



PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale  
Agence nationale de la sécurité des systèmes d'information

## **Certification Report ANSSI-CC-2011/17**

### **LinqUs USIM 128k platform on SC33F640E**

*Paris, 17<sup>th</sup> of June 2011*

**Courtesy Translation**



## Warning

This report is designed to provide sponsors with a document enabling them to assess the security level of a product under the conditions of use and operation defined in this report for the evaluated version. It is also designed to provide the potential purchaser of the product with the conditions under which he may operate or use the product so as to meet the conditions of use for which the product has been evaluated and certified; that is why this certification report must be read alongside the evaluated user and administration guidance, as well as with the product security target, which presents threats, environmental assumptions and the supposed conditions of use so that the user can judge for himself whether the product meets his needs in terms of security objectives.

Certification does not, however, constitute a recommendation product from ANSSI (French Network and Information Security Agency), and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.



Any correspondence about this report has to be addressed to:

Secrétariat général de la défense et de la sécurité nationale  
Agence nationale de la sécurité des systèmes d'information  
Centre de certification  
51, boulevard de la Tour Maubourg  
75700 PARIS cedex 07 SP  
France

[certification.anssi@ssi.gouv.fr](mailto:certification.anssi@ssi.gouv.fr)

Reproduction of this document without any change or cut is authorised.



<i>Certification report reference</i>	<b>ANSSI-CC-2011/17</b>	
<i>Product name</i>	<b>LinqUs USIM 128k platform on SC33F640E</b>	
<i>Product reference / version</i>	<b>T1017287 / Release A</b>	
<i>TOE reference / version</i>	<b>S1092122/ Release A</b>	
<i>Protection profile conformity</i>	<b>[PP JCS-O], version 2.6 Java Card System Protection Profile - Open Configuration</b>	
<i>Evaluation criteria and version</i>	<b>Common Criteria version 3.1 revision 3</b>	
<i>Evaluation level</i>	<b>EAL 4 augmented ALC_DVS.2, AVA_VAN.5</b>	
<i>Developers</i>	<b>Gemalto</b> La Vigie, Av du Jujubier, ZI Athelia IV, 13705 La Ciotat Cedex, France	<b>STMicroelectronics</b> 190 avenue Celestin Coq, ZI de Rousset, B.P. 2, 13106 Rousset, France
<i>Sponsor</i>	<b>Gemalto</b> La Vigie, Av du Jujubier, ZI Athelia IV, 13705 La Ciotat Cedex, France	
<i>Evaluation facility</i>	<b>THALES - CEACI (T3S – CNES)</b> 18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France Phone: +33 (0)5 62 88 28 01 or 18, email : nathalie.feyt@thalesgroup.com	
<i>Recognition arrangements</i>	<b>CCRA</b> 	<b>SOG-IS</b> 
	<b>The product is recognised at EAL4 level.</b>	

# Introduction

## The Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated April, 18th 2002, modified. This decree stipulates that:

- The French Network and Information Security Agency draws up **certification reports**. These reports indicate the features of the proposed security targets. They may include any warnings that the authors feel the need to mention for security reasons. They may or may not be transmitted to third parties or made public, as the sponsors desire (article 7).
- The **certificates** issued by the Prime Minister certify that the copies of the products or systems submitted for evaluation fulfil the specified security features. They also certify that the evaluations have been carried out in compliance with applicable rules and standards, with the required degrees of skill and impartiality (article 8).

The procedures are available on the Internet site [www.ssi.gouv.fr](http://www.ssi.gouv.fr).



