HID Global CID (PT Jasuindo HID Security)

Raya Lingkar Timur Km. 1

Block B, Banjarsari Sidoarjo

INDONESIA

www.hidglobal.com

HID Global CID Public Site Security Target

Common Criteria version 3.1 revision 5

Assurance Level EAL 5+

Version	0
Date	2020-12-2
Reference	PK-SC-008
Classification	PUBLIC

Table of Contents

List of Tables

1 Introduction

1.1 SST Overview

The Site Security Target refers to HID Global CID (PT Jasuindo HID Security) Factory (hereinafter referred as "JAWS"). The site can be part of the production flow for Security IC's used for identification products. The site provides the assembly of inlays, e-covers, datapage and similar products. Therefore this site is suitable for any type of HID Global CID security products including secure IC.

This chapter is divided into the sections "SST Reference and Site Reference" and "Site description".

Table 1-1 SST Identification

Title	HID Global CID Public Site Security Target
Version	0
Date of Issuance	2020-12-2
Authors	Arief WAHYU
Site Reference	HID Global CID (PT. Jasuindo HID Security)
Site Address	Jalan Raya Lingkar Timur Km. 1, Block B, Banjarsari, Sub-district of Buduran, District of Sidoarjo, Province of East Java, Indonesia
Product type	Inlays, e-covers, datapage and similar products
Reference	PK-SC-008

1.2 Site Description

1.2.1 Physical scope of the site

The factory and office of JAWS is located at JI. Raya Lingkar Timur Km. 1, Block B, Banjarsari, Sub-district of Buduran, District of Sidoarjo, Province of East Java, Indonesia.

JAWS is located in the premises of PT Jasuindo Tiga Perkasa, Tbk. (hereinafter referred as "JTP"). It is a complex of factory building owned by JTP. The area of JAWS, either outside or inside the factory buildings, is classified according to the level of security requirements for the different activities held and its relation to sensitive assets and process. The minimum requirement is expressed by a physical level which are:

- Non Secure Area (Public/Level 1). The security system installed is CCTV and electronic card reader only.
- Secure Area (Level 2). The security system installed is CCTV, electronic card reader, use keypad of personal identification code (double authentication), and body checking by security guard.
- High Security Area (level 3), The security system installed is CCTV with infrared camera, dual control access door with finger print authentication, and body checking by security guard.

The rooms in scope of the site certification are located in the building of JAWS comprises the following rooms:

Two rooms consist of office and meeting room in the second floor, and the lobby on the first floor with public access.

The rooms which classified as secure area are the rooms of server, warehouse, shredding, preparation, inlay manufacturing, finishing, manager, lamination, test center and laboratory. There is a vault room as high secure area.

1.2.2 Logical scope of the site

JAWS provides a process of production in this facility as follows:

- embedding of contactless chip/module with single interface Security IC into paper and or plastic by machine and or manual (soldering)
- lamination and trimming of inlay (paper inlay or plastic inlay)
- cover gluing for e-cover product (if required)
- packing and delivery, to be handed over to the transporter (chosen by the customer)
- destruction of secure (sensitive) materials and defective products
- acceptance tests (electrical and mechanical)

The finished product from this facility is delivered to the consumer by third party delivery vehicle service or transporter company which is arranged directly by the customer.

The finished product of JAWS could be as inlay only or e-cover (or similar products). The scope of e-cover is just to put the cover with cover gluing process.

The process of receiving and storage of raw material at the warehouse has been specifically designed for securely handle secure materials. The chip/module as secure material is stored inside of a vault located inside the high-security level area with limited access and only for authorised person.

During the production process, all related data and documents are secured in the secured server of computer with limited access based on a need to have principle, e.g. production

manager and supervisor, QC manager and supervisor. The area of production, incl. for the warehouse, is categorized as secure area which only for the authorised employees given an electronic access to enter.

Communication with the customer to submit the electronic data of finished product, called as “white-list”, through an electronic mail (email) is done by an authorised employee from QC department by using an encrypted file.

During the shipment / delivery process, in case any request from the customer to submit an electronic data of the finished product, together within the shipment / delivery, through a data carrier such as compact disc shall use an encryption.

JAWS also provides service of destruction of secure (sensitive) materials.

Human resources, security guards and IT administration are managed by PT Jasuindo Tiga Perkasa, Tbk. (parent company of JAWS).

1.3 Inclusion in a TOE life-cycle

This SST covers the embedding of the programmed IC into a plastic or paper substrate, optionally equipping it with an antenna (for ISO 14443 interface), and optionally exposing IC contacts (for ISO 7816-2 interface). This activity is referenced as step 4 in Table 1-2 shows a generic life cycle of smartcard product (for example: passport, identity, QSCD, bank card).

Table 1-2 Generic life cycle

Phase	Step	Actor
Development	Step 1 : Development of the IC and the IC Dedicated Software	IC developer and manufacturer
	Step 2 : Development of native application or Applet	Embedded software developer
Manufacturing	Step 3 : Loading of the applet or native application	IC developer and manufacturer
	Step 4 : Manufacturing of inlays e-covers, datapage or similar device	JAWS
	Step 5 : pre-personalization	Pre-personalization agent
Personalization	Step 6: personalization	Personalization agent
Operational Use		Final user

In step 3, the **IC Manufacturer** produces the TOE integrated circuit (IC), containing the IC Dedicated Software and the Embedded Software (native application or applet), and creates in the IC persistent memory the high-level objects.

The TOE is securely delivered from the **IC Manufacturer** to JAWS.

The services provided by JAWS are related to step 4.

JAWS securely delivers the final product to **Pre-personalization Agent** (for step 5) defined by the client. Delivery process is also defined by the client.

2 Conformance Claims

The evaluation is based on Common Criteria Version 3.1, release 5:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5, April 2017,*[R1*].
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017, *[R2*]

This SST is CC part 3 conformant. For the evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 5, April 2017,*[R3*].
- Supporting Document, Site Certification, October 2007, Version 1.0, Revision 1, CCDB-2007-11-001 *[R4*].
- Guidance for Site Certification, Bundesamt für Sicherheit in der Informationstechnik, Version 1.1 , 2013-12-04. *[R5*].

