THURSBY Software

Software Product Description

Sub Rosa® v5.0 for iOS

FIPS 140-2 CAC, and PIV enabled browser and e-mail app for iPad, iPhone, and iPod

OVERVIEW

Sub Rosa for iOS is the solution for secure web browsing and two-factor authentication on a mobile device. Our Enhanced OWA Client provides a feature filled calendar and mail viewer with the added ability to sign, encrypt, and decrypt messages in a user friendly format.

SYSTEM REQUIREMENTS

- iOS 11.0 and above
- Thursby Card reader Hardware

FEATURES

Enhanced OWA Client

- Connect with Microsoft Exchange 2010, Exchange 2013, and Office 365 OWA
- Uses two factor authentication to log into the mail server
- All mail features use a familiar native iOS user interface
- Users can read and send both signed and encrypted e-mail
- Sub Rosa integrates with Global Address List (GAL) to locate recipient information and encryption certs
- Users can add attachments using their camera (both still or video) and can send files from other applications
- For security purposes, no e-mail data or attachments can be saved or delivered to other applications
- Users may sort messages using different methods
- Conversation mode is supported
- The user's iOS contacts can be used to look up e-mail recipients
- Sub Rosa properly handles saving encryption certificates from digitally signed e-mail messages and can use them to send encrypted mail to the original sender
- Users may search for mail in folders, subfolders, or the entire mailbox
- Search results are highlighted in messages that are found
- **Viewing messages**
  - Sub Rosa displays both HTML and plain text messages and can display most attachments including Microsoft Office, PDF, and graphics files
  - Users may respond to messages using reply, reply-all, forward, and forward as attachment
- **Composing messages**
  - Users may add recipients, can look up recipients in their device contacts, or in the global address list
  - Sub Rosa properly handles delivering encrypted e-mail to blind copy recipients making sure their identity is not disclosed to other recipients
  - The user's e-mail signature can be added to messages depending on their Outlook or OWA configuration
  - Messages are automatically saved as drafts allowing the user to read other messages and then continue composing a message
  - Drafts are saved on the mail server if it is available
- **Calendaring**
  - View events in month, week, day, and schedule view
  - Enable multiple calendars and assign color identifier
  - Create and manage appointments
  - Schedule meetings with invitees
  - Respond to meeting invitations
  - Edit events and notify attendees
  - Cancel meetings and delete appointments

Smart Cards and Readers

- Sub Rosa integrates with Thursby's FIPS 201 validated smart card readers providing ready to use support for CAC and PIV cards, as well as Alt-Tokens
- Sub Rosa can recognize and use Dual Persona CACs
- Support for PIV key history is included so that old e-mail can be decrypted with older keys stored in the PIV key history
- Precise Biometric's Tactivo, and Identiv iAuthenticate readers are also supported

Web Browser

- HTML 5 and Javascript support
- Display web sites from http and https URLs
- Full tabbed browsing
- Bookmarks are supported including many pre-populated bookmarks for US government and military sites
- Leverages smart cards for client authentication, handling PIN entry as needed
- Includes a database of many military sites and can choose the correct CAC certificate for authentication
- Users may change the default home page, User Agent, and cookie storage policy
- Users can print web pages and can preview, print, and export many document types from web sites including PDF and Microsoft Office documents
- QR code scanning is included using the iPhone or iPad camera

Security Features

- Sub Rosa includes FIPS 140-2 validated cryptography
- A zero-data-at-rest mode can be turned on preventing any user data from being written to their device persistent storage or exported to other applications
- A secure reset feature is provided to wipe all user data from memory and terminate all network connections
- A screen lock feature is provided to lock the application screen when a smart card is removed from the card reader
- A Do Not Track setting is provided
- Symmetric Key wrapping
- Symmetric Encrypt/Decrypt
- Public Key Infrastructure and Enablement* (see details below)

Secure Networking

- TLSv1.0, v1.1, v1.2 (no SSLv3)
- Client certificate authentication

Toolkit

- Manage connections from multiple concurrent client applications
- Provide notifications of CCID reader state change
- Provide notifications of token state change
- Perform cryptographic operations for client applications
- Serve objects from supported tokens to client applications (printed info, certificates, facial image)

Third Party and Partner App Integration

- Apps built with the PKard Toolkit can use Sub Rosa as the Authenticating Agent

*Public Key Infrastructure and Enablement

Sub Rosa provides its own certificate trust policy independent of the iOS operating system. The underlying OS does not allow the user to determine what their roots of trust are, causing many foreign government controlled root Certificate Authorities (CA) to be trusted. Sub Rosa eliminates this risk by only trusting US government roots that are part of the FCBA, and google.com's intermediate CAs. Sub Rosa's trust policy also prevents the possibility of spoofing e-mail digital signatures that can occur in Apple's Mail application if root CAs are controlled by foreign governments While Sub Rosa's trust policy is intentionally restricted, Thursby Support can provide customizations that are digitally signed by Thursby and can be installed in the field.

Thursby Software System, LLC
4901 South Collins Street
Arlington, Texas 76018 USA

www.thursby.com
sales@thursby.com
+1 (817) 478-5070

24 May 2019