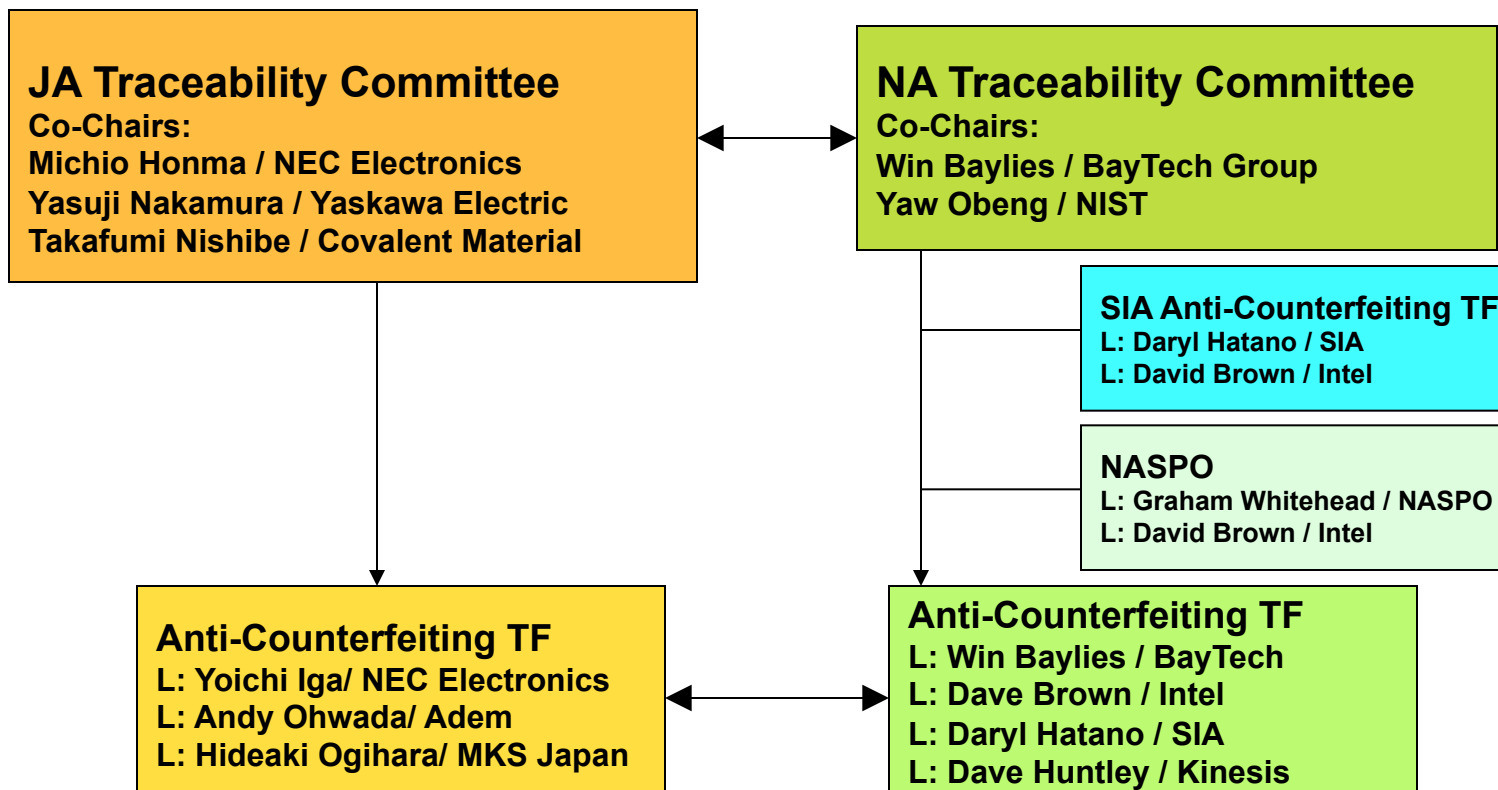


SEMI Standards Anti-Counterfeiting Task Force

Dr. Yaw Obeng, Co-Chair of NA Traceability Committee

International Leadership & Support



Meeting Information

- Recent meetings
 - October 14, 2008 in San Jose, CA (SEMI HQ Office)
 - December 3, 2008 in Makuhari Japan (SEMICON Japan)