The evaluation of the site comprises the following assurance components:

ALC_CMC.4, ALC_CMS.5, ALC_DVS.2, ALC_LCD.1[1], [2]

The assurance level chosen for the SST is compliant to the Protection Profile (PP) *[R6]* and therefore suitable for Security ICs.

The chosen assurance components are derived from the assurance level EAL5 of the assurance class "Life-cycle Support". For the assessment of the security measures, attackers with high attack potential are assumed. Therefore this site supports product evaluations of products up to EAL5 augmented with ALC_DVS.2 and AVA_VAN.5.

[1] Since the delivery methods are defined upfront by the client (see A. Product-Delivery), the site does not contribute to ALC_DEL and does not have any negative impact to it. Therefore the site does not claim conformance to ALC_DEL

[2] As the site does not directly contribute to the development of the intended TOE in the sense of Common Criteria, the site does not contribute to ALC_TAT and does not have any negative impact to it. Therefore the site does not claim conformance to ALC_TAT

The assurance components chosen for the Site Security Target are compliant to the Protection Profile (PP) *[R6]*. Therefore the scope of the evaluation is suitable to support product evaluations up to assurance level EAL5 conformant to Part 3 *[R2]* of the Common Criteria.

Support of transport or delivery for security products is limited to the boxing and labelling for the shipment as well as the notification of the client. The transport or delivery of security products is not part of the evaluation. This is organised and under the control of the client.

3 Security Problem Definition

The Security Problem Definition comprises security problems derived from threats against the assets handled by the site and security problems derived from the configuration management requirements. The configuration management covers the integrity of the TOE and the security management of the site. The goal is to achieve and hold a high security level to counter attacks with high attack potential at the site.

3.1 Assets

The following assets are handled at the site:

- Modules (contains IC)
- Inlays,
- E-covers,
- Datapage,
- Rejects of secure materials, such as modules, inlays, e-covers, datapage and finished products,
- Documentation of evaluated products,
- Chip serial ID number and related chip card number

3.2 Threats

All threats endanger the integrity and confidentiality of the intended TOE and the representation of parts of the TOE. The intended TOE protects itself in operational use. However, during the development, production, test and assembly the TOE and the representation of parts of the TOE are vulnerable to such attacks.

T.Smart-Theft: An attacker tries to access sensitive areas of the site for manipulation or theft of sensitive configuration items. The attacker has sufficient time to investigate the site outside the controlled boundary. For the attack, the use of standard equipment for burglary is considered. In addition the attacker may be able to use specific working clothes of the site to camouflage the intention.

This attack already includes a variety of targets and aspects with respect to the various assets listed in the section above. It covers the range of individuals that try to get unregistered or defect devices that can be used to further investigate the functionality of the device and search for possible exploits. Such an attacker will have limited resources and a low financial budget to prepare the attack. However the time that can be spent by such an attacker to prepare the attack and the flexibility of such an attacker will provide notable risk. It is expected that such an attacker can be defeated by state-of-the-art physical, technical and procedural security measures like access control and surveillance. In general, an access control concept with two or three levels is to be implemented. If two levels are implemented, the more restrictive level of the access control prevents the simple access using a lost or stolen access token. Other restrictions may be the need for parallel access by two employees. The technical measures includes automated measures to support the surveillance.

T.Rugged-Theft : An experienced thief with specialized equipment for burglary, who may be paid to perform the attack, tries to access sensitive areas and manipulate or steal sensitive configuration items.

Although this attack is applicable for each site the risk may be different regarding the assets. These attackers may be prepared to take high risks for payment. They are considered to be sufficiently resourced to circumvent security measures and do not consider any damage done to the affected company. The target of the attack may be products that can be sold or misused in an application context. This can comprise devices at a specific testing or personalization state for cloning or introduction of forged devices. Those attackers are considered to have the highest attack potential.

Such attackers may not be completely defeated by the physical, technical and procedural security measures. Special measures like storage of items in safes or strong rooms or the splitting of sensitive data like keys provide additional protect against such attacks. Also the unique registration of the products can support the protection if they can be disabled or blocked.

T.Computer-Net: A hacker with substantial expertise, standard equipment, who may be paid to attempt to remotely access sensitive network segments to get data such as test data or other sensitive production data or modify the testing or production process at the site.

A logical attack against the network of the site provides the lowest risk for an attacker. The target of such an attack is to access the company network to get information that may allow to attack a product or manipulate a product or retrieve information to allow or change the configuration or the personalization. In addition, a successful access to a company network leads to loss of reputation of the company processing the product or the company that produces the product.

Such attackers are considered to have high attack potential because the attacker may have appropriate technical equipment to perform such an attack. Furthermore, the attacker may have the resource to develop or buy software or hardware which can exploit known vulnerabilities within the tools and software used by the company.

Therefore, also for the company network a protective concept with more than one level is expected. This comprises a firewall to the external network, and further limitations of the network users and the network services for internal sub-networks. In addition, computer users have individual accounts which require authentication using e.g. a password. For specific tasks or processes standalone networks may be required. The protection must be supported by appropriate measures to update and maintain the computer and network systems and analyse logs that may provide indications for attack attempts.

T.Accident-Change: An employee, contractor or student trainee may exchange products of different production lots or different clients during production by accident.

Employees, contractors or student trainees that are not trained may take products or influence production systems without considering possible impacts or problems. This threat includes accidental changes e.g. due to working tasks of student trainees or maintenance tasks of contractors within the development, production or test area.

Such accidental changes can include the modification of configurations for tools that may have an impact on the TOE, the wrong assignment of tools for a dedicated process step. Further examples may be machine failure or misalignment between operators that are responsible for products of different clients or different products of the same client are mixed during production. This also includes the disposal of sensitive products using the standard flow and not the controlled destruction.

T.Unauthorised-Staff: Employees or subcontractors not authorised to get access to products or systems used for production get access to products or affect production systems or configuration systems, so that the confidentiality and/or the integrity of the product is violated. This can apply to any production step and any configuration item of the final product as well as to the final product or its configuration.

