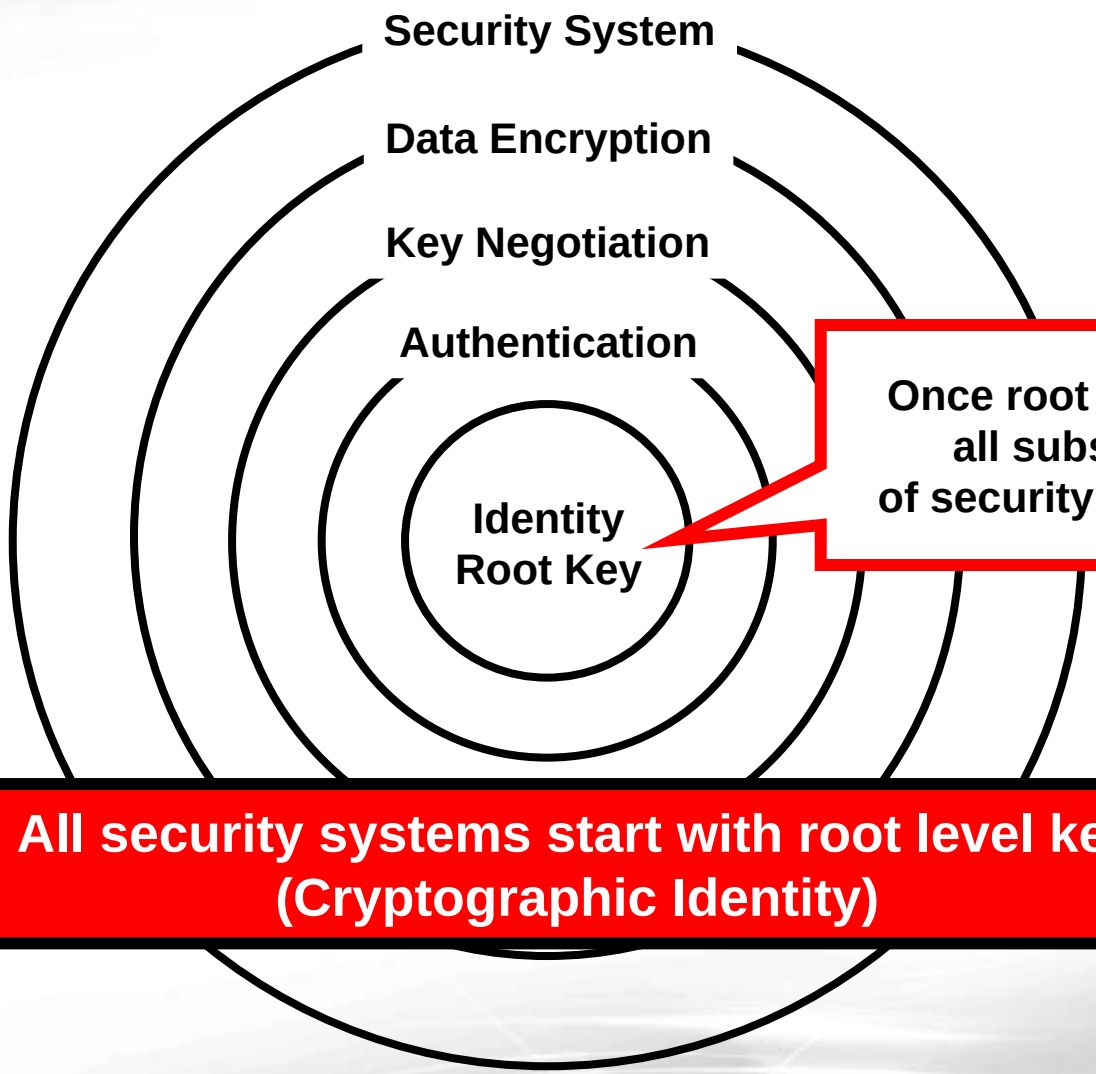

# Using BroadSAFE™ Technology

07/18/05

# Layers of a Security System




Once root is compromised, all subsequent layers of security are compromised

**All security systems start with root level key (Cryptographic Identity)**

BROADCOM.
Connecting everything®

# Deployment of Technology

- Stateless Key Management Client (μHSM)
  - Standalone for “strong device authentication”
  - Network connected devices
  - Key Management flexibility with low system cost impact
  - Client / Server Key Management Model
- Trusted Platform Module (TPM)
  - Standalone key management capability (peer to peer)
  - Standards based solution
  - Larger silicon footprint

