# RightPlug Product Authentication Strategy

## Introduction

The RightPlug Standard defines requirements for electronic encoding of electrical plugs. The types of information stored in encoded plugs and applications that make use of encoded information are virtually unlimited.

This document describes a system and method to verify authenticity of an electrical product in the field, and receive additional information about the product such as product recalls, supplementary instructions etc.

## Product Authentication

Product authentication has begun to receive increasing attention with the rise of counterfeit and adulterated products entering the market. Counterfeit products have been in the market for a period of time however, the complexity of items counterfeited has increased to the point where large electrical products are brought to market without the control or oversight of the apparent manufacturer.

Manufacturers suffer from erosion of brand reputation and profitability though brand and trademark theft.

Common authentication technologies employ many of the same technologies used to protect currency from counterfeiting: color changing inks, holograms, nanotechnology, and product serialization to name a few. These technologies provide a means to confirm a suspected counterfeit, but do little to simplify the task of authentication for consumers since they require skill and knowledge to inspect and detect the specific features of a particular product.

### Regulatory Certification – A Special Case

Consumers are well aware of the various certification marks applied to product that meet applicable safety standards; CSA, UL. ETL, TUV to name a few. There have always been cases of products bearing a certification mark without testing, however, the occurrence of such violations has increased drastically in recent years.

The legal protection of registered trade marks, service marks and certification marks is apparently insufficient to deter the marketing of products with bogus claims of regulatory compliance. Consumers can no longer rely on the simple presence of a recognized mark to ensure a product meets applicable safety requirements.

## Product recalls

Responsible manufacturers issue voluntary product recall notices if they detect a manufacturing or design defect that results in a safety risk. In the United States, the Consumer Product Safety Commission (CPSC) has the power to issue product recalls. Canada is in the process of developing regulations with similar objectives.

Although manufacturers make best efforts to notify consumers of recalls, the primary responsibility lies with consumers to check for recalls of products they own. The difficulty associated with this task is daunting and results in most consumers simply not checking and remaining unaware of potential hazards.

## Supplementary Information

All products from responsible manufacturers are shipped with sufficient documentation to allow a consumer to use the product safely. In many, if not most cases, the documentation is quickly lost or discarded. Products that are re-sold as "used" rarely include documentation, significantly increasing the risk to the second owner.

## Product Authentication Use Cases

### Authentication by Electrical Receptacles

The most effective application for authentication is an electrical receptacle that only delivers electricity to verified products. Denying power to products that cannot be authenticated greatly enhances safety, and makes it extremely difficult for counterfeit product to remain undetected and be successful in the market.

### Authentication by Consumer

Product authentication by consumers is not considered to be a primary deterrent, however it does have its place. The key to effective consumer authentication is automation and elimination of any skill or knowledge requirement. Both authentication kiosks and home authentication kits are possible implementations.

### Authentication by Enforcement Personnel

Product authentication at port of entry is a primary means to exclude counterfeit product from the marketplace. However, effort and product knowledge required to perform authentication make it difficult to routinely inspect even a small portion of imports.

An ideal solution is to minimize the effort, and to eliminate the need for special knowledge and skill situation, to perform a product authentication

### Authentication of Regulatory Certification

Aside from basic product authentication, confirmation of regulatory certification is key to increasing public safety. There are numerous products manufactured by reputable companies that are safety certified for specific markets, yet are available for sale in other markets. In other cases, certain products are marked with the logo of a safety certification organization but have not been tested.

A complete product authentication must include secure verification of safety certification, and provide alerts when a product does not bear a relevant certification for a particular jurisdiction.

## Product Recall Use Cases

Product recalls can be issued from a number of sources, in all cases it is desirable to convey specific information to the consumer:

- Whether any active recall notices apply to a particular unit.
- Whether it is safe to continue using a recalled product.
- Remedial action to be taken.

### Recall Issued by Manufacturer

Manufacturers typically issue recalls when a design or manufacturing defect that affects consumer safety is identified. Communication of recall notices is problematic since despite best efforts, manufacturers rarely have records related to the current owners of products.

### Recall Issued by Other Organization

In several jurisdictions, there are (typically governmental) organizations that have the power to compel manufacturers to issue recalls, or issue recalls directly.

Standards compliance organizations are authorized to test products against safety standards. In some cases products have their certification rescinded, but there is no practical way for consumers to learn if products in their possession are affected, unless a recall is subsequently issued.

### Recall Lookup by Retail Vendor

In some cases a product recall occurs soon enough for a retailer to pull product from the shelf. In these cases, an automated means to rapidly identify recalled product while still on the shelves is advantageous.

