Rambus

Common Criteria

Site Certification

Site Security Target
Rambus Headquarters

Document Revision: G
Document Date: 06-Jul-2022
Document Number: 001-001100-502/1
Document Status: Accepted

Rambus Inc. Corporate Headquarters
4453 North First Street, Suite 100
San Jose, CA 95134
USA
Phone: +1 408-462-8000
Website : https://www.rambus.com/
Contact : sipsupport@rambus.com

Table of Contents

1 Document Introduction 6
1.1 Reference 6
1.2 Revision History 6
1.3 Terms and Abbreviations 6
2 SST Introduction 7
2.1 Identification of the Site 7
2.2 Site Description 7
2.2.1 Rambus Inc (Headquarters) 7
2.2.2 Rambus Datacentre 7
3 Conformance Claim 8
4 Security Problem Definition 9
4.1 Assets 9
4.2 Threats 9
4.3 Organisational Security Policies 10
4.4 Assumptions 10
5 Security Objectives 11
5.1 Security Objectives Rationale 12
6 Extended Assurance Components Definition 14
7 Security Assurance Requirements 15
7.1 Application Notes and Refinements 15
7.1.1 CM Capabilities (ALC_CMC.4) 15
7.1.2 CM Scope (ALC_CMS.4) 15
7.1.3 Delivery (ALC_DEL.1) 15
7.1.4 Development Security (ALC_DVS.2) 15
7.1.5 Life-cycle Definition (ALC_LCD.1) 15
7.1.6 Tools and Techniques (ALC_TAT.1) 15
7.2 Security Requirements Rationale 16
7.2.1 Security Requirements Rationale – Dependencies 16
7.2.2 Security Requirements Rationale – Mapping 16
8 Site Summary Specification 19
8.1 Preconditions Required by the Site 19
8.2 Services of the Site 19
8.3 Objectives Rationale 19

8.3.1 O.Physical-Access 19
8.3.2 O.Security-Control 19
8.3.3 O.Alarm-Response 20
8.3.4 O.Internal-Monitor 20
8.3.5 O.Maintain-Security 20
8.3.6 O.Logical-Access 20
8.3.7 O.Logical-Operation 20
8.3.8 O.Config-Dev-Env 20
8.3.9 O.Config-Activities 21
8.3.10 O.Staff-Engagement 21
8.3.11 O.Transfer-Data 21
8.3.12 O.Control-Scrap 21
8.3.13 O.Lifecycle-Doc 21
8.4 Security Assurance Requirements Rationale 21
8.4.1 CM Capabilities (ALC_CMC.4) 21
8.4.2 CM Scope (ALC_CMS.4) 21
8.4.3 Delivery (ALC_DEL.1) 22
8.4.4 Development Security (ALC_DVS.2) 22
8.4.5 Lifecycle Definition (ALC_LCD.1) 22
8.4.6 Tools and Techniques (ALC_TAT.1) 22
8.5 Assurance Measure Rationale 22
8.5.1 O.Physical-Access 22
8.5.2 O.Security-Control 22
8.5.3 O.Alarm-Response 22
8.5.4 O.Internal-Monitor 22
8.5.5 O.Maintain-Security 22
8.5.6 O.Logical-Access 22
8.5.7 O.Logical-Operation 23
8.5.8 O.Config-Dev-Env 23
8.5.9 O.Config-Activities 23
8.5.10 O.Staff-Engagement 23
8.5.11 O.Transfer-Data 23
8.5.12 O.Control-Scrap 23
8.5.13 O.Lifecycle-Doc 23
8.6 Mapping of the Evaluation Documentation 25
9 References 28
9.1 Literature 28
9.2 Internal References 28

List of Tables

Table 1 Threats and OSP Security Objectives Rationale 13
Table 2 Rationale for ALC_CMC.4 17
Table 3 Rationale for ALC_CMS.4 17
Table 4 Rationale for ALC_DEL.1 17
Table 5 Rationale for ALC_DVS.2 17
Table 6 Rationale for ALC_LCD.1 18
Table 7 Mapping of the Evidence for ALC_CMC.4 26
Table 8 Mapping of Evidence for ALC_CMS.4 26
Table 9 Mapping of Evidence for ALC_DEL.1 26
Table 10 Mapping of Evidence for ALC_DVS.2 27
Table 11 Mapping of Evidence for ALC_LCD.1 27
Table 12 Mapping of Evidence for ALC_TAT.1 27

1 Document Introduction

1.1 Reference

Title: Site Security Target – Rambus Headquarters
Version: Revision G
Date: 06-July-2022
Company: Rambus Inc
Name of site: Rambus Headquarters
EAL-Level: EAL4+

