

## EOL1007-NetJseries

This is an End of Life Notice concerning the "AEP Net ED20M J Series" encryptor and "AEP Net Keyper J Series" Hardware Security Module (HSM). Please review this notification in its entirety.

### "AEP Net ED20M J Series" encryptors, "AEP Net Keyper J Series" HSMs - End of Life Notice

AEP Networks is discontinuing support of "AEP Net ED20M J Series" encryptors and "AEP Net Keyper J Series" HSMs.

Since December 2000 the original AEP Net ED20M J Series encryptor has been securing Critical National Infrastructure to the Enhanced Grade, accredited through CESG Assisted Products Service (CAPS). The AEP Net platform remains unique to this day as the only such product with fully centralised 'over the air' Policy and Key Management. The AEP Net Keyper J Series HSMs play a key role in securing the standalone PKIs used to manage these systems.

However, these products have since been superseded by the AEP Net ED20M, ED100M, and Net CA HSM **E Series**, which offer enhanced capacity and functionality in a ROHS compliant platform, and so now at the end of its 'natural' ten year lifespan AEP Networks hereby provide notice that 31 Dec 2010 will be the last opportunity to renew support on the "AEP Net ED20M J Series" encryptors and "AEP Net Keyper J Series" HSMs, for up to 12 months (unless otherwise agreed).

Specific products affected	Products NOT affected
<u>Net ED20M</u> J series encryptor <ul style="list-style-type: none"> <li>J**** Serial numbers</li> </ul> <u>Net Keyper</u> J series HSM <ul style="list-style-type: none"> <li>J**** Serial numbers</li> </ul>	<u>Net ED20M</u> E series encryptor <ul style="list-style-type: none"> <li>E***** Serial numbers</li> </ul> <u>Net ED100M</u> E series encryptor <ul style="list-style-type: none"> <li>E***** Serial numbers</li> </ul> <u>Net Keyper</u> E series HSM <ul style="list-style-type: none"> <li>E***** Serial numbers</li> </ul> <u>Net CA</u> E Series HSM <ul style="list-style-type: none"> <li>E***** Serial numbers</li> </ul> <u>Net Remote</u> <ul style="list-style-type: none"> <li>All serial numbers</li> </ul>
J**** serial number format: J followed by four numbers: e.g. J1234, J0123, J9898, ..	E***** serial number format: E followed by seven numbers: e.g. E1234567, E7654321, E0987654, ..

### Customer Notes

AEP Networks or authorised AEP Networks partners will be contacting affected customers product to obtain acknowledgment of this notification, solicit a forecast for last-time support renewal and assist with selection of replacement products as required.

### Support

Customers with valid support contracts will continue to receive support until 31 Dec 2011.

### Affected Products: Last chance to purchase Hardware Maintenance and Support

Support	Notes	Last Order Date	End of Support
AEP Net ED20M J Series	Available until 31 Dec 2011	31 Dec 2010	31 Dec 2011
AEP Net Keyper J Series	Available until 31 Dec 2011	31 Dec 2010	31 Dec 2011

### Alternative Solutions from AEP Networks

AEP Net ED20M J Series encryptors can be replaced with AEP Net ED20M or ED100M E Series encryptors. Advantages of the E Series encryptor platform include:

- WAN interface operates at up to 100Mbps, with encrypted traffic throughput of over 160 Mbps full duplex (using 1,464 byte MTU)
- 0% packet loss during SA handover
- Supports connectivity from the award winning AEP Net Remote
- Twice the memory of the J Series
- Support for 2,000 Security Associations (compared with 1,000 of J Series)
- Support for twice as many static routes as J Series
- Support for Red default gateway

- Lead free in compliance with RoHS regulations implementing EU Directive 2002/95

The AEP Net Keyper J Series HSM is usually deployed as a component of the centralised AEP Net Management System (NMS). The NMS is provided as a bundle, with bundled support. Upgrade pricing to upgrade NMS deployments to the Net CA platform is available at a discount until 1<sup>st</sup> Sept 2010.

Advantages of the Net CA HSM (relative to the Unicert & Net Keyper HSM based CA) include:

Net CA Features	Benefits compared to Unicert & Net Keyper HSM based CA
Only CA accredited under CAPS	All CA's cryptographic functions performed in a dedicated tamper reactive module that is fully accredited to world-class standards
Batch certificate request processing compared to one at a time processing	Greatly reduces certificate management overhead, increasing the frequency with which this certificate renewals are performed, average duration of valid certificates and therefore increased encryption service availability
Two click certificate request processing compared to 19 clicks with multiple branching options per step	Reduced human errors. Increased encryption service availability
Mechanisms defending against incorrectly provisioned certificate policies	Reduces human error introduced by labour intensive monotonic tasks. Increased encryption service availability
Simple role based two factor authentication for high value transactions eliminates laborious six step authentication procedure to initialise CA functions with Unicert & Net Keyper HSM	Simplifies process to recover from power outage from a six page document to 'boot devices (optionally double-click two icons), done' .. Increased encryption service availability
Certificate Revocation List (CRL) generated automatically without requirement for smartcard based authentication, requiring just power to operate the NMS server and Net CA HSM	Increased encryption service availability
Heads up display of essential service parameters including subCA.crt expiry warning (configurable), LDAP server availability, CRL validity, unprocessed certificate requests, ..	Increased encryption service availability
Encryption service specific reports, e.g. certificates expiring in N days	Easy access to relevant reports without having to generate and parse complex custom reports from Oracle back end
Wizard guides user through Keymat update process	Process that would take AEP's most skilled engineers five hours on site work to inject new keymat has been performed by customer without AEP on site in under 10 minutes. Less costly support, less reliance on third parties. Increased encryption service availability
Oracle eliminated, replaced with XML based data storage	Database corruption events minimised, and CA data replication issues simplified to simple file sharing. Increased encryption service availability
Automatic and scheduled backups and advanced design facilitate recovery from either NMS server hardware Net CA HSM hardware in minutes	An order of magnitude easier to recover from otherwise severe failure events requiring on site support. Increased encryption service availability
Native support for 64-bit operating systems	Meets project demands for modern platforms
Additional tools for archive and backup management	Enabling offline archive and historical data management, search and audit analysis
More cost effective to deploy and support, with significantly lower price barriers for smaller scale projects	Higher returns on lower investment

If you have questions regarding this notification, please contact your AEP Networks account manager or e-mail [support@aepnetworks.com](mailto:support@aepnetworks.com)