

6th June 2011

Product End-of-Life Notice: UniCERT-based NMS & Net Keyper HSM

This is an end-of-life notice concerning AEP Networks' UniCERT-based Net Management System (NMS) and the associated Net Keyper Hardware Security Module (HSM). Please review this notification in its entirety.

AEP Networks and authorised partners will be contacting affected customers to obtain acknowledgement of this notification, solicit a forecast for last-time orders and assist with the selection of replacement products as required.

If you have any questions regarding this notification, please contact your AEP Networks representative or authorised partner, or e-mail: support@aepnetworks.com.

1. Reason for End-of-Life

The UniCERT NMS and Net Keyper HSM are used in the management of government-grade Net encryptors. However, these products have been superseded by the Net CA NMS and Net CA HSM, which have been shipping since October 2009 and are fully proven in a number of major customer networks; they offer enhanced functionality, improved ease of use, government certification and lower capital and operational costs (see section 5 for further details).

2. Affected Products

Specific Products / Part Numbers Affected	Products NOT Affected
<u>UniCERT NMS</u> <ul style="list-style-type: none"> • E-NET-M-E*K <u>Net Keyper HSM</u> <ul style="list-style-type: none"> • E-NET-KEY 	<u>Net CA NMS</u> <u>Keyper Model 9720 Enterprise HSM</u> <u>Keyper Model 9720 Professional HSM</u>

** The NMS part number varies for UK and EU government versions*

3. Last Order Dates

Product	Last Date to Order Product	Last Date to Order Support	End of Support
UniCERT NMS	30/Sep/11	31/Dec/11	31/Dec/12
Net Keyper HSM	30/Sep/11	31/Dec/11	31/Dec/12

Customers who should consider placing a last-time order for the affected products include:

- Existing customers without a valid support contract who require a spare Net Keyper HSM
- Existing customers with a single UniCERT NMS who require a secondary NMS for a disaster recovery site

4. Support

Unless otherwise specified, hardware and software support will be available until **31st December 2012** for customers with valid support contracts. After that date, support will be limited and may be subject to additional charges.

It is strongly recommended that all users fully migrate to the replacement products (which are not compatible with the end-of-life products) prior to the end of this support period. Special upgrade pricing is available, and AEP Networks offers a full range of professional services to assist customers with planning and implementing such a migration. Please contact AEP Networks or an authorised partner for further details.

5. Alternative / Replacement Products

End-of-Life Products	Alternative / Replacement Products
<u>UniCERT NMS</u> <ul style="list-style-type: none"> E-NET-M-E*K 	<u>Net CA NMS</u> <ul style="list-style-type: none"> E-NET-CAE-E* (Enterprise license) E-NET-CA25-E* (11-25 unit license) E-NET-CA10-E* (5-10 unit license) E-NET-CA4-E* (0-4 unit license)
<u>Net Keyper HSM</u> <ul style="list-style-type: none"> E-NET-KEY 	<u>Net CA HSM</u> <ul style="list-style-type: none"> E-NET-CA

** Part numbers vary for UK and EU government versions*

The following table summarises many of the additional functional capabilities and benefits that the Net CA NMS and Net CA HSM provide in comparison to the UniCERT NMS and Net Keyper HSM.

Net CA NMS Features	Benefits Compared to UniCERT NMS
The Net CA HSM is the only PKI component certified under the CESG Assisted Products Scheme (CAPS) in the UK.	All the CA's cryptographic functions are performed in a dedicated, tamper-reactive module that is fully certified to UK Government standards.
Certificate requests can be processed with as few as two clicks, and multiple requests can be processed in batches.	This greatly reduces certificate management overhead and the risk of human error, thus enabling the frequency of certificate renewals to be increased and reducing the risk of impacting the availability of the encryption service.
Additional mechanisms have been added to defend against incorrectly-provisioned certificate policies.	This further reduces the risk of human error impacting the availability of the encryption service.
Authentication for major transactions uses simple, role-based, two-factor authentication.	This significantly simplifies the process of recovering from a power outage.
Certificate Revocation Lists (CRLs) are generated automatically, without a requirement for smart card based authentication.	This means CRLs will be generated automatically as long as the Net CA and management PC remain powered, reducing the risk of service impact.
A dashboard display of essential service parameters is provided, including a configurable sub-CA expiry warning, LDAP server availability, CRL validity, unprocessed certificate requests, etc.	This reduces the risk of missing service-critical events that could impact availability if left unattended.
Useful encryption service reports are available (e.g. certificates expiring in 'n' days).	This provides easy access to relevant reports without having to generate and parse complex custom reports from the Oracle back end.
A wizard guides the user through the keymat update process.	This enables customers to undertake keymat updates quickly and safely, without relying on assistance from AEP Networks.
Oracle has been replaced with XML-based data storage.	This reduces the risk of database corruption, and enables CA replication by simple file sharing.
Automatic and scheduled backups facilitate rapid recovery from a failure of the Net CA or management PC.	This significantly reduces the impact of hardware failure and removes reliance on assistance from AEP Networks.
Supports 64-bit operating systems natively.	This provides customers with increased flexibility.
Additional tools are provided for archive and backup management.	This enables off-line archive and historical data management, search and audit analysis.
It is more cost effective to deploy and support, particularly for smaller projects.	This provides a greater return for a lower investment.