# Contents

<b>1. THE PRODUCT .....</b>	<b>6</b>
1.1. PRESENTATION OF THE PRODUCT.....	6
1.2. EVALUATED PRODUCT DESCRIPTION .....	6
1.2.1. <i>Product identification</i> .....	6
1.2.2. <i>Security services</i> .....	7
1.2.3. <i>Architecture</i> .....	8
1.2.4. <i>Life cycle</i> .....	10
1.2.5. <i>Guidance</i> .....	12
1.2.6. <i>Evaluated configuration</i> .....	12
<b>2. THE EVALUATION.....</b>	<b>13</b>
2.1. EVALUATION REFERENTIAL .....	13
2.2. EVALUATION WORK .....	13
2.3. CRYPTOGRAPHIC MECHANISMS ROBUSTNESS ANALYSIS.....	13
2.4. RANDOM NUMBER GENERATOR ANALYSIS .....	13
<b>3. CERTIFICATION.....</b>	<b>14</b>
3.1. CONCLUSION .....	14
3.2. RESTRICTIONS .....	14
3.3. RECOGNITION OF THE CERTIFICATE .....	15
3.3.1. <i>European recognition (SOG-IS)</i> .....	15
3.3.2. <i>International common criteria recognition (CCRA)</i> .....	15
<b>ANNEX 1. EVALUATION LEVEL OF THE PRODUCT.....</b>	<b>16</b>
<b>ANNEX 2. EVALUATED PRODUCT REFERENCES .....</b>	<b>17</b>
<b>ANNEX 3. CERTIFICATION REFERENCES .....</b>	<b>19</b>

# 1. The product

## 1.1. Presentation of the product

The evaluated product is the « LinqUs USIM 128k platform on SC33F640E, reference T1017287, release A » developed by Gemalto and STMicroelectronics.

This product is a (U)SIM Java Card platform embedded in an open (U)SIM card intended to be plugged in a mobile phone or other mobile devices.

This product can host applications that can be loaded and instantiated onto the product either before card issuance or in post-issuance through the mobile network, over-the-air (OTA) and in a connected environment and without physical manipulation of the TOE. Other administrative operations can also be done using OTA.

## 1.2. Evaluated product description

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operational environment.

This security target is conformant to [PP JCS-O] protection profile, this conformity is demonstrable. Security objectives have been added to the security target [ST] to deal with the Telecom characteristics of this product.

### 1.2.1. Product identification

The configuration list [CONF] identifies the product's constituent elements.

The certified version of the TOE can be identified by several means identified in the delivery sheet [DS].

- Response to the GetData command (0x00 0xCA 0x9F 0x7F), corresponds to the following CPLC<sup>1</sup> information:

IC Fabricator	0x47 0x50 (ST)
ICType	0x00 0x25 (SC33F640)
osId	0x00 0x27 (STM027)
osDate	0x03 0x40 (YDDD)
osVersion	0x01 0x0C

- Response to the GlobalPlatform GetData command (0x00 0xCA 0x00 0x66) of the card manager gives the Card Recognition Data:

	<b>TOE: S1092122</b>
Complete label of the product (including developer tools)	1.23.1.18

<sup>1</sup> Card manager Production Life Cycle



Software label	1.23.1.12
Card Recognition Data	0070666664736206072A864886FC6B01600B06092A864886FC6B020202630906072A864886FC6B03640B06092A864886FC6B048000640B06092A864886FC6B040255650A06082A864886FC6B05046619060A2B060104012A026E0102060B47544F463634300117010C  SCP <sup>1</sup> : 0x02, 0x 55 Software label: 0x01, 0x17, 0x01, 0x0C

Main difference between the product and the platform (the TOE) references rely on the identification of the list of pre-issuance<sup>2</sup> applications loaded on this smartcard.

All the applications that were present on the configuration made available to the evaluator are detailed in [App\_list]. This document lists the packages and applets, included in the product configuration, with there associated names and AIDs<sup>3</sup>.

The GetStatus command permits the user to check what the installed applets and packages are on the product at his disposal.

### 1.2.2. Security services

The product provides the following evaluated security services:

- Confidentiality and integrity of cryptographic keys and application data during execution of cryptographic operations;
- Confidentiality and integrity of authentication data and application data during execution of authentication operations;
- Isolation of applications belonging to different contexts from each other and confidentiality and integrity of application data among applications;
- Integrity of the application code execution.

