Short Public Report

Recertification No.: 20110310 Valid-4F®

1. Name and version of the IT product:*

Name of Product	:	Valid-4F® Self-Certification (Standard Edition)
Product Description	:	A product that enables individuals to quickly and simply certify, by and for themselves, over a mobile phone, to either private- or public sector entities, that they are who they claim to be, and that they are fulfilling certain conditions, including conditions relating to their (rough) whereabouts. This is referred to in this report as "**self-certification**". *This is the sole purpose of the Valid-4F® product.*
Version	:	Version 1.0 (2011, unchanged)

*Notes:

1) This product was originally evaluated under the name "Valid-V3".
2) 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:

ValidSoft (UK) Ltd
9 Devonshire Square
London EC2M 4YF
United Kingdom

Contact Persons and Contact Details:

Mr. Pat Carroll, CEO, Validsoft UK Ltd
Alexander Korff, Esq., Legal Counsel for ValidSoft UK Ltd
Address as above.
E: Pat.Carroll@validsoft.com, alexander.korff@elephanttalk.com

3. Time frame of the re-evaluation:

April – August 2014

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:

Ernst & Young (Spain)
Plaza Pablo Ruiz Picasso 1, Torre Picasso, 28020, 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 2011]

The TOE is a tool that enables individuals to quickly and simply certify, by and for themselves, over a mobile phone, to either private- or public sector entities, that they are who they claim to be, and that they are fulfilling certain conditions, including conditions relating to their (rough) whereabouts. This is referred to in this report as "self-certification". (See further at 7, below, including section 7.3 on what is, and what is not included in the TOE).

7. General description of the IT product:*

[unchanged from 2011]

7.1 Background:

In an increasingly mobile and global world, it is becoming more and more important, in many different contexts, that individuals can quickly and simply certify, by and for themselves, over a mobile phone, who they are, and that they are fulfilling certain conditions, including conditions as to whether they are, or not, in a particular country or jurisdiction. It is of course also crucial, in such circumstances, that the relevant self-certification is reliable and verifiable. The TOE makes such verifiable self-certification possible in a great many different contexts. The following is a typical example from actual practice:

* ***See the Glossary, attached at the end, for clarification of technical terms etc.***

Example:

In one EU Member State, the Government Department responsible for unemployment benefit payments allows claimants of such payments to self-certify, by mobile phone, that they still fulfil the conditions for the receipt of these payments.

To this end, they are contacted by mobile phone and must answer certain questions; the calling system verifies both the authenticity of the voice of the person answering the call (compared to a pre-recorded voice biometric) and the "liveliness" of the voice, and whether the phone, and thus the speaker, are in the country (this being a condition for the receipt of such benefits).

If the self-certification is successful, the claimant in question does not need to present him- or herself in person at the Department's offices - thus both saving the Department considerable administrative and personnel costs, and the claimant time and possible embarrassment.

7.2 Further details of the TOE: [See the illustration on p. 4 and the Chart on p. 5]

The TOE can check a number of factors in this respect, according to pre-specified settings, determined by the user entity in question: the tool is **highly versatile** in these respects, as further explained below (but at the same time, the tool is still always subject to restrictions that are crucial to ensure data protection compliance).

It is of course also crucial, in such circumstances, that the relevant self-certification is **reliable and verifiable**.

Finally, in order to respect the privacy and personal autonomy of the person concerned, it is felt by the developer to be crucial that it is guaranteed that the tool is only used in respect of individuals who have **voluntarily agreed** to this form of self-certification, after having been fully and clearly informed of the product and the details of the data processing involved, without any undue pressure.

(Hence the moniker "***v****oluntary*, ***v****ersatile*, ***v****erifiable* self-certification product", or "V3" for the pilot version.)

In spite of its versatility in terms of settings, the product is used in essentially one manner, in that the entity that has installed the product calls the person concerned, to check certain matters that must be self-certified by the person concerned in the call.

This basic tests and this scenario are broadly depicted on the following pages.

ILLUSTRATION:

The ValidSoft UK Ltd
Voluntary Versatile Verifiable Four-Factor (4F)
Self-Certification product

THE VERIFIED PERSON:
(AND HIS MOBILE PHONE)

THE VERIFIED FACTORS:

Factor no. 1:
Something you know

[something basic, like a PIN, or your date of birth, or the name of your dog]

Factor no. 2:
Something you are

[something that is unique to you, specifically your voice-biometric]

