DATA SHEET

ARUBAOS ADVANCED CRYPTOGRAPHY MODULE

Provides Maximum Deployment Flexibility

The ArubaOS™ Advanced Cryptography (ACR) module brings military-grade Suite B cryptography to Aruba Mobility Controllers, enabling user mobility and secure access to networks that handle controlled unclassified, confidential and classified information.

Approved by the U.S. National Security Agency (NSA), Suite B is a set of publicly available algorithms that serve as the cryptographic base for unclassified information and most classified information.

Unlike the previous generation of cryptosystems, known as Suite A or Type I, Suite B improves performance, eliminates unwieldy workflows and strict handling requirements, allows interoperability, and supports commercially available mobile devices – all at a fraction of the cost of Suite A.

The NSA has authorized the use of Suite B to facilitate the sharing of sensitive and classified information among multiple departments as well as to bring secure mobility to commercial laptops, tablets and smartphones.

The ArubaOS ACR module is a licensed option on any Aruba Mobility Controller, allowing governments and organizations that handle sensitive or confidential information to securely and cost effectively utilize commercial mobile technology for classified- grade networks.

SUITE B ALGORITHMS

- Advanced Encryption Standard (AES) Block Encryption with key sizes of 128 or 256 bits used with Galois/Counter Mode (GCM)
- Elliptic-Curve Digital Signature Algorithm (ECDSA) using NIST p256 and p384 curves
- Elliptic-Curve Diffie-Hellman (ECDH) key agreement
- Secure Hash Algorithm (SHA) using SHA-256 and SHA-384

SUITE B PROTOCOLS

- IPsec using Internet Key Exchange (IKE) or IKEv2 – RFC6379
- TLS 1.2 Suite B ciphersuites – RFC 6460
- Extensible Authentication Protocol (EAP) offload with TLS v1.2 – RFC 5246

DESIGNED FOR COMPATIBILITY

- Based on IEEE 802.1X framework with support for all secure EAP methods
- Supports the use of X.509v3 certificates using ECDSA

FUTURE-PROOF NETWORK ARCHITECTURE

- Elevate unclassified networks to classified status utilizing the same hardware
- Utilize classified-capable solutions when building new unclassified networks

SIMPLIFIED NETWORK DESIGN

- Rapidly deploy secure access locally and remotely using a single architecture
- Support multiple services on the same network infrastructure for both classified and unclassified access

FULLY ACCREDITED

- FIPS 140-2 validated
- Common Criteria (WLAN, VPN Gateway, and Firewall Protection Profiles)

UNIFIED SECURITY FRAMEWORK

Aruba enables universal authentication and encryption for wired and wireless users, regardless of access method. With the Aruba Virtual Intranet Access (VIA) client and ACR, every client that connects to the network – wireless or wired – can authenticate to an Aruba Mobility Controller.

Authentication is achieved using standard the 802.1X EAP or IKE, with credential validation through RADIUS or Online Certificate Status Protocol (OSCP).

VIA supports authentication using passwords, certificates, smart cards, token cards and other credentials that are supported by the chosen EAP type.