1.2 Revision History

Revision	Comment	Date	Author / Owner
0.1	Initial Version	12-Mar-2021	S.Kincaid
0.2	Internal version for markup	14-Apr-2021	S.Kincaid
0.3	Consolidated version with feedback from IT, Facilities, HR	21-Apr-2021	S.Kincaid
0.4	Updates based on feedback from lab	27-May-2021	S.Kincaid
A	First release, new document template	31-May-2021	S.Kincaid
B	Updates following review feedback from Brightsight (21-RPT-055 Mom Action Items v3.0)	21-Jul-2021	S.Kincaid
C	Updates following review feedback from Brightsight (21-RPT-055 Mom Action Items v5.0)	06-Sep-2021	S.Kincaid
D	Updates for O.Lifecycle-Doc, addressing 21-RPT-055 Mom Action Items v7.0 comments	12-Jan-2022	G. Goodwill
E	Make dates and site naming consistent	03-Mar-2022	G. Goodwill
F	Updates following EM3	28-Jun-2022	G. Goodwill
G	Update document number to public	06-Jul-2022	G. Goodwill

1.3 Terms and Abbreviations

Term	Meaning
ALC	Assurance LifeCycle
CC	Common Criteria
CM	Configuration Management
DCMS	Document Control Management System
EAL	Evaluation Assurance Level
EDL	Evidence Document List
IP	Intellectual Property
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SST	Site Security Target
ST	Security Target
TOE	Target of Evaluation

2 SST Introduction

This document is based upon the Eurosmart Site Security Target Template [1] with adaptations such that it fits the site (ie development site, no production).

2.1 Identification of the Site

Rambus uses a Datacentre for compute resources. This is a separate location from the main site. Therefore, two sites are detailed below.

Rambus Inc (Headquarters)
4453 North First Street, Suite 100,
San Jose, CA 95134
United States

Rambus Datacentre
Element Critical
Silicon Valley One
1360 Kifer Road
Sunnyvale, CA 94086
United States

2.2 Site Description

2.2.1 Rambus Inc (Headquarters)

The site is a six floor multi-tenant office building. Rambus leases and occupies approximately ninety percent of the first floor as well as the fifth floor and sixth floors in their entirety. The non-Rambus controlled areas of the building are not in scope.

There are physical and electronic security controls in place to ensure that only authorized personnel are permitted access to Rambus occupied spaces. Within the development and lab areas, only members of the development team have access to sensitive information such as source code, restricted documentation and development systems.

The site only supports

- IP Development (equivalent to Phase 2 in TOE Lifecycle as defined in PP-0084)
- IP design
- IP Dedicated Software development
- Delivery to Clients

2.2.2 Rambus Datacentre

This site is a Co-Location datacentre hosting Rambus' compute centre and storage. Within the datacentre, Rambus had a dedicated 'caged' space consisting of 3 rows of server racks and support equipment.

The site security plan has been developed in accordance to Rambus specifications. There are physical and electronic security controls in place to ensure that only authorised personnel are permitted access to the Rambus caged area.

This site supports

- Compute resources used in IP development

3 Conformance Claim

The evaluation is based on Common Criteria Version 3.1

- Common Criteria for Information Technology Security Evaluations, Part 1: Introduction and General Model; Version 3.1, Revision 5, April 2017 [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017 [3]

For the evaluation, the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 5, April 2017 [4]
- Supporting Document Guidance, Site Certification, October 2007, Version 1.0, Revision 1, CCDB-2007-11-001 [6]

The evaluation of the site comprises the following assurance components:

- ALC_CMC.4
- ALC_CMS.4
- ALC_DEL.1
- ALC_DVS.2
- ALC_LCD.1
- ALC_TAT.1

The assurance level chosen for this SST is compliant to the Protection Profile (PP) and therefore suitable for Security IP development.

The chosen assurance components are derived from the assurance level EAL4+ of the assurance class "Life-cycle Support". The augmentation is related to ALC_DVS.2. For the assessment of the security measures attackers with high attack potential are assumed. Therefore, this site supports product evaluations up to EAL4 augmented by ALC_DVS.2.

4 Security Problem Definition

The Security Problem Definition comprises security problems derived from threats against the assets handled by the site and security problems derived from the configuration management requirements. The configuration management covers the integrity of the TOE and the security management of the site.

The assets which the site handles can be classified as “sensitive” knowledge of the TOE at the highest.

Where required, adaptations of the items in this section have been made to suit the site.

4.1 Assets

Development Data:	The site has access to electronic information relating to the development such as Source Code, Specifications, Manuals and Guidance documents. The integrity and confidentiality of this data must be protected.
Development Tools:	In support of development activities, the site uses tools and systems such as IT equipment, compilers etc. The integrity of these tools and systems must be maintained.
Physical Assets:	The site has development systems and documents as required for the development activities. The integrity and confidentiality of this data must be protected.
Product:	The site manages the delivery of the product. The integrity and confidentiality must be protected.

4.2 Threats

T.Smart-Theft:	An attacker tries to access sensitive areas of the site for manipulation or theft of sensitive configuration items (confidentiality and/or integrity of Development Data, Development tools, Physical Assets). The attacker has sufficient time to investigate the site outside the controlled boundary. For the attack, the use of standard equipment for burglary is considered. In addition, the attacker may be able to use specific working clothes of the site to camouflage the intention.
T.Rugged-Theft:	An experienced thief with specialised equipment for burglary, who may be paid to perform the attack tries to access sensitive areas and manipulate or steal sensitive configuration items (confidentiality and/or integrity of Development Data, Development tools, Physical Assets).
T.Computer-Net:	A hacker with substantial expertise, standard equipment, who may be paid to attempt to remotely access sensitive network segments to get access to Development Data to compromise confidentiality and/or integrity or to access development tools to compromise the development process.
T.Unauthorised-Staff:	Employees or subcontractors not authorised to get access to assets such that the confidentiality and/or the integrity of the product is violated.
T.Staff-Collusion:	An attacker tries to get access to assets by gaining support from one employee through an attempted extortion or an attempt at bribery thereby compromising confidentiality and/or integrity of Development Data, Development tools and/or Physical Assets.

