EXECUTIVE OVERVIEW

MOBILITY SOLUTIONS FOR CLASSIFIED NETWORKS

ARUBA CNSA CRYPTOGRAPHY

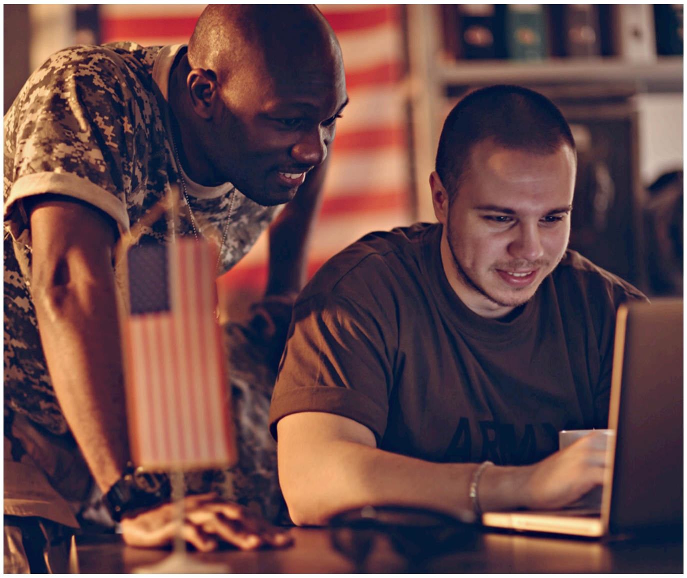
Government agencies are experiencing tremendous pressure to support commercial mobile devices – smartphones, tablets and laptops. At the same time, the most important applications used by various agencies reside on tactically secret networks, such as the U.S. Department of Defense SIPRNET, resulting in increased importance and usage of classified networks.

However, these organizations do not provide classified network access to all possible authorized users. The issue is typically attributed to the cost of installing certified connections for classified networks. The expense and usability challenges of using government-specific proprietary crypto systems (e.g. the US TYPE-1 system) and reports of poor performing SIPRNET connections are also issues.

Aruba, a Hewlett Packard Enterprise company, through the NSA Commercial Solutions for Classified (CSfC) program, has developed an alternative access architecture for classified network connectivity, which is approved for use through a standard government accreditation process. This alternative architecture makes use of CNSA cryptography, and is intended to be easier to deploy and manage. It will also offer better operational performance and work over multiple access methods, including wired, wireless and remote access.

This new architecture utilizing NSA-approved CNSA cryptography delivers a variety of strategic benefits to every government agency, including:

- **Enabling technology for new mission profiles:** Eliminates the challenges associated with Controlled Cryptographic Items (CCIs) to transform how the government uses mobility oriented communications.
- **Support for all access modes:** Simplifies the network design and increases overall security by adding access control and user firewalling to both classified WLAN users and classified wired users.



REQUIRED CNSA PROTOCOLS AND METHODS

- SHA-384 secure hash algorithms
- Elliptical Curve Digital Signature Algorithm certificates/signatures (ECDSA 384)
- Elliptical Curve Diffie-Hellman for key exchange (ECDH 384)
- AES-256 using the AES-GCM mode

- **Multiple services on the same WLAN:** Both unclassified and classified access available in different or the same coverage areas using a single Wi-Fi network infrastructure. Separation of user traffic according to NSA-approved guidelines ensures classified and unclassified traffic is not co-mingled – without the need for cross-domain solutions.
- **Support for both local and remote users:** Rapidly deploy secure access locally (using WLAN) and remotely (using remote wired or wireless) using a single network architecture.
- **High performance:** Up to 40 Gbps of AES-256 encrypted traffic throughput per 7280 Mobility Controller.
- **Increased user adoption and satisfaction:** Higher performance and longer battery life for mobile devices provides users greater flexibility to contribute to their agency missions.
- **Lower acquisition and operational cost advantage of a commercial solution** over a GOTS or proprietary solution.

