

Sub Rosa Pro[®] for iOS

User Guide



Description	3
Installing and First Launch	3
Using Sub Rosa Pro	4
Gestures	5
Sub Rosa Pro User Interface	5
1. Card Slot Status	5
2. Address Bar	6
2.1 QR Code Scanner	6
3. Google Search	6
4. Enhanced OWA Client	6
4.1 OWA Mailbox	7
4.2 Creating a Message	8
4.3 Message Attachments	8
4.4 S/MIME	8
4.5 Save	8
4.6 Delegated or Shared Mailboxes	9
4.7 Calendaring	9
4.7a Creating And Editing A New Calendar Item	10
4.7b Additional Calendars	10
Click Done when you are finished editing	10
5. Page Navigation	10
6. Share	11
6.1 Secure Reset	11
6.2 Print	11
6.3 Add/Edit Bookmark	11
6.4 Mail Link to this Page	11
7. Bookmarks	11
8. Tabs	11
9. Settings	12
9.1 Advanced	13
Activating Entrust IdentityGuard Derived Credential	14
Changing Your Entrust PIN	14
Importing Purebred Credentials	15
Troubleshooting	17
Requirements	18
Further Information and Support	18

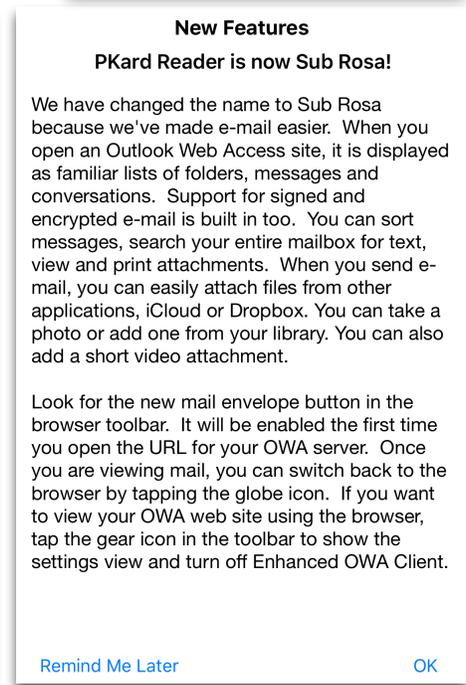
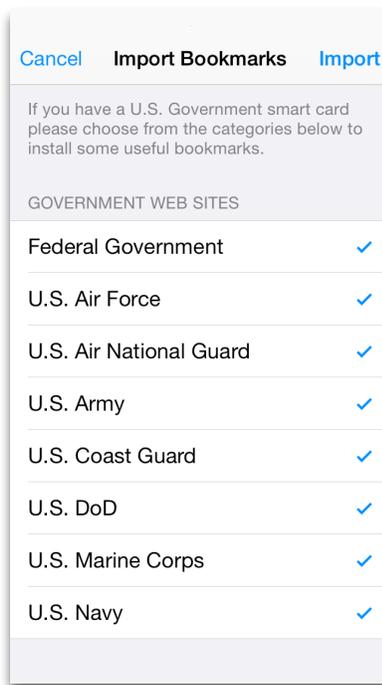
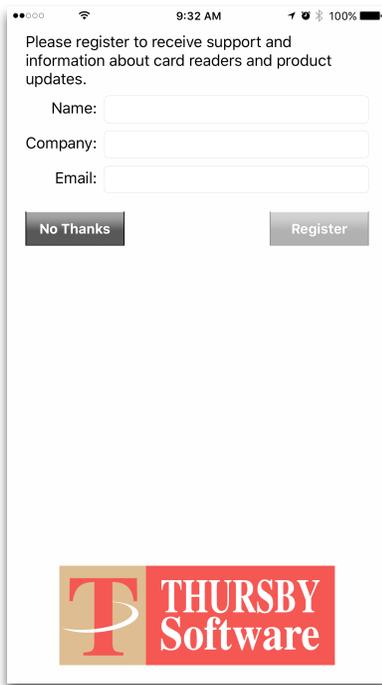
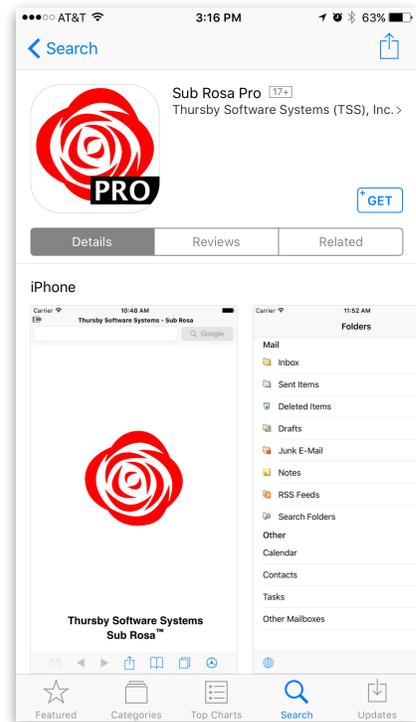
Description

Sub Rosa Pro is a mobile web browser utilizes two factor authentication using a smart card or derived credentials. Sub Rosa Pro does not require any certificates to be installed onto the iPad or iPhone and reads the certificates directly from the card.

Installing and First Launch

Connect your reader to your iOS device. You may be presented with a dialog stating the accessory requires an app. It will direct you to the App Store, and prompt you to download Sub Rosa Pro. If not, open the App Store and search for Sub Rosa Pro.