The product offers additional evaluated security services for applications management, relying on the GlobalPlatform framework:

- Privileges delegation: The MNO<sup>4</sup> as Card issuer is initially the only entity authorized to manage applications (loading, instantiation, deletion) through a secure communication channel with the card during the 7th phase of the smartcard (usage phase, see chapter 1.2.4). However, the MNO can grant these privileges to an Application Provider (AP) through the delegated management functionality of Global Platform (GP).
- Application signature verification: All loaded applications are associated at load time to a Verification Authority (VA) signature (Mandated DAP) that is verified on card by the on-card representative of the VA prior to the completion of the application loading operation and prior to the instantiation of any applet defined in the loaded application.
- Security Domain management: Application Providers have Security Domain keysets enabling them to be authenticated to the corresponding Security Domain

<sup>1</sup> Secure Channel Protocol

<sup>2</sup> loading realised before the 7th phase of the smart card life cycle

<sup>3</sup> Application Identifier

<sup>4</sup> Mobile Network Operator

and to establish a trusted channel between the TOE and an external trusted device. These Security Domains keysets are not known by the Card issuer.

### ***1.2.3. Architecture***

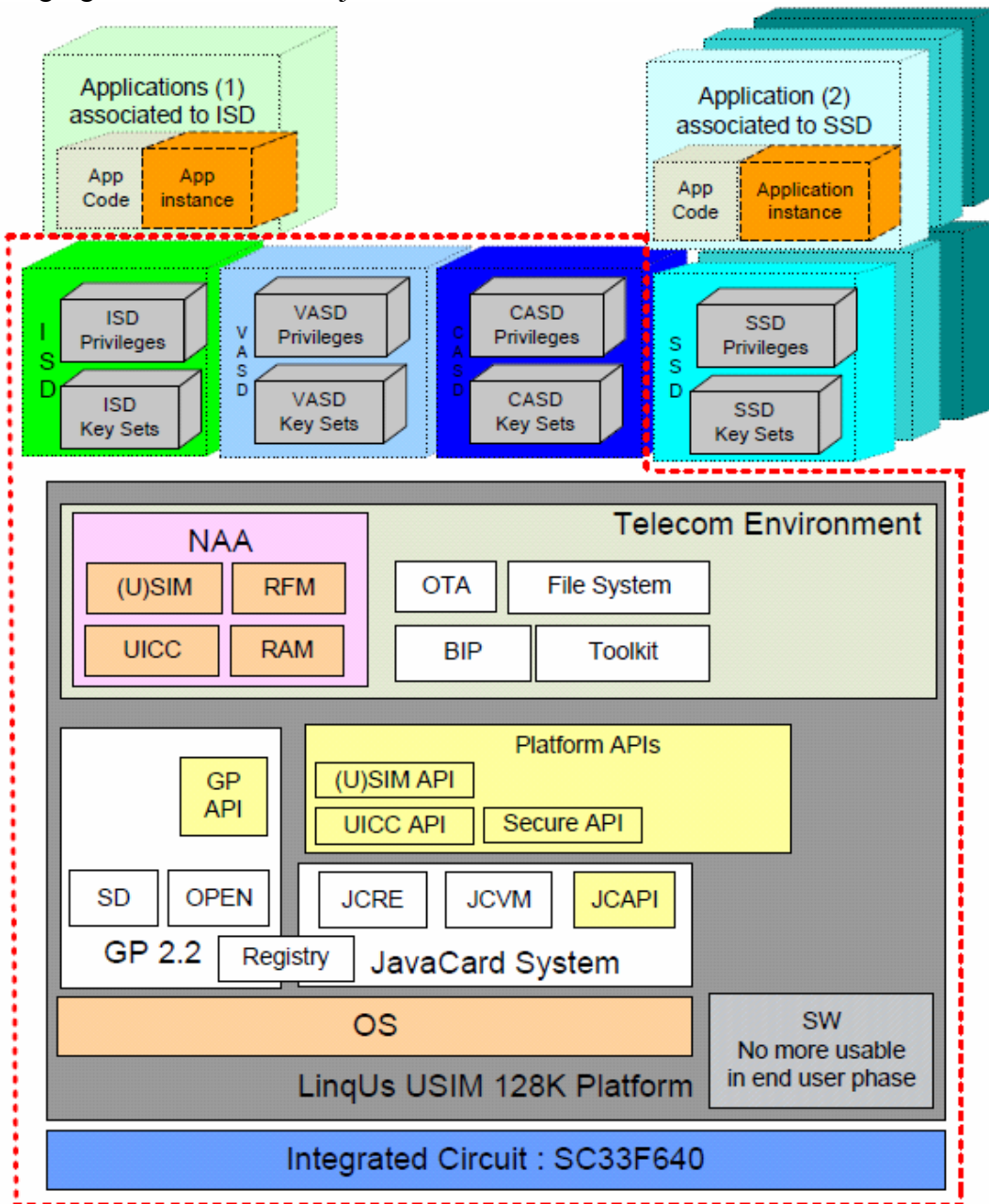
The product is composed of the following components:

