



**Short Public Report**  
**on the 2<sup>nd</sup> Re-certification of the VALid-SSD<sup>®</sup> product**

**Certification No.: EP-P--GMJBG1**

by

**Douwe Korff**

Emeritus Professor of International Law, London Metropolitan University (UK)  
(Legal Expert)

&

**Javier Garcia-Romanillos Henriquez de Luna**

CISA, CISM, CRISC, LA27000, LA22301 (Spain)  
(Technical Expert)

NB: This 2<sup>nd</sup> Re-evaluation report is based on the 1<sup>st</sup> Re-evaluation report, approved by the EuroPriSe Certification Authority in February 2015.

(As approved by the EuroPriSe Certification Authority on 27 January 2018)

**GLOSSARY OF TECHNICAL TERMS AND ABBREVIATIONS USED IN THIS REPORT IN RELATION TO THE DESCRIPTION OF THE TARGET OF EVALUATION (TOE):**

Client or User (= the controller)	the <i>Client</i> of the developer of the TOE (ValidSoft UK Ltd), i.e. the <i>User</i> of the TOE, this being the entity communicating with the <i>person concerned</i> (also) by mobile phone, typically in an authentication process, including more specifically an “ <i>Out-Of- Band</i> ” ( <i>OOB</i> ) authentication process.
HLR	The Home Location Register maintained by every Mobile [Phone] Network Operator ( <i>MNO</i> ), containing the details of every mobile phone registered with that <i>MNO</i> . In order to allow phone calls to be made to and from different countries, every <i>MNO</i> requires access to every other <i>MNO</i> ’s HLR that they have a roaming agreement with.
SIM Card	a SIM card or “Subscriber Identity Module” is a type of portable memory chip used in most modern cellular (i.e., mobile) telephones. The SIM card holds personal identity information, the cell phone number, phone book, text messages and other data. It can be thought of as a mini hard disk that automatically activates the phone into which it is inserted. See: <a href="http://www.wisegeek.com/what-is-a-sim-card.htm">http://www.wisegeek.com/what-is-a-sim-card.htm</a>
SIM Card Number (= IMSI Number)	The number, known technically as the “International Mobile Subscriber Identity” (or “IMSI”) number, by which a SIM card is identified within the global international e-communications system. Although normally a person’s SIM card (and thus this number) is associated with that person’s usually-used mobile phone, it is in fact easy to either put one’s SIM card into another phone while retaining the same mobile phone number (as explained on the website mentioned above), or to ask one’s <i>MNO</i> to associate one’s registered mobile phone number with a new SIM card (and thus with a new SIM card number); and the latter can be done fraudulently, in so-called “ <i>Pseudo-Device-Theft</i> ”.
MNO	Mobile Network Operator: a <i>TSP</i> that provides mobile telephone services to individuals who subscribe to their service (subscribers).
“Out Of Band” (OOB) authentication system	an authentication system in which one “band” or channel of communication, typically the mobile phone system, is used to verify a parallel communication on another “band” or channel, typically the Internet.
Person Concerned / Subscriber (= the data subject)	a person who has a mobile phone, i.e. who is a <i>subscriber</i> to a mobile phone service offered by an <i>MNO</i> , and who uses this mobile phone to communicate with a private- or public-sector entity that is using the TOE (the <i>Client</i> of the developer of the TOE, ValidSoft UK Ltd, who is also the <i>User</i> of the TOE), also and in particular in “ <i>Out-Of- Band</i> ” ( <i>OOB</i> ) authentication procedures.
“Pseudo Device Theft”	ValidSoft’s term for a type of fraud in which attackers deceive the <i>MNO</i> of which the <i>person concerned</i> is a subscriber that that individual has obtained a new <i>SIM card</i> for his or her mobile phone, or a new phone, but wants to retain the original mobile phone number. The <i>MNO</i> then substitutes (by ‘number porting’) the new (fraudulent) <i>SIM card number</i> for the original one, and calls or SMS messages to the original individual’s mobile phone will be passed on to the new (fraudulent) card - i.e., to a mobile phone controlled by the criminal - rather than to the mobile phone of the actual subscriber. This divergence of the call can undermine <i>OOB authentication systems</i> in particular.
TSP	Telecommunications Service Provider, or to use the fuller technical term in the <u>e-Privacy Directive</u> , a provider of “publicly available electronic communications services in [a] public communications network”. There are retail- and Business-to-Business (B2B) TSPs.



## Short Public Report

### Recertification No. EP-P-GMJBG1

#### 1. Name and version of the IT product or IT-based service:

- Name of Product:** VALid-SSD®  
(ValidSoft's SIM-Swap Detection (SSD) product to counter Sim Swap fraud)
- Product Description:** The TOE, VALid-SSD®, is a fraud prevention tool that allows the user of the TOE, who wants to communicate with the data subjects (also) by means of a mobile phone (i.e., by either making calls to the data subjects or by sending them SMS messages), typically in "Out-Of-Band" authentication processes, to check that the SIM card in the to-be-called mobile phone has not been swapped, in order to ensure the integrity of the call or message and process.  
*This is the sole purpose of the VALid-SSD® product.*
- Version:** Version 3.5, September 2012  
NB: This is the same version as the one that was evaluated in the original evaluation in 2012: the TOE has not changed in any way.

#### 2. Manufacturer or vendor of the IT product:

- Company Name:**  
ValidSoft Ltd
- Address:**  
Arthur Cox Building  
Earlsfort Terrace  
Dublin 2  
Ireland
- Contact Persons and Contact Details:**  
Mr. Pat Carroll, CEO, ValidSoft Ltd  
Alexander Korff, Esq., General Counsel for ValidSoft Ltd  
Address as above  
Emails: [Pat.Carroll@validsoft.com](mailto:Pat.Carroll@validsoft.com), [alexander.korff@validsoft.com](mailto:alexander.korff@validsoft.com)

**3. Time frame of evaluation:**

November 2017 – January 2018

**4. EuroPriSe Experts who evaluated the IT product:**

**Name of the Legal Expert:**

Prof. Douwe Korff

**Address of the Legal Expert:**

Wool Street House  
Gog Magog Hills  
Babraham  
Cambridge CB22 3AE  
United Kingdom

**Name of the Technical Expert:**

Javier Garcia-Romanillos Henriquez de Luna

**Address of the Technical Expert:**

Calle Zurbarán 7, 6B, 28010 Madrid, Spain

**5. Certification Authority:**

**Name:** EuroPriSe Certification Authority

**Address:** Joseph-Schumpeter-Allee 25  
53227 Bonn  
Germany

**Email:** [contact@european-privacy-seal.eu](mailto:contact@european-privacy-seal.eu)

## 6. Specification of Target of Evaluation (ToE):

The sole purpose of the VALid-SSD<sup>®</sup> product is to check whether a potentially fraudulent SIM swap has occurred. In this, VALid-SSD<sup>®</sup> acts as a stand-alone product, but one that is designed to be integrated with authentication systems it supports (including but not limited to ValidSoft's own VALid<sup>®</sup> authentication and VALid-POS<sup>®</sup> solutions).

The VALid-SSD<sup>®</sup> product works by “looking up” the SIM card numbers of the to-be-checked mobile phones, and then correlating the initially established SIM card numbers of mobile telephone subscribers registered with the VALid-SSD<sup>®</sup> user against the SIM card numbers identified in a look-up at the point of (or shortly after: see below) an OOB authentication session.

When VALid-SSD<sup>®</sup> determines that a mobile subscriber's SIM card number has changed (or has recently changed), this is passed on to the Client/User of VALid-SSD<sup>®</sup>. A Client/User may choose to treat an unrecognised SIM card number as suspicious and take the action it deems appropriate.

The TOE can be associated with the user's authentication systems in different ways. One possibility is to carry out the lookup, and thus the verification, shortly after the user's own authentication process has been completed - i.e., in essence as a subsequent extra check. This method can be chosen in circumstances in which remedial action against a probably fraudulent act can still be taken some time after the act.

Alternatively, the lookup can be built into an authentication system right at the beginning, before the user's own authentication process, so that, if the TOE reports that a SIM swap has occurred, the normal authentication process can be aborted immediately.

The point to be made here is that the SSD lookup thus effectively stands on its own: it is linked to, but separate from the user's wider authentication processes.

## 7. General description of the IT product:

### 7.1 Background:

In an increasingly mobile and global world, individuals, companies and public authorities want to communicate more and more by means of various electronic communications channels, including both the Internet and mobile phone networks. In this, it is often crucial that the integrity of the communication is guaranteed - more in particular, that measures are taken to ensure that if a mobile phone is called, or if an SMS (“text”) message is sent to a mobile phone, the call or the message actually gets put through to the intended mobile phone. This is particularly important in so-called “Out Of Band” (OOB) authentication systems, in which the mobile phone communication system is used to verify a parallel communication on another system (“band” or channel), typically the Internet.

More specifically, such OOB authentications may involve the making of a call, or the sending of an SMS message, to the mobile phone of an individual whose online actions are to be authenticated. These communications all assume (or at least would like to assume) that when a communication is made to the mobile telephone number of the individual in question, the communication will be terminated to the actual mobile phone of that individual. However, calling, or sending a message to a specific mobile number does not, as such, fully guarantee that the call or message will be terminated to the phone originally associated with that number.

This is because the mobile phone in question is identified within the international e-communications system by a number, known as the International Mobile Subscriber Identity (“IMSI”) number (in this report hereafter referred to more simply as the SIM card number), which is changed when a new SIM card is used. Typically, this happens legitimately when a subscriber loses or replaces his or her mobile phone, and obtains a new SIM card. However, increasingly this also occurs as a consequence of what ValidSoft calls “Pseudo Device Theft”.

In such “Pseudo Device Thefts”, attackers deceive the MNO of which the individual is a subscriber that that individual has obtained a new SIM card for his or her mobile phone, or a new phone, but wants to retain the original mobile phone number. The MNO then substitutes the new (fraudulent) SIM card number for the original one, and calls or SMS messages to the original individual’s mobile phone will be passed on to the new (fraudulent) card - i.e., to a mobile phone controlled by the criminal - rather than to the mobile phone of the actual subscriber. This divergence of the call can undermine the OOB authentication systems mentioned earlier.