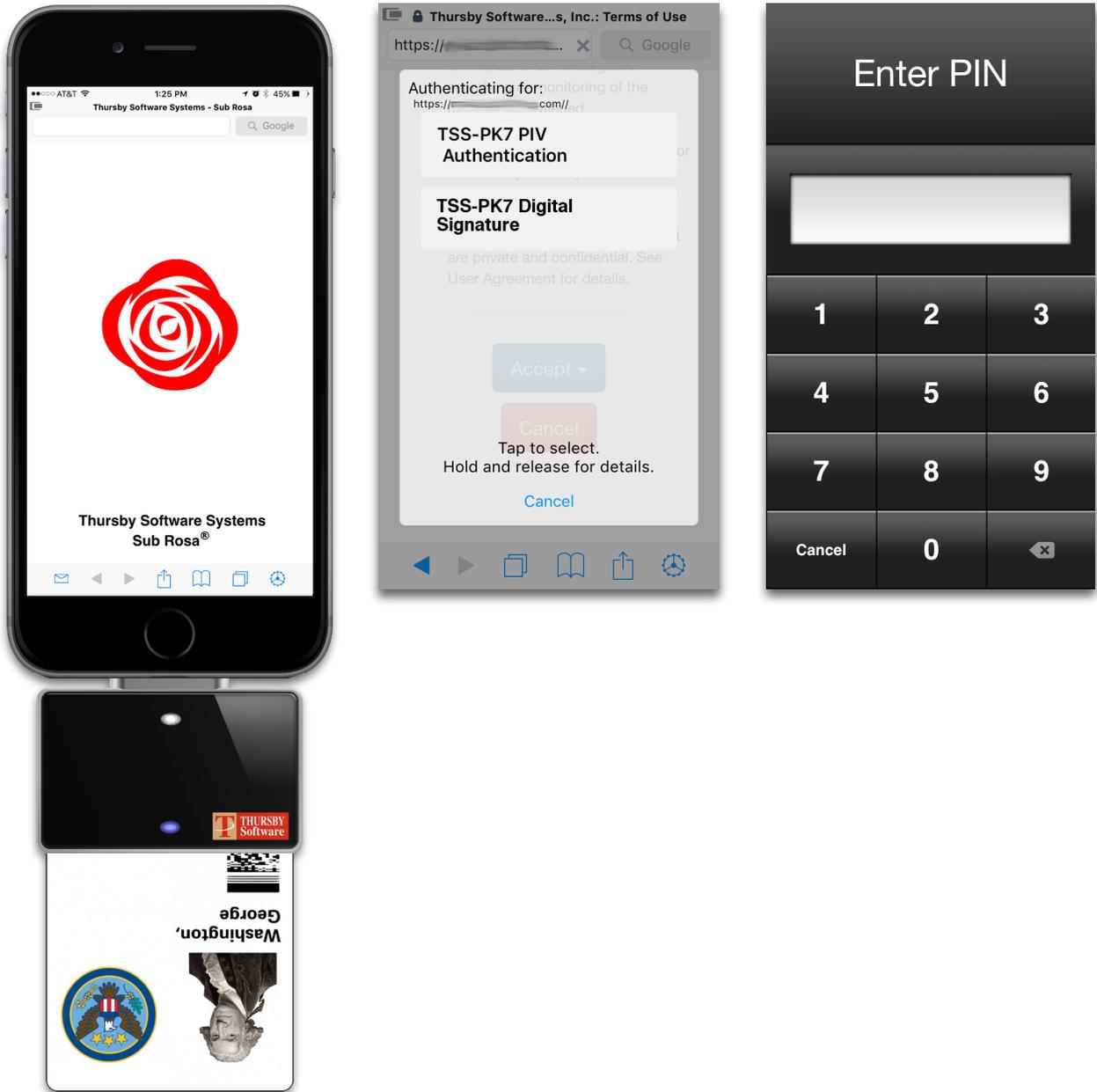
Once the application is installed, tap the icon to launch Sub Rosa Pro. You will be prompted to register, asked to select a group of bookmarks based on the branch of government with which you are associated, and notified of any new features in the app.



Using Sub Rosa Pro

To use Sub Rosa Pro, connect the reader to your device, insert your smart card into the reader, and then type in the desired URL, use one of the provided bookmarks, or use the camera icon to scan a QR code. When authentication is needed, you may be prompted to select a certificate and then enter the card's PIN number.

If you have derived credentials, or certificates you imported from Purebred, you will see them in the certificate list with the credential name to the left of the certificate.



Gestures

Sub Rosa Pro has a few gestures that you may notice by using the app. Scrolling down will cause the Address bar and Toolbar to scroll out of view. Scrolling back up will bring them back. If you do a long scroll upward, then you will see our Tabs menu appear; another long scroll upward will make it go away.

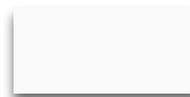
Sub Rosa Pro User Interface

Detailed below are descriptions of each button and icon you will find within the app:



1. Card Slot Status

The card slot status is a visual indicator that the hardware is functioning properly.



No icon indicates that no reader could be found.



The card reader is ready, but no card has been inserted.



The card reader is ready, and the card has finished initializing.



The card reader is ready, and the card is ready to use.



The card reader is ready, but the card is powered off.

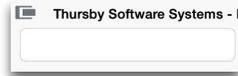


There was a problem initializing the reader.



There was a problem initializing the card, or the card is not supported.

2. Address Bar

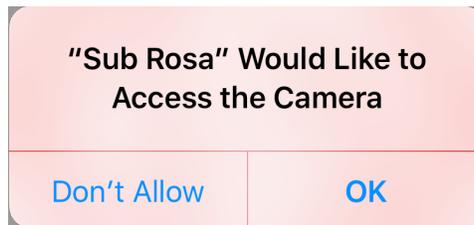
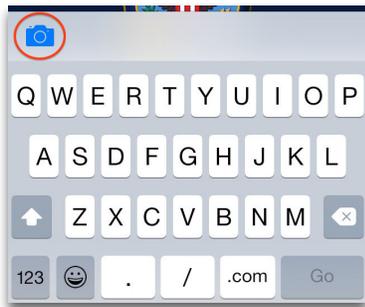


The address bar works just like any other browser's address bar. While most sites should be accessible, the only time you should run into an issue is if the site is using a very old/expired certificate, if the SSL certificate was signed by an authority not in our trust list and is inaccessible, or running a protocol that isn't supported by Apple's iOS; e.g. Flash, Java, or Active X.

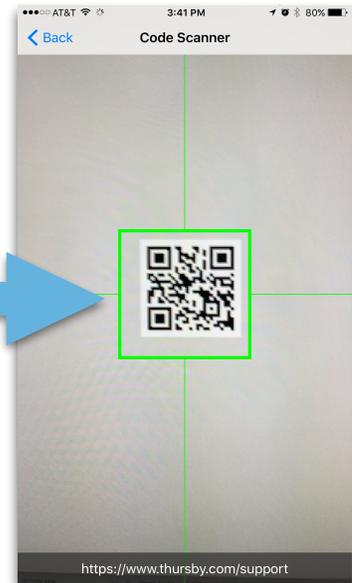
2.1 QR Code Scanner



When you tap the address bar, not only will you see the keyboard, but there will also be a camera icon just above the keyboard. This camera will open our QR scanner to allow you to scan the QR code of a URL. If this is the first time Sub Rosa Pro has accessed your camera, you will also see a prompt asking you to allow it.



