

The NAVY's Choice for Secure Wireless



An EFJohnson company
TECHNOLOGIES

Shipboard Wireless

Balances Greater Mobility with Information Assurance and Network Security

The Challenge

Although Broadband wireless networks (i.e., IEEE 802.11) and wireless technology applications have become common place in the commercial arena, leveraging this commercially available capability for Navy implementation has proven problematic based on the cost, the processes involved to meet the Navy's stringent security requirements, and the time it takes to develop, demonstrate and test a product within the minimum two year Navy acquisition cycle to rapidly deploy a new technical capability.

Commercially available wireless networks typically capitalize on commercial efforts to incorporate best practices with regards to Information Assurance (IA) and Network Security. The bulk of these solutions do not satisfy the more stringent requirements necessary to satisfy IA and Security requirements mandated by Federal and Department of Defense (DoD) criteria regarding the use of wireless technology. These requirements include incorporation of Federal Information Processing Standard (FIPS) 140-2 and DoD Directive 8100.2. Additionally, the resulting network must satisfy Certification and Accreditation (C&A) in accordance with the DoD Information Assurance Certification and Accreditation Process (DIACAP). The C&A process verifies that IA and security requirements, policies, controls, risks and risk mitigations have been fully addressed and verified prior to being granted Authority to Operate (ATO) by the cognizant Designated Approval Authority (DAA).

Implementation of wireless technology that incorporates IA and required Security features and satisfies C&A requirements will afford the Navy greater capabilities by extending the capabilities of the Integrated Shipboard Network System (ISNS) – the shipboard Local Area Network (LAN) program of record – by providing wireless connectivity ubiquitously within the lifelines of ISNS-equipped Navy ships. In addition, the use of wireless technology would enable ISNS to be utilized for secure short range ship to ship connectivity in support of ship assigned missions such as Expanded Maritime Intercept Operations (EMIO).



The Solution

As the leading provider of Secure Wireless technology solutions, 3e Technologies International (3eTI), a wholly owned subsidiary of EF Johnson Technologies, responded to the Navy's wireless technology challenges. Through 3eTI's pioneering efforts to bring wireless technology to the Navy fleet, and through prototype development efforts sponsored Program Executive Office for Ships (PEO Ships) Science and Technology (S&T) Manager under a Small Business Innovative Research program, 3eTI tackled the seemingly daunting IA and Security requirements levied on commercial wireless head on and produced the world's first FIPS 140-2 Validated™ Wireless Access Point. In addition to its FIPS validation, 3eTI's AirGuard™ 3e525A-3 Wireless Access Point provides secure mesh network, gateway, and bridge / repeater capabilities for wireless voice, video and data applications. It features a dual-radio configuration with a 2.4 GHz (802.11a/b/g) Wi-Fi radio and a 5.8 GHz (802.11a/b/g) radio packaged in a Military IP66 outdoor rugged, weatherproof enclosure. The 3e525A-3 operates on Power-over-Ethernet and can be used for a variety of secure communication applications including homeland defense, military, law enforcement, public safety and industrial / commercial applications.

Working with PEO Ships S&T, 3eTI successfully demonstrated a secure end-to-end wireless LAN (WLAN) extension of USS COLE's (DDG 67) ISNS unclassified shipboard network utilizing the 3e525A-3 and 3eTI-developed FIPS 140-2 Validated™ Security

The NAVY's Choice for Secure Wireless



An EFJohnson company
TECHNOLOGIES

Shipboard Wireless

Balances Greater Mobility with Information Assurance and Network Security

Server and Cryptographic Client software that fully satisfied DoD IA and Navy C&A requirements during the Navy's Trident Warrior 2006 experiment.

Additionally, 3eTI also demonstrated a viable capability to support the Navy's EMIO mission using secure wireless technology. 3eTI's secure solution for EMIO features the 3e525A-3 on the Navy host vessel providing a secure wireless data link to a small wireless, battery-powered, Internet Protocol Router – the 3e523S-1 – carried by the EMIO boarding party to send data collected on the vessel of interest back to the Navy host vessel.

The resulting secure wireless technology solutions for ISNS extension and EMIO were transitioned by PEO Ships S&T under a Rapid Technology Transition agreement with PEO Command, Control, Communications, Computers and Intelligence (C4I) to its IT-21 ISNS program of record. PEO C4I is implementing WLAN featuring 3eTI's 3e525A-3, 3e030 Security Server, and 3e010 Crypto Clients to the fleet with ISNS Mod 2 upgrades. As of 2010, ISNS Mod 2 has deployed to USSs GEORGE H.W. BUSH (CVN 77), MOUNT WHITNEY (LCC 20), BOXER (LHD 4), and COLE with additional deployments planned this year for USS NIMITZ (CVN 68) and upgrades to the PEO Ships S&T deployed WLANs on USS HOWARD (DDG 83) and USS MASON (DDG 87). In support of the Navy's EMIO mission requirements, PEO C4I is also deploying Wireless Reach Back System AN/SSQ-131 (WRBS) kits produced by 3eTI and featuring 3eTI's secure wireless technology. The kits utilize 3eTI's 3e525A-3 and 3e523S-1 to provide the secure wireless data link between the Navy host vessel and Visit, Board, Search, and Seizure (VBSS) teams onboard a vessel of interest. As of 2010, 61 WRBS kits have been delivered out of a total authorization for 157 kits.



The Benefits

3eTI's secure wireless technology solutions for the Navy deliver increased efficiency, access to shipboard unclassified LAN services and an overall improvement in Force Protection through a significant reduction in the "data collection to identification" time cycle for EMIO. The 3e525A-3 utilized in the ISNS Mod 2 operates on IEEE 802.3af Power-over-Ethernet (POE), saving the time and costs associated with power line cabling and enabling mobility and ubiquitous access to ISNS LAN services securely throughout the interior of the ship.

3eTI's end-to-end secure wireless solutions includes FIPS 140-2 Validated™ security software (3e030) and middleware — important components of a complete system. As the only licensee of Intel® Centrino® mobile technology source code today, 3eTI has developed crypto client software that provides secure WLAN for laptop or desktop computers using either the Centrino or Atheros® platforms. The crypto client software (3e010) meets 802.11 Wi-Fi standards and is FIPS 140-2 Validated™.

3eTI's crypto client software is supported by security server software, which runs on a Windows™ 2000 or newer system and generates a dynamic key for each user and user session. It also authenticates each user by distributing and managing digital certificates based upon DoD standards, making it among the most secure applications available today.

In addition to providing excellent security for wireless applications within the federal government, Department of Defense, and civilian agencies, 3eTI's security solutions are ideal for the commercial market, where security also plays an important role. For industries such as financial services and health care — where HIPAA regulations require health information privacy and data integrity — protecting a client's personal information is required by law.