Factor no. 3:
Something you have

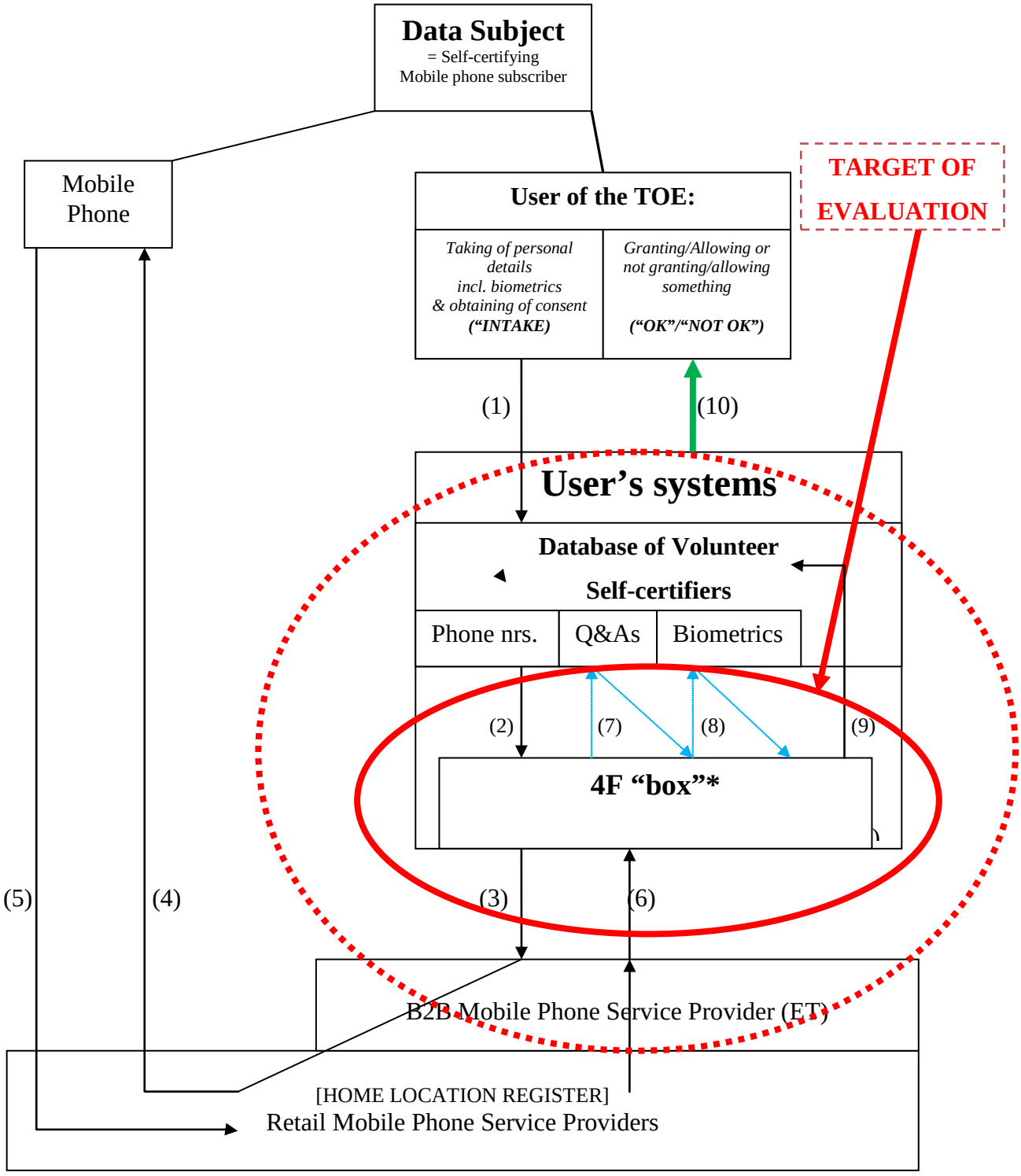
[i.e., your mobile phone SIM card]

Factor no. 4:
Somewhere you are

[i.e., whether you and your mobile phone/SIM card are, or are not, in a given country or jurisdiction]

"LIVELINESS TEST"

CHART: **The TOE in context**
(NB: SEE LEGENDA ON P. 7)



*NOTE: It is important to stress that this "box", in reality, consists of no more than a number of software programs run from a dedicated carrier installed at the offices of the user: the "box" is not a real physical thing, but rather entirely virtual, which is why in this report it is always referred to in quotation marks.

LEGENDA FOR CHART ON P. 6:

- The **red circle in bold** indicates the scope of the TOE: it includes all the processing within the 4F "box", and the data flows into and out of the "box", including: *****

- The **blue arrows** which indicate the making of the various checks described on p. 5, above, and further discussed in the text on the following pages.

- The dotted red circle indicates the core context of the TOE, and includes certain matters which, while formally outside the TOE, are nevertheless discussed in this Evaluation Report, because they are too important to the use of the TOE to be ignored. *****

* *For a detailed discussion of what is, and what is not, within the scope of the TOE see section 7.3, below.*

- The **green arrow** indicates what happens after the checks have been made.

- The database referred to in the chart as the "Database of Volunteer Self-Certifiers" will be given different names by different users of the TOE. A social welfare department may, for instance, call it its Claimants Database; a Stock Exchange its Traders Database; etc.

- The letters "Q&As" stand for "Questions & Answers": these are the questions and answers recorded from the data subjects at the Intake, as discussed above.

- The word "biometrics" in the chart indicates the two types of software used, i.e. both the "biometric sample test engine" (or more simply the "biometric engine") and the "speech recognition engine".

