
WHITE PAPER

CLASSIFIED NETWORKING SOLUTIONS

POLICY-COMPLIANT COMMERCIAL MOBILITY
TECHNOLOGY WITH LOWER COSTS AND
HIGHER PERFORMANCE



TABLE OF CONTENTS

GOVERNMENT AGENCIES RECOGNIZE THE BENEFITS OF MOBILITY	3
THE DEMAND FOR CLASSIFIED NETWORK ACCESS IS INCREASING	3
CONVERGENCE OF COMMERCIAL MOBILITY AND CLASSIFIED ACCESS	3
THE FIRST COMMERCIAL SOLUTION FOR CLASSIFIED WIRED, WIRELESS AND REMOTE ACCESS	4
AFFORDABLE CLASSIFIED MOBILITY USING SUITE B	5
CONSISTENT ACCESS VIA NETWORK ON-RAMPS	6
THE BENEFITS OF SIMPLIFIED MANAGEMENT	7
THE BUSINESS CASE FOR ARUBA	7
CONCLUSION	7
ABOUT ARUBA NETWORKS, INC.	8

GOVERNMENT AGENCIES RECOGNIZE THE BENEFITS OF MOBILITY

Government agencies are experiencing tremendous pressure from their end users to support commercial, consumer-grade mobile devices – smartphones, tablets and laptops.

Just as in the corporate world, workers in the public sector have become accustomed to the productivity enhancements that these mobile devices bring to their lives and understand the value they could offer in the workplace.

A variety of mobile devices like iPhones and iPads have been fielded by the end users themselves. These users want wireless LAN (WLAN) access when on-site, and they want 3G/4G support for global field mobility.

Some end users, in attempts to fulfill their communication requirements, utilize these commercial-grade devices in an unsecure manner to conduct classified voice and data communications – which can put their agencies at risk.

THE DEMAND FOR CLASSIFIED NETWORK ACCESS IS INCREASING

Over the past decade, military, intelligence community and civilian agencies have been transitioning to network-centric applications to support their operations.

The most important applications used by these agencies reside on tactically secret networks, such as the U.S. Department of Defense SIPRNET. As a result, classified networks have experienced a dramatic increase in importance and usage.

At the same time, these networks tend to be underutilized because of:

- The huge expense of installing classified networks that are policy compliant and accredited.
- Usability issues with government-sponsored proprietary cryptology systems, such as a high-assurance Type 1 system.
- Reports of low performance when using these cryptosystems for network access.

“The vision we’re looking at is, every soldier is issued a phone”

Michael McCarthy, Director of Operations at the Brigade Modernization Command Mission Command Complex, U.S. Army

Source: Network World

CONVERGENCE OF COMMERCIAL MOBILITY AND CLASSIFIED ACCESS

The need to increase classified access, support personal mobility and reduce costs for taxpayers has prompted government agencies to find ways to utilize commercial technology in their networks. Commercial technology delivers important advantages, including:

- Higher performance.
- Lower purchase and operations costs.
- Increased productivity and rapid innovation.

“The National Security Agency is testing a new mobile infrastructure, largely composed of commercial tools, to secure top secret information on portable devices, such as smartphones and tablet computers...”

Source: Nextgov.com

To meet the converged needs of classified access and mobility, the U.S. National Security Agency (NSA) instituted the Commercial Solutions for Classified (CSfC), which calls for an end-to-end architecture to provide commercial off-the-shelf (COTS) mobile devices with secure connectivity to classified networks and applications. The primary underlying information assurance technology defined in this program involves Suite B cryptographic algorithms.

Suite B cryptography modernizes the communications infrastructure for highly sensitive environments while improving the strength and performance of cryptographic algorithms for key exchange, digital signatures and hashing.

In order to protect classified or other high-value networks from brute-force and other attack vectors, it replaces or augments both the asymmetric cryptography algorithms used during key exchanges and symmetric cryptography algorithms used for unique user-session data encryption.

