Background Statement for SEMI Draft Document 4845
NEW STANDARD: Specification for Organization Identification by Digital Certificate Issued from CSB（Certificate Service Body） for Anti-Counterfeiting Traceability in Components Supply Chain

Note: This background statement is not part of the balloted item. It is provided solely to assist the recipient in reaching an informed decision based on the rationale of the activity that preceded the creation of this document.

Note: Recipients of this document are invited to submit, with their comments, notification of any relevant patented technology or copyrighted items of which they are aware and to provide supporting documentation. In this context, "patented technology" is defined as technology for which a patent has issued or has been applied for. In the latter case, only publicly available information on the contents of the patent application is to be provided.

Background Statement

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 methods to validate the integrity of goods from non-certified distributors or suppliers. SEMI T20 was formed to solve such this problem.

There are different types of semiconductor devices, whose commercial distributions are diverse. For example, in the semiconductor devices mainly for business-to-business transactions and intended for the use in automobiles and the like, it is required to realize measures against counterfeit products and quality traceability at the same time. Such applications are not supported in SEMI T20.

With an aim to realize the said requirements, this document proposes a mechanism to be offered to the users with such requirements.

This informational (blue) ballot will be discussed at the Japan Traceability Committee Meetings on September 24th at SEMI Japan Tokyo Office.

Semiconductor Equipment and Materials International
3081 Zanker Road
San Jose, CA 95134-2127
Phone:408.943.6900 Fax: 408.943.7943

DRAFT
Document Number: 4845
Date: 2010/08/23

INFORMATIONAL (BLUE) BALLOT

SEMI Draft Document 4845
NEW STANDARD: Specification for Organization Identification by Digital Certificate Issued from CSB （Certificate Service Body ） for Anti-Counterfeiting Traceability in Components Supply Chain

1 Purpose

1.1 Counterfeiting is a serious and growing problem in the worldwide electronics industry. According to this problem, risk on the human life has become extremely high, when such products are used in cars, medical equipments, or etc. One of the effective measures is to identify all the buyers of components using Supply Chain trace system. In order to identify all the buyers of components within logistics, it is necessary to specify the identification of components, container-box[1] , and the organization.

1.1.1 *The Common Form to The Portion of The X.509 Certificate* — There is an effective method of using the X.509 certificate for identifying buyers in Supply Chain trace system. In order to quickly and reliably identify the suspicious organization contaminated by counterfeit components, the organization's contact information must be correct, common and compact. This standard provides the correct, common and compact form of the organization's contact information, recorded on the X.509 certificate.

1.1.2 *CSB* — In order to make the anti-counterfeiting trace truly effective, the interoperation of CSB will be required. Because the counterfeit component may be mixed in international Supply Chain, some international management criteria for the interoperation of CSB is needed. Concurrently, the international framework will be required. That promotes the accreditation of CSB which makes the anti-counterfeiting trace truly effective.

2 Scope

2.1 The form of the organization contact information, recorded on X.509 digital certificate.

2.2 CSB's management criteria

NOTICE: This safety guideline does not purport to address all of the safety issues associated with its use. It is the responsibility of the users of this safety guideline 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 Documents*

SEMI Document 4847 — Traceability by Self Authentication Service Body and Authentication Service Body

3.2 *International Telecommunication Union (ITU)* [2]

ITU-T Recommendation X.509 (2005) — Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, 08/05

3.3 *The European Telecommunications Standards Institute (ETSI)* [3]

ETSI TS 102042 — Electronic Signatures and Infrastructures (ESI); Policy requirement for certification authorities issuing public key certificates

4 Terminology

4.1 Abbreviation and Acronyms

4.1.1 *TTP* — Trusted Third Party

[1] The method of identifying the components and container box in the logistics is specified by SEMI Document 4874.