**The TOE evaluated in this report has the sole purpose of detecting such a divergence.**

## 7.2 Further details of the TOE:

As explained above, the sole purpose of the TOE is to ensure the integrity of a communication with a mobile phone (the making of a call or the sending of an SMS message) that a user of the TOE wants to initiate, or has recently made.

The TOE is therefore linked to the user’s system that makes the call or sends the message, in that, either right at the beginning of this process, before the actual putting through of the call or the message, or shortly afterwards, the TOE checks that the SIM card of the mobile phone in question has not been swapped. It does this by “looking up” the SIM card number associated with the phone number on record: if that number has changed since the last look-up, this means that the SIM card has been swapped, possibly fraudulently. The two charts on page 25 f. outline the data flows involved in the use of the TOE. These are discussed after that.

Here, we should stress that this is all that the TOE does: it carries out the lookups, and passes on the results of these (in the form of a “SIM not swapped” [+] / “SIM swapped” [-] / “Fail” [0] = check was not possible) to the user of the TOE.

### 7.3 What is and what is not included in the TOE:

The TOE is essentially quite simple: it consists of a carrier with software (the VALid-SSD™ “box”), which has a database at its heart, with two data flows to and from the user’s own systems, and two to and from the databases accessible to all Mobile Network Operators (which are accessed through the systems of the partner-TSP that supports the TOE).

In general terms, the Target of Evaluation (TOE) includes all the data, data flows and data processing within the SSD “box”, and the data processing relating to data flows into and out of the “box” of which the user of the “box” is the controller, but it does not include other data, or processing by the controller prior to or after his use of the “box”, or processing by others (including ValidSoft’s partner-TSP) except insofar as certain legal arrangements between the controller and others are concerned, as reflected in the product documentation and relevant guarantees and warranties.

More specifically:

- ✓ The evaluation covered the question of the status of each entity involved in the processing of data by means of the SSD “box”, in data protection terms, i.e. the question of who is to be regarded as the “controller” of (some or all of) the processing, and who as “processor(s)” and “third party(-ies)”;<sup>\*</sup> and
- ✓ The evaluation also included an assessment of the compliance with all relevant EC data protection requirements by the controller of the processing relating to the use of the VALid-SSD® “box”, in the light of the determination of the various entities’ status;<sup>\*</sup>

\*Note:

The evaluation concluded that the user of the SSD “box” is to be regarded as the controller of all the processing associated with the use of the SSD “box”. This affected the scope of the evaluations of the different data flows. It also meant that the terms “controller [of the processing associated with the use of the SSD “box”]”, “user [of the SSD “box”]” and “the client” are often used interchangeably (although we have tried to avoid confusion).

With regard to the various phases of the processing and the specific data flows:

PROCESSING PRIOR TO THE USE OF THE TOE:

- *The TOE and this evaluation did NOT cover the processing of personal data by the user of the TOE prior to the latter’s use of the TOE, the user’s own processing systems and databases, the obtaining of the mobile numbers of the data subjects by the user of the TOE, or the storing of those numbers in the user’s own databases (such as, typically, the user’s customer database), EXCEPT THAT:*
- ✓ The evaluation did include the Conditions of Use for the TOE that stipulate that the user of the TOE must have obtained those mobile phone numbers lawfully (and in particular in accordance with all the requirements of the relevant [= applicable] national data protection law and EU data protection rules), and that that user must have a valid legal basis for the making of telephone calls, or the sending of SMS messages (as applicable), to the mobile phones of the data subjects; and
- ✓ The evaluation did cover the Conditions of Use for the TOE that require the controller/user of the TOE to adopt appropriate (state of the art) security and confidentiality measures in relation to the data obtained or processed in relation to the user’s use of the TOE, in particular in relation to the data flows into and out of the TOE;

BUT:

- *The evaluation did NOT cover the question of actual compliance with the requirements of national or EC data protection rules by the user beyond the provision of the relevant guarantees and warranties and penalty clauses; and*
- *The evaluation similarly did NOT include an assessment of the actual data security and –confidentiality measures adopted by the controller/user of the TOE other than in direct relation to the data flows to and from the “box”.*

INITIAL PROCESSING TO POPULATE THE SSD DATABASE, AND THE SUBSEQUENT CARRYING OUT OF SIM SWAP DETECTION “LOOKUPS”:

- ✓ The TOE and this evaluation included the sending of the mobile phone numbers of the data subjects by the user of the TOE to the SSD “box”;
- ✓ The TOE and this evaluation furthermore covered all processing within, and/or carried out by means of, the TOE (i.e., within the SSD “box”);
- ✓ The TOE and the evaluation also covered the obtaining of the “Results” of the lookups, by the user of the TOE, through the SSD “box”, from the partner-TSP;

and as concerns the carrying out of the actual lookups by the partner-TSP with the aim of obtaining the SIM card numbers associated with the mobile phones in question:

- ✓ The TOE and the evaluation covered the sending of the mobile phone numbers from the SSD “box”, by the user of the TOE, to the partner-TSP’s systems, and the receiving by return, by the “box”, from the partner-TSP, of the SIM card numbers associated with those phone numbers, and the encryption of these numbers within the “box” in such a way that the user cannot actually “see” them.

BUT:

- *The TOE and this evaluation as such did NOT cover the internal processing by the partner-TSP of the data sent to its systems from the SSD “box”, or the processing involved in the accessing, by the partner-TSP, of the MNOs’ HLRs, and the extraction by the partner-TSP of the SIM card numbers from the HLRs prior to the passing on of those numbers to the user of the TOE;*
- *The TOE and this evaluation did NOT cover the arrangements between the partner-TSP and the other MNOs, other than insofar as this is dealt with (or should be dealt with) in any warranties provided by the partner-TSP to the clients; and*
- *The TOE and this evaluation did NOT address general issues concerning the relationship between the person in whose name the mobile in question is registered and the MNO with which s/he has a relationship, or between that MNO and other MNOs, including in particular the partner-TSP, beyond the question of the warranties,*

EXCEPT THAT:

- ✓ Given the crucial importance of the obtaining of the SIM card numbers by the partner-TSP, and the passing on of those numbers to the SSD “box” (and thus strictly speaking to the clients/users of the TOE, although they are fully encrypted and not identifiable to the user), this evaluation did address the question of the legal basis of this obtaining of the SIM card numbers by the partner-TSP, and their further processing by the partner-TSP, including the question of “applicable law” in this respect, and whether this law allows such lookups and disclosures if made in accordance with the legal arrangements made by the parties concerned in relation to the use of the TOE; and
- ✓ This evaluation also included an assessment of the Conditions of Use and other legal arrangements (such as warranties or assurances) that are stipulated, or must be put in



place, between the client/user of the TOE, the developer of the TOE (ValidSoft UK Ltd.) and the partner-TSP, in respect of the above processing;

BUT:

- *It did NOT include an assessment of whether the partner-TSP actually acts in accordance with these guarantees and warranties.*

PROCESSING BY THE USER OF THE TOE UPON RECEIPT OF THE RESULTS OF THE LOOKUPS FROM THE TOE

As described earlier, the “*Result*” of each SIM Swap check by means of the SSD “box” is simply (and only) passed on to the client/user of the TOE, in the form of a simple “*Positive*” (+) (SIM not recently changed), “*Negative*” (-) (SIM was recently changed), or “*Fail*” (0) (check not possible) message; but it is then up to the user of the TOE to decide what use to make of the “*Result*”. Consequently:

- ✓ The evaluation covered the legal arrangements between the developer of the TOE, ValidSoft UK Ltd, the partner-TSP, and the clients/users of the TOE in respect of the passing on of the “*result*” to the clients/users of the TOE,

BUT:

- *It did NOT include the client’s own processing of the data after the passing on of the “Result” from the SSD “box” to the client, i.e., it did NOT cover the way in which these results are further processed or used by the client; and*
- *It did NOT address general issues concerning the relationship between the client/user of the TOE and the data subjects,*

EXCEPT THAT:

- ✓ The evaluation did cover the stipulations in the Condition of Use for the product that the data may only be used for the stipulated purpose; and that a user may not use a “*Result*” in any way incompatible with the in-principle prohibition on the taking of fully-automated “*significant*” decisions, contained in Article 15 of Directive 95/46/EC, or with the rules in the relevant (applicable) law implementing that article; and
- ✓ The evaluation did cover the Conditions of Use for the TOE and the adequacy of the SSD documentation, in relation to the question of whether the documentation adequately alerts the user to the need to ensure transparency about the processing vis-à-vis those data subjects (*but the evaluation did not include an assessment of the adequacy or otherwise of the actual contracts between the user of the product and the data subjects*).

THE MAKING OF CALLS, OR THE SENDING OF SMS MESSAGES, BY THE USER OF THE TOE TO THE DATA SUBJECTS

- *The TOE does not and this re-evaluation did NOT cover the actual making of a call, or the sending of an SMS message, by the user of the TOE to the data subjects,*

EXCEPT THAT (AS ALREADY NOTED):

- ✓ The evaluation did include the Conditions of Use for the TOE that stipulate that the user of the TOE must have obtained the mobile phone numbers of the data subjects lawfully (and in particular in accordance with all the requirements of the relevant [= applicable] national data protection law and EU data protection rules), and that that user must have a valid legal basis for the making of the telephone calls, or the sending of the SMS messages (as applicable), to the mobile phones of the data subjects.

## 8. Transnational issues:

The product is in principle offered to potential clients anywhere in the world. The product also invariably (even if offered to such clients in the EU/EEA) involves worldwide transborder data flows: this is inherent in the making of calls to mobile phones. However, within the TOE, the product only involves one data flow that is subject to the restrictions in Articles 25 and 26 of the main Data Protection Directive, and even this only when the product is used by a client in a non-EU/EEA country: this is the data flow in which, for such clients, the very limited “results” data are sent from the systems of the partner-TSP in the Netherlands (which in such cases hosts the SSD system) to the user/client’s systems outside the EU/EEA.

