TABULA RASA

Trusted Biometrics under Spoofing Attacks

http://www.tabularasa-euproject.org/

Funded under the 7th FP (Seventh Framework Programme)
Theme ICT-2009.1.4
[Trustworthy Information and Communication Technologies]

D7.6: Ethical Monitoring Report (Final)

Due date: 30/09/2013
Submission date: 27/09/2013
Project start date: 01/11/2010
Duration: 42 months
WP Manager: Emilio Mordini
Revision: 1

Author(s): A.P. Rebera, E. Mordini (CSSC)

Project funded by the European Commission in the 7th Framework Programme (2008-2010)		
Dissemination Level		
PU	Public	Yes
RE	Restricted to a group specified by the consortium (includes Commission Services)	No
CO	Confidential, only for members of the consortium (includes Commission Services)	No

D7.6: Ethical Monitoring Report (Final)

Abstract:

This deliverable documents the ethical monitoring of the TABULA RASA project in the period from month 18 [April 2012] to month 35 [September 2013]. In it we:

- Briefly recapitulate the methodology and internal procedures employed to monitor ethical issues in the project.
- Describe the project demonstration events, regarding which CSSC requested clarification.
- Report the monthly monitoring of the project.

IMPORTANT NOTE

This version is submitted early in order that the reviewers have sufficient time to see it before the Review Meeting, scheduled for 9-10 October in Brussels. Sections 4.17 and 4.18 will be completed at a later date (but before submission to the EC).

Contents

1. Introduction

This deliverable reports on ethical monitoring activities in the Tabula Rasa project in the period from month 18 [April 2012] to month 35 [September 2013]. (The project's ethical monitoring activities in the period to month 18 are documented in D7.3.)

In the present document we:

- Briefly recapitulate the methodology and internal procedures employed to monitor ethical issues in the project (§2).
- Discuss the main ethical concerns raised by the project in this period (§3). This was the need to clarify the nature of proposed demonstration events.
- Report the monthly monitoring of the project (§4).

2. Recapitulation of Monitoring Methodology

This section summarizes the ethical monitoring methodology (which is described in full in D7.3).

1.) All ethical monitoring in the project is carried out by CSSC.

2.) Ethical monitoring comprises four main tasks:

a) Ethical monitoring of project deliverables
CSSC reviews every deliverable, including early drafts where possible (these document are available through the project's SVN repository).

b) Ethical monitoring of other project documents and communications
These include meeting minutes, Quarterly Reports, and emails.

c) Serving as an internal ethical advisory board
CSSC has developed an Ethical Incident Report Form (EIRF) through which partners can report any actual/potential ethical issues or pose any questions/ comments.

d) Annual internal review
This is a purely internal (CSSC) activity involving no partners outside WP7 (i.e. no other partners at all).

3. Specific Issues Arising

The only significant issue arising in this period was the demonstration events held at the 6th IAPR International Conference on Biometrics (ICB-2013), June 4-7, 2013, in Madrid, and the similar demonstration to be held in Brussels in October 2013. These are not "problems" exactly, but CSSC nonetheless took steps to ensure good practice. We requested clarification from each presenter on their handling of personal data (if any), and on the gaining of informed consent from participants/volunteers (if necessary). This request was formally made at a project technical meeting in Southampton, 4 March, 2013 (recorded in the minutes).

The details of each partners activities are here described. These descriptions (with very minor amendments) were provided by the partners themselves, to CSSC. Additional forms (consent forms, EULA) are included as annexes to this document.

3.1. Key Lemon

Demonstration in Madrid, June 2013
KeyLemon will integrate the countermeasures developed in Tabula Rasa into its desktop application, which allows a registered user to log into or unlock his Windows or Mac session using face recognition. We will demonstrate the effect of the countermeasures for 2D face against someone trying to spoof the identity of another user to enter his session.

To illustrate the effect of the countermeasures, we will proceed as follows:

1. The user first logs in manually using his password and creates his face model through a wizard.
2. Once the face model is created, the user locks his session and logs in again by presenting his face to the webcam to illustrate the face recognition system (with countermeasures activated).
3. Then, while disabling the countermeasures, the demonstrator is challenged by different spoofing attacks which should allow the hijacker to enter the session of the user.
4. Finally, we activate the countermeasures and reproduce again the same attacks as in the previous point. The hijacker should no longer be able to enter the session.

Concretely, this means we will prepare a PC (or Mac) and create a fake windows account for the demo. We will setup a password to access the windows account.

Then, we will ask a tester to create his face model and confirm the face model with the password of the session. The biometric model created is a binary file which contains some features representing the identity of a person. We cannot get the images (which have been used to create

the model) back. The biometric model is encrypted is stored locally in the user data folder. We save also one picture of the user to display it in the desktop application (so the user can see that this model corresponds to this lighting condition, as we allow the user to create several models). The windows account created for the demo will be deleted after the demo.

The demonstration will involve probably less than 50 participants (but this has not been fixed yet).

When installing the software our end-user must accept an EULA. If we launch a test for some users of our community, they will have to install the software and accept the EULA. For the tests at Brussels, we may (if required) prepare a paper in which we will engage to remove all data from the windows session once the demo is accomplished.[1]

Demonstration in Brussels, October 2013

KeyLemon will update its desktop application which allows a registered user to log into or unlock his Windows or Mac session using face recognition. We will demonstrate the effect of the countermeasures for 2D face against someone trying to spoof the identity of another user to enter his session. The demo will integrate two initial countermeasures provided by IDIAP: Motion based spoofing detection and eye-blink based spoofing detection.

To illustrate the effect of the countermeasures, we will process as follow:

1. The user first logs in manually using his password and creates his face model through a wizard. This is the enrollment step.
2. Once the face model is created, the user locks his session and logs in again by presenting his face to the webcam to illustrate the face recognition system (with countermeasures activated).
3. Then, while disabling the countermeasures, the demonstrator is challenged by different spoofing attacks which should allow the hijacker to enter the session of the user.
4. Finally, we activate the countermeasures and reproduce again the same attacks as in the previous point. The hijacker should no longer be able to enter the session.

The attacks could be one of the following (as described in D2.1 and D2.3)

1. photo displayed with small screen devices (e.g. iPhone)
2. printed photo taken with a HD digital camera
3. photo displayed with large screen devices (e.g. iPad)
4. video displayed with small screen devices
5. video displayed with large screen devices

We will bring a couple of laptops (windows and mac). To perform the attacks, some devices will be available (smartphone, digital camera, tablet). We may also take a printer to make some printed photos (corresponding to the person who will enroll during the demo).