### Recall Lookup by Enforcement Personnel

Identification of products with suspended regulatory certifications, recall notices or import restrictions is another objective of import examinations and is easily combined with a product authentication check.

### Recall Lookup by Consumer

Product recall notices can be difficult to interpret. Consumers often are either not aware of recalls or have difficulty determining if a recall applies to a product they own. Ideally, the same methods used for product authentication should also check for product recalls.

### Recall Scope Resolution

Recall notices frequently refer to a specific subset of product manufactured at a particular facility during a particular time period. In addition to general product identification information, a product must be further identified by information that includes date/facility and/or production batch.

### Automated Recall Notifications

Home Automation Recalls

Home automation systems with outlet devices linked to central computers provide an excellent opportunity for automated recall identification and notification. Outlets that are capable of reading encoded plugs and conveying that information to a home controller enable automated product validation and recall checks.

Consumer Recall Software

A low cost home electrical safety kit, including a USB plug reader and software, allows a consumer to scan their electrical plugs once, and have an automated software application or web-based service monitor for recalls and issue notifications as required.

## Product Supplementary Information Use Cases

Supplementary product information covers any information provided by a manufacturer related to a product including:

- User guide and other documentation shipped with the product
- Service manuals
- Drawings
- Parts lists

### Information Lookup by Consumer

Consumers frequently discard or misplace documentation shipped with a product. Re-sold products rarely include documentation, depriving a purchaser of the opportunity to review critical safety information.

Access to product documentation is not universal, and frequently difficult. The same procedure used to authenticate a product and check for recall or other safety notices can also identify any product documentation that may be available.
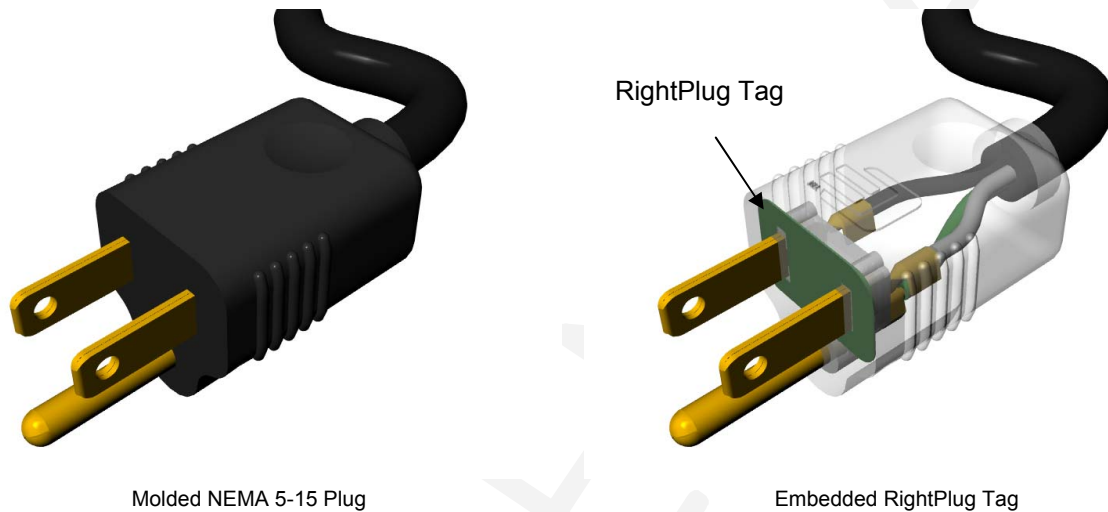
### Information Lookup by Service Personnel

Outside of the information provided to consumers, there is extensive manufacturer documentation intended for service personnel. Rapid access to such documentation is easily enabled by the identification information encoded in an electrical plug.

## RightPlug for Product Authentication

### About RightPlug

RightPlug is a specification for electronic encoding of electrical plugs. Other than the embedded RightPlug Tag, encoded plugs are essentially the same as any other electrical plug, including regulatory approvals.

The RightPlug Standard is managed by the RightPlug Alliance, a not-for-profit organization consisting of member organizations that either manufacture electrical products, or are involved in safety of electrical products.

RightPlug Tag

Molded NEMA 5-15 Plug                                    Embedded RightPlug Tag

The RightPlug standard defines the mechanical, electrical and data organization requirements for encoded plugs as an extension to and in accordance with existing plug standards. The standard has been defined with extensibility and backward compatibility as a core requirement.

### RightPlug Capabilities & Limitations

RightPlug encoding tags are passive RF memory devices with an extremely limited range. They are designed to be readable when the blades are partially inserted into a receptacle, and have a theoretical maximum read range of 10 centimeters but a somewhat shorter practical read range. Limited read range is a tradeoff between the benefits of long read range for authentication applications and short read range for consumer privacy.