- Next meetings
 - April 2, 2009 in Milpitas, CA (Sheraton-San Jose)
 - July 16th, 2009 in San Francisco (SEMICON West)

semr

SEMI T20-1108 SPECIFICATION FOR SYSTEM ARCHITECTURE FOR AUTHENTICATION OF SEMICONDUCTORS AND RELATED PRODUCTS

This standard was technically approved by the global Traceability Committee. This edition was approved for publication by the global Audit and Review Subcommittee on August 29, 2008. It was available at www.semi.org in October 2008 and on CD-ROM in November 2008.

1 Purpose

1.1 The electronic component supply chain is frequently contaminated by counterfeit and tainted product. The risk of procuring contaminated goods increases when authorized (certified) distribution networks run out of product. This may occur with supply shortfalls or terminated products. Then, purchasing policy may also force procurement from non-certified distributors. The semiconductor industry currently lacks standard methods to validate the integrity of goods from non-certified distributors or suppliers.

1.2 The purpose of this specification is to describe the system architecture aspect of the authentication process to establish the trusted identity of products or objects.

1.3 This specification is the basic element of a suite of standards aimed at enabling automated, reliable and secure product authentication for the semiconductor industry.

NOTE 1: The other aspects of the process are covered in other documents now under development within the Anti-Counterfeiting Task Force of the Traceability Committee. When approved, these documents will be cited in this specification.

NOTE 2: It is expected that additional revisions will be made soon after the publication of this edition of the standard.

2 Scope

2.1 This specification covers structure, behavior, and services for the organizations and objects involved in product authentication.

2.2 An essential aspect of authentication involves the establishment of trusted relationships between the authentication service provider (ASP) and its manufacturer clients, which in some circumstances may be part of the same organization. The nature of establishing such relationships is beyond the scope of this specification.

2.3 This specification covers the ability to check the authentication of a product within the supply chain. It does not cover the traceability of any product through the supply chain, although by permitting but not requiring supply chain buyers to become trusted it can relatively easily be extended in this direction.

2.4 The following items are outside the scope of this specification:

- Object labeling,
- Communication protocols,
- Authentication service provider qualifications,
- Format and content of authentication codes, and
- Recovery procedure when service errors occur.

NOTE: This standard does not purport to address safety issues, if any, associated with its use. It is the responsibility of the users of this standard to establish appropriate safety and health practices and determine the applicability of regulatory or other limitations prior to use.

1 SEMI T20-1108 © SEMI 2008

semr

SEMI Draft Document 4487 New Standard: SPECIFICATION FOR OBJECT LABELING FOR DETECTING AND PREVENTING COUNTERFEITING OF SEMICONDUCTORS AND RELATED PRODUCTS

Document Number: 4487
Date: 2/12/2009

1 Purpose

1.1 Background

1.1.1 The electronic component supply chain is frequently contaminated by counterfeit and tainted product. The risk of procuring contaminated goods increases when authorized (certified) distribution networks run out of product. This may occur with supply shortfalls or terminated products. Then, purchasing policy may also force procurement from non-certified distributors. The semiconductor industry currently lacks standard methods to validate the integrity of goods from non-certified distributors or suppliers.

1.1.2 SIA's Anti-Counterfeiting Task Force has proposed solving these problems through the use of global, open, common-based industry standards that cover (1) system architecture, (2) object labeling, (3) authentication service communication, and (4) authentication service provider qualifications.

1.1.3 This standard is part of a suite of standards aimed at the system architecture, object labeling, authentication service communication and authentication service provider qualifications that enable enabling, automated, reliable and secure product authentication for the semiconductor industry. This particular standard describes the object labeling aspect.

1.2 The approach that is covered by this guide involves (1) labeling by trusted manufacturers of batches of authentic parts with Authentication Codes on the product package or device and (2) an authentication service, available to anyone considering purchase of goods, using the Authentication Code for validation.

1.3 This standard is intended to provide a common format, syntax, and content for printed, machine-readable codes on objects to facilitate communication of data essential for authentication. These labels differ from current commercial practice in that they provide no direct information about the product.