Try it here!



3. Google Search

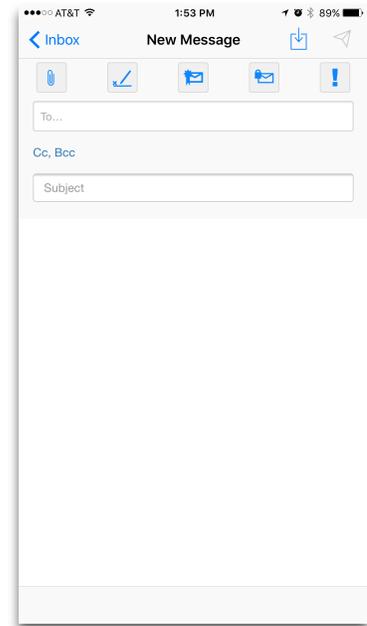
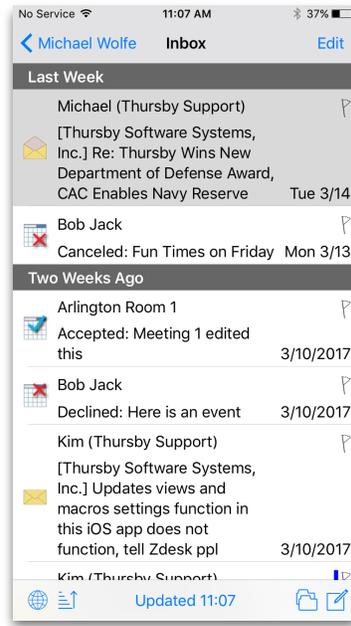
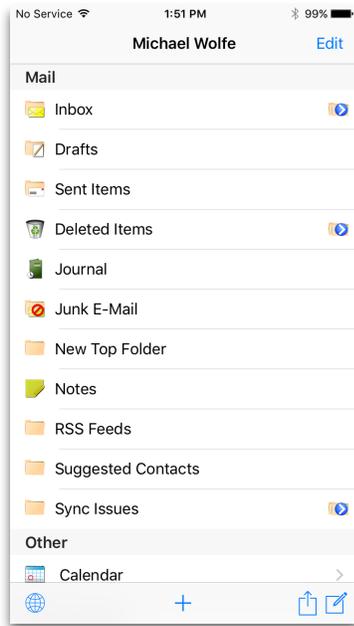


Our Google search bar provides a search box to carry out web searches, and functions much like you'd expect in any other web browser.

4. Enhanced OWA Client



With Enhanced OWA Client enabled, Sub Rosa Pro will open your webmail in a view similar to an email client with advanced features such as S/MIME. You can switch between your mailbox and the browser by tapping either the Envelope button or the Globe button. If the URL for your webmail changes, simply go to the new URL in the browser to update URL Sub Rosa Pro has cached.



Other features that are included in Enhanced OWA view is the ability to create new folders by tapping the + or deleting folders by tapping the Edit button, connecting to shared mailboxes as well as view your calendar.

4.1 OWA Mailbox

When viewing your mailbox, you will see the different folders that you can find in an email client. Once a folder is selected, Sub Rosa Pro pulls messages from the server and displays them as a list. When you get to the bottom of the list you can swipe up to prompt Sub Rosa Pro to get more messages from the server. When viewing your email, you can sort them by tapping the sort  button will allow you to sort the list with the same options you see in a browser.

Folders that contain a  icon have sub folders within them. Tapping this button will drill down into the folder structure and display additional folders that reside within the parent folder.

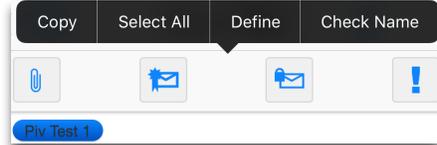
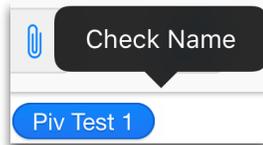
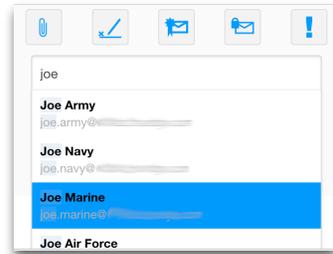
Folders with numbers next to the name indicate that there are unread messages in the folder. Tapping the on the folder name will display all emails within the folder. When viewing sub folders, you can go back to the parent folder by tapping the folders name in the upper left corner.

While you are viewing the list of emails within the folder, you can quickly view the sub folders within it by tapping Sub Folders  icon in the lower right portion of the screen.

4.2 Creating a Message



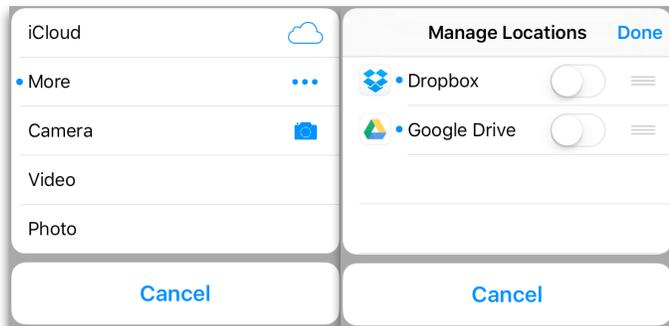
Creating a message works just like any other email client. To begin, tap the compose button. The To: field will automatically attempt to find the address you're typing in your local contacts and your Address Book stored in OWA; you may see a prompt to allow access to your contacts. To verify that the email address is in the GAL, double tap the email address or address field once it has been added, then tap "Check name". If you are in the middle of composing an email, but need to look at another, Sub Rosa will save the email as a temporary draft. To get back to this email, tap the compose button and continue where you left off. To send the email, tap the paper airplane icon in the upper right corner.



4.3 Message Attachments



To attach an item to your email, tap the paper clip button to display the different locations available to pull the attachment. If you access your photos you may see a prompt asking if Sub Rosa Pro can access your photos. Sub Rosa's Enhanced OWA Client will enable you to preview attachments, but does not allow attachments to be saved outside of the app.