4.3 Organisational Security Policies

P.Config-Dev-Env — The development environment includes the use of Configuration Management Systems for file versioning (source code) and for Problem tracking (flaws and issues). Users are trained in the correct usage of such systems and must follow the proscribed procedures during development.

P.Lifecycle-Doc — This site uses life cycle documents that describe

- Configuration Management Systems and Use
- Configuration items List
- Design & Development Procedure
- Development tools
- Global Security Policy
- Secure Delivery Process / Data Transfer

P.Config-Activities — Activities shall be performed in accordance with the Lifycycle documentation (P.Lifecycle-Doc) using the Development Environment (P.Config-Dev-Env)

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

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

P.Product-Transport: — Technical and organisational 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 to protect the product during transport.

4.4 Assumptions

A.Inherit-Secure-IT: — Local IT equipment such as workstations is connected to a secure remote IT infrastructure by an encrypted secure network connection. The entire system (workstations, network and servers) is managed according to Rambus IT policies. The entire filesystem of local workstations is encrypted.

A.Project-Security — Rambus IT and/or Project Manager sets up access (user accounts) to project workspaces and the relevant configuration management resources (user access) at the creation of a project.

5 Security Objectives

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

O.Config-Dev-Env: The development environment includes the use of Configuration Management Systems for file versioning (source code) and for Problem tracking (flaws and issues). Users are trained in the correct usage of such systems and must follow the proscribed procedures during development.

O.Lifecycle-Doc: This site uses life cycle documents that describe:

- Configuration Management Capabilities
- Configuration Management Scope
- Delivery
- Development Security
- Lifecycle Definition
- Tools and Techniques

O.Config-Activities: Activities are performed in accordance with the Lifecycle documentation (P.Lifecycle-Doc) using the Development Environment (P.Config-Dev-Env)

O.Physical-Access: The combination of physical partitioning between the different access control levels together with technical and organizational security measures allows a sufficient separation of employees to enforce the “need to know” principle. The access control shall support the limitation for the access to these areas including the identification and rejection of unauthorized people. The access control measures ensure that only authorized registered employees can access restricted areas. Assets are handled in restricted areas only.

O.Security-Control: Assigned personnel of the site operate the systems for access control. After hour alarm monitoring and response is managed by Rambus through their owned and operated 24/7 Rapid Response Center (RRC). Technical security measures to include video monitoring and recording, glass break detection, door contacts, and motion sensors support the enforcement of the access controls. Rambus employees are responsible for registering and ensuring escort of visitors, contractors and suppliers.

O.Alarm-Response: The technical and organizational security measures ensure that an alarm is generated before an unauthorized person gets access to any sensitive configuration item (asset). After the alarm is triggered the unauthorized person still has to overcome further security measures. The reaction time of the employees or guards is short enough to prevent a successful attack. Details are described in [GSP]

O.Internal-Monitor: The Rambus Security Governance Leadership Committee (SGLC) meets regularly with the Rambus Operational Working Group (OWG) which meets quarterly. Together the SGLC and OWG are responsible for risk identification and ensuring appropriate security physical and logical controls, processes and procedures are implemented and maintained. These groups ensure that Rambus’s security posture is aligned with risk categories which are measured and reviewed on an annual basis. Furthermore, an internal audit is performed every year to control the application of the security measures.

O.Maintain-Security:	Technical security measures are maintained regularly to ensure correct operation. The logging of sensitive systems is checked regularly. This Includes monitoring and audit of 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. Logical-Access:	The site enforces a logical separation between the internal network and the internet by a firewall. The firewall ensures that only defined services and defined connections are accepted. Furthermore, the internal network is separated into a development network and an office network. Access to the development network and related systems is restricted to authorised employees that work in the related area or that are involved in the configuration tasks. Every user of an IT system has its own user account and password. An authentication using user account and password is enforced by all computer systems.
O. Logical-Operation:	All users have a unique username and authenticate using a password. All network segments and the computer systems are kept up-to-date (software updates, security patches, virus protection). The backup of sensitive data and security relevant logs is applied according to the classification of the stored data.
O. Staff-Engagement:	All employees who have access to assets are checked regarding security concerns and have to sign a non-disclosure agreement. Furthermore, all employees are trained and qualified for their job.
O. Transfer-Data:	Sensitive electronic configuration items (data or documents in electronic form) are protected with cryptographic algorithms to ensure confidentiality and integrity. The associated keys must be assigned to individuals to ensure that only authorised employees are able to extract the sensitive electronic configuration item. The keys are exchanged based on secure measures and they are sufficiently protected.
O. Control-Scrap:	The site has measures in place to destroy sensitive documentation, erase electronic media and destroy sensitive configuration items so that they do not support an attacker.