[1] For this EULA see Annex 1.

For the tests at Brussels, we may (if required) prepare a paper in which we will engage to remove all data from the windows session once the demo is accomplished.[2]

3.2. IDIAP

For the spoofing challenge in ICB 2013, no personal data will be recorded from the participants. All captured data (image, speech or fingerprint) will be processed and the results will be displayed live, but they won't be saved.

Each partner will enrol around 4 persons from their team to be attacked. This enrolment data won't be made public and will be deleted after the challenge.

Only for fingerprint, is there a possibility to enrol participants so that they can forge spoofing attacks towards themselves. In that case, consent forms will be available. But this part is still under discussion and will be finalized by the end of this month.[3]

3.3. STARLAB

1. The demo aims to demonstrate both the potential vulnerability of our multimodal EEG-ECG system to a replay attack and the effectiveness of some of the developed countermeasures.

The enrolment of a user is not a quick process: it is needed to record 4 two-minutes-long takes of signal. So I propose that the users authenticated during the demo should be already enrolled on the system. That means that either I enrol myself in advance or some of the people from the consortium enrol at some time during the two days before the review.

The system will have a setting which will allow to select whether the liveness detection countermeasure is activated or not. So the demo will show what happens when the signal of an enrolled user is played back to the sensor electrodes when the liveness detector is both deactivated and activated. Hopefully the authentication will succeed and fail respectively.

The biometric software will be connected to our brain stimulation control software so only when the user is correctly authenticated the brain stimulation session will start (the authentication prior to a brain stimulation session is one of the use cases described on D2.1).

2. We will bring a couple of laptops, one with the biometric system and the brain stimulation

[2] For this EULA see Annex 1.
[3] For consent form see Annex 2.

software and another one which will perform the replay attack.

3. We will bring our Enobio sensor to record the signals, the device which will perform the replay attack and also a small pcb board that will help to connect the replay device to the Enobio sensor electrodes.

4. The fakes will be just binary files containing the electrophysiological signals of the genuine users. These files will be used by the laptop performing the replay attack.

5. An Internet connection is not needed.

6. No special set is needed for the demo, just a table for the laptops and a chair where the user can be seated and stay in front of the laptop performing the authentication.

7. The preparation of the demo might take 5 minutes. This include the placement of the electrodes, and check that the received signals are correct. Then the authentication process takes 2 minutes of recording. If we try to authenticate tree times (genuine, attack with no countermeasure and attack with countermeasure) then it would be around 6-8 minutes.[4]

3.4. MORPHO

Details of how the demonstration is organised, including:

a) whether you will collect (or already have)any personal data; if so, what kind…

- The proposal is to not collect data for longer than the demo. An enrol phase will be performed to register someone in the database.
- Then, an acquisition phase of real modality to demonstrate the recognition system.
- Then, an acquisition phase of the spoofing attack to show the vulnerability of the recognition system without countermeasure.
- Then, an acquisition phase of the spoofing attack with the countermeasure to show the countermeasure efficiency.
- At the end of the demo , the complete database should be deleted.

b) (roughly) how many subjects you will collect data from…

- My feeling is to enrol for the final demo only reviewers and demo people.

c) how the data will be stored, and when it will be erased…

[4] For consent form see Annex 6

- Store on HDD, and deleted at the end of the demo.[5]

3.5. EURECOM

Details of how the demonstration is organized, including:

a) what personal data you will take…

- While we will be providing the facility to enrol new identities in our system, normally we won't need to do this for demonstration purposes.
- If we do collect personal data, then it will be a few seconds of speech, together with a personally chosen identifier (which could be their name if they are unimaginative).

b) how many subjects you will collect data from…

- I would estimate very few, possible none. We don't expect interest in speaker verification to be the same as that for the other demos in Madrid, since the speaker verification community is rather unrepresented at ICB. We will only collect data from those people who wish to test the system on their own voice.

c) how the data will be stored, and when it will be erased…

- Data will be stored on a personal computer. As soon as it is collected, it will be treated with feature extraction and the original audio data will be discarded immediately. While the feature extraction routine is not totally irreversible, features lack for e.g., prosodic information, which would be necessary to synthesize new speech representative of the original speaker.
- We have already collected some data from consortium members during the meeting in Southampton and a connected visit to IDIAP. This data we *have* stored in raw form and a subset of it has been released to the community (consent forms were signed).[6]

3.6. UOULU & UNICA

The idea of fingerprint spoofing challenge demo is to explain spoofing and anti-spoofing in fingerprint biometric recognition. We have already enrolled three persons (from Tabula Rasa people) in the system and made their artificial fingers. So, we will use that for explaining the fingerprint spoofing and anti-spoofing.

Besides that, we also invited contestants to prepare their artificial/gummy fingers at home if they want to. Once onsite and after enrolment, the contestants can try to use their artificial/gummy

[5] For consent form see Annex 7
[6] For consent form see Annex 3.

fingers to spoof their real fingerprints. All the data will be stored in the HDD and will be erased after the demo (the same day).[7]

3.7. CASIA

Face Recognition with Anti-spoofing – ICB 2013 TABULA RASA Spoofing Challenge
Our system will run on a laptop and capture face images using a device with two cameras. One is Visual (VIS) and the other is Near Infrared (NIR) camera. Because the NIR camera should work under active lighting, the system needs two power sockets (one for the camera and one for the laptop).

The system has two main modules: face recognition and face anti-spoofing. The face recognition is based on VIS face images and the anti-spoofing is based on NIR face images. Compared to VIS, the NIR spectrum can counter the spoofing attacks more efficiently. The workflow of the system is as follows.

1. Enrolment: A subject sits in front of the system. Then, we capture a face image of the subject, and input his name (optional). The name and image are enrolled into the system, and the related data are stored in MySQL database.
2. Recognition: When a enrolled subject faces to the camera, the system will recognize him and show his name and the similarity score.
3. Attacking the System: When a printed photo of a enrolled subject is placed in front of the camera, the system will be fooled by the photo.
4. Anti-spoofing: Then we enable the anti-spoofing module of the system. And place the printed photo in front of the camera again. The system should reject the photo at this time.

Data privacy

1. In the period of demonstration, we collect the names (optional) and face images of participants on site.
2. Those participants who signed consent form will be enrolled into the system.
3. The names and face images are stored in MySQL database and a folder named “ForEnroll” in the laptop.
4. At the end of demonstration, all data in MySQL database and “ForEnroll” folder will be deleted.[8]

[7] For consent form see Annex 4.
[8] For consent form see Annex 5.