[2] International Telecommunication Union (ITU), Place des Nations 1211 Geneva 20 Switzerland; http://www.itu.int/en/pages/default.aspx

[3] ETSI Secretariat, 650, Route des Lucioles 06921 Sophia-Antipolis Cedex, FRANCE Tel.: +33 (0)4 92 94 42 00 Fax: +33 (0)4 93 65 47 16 ; http://www.etsi.org/website/homepage.aspx

4.1.2 *CSB*[4] — Certification Service Body

4.2 Definitions

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

5 Requirements

5.1 *The Advantages of The Method of Using The X.509 Certificate* — Counterfeiting is a serious and growing problem in the worldwide electronics industry. According to this problem, risk on the human life has become extremely high, when such products are used in cars, medical equipments, or etc. One of the effective measures is to identify all the buyers of components using Supply Chain trace system. 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. There is an effective method of using the X.509 certificate[5] for identifying buyers in Supply Chain trace system. In order to quickly and reliably identify the suspicious organization contaminated by counterfeit components, the organization's contact information must be correct, common and compact. The advantages of the method are shown as follows.

5.1.1 Because the organization's contact information on a digital certificate is identified by TTP, it can be reliable.

5.1.2 Because digital certificate can use SSL, therefore, encrypted communication and identification of both the client and the server will be supported.

5.1.3 Because the X.509 certificates are already supported with common OS or many generally available applications, proposed system will be made without any special software.

5.2 The Requirements Which Makes The Anti-counterfeiting Trace Truly Effective By The Method Using The X.509 Certificate

5.2.1 The Common Form to The Portion of The X.509 Certificate

5.2.1.1 The standard which defines the profile of the digital certificate exists only in the ITU-T Recommendation X.509. However, because the profile which X.509 defines has some ambiguity, and in order to enable automatic processing, it is necessary to specify the common form of the organization contact information, recorded in X.509 certificate. The requirements for a common form are shown as follows.

5.2.1.1.1 Organization's contact information must be correct so that it can be used for the contact to the organization.

5.2.1.1.2 Organization's contact information must be common so that it can be used in many Supply Chain trace systems.

5.2.1.1.3 Organization's contact information must be compact so that many logs can be recorded into Supply Chain trace system.

5.2.1.2 In addition, in order to use a digital certificate till term-of-validity expiration, it is desirable not to change recorded information. The frequently changed information may be better to record on the repository of the certificate authority without recording it on the digital certificate. In accessing the above-mentioned repository, it is necessary to set up URL of the repository, OID which identifies an organization, and the local number managed in the organization. The requirements for common form[6] are shown as follows.

(a) Subject: "Basic Certificate Fields"

① Country Name (Mandatory)
The two character country code in Latin alphabet in alpha-2 of ISO3166-1.
※Data type (the number of characters): Printable String(2)

② State Name (Mandatory)

[4] CSB is synonymous as TTP.

[5] A digital certificate is used as a secure envelope which stores the contact information of the access organization (Therefore, the secure envelope shall not be used for an electronic signature nor electronic authentication).

[6] Any option on a common form shall not be deleted.

Name of State, Province, etc.
※Data type (the number of characters): Printable String(32)
③ Locality Name (Mandatory)
Name of City, etc
※Data type (the number of characters): Printable String(32)
④ Organization Name (Mandatory)
Organization Name (full name in alphabet characters)
※Data type (the number of characters): Printable String(64)
⑤ Organization UnitName1 (Mandatory)
OID defined by ISO (Object IDentifier)
※Data type (the number of characters): Printable String(64)
⑥ Organization UnitName2 (Mandatory)
Local number which the organization manages
※Data type (the number of characters): Printable String(64)
⑦ Organization UnitName3 (Mandatory)
URL which exhibits the table of the organization's contact information which was unable to be recorded on the X.509 certificate.
e.g. Organization address
※Data type (the number of characters): Printable String(64)
⑧ Organization UnitName4 (Mandatory)
Unit name, Department name, etc.
※Data type (the number of characters): Printable String(64)
⑨ Organization UnitName5 (Option)
The organization's international telephone number
※Data type (the number of characters): Printable String(64)
⑩ Common Name (Mandatory)
Subject real name or pseudonym or ID
(Divide it to distinguish real name from pseudonym/ID.)
e.g. PN-Bond, ID-007
※Data type (the number of characters): Printable String(64)