As concerns the question of “applicable law”, the original evaluation and the first (2015) re-evaluation both concluded, and the current (2018) re-evaluation also finds, that:

- if the client/user of the TOE is established in the EU/EEA, the “applicable law” in relation to all the processing within the TOE will be the national law of the EU/EEA Member State where that client is established (only); and
- if the client is not established in the EU/EEA, that non-EU/EEA based controller must comply with Dutch data protection law (only) because under the arrangements evaluated the SSD “box” is based with a partner-TSP in the Netherlands, and because that “box” constitutes “equipment/means” used for the processing: cf. Art. 4(1)(c) of Directive 95/46/EC).

However, in respect of the latter finding, the current (2018) re-evaluation added that if the SSD “box” were to be placed with a partner-TSP in the UK (as is envisaged), UK data protection law (only) would apply to non-EU/EEA-based clients/users of the TOE (at least for as long as the UK is an EU Member State).<sup>1</sup>

## 9. Tools used by the manufacturer of the IT product:

The TOE essentially consists of a relatively simple software programme installed on a dedicated carrier or “box” linked to the client’s own computers. The software is provided to the client in the form of a configurable software component and is designed to work on a range of platforms that may be adapted to the client’s needs. The main system (ToE) is written in Java. The databases are either hosted on the client’s own environment or at the partner in charge, adapted to their database system (DBMS).

Note: In this report, we often refer to the product as a “box”. However, this is only for ease of reference and to enable the reader to envisage the processing: the product as such really only consists of software; the “box” referred to is thus a purely virtual “box”. For that reason, the word is always placed in quotation marks.

The software facilitates the backup of databases and their restoration, but the constraints are to be defined by the client. The software also facilitates relevant user access

---

<sup>1</sup> The current (2018) re-evaluation does not address the implications of so-called “Brexit”, presumed to happen in March 2019 (although a “transitional”/“implementation” period after that is also planned, during which the EU data protection regime may well continue to apply). As and when the UK would become a “third country” in EU/EU data protection terms, this would constitute a significant change in the legal environment within which the TOE is used, which will require a new evaluation (just as the coming into force of the GDPR will also in due course require a new evaluation).

management, but again this maintenance is the responsibility of the client. The software also facilitates encryption of the internal databases.

**10. Edition of EuroPriSe Criteria used for the evaluation:**

EuroPriSe Criteria, version 2011-11.

**11. Modifications / Amendments of the IT product or IT-based service since the original certification**

The TOE has not changed. Nothing has been added to the TOE. Nothing has been removed from the TOE.

**12. Changes in the legal and/or technical situation since the original certification**

Since the original certification of the TOE in 2012, there have been no changes to the legal or technical requirements that might affect our assessments. However, in 2014, the Article 29 Working Party did issue an opinion on anonymisation techniques that has some relevance, in that the data processed by the partner-TSP can be compared to pseudonymous data. We addressed this in our 1<sup>st</sup> re-evaluation report in section 12, sub-section B; the relevant text is repeated in section 13, sub-section B, below (on p. 25, with a footnote referring to that WP29 opinion).

In the current (2018) 2<sup>nd</sup> re-evaluation, we noted two further legal issues and (in parentheses) a possible future practical change. First of all, we noted that in its Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting (WP224 of 25 November 2014), the WP29 expanded upon the its earlier Opinion 04/2012 on Cookie Consent Exemption (WP194 of 7 June 2012), to deal with the then fairly new phenomenon of “device fingerprinting”. After examining the opinion, we concluded that the use of the TOE does involve such “device fingerprinting”, but that this did not affect our assessment that the TOE (as evaluated) fully complied with EU data protection law.

Secondly, we noted that in January 2018, the Second Payment Services Directive (PSD2) came into effect, but found that this repeated, in Article 97, the provision in its predecessor, the Payments Directive (Article 79), explicitly stipulating that Member States must, in their laws, allow the processing of payment data for fraud prevention (etc.) purposes. Our earlier conclusion, that this underlined that such processing (also) served a “public interest” and was thus also legitimate on that basis, therefore again remained unchanged.

Finally, as already noted, we mentioned in our 2018 re-evaluation report, in parentheses, that in the (not yet achieved but soon-expected) actual deployment of the TOE, the developer of the TOE, ValidSoft, will probably be using a Partner-TSP in the UK, rather than one in the Netherlands. While not yet addressing this yet in full in the report (since it has not yet happened), we do note in various places that, although this could affect the “applicable law” in some cases (as noted earlier), it would not affect our overall assessments of the legality of the processing.

### 13. Evaluation results:

*NB: The legal evaluation carried out by the Legal Expert was based on the EuroPriSe Criteria Catalogue, Version 2011-11. The summary in this short report broadly, but not in every detail, follows the structure of the Catalogue. Next to the headings covering the selected main issues, below, a reference is therefore provided in blue square brackets to the relevant part or section in the Criteria Catalogue. Note that some issues that are not covered in the Catalogue have been added.*

#### A. LEGAL EVALUATION

##### A.1 Fundamental issues [Criteria Catalogue, Part 2 – Set 1]

###### **The purpose of the processing** [Criteria Catalogue, sections 1.1.1 & 2.3.1]

The processing (i.e., all of the processing operations and data flows covered by the TOE) serves (serve) only one purpose:

###### PURPOSE OF THE PRODUCT:

The TOE, VALid-SSD<sup>®</sup>, is a fraud prevention tool that allows the user of the TOE, who wants to communicate with the data subjects (also) by means of a mobile phone (i.e., by either making calls to the data subjects or by sending them SMS messages), typically in “Out-Of-Band” authentication processes, to check that the SIM card in the to-be-called mobile phone has not been swapped, in order to ensure the integrity of the call or message and process.

Or in brief: The carrying out of “SIM SWAP DETECTION CHECKS”.

This is the sole purpose of the VALid-SSD<sup>®</sup> product.

The evaluation concluded that this is very clear and precisely-delineated purpose, and therefore rated the product “*excellent*” in terms of purpose-specification.

###### **The roles of the different entities** [Criteria Catalogue, section 1.1.3]

The evaluation concluded that the way in which the product is designed and will be used means that the customer using the product (ValidSoft’s client) is to be regarded as the “controller” of all the processing within the TOE: it is the user/client who decides to use this product for its own purpose (as described above); and it is the client who decides on the means to be used this end - which is the product.

This covers the internal disclosure of data by the user to the SSD “box”, the external disclosure of data to a third party, the partner-TSP; the obtaining of data from that third party (\* see Note, below); the internal processing within the SSD “box” (to generate a “Result”) (also when the “box” is hosted by the partner-TSP: \* see again the Note, below), and the final transfer of the data (mobile phone number and this “Result”) to the user’s own systems.

We should add that the user of the TOE is also undoubtedly the controller in respect of the original obtaining of the relevant personal data, including the mobile phone numbers, from the data subjects. That process is as such outside of the TOE, except insofar as the Conditions of Use for the TOE specify that the mobile phone numbers must have been

obtained fairly and lawfully, and that the making of the call or the sending of the SMS message to the relevant mobile phone must be lawful.

\* Note: The above does not cover the disclosure of the data sent by the partner-TSP to the “box” (which is the mirror of the obtaining of those data by the client in the same data flow), because the processing by the partner-TSP - i.e. the routing of the signal to the global MNO systems (in particular, to the MNOs’ “Home Location Registers” or HLRs) - is outside the TOE: see section 7.3, above. However, the evaluation nevertheless noted that it is the partner-TSP (i.e., ET) that must be regarded as the controller of the collecting of the data sent to the “box” from the global system, and of the disclosure of these data to the SSD “box”. At the same time, when the “box” is installed with the partner-TSP, that partner-TSP acts as a processor for the controller/user of the TOE with regard to the processing taking place within the “box”. This has implications in various contexts, including the questions of “applicable law” and of the legal basis and legality of this processing, as discussed in the relevant sub-sections, below.

### **Processed personal data** [\[Criteria Catalogue, section 1.1.2\]](#)

#### *Personal data:*

The evaluation treated basically all the data processed within the TOE as “personal data”.

#### *Sensitive data:*

No “special categories of data” (“sensitive data”), as defined in Article 8 of Directive 95/46/EC, are processed in the context of the use of the VALid-SSD<sup>®</sup> product.

#### *Traffic- and location data:*

No “location data”, as defined in Article 2(c) of Directive 2002/58/EC (the “e-Privacy Directive”), are processed in the context of the use of the TOE.

However, the SIM card number (IMSI number) associated with a particular mobile phone and a particular subscriber, does in our opinion fall within the definition of “traffic data” as defined in Article 2(b) of that directive, which reads as follows:

‘traffic data’ means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

In fact, as explained above, the whole purpose of checking whether a SIM card has been swapped is to enhance the integrity of the process: of the “conveyance of a communication on an electronic communications network”.

The processing of the SIM card data must therefore be assessed under Article 6 of the e-Privacy Directive. This is done in section A.2, below.

### **Data Avoidance and Minimisation** [\[Criteria Catalogue, sections 1.2.1, 2.2.2, and 2.2.3\]](#)

The evaluation found that all personal data, and in particular all internal and external data disclosures of personal data within the TOE, are kept to the absolute minimum. The use of the VALid-SSD<sup>®</sup> product involves only the absolute minimum amount of data required in this dataflow for the effective, reliable and verifiable carrying out of the SIM Swap Detection checks involved in the use of the TOE. Although strictly speaking outside the TOE, the evaluation found that this was also true of the processing by the partner-TSP in

the course of performing the actual “look-ups”. Moreover, in the passing on to the user of the VALid-SSD® product of the “results” of the “look-ups”, through the VALid-SSD “box”, **no** data are provided to the user other than this “result”, in “yes” / “no” / “fail” format and a lookup reference number, in relation to the mobile phone number provided by the user.

Note: The partner-TSP passes on the SIM card numbers of the “looked-up” mobile phones to the “box”, but those numbers are then held in the “box” in a fully-encrypted format, and cannot be decrypted by the client/user of the “box”, even though formally that client/user is the controller of the data.

Because of this maximum possible data avoidance and minimisation, the evaluation rated the product “excellent” on this issue.