Especially maintenance tasks of subcontractors may require the access to computer systems storing sensitive data. The implemented security measures may not work because a special dedicated access may be used to the network or specific tools may be used for this dedicated task. This comprises e.g. tools which process the layout data e.g. in the design centre, the mask shop and/or the wafer foundry as well as sensitive test and/or configuration data within the test center.

Also other subcontractors like cleaning staff or maintenance staff for the building get limited access that may allow them to start an attack. The disposal of defect equipment and/or sensitive configuration items must be considered.

The attack potential depends on the trustworthiness of the subcontracted company and the access required within the company. Related to these different measures are required.

T.Staff-Collusion: An attacker tries to get access to material processed at the site. The attacker tries to get support from one employee through an attempted extortion or an attempt at bribery.

Personal accountability is to be traceable as far as possible. Handover procedures with dual control, enforcement of parallel access by two authorised employees and the split of sensitive knowledge like personalization keys can be implemented to prevent such an attack. The measures depend on the assets that must be protected at the site.

T.Change-Shipping: An attacker might try to change addresses or labels during the preparation of the shipment or might try to masquerade a pick-up service.

3.3 Organisational Security Policies

The following policies are introduced by the requirements of the assurance components of ALC for the assurance level EAL5. The chosen policies support the understanding of the production flow and the security measures of the site. In addition, they allow an appropriate mapping to the Security Assurance Requirements (SAR).

The documentation of the site under evaluation is under configuration management. This comprises all procedures regarding the evaluated test and assembly flows and the security measures that are in the scope of the evaluation.

P.Config-Items: The configuration management system shall be able to uniquely identify configuration items. This includes the unique identification of items that are created, generated, developed or used at a site as well as the received and transferred and/or provided items.

The site is not involved in TOE development, the only configuration items are procedures and production process.

The identification is ensured by the internal quality procedure. This holds also for test tools and other items that are provided to the site for local use. For configuration items that are created, generated or developed at the site the naming and identification is specified.

P.Config-Control: The procedures for setting up the production process for a new product as well as the procedure that allows changes of the initial setup for a product shall only be applied by authorised personnel. Automated systems shall support the configuration management and ensure access control or interactive acceptance measures for set up and changes. The procedure for the initial set up of a production process ensures that sufficient information is provided by the client.

The product setup includes the following information (i) identification of the product, (ii) properties of the product when received at the site (iii) properties of the product when it is prepared for shipping, (iv) classification of the items (which are security relevant), (v) how the product is tested after production, (vi) which address is used for transport.

P.Config-Process: The services and/or processes provided by a site are controlled in the configuration management plan. This comprises tools used for the production of the product, the management of flaws and optimisations of the process flow as well as the documentation that describes the services and/or processes provided by a site.

The documentation describing the processes are under version control. Tools and data bases are used to support the production of the site. This comprises e.g. configuration management tools and commercial data base systems. The configuration control comprises data and parameter for testing and quality parameters.

P.Reception-Control: The inspection of incoming items done at the site ensures that the received configuration items comply with the properties stated by the client. Furthermore, it is verified that the product can be identified and a released production process is defined for the product. If applicable this aspect includes the check that all required information and data is available to process the items.

P.Accept-Product: The testing and quality control of the site ensures that the released products comply with the specification agreed with the client. The acceptance process is supported by tests of the final products. Records are generated for the acceptance process of the configuration items. Thereby, it is ensured that the properties of the product are ensured when internally shipped.

P.Zero-Balance: The site ensures that all sensitive items (security relevant parts of the security products of different clients) are separated and traced on a device basis. Two employees acknowledgement (four-eyes principle) is applied for functional and defect assets hand over. According to the production process and security policy the defect assets are destroyed at the site.

P.Transport-Prep: Technical and organisational measures shall ensure the correct preparation for the shipment of products. Procedures are in place to confirm the shipping address, check the forwarder before handing over products and ensure the preparation of the shipment conform to the requirements of the client.

P.Data-Transfer: Any data in electronic form (e.g. product specifications, test programs, test program specifications, release information etc.) that is classified as sensitive, by the client or JAWS, is encrypted to ensure confidentiality of the data. In addition to, measures are used to control the integrity of the data after the transfer.

3.4 Assumptions

JAWS site is operating in a production flow and therefore must rely on preconditions provided by the client. This means, each site relies on the materials and information received by the client. This is reflected by the assumptions which are to be fulfilled by the client.

A.Item-Identification : Each configuration item received by the site is appropriately labelled to ensure the identification of the configuration item.

A.Product-Specification : The client must provide appropriate product specifications, process limits, process parameters, test requirements, tests tools, test limits, bond plans in order to ensure an appropriate production process. The provided information includes the classification of each part of the deliverables (products, documents, data and keys). All these data have to be provided to JAWS in encrypted format.

A.Product-Integrity: The self-protecting features of the devices are fully operational and it is not possible to influence the configuration and behaviour of the devices based on insufficient operation conditions or any command sequence generated by an attacker or by accident.

A.Product-Delivery: The delivery address and the packing requirements are part of the product setup. They are defined by the client. The recipient of the finished inlays (or e-covers, datapage or similar products) is identified by the information and address provided by the client. In case the provided address is an external customer address the client is responsible of informing the external customer.

A.Shipment: The forwarder is selected by the client and the shipping and tracing of the shipment is under control of the client. The hand over of the products between the client and JAWS is applied in the loading bay of JAWS for receipt and delivery.

The assumptions are outside the sphere of influence of JAWS. They are needed to provide an appropriate production process, assign the product to the released production process and ensure the proper handling, storage and destruction of all configuration items related to the products.

4 Security Objectives

The Security Objectives are related to physical, technical and organisational security measures, the configuration management as well as the transport.

O.Physical-Access: The combination of physical partitioning between the different access control levels together with technical and organisational security measures allows a sufficient separation of employees to enforce the “need to know” principle. The access control supports the limitation for the access to these areas including the identification and rejection of unauthorised people. The site enforces three levels (non secure, secure and high secure) of access control to the common part of the site (secure level) and to the production area of the site (high secure level). The access control measures ensure that only registered employees can access production area. Sensitive products are handled in production area only.

