

SEMI T21-0314

SPECIFICATION FOR ORGANIZATION IDENTIFICATION BY DIGITAL CERTIFICATE ISSUED FROM CERTIFICATE SERVICE BODY (CSB) FOR ANTI-COUNTERFEITING TRACEABILITY IN COMPONENTS SUPPLY CHAIN

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 December 23, 2013. Available at www.semiviews.org and www.semi.org in March 2014; originally published February 2012.

1 Purpose

1.1 Counterfeiting is a serious and growing problem in the worldwide industry. Various risks to the human security and life have become extremely high, when such counterfeited products are used in cars, and medical equipment, for example. One of the effective measures is introducing track and traceability supply chain system to identify all the buyers of components. In order to identify all the buyers of components within the logistics world, it is necessary to specify the identification of components, container-box, and the organization.

NOTE 1: The method of identifying the components and container box in the logistics is specified by the SEMI draft document for Specification for Traceability by Self Authentication Service Body and Authentication Service Body which is under development.

1.1.1 *Common Form of the Certificate Profile* — There is an effective method of using X.509 certificate¹ for identifying buyers in supply chain track and trace system. It is important that the organization information recorded on the certificate not only be correct, but to enable automation of track. Because the profile which X.509 defines has some ambiguity, it is necessary to standardize profiles into a common form.

1.1.2 *CSB's Accreditation Criteria* — In order to make the anti-counterfeiting track and trace truly effective, the interoperation of CSB are required. In order to verify X.509 certificates issued from many CSBs, each CSB needs to be chained with the public rootCA.

2 Scope

2.1 Common form of the certificate profile.

2.2 CSB's accreditation criteria.

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 *SEMI Standards and Safety Guidelines*

SEMI T20 — Specification for Authentication of Semiconductors and Related Products

NOTE 2: The SEMI global Traceability Committee is developing a Specification for Traceability by Self Authentication Service Body and Authentication Service Body intended to be used in conjunction with this Document.

3.2 *ISO Standards*²

ISO 3166-1 — Codes for the representation of names of countries and their subdivisions, Part 1: Country codes

ISO/IEC 9594-8/ITU-T Rec. X.509 — Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

¹ Although use of the certificate is an option, it shall be based on the common form when using it. It is transmitted to the supply chain track and trace system by SSL client authentication. It follows the privacy laws of the provinces, states and country when recording personal information on it.

² International Organization for Standardization, ISO Central Secretariat, 1 rue de Varembé, Case postale 56, CH-1211 Geneva 20, Switzerland; Telephone: 41.22.749.01.11, Fax: 41.22.733.34.30, <http://www.iso.ch>

3.3 ETSI Standards³

ETSI TS 102042 — Electronic Signatures and Infrastructures (ESI); Policy Requirement for Certification Authorities Issuing Public Key Certificates

3.4 Other Documents

WebTrust for CA — CA criteria designated from many browsers.⁴

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

4 Terminology

4.1 Abbreviations and Acronyms

4.1.1 CA — certification authority

4.1.2 CSB — certificate service body

4.1.3 TTP — trusted third party

4.2 Definitions

4.2.1 *certificate service body (CSB)* — profit and nonprofit body which is issuing certificate.

4.2.2 *public rootCA* — rootCA by which the certificate is registered in common operating systems (OS) and browsers.

4.2.3 *rootCA* — rootCA is the CA that is at the top of a certification hierarchy.

4.2.4 *SSL* — The protocol which enciphers information and communicates on the Internet; Or send/receive exclusively encrypted information.

5 Requirements

5.1 Common Form of the Certificate Profile

5.1.1 Because the profile which X.509 defines has some ambiguity, it is necessary to standardize profiles into a common form.

5.1.2 The common form shall compact fields as much as practical so that many logs can be recorded into supply chain track and trace system.

5.1.3 The common form is shown in Tables 1 and 2.

Table 1 Basic Certificate Fields

Certificate Fields	Data Type (number of characters)	Definition It shall use alphanumeric characters (capital letters are included), HYPHEN, SPACE, and PERIOD.	Example	
			For personnel	For section/role
Subject				
CountryName	Printable String (2)	<u>Mandatory:</u> The two character country code in alpha-2 of ISO3166-1 All capital letter	JP	

³ The European Telecommunications Standards Institute, ETSI Secretariat, 650 Route des Lucioles 06921 Sophia-Antipolis Cedex, France; Telephone: 33.0.4.92.94.42.00, Fax: 33.0.4.93.65.47.16, <http://www.etsi.org/website/homepage.aspx>

⁴ Robert Gold, Managing Partner at Bennett Gold LLP, Chartered Accountants, Toronto, Canada; Telephone: 416.449.2249, Fax: 416.449.4133, <http://www.webtrust.net>