(b) subjectAltName: "Standard Certificate Extensions"
① rfc822Name (Option)
Subject's e-mail address
※Data type (the number of characters): IA5String(128)

5.2.2 CSB's Management Criteria

5.2.2.1 In order to make the anti-counterfeiting trace truly effective, the interoperation of CSB will be required. Because the counterfeit component may be mixed in international Supply Chain, some international management criteria for the interoperation of CSB is needed. Concurrently, the international framework will be required. That promotes the accreditation of CSB which makes the anti-counterfeiting trace action truly effective. Regarding the international framework, it should not be discussed here because it is not direct issue for standard[7].

5.2.2.2 Although there is the following problem issue, ETSI-TS-102042 and Webtrust will stay as current management criteria.

5.2.2.2.1 ESTI is dependent on the specifics of EU countries.

5.2.2.2.2 Because Webtrust is operated only by accountants, the principle of market mechanism is not working there.

[7] Based on the member's opinion of SEMI in each country, SEMI may act as such international framework for the time being.

5.2.2.3 CSB's management criteria which are proposed in reference to the criteria of Digital Signature Act of Japan by putting into the chapter structure of ETSI-TS-102042 are shown as follows.

① Obligations and liability

i. CSB obligations

For example, the following item should be written.

・Guarantee and warranty

・Fee or its written URL

ii. Subscriber obligations

For example, the following item should be written.

・Submission without any untruth

・Management of the user signature key, activation PIN, and etc.

・Revocation when a signature key carries out a compromise, and etc.

iii. Information for relying parties

For example, the following item should be written.

・Publication of CA certificate, CP/CPS, CRL, and etc.

iv. Liability

For example, the following item should be written.

・Disclaimers or limitations of liability in accordance with applicable laws.

② Requirements on CA practice

i. Certification practice statement

For example, the following item should be written.

・Publication of contact information, operating information, etc.

ii. Public key infrastructure - Key management life cycle

For example, the following item should be written.

・CA key's generation, management, etc.

iii. Public key infrastructure - Certificate management life cycle

For example, the following item should be written.

・Identification, revocation conditions, etc.

iv. CA management and operation

For example, the following item should be written.

・security management, protection of personal information, record preservation, termination, termination, etc.

v. Organizational

For example, the following item should be written.

・Ensure that its organization is reliable

③ Framework for the definition of other certificate policies

i. Certificate policy management

For example, the following item should be written.

・Approval

ii. Additional requirements

For example, the following item should be written.

・Specific policy adds to or further constrains the requirements of the certificate policy for subscribers and relying parties

iii. Conformance

For example, the following item should be written.

・Conformance to the present document and the applicable certificate policy

Semiconductor Equipment and Materials International
3081 Zanker Road
San Jose, CA 95134-2127
Phone:408.943.6900 Fax: 408.943.7943

RELATED INFORMATION 1
SUPPLEMENTARY EXPLANATION

NOTICE: This related information is not an official part of this standard and was derived from (**origin of information**). This related information was approved for publication by (**method of authorization**) on (**date of approval**).

R1-1 The Starting Point of This Specification

R1-1.1 Counterfeiting is a serious and growing problem in the worldwide electronics industry. According to this problem, risk on the human life has become extremely high, when such products are used in cars, medical equipments, or etc. One of the effective measures is to identify all the buyers of components using Supply Chain trace system.

R1-1.1.1 The anti-counterfeiting activity is performed after receiving returned goods. (as shown by 2 of Figure R1-1) The main problems of this measure are that all the buyers of components cannot identify in Supply Chain.

