CRYPTO
Part of Fox-IT

CLASSIFICATION
PUBLIC

Site Security Target Lite

Fox Crypto SkyTale development site

Date	19 February 2025
Reference	Fox-SST-20220140-2023
Principal	Fox Crypto B.V.
	Olof Palmestraat 6 2616 LM Delft
Author(s)	Ellen Wesselingh
Version	1.5

FOR A MORE SECURE SOCIETY

DOCUMENT CLASSIFICATION

This document is classified as *PUBLIC*. Any information published in this document and its appendices is intended exclusively for the addressee(s) as listed on the document management distribution list. Only these addressee(s) and additional persons explicitly granted permissions by any of these originally authorized addressee(s) may read this document. Any use by a party other than the addressee(s) is prohibited. The information contained in this document may be *PUBLIC* in nature and fall under a pledge of secrecy.

If your name is not listed on the document management page or if you have not obtained the appropriate (written) authorization to read this document from an authorized addressee, you should close this document immediately and return it to its original owner.

Misuse of this document or any of its information is prohibited and will be prosecuted to the maximum penalty possible. Fox Crypto cannot be held responsible for any misconduct or malicious use of this document by a third party or damage caused by its contained information.

Fox Crypto B.V.

Olof Palmestraat 6
2616 LM Delft
P.O. Box 638
2600 AP Delft
The Netherlands

T +31 (0)15 284 79 99
F +31 (0)15 284 79 90
crypto@fox-crypto.com
www.fox-crypto.com

Copyright © Fox Crypto B.V.

All rights reserved. Nothing in this publication may be reproduced, stored in a computer database or made public in any form or manner, be it electronic, mechanical, by photocopying, with a recording device or in any other way whatsoever, without previous written permission of Fox Crypto B.V.

Trademark

Fox Crypto and the logo of Fox Crypto are trademarks of Fox Crypto B.V.
All other trademarks included in this document are the property of the indicated organisations.

Document management

Version management	
Case name	Fox Crypto SkyTale development site
Reference	Fox-SST-20220140-2023
Principal	Fox Crypto B.V.
Subject	Report
Date	19 February 2025
Version	1.5
Status	Final
Author(s)	Ellen Wesselingh

Management summary & reading guide

This document is the Site Security Target, it describes the development security measures to provide assurance about the confidentiality and integrity for all TOE parts and TOEs under development.

Chapter 1 ASE_INT: Introduction identifies the site and describes the site in general terms.

Chapter 2 ASE_CCL: Conformance claims describes to which Common Criteria version conformance is claimed, and the scope (breadth and depth) of the claims. Currently all assurance class Life Cycle Definition (ALC_LCD) are in scope.

Chapter 3 ASE_SPD: Security Problem Definition describes the assets that are to be protected, the threats against which the assets have to protected, and the organisational policies and assumptions together provide an adequate level of protection.

Chapter 4 ASE_OBJ: Security Objectives defines the objectives and provides proof that the objectives completely cover the threats and organisational policies.

Chapter 5 ASE_ECD: Extended Assurance Components Definition claims no extended assurance components.

Chapter 6 ASE_REQ: Security Assurance Requirements describes all the Common Criteria assurance components that are claimed and provides proof that the objectives completely cover the assurance components.

Chapter 7 ASE_TSS: Site Summary Specification shows which assurance class Life Cycle Definition (ALC) families are covered.

Terms and abbreviations

C

CC	Common Criteria

E

ENISA	European Union Agency for Cybersecurity. Maintainer of the EU Common Criteria scheme (https://certification.enise.europa.eu/)

J

JIL	Joint Interpretation Library. An expert group under SOG-IS, that provides specialised additional guidance on specific topics.

S

SOG-IS	Senior Officials Group Information Systems Security (https://www.sogis.eu/)
SST	Site Security Target (lite). This is a generalised version of the full Security Target.

T

TOE	Target of Evaluation

Table of Contents

1 ASE_INT: Introduction

This Site Security Target describes the security practices during SkyTale development on the Fox Crypto B.V. site located in Delft, Netherlands. The Site Security Target will be referred as SST hereafter.

1.1 SST and Site Identification

This SST lays down the claim for a Common Criteria for Information Technology Security Evaluation of the development site, located in Delft, Netherlands. The Common Criteria for Information Technology Security Evaluation will be referred to as CC hereafter.

This section describes the location of the Fox Crypto SkyTale development site, and provides a general overview of the business operations and the confidential information handled there.

Table 1: SST identification

SST attribute	Value
Name	Site Security Target Fox Crypto SkyTale development site
Version	1.5
Reference	Fox-SST-20220140-2023
Issue Date	19 February 2025

Table 2: Site identification

Site attribute	Value
Company	Fox Crypto B.V.
Name of the site	Fox Crypto SkyTale development
Location	Olof Palmestraat 6, 2616 LM Delft

1.2 Physical scope of the site

The site is located inside the building on the first, second and third floors. The building is occupied by Fox-IT B.V. and Fox Crypto B.V., both subsidiaries from Fox-IT Group B.V..

The whole building is jointly security controlled by Fox-IT B.V. and Fox Crypto B.V., the development rooms are security controlled by Fox Crypto B.V.. Only authorised persons are allowed to enter the building. Further authorisation is required to enter the development rooms.

1.3 Logical scope of the site

The site is used by Fox Crypto B.V. for development of security hardware and (embedded) software. Development servers, dedicated development network and developer systems are all located in the development rooms. There is no remote access to the development environment.

Configuration management is managed centrally from a configuration management server. An overall measurable Life Cycle Model is used, that is further detailed on development team level. The activities on site are conformant to the phases of the composite product as defined in Protection Profile (PP) BSI-PP-0084 [Ref:1] . Phases that are ***not*** part of the scope are presented in strikethrough font.

Phase 1: IC (Composite) Embedded Software Development

Phase 2: IC (System Hardware) Development

~~Phase 3: IC (Composite) Manufacturing~~

~~Phase 4: IC Packaging~~

~~Phase 5: Composite Product Integration~~

~~Phase 6: Personalisation~~

The SkyTale product range does not consist of IC development, therefore the "IC" term must be omitted from the above listed phases. Phase 4 must be understood as production of a system consisting of hardware, firmware, and software.

As personalisation is done on the site of the customer, and Delivery (ALC_DEL) is not claimed, personalisation is not part of the claim.

1.4 Assets and Common Criteria classification

Table 3: mapping assets to Common Criteria categories

Asset	CC
• Cryptographic materials	• Critical
• Design documentation	• Sensitive
• Risk analysis, vulnerability analysis	• Critical
• Verification documentation (external testing)	• Critical
• Development tools and samples	• Sensitive
• Guidance documentation	• Restricted
• Hardware (prototype)	• Critical
• Hardware (0-series / production)	• Critical
• (product specific) Security policies and procedures	• Sensitive
• Source code	• Critical

1.5 Compartments and activities

Development rooms are located on the first, second and third floor of the site. Development activities are compartmentalized by function:

- server rooms (first and second floor)
- meeting rooms (1B wing and third floor)
- CCI storage (third floor)
- security, quality and compliance (2A wing)
- architecture (third floor)
- hardware engineering (third floor)
- FPGA engineering (third floor)
- software engineering (third floor)
- production engineering (1B wing)
- climate testing (third floor)
- consultancy delivery and support, sales (2A wing)

2 ASE_CCL: Conformance claims

This Site Security Target claims conformance to the following standard:

1 Common Criteria for Information Technology Security Evaluation, Version 3.1 Release 5, Parts 1 [Ref:2] and 3 [Ref:3] .

2.1 Evaluation methodology

Meth 1. Common Methodology for Information Technology Security Evaluation, Version 3.1, Release 5 [Ref:4]

Meth 2. Supporting Document Guidance, Site Certification CCDB-2007-11-001, Version 1.0, Revision 1 [Ref:5]

Meth 3. Joint Interpretation Library. Minimum Site Security Requirements, Version 3.1 [Ref:3],[Ref:6] or EUCC SCHEME STATE-OF-THE-ART DOCUMENT. Minimum Site Security Requirements, Version 1.1

As this evaluation is intended to be used for future product evaluations, the Cyber Security Act and the EUCC defining document apply [Ref:7],[Ref:8] .

2.2 Package conformance claim

This Site Security Target claims conformance to the following assurance components:

CnfCl 1. ALC_CMC.5

CnfCl 2. ALC_CMS.5

CnfCl 3. ALC_DVS.2

CnfCl 4. ALC_FLR.3

CnfCl 5. ALC_LCD.2

CnfCl 6. ALC_TAT.3

This is commensurate with EAL 7 augmented with ALC_FLR.3.

