SEMI T20.3-0710 (Reapproved 0322)
SPECIFICATION FOR SERVICE COMMUNICATION 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 June 2010; previously published April 2016.

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 authentic products have specific identification; for example, an unpredictable random code issued by some authentication organization, on them most (but not all) counterfeits can be detected 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 one element of a suite of Standards[1] aimed at enabling automated, reliable, and secure product authentication for the semiconductor industry, thereby reducing the presence of illegal counterfeit items in the marketplace.

1.3.1.2 It provides an XML schema that corresponds to the product authentication objects, attributes, and associations described in SEMI T20 that enable automated, reliable and secure product authentication for the semiconductor industry.

1.3.1.3 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 and is also included as appendices to this Standard.

2 Scope

2.1 This Specification 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 Specification provides any interested party (without restriction) the communication protocols to check the authentication of a product within the supply chain.

2.3 This Specification also covers implementation of SEMI T20 services using web services.

[1] This suite of Standards was 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.

Documents Document Sharing Hub
Full document details: SEMI T20.3-0710-0322R

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 Limitations

3.1 This Specification 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 Specification.

4 Referenced Standards and Documents

4.1 *SEMI Standards and Safety Guidelines*

SEMI E121 — Guide for Style and Usage of XML for Semiconductor Manufacturing Applications

SEMI T20 — Specification for Authentication of Semiconductors and Related Products

SEMI T20.1 — Specification for Object Labeling to Authenticate Semiconductors and Related Products in an Open Market

SEMI T20.2 — Guide for Qualifications of Authentication Service Bodies for Detecting and Preventing Counterfeiting of Semiconductors and Related Products

4.2 *OMG Standards*[2]

OMG formal/2007-11-02 — Unified Modeling Language Superstructure, v2.1.2

OMG formal/2007-11-04 — Unified Modeling Language Infrastructure, v2.1.2

4.3 *World Wide Web Consortium Documents*[3]

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

Web Services Architecture (Working Draft 8)

Web Services Glossary (Working Draft 8)

Namespaces in XML[4]

XML Schema Part 0: Primer[5]

XML Schema Part 1: Structures[6]

XML Schema Part 2: Datatypes[7]

XML Path Language (Xpath)[8]

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

5 Terminology

5.1 Many terms, acronyms and symbols associated with anti-counterfeiting techniques are listed in SEMI T20.

---

[2] Object Management Group, 140 Kendrick Street, Building A, Suite 300, Needham, MA 02494, USA. Telephone: +1.781.444.0404; Fax: +1.781.444.0320; http://www.omg.org.

[3] World Wide Web Consortium documents are available from Massachusetts Institute of Technology Laboratory for Computer Science, 200 Technology Square, Cambridge, MA 02139, USA. Telephone: +1.617.253.2613; Fax: +1.617.258.5999; http://www.w3.org/TR/REC-xml.

[4] http://www.w3.org/TR/1999/REC-xml-names-19990114/

[5] http://www/w3/org/TR/xmlschema-0/

[6] http://www/w3/org/TR/xmlschema-1/

[7] http://www/w3/org/TR/xmlschema-2/

[8] http://www/w3/org/TR/xpath/

Documents
Document Sharing Hub

Full document details: SEMI T20.3-0710-0322R

5.2 Other terminology used in this Specification is as follows:

5.2.1 *Abbreviations and Acronyms*

5.2.1.1 *SOAP* — Simple Object Access Protocol

5.2.1.2 *UML* — Unified Modeling Language

5.2.1.3 *W3C* — World Wide Web Consortium

5.2.1.4 *WSDL* — Web Service Definition Language

5.2.1.5 *XML* — eXtensible Markup Language

5.2.1.6 *XSD* — XML Schema Definition

5.2.2 *Definitions*

5.2.2.1 *eXtensible Markup Language (XML)* — a markup language used for representing data rich with context and content in documents and in communications. XML is an extension of SGML, a document-oriented markup language. It was created by the W3C for use on the Internet. XML can represent object-oriented structures.

5.2.2.2 *Unified Modeling Language (UML)* — a notation for representing object-oriented designs and views.

6 Conventions

6.1 This Standard follows the guidelines for XML as outlined in SEMI E121.

6.2 The user of this Specification is expected to have a working knowledge of the UML, XML, and Schema specifications. This Specification does not provide tutorial information on these subjects.

7 Services Mapping

7.1 The actual WSDL service definitions are contained in separate documents and in Appendices 1 through 4. The contents of the WSDL service definitions documents constitute the core part of this Specification.

7.2 *Error Handling* — If the service body encounters an error an HTTP 500 'Internal Server Error' response is returned including a SOAP Fault element, containing code, string, actor and detail. Actor and detail are provided by the service provider. The strings and codes for the reserved errors are shown in Table 1. See the architecture standard for which reserved errors can be generated by each service.

