID Token), is a device used to access a digital asset, (i.e. a computer system, or specific system functions). SecurID Tokens are used by organizations to protect private information and ensure that individuals, devices and applications exchanging information are authorized to do so.

   The SecurID Token is part of a two-factor authentication process in which a User can access a system and/or submit an approval by entering their User ID and password, for that system, followed by entering a four-digit PIN, (assigned when a user performs the initial SecureID Token validation) along with the six-digit code provided by the SecurID Token. This six-digit code is refreshed periodically, providing additional security.

2. **Why does Ginnie Mae require the use of a SecurID Token?**
   Ginnie Mae requires the use of SecurID tokens to ensure that the individuals performing the submission or approval function(s) in Ginnie Mae's Systems, including GMEP and Ginnie*NET,* are authorized to do so.

3. **Do I need to have a SecurID Token to access GMEP and Ginnie*NET*?**
   No. You can access GMEP and Ginnie*NET* the same way you do now, using the same User ID and Password credentials. A SecurID Token is required only for certain submissions and approvals in those systems.

4. **How do I know if I need a SecurID Token?**
   You need a SecurID Token if you are responsible for requesting Commitment Authority, Managing and submitting Master Agreements, or Requesting Pool Transfers via GMEP. You will also need a SecurID Token for submitting pools and reports in Ginnie*NET*.

5. **If I'm able to submit pools and reports in Ginnie*NET* using the fingerprint scanner, do I still need to obtain a SecurID token for Ginnie*NET*?**
   Yes. SecurID Tokens will replace the Biometric fingerprint scanner device for submissions in Ginnie*NET*. For instance, Tokens will be needed for pool submissions, pool certifications, or reporting and remittance advice submissions. Hence, even if you perform those functions without a SecurID Token now—by using the fingerprint authentication process—you will need a SecurID Token when the use of fingerprint scanners is phased out.

6. **If I currently have access to and use Ginnie*NET*, but do not need to use the fingerprint scanner, do I need a SecurID Token?**
   No. If you currently use Ginnie*NET*, but are not required to use the fingerprint scanner to complete your work, you will not need a SecurID Token. You will, however, need to submit an updated User Registration Form(Appendix III-29) to a Security Officer in your organization. See Ginnie Mae Systems User Registration form on Ginnie Mae's Modernization webpage.

7. **When will the new SecurID Token requirement for Ginnie*NET* go into effect?**
   The SecurID Token functionality in Ginnie*NET* is targeted to go into effect mid November 2015. Ginnie Mae will issue an All Participants Memo (APM) to announce the effective date. All pools

submitted to Ginnie*NET* or certified by a Document Custodian on or after the effective date *must* be submitted or certified using a SecurID Token.

8. **How will the SecurID Token be used in Ginnie*NET*?**
   After you have logged into Ginnie*NET*, and are ready to submit pools or reports, or to certify pools, the system will prompt you for your GMEP User ID and password, and subsequently for your four-digit PIN, plus the six-digit code from your SecurID Token. This process must be completed for each submission.

9. **Will the upcoming Changes to GinnieNET affect how I use SecureID tokens in GMEP?**
   No. The use of the SecurID Tokens in GMEP will remain the same. After you have logged into GMEP and are ready to submit Master Agreement(s), Commitment Authority requests, Pool Transfer requests, and the like, GMEP will prompt you to enter your four-digit PIN, plus the six-digit code from your SecurID Token. This must be completed each time you submit a new action.

10. **What is the process to replace, reassign, or deactivate a SecurID Token?**
    Security Officers for each organization should contact Ginnie Mae Relationship Services at 1-800-234-4662 (Option 1), or Ginniemae1@bnymellon.com as soon as possible to arrange deactivation of the SecurID Token. Be sure to note the subject line of your email that you are inquiring about SecurID Tokens.

