CREATING A DIGITAL CERTIFICATE

In IPC-1792, every product or part produced by a stakeholder must include a Digital Certificate to verify authenticity.

The following describes the nature (format) of the digital certificate and its transmission.

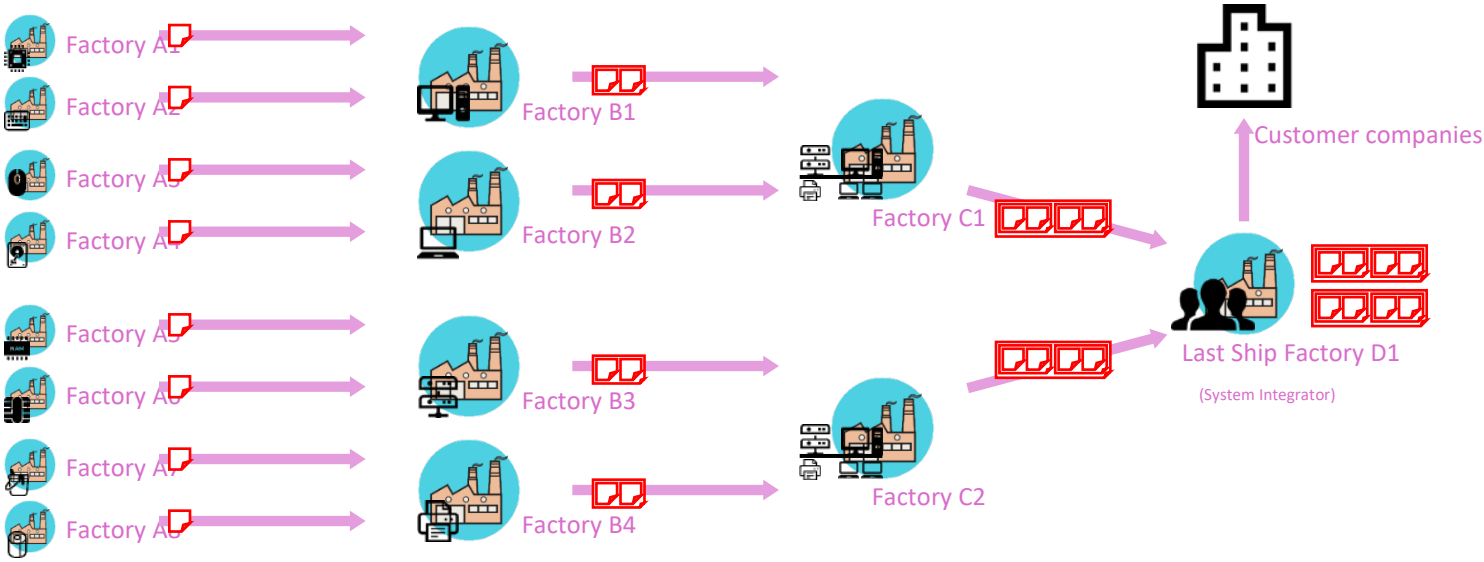
The core principle of IPC-1792 is to safeguard the integrity of shipped products by attaching a Digital Certificate. This certificate contains product details and a Digital Diploma verifying the product's origin.

The operation of the Digital Certificate during normal shipping works as follows:

- When an upstream stakeholder ships a product, it attaches key product details (manufacturing date, factory, production line, etc.) along with its Digital Diploma. Together, these form the Digital Certificate, which is then sent to the downstream stakeholder.
- The downstream stakeholder receiving the product and its Digital Certificate then issues its own Digital Certificate. This includes its product details, its Digital Diploma, and all certificates received from upstream stakeholders.

By repeating this process, the final stakeholder delivering to the customer consolidates all certificates, ensuring complete security assurance across the supply chain. IPC-1792 achieves this by passing trust downstream in a bucket-brigade fashion.

