TIEMPO S.A.S., 110 Rue Blaise Pascal,
Bâtiment Viseo - Inovallée
38330 Montbonnot St-Martin
France

SST_Lite_Tiempo_Development_Site_Montbonnot

Montbonnot-Saint-Martin Site Certification

Security Level 1: Public

PRSC-L1-1023-V2.1

Revision: 2.1

Date: 11/08/2023

TIEMPO S.A.S. Public

TIEMPO S.A.S. - Confidential Information
This document cannot be copied or transmitted without prior written authorization by TIEMPO S.A.S.

Tiempo Trademarks and Copyright Information

Tiempo S.A.S. is disclosing this documentation to you solely for use in the development of designs to operate with Tiempo S.A.S. IP products. Forwarding or copying of this document, in whole or part, or disclosure of its contents, to other than the authorized recipient, without prior authorization of Tiempo S.A.S., is strictly prohibited.

TIEMPO S.A.S. MAKES NO WARRANTY OF ANY KIND, WHETHER EXPRESS, OR IMPLIED, REGARDING THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

This document contains confidential and proprietary information that is the property of Tiempo S.A.S.

Role	Initials	Position
Redactor	J.KE.	Software developer
Proofreader	A.BO.	Hardware designer
Validator	M.RE.	CTO

TIEMPO S.A.S. Public

Contents

TIEMPO S.A.S. Public

TIEMPO S.A.S. Public

Figures and Tables

TIEMPO S.A.S. Public

1 Overview

1.1 Version

Version	Date	Author	Description
1.0	13/09/2021	A.BO.	First release (Site Certification 2021)
1.1	05/10/2021	A.BO.	Updated Version – Additional precisions for configuration management (Site Certification 2021)
2.0	31/05/2023	J.KE.	Adding ALC_FLR aspects (Site Certification 2023)
2.1	11/08/2023	J. KE	Adding FLR user guide reference in table 8-2, and typo correction in paragraph 58 (ALC_FLR.1 -> ALC_FLR.2)

Table 1-1 - Document Version

1.2 Purpose

1 This document was prepared to submit the site certification of the TIEMPO's site of Montbonnot-Saint-Martin.

1.3 Scope

2 This document describes the security features of TIEMPO's Montbonnot-Saint-Martin site.

1.4 Reference

[1] Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, BSI-CC-PP-0084-2014, Eurosmart, 2014.
[2] Site Certification, Supporting Document Guidance, ref. CCDB-2007-11-001, Version 1.0, Revision 1, October 2007.
[3] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; April 2017, Version 3.1, Revision 5, CCMB-2017-04-001.
[4] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; April 2017, Version 3.1, Revision 5, CCMB-2017-04-002.
[5] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; April 2017, Version 3.1, Revision 5, CCMB-2017-04-003.
[6] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; April 2017, Version 3.1, Revision 5, CCMB-2017-04-004.
[7] Joint Interpretation Library, Minimum Site Security Requirements, Version 3.0, February 2020.
[8] Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile, Version 1.5, BSI-CC-PP-0117-2022, Eurosmart, 2022.
[9] Site Security Target Template, Version 1.0, published by Eurosmart, 2009-06-21.
[10] Tiempo, ALC_CM – Configuration Management, Montbonnot-Saint-Martin Site, Revision

TIEMPO S.A.S. Public

1.6, 3 April 2023.
[11] Tiempo, ALC – Life Cycle Definition and Delivery, Montbonnot-Saint-Martin Site, Revision 1.0, 28 September 2020.
[12] Tiempo, ALC_DVS – Development Security, Montbonnot-Saint-Martin Site, Revision 1.0, 20 September 2020.
[13] Tiempo, ALC_TAT – Tools and Techniques, Montbonnot-Saint-Martin Site, Revision 1.1, 4 May 2023.
[14] DIN 66399 Office machines, Destruction of data carriers, Parts 1 to 3, Edition 2012-10.
[15] Tiempo, Questionnaire pour audit de site, 16 May 2023.
[16] Tiempo, ALC_FLR - Flaw Remediation procedures Montbonnot-Saint-Martin Site, Revision 1.2, 24 April 2023.
[17] Tiempo, ALC_FLR - Flaw Remediation User Guide Montbonnot-Saint-Martin Site, Revision 1.0, 07 August 2023.

1.5 Glossary

Word	Meaning
Requirement	This refers to a specification that project shall fulfill.
Functional requirements	These requirements refer to high level product requirement that are discussed and analyzed between marketing and R&D and are possibly visible to customer.

Table 1-2 - Glossary

1.6 List of Abbreviations

Abbreviation	Meaning
AST	CC Assurance Class for Site Security Target Evaluation
CC	Common Criteria
CCDB	Common Criteria Development Board
EAL	Evaluation Assurance Level
HW	Hardware
IC	Integrated Circuit
OSP	Organizational Security Policy
SSS	Site Summary Specification
SST	Site Security Target
TOE	Target of Evaluation

Table 1-3 - List of abbreviations

TIEMPO S.A.S. Public

2 Introduction

3 This document describes the security target of the Montbonnot-Saint-Martin development site of Tiempo Secure.

4 Note that in the document we use IC for short to refer to both the development of whole integrated circuits in the context described in [1] as well as the development of secure subsystems which are integrated as hard macros in multi-purpose SoC architectures in the same vein as the applications described in [8].

2.1 SST reference

Title	SST_Lite_Tiempo_Development_Site_Montbonnot
Reference	Montbonnot_SST_Lite_V2.1
Version	V2.1
Company	Tiempo Secure SAS
Site location	Inovallée - Immeuble Viséo, 110 rue Blaise Pascal, 38330 Montbonnot-Saint-Martin, France
Product type	Security ICs and Security IC Dedicated Software
EAL-Level	EAL6

Table 2-1 - SST reference

2.2 Site Description

2.2.1 Physical Scope

5 Montbonnot-Saint-Martin site is located at 110 rue Blaise Pascal, 38330 Montbonnot-Saint-Martin.

6 The site is part of the “Viséo” complex and occupies one of its four buildings. Indeed, the site takes one aisle of the first floor of Building D.

Figure 2-1 Tiempo Montbonnot-Saint-Martin site

TIEMPO S.A.S. Public

7 The Montbonnot-Saint-Martin site is Tiempo's main office and its corporate headquarters.

8 Tiempo's development processes take place in the Montbonnot-Saint-Martin site. This includes Hardware Design, Software development, Developmental Testing and Verification and Quality Control.

2.2.2 Logical Scope

9 In the context of the protection profiles PP-0084 [1] and PP-00117 [8], the typical life cycle for Smart card products comprises the following phases:

- Security IC Embedded Software Development (Phase 1)
- IC Development (Phase 2)
- IC Manufacturing and Testing (Phase 3)
- IC Packaging (Phase 4)
- Security IC Product Finishing Process (Phase 5)
- Security IC Personalization (Phase 6)
- Security IC End-usage (Phase 7)

10 The main activities of the Montbonnot-Saint-Martin site are the following (phase 2):

- Security IC Design, test and Validation
- IC Dedicated Software development, testing and validating
- Secure Circuits qualification routines development
- Secure Circuits characterization routines development
- Secure Circuits validation routines development
- Secure Circuits test, validation, characterization and qualification

TIEMPO S.A.S. Public

3 Conformance Claim

11 This Security Target has been built with the Common Criteria for Information Technology Security Evaluation; Version 3.1:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; April 2017, Version 3.1, Revision 5, CCMB-2017-04-001 [3].
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; April 2017, Version 3.1, Revision 5, CCMB-2017-04-003 [5].

12 This SST is Common Criteria Part 3 [5] conformant.

13 For the evaluation, the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; April 2017, Version 3.1, Revision 5, CCMB-2017-04-004 [6].
- Supporting Document, Site Certification, October 2007, Version 1.0, Revision 1, CCDB-2007-11-001 [2].
- Minimum Site Security Requirement V3.0 February 2020 [7].

14 There are no extended components required for this SST.

15 The evaluation of the site comprises the following assurance components:

- ALC_CMC.5
- ALC_CMS.5
- ALC_DVS.2
- ALC_FLR.2
- ALC_LCD.1
- ALC_TAT.3
- ALC_DEL.1 (The generic activities of the site are not directly related to the shipping of Security IC Products. Therefore, this site does not claim conformance to ALC_DEL.)

16 The assurance level chosen for the SST is compliant to the Security IC Platform Protection Profile and is therefore suitable for the evaluation of software and Hardware design for Security ICs.

17 The chosen assurance components are derived from the assurance level EAL6 of the assurance class "Life-cycle Support". For the assessment of the security measures attackers with a high attack potential are assumed. Therefore, this site supports potentially augmented product evaluations up to EAL6.

TIEMPO S.A.S. Public

4 Security Problem Definition

18 The Security Problem Definition comprises security problems derived from threats against the assets handled by the site.

4.1 Assets

19 This section broadly describes the assets handled at the site:

- TOE Development information: This includes the relevant information for the knowledge of the TOE (functional specifications, design documentation, guidance documents, source codes, IC and embedded software representations, etc.). This information is available at the site in the form of electronic scripts and documents. The integrity and the confidentiality of these resources must be protected.
- TOE Development tools: This includes the software tools that are used for the development of the TOE such as source code compilers, RTL synthesis and testing tools, Place & Route tools, etc. Also, this includes the tools that are used for configuration management as well as IT infrastructure hardware. The integrity of these tools must be protected.
- TOE physical samples: This includes the TOE secure wafers, modules, chips, packages as well as printed circuit boards (PCB) used for testing and qualification procedures. The integrity and the confidentiality of these resources must be protected.
- Testing equipment: This includes the hardware equipment (Oscilloscope, Interface adapters, smartcard readers, etc.) used for the testing and qualification procedures. The integrity and the availability of these devices must be ensured.
- Security devices: This includes the protection devices and mechanisms available in the site such as HSMs, safe boxes, etc. The integrity and the availability of these devices must be ensured.
- Security information: This includes the information regarding the systems and security mechanisms configuration such as protection devices configuration, cryptographic keys, password, etc. The integrity and the confidentiality of these resources must be protected.