B. Obtaining a SecurID Token

1. **How do I obtain a SecurID Token?**
   If you already have a GMEP ID, you must complete *SecurID Token Request Form* (see Ginnie Mae's Modernization webpage) and submit the completed form to your organization's Security Officer. If you do not have a GMEP ID, you will need to complete and submit a *Ginnie Mae Systems User Registration Form* and the *SecurID Token Request Form* to your organization's Security Officer. The Security Officer must submit those forms to Ginnie Mae's Pool Processing Agent. The SecurID Token will be sent to your Security Officer, who should then contact you to pick it up

2. **Who is my organization's Security Officer?**
   If you do not know who your Security Officer is, please contact Ginnie Mae Relationship Services at 1-800 234-4662 (Option 1), or Ginniemae1@bnymellon.com.

3. **Where do I obtain the forms I need to submit to my Security Officer?**
   The Ginnie Mae System Access User Registration Form and the SecurID Token Request Form may both be found with on Ginnie Mae's modernization webpage at:
   http://ginniemae.gov/doing_business_with_ginniemae/modernization/Pages/default.aspx

4. **Do I have to resubmit or update the Ginnie Mae Enrollment Administrator and GinnieNET Authorized Signatories Form, Appendix III-14?**
   No. The Ginnie Mae Enrollment Administrator and GinnieNET Authorized Signatories Form will no longer be required. Only the forms listed in the link provided for Question 3, immediately above are required.

5. **When can I submit the new User Registration Form and/or the SecurID Token Request Form**?
   You may complete and submit these forms to one of the Security Officers in your organization immediately.

6. **I have received my SecurID Token, what do I do next?**
   You need to enable and then validate the SecurID Token before it is ready to use. Instructions on how to enable and validate SecurID Tokens are available on Ginnie Mae's website at: http://ginniemae.gov/doing_business_with_ginniemae/modernization/Pages/default.aspx . This process takes less than 15 minutes.

C. Issuer User Specific FAQ'S

1. **Do I have to be listed on the form HUD-11702 to be issued a SecurID Token?**
   Yes, individuals representing an Issuer must be listed on the Issuer's form HUD-11702 (Resolution of Board of Directors and Certificate of Authorized Signatures) in order to be assigned a SecurID Token. This ensures that the individual performing the function on Ginnie Mae's System(s) is authorized to do so.

2. **If I am currently authorized to use Ginnie*NET* for pool processing and I already have a SecurID Token for use on GMEP, will my current SecureID Token work for the new Ginnie*NET* requirement automatically?**
   Yes. Your User ID and SecurID Token will automatically link to Ginnie*NET*, but you must submit an updated Issuer User Registration Form (you can access the form through the Modernization page on Ginnie Mae's website) to your Security Officer indicating that you will use your SecurID Token for completing submissions through Ginnie*NET*. The SO must also add the appropriate role to the user in GMEP.

3. **Will Ginnie*NET* continue to be used for entering pool data?**
   Yes. Pool Data will continue to be entered in Ginnie*NET*. However, once the SecurID Token functionality replaces the fingerprint biometric security access to Ginnie*NET,* in order to submit pools or investor reports or certify pools, a User will be required to enter both, the GMEP identification and password as well as a PIN number and the SecurID Token information, in order to access Ginnie*NET* for submission.

D. Security Officer Questions

1. **I am a Security Officer, how do I obtain a SecurID Token for myself or others in my company?**
   Normally a Security Officer does not need a SecurID Token to perform Security Officer functions. However, if the Security Officer has an assigned GMEP User ID and password and wishes to perform certain User functions on GMEP, then the Security Officer will need to complete the RSA SecurID Token User Request Form and provide it to another Security Officer within the organization to process.

   If you do not have a GMEP User ID and password, you will need to complete the User Registration Form in addition to the RSA SecurID Token User Request Form and provide it to another Security Officer within your organization to process. You may order SecureID Tokens for other Users in your company. Before ordering a SecurID Token for another user, you must receive and review the user's complete User Registration Form and SecurID Token Request form (which can be found on the Modernization page on Ginnie Mae's website at http://ginniemae.gov/doing_business_with_ginniemae/modernization/Pages/default.aspx .

