



LE1-1930

Future Research

Deliverable D 5.2 - public version



This is the public version of deliverable 5.2 (confidential)

Contents:

1. INTRODUCTION.....	2
2. TELEMATICS SERVICES REQUIRING ACCESS PROTECTION.....	3
2.1 THE CALLING CARD DEMONSTRATOR.....	3
2.2 THE INTEGRATED MESSAGE SERVICE DEMONSTRATOR.....	3
2.3 THE BANKING DEMONSTRATOR.....	3
3. REGULATION OF USE OF BIOMETRIC PERSON AUTHENTICATION TECHNIQUES	3
5. STANDARDISATION AND ASSESSMENT OF SPEAKER VERIFICATION TECHNOLOGY .	3
4.1 HARDWARE	3
4.2 SOFTWARE.....	3
4.3 SYSTEMS INTEGRATION	3
4.4 TECHNOLOGY ASSESSMENT	3
4.5 ASSESSMENT OF APPLICATIONS USING SV	3
6. TECHNICAL DEVELOPMENT IN SPEAKER VERIFICATION.....	3
5.1 INCREMENTAL ENROLMENT.....	3
5.2 EXTENSION OF THE TECHNOLOGY TO CELLULAR NETWORKS	4
5.3 SUPPRESSION OF ADDITIVE NOISE	4
5.4 TEXT-INDEPENDENT SV TECHNOLOGY	4
5.5 SV BASED ON USER SELECTED PASSWORDS	4
5.6 RAPID ADAPTATION FOR ASR AND SV	4
6. USER REQUIREMENTS AND MARKETING RESEARCH.....	4
6.1 END USER REQUIREMENTS.....	4
6.2 INTEGRATION WITH OTHER BIOMETRIC AUTHENTICATION.....	4
6.3 REQUIREMENTS OF SERVICE PROVIDERS	4
7. HUMAN FACTORS RESEARCH.....	4

This work has been supported by:

- the Telematics programme of the European Union
- the Office Federal de l'Education et de la Science (in Switzerland)



1. Introduction

This document identifies and explains several issues that need additional Research & Development in order to prepare Speaker Verification technology for use in large scale applications with the general public. Most of the thinking underlying the contents of this document has been guided by close-to-market applications that will involve large numbers of customers.

It should be noted that the choice of completely different applications, specifically applications with small and select customer populations, might have given rise to different priorities for the R&D work that is proposed. The R&D issues discussed in this document are all closely related to telematics services.

It is acknowledged that Speaker Verification, as most other biometric person authentication techniques, can also be used for the protection of access to premises (rooms and/or floors in buildings, buildings as a whole, but even countries).

Developing technology for premises access protection might also have led to different R&D priorities. However, we are convinced that only the relative priority assigned to the research topics would have changed if we had decided to focus on another type of applications.

All research sketched in this document will yield results which can be re-used in most other application domains than telematics services as well.

This document lends heavily and freely from the proposal for the PICASSO project, submitted by the CAVE consortium in reply to the 4th call for proposals in the LE programme. We think that that is in accordance with the original aims of workpackage 5, as that intended to lay the ground for R&D in the period following the completion of the CAVE project.

Details on the PICASSO project will be available through the PICASSO web page. The URL will be published on the CAVE web page (<http://www.kpn-telecom.nl/CAVE>)

In the confidential version of the D 5.2 deliverable following issues have been addressed. (please refer the Picasso website)



2. Telematics Services requiring access protection

2.1 THE CALLING CARD DEMONSTRATOR

2.2 THE INTEGRATED MESSAGE SERVICE DEMONSTRATOR

2.3 THE BANKING DEMONSTRATOR

3. Regulation of Use of Biometric Person Authentication Techniques

4.

5. Standardisation and Assessment of Speaker Verification Technology

4.1 HARDWARE

4.2 SOFTWARE

4.3 SYSTEMS INTEGRATION

4.4 TECHNOLOGY ASSESSMENT

4.5 ASSESSMENT OF APPLICATIONS USING SV

6. Technical development in Speaker Verification

7.

5.1 INCREMENTAL ENROLMENT



5.2 EXTENSION OF THE TECHNOLOGY TO CELLULAR NETWORKS

5.3 SUPPRESSION OF ADDITIVE NOISE

5.4 TEXT-INDEPENDENT SV TECHNOLOGY

5.5 SV BASED ON USER SELECTED PASSWORDS

5.6 RAPID ADAPTATION FOR ASR AND SV

6. User Requirements and Marketing Research

6.1 END USER REQUIREMENTS

6.2 INTEGRATION WITH OTHER BIOMETRIC AUTHENTICATION

6.3 REQUIREMENTS OF SERVICE PROVIDERS

7. Human Factors Research