Company Background

- Founded: 1998
- Employees: 62
- The marriage of two companies:
  - Baltimore Technologies Hardware Group (Zergo) (Security)
  - AEP Systems (SSL Acceleration)
- Headquarters: Dublin, Ireland. US Headquarters: Boston, MA
- Sensitive Crypto Products Developed in the UK at a government cleared secure facility
- Regional Offices: Hong Kong, Palo Alto & UK
- Core Intellectual Property: Evolved from experience in cryptographic accelerator and hardware security technology
Mission Statement

To deliver hardware security and acceleration solutions that are fast and cost-effective to deploy
AEP SureWare Range
PK Enabling Products

- **AEP SureWare Keyper**
  Hardware security modules that offer security and performance for protected key storage, high-speed signature and hardware key generation

- **AEP SureWare A-Gate: AG-50**
  SSL VPN hardware appliances that provide secure and authenticated access from any Internet browser to internal applications

- **AEP SureWare Net: Net ED20M, Net EC20M**
  High security VPN encryptors that protect IP traffic across WAN & LAN networks

- **AEP SureWare Runner: Runner 1000 / 2000 / S1000**
  Acceleration hardware that off-loads compute-intensive cryptographic functions from a server
Customers
AEP-SureWare Keyper

- **AEP-SureWare Keyper Professional**
  - Network attached
  - FIPS 140-1 level 4
  - ITSEC E3
  - PKI applications such as Baltimore UniCERT, MS Certification Services, ValiCERT OCSP, Kyperpass OCSP, Netscape CA, RSA CA
  - General crypto applications via industry standard PKCS#11, MS CSP or JCE (Java) interfaces

- **AEP-SureWare Keyper PCI**
  - PCI card
  - FIPS 140-1 level 3
  - PCI variant of Professional
  - PCI card removal detection
AEP-SureWare Certification / Tamper Detection

- **FIPS 140-1 L4**
  - Mesh: penetration attack
  - Power detection
  - Temperature outside 0 to 45 degrees C

- **FIPS 140-1 L3**
  - No mesh: potted or enclosure removal detection
  - Power detection
  - Temperature outside 0 to 45 degrees C
AEP-SureWare Keyper Features

- **Standard crypto facilities**
  - Sign/verify
  - Key wrap/unwrap (can be securely switched on/off)
  - Bulk encrypt/decrypt/MAC/verify
  - 512 to 2048 bit RSA, 56 to 168 bit DES, DSA, DH
  - Key policy determines key use
  - Hardware random number generator – full entropy
  - SHA-1/MD-5

- **Key Store**
  - 500 2048 bit or 1,000 1024 bit RSA keys

- **Performance**
  - 150 1024 bit RSA signs/sec

- **Authorized key backup/restore**

- **Security Officer ‘user’ groups**

- **Up to 16 balanced by load**

- **Fault tolerant/peak load SCALEABLE (with AEP-SureWare Load Balancer)**

- **Secure firmware update**
AEP-SureWare Keyper Professional Application Support

- UniCERT
- KeyTools/Java/C++
- PKCS#11 Adapter
- AEP-SureWare Load Balancer
- AEP-SureWare Keyper Pro v2.2
- Customer app
- Microsoft CS
- RSA Full Provider

AEPsystems
AEP-SureWare Keyper Professional Platforms

- **Sun Solaris (on SPARC)**
  - v2.6 (32 bit)
  - V2.7 (unofficial, customers do use with this successfully)
  - v8 (32 and 64 bit)
  - V9 (planned)

- **Hewlett-Packard (on PA-RISC)**
  - HP-UX v11 (32 and 64 bit)

- **Microsoft Windows (on Intel)**
  - NT4 (On Intel)
  - 2000
  - XP Pro (32 bit)
  - .Net Server (32 bit)

- **Java**
  - Solaris (32 bit) & Windows (32 bit) with Baltimore’s KeyTools product
AEP-SureWare Keyper Professional Hardware

- 2x16 LCD
- Ready, alert, LAN LEDs
- ISO 7816 smart card reader
- Restart button
- Fold up keypad
- Key switch
- Erase key button
- V24 compatible diagnostics port
- 10/100 FD/HD ethernet
- FIPS 140-1 L4 ACCE module inside

*10 yr battery life
*External PSU
*Rack mount option
AEP-SureWare Keyper Professional Deployment

CA 1
Solaris

RA
Win XP

ARM
Win 2000

CA 2
HP-UX

Local private network

AEP-SureWare Keyper Pro
AEP-SureWare Keyper Pro
AEP-SureWare Keyper PCI

2x16 LCD

ISO 7816 smart card reader

Keypad

FIPS 140-1 L3 ACCE module

*10 yr battery life
AEP-SureWare Keyper PCI Deployment
Why AEP SureWare Keyper?