Once you have reviewed the forms for completeness and accuracy, you may submit the forms to Ginnie Mae Relationship Services. Ginnie Mae Relationship Services will send you the

SecurID Tokens for distribution. The Security Officer also must create the User ID in GMEP and a second Security Officer must approve.

2. **What information do I (Security Officer) need to obtain from a Ginnie*NET* user in my company who is requesting a SecurIDToken?**
   To request a SecurID token, GinnieNET users must submit an updated User Registration Form. If you work for an Issuer or if you work for a Document Custodian, the appropriate forms are available on Ginnie Mae's website at: http://ginniemae.gov/doing_business_with_ginniemae/modernization/Pages/default.aspx .

3. **How will I assign the Ginnie*NET* roles listed in the User Registration Form in GMEP?**
   The Security Officer interface in GMEP that will enable you to assign the Ginnie*NET* user roles listed in the User Registration Form. We will notify Issuers when this interface is added to GMEP. Ginnie Mae also will host training calls for Security Officers to communicate the new process.

4. **I am a Security Officer, but I was not the Enrollment Administrator for Ginnie*NET*, do I have to maintain the Ginnie Mae Enrollment Administrator and Ginnie*NET* Authorized Signatories Form, Appendix III-14, updated?**
   No. The Ginnie*NET* Enrollment Administrator role is being merged into the GMEP Security Officer functions. However, Issuers may wish to retain a different Security Officer for each system. Although these forms have not yet been removed from the MBS Guide, the Ginnie Mae Enrollment Administrator and GinnieNET Authorized Signatories form (Appendix III-14) will be replaced by a new Ginnie Mae Systems Access form (A copy of the form is available on the modernization page on Ginnie Mae's website).

5. **Will a second SO have to approve the access?**
   In order to create a new User ID in GMEP, you need the approval of two Security Officers (SO) who are different from the individual requesting the User ID. The same number of SOs is required to complete the Secur ID Token Holder and Authorized Ginnie*NET* signer role in GMEP.

6. **How do we add a new SO?**
   The individual taking over as an SO needs to submit the Security Officer Registration form found in Appendix III-29.

7. **Can the Verify Role Assignment check be completed by both the SO and the user.**
   Yes. Security Officers can complete the "Verify Role Assignment" check for any GMEP User ID that is associated with the organization(s) for which the SO is responsible, by entering the User's ID and assigned Organization number. The User can also complete the "Verify Role Assignment" check by entering his or her User's ID and assigned Organization number.

   The Verify Role Assignment check will validate various factors to determine whether the user and SO have completed all the steps necessary for that user to perform submissions in GinnieNET using a SecurID token. A detailed list of what steps need to be taken pursuant to the messages in the Verify Role Assignment check follows:

