



## ECC RFID Security for Item-level Tagging

Mike Harvey, Certicom  
Hank Tomarelli, Texas Instruments

2007 RFID Forum, Canada - July 2007

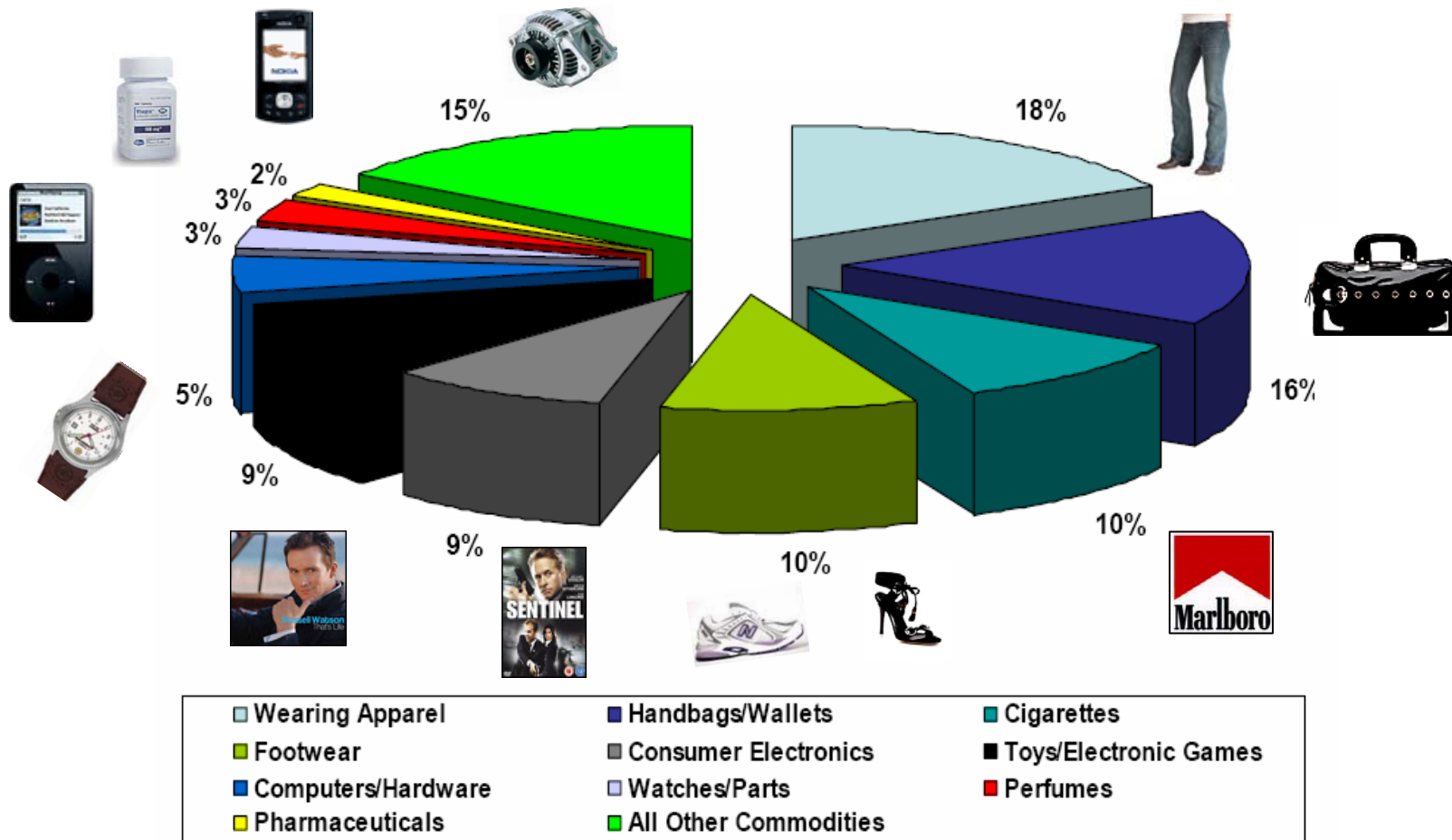
# Agenda

- **Counterfeiting: call to arms ... and opportunities**
- **Benefits of electronic security**
- **ECC & RFID for product authentication**
- **Authentication Process Flow**
- **Components for your solution**
- **Value proposition**



# The Market Driver: Counterfeit Products Proliferate

In 2005, \$93,234,510 in counterfeit products seized by U.S. Customs & Border Control



# Benefits of Electronic Security



Let Your Fingers Do the Walking!



Let Your PRODUCTS Do the TALKING!