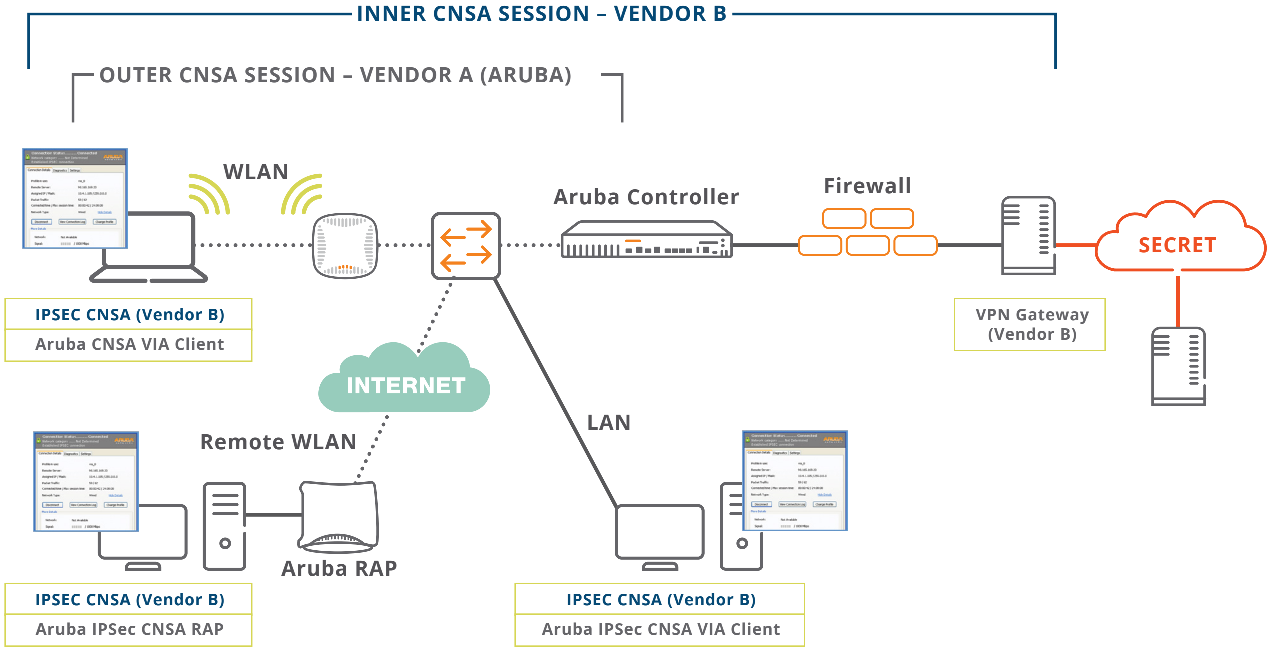
The Aruba Classified Mobility product family.

Aruba Mobility Solutions for Classified Networks provide government IT organizations the technology they need to embrace mobility in a meaningful way. It does so by securely unifying disparate computing infrastructures into one seamless network access solution – for government employees, contractors, visitors, and military personnel in-garrison or in-deployment.

For the first time, government agencies that handle sensitive but unclassified, confidential and classified information can benefit from the lower purchase costs, lower operational costs and faster pace of innovation available through commercial off-the-shelf (COTS) solutions.

ADVANTAGES OF THE ARUBA CLASSIFIED MOBILITY SOLUTION

- Enables the use of commercial mobile devices in classified environments as well as same device access over 3G/4G carriers for classified activities.
- Secure access to multiple services, both unclassified and classified, over the same WLAN infrastructure.
- A high-performance WLAN that supports mobility and operates without physical hardened network connections enables secure access for larger user populations.
- 10% of the purchase cost of a Type 1-ceritified solution and less costly to operate.
- Future-proof new unclassified networks with classified-capable solutions in anticipation of elevating them to classified status at a later date.



Example Classified Access Architecture with Aruba CNSA Cryptography.