



Short Public Report

Recertification No.: 20090923 Valid-POS® 2017

1. Name and version of the IT product:*

Name of Product : Valid-POS® Standard Edition

Product Description : The product, Valid-POS® (“Point-Of-Sale”) is a tool that allows the user of the product, a bank or payment processor, to check if a bank card that is being presented for a payment at an Automated Telling Machine (ATM) or at a Point-of-Sales (POS) terminal, is in the same country or roughly in the same area as the bank card holder’s mobile phone. This greatly enhances the efficacy of the user’s anti-fraud measures.

This is the sole purpose of the Valid-POS® product.

Version : Version 2 (2012, unchanged)

*Note: This product is not currently offered under any other names, but this may in due course be offered in “branded” versions.

2. Manufacturer of the IT product:

Company Name:

ValidSoft UK Ltd.

Company Address:

35 New Broad Street
London EC2M 1NH
United Kingdom

Contact Person and Contact Details:

Alexander Korff, Esq., (ValidSoft UK Ltd General Counsel)
Address as above.

Phone: +44(0)7747128702

Email: alexander.korff@validsoft.com

3. Time frame of the re-evaluation:

December 2016 – January 2017

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, UK

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 GmbH

Address:

Joseph-Schumpeter-Allee 25

D-53227 Bonn

Germany

6. Specification of Target of Evaluation (ToE): [unchanged from 2012]

The target of this evaluation (TOE) is a tool to assist financial institutions in identifying possibly fraudulent credit- and debitcard “card-present” transactions at Automated Telling Machines (ATMs or “cashpoints”) and at Point of Sale (POS) terminals, as used in supermarkets, retailers, restaurants, etc. Basically, the TOE verifies, with the help of the partner-TSP, Elephant Talk, whether the card that is being presented is in the same country or area as the mobile phone that the cardowner has registered with the bank.

The tool is used, in somewhat different ways, for both in-country transactions (i.e., for transactions taking place within the country where the card has been issued) and for out-of-country transactions (when the card is used in a different country from the one where it was issued).

The tool seeks in particular to reduce the percentage of “false positives” (transactions wrongly identified as probably fraudulent by the banks’ or payment processors’ own “risk engines”), and therefore wrongly declined, from approx. 90% to less than 10%.

Further details are provided at 7.2 and 7.3, below; see also the Chart at 14, below.

7. General description of the IT product or IT-based service:

7.1 Background:

Plastic Card fraud has reached unprecedented levels around the world. In the US in 2008, Credit Card fraud reached over \$15.5bn, a 100% increase over the previous year. The total value of card-not-present transactions is expected to grow from \$9 billion in 2013 to nearly \$19 billion in 2018.¹ The picture is the same across Europe and the rest of the world. UK payment association Apacs recently published figures showing a massive 126% rise in fraud committed on UK cards abroad in the six months to June 2007. There was also 44% jump in card not present fraud, which rose from £95.3 million to £137 million.² In Germany, it is estimated that the cost of fraud is running at up to 40 basis points of card transaction value. The total fraud in Europe is estimated at between €5bn and €7bn in 2008.

Unfortunately these are only headline numbers and the real cost of fraud to the industry is 2 to 3 time greater due to resolution costs, administration costs, legal costs, restitution, etc. Leading Research Analysts are predicting that this type of fraud will treble in the next 3 to 5 years. With much of the proceeds from card fraud funding organised crime and terrorist activities it is not surprising that plastic card fraud is now the #1 fear of the US consumer.

Due to the limitations of current fraud detection technology in use today, the banking industry carries a significant cost in terms of False Positives. A False Positive occurs when a genuine transaction is incorrectly deemed to be fraudulent. The industry average for false positives is 9 in 10, - this means that for those transactions that are considered to be fraudulent, out of every 10 such transactions typically 1 is fraud and the remaining 9 are false positives. This equates to a 90% failure and the consequences are significant for both the industry and consumers alike.

Current detection and prevention technology is based on risk engines that typically analyse transactions based on historical spending patterns/activity. As reported above this approach results in high false positives. A telephone call needs to be placed and/or received from each customer for each false positive or fraud event. As a consequence the bank is forced to limit the amount of transactions it can process in order to balance the cost of resolution vs. actual fraud. This means that fraud transactions slip through the net. It is clear that existing detection and prevention technology is inadequate and a new approach is required. VALid-POS[®] seeks to provide the answer to this demand.

¹ Source:

<http://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php>

² Source:

<https://www.finextra.com/newsarticle/17598/card-fraud-patent-to-go-under-the-hammer>

7.2 Further details of the TOE: [See also the Chart in section 12]

The TOE essentially consists of a software programme - a virtual “box”³ - linked to the client’s own computers. The “box” can be installed at the client’s premises, or it can be hosted by a TSP based in the EU, Elephant Talk (ET), which has agreed to support the use of the TOE (subject to various legal conditions and arrangements, discussed at 11.A.5, below).⁴

If a proposed ATM- or POS-terminal transaction is assessed as potentially fraudulent by the client’s own risk engine, non-intrusive information on the ATM or POS terminal is sent over a secure link from the client to the “box”, together with the number of a mobile phone which the card-holder has registered with the bank that issued the card, and a unique lookup reference number. The information as sent from the client’s databases to the “box” does not reveal the geographical location of the ATM or POS terminal: for the “box”, it is simply a unique (abstract) number. The “box” passes the telephone number on to ET. ET carries out a “lookup” of the mobile phone in question and, on the basis of this lookup, sends non-intrusive (and largely obfuscated) information on the whereabouts of that mobile phone to the “box”. The obfuscation means, in particular, that the information as sent from ET to the “box” does not reveal the geographical location of the mobile phone: for the “box”, this too is simply a unique (abstract) number. Even so, this communication too is securely encrypted.

The software in the “box” correlates the data from the client and the data from the partner-TSP (ET) and - although neither the data sent to the “box” by the client nor the data sent to the “box” by ET consist of any actual geographical information - can determine from this whether it is likely that the card is in the same country or area as the mobile phone: if this is not the case, this suggests that the transaction is indeed potentially fraudulent, and that the client should indeed decline the transaction (as the client’s own risk engine suggested) - but that is up to the client. On the other hand, if the mobile phone is in the same country or area as the card, it is less likely that the transaction is fraudulent, and therefore more likely that the client’s risk engine’s conclusion was a “false positive”. The operation differs depending on whether the proposed card transaction is out-of-country or in-country, as explained below:

Out of country transactions:

For out-of-country transactions (i.e., for situations in which a card is presented at an ATM or POS terminal that is not in the country in which the card was issued), the correlation is very simple: the software simply checks whether the country where the

³ In this report, we will often refer to the product - that is: the lookup engine and the databases that constitute 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, which is installed on a client’s system; the “box” referred to is thus a purely virtual “box”. For that reason, the word is always placed in quotation marks.

