

Cutting the cord for classified

Helping customers improve service quality, save money, and meet requirements for assured communications using commercial wireless devices and networks



- For customers requiring a high level of assurance in wireless communication, Perspecta Labs designs solutions that meet the NSA standards for carrying classified data over wireless networks
- Perspecta Labs has the technology, experience, and certifications to design and implement integrated hardware and software solutions for assured communications across commercially available wireless devices

Efficiently operating commercial and government enterprises requires highly assured network communication. This usually means a traditional approach of utilizing wired networks in order to avoid attacks, exfiltration and impersonation—but this also limits interconnection. In this case study, we explore how implementing a wireless network allowed a customer to have high confidence in the protection of their communication while also eliminating cost and complexity of configuring and running a wired network.

The challenge

A Perspecta Labs customer is routinely on the move with a set of shared commodity laptop computers that access a highly protected infrastructure network. To meet user requirements, the customer carries its laptops and specialized networking and encryption equipment to each new site. As the customer moves to a new location,

technicians set up a wired network joining the laptops, encryption equipment and a local router gateway to the infrastructure network. Because the laptops are shared among the personnel, each laptop is configured to connect to a Microsoft Active Directory server, enabling a new user to walk up to and use any workstation without a user-specific configuration change being required on the workstation.

While the existing solution delivered a secure communication capability, it carried an unacceptable cost in terms of the set-up time and the traveling weight of the cables and associated networking equipment. Additionally, each new location introduced potential troubleshooting costs as the physical network is repeatedly broken down and manually re-established, introducing opportunities for equipment failure and human error.

The solution

Perspecta Labs designed and implemented a wireless solution that was in compliance with the National Security Agency's (NSA) Commercial Solutions for Classified (CSfC) program. CSfC is the NSA approved process for using commercially available technologies to protect classified information. The program defines a path for NSA-designated trusted integrators to design, implement and receive approval to operate qualified solutions that leverage commodity or commercial off-the-shelf (COTS) hardware and software products to carry classified communications.

In this case, after designing and implementing a COTS-based Wi-Fi solution to replace the copper network, Perspecta Labs guided the customer through CSfC registration, integration exercises and deployment.

Our customer had a goal of using low-cost, readily available commodity hardware to enable highly assured communication of classified data over an otherwise unprotected wireless network.

To achieve this goal, Perspecta Labs defined target systems, components and technologies and devised processes and configurations compatible with relevant CSfC capability packages. The Perspecta Labs solution provided an automated mechanism for converting standard Army Gold Master (AGM)-based systems from wired assets to wireless assets capable of and permitted to connect to Secret Internet Protocol Router—or SIPR—networks. Perspecta Labs delivered a fully CSfC-capable system compliant with NSA-defined Mobile Access

Capability Package (MACP) for validation and subsequent use. Perspecta Labs also designed a solution compliant with the NSA-defined Campus Wireless LAN (CWLAN) Capability Package.

The results

Because Perspecta Labs is recognized by NSA as a trusted integrator under the CSfC program, we were able to design and implement a highly assured wireless solution, and obtain approval to operate it as a classified system.

The customer benefits of this solution include the ability to establish a mobile unit using COTS Wi-Fi products, supporting unmodified unicast and multicast classified IP traffic, no longer needing to carry and configure a wired network to new tactical locations where classified communication will be needed. Additionally, the wireless capability reduces the traveling weight of the unit, and reduces the complexity and durations of the setup operations in new locations.

About Perspecta Labs

At Perspecta Labs, we refuse to think inside the box. As the innovation hub of Perspecta, we are molding the future of emerging technologies. Our experts conduct leading research in cybersecurity, mobile communications, machine learning and internet of things technologies that provides customers with transformative insights and real-time situational intelligence. With our finger on the pulse of next-gen technology, you'll gain an essential edge.

Contact the Perspecta Labs CSfC experts:
trusted.csfc@perspectalabs.com