Encoding tags are based on ISO 14443, selected for low cost both for the encoding tags and readers.

Data contained within tags is organized as a series of 32-bit data words. Currently available tag silicon supports 14 X 32 bit write-protectable data words and from 0 to 112 read/write data words.

**Encoded Identification Information**

24-bit Manufacturer ID (MID)

- Assigned by RightPlug Alliance
- Allows for over 16 million MID codes

16-bit Product ID (PID)

- Assigned by RightPlug Alliance
- Globally unique product ID includes MID:PID
- Allows for over 65 thousand PID codes *per MID code*
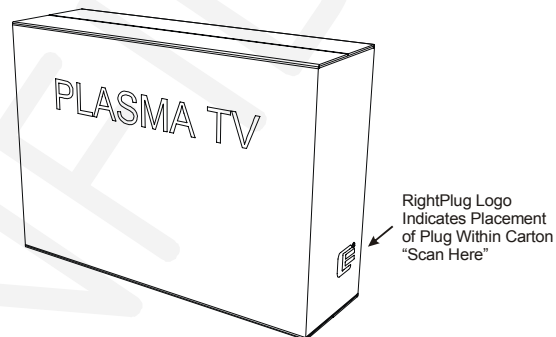
24-bit Production Lot ID (LID)

- Optionally assigned and programmed by manufacturer
- Encodes date/facility of manufacture, batch code or other manufacturer-specific information
- Helps isolate scope of product recalls

16-bit Product Variant/Version ID (VID)

- Optionally assigned and programmed by manufacturer
- Encodes additional information about a particular product variant
  - Product versions
  - Product variant (i.e. configuration options)
- Helps isolate scope of product recalls
- Supports manufacturer version changes and multiple product variants with a single Product ID

In-Carton Authentication

Since RightPlug tags have a limited read range, product packaging requirements are necessary to ensure the encoded plug is readable through the product carton, and that the location of the plug is easily identified. In the following example, the RightPlug logo indicates the placement of the plug, and makes it easy to scan the plug for authentication purposes without opening the carton.



RightPlug Logo
Indicates Placement
of Plug Within Carton
"Scan Here"

### Authentication Methods

Stand-alone Authentication

Certain types of devices are unlikely to have external communication capabilities. Authentication must be possible using just the information present in the encoded plug, although without an external authentication authority the reliability of the authentication will be reduced.

*Example: An electrical outlet is designed to operate safely with authentic RightPlug encoded plugs, but may not provide the level of safety expected by the user if a counterfeit (possibly improperly encoded) plug is used. It is desirable for the receptacle to have a high level of confidence that an encoded plug is authentic before delivering power.*
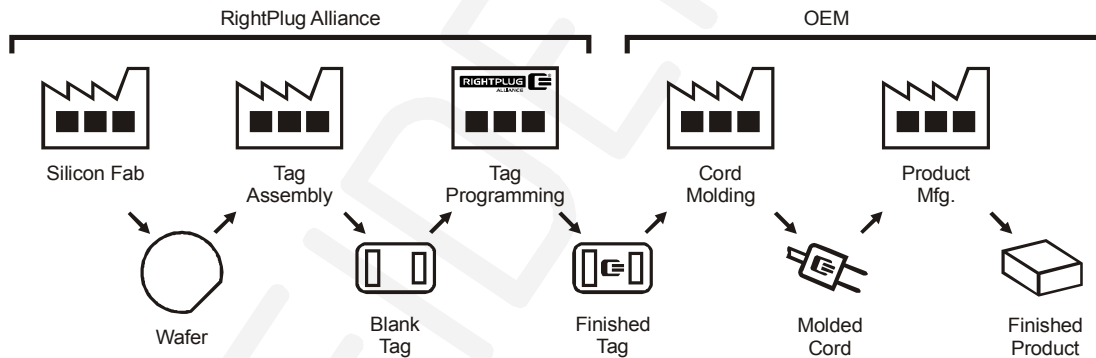
On-line Authentication

Some devices are likely to have external communication capabilities either though a direct internet connection or though indirect means via other equipment. Authentication may include basic verification using only information contained within an encoded plug, and may also use an external server that makes use of a database to perform a much more reliable authentication.

