

FIPS 140-2 VALIDATED CAMBIUM PTP SOLUTIONS

SAFEGUARD YOUR PTP COMMUNICATIONS WITH FIPS 140-2



Most government and military organizations require Federal Information Processing Standard (FIPS) 140-2 protection to secure highly sensitive data, voice and video communications. State and local agencies as well as financial, healthcare, manufacturing and other business enterprises also need FIPS140-2 to safeguard their informational assets and comply with government regulations. At Cambium Networks, we have made and continue to make significant investments in secure technologies to protect your confidential communications. Our FIPS 140-2 validated Cambium Point-to-Point (PTP) 600 Series Solutions and our FIPS 140-2 compliant Cambium PTP 800 Series Solutions offer high-performance connectivity with powerful protection for your wireless communications.



TM: Certification Mark of NIST (National Institute of Standards and Technology), which does not imply product endorsement by NIST, the U.S. or Canadian Governments.



Cambium PTP 600 Connectorized
Cambium PTP 600 Integrated
Cambium PTP 800 Outdoor Unit
and Compact Modem Unit

CAPABILITIES

FIPS 140-2 Level 2 security is a module that meets regulatory requirements for cryptographic algorithms, key security and tamper-evidence and is an optional module that is available on our PTP 600 Series outdoor radio units. All PTP 600 radios configured with FIPS 140-2 also require 128-bit or 256-bit AES encryption. Together AES encryption and FIPS 140-2 protection provide extremely robust security to protect your communications from malicious incidents.

With FIPS 140-2 Level 2 Security, our cryptographic module supports only FIPS-approved-and-allowed algorithms for AES (Advanced Encryption Standard) wireless link encryption and TLS (Transport Layer Security) connections. Level 2 Security also includes tamper-evident seals that must be broken to attain physical access to the plain-text cryptographic keys and critical security parameters within the radios. Two tamper-evident labels are affixed to each PTP 600 radio and should be checked at least every 30 days. If tamper evidence is observed, the radio should be removed from service and inspected closely.

Further security is provided through identity-based authentication with FIPS-mode password complexity and roles assigned to each user, including security administrator, system administrator and read-only user. Each user's assigned role determines the operations which can be accessed and performed.

COMMUNICATIONS AGILITY

PTP 600 radios leverage a combination of field-tested technologies to overcome obstacles, interference and fading and to deliver reliable communications in virtually any environment. The systems offer high-speed throughput, carrier-grade availability, excellent durability and robust, multi-level security. As a result, U.S. Federal Department of Defense (DoD) and civilian agencies can deploy mission-critical wireless broadband networks where and when needed. With up to 99.999% availability and extremely low latency, the systems are ideally suited to backhaul Land Mobile Radios (LMRs), video surveillance cameras, mesh nodes or hot spots, and command centers.

PTP 800 solutions provide civilian and military agencies with affordable traditional microwave capabilities that are excellent for applications such as added backbone capacity, network redundancy and edge communications.

PAIRING PTP 600 AND FIPS 140-2

PTP 600 Series solutions operating in the 2.5, 4.5, 4.8 and 4.9 GHz licensed radio frequencies and the 5.4, 5.8 and 5.9 GHz license-exempt radio frequencies support the FIPS 140-2 mode. With new and existing PTP 600 deployments, you have the option to include FIPS 140-2 Level 2 on any PTP 600 system by purchasing a license key and downloading the FIPS version of the software from our Web page.

Each PTP 600 radio is encased in a highly-durable cast metal casing and cover plate and sealed with two tamper-evident labels. The only difference between the Connectorized and Integrated enclosures is that the radios have differing types of cover plates.

INTEROPERABILITY

In addition to FIPS 140-2 validation, our PTP 600 systems are tested and MEF9 certified as compliant with the Metro Ethernet Forum's (MEF's) essential specifications. This means you can be confident that your PTP 600 solution will operate seamlessly with your existing MEF9-compliant network equipment.



PTP 600 radios are MEF9 certified.

FIPS 140-2 validation may be confirmed at:

<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#1515>

Our certificate number is 1515. If the URL does not take you directly to certificate #1515, scroll down to that certificate number.

PTP 800 certification status may be confirmed at:

<http://csrc.nist.gov/groups/STM/cmvp/inprocess.html>