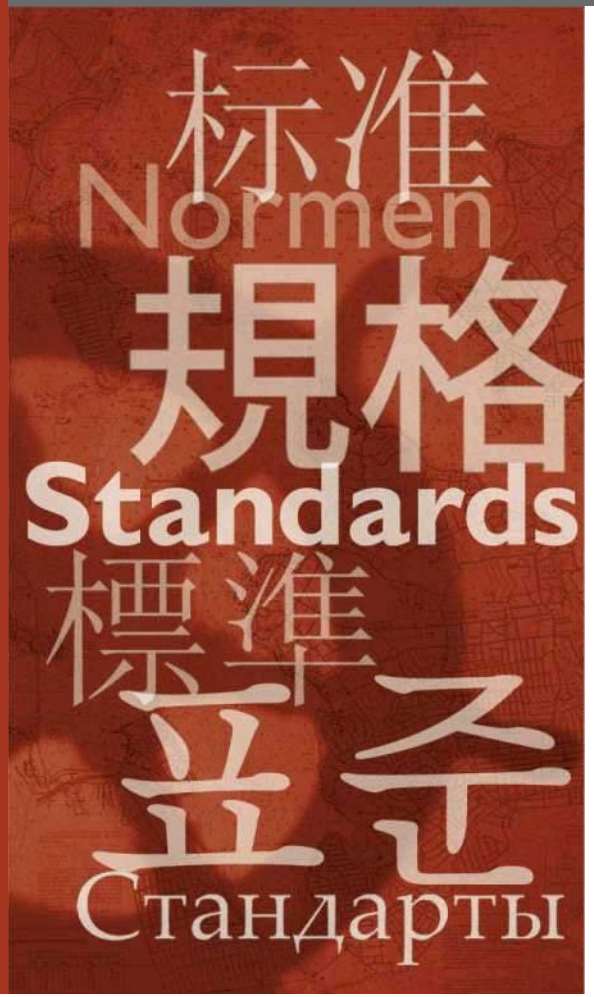
Protect Your Product:
Counterfeit Prevention through Product Authentication



SEMICON West 2007

Workshop

Wednesday, July 18, 2007

semi

Agenda

- Introduction
- Demonstration of covert technologies
- Security Codes on labels
- Security Codes in RFID
- Authentication Service Providers
- Roundtable discussion

Meet your speakers

- David A. Brown
  - Engineer turned sleuth
  - MSEE 1978, Purdue
  - 10 years in microprocessor failure analysis
  - 9 years intellectual property transfer deals
  - 10 years product fraud investigations
- Elliott Grant
  - PhD Manufacturing Engineering 1997, Cambridge
  - CEO YottaMark, Inc.
  - Formerly McKinsey & Co.

Meet your speakers

- Dan Schwarz
  - BA Mathematics & Computer Science, St. John's University
  - Director, New Product Development
  - 15 years professional IT
- Jason D. Warschauer
  - BS Electrical Engineering, Iowa State University
  - Field Applications Support, Texas Instruments RFID Systems
  - 5 Years RFID Engineering

Meet your speakers

- Gene Panger
  - BA Economics, 1983, St. Olaf College
  - Director, Management Board Advisor
  - 20 years international trade

Elephant in the living room

Current strategy

- In general
  - Many layers of security technologies
  - Most technologies are covert
  - Most technologies based on trade secrets
  - Each product uses unique set of layering
- The usual strategy is based on secrecy
  - Once too many secrets are discovered, new combinations of layering are swapped in
- The result
  - Lots of confusion
  - Lots of opportunity to compromise protocols
  - Lots of re-training costs

Are strategies working?