*Example: A hand-held authentication device is used by customs inspection personnel to rapidly validate incoming merchandise while still in it's packaging. It is desirable for the external authentication server to perform a much more thorough validation of the encoded information, including providing detailed product identity information for subsequent in-person verification.*

## Authentication Security

### RightPlug Encoding Transponder Process



| Facility | Description |
|---|---|
| Qualified silicon manufacturer | Silicon manufacturer makes qualified components customized with unique serial numbers incorporating the RightPlug Alliance Silicon Vendor ID and supplies transponders in wafer form. |
| Authorized Tag Assembly Subcontractor(s) | One or more authorized subcontractors assemble transponder ICs from wafer into un-programmed tag assemblies. |
| RightPlug Alliance Facility or Authorized Subcontractor(s) | Tag assemblies are custom-programmed with product-specific information, marked with a unique part number. Tags are registered in the Authentication Database. |
| OEM or OEM Subcontractor | Product-specific tags are assembled into molded cords. |
| OEM or OEM Subcontractor | Product-specific cords are incorporated into finished product. |

**Potential Threats**

| Threat | Description | Defense |
|--------|-------------|---------|
| COTS Silicon | Plugs encoded with commercial off-the-shelf contactless transponders. | Silicon Security |
| Diverted Silicon | Authorized RightPlug silicon (i.e. wafer or dice) diverted through any means to unauthorized third-party. | Authentication Server, Audit Trail |
| Diverted Blank Transponders | Authorized RightPlug silicon assembled into transponders by authorized vendor, diverted through any means to unauthorized third-party. | Authentication Server, Audit Trail |
| Diverted Finished Transponders | Authorized RightPlug transponders custom-programmed with product-specific information by RightPlug Alliance or authorized subcontractor, diverted through any means to unauthorized third-party. | Authentication Server, Audit Trail<br><br>OEM Authentication Server. |
| Diverted Encoded Plugs | Authorized RightPlug silicon assembled into transponders by authorized vendor, diverted through any means to unauthorized third-party. | Authentication Server, Audit Trail<br><br>OEM Authentication Server, OEM Audit Trail. |
| Custom Silicon | Sophisticated third-party produces counterfeit custom silicon and assembles counterfeit transponders with data duplicated from authentic products. | Authentication Server<br><br>OEM Authentication Server<br><br>*Authentication Heuristics* |

**Silicon Security**

"Silicon Security" refers to key requirements for encoding transducer integrated circuits that precludes the use of commercial off-the-shelf (COTS) components.

- The advantage of using COTS components is reduced cost though consolidated production volumes with other applications, and greater confidence in proper component functionality though increased field experience.
- The only disadvantage to COTS components is the ease of duplication by third parties using readily available components.
- All contactless memory devices have a unique device identifier (UID). The "uniqueness" of the identifier is managed by incorporating an Integrated Circuit Manufacturer ID as part of the UID, and making each manufacturer responsible for managing uniqueness within their own UID-Space. Integrated Circuit Manufacturer IDs are assigned according to ISO/IEC 7816-6.

RightPlug Alliance has found a compromise by using COTS components but by special arrangement with the silicon supplier, the components are assigned UIDs with the RightPlug Alliance Integrated Circuit Manufacturer ID (0x2D) in place of their own.

Basic authentication becomes a simple process of verifying the Integrated Circuit Manufacturer ID reported by the plug encoding transponder matches the RightPlug Alliance ID.

This solution is not immune to circumvention; however it eliminates casual duplication of transponders using readily available parts. Furthermore, the level of sophistication required to create counterfeit transponders is elevated significantly. An organization that is capable of creating or sourcing semi-custom or custom silicon is also easier to trace and prosecute.

**RightPlug Authentication Server**

The second defense against counterfeit encoding transponders is an authentication server maintained by the RightPlug Alliance.

Prior to delivery to OEMs, all transponders are irrevocably configured with product-specific information. As part of the same process, a record of each transponder UID in a particular production batch is entered into the Authentication Database.

The RightPlug Authentication Server is internet-connected and has access to the Authentication Database. Any encoding transponder may be authenticated by transmitting certain data read from the transponder for comparison with the Authentication Database. As well as verifying that the transponder data matches stored information, the authentication process returns detailed product identification information to the requester, permitting verification that the product matches the encoded information.

Since the authentication interface is fully automated, transponders may be authenticated within seconds enabling rapid verification of entire shipments of product.

This method of authentication detects:

- Diverted Silicon & Diverted Blank Transponders – the silicon UID will have the correct Manufacturer ID, but will not appear in the Authentication Database since it has not been configured with product-specific information by the usual process. *See also Authentication Heuristics below.*

- Diverted Finished Transponders & Encoded Plugs – the transponder will be validated since it has passed through the proper configuration process. Additionally, since product identification information is returned along with authentication results the requesting party has the opportunity to determine if the product itself matches the encoded information. *See also OEM Authentication Server below.*

**Transponder Audit Trail**

In order to detect diversion of silicon components or blank transponders, though actions or neglect of a subcontractor or otherwise, subcontractors are required to maintain an electronic audit trail.

