

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 Audits and Reviews 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 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 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 standards¹ 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.

NOTICE: 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 This suite of standards is being developed in response to a request from the Anti-Counterfeiting Task Force of the Semiconductor Industry Association, 181 Metro Drive, Suite 450, San Jose, CA 95110.

3 Referenced Standards and Documents

3.1 ANSI Standard²

ANSI MH10.8.2 — Data Identifier and Application Identifier Standard

3.2 OMG Standards³

OMG Specification formal/2007-11-02 — OMG Unified Modeling Language (OMG-UML) Superstructure, V2.1.2

OMG Specification formal/2007-11-04 — OMG Unified Modeling Language (OMG-UML) Infrastructure, V2.1.2

NOTICE: Unless otherwise indicated, all documents cited shall be the latest published versions.

4 Terminology

4.1 Abbreviations and Acronyms

4.1.1 ACS — anti-counterfeiting system

4.1.2 ASP — authentication service provider

4.1.3 UML — Unified Modeling Language

4.2 Definitions

4.2.1 *authentication code* — encrypted serial number issued by an ASP in response to a request from a manufacturer for marking its product.

4.2.2 *authentication service provider* — a company or an organization that has registered with the registry and has met the specified qualifications.

NOTE 3: These qualifications are covered in another standard now under development by the Anti Counterfeiting Task Force of the Traceability Committee and are beyond the scope of this specification.

4.2.3 *buyer* — an entity that buys a product. A buyer may be part of a supply chain or an end user.

4.2.4 *end user* — buyer of a product for its intended purpose, for example, a maker of cell phones or laptops.

4.2.5 *interested party* — an entity interested in determining the authenticity of a product, including buyers, law enforcement, customs, etc.

4.2.6 *manufacturer* — maker of a product for sale to buyers.

4.2.7 *registry* — a list of approved ASPs that is maintained by an independent standards authority so that the qualifications of ASPs can be verified by interested parties.

4.2.8 *supply chain* — entities that distribute or resell a product.

4.2.9 *trusted, adj.* — a type of manufacturer that has established its identity and purpose to the satisfaction of an ASP.

5 Object Modeling

5.1 Unified Modeling Language (UML)

5.1.1 This specification uses UML notation for all class diagrams and for any object and activity diagrams provided as examples.

5.1.2 *Class Diagrams* — UML class diagrams have clearly defined meaning and are a part of this specification. Detail contained in these diagrams is not necessarily repeated in the text.

5.1.3 *Name of a Class* — The text capitalizes class names and services. Class attributes begin with lowercase letters.

² Available from <http://www.autoid.org>

³ Object Management Group, Inc. Website: www.omg.org.

5.1.4 *Abstract and Concrete Classes* — Each class is specified as Abstract or Concrete. Abstract classes are not directly implemented (i.e., there are no instances). All classes defined as concrete may be directly implemented. In UML class diagrams, abstract class names are shown in *italics*. All classes used in this specification are concrete.

5.1.5 *Class Attribute Definition* — The attributes of a class are defined in table format as illustrated by Table 1. Note that the “+” sign in front of attributes in UML class diagrams indicates “public” attributes. All attributes defined in this specification are public, therefore the “+” sign is omitted.

Table 1 Attribute Table Format

Attribute Name	Definition	Access	Reqd	Form
		RO or RW	Y or N	String or Integer

5.1.5.1 *Access* — Attributes may be settable (ReadWrite or RW) or not settable (ReadOnly or RO) through an interface to the service provider. Note that all attributes defined in this specification are ReadOnly (RO).

5.1.5.2 *Reqd* — Is this attribute required? Y – Yes, or N – No.

6 Requirements

6.1 *ACS Class Diagram* — Figure 1 is a UML class diagram that illustrates the requirements defined in the remainder of this section. Only the highlighted classes and the associations between them represent requirements.

NOTE 4: The symbols and other items included in this and subsequent figures are fully described in OMG formal/2007-11-02 and OMG formal/2007-11-04. See also http://www.omg.org/gettingstarted/what_is_uml.htm#12DiagramTypes for UML diagram types.

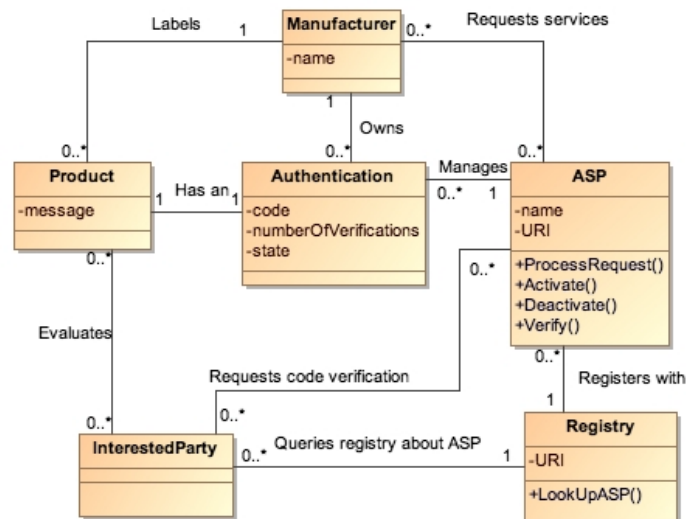


Figure 1
Product Authentication: Class Diagram

6.1.1 *Product* — Table 2 shows the attributes for each Product that is marked with an authentication code intended to guarantee the authenticity of that product to an InterestedParty.

Table 2 Product Attributes

Attribute Name	Description	Access	Reqd	Form
message	A text string of variable length with the text syntax defined by ANSI MH10.8.2 so that there is a standardized way to interpret the message content. Manufacturer determines what fields to include, and the content for those fields.	RO	Y	String