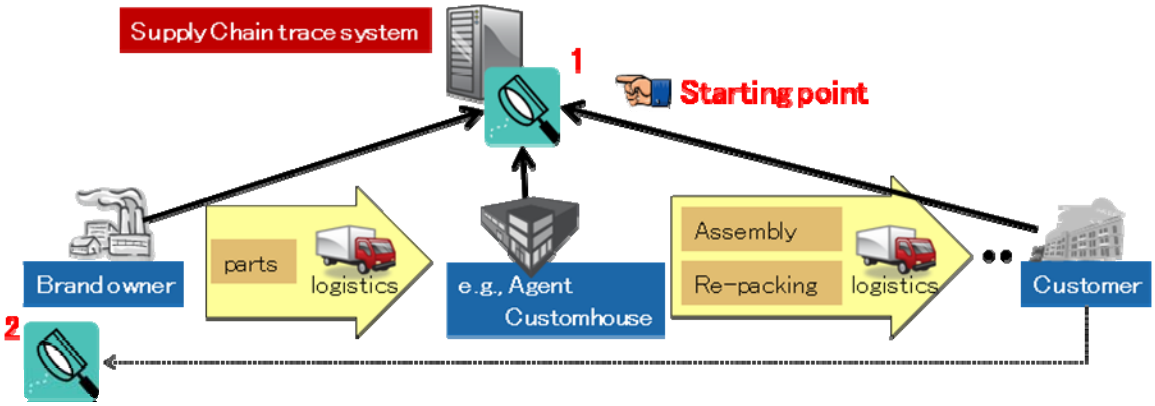

Figure R1-1
The Starting Point of This Specification

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

The following figure refers to a principle of the Supply Chain trace system proposed 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[8], and the organization.

[8] The method of identifying the components and container-box in the logistics is specified by the SEMI international standards 4847 (T20).