4.2 Threats

Identifier	Description	Affected Assets
T.Smart-Theft	An attacker tries to access sensitive areas of the site for manipulation or theft of assets. The attacker is assumed to have sufficient time to investigate the site outside the controlled boundary. For the attack, the use of standard equipment for burglary is considered. Potential attackers could be either existing employees of the company or external attackers whom are not existing	- TOE Development information - TOE Development tools - TOE physical samples - Testing equipment - Security devices - Security information

TIEMPO S.A.S. Public

Identifier	Description	Affected Assets
	employees.	
T.Rugged-Theft	An attacker with specialized equipment for burglary, who may be paid to perform the attack, tries to access sensitive areas and manipulate or steal assets	- TOE Development information - TOE Development tools - TOE physical samples - Testing equipment - Security devices - Security information
T.Computer-Net	A possibly paid hacker with substantial expertise using standard equipment attempts to remotely access sensitive network segments to get access to the data with the intention to violate confidentiality and possibly integrity or development computers with the intention to modify the development process.	- TOE Development information - Security information
T.Accident-Change	Employees or subcontractors 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 or maintenance tasks within the development, production or test area. 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. 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.	- TOE Development information - TOE Development tools - TOE physical samples - Testing equipment - Security devices - Security information
T.Unauthorized-Staff	Employees or subcontractors not authorized to get access to development tools and resources used for Security IC development may get access to these resources or affect development systems or configuration systems, so that the confidentiality and/or the	- TOE Development information - TOE Development tools - TOE physical samples - Testing equipment - Security devices - Security information

TIEMPO S.A.S. Public

Identifier	Description	Affected Assets
	integrity of the design is violated. This can apply to any development step and any configuration item of the final product as well as to the final product or its configuration.	
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.	- TOE Development information - TOE Development tools - TOE physical samples - Testing equipment - Security devices - Security information
T.Attack-Transport	An attacker might try to get data, specifications or products during the internal shipment. The target is to compromise confidential information or violate the integrity of the products during the stated internal or external shipment process to allow a modification, cloning or the retrieval of confidential information at later life cycle states. Confidential information comprises design information, test documentation and test data as far as classified as sensitive.	- TOE Development information - TOE physical samples - Security information

Table 4-1 - Threats

4.3 Organizational security policies

20 The following policies are introduced by the requirements of the life cycle assurance components (ALC) for the assurance level EAL6. 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).

Identifier	Description
P.Config-Items	The configuration management system shall be able to uniquely identify configuration items. This includes the unique identification of items that are developed or used at the site as well as the received and transferred and/or provided items. The configuration management relies completely on the naming and identification of the received configuration items. Each item is assigned to an internal unique identification once it is created, generated or developed at the site or received from an external partner. The configuration management system manages the TOE development information, the TOE physical samples, Security

TIEMPO S.A.S. Public

Identifier	Description
	information as well as the utilized equipment and tools of the site.
P.Config-Control	Well-specified procedure shall be defined to guide, control and monitor the creation of new configuration items as well as their subsequent modification. Indeed, automated configuration management systems shall enforce access restrictions so as to disallow unauthorized modification of the configuration items. Moreover, these systems shall implement interactive acceptance procedures which control and monitor item creation and changes. The configuration management system shall track the following information for each of the managed items: • Identification of the item • Properties of the item when created/received at the site • Classification of the items (Type, Security level, etc.) • Employee(s) responsible for the internal management of the item and its destruction once it becomes obsolete or defective • Configuration change history of the processed item • Current location of the item (within the site, shipped to an external partner, etc).
P.Config-Process	The services and/or processes provided by the site are controlled in the configuration management plan. This comprises incoming items and tools used for development and testing, the management of flaws and optimizations of the process flow as well as the documentation that describes the services and/or processes provided by the site. The documentation that describes the process descriptions and the security measures of the site is under version control. Measures are in place to ensure that the evaluated status is ensured. In most cases tools are used to support the processes at the site.
P.Flaw-Remediation	The site oversees security flaw remediation. The procedures in place within the site must show how flaw remediation is managed giving assurance on the following topics: • Acceptance and acting upon all reports of security flaws and requests for corrections to those flaws. • Flaw remediation guidance to address the TOE customers.
P.Reception-Control	The inspection of incoming items done at the site ensures that the received configuration items comply with the properties managed by the configuration management system. 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 are available to process the configuration items.
P. Product-Transport	Technical and organizational measures shall ensure the correct labelling of the product. A controlled internal shipment and/or the external delivery shall be applied. The transport supports traceability up to the acceptor. If applicable or required, this policy shall include measures for packing if required to protect the product during transport.

TIEMPO S.A.S. Public

Identifier	Description
P.Transfer-Data	Any data in electronic form (e.g. design specifications, source codes, test program specifications, release information etc.) that is classified as sensitive or higher security level shall be encrypted before being transferred to ensure confidentiality of the data. In addition, measures are used to control the integrity of the data after the transfer.

Table 4-2 - Organizational security policies

4.4 Assumptions

21 Tiempo Secure is operating in a production flow and therefore must rely on preconditions provided by previous sites which intervene in the TOE life cycle. This is reflected by the following assumptions:

Assumption	Description
A.Item-Identification	Each configuration item received by the site is appropriately labelled to ensure the identification of the configuration item.
A.Product-Manufacturing	The IC manufacturing is not performed in the Montbonnot-Saint-Martin site. A graphical database representation of the IC is sent from the site to the manufacturing site in an encrypted, secure communication. The manufacturing site is responsible for ensuring the security of the IC during this phase.
A.Product-Testing	Some IC testing and qualification procedures are not performed in the Montbonnot-Saint-Martin site. A shipment compliant with the predefined security procedures enables sending the relevant IC samples (chips, PCB boards, etc.) as well as the relevant specification documents to the testing site. The testing site is responsible for the security of the IC during this phase.
A.Multisite-Development	In case TOE development is performed together with other development sites (i.e. 'multisite development'), all other sites have to cover all CC assurance components as defined in chapter 3 (or higher). In addition, the site has to be resistant to attackers with high attack potential (i.e. AVA_VAN.5). A trusted communication channel must exist to the remote sites.

Table 4-3 - Assumptions

22 These assumptions are outside the sphere of influence of Tiempo. They are needed to account for the phases of the TOE life-cycle which do not occur within the site.

TIEMPO S.A.S. Public

5 Security Objectives

23 The Security Objectives are related to physical, technical, and organizational security measures, the configuration management as well as the internal and/or the external delivery.

Objective	Description
O.Physical-Access	The combination of physical partitioning between the different access control levels together with technical and organizational security measures shall allow a sufficient separation of employees in order to enforce the “need to know” principle. The access control shall support the limitation for the access to these zones including the identification and rejection of unauthorized people. The access control measures shall ensure that only registered employees can access restricted areas. Assets shall be handled in restricted areas only.
O.Security-Control	Assigned personnel of the site shall operate the systems for access control. Outside of workhours, surveillance and response to alarms shall be outsourced to a 3rd party security company. Technical security measures like motion sensors and similar kind of sensors shall be used to support the enforcement of the access control. Tiempo personnel shall be responsible for registering and ensuring escort of visitors, contractors and suppliers.
O.Alarm-Response	The technical and organizational security measures shall ensure that an alarm is generated before an unauthorized person gets access to any asset. Additional security measures shall be implemented to further impede the unauthorized access to the asset while the alarm is being processed. The reaction time of the employees and/or guards shall be swift enough to prevent a successful attack.
O.Internal-Monitor	The site shall perform regular security management meetings to review security incidences, to verify that maintenance measures are applied and to reconsider the assessment of risks and security measures. Furthermore, an internal audit is performed every year to control the application of the security measures.
O.Maintain-Security	Technical security measures shall be maintained regularly to ensure correct operation. The logging of sensitive systems shall be checked regularly. This comprises the access control system to ensure that only authorized 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.Network-separation	The development network of the site must consist of secured VLANs which are isolated from the outside world (internet). These secure VLAN networks shall only connect: (1) The development workstations provided by Tiempo; (2) Additional equipment (e.g. oscilloscope) approved by Tiempo.
O.Logical-Access	The site shall ensure authorized user access and prevent unauthorized user access to information systems or operating systems. The access must be based on the “need to know” principle.
O.Logical-Operation	The integrity of software and information systems shall be ensured. Systems and computers must be kept up to date (software updates, security patches, virus protection, spyware protection). A back up of