- Counterfeiting will reach $1.2T in 2009*
  - All industries, worldwide.
    - (Not just electronics)
  - Up 40% from today

- That's not what I call success
    - Current strategies are not working very well

* Faking out the Fakers, BusinessWeek June 4, 2007

Barriers to talking

- We don’t trust each other
- We don’t want to help our competitors
- We don’t want to help the bad guys
- My boss/company won’t let me talk
- Telling you makes my program less effective
- My problem is unique: You can’t help me
- It’s against the law to disclose certain data

- Most barriers are opinion-based & self-imposed
  - I’m no exception, there are things I won’t tell you

Detection overhead is too high

- Covert technologies are nice but:
  - By definition, very few know how to use one
  - Access to technology must be controlled
  - Detection equipment is usually needed
  - Effectiveness is limited by detection capacity
- Let's look at an example:

Covert technology example:

- Lets design a layered security label
  1. ~~Security paper stock~~ (oops, too expensive)
  2. OVD, such as a hologram
  3. Taggent 1, UV ink watermark
  4. Taggent 2, DNA bases
  5. Microtext

Mimic attack:

- Within days, counterfeiters will create this:
  1. OVD
     - Quickly mimicked with similar color & similar design
  2. Taggent 1, UV ink watermark
     - Noticed and copied
  3. Taggent 2, DNA bases
     - Ignored
  4. Microtext
     - Noticed and mimicked

Covert technology example:

- Lets design a layered security label
  1. ~~Security paper stock~~ (oops, too expensive)
  2. OVD, such as a hologram
  3. Taggent 1, UV ink watermark
  4. Taggent 2, DNA bases
  5. Microtext

Demo using covert technologies

- Attack occurs in distribution network
  - Fake batch of components slipped in
- Mfg unknowingly buys fake components
  - Fake security label fools all inspectors
- Mfg builds TV using bad components
- Result:
  - TV works poorly if at all

So, what went wrong?

Examples of success

- Public Authentication Tools
  - Make sure you get what you paid for
- Product Activation
  - Some software products now use this

- These techniques interact with end users

Demonstration

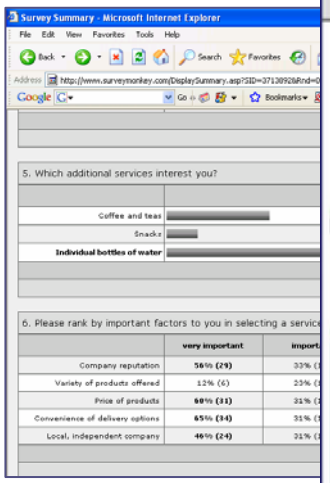
- **Code Authentication** via website
- Verifying other **security layers**
- **'Edge-ware'** operates across the enterprise' boundaries

