1. When a user puts in his/her credentials, is that a onetime occurrence? Many newer devices (Windows Vista/7/8, MacOS X, iPhone, iPAD, Android) can configure themselves automatically and store credentials so this should be a onetime occurrence (until your password changes, of course).

2. If I leave the campus and return tomorrow or next week, will I auto connect to SecurePublic without have to put in my credentials again? Many devices will connect automatically by themselves and others can be setup to do this.

3. I get prompted to accept a certificate, is that necessary and will I only have to do that once? If you are prompted to accept a certificate, you must accept it; but you should only have to do this once.

4. What happens when I have to change my UTAD password, will I have to authenticate again to SecurePublic with my new PW? You will have to authenticate with your new password. However, you may be able to input and store your new password into your particular device(s) so that the new password will be sent automatically.

5. Can I connect to SecurePublic if I am a Alumni that still has a UT email account? You must have valid utad credentials to use SecurePublic. All other user classifications can utilize the UT SSID Public.

6. Can I connect to SecurePublic if I am an affiliate in Banner (ie. Promedica, Volunteer Faculty)? You must have valid utad credentials to use SecurePublic.

7. Is there a time limit of inactivity on SecurePublic where I will have to re-authenticate? Inactivity timeouts are a general feature of wireless networking and are a part of SecurePublic too. Devices that go to sleep or turn off their radios to conserve battery life or devices that move out of range of an access point will inevitably be disconnected. However, many of these devices can store authentication credentials and can be configured to connect automatically whenever the device wakes or comes within range of an access point again.

8. If I wipe my device, will I have to re-authenticate and accept the certificate again when I try to connect? Wiping a device generally destroys all configuration information on that device requiring reauthentication and certificate reacceptance.