Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 8/18

(Certification No.)

Certificazione di Sito

(Site Certification)

LFoundry Avezzano (Italy) and LFoundry Landshut (Germany)

Sviluppatore: **LFoundry s.r.l.**
(Developer)

I siti indicati in questo certificato sono risultati conformi ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per i componenti di garanzia:

The sites identified in this certificate comply with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance components:

ALC_CMC.4, ALC_CMS.5, ALC_DEL.1,
ALC_DVS.2, ALC_LCD.1, ALC_TAT.2

Il Direttore
(Dott.ssa Rita Forsi)

Roma, 18 settembre 2018

Common Criteria

This page is intentionally left blank

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Site Certification Report

LFoundry Avezzano (Italy) and LFoundry Landshut (Germany)

OCSI/CERT/SEL/02/2015/RC

Version 1.0

18 September 2018

Courtesy translation

Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	18/09/2018

2 Table of contents

3 Acronyms

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
DPCM	Decreto del Presidente del Consiglio dei Ministri
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GDS	Graphic Database System
IC	Integrated Circuit
ICT	Information and Communication Technologies
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza (Evaluation Facility)
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica (Certification Body)
PP	Protection Profile
R&D	Research and Development
SST	Site Security Target
TOE	Target of Evaluation

4 References

4.1 Criteria and regulations

[CC1] CCMB-2012-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 4, September 2012

[CC2] CCMB-2012-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 4, September 2012

[CC3] CCMB-2012-09-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 4, September 2012

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2012-09-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 4, September 2012

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di Certificazione della Sicurezza Informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di Certificazione della Sicurezza Informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di Certificazione della Sicurezza Informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[SOGIS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3, January 2010

4.2 Technical documents

[BSI-35] Security IC Platform Protection Profile, Version 1.0, 15 June 2007, Eurosmart, BSI-CC-PP-0035-2007

[BSI-84] Security IC Platform Protection Profile wirh Augmentation Packages, Version 1.0, 13 January 2014, Eurosmart, BSI-CC-PP-0084-2014

[ETR] ETR for Site Certification “LFoundry Avezzano and Landshut site”, LVS Selta, version 1.0, 20 June 2018 (confidential document)

[SC-CC] Common Criteria Supporting Document Guidance - Site Certification - Version 1.0, Revision 1, October 2007, CCDB-2007-11-001

[SC-SOGIS] SOGIS - Joint Interpretation Library - Minimum Site Security Requirements, Version 2.1 (for trial use), December 2017

[SST] Site Security Target “LFoundry Avezzano and Landshut site”, LFoundry, Revision 8, 8 June 2018 (confidential document)

[SST-Lite] Site Security Target Lite “LFoundry Avezzano and Landshut site”, LFoundry, Version 1, 13 June 2018 (sanitised public document)

[ST-AR] Site Technical Audit Report – LFoundry Landshut site, LVS Selta, Version 1.0, 4 June 2018 (confidential document)

[ST-SAN] CCRA Supporting Document, “ST sanitising for publication”, Version 1.0, April 2006, CCDB-2006-04-004

5 Recognition of the certificate

Currently the Recognition Agreements in place (SOGIS-MRA and CCRA) do not cover the recognition of Site Certificates. However, the evaluation process performed was outlined according to the rules of the agreements and by using the available supporting documents on Site Certification: “Common Criteria Supporting Document Guidance - Site Certification” [SC-CC] and “SOGIS - Joint Interpretation Library - Minimum Site Security Requirements” [SC-SOGIS].

Therefore, the results of this evaluation and certification procedure can be re-used in a subsequent product evaluation and certification procedure by the product certificate issuing scheme depending on its scheme policy.

5.1 European Mutual Recognition Agreement (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT-Products. A higher recognition level for evaluations beyond EAL4 is provided for IT-Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on http://www.sogisportal.eu.

5.2 International Mutual Recognition Agreement (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] has been ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL 2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on http://www.commoncriteriaportal.org.

6 Statement of Certification

This document reports the results of the Site Certification for LFoundry Avezzano (Italy) and LFoundry Landshut (Germany) production sites.

The results from a site certification can be re-used for product certifications. For products which have been certified using a site certificate an individual certificate will be issued.

The Certification Results contain the description of the site, the activities for which the site is responsible within a product life cycle, the details of the evaluation and instructions for the clients of the site.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The evaluation has been conducted on the basis of the complete Site Security Target [SST], which is referred to in the following of this report. The published version of the Site Security Target [SST-Lite] has been produced and verified according to the supporting document [ST-SAN] provided by the CCRA international agreement and contains no substantial differences compared to the full version.

The objective of the evaluation is to provide assurance that the site complies with the security problem definition described in the associated Site Security Target [SST]; the potential clients of the site should review also the Site Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM], and following the recommendations contained in the supporting documents provided by the international agreements CCRA and SOGIS, [SC-CC] and [SC-SOGIS], respectively.