2.3 Package claim rationale

The chosen assurance components are derived from the assurance level EAL7 of the assurance class "Life-cycle Support". For the assessment of the security measures, attackers with high attack potential are assumed. Therefore, this site supports product evaluations up to EAL7.

3 ASE_SPD: Security Problem Definition

The security problem definition describes the assets handled at the development site, and the threats against those assets. The organisational security policies and assumptions to counter the threats are elaborated.

3.1 Assets

The assets (sensitive configuration items) handled at the site are:

- Cryptographic materials
- Design documentation
- Development tools and samples
- Guidance documentation
- Hardware
- (product specific) Security policies and procedures
- Source code

3.2 Threats

All threats are described in terms of a threat agent, an asset, and an adverse action. The threats to the assets are defined as follows:

T.LOGIC-THEFT

An attacker with high attack potential, access to bespoke hacker tooling, is highly skilled in hacking and has sufficient time, tries to enter the development IT systems to compromise the confidentiality and / or integrity and /or availability of the assets.

T.PHYSICAL-THEFT

An attacker with high attack potential, access to bespoke burglary tooling, elaborate social engineering skills and sufficient time tries to physically enter the development rooms and steal assets present, thus compromising the confidentiality and / or integrity and /or availability of the assets.

T.STAFF-ATTACK

An attacker with high attack potential tries to manipulate personnel into compromising the confidentiality and / or integrity and / or availability of the assets. This threat includes an attack by an insider threat.

T.STAFF-MISTAKE

A legitimate staff member accidentally changes one or more assets by mistake, thus compromising the confidentiality and / or integrity and /or availability of the assets.

T.TRANSPORT-ATTACK

An attacker with high attack potential tries to steal or compromise assets during transport to or from a subcontractor, or during transport to the customer. This may compromise the confidentiality and / or integrity and /or availability of the assets.

3.3 Organisational Security Policies

The organisational policies to support the confidentiality, integrity and availability of assets are shown in table 3 [Ref:3],[Ref:6] . For efficiency reasons table 3 also shows that all Organisational Security Policies [1] are enforced by at least one Security Objective, showing a direct mapping to ref [Ref:3],[Ref:6] .

Table 3: Organisational Policies

Objective [2]		Covered by policy(policies)
O.DSS	P.DSD.1	The evaluation evidence for the evaluation of development security is the ST and the development security documentation (DSD). Therefore, the developer has to establish, implement, operate, monitor, maintain, review, and improve a documented development security system (DSS) within the context of the organization's overall business activities and the risks it faces.
	P.DSD.2	The DSD shall document and the evaluator shall examine the development confidentiality and integrity policies that detail - what information relating to the TOE development needs to be kept confidential, and which members of the development staff are allowed to access such material; - what material must be protected from unauthorised modification in order to preserve the integrity of the TOE, and which members of the development staff are allowed to modify such material.
	P.DSD.3	Policies shall contain a description of developers organization, relevant roles, and the security measures implemented. According to ALC_DVS the following types of security measures shall be considered for documentation - Physical, e.g. access control and intrusion detection - Procedural, e.g. granting and revoking access rights, transfer of protected material, roles and responsibilities for security personnel - Personnel, e.g. check of trustworthiness - Other security measures, e.g. logical protection of any development machines
O.MANAGEMENT	P.MANAGEMENT	The overall Security Policy shall define developer's approach to security and the area of applicability. It shall establish an overall sense of direction and principles for action with regard to confidentiality and integrity needs of the TOE.
O.AUDIT	P.AUDIT	The responsibilities and requirements for planning and conducting audits, for reporting results, and maintaining records shall be defined in a documented procedure.
O.REVIEW	P.REVIEW	The management review process should be documented.
O.IMPROVE	P.IMPROVE	Policies shall define how effectiveness of security measures is maintained despite evolving threats and in consideration of possible deficiencies.
O.ASSET-MGT	P.ASSET-MGT.1	DSD should define ownership and management of all assets.

1: All policies taken from [Ref:3],[Ref:6] , except P.LIFECYCLE.
2: Objectives are introduced in chapter 4.

	P.ASSET-MGT.2	Rules for the acceptable use of information and assets should be identified and documented in line with the classification policies.
	P.ASSET-MGT.3	The developer shall have a classification policy.
	P.ASSET-MGT.4	The developer shall have predefined labelling and handling procedures for all used combinations of defined levels and information, data, and material implemented in accordance with the classification scheme adopted by the organization.
	P.ASSET-MGT.5	The developer shall have predefined handling procedures for all important assets in line with protection needs.
	P.ASSET-MGT.6	Approach to and deployment of configuration management shall be defined in a policy.
	P.ASSET-MGT.7	Whenever parts of the TOE are imported from external sources, import procedures should define how developer enforces integrity and authenticity of the imported parts.
O.HR	P.HR.1	DSD shall include policies for hiring and onboarding which ensure careful selection of trustworthy staff.
	P.HR.2	The developer shall have documents defining security roles and responsibilities of employees, contractors and third party users, in accordance with the organization's security policy (e.g. in job descriptions, project plans, contracts etc).
	P.HR.3	The approach to regular awareness training should be defined in a policy.
	P.HR.4	A policy should define monitoring measures implemented in order to detect irregular behaviour in line with local legislation.
	P.HR.5	The developer shall have appropriate procedures for employment termination and change of job, including revocation of access rights.
O.PHYSICAL	P.PHYSICAL.1	A security policies shall define the two layer security concept and detail the concerted function of the two layers.
	P.PHYSICAL.2	An access control policy shall be in place, including regulations for visitors and contractors. Access shall only be granted on a need-to-know basis.
	P.PHYSICAL.3	A policy shall define access regulations for service functions, e.g. housekeeping, facility management, cleaning staff.
	P.PHYSICAL.4	Where applicable, policies shall detail access rights for officials and supporting forces, e.g.rfire fighters.
	P.PHYSICAL.5	A Policy shall detail measures implemented to ensure detection and prevention of unauthorised access to offices, rooms, and facilities. This shall include clear security procedures and safety regulations as well as - where applicable - outsourcing.
	P.PHYSICAL.6	A disaster prevention and recovery policy is required, detailing the measures implemented to protect the TOE.
	P.PHYSICAL.7	An access control policy based on need-to-know principle shall be developed, implemented, and maintained.
	P.PHYSICAL.8	The security policy shall consider that the design and layout of sites and premises should avoid high security areas next to public areas.

	P.PHYSICAL.9	The security policy shall include a visitor regulation which has to be established, documented, and reviewed based on security requirements for access.
	P.PHYSICAL.10	The security policy shall (if applicable) define measures to ensure that TOE components shall be protected against tampering or theft during transit between physically separate secure areas. Measures during transit shall correspond to the confidentiality and integrity classification.
	P.PHYSICAL.11	A policy shall define handling and placing of security relevant equipment in order to protect against failures which could affect availability of those equipment, and interception or damage.
O.OPERATION	P.OPERATION.1	Operating procedures shall be documented, maintained, and made available to all users who need them.
	P.OPERATION.2	Formal management responsibilities and procedures should be in place to ensure satisfactory control of equipment, software, or procedures, and all related changes.
	P.OPERATION.3	A procedure shall define the level of separation between development, test and operational environments, and describe the controls implemented.
	P.OPERATION.4	Contract and vendor management policies shall define roles and responsibilities for managing the relationship with third parties.
	P.OPERATION.5	A planning process for communication and operation systems shall be defined and documented.
	P.OPERATION.6	Test procedures and acceptance criteria for new processing systems, upgrades, and new versions shall be established.
	P.OPERATION.7	A policy shall prohibit the use of unauthorized software.
	P.OPERATION.8	A policy shall define compulsory protective measures to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium.
	P.OPERATION.9	Management procedures and responsibilities shall be defined for malicious code protection on systems, including training in their use, alerting, reporting, and recovering from malicious code attacks.
	P.OPERATION.10	A security policy shall define authorized mobile code operations.
	P.OPERATION.11	A documented procedure approved by the Security Manager shall define secure back-up creation, storage, and destruction operations, ensuring the same level of security as for the original data.
	P.OPERATION.12	Developer shall specify network security in terms of network architecture and preventive and detective measures.
	P.OPERATION.13	A policy shall restrict network traffic through the entry point into the development area's network to its minimum.
	P.OPERATION.14	Appropriate operating procedures should be established to protect documents, computer media, mobile devices, input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction.
	P.OPERATION.15	Where confidentiality and/or integrity are required, procedures shall be in place for the management of removable media.