3.8. BIOMETRY

Setup description:

* 2 Android phones

- Smartphone, Samsung Galaxy Nexus

- Smartphone, Samsung Nexus S2

* Good Wifi connection

* Access to Authentiation Server and the SIP server

Step1:

Werner (from BIOMETRY) places a SIP call with his mobile phone, the adaptive trust level raises from 10% to 19%

Step2:

EURECOM places a phone call with Werner's phone and plays artificial or synthesized voice into the phones microphone and if success, the trust level raises.

Step3:

EURECOM protection is activated on our Authentication Server EURECOM places a phone call with Werner's phone and plays artificial voice into the phones microphone and the trust level does not raise.

In addition, BIOMETRY will prepare a film that can be shown as demo.

4. Journal of Ethical Monitoring

This section reports on the monitoring that has taken place in the period from month 18 [April 2012] to month 35 [September 2013].

4.1. Month 18 (April 2012)

Docs reviewed:

- D61 Skeleton – No comments.
- Minutes of Nice Technical Meeting in Feb – No comments.
- D3.3 – No comments.

4.2. Month 19 (May 2012)

Docs reviewed:

- Draft agenda for technical meeting in June in Finland. No comments.
- D61 Draft. No comments.

4.3. Month 20 (June 2012)

Docs reviewed:

- Minutes of technical meeting in June in Finland. No comments.
- Skeleton of D52. No comments.
- D23. No comments.
- D24. No comments.

4.4. Month 21 (July 2012)

Docs reviewed:

- D3.4 draft. No comments.
- D42 Skeleton. No comments.
- D53 skeleton. No comments

Other:

- Posted a question to list on age-related issues of spoofing (9/7/12)

4.5. Month 22 (August 2012)

Docs reviewed:

- Mini-project proposals. No issues, but will seek clarification from Coordinator on CSSC monitoring role for these.

4.6. Month 23 (September 2012)

Docs reviewed: *none*

Other:

- Emailed Sebastien to confirm CSSC role in monitoring the mini-projects

4.7. Month 24 (October 2012)

Docs reviewed: *none*

4.8. Month 25 (November 2012)

Docs reviewed:

- Minutes of Cagliari Technical/Review Meeting (See emails from SM, 12/11/12 [draft], 22/11/12 [final]

Other:

- Annual Internal Review Meeting for ethical monitoring (A.P. Rebera & E. Mordini). *No major issues to report.*

4.9. Month 26 (December 2012)

Docs reviewed: *none*

4.10. Month 27 (January 2013)

Undertook a review of the SVN to ensure everything reviewed.
Docs reviewed:

- D32 – no issues
- D33 – no issues
- D34 – no issues
- D41 – no issues
- D42 – no issues

- D53 – no issues
- D54 – no issues
- D61 – no issues

4.11. Month 28 (February 2013)

Docs reviewed: *none*

4.12. Month 29 (March 2013)

Docs reviewed:

- D4.3 (draft)
- D4.4 (draft)
- Minutes of Southampton meeting (requested note for Partners to provide info on DP for the demos be added).

4.13. Month 30 (April 2013)

Docs reviewed: *none*

4.14. Month 31 (May 2013)

Docs reviewed:

- D43 (no issues)
- D44 (no issues but incomplete)

4.15. Month 32 (June 2013)

Docs reviewed:

- D44 (no issues but incomplete)
- Meeting minutes (Madrid technical meeting) (no issues).

4.16. Month 33 (July 2013)

- D44 (no issues)

4.17. Month 34 (August 2013)

4.18. Month 35 (September 2013)

5. Annex 1 – Key Lemon EULA

A. KeyLemon End User License Agreement
B. Microsoft Visual C++ 2008 Runtime Libraries (x86, IA64 and X64), Service Pack 1

A. KEYLEMON END-USER SOFTWARE LICENSE AGREEMENT

KeyLemon S.A., Martigny, Switzerland
Version 1.2, March 2009

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("LICENSE") CAREFULLY BEFORE USING THE SOFTWARE., YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU ARE ACCESSING THE SOFTWARE ELECTRONICALLY, SIGNIFY YOUR AGREEMENT TO BE BOUND BY THE TERMS OF THIS LICENSE BY CLICKING THE "I ACCEPT THE AGREEMENT" BUTTON. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, DO NOT USE THE SOFTWARE AND CLICK "I DO NOT ACCEPT THE AGREEMENT".

These General Terms and Conditions (the "Terms") apply to all royalty-free contracts and/or purchase orders binding upon KeyLemon SA, a Swiss company with registered office at Rue Marconi 19, 1920 Martigny, Switzerland ("KeyLemon") and the client (the "Client") (the "Contract" and, together with the Terms, the "Agreement"), which shall prevail in case of inconsistency with these Terms and pursuant to which KeyLemon will provide the Client with a royalty-free software license (the "Software") and/or royalty-free services (the "Services")

1. Definitions

In this Agreement, the following terms shall have the following meanings:

1.1. "Affiliate" shall mean, with respect to any person or entity, any other person or entity directly or indirectly controlling, controlled by or under common control with, such person or entity. A company or other entity has "control" over another company or entity if it owns, directly or indirectly, at least 50% of the voting rights in the other company or entity or if it controls the composition of the board of directors of the other company or entity.

1.2. "Confidential Information" shall mean, for either party, (i) its business information, (ii) its Intellectual Property, (iii) trade secrets, proprietary or confidential information, documents, data, in original or copies, source codes, logos, images, business plans, database and statistics, software, reports, memorandum, know-how or technology, derivative works, excluding information which is either marked "Confidential" or regarding which the information's confidential character is apparent under the circumstances that (a) is shown to be previously known to the receiving party not as a result of a breach of a non disclosure undertaking, (b) is independently developed by the receiving party without any help or reference to the disclosing party's confidential information as evidence by written document, (c) is acquired by the receiving party from a third party which was not, to the receiving party's knowledge, under an obligation to the disclosing party not to disclose such information, or (d) which is or becomes publicly available through no breach by the receiving party.