The Suite B algorithms have better overall cryptographic strength and utilize more efficient underlying computation methods, making them more appropriate for high-performance applications.

The required Suite B protocols and methods are:

- SHA-256 and SHA-384 secure hash algorithms.
- Elliptical Curve Digital Signature Algorithm certificates/signatures (ECDSA 256/384).
- Elliptical Curve Diffie-Hellman for key exchange (ECDH 256/384).
- AES-128 and AES-256 user-data symmetrical cryptography, with the AES-GCM mode.

THE FIRST COMMERCIAL SOLUTION FOR CLASSIFIED WIRED, WIRELESS AND REMOTE ACCESS

Aruba Networks® now offers government agencies a significantly improved approach.

Aruba leverages Mobility-Defined Networks, which automate infrastructure-wide performance optimization and trigger security actions that used to require manual IT intervention.

Mobility-Defined Networks control the dynamic mobility environment by correlating real-time data about users, devices, apps and location. Self-healing and self-optimization functions dramatically reduce helpdesk tickets and protect enterprise data.

“ The exciting thing about Suite B, and it’s very prominent in our planning and road mapping, is that it’s going to allow us to build out our next generation mobile infrastructure ”

**Travis Howerton, Chief Technology Officer,
National Nuclear Security Administration**

Source: SecurityInfoWatch.com

Aruba employs a software approach that extends mobility intelligence across wired and wireless networks all the way to users, devices and apps. This makes Aruba Mobility-Defined Networks amazingly easy to deploy without any changes to the existing infrastructure.

Working with various government agencies responsible for network security technology and policy compliance, Aruba has developed a vastly improved access architecture for networks that handle sensitive but unclassified, confidential and classified information.

“ Smartphones and PDAs are gaining traction among a range of federal audiences as agencies and departments seek to enable greater mobility... ”

Source: Washington Technology

This new architecture uses NSA-approved Suite B cryptographic capabilities to deliver a variety of strategic benefits to every government agency, including:

- Easier and more affordable deployment and management.
- Better operational performance.
- An inexpensive way to provide secure wired, wireless and remote access to authorized users.

In addition to the cost savings afforded by commercial technology, the Aruba solution delivers a variety of strategic benefits, including:

- Improved classified network access for authorized personnel. A high-performance WLAN that supports mobility and operates without physical hardened network connections enables secure access for a larger user population at much lower expense.
- Lower costs of deployment and operations. The Aruba solution is as little as 10% of the purchase cost of a Type 1-certified solution and also costs less to operate.
- Higher user adoption and satisfaction. The Aruba solution offers faster performance and increased battery life for mobile devices. It also removes the hassles of operating Controlled Cryptographic Items (CCIs) and securing them when not in use. With expanded mobile access, users have more flexibility to contribute to their agency missions. The advantages include:
 - Using commercial mobile devices in classified environments.
 - Using the same mobile devices while connected to 3G/4G carrier networks for classified activities.
 - Enabling cross-agency and cross-government collaboration by connecting interoperable networks for first responders or coalition governments.
 - Secure access to multiple services, both unclassified and classified, over the same WLAN infrastructure.

- A network architecture that's ready for the future. Aruba's Suite B implementation makes it possible to utilize classified-capable solutions when building new unclassified networks, in anticipation of elevating them to classified status at a later date.

In addition, it improves security on new unclassified networks in anticipation of the deprecation of older cryptographic methods. Finally, it allows unclassified networks to operate at a classified level without deploying government-proprietary technology.

- An affordable way to provide secure wired, wireless and remote access to authorized users. Using a single group of Aruba solution elements, users can be offered any combination of mobile and fixed network access in a variety of policy-compliant deployment scenarios. Access to applications in each scenario is provided in exactly the same manner without requiring different client configurations, ensuring end user satisfaction and ease of use.