TIEMPO S.A.S. PUBLIC

Objective	Description
	sensitive data must be applied. Development computers enforce that every user authenticates using a password and has a unique user ID.
O.Config-Items	The site shall define a configuration management system that assigns a unique internal identification to the configuration item (source code, specification document, engineering sample…) and to each product. The system shall manage configuration.
O.Config-Control	The product configuration and the development data created within the site shall be released through a formal release. The site shall ensure the correct control of the changes and shall ensure the correct operation of the planned processes.
O.Config-Process	Development, testing and qualification endeavors and their corresponding documentation shall be formally structured in terms of tools, methodology and procedures.
O.Flaw-Remediation-Monitor	All security flaw discovered by development/production teams or must be monitored and managed through the configuration system. All security flaws raised by the TOE users are monitored in the flaw remediation tool and internally for development endeavors in the configuration system.
O.Flaw-Remediation-External	The flaw remediation tool allows customers to submit flaw reports and is used to communicate the status and the identified corrective actions to TOE users.
O.Zero-Balance	The site shall ensure that all security products are traced and counted on an object basis and tracked until they are either shipped or destroyed.
O.Reception-Control	Upon reception of a product, the site shall ensure an incoming inspection. The inspection shall cover the received quantity of products, the identification and the assignment of the product to a related internal production process.
O.Control-Scrap	The site shall define measures to destroy secure products, sensitive documentation, erase electronic media and destroy sensitive configuration items so that they do not support an attacker.
O.Staff-Engagement	The site shall ensure that employees are suitable for their roles and understand their responsibilities. All employees who have access to assets shall be checked regarding security concerns and must have to sign a non-disclosure agreement. Furthermore, all employees shall be trained and qualified for their job. All contractors and visitors must be escorted by a trained employee at all times.
O.Product-Transport	The site shall define the processes for the shipment of finished or unfinished secure products. This includes internal transfers (within the same or to different premises) and shipment to address defined by the customer.
O.Data-Transfer	Sensitive electronic configuration items (data or documents in electronic form) shall be protected with cryptographic algorithms to ensure confidentiality and integrity. The associated keys must be assigned to individuals to ensure that only authorized employees can extract the sensitive electronic configuration item. The keys must be exchanged based on secure measures.
O.Multisite-Development	The site provides measures for regular synchronization of development repositories between sites in case of multisite

TIEMPO S.A.S. Public

Objective	Description
	development. The site provides measures to merge versions of configuration items resulting from concurrent use on different sites between synchronization periods. Access control mechanisms applied to the configuration management system are also active during synchronization and merging. Access from other development sites to local development repositories is restricted and development information exchange goes through secure channels and is handled by assigned staff which reviews the information before introducing it to the local development repositories. Other development sites cannot access local single development repositories.

Table 5-1 - Security Objectives Description

5.1 Security Objectives Rationale

24 The SST includes a Security Objective Rationale with two parts. The first part includes the tracing which shows how the threats and OSPs are covered by the Security Objectives. The second part includes a justification that shows that all threats and OSPs are effectively addressed by the Security Objectives.

25 Note that the assumptions of the SST cannot be used to cover any threat or OSP of the site. They are seen as pre-conditions fulfilled either by the site providing the sensitive configuration items or by the site receiving the sensitive configuration items. Therefore, they do not contribute to the security of the site under evaluation.

26 The Table 5-2 describes the Security Objectives Rationale.

Threat and OSP	Security Objective	Rationale
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Maintain-Security O.Staff-Engagement O.Internal-Monitor O.Control-Scrap O.Multisite-Development	The physical protection, the detection of a potential unauthorized intrusion, as well as the swift response are provided by O.Physical-Access, supported by O.Security-Control, O.Alarm-Response. O.Maintain-Security ensures that these systems operate optimally. O.Staff-Engagement ensures that all employees are trained sufficiently for their roles. O.Internal-Monitor ensures the review of the effectiveness of these systems and the corresponding procedures. O.Control-Scrap ensures that scrap material cannot be utilized maliciously once it has reached end-of-life status. O.Multisite-Development ensures that staff from different development sites does not have direct access to the local development repositories. Together, these objectives will therefore counter T.Smart_Theft.
T.Rugged-Theft	O.Physical-Access O.Security-Control	The physical protection, the detection of a potential unauthorized intrusion, as well as the swift response

TIEMPO S.A.S. Public

Threat and OSP	Security Objective	Rationale
	O.Alarm-Response O.Maintain-Security O.Staff-Engagement O.Internal-Monitor O.Control-Scrap	are provided by O.Physical-Access, supported by O.Security-Control, O.Alarm-Response. O.Maintain-Security ensures that these systems operate optimally. O.Internal-Monitor ensures the review of the effectiveness of these systems and the corresponding procedures. O.Staff-Engagement ensures the employees are suitable for their roles. O.Control-Scrap ensures that scrap material cannot be utilized maliciously once it has reached end-of-life status. Together, these objectives will therefore counter T.Rugged_Theft.
T.Computer-Net	O.Physical-Access O.Network-separation O.Logical-Access O.Logical-Operation O.Internal-Monitor O.Maintain-Security O.Control-Scrap O.Staff-Engagement O.Multisite-Development	The physical protection, the detection of a potential unauthorized intrusion, as well as the swift response are provided by O.Physical-Access. These measures prevent a potential attacker from being able to access the internal network net from within the developing site. O.Network-separation guarantees that the internal development networks are not connected to anything that an attacker could use to set up a remote connection. The logical protection of data is provided by O.Logical-Access by securing the access of sensitive data. The configuration management and the integrity of the information systems are provided by O.Logical-Access and O.Logical-Operation. O.Maintain-Security ensures that these systems operate optimally. O.Internal-Monitor ensures the review of the effectiveness of these systems and the corresponding procedures. O.Control-Scrap ensures that scrap material cannot be utilized maliciously once it has reached end-of-life status. O.Staff-Engagement ensures that the staff is aware of its duties (signing NDAs, secure exchange of sensitive data etc.). O.Multisite-Development ensures that staff from different development sites does not have direct access to the local development repositories. Together, these objectives will therefore counter T.Computer-Net.
T.Accident-Change	O.Staff-Engagement O.Config-Control O.Config-Process O.Zero-Balance O.Multisite-	O.Staff-Engagement ensures that all employees are trained and aware of the relevant procedures which must be followed when handling secure products or data. O.Config-Process and O.Config-Control ensures

TIEMPO S.A.S. Public

Threat and OSP	Security Objective	Rationale
	Development	that the correct operations are performed and that changes are done by authorized employees only. O.Zero-Balance ensures the tracing of each product and prevent from an accidental mix of products. O.Multisite-Development ensures that staff from different development sites does not have direct access to the local development repositories. Together, these objectives will therefore counter T.Accident-Change.
T.Unauthorized-Staff	O.Physical-Access O.Security-Control O.Network-separation O.Alarm-Response O.Staff-Engagement O.Logical-Access O.Logical-Operation O.Config-Control O.Zero-Balance O.Control-Scrap O.Internal-Monitor O.Maintain-Security O.Multisite-Development	O.Physical-Access and O.Network-separation ensures the access to sensitive information is restricted to authorized employees only and supported by O.Security-Control, ensures that the subcontractors who need the access to restricted area are always escorted by an authorized employee. O.Alarm-Response supports O.Physical-Access and O.Security-Control by ensuring that a response will be given to the alarm systems and that this response is quick enough to prevent access to the assets. O.Maintain-Security ensures that these systems operate optimally. O.Staff-Engagement ensures that hired people and subcontractors are trustworthy and that employees and subcontractors are aware of their roles and of the security rules. O.Logical-Access ensures the access to sensitive data to authorized employees only. O.Logical-Operation ensures that every employee authenticates using a password and has a unique user ID. O.Config-Control ensures that changes are done by authorized persons only. O.Zero-Balance ensures the detection of any stolen product. O.Control-Scrap ensures that scrap material cannot be utilized maliciously once it has reached end-of-life status. O.Internal-Monitor ensures the review of the effectiveness of these systems and the corresponding procedures. O.Multisite-Development ensures that staff from different development sites does not have direct access to the local development repositories. Together, these objectives will therefore counter T. Unauthorized-Staff.
T.Staff-Collusion	O.Physical-Access O.Network-separation O.Security-Control	O.Physical-Access, O.Network-separation and O.Security-Control ensures the need to know principals are applied to restrict access. O.Alarm-Response supports O.Physical-Access,

TIEMPO S.A.S. PUBLIC

Threat and OSP	Security Objective	Rationale
	O.Alarm-Response O.Staff-Engagement O.Logical-Access O.Config-Control O.Zero-Balance O.Control-Scrap O.Internal-Monitor O.Maintain-Security O.Multisite-Development	O.Network-separation and O.Security-Control by ensuring that a response will be given to the alarm systems and intrusion flagging security controls and that this response is quick enough to prevent access to the assets. O.Staff-Engagement ensures that hired people are trustworthy and are trained. O.Config-Control ensures that changes are done by authorized persons only and providing tracing of the changes. O.Zero-Balance ensures the tracing of each product and of each transaction of products. O.Control-Scrap ensures the prevention of any theft of scrap products. O.Data-Transfer ensures that the sensitive data are stored encrypted with the keys of limited authorized employees. O.Internal-Monitor ensures the review of the efficiency of these systems and together with O.Maintain-Security ensure that the above is managed and maintained. O.Multisite-Development ensures that staff from different development sites does not have direct access to the local development repositories. Together, these objectives will therefore counter T.Staff-Collusion.
T.Attack-Transport	O.Product-Transport O.Data-Transfer	O.Product-Transport ensures the protection of the product during transport and the detection of any incident. O.Data-Transfer ensures the protection of data during the internal and external transfer.
P.Config-Items	O.Config-Items	O.Config-Items ensures that all configuration items for secure products are uniquely identified.
P.Config-Control	O.Config-Items O.Config-Control O.Logical-Access	O.Config-Control ensures the right product configuration and the proper release through a formal defined process. Supported by O.Logical-Access, it also ensures that set up and changes are done by authorized persons only. O.Config-Items ensures that all configuration items for secure products are uniquely identified.
P.Config-Process	O.Config-Process	O.Config-Process defines the configuration control procedures and processes.
P.Flaw-Remediation	O.Flaw-Remediation-Monitor O.Flaw-Remediation-External	The Security Objectives directly enforces the OSP.
P.Reception-Control	O.Reception-Control	The identification of received products and its assignment to an internal production process is defined by O.Reception-Control.