O.Security-Control: Assigned personnel of the site or guards operate the systems for access control and surveillance and respond to alarms. Technical security measures like video control, motion sensors and similar kind of sensors support the enforcement of the access control. These personnel are also responsible for registering and ensuring escort of visitors, contractors and suppliers.

O.Alarm-Response: The technical and organisational security measures ensure that an alarm is generated before an unauthorised access to any sensitive asset is possible. Further unauthorised access on sensitive material after triggering an alarm is averted by further security measures and that the reaction time on the alarm is short enough to prevent a successful attack.

O.Internal-Monitor: The site performs security management meetings regularly. In scope of these meetings, security incidents are reviewed, maintenance measure appliance is verified and the assessment of risks and security measures is reviewed. Furthermore, an internal audit is performed on regular basis to ensure appliance of the security measures.

O.Maintain-Security: Technical security measures are maintained regularly to ensure correct operation. The logging of sensitive systems is checked regularly. This comprises the access control system to ensure that only authorised employees have access to sensitive areas as well as computer/network systems to ensure that they are configured as required to ensure the protection of the networks and computer systems.

O.Logical-Access: The site enforces a physical separation between the internal production area network and the internet: internal production area network is not connected to internet. Furthermore, the internal network is physically separated into a production area network and an office network. Specific networks are physically separated from any other network to enforce access control. Access to the production area network and related systems is limited to authorised employees that work in the related area or that are involved in the configuration tasks of the production systems. An authentication using user account and password is enforced by all computer systems.

O.Logical-Operation: All network segments and the computer systems are kept up-to-date (software updates, security patches, virus protection, spyware protection). The backup of sensitive data and security relevant logs is applied according to the classification of the stored data. Access to the backup is also restricted to authorised person only.

O.Config-Items: The site has a configuration management system that assigns a unique internal identification to each product to uniquely identify the internal associated procedures and guidance and allow an assignment to the client.

O.Config-Control: The site applies a release procedure for the setup of the production process for each new product. In addition, the site has a process to classify and introduce changes for services and/or processes of released products. Minor changes are handled by the site, major changes must be acknowledged by the client. A designated team is responsible for the release of new products and for the classification and release of changes. This team comprises specialists for all aspects of the services and/or processes. The services and/or processes can be changed by authorised personnel only. Automated systems support configuration management and production control.

O.Config-Process: The site controls its services and/or processes using a configuration management plan. The configuration management is controlled by tools and procedures for the production of the product, for the management of flaws, for the management of roles separation and optimisations of the process flow as well as for the documentation that describes the services and/or processes provided by a site.

O.Acceptance-Test: The site delivers configuration items that fulfil the specified properties. Parameter checks, functional and/or visual checks and tests are performed to ensure the compliance with the specification. The test results are logged to support tracing and the identification of systematic failures.

O.Staff-Engagement: All employees who have access to sensitive configuration items and who can move parts of the product out of the defined production flow are checked regarding security concerns and have to sign a nondisclosure agreement. Furthermore, all employees are trained and qualified for their job.

O.Zero-Balance: The site ensures that all sensitive products (intended TOE of different clients) are separated and traced on a device basis. Two employees acknowledgement during hand over is applied for functional and defective devices. All devices are tracked until they are either shipped or destructed locally.

O.Reception-Control: Upon reception of product an initial incoming inspection is performed. The inspection comprises the received amount of products and the identification and assignment of the product to a related internal production process.

O.Shipping-Support: The address of the receiver of a finished product is maintained in the system. In addition to the packing procedures are applied as specified by the client. The forwarders are registered.

O.Control-Scrap: The site has measures in place to destruct sensitive documentation, erase electronic media and destroy sensitive configuration items so that they do not support an attacker. Rejected or defect devices are destructed locally.

O.Transfer-Data: Sensitive electronic configuration items (data or documents in electronic form) are protected with cryptographic algorithms to ensure confidentiality and integrity. The associated keys are managed accordingly to JAWS security policy.

4.1 Security Objectives Rationales

The following tracing shows which security objectives address which threats and organisational security policies. The note provides further information how the security objectives address the threats or organisational security policies.

Table 4-1 security objectives

	O.Physical-Access	O.Security-Control	O.Alarm-Response	O.Internal-Monitor	O.Maintain-Security	O.Logical-Access	O.Logical-Operation	O.Config-Items	O.Config-Control	O.Config-Process	O.Acceptance-Test	O.Staff-Engagement	O.Zero-Balance	O.Reception-Control	O.Shipping-Support	O.Control-Scrap	O.Transfer-Data
T.Smart-Theft	X	X	X	X	X												
T.Rugged-Theft	X	X	X	X	X												
T.Computer-Net				X	X	X	X									X	
T.Accident-Change						X	X	X		X	X	X	X				
T.Unauthorised-Staff	X	X	X	X	X												
T.Staff-Collusion				X	X							X					
T.Change-Shipping															X		
P.Config-Items								X									
P.Config-Control								X	X								
P.Config-Process										X							
P.Reception-Control														X			
P.Accept-Product									X	X	X						
P.Zero-Balance				X								X	X			X	
P.Transport-Prep										X					X		
P.Data-Transfer																	X

The threats **T.Smart-Theft** and **T.Rugged-Theft** are covered by **O.Physical-Access** that ensures that all unauthorised people who have a legitimate need to visit the production area are always accompanied.

O.Security-Control and **O.Alarm-Response** ensure that the unauthorised people cannot circumvent this .

O.Internal-Monitor and **O.Maintain-Security** ensure that the above is managed and maintained.

The threat **T.Computer-Net** is covered by **O.Logical-Acces** that ensures that network is physically separated into a production network and an office network. It ensures that no remote access are possible to the production network.

O.Internal-Monitor, **O.Logical-Operation** and **O.Maintain-Security** ensure that the production network is managed and maintained.

O.Control-Scrap ensures that attackers cannot obtain sensitive data that may come from the production area on discarded hard disks.

The threat **T.Accident-Change** is covered by **O.Logical-Acces** that ensures that Users have their own account with dedicated password and the account is limited to the access rights required by the job task and their responsibility following a strict “need to know principle”.