1.4 This standard covers labels or package marking that contain a two-dimensional matrix bar code symbol (hereafter CD Data Matrix) and its associated human-readable information. This symbol (an alphanumeric substantially more information than can one-dimensional (linear) bar code symbols), it is included to provide for a smooth transition from existing traceability and labeling practices to the comprehensive, unified system envisioned for the future in which common reading equipment can be used throughout the supply chain.

2 Scope

2.1 This standard covers labels for objects used for packaging semiconductor and electronic components, including intermediate container, product package, or shipping pack, and for direct part mark in the structure where packaged device marking is desired and practical.

2.2 This standard does not specify the location of the security label on the package or device. The location of package identification labels is covered in CEA-G1-A. The location of device marking is covered in CEA-706-A.

2.3 This standard covers the syntax and content of the code fields on the label.

2.4 This standard includes descriptions of the characteristics of the code formats to be employed.

2.5 The materials of construction and the adhesives used to apply the label are beyond the scope of this document.

2.6 The dimensions in this standard are applicable to labels printed with printers which have nominal resolutions of 20 dots per inch (dpi). Printers with higher resolution may be used. In such cases, it is necessary to ensure that the level of care that fits the package to be employed.

2.7 The format of the 2D Data Matrix Code is specified in ISO/IEC 16252.

2.8 The labels in this standard are compatible with SEMI T20 (Document 4486).

Page 1 Doc. 4487 © SEMI

semr

SEMI Draft Document 4488 NEW STANDARD: SPECIFICATION FOR SERVICE COMMUNICATION FOR PREVENTING AND DETECTING SEMICONDUCTOR COUNTERFEIT PRODUCTS

Document Number: 4488
Date: 2/12/2009

1 Purpose

1.1 The electronic component supply network is frequently contaminated by counterfeit and tainted product. The risk of procuring contaminated goods increases when authorized (certified) distribution networks run out of product. This may occur with supply shortfalls or terminated products. Then, purchasing policy may also force procurement from non-certified distributors. The semiconductor industry currently lacks standard methods to validate the integrity of goods from non-certified distributors or suppliers.

1.2 SIA's Anti-Counterfeiting Task Force has proposed solving these problems through the use of global, open, common-based industry standards that cover (1) system architecture, (2) object labeling, (3) authentication service communication, and (4) authentication service provider qualifications.

1.3 This standard is part of a suite of standards aimed at enabling automated, reliable and secure product authentication for the semiconductor industry. This standard describes the authentication service communication aspect.

1.4 It provides an XML schema that corresponds to the product authentication objects, attributes, and associations described in SEMI 4486 that enable automated, reliable and secure product authentication for the semiconductor industry.

1.5 It maps the services of SEMI T20 to XML Web Services. The Web Services Definition Language (WSDL) representation of this standard is contained in separate documents (see 17 for a discussion of XML schema) and is also included as appendices to this standard.

2 Scope

2.1 This standard covers representation of the SEMI T20 object model in an XML schema. This specification does not add new domain information or concepts to the model. The only additions made are those needed to render a useful XML schema.

2.2 This standard also covers implementation of SEMI T20 services using web services.

NOTE: This standard does not purport to address safety issues, if any, associated with its use. It is the responsibility of the users of this standard to establish appropriate safety and health practices and determine the applicability of regulatory or other limitations prior to use.

3 Limitations

3.1 This standard does not define the secure connection used to access the web service. The web services defined are, however, intended to operate over a secure connection.

3.2 A key aspect of this architecture is that an authentication request must be cleared through a trusted portal but the URL of the portal is not specified in this standard.