4.4 S/MIME

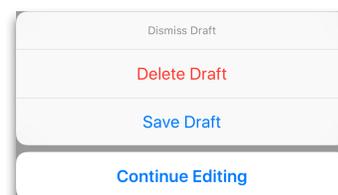


In Enhanced OWA Client, you have the ability to sign, encrypt, and decrypt email. When composing a message you will see two buttons at the top with envelopes. The one on the left is to mark that you would like to Sign the email, and the one on the right is to mark that you would like to Encrypt the email; you can select both if you wish. Any encrypted email that you open may prompt you to enter your PIN, and any email that you sign will prompt you to enter your PIN. Encrypting an email does not require your PIN.

4.5 Save

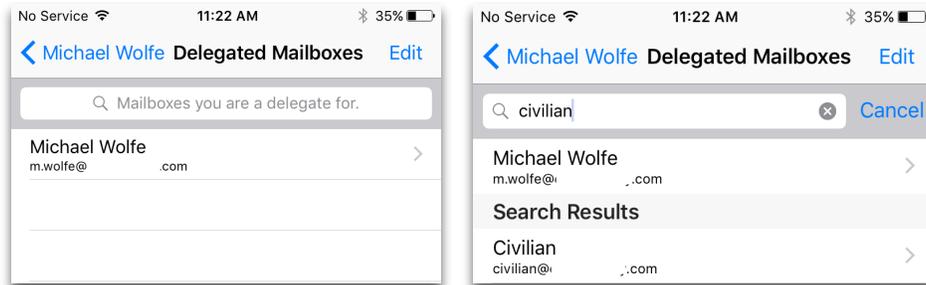


Tapping the save button prompts you to discard the draft, save the draft or continue editing.



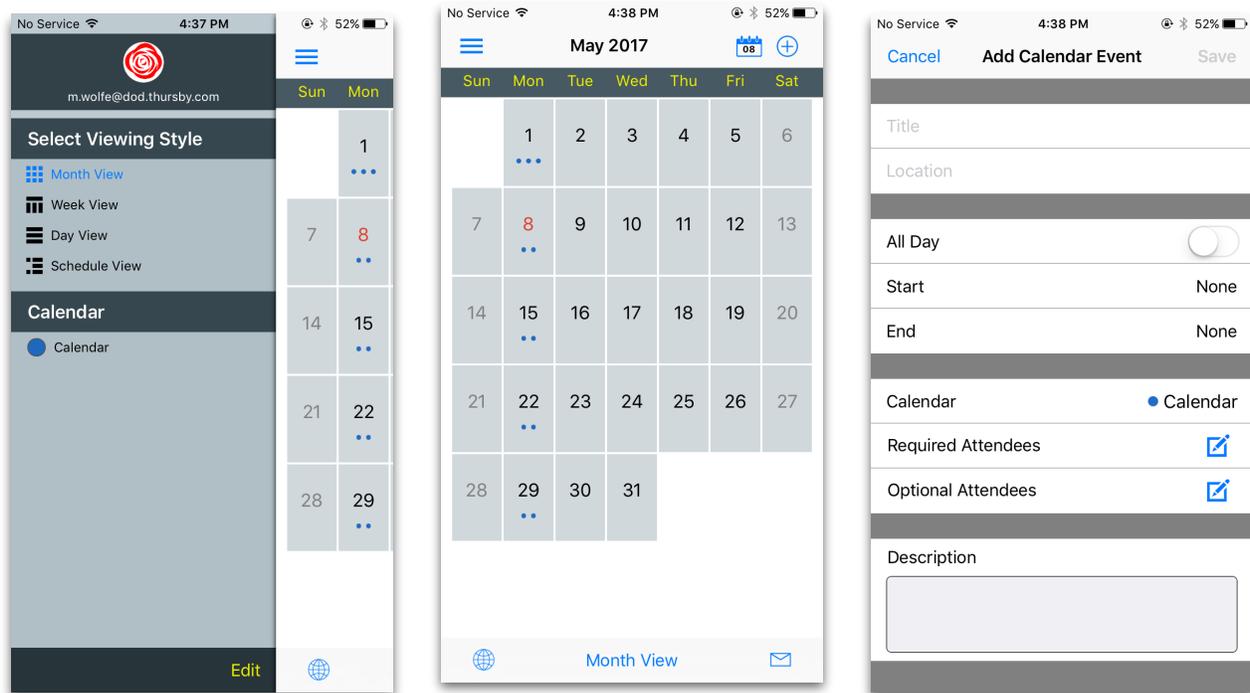
4.6 Delegated or Shared Mailboxes

To connect to your shared or delegated mailbox, tap “Delegated Mailboxes”, then enter the email address of the mailbox you can access and select it.



4.7 Calendaring

Enhanced OWA Client includes an intuitive calendar that is capable of pulling your past, and current appointments and events. The user is able to create new personal events, or new appointments with invitee’s. Like the native calendar on your phone, you have the ability to change your view to Schedule, Day, Week, or Month view. You can edit or delete the events and appointments of which you are the owner.



When you first open the calendar, the left side panel is exposed to show you the different views available, and your calendars. To dismiss the side panel, tap the hamburger menu, or swipe the panel divider bar to the left. The default view that is opened is the Month view. If you change views between sessions, the last view you used will be the one that is displayed.

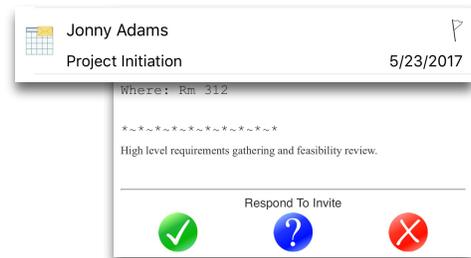
4.7a Creating And Editing A New Calendar Item

To create an event, tap the plus + in the top right corner of the app window. The “Add Calendar Event” window has the same fields you would find in most Calendar apps. When you are adding an Attendee, Sub Rosa will query the GAL for the users email address and display it for you to select. Once you have finished creating the event, tap Save. Any attendees will be emailed with the option to accept, decline, or tentatively attend the event.

You can edit any calendar items you are the creator of by going to the day of the event, tapping on the event you wish to modify, then tap the edit icon in the upper left corner. Once you have made your changes, tap Save or Send in the upper right corner.

Note: The text of the button is determined by if you have invited other people to the event. If changes are made, tapping send will email the invitees and notify them of the changes.