O.Logical-Operation ensures that the production network used backup and appropriate storage of the backup are applied to prevent the loss of data.

O.Config-Items ensures that each received item is assigned to a unique product part number.

O.Config-Process ensures that a team of employees responsible for the product handling and the production is defined to plan, organise and control the production process.

O.Acceptance-Test ensures that acceptance tests are performed to ensure the compliance with the specification.

O.Staff-Engagement ensures that all employees get training that shall ensure the knowledge of the processes.

O.Zero-Balance ensures that any missing security device can be detected by this process.

The threat **T.Unauthorised-Staff** is covered by **O.Physical-Access** that ensures that all unauthorised people who have a legitimate need to visit the production area are always accompanied.

O.Security-Control and **O.Alarm-Response** ensure that the unauthorised people cannot circumvent this.

O.Internal-Monitor and **O.Maintain-Security** ensure that the above is managed and maintained.

The threat **T.Staff-Collusion** is covered by **O.Staff-Engagement** that ensures that all staff is aware of its reponsibilities (signing NDAs, work contracts and being trained).

O.Internal-Monitor and **O.Maintain-Security** ensure that the security measures to protect assets are managed and maintained.

The threat **T.Change-Shipping** is covered by **O.Shipping-Support** that ensures that the shipping information and the preparation procedure for the shipment are managed to prevent wrong shipments.

The OSP **P.Config-Items** is covered by **O.Config-Items** which assigns unique numbers to the internal procedures and guidance.

The OSP **P.Config-control** is covered by **O.Config-Items** and **O.Config-Control** ensures that the services and processes provided by the site ,described in the internal procedures and guidances, are in the scope of the configuration control.

The OSP **P.Config-Process** is covered by **O.Config-Process** that ensures that the services and processes provided by the site, described in the internal procedures and guidances, are in the scope of the configuration control.

The OSP **P.Reception-Control** is covered by **O.Reception-Control** that ensures the correct assignment of the input of the production.

The OSP **P.Accept-Product** is covered by **O.Config-Process** and **O.Config-Control** that ensure that the internal procedures and guidances associated to a production, are in the scope of the configuration control.

O.Acceptance-Test ensures parameter checks, functional and/or visual checks and tests are performed to ensure the compliance with the specification

The OSP **P.Zero-Balance** is covered by **O.Internal-Monitor** that ensures that the security measures to protect assets are managed and maintained.

O.Staff-Engagement ensures that all staff is aware of the rules to apply.

O.Zero-Balance and **O.Control-Scrap** ensure that all rejected products are locally destroyed.

The OSP **P.Transport-Prep** is covered by **O.Config-Process** that ensure that the correct preparation for shipment for the production are in the scope of the configuration control.

O.Shipping-Support ensure the correct preparation for the shipment of products

The OSP **P.Data-Transfer** is covered by **O.Transfer-Data** that ensures that the transmission of data classified as sensitive is protected using encryption according to JAWS security policy.

5 Extended Components Definition

No extended components are currently defined in this SST.

6 Security assurance requirements

The security assurance requirements shall support an evaluation according to the assurance level EAL5.

The Security Assurance Requirements (SARs) are:

- Class ALC: Life-cycle support CM capabilities (ALC_CMC.4),
- CM scope (ALC_CMS.5),
- Development security (ALC_DVS.2),
- Life-cycle definition (ALC_LCD.1)

6.1 Security Assurance

6.1.1 Application Notes and Refinements

The description of the site certification process [*R4*] includes specific application notes. The main item is that a product that is considered as TOE is not available. Since the term “TOE” is not applicable in the Site Security Target the associated processes for the handling of products are in the focus and described in this Site Security Target. Theses processes are subject of the evaluation of the site.
Many of the products processed by JAWS are considered to follow the life cycle model defined in the Security IC Platform Protection Profiles [*R6*]. Therefore relevant aspects of the refinements defined in the Protection Profiles [*R6*] are reproduced in this Site Security Target if they are considered as relevant for the evaluation process. Since a TOE is not available the application notes of [*R4*] are also applied for the refinements of the Protection Profile.

6.1.2 CM capabilities : ALC_CMC.4

For ALC_CMC, one should describe all elements that are relevant for identifying and labeling different versions of the configuration items listed by ALC_CMS and the relation between these two.

The configuration control and a defined change process for the procedures and descriptions of the site under evaluation are mandatory. The control process must include all procedures that have an impact on the evaluated production processes as well as on the site security measures.

The CM system provides :

- automated means to assist in determining that the correct configuration items are used in generating the TOE,
- automated measures such that only authorised changes are made to the configuration items.

6.1.3 CM scope ALC_CMS.5

The scope of the configuration management for a site certification process is limited to the documentation relevant for the SAR for the claimed life-cycle SAR and the configuration items handled at the site.

6.1.4 Development security : ALC_DVS.2

The CC assurance components of family ALC_DVS refer to (i) the “development environment”, (ii) to the “TOE” or “TOE design and implementation”. The component ALC_DVS.2 “Sufficiency of security measures” requires additional evidence for the suitability of the security measures.

The TOE Manufacturer must ensure that the development and production of the TOE is secure so that no information is unintentionally made available for the operational phase of the TOE. The confidentiality and integrity of design information, test data, configuration data must be guaranteed, access to any kind of samples (customer specific samples or open samples) development tools and other material must be restricted to authorised persons only, scrap must be controlled and destroyed.

Based on these requirements, the physical and logical security of the site are in the focus of the evaluation. Beside the pure implementation of the security measures also the control and the maintenance of the security measures must be considered.

6.1.5 Life-cycle definition : ALC_LCD.1

The site is not equal to the entire development environment. Therefore, the ALC_LCD criteria are interpreted in a way that only those life-cycle phases have to be evaluated which

are in the scope of the site. The PP [R6] provides a life-cycle description there specific life-cycles steps can be assigned to the tasks at site. This may comprise a change of the life-cycle state if e.g. testing or initialisation is performed at the site or not.
The PP [R6] does not include any refinements for ALC_LCD. For a site under evaluation the dependencies to other sites must be explained if they are not covered by the obvious deliverables.