Message Received	Action to be Taken
Succeeded	No more action. Task is complete.
Userid is Active	No action required.
Userid is Not Active	User’s GMEP login needs to be approved by a secondary SO.
Userid Does not Exist	Make sure the correct GMEP login ID was entered for the user.
SecurId Token Role is Active	No action required.
SecurId Token Role is Not Active	Ensure user has been given SecurID token role and has been approved by secondary SO.
SecurId Token Role is not found	SecurID Token Holder role has not been assigned to this User ID. Need to assign the role before it can become activated.
GNET Authorized Role is Active	No action required.
GNET Authorized Role is Not Active	Ensure user has been given Ginnie*NET* Authorized Signer role and has been approved by secondary SO.
GNET Authorized Role is not found	Ginnie*NET* Authorized Signer role has not been assigned to this User ID. Need to assign the role before it can become activated.
Organization is Active	No action required.
Organization is Not Active	Ensure you have entered the correct Company ID (Issuer or Document Custodian ID)
Organization is not found	Ensure you have entered the correct Company ID (Issuer or Document Custodian ID)
OrgID assignment is Active	No action required.
OrgID assignment is Not Active	The Company ID is assigned to this user but not yet approved by Security Officer. A Security Officer must approve the change
OrgID Not found on User Profile	The Company ID (Issuer ID or Document Custodian ID) entered is not associated with this user. First, ensure that you have entered the correct Company ID and User ID. If validation continues to fail after confirming the Company ID and User ID, ensure that an SO assigns this Company ID to this user’s GMEP Profile. See Quick Reference Card IS-3 or DC-3, for Issuers or Document Custodians respectively.
OrgID setup for GNET Authorized Role and is Active	No action required.
OrgID setup for GNET Authorized Role and is Not Active	The Company ID entered above has been assigned to this user in the “Authorized GinnieNET Signer Role for Issuers” Screen in GMEP, but the assignment has not been approved. A Security Officer must approve the change.
OrgID Not setup for GNET Authorized Role	The Organization Company ID entered was not selected for this user in the “Authorized Ginnie*NET* Signer Role for Issuers” Screen. First, ensure that you have entered the correct Company ID and User ID. If validation continues to fail after confirming the Company ID and User ID, ensure that an SO assigns the relevant Company ID to this user on the “Authorized GinnieNET Signer Role for Issuers” Screen. See Step 9 in Quick Reference Cards IS-3 and DC-3 for Issuers and Document Custodians, respectively. Also, ensure that secondary SO approves the assignment.
User is Authorized Signer	No action required.
User is not Authorized Signer	Ensure user is listed on the form HUD 11702 and that the spelling of the user’s name in the GMEP profile matches the user’s name as listed in the form HUD 11702.
Authorized Signer for Subservicer	No action required.
Not an authorized signer for subservicer	This message will only appear if the user is not listed on the form HUD 11702 for the Company ID entered. This failed validation message indicates that, although the user belongs to an organization that is subservicing for the Company ID entered, the user is not listed as an authorized signer on the subservicer’s form HUD 11702. Ensure user is listed on the Issuer or its subservicer’s form HUD 11702 and that the spelling of the user’s name in the GMEP profile matches the spelling of the name on the relevant form HUD 11702.
Not employed by organization subservicing for issuer	The User ID entered is not associated with relevant Issuer or Subservicer/Organization. Ensure that you have entered the correct User ID and Company ID.
Only Security officer can request information of another user	This message will only appear if the user performing the role verification is not a Security Officer. Users who are not Security Officers can only verify roles assigned to their own profile. Ensure that the user enters the User ID that has been assigned to that specific user.
Security officer not associated to account	This message will only appear if the user performing the role verification is a Security Officer. When this message appears the validation has failed because the Security Officer attempted to verify the role of a user that is not associated with the organization that employs the Security Officer (i.e. the User ID entered was not given by the Issuer or a Subservicer of that Issuer). Ensure you have entered the correct User ID and Company ID. If you need to add another Issuer ID to the list of organizations associated with the relevant Security Officer or user, please Contact Ginnie Mae Relationship services at (800) 234-4662.
Overall Validation Failed	Address the failed validation messages.

8. Do we have to wait until 9/28 to start the process?

The SOs can assign the Ginnie*NET* Authorized Signer Role in GMEP now. The SO must complete the User Registration form listing the new role. This form can be found on the 2015 modernization page on Ginnie Mae's website.

9. How many SOs can I have?

An Issuer may employ as many Security Officers as the Issuer believes are necessary and appropriate to meet their business needs.

10. What if a person has GMEP access (with token pending) but does not have Ginnie*NET* access?

If the individual does not need to submit information through Ginnie*NET*, then nothing further needs to be done. On the other hand, if the individual will need to submit information through Ginnie*NET* for pooling, reporting, or HUD-11708 processing , the individual must request and be granted the relevant roles in Ginnie*NET* from your organization's Ginnie*NET* Enrollment Administrator and the SO must assign the Authorized Ginnie*NET* role in GMEP.

11. Do we complete Appendix III-29 in order to sign up a new security officer? Does that get mailed in?

Yes, the original executed Appendix III-29 must be mailed in to Ginnie Mae's Relationship Services.

12. For this next cutoff, we will continue using the finger scanner to submit the RPB and 11710D in GinnieNET. Is that correct?