What is being checked

As illustrated in the picture on p. 5, ValidSoft's *Four-Factor ("4F") Self-Certification Product* (hereafter also often referred to briefly as "4F" or "the product") allows the user of the product to verify self-certification by individuals, with reference to four factors and a supplementary enhanced "liveliness" check:

- The product checks **Something that the person knows**: this can be a PIN, or the person's date of birth (DOB), or a pre-agreed fact, such as the name of the person's dog. The verification in this respect is done by the product asking the person the relevant question, e.g., "*please speak the agreed four numbers into the phone*", or "*what is your date of birth (date, month, year)?*", or "*what is the name of your dog?*".
- The product checks **Something that is unique to the person**: although in theory, this could be any unique biometric (such as a fingerprint or iris scan), for the TOE in practice only a voice biometric will be used. The person concerned provides a sample of his or her voice upon enrolment; this sample is used to create a derivate ("voice-print" or "signature"), and the voice answering the phone is checked against this derivative/voice-print/signature (with the actual recording being destroyed, and with safeguards against attempts to "fool" the system (ToE), as described in detail later: see also the last bullet-point, about "liveliness").
- The product checks **Something that the person has**: i.e., the person's mobile phone, or to be more precise, the SIM card containing the phone number which the person has registered with the user of the product. This is done by simply matching the number of the phone used to make the certification call against the number which the person registered upon enrolment (but again with built-in safeguards).
- The product checks **Something about where the person is**: this is always done in very broad terms only, i.e., in respect of whether a person is, or is not, in a particular country (as in the Example on p. 3), or in a particular jurisdiction covering several countries (e.g., the BeNeLux).
- Finally, the product enhances the above checks, and in particular the biometric voice test, by verifying that the person concerned is actually providing the answers him- or herself, from the place where the phone (or rather, the SIM-card) is at the time, and is not using evasion methods such as call forwarding or pre-recorded spoken text. This is referred to as the "**liveliness check**".

The basic scenario in which the TOE is used

The basic typical scenario for the use of the product is on the lines of the one provided in the Example on p. 3, above, self-certification by an unemployment benefit claimant.

For the self-certification in that case, and in all cases covered by this EuroPriSe evaluation, the self-certification is initiated by the user of the product (i.e., in that example, the Government Department responsible for paying unemployment benefit).

However, the TOE can be used for many other types of self-certification: the TOE can be tuned to meet the requirements of each specific context; its versatility is one of its main hallmarks.

However, the basic set-up for all cases can be described in broad terms and charts on the above basis.

Basically, whenever the TOE is used there are three elements to the product:

- a computer system that makes and handles calls to the mobile phones of individuals who have signed up to the arrangement, and that records an exchange of automated pre-recorded questions and the actual answers given to those questions;
- use of a dynamic voice-biometric identification system;
- a check on whether the individual's responses are "live"; and
- a system to ascertain, with the help of a Telecommunications Services Provider (TSP), the rough whereabouts (in country/jurisdiction, or not) of the phone of the person concerned, that has been registered with the user of the TOE.

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

The scope of the TOE is indicated in the Chart on p. 5 by a solid red oval, and the TOE as such is limited to the product as provided by the developer (the applicant for the seal), as thus circumscribed.

However, as also already mentioned, there are aspects of the use of the product, including in particular the *Intake* process, the "*Lookup*" of the phone by the partner-TSP, the *Biometric Verification* and the *Overall Results* to which the use of the product may lead, that are too important to leave out of this report, even though as such they fall outside of the scope of the TOE. What is more, the developer of the product has included many important measures and binding requirements in these respects in its standard Terms and Conditions for the use of the product, which are a mandatory part of any contract with a user, and has also included important clauses relating to these matters in its contract with the partner-TSP. These conditions and clauses are discussed in detail in section 13.A.5 below. In the Chart on p. 5, these still-also-considered measures are indicated by means of a wider dotted red oval.

8. Transnational issues: [unchanged from 2011]

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, data are sent from the systems of the partner-TSP in the Netherlands to the user/client's systems outside the EU/EEA: see section 13.A.1, below.

As concerns the question of "applicable law", we concluded 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)

9. Tools used by the manufacturer of the IT product: [unchanged from 2011]

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 databases are also hosted on the client's own environment, 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, which is installed on a client's own system; 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 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 November 2011

11. Modifications / Amendments of the IT product since the last (re)-certification: [unchanged from 2011]

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:

Since the last re-evaluation in 2011, there have been no changes in the law (the EC data protection directives) or in the interpretation of or guidance on the law (in particular, in guidance issued by the Article 29 Working Party or the EDPS) that in any way affect our legal evaluations in that last re-evaluation report.

There have also been no changes in technical standards, and in that respect our evaluations of 2011 also still stand.

The only matter that needed specific assessment was therefore whether the technical specifications of the TOE were still "state of the art", and more in particular whether our assessment of the "non-matchability" of the voiceprints used in the TOE was still valid. We concluded that although there have been important developments in biometric technology since 2011, these do not affect this "non-matchability": see the update for this 2014 recertification in section 16, below.

13. Evaluation results: [largely unchanged from 2011; final para. added]

A. LEGAL EVALUATION

General Note:

In respect of several matters addressed in the evaluation, the most that the developer and vendor of the TOE can do, is alert the clients to their duties under European data protection law, and make it Conditions of Use of the product that the clients fulfil their obligations under their applicable law. As we shall see in section A.5, below, these Conditions of Use are detailed and strict: they were essential to the assessment that the TOE is compliant with European data protection law, and thus to the awarding of the seal.