Layering security with codes

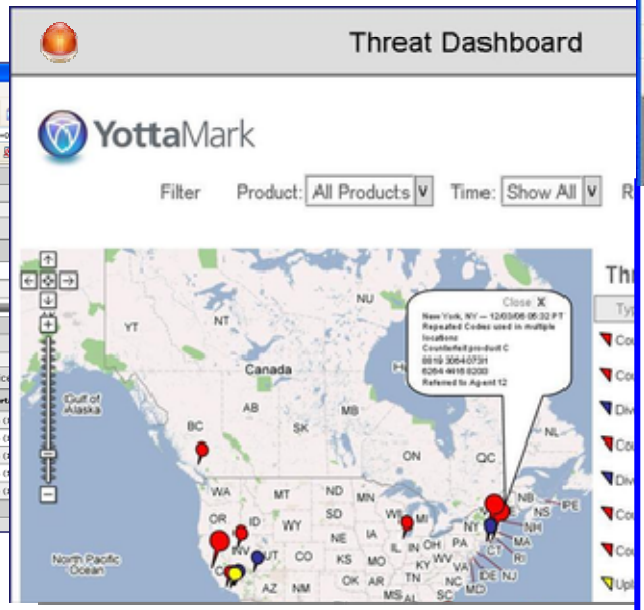
Ambient illumination

UV illumination

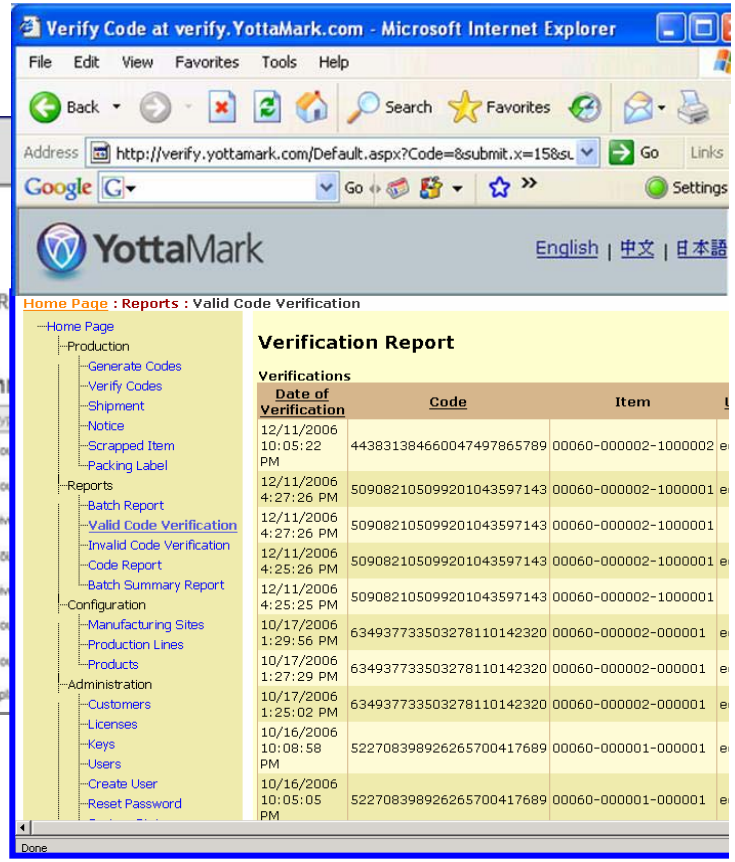
Real-time intelligence



Statistics



Threat Mapping



Audit Tools

Automated Alerts

Why it works

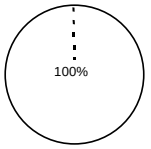
PROBABILITY OF FRAUD DETECTION
CONFIDENTIAL

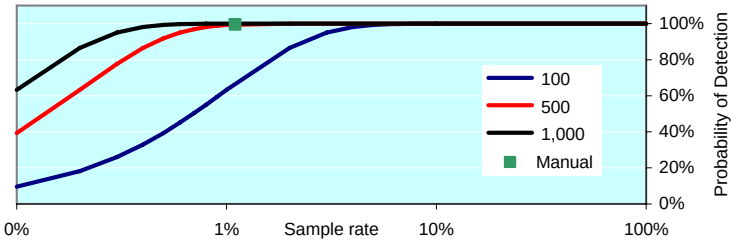
Number of counterfeits made	501
Log slider	
Sample rate	1.1%
Log slider	
Threshold (k)	5
Toggle	
Probability of detecting forged codes	99.6%
Probability of detecting cloned codes	64.5%
Probability of detecting Doppelgangers	5.9%

NOTES
- each line on the chart represents a number of counterfeits put in the supply chain
- the dials and the green dot on the chart represent data entered manually above
- threshold (k) is the number of identical codes seen before an alert is triggered

