



Software Product Description

PKard® for Good Technology v2.2

FIPS 140-2 CAC, PIV, and Derived Credential enabled browser app for iPad, iPhone, and iPod

OVERVIEW

The PKard for Good Technology secure browsing app allows users to securely access web-based email, portals and collaboration sites using strong two-factor authentication. Used in conjunction with the Good Secure Mobility Platform by BlackBerry®, PKard for Good allows you to view Microsoft Exchange email in a user friendly format and allows you to sign, encrypt, and decrypt email. It includes built-in support for Good Technology MDM so that organizations may use Good configuration policy for scalable deployment and security.

SYSTEM REQUIREMENTS

- iOS 8.4 through 10.1
- Good Mobile Messaging Server 8.3.1.4
- Good Proxy Server v2.3.53.69
- Good Control Server v2.3.53.62

FEATURES

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 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

Smart Cards

- PKard for Good integrates with Thursby's FIPS 201 validated smart card readers providing ready to use support for CAC and PIV cards
- PKard for Good 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
- Tactivo smart card readers are also supported

Derived Credentials

- PKard for Good supports Authentication using Entrust Derived Credentials

Secure Networking

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

Security Features

- PKard for Good includes FIPS 140-2 validated cryptography
- Conforms to Good's Data Leakage Policy
- A zero data at rest mode can be enabled to prevent user data from being written to persistent storage or exported to other applications
- Certificate trust policy to verify peer without implying trust of all certificates from a given CA
- 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
- Users may control how cookies are stored
- A Do Not Track setting is provided
- Symmetric Key wrapping
- Symmetric Encrypt/Decrypt
- Public Key Infrastructure and Enablement*

Managed Deployment

- Administrators can performed managed deployment through the use of pkardmanagement Policy Files
- New policies can be merged with existing policies
- Restrictions can be enforced per policy.

Good MDM Support

- Respond to GD Public Key Infrastructure Service 1.0.0.0 requests for S/MIME
- Good Dynamics managed app

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 PKard for Good as the Authenticating Agent

*Public Key Infrastructure and Enablement

PKard for Good 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 CAs to be trusted. PKard for Good eliminates this risk by only trusting US government roots that are part of the FCBA, and google.com's intermediate CAs. PKard for Good'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 PKard for Good'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 Systems, Inc.
4901 South Collins Street
Arlington, Texas 76018 USA

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

PKard is a registered trademark of Thursby Software Systems, Inc.
Sub Rosa is a trademark of Thursby Software Systems, Inc.
iPad, iPhone, and iPod are registered trademarks of Apple, Inc.
All other trademarks are the property of their respective owners.