- The microcontroller SC33F640 revision E,
- A Java Card System which manages and executes applications called applets. It also provides APIs to develop applets on top of it, in accordance with the Java Card specifications.
- GlobalPlatform (GP) packages (partially evaluated), which provides an interface to communicate with the smart card and manage applications in a secure way
- Platform APIs, which provides ways to specifically interact with (U)SIM applications.
- Telecom environment including network authentication applications (not evaluated) and Telecom communication protocol.





The following figure describes the major items included in the TOE:



(2) : Standard applet

(1) : (2) + Telecom applet +Toolkit applet

USIM, SIM,UICC, RAM, RFM linked to ISD

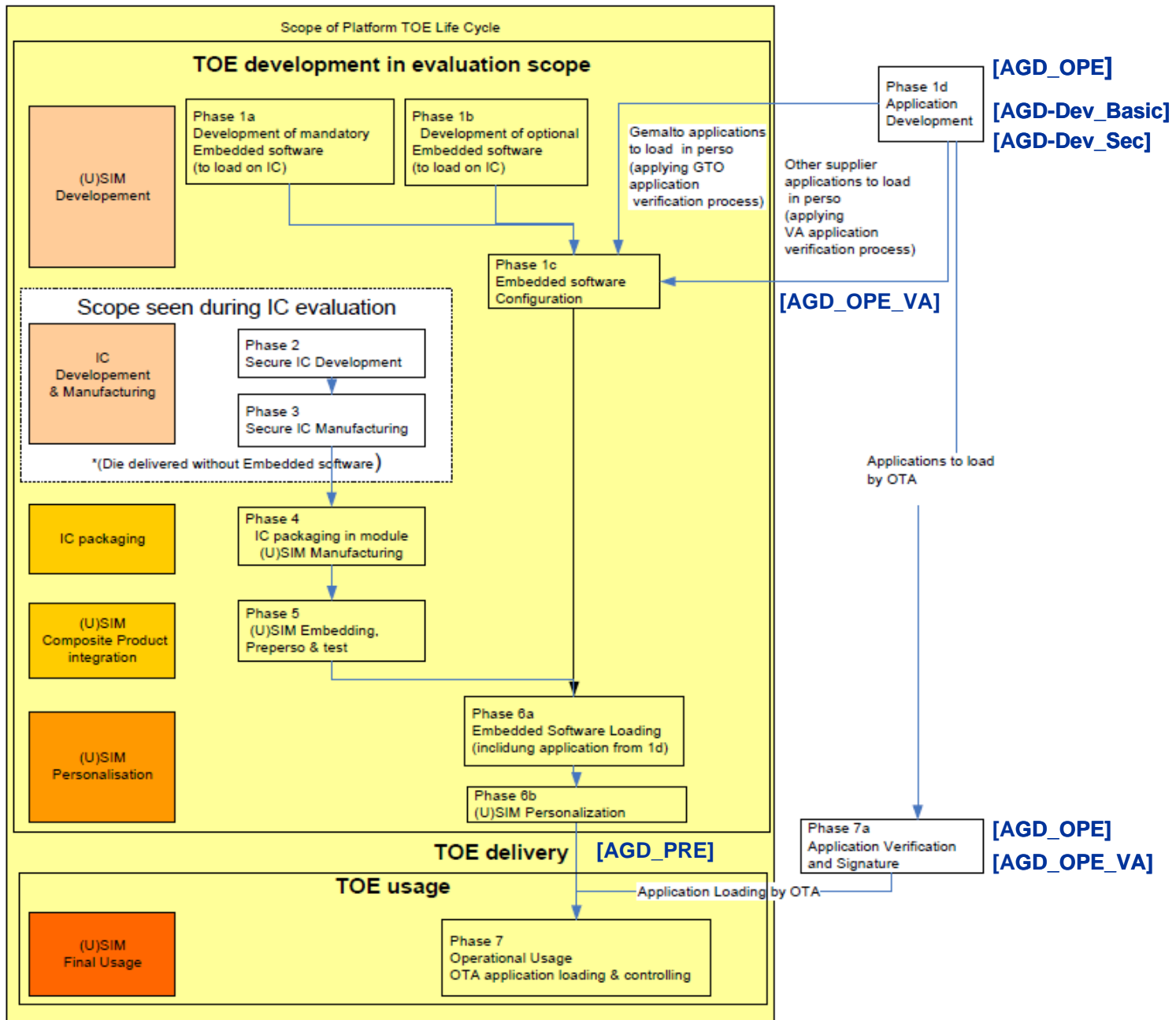
As identified in chapter 1.2.4 here after, the evaluated product has been personalized. Thus all the creation of Security Domains identified in the previous figure has been studied during the evaluation. The product at the disposal of the ITSEF actually contains those Security Domains.

