Background Statement for SEMI Draft Document 4847
NEW STANDARD: Traceability by Self Authentication Service Body and Authentication Service Body

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: 4847
Date: 2010/08/23

INFORMATIONAL (BLUE) BALLOT

SEMI Draft Document 4847
NEW STANDARD: Traceability by Self Authentication Service Body and Authentication Service Body

1 Purpose

1.1 Damage resulting from counterfeit goods is increasing and however, only the measures to counter counterfeit goods, such as conventional hologram labels, are insufficient. For the future, it will be necessary to give unique authentication codes to individual products and devices in the market for identification.

1.2 Assigning unique codes (authentication codes) to individual products will also lead to prevention of the production of dead copies. Integrated management of authentication codes will also Verification of products because the system will know either of the products is false if the same code is used at different places.

1.3 Meanwhile, collecting information on the pass points of authentication codes allows the shipment process of products to be identified. Once the shipment route of products is defined, the system will see in which stage a counterfeit product has been included.

1.4 Linking the authentication codes assigned to individual devices with the manufacturing data of products also allows traceability of product quality to be obtained.

1.5 These unique authentication codes are embedded within two-dimensional codes. Operation, combining the authentication/verification system by the barcode reader with the mechanism of product shipping process trace or quality trace, permits implementation of efficient measures to counter counterfeit goods and a traceability mechanism.

1.6 In this regard, building an authentication code issuance management and authentication system by a specific ASP costs high and tends to present a problem with its operation.

1.7 Therefore, as a mechanism with a large cost advantage that assimilates problems with the business model of each company and the operation of industries, combination of the SASB (Self Authentication Service Body) offered by each company with the ASB (Authentication Service Body) operated by each industry shall make up the entire system.

1.8 The purpose of this specification is to describe the authentication process to establish trusted identities of products and the mechanism of traceability for establishing identities in the product shipping process and traceability for linking manufacturing conditions.

1.9 This specification is a standard intended to enable reliable and safe product authentication and traceability through systemization for the semiconductor industry. Then, this will reduce the existence of illegal counterfeit items in the market.

1.10 Figure 1 shows the image of the elimination system of counterfeit goods through Verification by using the industrial ASB and SASB.

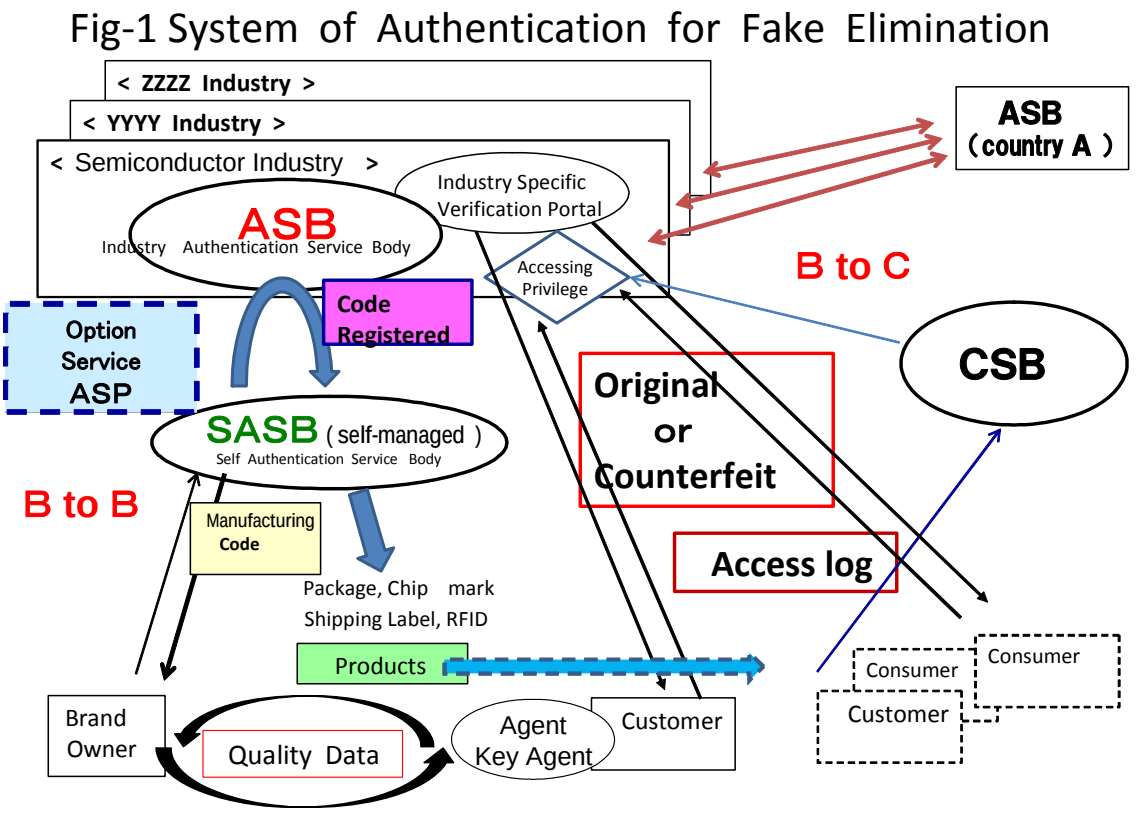

Figure 1 System of Authentication for Fake Elimination

1.11 The Figure 2 shows an image when stamping the authentication codes for device and license plate on devices or displaying them on the outer case, intermediate box, and device tray.

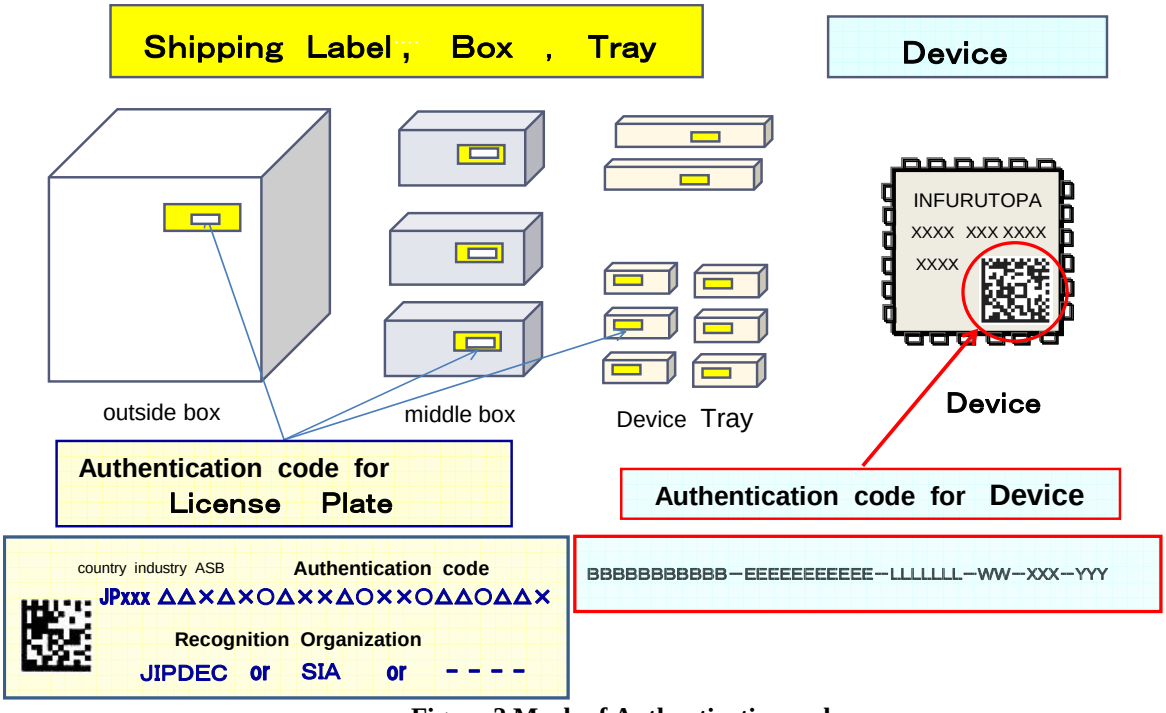

Figure 2 Mark of Authentication code

2 Scope

2.1 These specifications define the structure, behaviors, and services for the organization configuration and objects for authenticating the semiconductors and relevant products using the industrial ASB and SASB.

2.2 These specifications define the structure, behaviors, and services for the configuration and objects for generating the access logs in the distribution points of the semiconductors and relevant products using the industrial ASB and SASB.

2.3 These specifications define the structure, behaviors, and services for the configuration and objects of the quality traceability of the semiconductors and relevant products using SASB.

2.4 These specifications define the requirements and qualifications when industrial ASB offers the services defined in sections 2.1 and 2.2.

2.5 These specifications define the requirements and qualifications when SASB offers the services defined in sections 2.1, 2.2, and 2.3.

2.6 These specifications define the format and content of the authentication codes issued by industrial ASB for devices and license plates.