Table 1 Mapping Errors to SOAP Faults

Code	*String*	*Description*
1	ServiceNotAvailable	ASB server is down or otherwise unavailable.
2	CodeDoesNotExist	Code is not authentic or has been terminated.
3	InactiveCode	The requested code has been marked as inactive.
4	RequestDenied	Requester not an ASB trusted BrandOwner.

7.3 *Registry Services Mapping* — Table 2 shows the web services to be provided by the Registry and how they map to the services described in SEMI T20.

Documents Document Sharing Hub

Full document details: SEMI T20.3-0710-0322R

Table 2 Registry Services Message Mapping

Service Name	*Web Service*	*Comments*
List	List	List the ASB name, ASB URL, ASB level of certification, and date of registration on the Registry website and advise the ASB that the registration is complete. Information listed is that provided by the ASB to the Registry.
Update	Update	Update the ASB name, ASB URL, ASB level of certification, and date of registration on the Registry website and advise the ASB that the registration is updated. Information listed is that provided by the ASB to the Registry in its annual (or more frequent) reconfirmation of its registration.

7.3.1 *List Service* — Table 3 shows how the service parameters described in SEMI T20 map to the web service parameters.

Table 3 List Service Parameters Mapping

Parameter Name	*Required*	*Web Service Parameter*	*Type*	*Parameter Value Range*
ASB name	Y	ASBId	String	Identifier of responsible ASB marked on product.
ASB URL	Y	ASBURI	String	URL of responsible ASB.
ASB Level of Certification	Y	ASBLevelOfCertification	string	Third party level of certification of the information, supply, and operational security of the ASB.
Date of Registration	Y	DateOfRegistration	string	Date on which the Registry posts the initial or updated information from and ASB on the Registry Web site.

7.3.2 *Update Service* — Table 4 shows how the service parameters described in the architecture standard map to the web service parameters.

Table 4 Update Service Parameters Mapping

Parameter Name	*Required*	*Web Service Parameter*	*Type*	*Parameter Value Range*
ASB name	Y	ASBId	string	Identifier of responsible ASB marked on product.
ASB URL	Y	ASBURI	string	URL of responsible ASB.
ASB Level of Certification	Y	ASBLevelOfCertification	string	Third party level of certification of the information, supply, and operational security of the ASB.
Date of Registration	Y	DateOfRegistration	string	Date on which the Registry posts the initial or updated information from and ASB on the Registry Web site.

7.4 *ASB Services Mapping* — Table 5 shows the web services to be provided by an ASB and how they map to the services described in SEMI T20.

Documents
Document Sharing Hub

Full document details: SEMI T20.3-0710-0322R

Table 5 ASB Services Message Mapping Table

Service Name	*Web Service*	*Comments*
Request	RequestCodes	Generate and return a number of Authentication codes for a specified Product in response to a request from the BrandOwner of that Product. If service is unsuccessful, return an error.
Verify	Verify	Verify that the specified Authentication code is valid. If so, increment the number of verifications and return the Product message. If service is unsuccessful, return an error.
Deactivate	Deactivate	Deactivate an active Authentication code. Future attempts to Verify will fail. If service is unsuccessful, return an error.
Activate	Activate	Activate an Authentication code that has been deactivated. Future attempts to Verify will succeed. If service is unsuccessful, return an error.
Terminate	Terminate	Close out an Authentication code as requested by the BrandOwner. Future attempts to Verify will not succeed. If service is unsuccessful, return an error.

7.4.1 *Request Service* — Table 6 shows how the service parameters described in SEMI T20 map to the web service parameters.

Table 6 Request Service Parameter Mapping

Parameter Name	*Required*	*Web Service Parameter*	*Type*	*Parameter Value Range*
Product	Y	Product	string	Valid product.
Count	Y	Count	nonNegativeInteger	>0
Codes	Y	Codes	ArrayOfString	The number of Codes returned should equal the Count specified.

7.4.2 *Verify Service* — Table 7 shows how the service parameters described in SEMI T20 map to the web service parameters.

Table 7 Verify Service Parameter Mapping

Parameter Name	*Required*	*Web Service Parameter*	*Type*	*Parameter Value Range*
Code	Y	Code	string	Valid authentication code.
BrandOwner	Y	BrandOwner	string	Name of BrandOwner of Product.
Product	Y	Product	string	Product information returned if code is valid.

7.4.3 *Deactivate Service* — Table 8 shows how the service parameters described in T20 map to the web service parameters.

Table 8 Deactivate Service Parameter Mapping

Parameter Name	*Required*	*Web Service Parameter*	*Type*	*Parameter Value Range*
Code	Y	Code	string	Valid authentication code.

7.4.4 *Activate Service* — Table 9 shows how the service parameters described in SEMI T20 map to the web service parameters.

Documents Document Sharing Hub
Full document details: SEMI T20.3-0710-0322R