Even so, in any context in which this is the case - i.e., in any context in which compliance with the European standards depends on the Client/User of the TOE acting in conformity with those Conditions of Use, the evaluators have only rated the product "*adequate*" on the EuroPriSe assessment scale, even if those Conditions themselves were as strict and detailed as they could be. The evaluators only awarded a score of "*excellent*" (score 1, the highest score) when the product itself ensured full compliance with the European standards.

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, **Self-Certification** - that is: the verifiable certification, by an individual, over a mobile phone, to either a private- or a public sector entity, that he or she is who he or she claims to be, and that he or she is fulfilling certain conditions set by that entity, including conditions as to his or her whereabouts.

Notes:

(1) The individual is referred to as the *person concerned* or the *data subject*; and the entity is referred to as the *client* [of the developer of the TOE, ValidSoft] or the *user* [of the TOE].

(2) The conditions in question will of course relate to something else: the something for which the conditions are conditions, e.g., a welfare benefit. The purpose of the overall processing for which the TOE is used will therefore be related to this something else. In the Example on p. 3, the controller/user of the TOE is a State welfare office, and the purpose of the general processing by that office is to assess eligibility of the data subjects for the relevant benefit. In that case, the TOE is therefore used to check if a data subject fulfils the conditions for that benefit, by means of self-certification. But the purpose of the TOE remains that self-certification only; the use of the result of the self-certification process by the user of the TOE for the wider purpose of deciding whether to pay (or continue to pay) the benefit, or not, is a separate matter, outside of the TOE.

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 entity that has installed the product, ValidSoft's client) is to be regarded as the "controller" of basically all the processing associated with, or carried out with the help of, the TOE: it is the user/client who decides to use this product for its own purpose (see above on that purpose); 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 4F "box" (Data Flow (2) in the Chart on p. 5), the external disclosure of data to a third party, the partner-TSP (Data Flow (3)); the obtaining of data from that third party (Data Flow (6)) (* see Note, below); the internal processing within the 4F "box" and the data exchanges with the user's own systems (Data Flows (7) & (8)); and the internal disclosure of the "results" of that processing from the "box" to the product user's own systems (Data Flow (9)).

We should add that the user of the TOE is also undoubtedly the controller in respect of the original obtaining of relevant personal data in the "Intake" process, and of the entering of those data into its own systems (in Data Flow (1)) - although that process is as such outside of the TOE, except insofar as the Conditions of Use for the TOE specify certain matters that must be complied with in this connection, in particular as concerns the obtaining of the free, informed, expressed consent of the Volunteer Self-Certifiers to the use of the TOE, as discussed in section A.2, 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 A.5, below, those legal arrangements are rated "excellent".

*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), because that processing by the partner-TSP (ET) is outside the TOE. However, we should nevertheless note 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", and of the disclosure of these data to the "box". This has implications in various contexts, including the questions of "applicable law", as discussed above, at 8, and of the legal basis and legality of this processing, as discussed at A.2, below.

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 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 / Biometric data:

No "special categories of data" ("sensitive data"), as specifically defined in Article 8 of Directive 95/46/EC, are processed in the context of the use of the 4F product.

However, the TOE does involve the processing of audio-biometric data. *In fact, the evaluation and certification of the TOE in the end strongly focussed on the*

compatibility of the processing of this data with the European standards generally, and on the question of the "non-matchability" of the audio-biometric data in particular.

On the general issues, the evaluation concluded, with reference to the views of the Article 29 Working Party, set out in WP80 of 1 August 2003, that with regard to the vast majority of data subjects, none of the biometric data processed within the TOE (or indeed, by the user of the TOE outside of the TOE, in relation to the TOE) are "sensitive" in the formal sense under the Working Party's tests.

It was conceivable that in some cases, the original recording could reveal a medical condition, e.g., stuttering or a neurological disease. However, this recording is destroyed, and the voice derivative/voice-print/signature that is retained would not as such show this, or be analysed for this.

Even so, the evaluation noted that there are two *caveats* to the above. First of all, Recital 33 to the Directive refers more generally to "data which are capable by their nature of infringing fundamental freedoms or privacy". The Article 29 Working Party notes this in its important opinion on the concept of personal data, and remarks there that "general identifiers" which are linked to "biometric indicators" could be regarded as such, and as then falling within Article 8(7) (See Opinion No. 4/2007 on the concept of personal data, WP136 of 20 June 2007, under the heading "'Directly' or 'indirectly' identifiable", pp. 14 – 15). In the case of the TOE, the user of the TOE may well be using such an identifier, e.g., in the Example on p. 3, a welfare claimant's national security number.

Secondly, in its Working Document on Biometrics, the Working Party supports the use of biometric systems that do not memorise traces in a terminal access device nor store them in a central database (see point 3.2 of the Document). It then goes on to say that if it is planned that such systems (i.e., systems in which traces are memorised in a terminal access device, or are stored in a central database) are to be used, then:

> in the light of the risk of (re)use for different purposes as well as of the specific dangers in case of unauthorised access, the Working Party recommends that Member States should consider submitting them to prior checking by data protection authorities in accordance with Article 20 of Directive 95/46/EC, as this kind of processing is likely to present specific risks to the rights and freedoms of data subjects. (WP80, section 3.5, p. 8)

In view of the above, the evaluation assessed all of the processing of the biometric data within the TOE as if those data were sensitive data. This informed in particular the assessments of the issues of data avoidance and –minimisation (including the crucial issue of *the "[non-]matchability" of the biometric voice-prints*), consent, and the closely-related matter of the informing of data subjects, as is noted under these headings, below (respectively in this section, and in sections A.2 and A.3).