2.7 These specifications are intended for the verification function in the distribution points. The verification function is not intended to get the product traceability in the supply chain. But, this verification function can be relatively easily extended to the product traceability function by accepting the credit accommodations, if not requesting them, from the buyers in the supply chain.

2.8 These specifications are not intended for the items below:

2.8.1 Label of measures

2.8.2 Communication protocol

2.8.3 Recovery procedure on the occurrence of service error

3 Reference Standards and Documents

3.1 *SEMI Standards and Documents*

SEMI T20 — System Architecture for Preventing / Detecting Semiconductor Counterfeit Products

3.2 *ISO Specification*

ISO 16022 — Information technology, Automatic identification and data capture techniques, Data Matrix bar code symbology specification

3.3 ISO 3166-2 — Codes for the representation of names of countries and their subdivisions, Part 2. Country subdivision code

4 Terminology

4.1 *Abbreviations and Acronyms*

4.1.1 *ASB* — Authentication Service Body

4.1.2 *SASB* — Self Authentication Service Body

4.2 *Definition*

4.2.1 *Industrial ASB* — ASB is an agency to issue and register the authentication codes for products and license plates and offer the scheme for verification using the authentication codes. ASB is an agency to manage the access logs read in the distribution points. ASB is to be set up for each country and industry. Therefore, ASB in this document indicates the ASB for each industry.

4.2.2 *SASB* — SASB is an agent which has the function to associate the authentication codes with the products to which the authentication codes are allocated and the scheme of quality traceability.

4.2.3 *Authentication Code* — Unique and discontinuous code issued by ASB for identifying a device or license plate. The authentication codes consist of authentication codes for devices and authentication codes for license plates for packages and delivery labels.

4.2.4 *Authentication Code for Device* — Unique and discontinuous invalidatable code issued by ASB for allocating it to each semiconductor device.

4.2.5 *Authentication Code for License Plate* — Unique and discontinuous invalidatable code issued by ASB for allocating it to each outer case, intermediate box, and device tray.

4.2.6 *Verification* — Verification is to determine that the goods are not counterfeit by comparing the authentication codes allocated to the devices or license plates with the codes registered in ASB.

4.2.7 *Quality Traceability* — In order to enable the tracing of production history data of device, the association information as a trigger is incorporated into the authentication code for the device. Thus, this quality traceability enables you to trace back to the production history data when identifying the parts configuration of final product or taking measures against a problem in the market. The traceability of the product quality is enabled by associating the authentication code allocated to each device with the product's manufacturing data.

4.2.8 *Access Traceability* — Traceability using the access logs when the authentication code for license plate is read in the distribution point and when the authentication code in ASB is accessed for verification.

4.2.9 *Code Issuance* — The code issuance is a series of operations of generating a code, confirming its uniqueness, registering the code, and issuing (notifying of) the code. The issuance of authentication code has the functions below:

4.2.9.1 *Generate an Authentication Code*

4.2.9.2 *Confirm a Uniqueness of Authentication Code*

4.2.9.3 *Register an Authentication Code*

4.2.9.4 *Issue an Authentication Code*

4.2.10 *User* — The user represents the followings:

4.2.10.1 *End User*

4.2.10.2 *Customer*

4.2.10.3 *Distributor*

4.2.10.4 *Brand Owner*

4.2.10.5 *Buyer*

5 Notation

5.1 *Unified Modeling Language (UML)*

5.1.1 These specifications apply the UML notation method to all class diagrams, the objects taken for examples, and the activity diagrams.

5.1.2 Class diagram: As the meaning of class diagram is definitely defined in the UML class diagram, these specifications are compliant with it. The details indicated by the diagram are not necessarily repeatedly described in this body text.

5.1.3 Class name: The initial letters of class name and service are capitalized. The class attribute is written in lower case letters.

5.1.4 Abstract and concrete classes: A class is either abstract or concrete. The abstract class is not directly implemented (that is, no instance). The class defined as concrete can be directly implemented. UML class diagram represents the abstract class name in italic letters. All classes used in these specifications are concrete classes.

5.1.5 Class attribute definition: The class attribute is defined in a table format, as shown in Table-1. UML class diagram represents the "public" attribute by attaching a plus (+) sign to the front of the attribute. All attributes defined in these specifications are public. Therefore, the plus (+) sign is omitted.

Table 1 Attribute Table Format

Attribute Name	*Definition*	*Access*	*Necessity*	*Type*
		RO or RW	Y or N	String or Integer

5.1.5.1 Access: The attribute becomes configurable (readable and writable: RW) or unconfigurable (read only: RO) through the interface to a service provider. Be aware that all attributes defined in these specifications are read only (RO).

5.1.5.2 Mandatory: Represents whether the attribute is mandatory or not. Y means mandatory and N does not mean mandatory.

5.1.6 Describe a number to express multiplicity by relations between Class in the place that is near to related Class. ex. Brand Owner has plural (multiplicity) Products, but Brand Owner of Products is one.

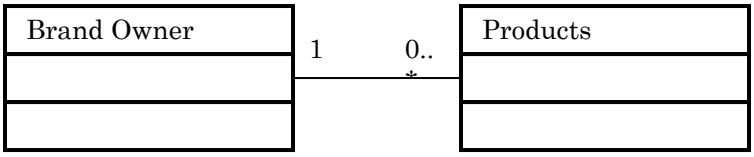

Table 2 Multiplicity List

multiplicity	*Description*
0..*	More than 0
0..1	0 or 1
1	Only as for 1
1..*	More than 1

5.2 Service notation: The service is a function or method offered by a service agency. The service either requires or does not require a response (R and N types).

5.2.1 Definition of Service

5.2.1.1 The service definition table defines the service corresponding to the supposed service resource, as shown in the table below:

Table 3 Service Definition Table Format

Service Name	*Description*	*Type*

5.2.1.2 The type is either R which requires a response or N which does not require a response.

5.2.2 Definition of Service Parameter

5.2.2.1 The definition table of service parameter defines the name, description, and type of parameters used in the service, as shown in the table below:

Table 4 Service Parameter Table Format

Parameter Name	*Description*	*Type*

5.2.2.2 A row is allotted to each parameter of service in the table.

5.2.3 Definition of Service Message

5.2.3.1 The definition table of service message defines the parameters of the service as shown in the table below:

Table 5 Service Message Table Format

Parameter Name	*Request/Indication* *(Req/Ind)*	*Response/Confirmation* *(Res/Cnf)*	*Comment*

5.2.3.2 The columns, Request/Indication and Response/Confirmation, correspond to the direction of message flow. A message issued by a sender is called a "Request". A recipient calls this message "Indication". The recipient can send a "Response", but this is a "Confirmation" from the point of view of the first sender.

5.2.3.3 The signs below are to be filled in both Request/Indication or Response/Confirmation column for defining the parameters.

Table 6 Service Message List

M	Mandatory parameter: Must be a valid value.
C	Conditional parameter: Existent under some circumstances, but otherwise, nonexistent. It is optional or dependent on other parameter whether the value can be present.
-	Any parameter is not used

6 Verification Requirements

6.1 *Verification Class Diagram* — The Figure3 shows the UML class diagrams of the requirements defined in this section.

