Tx Systems
iOS-CAC Documentation

Full Mobile CAC Authentication Solution / Proof of work

Christian Houser
iOS Technical Specialist
Mobile: +1 (858) 622-2015
Christian@txsystems.com

1.0 Introduction

1.0.1 About iOS-CAC

iOS-CAC (Common Access Card) authentication allows military personnel and contractors to securely access Department of Defense (DoD) websites and applications on iOS devices, such as iPhones and iPads. This authentication is required for secure access to critical services, including email, personnel systems, and other DoD resources, which mandate the use of CAC for identity verification. By configuring iOS devices with the correct certificates, users can seamlessly authenticate to these systems using their CAC cards.

1.0.2 Purpose

This guide outlines the steps for configuring iOS devices to enable CAC authentication. Proper configuration ensures that military and DoD contractors can securely access DoD websites and other protected services, which often contain sensitive information requiring CAC-based authentication.

1.0.3 Prerequisites

- iPhone running iOS 16 later or iPad running iOS 16.1 or later
- A compatible USB-C Smart Card Reader (e.g., Identiv or similar reader)
- A valid DoD-issued CAC
- A .mobileconfig file with the correct DoD certificates found at
- Network connection to access DoD websites

2.0 Installation Steps

Step 1: Obtain and Download DoD Certificates

- Ensure you have the necessary DoD certificates for authentication. These can be packaged in a .mobileconfig file for ease of installation.
- Download the .mobileconfig file containing DoD certificates from a secure source (e.g., official website or company-provided link).

Step 2: Install the Certificates

- Tap the button “Download Certificates” to download the file named “Certificates for CAC Authentication”
- You will be prompted with a message stating, “This website is trying to download a configuration profile. Do you want to allow this?” **Select Allow**
- The profile will then be downloaded. Now navigate to the settings app on your device.
- Find and click the tab named “Profile Downloaded”. **Select Install**
- A secondary tab will open telling you that you must manually trust the “DoD Root CA’s” **Select Install, then Install Profile**
- Search “Trusted Certificates” in the settings search bar. Or navigate from General - About - Trusted Certificates. Now tap each DoD Root CA to enable full trust on these certificates.
- You are now ready to authenticate.

Step 3: Connect Your Smart Card Reader

- Plug in your USB-C CAC Smart Card Reader to your iOS device
- Insert your CAC into the reader.

Step 4: Test the CAC Authentication

- Navigate to a DoD website that requires CAC authentication, such as https://web.mail.mil.
- When prompted, select your CAC certificate and enter your PIN.
- You are now able to access DoD websites on your iOS Mobile Device

You should now be authenticated and have access to the DoD services.

3.0 Troubleshooting

Common issues:

- **Reader not detected**: Ensure the card is fully inserted and your reader is also fully inserted
- **Authentication failed**: Verify that the correct certificate profile has been installed, and the card reader is supported by iOS.
- **Enable Full Trust Certificates**: Ensure that the “DoD Root CA’s” are fully trusted by navigating to the Settings App and Enabling Full Trust under the Trusted Certificates Tab. General - About - Trusted Certificates.

3.0.1 Conclusion

Access to DoD websites and systems, such as email and personnel portals, requires enhanced security due to the sensitive nature of the information. CAC authentication ensures that only authorized users can access these resources, preventing unauthorized access and protecting classified or sensitive data. By following these steps and using a CAC card and a smart card reader, iOS users can securely authenticate themselves in compliance with DoD regulations.