In other respects, too, the evaluation gaven special attention to the views of the Article 29 Working Party in its Working Document on Biometrics, e.g., in relation to fair collection and proportionality. The latter has particular implications in respect of the technical design of the TOE and of the user's own systems. Thus, the Working Party says:

> Where biometric data are intended to be used as a key to link databases containing personal data particularly difficult issues may arise whenever the data subject has no possibility to object to the processing of biometric data. This may commonly occur in relations between citizens and public authorities.
>
> In this perspective, it would be desirable that templates and their digital representations be processed with mathematical manipulations (encryption, algorithms or hash functions), using different parameters for every biometric product in use, to avoid the combination of personal data from several databases through the comparison of templates or digital representations.

In the technical assessment, the evaluation gave special attention to these issues insofar as they relate directly to, and fall within, the TOE.

In other respects - in particular, as concerns the databases maintained and controlled by the user of the TOE, including the biometric engines as such, the processing, and the databases, are outside of the TOE. ***However***, this issue was so important that the evaluation nevertheless examined and assessed the Conditions of Use for the TOE, which include important stipulations to ensure that the TOE will only be used as part of wider operations that comply with the requirements spelled out by the Article 29 Working party: see section A.5, below.

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 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 the controller of the processing under evaluation (the client/user of the TOE) does not at any stage process traffic- or location data of the kind defined by the e-Privacy Directive; and that thus no traffic- or location data are processed within the TOE as such – but: (i) that if one were to hold that some minimal traffic data are processed within the TOE, this is still fully lawful because it happens with full, free, informed and specific consent; and (ii) that that aside it is clear that ET does process traffic data in support of the use of the TOE, and that this still had to be looked at in the evaluation (as is done in section A.2, below).

Data Avoidance and Minimisation [Criteria Catalogue, sections 1.2.1, 2.2.2, and 2.2.3, and added section 1.2.1.*bis*]

The evaluation concluded that by and large all personal data, and in particular all internal and external data disclosures within the TOE are kept to the absolute minimum, and anonymised to the furthest extent possible.

However, there were two issues that were given special attention. The first was the possibility that some users of the TOE might record the self-certification calls made with the help of the TOE. This could happen in particular in countries (such as the United Kingdom) where the recording of telephone calls between consumers and companies is ubiquitous, and legal.

From a European data protection perspective, this raised the concent that this might lead to the creation of voice-recording (i.e., biometric) samples that could be "matched" against other recordings held by the same, or indeed some other controller. The TOE protects against this, in that it is a Condition of Use that these recordings are stored in such a way as to make this effectively impossible, and destroyed within a few days if no issues arise that warrant their further retention.

This second issue centres on the same question of "matchability", but in relation to the "voice-prints" created and used to allow the biometric check within the TOE itself: the issue was whether the "voice-prints" used in the biometric checks in the TOE could be used to "match" the data processed in the TOE with other data, held in other databases containing other audio-biometric data.. This issue was explored in great detail in the context of the 2011 evaluation, at the request of the *EuroPriSe* Certification Authority.

In the end, the EuroPriSe evaluators concluded that if the TOE is used in accordance with the Conditions of Use for the product (and in particular in accordance with a crucial clause in these conditions), the "voice-prints" used in the biometric checks in the TOE could not be "matched" with other biometric samples or "voice-prints" in other databases, whether held by the specific Client/User of the TOE or anyone else.

Indeed, given the great lengths to which the developer of the product, ValidSoft, has gone in this respect, the evaluation awarded the product the score "*excellent*" (score 1) in this regard.

This was undoubtedly the single most important issue for both the original 2011 evaluation and the present re-evaluation of the product, and the measures taken by the developer of the product in this respect were crucial to the awarding of the seal.

In the 2011, report, the experts therefore undertook to keep this issue in particular under review for further re-evaluations. As further explained in the update for this 2014 recertification in section 16, below, the experts concluded that although there have been important technical developments in biometric technology since 2011, these do not affect the non-matchability of the voiceprints.

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.

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) and by the other Mobile Network Operators (MNOs), even though as such this processing is outside the TOE.

Processing on the Basis of Consent [Criteria Catalogue, section 2.1.1.1]

It is a fundamental Condition of Use for the TOE that it will only ever be used by the user of the TOE in relation to individuals who have completely voluntarily given their **free, informed and valid consent** to this.

More specifically, the Conditions of Use 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. This information (which the vendor of the TOE, ValidSoft, recommends that users provide in the form of a simple leaflet: see the "Client Recommendations" in the Core Model Product Guide) must stress that authorising the use of the TOE is entirely voluntary: it is a Condition of Use, and must be stressed in the information, that it is not a condition for the obtaining of whatever it is that the user offers or administers (e.g., in the Example on p. 3, for the obtaining of a welfare benefit) that the data subject agrees to the use of the TOE. More specifically, for private-sector users of the TOE who use the TOE in a contractual context, the Conditions of Use for the TOE stipulate that it shall not be a condition for the entering into or performance of the contract that the data subjects consent to the use of the TOE. For public-sector users, there is the additional condition 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 this. In all cases, the users must of course also always fully comply with any further conditions or formalities for the use of the TOE or parts of the TOE (such as for the processing of biometric data), e.g., that a "prior check" be carried out or requested before the TOE is used. Consent, even if fairly obtained and freely given and valid, does not override such requirements.