5.1 Security Objectives Rationale

The SST includes a Security Objectives Rationale with two parts. The first part includes a 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. Refer to ‘Rationale’ column in Table 1.

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.

Threat / OSP	Security Objective(s)	Rationale
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response to the threat
T.Rugged-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response to the threat
T.Computer-Net	O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Config-Dev-Env O.Staff-Engagement	The development network is not connected to anything that an attacker could use to set up a remote connection.
T.Unauthorised-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Config-Dev-Env O.Staff-Engagement O.Control-Scrap	Physical and logical access controls prohibit access to assets. Secure destruction of scrap limits the amount of assets
T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Transfer-Data O.Control-Scrap	The application of internal security measures combined with the hiring policies that restrict hiring to trustworthy employees limits unauthorized access to assets.
P.Config-Dev-Env	O.Config-Dev-Env	The security objective directly enforces the OSP
P.Lifecycle-Doc	O.Lifecycle-Doc O.Transfer-Data	The security objective directly enforces the OSP
P.Config-Activities	O.Config-Activities	The security objective directly enforces the OSP
P.Config-Items	O.Lifecycle-Doc	The security objective directly enforces the OSP
P.Config-Control	O.Lifecycle-Doc	The security objective directly enforces the OSP
P.Product-Transport	O.Transfer-Data	The security objective directly enforces the OSP

Table 1 Threats and OSP Security Objectives Rationale

6 Extended Assurance Components Definition

No extended components are currently defined in this SST template.

7 Security Assurance Requirements

Sites using this site security target require an evaluation against evaluation assurance level EAL4+.

The Security Assurance Requirements (SAR) are:

- CM Capabilities (ALC_CMC.4)
- CM Scope (ALC_CMS.4)
- Delivery (ALC_DEL.1)
- Development Security (ALC_DVS.2)
- Life-cycle Definition (ALC_LCD.1)
- Tools and Techniques (ALC_TAT.1)

The Security Assurance Requirements listed above fulfil the requirements of [4] because hierarchically higher components are used in this SST. In addition, the minimum set of SARs is extended by SAR of the assurance components for "Delivery" (ALC_DEL), "Life-cycle definition" (ALC_LCD.1) and "Tools and techniques" (ALC_TAT.1).

7.1 Application Notes and Refinements

The description of the site certification process [6] 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 SST the associated processes for the handling of products are in the focus and described in this SST. These processes are subject of the evaluation of the site.

7.1.1 CM Capabilities (ALC_CMC.4)

Refer to “Application Notes for Site Certification” in Section 5.1 (Application Notes for ALC_CMC) in [6]

7.1.2 CM Scope (ALC_CMS.4)

Refer to “Application Notes for Site Certification” in Section 5.2 (Application Notes for ALC_CMS) in [6]

7.1.3 Delivery (ALC_DEL.1)

Refer to Section 5.3 (Application Notes for ALC_DEL) in [6]

7.1.4 Development Security (ALC_DVS.2)

Refer to “Application Notes for Site Certification” in Section 5.4 (Application Notes for ALC_DEV) in [6]

7.1.5 Life-cycle Definition (ALC_LCD.1)

Refer to “Application Notes for Site Certification” in Section 5.6 (Application Notes for ALC_LCD) in [6]

7.1.6 Tools and Techniques (ALC_TAT.1)

Refer to “Application Notes for Site Certification” in Section 5.7 (Application Notes for ALC_TAT) in [6]

7.2 Security Requirements Rationale

7.2.1 Security Requirements Rationale – Dependencies

The dependencies for the assurance requirements are as follows:

- CM Capabilities (ALC_CMC.4): ALC_CMS.1, ALC_DVS.2, ALC_LCD.1
- CM Scope (ALC_CMS.4): None
- Delivery (ALC_DEL.1): None
- Development Security (ALC_DVS.2): None
- Life-cycle Definition (ALC_LCD.1): None
- Tools and Techniques (ALC_TAT.1): ADV_IMP.1

7.2.2 Security Requirements Rationale – Mapping

SAR	Security Objective	Rationale
ALC_CMC.4.1C: The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling	O.Config-Dev-Env O.Lifecycle-Doc O.Config-Activities	Appropriate and consistent labelling is ensured through the application (O.Config-Activities) of the CM Plan (O.Lifecycle-Doc) & the use of O.Config-Dev-Env
ALC_CMC.4.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.Lifecycle-Doc	The methods used to uniquely identify the configuration items are described in the CM Plan (O.Lifecycle-Doc)
ALC_CMC.4.3C: The CM system shall uniquely identify all configuration items.	O.Config-Dev-Env O.Lifecycle-Doc O.Config-Activities	Unique identification of all CIs is realized by performing the CM activities (O.Config-Activities) in accordance with the CM-Plan (O.LifeCycle-Doc)
ALC_CMC.4.4C: The CM system shall provide automated measures such that only authorised changes are made to the configuration items.	O.Config-Dev-Env O.Lifecycle-Doc O.Config-Activities	The configuration management systems (O.Config-Dev-Env) used (O.Config-Activities) according to the CM-Plan (O.LifeCycle-Doc) enforces automated measures (O.Logical-Access) such that only authorized changes are made to the configuration items.
ALC_CMC.4.5C: The CM system shall support the production of the product by automated means.	O.Config-Dev-Env O.Lifecycle-Doc O.Config-Activities	The software on the development computers (O.Config- Dev-Env) supports automated production of products when used (O.Config-Activities) in accordance with the CM-Plan (O.LifeCycle-Doc)
ALC_CMC.4.6C: The CM documentation shall include a CM plan.	O.Lifecycle-Doc	The life cycle documentation (O.Lifecycle-Doc) includes a CM Plan
ALC_CMC.4.7C: The CM plan shall describe how the CM system is used for the development of the product.	O.Lifecycle-Doc	The life cycle documentation (O.Lifecycle-Doc) describes how the CM system is used for the development of the product
ALC_CMC.4.8C: The CM plan shall describe the procedures used to accept modified or newly created configuration items (as part of the product).	O.Lifecycle-Doc	The acceptance procedures for modified or newly created configuration items are described in the CM-Plan (O.LifeCycle-Doc).
ALC_CMC.4.9C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.Lifecycle-Doc	All configuration items are listed in the Configuration Items list (O.LifeCycle-Doc)