	P.OPERATION.16	All procedures and authorization levels should be clearly documented.
	P.OPERATION.17	Formal procedures for the secure disposal of media shall minimize the risk of sensitive information leakage to unauthorized persons. The procedures for secure disposal of media containing classified information should be commensurate with the classification of that information.
	P.OPERATION.18	Formal exchange policies, procedures, and measures shall be defined and deployed in order to protect the exchange of information through the use of all types of communication facilities.
	P.OPERATION.19	A policy shall detail monitoring measures, particularly logging and assessment of log files.
O.ACCESS-CONTROL	P.ACCESS-CONTROL.1	An access control policy shall be established, documented, and regularly reviewed based on business requirements (security needs to protect confidentiality and/or integrity of TOE) for access. This policy shall detail access control rules for every role (user or group of users).
	P.ACCESS-CONTROL.2	A policy regarding user access management shall be established and documented. It details how access rights and privileges are granted and the roles used.
	P.ACCESS-CONTROL.3	A policy regarding password quality shall be established and documented.
	P.ACCESS-CONTROL.4	A policy shall detail users responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.
	P.ACCESS-CONTROL.5	A password policy shall require users to follow good security practices in the selection and use of passwords.
	P.ACCESS-CONTROL.6	A policy regarding network access management shall be established and documented. It details the network architecture, network connections, network access control and other security measures.
	P.ACCESS-CONTROL.7	Dedicated processes and guidelines for business partner access and interconnections with/to business partners shall be defined and documented.
	P.ACCESS-CONTROL.8	A policy shall be established and documented describing the measures taken to prevent unauthorized access to operating systems.
	P.ACCESS-CONTROL.9	A policy shall detail the measures taken to restrict access to applications and information, and to isolate systems with sensitive, critical, or very critical content.
	P.ACCESS-CONTROL.10	A policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing (laptop, handheld devices) and communication facilities (smart phones etc.).
	P.ACCESS-CONTROL.11	A policy, operational plans and procedures shall be developed and implemented for remote access and teleworking activities if applicable.
O.INFORMATION-SYSTEMS	P.INFORMATION-SYSTEMS.1	A procurement policy should define the steps necessary to mitigate risks from IT systems (HW and SW) in use.
	P.INFORMATION-SYSTEMS.2	Software development, implementation, and utilization of applications developed by or on behalf of developer should be detailed.

	P.INFORMATION-SYSTEMS.3	Installation and verification of off-the-shelf products should be defined.
	P.INFORMATION-SYSTEMS.4	A policy shall detail measures implemented to ensure integrity and authenticity of data related to the TOE or to proper operation of security systems.
	P.INFORMATION-SYSTEMS.5	A policy on the use of cryptographic controls for protecting information shall be developed, implemented and maintained.
	P.INFORMATION-SYSTEMS.6	Administrator rights shall be regulated in a policy describing how they are granted, monitored, and revoked.
	P.INFORMATION-SYSTEMS.7	Access for vendors and service partners shall be detailed in a policy.
	P.INFORMATION-SYSTEMS.8	A policy shall define installation of software on operational systems, including developers approach to updates and patches.
	P.INFORMATION-SYSTEMS.9	A policy shall describe generation and utilization of test data, where applicable.
	P.INFORMATION-SYSTEMS.10	The release process for development applications and tools shall be documented.
	P.INFORMATION-SYSTEMS.11	A change management policy shall be defined and effective.
	P.INFORMATION-SYSTEMS.12	Perpetuation of confidentiality across applications, tools, and networks shall be documented.
	P.INFORMATION-SYSTEMS.13	A policy should detail developer's approach to updating and patching.
O.INCIDENTS	P.INCIDENTS.1	The developer shall have a security incident management policy providing suitable feedback processes to ensure timely communication of security incidents. In particular, minimum criteria for reporting an event should be defined.
	P.INCIDENTS.2	Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to security incidents.
O.BUSINESS-CONTINUITY	P.BUSINESS-CONTINUITY.1	A managed process shall be developed and maintained for business continuity throughout the organization that addresses the security requirements.
	P.BUSINESS-CONTINUITY.2	Business continuity plans shall be documented and deployed in order to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, security relevant processes.
O.COMPLIANCE	P.COMPLIANCE	A policy should detail developers approach to the identification of relevant legislation, statutory, regulatory and contractual requirements, third party intellectual property rights, and other applicable regulations.
O.LIFECYCLE	P.LIFECYCLE	The site follows the life cycle documentation that describes: 1. Configuration Management; 2. Development security; 3. Flaw remediation processes; 4. Development process lifecycle; 5. Development tools.

3.4 Assumptions

The assumptions to support the confidentiality, integrity and availability of assets are references [Ref:3], [Ref:6] :

A.ARRIVAL

Any item that arrives at the development site is appropriately labelled and accompanied by proper packing documentation.

A.REACT

Emergency services and own personnel are capable to respond within the agreed reaction time.

4 ASE_OBJ: Security Objectives

This chapter describes the security objectives for the development site in response to the security problem identified in chapter 3 ASE_SPD: Security Problem Definition . The objectives below are taken from the JIL Minimum Site Security Requirements document. Alternatively, the EUCC SCHEME STATE-OF-THE-ART DOCUMENT Minimum Site Security Requirements, which contains the same requirements, may be used [Ref:3], [Ref:6] . For the Control objectives and controls, only the high level objectives are presented here. The low level objectives are implicitly included by reference to the overall objectives from the Control objectives and controls.

4.1 Definition of Security Objectives

4.1.1 Development Security System and Documentation

O.DSS

As required by ALC_DVS.1.1C and ALC_DVS.2.1C, respectively, the Development Security Documentation (DSD) shall describe the physical, logical, 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.

DSD shall identify all locations where development occurs, the development activities, and the security measures applied at each location linked to such activities and for transports between different locations.

If ALC_DVS.2 is claimed 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 according to the attack potential claimed in the ST (AVA_VAN.5).

4.1.2 Management responsibility

O.MANAGEMENT

The developer shall have well defined, documented, and assigned roles and responsibilities for all activities which may have an impact on confidentiality and integrity of the TOE.

All resources necessary to maintain confidentiality and integrity of the TOE shall be identified and available.

All physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE shall be effective.

4.1.3 Internal DSS audits

O.AUDIT

Internal audits shall ensure that security measures are implemented in a meaningful and concerted way, and that security measures effectively support the intended purpose.

4.1.4 Management review of the DSS

O.REVIEW

Management should ensure that the developer has well defined, documented, and assigned roles and responsibilities for all activities which may have an impact on confidentiality and integrity of the TOE.

All physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE should be effective.

4.1.5 DSS improvement

O.IMPROVE

Effectiveness of physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE shall be reviewed and improved where necessary.

4.1.6 Control objectives and controls

O.ASSET-MGT

Assets shall be clearly identified with the type of protection (confidentiality, integrity, authenticity) assigned, and managed.

Every asset shall have an owner.

O.HR

The overall objective is to reduce the risk of theft, fraud or misuse of facilities by ensuring that employees, contractors, consultants, students, and third party users understand their responsibilities, and are suitable for the roles they are considered for.

O.PHYSICAL

Physical security shall prevent unauthorized physical access to the organization's premises, secure areas, delivery and loading areas, assets, and information which may impair integrity or - where required - confidentiality of the TOE.

Integrity and - for security systems - availability of security relevant equipment shall be ensured to prevent loss, damage, theft, compromise, or loss of integrity of assets and security controls.

O.OPERATION

Operations and communication related to the TOE as well as to supporting infrastructures and resources shall be protected against internal and external threats.

O.ACCESS-CONTROL

Access (logical and physical) to information systems including access to business processes, to networks, to operating systems, to applications, and to information shall be controlled and restricted on a need-to-know basis.

Users, user roles, and user responsibilities shall be managed and controlled.

O.INFORMATION-SYSTEMS

Security shall be an integral part of information systems. IT systems shall be secured to a level ensuring integrity and confidentiality of the TOE, and safeguarding availability and proper operation of security systems.

Information systems include operating systems, infrastructure, business applications (e.g. development environments, configuration management systems), and services, either off-the-shelf products or user-developed applications.

O.INCIDENTS

Effective management of information security incidents shall ensure an appropriate level of security.

