Smart Card Authentication

Secure CAC/PIV Mobile File Management

Acronis mobilEcho® for iOS meets the needs of US DoD, Federal, State and Local governments and corporate iPhone and iPad users for simple and straightforward two-factor authenticated CAC, PIV, PIV-I and CIV smart card access to files.

mobilEcho empowers employees who choose iPhones & iPads with secure, managed access to documents stored on enterprise storage including file servers, NAS such as NetApp, EMC or Isilon and SharePoint sites with built in editing for Microsoft Office files including Microsoft Word, Excel and PowerPoint. mobilEcho supports the common use of searching for a document on a server, opening and editing that document and saving the edited version back to the server, all from an iPhone or iPad.

Authenticate to access files on:

- Windows and any file servers accessible by SMB/CIFS
- Microsoft SharePoint sites, including Office 365 hosted sites
- Network Attached Storage (NAS) such as NetApp, Isilon, EMC and Western Digital

Thursby Inside

The Secure CAC/PIV technology is licensed from Thursby Software, Inc. The smart card technology is the same code used by the Pentagon, Army, Navy, White House, NIH and SEC across tens of thousands of Mac users since the mid 2000s.

Smart Card Reader Support

mobilEcho supports a variety of smart card readers including:

- Thursby
- Indentive iAuthenticate
- Precise Biometrics

Reader hardware and card are not included.

Protecting the App

When mobilEcho's primary authentication is configured to use Smart Cards, the mobilEcho app will require that the user's Smart Card is inserted into the reader before the user can use the app. The user will see a lock screen asking them to insert their card if they start the app without the card inserted. If the user is in the app with their card inserted and they remove the card, the app will immediately lock.

Protecting the Servers

The credentials on the Smart Card are also used to authenticate with servers. The mobilEcho client app establishes a session with the mobilEcho server when a user authenticates. This session has a 15 minute idle timeout by default, but is configurable on a server-wise basis. If a user is doing username/password authentication, they would be prompted to enter their password again the next time they try to access a network resource, assuming their 15 minute idle time had elapsed. If using certificates or Smart Cards, the client app just re-authenticates as needed, since the certificate is stored within the app or the Smart Card is inserted and ready to be used for re-authentication. The need to enter a PIN to unlock the card is dictated by the card's configuration and all of that process is handled by the Thursby PKard app.

Highlights:

- Securely access files on Windows and any file servers accessible by SMB/CIFS, Microsoft SharePoint sites including Office 365 and Network Attached Storage (NAS) such as NetApp, Isilon, EMC and Western Digital.
- Fully managed client providing Active Directory-group based policies for nearly every setting in the mobilEcho app.
- Built in Office document editor for Microsoft Office .doc & .docx, Microsoft Excel .xls & .xlsx and Microsoft Powerpoint .ppt & .pptx
- Built in PDF viewing and annotation.
- Fully supported commercial software with a multi-year history and tens of thousands of users.
- CAC (Common Access Card), PIV (Personal Identity Verification), PIV-I, CIV (Commercial Identity Verification) and Dual Persona cards via Thursby's proven PKard technology.
- Avoids clumsy, inconvenient and incomplete workarounds such as virtualized Windows, boot camp or thumb drives.

Requirements:

- mobilEcho iOS app, version 4.5.2 or later
- Thursby PKard Reader app, version 2.0.3 or later
- iOS 6 or iOS 7

For additional information please visit http://www.acronis.com/mobilecho
or contact us at sales@grouplogic.com

To purchase Acronis products, visit www.acronis.com or search online for an authorized reseller.
Acronis office details can be found at http://www.acronis.com/company/worldwide.html