4 Referenced Standards and Documents

4.1 SEMI Standards

E121 – Guide for Style and Usage of XML for Semiconductor Manufacturing Applications

SEMI T20 (Document 4486) – System Architecture for Detecting and Preventing Counterfeiting of Semiconductors and Related Products

4.2 World Wide Web Consortium Documents

Extensible Markup Language (XML) 1.0 (Second Edition, Namespace in XML)

Web Services Architecture (Working Draft #)

Page 1 Doc. 4488 © SEMI

semr

SEMI Draft Document 4489 New Standard: GUIDE FOR QUALIFICATIONS OF AUTHENTICATION SERVICE BODIES FOR DETECTING AND PREVENTING COUNTERFEITING OF SEMICONDUCTORS AND RELATED PRODUCTS

Document Number: 4489
Date: 2/12/2009

1 Purpose

1.1 The electronic component supply network is frequently contaminated by counterfeit and tainted product. The risk of procuring contaminated goods increases when authorized (certified) distribution networks run out of product. This may occur with supply shortfalls or terminated products. Then, purchasing policy may also force procurement from non-certified distributors. The semiconductor industry currently lacks standard methods to validate the integrity of goods from non-certified distributors or suppliers.

1.2 SIA's Anti-Counterfeiting Task Force has proposed solving these problems through the use of global, open, common-based industry standards that cover (1) system architecture, (2) object labeling, (3) authentication service communication, and (4) authentication service provider qualifications as key in implementing this solution approach.

1.3 The approach that is covered by this guide involves (1) labeling by trusted manufacturers of batches of authentic parts with secure batch numbers (encrypted serial number) on the product package and (2) a so-called authentication service available to anyone considering purchase of a batch of parts, using the encrypted batch number as the basis for a validation check of the license plate.

NOTE 1: The nature of the license plate and its location on the product package are expected to be specified in the standard covering object labeling now under development in the Anti-Counterfeiting Task Force of the Traceability Committee.

NOTE 2: This guide covers the qualifications required of authentication service providers.

2 Scope

2.1 This guide describes the qualifications required for an authentication service provider (ASP) to certify the authenticity of the encrypted serial number that is described in 4.1.2. This authentication service involves the storage, examination and verification of the encrypted serial number submitted to the ASP by a product provider (e.g., a semiconductor or electronic component manufacturer and product user (e.g., a distributor, value-added manufacturer)).

2.2 This guide includes:

- 2.2.1 Information, supply, and operating security requirements,
- 2.2.2 Requirements for verifying the authenticity of products through secure codes, and
- 2.2.3 ASP communication requirements.

NOTE: This standard does not purport to address safety issues, if any, associated with its use. It is the responsibility of the users of this standard to establish appropriate safety and health practices and determine the applicability of regulatory or other limitations prior to use.

3 Limitations

3.1 This guide does not address system architecture, object labeling or authentication service communication.

NOTE 3: These issues are being developed in other related standards.

3.2 This guide also does not address the requirements for batch processing multi and verification of authentication service providers. This aspect is covered in ISO/IEC 27002 and ISO 28000.

4 Referenced Standards and Documents

4.1 SEMI Standards

SEMI 4486 – Technology for Secure Technology

SEMI T20 (Document 4486) – System Architecture for Detecting and Preventing Counterfeiting of Semiconductors and Related Products