Emails that contain an event sent from OWA or Outlook contain buttons which allow the user to Accept, Decline, or mark that they may attend the meeting.

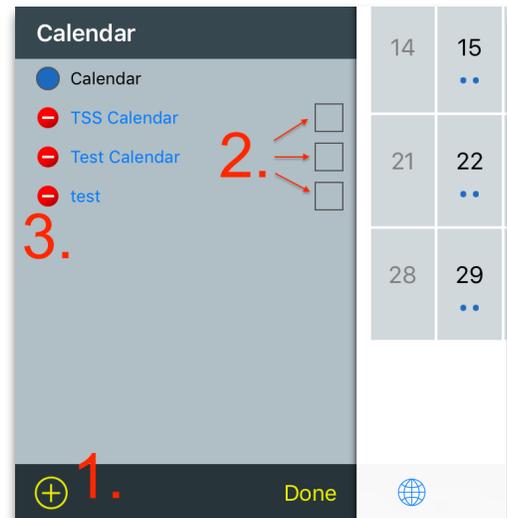


4.7b Additional Calendars

To create a new calendar, swipe open the side panel, tap the Edit button at the bottom of the panel, tap the + ¹, name your Calendar, then tap the box next to the name to place a check in it; calendars with a check will be displayed, hidden calendars do not have a check.

To hide calendars, swipe open the side pane, tap the Edit button at the bottom of the panel and remove the check ².

To delete Calendars, swipe open the side pane, tap the Edit button at the bottom of the panel, then tap the red circle ³ to the left of the calendar you wish to delete.



Click Done when you are finished editing

5. Page Navigation

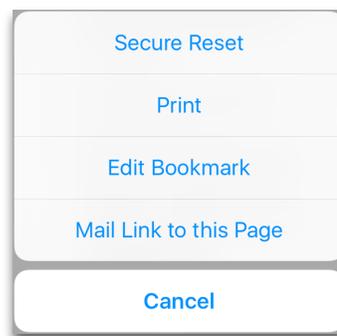


These buttons allow you to browse back and forth to pages you have previously visited.

6. Share



The Share button allows you to perform different tasks such as Secure Reset, Printing the page, adding or editing a bookmark, or send a link to the page you are on. When viewing a document like a PDF, you can use the Share button to open the document in a different app.



6.1 Secure Reset

Secure Reset will remove any browser and certificate cache, as well as close any open tabs. This is a great utility to use if you are having trouble accessing a website.

6.2 Print

The Print button allows you to print the page to any printers that are compatible with Apple AirPrint.

6.3 Add/Edit Bookmark

Add Bookmark allows you to create your own custom bookmarks based on the page you are currently visiting in Sub Rosa Pro. If the page you are on is already bookmarked, then this button will change to Edit.

6.4 Mail Link to this Page

Mail Link to this Page opens up a new email for you to send a link to the page you are visiting.

7. Bookmarks



During the setup of Sub Rosa Pro you were prompted to select the branch or branches of government and military with which you are associated. This selection allows Sub Rosa Pro to create bookmark folders and populates them with some of the most common URL's. These bookmarks are not permanent, and can be deleted or edited. This is where any custom bookmarks that you have created will be stored.

8. Tabs

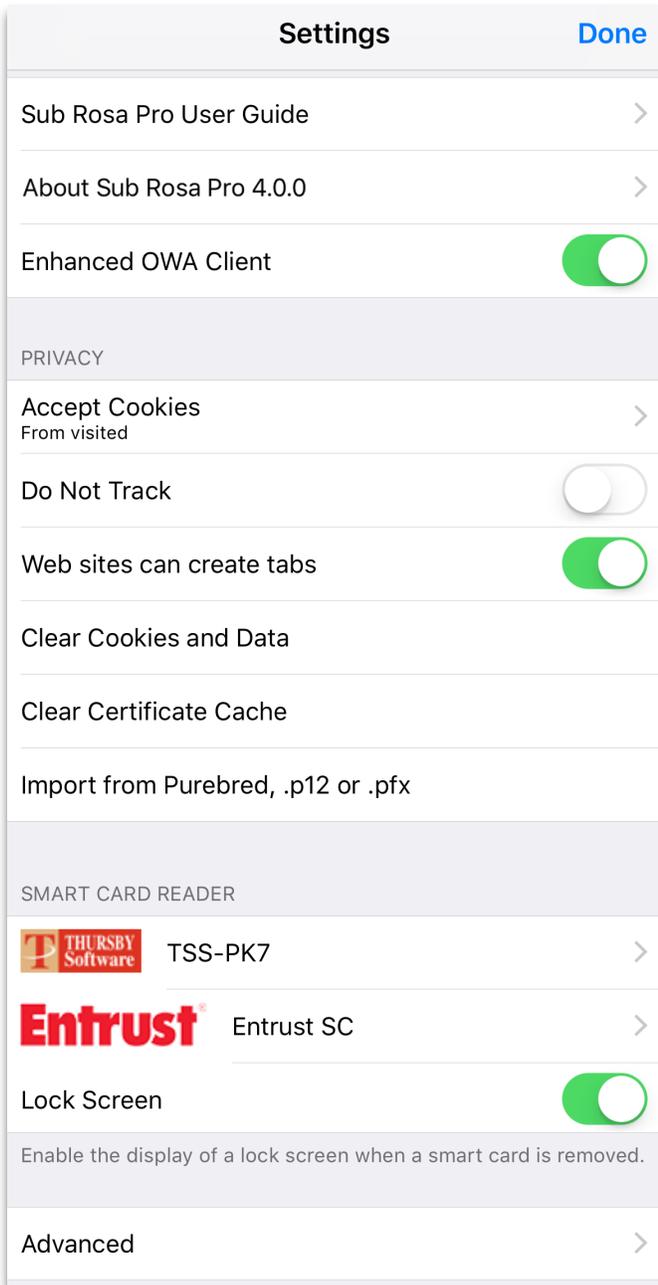


The tabs button allows you to open new tabbed windows, or access tabbed windows. The plus sign will create a new tab. To close a window, tap the tab button to display all open windows, then drag the desired window in an upward motion.



9. Settings

The Settings menu contains a variety of options that you can enable or disable.



Sub Rosa Pro User Guide opens this guide.