⁴ ET is therefore hereafter often referred to as “the partner-TSP”, usually with ET still added for clarity, in brackets. In future, actual deployments, ValidSoft may also consider other partner-TSPs in the Netherlands or the UK, but such actual deployments and such new partners would require a new evaluation, or at least an evaluation update, in accordance with the *EuroPriSe* requirements.

ATM or POS terminal is situated in the same country as the country where the cardholder's mobile phone is at the time of the check.

In-country transactions:

For in-country transactions, the system is more sophisticated in that, from the data supplied by the banks and the partner-TSP (ET), it discerns patterns linking ATM/Point-of-Sale devices and the mobile network - but, crucially for the purpose of the EuroPriSe evaluation, without the system (or the client/user of the product) being provided with actual traffic- or location data. Based on these rules, a transaction confidence indicator can be applied to a transaction.

In either case (out of country or in-country), the outcome of the correlation is passed on to the client in the form of a “**Result**”. This can be “**Confirm**” (the ATM or POS-terminal and the phone are in the same country or area, and the transaction is therefore probably genuine), or “**Refute**” (the ATM or POS-terminal and the phone are not in the same country or area, and the transaction is therefore probably fraudulent), or “**Unsuccessful**” (e.g., because the phone was not switched on). To a successful lookup, the “box” furthermore adds a **Score** indicating the level of confidence with which the result is reached. It is left up to the Client to decide whether or not to allow the payment, taking into account this result.

These results are also retained (with the lookup reference number) in a “Result Log” within the VALid-POS® “box”. However, the system keeps all processing and retention of personal data to the absolute minimum, as further discussed in section 13. Here, it may suffice to note that the partner-TSP (ET) does not retain any details of the lookup (beyond recording that a lookup took place, but without the specific mobile telephone number being stored). The “box” also does not retain detailed information: beyond the brief “learning” period for in-country checks, it only retains the “results” with reference to a number given to each lookup request by the client.

Crucially, in spite of this minimal personal data processing, the TOE manages to reduce “false positives” for card-present card fraud by some 90%.

7.3 What is and what is not included in the TOE: [unchanged from 2012]

The Target of Evaluation (TOE) includes all data, data flows and data processing within the VALid-POS® “box”, and the 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 (the client/user of the TOE) prior to or after his use of the “box”, or processing by the partner-TSP (ET), except insofar as certain legal arrangements are concerned, as noted below and as further discussed at 13.A.5.

Note:

As already indicated above, the evaluation concluded that the user of the VALid-POS® “box” (i.e. the bank or payment processor) is to be regarded as the controller of all the processing associated with the use of the VALid-POS® “box”. This affects the scope of the evaluations, as noted below. This also means that in the text, below, the terms “*controller* [of the processing associated with the use of the VALid-POS® “box”]”, “*user* [of the VALid-POS® “box”]” and “*the client*” are used interchangeably (although we have tried to avoid confusion)

The TOE (and the evaluation) therefore include and exclude the following (exclusions are set out in *italics*):

General:

- ✓ The evaluation assessed compliance with all relevant EC data protection requirements by the controller of the processing (the user of the product) relating to his use of the VALid-POS® “box”, and it covered the legal arrangements between that controller and other parties to ensure this compliance (see section 11.A.5, below), but:
 - *It did not cover the question of actual compliance with the requirements of the EC directives by those other parties beyond the legal arrangements.*

Processing inside the VALid-POS® “box”:

- ✓ The evaluation covered all processing of all data within the VALid-POS® “box”, including the questions of data minimisation, data security and integrity, data retention.

The various data flows into and out of the VALid-POS® “box”:

There are only four data flows within the TOE (see the Chart in section 14):

- (1) The sending of an ATM or POS-terminal reference and a mobile phone number by the client to the VALid-POS® “box”;
- (2) The passing on of the mobile phone number from the “box” to the partner-TSP (ET);
- (3) The passing on of obfuscated data on the whereabouts of the phone from ET to the “box”; and
- (4) The passing on of the “result” of the data analysis within the “box” from the “box” to the client.

Because the evaluation concluded that the user of the VALid-POS® “box” is to be regarded as the controller of the processing associated with the use of the VALid-POS® “box”, the evaluation covered the first, second and fourth of these data flows in full. Accordingly:

- ✓ The evaluation assessed whether the product and the product information ensured that (provided the product is used in accordance with the contracts and Conditions of Use) all of these (internal and external) disclosures are in accordance with all relevant EC data protection requirements,; and
- ✓ The evaluation assessed whether the contracts and Conditions of Use for the VALid-POS® product adequately spell out what the user of the product must do in its contracts with its customers or in its standard Terms & Conditions, and in its legal arrangements with other parties (see at 13.A.5), but:
 - *It does not cover the bank’s or payment processor’s own processing of the data prior to the passing on of data to the VALid-POS® “box”, and in particular does not include the bank’s or payment processor’s own risk assessment (as performed by their own risk engine);*

- *It does not include the client’s own processing of the data after the disclosure of the “Result” from the VALid-POS® “box” to the client, i.e., it does not cover the way in which these results are further processed or used by the client (except for the stipulation in the Conditions of Use of the product that the data may only be used for fraud prevention). In particular, it does not address the question of whether the client is, or is not, justified in not authorising (or subsequently challenging) a transaction as possibly, or probably, fraudulent; and*
- *It does not address general issues concerning the relationship between the card-issuing bank and the cardholder, other than in relation to the use of the relevant (internally and externally disclosed) data for the purpose of fraud detection and prevention. And in that latter respect, it is limited to evaluating the adequacy of the legal arrangements imposed on the user of the product by the developer of the product, especially in terms of transparency vis-à-vis the cardholders. The evaluation does not include an assessment of the adequacy or otherwise of the actual contracts between the user of the product and the bank customers/card holders, or of the bank’s or payment processor’s standard Terms & Conditions.*

On the remaining (third) data flow (the passing on of obfuscated data on the whereabouts of the phone from ET to the “box”), the evaluation covered:

- ✓ The legal arrangements between the client and the partner-TSP (ET) in relation to the data exchanges between the VALid-POS® “box” and ET, including the warranties that are provided by ET (as further noted at 13.A.5); and in the light of these legal arrangements,
- ✓ The question of whether the collecting of data by the user of the VALid-POS® “box” (i.e., by the bank or payment processor), from the partner-TSP (ET), through the “box”, is in accordance with the relevant EC data protection requirements; but
- *It does not cover the processing, by the partner-TSP (ET), of the data provided to it by the clients via the VALid-POS® “box”, beyond assessing the adequacy of the relevant guarantees and warranties provided by ET, i.e., it does not assess whether ET actually acts in accordance with such guarantees and warranties -*
- HOWEVER, given the crucial importance of the support for the TOE by ET, the evaluation did address the question of the legal basis of this support: see section 11.A.2, under the subheading “processing of traffic- and location data”.

8. Transnational issues:

[unchanged from 2012]

The TOE is offered to potential clients (in particular, banks and payment processors) worldwide. The evaluation addressed two issues in this connection: transborder data flows and the question of “applicable law”.