## A.2 Legal Basis for the Processing [Criteria Catalogue, Part 2 – Set 2]

### **Legal basis for the processing generally**

There are basically three scenarios to be considered in terms of legal bases:<sup>2</sup>

- A. The use of the TOE by private-sector Clients, in relation to data subjects who signed up to the relevant service or product since the Client started using the Software (“new [private sector] customers”);
- B. The use of the TOE by public-sector Clients, in relation to data subjects who signed up to the relevant service or product after the Client started using the Software (“new [public sector] customers”); and
- C. The use of the TOE by either private- or public-sector Clients, in relation to data subjects who signed up to the relevant service or product before the Client started using the Software (“existing customers”).

The legal bases for the use of the TOE were evaluated separately for these three scenarios, as summarised below. At the end, we provide a simple Chart summarising the evaluation’s conclusions in this respect.

#### Scenario A: (private sector, new customers)

For private-sector users of the TOE, the use of the TOE in relation to new customers will - and must - be related to a lawful and valid contract between that user of the TOE and the data subjects. A typical example would be a contract between a bank and a bank customer (the data subject) about the use of Internet banking. Specifically, the bank may offer a system under which an individual trying to make an online Internet payment from his account to someone else’s account, will be sent an Out-of-Band (OOB) SMS message with a validation code, which the customer has to type into the PC s/he is using to make

---

<sup>2</sup> There is a fourth possible future scenario, in which the use of the Software would be made compulsory in a country, even without the data subjects’ consent. However, this is not contemplated anywhere at the moment, and this fourth scenario was therefore essentially left out of the evaluation for the time being. If this scenario were to arise, the developer will report this to the Certification Body and the matter will then be evaluated separately.

the online payment. In such a case, it is of course crucial that the bank can be sure that the message will reach the actual customer, and the actual mobile phone as registered with the bank. The contract allowing the customer/data subject to use Internet banking with this validation SMS security feature will therefore specify that the customer must provide a mobile telephone number to which the code is to be sent.

(The bank may offer other means of making an online Internet payment, e.g., by using a “PINs-entry” machine, without using the TOE, but that is of course a separate matter: if the bank uses the OOB validation code SMS system, just mentioned, and if the customer chooses that system, then there is an obvious need to ensure the integrity of the SMS communication.)

The evaluation noted that it is a fundamental Condition of Use for the TOE that in this scenario the user of the TOE fully informs the data subject of his (the user’s) intention to carry out Out-of-Band (OOB) integrity checks (without of course using technical language that would be meaningless to ordinary customers), before the data subject signs up to the service or product (and thus to the OOB/SSD checks). That information must furthermore be provided in a way that clearly distinguishes it from the general “small print” terms and conditions of the contract between the user of the TOE and the data subject. The vendor of the TOE, ValidSoft, recommends that users provide this information in the form of a simple leaflet. In other words, any private-sector user of the TOE may only use the TOE in relation to new customers who have freely signed up to the product or service in question (typically, to online Internet banking with SMS-sent code), and who freely provided their mobile phone numbers to the controller for the reception of the code, in full knowledge that such checks could and would be carried out.

The evaluation concluded that in this scenario all processing by the user of the TOE in relation to the use of the TOE by private-sector entities can in principle be said to be based on the free, informed and valid consent of the data subject.

The evaluation found that the voluntariness of this consent is not affected by the fact that the consent of the data subject to such checks is made a condition for the entering into the contract for such an SMS-code-based system: for such a system, a check of the integrity of the OOB channel (the SMS communication) is crucial.

**The evaluation therefore concluded that in this scenario all processing by the user of the TOE in relation to the use of the TOE by private-sector entities can in principle be said to be based on the free, informed and valid consent of the data subject, obtained under a contract.**

Note: The evaluation also concluded that in principle the processing associated with the use of the TOE could also be justified on the basis of two further criteria: processing on the basis of the “balance” provision (Article 7(f) of the Directive 95/46/EC), and processing in relation to the carrying out of a “task in the public interest”, i.e. fraud detection and –prevention (Article 7(e)), but that the vendor of the TOE does not rely (and does not need to rely) on those criteria. Rather, for scenario A, consent obtained in a contractual context should be seen as the main criterion.)

Scenario B: (public sector, new customers)

In the public sector, OOB authentication systems can also be used, e.g., to allow a person who obtains welfare benefits from the State access to such benefits, or to relevant information or websites. Since such methods are still relatively new to the public sector, they are so far (to the evaluators' best knowledge) nowhere made compulsory: if anything, the data subjects (welfare beneficiaries) are offered the opportunity to use such new systems instead of face-to-face meetings and attendances at welfare offices, which are costly and burdensome to all concerned. They can avail themselves of this offer, or not, as they like.

In this case, the Conditions of Use for the product stipulate the same as for the above-mentioned private-sector users, i.e.: that the user of the TOE must fully inform the data subject, in non-technical language, of his (the user's) intention to carry out such OOB integrity checks, before actually carrying out any such checks; and that that information must be provided in distinct, clear terms (preferably in the form of a booklet). In addition, the public-sector user of the TOE may only use the TOE in relation to individuals who have freely signed up to the product or service in question (in the above example: to the obtaining of welfare benefits or information on such benefits), and who have freely provided their mobile phone numbers to the controller, in full knowledge that OOB integrity/SIM Swap Detection checks could and would be carried out.

The evaluation concluded that in such cases, as in the above private-sector contexts, the processing related to the use of the TOE is again all based on the free and informed consent of the data subjects. However, in this case there is an additional Condition of Use for the TOE, which is that the user of the TOE may only use the TOE, even with the consent of the data subjects, if the relevant national law allows, but does not require this. Moreover, in any case, such users must of course also always fully comply with any further conditions or formalities for the use of the TOE, e.g., that a "prior check" be carried out or requested before the TOE is used.

The evaluators felt that for this (public-sector) scenario, it was best not to look at this from the perspective of a contract, because the use of contracts in the public sector can be problematic. Rather, they saw the context as a typical public-sector state body-citizen agreement that must be linked to the statutory basis for the activities of the state body in question (and which, as just noted, should clearly allow for the use of such a product and such agreements).

**The evaluation concluded that the strict legal arrangements concerning the use of the TOE by public-sector controllers in relation to new customers ensure that the processing of all the data processed within (and indeed otherwise related to) the TOE will always be on the basis of free, informed and valid consent, obtained under a voluntary arrangement with the user, and that these legal arrangements also ensure full compliance with any other still-applicable national-legal requirements, conditions and formalities.**

Scenario C: (private- or public sector, existing customers)

The evaluation found that it could be argued that the legal arrangements concerning the use of the TOE by private- or public-sector controllers ensure that the processing associated with the use of the TOE in relation to existing customers too is based on free,



informed and valid consent (for private-sector controllers, obtained under a contract, and public-sector controllers under comparable agreements), and/or is legitimate on the basis of the “balance” criterion. However, the evaluation concluded that those arguable grounds were not solid enough for the European Privacy Seal.

Rather, the evaluation held that the most appropriate criterion under which to assess the use of the TOE in relation to existing customers is the criterion spelled out (among others) in Article 7(e) of Directive 95/46/EC:

processing [that] is necessary for the performance of a task carried out in the public interest...

This applies to both public- and private-sector bodies, but the evaluation discussed the issue separately for them.

#### PUBLIC-SECTOR USERS:

The evaluation found that it may be assumed that public-sector bodies perform tasks “in the public interest”, as defined in the legislation defining the tasks of the body in question. More specifically, when public-sector bodies try to detect, prevent, stop, or when not prevented or stopped, prosecute fraud perpetrated in relation to the activities of the bodies concerned - e.g., welfare payments fraud - they are of course also “carrying out a task in the public interest”. Public-sector bodies could therefore, in the opinion of the evaluators, generally base the use of the TOE on this criterion for lawful processing - although they also stressed again that that specific use of the specific product to those ends would still have to be clearly covered by, and allowed under, relevant national law.

#### PRIVATE-SECTOR USERS:

The evaluation emphasised that it is not only public-sector bodies that “carry out tasks in the public interest”, especially not when it comes to fraud: in practice, most detection and prevention of fraud is carried out by private-sector entities, especially financial institutions. Our earlier evaluations found that this was expressly recognised in Article 79 of the Payments Directive (Directive 2007/64/EC), with specific reference to data protection:

##### *Article 79*

##### **Data protection**

Member States shall permit the processing of personal data by payment systems and payment service providers when this is necessary to safeguard the prevention, investigation and detection of payment fraud. The processing of such personal data shall be carried out in accordance with Directive 95/46/EC.

For the present re-evaluation, we note that this expressly re-affirmed in Article 94(1) of the Payments Directive’s successor, the Payments Services Directive (Directive (EU) 2015/2366, commonly referred to as PSD2), which came into force in January 2018:

##### *Article 94*

##### **Data protection**

1. Member States shall permit processing of personal data by payment systems and payment service providers when necessary to safeguard the prevention, investigation and detection of payment fraud. The provision of information

to individuals about the processing of personal data and the processing of such personal data and any other processing of personal data for the purposes of this Directive shall be carried out in accordance with Directive 95/46/EC, the national rules which transpose Directive 95/46/EC and with Regulation (EC) No 45/2001.

This provision is not affected by the second paragraph of Article 94, which reads:

2. Payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user.

Rather, the two provisions, read together, in our view should be read as saying that, once a payment service provider is given consent by a user of that provider's services to process personal data for the provision of those services, that provider may (and should, under relevant Member States' laws, be allowed to) also process the relevant personal data for fraud prevention (etc.) purposes. In other words, processing of a payment service user's personal data for the purposes of prevention, investigation and detection of payment fraud is a "compatible" use of those data.

NB: In the UK, PSD2 has been implemented by the Payment Services Regulations 2017, which came into force in steps, and fully in force since 13 January 2018. The Regulations effectively repeat the second paragraph of Article 94 PSD2 in Regulation 97. It does not contain a provision on the lines of Article 94(1) PSD2 – but this is presumably because the UK Data Protection Act, as interpreted by the UK's courts, already allows private entities to process personal data also for fraud prevention purposes, without the consent of the data subjects. In combination, the UK DPA and the UK Payment Services Regulations 2017 therefore provide for the same regime as does the PSD2.

