



Packet Clearing House
572 B Ruger Street, Box 29920
The Presidio of San Francisco
San Francisco, California
9 4 1 2 9 - 0 9 2 0 U S A
+1 415 831 3100 main
+1 415 831 3101 fax

CONVEYANCE LETTER

Saturday, October 1, 2016

To whom it may concern:

The device being transported in this case (Pelican 1490, PCH property tag 1508) contains a backup of sensitive security information. It is being transported on United Airlines flight 869, departing San Francisco on Saturday, October 1, 2016, arriving Hong Kong on Sunday, October 2, and United Airlines flight 895, departing Hong Kong on Sunday, October 2, arriving Singapore on the same day. It is being transported by Mr. William Edward Woodcock IV, a director of Packet Clearing House. Mr. Woodcock was born August 16, 1971, and travels on U.S. passport 464406862, issued November 5, 2009.

The device was manufactured in the United Kingdom, and is not subject to United States export control. Specification sheets and original bill-of-sale are attached to this letter.

This case, and the device, may be X-rayed without harm.


Anyone requiring this briefcase to be opened must produce government-issued identification and must complete and sign an entry on the enclosed Safe Log, stating the reason the briefcase has been opened, the date and time, and confirming that they have not tampered with the contents. This entry must be countersigned by Mr. Woodcock.

In the extremely unlikely event that it should prove necessary to open the tamper-evident bag that encloses the device, continuous video recording is required from before the bag is opened until the device is re-sealed in a new tamper-evident bag. Anyone who touches the device, and their supervising officer, must show government-issued identification, must sign the attached exception sheet, noting the serial number of the device (H1411033), the prior tamper-evident bag number (A4128466), and the new tamper-evident bag number, and must sign an affidavit stating their reason for having handled the device. Under no circumstances may the device leave the direct observation and supervision of Mr. Woodcock. Any attempt to tamper with the device will cause it to erase the contents of its memory, rendering it useless and initiating an investigation.



Thank you in advance for your full cooperation,

A handwritten signature in blue ink, appearing to read 'P. Rowland', is written over the typed name.


Peter Rowland
Logistics Officer

115	CA deletes the files on the SCRIPTS FD and unmounts by executing: <pre>rm -rf /media/SCRIPTS/*</pre> <pre>umount /media/SCRIPTS</pre> and removes the SCRIPTS FD for reuse.		03:01
-----	--	--	-------

Return KSK-HSM-02-BRK HSM to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
116	CA presses the RESTART button on the HSM and waits for the self-test to complete. CA then disconnects the HSM from power and laptop (serial and Ethernet), placing the HSM into a new TEB and sealing it.		03:05
117	CA reads out TEB number and HSM serial number and allows participants to verify them while the EW records the TEB and HSM serial numbers here: TEB# <u>A4128467</u> HSM Serial#: <u>H1411035</u>		03:07

Return Other HSMs to a Tamper Evident Bag

Step	Activity	Initial	Time (UTC)
118	CA reads out the 3 TEB numbers and 3 HSM serial numbers and allows participants to verify them while the EW records the TEBs and HSM serial numbers here: KSK-HSM-02-SIN TEB# <u>A4128466</u> KSK-HSM-02-SIN HSM Serial#: <u>H1411033</u> ZSK-HSM-02-SJC TEB# <u>A4128464</u> ZSK-HSM-02-SJC HSM Serial#: <u>H1412044</u> ZSK-HSM-02-ZRH TEB# <u>A4128465</u> ZSK-HSM-02-ZRH HSM Serial#: <u>H1411034</u> CA ensures these 3 HSMs leave the CA to be delivered to their appropriate destinations.		03:12

Quotation To:
 BILL WOODCOCK
 PACKET CLEARING HOUSE INC
 1600 SHATTUCK AVE STE212
 BERKELEY CALIFORNIA 94709
 United Kingdom

Phone: 01889 271777
 Email:



Quote 10102
 Quote Date: 13/05/2016
 Quote Expires: 23/05/2016

Sales Person: Daryl Hyett

Quotation

Ultra Electronics Ltd - AEP
 419 Bridport Road
 Greenford Middlesex UB6 8UA
 United Kingdom

Phone: +44 (0) 208 813 4567
 Fax: +44 (0) 208 813 4568
 Email: customerorders@ultra-aep.com

Page 1 of 1

<u>Line</u>	<u>Part Number</u>	<u>Description</u>	<u>Quantity</u>	<u>Unit Price</u>	<u>Total Price</u>
1	AEP-KEY-PLS-10	KeyperPlus 10 (10 key licence with ECC)	5.00	EA 8,830.00	44,150.00
2	AEP-Delivery	Delivery Charge	1.00	EA 650.00	650.00

