The global leader in cryptographic key management.
Chrysalis-ITS
The World’s Most Trusted Hardware Security Products

- Thousands of systems worldwide since 1994
- The only hardware security vendor in the world to achieve both FIPS and Common Criteria certification
- Trusted by over 200 blue chip customers in 50+ countries
- Used by 84% of Fortune 500 deploying PKI

Salomon Smith Barney, Fortune 500 CIO Survey, August 2000
Chrysalis US Gov. Installations

- DISA
- Federal Bridge
- DOD PKI
- Dept. of Labor
- D.I.A.
- Dept of Treasury
- U.S. Border Patrol
- NASA
- Dept. of Agriculture

- Dept. of Energy
- Bureau of Public Debt
- DMDC
- State Dept.
- Various Intel Agencies
- DEA
- FDA
- Patent & Trade
- Federal Reserve
Chrysalis-ITS Security Hardware

Hardware solutions for securing:

- Identities
- Communications
- Data
- Transactions
Chrysalis-ITS Advantage:

3 Layers of Security

1. 3DES Key Encryption

2. “M of N” Access Control

3. Tamper Proof Hardware

Private keys are never stored on an unsecured hard disk!
A Challenge

- HSMs and cryptography are essential for securing online transactions and access to sensitive information.
- Traditional HSMs are cumbersome and expensive to deploy:
  - Require servers to be shutdown and opened for hardware installation
  - Require one HSM per server

Chrysalis Goal
Make HSMs more easily deployable and widely applicable

Solution
Transform HSMs into a shareable service deployed over the network
Product Positioning

- Luna CA³ is a root key management HSM
- Luna SA delivers a network-based HSM sharable by multiple servers
- Axenta is an appliance that securely runs applications and is built on the Luna SA platform
Chrysalis Secure Appliance Technology

Hardware Security
- Hardened packaging
- Tamper detection
- FIPS validation

Software Security
- Hardened OS
- Secure boot
- PKI signed code

Operational Security
- 2-factor authentication
- Multi-person authorization
- Digitally-signed logs
The K3
Chrysalis Cryptographic Engine

- Latest Chrysalis cryptographic processor
- 1200 RSA 1024 signings per second
- Being validated to FIPS 140-2 Level 3
- New features
- More code and key storage
- More algorithms: AES, SHA-2, E-Sign …
- Improved security design
Harnessing K3’s Capabilities

Build a secure server around the K3 to allow it to be securely shared across a network.
Luna SA - HSM Server

- Administration
  - SSH, SNMP*
- Network Trust Link Service (NTLS)
- Backup
- Independent HSM Partitions
- Internal K3 HSM
- PED
- Luna CA³ Compatibility

* October 2002
Network Trust Links

Transport Crypto API securely over the network

- Crypto keys remain in the HSM--only the API is transported (PKCS #11, CAPI, OpenSSL)
- Highly portable to any platform that supports TCP/IP

1. IP address
2. SSL
3. Digital certificates for server & client
4. Process-level password

Network Trust Link
High Availability & Load Sharing

HSM server requests are cycled between active units

- Increase availability, performance, disaster recovery
- Luna SA’s can be located anywhere on the network
Summary

Luna SA is a breakthrough HSM product that fundamentally changes the deployment model for HSMs

- Lower Total Cost of Ownership
  - HSM sharing lowers capital costs
  - Fewer boxes to own, install and manage
  - Increased performance is a software upgrade
- HSM functionality deployed as a service over the network
- Fully compatible with current Luna HSM family
- Application programmable via upgrade to Axenta