Yes, for October 2015 you will continue to use the fingerprint scanner for the HUD-11710D. Beginning October 1, the RPB is reported only through the RFS module in GMEP; the form HUD-11710D must continue to be submitted through Ginnie*NET*, which requires use of the fingerprint scanner until the SecurID Token solution is fully implemented in Ginnie*NET*.

13. I am a User as well as a Security Officer (SO). Can I assign myself the role to submit the loans on the Ginnet*NET* system and the other SO who is offsite and does not submit loans verify my assignment? Then vice versa for other SO who is my back up?

All role assignments in GMEP, including the new Authorized Ginnie*NET* Signer role require the approval of two security officers who are different from the individual requesting the relevant role.

14. So everyone registered under GMEP needs access to Ginnie*NET* as well?

No, only those users who will submit documents through Ginnie*NET* Host communications will need to go through this process to ensure that the token will work for them.

15. Where should the Appendix III-29 be submitted?

The original signed Appendix III-29 must be mailed to Ginnie Mae Relationship Services to the following address: Ginnie Mae Relationship Services, c/o The Bank of New York, 101 Barclay Street – 8 East, New York, New York 10286-0001.

16. Our Enrollment Officer has taken a different position, how do I change the Enrollment Officer?

See the Ginnie*NET* Single Family Training Guide.

17. I am a Security Officer.   Where can I find the list of assigned roles for my organization and what they mean so we can ensure all the roles are up to date?

The company's Security Officer can run a User access report from GMEP. To run the report the SO would need to enter the user's ID. The system report will display the roles assigned and what they mean (for example, CM Issuer Access or e-Notification User).

18. Can you please show us how to "validate the token"?

SecurID Token Validation Instructions are available on Ginnie Mae's 2015 Modernization webpage.

19. Does the second security officer also have to be on the HUD-11702?

If that Security Office also will have signatory authority for the Issuer, then the Security Officer's signature must appear on the form HUD-11702. If the individual is not signing documents for Ginnie Mae submission, but is only acting as a backup Security Officer, then the signature currently is not required to appear on the form HUD-11702.

20. Today a non 11702 individual goes into Ginnie*NET* and prepares everything up to the point of actually submitting the document using the fingerprint. Will this still be an option, for someone to prepare and the authorized signer who has aSecurID Token to actually perform the submission?

Yes, that is still an option.

21. Did implementation get delayed? I thought this was supposed to start with October 1 reporting, but you said earlier that we would still use fingerprints on 10/1.

Yes, implementation of the SecurID Token solution for pool delivery through GinnieNET was delayed to mid-November 2015, in order to allow Issuers time to assign the User Roles and Users to obtain and validate SecurID Tokens. Streamlined Investor Reporting of RPBs through the RFS module of GMEP begins October 1, however. Please see APM 15-15 for more information on the implementation of Streamlined Investor Reporting.

22. If you are the current SO and user with both fingerprint access and a token, do you need to do anything for yourself?

All Ginnie*NET* users that currently use the fingerprint scanner to submit in Ginnie*NET* will need to request and be assigned the "Authorized Ginnie*NET* Signer" role in the portal and will need to ensure that they perform the "Verify Role Assignment Check." All role assignments in GinnieNET, including assignments of the "Authorized GinnieNET Signer" role need to be approved by at least two Security Officers who are different from the individual requesting the role assignment.

23. Do we order all the tokens at one time from GNMA?

Yes, that would be ideal.

24. Do you need the Fingerprint Scanners Back? Do we get a refund?

No you keep the fingerprint scanners.   There will be no refund.

25. Can you review the process for signing up an additional security officer?

Please submit the Security Officer Registration form found in Appendix III-29.

26. What if you have forgotten your 4 digit pin that was assigned?

Call Ginnie Mae's Relationship Services at 1-(800) 234-4662 (Option1) for assistance.

27. If you deactivate a user, does it deactivate the SecurID token?

No, you must obtain the individual's token and return it to Ginnie Mae Relationship Services.