The sites identified in this certificate comply with the requirements for the assurance components of the ALC class of Common Criteria and AST class introduced and refined in the supporting document [SC-CC].

This certificate applies only to the specific site as indicated above and in conjunction with the complete content of the Certification Report and the Site Security Target {SST}.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA]. However the Certification Body with such a document does not express any kind of support or promotion of the site.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the LFoundry Avezzano (Italy) and LFoundry Landshut (Germany) production sites to provide assurance to the potential clients that the site security features comply with its security requirements, as defined in the document Site Security Target [SST], chapter 4 - Security Problem Definition.

In addition to the present Certification Report, the potential clients of the site should review also the Site Security Target [SST], in order to gain a complete understanding of the security problem addressed.

7.2 Executive summary

Name of Site	LFoundry Avezzano and Landshut
Site Security Target	"LFoundry Avezzano and Landshut site" Site Security Target, Revision 8, 8 June 2018 (confidential document)
Site Security Target Lite	"LFoundry Avezzano and Landshut site" Site Security Target Lite, Version 1, 13 June 2018 (sanitised public document)
Assurance Components	ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1 and ALC_TAT.2
Site operator	LFoundry s.r.l.
Sponsor	LFoundry s.r.l.
LVS	Selta
CC version	3.1 Rev. 4
Kickoff date	12 March 2015
Completion date	20 June 2018

7.3 Identification of the Site

LFoundry company is deployed in two different sites:

1) LFoundry Avezzano site, located in Via Antonio Pacinotti, 7 - 67051 Avezzano (AQ), Italy.

2) LFoundry Landshut site, located in Zweigniederlassung Landshut, Erhard-Ludwig Strasse 6 - 84034 Landshut, Germany.

7.3.1 Avezzano site

The Avezzano site consists of a manufacturing building (wafer Fab) and other areas involved in IC production management within the support building, with additional utilities buildings. The entire site is surrounded by a fence.

The site does not directly contribute to the development of the intended TOE in the sense of CC. Nevertheless, the process flow conducted at the site includes the realization of the IC on wafers. Using the received photomask and the client specifications, the site does perform the IC construction on wafers. The wafers are then delivered to the client. As this is regarded as internal shipment, it is covered under aspect ALC_DVS.2 instead of ALC_DEL.1 that covers the delivery to an external customer which the site does not conduct.

The following LFoundry services are performed during the activities mentioned above:

- receipt, identification, registration and storage of mask sets;
- receipt of GDS2 file provided by Landshut site;
- wafer production;
- quality assurance;
- secure wafer delivery to clients.

Accountability for the management of the previous service is mainly owned by the following Departments/Organization Unit:

- Procurement & Logistics;
- R&D;
- ICT;
- Manufacturing;
- Process Engineering;
- Customer and Product Quality;
- Security.

7.3.2 Landshut site

The German site performs the design activities (integration of LFoundry proprietary modules with client design) and technology development, marketing and sales.

The Landshut's site consists of office area distributed in 4 levels. Various surveillance and alarming systems at the floor and basement levels inside the building ensure site protection and control and alarming by 24 hours 7 day. The following LFoundry services are performed during the activities mentioned above:

- receipt of GDS2 file provided by clients;
- mask data preparation;
- mask data transfer to the mask shop;
- GDS2 file transfer to Avezzano site.

Accountable for the management of the previous service are the following Departments/Organization Unit:

- R&D Team Landshut;
- ICT.

The areas involved in design activities are located at the first floor, while the data preparation room and the server room are at basement.

7.3.3 Services of the Site

LFoundry produces IC on wafers. The development process for devices using this production process is supported by an appropriate gate library. LFoundry has capability for integrate proprietary module with customer's ones.

LFoundry site provides three services.

- Data Preparation service at Landshut site: the client sends to LFoundry (Landshut site) the device design (GDS2) in order to integrate it with the LFoundry property modules and build the mask layout to be produced by the Mask Shop.
- Wafer Manufacturing at Avezzano site: wafers with Security ICs are built according to the received specifications.
- Rejects analysis at Avezzano site: after the end of the production cycle, LFoundry Laboratory provides information to analyse the cause of functional failures found during processes performed.

7.4 Life cycle phase

Based upon the life-cycle defined in Security IC Platform Protection Profiles ([BSI-35] and [BSI-84]), LFoundry covers parts of the life cycle phase 3 related to the:

- integration and photomask fabrication (Mask data preparation);
- IC production (wafer production).

7.5 Security problem definition

The Security Problem Definition comprises security problems derived from threats against the assets handled by the site. The security problem is defined in a different way for both sites, according the different management of configuration items in Landshut and Avezzano.