TIEMPO S.A.S. Public

Threat and OSP	Security Objective	Rationale
P. Product-Transport	O.Config-Items O.Product-Transport	O.Config-Items ensures the correct labelling of the product. O.Product-Transport ensures the protection of the product during transport and the detection of any incident.
P.Transfer-Data	O.Data-Transfer	O.Data-Transfer ensures the protection of the Sensitive electronic configuration items (data or documents in electronic form).

Table 5-2 - Mapping of the Security Objectives

TIEMPO S.A.S. Public

6 Extended Components Definition

27 No extended components are defined in this Site Security Target.

TIEMPO S.A.S. Public

7 Security Requirements

28 Tiempo using this Site Security Target requires a TOE evaluation up to evaluation assurance level EAL6.

29 The Security Assurance Requirements (SAR) are chosen from the class ALC (Life-cycle support) as defined in [5]:

- CM capabilities (ALC_CMC.5)
- CM scope (ALC_CMS.5)
- Delivery (ALC_DEL.1)
- Flaw remediation (ALC_FLR.2)
- Development security (ALC_DVS.2)
- Life-cycle definition (ALC_LCD.1)
- Tools and techniques (ALC_TAT.3)

30 Because hierarchically higher components are used in this SST, the Security Assurance Requirements listed above fulfil the requirements of:

- Common Criteria, Site Certification, Supporting Document Guidance [2]
- Eurosmart, Security IC Platform Protection Profile [1]
- Eurosmart, Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile [8]

7.1 Application Notes and Refinements

31 The description of the site certification process [2] includes specific application notes. The main item is that a product that is considered as intended TOE is not available during the evaluation. Since the term “TOE” is not applicable in the Site Security Target, the associated processes for the handling of products, or “intended TOEs” are in the scope of this Site Security Target and are described in this document. These processes are subject of the evaluation of the site.

7.1.1 CM Capabilities (ALC_CMC.5)

32 Refer to subsections:

- ‘Application Notes for Site Certification’ in [2] 5.1 ‘Application Notes for ALC_CMC’
- ‘Refinements of the TOE Assurance Requirements’ in [1] 6.2.1.4 ‘Refinements regarding (ALC_CMC)’

7.1.2 CM Scope (ALC_CMS.5)

33 Refer to subsections:

- ‘Application Notes for Site Certification’ in [2] 5.2 ‘Application Notes for ALC_CMS’
- ‘Refinements of the TOE Assurance Requirements’ in [1] 6.2.1.3 ‘Refinements regarding (ALC_CMS)’

7.1.3 Development Security (ALC_DVS.2)

34 Refer to subsections:

- ‘Application Notes for Site Certification’ in [2] 5.4 ‘Application Notes for ALC_DVS’

TIEMPO S.A.S. Public

- 'Refinements of the TOE Assurance Requirements' in [1] 6.2.1.2 'Refinements regarding (ALC_DVS)'

7.1.4 Life-cycle Definition (ALC_LCD.1)

35 Refer to subsection:
- 'Application Notes for Site Certification' in [2] 5.6 'Application Notes for ALC_LCD'

7.1.5 Tools and Techniques (ALC_TAT.3)

36 Refer to subsection:
- 'Application Notes for Site Certification' in [2] 5.7 'Application Notes for ALC_TAT'

7.1.6 Delivery Procedure (ALC_DEL.1)

37 Refer to subsections:
- 'Application Notes for Site Certification' in [2] 5.3 'Application Notes for ALC_CMC'
- 'Refinements of the TOE Assurance Requirements' in [1] 6.2.1.1 'Refinements regarding (ALC_DEL)'

38 According to those application notes, ALC_DEL requirements should only be applied to sites that actually deliver to end-users. Therefore, since this site does not deliver to end-users, ALC_DEL is not applicable to this SST.

7.1.7 Flaw remediation (ALC_FLR.2)

39 Refer to subsection:
- Application Notes for Site Certification' in [2] 5.5 'Application Notes for ALC_FLR'

7.2 Security Requirements Rationale

40 The Security Assurance Rationale maps the content elements of the selected assurance components of [5] to the Security Objectives defined in this SST. The refinements described above are considered.

41 The site has a process in place to ensure an appropriate and consistent identification of the products. If the site already receives configuration items, this process is based on the assumption that the received configuration items are appropriately labeled and identified, refer to A.Item-Identification.

42 Note: The content elements that are changed from the original CC [5] per the application notes in the process description [4] are written in italic. The term TOE can be re-placed by configuration items in most cases. In specific cases, it is replaced by product (in the sense of "intended TOE").

7.2.1 Security Requirements Rationale – Dependencies

43 The dependencies for the assurance requirements are as follows:
- ALC_CMC.5: ALC_CMS.1, ALC_DVS.2, ALC_LCD.1
- ALC_CMS.5: None

TIEMPO S.A.S. Public

- ALC_DVS.2: None
- ALC_FLR.2: None
- ALC_LCD.1: None
- ALC_TAT.3: ADV_IMP.1

44 Some of the dependencies are not (completely) fulfilled:

- ALC_LCD.1 is only partially fulfilled as the site does not represent the entire life-cycle of the product (e.g. the manufacturing phase is not performed within the site). This is in-line with and further explained in [2] 5.1 'Application Notes for ALC_CMC'.
- ADV_IMP.1 is not fulfilled as the site is not certified for a specific TOE product. This is in-line with and further explained in [2] 5.7 'Application Notes for ALC_TAT'.

7.2.2 Security Requirements Rationale – Mapping

SAR	Security Objective	Rationale
ALC_CMC.5.1C The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.	O.Config-Items	Appropriate and consistent labeling is ensured through the use of the configuration management systems. The configuration management system manages all TOE relating hardware, software and information (O.Config-Items).
ALC_CMC.5.2C The CM documentation shall describe the method used to uniquely identify the configuration items.	O.Reception-Control O.Config-Items O.Config-Control O.Config-Process	When an new item is created or received from an external source (O.Reception-Control), it systematically gets an internal unique ID for identification (O.Config-Items). The configuration items are tracked throughout the life-cycle of the TOE (O.Config-Process & O.Config-Control).
ALC_CMC.5.3C The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.	O.Config-Control O.Config-Process	The control procedures put in place for the configuration systems ensures that only authorized personnel is allowed to propose changes configuration (O.Config-Control). These change proposals are reviewed by competent personel as part of the acceptance process before being adopted (O.Config-Process).
ALC_CMC.5.4C The CM system shall uniquely identify all configuration items.	O.Reception-Control O.Config-Items	When an new item is created or received from an external source (O.Reception-Control), it systematically gets an internal unique ID for

TIEMPO S.A.S Public

SAR	Security Objective	Rationale
		identification (O.Config-Items).
ALC_CMC.5.5C The CM system shall provide automated measures such that only authorized changes are made to the configuration items.	O.Security-Control O.Config-Control O.Logical-Access O.Logical-Operation O.Network-separation O.Multisite-Development	The configuration management system implements access restrictions which are set by the security manager (O.Config-Control). Moreover, external unauthorized change is prevented by physical and logical security measures (O.Logical-Access, O.Logical-Access, O.Logical-Operation, O.Network-separation, O.Multisite-Development).
ALC_CMC.5.6C The CM system shall support the production of the *product* by automated means.	O.Config-Process O.Config-Items	The configuration system allows to reproduce a development resource using the unique ID of the resource (O.Config-items) when used in accordance with the predetermined configuration management procedures (O.Config-process).
ALC_CMC.5.7C The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.	O.Config-Control O.Config-Process	The predetermined configuration management procedures (O-Config-Process) stipulate that the person responsible for accepting a configuration item into CM is not the same as the one who developed (O.Config-Control).
ALC_CMC.5.8C The CM system shall clearly identify the configuration items that comprise the TSF.	O.Config-Items	The definition of the configuration item corresponding to the TSF identifies the configuration items that comprise the TSF (O.Config-Items).
ALC_CMC.5.9C The CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.	O.Config-Items O.Config-Control	The configuration management systems (O.Config-Items, O.Config-Control)) are configured such that an audit trail (showing originator, date and time) is automatically generated.
ALC_CMC.5.10C The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.	O.Config-Items O.Config-Control	The configuration management systems (O.Config-Items, O.Config-Control)) are configured in such a way as to allow to

TIEMPO S.A.S PUBLIC

SAR	Security Objective	Rationale
		define the relationship between items and consequently the impact of a given change on other configuration items.
ALC_CMC.5.11C The CM system shall be able to identify the version of the implementation representation from which the TOE is generated.	O.Config-Items	The definition of the configuration item corresponding to the TOE identifies the implementation resources which are used to generate the TOE (O.Config-Items).
ALC_CMC.5.12C The CM documentation shall include a CM plan.	O.Config-Process	The documentation of the Configuration Management System [10] includes a CM plan (O.Config-Process).
ALC_CMC.5.13C The CM plan shall describe how the CM system is used for the development of the *product*.	O.Config-Control O.Config-Process	The development, testing and qualification endeavors performed on the site are managed using formally defined procedures and methodologies (O.Config-Process) which are defined in the documentation of the configuration management system [10]. O.Config-Control ensures that these procedures are systematically heeded.
ALC_CMC.5.14C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the *product*.	O.Config-Process	The acceptance procedures for modified or newly created configuration items are part of the configuration management plan (O.Config-Process).
ALC_CMC.5.15C The evidence shall demonstrate that all configuration items are being maintained under the CM system	O.Reception-Control O.Config-Items O.Config-Control O.Config-Process O.Zero-Balance	The objectives O.Config-Items, O.Reception-Control, O.Config-Control & O.Config-Process are adhered to and this is supported by the evidence on site and in the CM documentation [10]. Indeed, the configuration items are tracked throughout the life-cycle of the TOE (O.Config-Process). Each item gets an internal unique identification for identification (O.Config-Items). The contributed zero balancing prevents an unnoticed loss of

TIEMPO S.A.S. Public

SAR	Security Objective	Rationale
		secure objects by dedicated internal processes (O.ZeroBalance).
ALC_CMC.5.16C The evidence shall demonstrate that all configuration items have been and are being maintained under the CM system	O.Config-Items O.Config-Control O.Config-Process	The objectives O.Config-Items, O.Config-Control & O.Config-Process are adhered to and this is supported by the evidence on site and in the CM documentation [10].