- **Product authentication**
- **Data availability**
  - Immediate and future decision making
  - End user safety
  - Audit trail relative to regulatory needs
  - Inventory management
- **Addresses privacy needs**



TEXAS INSTRUMENTS



certicom

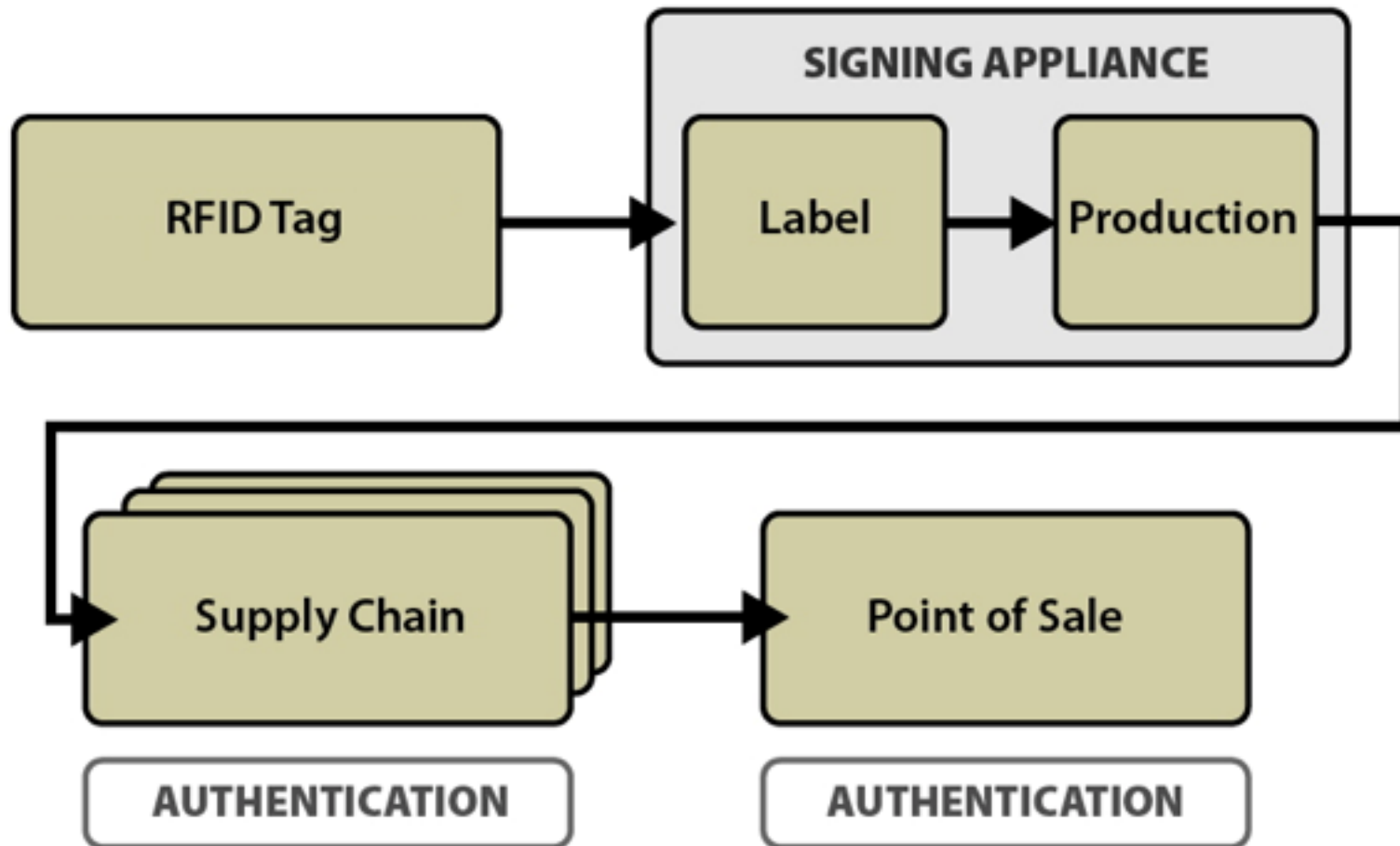
# ECC and RFID Product Authentication

- **ECC - next generation public key cryptography**
- **Digital signatures provide non-repudiation**
  - Non-repudiation prevents an entity from denying previous commitments or actions
  - Allows off-network authentication
- **Standards based**
  - IEEE 1363a-2004 standard
  - ECPVS digital signature for authentication with encryption to protect privacy of product info
- **Performance**
  - ECC 160 bit curve has equivalent security level to 1024 bit RSA



	EPC Number (bits)	Digital Signature (bits)	Total (bits/user memory)
ECC – 160 bits	96	256	352

# Authentication Process Flow



# Product Authentication Components

- **RFID tag**
  - Unique Tag Identification Number (UID)
  - User memory >256 bits
  - Lockable user memory
- **Key agent**
  - Software running on an RFID reader at the manufacturing facility
  - Communicates with reader middleware and warehouse management systems
- **Signing appliance**
  - Connected to the key agent via TLS
  - Signing key used to create a unique digital signature on the RFID tag and encrypt data in a single step
  - Signing key protected with FIPS 140-2 level 3 HSM
- **Authentication agent**
  - Software running on a handheld or PC
  - Can be integrated with existing software
  - Verification key is used to authenticate the digital signature and decrypt the data



# Value Proposition: ECC RFID Security

## ***Differentiate Your Product and Protect it Against Counterfeiting***

- “Anywhere, anytime” authentication and data capture
- “Product talking” drives new product features and channel efficiencies
- IEEE 1363a standard cryptography
- Addresses infrastructure, privacy and security requirements
- Easy implementation into current systems





## Contacts:

Hank Tomarelli  
Texas Instruments  
(214) 567-5418  
[j-pearson2@ti.com](mailto:j-pearson2@ti.com)

Mike Harvey  
Certicom Corp.  
(905) 501-5525  
[MHarvey@certicom.com](mailto:MHarvey@certicom.com)

**Demo on Request**