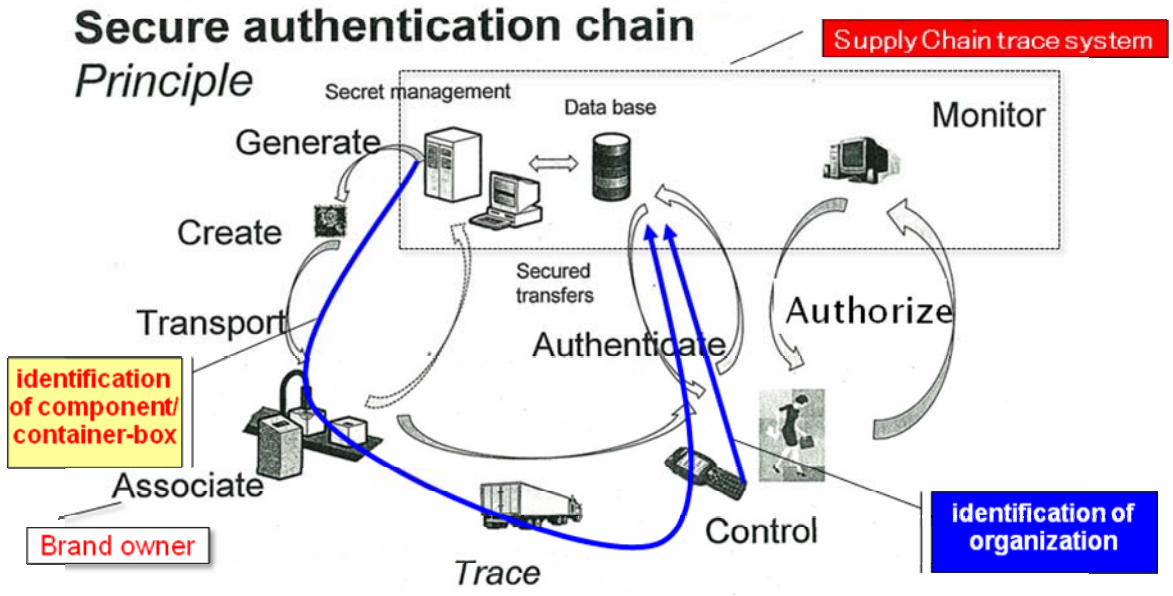

Figure R1-2
Relation between This Specification and The Principle of ISO/PC246

R1-3 Method of Organization Identification

R1-3.1 There is an effective method of using the X.509 certificate[9] for identifying buyers in Supply Chain trace system. In order to quickly and reliably identify the suspicious organization contaminated by counterfeit components, the organization's contact information must be correct, common and compact. The advantages of the method are shown as follows.

R1-3.1.1 Because the organization's contact information on a digital certificate is identified by TTP[10], it can be reliable.

R1-3.1.2 Because digital certificate can use SSL, therefore, encrypted communication and identification of both the client and the server will be supported.

R1-3.1.3 Because the X.509 certificates are already supported with common OS or many generally available applications, proposed system will be made without any special software.

[9] Here, a digital certificate is used as a secure envelope which stores the contact information of the access organization (Therefore, the source envelope shall not be used for an electronic signature nor electronic authentication).

[10] Here, CSB is synonymous as TTP.

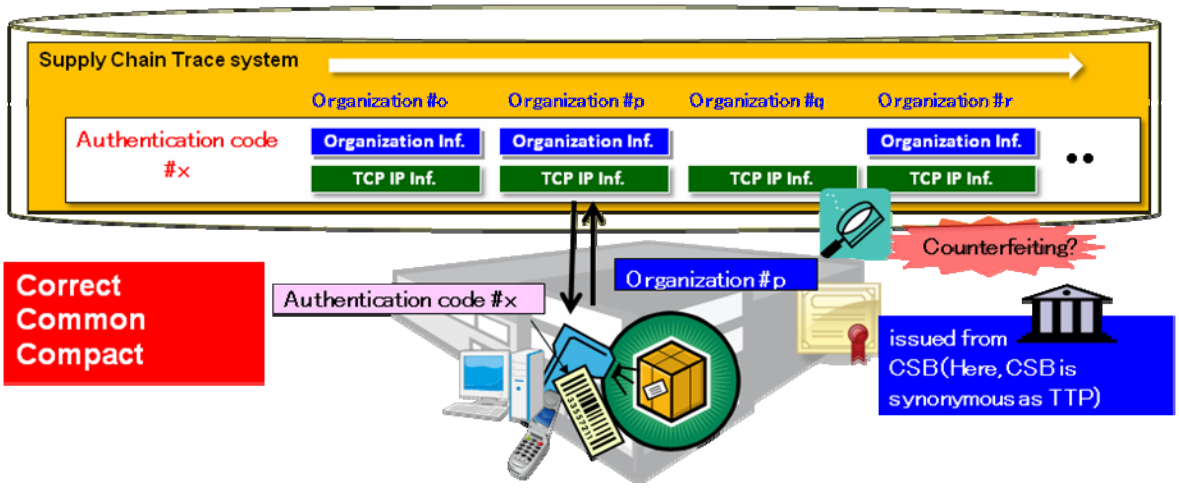

Figure R1-3
Method of Organization Identification

R1-4 The Common Form to The Portion of The X.509 Certificate

R1-4.1 The standard which defines the profile of the digital certificate exists only in the ITU-T Recommendation X.509. However, because the profile which X.509 defines has some ambiguity, and in order to enable automatic processing, it is necessary to specify the common form of the organization contact information, recorded in X.509 certificate. The requirements for a common form are shown as follows.

R1-4.1.1 Organization's contact information must be correct so that it can be used for the contact to the organization.

R1-4.1.2 Organization's contact information must be common so that it can be used in many Supply Chain trace systems.

R1-4.1.3 Organization's contact information must be compact so that many logs can be recorded into Supply Chain trace system.