Table 7-1 - Mapping and Rationale for ALC_CMC

SAR	Security Objective	Rationale
ALC_CMS.5.1C The configuration list shall include the following: the *product* itself; the evaluation evidence required by the SARs; the parts that comprise the *product*; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan.	O.Config-Items O.Config-Control O.Config-Process	The configuration list is generated from the configuration management systems (O.Config-items). The configuration items are tracked throughout the life-cycle of the TOE. Each item gets an internal unique identification for identification (O.Config-Items). The procedures are detailed in the CM plan (O.Config-Process). The CM plan is described in the Configuration Management System [10]. The generic configuration list is described in section 3.2 of the Configuration Management System [10].
ALC_CMS.5.2C The configuration list shall uniquely identify the configuration items.	O.Config-Items	The configuration list is generated from the configuration management systems and contains the unique IDs (O.Config-Items) which are assigned to each configuration item.
ALC_CMS.5.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.	O.Config-Items	The configuration list indicates the developer / subcontractor for each configuration item (O.Config-Items).

Table 7-2 - Mapping and Rationale for ALC_CMS

SAR	Security Objective	Rationale
ALC_DVS.2.1C the development	O.Physical-Access	The development security

TIEMPO S.A.S. Public

security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the *product* design and implementation in its development environment.	O.Security-Control O.Internal-Monitor O.Network-separation O.Alarm-Response O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Maintain-Security O.Control-Scrap O.Product-Transport O.Data-Transfer O.Multisite-Development O.Zero-Balance O.Reception-Control	documentation [12] describes the physical (O.Physical-Access, O.Security-Control, O.Multisite-Development, O.Alarm-Response), procedural (O.InternalMonitor, O.Maintain-Security, O.Control-Scrap, O.Zero-Balance, O.Reception-Control, O.Data-Transfer), personnel (O.Staff-Engagement), and other(O.Network-separation, O.Logical-Operation, O.Logical-Access) security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment.
ALC_DVS.2.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the *product*.	O.Internal-Monitor O.Maintain-Security	The development security documentation [12] describes the monitoring procedures (O.Internal-Monitor, O.Maintain-Security) which are put in place to ensure that the security measures are followed during the development activities performed on the site.
ALC_DVS.2.3C The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the *product*.	O.Physical-Access O.Security-Control O.Internal-Monitor O.Network-separation O.Alarm-Response O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Maintain-Security O.Control-Scrap O.Product-Transport O.Data-Transfer O.Multisite-Development O.Zero-Balance O.Reception-Control	The development security documentation [12] describes the physical (O.Physical-Access, O.Security-Control, O.Multisite-Development, O.Alarm-Response), procedural (O.InternalMonitor, O.Maintain-Security, O.Control-Scrap, O.Zero-Balance, O.Reception-Control, O.Data-Transfer), personnel (O.Staff-Engagement), and other(O.Network-separation, O.Logical-

TIEMPO S.A.S. PUBLIC

		Operation, O.Logical-Access) security measures adhered to in order to provide the necessary level of protection to maintain the confidentiality and integrity of the intended TOE.

Table 7-3 - Mapping and Rationale for ALC_DVS

SAR	Security Objective	Rationale
ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the product.	O.Config-Control O.Config-Process O.Flaw-Remediation-Monitor	The flaw remediation tool and the CM system defined in O.Config-Process ensures that all security flaws are tracked for all versions of the TOE.
ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.	O.Config-Process O.Flaw-Remediation-Monitor	O.Config-Process ensures that all security flaws are tracked, the impacts are analyzed and the status is documented.
ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.	O.Config-Process O.Config-Items O.Flaw-Remediation-Monitor	O.Config-Items ensures that corrective actions are identified. O.Config-Process ensures that corrective actions will need to be provided before marking security flaw report as resolved. O.Flaw-Remediation-Monitor ensures that the internal status of the flaw is updated once the security flaw report is resolved.
ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections, and guidance on corrective actions to product users.	O.Flaw-Remediation-External	The flaw remediation tool covered by O.Flaw-Remediation-External ensures that the user is notified as to the status of the flaw. Once, the flaw is resolved, all needed information and flaw remediation guidance are communicated through the flaw remediation tool.
ALC_FLR.2.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE	O.Flaw-Remediation-External	The flaw remediation procedures that are required by O.Flaw-Remediation-

TIEMPO S.A.S. PUBLIC

users reports and enquiries of suspected security flaws in the product.		External and implemented by the flaw remediation tool enable the reception from TOE users and the logging of subsequent enquiries about potential security flaws in the product.
ALC_FLR.2.6C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to product users.	O.Config-Process O.Flaw-Remediation-Monitor O.Flaw-Remediation-External	O.Flaw-Remediation-Monitor and O.Config-Process provides the framework for the definition of formal procedures which are meant to ensure that the security flaws are processed and remediated. O.Flaw-Remediation-External ensures that the corrective actions identified are communicated to product users to remediate the reported security flaws.
ALC_FLR.2.7C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.	O.Config-Process O.Flaw-Remediation-Monitor	O.Flaw-Remediation-Monitor and O.Config-Process provide the framework for the definition of procedures which ensure that the required validation endeavors are undertaken before communicating the corrections to TOE users.
ALC_FLR.2.8C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the product.	O.Flaw-Remediation-External O.Flaw-Remediation-Monitor	O.Flaw-Remediation-External and O.Flaw-Remediation- Monitor provide the framework for the creation of a procedural system (submission forms, status tracking etc.) which allows the TOE users of reporting the security flaws that are detected during the operation phase of the TOE. O.Flaw-Remediation-External ensures that only authentic TOE users are allowed access to the system.

Table 7-4 - Mapping and Rationale for ALC_FLR

SAR	Security Objective	Rationale
ALC_LCD.1.1C The lifecycle definition	O.Config-Process	A predetermined model is

TIEMPO S.A.S. PUBLIC

documentation shall describe the model used to develop and maintain the *product*.		defined to describe the steps of the life cycle that are performed on site [11]. The configuration items are tracked throughout the life-cycle of the TOE (O.Config-Process).
ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the *product*.	O.Config-Process O.Zero-Balance	The configuration items are tracked throughout the life-cycle of the TOE (O.Config-Process). The contributed zero balancing prevents an unnoticed loss of secure objects by dedicated internal processes (O.Zero-Balance).

Table 7-5 - Mapping and Rationale for ALC_LCD

SAR	Security Objective	Rationale
ALC_TAT.3.1C Each development tool used for implementation shall be well-defined.	O.Config-Items	Each tools is identified and inducted as a configuration information for the configuration item which identifies the relevant TOE for which the tool is used for development (O.Config-Items). The currently used versions of the development tools are listed in the Tools and Techniques documentation [13].
ALC_TAT.3.2C The documentation of the development tool shall unambiguously define the meaning of all statements used in the implementation.	O.Config-Process	The development methodologies (O.Config-process) are defined according to the exploited tools purposes and their utilization in the development activities. These purposes and utilization procedures are defined in the documentation issued by the tool's provider. This documentation unambiguously defines the meaning of all statements used in the implementation. These documentations are available in the configuration management system.
ALC_TAT.3.3C The documentation of	O.Config-Process	The development

TIEMPO S.A.S Public

SAR	Security Objective	Rationale
the development tool shall unambiguously define the meaning of all implementation dependent options.		methodologies (O.Config-process) are defined according to the exploited tools purposes and their utilization in the development activities. These purposes and utilization procedures are defined in the documentation issued by the tool's provider. This documentation unambiguously defines the meaning of all implementation dependent options used in the development. These documentations are available in the configuration management system.

Table 7-6 - Mapping and Rationale for ALC_TAT

TIEMPO S.A.S. Public

8 Site Summary Specification

8.1 Services of the Site

45 The Montbonnot-Saint-Martin site supports the following activities:

- Development and testing of embedded software for Security IC products.
- Development and testing of the hardware design of Security IC products.
- Development of software testing routines for the evaluation and characterization of Security IC products.
- Definition of testing procedures for the evaluation and characterization of Security IC products.
- Testing, validation, characterization and qualification of Security IC products.
- Providing software development kits as well as license tokens to be used to develop software to be loaded on TESIC family TOEs.

46 The site maintains a certified Quality Management System as a basis for all processes including an Information Security Management System, that covers the SAR ALC_DVS.2, the SAR ALC_CMS.5 and contributes also to cover the SAR ALC_CMC.5.

47 The site proposes a formalized process for electronic design of Security ICs. Each step of the process is monitored using a configuration management system which enables to cover the SARs ALC_LCD.1, ALC_CMC.5, ALC_TAT.3 and ALC_CMS.5.

48 The site proposes a formalized process for embedded software development. Each step of the process is monitored using a configuration management system which enables to cover the SARs ALC_LCD.1, ALC_CMC.5, ALC_TAT.3 and ALC_CMS.5.

49 The site develops testing programs which are used to test, evaluate and characterize Security ICs. The test program development process enables to cover the SAR ALC_TAT.3.