Transborder data flows:

The use of the product will almost invariably involve transborder data flows, including exports of data from the EU/EEA to third countries, including third countries without “adequate” data protection. The compatibility of such data exports with the European standards is assessed in section 13.A.3, below, under the heading “transfers to third countries”.

Applicable law:

The evaluation also examined the question of “applicable law” (Article 4 of Directive 95/46/EC). The evaluation concluded that if the client (being the controller: see the Note on p. 5, above) 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 (and that national law only).

In respect of clients (controllers) established outside the EU/EEA, the evaluation concluded that the reliance by them on the assistance of the partner-TSP (ET) meant that they used “means” in the place of establishment of ET; and that therefore the law of the place of establishment of ET applies to their (the clients’) processing of personal data within the TOE (as well of course as to the processing by ET itself). A crucial conclusion of the evaluation, confirmed by the Certification Body when it awarded the seal, is that as long as the clients comply with the Conditions of Use for the product, as laid down in the legal documents discussed in section 13.A.5, below, they will also comply with the relevant European standards in this respect.

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

[unchanged from 2012]

The TOE essentially consists of a relatively simple software program installed on a dedicated carrier or “box”⁵ 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 host platforms that may be adapted to the client’s needs. The databases are usually hosted on the client’s own environment, adapted to their database system, but can also be hosted with the partner-TSP, ET. Specifically:

Software	:	written using Java and JSP running under Tomcat
Database	:	MS SQL Server, but may be adapted to the client’s needs
Communications	:	secured with at least SSLv3.0/TLSv1.0
Encryption method	:	SHA-256 and algorithm PBEWithMD5AndTripleDES.

10. Edition of EuroPriSe Criteria used for the evaluation:

EuroPriSe Criteria, version November 2011.

⁵ See footnote 1, above.

11. Modifications / Amendments of the IT product since the last re-certification:

[unchanged from 2012]

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 last re-certification:

For the September 2011 re-evaluation, the requirement profile needed updating in one respect: as concerns the application of the main data protection directive (Directive 95/46/EC), and the non-application of the e-Privacy Directive (Directive 2002/58/EC), to the processing of geographic data by the users of the TOE. This update followed from the issuing of a new Opinion on the processing of geographical data in smartphones, issued by the Article 29 Working Party.

The 2012 Recertification Report incorporated the additional comments and analyses provided in this respect in the September 2011 Update Check Report, in the paragraphs on the legal basis of the processing of the personal data generally, and of traffic- and location data, re-stated in sub-section A.2 in section 13, below; and it added some further information in respect of some processing that is outside the TOE but still important to the TOE, in the latter paragraph (on processing of traffic- and location data).

The 2017 re-evaluation found that of all the the WP29 opinions and working documents from April 2014 to January 2017, only WP224, the WP's Opinion 09/2014 on "device fingerprinting" (dated 25 November 2014), contained possibly relevant observations, i.e., that the requirements set out in the WP29 Opinion 04/2012 in relation to cookies also applied to "device fingerprinting" technologies, which should be regarded as "similar technologies" to cookies. However, since in the use of the TOE the devices (mobile phones) of the data subjects (bank customers) are uniquely identified, but only by the mobile phones' calling number, and since the banks are provided with these phone numbers by their customers and do not actively access information on the customers' devices, it was concluded that Art. 5(3) e-Privacy Directive and the WP29's opinion on device fingerprinting are not applicable here.

In addition, it was found that the first sentence in the first paragraph of Article 94 of the second Payment Services Directive (PSD2), as adopted and now in force, if anything reaffirmed that the processing of personal data by banks on their own existing customers for fraud prevention purposes is fully justified in terms also of the PSD2 as necessary for the performing of a task in the public interest provided all other EU data protection requirements are met; and they are all fully met in the Valid-POS product.

In sum, the re-evaluation concluded that nothing in Opinion 09/2014, or in any of the other opinions and working documents issued by the Art29WP since the 2014 renewal of the European Privacy Seal to the TOE, or in the PSD2, required any change in the assessments.

Moreover, the EuroPriSe Criteria Catalogue requirements relevant to the TOE have not changed. There are no new technical standards relevant to the TOE. The state of the art has not changed.

13. Evaluation results:

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 TOE serves only one purpose: to assist financial institutions in countering the fraudulent use of credit- and debit cards, both in-country and abroad, by reducing the levels of “false positives” generated by the institutions’ own risk engines. More briefly: fraud prevention. No other, further purpose or purposes is, are or can be served by the 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 (the client) is to be regarded as the “controller” of basically all the processing within, or carried out with the help of, the TOE: it is the user/client (in practice, a bank or Payment Processor) who decides to use this product for its own purpose - to prevent fraud; 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 (the bank or the Payment Processor) to the VALid-POS[®] “box”, the external disclosure of data to the partner-TSP (ET); the obtaining of data from that third party;* the internal processing within the VALid-POS[®] “box”; and the internal disclosure of the “results” of that processing from the “box” to the product user’s own systems. (* see the Note below).

The evaluation concluded, and the certification confirmed, that the client must still be regarded as the controller of the processing within the TOE, also in the scenario in which the “box” is hosted by the partner-TSP (ET), because even in this situation, it will still be the client who determines the purposes and means of the processing; in this case, for this processing within the TOE, the partner-TSP (ET) will be a processor acting on behalf of the controller (the client/user of the product). On the other hand, the partner-TSP (ET) is the controller of the processing it carries out (outside of the TOE) to perform a “lookup” (see again the Note below).

The evaluation stressed that the above requires appropriate contractual etc. arrangements, and found, upon examination, that such arrangements are in place. Indeed, as noted in section 13.A.5, below, those legal arrangements are rated “excellent”.

Note *: The above does not cover the processing carried out by the partner-TSP (ET), in order to perform a “lookup”, or the disclosure of the data sent by ET to the “box” (which is the mirror of the obtaining of those data by the client), irrespective of whether the “box” is hosted by ET or not, because that processing by ET - of which ET (rather than the client) is the controller - is always outside the TOE: see section 7.3, above. However, given the importance of this processing by ET for the product, the evaluation nevertheless included an assessment of the legal basis of this processing: see section 13.A.2, under the subheading “processing of traffic- and location data”.

Given the complexity of the roles of the entities involved, the evaluation rated this issue “adequate” (but as already noted, it rated the legal arrangements covering the relationships as “excellent”: see again section 13.A.5, 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-POS[®] product.

Traffic- and location data:

Although this is not covered specifically in the Criteria Catalogue, other than in relation to the question of legal basis, as discussed in section 13.A.2, below, the preliminary question does arise whether “traffic- and location data” as defined in the e-Privacy Directive (Directive 2002/58/EC) are being processed.

On the basis of extensive analysis, the evaluation concluded that (for both cross-border and in-country lookups) the data that are sent to the “box” by ET are not of sufficient granularity to constitute “traffic- and location data”, and that the client also does not “reconstitute” such data. In other words, no “traffic- or location data” within the meaning of the e-Privacy Directive are processed within the TOE.

