

SEMI T20-0710 (Reapproved 0322) SPECIFICATION FOR AUTHENTICATION OF SEMICONDUCTORS AND RELATED PRODUCTS

This Standard was technically approved by the Traceability Global Technical Committee. This edition was approved for publication by the global Audits and Reviews Subcommittee on September 7, 2021. Available at www.semiviews.org and www.semi.org in March 2022; originally published November 2008; previously published April 2016.

NOTICE: Paragraphs entitled ‘NOTE:’ are not an official part of this Standard or Safety Guideline and are not intended to modify or supersede the official Standard or Safety Guideline. These have been supplied by the global technical committee to enhance the usage of the Standard or Safety Guideline.

NOTICE: The section symbol (§) is used to reference a numbered section, paragraph, or header and all subordinate paragraphs, headers, and embedded material (i.e., EXCEPTIONs, lists) therein. The paragraph symbol (§) is used to reference a particular numbered paragraph and embedded material therein. When duplicated (i.e., §§ and §§) the symbols are used to reference more than one section or paragraph, respectively.

1 Purpose

1.1 *Assumed Commercial Environment*

1.1.1 Large quantities of semiconductor device products are distributed in the business world to be embedded into various electronics products such as television sets, computers, automobiles or their components, and so on. 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.

1.2 *Authentication of Distributed Products*

1.2.1 A product may be substituted by counterfeiting the item secretly anywhere in a chain of distribution. If the product has specific identification; for example, an unpredictable random code, on it issued by some authentication organization, it can be determined whether it is genuine or not anywhere in the distribution chain.

1.2.1.1 When authentication is practiced consistently at key points in the trade stream, and when it is left open for any party to participate, it drives unintended counterfeit purchases to a minimum in a way that can be deployed easily and relatively inexpensively in a wide variety of settings.

1.3 *Availability of Standards*

1.3.1 The semiconductor industry has lacked standardized methods to validate the integrity of goods from non-certified distributors or suppliers. The purpose of this Specification is to describe the system architecture aspect of an authentication process to establish the trusted identity of products or objects.

1.3.1.1 This Specification is the basic element of a suite of Standards¹ aimed at enabling automated, reliable, and secure product authentication for the semiconductor industry, thereby reducing the presence of illegal counterfeit items in the marketplace.

NOTE 1: The other aspects of the process are covered in other Standards now under development within the Anti-Counterfeiting Task Force of the Traceability Committee. When approved, these Standards will be appended to this Specification as Subordinate Standards.

2 Scope

2.1 This Specification covers structure, behavior, and services for the organizations and entities involved in authentication of semiconductor and related products or objects through the use of secure serialization.

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, USA.

2.2 In the market place, secure serialization is one layer among a number used to affirm authentication, support investigations and seizures, and identify trade stream transactions that do not fit expected paths, and so forth. The principal of accommodating multilayer strategies is not excluded from the Specification. These choices are left to brand owners to decide.

2.2.1 Secure serialization is a solution that will provide the most benefit from wide-scale adoption and the use of a standardized methodology. It is not being presented as the only the solution nor as the final solution. It is an important ingredient in an effective response to fraud and counterfeiting.

2.2.2 Secure serialization systems alone do not prevent the copying or theft of codes. They can be, however, effective at detecting that such fraud has occurred. Secure serialization is a deterrent and an early warning system. More comprehensive solutions can be created with the optional addition of copy prevention technologies.

2.3 This Specification covers the ability of any interested party (without restriction) 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 Interoperability with other industries is valuable. The procedures of this Specification could be extended to other industries, with suitable modifications. Such an extension is, however, beyond the scope of the present Specification.

2.5 An essential aspect of authentication involves the establishment of trusted relationships between the Authentication Service Body (ASB) and its brand owner 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.

2.6 *Internet Accessing Capability*

2.6.1 This Specification basically assumes specified services between parties through the Internet. However, it neither suggests specific types or means of such communications nor restricts implementation of any desirable mode.

NOTE 2: Some aspects of these communication-related items are covered in a companion Subordinate Standard still under development in the Traceability Committee.

2.7 *Authentication Service Body*

2.7.1 This Specification assumes the existence of ASBs. This Specification does not cover the qualifications of ASBs or restrict the nature of such an organization.