USD

Quotation Total: .USD 44,800.00

Payment Terms:30DY
 VAT will be applied at the appropriate rate :
 Subject to the terms of our Sales Contract exclusive of all other agreements or obligations
 Licence and maintenance charges to be paid annually in advance
 Subject to Ultra Electronics Ltd - AEP Standard Terms and Conditions
 E&OE



Packet Clearing House
572B Ruger Street, Box 29920
The Presidio of San Francisco
San Francisco, California
9 4 1 2 9 - 0 9 2 0 U S A
+1 415 831 3100 main
+1 415 831 3101 fax

Purchase Order

PO#: PCH_AEP_2016_1

Friday, May 13, 2016

Vendor:

Ultra Electronics Ltd - AEP
419 Bridport Road
Greenford Middlesex UB6 8UA United Kingdom
customerorders@ultra-aep.com

Line	Description	Total
1	5 KeyperPlus units plus shipping. AEP Quote 10102	\$44,800.00
TOTAL:		\$44,800.00

Ship To:

Packet Clearing House
attn: Peter Rowland
1600 Shattuck Ave. #212
Berkeley, CA 94709
United States

Bill To:

Packet Clearing House
1600 Shattuck Ave. #212
Berkeley, CA 94709
United States
accounting@pch.net

Peter Rowland
Business Manager



From: **Peter Clements** Peter.Clements@ultra-cis.com
Subject: FW: Payment Request from ULTRA ELECTRONICS LIMITED t/as Ultra electronics CIS
Date: June 6, 2016 at 7:51 AM
To: peter@pch.net
Cc: Daryl Hyett Daryl.Hyett@ULTRA-AEP.COM, Ges Muir Ges.Muir@ultra-cis.com

PC

Dear Peter,

As requested please find details of your order listed below, if you have any questions please don't hesitate to contact me;

Your order has been dispatched please see details below:

Date	27/05/16
Customer PO#	PCH_AEP_2016_1
AEP Ref#	850671
Courier Used	Fedex
AWB/Tracking #	776388441230
Product Type	KEY-PLUS

Serial Number	Tamper Bag Ref
H1406001	PS417130
H1411033	PS417132
H1411034	PS417129
H1411035	PS417133
H1412044	PS417131

Upon receipt please check that the serial number and tamper evident bag number match the details above. If they do not it could indicate the goods have tampered with. If you believe the goods have been tampered with during transit please contact AEP Immediately at customerorders@ultra-aep.com

