MINUTES OF A MEETING TITLED
Protect Your Product: Counterfeit Prevention Through Product Authentication.
on
18th July, 2007
held at SEMICON West, San Francisco, CA

Present

Attendees included representatives from many organizations, including, but not limited to: Intel, Texas Instruments, Linear, SUN, National Semiconductor, Arrow, YottaMark, BRADY, ITW, IDEA, JDS Uniphase, TUV, VerifyBrand, the US Dept. of Commerce, SEMI, SIA.

Call to Order

Ms. Karson of YottaMark, Inc. called the meeting to order.

Overview

Mr. David Brown of Intel introduced the size and scope of the counterfeiting problem, and discussed and illustrated limitations of current ‘hard to copy’ label features, such as color-shifting inks, holograms, DNA taggants, UV/IR inks, etc. He argued for the use of unit level secure codes that can be checked easily, based on experience from other industries, and success of programs to verify microprocessors with a public, online verification tool.

Demonstrations

Dr. Elliott Grant of YottaMark gave a demonstration of a secure-code based authentication system using printed barcodes and a website, and discussed the statistical underpinnings of the strength of such as system. Dr. Grant also showed how such a system could enhance the usefulness of said ‘hard-to-copy’ features as well as provide valuable intelligence back to the rights owner.
Mr. Jason Warschauer of TI and Mr. Dan Schwarz of VerifyBrand demonstrated a code-based system using RFID tags with both verification of the RFID unique ID code on a website and a public key (unconnected) reader to verify a digital signature in the tag.

Standards Outline Proposed

Mr. Gene Panger of TUV discussed the role of Authentication Service Providers (ASPs) and the scope of the proposed standard.

Questions were asked and extensive discussion ensued. Feedback was gathered from the attendees on issues they see and questions they would like to see answered by the standard. These issues and topics are summarized in Exhibit A.

Adjournment

There being no further business, the meeting was adjourned.

Minutes recorded by Elliott Grant

Exhibit A. Issues and Topics Raised

- Trust in the system
    - How will a brand owner know that an ASP is trustworthy?
    - How will an ASP know that a customer is who he claims to be?
    - How will a brand owner know that a label converter is trustworthy?
- Handling supply chain complexity
    - How does a distributor continue the chain of custody for legitimately re-sold, used or partially consumed parts (e.g. a partial reel)?
    - How will the system handle the breaking down of lots, where a lot may have only one encrypted ID?
- Data security
    - In some cases, it may be illegal to divulge certain information (e.g., Shipper information) as part of an authentication
- Who pays for the solution?

- Related issues, but outside the intended scope of the standard
    - How can chip manufacturers authenticate consumables?
    - How to authenticate legacy /obsolete product
    - How to detect grey market diversion
    - How will the supply chain be educated about the codes?
    - How will this affect the role and value proposition of ‘qualified’ distributors, vs. independent distributors?
    - What can be done about willful purchasing of counterfeit product (e.g. consumables)?