In addition to proactively detecting diversion of components, the audit trail provides for forensic identification of a diverted transponder discovered in the field. Using only the UID a transponder's history can be determined, including the probable point of diversion.

**Authentication Heuristics**

Although made extremely difficult by Silicon Security, it is possible for transponders to be manufactured by a third party. In this case it is probable that the transponder encoding data will be duplicated from existing valid product.

"Authentication Heuristics" refers to maintaining and analyzing records of Authentication Requests in order to detect patters that suggest particular transponders may have been duplicated, or that a particular party is making use of the authentication service to weed out non-compliant transponders from a batch.

- Multiple authentication requests from various locations for a particular UID are indicative of cloned transponders

- Authentication requests from a single location for multiple similar transponders, particularly with some authentication failures, is indicative of semi-cloned transponders with "intelligent guess" UIDs.

**OEM Authentication Server**

The RightPlug Authentication Database confirms that a particular transponder has followed the proper process to the point of shipment to an OEM or their designated cord manufacturing subcontractor. In order to confirm that a finished product has followed the OEM manufacturing process, the OEM optionally maintains a separate authentication database recording transponders that have been incorporated into finished goods. After verification with internal databases, the RightPlug Authentication Server additionally verifies the subject transponder with the OEM Authentication Database via an OEM Authentication Server.

This method of authentication detects:

- Diverted Finished Transponders & Encoded Plugs – the basic transponder will be validated since it has passed through the proper configuration process but, for OEMs that maintain an OEM Validation Server, the validation will fail since it has not passed though the OEM manufacturing process and does not appear in the OEM Authentication Database.

**OEM Audit Trail Information**

RightPlug records follow transponders to the point of shipment of programmed transponders to an OEM. OEMs that wish to have a complete audit trail must continue record keeping from receipt of transponders to completion of finished product.

Without the OEM Audit trail Information, it is not possible to easily detect diversion of transponders, or to identify the probably point of diversion within an OEMs process.

**Product Database**

The product database contains a manufacturer-supplied definition for each product and each product version/variant.

**Product**             One or more items from a single manufacturer with identical characteristics from a consumers point of view.

**Version**             A permanent design or configuration change of a product.

**Variant**             One of multiple design or configuration options of a product.

Manufacturers frequently update product designs, and in many cases offer several variants of essentially the same product. While it is desirable to require a completely unique product definition for each product variant, it is impractical for a number of reasons:

- A number of pre-programmed transponders will be in process at any given time
- Product revisions should not obsolete in-process transponders and molded cords
- It is impractical for multiple product versions to require unique transponders, especially in cases where manufacturers do not know the relative proportion for each variant.

Product Version/Variant ID (VID) is a means for manufacturers to stock a single transponder or molded cord type for a particular product, to be customized with product variant information as required.

Each product version or variant is registered in the Product Database and supplements or overrides certain information in the basic product definition.

Transponder Template

The Product Database contains much more information than can be stored in an encoding transponder. Each Product/Version/Variant has a Transponder Template that defines the information to be stored in each encoding transponder.

**Authentication Database**

The Authentication Database is created as transponders are programmed using a particular Transponder Template. A record of each transponder programmed is maintained for subsequent verification as part of the authentication process.

**Recall Database**

Manufacturers, and in some jurisdictions regulatory organizations, occasionally issue product recalls. The objective of the Recall Database is to provide an automated means of checking for product recalls as part of the authentication process.

Manufacturers, and authorized third parties, register recalls in the Recall Database, providing sufficient information to determine if a particular product is subject to the recall based on the MID, PID, VID and LID data within the encoding transponder.

### Documentation Database

The objective of the Documentation Database is to provide an automated means to retrieve product documentation at any point in the product life cycle.

Manufacturers optionally supply links to product documentation either as part of the initial product definition, or as a separate step. Manufacturers host the product documentation on their own servers and retain the option to restrict access to certain types of documentation.

End-users have easy access to product documentation as a side-effect part of the authentication process.

Service technicians have rapid access to technical drawings, service bulletins, recall notices and other key information specific to the product version/variant/lot being serviced.

### OEM Authentication Database

The optional OEM Authentication Database serves the same purpose as the RightPlug Authentication Database, extending coverage to include the VID and LID fields programmed by the manufacturer.