O.BUSINESS-CONTINUITY

Business continuity management shall ensure uninterrupted availability of processes, systems, and tools necessary to maintain the required level of security and/or integrity of the TOE and its parts.

O.COMPLIANCE

Breaches of any statutory, regulatory or contractual obligations related to the TOE should be prevented.

4.1.7 Additional objective(s)

O.LIFECYCLE

The developer has defined a measurable life-cycle model to be used in the development and maintenance of the TOE. The site follows the life cycle documentation that describes:

1 Description of configuration management systems and their usage;
2 A configuration items list;
3 Development security;
4 Flaw remediation processes;
5 Development process lifecycle;
6 Development tools.

4.2 Security Objectives Rationale

The Security Objectives Rationale shows how the threats and OSPs are covered by the Security Objectives. The fact that the Security Objectives are taken from Minimum Site Security Requirements [Ref:3] , provides an argument that ALC_DVS.2 – the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE – can be claimed.

ALC_DVS.2 is claimed and the development security documentation justifies that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of a TOE developed at the site according to an attack potential consistent with an Advanced Persistent Threat (APT) or Common Criteria Vulnerability Analysis level of AVA_VAN.5.

The assumptions defined in this Site Security Target are considered as preconditions fulfilled either by other parties (sender, emergency services). Therefore, they do not contribute to the security of the site under evaluation. Table 4 shows the objectives that cover the threats and the organisational security policies.

Table 4: Threats, organisational policies, assumptions and objectives with rationale

Threat/Organisational Policy	Objective(s) / Assumption(s)	Rationale
T.LOGIC-THEFT	O.DSS O.MANAGEMENT O.AUDIT O.REVIEW O.IMPROVE O.HR O.OPERATION O.ACCESS-CONTROL O.INFORMATION-SYSTEMS O.INCIDENTS O.BUSINESS-CONTINUITY O.COMPLIANCE A.ARRIVAL A.REACT	The combination of physical, technical and organizational measures detects unauthorized access and allows for appropriate and timely response to any threat (A.THREAT). This provides assurance that the confidentiality and integrity of the TOE and all its parts (A.ARRIVAL) is safeguarded at all times during the development process.
T.PHYSICAL-THEFT	O.DSS O.MANAGEMENT O.AUDIT O.REVIEW O.IMPROVE O.HR O.PHYSICAL O.ACCESS-CONTROL O.INFORMATION-SYSTEMS O.INCIDENTS O.BUSINESS-CONTINUITY O.COMPLIANCE A.ARRIVAL A.REACT	The combination of physical, technical and organizational measures detects unauthorized access and allows for appropriate and timely response to any threat (A.REACT). This provides assurance that the confidentiality and integrity of the TOE and all its parts (A.ARRIVAL) is safeguarded at all times during the development process.
T.STAFF-ATTACK	O.DSS O.MANAGEMENT O.AUDIT O.REVIEW O.IMPROVE O.ASSET-MGT O.HR O.OPERATION O.ACCESS-CONTROL O.INCIDENTS O.BUSINESS-CONTINUITY O.COMPLIANCE	Physical and logical access control measures limit the access to assets to authorised persons only. Organisational measures prevent uncontrolled access to assets. All activities on development systems can be traced back to a person.

T.STAFF-MISTAKE	O.DSS O.MANAGEMENT O.AUDIT O.REVIEW O.IMPROVE O.ASSET-MGT O.HR	Automated measures and four eyes procedures prevent accidental mistakes by staff. All staff are adequately educated and capable of doing their job. Knowledge transfer is encouraged, where possible and necessary.
T.TRANSPORT-ATTACK	O.DSS O.MANAGEMENT O.AUDIT O.REVIEW O.IMPROVE O.HR O.PHYSICAL O.ACCESS-CONTROL O.INCIDENTS O.BUSINESS-CONTINUITY O.COMPLIANCE	Procedural, physical and logical measures provide assurance that – even in the event an asset is attacked during transport – the confidentiality and integrity of the asset is protected during transport.
P.DSD.1 - P.DSD.3	O.DSS	The Development Security System (O.DSS) and the accompanying Development Security Documentation (P.DSD.1 – P.DSD.3) provide a complete system and appropriate documented view on the complete set of measures to guarantee the confidentiality and integrity of any TOE being developed at this site.
P.MANAGEMENT	O.MANAGEMENT	Management responsibility is addressed adequately at all management levels. A continuous awareness program at all organisational levels guarantees continued awareness of responsibilities at all organisational levels.
P.AUDIT	O.AUDIT	The Development Security System is audited at regular intervals, providing assurance that it is up to date and an accurate representation of daily operations.
P.REVIEW	O.REVIEW	A regular review process of incidents is in place which provides assurance that omissions in the implementation of the Development Security System are discovered and addressed in a timely manner.
P.IMPROVE	O.IMPROVE	The reviews and audits at regular intervals provide assurance about a continuous improvement cycle.
P.ASSET-MGT.1 - P.ASSET-MGT.7	O.ASSET-MGT	The asset management system provides assurance that all assets (including all relevant development systems and TOE parts) are under configuration management and thus the developer is in control of all changes to those assets.
P.HR.1, P.HR.2	O.HR	All personnel is screened prior to employment at a level commensurate with their job description, signs a non-disclosure agreement and is capable of doing their job securely. An onboarding program and continuous awareness training provide assurance of the capability of the personnel to work in ways to assure the confidentiality and integrity of all TOE parts in development.

P.PHYSICAL.1 - P.PHYSICAL.11	O.PHYSICAL	Physical security measures are in place to stop an attacker from compromising the assets on site.
P.OPERATION.1 - P.OPERATION.19	O.OPERATION	Operational security measures are in place to stop an attacker from compromising the assets on site.
P.ACCESS-CONTROL.1 - P.ACCESS-CONTROL.11	O.ACCESS-CONTROL	Access control measures are in place to provide assurance that only authorised personnel have access to assets.
P.INFORMATION-SYSTEMS.1 - P.INFORMATION-SYSTEMS.13	O.INFORMATION-SYSTEMS	Security and access control measures are applied on all information systems used for development of TOEs in the designated development environment.
P.INCIDENTS.1, P.INCIDENTS.2	O.INCIDENTS	Incidents are handled in a controlled an regular manner to provide assurance that the site is up to date at all times to guarantee confidentiality and integrity of all TOE parts at all times. If a confidentiality or integrity breach has happened, this will be detected.
P.BUSINESS-CONTINUITY.1, P.BUSINESS-CONTINUITY.2	O.BUSINESS-CONTINUITY	The business continuity plan guarantees business continuity following business risk assessment.
P.COMPLIANCE	O.COMPLIANCE	The compliance structure, processes and procedures guarantee continuous compliance.
P.LIFECYCLE	O.MANAGEMENT, O.AUDIT, O.REVIEW, O.IMPROVE, O.ASSET-MGT, O.OPERATION, O.INFORMATION-SYSTEMS, O.INCIDENTS, O.BUSINESS-CONTINUITY, O.COMPLIANCE, O.LIFECYCLE	Procedural, physical, logical and technical measures provide assurance that all TOE parts are under the control of the developer during the entire lifecycle.

Table 5 demonstrates full coverage of Threats being countered and that all Organisational Security Policies are enforced by at least one Security Objective. Coverage of all Organisational Security Policies by at least one Objective is also demonstrated in table 3.