- The only FIPS 140-1 Level 4 HSM
- Proven track record with over 1,000 network installations
- Support for industry leading applications
- Support for Solaris & Windows, PKCS#11, MicroSoft CAPI, and Java JCE
- Secure key storage, back-up, and recovery
- Hot removal, scalable up to 16 boxes
- Fault tolerant and load balancing
AEP SureWare Net

- High security product targeted at Public Sector SBU and high value Finance industry solutions
- Purpose-designed to meet stringent Government security standards
- Purpose-designed to meet Managed Service Providers’ requirements
- Network integration and central management functionality designed to minimise implementation and running costs
AEP SureWare Net VPN Encryption

Network Security Gateway Encryption

- Fully Managed IP encryption
- Full PKI Key Management
- Separate Network Management
- IPSEC ESP Tunnelling
- Ethernet Full Wire Rate Performance
Key Features

- **Key Management**
  - On-Line CA
  - Encryptor generated Public/Private key pairs
  - Encryptor generated traffic keys

- **Security Policy Implementation and Enforcement**
  - Certificates
  - Certificate Revocation
  - Encryption network configuration
  - Encryptor configuration

- **Algorithms can be updated**

- **Subnet Support**
  - Up to 10 sub-nets per encryptor

- **QoS enabled**

- **NAT, SNMP, DHCP**
  - Network protocol support

---

**Value Added Functionality:**
- Independently assured defence against active network attacks
  - Aggressive payload, trojan horse, spoofing, replay, man-in-the-middle
  - Defence against availability attacks
  - Resistant to swamping
  - Control of end-user network access capability

---

**Formal Approvals:**
- CAPS*
- ITSEC E3
- DIPCOG**
- Crypto kernel assessed to FIPS 140-1(4)
- EU Council of Ministers assessment
- European Commission assessment

---

*UK Government Approval Scheme
**UK Ministry of Defence Approval Scheme
AEP SureWare Net Users

- Defence Departments
- Defence Industry
- National and International Government
- National and International Criminal Justice Agencies

- Reference sites:
  - 2 UK National Criminal Justice Networks
  - Pan European Criminal Justice Network
  - Pan European Diplomatic Network
  - Pan European Government Infrastructure Network
The Security Pyramid

Classified

Confidentiality

Integrity

Commercial / Sensitive But Unclassified / FIPS / ITSEC / Common Criteria

Commercial

AEPSureWare Net ED20M

AEP SureWare Net EC20M

AEP SureWare Net CD20M
AEP SureWare Net for the US Market

- Established high-security encryption system designed and built in the United Kingdom
- Deployed on Classified and SBU systems in Europe
- New type of COTS Product
- Purpose built to meet government standards
- AEP Systems commitment to FIPS
  - one of only 3 manufacturers to have a Level 4 certified product
AEP SureWare A-Gate

- **Secure SSL VPN Appliance**
  Next generation security appliance for secure remote access

- **Authenticated Access**
  Provides secure and authenticated access between internal Web/RDP servers and Web browsers

- **Industry Protocols**
  Encrypts communications using SSL

- **Simplified Usage**
  Easier to use and set up than a traditional VPN

- **Flexible Deployment**
  Supports more user access scenarios
Save Time & Money

- Simplifies usage & deployment of secure remote access
  - Allows authorized out-of-office staff to connect to corporate resources securely from anywhere at anytime
  - Enables secure partner access with no impact or access requirements on partner systems

- Reduces IT spend
  - Reduces deployment time and management overhead typically associated with traditional VPNs
  - Negates floating laptop requirement for occasional travellers
Benefits and ROI

- **Lower TCO than traditional IPsec VPN**
  - 40% savings over IPsec VPN in year 1
  - 30% savings over IPsec VPN in subsequent years

- **Reduced hardware costs**
  - No need for floating laptops for occasional travelers
    - Typical SME would have 5-10 spares
  - Light users (e.g. e-mail only) can operate without laptops

- **Rapid Deployment**
  - Notify user of URL
  - Use existing enterprise authentication schemes
  - Avoid costs of retrofitting systems to support secure access

*Produced by the Yankee Group
http://www.yankeegroup.com
SureWare A-Gate as a PK Enabler

- Provides secure authenticated access to corporate resources from anywhere
- Minimal administration required to configure and deploy secure remote access
- Routine maintenance can be carried out remotely
- One-time cost. No further investment needed post-deployment
- Integrates with existing network and PKI systems
- Extend enterprise applications to employees, business partners and customers
SureWare Runner

- An SSL accelerator used to offload the processing of secure transactions from a server or appliance

- Why?
  - Because SSL processing is CPU intensive
  - Servers providing SSL connections spend over 90% of their processor time handling cryptography (source: RSA)
What Does AEP SureWare Runner do?

- Reduces IT spend
  - Less servers needed to process SSL
  - Smaller data center
- Improves customer response time
  - Increases the processing time for SSL
- Delivers more CPU resource to applications
Benefits

- Easy-to-deploy
- Offers good price performance
- Extensive OS & API support
- Multiple form factors
- HP and Microsoft ‘Designed for Windows’ certified
Return on Investment

- Reduces IT Spend
  - Improved ROI from existing hardware

- Alleviates server bottlenecks
  - Better server response times
  - Better customer experience

- Allows more applications to be delivered to the Web eg Microsoft .Net

- Plug & Play solution that is easy-to-deploy

- Extensive OS, API & form factors supported
Form Factors

AEP SureWare Runner PMC

AEP SureWare Runner IDE

AEP SureWare Runner PCI

AEP SureWare Runner S1000
AEP Systems
Product & Technology  Differentiators

- **Full hardware security product capability:**
  - Complete product design / development (hardware and software)
  - ASICs to appliances
  - Boards to high-security HSMs

- **High-speed, high-security products:**
  - SureWare Keyper speed up to 2000 TPS
  - SureWare Net at full wire rate
  - FIPS 140-1(2) Level 4 / ITSEC / CC capability

- **Secure appliances:**
  - Ability to deliver accredited appliances
High-Speed Security Solutions