ALC_CMC.4.10C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	O.Config-Dev-Env O.Lifecycle-Doc	The Configuration Item list (O.LifeCycle-Doc) is generated from the CM systems (O.Config-Dev-Env)

Table 2 Rationale for ALC_CMC.4

SAR	Security Objective	Rationale
ALC_CMS.4.1C: The configuration list shall include the following: clear instructions how to consider these items in the list; the evaluation evidence required by the SARs of the life-cycle; development and production tools and security flaw reports and resolution status.	O.Lifecycle-Doc	The life cycle documentation (O.Lifecycle-Doc) includes a CM-plan and a Configuration Item list
ALC_CMS.4.2C: The configuration list shall uniquely identify the configuration items.	O.Lifecycle-Doc	The Configuration Item list (O.Lifecycle-Doc) uniquely identifies the configuration items as described in the CM-Plan (O.Lifecycle-Doc)
ALC_CMS.4.3C: For each configuration item, the configuration list shall indicate the developer/subcontractor of the item.	O.Lifecycle-Doc	The Configuration Item list (O.Lifecycle-Doc) indicates the developer/subcontractor for each configuration item as described in the CM-Plan (O.Lifecycle-Doc)

Table 3 Rationale for ALC_CMS.4

SAR	Security Objective	Rationale
ALC_DEL.1.1C: The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.	O.LifeCycle-Doc O.Transfer-Data	All external deliveries are done according to the life cycle documentation (O.LifeCycle-Doc) supporting confidentiality and integrity (O.Transfer-Data).

Table 4 Rationale for ALC_DEL.1

SAR	Security Objective	Rationale
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	O.Lifecycle-Doc O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Control_Scrap O.Staff-Engagement O.Transfer_Data	The development security documentation (O.LifeCycle-Doc) describes the physical (O.Physical-Access, O.Security-Control, O.Alarm-Response); Procedural (O.Internal-Monitor, O.Maintain-Security, O.Control-Scrap); personnel (O.Staff-Engagement); and other(O.Logical-Access, O.Logical-Operation) 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 justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.	O.Lifecycle-Doc	The life cycle documentation (O.Lifecycle-Doc) justifies that the security measures do provide the necessary level of protection to maintain confidentiality and integrity of the TOE development and implementation.

Table 5 Rationale for ALC_DVS.2

SAR	Security Objective	Rationale
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.	O.Lifecycle-Doc	The model used to develop the intended TOE is described in the life cycle documentation (O.LifeCycle-Doc).
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.	O.Lifecycle-Doc	The life cycle documentation (O.Lifecycle-Doc) describes the controls over the development and maintenance the TOE

Table 6 Rationale for ALC_LCD.1

SAR	Security Objective	Rationale
ALC_TAT.1.1C: Each development tool used for implementation shall be well-defined.	O.Lifecycle-Doc	The model used to develop the intended TOE is described in the life cycle documentation (O.LifeCycle-Doc).
ALC_TAT.1.2C: The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.	O.Lifecycle-Doc	The life cycle documentation (O.Lifecycle-Doc) describes the controls over the development and maintenance the TOE
ALC_TAT.1.3C: The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.	O.Lifecycle-Doc	The life cycle documentation (O.Lifecycle-Doc) describes the controls over the development and maintenance the TOE

Table 7 Rationale for ALC_TAT.1

8 Site Summary Specification

8.1 Preconditions Required by the Site

Site activities are performed using IT equipment and infrastructure (workstations, servers, configuration management systems) controlled by Rambus.

Remote workstations are purchased, configured, controlled, and maintained by Rambus and are connected using an encrypted link. The workstations employ full disk encryption.

Account setup, access permissions, tools and their usage, is set up and controlled by Rambus.

Applicable policies are in place and available.

Physical assets are securely destroyed.

8.2 Services of the Site

The following services are provided by the site:

- Development of IP and associated software for integration within a consumer's secure IC
- Development environment
- CM System administration
- Generation and delivery of the product
- An appropriate space for evaluation of IPs and software as part of the development procedures.