1.3. "Intellectual Property" shall mean all of the following now or hereafter owned by a party or used in its business: (i) patents and patentable inventions; (ii) ideas, know-how, discoveries, improvements, derivative works and utility models; (iii) trade marks, including all business and trade names, domain names and internet keywords, logos and services marks; (iv) processes, computer programs, software and databases (including source code); (v) trade secrets and the right to limit the use or disclosure thereof; (vi) all components of copyright (including mask works, rights of reproduction, transcription, distribution, and publishing rights) and other exclusive rights of economic utilization of work; (vii) design rights and analogous rights (whether registered or unregistered); (viii) logos and rights in designs and inventions; (ix) business names and rights protecting goodwill or reputation; (x) database rights (including extraction and re-utilization rights) and rights in compilations; (xi) rights in domain names and web sites; (xii) any rights similar to any of the foregoing which come into existence (whether by introduction of a new right through legislation or by some other means); (xiii) applications for any of the foregoing; (xiv) rights and interests in any of the foregoing; and (xv) all rights or forms of protection of a similar nature to any of the foregoing or having equivalent effect anywhere in the world belonging to or used by a party.

1.4. In this Agreement, unless the context otherwise requires: (i) a reference to the masculine gender shall include the feminine and neuter and the singular number shall include the plural and vice versa and words importing persons shall include firms, companies, corporations, bodies corporate, associations, partnerships or permanent establishments; and (ii) a reference to a person shall include a reference to that person's legal personal representatives, successors and permitted assigns.

2. Legal scope and contract validity

2.1. The Agreement and/or the Terms apply to the exclusion of any of Client's general terms and conditions of

business.

2.2. Details regarding the scope of Software and/or Services, performance and technical specifications can be found in the proposal documentation.

2.3. Unless otherwise specified in any Contract, proposals are binding for KeyLemon for a period on one (1) month.

3. Subject matter and obligations of KeyLemon

3.1. KeyLemon grants the Client a non-exclusive, non-transferable, non-assignable, non-commercial license to use the Software for evaluation purpose only, subject to Client full compliance with the terms of this Agreement. The Software should not be used in a commercial operating environment.

4. Obligations of Client

4.1. Client's use of the Software and/or the Services is subject to the limitations set forth in the Contract and/or Client full compliance with the terms of this Agreement.

4.2. Client shall not, in particular: (a) remove, conceal or alter any copyright or other proprietary notice incorporated in the Software; (b) modify the Software and shall not permit the reverse engineering, disassembly, decompilation, translation of adaptation of the Software, except to the extent expressly authorized by applicable law notwithstanding this limitation; or (c) use, combine, duplicate, store, sell, license, distribute, transfer, publish or otherwise use or permit the use of all or any portion of the Software or any other data transmitted by KeyLemon, except to the extent necessary to perform the Agreement.

4.3. In case of breach of the obligations set forth in this section by Client, KeyLemon shall be entitled, without further notice and without prejudice to other remedies, to immediately terminate the license to the Software and/or reduce or suspend the provision of the Services.

5. Consideration

5.1. The Software and the Services, if any, are provided to Client on a royalty-free basis.

6. Intellectual Property

6.1. All Intellectual Property with respect to the Software, the Services and related materials shall remain the exclusive property of KeyLemon (or its licensors). All improvements and derivative works created by KeyLemon, Client or third party with respect to the Software and/or the Services shall remain the exclusive property of KeyLemon. Client has no right to use the Intellectual Property embodied in the Software and/or the Services for any purposes other than contemplated under the Agreement and may, in particular, not copy (in whole or in part), modify, distribute or display any of the Intellectual Property of KeyLemon.

6.2. To the extent that Client obtains any Intellectual Property right, title and interest in and to any and all improvements and derivative works of the Software, Client irrevocably assigns to KeyLemon all of its worldwide right, title and interest in and to any and all improvements and derivative works of the Software. Client agrees to perform all acts reasonably necessary to perfect the foregoing assignment and to enforce and defend the assigned Intellectual Property rights. If any or all of the foregoing subject matter is not assignable for any reason, then Client hereby grants to KeyLemon a worldwide, perpetual, unrestricted, royalty-free, fully paid up, exclusive license, including the right to grant sublicenses, under all such Intellectual Property rights to the non-assignable subject matter.

6.3. Subject to section 6.4 below, KeyLemon will defend or settle, under its sole direction and contingent on Client's total cooperation, any claim alleging that the use of the Software and/or the Services infringes any patent, trademark or copyright. In the event of such a claim, KeyLemon reserves the right, subject to providing equivalent services and licensed material, at its sole option, to either (i) modify or replace the affected parts so that the Software and/or the Services become non-infringing, (ii) or terminate the Agreement immediately if option (i) listed above is commercially impracticable, without any possible claim from Client against KeyLemon. This paragraph states the entire liability of KeyLemon for any Intellectual Property infringement involving use of the software and/or the Services.

6.4. Client shall indemnify and hold KeyLemon harmless for any award of costs and damages against KeyLemon to the extent that it is based on a third party claim regarding a damage allegedly suffered as a result or in connection with any use of the Software and/or the Services made in breach of any terms of this Agreement.

7. Confidentiality

7.1. Client shall keep strictly confidential all Confidential Information of KeyLemon of which it may become

aware, whether or not relating to or arising out of the Agreement and/or the use of the Software and/or the Services and shall use such Confidential Information solely for the purpose of fulfilling its obligations here under. Client shall use all reasonable and prudent efforts to protect and safeguard KeyLemon Confidential Information from misuse, loss, theft, publication or the like.

8. Representations, Warranties and Covenants

8.1. By KeyLemon

8.1.1. Client acknowledges that any and all of the Software and/or Services are provided to it "as is" and "as available" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, satisfactory quality, fitness for a particular purpose, reasonable care and skill, non-infringement, accuracy, reliability, completeness, or about results to be obtained from using the Software and/or the Services.

8.1.2. KeyLemon does not warrant that the use of the Software and/or the Services will be uninterrupted, error-free or that defects can be corrected.

8.2. By Client

8.2.1. Client represents, warrants and covenants that (a) it has full authority to enter into the Agreement and it will comply with all the terms, conditions and obligations of the Agreement; (b) it compiles with all applicable laws, statutes, ordinances and regulations regarding its use of the Software and/or the Services (including without limitation those governing antitrust, false advertising, tax and export control, unfair competition, privacy and data protection, including of its customers).

8.2.2. Client is responsible for paying all applicable fees and taxes incurred in connection with the use of the Software and/or the Services.

8.2.3. Client further covenants that it will not grant to any of its Affiliates the right to use any of the Software and/or the Services, unless Client (a) informs KeyLemon of such use in advance and KeyLemon consents to it in writing (such consent not to be unreasonably withheld), (b) shall cause such Affiliate(s) to fully comply with all the obligations, representations, warranties and covenants set forth in the Agreement, and (c) shall remain liable to KeyLemon in case of breach of the obligations, representations and warranties set forth in the Agreement by such Affiliate(s).