In addition, as far as the processing of biometric data (voice-prints, and where applicable, voice recordings) is concerned, the Conditions of Use specifically stress that the data subjects should be specifically informed of the risks inherent in any processing of such data, and expressly told that it is not a condition for the obtaining of whatever service or benefit the self-certification relates that the data subjects give their consent to this, or should feel they have to provide such samples.

The evaluation concluded that these strict legal arrangements concerning the use of the TOE ensure as far as can possible be ensured that the processing of all the data processed within (and indeed otherwise related to) the TOE - including the audio-biometric data - will always be on the basis of free, informed and valid consent; and that these legal arrangements also ensure full compliance with any other still-applicable national-legal requirements, conditions and formalities in this respect. ***The evaluation therefore rated the product* "processing fully permitted"** ***(score 1) on this point.***

This assessment was also crucial in the decision of the EuroPriSe Certification Body in respect of the legality of the processing of the voice-prints generally, as noted under the previous heading.

Processing of traffic- and location data [Criteria Catalogue, sections 2.1.4.2 & 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 traffic data. The same of course applies to the Mobile Network Operators (MNOs) from whom ET obtains the data.

In principle, it should suffice to recall that the evaluation found that all processing relating to the use of the TOE takes place on the basis of the free, specific and informed and valid consent of the data subjects: see the previous sub-section. This applies both to the processing by the user of the TOE per se and to the processing by ET in support of the use of the TOE, and indeed to any processing relating to the use of the TOE, by anyone: the data subject is clearly and fully informed of all of this processing, and consents freely to all of this processing. The processing of traffic data in support of the use of the TOE is therefore lawful under Article 6(3) of the e-Privacy Directive.

Note: The law in some Member States is phrased in terms that suggest that the consent must be obtained by the Mobile Network Operator (MNO). This is not in accordance with the e-Privacy Directive as interpreted by the Article 29 Working Party. However, the issue is still resolved in relation to the TOE, in that, first, the Conditions of Use for the TOE include a clause with third-party effect, which must be accepted by the User of the TOE, ensuring that the product will only be used with the full, free, informed and valid consent of the data subjects; and second, ValidSoft has provided the EuroPriSe Certification Authority with an assurance that the MNOs will be informed of this, in a way that effectively conveys the consent of the data subjects to those MNOs.

In view of the EuroPriSe evaluators, this arrangement more than meets the requirements of European data protection law, and adequately deals with the specific problem in these countries.

A.3 Selected other topics

Informing of Data Subjects [Criteria Catalogue, section 2.2.1]

As already noted in relation to the obtaining of consent, above, the Conditions of Use 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. The Conditions of Use also require special, detailed informing of the data subjects about the risks inherent in the processing of biometric data.

The vendor of the TOE, ValidSoft, recommends that users provide this information in the form of a simple leaflet, and even provides template information notices to this end (in the Core Model Product Guide to the TOE).

The evaluation concluded that the above clearly met all the requirements of Articles 10 and 11 of the main data protection directive (Directive 95/46/EC), as well as the special information requirements of Articles 6 and 9 of the e-Privacy Directive (Directive 2002/58/EC).

Disclosures of Data to Third Parties [Criteria Catalogue, section 2.2.3]

The evaluation concluded that the technical- and security arrangements and the Conditions of Use and the other legal arrangements for the TOE ensured that all the disclosures of data to third parties are kept to the absolute minimum, and are fully secured.

The TOE was therefore rated* "excellent" *(score 1) in this respect, too.

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 main EC

Data Protection 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 Data Flow (6), in which nothing more than a "YES/NO" result is sent by ET to the user of the product, indicating no more than that the data subject is, or is not, in a particular country.

Provided that the Conditions of Use in this respect are complied with (on the lines of the template information notices provided in the Core Model Product Guide), the data subjects are, moreover, fully informed of this, and consented to this freely and voluntarily.

These very limited transborder data flows therefore fully meet the requirements of the Directive.

Automated Individual Decisions [Criteria Catalogue, section 2.4.3]

All that the TOE does, is generating a "Result" in terms of "Positive", "Negative" or "Failed Call". What the consequences are of this information is effectively left up to the user of the TOE and thus in principle outside the TOE. In the Example on p. 3, for instance, it may mean that a State benefit agency either simply continues paying a benefit, or will call the person into its offices to see if he or she is still entitled to the relevant benefit.

However, it is a Condition of Use for the TOE that a user may not use such 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.

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.

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.

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

A.5 Documentation of the product: the legal arrangements[1] [Criteria Catalogue, section 3.1.8]

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

- ✓ The "Core Model Product Guide";
- ✓ The Conditions of Use of the 4F Self-Certification 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 UK Ltd, and the User of the product (and which forms an integral part of the Agreement); and
- ✓ The contract between the developer and vendor of the product, ValidSoft UK Ltd, and the partner-TSP, Elephant Talk (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 Users or Clients of the product, as third-party beneficiaries.