8.3 Objectives Rationale

The following rationale provides a justification that shows that all threats and OSP are effectively addressed by the Security Objectives.

8.3.1 O.Physical-Access

Access to Rambus spaces is controlled by Access Control System, Intrusion Detection System, Video Surveillance System (CCTV) and a Master Key System. Access to Rambus occupied spaces is only possible through staffed Reception Areas which include access-controlled doors and turnstiles. Rambus occupied space is monitored 24/7 by a Rambus Rapid Response Centre (RRC). The physical, technical and organizational security measures ensure a separation of the site into 3 security levels, Site Perimeter, Internal Perimeter, and Restricted Area. The access control measures ensure only registered/authorized persons can gain access to sensitive areas. This is supported by O.Security Control that includes maintenance of the access control and the control of visitors. The physical security measures are supported by O.Alarm-Response that includes providing in person response to any alarm system activation.

Thereby, the threats T.Smart-Theft, T.Rugged-Theft can be prevented. The physical security measures together with the security measure provided by O.Security-Control enforce the recording of all actions. Thereby also T.Unauthorized-Staff is addressed.

8.3.2 O.Security-Control

Outside business hours, guards patrol the perimeter with the alarm system and motion sensors being activated. The CCTV system is always active. Security control is further supported by O.Physical-Access and O.Alarm Response.

Thereby, the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorized-Staff are addressed.

8.3.3 O.Alarm-Response

The alarm system is connected to a 24/7 Rambus Rapid Response Centre (RRC). O.Physical-Access requires a certain time to overcome the access control.

Thereby, the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorized-Staff are addressed.

8.3.4 O.Internal-Monitor

Regular security management meetings are scheduled to review the established security measures.

Thereby, the threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion are addressed.

8.3.5 O.Maintain-Security

The security relevant systems enforcing O.Physical-Access, O.Security-Control and O.Logical-Access are checked regularly and maintained by suppliers.

Thereby, the threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion are addressed.

8.3.6 O.Logical-Access

The internal network is separated from the internet by a firewall. The internal network is sub-divided by internal firewalls. Access to internal networks / sub-networks is only possible by authorized users. Rambus maintains the access lists.

Thereby, the threats T.Computer-Net and T.Unauthorised-Staff are addressed.

8.3.7 O.Logical-Operation

All logical protection measures are maintained and updated regularly by Rambus.

Thereby, the threats T.Computer-Net and T.Unauthorised-Staff are addressed.

8.3.8 O.Config-Dev-Env

Logical protection measures are maintained and updated as required. SVN and Perforce version control systems are used to control source code thereby enabling unique identification of assets. JIRA is used to manage bugs and issues.

Thereby, T.Computer-Net, T.Unauthorised-Staff and P.Config-Dev-Env are addressed

8.3.9 O.Config-Activities

All configuration items relating to the product are uniquely identified. Products are uniquely identified by customer part numbers that link to the configuration items. Specifications, procedures and process documents are stored in a Document Control Management System.

Thereby, P.Config-Activities is addressed.

8.3.10 O.Staff-Engagement

Prior to hiring, staff are interviewed. All employees sign an NDA and code of conduct when hired. Further they must undergo initial security awareness training which is repeated annually thereafter.

Thereby, T.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion are addressed.

8.3.11 O.Transfer-Data

Product deliveries are managed by authorized individuals (e.g., Program Manager). All data is encrypted and provided to the consumer via a dedicated management system accessible by authorized individuals. Notifications of deliveries are automated. Log files are available detailing the delivery and reception.

Thereby, T.Staff-Collusion, P.Lifecycle-Doc and P.Product-Transport are addressed.

8.3.12 O.Control-Scrap

Scrap in the form of printed documentation or electronic media are securely destroyed.

Thereby, T.Unauthorised-Staff and T.Staff-Collusion are addressed.

8.3.13 O.Lifecycle-Doc

The security of the site is maintained according to Rambus security documentation that covers all physical and logical measures. The product is developed and delivered according to Design & Development Procedure and Secure Delivery Process respectively.

Thereby, P.Lifecycle-Doc, P.Config-Items and P.Config-Control are addressed.

8.4 Security Assurance Requirements Rationale

8.4.1 CM Capabilities (ALC_CMC.4)

Configuration management is described in Rambus ALC Overview [ALC] which references SVN and Perforce usage documents.

8.4.2 CM Scope (ALC_CMS.4)

Configuration management is described in Rambus ALC Overview [ALC] which references SVN and Perforce usage documents.

8.4.3 Delivery (ALC_DEL.1)

The delivery process is described in Rambus ALC Overview and in “Secure Data Handling Requirements for Intellectual Property and Information” (Doc No 000425, located in DCMS).

8.4.4 Development Security (ALC_DVS.2)

Development Security is described in Rambus ALC Overview [ALC]

8.4.5 Lifecycle Definition (ALC_LCD.1)

Lifecycle Definition is described in Rambus ALC Life Cycle Model [LCM]

8.4.6 Tools and Techniques (ALC_TAT.1)

Tools are listed in the HW and SW Tool Lists [TAT]

8.5 Assurance Measure Rationale

8.5.1 O.Physical-Access

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

8.5.2 O.Security-Control

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

8.5.3 O.Alarm-Response

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

8.5.4 O.Internal-Monitor

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

8.5.5 O.Maintain-Security

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

8.5.6 O.Logical-Access

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and

implementation including the initialization in its development and production environment. Thereby this objective is suitable to meet the Security Assurance Requirement.