(It may be noted, however, that that issue aside, it has become clear from an Article 29 Working Party Opinion that the rules in the e-Privacy Directive on the processing of traffic- and location data in any case only apply to e-communication service providers, and not to entities such as the users of the TOE. This is discussed under the heading “processing of geolocation data”, below.)

However, the evaluation also concluded that it was indisputable that the partner-TSP (ET) processes traffic- and location data in order to carry out the lookup asked for by the client (in an automated way, via the VALid-POS[®] “box”). It was felt that although this processing was as such outside the TOE, the matter was too closely related to the use of the product to be left out of the evaluation, and the legal basis for this processing was therefore still carefully examined. The results of this assessment are summarised in section 13.A.2, below, under the heading “processing of traffic- and location data”. Suffice it to note here that the evaluation concluded that the processing was lawful, again especially also in the light of the very strict legal arrangements (discussed in section 13.A.5, below).

Data Avoidance and Minimisation

[Criteria Catalogue, sections 1.2.1, 2.2.2, and 2.2.3]

The evaluation concluded that it would not be possible to check whether proposed credit- or debitcard transactions are (or are not) possibly fraudulent, without using data that is linked specifically to the card in question, and indeed to the ATM or POS-terminal at which the card is presented. It is also impossible to carry out the cross-check of whether the cardholder's (registered) mobile phone is near (or in the same country as) the ATM or POS-terminal where the card is presented without looking up where that phone is.

That said, the evaluation also concluded that all personal data, and in particular all internal and external data disclosures made in the course of using the product, are kept to the absolute minimum, and anonymised to the furthest extent possible.

Specifically, the evaluation concluded that the personal data passed on by the client to the "box", and from the "box" to the partner-TSP (ET), are kept to the absolute minimum. The same applies to the data that make up the "result" that is sent from the "box" to the client at the end of the VALid-POS[®] process.

Most importantly, however, from the data that are sent to the VALid-POS[®] "box" by the partner-TSP (ET), the client only learns:

- ✓ for out-of-country transactions:
 - that the mobile phone is in a particular country; and
- ✓ for in-country transactions:
 - that the mobile phone is in the same broad geographical area as the credit- or debitcard (but without that broad geographical area being identified).

This can be done in this minimal-data way because, as explained at 7.2, above, the VALid-POS[®] product does not depend on the granularity value of the information: rather, it relies on the uniqueness of the returned value.

The evaluation found this to be the most important data-minimisation measure in the whole VALid-POS[®] process. The evaluation consequently rated the product "excellent" on data avoidance and minimisation.

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

On the basis of a close examination of the legal arrangements (further discussed at A.5, below), the evaluation concluded that the main basis for the processing within the TOE was consent, obtained in a contractual context. This applies in particular to new customers/cardholders of the banks, as further explained below. As concerns existing customers/cardholders, who have provided their mobile phone number to the bank before the bank started using the product, the situation is somewhat more complex, as also further discussed below.

Some further special consideration was given to the question of the legal basis for the processing of traffic- and location data by the partner-TSP (ET), even though as such this processing is outside the TOE.

Processing on the basis of consent, provided in a contract (with reference to another legal basis of processing, “balance”) (Art. 7, paras. (a), (b) and (f) of Directive 95/46/EC)

[Criteria Catalogue, sections 2.1.1.1 and 2.1.1.2, addressed jointly, with a brief reference in a note to the issue covered by section 2.1.1.5]

The evaluation concluded that all the processing by the client of data on the cardholders in relation to its use of the TOE, should be to be treated as processing of personal data in relation to the contract between these parties, and therefore had to be assessed with reference to Article 7(b) of the Directive. The evaluation noted that any contract under which a bank issues a credit- or debitcard of course will invariably allow for the use of the cardholders data also for the secondary purpose of preventing fraudulent use of the card; and that such secondary use was also, in any case, compatible with the primary use of the contract: to allow the use of the card for financial transactions.

The evaluation also concluded that the processing (i.e., all the processing operations within the TOE) are “necessary” in the sense of Article 7(b) of Directive 95/46/EC. Of course, it is not necessary for every bank or payment processor to use the specific product, VALid-POS[®]. But the evaluation found that that is not how this article should be read. Rather, Article 7(b) relates to processing that is necessary to allow the proper implementation of the contract between the bank and its cardholder. The evaluators felt that this undoubtedly covered appropriate checks to prevent fraud; and that the product was undoubtedly an appropriate means of performing those. They therefore concluded that, the use of the TOE in accordance with the Conditions of Use for the product could indeed be said to be “necessary” for the performance of the contract relating to card use between the bank and the cardholder.

The evaluation nevertheless welcomed the fact that the (legally binding) Conditions of Use for the product go well beyond simple reliance on the banks’ standard Terms & Conditions, in that they stipulate that both existing and new cardholders must be fully informed, in the terms and conditions for the use of their card, of the use of their mobile phone number for fraud prevention purposes, before that number is used in this way; and that they must be offered an opt-out from this.

The developer of the VALid-POS[®] product has indeed gone beyond this, by providing its Clients, in the “Core Model Product Guide” to the product, with template texts for the provision of the relevant information by its clients to the clients’ customers (the cardholders).

The evaluation concluded that, provided the clients comply with these stipulations (as they are legally required to do under the Licensing Agreement for the product, subject to contractual penalties if they fail to do so), the clients’ customers can actually generally be said to have consented to the use of the VALid-POS[®] product (even if that specific product is not necessarily expressly identified or mentioned by name in the clients’ information).

This is manifestly clear as concerns new cardholders: they are clearly informed, in advance, of the use of their mobile phone data to check whether they are in the vicinity of an ATM or POS-terminal where their card is presented; they provide their mobile phone number in this knowledge; it may not be made a condition of use for the card that they provide their mobile number; and they can even later opt out of this use of their mobile phone data.

The evaluation concluded that it is strongly arguable that this also holds true for existing customers (cardholders). In strictly legal terms, their original contract will have bound them, not just to the original terms of that contract, but also to any changes in the terms and conditions, provided they were duly informed of those changes. In legal terms, their original agreement (= consent) to the contract, and to those terms and conditions, therefore extends to any new (revised) terms and conditions, of which they were duly notified (provided of course that those terms and conditions were fair and lawful under contract- and consumer law, etc., but that was not an issue here).

Yet again, the arrangements for the product go beyond this: the Conditions of Use for the product stipulate that the attention of the data subjects (existing cardholders) must be expressly drawn to the new uses of their mobile phone data (if they previously provided those; if not, they are in the same position in this regard as new customers); and that they must be expressly informed of their right to opt out of the new use of those data. The evaluation concluded that if, after this, they continue to use their card, and do not use the opt-out, they too will have effectively consented to the new use of their mobile phone data.