BROADCOM.
Connecting everything®

# BroadSAFE Security

- BroadSAFE Hardware Security Technology
  - Tamper resistant hardware for key storage
  - Standard CMOS processing provides integration capability
  - Private key generation internal to device (internal True Random Number Generator)
- Deployed Now
  - Existing switching products
  - Existing networking VoIP Devices
  - Interoperates with TPM architecture (v1.1b and v1.2)
- BroadSAFE Flexibility
  - Interoperable with security standards (IPsec, SSL, TLS, SRTP, SIP, 802.1x, etc.)
  - Open / Standards Based Key Management Interface
  - Capability to provide custom based solutions

BROADCOM.
Connecting everything®

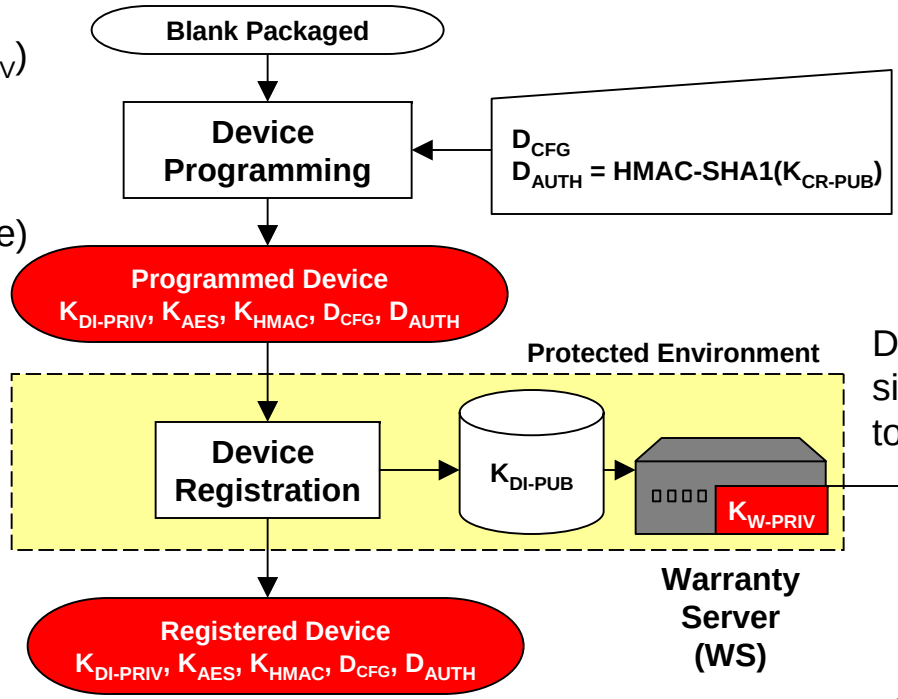
# Unique DSA Key Pair

- DSA Key Generation
  - Simple key generation based on internal generated random number
  - 160 bit key is random number processed per FIPS186-2
  - Unique per device
  - Key generation time in uSec versus several minutes for RSA of equivalent strength
  - Modulus and Generator values can be well known (stored in ROM versus NVM)
  - NVM requirements ONLY 160 bits for DSA Key
- DSA Key Pair Creation
  - Done during device manufacture
    - No programming required at OEM or end user
  - Certificate can be issued to travel with device
    - Public value can be stored outside the security boundary
  - Private key is only used to sign data within hardware security boundary
  - Private key is never exposed

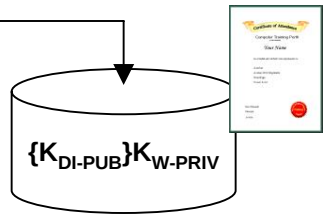
BROADCOM.
Connecting everything®

# Manufacturing Flow

DSA Private key ($K_{DI-PRIV}$) generated in protected security hardware (never exposed, unknown to manufacture)