50 The site provides flaw remediation procedures which allows the secure handling of security flaws observed during operation of the TOE from their registration to their remediation. These procedures enable the coverage of the SAR ALC_FLR.2.

51 The site provides testing equipment which can be used along with the corresponding testing procedures to validate and qualify Security IC products. This contributes to covering the SARs ALC_LCD.1 and ALC_TAT.3.

52 The site defines secure destruction procedures for the components which reached end-of-life status which contribute to the coverage of the SARs ALC_DVS.2 and ALC_CMC.5.

53 The site also hosts services that support the processes above from an operational and organizational point of view: Industrialization, Supply Chain, IT & Tools, Facilities & Equipment's, Quality & Security, Suppliers Management Services, etc.

8.2 Security Assurance Requirements Rationale

54 The Security Assurance rationale is provided in section 7.2. This section gives more justification for the selected Security Assurance Requirements.

- CM capabilities (ALC_CMC.5)
- CM scope (ALC_CMS.5)
- Delivery (ALC_DEL.1)
- Development security (ALC_DVS.2)

TIEMPO S.A.S. Public

- Flaw Remediation (ALC_FLR.2)
- Life-cycle definition (ALC_LCD.1)
- Tools and techniques (ALC_TAT.3)

55 The chosen assurance level ALC_CMC.5 of the assurance family “CM capabilities” is suitable to support the production of high volumes due to the formalized acceptance process and the automated support. The identification of all configuration items supports an automated and industrialized production process. The requirement for authorized changes and ability to identify the changes and version of the implementation will support the integrity and confidentiality required for the products. Responsibility of different departmental teams is also clearly identified for accepting or authorizing any change on the configuration items. Therefore, these assurance requirements stated will meet the requirements for the configuration management.

56 The chosen assurance level ALC_CMS.5 of the assurance family “CM scope” supports the control of the development and test environment. This includes product related documentation and data as well as the documentation for the configuration management and the site security measures. Since the site certification process focuses on the processes based on the absence of a concrete TOE, these security assurance requirements are suitable.

57 The security assurance requirement of the assurance class "Delivery" is suitable to define a controlled process for delivery products to the intermediate parties which intervene in the life-cycle of the Security IC. The confidentiality and integrity of the product during transport is addressed by this assurance class. Since the Protection Profile requires the same assurance level it is considered to be sufficient.

58 The chosen assurance level ALC_FLR.2 of the assurance family “Flaw remediation” is suitable to support the conformance claims required by the Protection Profiles of the TOE products developed within the site.

59 The chosen assurance level ALC_LCD.1 of the assurance family “Life-cycle definition” is suitable to support the controlled development and production process within the site. This includes the documentation of these processes and the procedures for the configuration management. Because the site provides only a limited support of the described life-cycle for the development and production of Security ICs, the corresponding security objectives focus on the specific part of the life-cycle which is handled within the site. 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.

60 The security assurance requirements of the assurance class "Tools and Techniques" shall support the secure development and production of the TOE. The control, capabilities and configuration of the tools contribute to achieve reproducible and consistent development, production and test processes. Therefore, this Security assurance requirement is suitable for this type of product.

8.3 Objective Rationale

61 The objectives rationale is provided in section 5. The following section provides a more detailed rationale on how the threats and organizational security policies are effectively addressed by the security objectives.

62 Table 8-1 below describes the mapping between the security objectives, the threats and the organizational security policies.

TIEMPO S.A.S. Public

	O.Physical-Access	O.Security-Control	O.Alarm-Response	O.Internal-Monitor	O.Maintain-Security	O.Network-separation	O.Logical-Access	O.Logical-Operation	O.Config-Items	O.Config-Control	O.Config-Process	O.Flaw-Remediation-Monitor	O.Flaw-Remediation-External	O.Zero-Balance	O.Reception-Control	O.Control-Scrap	O.Staff-Engagement	O.Product-Transport	O.Data-Transfer	O.Multisite-Development
T.Smart-Theft	x	x	x	x	x											x	x			x
T.Rugged-Theft	x	x	x	x	x											x	x			
T.Computer-Net	x			x	x	x	x	x								x	x			x
T.Accident-Change										x	x			x		x				x
T.Unauthorised-Staff	x	x	x	x	x	x	x	x		x				x		x	x			x
T.Staff-Collusion	x	x	x	x	x	x	x			x				x		x	x			x
T.Attack-Transport																		x	x	
P.Config-Items									x											
P.Config-Control									x	x	x									
P.Config-Process											x									
P.Flaw-Remediation												x	x							
P.Reception-Control															x					
P. Product-Transport									x									x		
P.Transfer-Data																			x	

Table 8-1 - Objectives Mapping

8.3.1 O.Physical-Access

63 A Closed-Circuit Television (CCTV) is used in the Entrance hall of the site. This camera monitors all entrances and the access to the office is only possible via access-controlled doors.

64 The Office doors are controlled with a magnetic contact system. The doors can only be opened by badging and when necessary, a sound alarm is triggered in case this door is forced.

65 The Office Entrance Doors as well as the windows also include an alarm system and motion sensors. This alarm is activated/deactivated by a digital code.

66 The previously described physical security measures are supported by O.Alarm-Response providing an alarm system and O.Security-Control. Thereby the threats T.Smart-Theft, T.Rugged-Theft, T.Staff-Collusion and T.Unauthorized-Staff can be prevented.

8.3.2 O.Security-Control

67 During working hours, the employees monitor the site and the surveillance system. The alarm system is connected to a central command center that is manned 24 hours. During off- hours, the alarm system is used to monitor the site.

68 The CCTV system as well as the motion sensors support these measures because they are always enabled. Further on, the security control is supported by O.Physical-Access requiring different level of access control for the access to secure product during operation as well as

TIEMPO S.A.S. Public

during off-hours.

69 This addresses the threats T.Smart-Theft, T.Rugged-Theft, T.Unauthorized-Staff and T.Staff-Collusion.

8.3.3 O.Alarm-Response

70 During working hours, the employees monitor the alarm system. The alarm system is connected to a central command center that is manned 24 hours. During off-hours, an intervention patrol supports the alarm system.

71 O.Physical-Access requires certain time to overcome the different level of access control. The response time of the intervention patrol and the physical resistance match to provide an effective alarm response.

72 This addresses the threats T.Smart-Theft, T.Rugged-Theft, T.Unauthorized-Staff and T.Staff-Collusion.

8.3.4 O.Internal-Monitor

73 Regular security management meetings are implemented to monitor security incidences as well as changes or updates of security relevant systems and processes. This comprises also logs and security events of security relevant systems. Major changes of security systems and security procedures are reviewed in general management systems review meetings. Upon introduction of a new process, a formal review and release for mass production is made before being generally introduced.

74 This addresses T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorized-Staff and T.Staff-Collusion.

8.3.5 O.Maintain-Security

75 The security relevant systems enforcing or supporting O.Physical-Access, O.Security-control and O.Logical-Access are checked and maintained regularly by the suppliers. Logging files are checked regularly for technical problems and specific maintenance requests.

76 This addresses T.Smart-Theft, T.Rugged-Theft, T.Unauthorized-Staff and T.Computer-Net.

8.3.6 O.Network-separation

77 The development network is separated from the internet with a firewall. The development network is further separated into sub-networks by internal firewalls. These firewalls allow only authorized information exchange between the internal sub-networks.

78 This VLAN network only connects:
- The development workstations provided by Tiempo;
- Additional equipment (e.g. oscilloscope) approved by Tiempo.

79 The objective is supported by O.Internal-Monitor based on the regular checks of the access logs regarding security relevant events.

80 This addresses T.Computer-Net, T.Unauthorized-Staff and T.Staff-Collusion.

TIEMPO S.A.S. Public

8.3.7 O.Logical-Access

81 Each user is logging into the system with his personalized username and password. One of the objectives is also to supported by O.Internal-Monitor based on the checks of the logging regarding security relevant events.

82 The individual accounts are addressing T.Computer-Net. All configurations are stored in the database of the internal system. This addresses the threats T.Computer-Net, T.Unauthorized-Staff and the OSP P.Config-Control.

8.3.8 O.Logical-Operation

83 All logical protection measures are maintained and updated as required. Critical items such as virus scanners are updated daily. The backup is sufficiently protected and is only configurable by the IT administrator.

84 This addresses T.Computer-Net.

8.3.9 O.Config-Items

85 The site has a configuration management system that assigns a unique internal identification to each item of development data, specification documents, engineering samples, etc. All the product configuration information is stored in databases, covering materials, process, test programs.

86 This addresses the OSP P.Config-items, P.Config-Control and P.Product-Transport.

8.3.10 O.Config-Control

87 The site has a configuration management system which allows to monitor and track the changes and modifications which impact any of the monitored items.

88 This addresses the threats T.Accident-Change, T.Unauthorized-Staff, T-Staff-Collusion and the OSP P.Config-Control.

8.3.11 O.Config-Process

89 The site has defined formal change procedure for development data and products. Additionally, formally defined procedures for operations such as the release of a product and the error tracking have been defined.

90 This addresses the threats T.Accident-Change and the OSPs P.Config-Control and Config-Process.

8.3.12 O.Flaw-Remediation-Monitor

91 The site has defined a procedural process to handle TOE flaws that may be discovered by development/production teams or raised by the TOE users. The process is implemented through the configuration management system and allows to monitor the managed flaws and their status and matches each flaw with the relevant release of the TOE.

92 This the OSP P.Flaw-Remediation.

TIEMPO S.A.S. Public

8.3.13 O.Flaw-Remediation-External

93 The site has a flaw remediation tool aimed at enabling the TOE users to submit flaw reports that are then handled internally in the configuration system.