Table 5: Threats and objectives coverage

Threat/Organisational Policy	O.DSS	O.MANAGEMENT	O.AUDIT	O.REVIEW	O.IMPROVE	O.ASSET-MGT	O.HR	O.PHYSICAL	O.OPERATION	O.ACCESS-CONTROL	O.INFORMATION-SYSTEMS	O.INCIDENTS	O.BUSINESS-CONTINUITY	O.COMPLIANCE	O.LIFECYCLE
T.LOGIC-THEFT	X	X	X	X	X		X		X	X	X	X	X	X	
T.PHYSICAL-THEFT	X	X	X	X	X		X	X		X	X	X	X	X	
T.STAFF-ATTACK	X	X	X	X	X		X		X	X		X	X	X	

T.STAFF-MISTAKE	X	X	X	X	X	X	X								
T.TRANSPORT-ATTACK	X	X	X	X	X		X	X		X		X	X	X	
P.DSD [3]	X														
P.MANAGEMENT		X													
P.AUDIT			X												
P.REVIEW				X											
P.IMPROVE					X										
P.ASSET-MGT [4]						X									
P.HR [5]							X								
P.PHYSICAL [6]								X							
P.OPERATION [7]									X						
P.ACCESS-CONTROL [8]										X					
P.INFORMATION-SYSTEMS [9]											X				
P.INCIDENTS [10]												X			
P.BUSINESS-CONTINUITY [11]													X		
P.COMPLIANCE														X	
P.LIFECYCLE		X	X	X	X	X			X		X	X	X	X	X

3: P.DSS comprises P.DSD.1 to P.DSD.3
4: P.ASSET-MGT comprises P.ASSET-MGT.1 tot P.ASSET-MGT.7
5: P.HT comprises P.HR.1 and P.HR.2
6: P.PHYSICAl comprises P.PHYSICAL.1 to P.PHYSICAL.11
7: P.OPERATION comprises P.OPERATION.1 to P.OPERATION.19
8: P.ACCESS-CONTROL comprises P.ACCESS-CONTROL.1 to P.ACCESS-CONTROL.11
9: P.INFORMATION-SYSTEMS comprises P.INFORMATION-SYSTEMS.1 to P.INFORMATION-SYSTEMS.13
10: P.INCIDENTS.1 comprises P.INCIDENTS.1 and P.INCIDENTS.2
11: P.BUSINESS-CONTINUITY comprises P.BUSINESS-CONTINUITY.1 and P.BUSINESS-CONTINUITY.2

5 ASE_ECD: Extended Assurance Components Definition

No extended components are defined in this Site Security Target.

6 ASE_REQ: Security Assurance Requirements

6.1 Conformance claim assurance families

The security assurance requirements for this Site Security Target are as follows:

CnfCl 1. ALC_CMC.5 (CM capabilities);
CnfCl 2. ALC_CMS.5 (CM system);
CnfCl 3. ALC_DVS.2 (Development security);
CnfCl 4. ALC_FLR.3 (Flaw remediation);
CnfCl 5. ALC_LCD.2 (Life cycle definition);
CnfCl 6. ALC_TAT.3 (Tools & Techniques).

The dependencies for the assurance requirements named above are as follows:

Dep 1. ALC_CMC.5: ALC_CMS.1 TOE CM coverage, ALC_DVS.2 Sufficiency of security measures , ALC_LCD.1 Developer defined life-cycle model;
Dep 2. ALC_CMS.5: No dependencies;
Dep 3. ALC_DVS.2: No dependencies;
Dep 4. ALC_FLR.3: No dependencies;
Dep 5. ALC_LCD.2: No dependencies;
Dep 6. ALC-TAT.3: ADV_IMP.1 Implementation representation of the TSF.

The following dependencies are not completely fulfilled:

Dep 7. ALC_LCD.2: is part of this Site Security Target but does not cover product specific information of the life-cycle definition. This Security Target only covers the general life cycle processes.
Dep 8. ALC_TAT.3: is part of this Site Security Target but does not cover product specific information of the implementation representation. This Security Target only covers the development tooling that is used for the development of all TOE versions.

6.2 Security Assurance Evidence

The evidence is provided in the Site Security Certification file. For each assurance class or family claimed, a memo with the evidence listed is provided:

Table 6: Evidence of ASE coverage

Assurance class	Memo listing the evidence provided
ASE	01. (CR) SSC_MEM_FOX-CRYP_0001 - Site Security Certification File

Table 7: Evidence of ALC coverage

Assurance family	Memo listing the evidence provided

ALC_CMC.5	01. (CR) SSC_MEM_FOX-CRYP_0002 - Configuration Management
ALC_CMS.5	
ALC_DVS.2	01. (CR) SSC_MEM_FOX-CRYP_0003 - Development Security
ALC_FLR.3	01. (CR) SSC_MEM_FOX-CRYP_0004 - Flaw Remediation
ALC_LCD.2	01. (CR) SSC_MEM_FOX-CRYP_0005_Life Cycle Definition
ALC_TAT.3	01. (CR) SSC_MEM_FOX-CRYP_0006 - Tools and Techniques

6.3 Rationale

The claims in this security target are about TOE development processes rather than a specific TOE. The processes are the focus of the examination for all ALC components claimed. Tables 6 to 12 provide a mapping between the SAR components and give a rationale how each component is met.

Table 8: ALC_CMC security assurance requirements, objectives and rationale for coverage

ALC_CMC.5 SAR	Objective(s)	Rationale
ALC_CMC.5.1D The developer shall provide the TOE and a reference for the TOE.	O.ASSET-MGT	All TOE parts and development systems are uniquely labelled under the CM system. This ST does not describe a specific TOE, but it shows that the developer uses sufficient CM processes and procedures to be capable to fulfil this requirement.
ALC_CMC.5.2D The developer shall provide the CM documentation.	O.ASSET-MGT	The developer has described the CM system, processes and procedures.
ALC_CMC.5.3D The developer shall use a CM system.	O.ASSET-MGT	The developer uses a CM system.
ALC_CMC.5.1C The TOE shall be labelled with its unique reference.	O.ASSET-MGT	All TOE parts and development systems are uniquely labelled under the CM system.
ALC_CMC.5.2C The CM documentation shall describe the method used to uniquely identify the configuration items.	O.ASSET-MGT	The CM documentation completely describes the method used to uniquely label each configuration item. Configuration items do not include non-IT items such as pens, desks etc. They do include all IT systems used for TOE development, generic office equipment (PC or laptop type, exact version of operating system) may be omitted.
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.ASSET-MGT	The CM documentation justifies that the acceptance procedures assure an adequate and appropriate review of all configuration item changes.
ALC_CMC.5.4C The CM system shall uniquely identify all configuration items.	O.ASSET-MGT	The CM system uniquely identifies all configuration items.
ALC_CMC.5.5C The CM system shall provide automated measures such that only authorised changes are made to the configuration items.	O.ASSET-MGT	The CM system provides automated means to assure only authorised changes can be made to the configuration items.
ALC_CMC.5.6C The CM system shall support the production of the TOE by automated means.	O.ASSET-MGT	The CM system supports the production of the TOE by automated means where applicable.

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.ASSET-MGT	The CM system ensures the four eyes principle when it comes to accepting a configuration item into CM, providing assurance that the person responsible for accepting a configuration item into CM is not the person who developed it.
ALC_CMC.5.8C **The CM system shall identify the configuration items that comprise the TSF.**	O.ASSET-MGT	The CM system labels all configuration items, configuration items that comprise the TSF are specifically labelled to indicate so.
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.ASSET-MGT	All changes to configuration items are automatically logged, supporting the audit of all changes to the TOE. Logging includes including the originator, date, and time in the audit trail.
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.ASSET-MGT	The CM system provides an automated means to identify all other configuration items that are affected by the change of a given configuration item.
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.ASSET-MGT	The CM system supports identification of the version of the implementation representation from which the TOE is generated.
ALC_CMC.5.12C The CM documentation shall include a CM plan.	O.ASSET-MGT	There is a CM plan.
ALC_CMC.5.13C The CM plan shall describe how the CM system is used for the development of the TOE.	O.ASSET-MGT	The CM plan describes how the CM system supports TOE development.
ALC_CMC.5.14C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.	O.ASSET-MGT	The CM plan describes the procedures for accepting modified or newly created configuration items as part of the TOE.
ALC_CMC.5.15C The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.ASSET-MGT	The CM system completely covers all configuration items, supporting confidentiality and integrity of all TOE parts under development.
ALC_CMC.5.16C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	O.ASSET-MGT	The CM plan and CM system are aligned.

Table 9: ALC_CMS security assurance requirements, objectives and rationale for coverage

ALC_CMS.5 SAR	Objective(s)	Rationale
ALC_CMS.5.1D The developer shall provide a configuration list for the TOE.	O.ASSET-MGT	O.ASSET-MGT supports the generation of the correct and complete configuration list.
ALC_CMS.5.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaw reports and resolution status; **and development tools and related information.**	O.ASSET-MGT O.INFORMATION-SYSTEMS	O.ASSET-MGT supports the generation of the correct and complete configuration list, O.INFORMATION-SYSTEMS assures the complete configuration list includes all development tooling used.
ALC_CMS.5.2C The configuration list shall uniquely identify the configuration items.	O.ASSET-MGT	O.ASSET-MGT supports the generation of the correct and complete configuration list.

ALC_CMS.5.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.	O.ASSET-MGT O.INFORMATION-SYSTEMS	O.ASSET-MGT supports the generation of the correct and complete configuration list, O.INFORMATION-SYSTEMS assures the complete configuration list includes all developers of the items.