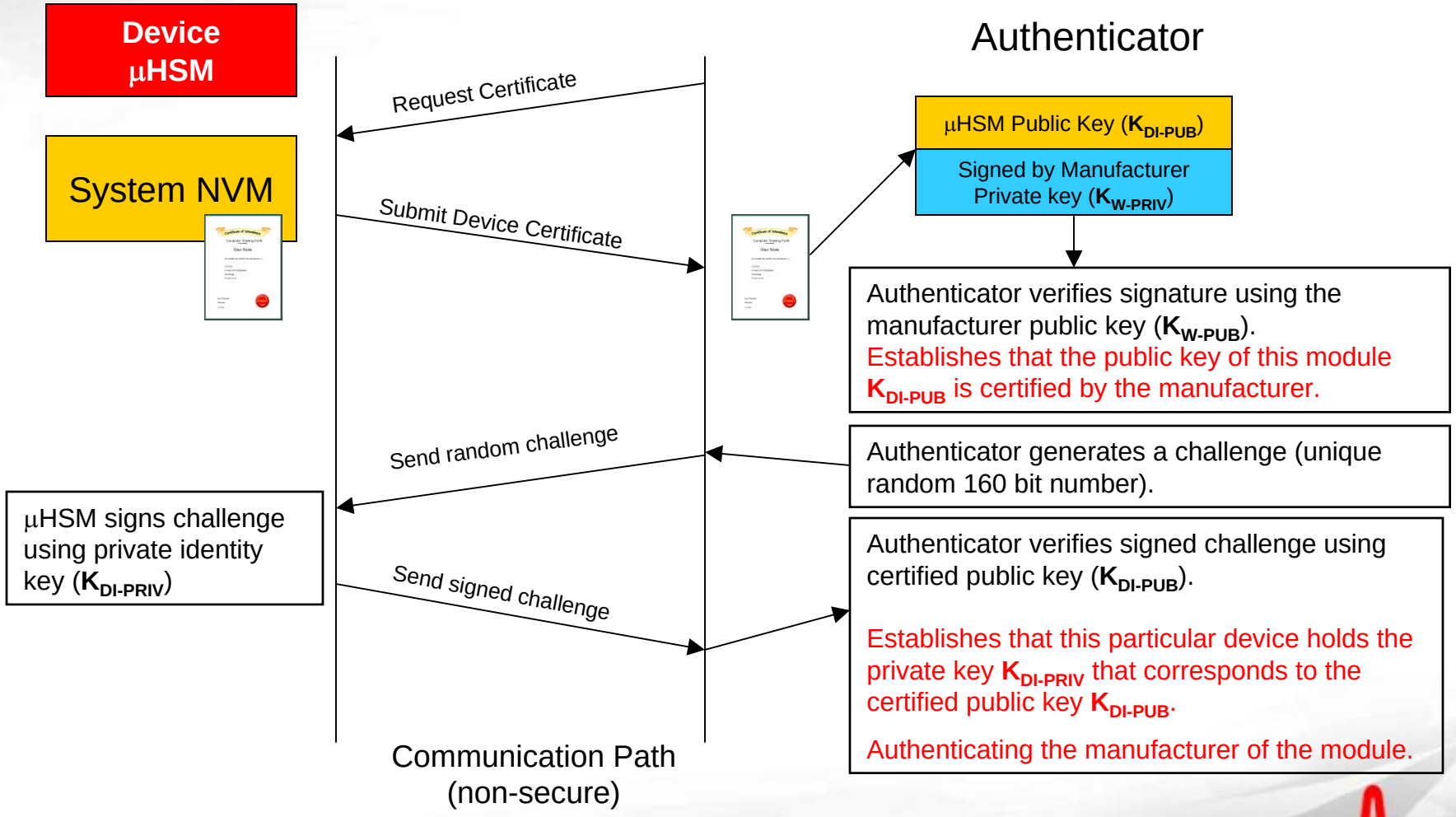

DSA Public Key ($K_{DI-PUB}$) signed by manufacturer to generate certificate




Certificate Database

BROADCOM
Connecting everything

# Simple Strong Authentication




**NOTE: Every device contains a unique $K_{DI-PRIV}$ and corresponding $K_{DI-PUB}$**

BROADCOM
Connecting everything

# BroadSAFE™ Key Protection

- Keys must be protected in Hardware
  - Key material is the target of attack
  - Aggregation of key material increases the value / risk of attack
  - Key management aggregates key material
    - Key generation
    - Key backup
    - Key policy
  - Key value goes up over time
  - Software almost impossible to make secure across all platforms
    - (Microsoft, Linux, IOS, etc.)

- Hardware key protection for about the same cost as software
  - BroadSAFE Automated Hardware Key Management System
  - Integration of strong hardware key protection into client devices
  - Embedded Hardware Technology