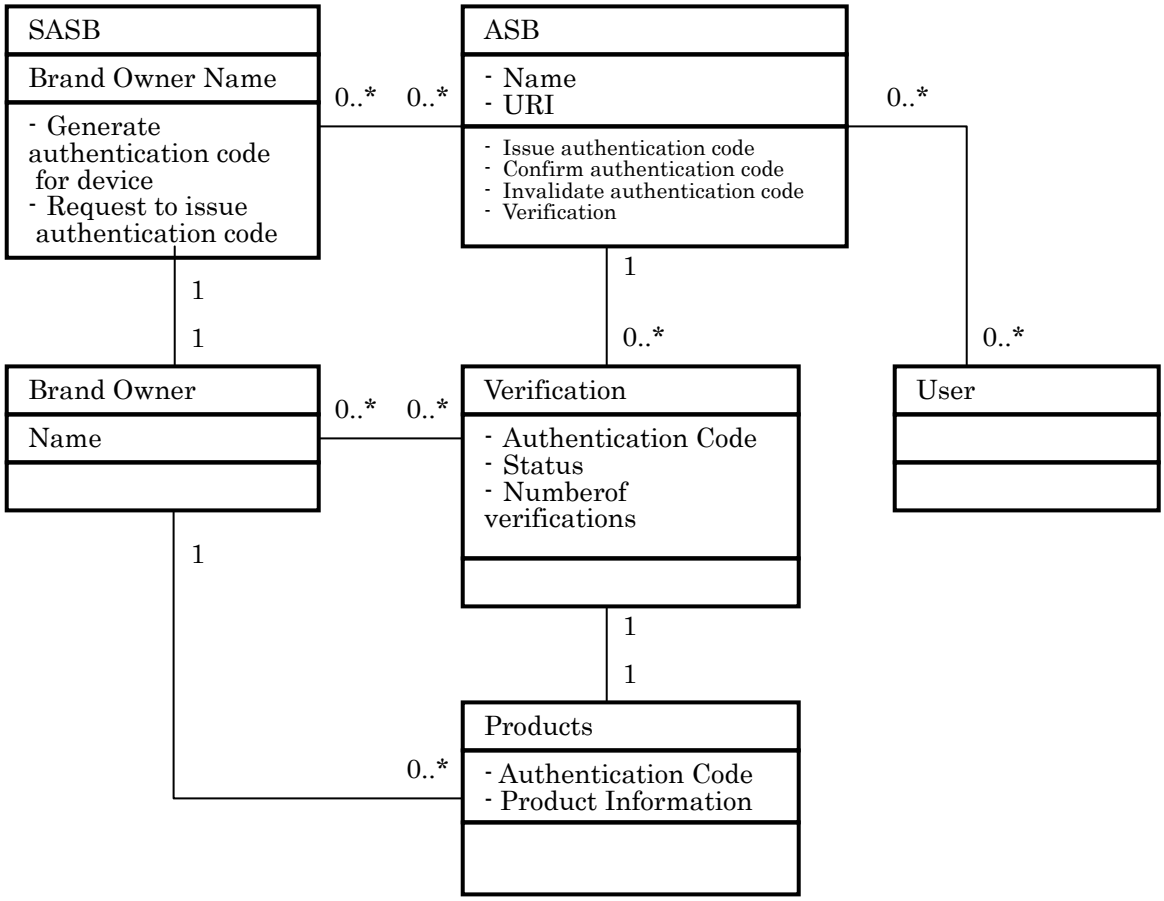

Figure 3 Verification Class Diagram

6.1.1 ASB (Authentication Service Body)

6.1.1.1 ASB issues the authentication code for the license plate.

6.1.1.2 ASB issues the authentication code for device generated by SASB.

6.1.1.3 ASB verifies the code.

NOTE 1: For information on the requirements for ASB, refer to "9. Requirements and Qualifications for ASB".

Table 7 ASB Attribute

Attribute Name	*Description*	*Access*	*Necessity*	*Type*
Name	ASB's identification name	RO	Y	String
URI	Uniquely represents the access destination of service offered by ASB	RO	Y	String

6.1.2 SASB (Self Authentication Service Body)

6.1.2.1 SASB generates the authentication code for device.

6.1.2.2 SASB requests ASB to issue the authentication code for device.

6.1.2.3 SASB requests ASB to issue the authentication code for license plate.

6.1.2.4 SASB offers the authentication code issued by ASB on the request of a brand owner.

6.1.2.5 SASB can request ASB to invalidate the authentication code issued.

NOTE 2: For information on the requirements for SASB, refer to "10. Requirements and Qualifications for SASB".

Table 8 SASB Attribute

Attribute Name	*Description*	*Access*	*Necessity*	*Type*
Brand owner name	Brand owner name offered by ASB	RO	Y	String

6.1.3 Brand Owner

6.1.3.1 The brand owner requests SASB to issue the authentication codes for device and license plate.

6.1.3.2 The brand owner attaches the authentication code to the device, outer case, intermediate box, or device tray.

6.1.3.3 The brand owner can request SASB to invalidate the authentication code issued.

Table 9 Brand Owner Attribute

Attribute Name	*Description*	*Access*	*Necessity*	*Type*
Name	Brand owner name offered by ASB	RO	Y	String

6.1.4 *Products* — The Products represent the devices to which the authentication codes for devices are allocated and the outer case, intermediate box, or device tray to which the authentication codes for license plates are allocated.

Table 10 Products Attribute

Attribute Name	*Description*	*Access*	*Necessity*	*Type*
Authentication code	Authentication code for device or license plate	RO	Y	String
Product Information	The brand owner determines the attribute's field and its content	RO	Y	String

6.1.5 *Verification* — The User requests ASB to verify the product's authentication code. The authentication process can be repeated as many times as you want until the authentication code is invalidated.

Table 11 Verification Attribute

Attribute Name	*Description*	*Access*	*Necessity*	*Type*
Code	Authentication code issued by ASB and attached to product	RO	Y	String
Verification count	Count verified after the code was issued	RO	Y	String
Status	Status is either valid or invalid.	RO	Y	String

6.2 *Service* — Service which ASB and SASB should offer to a brand owner or user.

6.2.1 *ASB Service* — Service which ASB should offer to SASB or user

Table 12 ASB Service

Service Name	*Description*	*Type*
(1) Authentication code issuance for device	Confirms the uniqueness of the generated authentication code for device on the request of SASB, and registers it and notifies SASB of it. When the service fails, returns an error.	R
(2) Authentication code issuance for license plate	On the request of SASB, issues the authentication code for license plate for particular product. When the service fails, returns an error.	R
(3) Code invalidation	Invalidates specific authentication code on the request of SASB and returns a notice. When the service fails, returns an error.	R
(4) Code confirmation	Extracts the information of the registered authentication code on the request of SASB and notifies SASB of it. When the service fails, returns an error.	R
(5) Verification	Verifies whether the specific authentication code is genuine on the request of the user and returns the result. When the service fails, returns an error.	R

6.2.1.1 *Authentication Code Issuance for Device* — Confirms the uniqueness of the generated authentication code for device on the request of SASB, and registers it and notifies SASB of it.

Table 13 Authentication Code Issuance for Device, Service Parameter

Parameter Name	*Description*	*Type*
Quantity	Number of authentication codes for device requested for issuance	String
Manufacturer name	Name of brand owner requesting the issuance of authentication code for device	String
Code	Code generated by SASB	String
Format	Format of data matrix code	Format List
Product Information	Product details	String
Issued code	Authentication code for device registered and formally issued by ASB	String
Error	Error returned when a service failed ・ "Service unavailable": Unavailable because the server is being down, the network is being down, etc. ・ "Failed to acquire information": The data is insufficient ・ "Quantity mismatch": The number requested for issuance and the number of actual generated authentication codes for device do not match	String

Table 14 Authentication Code Issuance for Device, Service Definition

Parameter Name	Request/ Indication	Response/ Confirmation	Comment
Quantity	M	-	
Manufacturer name	M	-	
Code	M	-	
Format	M	-	
Product Information	M	-	
Registered code	-	C	SASB is notified of those codes which can be registered

6.2.1.2 Authentication code issuance for license plate — Issues the authentication code requested by SASB.

Table 15 Authentication Code issuance for License Plate, Service Parameter

Parameter Name	*Description*	*Type*
Quantity	Number of codes requested for issuance	String
Manufacturer name	Name of brand owner requesting the issuance of code	String
Product Information	Product details	String
Issued code	Authentication code issued for license plate	String
Error	Error returned when a service failed · "Service unavailable": Unavailable because the server is being down, the network is being down, etc. · "Failed to acquire information": The data is insufficient · "Quantity mismatch": The number requested for issuance and the number of actual codes do not match (requested number cannot be issued)	String

Table 16 Authentication Code Issuance for License Plate, Service Definition

Parameter Name	*Request/ Indication*	*Response/ Confirmation*	*Comment*
Quantity	M	□	
Manufacturer name	M	□	
Product Information	M	□	
Code	□	M	

6.2.1.3 *Code Invalidation* — Invalidates the registered authentication code on the request of SASB.

Table 17 Code Invalidation, Service Parameter

Parameter Name	*Description*	*Type*
Code	Code to be invalidated	String
Manufacturer name	Name of brand owner requesting the invalidation of code	String
Notice	Returned when a service is finished · "Requested invalidation of code has finished"	String
Error	Error returned when a service failed · "Service unavailable": Unavailable because the server is being down, the network is being down, etc. · "Failed to acquire information": The data is insufficient · "Nonexistent code": The code is not registered · "This code is already invalidated": The code has already been invalidated · "No authority to request invalidation": The request is from other than SASB requested for issuance	String

Table 18 Code Invalidation, Service Definition

Parameter Name	*Request/ Indication*	*Response/ Confirmation*	*Comment*
Code	M	□	
Manufacturer name	M	□	
Notice	□	M	

6.2.1.4 *Code Confirmation* — Extracts the information of the registered authentication code on the request of SASB and notifies SASB of it.

Table 19 Code Confirmation, Service Parameter

Parameter Name	*Description*	*Type*
Code condition	Condition to extract and search the code to be confirmed	String
Manufacturer name	Name of brand owner requesting the confirmation of code	String
Code	Code to be confirmed	String
Code information	Code property and its incidental information	String
Error	Error returned when a service failed ・ "Service unavailable": Unavailable because the server is being down, the network is being down, etc. ・ "Failed to acquire information": The data is insufficient ・ "No authority": The request is from other than the manufacturer requested for issuance ・ "Code meeting the condition is not existent": The code is not registered or the code condition is not proper	String

Table 20 Code Confirmation, Service Definition

Parameter Name	*Request/ Indication*	*Response/ Confirmation*	*Comment*
Code condition	M		Specify the condition to extract and search the code
Manufacturer name	M	-	
Code	-	M	
Code information	-	M	

6.2.1.5 *Verification* — Verifies whether the specific authentication code is genuine on the request of the user and returns the result.