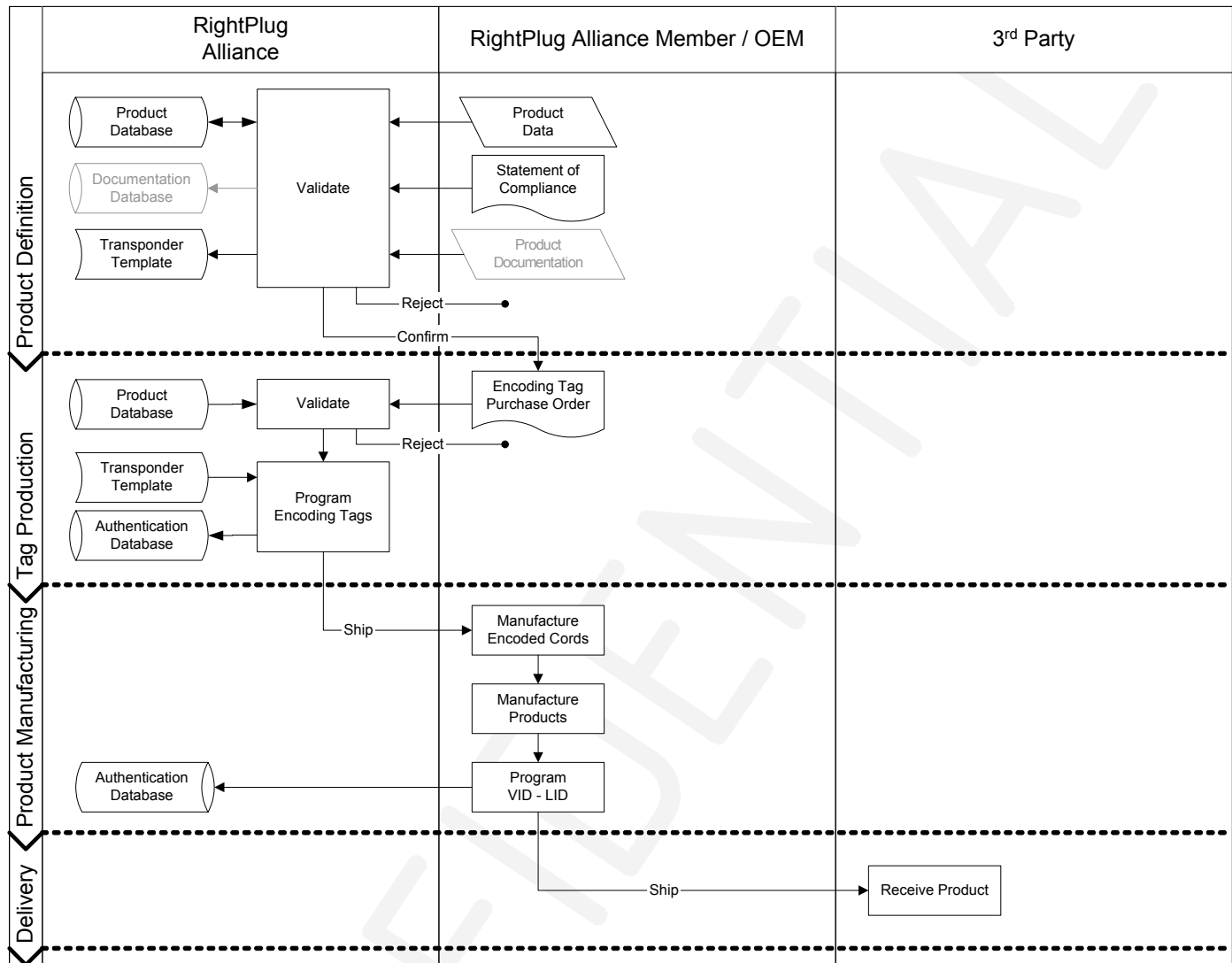## RightPlug Tag Process Flow

### Encoding Tag Manufacturing



Unassembled transponder ICs and blank assembled tags are the most likely targets for diversion. Transponder ICs are ordered in wafer form from the manufacturer, which are subsequently shipped to the transponder assembly subcontractor. A shipping report transmitted by the IC manufacturer, and a receiving report transmitted by the transponder assembly subcontractor ensure detection of diverted transponder ICs.

Transponder ICs are assembled into tags by the transponder assembly subcontractor, then shipped to the RightPlug Alliance. A shipping report transmitted by the IC manufacturer, and a receiving check ensure detection of diverted tags.

**End-Product Development and Manufacturing**



## Product Definition

The OEM creates a product definition in compliance with the RightPlug Standard. The product definition includes all required and optional information necessary to produce programmed transponders for the target product.

Links to relevant product documentation are optionally included in the product definition.

Products that have regulatory certifications require a statement of compliance supplied by the manufacturer certifying that the related products or version/variant are recognized as stated in the product definition.