However, as noted under the next sub-heading, the evaluation nevertheless also examined whether, with regard to cardholders who had provided their mobile phone numbers prior to the use of the product, there was a possible alternative legal basis for the processing of that datum.

Here, it will therefore suffice to note that the evaluation concluded that:

- (i) *at least for new cardholders*, all processing of personal data - including the processing of cardholders' mobile phone numbers - within the TOE was fully based on the consent of the data subjects, given in a contractual context; and
- (ii) it was strongly arguable that the same applies in respect of existing cardholders, but this need not be finally resolved because, as discussed under the next heading, the processing can also be fully based on an alternative criterion, processing on the basis of a public interest.

Note:

The evaluation found that, in principle, the processing within the TOE could also be argued to be permitted on the basis of the "balance" provision (Art. 7(f) of the Directive), but welcomed the fact that the arrangements did not rely on this.

Processing on the Basis of a Public Interest or Task (Art. 7(e) of Directive 95/46/EC)

[\[Criteria Catalogue, section 2.1.1.5\]](#)

The evaluation noted that Article 94(1) of the Second Payment Services Directive (PSD2)⁶ expressly stipulates the following:

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.

The evaluation noted that this is a mandatory clause: the Member States **must** (“shall”) permit such processing (but they must at the same time ensure that it meets the requirements of Directive 95/46/EC, and also of Directive 2002/58/EC).

The evaluation found that this clause is a clear recognition of the fact that processing of personal data by payment systems and payment service providers serves an important public interest (as well, of course, as the private [financial] interests of the banks and the cardholders). This means that such processing can be said to be carried out (also) “for the performance of a task carried out in the public interest”, as mentioned in Article 7(e) of Directive 95/46/EC.

However, there is still the need to comply with all other requirements of Directive 95/46/EC, and indeed Directive 2002/58/EC, including especially the informing requirements. In practice, this means that cardholders should still, at least, be informed of the use of their mobile phone data for fraud detection and –prevention purposes, and indeed that they should be able to opt out of such uses of those data. In other words, the requirements in terms of Article 7(e) of Directive 95/46/EC, just noted, are in practice not all that different in the present case from those imposed by Article 7, paras. (a) and (b), as discussed under the previous sub-heading.

The evaluation found it nevertheless useful to note that, to the extent that the processing of data on existing cardholders could perhaps not be based on their consent, obtained in a contractual context, all processing of personal data - including the processing of cardholders’ mobile phone numbers - within the TOE is carried out “for the performance of a task carried out in the public interest”, fraud prevention; and the evaluators also concluded, on the basis of the same considerations as were spelled out in relation to processing to perform a contract, that the processing is “necessary” for that public interest. To the extent that the processing of personal data (including mobile phone data) on existing cardholders might therefore not be based on consent, obtained in a contractual context, it can therefore be based on the alternative criterion in Article 7(e).

⁶ Full title: Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, repealing Directive 2007/64/EC.

Processing on the Basis of Balancing of Interests (Article 7(f) of Directive 95/46/EC)

As noted in section 2.1.1.2 of the original evaluation report, we believe that all the processing by the client using the TOE is covered best by Article 7(b) of the Directive, as “necessary” for the taking of the “step” to authorize the cash withdrawal or payment; and covered by the consent of the cardholder, given under the contract with the card-issuer (with full, specific information, and an opt-out).

However, we feel we may mention that, in our opinion, if it were to be argued that the processing by the client could not be based (solely) on that criterion, it is fully justified under Article 7(f), which allows for a balancing of the rights and interests of the various parties involved.

Specifically, we are of the opinion that all the processing by the client (to the extent that it is not already justified under Article 7(b)), is “necessary” to protect the “legitimate interests” of the controller (the bank or Payment Processor), and/or of the (possibly different) bank operating the ATM, and/or the company holding the POS-terminal where the card is presented; and we feel that these interests are clearly not overridden by any interests (let alone the fundamental rights) of the data subject, in whose name the card is registered. On the contrary, appropriate checking of a proposed card transaction to prevent fraudulent use of the card is also very much in the interest of the cardholder. As explained under the heading “processing of geolocation data”, below, we conclude that the above also applies to the processing of (minimal) geographical data by the users of the TOE.

(The question of course again arises of what constitutes an “appropriate” check, and in particular if the process otherwise fully complies with data protection rules - but that again is dealt with in the rest of this report.)

Scope and applicability of Directive 2002/58/EC

In 2011, the Article 29 Working Party has issued an opinion on geolocation services on smart mobile devices.⁷ This makes clear 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 the original evaluation report on the TOE, i.e., it does not apply to any other entities, such as companies that provide (value-added) location- or information society services.⁸ Rather, the latter’s use of any geographical information (be it derived from e-communication base stations, WiFi information or GPS) is subject to the general rules in the general data protection directive (Directive 95/46/EC).

We will therefore below discuss separately, first, the issues arising under the e-Privacy Directive as far as the processing by ET is concerned (even though that is strictly speaking outside the TOE). We will then, in an added section, briefly discuss the

⁷ [Opinion 13/2011 on Geolocation services on smart mobile devices](#), 16 May 2011, WP185.

⁸ *Ibid.*, section 4.2.1, *Applicability of the revised e-Privacy directive*, on pp. 8 – 9.

question of the processing of (extremely basic) geographical information by the user of the TOE, by means of the “box”.

Processing of traffic- and location data by the partner-TSP, ET

[Criteria Catalogue, sections 2.1.4.2 and 2.1.4.3]

In sub-section A.1, above, it was already noted that no traffic- or location data are processed within the TOE, but that the partner-TSP (ET) does process such data.

The partner-TSP (ET) does not itself obtain the consent of the data subjects on whom it processes data (i.e., the mobile phone subscribers) for this processing. However, the Article 29 Working Party has made clear that for the processing of traffic- and location data for “value-added services”, the relevant consent can be obtained by a third party, i.e. the party offering the “value-added service” requested by the data subject.⁹ The consent obtained under the contracts between the users of the TOE and the cardholders is therefore important.

In addition, the evaluation found that under the law of the place of establishment of the partner-TSP (ET) (which is the applicable law in this respect), the partner-TSP (ET) could in any case process traffic- and location data for fraud prevention purposes, without the consent of the data subjects, also in support of anti-fraud measures by private entities (such as the users of the TOE); and that this was allowed under Article 15 of Directive 2002/58/EC.

Taking the above into account, the evaluation concluded that with regard to new customers/cardholders, the legal basis for the processing of the traffic and location data could be either the cardholders’ prior consent, or Article 15 of Directive 2002/58/EC, but that as concerns existing customers (i.e., customers who obtained a credit- or debitcard, and provided their mobile phone number to a bank, prior to the use of the TOE), Article 15 was a sufficient legal basis in itself, especially in view of the extensive arrangements to ensure that the data subjects/existing cardholders were fully informed of the processing and offered an opt-out from it, provided that the carrying out of the lookups was done by the partner-TSP (ET), which is established in a country that applies Article 15 of the e-Privacy Directive in the manner described above, also to the benefit of private entities. The developer of the product has provided assurances to that effect, in relation to ET, and the seal will be awarded on that basis.