AFFORDABLE CLASSIFIED MOBILITY USING SUITE B

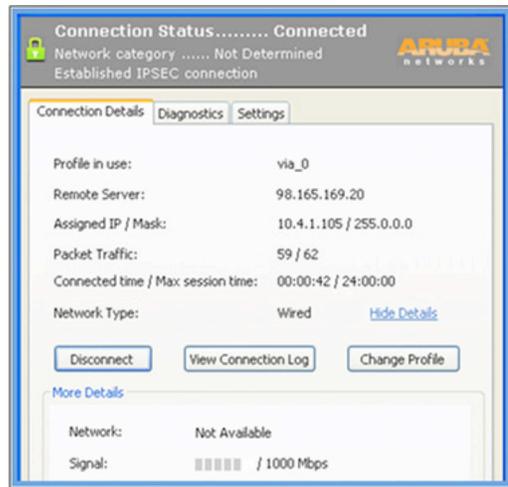
The Aruba Advanced Cryptography (ACR) module, available in ArubaOS™ Release 6.1, brings Suite B cryptography to government agencies of all sizes.

The ACR module is available with Aruba 7200 series Mobility Controllers, 6000 Mobility Controller with M3 controller modules, 3000 Series Mobility Controllers and 600 Series Mobility Controllers. The ACR module with Suite B encryption includes the following capabilities:

- SHA-256 and SHA-384 secure hash algorithms.
- ECDSA certificates/signatures during user/device authentication.
- ECDH for key exchange.
- AES-128-GCM and AES-256-GCM for Suite B symmetric cryptography.
- AES-128-CBC, AES-128-CCMP legacy modes.

- WLAN mode: bSec (802.11i enhanced with Suite B) using EAP-TLS 1.2
- VPN mode: IPsec + Suite B using IKEv2
- Seamless PKI integration with OCSP and CRL support, and with TPM hardware in Aruba Mobility Controllers and 802.11ac APs.

Additionally, the Aruba Virtual Intranet Access™ (VIA™) software agent, available for a variety of mobile and laptop devices, provides an end-to-end secure Suite B tunnel from the device to the Mobility Controller. The VIA client is a soft-installable NIC/IP stack client driver shim that detects whether the client device is connected to a trusted or untrusted network.



Aruba Virtual Intranet Access (VIA) software agent connection status screen.

It then uses a combination of authentication and encryption to create a secure Suite B-enhanced connection to its home Mobility Controller. It can operate in bSec mode (802.11i enhanced with Suite B) as a WLAN client supplicant, Ethernet LAN IPsec mode, or remote access IPsec mode.



The Aruba Mobility Controller product family.

Aruba Mobility Controllers, 802.11ac APs, ArubaOS and vIA are being validated through the U.S. National Institute of Standards and Technology (NIST), U.S. National Information Assurance Partnership (NIAP) Common Criteria, NSA and other agencies for deployment as part of a classified access network architecture.

When combined with other appropriate networking and security technologies, they provide a policy-compliant, classified-capable access network connection for LAN, WLAN and remote access requirements.