Table 10: ALC_DVS security assurance requirements, objective and rationale for coverage

ALC_DVS.2 SAR	Objective(s)	Rationale
ALC_DVS.2.1D The developer shall produce and provide development security documentation.	O.DSS O.MANAGEMENT O.AUDIT O.REVIEW O.IMPROVE O.ASSET-MGT O.HR O.PHYSICAL O.OPERATION O.ACCESS-CONTROL O.INFORMATION-SYSTEMS O.INCIDENTS O.BUSINESS-CONTINUITY O.COMPLIANCE O.LIFECYCLE	All objectives contribute to security (confidentiality and integrity of a TOE and its parts) and are documented.
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.DSS O.MANAGEMENT O.AUDIT O.REVIEW O.IMPROVE O.ASSET-MGT O.HR O.PHYSICAL O.OPERATION O.ACCESS-CONTROL O.INFORMATION-SYSTEMS O.INCIDENTS O.BUSINESS-CONTINUITY O.COMPLIANCE O.LIFECYCLE	O.DSS guarantees that all physical, logical, procedural, personnel, and other security measures are properly documented, including documentation where development is done, development activities, and security measures applied at each location, including delivery procedures between development sites. O.MANAGEMENT supports that all measures as documented by O.DSS have an owner and are effective. O.AUDIT checks whether all measures are indeed effective. O.REVIEW supports regular review of O.DSS at management level, assuring continued proper attention in the maintenance of all measures. O.IMPROVE as part of the audit, review and improvement cycle supports continuous monitoring and improvement of the DSS. O.ASSET-MGT assures that every asset has an owner who is responsible for its security. O.HR assures that only trustworthy personnel has access to the development areas. O.PHYSICAL assures that only authorised personnel or visitors under guidance of authorised personnel have access to the development areas. O.OPERATION supports that all elements of the development process are protected against internal and external threats.

		O.ACCESS-CONTROL supports access strictly on a need-to-know basis. O.INFORMATION-SYSTEMS assures that the complete development environment (all physical properties, systems and other elements) supports the security (confidentiality and integrity) of the TOE and its parts. O.INCIDENTS ensures effective handling of all security incidents. O.BUSINESS-CONTINUITY assures uninterrupted availability of processes, systems, and tools. O.COMPLIANCE assures compliance with all regulatory requirements. O.LIFECYCLE provides assurance that the developer is in control of the entire lifecycle of any TOE being developed at the site.
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.DSS O.MANAGEMENT O.AUDIT O.REVIEW O.IMPROVE O.ASSET-MGT O.HR O.PHYSICAL O.OPERATION O.ACCESS-CONTROL O.INFORMATION-SYSTEMS O.INCIDENTS O.BUSINESS-CONTINUITY O.COMPLIANCE O.LIFECYCLE	The documentation justifies that the security measures provide the necessary level of protection. By adhering to the Minimum Site Security Requirements [Ref:3],[Ref:6], assurance is provided that the measures are adequate.

Table 11: ALC_FLR security assurance requirements, objectives and rationale for coverage

ALC_FLR.3 SAR	Objective(s)	Rationale
ALC_FLR.3.1D The developer shall document and provide flaw remediation procedures addressed to TOE developers.	O.DSS O.ASSET-MGT O.HR O.OPERATION	The security measures as defined in O.DSS provide the necessary level of protection to maintain the confidentiality and integrity of the TOE according to the attack potential claimed in this ST (AVA_VAN.5). O.ASSET-MGT assures traceability of all TOE instances to support the flaw remediation tracking. O.HR assures that the personnel working on the flaw remediation process are suitable for their role. O.OPERATION protects the communication in the flaw remediation process.
ALC_FLR.3.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.	O.DSS O.ASSET-MGT O.HR O.OPERATION	The security measures as defined in O.DSS provide the necessary level of protection to maintain the confidentiality and integrity of the TOE according to the attack potential claimed in this ST (AVA_VAN.5). O.ASSET-MGT assures traceability of all TOE instances to support the flaw remediation tracking.

		O.HR assures that the personnel working on the flaw remediation process are suitable for their role. O.OPERATION protects the communication in the flaw remediation process.
ALC_FLR.3.3D The developer shall provide flaw remediation guidance addressed to TOE users.	O.DSS O.ASSET-MGT O.HR O.OPERATION	The security measures as defined in O.DSS provide the necessary level of protection to maintain the confidentiality and integrity of the TOE according to the attack potential claimed in this ST (AVA_VAN.5). O.ASSET-MGT assures traceability of all TOE instances to support the flaw remediation tracking. O.HR assures that the personnel working on the flaw remediation process are suitable for their role. O.OPERATION protects the communication in the flaw remediation process.
ALC_FLR.3.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.	O.DSS O.ASSET-MGT O.HR O.OPERATION	The security measures as defined in O.DSS provide the necessary level of protection to maintain the confidentiality and integrity of the TOE according to the attack potential claimed in this ST (AVA_VAN.5). O.ASSET-MGT assures traceability of all TOE instances to support the flaw remediation tracking. O.HR assures that the personnel working on the flaw remediation process are suitable for their role. O.OPERATION protects the communication in the flaw remediation process.
ALC_FLR.3.2C 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.DSS O.ASSET-MGT O.HR O.OPERATION	The security measures as defined in O.DSS provide the necessary level of protection to maintain the confidentiality and integrity of the TOE according to the attack potential claimed in this ST (AVA_VAN.5). O.ASSET-MGT assures traceability of all TOE instances to support the flaw remediation tracking. O.HR assures that the personnel working on the flaw remediation process are suitable for their role. O.OPERATION protects the communication in the flaw remediation process.
ALC_FLR.3.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.	O.DSS O.ASSET-MGT O.HR O.OPERATION	The security measures as defined in O.DSS provide the necessary level of protection to maintain the confidentiality and integrity of the TOE according to the attack potential claimed in this ST (AVA_VAN.5). O.ASSET-MGT assures traceability of all TOE instances to support the flaw remediation tracking. O.HR assures that the personnel working on the flaw remediation process are suitable for their role. O.OPERATION protects the communication in the flaw remediation process.
ALC_FLR.3.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.	O.DSS O.ASSET-MGT O.HR O.OPERATION	The security measures as defined in O.DSS provide the necessary level of protection to maintain the confidentiality and integrity of the TOE according to the attack potential claimed in this ST (AVA_VAN.5). O.ASSET-MGT assures traceability of all TOE instances to support the flaw remediation tracking. O.HR assures that the personnel working on the flaw remediation process are suitable for their role.

		O.OPERATION protects the communication in the flaw remediation process.
ALC_FLR.3.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.	O.DSS O.ASSET-MGT O.HR O.OPERATION	The security measures as defined in O.DSS provide the necessary level of protection to maintain the confidentiality and integrity of the TOE according to the attack potential claimed in this ST (AVA_VAN.5). O.ASSET-MGT assures traceability of all TOE instances to support the flaw remediation tracking. O.HR assures that the personnel working on the flaw remediation process are suitable for their role. O.OPERATION protects the communication in the flaw remediation process.
ALC_FLR.3.6C The flaw remediation procedures shall include a procedure requiring timely response and the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.	O.DSS O.ASSET-MGT O.HR O.OPERATION	The security measures as defined in O.DSS provide the necessary level of protection to maintain the confidentiality and integrity of the TOE according to the attack potential claimed in this ST (AVA_VAN.5). O.ASSET-MGT assures traceability of all TOE instances to support the flaw remediation tracking. O.HR assures that the personnel working on the flaw remediation process are suitable for their role. O.OPERATION protects the communication in the flaw remediation process.
ALC_FLR.3.7C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.	O.DSS O.ASSET-MGT O.HR O.OPERATION	The security measures as defined in O.DSS provide the necessary level of protection to maintain the confidentiality and integrity of the TOE according to the attack potential claimed in this ST (AVA_VAN.5). O.ASSET-MGT assures traceability of all TOE instances to support the flaw remediation tracking. O.HR assures that the personnel working on the flaw remediation process are suitable for their role. O.OPERATION protects the communication in the flaw remediation process.
ALC_FLR.3.8C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.	O.DSS O.ASSET-MGT O.HR O.OPERATION	The security measures as defined in O.DSS provide the necessary level of protection to maintain the confidentiality and integrity of the TOE according to the attack potential claimed in this ST (AVA_VAN.5). O.ASSET-MGT assures traceability of all TOE instances to support the flaw remediation tracking. O.HR assures that the personnel working on the flaw remediation process are suitable for their role. O.OPERATION protects the communication in the flaw remediation process.
ALC_FLR.3.9C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.	O.DSS O.ASSET-MGT O.HR O.OPERATION	The security measures as defined in O.DSS provide the necessary level of protection to maintain the confidentiality and integrity of the TOE according to the attack potential claimed in this ST (AVA_VAN.5). O.ASSET-MGT assures traceability of all TOE instances to support the flaw remediation tracking. O.HR assures that the personnel working on the flaw remediation process are suitable for their role. O.OPERATION protects the communication in the flaw remediation process.