Processing of geolocation data by the users of the TOE

As noted earlier, the WP29 has concluded that the processing of geographical information of any kind (derived from e-communications base stations, WiFi locations or GPS), by any entity other than e-communications service providers, should be assessed under the rules of the general data protection directive, Directive 95/46/EC (and not under the e-Privacy Directive, Directive 2002/58/EC, as amended).¹⁰

⁹ See WP29 Opinion 5/2005 on the use of location data for value-added services (WP115), p. 6

¹⁰ See footnote 5, above.

For typical value-added services, this will require the consent of the data subject - but, notably, this is “ordinary” consent, of the kind mentioned in Article 7(a) of the Directive and defined in Article 2(g), and not the more demanding “explicit consent” referred to in Article 8(2)(a).¹¹ This means that the WP29 holds that, certainly for the present, geographical information about a person’s whereabouts should be treated as personal data, but not as “sensitive” data. Indeed, the majority of Member States (and, apparently, of members of the WP29) feel that neither geographical nor location data should be added to the list of “sensitive” categories of data when the general directive is revised or replaced, as is due in the near future; and indeed the now-adopted General Data Protection Regulation does not include them in that category (see Art. 9 of the Regulation which by the way leaves the e-Privacy Directive in place: see Art. 95).

This in turn means that in certain cases, of less typical kinds of “services”, the processing can also, where appropriate, be based on any of the other, alternative “criteria for making processing lawful”, listed in Article 7 of the general directive. This includes processing on the basis of the “balance” criterion in Article 7(f) - albeit of course always provided any other applicable requirement, especially on informing of data subjects etc., is also fully complied with. The WP29 explicitly accepts this for WiFi points based geographical information, even if for “normal” information-based services it would normally wish to base the processing on (ordinary) consent, but it must follow from its basic approach that for not-so-ordinary activities, such as fraud prevention, the “balance” criterion can be relied on as a basis for the processing of geographical information (to the extent that it is not covered by special exceptions adopted by Member States in accordance with Article 13(1)(d) of the general directive).

A.3 Selected other topics

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

As noted at sub-section A.2, above, the (binding) Conditions of Use for the TOE are very demanding in terms of informing the data subjects (the cardholders/mobile phone owners), and the “Core Module Product Guide” for the product provides clear and detailed recommended information templates.

This is an area in which the product - taking into account the legal requirements surrounding the use of the product - clearly meets the European standards.

In this context, the evaluation also welcomed the strong guarantees and warranties in the contract between ValidSoft and its partner-TSP (ET), which include a warranty from ET that ET, under the law of its country of establishment (in the EU), is legally permitted to carry out the processing in support of the TOE, i.e. the lookup and the passing on of the (largely obfuscated) network segment data; and that it has complied with all relevant requirements, including information requirements, in this respect. See further at section 13.A.5, below.

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

This is only relevant to the situation in which the VALid-POS[®] “box” is installed (hosted) within the premises of the partner-TSP (ET). The evaluation concluded that in

¹¹ See section 5.2.1, pp. 13 – 16, of the Opinion.

that case, while the client bank remained the controller, ET acts as processor for the client in its management of the VALid-POS[®] “box”. At the same time, in this situation (as in the ones in which ET does not host the “box”), ET is also a separate third-party controller, in particular in its carrying out of a lookup.

The evaluation concluded that there is nothing in the European rules that stands in the way of some of the processing within the TOE being delegated to a processor, provided the relevant general requirements for processing by a processor are met.

These requirements are basically quite simple: there must be a written contract or similar binding instrument, stipulating in particular that the processor shall only process the data sent to it by the controller on the instructions of the controller, and as instructed by the controller; and requiring the processor to comply with the data security requirements of the law of the place of establishment of the processor (cf. Article 17(2), (3) and (4) of the main Directive).

In the VALid-POS[®] scheme, ET is bound in this way through written undertakings between it and the developer and vendor of the VALid-POS[®] product, ValidSoft Limited, contained in a detailed Annexe to this contract, which also extend to (and can be legally invoked by) the users of the product, and of which the users of the products (the clients) are informed in the product information. In this situation, in which the “box” is hosted by ET, the users of the product also have the right to verify that the processing within the “box”, carried out by ET in its capacity as processor, conforms to these undertakings. Specifically, this is facilitated by the automated keeping of tamper-proof logs of the processing within the VALid-POS[®] “box”.

The evaluation concluded that these binding written undertakings and logging etc. arrangements fully met the requirements of Article 17 of the Directive. Indeed, the legal arrangements overall were rated “excellent”, as further discussed in section 13.A.5, below.

Transfers to Third Countries

[Criteria Catalogue, section 2.4.2]

As already noted at A.1, above, above, the evaluation concluded that the use of the product almost always will involve transborder data transfers, including transfers of personal data to third countries without adequate data protection.

The evaluation concluded that these transfers were nevertheless allowed, because they are “necessary 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 Directive. In particular, the evaluation concluded that the contract under which the lookups take place (i.e., the contract between ValidSoft and the partner-TSP (ET)) was “concluded in the interest of the data subject”. It noted that Article 26(1)(c) does not say that the contract has had to be concluded solely in the interest of the data subject. Clearly, it suffices that the contract is also in the interest of the data subject.

The evaluation also concluded that the transborder data export flows in question are “necessary” in the sense of Article 26(1)(c). Indeed, the contract would be meaningless and useless without these transfers (at least in cases in which the clients/users of the product/banks are outside the EU/EEA).

The evaluation concluded that, because the transborder data flows are lawful under Article 26(1)(c), it was not necessary for the users of the product to use standard contract clauses of the kind envisaged in Article 26(4) of the Directive, or to adopt Binding Corporate Rules, such as are being encouraged under Article 26(2), etc. However, it is still important to note that the evaluation concluded that the TOE provides for further, enhanced protection, also in respect of exports of data to third countries without adequate protection: this confirms that such exports (even if allowed under Article 26(1)(c)) will not result in any erosion of the rights of data subjects.

Formalities

[Criteria Catalogue, section 2.5]

It is made clear in the (legally binding) Conditions of Use for the product 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 requires the client to comply with any legal requirement of the relevant applicable law to carry out a Data Protection and Security Audit.

The evaluation concluded that this met the requirements of the European rules (but see the Note under the next heading, below).

A.4 Data subjects’ rights

[Criteria Catalogue, Set 4]

It is made clear in the (legally binding) Conditions of Use for the product that the client is required to comply with all relevant requirements of the applicable law in relation to data subject rights, including the right to confirmation of processing, the right of access, rectification or erasure, the right to object, etc. As noted below, at A.5, the legal arrangements also ensure that the data subjects are fully informed of their rights, including their right to be informed about any information on them (or their credit- or debitcard) in the VALid-POS[®] results log.

The evaluation concluded that this met the requirements of the European rules.

