



## Key business benefits

- Protects top-level cryptographic keys
- Supports over-the-air re-keying (OTAR)
- Enables closed user groups
- Provides certificate revocation capability
- Supports backup device for resilience
- Certified for UK/EU government use

## Applicable markets

- Governments: UK, EU and international
- Defence: UK MoD, NATO and international
- Intelligence and diplomatic services
- NGOs
- Critical national infrastructure
- Managed service providers
- Commercial enterprises

## Net CA Datasheet

The Net CA (Certification Authority) is a special-purpose HSM (hardware security module) that provides high-assurance digital signing and key storage mechanisms to support the centralised, PKI-based key management capability of the Ultra Electronics AEP Net encryption solution. It is designed to minimise the manual handling of private cryptographic keys and, importantly, eliminates the need for any key handling at the remote encryptors.

## Government Certification

The Net CA is certified by the UK Government's CAPS (CESG Assisted Products Service) up to Enhanced Grade level and approved by the EU Council to protect CONFIDENTIAL UE.



AEP



### Painless Key Management

Controlled via a simple, PC-based GUI (graphical user interface), Net CA enables CNOC (cryptographic network operations centre) staff to process key updates quickly and simply, enabling even the largest encryption systems to be centrally re-keyed in a matter of minutes. It also allows certificates to be revoked from the management centre, which means a lost or stolen encryptor can be rapidly and securely isolated from the network, without the requirement for a full system re-key that is incumbent on competing systems.

Net CA writes certificates and CRLs (certificate revocation lists) to an LDAP directory from where they are retrieved by the encryptors. This data is also recorded to enable the LDAP directory to be reconstructed or the Net CA to be replaced if required. An audit log of operator actions and cryptographic events is maintained within the Net CA's secure cryptographic kernel and can be interrogated by means of a GUI.

### Cryptographic Communities of Interest

Net CA also provides the tools for managing CCOI (cryptographic communities of interest) policies, which enable assured data separation between encryptors using a common management system. This is valuable for separating different user communities within an organisation, or for separating different customers when the encrypted network is operated by a managed service provider.

### Security features

- Dedicated application specific hardware platform with special-purpose embedded firmware
- High quality, hardware random number generator
- Continuous self-monitoring of cryptographic functions
- Sophisticated tamper protection
- Secure auditing and accounting functions
- Certified to UK CAPS Enhanced Grade standard
- Approved by the EU Council for CONFIDENTIEL UE
- Supports High Availability Net CA configurations that eliminate single points of HSM failure

### Better Availability Increases Security

The Net CA user interface includes a range of visual cues and easily accessible information to assist in the maintenance of an estate of managed certificates, making it simple to take the steps required and to avoid the pitfalls and service outages associated with expired certificates.

More effective key management is proven to lead to better encryption service availability and therefore to increased security.



## Net CA in operation

Net CA is installed at the Net Management System (NMS) for a Net encryption system. Whenever an encryptor is commissioned (and at key update intervals) certificate requests are received by the NMS for processing. Operations staff authorise the issuing of certificates using the GUI of the Net CA Control Tool utility, and these are automatically posted to the LDAP directory. Operations staff can revoke a certificate and manually publish a new CRL whenever required. In addition, CRL updates are automatically published at intervals determined by the user organisation's policy.

To perform manual actions, operations staff must first authenticate to the Net CA using a smart card token and PIN. There are two classes of operator: a standard operator, who is able to process certificate requests and revoke certificates, and an administrator, who can modify certificate policies, CCOIs and update the CA keys stored in the Net CA.

## Technical specifications

|                            |  |  |
|----------------------------|--|--|
| <b>Physical interfaces</b> | LAN  | 10/100 Mbps Ethernet   |
|                            | Serial Port  | V.24   |
| <b>Environmental</b>       | Temperature<br>Humidity  | Operating: 5 to 40°C / Storage: -15 to 65°C<br>25 - 90% (non-condensing) |
| <b>Physical dimensions</b> | Height   | 51 mm  |
|                            | Width  | 223 mm   |
|                            | Depth  | 244 mm   |
| <b>Weight</b>              | < 3kg (including power supply)   |  |
| <b>Power</b>               | External, universal in-line AC power supply<br>100 - 240V, 47 – 63 Hz, 42W maximum     |  |
| <b>Electrical safety</b>   | EN 60950-1, UL 60950, CSA 60950<br>CB Certificate (IEC 60950-1)                        |  |
| <b>EMC</b>                 | EN 55022 Class B, EN 55024<br>EN 61000-3-2, EN 61000-3-3<br>FCC CFR 47 Part 15 Class A |  |
| <b>MTBF</b>                | > 50,000 hours, based on British Telecom HRD5 standard                                 |  |