Table 21 Verification, Service Parameter

Parameter Name	*Description*	*Type*
User name	Name of the user requesting verification	String
Code	Authentication code whose verification is requested	String
Response	Returned when a service is finished ・ The code is registered (normal): "The code is formally registered valid code" ・ The code is not registered (illegal): "Nonexistent code"	String
Manufacturer name	Name of brand owner of the product	String
Product Information	Product details	String
Error	Error returned when a service failed ・ "Service unavailable": Unavailable because the server is being down, the network is being down, etc. ・ "Failed to acquire information": The data is insufficient ・ "No user authority": The user is not registered	String

Table 22 Verification, Service Definition

Parameter Name	*Request/ Indication*	*Response/ Confirmation*	*Comment*
User name	M	-	
Code	M	-	
Response	-	M	
Manufacturer name	-	C	Returned when the code is valid
Product Information	-	C	Returned when the code is valid

6.2.2 *SASB Service* — Service which SASB should offer to a brand owner and behavior of SASB

Table 23 SASB Service and Behavior

Service Name	*Description*	*Type*
(1) Authentication code issuance request for device	Requests ASB to issue the authentication code for device on the request of a brand owner. When the service fails, returns an error.	R
(2) Authentication code issuance request for license plate	Requests ASB to issue the authentication code for license plate on the request of a brand owner. When the service fails, returns an error.	R
(3) Authentication code generation for device	Generates the authentication code for device.	N

6.2.2.1 *Authentication Code Issuance Request for Device* — Requests to issue the authentication code for device on the request of a brand owner.

Table 24 Authentication Code Issuance Request for Device, Service Parameter

Parameter Name	*Description*	*Type*
Quantity	Number of codes requested for issuance	String
Format	Format of data matrix code	Format list
Product name_Assy Info	Product name and assembly information used in the non-secret area in the device authentication code	String
Secret information	Information filled in the secret area	String
Product Information	Product details	String
Code	Authentication code for device issued by ASB	String
Error	Error returned when a service failed ・ "Service unavailable": Unavailable because the server is being down, the network is being down, etc. ・ "Failed to acquire information": The data is insufficient	String

Table 25 Authentication Code Issuance Request for Device, Service Definition

Parameter Name	*Request/ Indication*	*Response/ Confirmation*	*Comment*
Quantity	M	□	
Format	M	□	
Product name_Assy Info	M	□	
Secret information	M	-	
Product Information	M	-	
Code	□	M	

6.2.2.2 Authentication code issuance request for license plate — Requests ASB to issue the authentication code for license plate on the request of a brand owner.

Table 26 Authentication Code Issuance Request for License Plate, Service Parameter

Parameter Name	*Description*	*Type*
Quantity	Number of codes requested for issuance	Number
Product Information	Product details	String
Authentication code for license plate	Authentication code for license plate issued by ASB	String
Error	Error returned when a service failed ・ "Service unavailable": Unavailable because the server is being down, the network is being down, etc. ・ "Failed to acquire information": The data is insufficient	String

Table 27 Authentication Code Issuance Request for License Plate, Service Definition

Parameter Name	*Request/ Indication*	*Response/ Confirmation*	*Comment*
Quantity	M	□	
Product Information	M	-	
Authentication code for license plate	□	M	

6.2.2.3 *Authentication Code Generation for Device* — Generates the authentication code for device.

Table 28 Authentication Code Generation for Device, Behavior Parameter

Parameter Name	*Description*	*Type*
Quantity	Number of codes requested for issuance	String
Format	Format of data matrix code	Format List
Product name_Assy Info	Product name and assembly information used in the non-secret area in the device authentication code	Product name_Assy Info
Secret information	Information filled in the secret area	String
Code	Code generated by SASB	String
Association information	Information associating the secret information with the code	String

Table 29 Authentication Code Generation for Device, Behavior Definition

Parameter Name	*Request/ Indication*	*Response/ Confirmation*	*Comment*
Quantity	M	□	
Format	M	□	
Product name_Assy Info	M	□	
Manufacturing Data	M	□	
Code	M	□	
Association information	M	□	

7 Access Traceability Requirements

7.1 *Access Traceability Class Diagram* — The Figure4 shows the UML class diagrams of the requirements defined in this section.

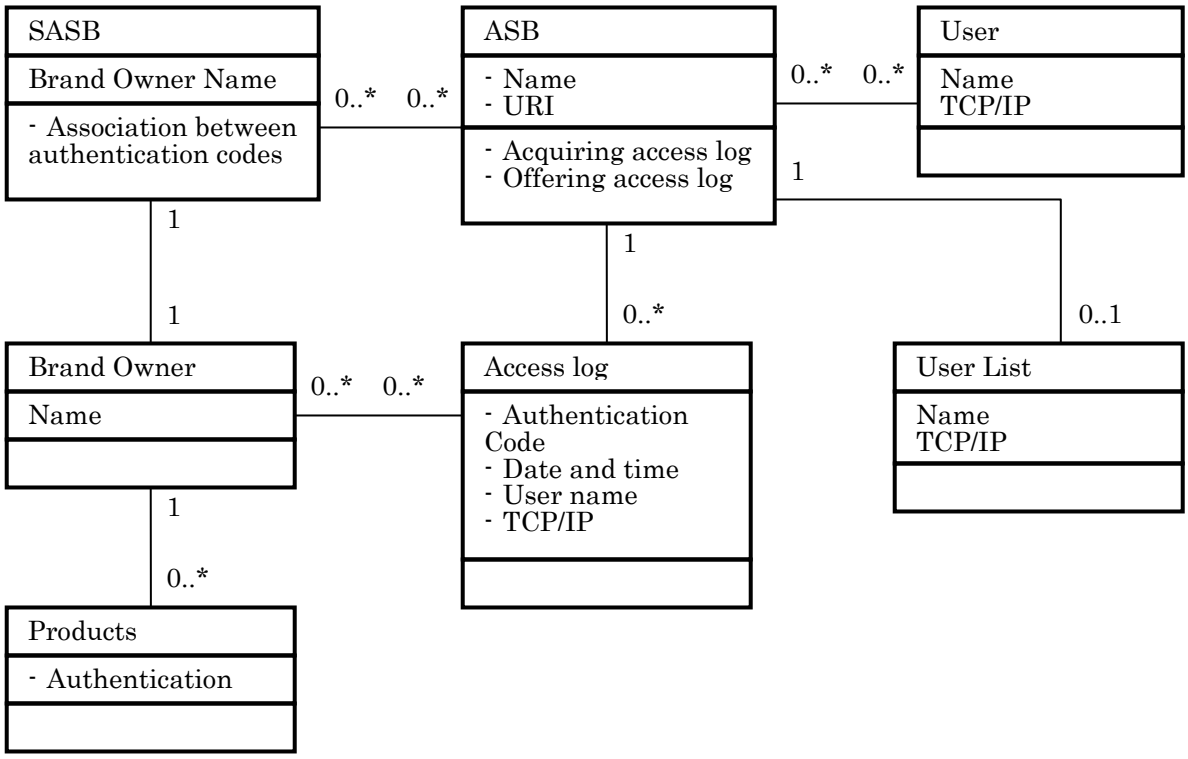

Figure 4 Access Traceability Class Diagram

7.1.1 ASB (Authentication Service Body)

7.1.1.1 ASB acquires and manages the access logs of the authentication codes for device and license plate.

7.1.1.2 ASB offers the access logs of the authentication codes for device and license plate to SASB.

NOTE 3: For information on the requirements for ASB, refer to "9. Requirements and Qualifications for ASB".

Table 30 ASB Attribute

Attribute Name	*Description*	*Access*	*Necessity*	*Type*
Name	ASB's identification name	RO	Y	String
URI	Uniquely represents the access destination of service offered by ASB	RO	Y	String

7.1.2 SASB (Self Authentication Service Body)

7.1.2.1 SASB manages the association information between the authentication codes for device and license plate.

7.1.2.2 SASB manages the association information between the authentication codes for license plate.

7.1.2.3 SASB requests ASB to offer the access logs.

NOTE 4: For information on the requirements for SASB, refer to "10. Requirements and Qualifications for SASB".

Table 31 SASB Attribute

Attribute Name	*Description*	*Access*	*Necessity*	*Type*
Brand owner name	Brand owner name offered by ASB	RO	Y	String

7.1.3 *Brand Owner* — The brand owner requests SASB to associate the authentication code for device with the authentication code for license plate.

Table 32 Brand Owner Attribute

Attribute Name	*Description*	*Access*	*Necessity*	*Type*
Name	Brand owner name offered by ASB	RO	Y	String

7.1.4 *Products* — The Products represent the device to which the authentication code for device is allocated and the outer case, intermediate box, or device tray to which the authentication code for license plate is allocated.

Table 33 Products Attribute

Attribute Name	*Description*	*Access*	*Necessity*	*Type*
Authentication code	Authentication code for device or license plate	RO	Y	String

7.1.5 *Access Log* — The access log is the pass log of the authentication code for device or license plate sent by the user.