9. Indemnification

9.1. KeyLemon's obligations regarding Intellectual Property infringements are set out in section 6.3 above.

9.2. Client shall indemnify and hold KeyLemon harmless for any award of costs and damages brought against KeyLemon to the extent that it is (i) based on a claim regarding modification, translation, customisation or localisation of the Software and/or Services by Client or third parties, or (ii) a third party claim regarding a damage allegedly suffered as a result or in connection with the use of the Software and/or the Services in beach of this Agreement.

10. Limitation of liabilities

10.1. KeyLemon shall bear no liability for breach of this Agreement, except in case of fraud or gross negligence and KeyLemon shall not be responsible for the acts or omissions of its auxiliaries.

10.2. Any legal proceeding based on or in connection with the Agreement or these Terms must be instituted within 3 (three) months of the date the cause of action first occurred.

10.3. In no event shall either party be liable for any consequential, indirect, incidental, punitive, or special damages, including without limitation damages for loss of profits, revenue, business interruption, loss of data, loss of business information arising out of Client's use of the Software and/or the Services (even if has been advised of the possibility of such damages).

10.4. KeyLemon is not responsible for problems which result from the use of the Software and/or the Services in conjunction with software of third parties or with hardware which is incompatible with the operating system or the technical specifications provided by KeyLemon.

11. Term and Termination

11.1. The term of the Agreement is set forth in the Contract, unless earlier terminated as provided for hereafter (the "Term").

11.2. The Agreement may be terminated, effective immediately upon written notice: (a) by the mutual written consent of both parties; (b) by either party, upon thirty (30) days written notice if the other party breaches any material term of the Agreement and fails to cure such breach in such 30-day period; (c) by KeyLemon if a proceeding is commenced by or against Client for relief under bankruptcy or similar laws and such proceeding is not dismissed within 60 (sixty) days or Client is adjudged bankrupt or insolvent.

11.3. Except if specifically provided for otherwise, termination of the Agreement for any reason shall

immediately terminate any Client's rights under the Agreement (in particular but not limited to any license granted), and Client shall return to KeyLemon all Software and Confidential Information, if any, unless KeyLemon notify Client that this latter must destroy such Confidential Information an send a written confirmation to KeyLemon after destruction.

12. Research and development activities

12.1. Nothing in this Agreement shall be construed to restrict KeyLemon's rights to freely (i) conduct research activities with regard to the Software (ii) develop commercial relationships with third parties in connection with its research activities, including selling the Software as a so-called "open source" of "free" software and (iii) develop, distribute or otherwise disposing of products similar to or competitive with the Software.

13. Third party warranty disclaimer

13.1. Each supplier and licensor to KeyLemon of any portion of the Software ("Third Party Supplier") disclaims all warranties express, implied, or otherwise including, without limitation, any warranty of merchantability or fitness for a particular purpose. In no event shall any Third Party Supplier be liable for any direct, indirect, consequential, incidental or other damages arising out of this Agreement or the use, license or delivery of any Software.

14. Attribution

14.1. Client agrees and warrants that it shall include an attribution notice on all of its sales support documentation that the Software was developed and provided to Client under a license by KeyLemon S.A. Martigny Switzerland.

15. Miscellaneous

15.1. No joint venture. The Agreement does not establish the relationship of a partnership, joint venture, franchise, or principal and agent among the parties, and neither party shall have any authority to incur obligations or take other actions on behalf of the other party to the Agreement.

15.2. Severability and waiver. If any of the terms, provisions, or conditions of this Agreement or the application thereof to any circumstances shall be ruled invalid or unenforceable, the validity or enforceability of the remainder of this Agreement shall not be affected thereby, and each of the other terms, provisions, and conditions of this Agreement shall be valid and enforceable to the fullest extent permitted by law. A waiver or consent regarding any term, provision, or condition of this Agreement given by KeyLemon on any one occasion shall be effective only in that instance and shall not be construed as a bar or waiver of any right on any other occasion.

15.3. Notices. Notices and other communications required to be given hereunder shall be effective when sent by either party by registered or certified mail to the other party at the address set forth on the Contract or to such other address as one party may from time-to-time designate by written notice to the other in the manner provided in this section.

15.4. Impossibility of performance. Neither of the parties hereto shall be liable in damages for any delay or default which is caused by conditions beyond its control, including but not limited to Acts of God, terrorism, war, civil unrest, sabotage, including attack by unknown forms of computer viruses, fire, natural disaster, act of government, strikes or labour disputes, inability of third parties to provide raw materials, power or supplies, or any other act or condition totally beyond the reasonable control of the party in question.

15.5. Entire Agreement and amendments. The Agreement constitutes the entire agreement between the parties regarding the subject matter, superseding all previous communications, representations or agreements, either by written or oral, with respect to the subject matter of the Agreement, except for confidentiality or non-disclosure undertakings, between the parties with respect hereto. No amendment or modification of the Agreement shall be made except by a written document signed by the parties to be bound thereby or the successor or assign of such party. The terms and conditions of this Agreement shall apply notwithstanding any additional or different terms and conditions of any ordering document or other instrument submitted by Client in connection with the delivery of the Software and/or the Services, which terms and conditions shall be void and of no effect.

15.6. Survival. The provisions of sections 5, 6, 7, 8.2, 9.2, 10 to 15 of the Terms shall survive the termination of the Agreement.

15.7. Successors and assigns. Client may not transfer, assign, sub-contract or sublicense, directly or indirectly, any of its rights or obligations under this Agreement without the prior written consent of KeyLemon. KeyLemon may freely transfer or assign its rights or obligations under this Agreement without the prior written consent of Client. Subject to the foregoing, this Agreement will be binding upon and inure to the benefit of the parties hereto, their successors and assigns.

15.8. Governing Law and Jurisdiction

15.8.1. This Agreement shall be governed and interpreted in accordance with the laws of Switzerland, without regard to principles of conflict of laws and without regard to the UN Convention on the International Sale of Goods (CISG).

15.8.2. Any dispute, controversy or claim arising out of or in connection with this Agreement, shall be submitted to the ordinary courts of the seat of KeyLemon.