2.8 *Object Labeling*

2.8.1 This Specification does not specify a particular encryption methodology for the creation of secure serial numbers, nor does it preclude the use of additional or alternate approaches to authentication.

NOTE 3: This Standard and the others comprising the suite are being based on existing ISO protocols to simplify wide-scale adoption.

2.9 *Encryption and/or Decryption Capability*

2.9.1 This Specification does not cover methods of encryption and/or decryption of the code or means to avoid its being cheated or forged. However, it should be noted that users of this Standard might need to have such capability to reduce further risks of counterfeiting products.

2.10 *Code Reading/Writing Capability*

2.10.1 This Specification does not cover devices to write or read code on products. Such devices may be required to utilize or implement this Standard.

2.11 *Recovery Procedure*

2.11.1 This Specification does not cover recovery procedures when service errors occur.

NOTICE: SEMI Standards and Safety Guidelines do not purport to address all safety issues associated with their use. It is the responsibility of the users of the Documents to establish appropriate safety and health practices, and determine the applicability of regulatory or other limitations prior to use.

3 Referenced Standards and Documents

3.1 *ANSI Standards*²

ANSI MH10.8.2 — Data Identifier and Application Identifier Standard

3.2 *OMG Standards*³

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

OMG 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 *ACAS* — Anti-Counterfeiting Authentication System

4.1.2 *ASB* — Authentication Service Body

4.1.3 *UML* — Unified Modeling Language

4.1.4 *URL* — Universal Resource Locator

4.2 *Definitions*

4.2.1 *anti-counterfeiting* — efforts or items to prevent distribution of unauthorized fraudulent replicas of semiconductor products in specific or global markets.

4.2.2 *Anti-Counterfeiting Authentication System* — a whole system or a part of a system in a specific technology field for reducing or eliminating the presence of unauthorized fraudulent replicas of products in the marketplace.

4.2.3 *authentication code* — encrypted serial number issued by an ASB in response to a request from a brand owner for marking its product.

4.2.4 *Authentication Service Body* — a company or an organization providing anti-counterfeiting authentication service that has registered with the registry and has met the specified qualifications.

NOTE 4: These qualifications are covered in a Subordinate Standard now under development by the Anti-Counterfeiting Task Force of the Traceability Committee.

4.2.5 *brand owner* — an entity, including independent or captive device manufacturers, fab-less suppliers, and authorized distributors, but excluding foundries, that is legally responsible for the integrity and performance of a product for sale to buyers.

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

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

4.2.8 *interested party* — any entity, for example, buyers, law enforcement agencies, customs, counterfeiters, etc., that desires to determine the authenticity of a product.

4.2.9 *product* — a single semiconductor device or circuit or a unit of packaged ones, usually in a sealed box for logistics or distribution.

4.2.10 *registry* — a list of approved ASBs that is maintained by an independent standards authority so that interested parties can verify the qualifications of ASBs.

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

² American National Standards Institute, 25 West 43rd Street, New York, NY 10036, USA; Telephone: +1.212.642.4900, Fax: +1.212.398.0023, <http://www.ansi.org>

³ Object Management Group, Inc., 109 Highland Ave., Needham, MA 02494, USA; Telephone: +1.781.444.0404, Fax: +1.781.444.0320, <http://www.omg.org>

4.2.12 *trusted, adj.* — a type of brand owner that has established its identity and purpose to the satisfaction of an ASB.

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.

NOTE 5: 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. Also refer to http://www.omg.org/gettingstarted/what_is_uml.htm#12DiagramTypes for UML diagram types.

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

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.

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 *Req’d* — Is this attribute required? Y – Yes, or N – No.

5.1.5.3 *Form* — The form of attributes in this Specification may be a string or an integer.

Table 1 Attribute Table Format

<i>Attribute Name</i>	<i>Definition</i>	<i>Access</i>	<i>Req’d</i>	<i>Form</i>
		RO or RW	Y or N	String or Integer

6 Requirements

6.1 Figure 1 is a diagram that shows typical activity and possible timing of authentication of products, verification of codes, and termination of authentication. Error messages sent when a service request fails are not indicated here.