Table 34 Access Log Attribute

Attribute Name	*Description*	*Access*	*Necessity*	*Type*
Code	Authentication code read by the user and sent to ASB	RO	Y	String
Date and time	Date and time when the log is acquired	RO	Y	Date
User name	Name of the user who sent the pass log	RO	Y	String
TCP/IP	User's TCP/IP	RO	Y	String

7.1.6 *User* — The user reads the authentication code for device or license plate.

The user notifies ASB of the read data.

Table 35 User Attribute

Attribute Name	*Description*	*Access*	*Necessity*	*Type*
Name	User name	RO	Y	String
TCP/IP	User's TCP/IP	RO	Y	String

7.1.7 User list — User List lists the user information.

Table 36 User List Attribute

Attribute Name	*Description*	*Access*	*Necessity*	*Type*
Name	User name	RO	Y	String
User information	User information such as the location	RO	Y	String

7.2 *Service* — Services which should be offered by ASB and SASB to the brand owner or user.

7.2.1 *ASB Service* — Services which should be offered by ASB to SASB or the user

Table 37 ASB Service

Service Name	*Description*	*Type*
(1) Access log record	Registers the concerned access log on the notification of pass by the user.	N
(2) Offering access log	Notifies of the access log of authentication code on the request of SASB. When the service fails, returns an error.	R

7.2.1.1 *Access Log Record* — Records the concerned access log on the notification of pass by the user.

Table 38 Access Log Record, Service Parameter

Parameter Name	*Description*	*Type*
User name	Name of the user accessed to ASB	String
User information	User's information	String
Date and time	Date and time accessed to ASB	Date
TCP-IP	Information of TCP-IP of accessed to ASB (IP address)	String
Authentication code for device	Authentication code read for device	String
Authentication code for license plate	Authentication code read for license plate	String

Table 39 Access Log Record, Service Definition

Parameter Name	Request/ Indication	Response/ Confirmation	Comment
User name	M	-	
User information	C	-	When the user is registered in User List
Date and time	M	-	
TCP-IP	M	-	
Authentication code for device	C	-	Authentication code for device
Authentication code for license plate	C	-	Authentication code for license plate

7.2.1.2 *Offering Access Log* — Notifies SASB of the access log of authentication code on the request of SASB

Table 40 Offering Access Log, Service Parameter

Parameter Name	*Description*	*Type*
Manufacturer name	Name of brand owner requesting to offer the access log	String
Log requirements	Authentication code, period, log types (temporary or archived log), etc.	String
Access log information	Information of company accessed to ASB, date and time, TCP-IP information (IP address), etc.	String
Error	Error returned when a service failed ・ "Service unavailable": Unavailable because the server is being down, the network is being down, etc. ・ "Failed to acquire information": The data is insufficient ・ "No authority": The request is from other than the SASB requested for registration ・ "Access log meeting the condition is not existent": The condition is not proper The authentication code inquired is not existent. The target company is not existent.	String

Table 41 Offering Access Log, Service Definition

Parameter Name	*Request/ Indication*	*Response/ Confirmation*	*Comment*
Manufacturer name	M	-	
Log requirements	M	-	
Access log information	-	M	

7.2.2 *SASB Service* — Services which SASB should offer to a brand owner

Table 42 SASB Service

Service Name	*Description*	*Type*
(1) Association between device and license plate	Associates the authentication codes between license plate and device according to the storage patterns.	R
(2) Association between license plates	Associates the authentication codes between license plates.	R
(3) Association information confirmation	Confirms and notifies of the trace information of authentication code. When the service fails, returns an error.	R

7.2.2.1 *Association between Device and License Plate* — Associates the authentication codes between license plate and device according to the storage patterns.

Table 43 Association between Device and License Plate, Service Parameter

Parameter Name	*Description*	*Type*
Authentication code for device	Authentication code for device	String
Authentication code for license plate	Authentication code for license plate allocated to the device tray	String
Notice	Notifies that the recording is finished	String
Error	Returns an error	String

Table 44 Association between Device and License Plate, Service Definition

Parameter Name	*Request/ Indication*	*Response/ Confirmation*	*Comment*
Authentication code for device	M	□	
Authentication code for license plate	M	□	
Notice	□	M	

7.2.2.2 *Association between License Plates* — Associates the authentication codes between license plates.

Table 45 Association between License Plates, Service Parameter

Parameter Name	*Description*	*Type*
Authentication code for license plate	Authentication code for license plate	String
Notice	Notifies that the recording is finished	String
Error	Returns an error	String

Table 46 Association between License Plates, Service Definition

Parameter Name	*Request/ Indication*	*Response/ Confirmation*	*Comment*
Authentication code for license plate	M	□	
Notice	□	M	

7.2.2.3 *Association Information Confirmation* — Confirms and notifies of the trace information of authentication code.

Table 47 Association Information Confirmation, Service Parameter

Parameter Name	*Description*	*Type*
Authentication code for device	Authentication code for device	String
Authentication code for license plate	Authentication code for license plate allocated to the device tray	String
Code linkage information *(association information)*	Information which associates the authentication codes between license plate and device	String
Error	The authentication code is not existent. The association is incomplete.	String

Table 48 Association Information Confirmation, Service Definition

Parameter Name	*Request/ Indication*	*Response/ Confirmation*	*Comment*
Authentication code for device	C	□	
Authentication code for license plate	C	□	
Code linkage information (association information)	□	M	

8 Quality Traceability Requirements

8.1 Quality traceability class diagram — The Figure5 shows the UML class diagrams of the requirements defined in this section.

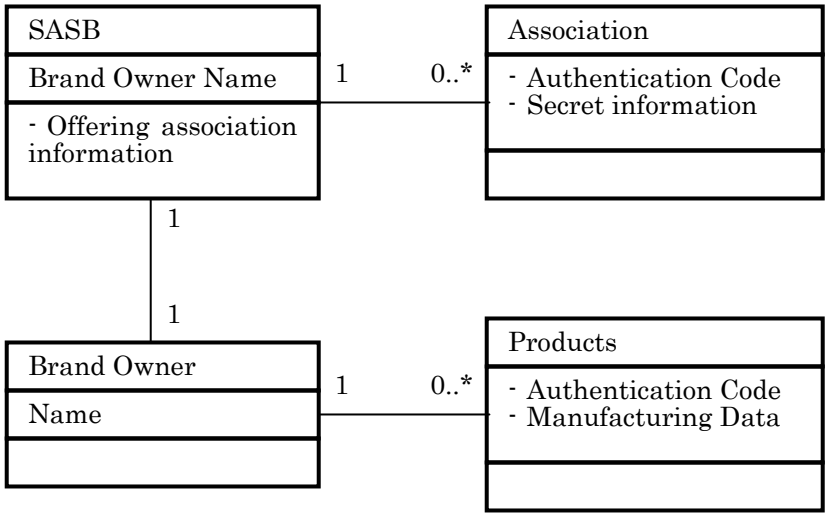

Figure 5 Quality traceability class diagram

8.1.1 *SASB (Self Authentication Service Body)* — SASB manages the association between the authentication code for device and preprocess production information.

NOTE 5: For information on the requirements for SASB, refer to "10. Requirements and Qualifications for SASB".

Table 49 SASB Attribute

Attribute Name	*Description*	*Access*	*Necessity*	*Type*
Brand owner name	Brand owner name offered by ASB	RO	Y	String

8.1.2 *Brand Owner* — The brand owner requests SASB to associate the authentication code for device with the preprocess production information.

Table 50 Brand Owner Attribute

Attribute Name	*Description*	*Access*	*Necessity*	*Type*
Name	Brand owner name offered by ASB	RO	Y	String

8.1.3 *Products* — The Products represent the devices to which the authentication codes for devices are allocated.

Table 51 Products Attribute

Attribute Name	*Description*	*Access*	*Necessity*	*Type*
Authentication code	Authentication code for device	RO	Y	String
Manufacturing Data	Production information of preprocess and post-process. The brand owner determines the attribute's field and its content.	RO	Y	String

8.1.4 Association information — The Association means to make it possible to derive the preprocess production information from the authentication code for device.

Table 52 Association Information, Attribute

Attribute Name	*Description*	*Access*	*Necessity*	*Type*
Authentication code	Authentication code for device	RO	Y	String
Secret information	Of all authentication codes for device, the information to be filled in the secret area	RO	Y	String

8.2 Service

8.2.1 SASB Service — Services which SASB should offer to a brand owner

Table 53 SASB Service

Service Name	*Description*	*Type*
(1) Offering association information	Notifies the brand owner of the secret information of the product to which the authentication code for device is allocated on the request of the brand owner.	R

8.2.1.1 Offering association information — Notifies the brand owner of the secret area information corresponding to the authentication code for device on the request of the brand owner.