Here the ISD corresponds to the Issuer Security Domain, VASD to the Verification Authority Security Domain, CASD to the Controlling Authority Security Domain and SSD to Supplementary Security Domain.

Some applications were already loaded in the SSD, they are all identified in the [App\_list] document.

### 1.2.4. Life cycle

The product's life cycle is organised as follow:



The product has been developed on the following sites:

#### Development sites

La Vigie  
Avenue du Jujubier  
ZI Athelia IV  
13705 La Ciotat Cedex  
France



8, rue de la Verrerie  
92197 Meudon Cedex  
France

12 Ayar Rajah Crescent  
Singapour 139941  
Singapour

#### **Embedded software configuration sites**

525, Avenue du Pic de Bretagne  
13420 Gemenos  
France

Ul. Skarszewska 2  
83-110 Tczew  
Pologne

#### **Packaging sites**

Rue de Saint Ulfrant  
27500 Pont-Audemer  
France

Ul. Skarszewska 2  
83-110 Tczew  
Pologne

#### **Pre-personalization site**

Rue de Saint Ulfrant  
27500 Pont-Audemer  
France

Ul. Skarszewska 2  
83-110 Tczew  
Pologne

#### **Personalization sites**

Rue de Saint Ulfrant  
27500 Pont-Audemer  
France

Ul. Skarszewska 2  
83-110 Tczew  
Pologne

The microcontroller's development and manufacturing sites are identified in the certification report [ANSSI-CC-2011/07].

Development of pre-issuance applications identified in [App\_list] has been performed in the La Ciotat Development site. Their delivery and verification have also been performed on the La Ciotat site, but by different teams than those who have developed them. According to [NOTE.10], the related procedures have been analysed and audited during the evaluation process.

Procedure to verify pre-issuance application developed by other team than those of Gemalto haven't been analysed, as all the pre-issuance embedded applications considered here are developed by Gemalto.

### ***1.2.5. Guidance***

As the evaluated life cycle corresponds to phases 1 to 6, the preparative guidance of the personalized product [AGD-PRE] is mostly dedicated to recommendations related to the VASD, CASD, ISD, and APSD Security Domain key management.

The operational guidance [AGD-OPE] provides recommendations for each of the following actors:

- The Mobile Network Operator as issuer of the (U)SIM Java Card platform;
- The Application Provider (AP), entity or institution responsible for the applications and their associated services;
- The Controlling Authority (CA), entity independent from the MNO represented on the (U)SIM card and responsible for securing the keys creation and personalization of the Application Provider Security Domain (APSD);
- The Verification Authority (VA), trusted third party represented on the (U)SIM card, acting on behalf of the MNO and responsible for the verification of applications signatures (mandated DAP) during the loading process.

[AGD-OPE] also identifies delivery recommendations that should be enforced for the delivery of new applications to be load in this product.

Moreover the guidance [AGD-Dev\_Basic] and [AGD-Dev\_Sec] describe development rules that have to be followed by applications on this product; and the guidance [AGD-OPE\_VA] describe verification rules that have to be followed by the Verification Authority.

### ***1.2.6. Evaluated configuration***

The open configuration of the product has been evaluated according to [NOTE.10]: this product corresponds to an open and isolating platform. Thus new applications loading that respect the constraints stated in chapter 3.2 and are loaded according to the audited process do not impact the current certification report.