## Solution highlights

- Supports centralised management of very large encrypted communities
- Enables OTAR (over-the-air re-keying) to eliminate key handling at remote encryptors
- Bulk key signing achieved with simple “select and click” operation
- Advanced CCOI capability
- Certificate revocation allows lost or compromised encryptors to be cryptographically isolated from the network
- Temporary loss of Net CA function does not prevent normal network operation
- Alternate Net CA option for business continuity / disaster recovery scenarios
- Local HSM resilience option supports high HSM availability in the event of unit failure
- Operational management uses a standard Windows Server

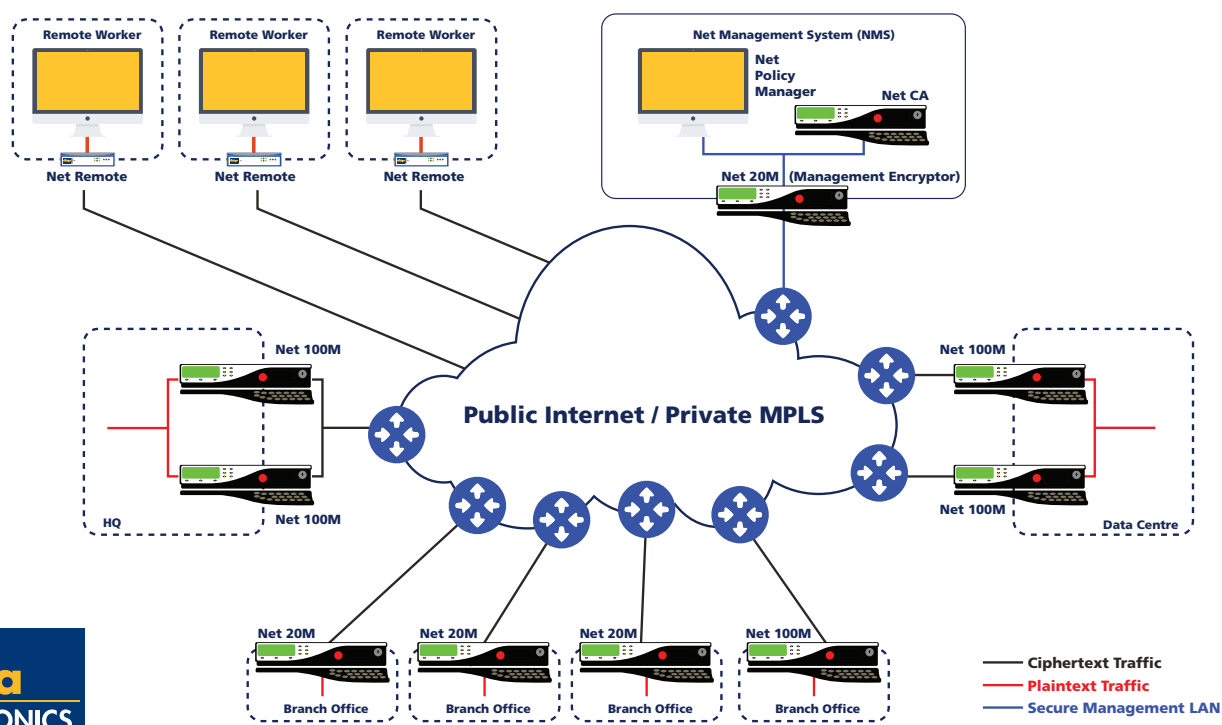
## Solution summary

The Ultra Encrypt line of products comprises:

- Net 100M and Net 20M encryptors
- Net Remote encryptor
- Net Management System (incorporating Net CA and Net Policy Manager)

AEP also offers a range of off-the-shelf and bespoke deployable secure communications solutions as well as comprehensive professional services and support capabilities.

## Ultra Encrypt - Typical Net Architecture



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](mailto:info@ultra-aep.com)  
[www.ultra-aep.com](http://www.ultra-aep.com)  
[www.ultra-electronics.com](http://www.ultra-electronics.com)

