SSO - Reset Password and Updating Password

Reset Password
When deciding how to reset a password, we found that we had two options: sending a new, automatically generated password to the user or sending a URL to the user to reset the password. Detailed below are pros and cons of each option.

Sending a new password
Pros
- Convenient for the user

Cons
- Persistent password is sent over email, which can be sniffed or intercepted through a MITM attack
- Locking someone out of their account is easy
    - If you know the email address of a user, you can lock them out of their account by resetting their password constantly

Sending a reset URL
Pros
- More secure
    - Password is not sent in plaintext
    - User will have to answer security questions before being able to reset password
    - Reset URL is not easily discovered (detailed further below)
    - 5 minute expiration

Cons
- Less convenient for user
    - User will have to answer and remember security questions
        - Potentially time consuming if user doesn't know answers

With these pros and cons in mind, we've decided that sending a reset URL would be the most secure way of resetting a password.

Sidenote: There's also the option of generating a random number that is sent to the user to input to reset the password. It works on the same practice as sending a reset URL, however, for the purposes of ease of use for the user, it was ultimately decided that a URL would be emailed to the user.

Generating Password Reset Tokens
Purpose: to send the user a unique url that obfuscates any knowledge as to who the token is intended for.

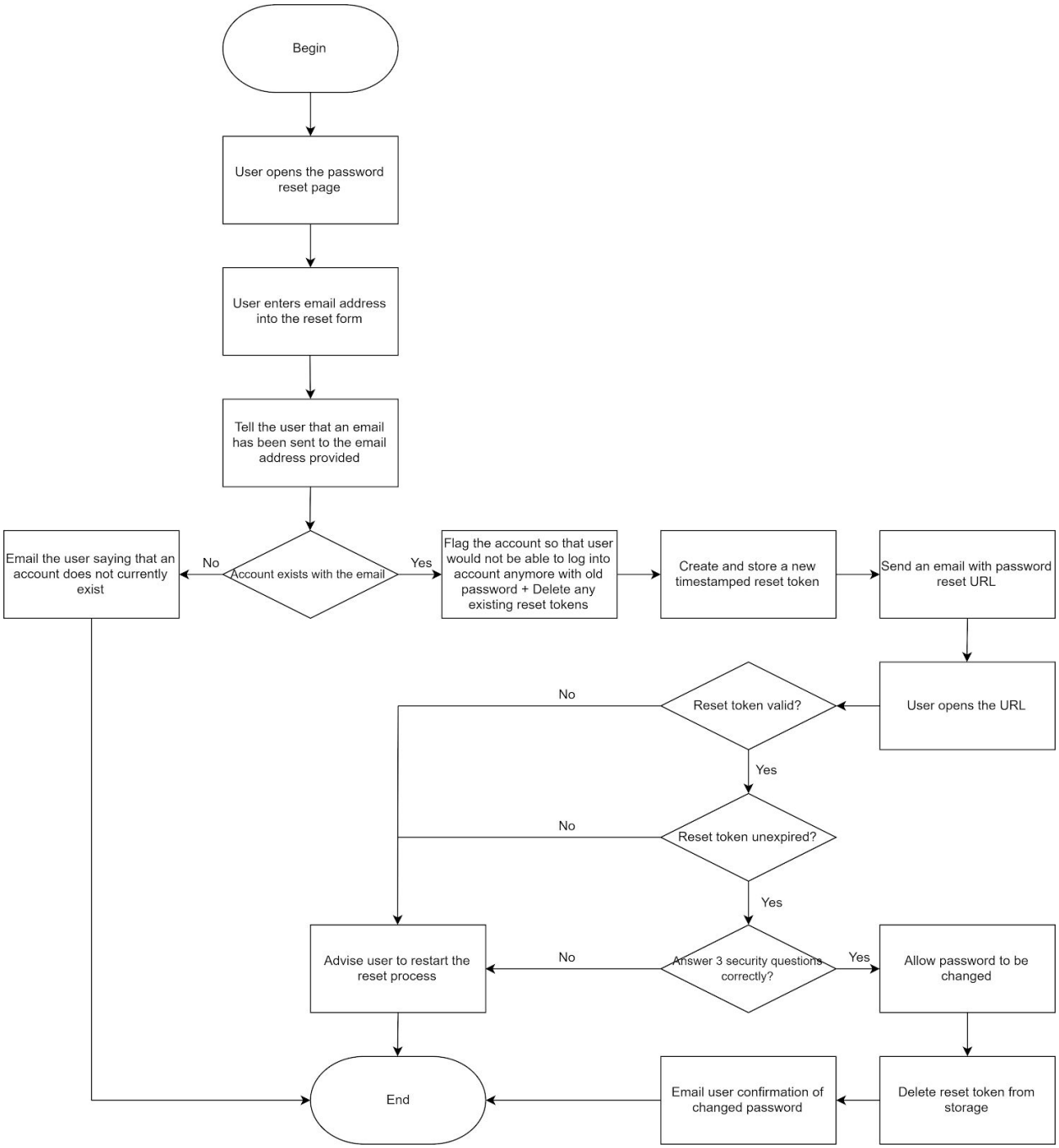
Generation: We will be using System.Security.Cryptography RNGCryptoServiceProvider class to generate our random string for the reset token. This reset token will 64 characters long with random numbers and letters.

Email Client
Originally, the emails were going to be sent through the SmtpClient class, however it's been deprecated and is no longer being supported. We found an alternative, open-source library called MailKit. So we will be using that.

Email Server
For the email server, Amazon offers an email service for users who have an application that is hosted in EC2. This service is free for up to 62,000 emails per month. Compared to setting up a custom email server, Amazon SES was a lot simpler so we chose it.

Password Reset Table
The password reset table has 7 columns, they are:
Guid ID - a unique id that is given to each reset token
string ResetToken - a cryptographically secure randomly generated string that identifies the reset token
Guid UserID - a unique id that identifies who the reset token is assigned to
Datetime ExpirationTime - a time that designates when the token expires
int ResetCount - an integer that keeps track of how many attempts have been made to reset the password with given reset token
bool Disabled - a boolean that determines if the reset token is unable to be used
bool AllowPasswordReset - a boolean that determines if the reset token can allow for a password reset

Flowchart for resetting password



Update Password

For updating the password, it’s pretty straight forward. As the user is already logged in, they already are authenticated. Therefore, updating the password is as simple as fulfilling the password requirements and clicking save.