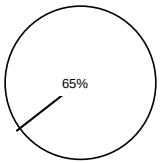
POWERED BY YottaMark

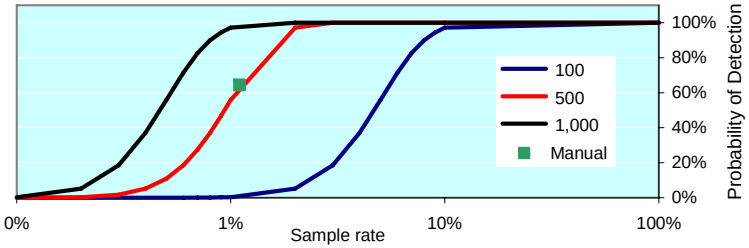
Prob. Detecting Fake Codes



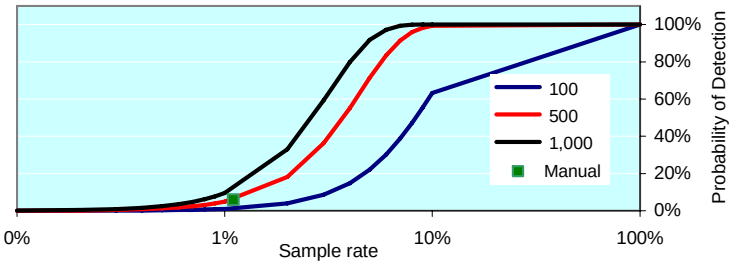


Prob. Detecting Cloned Codes



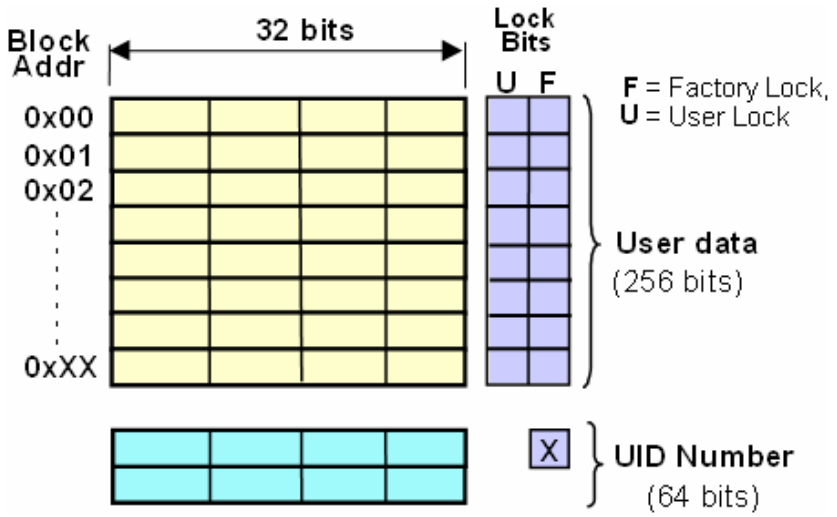


Prob. Detecting Doppelganger Codes



RFID authentication

- Serialized Data Carrier
  - Unique Identifier provides product serialization
  - Writable/Lockable Memory Space provides:
    - Traceability throughout supply chain
    - Authentication via Digital Signature



RFID authentication

- Network
  - Network Database manages Serial Numbers.
- No Network
  - Digital Signature Provides proof of origin
  - Signatures can be Metered