Page 1 Doc. 4489 © SEMI

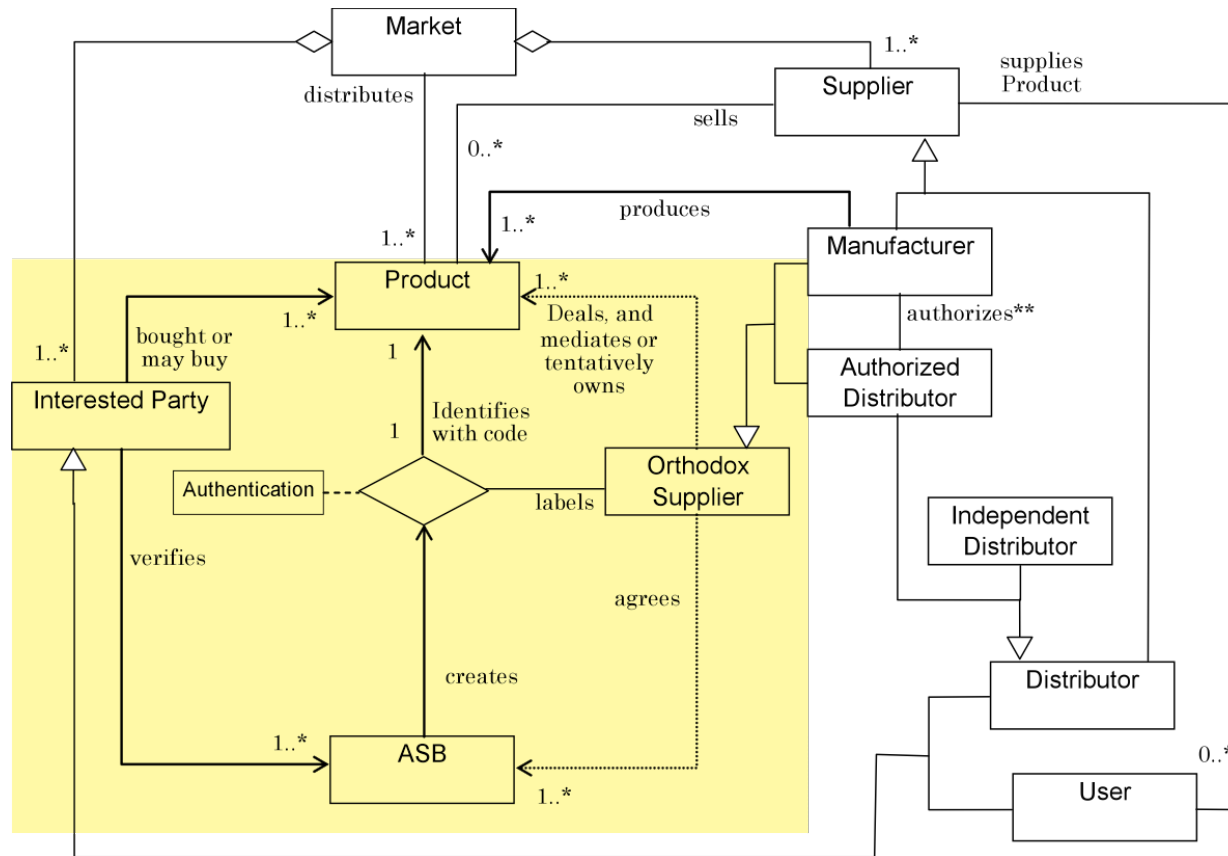
Purpose

- **Describe authentication process**
 - Ensure process is automated, reliable and secure
 - Establish trusted identity of products