Certificate Fields	Data Type (number of characters)	Definition It shall use alphanumeric characters (capital letters are included), HYPHEN, SPACE, and PERIOD.	Example	
			For personnel	For section/role
Subject				
StateName	Printable String (128)	<u>Mandatory</u> ^{#1} : Name of State, Province, etc. A head character is a capital letter.	Tokyo	
LocalityName	Printable String (128)	<u>Mandatory</u> ^{#2} : Name of City, etc. A head character is a capital letter. A delimiter is a hyphen.	Minato-ku	
OrganizationName	Printable String (64)	<u>Mandatory</u> ^{#3} : Name of Organization.	JIPDEC	
OrganizationUnit Name1	Printable String (64)	<u>Mandatory</u> ^{#4} : Unique number, which CSB manages. This value shall be set up together with OrganizationUnitName2 so that this certificate shall become unique. In order to distinguish in automatic tracking, it shall attach the Prefix “OU1-”.	OU1-1.2.392.200063.80.1.1	
OrganizationUnit Name2	Printable String (64)	<u>Mandatory</u> ^{#5 #6 #7} : Local number which organization manages. In order to distinguish in automatic tracking, it shall attach the Prefix “OU2-”.	OU2-007	
CommonName	Printable String (64)	<u>Mandatory</u> ^{#8} : Subject’s name (real name, section name, role or ID). In order to distinguish in automatic tracking, it shall attach the prefix “BN-” (business name which used as a formal common name in the organization, such as a real name and maiden name), “BO-” (organization/role), or “ID-”.	BN-Smith	BO-Supply(Mngr.)

#1 May be SPACE, because reservation of a memory space is aim of mandatory.

#2 May be SPACE, because reservation of a memory space is aim of mandatory.

#3 Registered in DUNS, etc.

#4 Can be used as a pointer to the open attribute information (the company name, etc. which cannot be written with the alphabet), which could not be recorded on the certificate.

#5 Can be used as a pointer to the secret attribute information (section name, etc.), which could not be recorded on the certificate.

#6 May set up values other than a pointer use.

#7 May be SPACE, because reservation of a memory space is aim of mandatory.

#8 About pseudonym, it will decide in the future.

Table 2 Standard Certificate Extensions

Certificate Fields	Data Type <i>(number of characters)</i>	Definition	Example	
			<i>For personnel</i>	<i>For section/role</i>
subjectAltName				
rfc822Name	IA5String (255)	<u>Option:</u> Subject's email address	smith@jipdec.or.jp	supply@jipdec.or.jp

5.2 *CSB's Accreditation Criteria*

5.2.1 Each CSB needs to be chained with the public rootCA accredited by the following criteria:

5.2.1.1 ETSI TS 102042

5.2.1.2 WebTrust for CA

5.2.2 Identification of certificate subjects shall be periodically audited by TTP.

RELATED INFORMATION 1 SUPPLEMENTARY EXPLANATION

NOTICE: The material in this Related Information is not an official part of SEMI T21 and was derived from the work of the global Traceability Technical Committee. This Related Information was approved for publication by full letter ballot procedures on December 24, 2011.

R1-1 Starting Point

R1-1.1 Counterfeiting is a serious and growing problem in the worldwide industry. Various risks on the human security and life have become extremely high, when such counterfeited products are used in cars, and medical equipment, for example. One of the effective measures is introducing track and traceability supply chain system to identify all the buyers of components.

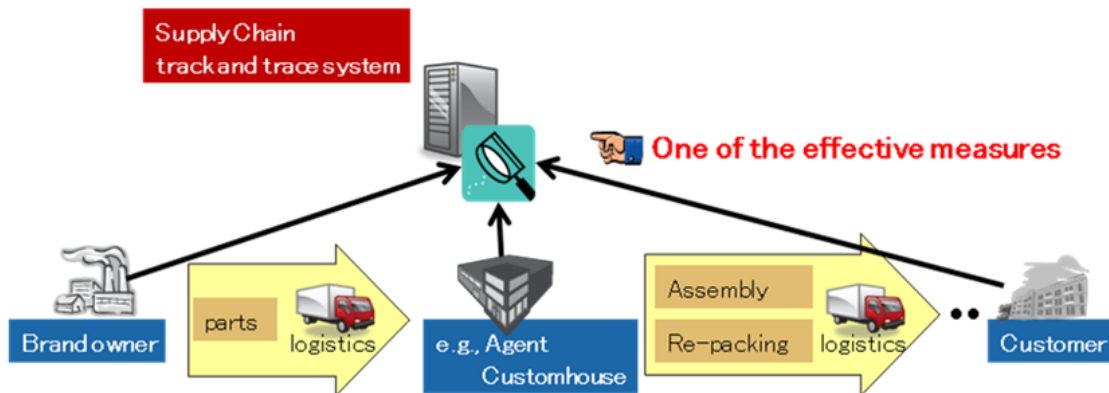


**Figure R1-1
Starting Point**

R1-2 Relation between This Specification and The Principle of ISO/PC246

R1-2.1 The following figure refers to a principle of the supply chain track and trace system proposed from AFNOR at ISO/PC246 meeting in March 2009. In order to identify all the buyers of components within logistics, it is necessary to specify the identification of components, container-box, and the organization.

NOTE 3: The method of identifying the components and container box in the logistics is specified by the SEMI Draft Document for Specification for Traceability by Self Authentication Service Body and Authentication Service Body.