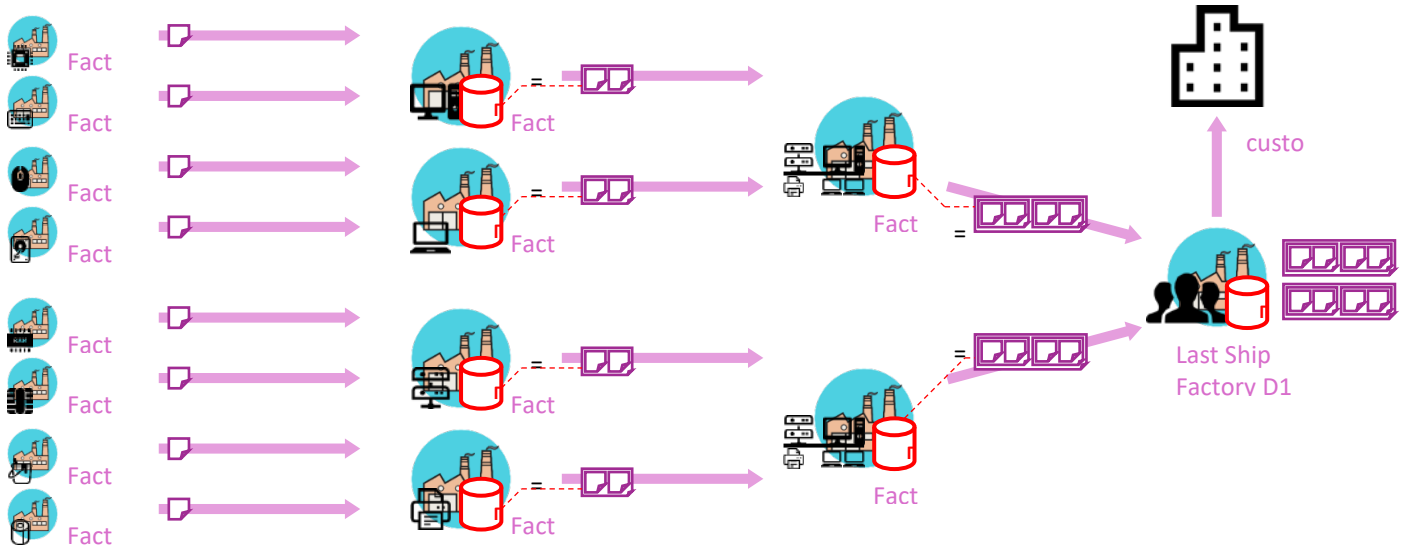
Currently, stakeholders must maintain records of when and to whom their products are shipped. IPC-1792 also requires stakeholders to retain Digital Certificates received from their upstream stakeholders.



There are two reasons for saving a Digital Certificate:

1) Verify impacted products shipped by the factory and the parts/materials that make up those products after a security risk has occurred
2) In the event of an incident, notify downstream supply chain stakeholders based on the Digital Certificate

It is optional whether the intermediate supply chain entity periodically checks the product validity of the upstream supply chain entity when the shipped product is received or during inventory management (i.e., if the Digital Diploma included in the Digital Certificate is validated by contacting the Cyber Security Diploma Manager).



Digital Diploma JSON Description

In supply chains, stakeholders share information, but the whole system can be at risk if one supplier cannot be trusted. With IPC-1792, stakeholders work together to communicate key information to ensure product authenticity and to notify the supply chain stakeholders of a cybersecurity incident.

The IPC-1792 digital diploma is electronic proof that a stakeholder is qualified to participate in the IPC-1792 system. This following describes the digital diploma format.

Configuring Digital Diplomas

An example implementation of Digital Diploma in JSON format is shown below.

```
"JSON":{
        "ver":    < About >,
        "dip": {< Digital Diploma (Factory Specific Information) >},
        "key": {< Public Key >},
        "doi":    < Date Published >,
}
```

IPC-1792 for Web – Digital Certificates and Digital Diplomas

Field ID	Field name	Instructions
ver	Schema Version	Shall match the identifier of the schema version used to create the digital diploma. Example:"ver": "1.3.0"
Dip/Facide	Factory ID	A 10 digit unique identifier. The Digital Diploma Manager defines and notifies the factory.
Dip/Fence	Plant name	Plant name. A string of up to 64 characters. For example, the name of a company or facility. A unique name is not required.
dip/mgr	Name of the plant manager	Name of the plant manager. This name is registered with the Digital Diploma Manager.
DIP/CO	Country	Country represented by a two-letter ISO 3166 code
Dip/Wiss	Diploma Issuer (Digital Diploma Manager)	Identifier of the Digital Diploma Manager responsible for publishing the Digital Diploma. A 10 character string defined for each Digital Diploma Manager.
Key/Pub Key	Public Key	The public key used for digital signatures. The key information registered with the certificate authority can be viewed by other factories.
doi	Issue Date	Timestamp A full or partial date without time, limited to the range 1900 01-01 to 2099-12-31. Only one non-empty field shall be provided. One of the following ISO 8601 formats shall be used: Other options are not supported. YYYY-MM-DD YYYY-MM YYYY-MM

The following is an example of Digital Diploma.


```
{
"JSON": {
    "ver": "2020-12",
    "dip": {
        "facid": "1234567890",
        "fence": "Example Co.,Ltd.",
        "mgr": "John Michael Smith",
        "co": "jp",
```

```
        "wiss": "PID-123456"
    },
    "key": "44GT44KM44...Gv5YWs6ZaL",
    "doi":"2025-12-31"
}
```