8.5.7 O.Logical-Operation

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

8.5.8 O.Config-Dev-Env

ALC_CMC.4.1C requires a documented process ensuring an appropriate and consistent labelling of the products.

ALC_CMC.4.2.C requires that a CM System that can uniquely identify the configuration items is used.

ALC_CMC.4.3C requires that the CM system uniquely identifies all configuration items.

The configuration list required by ALC_CMS.4.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information.

ALC_CMS.4.2C addresses the same requirement as ALC_CMC.4.3C.

In addition, ALC_LCD.1.1C requires that the life-cycle definition documentation describes the model used to develop and maintain the products. The objective meets the set of Security Assurance Requirements.

8.5.9 O.Config-Activities

ALC_CMC.4.1C requires a documented process ensuring an appropriate and consistent labelling of the products.

ALC_CMC.4.2C requires that a CM System that can uniquely identify the configuration items is used.

ALC_CMC.4.3C requires that the CM system uniquely identifies all configuration items.

The configuration list required by ALC_CMS.4.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information.

ALC_CMS.4.2C addresses the same requirement as ALC_CMC.4.3C.

In addition, ALC_LCD.1.1C requires that the life-cycle definition documentation describes the model used to develop and maintain the products. The objective meets the set of Security Assurance Requirements.

8.5.10 O.Staff-Engagement

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

8.5.11 O.Transfer-Data

ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this objective is suitable to meet the Security Assurance Requirement.

8.5.12 O.Control-Scrap

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

8.5.13 O.Lifecycle-Doc

ALC_CMC.4.1C requires that CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling

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

ALC_CMC.4.3C requires that CM system shall uniquely identify all configuration items.

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

ALC_CMC.4.5C requires that CM system shall support the production of the product by automated means.

ALC_CMC.4.6C requires that CM documentation shall include a CM plan.

ALC_CMC.4.7C requires that CM plan shall describe how the CM system is used for the development of the product.

ALC_CMC.4.8C requires that CM plan shall describe the procedures used to accept modified or newly created configuration items (as part of the product).

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

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

ALC_CMS.4.1C requires that configuration list shall include the following: clear instructions how to consider these items in the list; the evaluation evidence required by the SARs of the life-cycle; development and production tools and security flaw reports and resolution status.

ALC_CMS.4.2C requires that configuration list shall uniquely identify the configuration items.

ALC_CMS.4.3C: For each configuration item, the configuration list shall indicate the developer/subcontractor of the item.

ALC_DEL.1.1C requires that delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

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

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

ALC_LCD.1.1C requires that life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C requires that life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

ALC_TAT.1.1C: Each development tool used for implementation shall be well-defined.

ALC_TAT.1.2C requires that documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.1.3C requires that documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

8.6 Mapping of the Evaluation Documentation

The scope of the evaluation according to the assurance class ALC_CMS comprises the security products, the complete documentation of the site provided for the evaluation. The specifications and descriptions provided by the client are not part of the configuration management at Rambus Headquarters.

SAR	Aspects	Reference
ALC_CMC.4.1C: The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.	Sources are labelled in the CM system (SVN or Perforce). The version control system is used per O.Config-Dev-Env. Documents are labelled with Title & Document Number. Document Numbers and Part Numbers are assigned by the Part & Document Numbering issuer Configuration items are identified by the system automatically in conjunction with the product.	Refer to [ALC] for Configuration management system information Refer to [DDP] for details of Product and Document numbering
ALC_CMC.4.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	Sources are uniquely identified in the CM system (SVN or Perforce). The documentation can be uniquely identified by the Document Title and Document Number. Document Numbers and Part Numbers are assigned by the Part & Document Numbering issuer Configuration items are identified by the system automatically in conjunction with the product.	Refer to [ALC] for Configuration management system information Refer to [DDP] for details of Product and Document numbering
ALC_CMC.4.3C: The CM system shall uniquely identify all configuration items.	All configuration items can be uniquely identified by the CM system (SVN or Perforce)	Refer to [ALC] for Configuration management system information Refer to [DDP] for details of Product and Document numbering
ALC_CMC.4.4C: The CM system shall provide automated measures such that only authorised changes are made to the configuration items.	CM tools (SVN and Perforce) provide automated measures to only allow authorized changes to the configuration items. Access to and use of the CM tools is restricted to authorized users.	Refer to [ALC] for Configuration management system information Refer to [DDP] for details of Product and Document numbering
ALC_CMC.4.5C: The CM system shall support the production of the product by automated means.	CM tools (SVN and Perforce) support the development of the product by automated means	Refer to [ALC] for Configuration management system information Refer to [DDP] for details of Product and Document numbering
ALC_CMC.4.6C: The CM documentation shall include a CM plan.	The development environment is set up with a CM plan for each product	Refer to [ALC] for Configuration management system information Product specific CM plan is available.
ALC_CMC.4.7C: The CM plan shall describe how the CM system is used for the development of the product.	The CM plan is project specific within the development environment	Refer to [ALC] for Configuration management system information Refer to [DDP] for product development stages. Product specific CM plan is available.