6.2 Assurance dependencies

Table 6-1 SAR dependencies

Assurance family	Dependencies	Support of the Dependencies
ALC_CMC.4	ALC_CMS.1 ALC_DVS.1 ALC_LCD.1	Fulfilled.
ALC_CMS.5	No dependencies	N/A
ALC_DVS.2	No dependencies	N/A
ALC_LCD.1	No dependencies	N/A

7 Site Summary Specification

7.1 Preconditions required by the site

This section provides background information on the assumptions defined in section 3.4.

These assumptions can be seen as guidance for the client regarding the information and deliverables which are needed to allow the production under conditions described in this Site Security Target.

For the setup of the production process, the relevant specifications and product information is required by JAWS. In general, the release process can only be finished, if the required information is provided by the client. All these data/information has to be provided to JAWS in encrypted format. All finished products are tested. The tests are configured based on the provided specifications. The test environment allows functional tests to verify the operation after completion of the production. This cover the assumptions **A.Product-Specification**.

The assumptions **A.Product-Integrity** and **A.Item-Identification** are covered by the following rules.

JAWS has procedures in place to protect and maintain classified products and properties of his clients. The protection is based on the classification agreed with the client or printed on the received item or document. Any received configuration items are appropriately labelled and identified by the client.

For all classified items appropriate destruction procedures are in place. The rejected, defect or obsolete security products are destructed at the site if there is no request to return to the client.

The assumptions **A.Product-Delivery** and **A.Shipment** are covered by the following rules.

JAWS is not responsibility for any transport outside their premises. Any transport from or to the site is under the control of the clients of JAWS.

The client is responsible for delivering the products to JAWS.

The shipping after the production is supported by labelling and packaging the finished products. The products are labelled and packed as specified by the client. This includes the address of the receiver. The forwarder is selected by the client. JAWS verifies the identity of the car and the driver based on the provided pre-announcement by the client before any charge is handed over. The pre-announcement is performed for each transport. The tracing and further control and security measures for that transport is under the responsibility of the client.

7.2 Services of the site

JAWS provides assembled and embedded inlays, e-covers, datapage and similar products that are functionally tested.

The finished products are packed as specified by the client. The packing includes also the labelling for the shipment. Delivery addresses and packing requirements are provided by the client. The client can deliver special tapes or labels that allow a detection if the packet is opened during the shipment.

JAWS provides a service to destroy defect modules, inlays (and any finished or semi-finished products) to such an extent that no misuse of the defect devices is possible.

7.3 Security Assurance Requirements Rationale

The SAR Rationale does not explicitly address the developer action elements defined in [R2] because they are implicitly included in the content elements. This comprises the provision of the documentation to support the evaluation and the preparation for the site visit. This includes the requirement that the procedures are applied as written and explained in the documentation.

7.3.1 ALC_CMC.4

ALC_CMC.4.1C: The CM documentation shall show that a process is in place to ensure an appropriate and consistent labeling (refined for Site Certification).

ALC_CMC.4.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.4.3C: The CM system shall uniquely identify all configuration items.

ALC_CMC.4.4C: The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

ALC_CMC.4.5C: The CM system shall support the production of the TOE by automated means.

ALC_CMC.4.6C: The CM documentation shall include a CM plan.

ALC_CMC.4.7C: The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.4.8C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.4.9C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.4.10C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

The security assurance requirements of the assurance class "CM capabilities" listed above are suitable to support the production of complex products due to the formalized acceptance process and the automated support. The identification of all configuration items supports an automated and industrialised production process. The requirement for authorised changes support the integrity and confidentiality required for the products. Therefore this assurance level meets the requirements for the configuration management.

7.3.2 ALC_CMS.5

ALC_CMS.5.1C: The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; security flaw reports and resolution status and production tool related documentation (refined for Site Certification).

ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.

ALC_CMS.5.3C: For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

The security assurance requirements of the assurance class "CM scope" listed above support the control of the production and test environment. This includes product related documentation, the documentation for the configuration management, production tool documentation and the site security measures. Since the site certification process focuses on the processes based on the absence of a concrete TOE these assurance requirements are considered to be suitable.

7.3.3 ALC_DVS.2

ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

The security assurance requirements of the assurance class "Development security" listed above are required since a high attack potential is assumed for potential attackers. The configuration items and information handled at the site during development, production, testing and assembly of the product can be used by potential attackers for the development of attacks.

7.3.4 ALC_LCD.1

The security assurance requirements of the assurance class " Life-cycle definition" at the assurance level ALC_LCD.1 is suitable to support the controlled development and production process. This includes the documentation of these processes and the procedures for the configuration management. One site provides only a limited support of the described life-cycle for the development and production of Security ICs. However the assurance requirements are considered to be suitable to support the application of the site evaluation results for the evaluation of an intended TOE.

7.4 Assurance Measure Rationale

Table 7-1 SAR Rationale

	O.Physical-Access	O.Security-Control	O.Alarm-Response	O.Internal-Monitor	O.Maintain-Security	O.Logical-Access	O.Logical-Operation	O.Config-Items	O.Config-Control	O.Config-Process	O.Acceptance-Test	O.Staff-Engagement	O.Zero-Balance	O.Reception-Control	O.Shipping-Support	O.Control-Scrap	O.Transfer-Data
ALC_CMC.4.1C								X						X			
ALC_CMC.4.2C								X									
ALC_CMC.4.3C								X		X							
ALC_CMC.4.4C										X							
ALC_CMC.4.5C											X		X				
ALC_CMC.4.6C										X							
ALC_CMC.4.7C										X							
ALC_CMC.4.8C									X								
ALC_CMC.4.9C									X	X			X				
ALC_CMC.4.10C											X						
ALC_CMS.5.1C								X		X					X		
ALC_CMS.5.2C								X		X							
ALC_CMS.5.3C														X			
ALC_DVS.2.1C	X	X	X			X	X					X	X			X	
ALC_DVS.2.2C				X	X												X
ALC_LCD.1.1C									X	X							
ALC_LCD.1.2C											X		X				

O.Physical-Access

ALC_DVS.2.1C requires that the developer shall describe all physical security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this Security Assurance Requirement contributes to meet the objective.