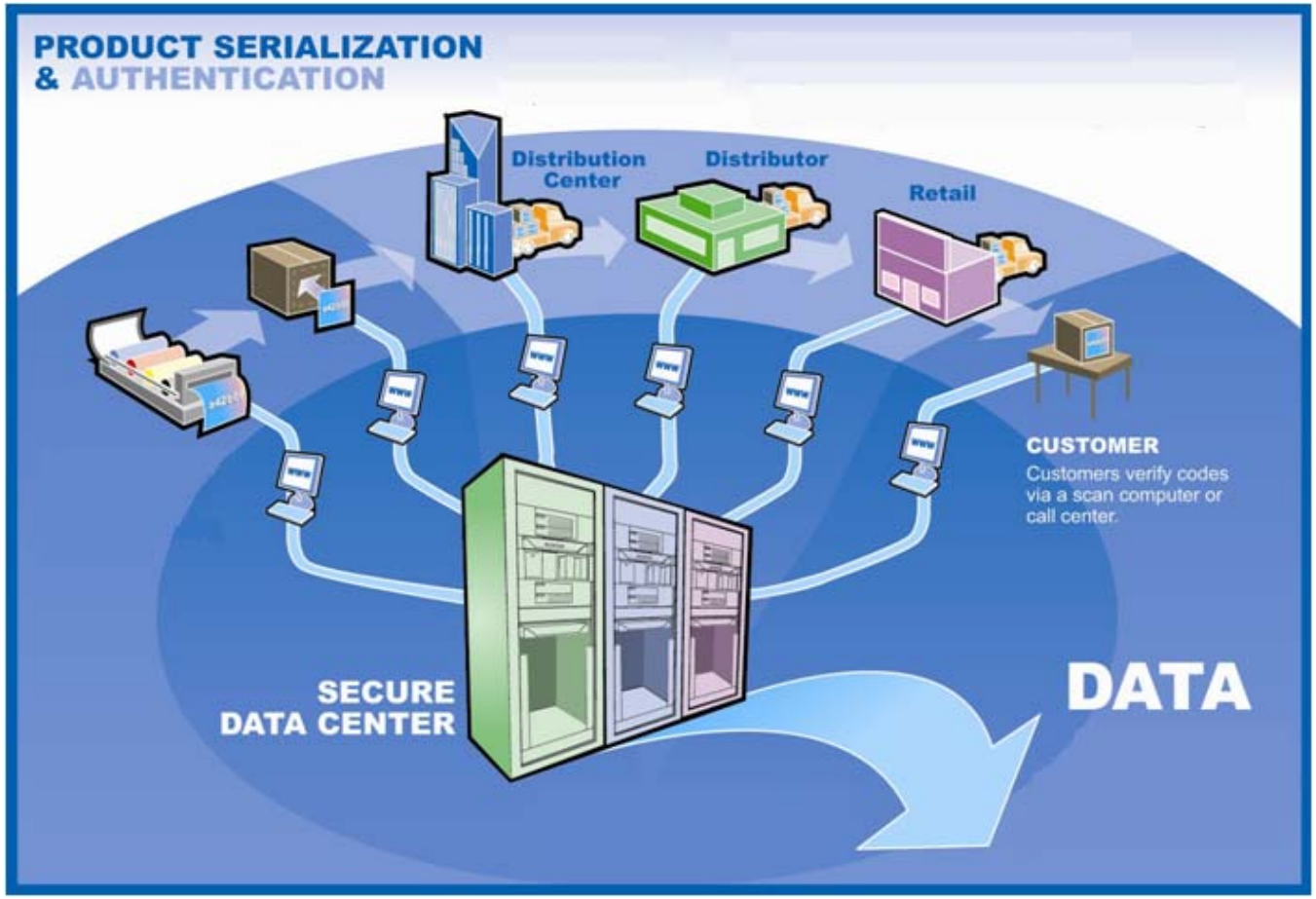
RFID closes the loop

- RFID Combined With:
  - Unique Serialization
  - Tamper Evident Packaging
  - Authentication
    - Network
    - No-Network - Digital Signature
- Addresses:
  - ☑ Over Production
  - ☑ Short Shipments
  - ☑ Shrinkage
  - ☑ Diversion
  - ☑ Counterfeiting

What is an authentication service provider?