94 The site has a flaw remediation tool aimed at communicating the flaw corrections to TOE users.

95 This the OSP P.Flaw-Remediation.

8.3.14 O.Zero-Balance

96 Chips and boards used for testing are uniquely identified throughout the whole process. At every process step the registration of good and scrapped/rejected elements is recorded.

97 This security objective is supported by O.Physical-Access, O.Config-Control and O.Staff-Engagement.

98 This addresses the threats T.Accident-Change, T.Unauthorised-Staff, T.Staff-Collusion.

8.3.15 O.Reception-Control

99 At reception secure products are identified by the shipping documents, packing labels and information in Tiempo's configuration management system supported by O.Config-Items. A product that cannot be identified is put on hold in a secure storage. Inspection at reception is counting the number of boxes and checking the integrity of security seals of these boxes if applicable.

100 The OSP P.Reception-Control is addressed by the reception control.

8.3.16 O.Control-Scrap

101 Products which reach their end-of-life status are identified and stored internally in a secure location. Subsequently, these products are destructed in a controlled and documented manner.

102 The destruction process ensures a transformation to small pieces that cannot be reconstructed and utilized by a potential attacker.

103 Sensitive information and information storage media are monitored regularly and useless data is destructed in a supervised and documented process.

104 Two shredders are used for documents/CDs destruction according to the Security Class 3 requirements of the DIN 66399 standard [14].

105 Supported by O.Physical-Access and O.Staff-engagement this addresses the threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion.

8.3.17 O.Staff-Engagement

106 All employees are interviewed before hiring. They must sign an NDA before they start working in the company. The formal training and qualification include security relevant subjects and the principles of handling and storage of secure products or secure information. The security objectives O.Physical-Access, O.Logical-Access, O.Network-separation, O.Internal-Monitor and O.Config-Items support the engagement of the staff.

TIEMPO S.A.S. Public

107 This addresses the threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Accident-Change, T.Unauthorised-Staff, T.Staff-Collusion.

8.3.18 O.Product-Transport

108 The external shipment of products developed internally is ruled by formally specified procedures which specify the necessary requirements in terms of recipient information, transportation mean and the internal employee which is tasked with tracking the location of the product while being shipped and communicating with the recipient to ensure the correct delivery.

109 This addresses the threat T.Attack-Transport and the OSP P.Product-Transport

8.3.19 O.Data-Transfer

110 The site defines formalized procedures which regulate the transfer of sensitive data internally and externally. These include security measures such as encryption and signing methods.

111 Additionally, this objective is supported by other security objectives such as O.Network-Separation and O.Logical-Access which implement the “need to know” principle.

112 This addresses the threat T.Attack-Transport and the OSP P.Transfer-Data.

8.3.20 O.Multisite-Development

113 The site formalized procedures which regulate the exchange of sensitive information between development sites. These include security measures such as encryption and signing methods.

114 Additionally, this objective is supported by other security objectives such as O.Network-Separation and O.Logical-Access which implement the “need to know” principle.

115 This addresses the threats T.Smart-Theft, T.Computer-Net, T-Accident-Change, T.Unauthorized-Staff and T.Staff-Collusion.

8.4 Assurance Measure Rationale

8.4.1 O.Physical-Access

116 ALC_DVS.2.1C requires the developer to describe all the physical, procedural, personnel, and other security measures that are necessary to protect the integrity and confidentiality of the TOE design and implementation including the initialization in its development environment.

117 ALC_DVS.2.3C requires that the evidence justifies the fact that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product.

118 Thereby, these Security Assurance Requirements contribute to meet the objective.

TIEMPO S.A.S. Public

8.4.2 O.Security-Control

119 ALC_CMC.5.5C requires that the CM system provides automated measures such that only authorized changes are made to the configuration items.

120 ALC_DVS.2.1C requires the developer to describe all the physical, procedural, personnel, and other security measures that are necessary to protect the integrity and confidentiality of the TOE design and implementation including the initialization in its development environment.

121 ALC_DVS.2.3C requires that the evidence justifies the fact that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product.

122 Thereby, these Security Assurance Requirements contribute to meet the objective.

8.4.3 O.Alarm-Response

123 ALC_DVS.2.1C requires the developer to describe all the physical, procedural, personnel, and other security measures that are necessary to protect the integrity and confidentiality of the TOE design and implementation including the initialization in its development environment.

124 ALC_DVS.2.3C requires that the evidence justifies the fact that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product.

125 Thereby, these Security Assurance Requirements contribute to meet the objective.

8.4.4 O.Internal-Monitor

126 ALC_DVS.2.1C requires the developer to describe all the physical, procedural, personnel, and other security measures that are necessary to protect the integrity and confidentiality of the TOE design and implementation including the initialization in its development environment.

127 ALC_DVS.2.2C requires that the development security documentation justifies that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

128 ALC_DVS.2.3C requires that the evidence justifies the fact that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product.

129 Thereby, these Security Assurance Requirements contribute to meet the objective.

8.4.5 O.Maintain-Security

130 ALC_DVS.2.1C requires the developer to describe all the physical, procedural, personnel, and other security measures that are necessary to protect the integrity and confidentiality of the TOE design and implementation including the initialization in its development environment.

131 ALC_DVS.2.2C requires that the development security documentation justifies that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

TIEMPO S.A.S. Public

132 ALC_DVS.2.3C requires that the evidence justifies the fact that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product.

133 Thereby, these Security Assurance Requirements contribute to meet the objective.

8.4.6 O.Network-separation

134 ALC_CMC.5.5C requires that the CM system provides automated measures such that only authorized changes are made to the configuration items.

135 ALC_DVS.2.1C requires the developer to describe all the physical, procedural, personnel, and other security measures that are necessary to protect the integrity and confidentiality of the TOE design and implementation including the initialization in its development environment.

136 ALC_DVS.2.3C requires that the evidence justifies the fact that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product.

137 Thereby, these Security Assurance Requirements contribute to meet the objective.

8.4.7 O.Logical-Access

138 ALC_CMC.5.5C requires that the CM system provides automated measures such that only authorized changes are made to the configuration items.

139 ALC_DVS.2.1C requires the developer to describe all the physical, procedural, personnel, and other security measures that are necessary to protect the integrity and confidentiality of the TOE design and implementation including the initialization in its development environment.

140 ALC_DVS.2.3C requires that the evidence justifies the fact that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product.

141 Thereby, these Security Assurance Requirements contribute to meet the objective.

8.4.8 O.Logical-Operation

142 ALC_CMC.5.5C requires that the CM system provides automated measures such that only authorized changes are made to the configuration items.

143 ALC_DVS.2.1C requires the developer to describe all the physical, procedural, personnel, and other security measures that are necessary to protect the integrity and confidentiality of the TOE design and implementation including the initialization in its development environment.

144 ALC_DVS.2.3C requires that the evidence justifies the fact that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product.

145 Thereby, these Security Assurance Requirements contribute to meet the objective.

TIEMPO S.A.S. Public

8.4.9 O.Config-Items

146 ALC_CMC.5.1C requires that the CM documentation show that a process is in place to ensure an appropriate and consistent labelling.

147 ALC_CMC.5.2C requires that the CM documentation describes the method used to uniquely identify the configuration items.

148 ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items.

149 ALC_CMC.5.6C requires that the CM system supports the production of the product by automated means.

150 ALC_CMC.5.8C requires that the CM system clearly identifies the configuration items that comprise the TSF.

151 ALC_CMC.5.9C requires that the CM system supports the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.

152 ALC_CMC.5.10C requires that the CM system provides an automated means to identify all other configuration items that are affected by the change of a given configuration item.

153 ALC_CMC.5.11C requires that the CM system is able to identify the version of the implementation representation from which the TOE is generated.

154 ALC_CMC.5.15C requires that the evidence demonstrates that all configuration items are being maintained under the CM system.

155 ALC_CMC.5.16C requires that the evidence demonstrates that all configuration items have been and are being maintained under the CM system.

156 ALC_CMS.5.1C requires that the configuration list includes the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan.

157 ALC_CMS.5.2C requires that the CL uniquely identify the configuration items.

158 ALC_CMS.5.3C requires that for each configuration item, the configuration list indicates the developer/subcontractor of the item.

159 ALC_FLR.2.3C requires that the CM system identify uniquely each security flaw and its corresponding corrective actions.

160 ALC_TAT.3.1C requires that each development tool used for implementation be well-defined.

161 All these content elements of the mentioned SARs require dedicated content of the CM documentation and the configuration list, properties of the CM system and content of the tools and techniques documentation. Thereby, these Security Assurance Requirements contribute to meet the objective.

8.4.10 O.Config-Control

162 ALC_CMC.5.2C requires that the CM documentation describes the method used to uniquely identify the configuration items.

163 ALC_CMC.5.3C requires that the CM documentation justifies that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.

TIEMPO S.A.S Public

164 ALC_CMC.5.5C requires that the CM system provides automated measures such that only authorized changes are made to the configuration items.

165 ALC_CMC.5.7C requires that the CM system ensures that the person responsible for accepting a configuration item into CM is not the person who developed it.

166 ALC_CMC.5.9C requires that the CM system supports the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.

167 ALC_CMC.5.10C requires that the CM system provides an automated means to identify all other configuration items that are affected by the change of a given configuration item.

168 ALC_CMC.5.13C requires that the CM plan describes how the CM system is used for the development of the TOE.

169 ALC_CMC.5.15C requires that the evidence demonstrates that all configuration items are being maintained under the CM system.

170 ALC_CMC.5.16C requires that the evidence demonstrates that all configuration items have been and are being maintained under the CM system.