O.Security-Control

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation including the initialization in its development and production environment. Thereby this Security Assurance Requirement contributes to meet the objective.

O.Alarm-Response

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation including the initialization in its development and production environment. Thereby this Security Assurance Requirement contributes to meet the objective.

O.Internal-Monitor

ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby this Security Assurance Requirement contributes to meet the objective.

O.Maintain-Security

ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby this Security Assurance Requirement contributes to meet the objective.

O.Logical-Access

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation including the initialization in its development and production environment. Thereby this Security Assurance Requirement contributes to meet the objective.

O.Logical-Operation

ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby this Security Assurance Requirement contributes to meet the objective.

O.Config-Items

ALC_CMC.4.1C requires a documented process ensuring an appropriate and consistent labelling of the products. A method used to uniquely identify the configuration items is required by **ALC_CMC.4.2C**. In addition **ALC_CMC.4.3C** requires that the CM system uniquely identifies all configuration items. The configuration list required by **ALC_CMS.5.1C** shall include the evaluation evidence for the fulfillment of the SARs, production tools and related information. **ALC_CMS.5.2C** addresses the same requirement as **ALC_CMC.4.3C**. Thereby these Security Assurance Requirements contribute to meet the objective.

O.Config-Control

ALC_CMC.4.8C requires the description of the procedures used to accept modified or newly created configuration items as part of the TOE. **ALC_CMC.4.9C** requests evidence to demonstrate that all configuration items are being maintained under the CM system. **ALC_LCD.1.1C** that the life-cycle definition documentation describes the model used to develop and maintain the products. Thereby these Security Assurance Requirements contribute to meet the objective.

O.Config-Process

The provision of automated measures such that only authorised changes are made to the configuration items as required by **ALC_CMC.4.4C**. **ALC_CMC.4.6C** requires that the CM documentation includes a CM plan. **ALC_CMC.4.7C** requires that the CM plan describe how the CM system is used for the development of the TOE. **ALC_CMC.4.9C** requests evidence to demonstrate that all configuration items are being maintained under the CM system. The configuration list required by **ALC_CMS.5.1C** shall include the evaluation evidence for the fulfillment of the SARs, production tools and related information. **ALC_CMS.5.2C** addresses the same requirement as **ALC_CMC.4.3C**. **ALC_LCD.1.1C** that the life-cycle definition documentation describes the model used to develop and maintain the products. Thereby these Security Assurance Requirements contribute to meet the objective.

O.Acceptance-Test

The testing of the products is considered as automated procedure as required by **ALC_CMC.4.5C**. The operation of the CM system in accordance with the CM plan is required by **ALC_CMC.4.10C**. **ALC_LCD.1.2C** requires control over the development and

maintenance of the TOE. Thereby these Security Assurance Requirements contribute to meet the objective.

O.Staff-Engagement

ALC_DVS.2.1C requires the description of personnel security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this Security Assurance Requirement contributes to meet the objective.

O.Zero-Balance

ALC_CMC.4.5C requires that the CM system supports the production of the TOE by automated means. **ALC_CMC.4.9C** requires evidence that all configuration items are being maintained under the CM system. **ALC_DVS.2.1C** requires security measures that are necessary to protect the confidentiality and integrity of the TOE. **ALC_LCD.1.2C** requires control over the development and maintenance of the TOE. Thereby these Security Assurance Requirements contribute to meet the objective.

O.Reception-Control

ALC_CMC.4.1C: The CM documentation shall show that a process is in place to ensure an appropriate and consistent labeling. **ALC_CMS.5.3C**: For each configuration item, the configuration list shall indicate the developer/subcontractor of the item. Thereby these Security Assurance Requirements contribute to meet the objective.

O.Shipping-Support

The configuration list required by **ALC_CMS.5.1C** shall include the evaluation evidence for the fulfillment of the SARs, production tools and related information including address of the receiver. Thereby this Security Assurance Requirement contributes to meet the objective.

O.Control-Scrap

ALC_DVS.2.1C requires that physical, procedural, personnel, and other security measures that are implemented to protect the confidentiality and integrity of the TOE design and implementation. Thereby this Security Assurance Requirement contributes to meet the objective.

O.Transfer-Data

ALC_DVS.2.2C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this Security Assurance Requirement contributes to meet the objective.

7.5 Objectives Rationale

Table 7-2 Objectives Rationale

	O.Physical-Access	O.Security-Control	O.Alarm-Response	O.Internal-Monitor	O.Maintain-Security	O.Logical-Access	O.Logical-Operation	O.Config-Items	O.Config-Control	O.Config-Process	O.Acceptance-Test	O.Staff-Engagement	O.Zero-Balance	O.Reception-Control	O.Shipping-Support	O.Control-Scrap	O.Transfer-Data
Security Policy	X	X	X	X	X	X	X					X	X				X
Quality Manual								X	X	X	X			X	X	X	X
Configuration Management Plan								X	X								
Production Process													X				X
Work contract / agreement												X					
NDA for employees												X					
Maintenance contracts		X		X	X												

The objective **O.Physical-Access** is covered by the **security policy**. This policy described that :

Access to JAWS buildings is controlled (level 0). The access control is enforced by a physical measures, and associated surveillance by cameras and alarm sensors.

Within the buildings, areas are separated:

- Security level 1 for administrative and financial purpose,
- Security level 2 for production purpose,
- Security level 3 for security vault.

The access to production area (Security level 2) is controlled by a physical measures (as tollgate), body check by security guards, and associated surveillance by cameras and alarm sensors.

Due to 24 hours production during the week, during weekend and public holidays a clear assignment of responsibilities, a short response time on any alarm or security relevant event is ensured.

During off-time a guard ensures a short response time.

The structural measures of the different levels provide an increasing resistance against overcoming the protection. Security policy [R8] described the level of resistance.

Described security measures limit the access to the production area and thereby support the observability.

The objective **O.Security-Control** is covered by the **Maintenance contracts** and **security policy** :

The observation and alarm system comprises CCTV that covers the surrounding of the whole building, motion sensors and opening sensors for doors and windows. The CCTV system allows to control the area where an alarm occurred.