In cases where a new version/variant of an existing product is being defined, the product definition includes only the information that is different from the root product definition.

The RightPlug Alliance server validates the supplied product definition according to the RightPlug Standard, assigns a Product ID and creates a Transponder Template.

## Tag Production

The OEM places an order for programmed transponders for a particular Product ID.

RightPlug server validates the order, and initiates production of the transponders using the corresponding Transponder Template simultaneously updating the Authentication Database.
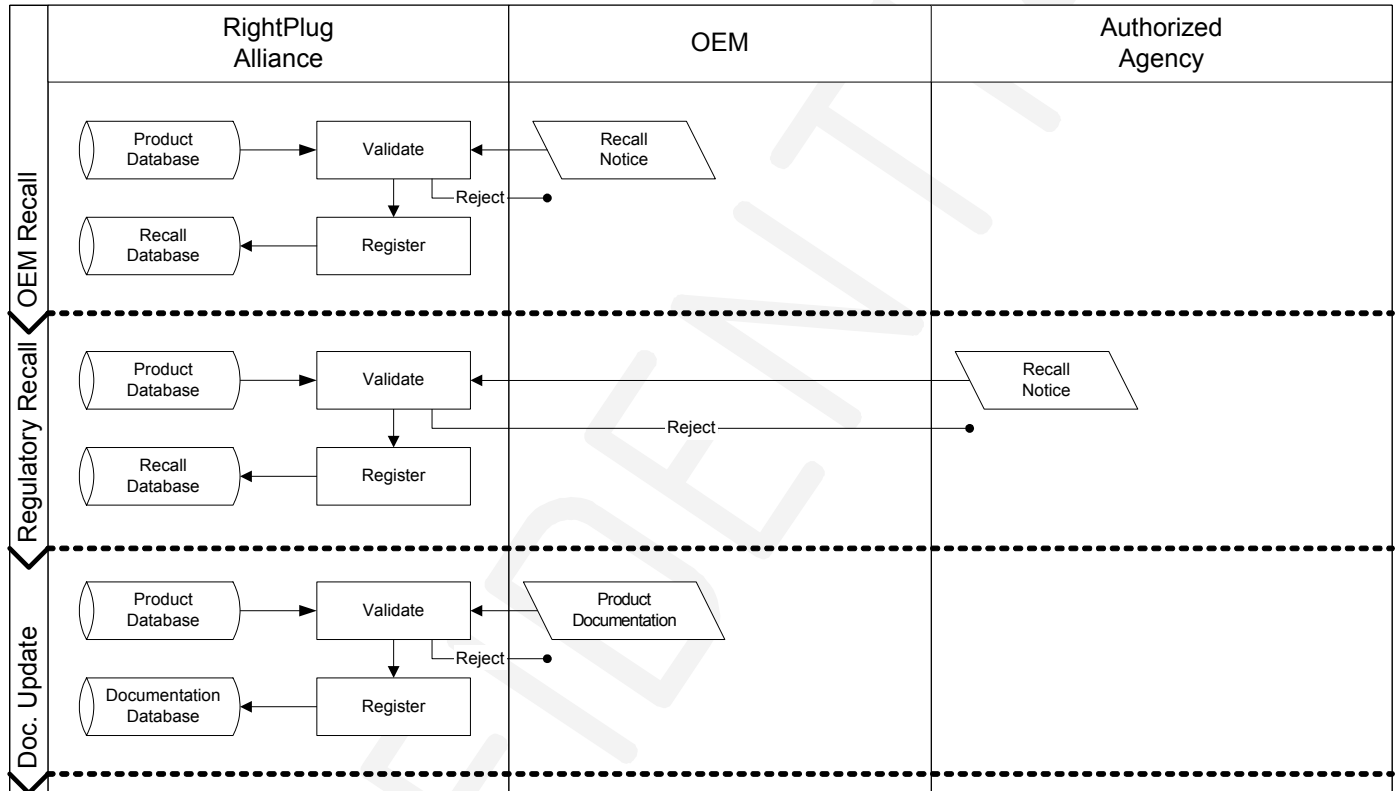
Product Manufacturing

Programmed transponders are received by the OEM and molded into cords which are subsequently incorporated into finished products. Version/Variant ID and Lot ID are optionally programmed into the transponders and added to the authentication database.