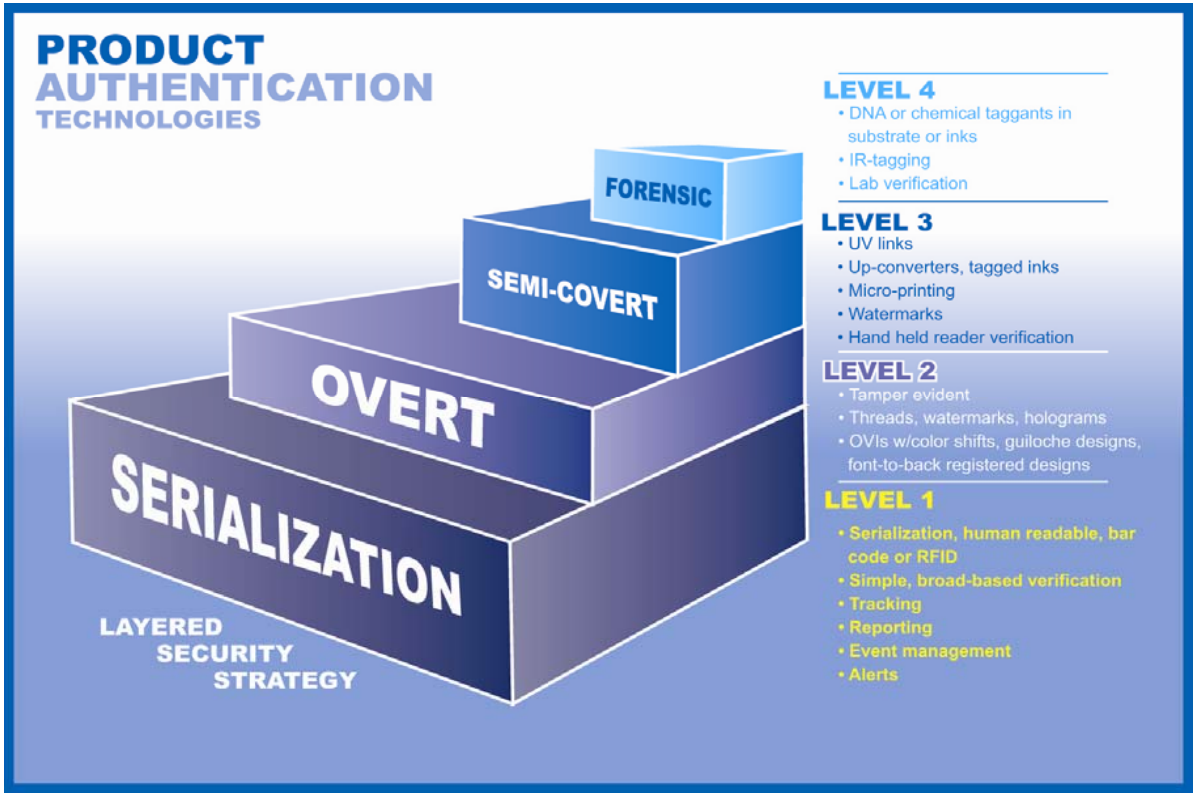
- Provides a method for uniquely identifying brand owner's products (serialization)
- Provides a platform for authenticating brand owner's products
- Provides analysis & reporting

Sample ASP lifecycle



How do ASPs help to protect products?

Adds a layer of security



How do ASPs help to protect products?

- Protect against warranty fraud
- Protect supply from the introduction of fraudulent goods
- Enable targeted product recalls
- Diversion detection
- Gain insight

Industries using authentication

- Aerospace
- Apparel & Sporting Goods
- Automotive
- Agricultural/Chemical
- Consumer Packaged Goods
- Electronics
- Health & Life Sciences

Applications

- Anti-Fraud
  - Counterfeit Detection
  - Consumer Product Authentication
  - Return and Warranty Verification
  - Gray Market Detection
- Product Tracking
- Recall Tracking
- Anti-Diversion

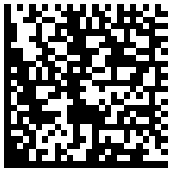
SIA-SEMI anti-counterfeit working group

Code based Security	Minimum Code Requirements	Provider Security
• Service generates and authenticates codes • Codes are unique to each unit (i.e., component, tray, reel, tape, box, etc.) • Security methods not based on codes are not covered by this standard (e.g. holograms, inks, taggents)	• Code length determined by requirements • Numeric or alphanumeric human-readable codes • Non-repeating • Non-predictable • Cancelable • Consumable	• ASP must gain and maintain secure supplier status as evidenced by third-party certification (e.g. NASPO)