Best Regards,

Peter Clements
Head of Compliance

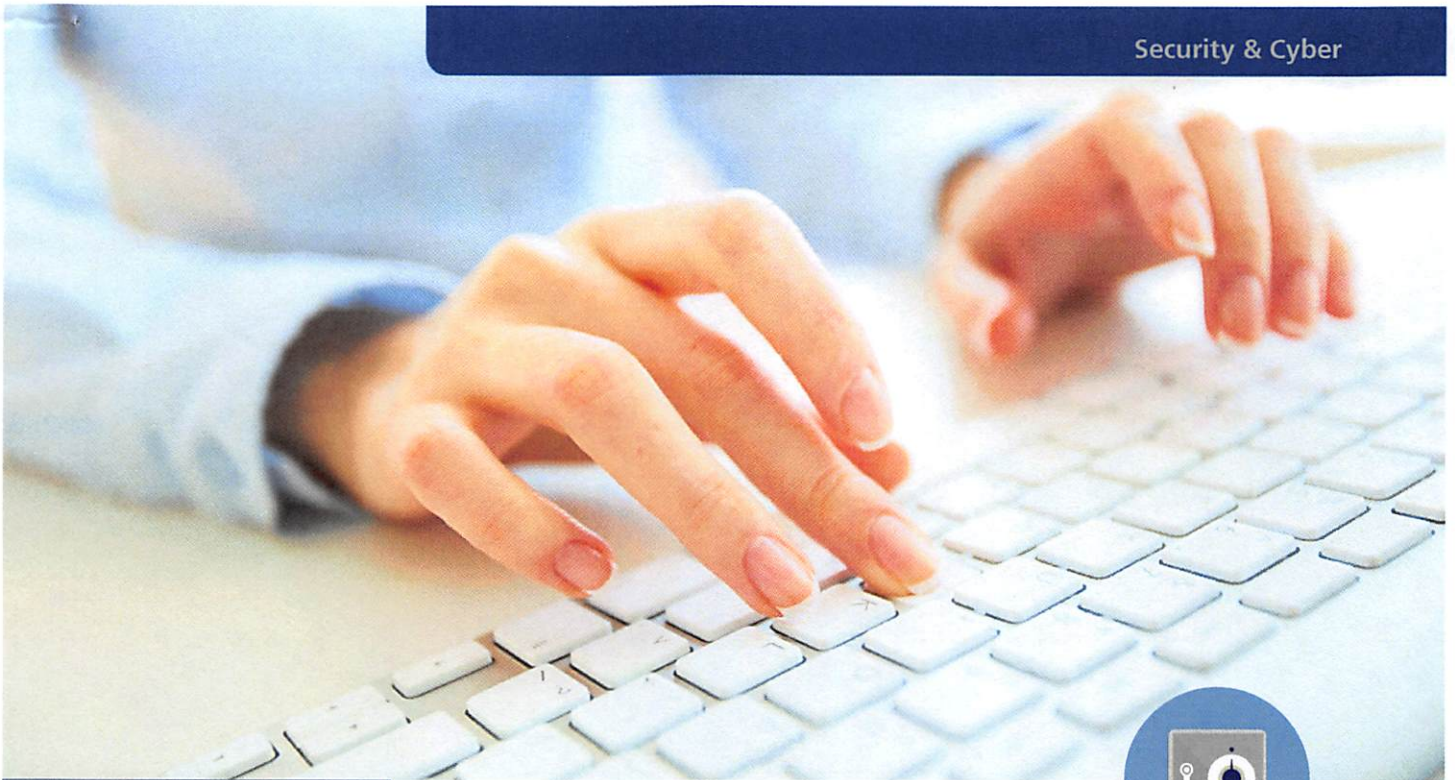
Ultra Electronics
COMMUNICATION & INTEGRATED SYSTEMS
419 Bridport Road, Greenford
Middlesex, UB6 8UA, United Kingdom

peter.clements@ultra-cis.com

Tel: +44 (0) 208 813 4701

Mob: +44 (0) 7799 894462

www.ultra-cis.com



Key business benefits

- Assurance - the only stand-alone FIPS 140-2 Level 4 HSM
- Capability - broad range of algorithms including AES, ECDSA
- Compatibility - supports numerous third-party security applications, operating systems
- Scalability - load-sharing across multiple devices
- Reliability - resilience and disaster recovery configurations
- Pedigree - long history of use in blue chip companies

Applicable markets

- Enterprise PKI, Authentication & VPN
- Registration, certification & validation authorities
- Digital Signature - Email, Doc, Code (Software), Firmware
- Internet domain name organisations, DNSSEC
- Online content providers
- Electronic gaming companies

Keyper™ HSM Datasheet

Where cryptographic services are used to protect an information system, trust and integrity are derived from the security of the underlying signing and encryption keys. This makes protection of these keys critical to the overall trust and integrity of a system.

Cryptographic key material can be stored and protected in a variety of ways and on a variety of media including software, smart cards and USB tokens. However, where protection is critical, the level of security offered by these solutions may not always be enough.

Storing and protecting key material on a physically separate Hardware Security Module (HSM) is the only viable option, making the HSM a critical element in the architecture of any security system.

Choosing the right HSM

In choosing a HSM, a range of options need to be considered:

- What connectivity does the HSM offer?
- What key storage capability does the HSM offer?
- What tamper detection does it provide?
- How many hosts can be connected to a single HSM?
- Can the HSM be upgraded at a future point without requiring a return to the manufacturer?

Keyper: The ultimate protection of key material

Ultra Electronics AEP has designed the Keyper range of HSMs to provide the ultimate level of protection for the most sensitive data and information systems. At the heart of Keyper is AEP's revolutionary ACCE technology.

ACCE is the next generation flexible crypto platform that provides the highest level of assurance – FIPS 140-2, Level 4. Based on this core technology, AEP has built a product range to cater to the PKI, VPN and Internet security markets. The Keyper HSM is ideally suited to businesses deploying a cryptographic system where the protection of cryptographic keys is a priority, for example, in organizations requiring certificate signing, code or document signing, bulk generation or ciphering of keys or data.