B. MICROSOFT VISUAL C++ 2008 RUNTIME LIBRARIES (X86, IA64 ET X64), SERVICE PACK 1

Les présents termes ont valeur de contrat entre Microsoft Corporation (ou en fonction du lieu où vous vivez, l'un de ses affiliés) et vous. Lisez-les attentivement. Ils portent sur le logiciel nommé ci-dessus, y compris le support sur lequel vous l'avez reçu le cas échéant. Ce contrat porte également sur les produits Microsoft suivants :

- les mises à jour,
- les suppléments,
- les services Internet et
- les services d'assistance technique

de ce logiciel à moins que d'autres termes n'accompagnent ces produits, auquel cas, ces derniers prévalent.

EN UTILISANT LE LOGICIEL, VOUS ACCEPTEZ CES TERMES. SI VOUS NE LES ACCEPTEZ PAS, N'UTILISEZ PAS LE LOGICIEL.

Dans le cadre du présent accord de licence, vous disposez des droits ci-dessous.

1. INSTALLATION ET DROITS D'UTILISATION. Vous êtes autorisé à : installer et utiliser un nombre quelconque de copies du logiciel sur vos dispositifs.
2. PORTEE DE LA LICENCE. Le logiciel est concédé sous licence, pas vendu. Ce contrat vous octroie uniquement certains droits d'utilisation du logiciel. Microsoft se réserve tous les autres droits. À moins que la loi en vigueur vous confère davantage de droits nonobstant cette limitation, vous pouvez utiliser le logiciel uniquement tel qu'explicitement autorisé dans le présent accord. À cette fin, vous devez respecter les restrictions techniques du logiciel qui autorisent uniquement son utilisation de certaines façons. Vous n'êtes pas autorisé à :
   - divulguer les résultats des tests d'évaluation du logiciel à un tiers sans l'autorisation préalable écrite de Microsoft ;
   - contourner les limitations techniques du logiciel ;
   - reconstituer la logique du logiciel, le décompiler ou le désassembler, sauf dans la mesure où ces opérations seraient expressément autorisées par la réglementation applicable nonobstant la présente limitation ;
   - faire plus de copies du logiciel que spécifié dans ce contrat ou par la réglementation applicable, nonobstant la présente limitation ;
   - publier le logiciel pour que d'autres le copient ;
   - louer ou prêter le logiciel ;
   - transférer le logiciel ou le présent contrat à un tiers ; ou
   - utiliser le logiciel pour des services d'hébergement commerciaux.
3. COPIE DE SAUVEGARDE. Vous êtes autorisé à effectuer une copie de sauvegarde du logiciel. Vous ne pouvez l'utiliser que dans le but de réinstaller le logiciel.
4. DOCUMENTATION. Tout utilisateur disposant d'un accès valide à votre ordinateur ou à votre réseau interne peut copier et utiliser la documentation à des fins de référence interne.
5. RESTRICTIONS À L'EXPORTATION. Le logiciel est soumis à la réglementation américaine relative à l'exportation. Vous devez vous conformer à toutes les réglementations nationales et internationales relatives aux exportations concernant le logiciel. Ces réglementations comprennent les restrictions sur les destinations, les utilisateurs finaux et l'utilisation finale. Pour plus d'informations, consultez le site www.microsoft.com/exporting.
6. SERVICES D'ASSISTANCE TECHNIQUE. Comme ce logiciel est fourni « en l'état », nous ne fournirons aucun service d'assistance.
7. INTÉGRALITÉ DES ACCORDS. Le présent contrat ainsi que les termes concernant les suppléments, les mises à jour, les services Internet et d'assistance technique constituent l'intégralité des accords en ce qui concerne le logiciel et les services d'assistance technique.
8. DROIT APPLICABLE.
   a) États-Unis. Si vous avez acquis le logiciel aux États-Unis, les lois de l'État de Washington, États-Unis d'Amérique, régissent l'interprétation de ce contrat et s'appliquent en cas de réclamation pour violation dudit contrat, nonobstant les conflits de principes juridiques. La réglementation du

pays dans lequel vous vivez régit toutes les autres réclamations, notamment, et sans limitation, les réclamations dans le cadre des lois en faveur de la protection des consommateurs, relatives à la concurrence et aux délits.

b) En dehors des États-Unis. Si vous avez acquis le logiciel dans un autre pays, les lois de ce pays s'appliquent.

9. EFFET JURIDIQUE. Le présent contrat décrit certains droits juridiques. Vous pourriez avoir d'autres droits prévus par les lois de votre pays. Vous pourriez également avoir des droits à l'égard de la partie de qui vous avez acquis le logiciel. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre ou pays si celles-ci ne le permettent pas.
10. EXCLUSIONS DE GARANTIE. LE LOGICIEL EST CONCÉDÉ SOUS LICENCE « EN L'ÉTAT ». VOUS ASSUMEZ TOUS LES RISQUES LIÉS À SON UTILISATION. MICROSOFT N'ACCORDE AUCUNE GARANTIE OU CONDITION EXPRESSE. VOUS POUVEZ BÉNÉFICIER DE DROITS DES CONSOMMATEURS SUPPLÉMENTAIRES DANS LE CADRE DU DROIT LOCAL, QUE CE CONTRAT NE PEUT MODIFIER. LORSQUE CELA EST AUTORISÉ PAR LE DROIT LOCAL, MICROSOFT EXCLUT LES GARANTIES IMPLICITES DE QUALITÉ, D'ADÉQUATION À UN USAGE PARTICULIER ET D'ABSENCE DE CONTREFAÇON.
11. LIMITATION ET EXCLUSION DE RECOURS ET DE DOMMAGES. VOUS POUVEZ OBTENIR DE MICROSFOT ET DE SES FOURNISSEURS UNE INDEMNISATION EN CAS DE DOMMAGES DIRECTS LIMITÉE UNIQUEMENT A HAUTEUR DE 5,00 $ US. VOUS NE POUVEZ PRÉTENDRE À AUCUNE INDEMNISATION POUR LES AUTRES DOMMAGES, Y COMPRIS LES DOMMAGES SPÉCIAUX, INDIRECTS OU ACCESSOIRES ET PERTES DE BÉNÉFICES.
12. Cette limitation concerne :
    - toute affaire liée au logiciel, aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers et
    - les réclamations au titre de violation de contrat ou de garantie, ou au titre de responsabilité stricte, de négligence ou d'une autre faute dans la limite autorisée par la loi en vigueur.
13. Elle s'applique également même si Microsoft connaissait l'éventualité d'un tel dommage. La limitation ou exclusion ci-dessus peut également ne pas vous être applicable, car votre pays n'autorise pas l'exclusion ou la limitation de responsabilité pour les dommages indirects, accessoires ou de quelque nature que ce soit.