Note relating to the issues of formalities and data subject rights (et al):

In respect of the matters addressed in this section and in the previous sub-section (and various other sections, including those relating to technical issues, below), the most that the developer and vendor of the TOE 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. In addition, for the situation in which the partner-TSP (ET) hosts the VALid-POS[®] “box” and acts as processor for the clients, ValidSoft can stipulate similar conditions in its contract with ET (which have third-party effect and thus also benefits the clients). These legal stipulations are discussed in section 13.A.5, below. Suffice it to note here that these legal arrangements have been rated “excellent” by the evaluation.

A.5 Documentation of the product: the legal arrangements¹²

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

- The “Core Model Product Guide” (and miscellaneous information provided to clients and prospective clients, such as PowerPoint slides for a presentation on the product, etc., which is also included in the documentation pack on the product, provided to clients);
- The standard contract between ValidSoft Ltd and a Client, including the Conditions of Use of the VALid-POS[®] product, which are set out in an Annex to this contract (and which forms an integral part of the contract); and
- The contract between the developer and vendor of the product, ValidSoft Ltd, and the partner-TSP (ET), including an Annex to this contract (which forms an integral part of the contract), which provide certain important guarantees and warranties, also to the clients/users of the product, as third-party beneficiaries.

The evaluation examined the relevant clauses in these contracts and annexes, and some further legal arrangements, in detail. Given the commercial sensitivity of the clauses and arrangements, it must suffice to describe them here in broad terms, while noting that the evaluation examined them in full.

Basically, the ValidSoft – Client contract ensures, inter alia:

- ✓ that the product (and the data generated in the use of the product) will only be used for fraud prevention purposes, and always fully in compliance with the relevant applicable national data protection law;
- ✓ that the customers (cardholders) are fully informed of the use of their mobile phone number for these purposes, and given the opportunity not to have their mobile phone number used for these purposes (as described in section 2.1, above); and
- ✓ that the client adopts state of the art security and encryption measures, and keeps these up to the latest standards.

Clients are subject to strict penalty clauses for failure to comply with the stipulations in the contract (or its annex, which is part of the contract).

ValidSoft has provided the EuroPriSe Certification Body with a formal, written Undertaking, guaranteeing that it will always use the clauses that were approved in the EuroPriSe certification process in any contract with a client to which the seal applies, and that it will always obtain written confirmation from the lawyers that draw up the relevant contract confirming that the clauses have been fully and properly incorporated in the overall contract.

¹² 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.

Under the ValidSoft – ET contract, inter alia:

- ✓ ET undertakes not to disclose any actual traffic or location data to in relation to the use of the TOE, a client (user of the TOE), but rather, to only send much more limited data to the VALid-POS[®] “box” in obfuscated form, using state of the art one-way encryption and a state of the art secure communications link;
- ✓ ET warrants that it is permitted, under the law of its country of establishment, to carry out lookups of mobile phone numbers for fraud prevention purposes, also in relation to private entities; and
- ✓ ValidSoft warrants that it will ensure, by means of binding Terms and Conditions in its contracts with its Clients, that its Clients will use the (obfuscated) data sent to them by ET only for the purposes of detecting and preventing credit- or debit-card fraud against them or their customers, and in a manner that fully complies with all relevant European data protection rules.

The Terms and Conditions referred to are, of course, the terms and conditions in the ValidSoft – Client contract, mentioned above.

Crucially, ET can give the warranty in the second bullet-point precisely because of the warranty that is given by ValidSoft about compliance with European data protection standards; and ValidSoft can give its warranty precisely because it has obtained the European Privacy Seal. In that sense, the obtaining of the seal thus squares an important legal circle.

An annex to the contract ensures that when the VALid-POS[®] “box” is hosted with ET, ET acts as processor for the users of the TOE insofar as the processing within the “box” is concerned (as discussed in section 1.2, above), and that its actions in this respect, as processor, are subject to all relevant European requirements, as listed in Article 17 of Directive 95/46/EC.

It should also be noted that the above clauses in the ValidSoft – ET contract (and the annex) are expressly given third-party effect for the benefit of the clients using the TOE. These clauses and this annex are therefore also made available, in the form provided to the EuroPriSe Certification Authority, on request and subject to a binding non-disclosure agreement, to such clients and potential clients.

The Undertaking provided by ValidSoft to the EuroPriSe Certification Authority, mentioned earlier, also confirms that the above-mentioned clauses will be incorporated in full and in binding form in the contracts mentioned prior to any marketing, by ValidSoft, of the VALid-POS[®] product in association with the seal.

Having very carefully and fully analysed all these various legal clauses, the evaluation concluded that they provide the highest possible guarantees of compliance with the requirements discussed earlier in this report. The evaluation therefore rated these clauses as “excellent”.

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. The evaluation noted that in all these respects, ultimately it was the client alone who could ensure compliance (although non-compliance would constitute a breach of contract, with possibly serious consequences, as discussed in section 13.A.5, above).

- ✓ 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.

The technical evaluation focussed on two aspects of these matters:¹³

- the default settings for the product in these respects, and the recommendations provided as to retaining those; and
- the logging and authorisation requirements on these matters.

¹³ A third 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 detail in the evaluation, is the question of documentation. However, as noted in the previous footnote, in this Recertification 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 13.A.5, above.