About displays the version and build number of Sub Rosa Pro that is installed. By tapping this button you are able to access the licensing agreement, and registration page.

Enhanced OWA Client enables or disables our Enhanced OWA Client.

Accept Cookies allows you to change how cookies are managed within the app.

Do Not Track a request will be sent to a website to not have your browsing data collected or tracked. However, what happens to your data depends on how a website responds to the request.

Allow New Tabs allows websites to open windows in a new tab. This does not affect tabs you open manually.

Clear Cookies and Data clears your current website information.

Clear Certificate Cache clears any cached certificate information.

Import from Purebred imports certificates from cloud sources such as iCloud, Google Drive and OneDrive.

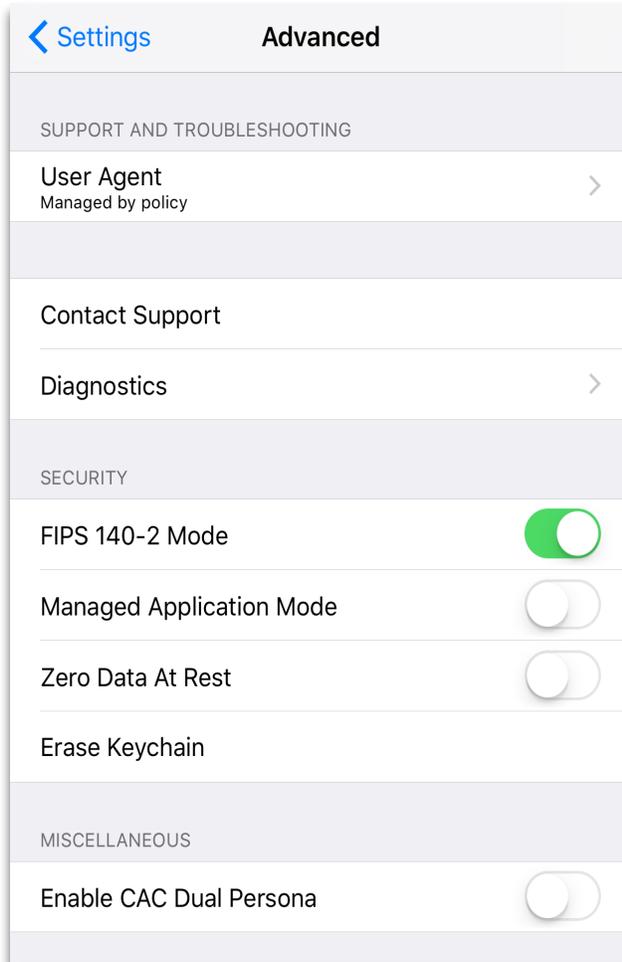
Tapping the reader icon displays basic information about the connected reader and your certificates.

Lock Screen enables or disables the Thursby lock screen when you exit the app or remove your card.

Advanced will allow you to change additional options within Sub Rosa Pro, and contact Thursby Support.

9.1 Advanced

The advanced section of our Settings menu allows you to change additional settings within the app, as well as enabling and sending diagnostic data to Thursby Support.



User Agent This allows Sub Rosa Pro to change the user agent it sends to websites. Changing the user agent allows our browser to emulate other web browsers and bypass some browser restrictions.

Contact Support will open your email and allow you to send an email to Thursby Support.

Diagnostics allows you to start diagnostic logging and then send the log file to Thursby Support.

FIPS 140-2 Mode forces FIPS140-2 level of encryption when connecting to web servers. Sub Rosa Pro will fail to connect if the server does not meet this specification.

Managed Application Mode is a Sub Rosa Pro feature that allows you to manage the apps settings. Please contact Thursby Support for more regarding management policies.

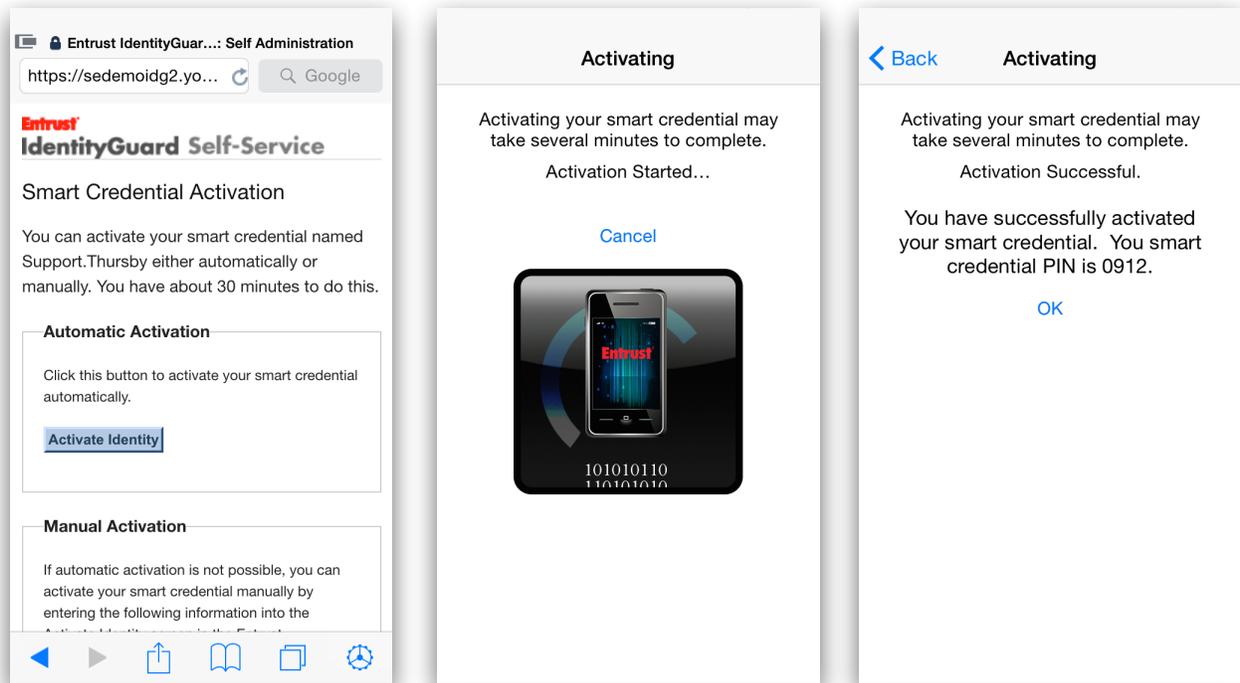
Zero Data At Rest configures Sub Rosa Pro to not store any information on the device.