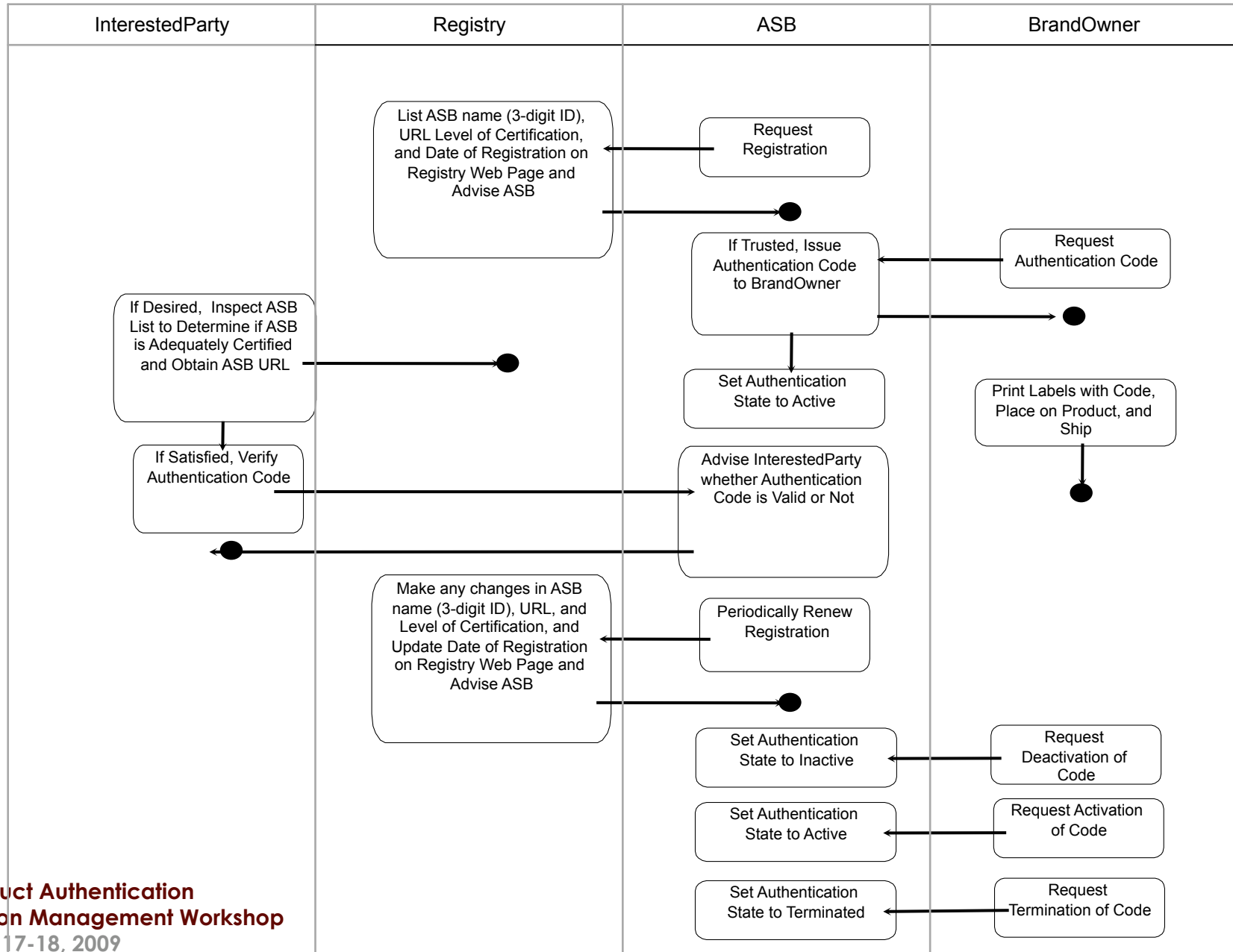
Standards

Document #	Topic	Status
T20-1108	Architectural Design	<i>Published</i> —Currently Under Revision
4487	Labeling	Under Development
4488	Authentication Service Communication	Under Development
4489	Authentication Service Body Qualifications	Under Development

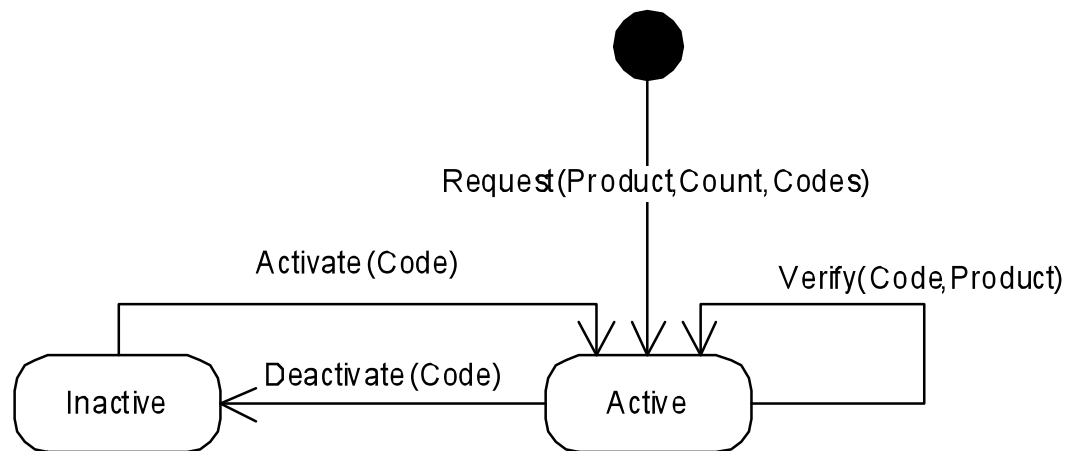
T20 Product Authentication Overview



Typical Product Authentication Cycle – State Diagram



Product Authentication State Diagram





Questions / Comments?

Please contact Susan Turner (sturner@semi.org) for more information