Table 54 Offering Association Information, Service Parameter

Parameter Name	*Description*	*Type*
Authentication code for device	Authentication code for device	String
Secret information	Of all authentication codes for device, the information to be filled in the secret area	String
Error	Returns an error	String

Table 55 Offering Association Information, Service Definition

Parameter Name	*Request/ Indication*	*Response/ Confirmation*	*Comment*
Authentication code for device	M	-	
Secret information	-	M	

9 Requirements and Qualifications for ASB

9.1 ASB shall meet the requirements defined in the Verification.

9.2 ASB shall meet the requirements defined in the access traceability.

9.3 ASB shall be validated that ASB meets the requirements above and is operating properly.

9.4 Each country determines the agency validating ASBs. In Japan, JIPDEC validates ASB in the semiconductor industry.

9.5 ASB shall take measures against the problems below in order to keep the reliability of codes.

9.5.1 Data tampering

9.5.2 Data leakage

9.5.3 Data loss

9.5.4 Abnormal stop of service

9.5.5 Function trouble

9.5.6 Illegal access

9.6 SAB shall rate the users and control their accesses based on the qualifications shown in the table below in order to prevent the illegal access.

9.7 ASB shall validate the usage of the users of levels 1 to 3. Each ASB shall determine the validation conditions.

Table 56 Authority to Use Information

Authority	*Level 1*	*Level 2*	*Level 3*	*Level 4*
Request to issue	○	○		
Browse access log information	○	○		
Browse optional product information	○		○	
Request to verify code	○	○	○	○

10 Requirements and Qualifications for SASB

10.1 SASB shall meet the requirements defined in the Verification.

10.2 SASB shall meet the requirements defined in the access traceability.

10.3 SASB shall meet the requirements defined in the quality traceability.

10.4 SASB shall be validated by ASB that SASB meets the requirements above and is operating properly.

10.5 SASB shall take measures against the problems below in order to keep the reliability of codes.

10.5.1 Data tampering

10.5.2 Data leakage

10.5.3 Data loss

10.5.4 Abnormal stop of service

10.5.5 Function trouble

10.5.6 Illegal access

10.6 SASB shall register the users for usage in order to prevent the illegal access. Each SASB shall determine the registration conditions.

11 Authentication Code Level

11.1 Codes are not applicable to all products. A Brand Owner judges the application for each business model and applies the codes to the products that need such codes.

11.2 The Brand Owner judges the application by using the levels in the following table for the application and operation of authentication codes.

Table 57 Authentication Code Level

Level	*Application*
Level 4	Cyber Security, Social Impact, Critical Infrastructure
Level 3	Safety, High Damage, Health Safety
Level 2	High Quality, High Cost/Value, Security
Level 1	Future Business Model / Risk, Traceability Effect

12 Authentication Code for Device

12.1 Data format

12.1.1 The code data area is composed of the non-secret and secret areas below. The non-secret area is mandatory and the secret area is optional. The Figure-6 shows the configuration of the authentication code for device.

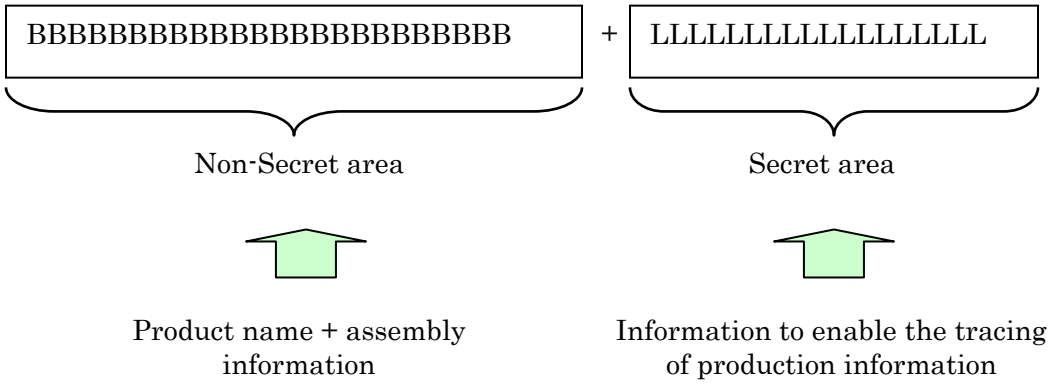

Figure 6 Configuration Example of Authentication Code for Device

12.1.1.1 Non-Secret area - The non-secret information shall be able to identify the product.

12.1.1.1.1 Number of letters: Not defined. However, total number of letters of non-secret and secret areas shall be defined in section 11.2.1.2.

12.1.1.1.2 Attribute: Alphanumeric

12.1.1.2 Secret area - The secret area contains the index data which enables to trace the preprocess production information in the semiconductor wafer processing. The data should be encrypted.

12.1.1.2.1 Number of letters: Not defined. However, total number of letters of non-secret and secret areas shall be defined in section 11.2.1.2.

12.1.1.2.2 Attribute: Alphanumeric

12.1.1.2.3 How to encrypt data: Not defined

12.2 Display — The authentication code for device should display both 2D code and HRI (Human Readable Identification).

12.2.1 2D code

12.2.1.1 Type - Display the authentication code for device in the data matrix ECC200.

12.2.1.2 Shape and maximum numbers of characters of the 2D code symbol — Table-58 lists the shapes and maximum numbers of characters of the 2D code symbols.

Table 58 Data Matrix ECC200 Code Table

Format	*No. of cells*	*Data cell*		*Information volume*		
		No. of cells	*No. of blocks*	*Numerals*	*Alphanumeric*	*Binary*
5	20x20	18x18	1	44	31	20
6	22x22	20x20	1	60	43	28
7	24x24	22x22	1	72	52	34
8	26x26	24x24	1	88	64	42

12.2.1.3 How to print: Not defined

12.2.1.4 Display location: Not defined

12.2.1.5 Dimension: Not defined

12.2.2 HRI: HRI shall display all or a part of non-secret area.

12.2.2.1 How to print: Not defined

12.2.2.2 Display location: Not defined

12.2.2.3 Dimension: Not defined

13 Authentication Code for License Plate

13.1 Data format

13.1.1 The code data is composed of country code, industrial ASB No., and individual authentication code.

13.1.1.1 Country code - Each semiconductor industry can arbitrarily determine the country code.

13.1.1.1.1 Number of letters: Two letters of alphabetic characters. A country code consists of two alphabetical characters

13.1.1.1.2 Content of code: Be compliant with the country code defined in ISO3166-2. It conforms to the country number in ISO 3166-2.

13.1.1.2 Industrial association ASB No. - The ASB number can be used after checking that the industry associations do not overlap with each other in the same country code.

13.1.1.2.1 Number of letters: Three letters of alphabetic characters.

13.1.1.2.2 Attribute: Alphanumeric

13.1.1.3 Individual authentication code — Unique code to be allocated on a per license plate basis.

13.1.1.3.1 Number of letters: 20 letters of alphabetic characters.

13.1.1.3.2 Attribute: Alphanumeric — The Figure7 shows the configuration of the authentication code for license plate.

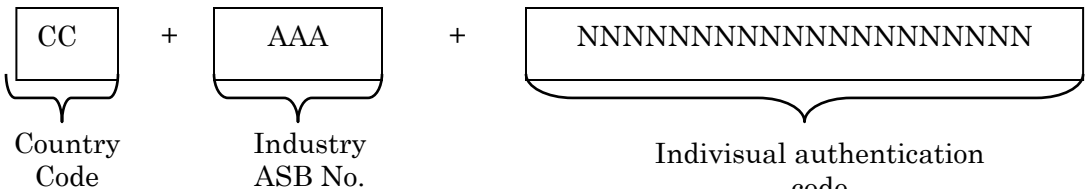

Figure 7 Configuration of The Authentication Code for License Plate

13.2 Display — The authentication code for license plate should display both 2D code and HRI (Human Readable Identification).

13.2.1 2D code

13.2.1.1 Type — Display the authentication code for license plate in the data matrix ECC200.

13.2.1.2 Shape and maximum numbers of characters of the 2D code symbol — Table59 lists the shapes and maximum numbers of characters of the 2D code symbols.

Table 59 Data Matrix ECC200 Code Table

Format	*No. of cells*	*Data cell*		*Information volume*		
		No. of cells	*No. of blocks*	*Numerals*	*Alphanumeric*	*Binary*
4	18x18	16x16	1	36	25	16

13.2.1.3 How to print: Not defined

13.2.1.4 Display location: Not defined

13.2.1.5 Dimension: Not defined

13.2.2 HRI: HRI shall display all data.

13.2.2.1 How to print: Not defined

13.2.2.2 Display location: Not defined

13.2.2.3 Dimension: Not defined

RELATED INFORMATION 1
Authentication Code & Service Flow

R1-1 The Figure R1-1 shows an image for marking the authentication code for device.

