WiMAX Technology

7955/7956

The WiMAX Security Processor

- AES-CCMP
- RSA/DH for PKM-EAP

Hifn Security Technology Benefits

- Line-rate WiMAX Security
- Cost-effective
- Low Power Consumption
- Ease of Integration Basestation
  – Reference Design Available

Hifn
Intelligent Secure Networking

WiMAX Technology

WiMAX is a new, standards based wireless technology, designed to solve the limitations both of Wi-Fi and last-mile broadband access.

WiMAX is the IEEE 802.16 Point-to-Multipoint broadband wireless access standard for systems in the frequency ranges 10 – 60 GHz and sub 11 GHz. Initially WiMAX will provide fixed nomadic, portable and, eventually, mobile wireless broadband connectivity.

WiMAX basestations transmit up to 30 miles, but typically, the cell-based topology would mean a more typical radius of 3 to 5 miles. WiMAX systems can deliver a capacity of up to 75 Mbps per channel, for fixed and portable access applications. This is enough bandwidth to simultaneously support hundreds of businesses with T-1 speed connectivity and thousands of residences with DSL speed connectivity. WiMAX technology will be incorporated in notebook computers and PDAs in 2006, allowing for urban areas and cities to become "MetroZones" for portable outdoor broadband wireless access.

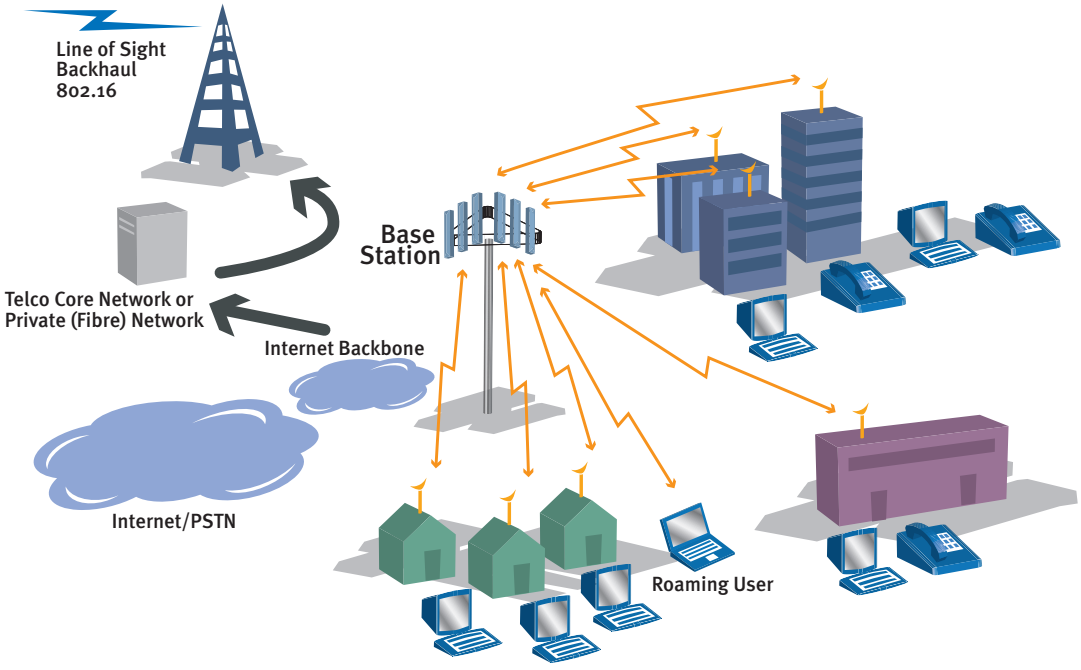
Wireless service providers and telecommunication equipment industries are rallying around WiMAX technology because of its tremendous cost advantages to provide last-mile connectivity to large parts of the world that are too expensive to serve with wired technologies.

Due to the issues with WEP in the 802.11 Wi-Fi arena, the standards bodies are not taking any chances with WiMAX, and have prioritized security from the beginning. Therefore, basestation designers require a dedicated high performance security processor.