R1-4.2 In addition, in order to use a digital certificate till term-of-validity expiration, it is desirable not to change recorded information. The frequently changed information may be better to record on the repository of the certificate authority without recording it on the digital certificate. In accessing the above-mentioned repository, it is necessary to set up URL of the repository, OID which identifies an organization, and the local number managed in the organization. The requirements for common form are shown as follows.

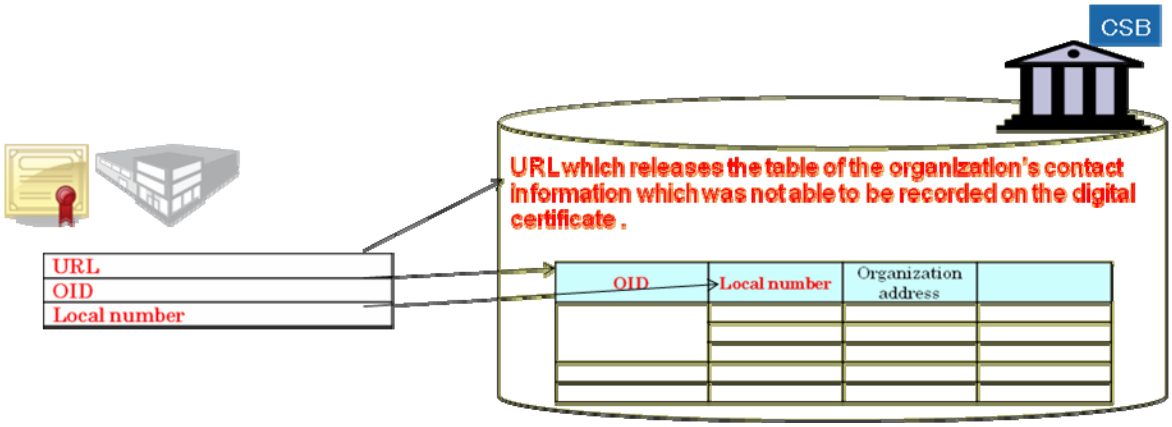

Figure R1-4
The Record Method of The Frequently Changed Information

Table R1-1 Basic Certificate Fields

Certificate Fields	Data type (The number of characters)	For personnel	For section/role	
Subject				
Country Name	Printable String (2)	JP		**Mandatory** The two (Latin alphabet) character country code of ISO3166-1 alpha-2
State Name	Printable String (32)	Tokyo		**Mandatory** State, Province Name, etc.
Locality Name	Printable String (32)	Minato-Ku		**Mandatory** City name, etc
Organization Name	Printable String (64)	JIPDEC		**Mandatory** Organization Name (alphabetic character full name)
Organization UnitName1	Printable String (64)	1.2.392.200063		**Mandatory** OID defined by ISO (Object IDentifier)
Organization UnitName2	Printable String (64)	007		**Mandator** Local number which the organization manages
Organization UnitName3	Printable String (64)	http://www.jipdec.or.jp/		**Mandator** URL which exhibits the table of the organization's contact information which was unable to be recorded on the X.509 certificate. e.g. Organization address
Organization UnitName4	Printable String 64)	Supply Department		**Mandatory** e.g. Unit name, Department name, etc.
Organization UnitName5	Printable String (64)	TEL8133436XXXX		Option The organization's international telephone number
Common Name	Printable String (64)	smith	supply	**Mandatory** Subject real name or pseudonym or number

Table R1-2 Standard Certificate Extensions

Certificate Fields	Data type (The number of characters)	For personnel	For section/role	
subjectAltName				
rfc822Name	IA5String (128)	smith @jipdec.or.jp	supply @jipdec.or.jp	Option Subject's e-mail address

R1-5 The Requirements Which Makes The Anti-counterfeiting Trace Truly Effective

R1-5.1 In order to make the anti-counterfeiting trace truly effective, the interoperation of CSB will be required. Because the counterfeit component may be mixed in international Supply Chain, some international management criteria for the interoperation of CSB is needed. Concurrently, the international framework will be required. That promotes the accreditation of CSB which makes the anti-counterfeiting trace action truly effective. Regarding the international framework, it should not be discussed here because it is not direct issue for standard.