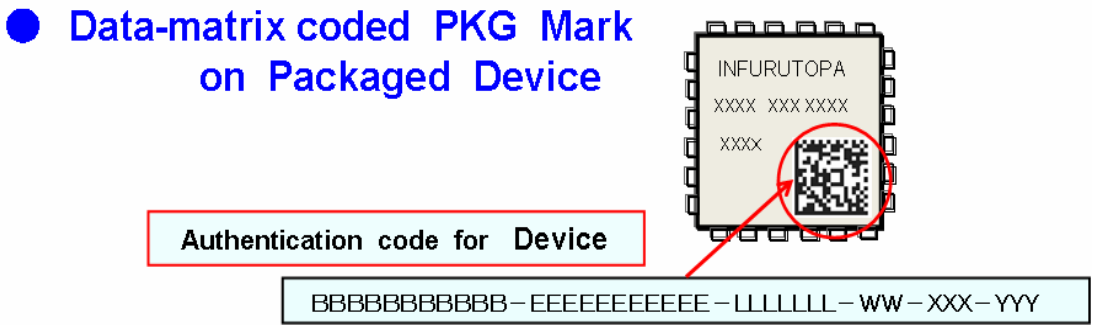

Figure R1-1 Image for Marking The Authentication Code for Device

R1-2 The FigureR1-2 shows an image when displaying the authentication code for license plate on the license plate.

Figure-2 Image when displaying the authentication code for license plate

Figure R1-2 Image When Displaying The Authentication Code for License Plate

R1-3 The FigureR1-3 shows the sequence diagram when issuing the authentication code for device.

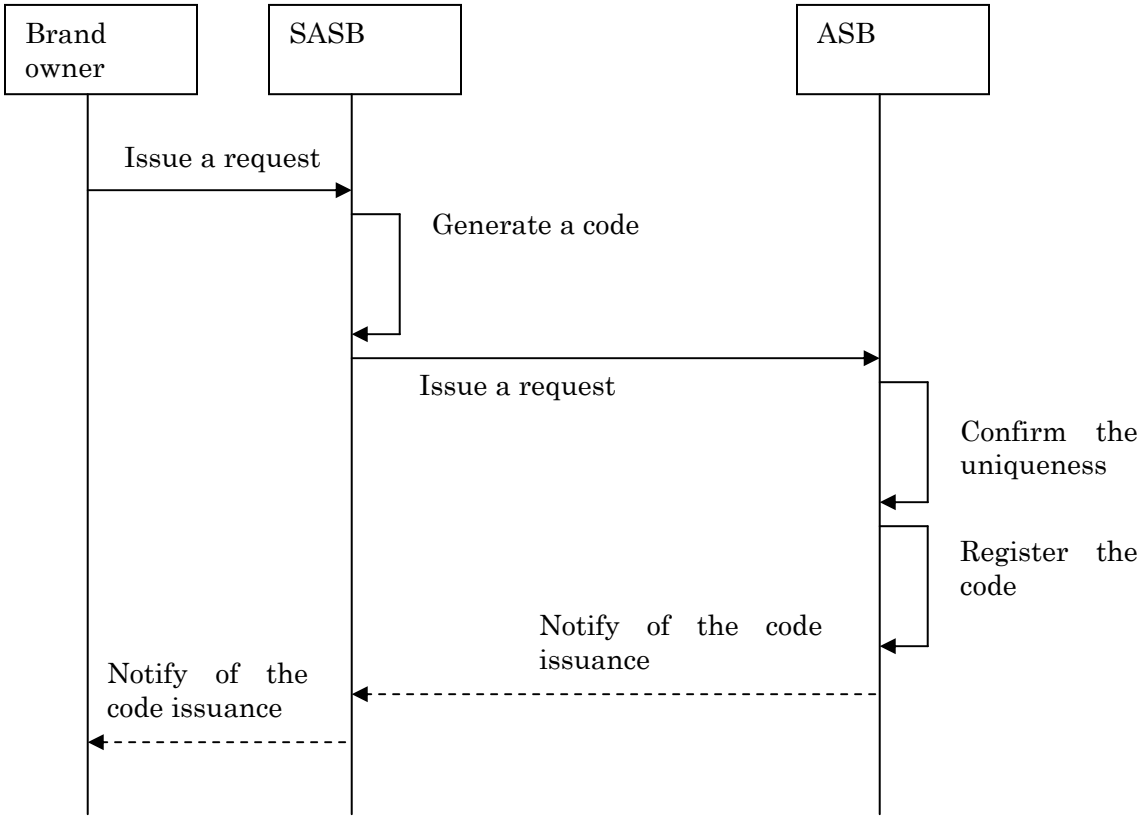

Figure R1-3 Sequence diagram when issuing authentication code for device

R1-4 The Figure R1-4 shows the sequence diagram when issuing the authentication code for license plate.

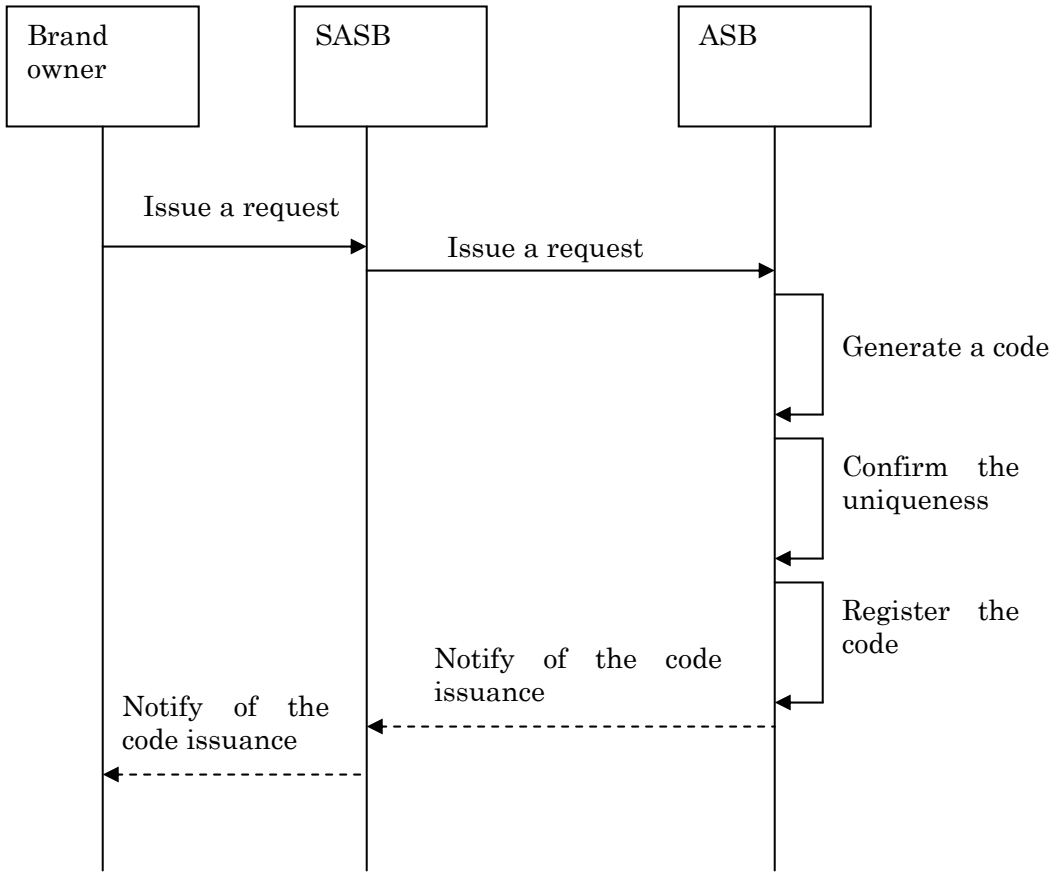

Figure R1-4 Sequence diagram when issuing authentication code for license plate

R1-5 The Figure R5-1 shows the sequence diagram for verification.