Our re-evaluation therefore again concluded, with reference to these new provisions, that payment fraud prevention - which is the only purpose served by the TOE, in either public- or private-sector contexts - is undoubtedly a "task carried out in the public interest" in the sense of Article 7(e) of the main Data Protection Directive; and that that task can be carried out by both public- and private-sector controllers. The evaluation thus found that the "public task" criterion can be relied on by both public- and private-sector bodies, especially in relation to fraud detection and –prevention.

The only remaining question to be answered in respect of that criterion was therefore whether the processing of personal data involved in the use of the TOE is "necessary" for that task. In that respect, the evaluation repeated (*mutatis mutandis*) the finding in relation to the other ValidSoft products that have been awarded the European Privacy Seal:

Of course, it is not necessary for every bank or Payment Processor or welfare office to use the specific product, VALid-SSD<sup>®</sup>. But that is not how this article should be read. Rather, Article 7(e) relates to processing that is necessary (*inter alia*) to carry out any appropriate measures that may be taken by controllers to prevent and stop fraud. The evaluation found that there was no doubt that the TOE is a highly appropriate means to that end. Moreover, as noted elsewhere in this report, the arrangements for the use of the product ensure that only the absolutely necessary minima of personal data are used, that there is complete transparency, and that in all other respects, too, the product is fully compliant with European data protection law.

**The evaluation therefore concluded that for this scenario the use of the VALid-SSD product is “necessary ... for the performance of a task carried out in the public interest”.**

The above conclusions with regard to the three scenarios are summarised in the Chart, below:

<u>Type of controller:</u>	<u>Type of data subject:</u>	<u>Legal basis for processing:</u>
Private sector user	New customer (typically, of a bank) <b>[Scenario A]</b>	Consent obtained under a contract
	Existing customer (typically, of a bank) <b>[Scenario C]</b>	- Public task (Art 79 Payments Directive)  <i>(Also arguably, but not relied on:</i> - <i>Consent obtained under a contract, and</i> - <i>Balance of interests)</i>
Public sector user	New customer (e.g., welfare claimant) <b>[Scenario B]</b>	Consent
	Existing customer (e.g., welfare claimant) <b>[Scenario C]</b>	- Public task  <i>Also arguably, but not relied on:</i> - <i>Consent, and</i> - <i>Balance of interests)</i>

### **Processing of traffic- and location data by the partner-TSP**

[\[Criteria Catalogue, sections 2.1.4.2 and 2.1.4.3\]](#)

As already noted, the evaluation concluded that no “location data”, as defined in Article 2(c) of Directive 2002/58/EC (the “e-Privacy Directive”), are processed in the context of the use of the TOE, but that the SIM card number (IMSI number) associated with a particular mobile phone and a particular subscriber, does fall within the definition of “traffic data” as defined in Article 2(b) of that directive.

In 2011, the Article 29 Working Party issued an opinion on geolocation services on smart mobile devices.<sup>3</sup> Although (as the title of the Opinion indicates), the Opinion was focussed on the processing of geolocation data, and “location data” as defined in Directive 2002/58/EC (the “e-Privacy Directive”), the Opinion also makes clear more generally that, according to the WP29, the e-Privacy Directive (Directive 2002/58/EC, as amended) only applies to electronic communication service providers, including the TSPs and MNOs referred to in this report, i.e., it does not apply to any other entities that may be processing the categories of data specifically regulated by the e-Privacy Directive, “traffic- and location data”.

<sup>3</sup> [Opinion 13/2011 on Geolocation services on smart mobile devices](#), 16 May 2011, WP185

In other words, we concluded in 2012, and re-affirmed in 2015, that the processing of the SIM card numbers by the users of the TOE is not subject to the e-Privacy Directive, but only to the more general rules in the main data protection directive, Directive 95/46/EC. Indeed, since traffic- and location data are not “sensitive data” in the sense of that general directive, the processing of the SIM card data by the users of the TOE must be assessed under the general rules in that directive, and need not comply with the stricter rules on the processing of sensitive data in that directive. This conclusion still stands at present, in January 2018.

However, it was felt by the EuroPriSe experts and the Certification Body already in 2012, but also in 2015 and now, in January 2018, that the legal basis for the processing of the traffic data in question (i.e., the SIM card data and related secondary data), by the partner-TSP, should still be examined. In that respect, they referred in the original 2012 evaluation report and in the 2015 first re-evaluation report to the detailed analysis in the Evaluation Reports on ValidSoft’s VALid-POS<sup>®</sup> product. These evaluations concluded that the same applies to the SSD product as applied to that product: the e-Privacy Directive (Directive 2002/58/EC), in Article 15, allows Member states to allow the processing of traffic- (and for that matter, location-) data for crime detection, -prevention and –prosecution purposes, also on behalf of anti-fraud measures taken by private entities; and the Dutch general data protection law and its Telecommunications Law – which was the law applicable to the Dutch partner-TSP involved – do indeed make use of this, and allow TSPs to disclose traffic- (and location-) data to private entities for these purposes. (We also noted in that report, in parentheses, in relation to the probable use of a UK-based partner-TSP in future actual deployments, that UK data protection law also allows this.)

**The evaluation confirmed that this same legal reasoning could and should also be applied to the SSD product, and that the processing of the SIM card and associated data by any Netherlands- (or UK-) based partner-TSP in support of the users of the TOE was therefore lawful, also in relation to VALid-SSD<sup>®</sup>, under the EU directives and the Dutch (and UK) data protection- and telecommunication laws.**

(The evaluators felt that the processing of the SIM card data by the partner-TSP supporting the use of the TOE, and by any other MNOs involved, arguably also met the requirement in Article 6(1) of the e-Privacy Directive that that processing must be “needed for the purpose of the transmission of a communication”, in that it is needed to ensure the integrity of a communication for which such integrity is essential.<sup>4</sup> However, given that the processing was in any case lawful under the above-mentioned EU and Dutch [and UK] legal rules, they felt that this needed not be examined further.)

---

<sup>4</sup> Article 6(1) of the e-Privacy Directive stipulates the following:  
“Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).”

### A.3 Selected other topics

#### **Data Collection (Information Duties)**      [[Criteria Catalogue, section 2.2.1](#)]

As already noted, the Conditions of Use for the use of the TOE stipulate that the user of the TOE must fully and clearly inform the data subjects, in easily-understandable language, how and when the TOE will be used in relation to them, if they agree to it; and that this information (which the vendor of the TOE, ValidSoft, recommends that users provide in the form of a simple leaflet) must stress that authorising the use of the TOE is entirely voluntary.

More specifically, it is a Condition of Use for the use of the TOE that the user of the TOE provide to the data subjects at least the information required by Articles 10 and 11 of the main Data Protection Directive, and by Articles 6 and 9 of the e-Privacy Directive. Of this mandatory information, the Conditions of Use mention the following expressly:

- the identity of the Client/user of the TOE, and that this Client/user is and will remain the controller of all processing involved in the use of the TOE;
- that the purpose of the processing is only the detecting of fraudulent use of the data subject's mobile phone, and that the data used for this purpose will only be used for this purpose and for no other purpose (except that, of course, the mobile phone number of the data subject is also used to make the call, or send the SMS message, in relation to which the check is carried out);
- that the use of the TOE is necessary for the provision of the optional service to which it is related, such as typically an online banking system, and that the free choice of the data subject to sign up to this service therefore also entails the giving of the latter's consent to the use of the TOE;
- that the Client/user of the TOE sends the data subjects' mobile phone numbers to a partner-TSP in the Netherlands\* in order to carry out this check, but that this partner-TSP cannot and does not discern the identity of the data subjects from this; and
  - \* NB: As noted above, in due course this may change to "in the UK".
- that they may withdraw their consent for the use of the TOE in relation to their phone at any time, but that that would entail loss of the service.

In relation to the third point (that the free choice of the data subject to sign up to the relevant service also entails the giving of the latter's consent to the use of the TOE), the developer/vendor of the product, ValidSoft UK Ltd, recommends in its "Client Recommendations" in the Core Model Product Guide that the data subjects should be asked to indicate their understanding of this point specifically in the agreement relating to the relevant service, e.g., by ticking a box to that effect, separately from the agreement relating to the service as such.

**The evaluation concluded that the above clearly meets all the requirements of Articles 10 and 11 of the main data protection directive (Directive 95/46/EC).**

As far as the information duties under the e-Privacy Directive (Directive 2002/58/EC) are concerned, the evaluation noted that Article 9 is not relevant, as it relates to location data, and no such data are processed in relation to the use of the TOE.

Although arguably the processing within the TOE is “for the purpose of the transmission of a communication” (Art. 6(1) of the e-Privacy Directive), and the information duties under Article 6(4) therefore arguably do not apply, the evaluation welcomed the fact that the Conditions of Use for the TOE still require the users of the TOE to inform their customers (who are also the subscribers to the mobile phones) of all the details of the SIM Swap Detection checks (in non-technical language), including:

- clarification that the processing involves the disclosure of the data subject’s mobile phone number and some administrative data (but not their identity) to the varying communications service providers through the systems of which the calls/texts are routed, both to make the actual call or send the actual message relating to the service in question, and to carry out the SIM Swap Detection checks;
- clarification of the fact that the user will cease to use the TOE in relation to any data subject who makes clear that he or she no longer wants to obtain the product or service in support of which the SIM Swap Detection checks are carried out; and that all data pertaining to such a data subject and his or her phone, obtained through the TOE, will be completely erased as soon as practical when this happens; and
- affirmation that data subjects may opt out of the use of the TOE in relation to their phone at any time (although that that may entail loss of the service).

**The evaluation found that, to the extent that the article was applicable, this fulfilled the requirements of Article 6(4) of the e-Privacy Directive.**

#### **Processing of Data by a Processor** [\[Criteria Catalogue, section 2.4.1\]](#)

As noted earlier, the evaluation concluded that the client/user of the product is to be regarded as the controller of all the processing within the scope of the TOE; and that outside the scope of the TOE, the partner-TSP, is the controller of the collecting of the data sent to the “box” from the global system, and of the disclosure of these data to the SSD “box”, i.e. of the lookups.