ALC_FLR.3.10C The flaw remediation guidance shall describe a means by which TOE users may register with the developer, to be eligible to receive security flaw reports and corrections.	O.DSS O.ASSET-MGT O.HR O.OPERATION	The security measures as defined in O.DSS provide the necessary level of protection to maintain the confidentiality and integrity of the TOE according to the attack potential claimed in this ST (AVA_VAN.5). O.ASSET-MGT assures traceability of all TOE instances to support the flaw remediation tracking. O.HR assures that the personnel working on the flaw remediation process are suitable for their role. O.OPERATION protects the communication in the flaw remediation process.
ALC_FLR.3.11C The flaw remediation guidance shall identify the specific points of contact for all reports and enquiries about security issues involving the TOE.	O.DSS O.ASSET-MGT O.HR O.OPERATION	The security measures as defined in O.DSS provide the necessary level of protection to maintain the confidentiality and integrity of the TOE according to the attack potential claimed in this ST (AVA_VAN.5). O.ASSET-MGT assures traceability of all TOE instances to support the flaw remediation tracking. O.HR assures that the personnel working on the flaw remediation process are suitable for their role. O.OPERATION protects the communication in the flaw remediation process.

Table 12: ALC_LCD security assurance requirements, objectives and rationale for coverage

ALC_LCD.2 SAR	Objective(s)	Rationale
ALC_LCD.2.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE, **that is based on a measurable life-cycle model.**	O.LIFECYCLE	The lifecycle model is measurable and defines the entire lifecycle of all the assets. Using a model for the development and maintenance of a TOE does not guarantee that the TOE meets all of its SFRs. It is possible that the model chosen will be insufficient or inadequate and therefore no benefits in the quality of the TOE can be observed. Using a life-cycle model that has been approved by a group of experts (e.g. academic experts, standards bodies) improves the chances that the development and maintenance models will contribute to the TOE meeting its SFRs. The use of a life-cycle model including some quantitative valuation adds further assurance in the overall quality of the TOE development process [Ref:3] .
ALC_LCD.2.2D The developer shall provide life-cycle definition documentation.	O.LIFECYCLE	The lifecycle model is measurable and defines the entire lifecycle of all the assets.
ALC_LCD.2.3D **The developer shall measure the TOE development using the measurable life-cycle model.**	O.LIFECYCLE	The lifecycle model is measurable and defines the entire lifecycle of all the assets. Using a model for the development and maintenance of a TOE does not guarantee that the TOE meets all of its SFRs. It is possible that the model chosen will be insufficient or inadequate and therefore no benefits in the quality of the TOE can be observed. Using a life-cycle model that has been approved by a group of experts (e.g. academic experts, standards bodies) improves the chances that the development and maintenance models will contribute to the TOE meeting its SFRs. The use of a life-cycle model

		including some quantitative valuation adds further assurance in the overall quality of the TOE development process [Ref:3] .
ALC_LCD.2.4D **The developer shall provide life-cycle output documentation.**	O.LIFECYCLE	The lifecycle model is measurable and defines the entire lifecycle of all the assets.
ALC_LCD.2.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE, **including the details of its arithmetic parameters and/or metrics used to measure the quality of the TOE and/or its development.**	O.LIFECYCLE	The lifecycle model is measurable and defines the entire lifecycle of all the assets, including arithmetic details or quality metrics of any TOE developed at the site.
ALC_LCD.2.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.	O.LIFECYCLE	The lifecycle model is measurable and defines the entire lifecycle of all the assets. It shows the developer is in control of the entire development and maintenance process, to the controlled decommissioning of the assets.
ALC_LCD.2.3C **The life-cycle output documentation shall provide the results of the measurements of the TOE development using the measurable life-cycle model.**	O.LIFECYCLE	The lifecycle model is measurable and defines the entire lifecycle of all the assets.

Table 13: ALC_TAT security assurance requirements, objectives and rationale for coverage

ALC_TAT.3 SAR	Objective(s)	Rationale
ALC_TAT.3.1D The developer shall provide the documentation identifying each development tool being used for the TOE.	O.OPERATION O.INFORMATION-SYSTEMS	O.OPERATION assures the supporting infrastructure and resources protect against internal and external threats. O.INFORMATION-SYSTEMS assures the protection of all assets against breaches to the confidentiality and / or integrity.
ALC_TAT.3.2D The developer shall document and provide the selected implementation-dependent options of each development tool.	O.OPERATION O.INFORMATION-SYSTEMS	O.OPERATION assures the supporting infrastructure and resources protect against internal and external threats. O.INFORMATION-SYSTEMS assures the protection of all assets against breaches to the confidentiality and / or integrity.
ALC_TAT.3.3D **The developer shall describe and provide the implementation standards that are being applied by the developer and by any third-party providers for all parts of the TOE.**	O.OPERATION O.INFORMATION-SYSTEMS	O.OPERATION assures the supporting infrastructure and resources protect against internal and external threats. O.INFORMATION-SYSTEMS assures the protection of all assets against breaches to the confidentiality and / or integrity.
ALC_TAT.3.1C Each development tool used for implementation shall be well-defined.	O.OPERATION O.INFORMATION-SYSTEMS	O.OPERATION assures the supporting infrastructure and resources protect against internal and external threats. O.INFORMATION-SYSTEMS assures the protection of all assets against breaches to the confidentiality and / or integrity.

ALC_TAT.3.2C 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.OPERATION O.INFORMATION-SYSTEMS	O.OPERATION assures the supporting infrastructure and resources protect against internal and external threats. O.INFORMATION-SYSTEMS assures the protection of all assets against breaches to the confidentiality and / or integrity.
ALC_TAT.3.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.	O.OPERATION O.INFORMATION-SYSTEMS	O.OPERATION assures the supporting infrastructure and resources protect against internal and external threats. O.INFORMATION-SYSTEMS assures the protection of all assets against breaches to the confidentiality and / or integrity.

Tables 12 to 18 demonstrate full coverage of CC components being covered by at least one Security Objective.

Table 14: CC ALC_CMC components and objectives coverage

CC ALC_CMC component	O.DSS	O.MANAGEMENT	O.AUDIT	O.REVIEW	O.IMPROVE	O.ASSET-MGT	O.HR	O.PHYSICAL	O.OPERATION	O.ACCESS-CONTROL	O.INFORMATION-SYSTEMS	O.INCIDENTS	O.BUSINESS-CONTINUITY	O.COMPLIANCE	O.LIFECYCLE
ALC_CMC.5.1D						X									
ALC_CMC.5.2D						X									
ALC_CMC.5.3D						X									
ALC_CMC.5.1C						X									
ALC_CMC.5.2C						X									
ALC_CMC.5.3C						X									
ALC_CMC.5.4C						X									
ALC_CMC.5.5C						X									
ALC_CMC.5.6C						X									
ALC_CMC.5.7C						X									
ALC_CMC.5.8C						X									
ALC_CMC.5.9C						X									
ALC_CMC.5.10C						X									
ALC_CMC.5.11C						X									
ALC_CMC.5.12C						X									

ALC_CMC.5.13C						X									
ALC_CMC.5.14C						X									
ALC_CMC.5.15C						X									
ALC_CMC.5.16C						X									

Table 15: CC ALC_CMS components and objectives coverage

CC ALC_CMS component	O.DSS	O.MANAGEMENT	O.AUDIT	O.REVIEW	O.IMPROVE	O.ASSET-MGT	O.HR	O.PHYSICAL	O.OPERATION	O.ACCESS-CONTROL	O.INFORMATION-SYSTEMS	O.INCIDENTS	O.BUSINESS-CONTINUITY	O.COMPLIANCE	O.LIFECYCLE
ALC_CMS.5.1D						X									
ALC_CMS.5.1C						X					X				
ALC_CMS.5.2C						X									
ALC_CMS.5.3C						X					X				

