UNCLASSIFIED

DoD Mobility Classified Capability - Secret 2.0.5

CAPABILITIES

- Provides SECRET (DMCC-S) mobile access to select DoD voice and data networks capabilities.
- Replaces the Secure Mobile Environment Portable Electronic Device (SME PED) and DMCC-S 1.0 supported mobile devices.
- Provides enhanced graphics and email experience through the new Integrated Commercial Solution (ICS) device.

PERFORMANCE

- Provides minimum acceptable voice quality when devices access 4G wireless networks with robust signal strength with a mean opinion score (MOS) of 2.0 or greater.
- Supports Voice over Internet Protocol (VoIP) communications with a one-way, mouth-to-ear latency of less than 900ms.
- Delivers VoIP communications with minimum packet error rates (less than 1%) and no audio dropouts in normal operations.
- Enables network communications with minimal latency and a round-trip time (RTT) of less than 400ms for any application via cellular networks.

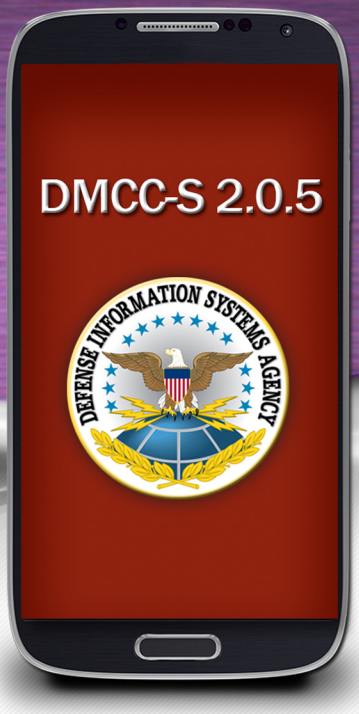
BENEFITS

- Available for DoD and Federal customers.
- New contract awarded to support new customer requests.
- Includes the use of commercial mobile devices (smart phones and hotspot devices) and commercial mobile architecture components (commercial VoIP, KNOX, and VPN applications).
- Managed by an enterprise Secret-Mobile Device Management (MDM) capability.
- Permits continuous monitoring and data auditing support.
- A National Security Agency (NSA)-approved smart phone.
- Secure Continental United States (CONUS) wireless carrier service via Verizon.
- Secure phone calls to DMCC, Defense Red Switch Network (DRSN), Enterprise Classified VoIP (ECVoIP), Voice-over Secure IP (VoSIP), and Secure Communictions Interoperability Protocol (SCIP) devices.
- Access to both DoD Enterprise Email (DEE) and non-DEE email via the Outlook Web Access webmail service.
- Two mobility gateways serve as multi-carrier entry points (MCEPs) that secure the device before features are used.

DMCC contact for inquiries and ordering information:
disa.meade.ie.mbx.secure-mobility-implementation-team@mail.mil • 301-225-8700

DoD Mobility Classified Capability - Secret 2.0.5

Quick Start Guide



1. DEVICE START UP

- Power on the device (depress power button on right side of device)
- Enter device encryption passcode if prompted
- Enter device unlock passcode
- Accept USG-IS User Agreement
- Press Home key to close Quark Security Shield

2. VERIFY VPN IS CONNECTED

- Open VPN Selector application
- Confirm connection to 2.0.5 Primary VPN (2.0.5 Wi-Fi Primary if OCONUS)
- A key symbol in the top status bar will verify VPN has connected

3. VERIFY OUTLOOK WEB APP (OWA) IS CONNECTED

- Open Internet browser application
- Click the "Proceed Anyway" button at the "Failed to Check Revocation" warning
- Proceed through Security Certification Notice
- Choose certificate containing end-user's name, select allow
- Verify Outlook Web App (OWA) is connected

4. VERIFY CELLCRYPT CALL FUNCTIONALITY

- Open Cellcrypt application
- Swipe upwards to open the numeric keypad
- Enter desired secure phone number
- Press green phone icon to place call

5. IMPORTANT NOTES

- The end-user's PIN will be mailed to their Defense Enterprise Email (DEE) email address

Coming Soon:

- DMCC-Top Secret (TS) Voice
- Firmware Over the Air (FOTA) updates
- Data at Rest (DAR) Applications

DISA

DEFENSE INFORMATION SYSTEMS AGENCY
DoD Mobility Program Management Office

For more assistance please contact your local Level 1 Service Desk or the Enterprise Services Desk:
COMM: 844-347-2457, OPTION 1>5>1 or DSN: 850-0032, 1>5>1