Delivery

Finished goods with fully encoded transponders embedded in plugs are delivered.
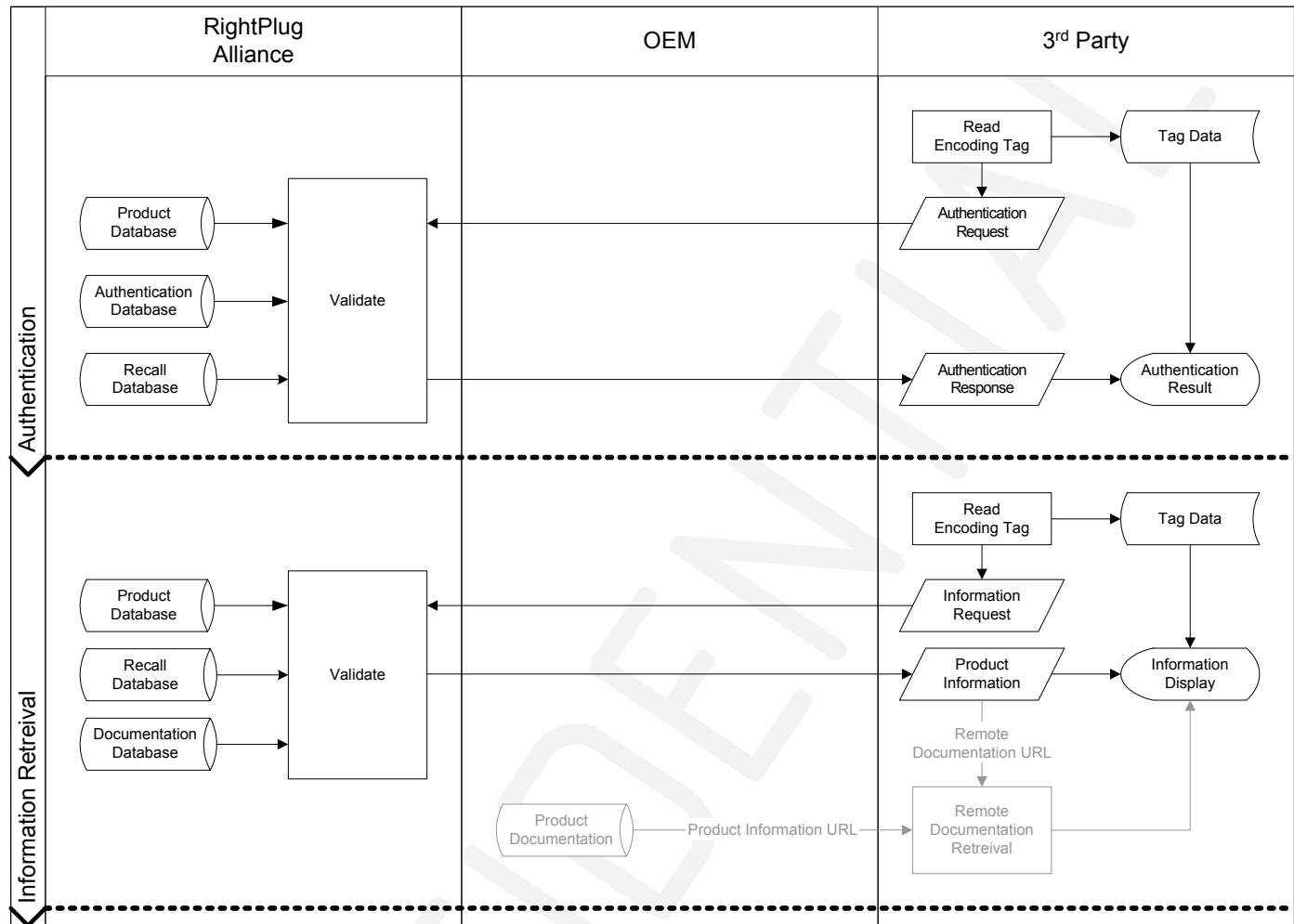
**Recalls and Documentation Update**



OEM Recall / Regulatory Recall

OEM or authorized third-party files a recall with the RightPlug server. The server validates the recall and stores the information in the Recall Database.

Documentation Update

OEM files a request to adds or updates links to product documentation with the RightPlug server. The server validates the documentation update and stores the information in the Documentation Database.

**Product Authentication and Information Retrieval**



## Authentication

Subsequent to scanning the plug of a product, product identification information is transmitted to the Authentication Server. The server:

- Confirms the product identification corresponds to a Product Definition in the Product Database
- Confirms that the unique transponder ID appears in the Authentication Database
- If an OEM authentication server is available, confirms that the unique transponder ID, Version/Variant and Lot ID match the OEM Authentication Database.
- Checks for recalls for the product
- Returns the results to the requester, along with detailed product description for comparison with actual product characteristics.

## Information Retrieval

Subsequent to scanning the plug of a product, product identification information is transmitted to the Authentication Server. The server:

- Performs product authentication
- Retrieves and returns relevant product documentation links