Erase Keychain clears the internal Keychain that stores Purebred and other imported credentials.

Enable CAC Dual Persona enables or disables PIV on CAC certificates from being displayed.

Activating Entrust IdentityGuard Derived Credential

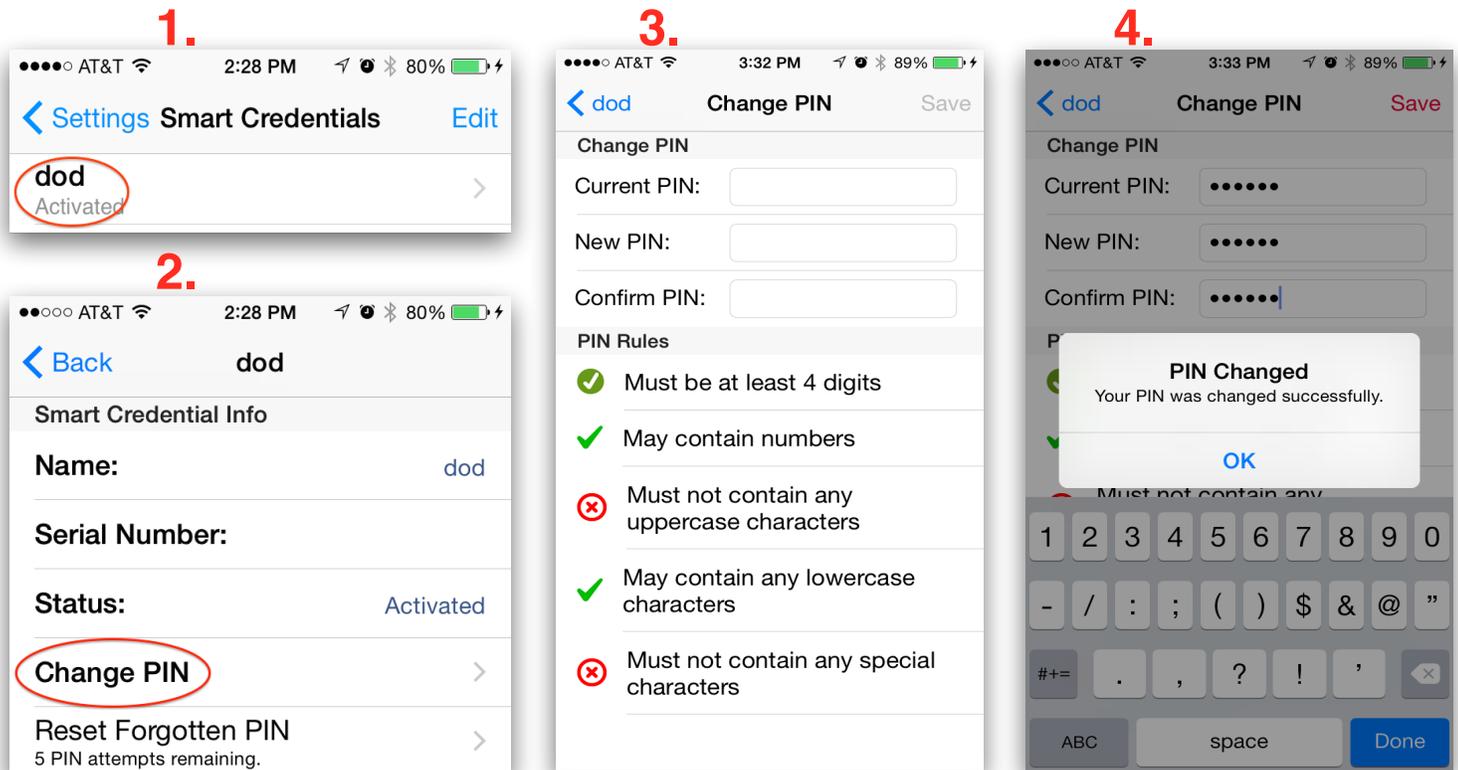
Before adding an Entrust derived credential to Sub Rosa Pro, you need to receive instructions for using the Entrust self service web site. **You must access this web site using Sub Rosa Pro.** Once you are logged into the web site, follow the instructions for provisioning your credential. After following the instructions you should see a web page, that looks similar to the images on the next page:



Click the Activate Identity button. Sub Rosa Pro will activate the credential and display your initial PIN.

Changing Your Entrust PIN

To change the PIN number that was assigned to your derived credential, tap the gear icon within Sub Rosa Pro, tap Entrust, then tap your credential ¹. In this menu, tap the change PIN button ², you will be prompted to enter the previous PIN, then the new PIN ³, then tap save. Your PIN must be at least 4 digits, may contain numbers or lowercase characters, and may not include special characters. When completed a dialog will appear stating that your PIN was changed successfully ⁴.

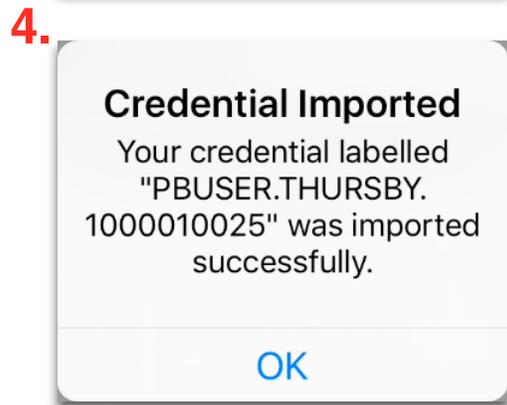
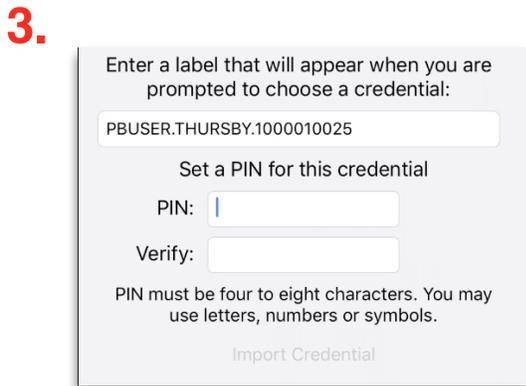
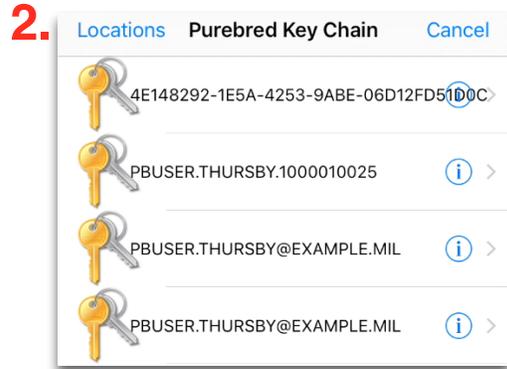
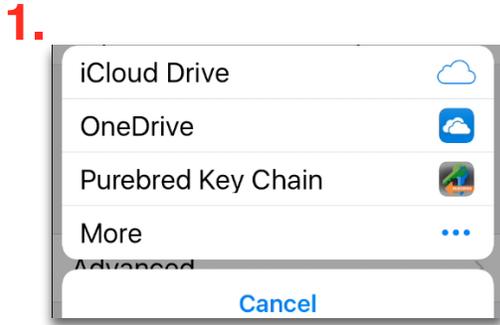


