# Net Management System (NMS)

## Datasheet

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

**Net CA** – Hardware Security Module (HSM) that functions as the Certification Authority to provide a standalone Public Key Infrastructure (PKI) for the network, creating X.509 certificate policies for encryptor authentication and Cryptographic Community of Interest (CCOI) management, and enabling assured device 'kill' via issuance of Certificate Revocation Lists (CRLs) in the event of encryptor removal or compromise.

**Net Policy Manager** – a software application running on a standard PC that provides the graphical user interface for global, group and element level encryptor configuration, including enrolment, VPN topology definition, resilience administration, accounting, centralised audit retrival, troublshooting and device 'stun'.

**Net Management Encryptor** – a Net 20M encryptor that is configured to act as a management encryptor, to authenticate and encrypt all management communications as well as protecting the CNOC.

### Features

- Government-certified solution up to UK/EU CONFIDENTIAL
- Centralised, PKI-enforced policy and key management
- On demand over the air keying and re-keying under CNOC control
- Policy based device 'stun' and cryptographically assured CRL-based 'kill' to manage device trust level changes
- Data separation using policy-based routing and/or assured CCOIs
- Cryptographically separated management traffic
- Administrator and operator role based separation
- Automated and on-demand NMS state backup, audit collection and device health checking (with troubleshooting tools)
- Non-critical to encryption service availability
- Alternate NMS option provides disaster recovery CNOC to maximise business continuity

### Key business benefits

High-assurance CNOC management solution designed to minimise operating costs and maximise availability.

- Rapid system deployment, global policy and key updates
- Minimises ordering, storage, handling and transportation of sensitive key material
- Eliminates the need for annual site visits to re-key equipment
- Provides assured and effective compromise management
- Highly scaleable to meet current and future policy and growth
- Intuitive graphical interface, reducing risk of misconfiguration
- Supports high-availability and Disaster Recovery (DR) configurations
- Enables service providers to operate multiple customer networks from a single CNOC
- Effective key management proven to increase encryption service availability and security

AEP | Ultra ELECTRONICS

## Centralised Policy Management

All network configuration and policy information, such as network topology, encryptor IP addresses and protected host information, is managed centrally with AEP's Policy Manager using an intuitive graphical user interface. Once a new policy is activated, this information is automatically pushed out to all the encryptors, allowing networks to be configured quickly and accurately.

## Painless Key Management

AEP has pioneered an on-line PKI approach to key management that substantially reduces the quantity of sensitive, physical key material required and completely eliminates the need for the transportation of such key material to remote sites. The basis of AEP's solution is the Net CA product, an HSM that acts as a CA and signs digital certificates for each encryptor. This is the only PKI component on the market with CESG Assisted Products Service (CAPS) certification.

## Managing Multiple Networks

The NMS can be used to manage multiple networks, which can be set up as either simple policy groups or full overlapping or non-overlapping CCOIs with assured data separation between user communities. This is particularly useful for service providers, who can safely operate different customer networks (even at different Impact Levels) from a single NMS. Assured data separation also applies to the management traffic, protecting it from the user community and vice versa.

## Resilience

The NMS is not availability critical - i.e. if it were to be taken off-line or a component were to fail, the network encryption will continue to operate. Nonetheless, AEP offers the option of local component resilience and/or an alternate NMS for a DR CNOC (this is a duplicate of the primary NMS with a replicated configuration that can take over at a moment's notice).

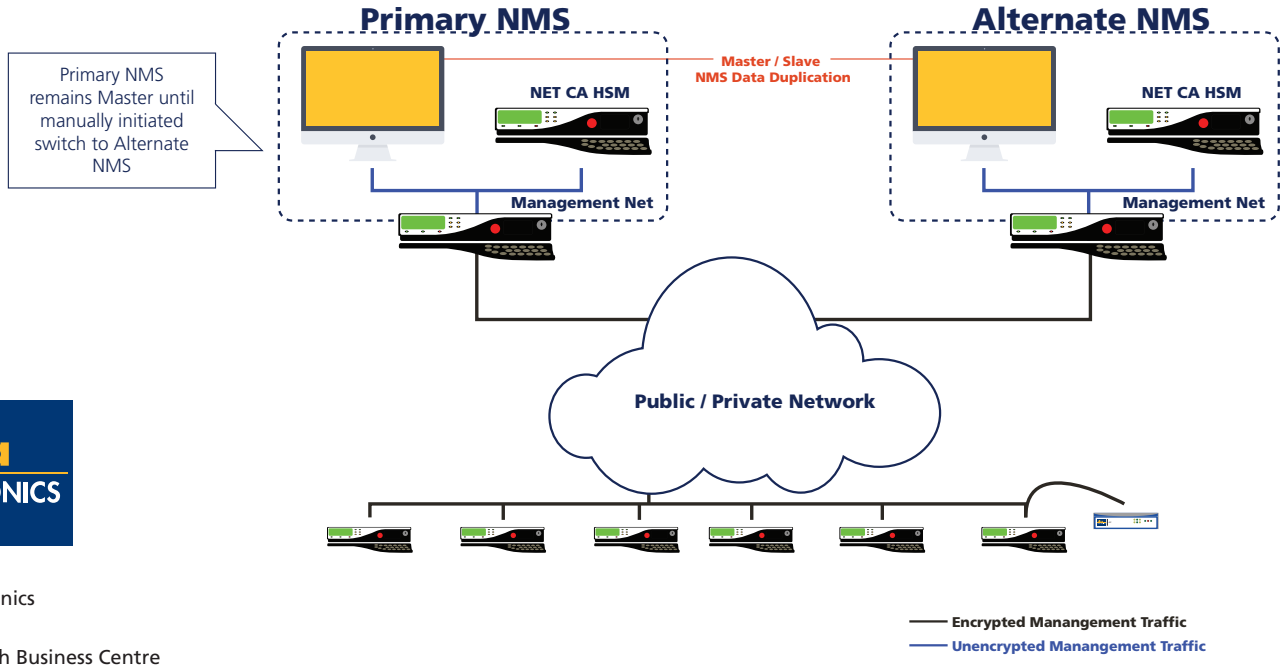
## Solution Summary

The NMS solution includes the Net CA HSM, Management Encryptor, Net Policy Manager and associated software utilities, as well as a smart card reader and smart cards.

The standard NMS is available with a number of different licensing options to support different sizes of network, whilst the Resilient NMS includes an additional Net CA HSM and Management Encryptor licensed for local resilience purposes. If an alternate NMS is required for a DR site, a separate NMS (or Resilient NMS) instance must be ordered.

- NMS (0-4 unit* license)
- NMS (5-10 unit* license)
- NMS (11-25 unit* license)
- NMS (unlimited Enterprise license)
- Resilient NMS (unlimited Enterprise license)

* A "unit" refers to a single, managed Net 20M / Net 100M encryptor or ten Net Remote encryptors.




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