XIPHRA MANAGEMENT SYSTEM

APPLICATIONS

- SITE-TO-SITE AND INTEGRATED REMOTE ACCESS VPNS
- MANAGED SECURITY SERVICE PROVISION
- END TO END COMMUNICATIONS PRIVACY
- DATA SEPARATION

XIPHRA™ MANAGEMENT SYSTEM

While Xiphra encryptors' blistering performance and security assurance is enabled through the use of dedicated hardware encryption, the success of large scale encryption systems is largely dependent on how well these systems are managed.

Costly downtime related to poor management of cryptographic keys and network topology that are often associated with competing systems is eliminated by the fully centralised Xiphra Management System (XMS).

The XMS is based upon the operating principles of AEP's widely proven Net Management System (NMS), that is currently used to maintain thousands of managed government encryptors internationally.

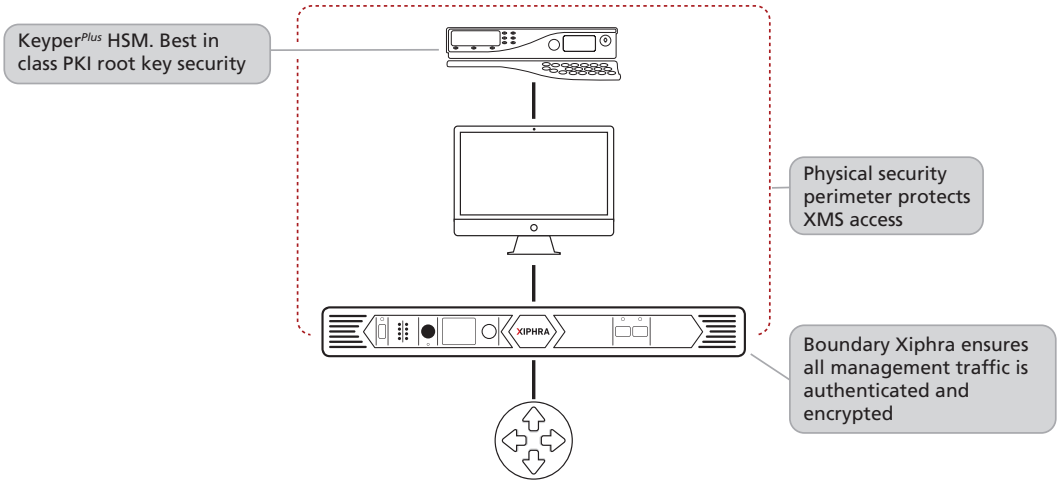
Put another way, superior key management and network topology management have been shown to deliver improved service availability as well as increased network security, at lower costs.

The XMS is designed to be used by either end-user organisations or service providers wishing to offer the next generation of scalable, centrally managed security services.

Xiphra Management System provides **the ultimate in cryptographic key management security** with the Ultra Safe Keyper*Plus*. Keyper™ HSMs are the only networked HSMs employing a FIPS 140-2 Level 4 validated cryptographic security module (maintaining this certification level for fifteen years), thus providing the highest-possible quality and physical security for the keys that underpin the PKI security of the entire system.

Fully centralised GUI based crypto estate management with centrally administered policy management, near real time VPN topology management and troubleshooting functions.

On demand Over the Air Re-keying eliminates the need for site visits to rekey devices, leading to increased service availability and better security. The whole estate can be fully rekeyed in less time than a cup of a tea. This translates to a tremendous cost saving.



BEYOND SEMICONDUCTOR

AEP

Ultra ELECTRONICS

XIPHRA

XMS FEATURES & BENEFITS

FEATURE	BENEFIT
Fully centralised GUI based estate management	XMS provides centrally administered policy management and troubleshooting functions
Remote device 'stun' and 'kill'	Supporting range of policies to manage actual and/or suspected device compromise scenarios
Application specific, dedicated management PKI	CA provides centralised certificate & key management, certificate revocation and cryptographically assured crypto policy enforcement, without the burdensome governance overheads normally associated with PKI deployments
Remote firmware upgrades	Maximises service availability and eliminates return to base or site visit upgrade overheads
On demand VPN topologies	Supports widest range of centrally defined and updated architectures including: full mesh, hub & spoke, overlapping star, partial mesh, etc.
Remote and local licensed feature upgrades	Solution features upgraded on demand to meet evolution of service requirements
Ease of deployment & on-going maintenance	XMS increases availability through improved key management, leading to increased service levels, reduced operational and lifecycle costs
Cryptographic separation of user/management traffic	Cryptographically isolated management is ideal for both service providers and self-managed deployments

EFFECTIVE CENTRALISED KEY MANAGEMENT PROVEN TO INCREASE ENCRYPTION SERVICE AVAILABILITY AND SECURITY, WHILST REDUCING COSTS

The Xiphra Management System is used to manage a deployment of the whole range of Xiphra encryptors. It comprises four elements that together allow network managers to maintain a high-assurance Cryptographic Network Operations Centre, supporting key pair certification for enrolling units, on demand real time 'over the air re-keying' (OTAR) and certificate revocation.

Xiphra Policy Manager a software application running on a standard workstation that provides the graphical user interface for global, group and element level encryptor configuration, including enrolment, VPN topology definition, resilience administration, troubleshooting and device 'stun'.

Xiphra Management Encryptor certificate policy enforces management encryptor mode, authenticating and encrypting all management communications as well as providing both boundary protection for XMS, and cryptographic isolation of management and mission traffic.

Keyper*Plus* Hardware Security Module (HSM) provides the ultimate in key management security for the standalone Public Key Infrastructure (PKI).

The application specific dedicated **Certificate Authority** (CA) creates X.509v3 certificate policies for encryptor authentication and management, and enables assured device 'kill' through issuance of the Certificate Revocation List (CRL) in the event of encryptor removal or compromise.

- Highly scalable, meeting current requirements and growing with the evolution of policy and service growth
- Provides assured and effective compromise management
- Can eliminate the ordering, transportation, storage and handling of sensitive crypto key material
- Automatic key generation, distribution and validation checks eradicate a whole class of potential human errors
- Rapid system deployments, global policy updates and on demand key renewals
- Foregoes the need for costly annual site visits to re-key equipment
- Intuitive graphical interface, reducing risk of misconfiguration

Ultra ELECTRONICS

making a difference

BEYOND SEMICONDUCTOR

Ultra Electronics
AEP
Knaves Beech Business Centre
Loudwater
High Wycombe
Buckinghamshire, HP10 9UT
Phone: +44 (0)1628 642 600
Email: info@ultra-aep.com
www.ultra-aep.com
www.ultra-electronics.com

Beyond Semiconductor
Brnčičeva ulica 41G
SI-1231 Ljubljana-Črnuče
Slovenia
Phone: +386 5 90 90 100
Email: info@beyondsemi.com
www.beyondsemi.com