The Security Problem Definition is about two sets of security problems:

- the first set comprises all kind of possible attacks regarding physical objects (e.g. wafers, or masks), mainly related to the unauthorized disclosure of information (e.g. design data) or the theft of the assets;

- the second one comprises instead the requirements for the configuration management (e.g. controlled production flow) and the control of security measures.

The security problems are described in terms of Threats, Organizational Security Policies and Security Objectives.

The assets, assumptions, threats and organizational security policies are defined in the document Site Security Target [SST], chapter 4. They are derived from the Security IC Platform Protection Profiles ([BSI-35] and [BSI-84]). Only aspects that are applicable to the life cycle phase 3 are considered here.

The security objectives for the site are derived from these threats and organizational security policies as stated in the Site Security Target [SST], chapter 5.

7.6 Assumptions and Preconditions required by the Site

Since the site covers only parts of the life cycle phase 3, related to the integration and photomask fabrication and IC production, LFoundry must rely on preconditions provided by the owner of the other parts of the life cycle.

This is reflected by the assumptions on the interface between the client, the site and the part of the production flow that is not under LFoundry direct control. These aspects have to be mainly followed by a client of the site.

Considering their relevance, the assumptions described in the chapter 4.4 of the Site Security Target [SST] are given below:

- **A.Internal-Shipment**: The recipient client of the transferred configuration items is identified by the address of the client site for physical items and by corresponding information for electronic items (e.g. e-mail address and digital signature).

- **A.Item-Identification.** Each configuration item received at the site is appropriately labeled by the sender, to ensure that each configuration item is uniquely identified.

- **A.Mask-Support.** The Photo Shop provides photo masks for the wafer production that are compliant with the production process released at the site. Further the masks must include identification data that fits to the production support of the site and are included in the configuration management system.

- **A.Product-Specification.** The client provides all the appropriate information (e.g. specifications, definitions, test requirements, test limits) to ensure the appropriate production process. The provided information includes the classification of the documents and asset, and clarifies the documents and items developed by the site that have to undergo a release process.

- **A.Product-Test.** The client is responsible for the functional testing of the finished devices on the wafer. Further the masks include appropriate test structure to support the parameter testing of the finished wafers.

- **A.Design-Integration**. The client's device design is such that no potential vulnerabilities are added to it by the integration for the photomask fabrication performed by the Data Preparation process at Landshut site.

- **A.Security.** All Sites' clients and suppliers are responsible for all security certifications related to their internal management and processing of physical and logical goods, as well related to exchanging goods with LFoundry. Based upon those certifications, the configurations items exchanged between LFoundry and its clients or suppliers are not compromised by internal management and processing performed by clients or suppliers as part of the life cycle activities that are not under LFoundry direct control.

Additional information on preconditions required from the client of the site and further explanations on the assumptions are given in chapter 8 of the Site Security Target [SST].

7.7 Documentation

This is a site certification and therefore the only deliverables existing is the internal documentation of the site as provided during the evaluation and as referred to in the evaluation referred document list. No guidance is provided by the site to be considered by the client in addition to the Site Security Target [SST].

7.8 Evaluation conduct

The full version of the Site Security Target [SST] is the basis for this certification. It is based on the Life Cycle Definition and the Security Problem Definition as outlined in the Security IC Platform Protection Profiles ([BSI-35] and [BSI-84]).

The certification of the site covers the following life cycle phase:

- Mask data preparation;

- wafer production.

The Site Security Target [SST] claimed the following Common Criteria Part 3 life cycle security assurance components to be part of the evaluation:

- CM capabilities – ALC_CMC.4

- CM scope – ALC_CMS.5

- Delivery – ALC_DEL.1

- Development security – ALC_DVS.2

- Life-cycle definition – ALC_LCD.1

- Tools and techniques – ALC_TAT.2

The assurance refinements outlined in the Site Security Target were followed in the course of the evaluation. The refinements of the components are consistent with those defined in the Security IC Platform Protection Profiles ([BSI-35] and [BSI-84]).

The specific scope of these components relevant to this site is explained in the Site Security Target [SST], chapter 7. As outlined in the Site Security Target, the activities of the site are not related to Delivery – ALC_DEL and Tools and techniques ALC_TAT. However, the components have been claimed in order to ensure the assessment of related items during the evaluation process and therefore to support the reuse of the evaluation results in a product evaluation accordingly.

For the assessment of the security measures attackers with high attack potential are assumed. This allows an evaluation of products using this site according to the assurance component AVA_VAN.5. For more details refer to the Site Security Target [SST], chapter 3 and 4.

8 Evaluation outcome

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The objective of the evaluation was to provide assurance that the site complies with the security problem definition described in the associated Site Security Target [SST]; the potential clients of the site should review also the Site Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM], and following the recommendations contained in the supporting documents provided by the international agreements CCRA and SOGIS, [SC-CC] and [SC-SOGIS], respectively.