As already noted, these clauses ensure in particular, *inter alia*, that the Client/user of the TOE will obtain the fully free and informed specific consent of each data subjects for the making of the 4F self-certification calls and for the check on whether or not the data subject is, or is not, in the specified country or (multi-country) jurisdiction; and that the Client/user of the TOE accepts liability if ever a call were to be made, or such a check made, in a case where such consent was not obtained.

Moreover, as also already noted, the developer of the product, ValidSoft UK Ltd., undertakes to inform all relevant MNOs in all countries in which the consent of the data subject is required for the making of the call, and/or (perhaps more importantly) for the carrying out of this check - which includes all EU/EEA Member States - of the above-mentioned legal arrangements, and of the warranty issued by all users of the TOE to all MNOs in such countries; and in this, ValidSoft UK Ltd. will specifically point out also the fact that the warranty has three-party effect and can thus be relied upon by any relevant MNO. ValidSoft UK Ltd. has affirmed this in a special, written undertaking to the EuroPriSe Certification Body.

The evaluation concluded that the contractual stipulations in these different contracts, taken together and with this Undertaking, provide extremely strong guarantees of compliance with the relevant European data protection standards.

The evaluators therefore awarded the TOE the rating "excellent" (score 1) in this regard.

1 In the Commentary, 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. 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 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 three aspects of these matters:

- network and transport security;
- 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.

In respect of these three issues (transport security, 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 end to end encryption, not only local but with other databases.

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: [unchanged from 2011]

See the Chart on page 5, above, for a depiction of the TOE and the data flows involved.

As that Chart shows, the use of the TOE generates the following data flows (NB: these have already been noted in section 7.3, with a discussion of what, in respect of each of them, is or is not included in the TOE):

(a) Processing that takes place before any data are sent to the 4F "box":

[The "Intake" and Data Flow (1) in the Chart]

(b) The making of a call

[Data Flows (2) – (6) in the Chart]

(c) The carrying out of the various checks by means of the 4F "box;

[Data Flows (7) and (8) in the Chart]

(d) The sending out of the "results" from the 4F "box"

[Data Flow (9) in the Chart]

(e) Processing after the sending out of the "results" from the 4F "box"

[Data Flow (10) in the Chart]

15. Privacy-enhancing functionalities: [unchanged from 2011, except for the cross-reference under the indents]

How does the IT product or IT-based service enhance privacy?

In an increasingly mobile and global world, it is becoming more and more important, in many different contexts, including the provision of social welfare benefits, that individuals can quickly and simply certify, by and for themselves, over a mobile phone, who they are, and that they are fulfilling certain conditions, including conditions as to whether they are, or not, in a particular country or jurisdiction. It is of course also crucial, in such circumstances, that the relevant self-certification is reliable and verifiable. The TOE makes such verifiable self-certification possible in a great many different contexts.

Crucially, the product achieves this without privacy-intrusive processing, in a way that is fully compliant with European data protection standards. The following features in particular were rated as "excellent" in our evaluation:

– **Purpose-specification and –limitation**, with the latter being achieved in particular also through very strong, legally-binding Conditions of Use for the TOE;

– The very strong legal assurances that the product will only ever be used with the **full, free, informed, specific and express consent** of the data subject, verifiably given or recorded in writing (or equivalent format) by the controller/user of the TOE, and ***conveyed to the MNOs*** concerned in an equally verifiable manner; and that it shall ***never be a condition*** for the provision of the service or benefit offered or administered by the controller/user of the TOE that the data subject gives such consent;

– **Data avoidance and –minimisation** and **proportionality**, also in terms of ***internal data disclosures*** and ***disclosures of data to third parties***; in terms of ***pseudonymisation and anonymisation*** of personal data wherever possible; and in particular in terms of the ***non-matchability of the "voice-prints"*** used in the biometric checks;* and

– **Product documentation**, including in particular the already-mentioned strong, legally binding ***Conditions Of Use***, and the equally strong ***contractual arrangements*** between the developed of the product, ValidSoft, and the partner-TSP, ET; ***clear guidance*** to users on many issues in the Core Model Product Guide, with ***template information notices*** on the core issues and a strong recommendation on the provision of further information in a ***leaflet*** explaining the use of the product in clear terms to the data subjects.

* On the continued non-matchability of the voice-prints, see the update for this 2014 recertification in section 16, below.

The product offers users an effective way of offering their customers the possibility of mobile self-certification, including verification of whether they are in a specified country, and biometric verification. In this, the users and their customers can be sure that the mobile phone lookups and biometric checks involved are fully compliant with European data protection law (in contrast to lookup services of dubious legality such as operate widely on the Internet, often from outside the EU/EEA).

The users of the product can moreover be assured of the lawfulness of the support from the partner-TSP, ET in the Netherlands; the retail-MNOs concerned are assured that self-certification calls are indeed only made in respect of individual subscribers to their services who have given their free, informed, express consent to this; and the partner-TSP and these MNOs are assured that the users of the product will comply with European data protection law in the processing which is assisted by the product and the partner-TSP.