The WiMAX standard requires that all traffic must be encrypted with CCMP (which is Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). CCMP uses AES to provide the encryption for secure transmission as well as data authentication for data integrity.

For end-to-end authentication, WiMAX uses PKM-EAP (Extensible Authentication Protocol), which relies on the TLS standard which uses public key cryptography.

The Hifn 7955 and 7956 security processors are ideally suited for WiMAX and offer a suitable



WiMAX Technology

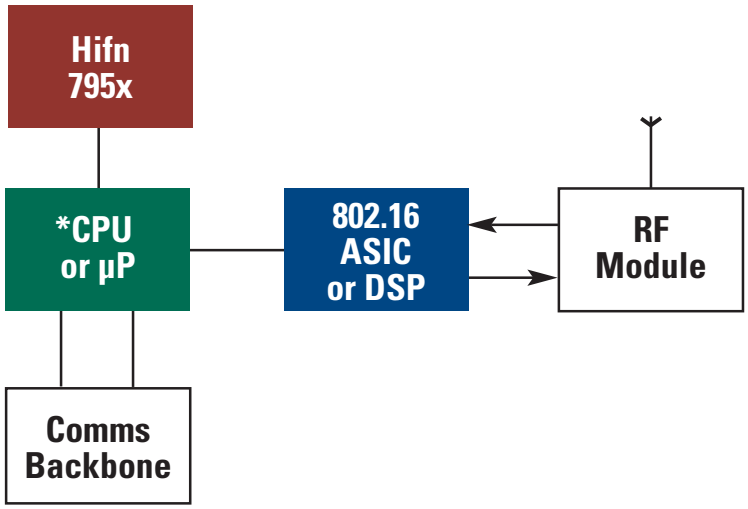
encryption / security solution for the evolving 802.16e standard. The symmetric key cores, which includes the ability to perform AES-CCM function, performs at 200 Mbps with 1500 byte packets. It is this small packet performance, coupled with the internal 32Kb of memory that makes the 795x processor ideal for WiMAX basestations by performing the complex encryption/decryption with minimal latency. For multiple-channel basestations, the 7956 processor offers all the features and functions of the 7955, but can perform AES-CCM with 1500 Byte packets at 275 Mbps.

The 795x also features a completely separate internal public key core, with a true random number generator, public key engine and independent 4Kb of internal memory. This means the PKM-EAP functions for authentication will never impact the CCMP performance.

Both the 7955 and 7956 security processors have a flexible bus interface allowing you to connect to virtually any kind of processor through either a PCI 2.2 (up to 64-bit 66Mhz), a PowerQuicc I or a PowerQuicc II bus They also include standard features, such as LZS data compression/decompression and IPsec security to support VPN connections on the backbone side.

The low-cost 144-pin TQFP is a single chip solution for WiMAX security functions, with no requirement for external memory or logic means there is a minimal impact of your Bill-Of-Materials cost, and with a typical power dissipation of less than 1W is ideal for any basestation design.

The Hifn 795x security processor is deployed in WiMAX basestations from various industry leaders, and is an integral part of WiMAX basestation reference designs from third party vendors.



* In some instances the 802.16 ASIC and CPU/uP may be a single integrated device.

Hifn Security Processor Selection Guide

Hifn Products	PCI	Streaming Bus	GigE Bus	LZS MPPC	3-DES AES	SHA MD5	RSA DSA	1k-bit RSA signatures set-ups per second	IKE main-mode tunnels per second	Hardware support for public keys up to	Hifn Intelligent Packet Processing	CCM Performance	Package
7955	■			■	■	■	■	84	70	3K bits		200 Mbps	144-pin TQFP
7956	■			■	■	■	■	84	70	3K bits		275 Mbps	144-pin TQFP

Hifn
Intelligent Secure Networking

750 University Avenue
Los Gatos, CA 95032
408.399.3500 tel
408.399.3501 fax
info@hifn.com
www.hifn.com