Importing Purebred Credentials

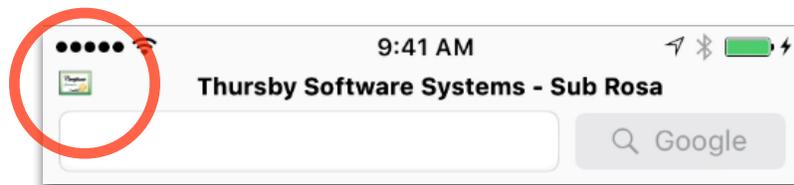
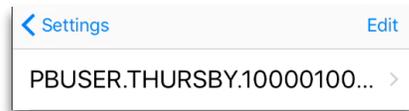
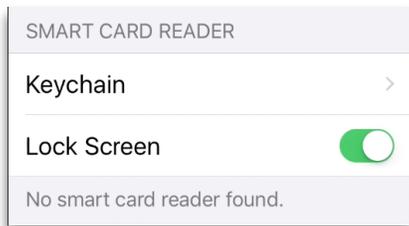
Note: This guide assumes your device has been provisioned with the Purebred app, and you have purebred credentials available to be imported.

To import Purebred credentials, open Sub Rosa Pro's Settings and tap import from purebred. You will be prompted to select a location to import the credential from; choose Purebred Key Chain ¹. You should now see a list of credentials in the Purebred Key Chain ². Select the credential you wish to import into Sub Rosa, enter a label to help you distinguish the credential from any other credential you might have, such as a smart card, and a PIN ³. You should then see a dialog box that the credential import was successful ⁴.

Note: The credential's private key is only stored in the Apple iOS Keychain, and is not stored inside the Sub Rosa sandbox



Once the credentials have been imported, you will now see “Smart Card Reader” in Sub Rosa’s settings. Tapping Keychain will view its credentials and you can see your credentials. Tapping on the certificate will allow you to view the certificate details and email it if needed. Once the credentials have been loaded, you will also see an new card slot status icon, indicating a purebred credential is available.



Troubleshooting

- When you connect the reader to your device, a white light should appear. If Sub Rosa Pro is opened, then the white light should stay solid. If the app is in the background, or if the device is locked, then the white light should slowly pulse until it is put to sleep. If this light appears, and doesn't stay on, open your devices Settings, tap General, tap About, and scroll to the bottom. You should see PKard Reader below SEID when the reader is connected. If you do not see PKard Reader, disconnect the reader, restart your device, and try again. If you continue to have an issue, please contact support.
- Inserting your card into the reader will activate a blue light at the bottom of the reader. When the card is idle, it will be a solid blue light. Anytime card data is being read the blue light will flicker on and off.
- Sub Rosa Pro is a mobile web browser and requires your device to be connected to the internet via cellular or WiFi. If you are unsure that your device is connected to the internet, open Safari and try going to www.thursby.com. If you are able to see this website, try logging into a CAC enabled web site with Sub Rosa Pro.
- If you have chosen the wrong certificate, tap share button, then tap Secure Reset. This will clear all certificate choices that we save as "Identity Preferences".
- Incorrectly entering your PIN number too many times will lock your CAC. If you see a notice that your CAC is locked then you will need to go to your nearest CAC office in order to get your CAC unlocked.
- You may see the error "Unable to establish a secure connection to the server" when attempting to log into a website. If after several attempts you still get this message, close the app by tapping your home button twice, and swipe the app off of the screen. Once the app is closed, open Sub Rosa, and try the website again.
- If a website is loading incorrectly, or is failing to log you in, closing the app, or using Secure Reset will remove any cached data from the browser and should correct the problem you are having. Either one of these actions will fix a majority of problems you may see or experience when using the application.
- "I am unable to send an encrypted email". Sending an encrypted email requires the recipients signing certificate to be available. If the recipient is in the GAL, the Sub Rosa should be able to look up this certificate. If the recipient has sent you a signed email, and you've opened it within Sub Rosa, or are replying to the email, then Sub Rosa should be able to use the cert. If you continue to have trouble sending an encrypted email, try sending an encrypted email using OWA on a Windows computer with Internet Explorer.
- "When should I be prompted to type in my PIN?" You will be required to enter your PIN number the first time your need to log into a website. This PIN entry will unlock

the card and you won't see another authenticate PIN prompt until the card has left the reader and returned. This action happens if you physically remove the card or card reader, if you force close the app, or if you use Secure Reset. You will also see a PIN prompt **every time** you sign an email. You will not, however, see a PIN prompt if you **only** encrypt an email, this action does not require a PIN. Decrypting an email will always prompt you to enter your PIN number.

Requirements

- Apple iPhone or iPad running iOS 8.4.1 or later
- Enhanced OWA Client supports Exchange 2010
- CAC, CIV, PIV, and PIV-I cards
- Thursby Software Systems, Inc. PKard® Reader hardware.
(Note: FIPS 140-2 encryption is not compatible with jailbroken devices)

Further Information and Support

- **Web** <http://thursby.com>
- **Forum** <http://thursby.com/forum>
- **Email** Thursby Software Systems, Inc.
 - sales@thursby.com or support@thursby.com
- **Phone** +1 (817) 478-5070