ALC_CMC.4.8C: The CM plan shall describe the procedures used to accept modified or newly created configuration items (as part of the product).	The CM plan is project specific within the development environment Documentation is managed by engineering after creation by the Part & Document Numbering issuer	Refer to [ALC] for Configuration management system information Refer to [DDP] for product development stages and Product and Document numbering
ALC_CMC.4.9C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	Evidence can be provided during site audit.	The development environment is set up centrally and organized per the product specific CM plan.
ALC_CMC.4.10C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	Evidence can be provided during site audit.	The development environment is set up centrally and organized per the product specific CM plan. Refer to [ALC] for Configuration management system information

Table 7 Mapping of the Evidence for ALC_CMC.4

SAR	Aspects	Reference
ALC_CMS.4.1C: The configuration list shall include the following: clear instructions how to consider these items in the list; the evaluation evidence required by the SARs of the life-cycle; development and production tools and security flaw reports and resolution status.	There is no TOE for a site certification; the list of evidence is in this document. Applicable documents are listed	The list of evidence is contained in [SST] The list of deliverables is described in [EDL]
ALC_CMS.4.2C: The configuration list shall uniquely identify the configuration items.	All configuration items are maintained in the CM systems. All documents can be uniquely identified	All configuration items are uniquely identified in [EDL]
ALC_CMS.4.3C: For each configuration item, the configuration list shall indicate the developer/subcontractor of the item.	The CM system records the developer who contributed to the development. All documents have an author listed	The developer of each configuration item can be identified [SST]. [EDL]

Table 8 Mapping of Evidence for ALC_CMS.4

SAR	Aspects	Reference
ALC_DEL.1.1C: The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.	The delivery document describes the process for delivery	Secure delivery process is described in [DEL]

Table 9 Mapping of Evidence for ALC_DEL.1

SAR	Aspects	Reference
ALC_DVS.2.1C: The development security documentation shall	Access control, CCTV, alarm system prevent access to unauthorized personnel.	All security measures are described in [GSP]

describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment	Tracing and control of visitors	All security measures are described in [GSP]
	Trustworthiness and training of employees	All security measures are described in [GSP]
ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the intended TOE.	This [SST] provides justification for the measures in place to maintain the confidentiality and integrity of the intended TOE	All information is in [SST]

Table 10 Mapping of Evidence for ALC_DVS.2

SAR	Aspects	Reference
ALC_LCD.1.1C: The life cycle definition documentation shall describe the model used to develop and maintain the intended TOE.	The product is developed according to Rambus development procedure	The development procedure is described in [DDP]
ALC_LCD.1.2C: The life cycle model shall provide for the necessary control over the development and maintenance of the intended TOE.	Rambus Development procedure	The development procedure is described in [DDP]

Table 11 Mapping of Evidence for ALC_LCD.1

SAR	Aspects	Reference
ALC_TAT.1.1C: Each development tool used for implementation shall be well-defined.	The product is developed according to Rambus development procedure	The development procedure is described in [DDP]
ALC_TAT.1.2C: The documentation for each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.	The product is developed according to Rambus development procedure	The development procedure is described in [DDP]
ALC_TAT.1.3C: The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.	The product is developed according to Rambus development procedure	The development procedure is described in [DDP]

Table 12 Mapping of Evidence for ALC_TAT.1

9 References

9.1 Literature

Site Security Target Template, Version 1.0, published by Eurosmart,“ Eurosmart, 21.06.2009

Ref	Description
[1]	Site Security Target Template; Version 1.0, Eurosmart, 21.06.2009
[2]	Common Criteria for Information Technology Security Evaluations, Part 1: Introduction and General Model; Version 3.1, Revision 5, April 2017
[3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017
[4]	Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 5, April 2017
[5]	JIL Minimum Site Security Requirements Version 3.0, February 2020
[6]	Supporting Document Guidance, Site Certification, October 2007, Version 1.0, Revision 1, CCDB-2007-11-001

9.2 Internal References

Ref	Description	Version	Location
[DEL]	Secure Data Handling Requirements for Intellectual Property and Information (spec 425)	D	DCMS
[DDP]	Design and Development Procedure (Spec 367)	C	DCMS
[SPEC-139]	Access control policy	D	DCMS
[SPEC-168]	Installation, Configuration & Maintenance of Firewalls	B	DCMS
[SPEC-172]	Disposal of Media	D	DCMS
[SPEC-175]	Network Security Management Procedure	D	DCMS
[SPEC-188]	Cryptographic Control Policy, Latest version	C	DCMS
[SPEC-210]	User Registration Procedure	F	DCMS
[SPEC-259]	Acceptable Use Policy – US & Non-EU	C	DCMS
[ALC]	Rambus ALC Overview	0.2	SharePoint
[LCM]	Rambus LifeCycle Model	0.2	SharePoint
[TAT]	HW_Tool_List SW_Tool_List	Latest	SharePoint
[SST]	This document	G	SharePoint

[EDL]	Evidence Document List	B	SharePoint
[GSP]	Rambus Global Security Policy	C	DCMS