Overall, this will make the service- or benefit conditions verifications of the users of the TOE therefore both more effective and more data protection-compliant. In that sense, the product shows that privacy protection and service- or benefit condition verification (as used in particular also to prevent social welfare fraud) are not a sub-zero game: one does not have to be less effective in fighting welfare fraud (etc.) by having to comply with data protection rules. On the contrary, here we have a product that achieves both better protection against welfare fraud, and stronger condition-verification generally, 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:

[unchanged from 2011, except for the update added at the end]

The evaluation did not rate 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 our opinion, all fully covered by the Conditions of Use of the product. We also feel that the matters relating to the partner-TSP are adequately dealt with in the contract between the developer, ValidSoft UK Ltd, and that TSP, ET in the Netherlands.

The one matter worth mentioning here is the need for the developer to keep abreast of technical developments, in particular in relation to biometric verifications, e.g., as concerns future possibilities to store more of the data used in such verifications on the mobile device held by the data subjects. The developer of the product has assured us (and the Certification Authority) that it will indeed remain committed to state-of-the-art technology incorporating the latest and most privacy-friendly and privacy-enhancing techniques and software.

Update for this 2014 recertification:

There have been important technological developments in the area of biometrics, including voice-biometrics, since our latest re-evaluation report in 2011. In particular, the algorithms used have been greatly improved, resulting in significantly higher levels of correct matching of actual voices (as obtained, e.g., over mobile phones) with the relevant voice-prints used in voice-biometric authentication systems. Voice-biometric systems have become more reliable and accurate.

However, this does not affect the issue of the non-matchability of the voiceprints used in the Valid-4F voicebiometric system. It is still the case that the voiceprints for any one deployment of the product can only be used for that deployment; they cannot be matched against any other voiceprints, of either different vendors or of other users of the Valid-4F product (say, a different bank, or a different social welfare agency). As also explained in 2011, the voiceprints created for each deployment can also not be used to re-engineer the original voice recordings, and those original voice recordings are destroyed very quickly after the creation of the voice prints.

We therefore conclude that our 2011 assessment of the non-matchability of the Valid-4F voiceprints is still correct: there have been no technical developments that have undermined this non-matchability.

17. Compensation of weaknesses: [unchanged from 2011]

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:

[unchanged from 2012 but less topics covered, as per new template]

EuroPriSe Requirement	Decision	Remarks
DATA AVOIDANCE AND MINIMISATION, *including the core issue of "non-matchability" of the voice-prints* (* see Note)	**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 The EuroPriSe evaluators also concluded that if the TOE is used in accordance with the Conditions of Use for the product (and in particular in accordance with a crucial clause in these conditions), the "voice-prints" used in the biometric checks in the TOE could not be "matched" with other biometric samples or "voice-prints" in other databases, whether held by the specific Client/User of the TOE or anyone else.
*Note: ***The issue of the "non-matchability" of the "voice-prints" was undoubtedly the single most important issue for the evaluation and certification of the product, and the measures taken by the developer of the product in this respect were crucial to the awarding of the seal.***		

continued overleaf

continued:

TRANSPARENCY	**excellent/ adequate**	The arrangements *vis-à-vis* the clients/ users of the TOE are rated "excellent", especially because of the very clear guidance in the CMPG. Those concerning the informing of data subjects are rated "adequate", but only because this can only be assured by the client/user of the TOE.
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".
More specifically:		
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.
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.

[signature sent by post]

Prof. Douwe Korff (legal Expert)

Cambridge, UK, 08 August 2014

[signature sent by post]

Javier Garcia-Romanillos Henriquez de Luna (Technical Expert)

Madrid, Spain, 08 August 2014

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

NB: A glossary clarifying technical terms used in this report is attached overleaf

GLOSSARY OF TECHNICAL TERMS USED IN THIS REPORT IN RELATION TO THE DESCRIPTION OF THE TARGET OF EVALUATION:

Self-certification	:	the verifiable certification, by an individual, over a mobile phone, to either a private- or a public sector entity, that he or she is who he or she claims to be, and that he or she is fulfilling certain conditions set by that entity, including conditions as to his or her whereabouts. The individual is referred to as the *person concerned* or the *data subject*; and the entity is referred to as the *client* [of the developer of the TOE, ValidSoft] or the *user* [of the TOE].
Person concerned (= the data subject)	:	the person who, by means of the TOE, can *self-certify* to the *user* of the product that he or she is who he or she claims to be, and that he or she fulfils certain conditions specified by the *user* (including conditions as to his or her whereabouts).
Client or user	:	the client of the developer of the TOE, i.e. the user of the TOE, this being the entity that allows the *person concerned* to *self-certify* to it that that person is who he or she claims to be, and that he or she fulfils certain conditions laid down by the client/user of the product; the client/user can be either a private- or a public-sector body.
TSP	:	Telecommunications Service Provider, or to use the full technical term in the e-Privacy Directive, a provider of "publicly available electronic communications services in [a] public communications network".
MNO	:	Mobile Network Operator: a *TSP* that provides mobile telephone services to individuals who subscribe to their service (subscribers).
Voice-print	:	An encrypted derivative of a biometric sample (here: of an audio-recording of the voice of a data subject who has voluntarily signed up to self-certification), as distinct from that actual recording (which is destroyed). Also referred to as a "[voice] signature". In order to remove any doubt in terms of terminology, we at times refer to this datum as "the derivative/voice-print/signature". NB: For a discussion of the "non-matchability" of the voice-prints, see the sub-section headed "*Data avoidance and – minimisation*" in section 13.A.1, below.