If the SSD “box” is installed at the client/user’s premises, and essentially operated by the client/user (subject to certain embedded restrictions), the use of the TOE therefore does not involve any processing by a processor.

However, if the SSD “box” is installed at the premises of the partner-TSP (as is an option for EU/EEA-based client/users of the product, and compulsory for non-EU/EEA-based client/users), then the partner-TSP will act as a processor in respect of the processing taking place within the “box”.

Under Article 17(2) of Directive 95/46/EC, this may only happen provided that the processor - i.e., in casu the partner-TSP - “provid[es] sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to

be carried out”, and “ensure[s] compliance with those measures”. In the light of the warranties and guarantees provided by the partner-TSP to ValidSoft and its clients/the users of the TOE (noted next), the evaluation concluded that this is indeed ensured.

Under Article 17(3) of the Directive, the arrangements between the controller (i.e., the client/user of the TOE) and the processor (i.e., in this case and in this limited regard, the partner-TSP) must be covered by contracts or other legal arrangements that are binding upon both of them, and that stipulate in particular that:

1. the processor shall act only on instructions from the controller, [and]
2. that the security and confidentiality requirements set out in Article 17(1), as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

The original 2012 evaluation and the 2015 re-evaluation found that ValidSoft and its partner-TSP at the time of these evaluations had in fact entered into precisely such an agreement in respect of the SSD product; and this has not changed at the time of the current re-evaluation. <sup>[see note \*]</sup> This agreement, moreover, expressly grants third-party rights in the above-mentioned respects to the clients of ValidSoft/users of the SSD product.

**The evaluation concluded that the contractual stipulations in all the different contracts and clauses between the parties, taken together, provide extremely strong guarantees of compliance with the relevant European data protection standards, and that this also, specifically, applies to the ValidSoft – partner-TSP clauses covering the processing by the partner-TSP in the capacity of a processor for the client/user/controller.** <sup>[see note \*]</sup> **These clauses are also in writing, and thus also fulfil the requirement to that effect in Article 17(4) of the Directive.**

NOTE\* (Yet again, we should note that, as and when the TOE goes into actual deployment, in a form for which the developer of the product, ValidSoft, will want to obtain a *EuroPriSe* certification, ValidSoft will probably use a UK-based partner-TSP – but that is not yet the case. Suffice it to note, therefore, that ValidSoft has already made clear to us in the context of the present re-evaluation, that in that case it will make its cooperation with that new (UK-based) partner-TSP subject to equivalent, equally strict, agreements on data protection as were evaluated in the original evaluation and the first re-evaluation. Provisionally, we can therefore already conclude that, if that will be the case, the TOE will again fulfil the requirements in that respect in relation to the new arrangements too. However, again, this will need to be further addressed, and will be further addressed, in any future re-evaluation or change report, in particular in any change report that would report on actual deployment of the TOE for which a seal is sought. But again, this will probably be done under the by then fully in force GDPR and probably an EU e-Privacy Regulation and relevant new UK law.)

### Transfers to Third Countries

[\[Criteria Catalogue, section 2.4.2\]](#)

When the TOE is used by an EU/EEA-based client, there are no transborder data flows within the TOE that are subject to the restrictions in Article 25 and 26 of the Directive; and when the TOE is used by a client based outside the EU/EEA, the only data flow that is subject to these restrictions is the data flow in which data are sent from the SSD “box” hosted at the systems of the partner-TSP in the EU. <sup>[see note \*]</sup> to the user/client’s systems

outside the EU/EEA. As already noted, this involves only the sending to the client, from the “box”, of a “YES/NO/FAIL” “Result”.

\* Note that the partner-TSP will always be based in the EU.

As noted earlier, the evaluation distinguished between different legal bases for the processing within the TOE, depending on whether the use of the TOE related to new or existing customers of the Client/User of the TOE, and on whether the user was a private- or a public-sector entity (see “Scenarios A, B & C”, above).

With regard to new customers (of either private- or public-sector users) (Scenarios A and B), the evaluation concluded that for private sector users of the TOE, all the processing within the TOE - including all the transborder data transfers that may occur within the TOE, both within the EU/EEA and to third countries (in the case of non-EU/EEA-based users of the product) - is based on the (free, informed, express) consent of the data subjects, obtained in a contractual context; and that all processing within the TOE in all current scenarios for the use of the product by public sector users, will also be on the basis of valid consent (but added that it should also be allowed by the relevant national law).

**For Scenarios A and B, the very limited possible transfers of data to third countries within the TOE (i.e., the transfer of no more than the “results” to the user of the product, in cases in which that user is non-EU/EEA-based) are also covered by these consents. They are therefore all permitted under Article 26(1)(a) of Directive 95/46/EC (transfers on the basis of “unambiguous consent”) and, at least for private-sector users, also under Article 26(1)(b) (transfers that are “necessary for the performance of a contract between the data subject and the controller”).**

**With regard to existing customers (again, of either private- or public-sector users) (Scenario C), the evaluation found that the (minimal) transfers of personal data to third countries in relation to the use of the TOE were necessary (also) “for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party”, and thus lawful under Article 26(1)(c) of the main Data Protection Directive.**

**Moreover, the evaluation found that the transfers of the limited data, in the above-mentioned limited circumstances, with regard to both new and existing customers, can also be said to be covered by Article 26(1)(d): transfers that are “necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims.”** The “important public interest” in question is, of course, the detection and prevention of fraud; and the SIM Swap Detection measures carried out by the TOE are of course also important in relation to possible legal claims, if a data subject, or the user of the product, loses money as a result of fraud. The evaluation found that the use of the product is also “necessary” in relation to these matters, not in the sense that all companies or bodies involved in financial or state benefit transactions need to use this particular product, but in the sense that all such companies or bodies do need to take measures to detect and prevent fraud, and that this product does so in an excellent, privacy-respecting way.



## Formalities

[Criteria Catalogue, section 2.5]

It is made clear in the Conditions of Use that the client is required to comply with all relevant substantive and formal requirements of the applicable law; and this stipulation also explicitly draws the attention of the user (client) to the possible duty of that user/client/controller to notify the processing operations to the relevant national Data Protection Authorities, or where this is required by that national law, to ask the authorities to carry out a “prior check” as envisaged in Article 20 of the Directive.

The Conditions of Use also require the client to comply with any legal requirement of the relevant applicable law to carry out a Data Protection and Security Audit.

**The evaluation found that this was sufficient in the context of this TOE.**

### A.4 Data subjects’ rights

[Criteria Catalogue, Set 4]

As noted earlier, the evaluation determined that the client (the user of the TOE) is the controller of all the processing operations within the TOE.

This means that, quite generally, the question of the scope and effective exercise of data subject rights (like the question of formal duties, such as the need for notification, prior checking, etc.) will be determined by the national law applicable to the client in this capacity as controller, and is not a matter that can be dealt with in day-to-day practice by the developer and vendor of the TOE, ValidSoft UK Ltd.

It follows from this that generally the most that that developer and vendor can do, is alert the clients to their duties in this respect, and make it conditions of use of the product that the clients fulfil their obligations under their applicable law; and this is exactly what is being done: the Conditions of Use for the TOE require the users of the TOE to inform data subjects of their own motion of various matters when they (the users) obtain the relevant data from the data subjects or (in respect of existing customers) when they start using the product; and they require them to grant the data subjects the right to be informed of details of the processing on request; the right of access to their data; the rights of correction, erasure or blocking, and to object to processing.

**Given that this is all that the developer of the TOE can do in these respects, the evaluation concluded that this suffices for the purpose of compliance with European data protection rules on these matters.**

Note: The evaluation concluded with regard to the e-Privacy Directive, that it was sufficient: that the evaluation found that that directive did not apply to the users of the product, but did apply to the processing in support of the product by the partner-TSP; that as noted earlier, the partner-TSP had a proper legal basis for the processing in support of the product, i.e. for the carrying out of the look-ups; and that beyond this specific issue - which in fact already was a matter outside of the TOE - the question of compliance, by the partner-TSP, with its obligations under the e-Privacy Directive was clearly outside the scope of the TOE, and thus did not need to be assessed in the evaluation.

## A.5 Documentation of the product: the legal arrangements<sup>5</sup>

The product is covered by certain clauses in or annexes to three main documents:

- ✓ The (binding) Conditions of Use of the VALid-SSD<sup>®</sup> SIM-Swap Detection Product, set out in an Annex to the Standard Agreement on the use of the TOE, concluded between the developer and vendor of the product, ValidSoft, and the User of the product (and which forms an integral part of the Agreement). The evaluation was based on the revised version of 28 September 2012, as added to and amended in February 2015 [which has not been further changed since then].
- ✓ The latest (January 2018) version of the “Core Model Product Guide”, v.1.12 (which replaces v.1.11 of September 2012), which is the main guide for Client/Users, v.1.11, of 11 October 2012, which incorporates the Client Recommendations referred to in this Evaluation Report from time to time and updates some security requirements (see section 5.1 of the CMPG);
- ✓ The binding Legal Clauses between the developer and vendor of the product, ValidSoft, and the partner-TSP,<sup>[see note \*]</sup> including two Annexes to these clauses (which form an integral part of the clauses), which provide certain important binding legal guarantees and warranties, including clauses with third-party effect to the benefit of the data subjects, also amended to meet the EuroPriSe requirements. The evaluation was based on the revised version dated 12 October 2012 [which has not been changed].

\* (Note that, as already clarified in the comments in parentheses in sub-section A.3, under the heading “*Processing of Data by a Processor*”, in any future arrangements with any future new (UK-based) partner-TSP in relation to any actual deployment of the TOE for which a seal will be sought, the same or equivalent guarantees and warranties will required of the partner-TSP.)

As noted in the various sections this report, these documents ensure, *inter alia*, that the client/user of the TOE, and the partner-TSP, will only use the product to ensure the integrity of a communication with a mobile phone when the communication (the making of a call or the sending of a text message) is lawful; that all the processing by means of the TOE (and indeed all the processing by the partner-TSP in support of the TOE) has a proper legal basis; that the data subjects are fully and fairly informed of the relevant details of the product (in non-technical language, and in a form that distinguishes this information from the other contractual matters), and granted all of their rights; etc., etc..