6. Annex 2 – IDIAP Consent Form

VoxSpoof Database Consent Form (10/2010)

In the framework of the Tabula Rasa project, Idiap is investigating spoofing of speech recognition systems. This project aims to develop reliable and efficient solutions to detect and circumvent various spoofing attacks in speech recognition systems. This research requires large amounts of audio / video data. Idiap intends to compile such a corpus.

We are kindly asking for your assistance in this corpus collection. By signing this form you authorize the inclusion of your data within this corpus.

The recorded data will initially be used in the context of the Tabula Rasa project for research purposes. It is possible that some or all of the data will be made available to the wider research community. Data may be put online for access in connection with research activities.

Please note that you remain solely responsible for the content of your behavior. If you are concerned about the content of your personal input, please advise us immediately.

_____

_____

1. The data collection is subject to the Swiss Federal Act on Data Protection (FADP).

2. The collected data may be regarded as personal data or, in some cases, as sensitive data according to article 3 let. a and c FADP.

3. The data are collected and processed by Idiap Research Institute for research purposes only.

4. The data will only be used for: *Research in speaker recognition including spoofing and anti-spoofing*

5. The Idiap Research Institute, based in Martigny (Valais/Switzerland), is a non-profit foundation specialized in the management of multimedia information and man-machine multimodal interactions. Idiap was founded in 1991 by the Town of Martigny, the State of Valais, EPFL (Ecole polytechnique fédérale de Lausanne), the University of Geneva and Swisscom, and is autonomous but connected to EPFL by a joint development plan. The contact details of the Idiap Research Institute is the following:

Consent Form – Release 1.3 (2010/10) Page 1/3

Idiap Research Institute
Centre du Parc
Rue Marconi 19
PO Box 592
CH - 1920 Martigny
Switzerland

T +41 27 721 77 11
F +41 27 721 77 12

http://www.idiap.ch
info@idiap.ch

6. The data will be collected and distributed by the Idiap Research Institute only. Idiap Research Institute warrants that it fulfills all conditions for processing data according to FADP and to the Ordinance on data protection.

7. The collected data will be distributed on the basis of an end-user license agreement (EULA), only to end users that have subscribed to the EULA. The data recipient may be affiliated to other research institutes or other entities than Idiap Research Institute.

8. The persons concerned with the data collection have an access right to their own data. Their consent can be withdrawn anytime at the following address: data-manager@idiap.ch. At receipt of a consent withdrawal, Idiap Research Institute shall make the best efforts to erase and destroy the data under its control within 15 office days. Idiap Research Institute shall hold no copy of the data under its control and restrain from further distributing the data.

9. After 15 days from the signature of the present form, the data may be distributed to third parties by Idiap on the basis of this consent form. Idiap will not have control over the transferred data.

In the event of consent withdrawal according to § 8, Idiap Research Institute makes no warranty with regard to data which is not under its control and shall not be held responsible for erasing data already transferred to third parties on the basis of the present consent form.

By signing this consent form, the undersigned expressly agrees with the above mentioned conditions and give Idiap Research Institute the right to collect, use, process and distribute the personal data at the conditions set forth under Item 7, without limitation in accordance with the above mentioned conditions, and expressly renounces to act against Idiap Research Institute on the basis of constitutional, civil, criminal, and Data protection law with regard to the collected data.

I, (please print name) ..... have read and understood this form and agree to authorize use of the recorded data on the terms indicated.

Signature:..... Date:.....

Please provide your email address (or other contact information) so that we can contact you if necessary:

.....

Consent Form – Release 1.3 (2010/10) Page 3/3

7. Annex 3 – EURECOM Consent Form

Consent Form

1.1 Purpose

EURECOM is carrying out scientific research on a number of physical features that may allow recognising people by using automated means. The overall goal of the study is to develop better technology for human recognition and to investigate and improve the security of said technology to spoofing.

1.2 Procedure

In order to test the technology for human recognition, a number of physical features will be recorded in a controlled environment, notably in a smart room. In the session you are invited to participate we will record signals from a microphone and a camera in the room.

During the sessions, you will be given a questionnaire by means of which we are going to collect personal characteristics like gender.

Each session will last a couple of minutes only, and individuals may discontinue their participation at any time for any reason without any need to give an explanation for their will to stop their participation.

1.3 Personal data handling

The goal of the study is only to evaluate the capability to recognise people using these features and to investigate spoofing countermeasures.
Data collected will not be used for any kind of commercial use or medical use.

All personal data stored during the acquisitions will be completely anonymised.
No personal data will be ever used for any purposes different from those stated in this form.

If you agree your data may be transferred to third parties (such as Universities) only for research purposes.

Your data will absolutely not be commercialised. You may exercise your rights of access, rectification and deletion of data at any time. In order to do so, you will need to communicate it to *EURECOM* by a letter addressed to

Nick EVANS
EURECOM
2229 route des Crêtes
06560 VALBONNE

or by e-mail to the following address: nick.evans@eurecom.fr

All personal data will be erased before January 2015.

1.4 Confidentiality

The researcher responsible for the data collection sessions will record the data collected in a file. These data will be identified only by a code and an identification number. The code of the study consists of a letter or digit to which a number assigned by the researcher is added afterward (eg, S01_02). The relationship between the ID number and your name is recorded in a computer and is stored separately and securely. This file will be accessible only under the supervision and responsibility of the principal researcher, *Prof. Nick EVANS*. The key to link your name to the code which identifies the data file will not be provided to anyone and the privacy of your data will be protected. The results of the study could be published in scientific books or articles or could be used for didactic purposes. However, your name will be never revealed in any document, publication or teaching materials.

1.5 Right to get more information about the study

You can ask any questions about the study at any time throughout the record. The principal researcher will be available to answer your questions, interests or concerns about the study. You will be informed of any new discovery that could occur throughout the study and that may affect your participation in future studies. If during the study and thereafter you wish to discuss your rights as a person who participates in an investigation, your participation in the study or your concerns about it, or if you do not want to continue in that investigation or future researches, please contact the principal researcher, *Prof. Nick EVANS*, at the address provided above any time you wish.

1.6 Refusal or cessation of participation

The participation in this *data collection session* is voluntary. You do not have to participate in this study if you do not want. If you choose to participate, you can change your mind or leave the study at any time without having to give explanations and without being yourself affected in any way. Similarly, at the discretion of the researcher responsible for the data collection sessions, you may be withdrawn from the study for any of the following reasons: (a) if the minimum requirements of the study are not met (b) if for any reason the study is interrupted.