171 ALC_CMS.5.1C requires that the configuration list includes the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan.

172 ALC_FLR.2.1C requires that the CM system track all the reported security flaws.

173 ALC_FLR.2.8C requires that the CM system provides access to TOE users to submit security flaw reports and follow the status of their handling procedures.

174 All these content elements of the mentioned SARs require dedicated content of the CM documentation and the configuration list, properties of the CM system. Thereby, these Security Assurance Requirements contribute to meet the objective.

8.4.11 O.Config-Process

175 ALC_CMC.5.2C requires that the CM documentation describes the method used to uniquely identify the configuration items.

176 ALC_CMC.5.3C requires that the CM documentation justifies that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.

177 ALC_CMC.5.6C requires that the CM system supports the production of the product by automated means.

178 ALC_CMC.5.7C requires that the CM system ensures that the person responsible for accepting a configuration item into CM is not the person who developed it.

179 ALC_CMC.5.12C requires that the CM documentation includes a CM plan.

180 ALC_CMC.5.13C requires that the CM plan describes how the CM system is used for the development of the TOE.

181 ALC_CMC.5.14C requires that the CM plan describe the procedures used to accept modified or newly created configuration items as part of the TOE.

182 ALC_CMC.5.15C requires that the evidence demonstrates that all configuration items are being maintained under the CM system.

183 ALC_CMC.5.16C requires that the evidence demonstrates that all configuration items have

TIEMPO S.A.S. Public

been and are being maintained under the CM system.

184 ALC_CMS.5.1C requires that the configuration list includes the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan.

185 ALC_FLR.2.1C and ALC_FLR2.8 requires that the CM plan describes procedures used to submit security flaw reports and track their status as they are maintained under the CM system.

186 ALC_FLR.2.2C requires that the CM documentation provides a submission form which allows to describe the nature and effect of each security flaw before its registration. Also, the CM system shall allow to track the status of the handling of the security flaws.

187 ALC_FLR.2.3C requires that the CM system includes means to enforce the necessity of providing a corrective action for each security flaw submitted by the TOE user.

188 ALC_FLR.2.4C requires that the CM documentation provides a framework for the preparation of guidance documents describing the flaw and the corresponding corrective actions for the benefit of TOE users.

189 ALC_FLR.2.5C requires that the CM system provides limited access to TOE users allowing them to submit flaw reports as well as a mean of allowing the developer to enquiry the vulnerability status of the TOE in its operation phase.

190 ALC_FLR.2.6C requires that the CM system includes means to enforce the necessity of providing a corrective action for each security flaw submitted by the TOE user. Also, once the corrective actions are identified, the CM system shall ensure that the corrective guidance is issued to TOE users.

191 ALC_FLR.2.7C requires that the CM system includes means to verify that comprehensive validation procedures have been undertaken before considering the security flaw resolved in order not to introduce new flaws.

192 ALC_LCD.1.1C requires that the lifecycle definition documentation describes the model used to develop and maintain the product.

193 ALC_LCD.1.2C requires that the life-cycle model provides for the necessary control over the development and maintenance of the product.

194 ALC_TAT.3.2C requires that the documentation of the development tool unambiguously defines the meaning of all statements used in the implementation.

195 ALC_TAT.3.3C requires that the documentation of the development tool unambiguously defines the meaning of all implementation dependent options.

196 All these content elements of the mentioned SARs require dedicated content of the CM documentation and the configuration list, properties of the CM system, content of the tools and techniques documentation and of the life-cycle documentation. Thereby, these Security Assurance Requirements contribute to meet the objective.

8.4.12 O.Flaw-Remediation-Monitor

197 ALC_FLR.2.1C and ALC_FLR2.8 requires that the flaw remediation procedures describe procedures used to submit security flaw reports and track their status as they are maintained under the flaw remediation tool and the CM system.

198 ALC_FLR.2.2C requires that the flaw remediation guidance provides a submission form which allows to describe the nature and effect of each security flaw before its registration.

TIEMPO S.A.S. Public

Also, the flaw remediation tool and the CM system shall allow to track the status of the handling of the security flaws.

199 ALC_FLR.2.3C requires that the flaw remediation procedures and the CM system include means to enforce the necessity of providing a corrective action for each security flaw submitted by the TOE user.

200 ALC_FLR.2.5C requires that the flaw remediation tool provides limited access to TOE users allowing them to submit flaw reports as well as a mean of allowing the developer to enquiry the vulnerability status of the TOE in its operation phase.

201 ALC_FLR.2.6C requires that the flaw remediation procedures and the CM system include means to enforce the necessity of providing a corrective action for each security flaw submitted by the TOE user. Also, once the corrective actions are identified, the flaw remediation procedures shall ensure that the corrective guidance is issued to TOE users.

202 ALC_FLR.2.7C requires that the CM system includes means to verify that comprehensive validation procedures have been undertaken before considering the security flaw resolved in order not to introduce new flaws.

203 ALC_FLR.2.8C requires that the flaw remediation tool provides access to TOE users to submit security flaw reports and follow the status of their handling procedures.

8.4.13 O.Flaw-Remediation-External

204 ALC_FLR.2.4C requires that the flaw remediation documentation provides a framework for the preparation of guidance documents describing the flaw and the corresponding corrective actions for the benefit of TOE users.

205 ALC_FLR.2.5C requires that the flaw remediation tool provides limited access to TOE users allowing them to submit flaw reports as well as a mean of allowing the developer to enquiry the vulnerability status of the TOE in its operation phase.

206 ALC_FLR.2.6C requires that, once the corrective actions are identified, the flaw remediation procedures shall ensure that the corrective guidance is issued to TOE users.

207 ALC_FLR.2.8C requires that the flaw remediation tool provides access to TOE users to submit security flaw reports and follow the status of their handling procedures.

8.4.14 O.Zero-Balance

208 ALC_CMC.5.15C requires that the evidence demonstrates that all configuration items are being maintained under the CM system.

209 ALC_DVS.2.1C requires the developer to describe all the physical, procedural, personnel, and other security measures that are necessary to protect the integrity and confidentiality of the TOE design and implementation including the initialization in its development environment.

210 ALC_DVS.2.3C requires that the evidence justifies the fact that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product.

211 ALC_LCD.1.2C requires that the life-cycle model provides for the necessary control over the development and maintenance of the product.

212 Thereby, these Security Assurance Requirements contribute to meet the objective.

TIEMPO S.A.S. Public

8.4.15 O.Reception-Control

213 ALC_CMC.5.2C requires that the CM documentation describes the method used to uniquely identify the configuration items.

214 ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items.

215 ALC_CMC.5.15C requires that the evidence demonstrates that all configuration items are being maintained under the CM system.

216 ALC_DVS.2.1C requires the developer to describe all the physical, procedural, personnel, and other security measures that are necessary to protect the integrity and confidentiality of the TOE design and implementation including the initialization in its development environment.

217 ALC_DVS.2.3C requires that the evidence justifies the fact that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product.

218 Thereby, these Security Assurance Requirements contribute to meet the objective.

8.4.16 O.Control-Scrap

219 ALC_DVS.2.1C requires the developer to describe all the physical, procedural, personnel, and other security measures that are necessary to protect the integrity and confidentiality of the TOE design and implementation including the initialization in its development environment.

220 ALC_DVS.2.3C requires that the evidence justifies the fact that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product.

221 Thereby, these Security Assurance Requirements contribute to meet the objective.

8.4.17 O.Staff-Engagement

222 ALC_DVS.2.1C requires the developer to describe all the physical, procedural, personnel, and other security measures that are necessary to protect the integrity and confidentiality of the TOE design and implementation including the initialization in its development environment.

223 ALC_DVS.2.3C requires that the evidence justifies the fact that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product.

224 Thereby, these Security Assurance Requirements contribute to meet the objective.

8.4.18 O.Product-Transport

225 ALC_DVS.2.1C requires the developer to describe all the physical, procedural, personnel, and other security measures that are necessary to protect the integrity and confidentiality of the TOE design and implementation including the initialization in its development environment.

226 ALC_DVS.2.3C requires that the evidence justifies the fact that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product.

TIEMPO S.A.S. Public

227 Thereby, these Security Assurance Requirements contribute to meet the objective.

8.4.19 O.Data-Transfer

228 ALC_DVS.2.1C requires the developer to describe all the physical, procedural, personnel, and other security measures that are necessary to protect the integrity and confidentiality of the TOE design and implementation including the initialization in its development environment.

229 ALC_DVS.2.3C requires that the evidence justifies the fact that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product.

230 Thereby, these Security Assurance Requirements contribute to meet the objective.

8.4.20 O.Multisite-Development

231 ALC_CMC.5.5C requires that the CM system provides automated measures such that only authorized changes are made to the configuration items.

232 ALC_DVS.2.1C requires the developer to describe all the physical, procedural, personnel, and other security measures that are necessary to protect the integrity and confidentiality of the TOE design and implementation including the initialization in its development environment.

233 ALC_DVS.2.3C requires that the evidence justifies the fact that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product.

234 Thereby, these Security Assurance Requirements contribute to meet the objective.

8.5 Mapping of the Evaluation Documentation

SAR	ALC documentation
ALC_CMC.5	Configuration Management System Documentation [10]
ALC_CMS.5	Configuration Management System Documentation [10]
ALC_DVS.2	Physical Security Documentation [12]
ALC_FLR.2	Flaw Remediation Documentation [16] Flaw Remediation User Guide [17]
ALC_LCD.1	Life Cycle Documentation [11]
ALC_TAT.3	Tools and Techniques Documentation [13]

Table 8-2 - Mapping of SARs and Evaluation Documentation

TIEMPO S.A.S. Public