**The evaluation found that the contractual, binding stipulations in these different contracts, taken together, provide extremely strong guarantees of compliance with the relevant European data protection standards, and consequently rated the TOE “excellent” in this respect.**

---

<sup>5</sup> In the Criteria Catalogue, these matters are addressed in the part dealing with the technical evaluation, but for the Short Public Report on the present TOE, they are more closely linked to the legal evaluation, and are therefore dealt with here. The issues covered by the technical evaluation proper are dealt with below, at B.

**B. TECHNICAL EVALUATION** [Criteria Catalogue, Part 2 – Set 3]

**B.1 General Duties**

The evaluation assessed in detail the following technical aspects of the TOE:

- ✓ physical access control;
- ✓ access to media and mobile devices;
- ✓ access to data, programs and devices;
- ✓ identification and authentication;
- ✓ use of passwords;
- ✓ organisation and documentation of access control;
- ✓ logging and logging mechanisms;
- ✓ network and transport security;
- ✓ back-up- and recovery mechanisms;
- ✓ data protection and security management (including requirements concerning the client's security policy and risk assessment);
- ✓ documentation and inventories;
- ✓ media management;
- ✓ the appointment and duties of a security officer;
- ✓ instruction of personnel, and the imposition of a formal duty of confidentiality on them;
- ✓ the carrying out of a data protection and security audit;
- ✓ incident management;
- ✓ test and release;
- ✓ disposal and erasure of data; and
- ✓ temporary files.

Overall in these respects, the evaluation concluded, first of all: that the default settings for the TOE met the European requirements, and that the legal clauses and recommendations, if followed, would ensure compliance with those requirements in all relevant respects. Specifically, as far as communication security and encryption are concerned, the “Core Model Product Guide” and the legal arrangements discussed at 11.A.5, above, stress (and require) that the client use “state of the art” technology in these respects, and updates this as technology develops.

However, in many respects, actual compliance again ultimately rests with the user of the product; and therefore, in these respects, the most that the developer and vendor can do, is alert the clients to their duties in this respect, and make it conditions of use of the product that the clients fulfil their obligations under their applicable law; and this is exactly what has been done in the legal clauses etc., discussed above, at A.5

**Given that this is all that the developer of the TOE can do in these respects, the evaluation concluded that this suffices for the purpose of compliance with European data protection rules on these matters.**

However, one matter that is (largely) in the hands of the developer, ValidSoft, has been further assessed:<sup>6</sup> the question of pseudonymisation and anonymisation. In that respect, the evaluation found that the product receives a mobile phone number and a reference number from the User or Client. The phone number is then queried to the partner-TSP. After that, the partner-TSP returns the IMSI number to perform the baseline, if it's the first time, or checks the IMSI, to see whether it has been modified or not. No other data from the customer is passed to the partner-TSP. Moreover, the legal clauses between VS and the partner-TSP stipulate clearly that the partner-TSP may only use the data to perform the relevant SIM-swap checks, to assist the anti-fraud measures of the users of the TOE, i.e. to check IMSI numbers (see in particular clause 2.3). Thus, even if it were to be technically possible for the partner-TSP to link some of the data to some identifiable persons by means of some further processing of the data, that would therefore still be prohibited under the clauses; and these clauses have third-party effect for the benefit of the data subjects.

In our opinion, the fact that the developer of the TOE has ensured that even the partner-TSP cannot identify the data subjects is an important contribution to the product in terms of data avoidance and minimisation. Perhaps the best way to put this is to say that the partner-TSP is put in a position similar to a processor or controller who receives only pseudonymised data from an original controller, for the purpose of performing an agreed (legitimate) task, for which identifiable data/links to the identity of the data subjects are not needed. To put this within the framework developed by the Article 29 Working Party in its opinion on anonymisation technologies,<sup>7</sup> the context and objectives of the data minimisation measures applied to the TOE (including both the minimisation of what is sent to the partner-TSP, which is the absolute minimum possible, and the strict contractual clauses on what the partner-TSP must, may, and may not do with the data) ensure optimal non-linkability in this context.

However, because the user of the TOE remains the controller of the processing; and because that user can of course identify the data subjects (who are its own customers/cardholders), we have based our second re-evaluation (like the original evaluation and the first re-evaluation) on the assumption that the data remain identifiable personal data at all times, in all the processing covered by the evaluation.

In addition, the IMSI number of the customer is not passed to the User or Client, but instead, only a “positive”, “negative” or “fail” message. (See the Note on p. 12)

**As already noted in the earlier section on “data avoidance and minimisation”, the evaluation concluded in relation to this, and the first and this second re-evaluations also confirmed, that the data processed within the TOE have been anonymised, and**

---

<sup>6</sup> Another aspect of the TOE that is covered in the Criteria Catalogue in the part dealing with the technical evaluation, and that has been addressed in substance detail in the evaluation, is the question of documentation. However, as noted in the text and in the previous footnote, in this Short Public Report, the relevant comments have been moved to the part dealing with the legal evaluation, because for the TOE they focussed on the legal arrangements: see section 11.A.5, above.

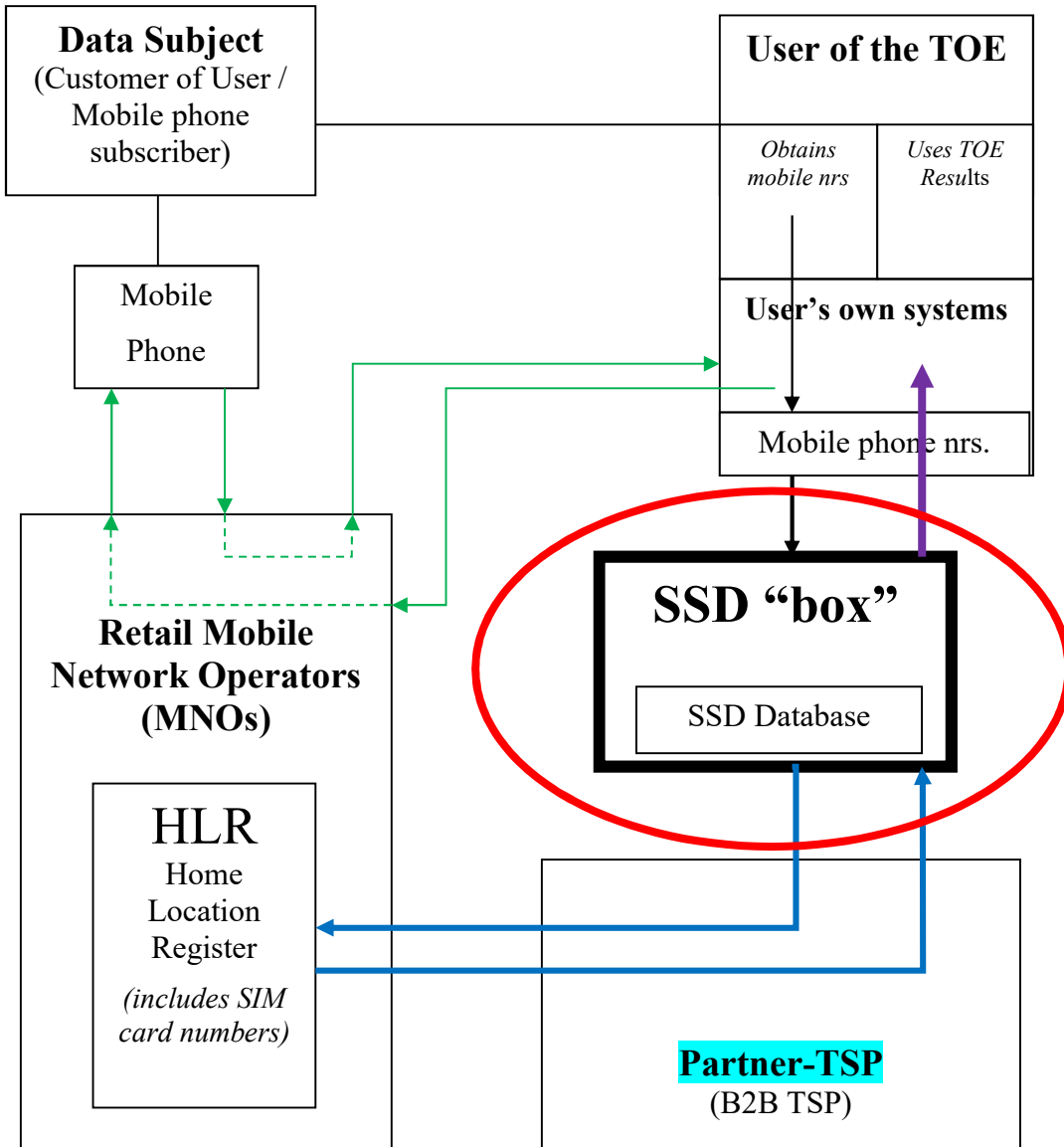
<sup>7</sup> Opinion 05/2014 on Anonymisation Techniques (WP216), adopted on 10 April 2014.

generally been kept in identifiable form to the minimum needed for the TOE’s purpose, and are thus in accordance with the European requirements. Indeed, all the evaluations found that the great lengths to which the developed has gone in this respect is one of the most positive features of the product, and therefore rated the product “excellent” in this respect.