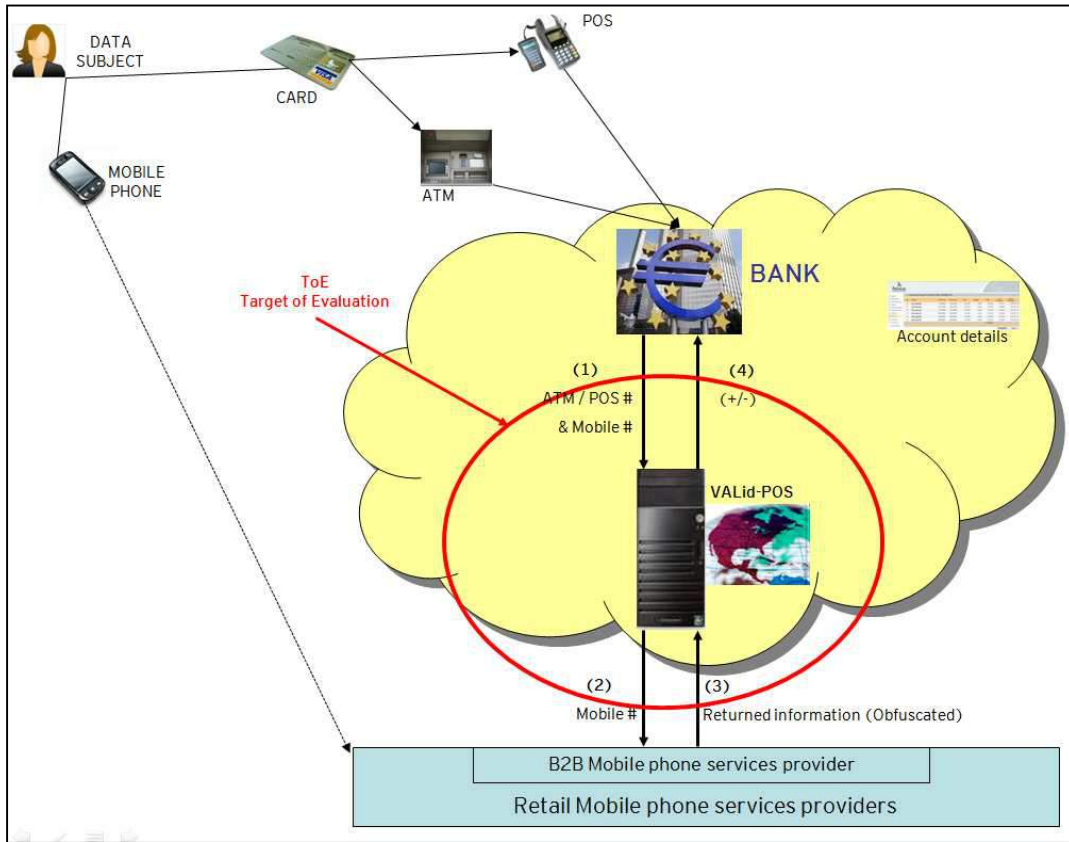
In respect of these two issues (default settings and logging and other recommendations), it will suffice to note that the evaluation concluded, first of all: that the default settings met the European requirements, and that the recommendations too, if followed, would ensure compliance with those requirements in the relevant respects. Specifically, as far as communication security and encryption are concerned, the “Core Model Product Guide” and the legal arrangements discussed at 13.A.5, above, stress (and require) that the client use “state of the art” technology in these respects, and updates this as technology develops.

Here, it may suffice to note the following main aspects:

- ✓ the password settings as delivered by default to the client ensure security and expiration;
- ✓ however, credential management may be integrated in another system such as Active Directory;
- ✓ users are not allowed to modify any kind of personal data held in the VALid-POS[®] database;
- ✓ the product does not allow remote access, and transport (data exchanged with TSP) is encrypted using standard SSL (128 bits or higher); and
- ✓ high level of pseudonymisation and anonymisation is ensured by obfuscating and shorting data.

Because, as already noted, it is ultimately the client alone who can ensure compliance (but, it should be stressed, only because of this), the evaluation rated the technical arrangements in all these respects as “adequate” rather than “excellent”.

14. Data flows:



Note:

There are only four data flows within the TOE, as indicated by the numbers (1) – (4) in the above chart:

- (1) The sending of an ATM or POS-terminal reference and a mobile phone number by the client to the VALid-POS[®] “box”;
- (2) The passing on of the mobile phone number from the “box” to the partner-TSP, ET;
- (3) The passing on of obfuscated data on the whereabouts of the phone from ET to the “box”; and
- (4) The passing on of the “result” of the data analysis within the “box” from the “box” to the client.

15. Privacy-enhancing functionalities:

The product deals with an issue that is of great concern to financial institutions, and also important to ordinary people with credit- or debitcards: the widespread use of fraudulent cards. Specifically, it can make the fraud-prevention measures of such institutions much more effective: see “Background” in section 7.1 of this short report. In this, the product shows two features that make it particularly commendable:

- ✓ It reduces all processed personal data, and all internal and external disclosures of personal data to the absolute minimum, and obfuscates important data to the maximum extent possible; and
- ✓ It 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 (ET), to lawfully assist the product in achieving its important aim.

In particular, the product offers banks and payment processors an effective way to make their fraud prevention measures more reliable.

Moreover, in this, the users of the product (the banks and payment processors) can be assured of the lawfulness of the support from the partner-TSP (ET); and ET is assured that the users of the product will comply with European data protection law in the processing which is assisted by the product.

Overall, the TOE will make the anti-fraud measures of financial institutions therefore 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 a 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 (ET) are adequately dealt with in the contract between ValidSoft Ltd and ET. See section 13.A.5, above.

17. Compensation of weaknesses:

[unchanged from 2012]

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:

EuroPriSe Requirement		Decision	Remarks
<i>High-level requirement:</i>			
DATA AVOIDANCE AND MINIMISATION		excellent	The evaluation concluded that all personal data, and in particular all internal and external data disclosures made in the course of using the product, are kept to the absolute minimum, and are anonymised to the furthest extent possible; and that the partner-TSP does not disclose any actual traffic- or location data
	<i>More specifically:</i>		
→	internal data disclosures	excellent	
→	external data disclosures	excellent	
<i>High-level requirement:</i>			
TRANSPARENCY		mainly excellent	The arrangements <i>viz-à-viz</i> the clients/users are “excellent”; and those concerning the informing of data subjects are rated “adequate” only because this can only be assured by the client/user of the TOE.
	<i>More specifically:</i>		
→	Informing of client/user of the TOE	excellent	The <u>Core Model Product Guide</u> for the product gives extensive, clear information to the user of the TOE
→	Informing of data subjects	adequate	The <u>Conditions of Use</u> provide important binding guidance for users of the product on how to inform the data subjects/cardholders.
<i>High-level requirement:</i>			
TECHNICAL-ORGANISATIONAL MEASURES		mainly adequate, some excellent	The evaluation concluded that the default settings for the TOE met all the European requirements. As far as communication security and encryption are concerned, the “Core Model Product Guide” and the legal arrangements require the client to use “state of the art” technology, and to update this as technology develops. It is only because it is ultimately the client alone who can ensure compliance that the evaluation rated the technical arrangements as “adequate” rather than “excellent”.

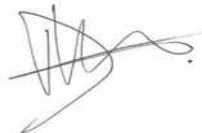
continues overleaf

continued:

	<i>More specifically:</i>		
→	Encryption	excellent	The evaluation concluded that the TOE as delivered ensures a very high and secure level of encryption, and that the legal arrangements ensure that the technical specifications will remain at the latest, state-of-the-art level.
→	Pseudonymisation and anonymisation	excellent	The evaluation concluded that the data processed within the TOE have been pseudonymised or anonymised, to the maximum extent possible for the TOE's purpose.
<i>High-level requirement:</i>			
DATA SUBJECTS' RIGHTS		adequate	The scope and effective exercise of data subject rights are determined by the national law applicable to the client in his capacity as controller. The most that the developer of the TOE 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. This is clearly done in the legal arrangements.

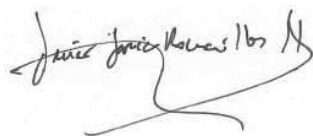
Experts' Statement

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



Prof. Douwe Korff (legal Expert)

Cambridge, UK, 02 February 2017



Javier Garcia-Romanillos Henriquez de Luna (Technical Expert)

Madrid, Spain, 02 February 2017

Re-certification Result

The above-named IT product passed the EuroPriSe evaluation.

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

Place, Date

Name of Certification Authority

Signature