All applications identified in [App\_list] have been verified according to [AGD-OPE\_VA].



## 2. The evaluation

### 2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 3.1 revision 3** [CC], with the Common Evaluation Methodology [CEM].

In order to meet the specificities of smart cards, the [CC IC] and [CC AP] guides have been applied.

### 2.2. Evaluation work

The evaluation has been performed according to the composition scheme as defined in the guide [COMP] in order to assess that no weakness comes from the integration of the software in the microcontroller already certified.

Therefore, the results of the evaluation of the microcontroller “SC33F640E” at EAL5 level augmented with ALC\_DVS.2 and AVA\_VAN.5, compliant with the [PP0035] protection profile, have been used. This microcontroller has been certified the 5 april 2011 under the reference ANSSI-CC-2011/07 [ANSSI-CC-2011/07].

The evaluation technical report [ETR], delivered to ANSSI the 31<sup>st</sup> May 2011 provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are “**pass**”.

### 2.3. Cryptographic mechanisms robustness analysis

The robustness of cryptographic mechanisms hasn't been analysed by ANSSI. Nevertheless the evaluation hasn't lead to the identification of design or construction vulnerabilities for the targeted AVA\_VAN level.

### 2.4. Random number generator analysis

The platform performs a cryptographic post-processing of the outputs of the material random generator provided by the underlying microcontroller that have been studied during this evaluation.

The evaluation hasn't identified exploitable vulnerabilities for the targeted AVA\_VAN level if the [AGD-Dev\_Sec] guidance is correctly applied.

## 3. Certification

### 3.1. Conclusion

The evaluation was carried out according to the current rules and standards, with the required competency and impartiality of a licensed evaluation facility. All the work performed permits the release of a certificate in conformance with the decree 2002-535.

This certificate testifies that the product “LinqUs USIM 128k platform on SC33F640E, reference T1017287, release A” submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 4 augmented.

### 3.2. Restrictions

This certificate only applies on the product specified in chapter 1.2 of this certification report.

The user of the certified product shall respect the security objectives for the operational environment, as specified in the security target [ST], and shall respect the recommendations in the guidance [GUIDES], in particular:

- Applications developers must follow the guidance for basic applications development [AGD-Dev\_Basic] or the guidance for secure applications development [AGD-Dev\_Sec] depending of the sensibility of the targeted application;
- The Verification Authority must follow the guidance for verification authority [AGD-OPE\_VA].

### 3.3. Recognition of the certificate

#### 3.3.1. European recognition (SOG-IS)

This certificate is released in accordance with the provisions of the SOG-IS agreement [SOG-IS].

The European Recognition Agreement made by SOG-IS in 2010 allows recognition from Signatory States of the agreement<sup>1</sup>, of ITSEC and Common Criteria certificates. The European recognition is applicable, for smart cards and similar devices, up to ITSEC E6 High and CC EAL7 levels. The certificates that are recognized in the agreement scope are released with the following marking:



#### 3.3.2. International common criteria recognition (CCRA)

This certificate is released in accordance with the provisions of the CCRA [CC RA].

The Common Criteria Recognition Arrangement allows the recognition, by signatory countries<sup>2</sup>, of the Common Criteria certificates. The mutual recognition is applicable up to the assurance components of CC EAL4 level and also to ALC\_FLR family. The certificates that are recognized in the agreement scope are released with the following marking:



---

1 The signatory countries of the SOG-IS agreement are: Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and United Kingdom.

2 The signatory countries of the CCRA arrangement are: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, the Republic of Korea, Malaysia, Netherlands, New-Zealand, Norway, Pakistan, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States of America.