CCTV are 24 hours monitored.

The access control system can only be configured by the security manager. Access to the logging of the access control system is also controlled.

The objective **O.Alarm-Response** is covered by the **security policy**. This policy described that :

the alarms are signalled to the security control room present on site at the site.

CCTV are 24 hours monitored by the security control room. The alarm system comprises also direct line to signal any kind of robbery to the nearest police station. This is done by the guard in the security control room.

The objective **O.Internal-Monitor** is covered by the **security policy** and **Maintenance contracts**.

Internal audits are regularly performed to control the security awareness of the employees. Furthermore, all employees have a training once a year to guarantee that each employee is aware of the security rules.

Security management meeting to be performed regularly: all security are discussed and considered for the actual assessment of the remaining risks. The internal monitoring covers also the control of the maintenance and verification procedures for the security measures.

The objective **O.Maintain-Security** is covered by the **security policy** and **Maintenance contracts** :

The alarm system, the video control system, motions sensors and the access control system require regular functional checks and maintenance to ensure the correct operation. According to JAWS security policy [R8], these checks are applied according to the recommendations of the manufacturer or installer and is described in the maintenance contracts (or warranty). Alerts are traced to allow the distinction between false alarms and attack attempts.

The logging of the access control system is checked and abnormal logs are verified to detect irregular behaviour of employees or manipulation attempts.

The objective **O.Logical-Access** is covered by the **security policy** :

The IT network is split into different segments for different purpose. The protection of the network segments is applied based on the classification of the operated data. The separation is enforced by network elements like a firewall and by physical separation where required. User accounts are managed to limit the access rights to the required level

The objective **O.Logical-Operation** is covered by the **security policy** :

Virus protection, patch management for operating systems and applications as well as the control of received data shall ensure the operation of the systems and the defence against malfunctions. Furthermore, backup and appropriate storage of the backup are applied to prevent the loss of data.

The objective **O.Config-Items** is covered by the **quality manual** and **Configuration Management Plan** :

Each production, including the internal associated procedures and guidance, has an unqiue identification number associated to the client.

The objective **O.Config-Control** is covered by the **quality manual** and **Configuration Management Plan**:

The configuration management covers the release and management of production. All productions get an internal product identification that is maintained in a data base. In addition, the development and change of internal procedures is released according to the quality process.

The objective **O.Config-Process** is covered by the **quality manual** :

The configuration management comprises automated measures to ensure the correct set up of a production and to ensure constant results within the production appropriate

procedures are defined. Further on a team of employees responsible for the product handling and the production is defined to plan, organise and control the production process. This includes also the change of production steps.

The objective **O.Acceptance-Test** is covered by the **quality manual** :

Each finished product is tested using a standardised functionality. Furthermore, optical inspections are performed to ensure the fulfillment of the form factors and the physical requirements of the finish products.

The objective **O.Staff-Engagement** is covered by the **Security policy**, **NDA for employees** and **work contract** :

The work contract specifies that employees will work on confidential information.

A non disclosure agreement signed by the employees provides a legal liability for the signing employee to protect sensitive information against disclosure.

Further on all employees get training that shall ensure the required security awareness and the knowledge of the processes.

The objective **O.Zero-Balance** is covered by the **Security policy** and **production process** The manual tracing of the defect devices together with the automated tracing of the functional devices ensure that no security devices are lost during the production and that all defect devices are destroyed by the secure destruction process of JAWS.

The objective **O.Reception-Control** is covered by the **quality manual** :

The incoming inspection ensures the correct identification of security product and the verification of the security measure applied to control the integrity during shipment. The process is the starting point of the internal tracing. If an assignment cannot be applied the product is separated until the identification is clarified.

The objective **O.Shipping-Support** is covered by the **quality manual** :

The transport is controlled by the client. The shipping process is initiated based on the request of JAWS. The security products are packed as requested by the client and handed over to the forwarder after verification of the forwarder. The finished products are properly labelled according to the client requirements.

The objective **O.Control-Scrap** is covered by the **security policy, quality manual** and **production process** :

All products comprising a security chip which cannot be delivered as functional product or returned to the client as scrap are locally destroyed to remain only small pieces that do not support an attacker.

The objective **O.Transfer-Data** is covered by the **quality manual** :

Classified electronic data and documents are protected with cryptographic algorithms during transfer. The keys are assigned to authorised employees only.

8 References

8.1 Acronyms

CC	Common Criteria
N/A	Not Applicable
PP	Protection Profile
QSCD	Qualified Signature Creation Device
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSB	Supplier Specification Booklet
SST	Site Security Target
TOE	Target of Evaluation

8.2 Glossary

NONE

8.3 Technical References

[R1] ***CCRA**: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, April 2017, version 3.1 rev.5, CCMB-2017-04-001*

[R2] ***CCRA**: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, April 2017, version 3.1 rev 5, CCMB-2017-04-003*

[R3] ***CCRA**: Common Methodology for Information Technology Security Evaluation (CEM), Part 2: Evaluation Methodology; Version 3.1, Revision 5, April 2017*

[R4] ***CCRA**: Supporting Document, Site Certification, October 2007, Version 1.0, Revision 1, CCDB-2007-11-001*

[R5] ***BSI**: Guidance for Site Certification, V1.1, 04/12/2013*

[R6] ***BSI :** Security IC Platform Protection Profile with Augmentation Packages e, Version 1.0, 13.01.2014, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014*

[R7] ***JAWS**: Quality Manual: "Quality, Environment and Occupational Health-Safety Manual", No.: MP-01, Rev.04, Date: 27 May 2019*

[R8] ***JAWS**: Security Policy: "Security Management System Manual", No.: MP-02, Rev.02, Date: 21 Jan. 2020*

[R9] ***JAWS**: Production Operational Practices Procedure; No.: PK-PD-004, Rev.11, Date: 7 June 2018*

[R10] ***JAWS**: Configuration Management Plan; No.: PK-SC-003, Rev.00, Date: 19 August 2020*

END OF DOCUMENT