BROADCOM.
Connecting everything®

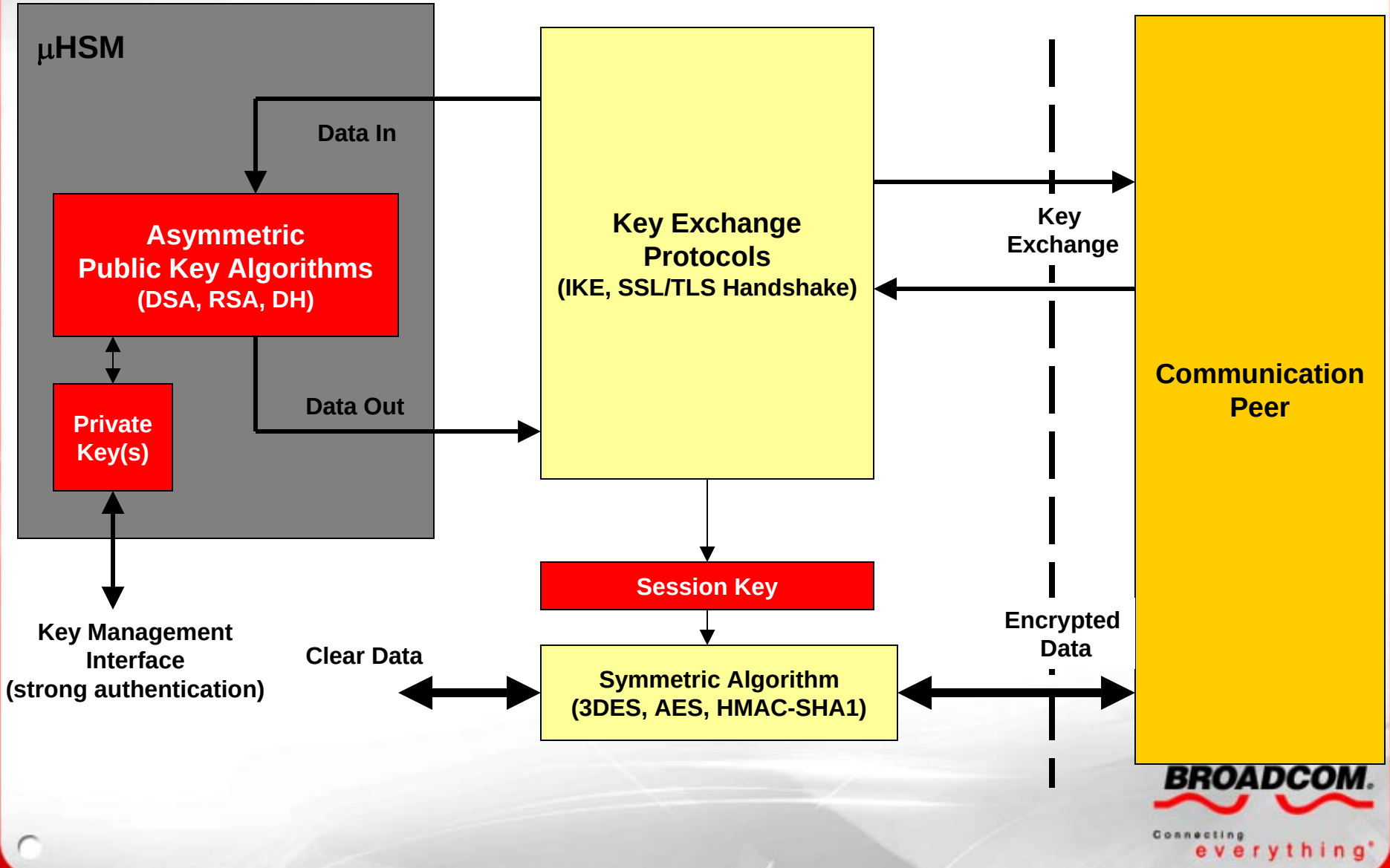
# Key Management

- Cryptography necessitates key management
  - Handling of cryptographic keys in your system
  - Have you locked the door and left the key under the mat?
- Key Handling
  - Generation of keys
  - Set capabilities and security limits of keys (policy)
  - Implement key backup and recovery
  - Prepare keys for storage
  - Key revocation and destruction
  - Multiple layers of security
- Authorized Key Usage
  - Smart-card K of N access control
  - Key linked to particular user / application / etc.
- Secure Audit Logs
  - Tracking key usage to provide audit trail
  - Liability protection
- Certified Security
  - FIPS140-2 Level 3 Security
  - Keys are never exposed outside of hardware in clear-text

# Key Delivery

- Strong device authentication
  - Established as part of generating a session with authenticator
- Key Delivery
  - Ephemeral DH session can be used to deliver device keys
  - Secure tunnel for key delivery to μHSM
- Security Protocol Agnostic
  - Any security protocol that uses Public Key Technology
  - Protection of device, system, user identity
    - Private keys of certificates encrypted so only unique μHSM can use them

# Security Applications



# BroadSAFE System

- Strong Cryptographic Authentication
  - "who you are" versus "who you say you are"
  - Unique embedded "private key identity" for each device
- Hardware Protection of Certificates and Keys
  - Identity is never compromised
  - Key material never leaves the tamper resistant hardware in clear text
  - FIPS140-2 Level 2 and Level 3 Solutions Available
  - Basis for any standard cryptographic security system (IPsec, SSL, TLS, etc.)
- Secure Management
  - Encrypted and authenticated Management traffic
  - Automated policy and key updates
  - Upgrade functions cryptographically in hardware after the device has been deployed

BROADCOM.
Connecting everything®