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS Selta).

The evaluation was completed on 20 June 2018 with the issuance by LVS of the Evaluation Technical Report [ETR], which was approved by the Certification Body on 25 July 2018. Then, the Certification Body issued this Certification Report.

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR] issued by the LVS Selta and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that the LFoundry Avezzano (Italy) and LFoundry Landshut (Germany) production sites comply with the requirements for the assurance components of the AST and ALC classes.

Table 1 summarizes the final verdict of each activity carried out by the LVS Selta.

The specific scope of these components relevant to this site is explained in the Site Security Target [SST], chapter 7. As outlined in the Site Security Target, the activities of the site are not related to Delivery – ALC_DEL and Tools and techniques ALC_TAT. However, the components have been claimed in order to ensure the assessment of related items during the evaluation process in order to support the reuse of the evaluation results in a product evaluation.

The assurance components are derived from the assurance level EAL5 of the CC assurance class "Life-cycle Support" augmented by ALC_DVS.2, while for the assessment of the security measures attackers with high attack potential are assumed, corresponding to the AVA_VAN.5 component.

Therefore, this Site Certification supports product evaluations up to the assurance level EAL5+, augmented by ALC_DVS.2 and AVA_VAN.5.

Assurance classes and components		Verdict
Security Target evaluation	**Class AST**	Pass
SST introduction	AST_INT.1	Pass
Conformance claims	AST_CCL.1	Pass
Security problem definition	AST_SPD.1	Pass
Security objectives for the development environment	AST_OBJ.1	Pass
Extended assurance components definition	AST_ECD.1	Pass
Derived security assurance requirements	AST_REQ.1	Pass
Site Summary Specification	AST_SSS.1	Pass
Life cycle support	**Class ALC**	Pass
Production support, acceptance procedures and automation	ALC_CMC.4	Pass
Development tools CM coverage	ALC_CMS.5	Pass
Sufficiency of security measures	ALC_DVS.2	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass
Compliance with implementation standards	ALC_TAT.2	Not applicable
Delivery procedures	ALC_DEL.1	Not applicable

Table 1 – Final verdicts for assurance components

The evaluation has confirmed for the type of product considered that the phases of the development and production life cycle and the related processes as stated in the SST is covered by the site.

The certification results only apply to the site as indicated in the certificate, the scope as defined in the Site Security Target and on the condition that all the stipulations are kept as detailed in this Certification Report.

8.2 Obligations and notes for the usage of the site

The relevant information for using the evaluated scope of the site within product evaluations is given in the Site Security Target [SST]. During a product evaluation the evidence for the fulfilment of the Assumptions given in section 4.4 of the SST shall be examined by the evaluator of the product when re-using the results of this site evaluation. Note that the sponsor of a potential product evaluation has to ensure that all information required by the Assumptions is made available.

The network for the processing of the received GDS2 data fulfils the requirements for network separation and allows secure data processing. LFoundry. needs to ensure that appropriate resources are assigned to this network. If a secure product requires mask data processing by LFoundry, they shall explicitly confirm to the client that the secure data processing network is used to process the mask data.

A Site Technical Audit Report [ST-AR] has been created in the course of the evaluation. This subset of the full audit report is valid to support a harmonized re-use of the site audit results.

For reusing the evaluation results in product evaluations, the specific scope of the assurance components as relevant at this site and outlined in the Site Security Target has to be assessed if it fits into the product life cycle considered.

The assets assessed, any limitations in covering confidentiality and integrity aspects and the resistance level to attacker (AVA_VAN) applied have to be considered according to the SST when re-using the evaluation results in a product evaluation.

8.3 Recommendations

The conclusions of the Certification Body OCSI are summarized in Section 6 – Statement of certification.

Potential clients of the LFoundry Avezzano (Italy) and LFoundry Landshut (Germany) production sites are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Site Security Target [SST].

This Certificate only applies to the site and its evaluated scope as indicated. The assurance components are only valid on the condition that all assumptions and preconditions required by the site, as given in this Certification Report and the Site Security Target [SST], are observed.

In particular, the Security Problem Definition for this sites comprises security problems derived from threats against relevant assets and for the type of TOE considered as well as security problems derived from the configuration management requirements. The assets, assumptions, threats and organizational security policies are defined in the document Site Security Target [SST], chapter 4. They are derived from the Security IC Platform Protection Profiles ([BSI-35] and [BSI-84]). Only aspects that are applicable to the life cycle phase 3 are considered here: Mask data preparation and wafer production. The security objectives for the site are derived from these threats and organizational security policies as stated in the Site Security Target [SST], chapter 5.

In case of changes to the certified site, the validity can be extended to the changed site, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified site, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.