Table 16: CC ALC_DEL components and objectives coverage

CC ALC_DEL component	O.DSS	O.MANAGEMENT	O.AUDIT	O.REVIEW	O.IMPROVE	O.ASSET-MGT	O.HR	O.PHYSICAL	O.OPERATION	O.ACCESS-CONTROL	O.INFORMATION-SYSTEMS	O.INCIDENTS	O.BUSINESS-CONTINUITY	O.COMPLIANCE	O.LIFECYCLE
ALC_DEL.1.1D						X	X								
ALC_DEL.1.2D						X	X								
ALC_DEL.1.1C						X	X								

Table 17: CC ALC_DVS components and objectives coverage

CC ALC_DVS component	O.DSS	O.MANAGEMENT	O.AUDIT	O.REVIEW	O.IMPROVE	O.ASSET-MGT	O.HR	O.PHYSICAL	O.OPERATION	O.ACCESS-CONTROL	O.INFORMATION-SYSTEMS	O.INCIDENTS	O.BUSINESS-CONTINUITY	O.COMPLIANCE	O.LIFECYCLE
ALC_DVS.2.1D	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ALC_DVS.2.1C	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ALC_DVS.2.2C	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Table 18: CC ALC_FLR components and objectives coverage

CC ALC_FLR component	O.DSS	O.MANAGEMENT	O.AUDIT	O.REVIEW	O.IMPROVE	O.ASSET-MGT	O.HR	O.PHYSICAL	O.OPERATION	O.ACCESS-CONTROL	O.INFORMATION-SYSTEMS	O.INCIDENTS	O.BUSINESS-CONTINUITY	O.COMPLIANCE	O.LIFECYCLE
ALC_FLR.3.1D	X					X	X		X						
ALC_FLR.3.2D	X					X	X		X						
ALC_FLR.3.3D	X					X	X		X						
ALC_FLR.3.1C	X					X	X		X						
ALC_FLR.3.2C	X					X	X		X						
ALC_FLR.3.3C	X					X	X		X						
ALC_FLR.3.4C	X					X	X		X						
ALC_FLR.3.5C	X					X	X		X						
ALC_FLR.3.6C	X					X	X		X						
ALC_FLR.3.7C	X					X	X		X						
ALC_FLR.3.8C	X					X	X		X						
ALC_FLR.3.9C	X					X	X		X						
ALC_FLR.3.10C	X					X	X		X						
ALC_FLR.3.11C	X					X	X		X						

Table 19: CC ALC_LCD components and objectives coverage

CC ALC_LCD component	O.DSS	O.MANAGEMENT	O.AUDIT	O.REVIEW	O.IMPROVE	O.ASSET-MGT	O.HR	O.PHYSICAL	O.OPERATION	O.ACCESS-CONTROL	O.INFORMATION-SYSTEMS	O.INCIDENTS	O.BUSINESS-CONTINUITY	O.COMPLIANCE	O.LIFECYCLE
ALC_LCD.2.1D															X
ALC_LCD.2.2D															X
ALC_LCD.2.3D															X
ALC_LCD.2.4D															X
ALC_LCD.2.1C															X
ALC_LCD.2.2C															X
ALC_LCD.2.3C															X

Table 20: CC ALC_TAT components and objectives coverage

CC ALC_TAT component	O.DSS	O.MANAGEMENT	O.AUDIT	O.REVIEW	O.IMPROVE	O.ASSET-MGT	O.HR	O.PHYSICAL	O.OPERATION	O.ACCESS-CONTROL	O.INFORMATION-SYSTEMS	O.INCIDENTS	O.BUSINESS-CONTINUITY	O.COMPLIANCE	O.LIFECYCLE
ALC_TAT.3.1D									X		X				
ALC_TAT.3.2D									X		X				
ALC_TAT.3.3D									X		X				

7 ASE_TSS: Site Summary Specification

The site provides the following services:

- Customer services: acquisition and sales activities, delivery and support (communication customer, flaw reporting) of products.
- Architecture for hardware, firmware, and software.
- Hardware engineering (mechanical and electrical), firmware engineering, software engineering.
- Test environment for testing of the engineered products.
- Secure development environment implementation and maintenance to provide the services mentioned.
- Secure storage of products produced.

The development site as defined in chapter 3 adheres to all objectives, policies and security measures as defined in the JIL document Minimum Site Security Requirements [Ref:3],[Ref:6] , and one additional objective O.LIFECYCLE. Chapter 6 shows the compliance to the CC assurance families and the completeness of coverage.

The assumptions are that any item that arrives at the development site is appropriately labelled and accompanied by proper packing documentation (A.ARRIVAL), and that emergency services and own personnel are capable to respond within the agreed reaction time (A.REACT).

In this Security Target, it has been shown that the development site covers all components of the assurance class life-cycle (ALC):

Table 21: CC assurance class lifecycle model (ALC) coverage

Component(s)	Rationale
ALC_CMC.5 and ALC_CMS.5	The configuration management system covers all configuration items of all TOEs developed at the site. This includes TOE development up to EAL7. The argumentation for each CC ALC_CMC and ALC_CMS component is provided in chapter 6 .
ALC_DVS.2	The site implements all JIL document Minimum Site Security Requirements [Ref:3],[Ref:6] , showing that development security is completely implemented according to a standard that allows for a claim that the measures are commensurate for development at a level of AVA_VAN.5, protecting against an attacker level of Advanced Persistent Threat (APT).The argumentation for each CC ALC_DVS component is provided in chapter 6 .
ALC_FLR.3	The site implements standardised flaw remediation procedures. These procedures ensure the maintenance of TOE security during the entire lifecycle up to decommissioning of any TOE. The argumentation for each CC ALC_FLR component is provided in chapter 6 .
ALC_LCD.2	The site implements a measurable lifecycle model and maintains it. The argumentation for each CC ALC_LCD component is provided in chapter 6 .
ALC_TAT.3	The site implements development tools and techniques. The argumentation for each CC ALC_TAT component is provided in chapter 6 .

The Minimum Site Security Requirements [Ref:3],[Ref:6] , a document drafted by an expert group on site security, documents in great detail the objectives, policies and security measures for a secure development site. For life cycle purposes, one additional objective was added because the Minimum Site Security Requirements document focuses on development security.

References

1. EUROSMART. Security IC Platform Protection Profile with Augmentation Packages. BSI-CC-PP-0084-2014

   Version 1.0, January 2014.

   https://www.commoncriteriaportal.org/files/ppfiles/pp0084b_pdf.pdf

2. Common Criteria for Information Technology Security Evaluation.

   Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

   https://www.commoncriteriaportal.org/cc/CCPART1V3.1R5.pdf

3. Common Criteria for Information Technology Security Evaluation.

   Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017.

   https://www.commoncriteriaportal.org/cc/CCPART3V3.1R5.pdf

4. Common Evaluation Methodology for Information Technology Security Evaluation.

   Evaluation methodology, Version 3.1, Revision 5, April 2017.

   https://www.commoncriteriaportal.org/cc/CEMV3.1R5.pdf

5. Supporting Document Guidance. Site Certification. CCDB-2007-11-001 Version 1.0, Revision 1, October 2007.

   https://www.commoncriteriaportal.org/files/supdocs/CCDB-2007-11-001-SiteCertificationProcessv1-0.pfd

6. Joint Interpretation Library. Minimum Site Security Requirements. Version 3.1, December 2023.

   https://www.sogis.eu/documents/cc/common/JIL-Minimum-Site-Security-Requirements-v3.1.pdf

7. Cybersecurity Certification.

   EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS, V1.1.1, May 2021.

   https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1

8. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2023 (Cybersecurity Act). Entry into force June 2019.

   https://eur-lex.europa.eu/eli/reg/2019/881/oj

Fox-IT
Fox-IT prevents, solves and mitigates the most serious threats caused by cyberattacks, data leaks, or fraud with innovative solutions for governments, defense agencies, law enforcement, critical infrastructure and banking and commercial enterprise clients worldwide. Fox-IT combines smart ideas with advanced technology to create solutions that contribute to a more secure society.
We develop products and custom solutions for our clients to guarantee the safety of sensitive and critical government systems, to protect industrial networks, to defend online banking systems, and to secure confidential data.

For more detailed information about Fox-IT, including partner details, please go to www.fox-it.com

CLASSIFICATION
PUBLIC

CRYPTO
Part of Fox-IT

Fox Crypto B.V.
Olof Palmestraat 6, Delft
P.O. Box 638, 2600 AP Delft
The Netherlands

T +31 (0)15 284 7999
F +31 (0)15 284 7990
crypto@fox-crypto.com

fox-crypto.com