## Annex 1. Evaluation level of the product

Class	Family	Components by assurance level							Assurance level of the product	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Name of the component
ADV Development	ADV_ARC		1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	Implementation representation of the TSF
	ADV_INT					2	3	3		
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	3	Basic modular design
AGD Guidance	AGD_OPE	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	Preparative procedures
ALC Life-cycle support	ALC_CMC	1	2	3	4	4	5	5	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	4	Problem tracking CM coverage
	ALC_DEL		1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			1	1	1	1	2	1	Developer defined life-cycle model
ASE Security Target Evaluation	ALC_TAT				1	2	3	3	1	Well-defined development tools
	ASE_CCL	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	Security problem definition
ATE Tests	ASE_TSS	1	1	1	1	1	1	1	1	TOE summary specification
	ATE_COV		1	2	2	2	3	3	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	1	Testing: basic design
	ATE_FUN		1	1	1	1	2	2	1	Functional testing
AVA Vulnerability assessment	ATE_IND	1	2	2	2	2	2	3	2	Independent testing: sample
	AVA_VAN	1	2	2	3	4	5	5	3	Advanced methodical vulnerability analysis





## Annex 2. Evaluated product references

[ST]	<p>Reference security target for the evaluation:</p> <ul style="list-style-type: none"> <li>- “Security Target LinqUs USIM 128k PK certified using SC33F640”, reference D117263, release 1.7</li> </ul> <p>For the needs of publication, the following security target has been provided and validated in the evaluation:</p> <ul style="list-style-type: none"> <li>- “Security Target LinqUs USIM 128k PK certified using SC33F640”, reference D117263, release 1.7p</li> </ul>
[ETR]	<p>Evaluation technical report :</p> <ul style="list-style-type: none"> <li>- “Evaluation technical report - Project: LIOUQUET2”, reference LI2_ETR, revision 2.0</li> </ul>
[CONF]	<ul style="list-style-type: none"> <li>- Delivery Sheet [DS], reference D1189308;</li> <li>- TOE software configuration list: “TOE file configuration list”, reference listeFichiersPhenix_1_23_1_18 ;</li> <li>- Documentation configuration list: “Documentation configuration list rev 2”, reference Action_List_LIOUQUET2, version 27052011;</li> <li>- Product pre-issuance packages [App_list]: “STM027 : LinqUs USIM 128k PK Certified”, reference Gemalto_STM027_profile description_vA6, release A6.</li> </ul>
[GUIDES]	<p>Preparative guidance :</p> <ul style="list-style-type: none"> <li>- Acceptance and installation guidance [AGD-PRE] : “Preparative Guidance for LinqUs USIM 128K PK certified”, reference D1185540, release 1.3</li> </ul> <p>Operational guidance:</p> <ul style="list-style-type: none"> <li>- Administration guidance [AGD-OPE] : “Guidance for Administration of LinqUs USIM 128K PK certified”, reference D1185542, release 1.3</li> <li>- Guidance for application development <ul style="list-style-type: none"> <li>• Guidance for basic application development [AGD-Dev_Basic]: “Rules for applications on Upteq mNFC certified product”, reference D1186227, release A03</li> <li>• Guidance for secure application development [AGD-Dev_Sec]: “Guidance for secure application development on Upteq mNFC platforms”, reference D1188231, release A04</li> </ul> </li> <li>- Guidance for Verification Authority [AGD-OPE_VA]: “Guidance for Verification Authority of LinqUs USIM 128K PK” reference D1185542_VA, release 1.3</li> </ul>
[PP JCS-O]	<p>Java Card System Protection Profile - Open Configuration, version 2.6, 19 April 2010.  <i>Certified by ANSSI under the reference ANSSI-CC-PP-2010/03</i></p>

[PP0035]	Security IC Platform Protection Profile, version 1.0, 15 June 2007. <i>Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI_PP_0035.</i>
[ANSSI-CC-2011/07]	Secured microcontrollers ST33F1ME, ST33F768E, SC33F768E, ST33F640E, SC33F640E, ST33F512E, SC33F512E and SC33F384E with the optional cryptographic library NesLib v3.0 <i>Certified by ANSSI under the reference ANSSI-CC- 2011/07</i>



### Annex 3. Certification references

Decree number 2002-535, 18th April 2002, modified related to the security evaluations and certifications for information technology products and systems.	
[CER/P/01]	Procedure CER/P/01 - Certification of the security provided by IT products and systems, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 version 3.0, revision 1, March 2009.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001 version 2.7 revision 1, March 2009.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[NOTE.10]	« Application note - Certification of applications on “open and cloisonning platform” », reference ANSSI-CC-NOTE/10.0EN, see ssi.gouv.fr
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010, voir www.ssi.gouv.fr
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 <sup>th</sup> January 2010, Management Committee.