



Australian Government

Department of Defence

Intelligence & Security

SCIP Bulletin

The ability to ensure secure communications is fundamental to the planning and execution of operations within Defence and in securing intelligence pertinent to Australia's national interest. The increasing need for interoperability with our coalition partners, as well as ageing sovereign communications equipment, has resulted in the development of a standard that will satisfy sovereignty and international interoperability requirements.

After extensive research and liaison with Defence, allied partners and industry, it was evident that adopting an internationally accepted standard would give Australia access to a greater variety of telephony devices. The accepted standard for secure telephony equipment, developed by the US National Security Agency, is the Secure Communication Interoperability Protocol (SCIP), formerly known as the Future Narrowband Digital Terminal standard. Australia has joined Canada, New Zealand, the UK, the US, NATO and other allies in adopting this standard as the protocol for secure voice interoperability.

SCIP represents a fundamental shift in the traditional secure communications paradigm. It prescribes a secure interoperable architecture that will enable any nation to build interoperable solutions to an agreed set of architectural and protocol standards. SCIP operates within the Public Key Infrastructure/Key Management Infrastructure framework for cryptographic key exchange. The SCIP architecture also includes a number of different cryptographic algorithms to allow for cryptographic separation of Communities of Interest, such as national, CCEB, NATO and coalition, thus providing for both sovereignty and international interoperability requirements.

The adoption of a standard, rather than a single cryptographic product, will allow greater flexibility in product and vendor selection. Moreover, this standard will allow greater interoperability between various SCIP-compliant devices on similar and disparate networks by adhering to a set of minimum essential requirements. These objectives are essential for Network Centric Warfare capability and the Global Information Grid, in which SCIP is integral to an infrastructure that will allow for the creation of shared battle space awareness and knowledge, leading to operational effectiveness and agility. SCIP will play a prominent role in the modernisation of our cryptographic inventory.

The SCIP-compliant products available for purchase are the Sectera BDI, Sectera Wireline Terminal, Sectera GSM, and Omni Wireline Terminal.

For more information on how SCIP may have an impact on your communication networks, please contact the DSD Cryptographic Liaison Project team at ISGQLPTeam@drn.mil.au, or telephone (02) 6266 9171 or (02) 6266 5761. For information relating to through life support and sustainment, Defence customers should contact the Chief Information Officer Group on (02) 6266 1888.

UNCLASSIFIED