R1-5.1.1 Based on the member's opinion of SEMI Standard in each country, the members may act as such international framework for the time being.

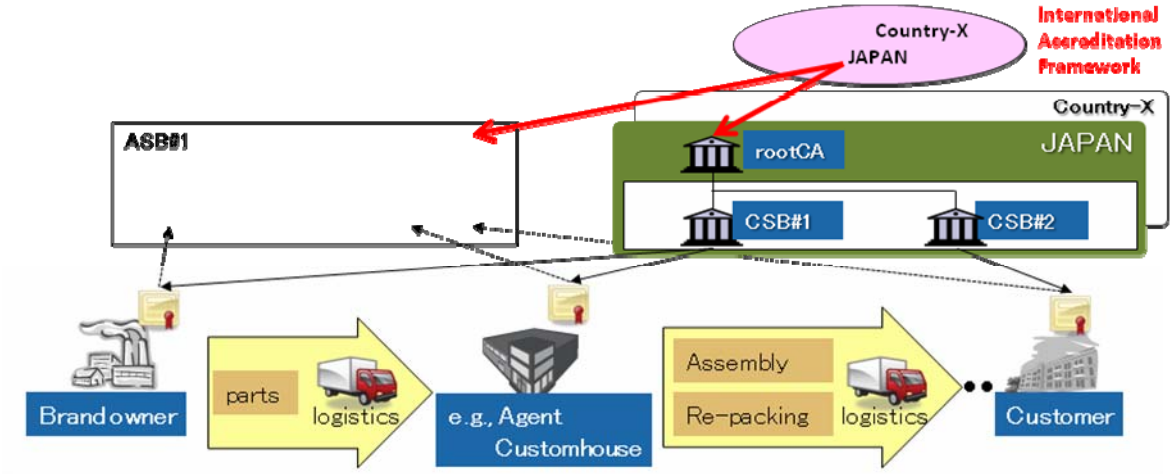

Figure R1-5
The Requirements Which Makes The Anti-counterfeiting Trace Truly Effective

R1-6 CSB's Management Criteria

R1-6.1 Although there is the following problem issue, ETSI-TS-102042 and Webtrust will stay as current management criteria.

R1-6.1.1 ESTI is dependent on the specifics of EU countries.

R1-6.1.2 Because Webtrust is operated only by accountants, the principle of market mechanism is not working there.

R1-6.2 CSB's management criteria which are proposed in reference to the criteria of Digital Signature Act of Japan by putting into the chapter structure of ETSI-TS-102042 are shown as follows. See Table R1-3.

Table R1-3 The Chapter Structure of ETSI-TS-102042

① Obligations and liability *CSB obligations *Subscriber obligations

*Information for relying parties *Liability
② Requirements on CA practice *Certification practice statement *Public key infrastructure - Key management life cycle *Public key infrastructure - Certificate management life cycle *CA management and operation *Organizational
③ Framework for the definition of other certificate policies *Certificate policy management *Additional requirements *Conformance

NOTICE: SEMI makes no warranties or representations as to the suitability of the standards set forth herein for any particular application. The determination of the suitability of the standard is solely the responsibility of the user. Users are cautioned to refer to manufacturer's instructions, product labels, product data sheets, and other relevant literature, respecting any materials or equipment mentioned herein. These standards are subject to change without notice.

By publication of this standard, Semiconductor Equipment and Materials International (SEMI) takes no position respecting the validity of any patent rights or copyrights asserted in connection with any items mentioned in this standard. Users of this standard are expressly advised that determination of any such patent rights or copyrights, and the risk of infringement of such rights are entirely their own responsibility.