28. So a non 11702 individual can log into Ginnie*NET* and select "submit," which will then take them to GMEP, at which point they log into GMEP and then the authorized signor submits in GMEP?

No. The user will never be taken to GMEP. Rather, the Ginnie*NET* authentication interface that previously prompted the user to use the fingerprint scanner will be replaced with a different Ginnie*NET* authentication interface that will request the GMEP User ID and password of an individual who is an Authorized Ginnie*NET* Signer and that individual's 10-digit SecurID passcode (comprised of the individual's four digit token pin plus the six digits displayed on the token). All of these interfaces appear within Ginnie*NET*.

The individual completing the new Ginnie*NET* Authentication interfaces using his or her GMEP login, password and SecurID passcode may be different from the individual who first logged in to Ginnie*NET*. Alternatively, the individual performing the actual submission may complete the authentication by logging into Ginnie*NET* from his or her station, as there is no longer a need to submit in Ginnie*NET* using the computer station attached to the fingerprint scanner.

29. Do we still need to create Private and Public Keys?Private and Public Keys are used for the Fingerprint Scanner. The Scanner is being replaced by the SecurID Token; thus, the Private and Public Keys function will no longer be used once the SecurID Token becomes functional.

E. Document Custodian User Specific FAQ's

1.   I am a Document Custodian, will I need a SecurID Token?

Yes. SecurID Tokens are required to electronically complete and recertify the form HUD-11715 (Master Custodial Agreement) and will be required in order to certify pools in Ginnie*NET.*

2.   Do I need to be on the HUD-11702 to obtain a SecurID Token?

No, unlike Issuers, Documents Custodian signatures do not need to be on a form HUD-11702 to obtain a SecurID Token.

3.   I am a Document Custodian with multiple locations, will I need a SecurID Token for each location?

It depends on how your custodial operations are managed. Pool Certifications and execution and submission of the Master Custodial Agreement (form 11715), require the use of a SecurID Token and may be performed at each location or by a single document custodian office as long as the user has proper access.

4. **Will the Document Custodian perform the Initial & Final Certification in the portal?**

No pool Certifications will still be performed in Ginnie*NET*. Therefore, the Document Custodian personnel will need to obtain and validate a SecurID Token.

F. Software Compatibility FAQ's

1.   What are the browser requirements to support the use of SecurID Tokens?

Internet browsers Microsoft Internet Explorer (IE) Versions 8, 9, 10 are fully supported. While SecurID Tokens may work with other browsers, Ginnie Mae will not offer support for browsers other than IE8, IE9 and IE10.

2. **What versions of Windows are required?**
   All versions of Windows are acceptable.

3. **Can I use App**le **iOS when accessing GMEP and using the SecurID Token?**
   No, Apple iOS is not supported by Ginnie Mae.

4. **What if I am using Internet Explorer 7 (IE7), will that work?**
   While the Internet Explorer version 7 (IE7) browser may continue to work with these applications, Ginnie Mae discontinued support for this browser version on October 26th, 2013, and recommends upgrading to IE8, IE9 or IE 10.

5. **Where can I find more information regarding these upcoming changes?**
   For the most up-to-date information, please visit the Ginnie Mae website at: http://ginniemae.gov/doing_business_with_ginniemae/modernization/Pages/default.aspx . Information and upcoming training opportunities also will be communicated via Ginnie Mae's Notes and News, directly from Ginnie Mae staff and Account Executives, and in upcoming Outreach Calls for Issuers, Document Custodians, and Security Officers. As information is updated and posted to Ginnie Mae's website, website subscribers will receive automatic notification.

6. **Who can I contact, if I still have questions?**
   For additional information, please contact your Account Executive directly, or the Ginnie Mae Relationship Services at 1-800-234-4662 (Option 1), or Ginniemae1@bnymellon.com.

7. We will be migrating to Internet Explorer version 11, and will be validating this in that environment. If we run into any issues, what tech support group can we contact?

Call Ginnie Mae Relationship Services at 1-800-234-4662 (Option1) for instructions.