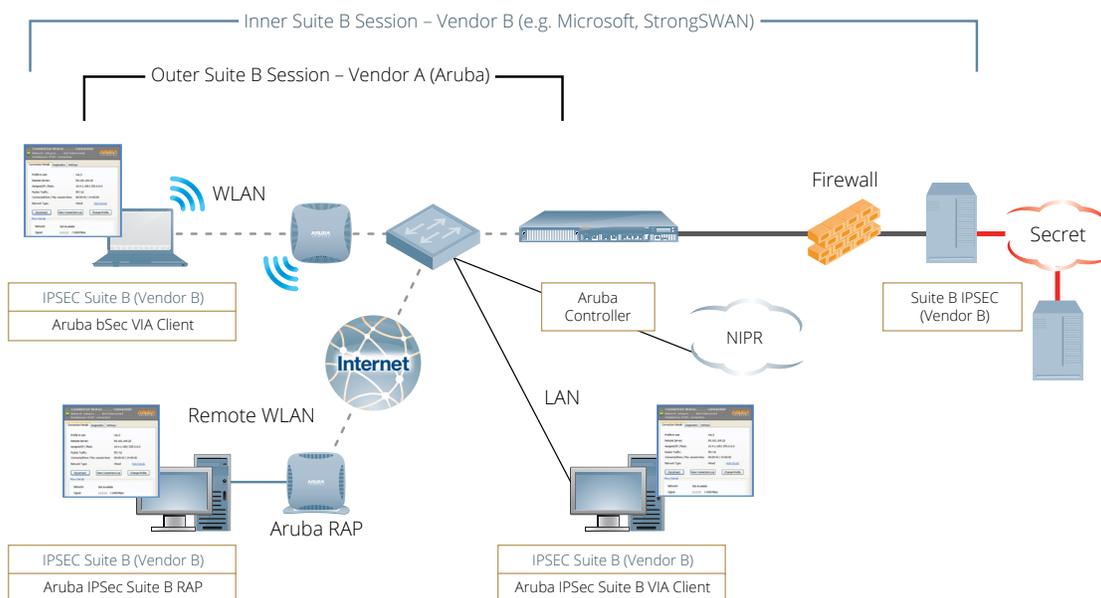
Physical separation of user traffic based on advertised network availability and logical separation of user traffic through the Mobility Controller’s cryptography and firewall functions ensure that classified and unclassified traffic are not co-mingled.

Because this solution is based on commercial cryptographic technology, it is available to U.S. government agencies as well as defense, government and private enterprise organizations worldwide.

CONSISTENT ACCESS VIA NETWORK ON-RAMPS

As part of the common network services at the core of Aruba Mobility-Defined Networks, Suite B support is available to networks accessible through a variety of on-ramps:

- **Wireless APs.** Aruba 802.11ac APs provide high-performance connectivity to mobile and fixed wireless devices, while providing best-in-class RF control using Adaptive Radio Management (ARM) and patented ClientMatch™ technologies.
- **Mobility Access Switches.** Aruba has extended the user-centric, services-based approach of the MOVE architecture to a new class of access switches. Designed to provide network access in wiring closets, Aruba Mobility Access Switches connect wired Ethernet devices such as virtual desktops, video surveillance cameras and wireless APs.
- **Remote APs.** An alternative operating mode for Aruba APs, Aruba Remote APs (RAPs™) automatically extend centralized resources to branch and remote locations using site-to-site VPN tunnels to the central data center. Using zero-touch configuration, personnel at these sites can easily set up their own RAPs with no IT assistance.
- **Outdoor APs.** Aruba outdoor APs combine a unique multi-radio, multi-frequency architecture, Adaptive Radio Management and hardened enclosures to bring high-performance networking to outdoor or deployable environments. Using the ArubaOS mesh features, they can connect to the backbone network wirelessly as an alternative to a wired AP connection.



Example of the Department of Defense SIPRNET access architecture using Aruba Suite B encryption.

THE BENEFITS OF SIMPLIFIED MANAGEMENT

With Aruba Mobility-Defined Networks, services are defined once via a centralized Aruba Mobility Controller in the data center. This eliminates the need to keep up with a profusion of wiring closets, firewalls, network access control (NAC) solutions, management systems and reporting tools that operate in separate domains.

As a result, network operations are consistent across the entire organization, regardless of user location, access method, mobile device or applications. Aruba easily accommodates users with multiple devices, including both legacy devices and commercial mobile technology, including smartphones, tablets and laptops.

With its user-centric approach, Aruba Mobility-Defined Networks also eliminate the need to maintain VLANs at the edge and manually configure user additions and changes.