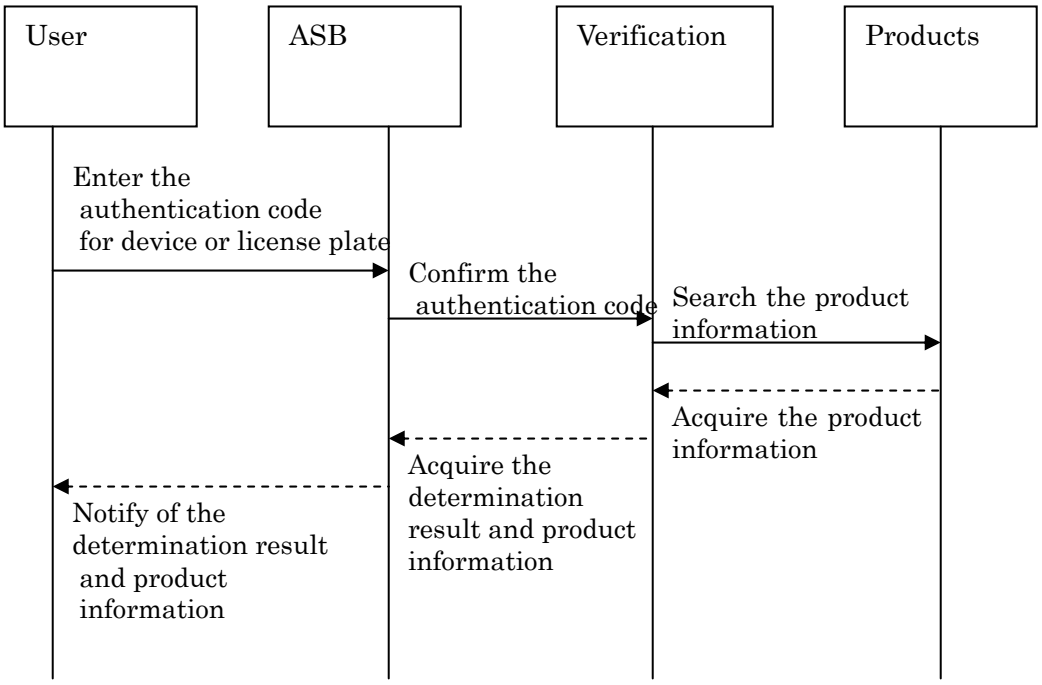

Figure R1-5 Sequence diagram for verification

R1-6 The Figure-R1-6 shows the sequence diagram for registering access log

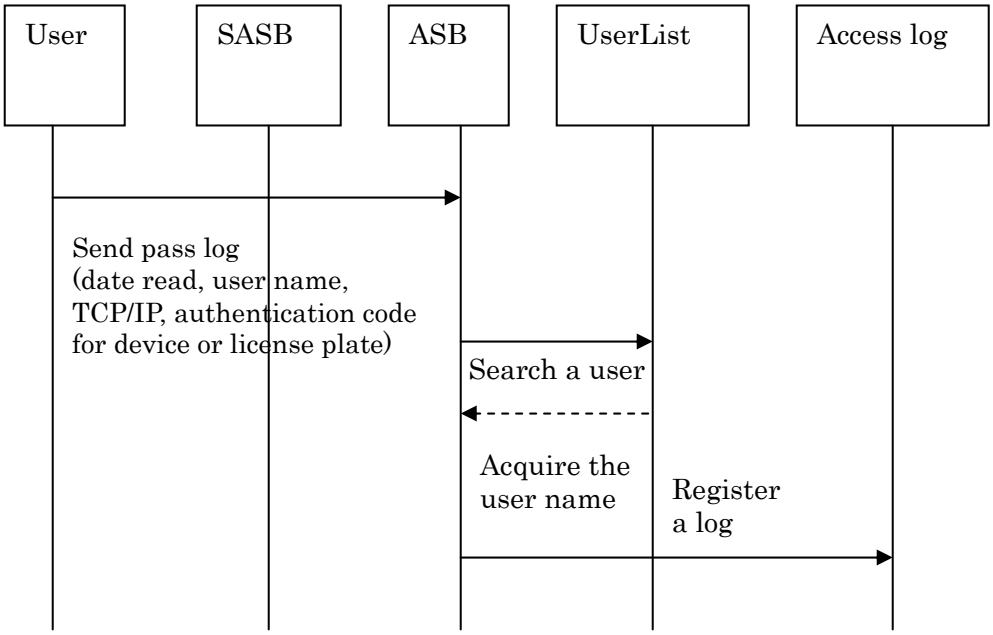

Figure R1-6 Sequence diagram for registering access log

R1-7 The Figure R1-7 shows the sequence diagram for confirming access log

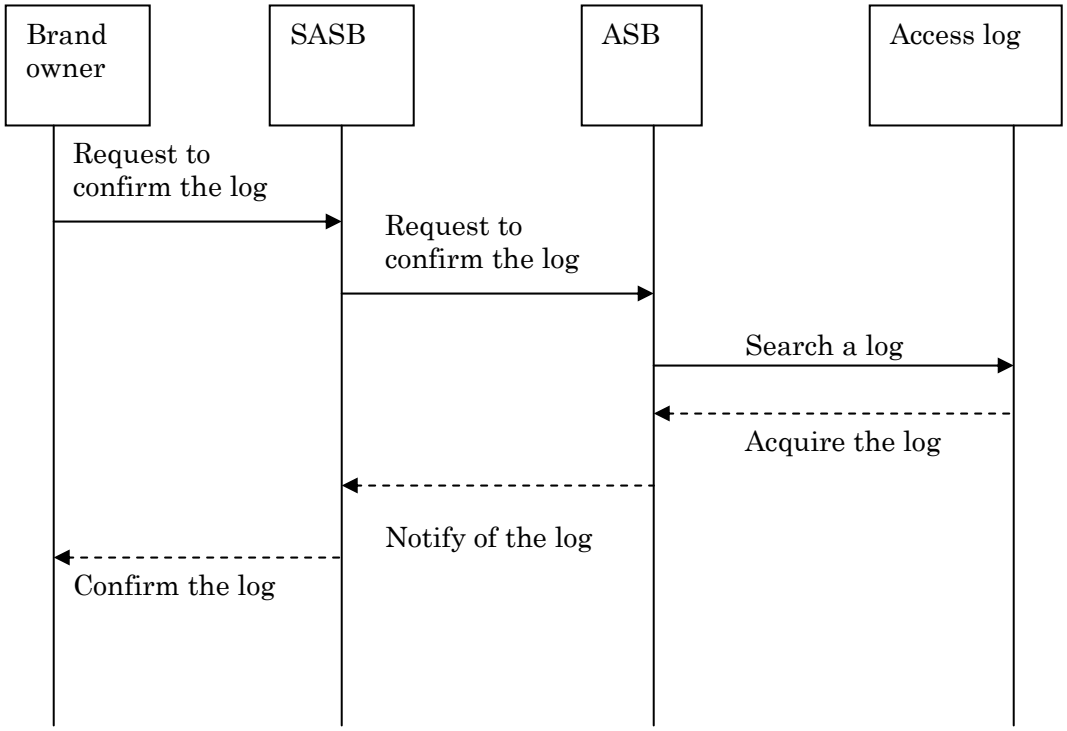

Figure R1-7 Sequence diagram for confirming access log

R1-8 The Figure R1-8 shows the sequence diagram when acquiring the manufacturing data from the device authentication code

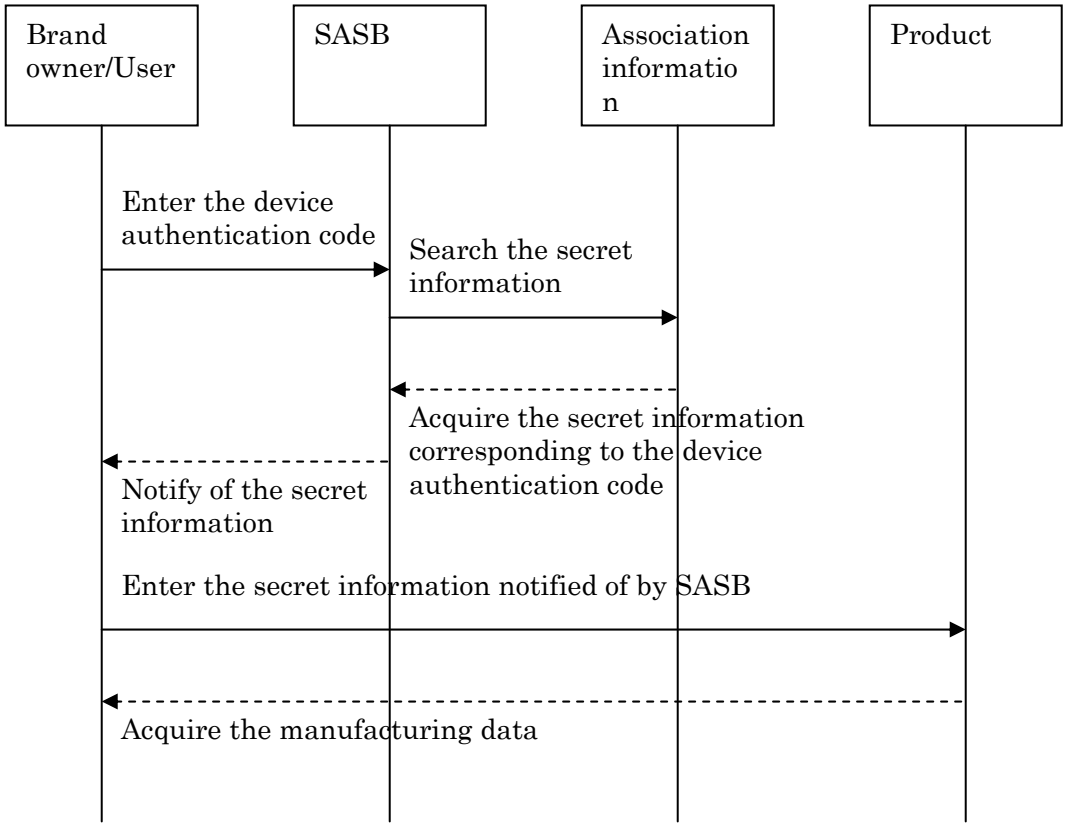

Figure R1-8 Quality traceability sequence diagram