The Keyper HSM is available in three models offering various levels of scale and performance:

- Keyper Professional
- Keyper Enterprise
- Keyper ^{Plus}

Keyper Features and Benefits

- Architecture - Built using ACCE giving tamper protection to FIPS 140-2 Level 4
- Design - Integrated smart card reader, PIN entry and cryptographic processing
- Fault Tolerance - Supports resilient configurations
- Scalability - Load balancing of multiple HSMs across multiple hosts
- Choice of Interfaces - PKCS#11, Microsoft CAPI, Java JCE/JCA
- Connectivity - Ethernet connectivity offering greater scalability and flexibility
- Manageability - Small footprint allows desktop use or rack mounting
- Field Upgradable – Upgrade firmware and algorithms in the field
- Authenticated Use of Keys - Optionally PIN activated
- Operating Systems - Linux, Free BSD, Solaris and Windows



"Security is a critical factor for ICANN's DNSSEC deployment, AEP's Keyper HSM & FIPS Level 4 was an easy choice"

Richard Lamb, ICANN

AEP



Technical Specifications

	Keyper Professional Keyper Enterprise	Keyper ^{Plus}
Product Dimensions	223 x 51 x 244 mm	
Power Requirements	100 – 240VAC, 47-63 Hz (42VA)	100 – 240VAC, 47-63 Hz (65VA)
Cryptographic Functions and Services	<ul style="list-style-type: none"> • RSA: 1024-4096 bit key length • DSA: 1024 bit key modulus • AES: 128-256 bit key length • DES/3DES: 112/168 bit key length • Hash: SHA-1, SHA-2, MD5 	<ul style="list-style-type: none"> • ECDSA curves: <ul style="list-style-type: none"> • P192 – P521 • brainpoolP224r1 - P512r1* • brainpoolP224t1- P512t1* • secp256k1* • ECDH curves: <ul style="list-style-type: none"> • P192 – P521 • brainpoolP224r1 - P512r1* • brainpoolP224t1- P512t1* • RSA: 1024 - 4096 bit key length • DSA: 1024 bit key modulus • AES: 128 - 256 bit key length • 3DES: 168 bit key length • SEED*: 128 bit key length • Hash: SHA-2, RIPEMD-160* <p>*In Beta, full release in Firmware Version 3</p>
Performance (key signing, using up to 8 connections)	<ul style="list-style-type: none"> • Keyper Professional: 300 tps (RSA 1024) • Keyper Enterprise: 1,200 tps (RSA 1024) 	<ul style="list-style-type: none"> • >3,500 tps (RSA 1024) • >2,000 tps (RSA 2048) • >950 tps (ECDSA 256)
Random Number Generation	Hardware random number generator with full entropy (FIPS 186-2 compliant)	
Administrator Roles	<ul style="list-style-type: none"> • Security Officer • Operator 	<ul style="list-style-type: none"> • Security Officer • Crypto Officer • Operator
Key Management	<ul style="list-style-type: none"> • Storage Master Key (SMK) import/export via smart cards in M of N components • Application Key import/export via smart cards protected with an internal Master Key (also via USB on Keyper^{Plus}) 	
Key Protection	<ul style="list-style-type: none"> • Red Key Store: keys actively erased when a tamper is detected • Black Key Store: large key store encrypted under the SMK 	
Key Storage	<ul style="list-style-type: none"> • 9,000 keys (RSA 1024) 	<ul style="list-style-type: none"> • 15,000 keys (any size)
Connectivity	<ul style="list-style-type: none"> • TCP/IPv4 over Ethernet at 10/100 Mbps full/half duplex with auto-negotiation • Up to 32 concurrent connections 	<ul style="list-style-type: none"> • TCP/IPv4 and IPv6 over Ethernet at 10/100/1000 Mbps full/half duplex with auto-negotiation • Up to 256 concurrent connections
Certification	<ul style="list-style-type: none"> • FIPS 140-2 Level 4 (cert. #1340) • Common Criteria EAL4+ 	<ul style="list-style-type: none"> • FIPS 140-2 Level 4
Operating Environment	<ul style="list-style-type: none"> • Operating temp: 5 to 40 °C (25 to 90% humidity, non-condensing) • Storage temp: -15 to 65 °C 	
Host Software	<ul style="list-style-type: none"> • Keyper Management Centre • PKCS#11 Provider • MS-CAPI Provider • MS-CNG Provider • Load Balancer (optional) 	

Ordering Information

Product	Ordering Part Number
Keyper Professional	KEY-PRO
Keyper Enterprise	KEY-ENT
Keyper ^{Plus}	KEY-PLS
Keyper ^{Plus} 10 Key Licence ¹	KEY-PLS-10
Keyper ^{Plus} Without ECC ²	KEY-PLS-NE

¹ Licensed for applications requiring a maximum of 10 private keys

² ECDSA and ECDH algorithms not available (can be subsequently soft-upgraded via license key)



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