1.7 Risks and discomforts

The personal risk by participating in this study does not exceed the risks of daily and normal life. None of the procedures represents a danger to the health or to the physical and mental integrity.

1.8 Compensation

There is no compensation for participating in this study.

1.9 Consent

By signing the present form, I understand and consent freely that my personal data, including biometric data, including my name and contact details, will be processed by EURECOM, Multimedia Department, 2229 route des Crêtes, 06560 Valbonne, FRANCE, and by appointed processors on behalf of the data controller, in accordance with applicable laws and with what is stated in the present clause.

I have been explained and informed of the purposes of this research. I understand that some personal data may reveal directly or indirectly sensitive data, including data revealing age, and that this is necessary for the project.

I declare to be aware that the data collected will not be used for any kind of commercial use, medical or clinical diagnosis.
I declare to be aware that my data may be transferred to third parties (such as Universities) only for research purposes.

I understand that my personal data will be encoded in order to safeguard confidentiality and that if results of the study are published, my identity will not be revealed. I also understand that I have the right to request access to my personal data, to correct, if applicable, and delete my personal data in conformity with the applicable legislation. For these purposes, I can contact *Prof. Nick EVANS* at the address provided above.
I have read the above and I understand that I can refuse to participate in this study without any direct or indirect negative consequence on my life.

By signing the present form, I agree with the above stated.

Date: _____ Place: _____

Name: _____

Signature: _____

E-mail: _____ Telephone: _____

8. Annex 4 – UOULU Consent Form

ICB 2013 TABULA RASA Fingerprint Spoofing Challenge

Consent Form

Tabula Rasa EU project (http://www.tabularasa-euproject.org/) aims to develop efficient solutions to detect and circumvent various spoofing attacks against different biometric systems.

The goal of this ICB 2013 Tabula Rasa Fingerprint Spoofing challenge is to demonstrate spoofing and anti-spoofing attacks in the particular case of fingerprint biometric recognition.

By signing this Consent Form, you expressly agree that your fingerprint data will be captured and saved into the system for enrollment. Your data will not be distributed nor used for any other purposes than this demo. Your data will be erased after this Fingerprint Spoofing Challenge.

I, (please write your name) ..... have read and understood this consent form and agree to authorize the capture of my fingerprint data for this Fingerprint Spoofing Challenge only.

Signature:..... Date:.....

9. Annex 5 – CASIA Consent Form

CASIA Data Collection Consent Form

CASIA (Institute of Automation, Chinese Academy of Sciences) is showing a face recognition with anti-spoofing system on ICB 2013 TABULA RASA Spoofing Challenge. To illustrate the face recognition and anti-spoofing ability of the system, we need enroll face images and names of some volunteers into the system.

We are kindly asking for you assistance in this challenge. After enrolled into the system, you can test the recognition performance and can try to attack the system by your printed photo or other kinds of fake samples.

By signing this form you authorize that we could use your data during the period of demo (June 4-7, 2013). At the end of demo, your data will be deleted from our system and computer.

The contact details of the CASIA (Institute of Automation, Chinese Academy of Sciences) is the following:

Zhongguancundonglu 95
100190 Beijing
China
T +86 10 62551575
F +86 10 82614508
http://www.ia.ac.cn

I, (please print name) ..... have read and understood this form and agree to authorize use of the recorded data on the terms indicated.

Signature:..... Date:.....

Please provide your email address (or other contact information) so that we can contact you if necessary:

.....

10. Annex 6 – STARLAB Consent Form

Consent Statement Form

Myself, the undersigned: _____

Date of birth: _____ Address: _____

City: _____ Province: _____

I DECLARE:

- voluntarily participate in the study of the "TABULA RASA - Trusted Biometrics under Spoofing Attacks";
- I have received in-depth explanations by the researcher regarding the request for my participation in the research;
- I have had the opportunity to ask questions and have received satisfactory answers;
- I have been informed about possible risks or discomforts reasonably foreseeable;
- I have been aware that participation is voluntary;
- Consent to the use of my personal data communicated and eventually of the electrocardiogram and electroencephalogram recordings of the complete experimental session, only for the purpose of research;
- I have been informed that:

1) I can withdraw from the experiment at any time, although this has already begun,
2) the result of the recordings can reveal directly or indirectly sensitive data such as data related to health status and that these data could be used during the project,
3) if the project results are published my identity would not be revealed,
4) is my right to access the documentation as long as I'm concerned,
5) I authorize the use of data for research purposes. This consent is valid within the meaning and effect of Law 15/1999 and therefore allows the processing of sensitive personal data for research and scientific publication.

Date _____

Signature of Research Participant _____

11. Annex 7 – MORPHO Consent Form

[COMPANY/ORGANISATION LOGO] *[PROJECT LOGO]*

AUTHORISATION FOR *[SPECIFY BIOMETRICS ACQUIRED]* BIOMETRIC DATA ACQUISITION FOR *[PROJECT NAME]* PROJECT

I, the undersigned, ...
Mr. – Mrs. – Ms.

Employed by.....

Authorise [COMPANY/ORGANISATION NAME] to collect and use my *[SPECIFY BIOMETRICS DATA]* data. The acquisitions *[DESCRIPTION OF ACQUIRED DATA]* will be anonymised before any exploitation then utilised exclusively for scientific research purposes.

Date: .....
(or from.....to.....)
Location: .....

These data could be transferred to other partners participating to the above mentioned project (*) and will be destroyed at the end of the project plus one year. Communication of these data to any third parties (company or individual) is prohibited. For the project partners, use of the collected data is strictly limited to research activities related to *[PROJECT NAME]* project.

[This paragraph is to adapt/modify to refers to national laws of the country where data collection takes place] In accordance with Articles 39 and subsequent of French Law No. 78-17 of 6 January 1978 relating to computers, files and freedom, any person may obtain and, if necessary, correct or delete personal information by sending a request to project coordinators, *[NAMES OF COORDINATORS]*. Those acquisitions and processing compliant with the CNIL (French Data Protection Authority)'s authorisation n°2010-336 dated 22 July 2010 and have been notified to the CNIL.

In duplicate, location: ..... date: .....

Signature preceded by the words "Read and approved"

(*) List of partners receiving data: *[PARTNER (COUNTRY)]*...

[URL OF PROJECT WEBSITE]