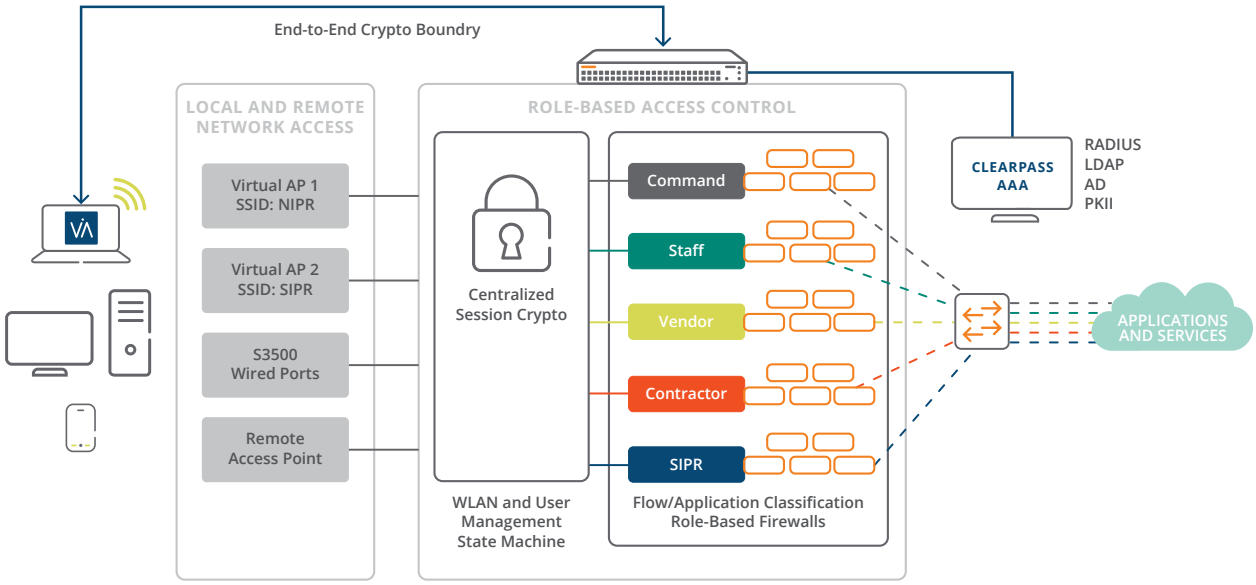

Figure 1: Centralized Security Architecture for Classified Networks

NSA CERTIFIED

Suite B has been certified by the NSA as part of its Cryptographic Modernization Program, and includes a common set of cryptographic algorithms for use in protecting unclassified information and most classified information up to the Top Secret level. The use of Suite B to protect national security systems in the United States is authorized by CNSSP-15.

More details on Suite B and Commercial Solutions for Classified may be found at https://www.nsa.gov/resources/everyone/csfc/.

ACR DEPLOYMENT SCENARIOS

ACR is deployed by activating the ACR module license on an Aruba Mobility Controller and by installing VIA on a wired or wireless device, smartphone or tablet.

ACR can be used to secure traffic between an Aruba Mobility Controller and local or remote wired and wireless clients, as well as between two Mobility Controllers on the same VLAN. The Aruba Remote Access Point (RAP) also supports Suite B.

DESIGNED FOR COMPATIBILITY

The Aruba ACR module is built on public security standards such as 802.1X, TLS, and IPsec. Secure EAP methods supported include EAP-TLS, TTLS, and PEAP, making ACR compatible with existing security mechanisms such as Smart Cards and PKI certificates.

ACR is designed to work seamlessly on top of existing Layer 2 and Layer 3 network infrastructures.

VIA WITH SUITE B

VIA is a VPN client that works with any Aruba Mobility Controller to enable secure connectivity to an enterprise data center from popular device operating systems.

Combining the best of IPsec and SSL VPN technology, VIA automatically establishes a secure connection whenever it is needed, and automatically negotiates transport protocols to use SSL when other protocols fail.

To enable Suite B connectivity, VIA has been enhanced to support RFC 6379 (Suite B Cryptographic Suites for IPsec). VIA is FIPS 140-2 validated, evaluated under Common Criteria as a VPN client, and listed on the CSfC Components List.

VIA with Suite B is enabled with the ArubaOS ACR module and supported on Windows, Mac OS, Linux, Apple iOS, and Android.

Figure 2: VIA Client Connection Status

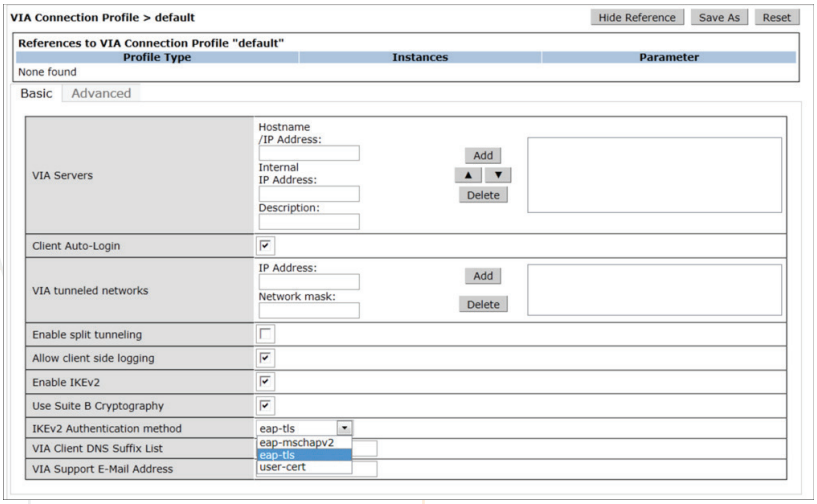

Figure 3: Enabling Suite B Cryptography on VIA

The ACR module is available as a license for Aruba Mobility Controllers and is ordered based on the number of concurrent Suite B sessions supported by the controller.

ORDERING INFORMATION

Part Number	Description
Q9B90AAE	Aruba Adv Crypto 1 Session Lic E-LTU

DS_OSACR_SK_052220