**14. Data flows:**

The Charts below and overleaf outline the data flows associated with the SSD product:

**CHART 1: The TOE in context**

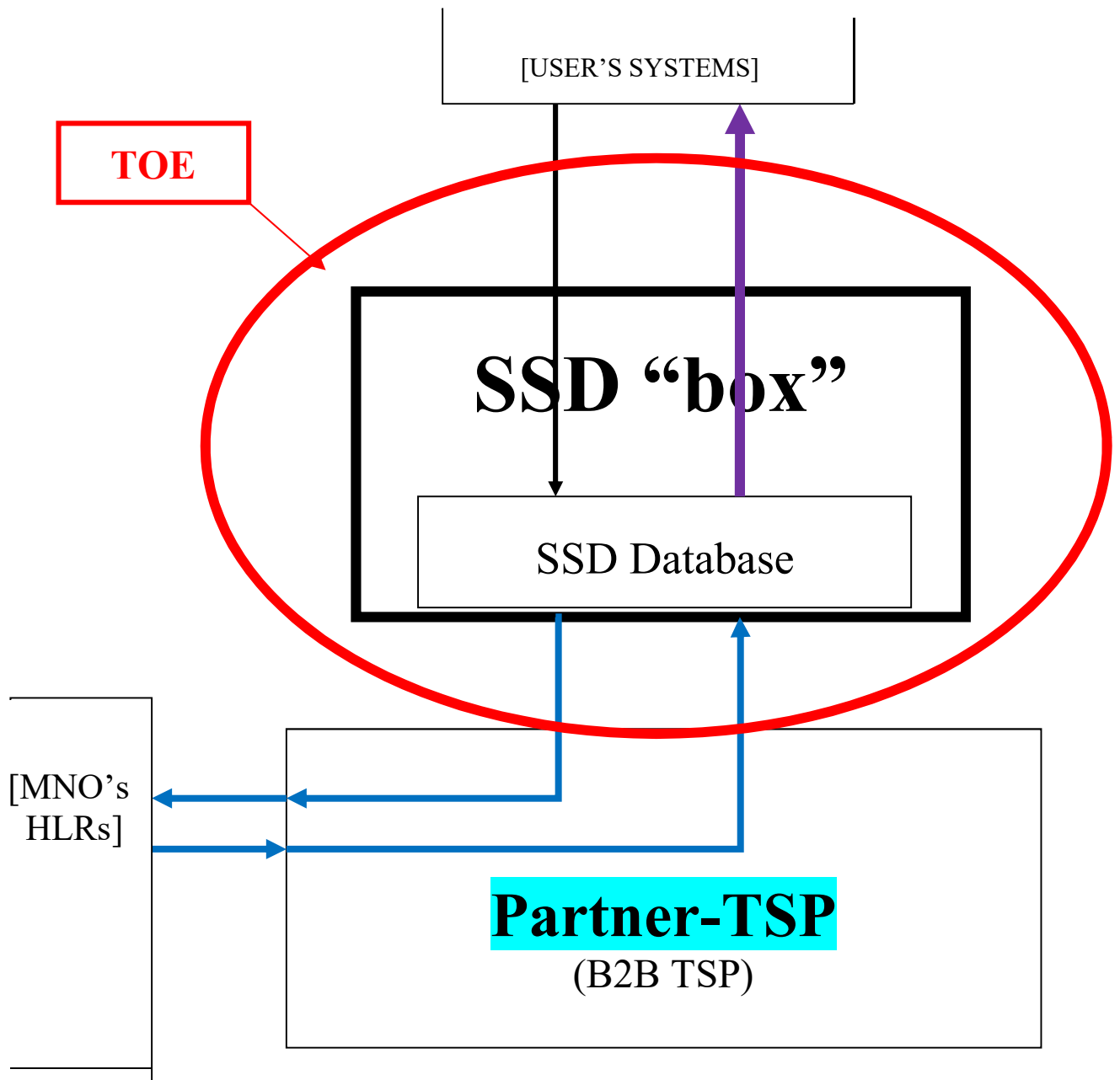


**LEGENDA:**

- The **RED OVAL** indicates the TOE, including in particular the VALid-SSD® product, consisting of a (virtual) “box” and database, and the associated dataflows. See *Chart 2 overleaf for an enlargement.*
- The **BLUE LINES** indicate the “lookups” carried out by the TOE.
- The **GREEN LINES** indicate the making of a call or the sending of an SMS message by the user of the TOE to the data subjects (outside of the TOE).
- The **PURPLE ARROW** indicates the passing on of the “Results” of the lookups to the user of the TOE.

**CHART 2: The TOE in detail**

[Cf. the Legenda on the previous page, under Chart 1]



Note: As can be seen from the above chart in particular, the TOE is essentially quite simple: it consists of a carrier with software (the VALid-SSD® “box”), which has a database at its heart, with two data flows to and from the user’s own systems, and two to and from the databases accessible to all Mobile Network Operators (which are accessed through the systems of the partner-TSP that supports the TOE).

## 15. Privacy-enhancing functionalities:

The product deals with an issue that is of increasing concern to financial institutions: fraudulent SIM swaps. These undermine the integrity of increasingly-important “Out-Of-Band” (OOB) authentication systems, such as the sending of a PIN number by a bank to a customer, by means of an SMS (“text”) message, for use in an online banking session by the customer. If criminals re-direct the message to themselves, they can often fraudulently access the customer’s bank account.

The TOE is very simple yet very effective in preventing such fraud, without impinging on the customers privacy or data protection rights and interests.

The following were specific matters that were rated “excellent” in data protection terms in the European Privacy Seal evaluation:

- ✓ clear and precise purpose-specification (SIM Swap Fraud Detection) and – limitation;
- ✓ maximum data avoidance and –minimisation, both generally and in relation to the absolutely minimal disclosures of data to even the users of the product (in that they only obtain a “Yes” [No SIM Swap] / “No” [SIM Swap] / “Fail” “Result” from the VALid-SSD® “box”; in relation to disclosures of data to third parties, i.e., to the partner-TSP; in relation to transborder transfers of data; and in relation to (maximum) pseudonymisation and anonymisation of data;
- ✓ strict legal arrangements and precise recommendations to users of the product on how to ensure full compliance with European and all relevant national data protection law in the use of the product;
- ✓ full compliance with the requirements of European law on the use of a processor by the user of the product; and
- ✓ clear transparency in terms of documentation and descriptions of the product.

The Conditions of Use and the Client Recommendations provided by the developer of the product furthermore ensure that for all the processing of personal data within the TOE there is a clear and valid legal basis (albeit that the legal basis differs depending on whether the product is used by a private- or a public-sector user, and on whether the processing relates to new or existing customers).

Also, as with the other ValidSoft products that have been awarded the European Privacy Seal, the TOE squares a difficult legal circle, in the sense that precisely because it is so highly-privacy-protective in the above ways, it makes it possible for the partner-TSP to lawfully assist the product in achieving its important aim.

Overall, the TOE, like the other ValidSoft products with the seal, will thus make the anti-fraud measures of financial institutions both more effective and more data protection-compliant. In that sense, the product shows that privacy protection and effective fraud (and general crime-) prevention measures are not a sub-zero game: one does not have to be less effective in fighting fraud (etc.) by having to comply with data protection rules. On the contrary, here we have another ValidSoft product that achieves both better protection against fraud, and higher standards of data protection, compared with the use of other, rogue products that operate in violation of European data protection rules.

**16. Issues demanding special user attention:**

The evaluators have not rated any of the issues as “additional safeguards needed”. There are a range of issues that users of the product must address, but these are, in their opinion, all adequately covered by the Conditions of Use of the product. They also concluded that the matters relating to the partner-TSP are adequately dealt with in the relevant clauses agreed (or to be agreed) with the partner-TSP. See section 11.A.5, above.

**17. Compensation of weaknesses:**

The evaluators have not rated any of the issues as “barely passing”, and there was therefore no need to address the question of whether such issues are compensated by the product.

**18. Decision table on relevant requirements:**

<i><b>EuroPriSe Requirement</b></i>	<i><b>Decision</b></i>	<i><b>Remarks</b></i>
Data Avoidance and Minimisation	<b>excellent</b>	All personal data, and in particular all internal and external data disclosures are kept to the absolute minimum. The partner-TSP is not provided with identifiable data and barred from identifying any data; and the users of the TOE are not provided with any e-communications data beyond what they already have, but rather only with a “Yes”/“No”/“Failure” result of the SIM-swap checks.
Transparency	<b>excellent</b>	ValidSoft’s Clients (the users of the TOE) are provided with full, detailed information, in particular through the Core Model Product Guide and the Conditions of Use for the product, which are set out in an Annexe to the contract between ValidSoft and the client (and which forms an integral part of the contract and have third-party effect to the benefit of the data subjects). There is moreover extensive one-on-one consultation between the vendor (ValidSoft) and its experts and the users’ (clients’) experts, and after-sale support.
Technical-Organisational Measures	<b>adequate</b>	The TOE is awarded “adequate” in respect of most technical aspects, because the actual measures to be taken, even if laid down in strict terms in the Conditions of Use, in practice still depend for their implementation on the client/user of the TOE, and are not in

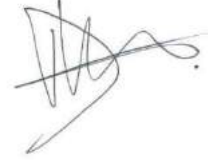


Valid-SSD 2nd Re-Certification SPR

		<p>the hands of the developer of the TOE, ValidSoft, beyond the imposition of such legal obligations. Some issues are not applicable; and in respect of data avoidance and minimisation the TOE was rated “excellent”, as already noted.</p>
<p><b>Data Subjects’ Rights</b></p>	<p><b>adequate</b></p>	<p>The TOE is awarded “adequate” in respect of the general data subject rights guaranteed by the main EC DP Directive (Dir. 95/46/EC), for the same reason as noted in respect of technical-organisational measures: because the actual measures to be taken, even if laid down in strict terms in the Conditions of Use, in practice still depend for their implementation on the client/user of the TOE, and are not in the hands of the developer of the TOE, ValidSoft, beyond the imposition of such legal obligations.</p> <p>We concluded that the e-Privacy Directive (Dir. 2002/58/EC) is not applicable to the processing within the TOE, and the data subject rights granted by that directive are therefore not applicable.</p>

### Experts' Statement

We affirm that the above-named IT product has been re-evaluated according to the EuroPriSe Criteria, Rules and Principles and that the findings as described above are the result of this evaluation.



Cambridge, UK,  
23 January 2018

Douwe Korff  
Em. Prof. of International Law

---

Place, Date

Name of Legal Expert

Signature of Legal Expert

---

Madrid, Spain  
23 January 2018

Javier Garcia-Romanillos Henriquez de Luna  
CISA, CISM, CRISC, LA 27000, LA 22301



---

Place, Date

Name of Technical Expert

Signature of Technical Expert

---

## Recertification Result

The above-named IT product passed the EuroPriSe evaluation.

It is certified that the above-named IT product / IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection.

Bonn, [DATE]          EuroPriSe CA

---

Place, Date

Name of Certification Authority

Signature