“As the U.S. Army ponders how to give every soldier a smartphone loaded with apps for military purposes...it is also exploring how it can quickly set up its own wireless network almost anywhere in the world”

Source: InfoWorld

THE BUSINESS CASE FOR ARUBA

With tight budgets and mobility at a critical juncture, Aruba Mobility-Defined Networks present a very compelling business case for government, civilian and military agencies:

- Significantly lower purchase costs compared to proprietary solutions. The Aruba medium-assurance solution is as little as 10% of the purchase cost of a high-assurance Type 1-certified solution. Additional operational savings come from:
 - Eliminating cumbersome CCI checkout and handling processes.
 - Accelerating the move from wired to 802.11ac Gigabit Wi-Fi, thereby reducing the number of Ethernet switches needed in favor of more cost-effective Wi-Fi access.
 - Moving to thin on-ramps at the edge that are easier to install and operate.

- Additional savings by operating multiple services on the same WLAN. Aruba supports unclassified and classified access in different or the same coverage areas using a single WLAN network architecture.
- Easier support for both local and remote users. Because it utilizes a single architecture and network design for local (using WLAN, WLAN mesh and wired) and remote (using remote wired and WLAN) access, it is simpler to manage.

Instead of employing well over a dozen steps to configure network access using a legacy approach, employees can configure the Aruba solution in just three simple steps.

- Improved security by supporting all access modes. Aruba Mobility Controllers manage classified WLAN users and classified wired users to simplify network design and strengthen the overall security posture by adding access control and user firewalling.
- A higher performance network. Aruba 7200 series Mobility Controllers support up to 40 Gbps of AES-256 encrypted throughput for tens of thousands of concurrent users.
- Lower end-user support costs and higher satisfaction. Aruba gives the entire workforce – employees with and without clearance as well as contractors and guests – a single, consistent way to access the appropriate agency resources.

Role-based access policies allow IT to control users and devices, so that personnel can switch effortlessly between desktops, laptops, tablets, smartphones and other mobile devices. By cutting down on the confusion and saving time for users, Aruba reduces IT service desk calls and increases user satisfaction.

Finally, employees accessing classified information via mobile devices gain significant benefits in terms of usability, application performance and battery life.

CONCLUSION

Aruba Mobility-Defined Networks give government IT organizations the technology they need to realize their vision 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 COTS solutions.

With Mobility-Defined Networks, access privileges are linked to a user's identity. That means government personnel have consistent, secure access to classified and non-classified network resources based on who they are – no matter where they are, what devices they're using or how they're connected.

ABOUT ARUBA NETWORKS, INC.

Aruba Networks is a leading provider of next-generation network access solutions for the mobile enterprise. The company designs and delivers Mobility-Defined Networks that empower IT departments and #GenMobile, a new generation of tech-savvy users who rely on their mobile devices for every aspect of work and personal communication. To create a mobility experience that #GenMobile and IT can rely upon, Aruba Mobility-Defined Networks™ automate infrastructure-wide performance optimization and trigger security actions that used to require manual IT intervention. The results are dramatically improved productivity and lower operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, Africa and Asia Pacific regions. To learn more, visit Aruba at www.arubanetworks.com. For real-time news updates follow Aruba on [Twitter](#) and [Facebook](#), and for the latest technical discussions on mobility and Aruba products visit Airheads Social at <http://community.arubanetworks.com>.



1344 CROSSMAN AVE | SUNNYVALE, CA 94089

1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com

©2014 Aruba Networks, Inc. Aruba Networks®, Aruba The Mobile Edge Company® (stylized), Aruba Mobility Management System®, People Move. Networks Must Follow®, Mobile Edge Architecture®, RFProtect®, Green Island®, ETIPS®, ClientMatch®, Bluescanner™ and The All Wireless Workspace Is Open For Business™ are all Marks of Aruba Networks, Inc. in the United States and certain other countries. The preceding list may not necessarily be complete and the absence of any mark from this list does not mean that it is not an Aruba Networks, Inc. mark. All rights reserved. Aruba Networks, Inc. reserves the right to change, modify, transfer, or otherwise revise this publication and the product specifications without notice. While Aruba Networks, Inc. uses commercially reasonable efforts to ensure the accuracy of the specifications contained in this document, Aruba Networks, Inc. will assume no responsibility for any errors or omissions. WP_SuiteB_041514