Code schema

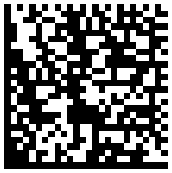
- 3 character prefix identifies ASP
- Colon delimiter
- Variable length numeric or alpha-numeric security code
- Person-readable
- 2D Datamatrix (ECC200) contains entire message - other symbologies or code carriers are optional
- Standard URL and instructions

TEMPLATE



AAA: NNNN NNNN NNNN
NNNN NNNN NNNN
Check at verify.sia.org

EXAMPLE



ZZZ: 1234 1234 1234 1234
1234 1234 1234 1234
Check at verify.sia.org

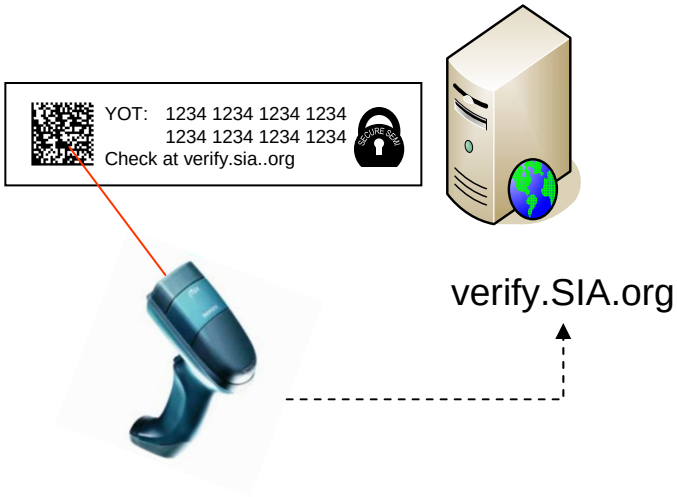
Process flow

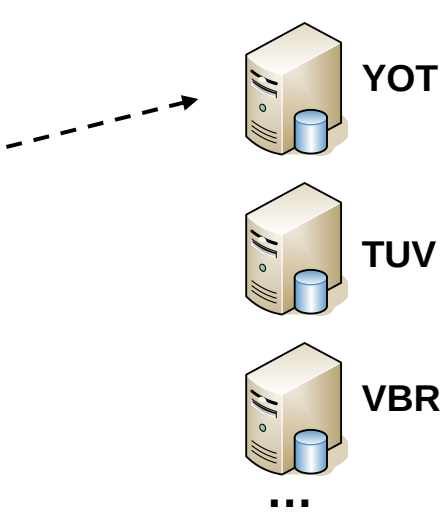
User receives product with SIA code

User scans or enters code into SIA URL or via web services

SIA Server directs code to appropriate ASP based on 3 letter prefix

ASP verifies code, and returns verification data in standard format





Verification: PASS
Verifications: 1

<standard semi label data>
Product: INTEL 3.6GHz
Manufactured: 03/07/2007
LOT#: 00234912

Note: Codes will be consumed based on brand owner's business rules (e.g. code will be consumed only when checked by an 'end user'. Supply chain checks will validate but not consume code.).

Market model

- Market forces determine ASP choices
  - Method used to secure codes (i.e., encryption, public/private key, symmetric key, random number generation, etc.)
  - Features beyond standard data structure (i.e. automated alerts, cell phone authentication, supply analytics, service, etc)

Next steps

- Stakeholders
  - International
  - Multiple domains
- Consensus building
- Standards development

Elephant in the living room

Contact us!

- Anti-Counterfeiting TF Leaders & Technical Experts:
  - Win Baylies (winba@comcast.net)
  - Dave Brown (david.a.brown@intel.com)
  - Daryl Hatano (dhatano@sia-online.org)
  - Dave Huntley (dave.huntley@kinesyssoftware.com)
- Information about the group:
  - Susan Turner (sturner@semi.org)