Project Number	AC095
Project Title	ASPeCT: Advanced Security for Personal Communications Technologies
Document Type	Intermediate Deliverable
Security Class	Public

Deliverable Number	D23
Title of Deliverable	Vocal password-based user authentication demonstration
Nature of Deliverable	Report
Document Reference	AC095/L&H/W27/DS/P/23/1
Contributing Work Packages	WP2.7, WP2.4
Contractual Date of Delivery	December 1997 (Y3M10)
Actual Date of Delivery	21 May 1998 (Y04M03)
Editor	Martine Lapère, Lernout & Hauspie

Abstract	This document provides a report on Deliverable D23, the demonstration of low-storage speaker verification which will be performed at the IS&N 98 conference in Antwerp, 25-28 May 1998.
Keywords	ACTS ASPeCT authentication biometrics compression smart cards speaker verification UIM UMTS

1. EXECUTIVE SUMMARY

ASPeCT Deliverable D23 is the first public deliverable from WP2.7. In association with WP2.4, WP2.7 has been developing the techniques of password-based speaker verification algorithms to comply with the constraints imposed by smart-card technology, and demonstrating the applicability and benefits in the context of mobile communications. Single and multiple password verification systems were examined during the scope of the project, of which [D21] deals with the single password, and [D22] with the multiple password verification system. D23 demonstrates the implementation of the the multi-password system and the storage and retrieval of the low-storage voice templates on the smart-card. The public demonstration will be held at the IS&N 98 conference, Antwerp, 25-28 May 1998.

2. TABLE OF CONTENTS

1. EXECUTIVE SUMMARY 2

2. TABLE OF CONTENTS 3

3. DESCRIPTION OF THE DEMONSTRATION 4

4. IMPLEMENTATION OF THE DEMONSTRATION 5

5. SYSTEM SETUP 6

6. CONCLUSION 8

7. REFERENCES 8

3. DESCRIPTION OF THE DEMONSTRATION

This document gives a short description of the interactive password based speaker verification demonstration system.

The first internal deliverable from this work [D21] gave a description of the algorithms that enable single password speaker verification. The voiceprints generated by this algorithm required only about a hundred bytes of storage per password, an amount designed to be small enough to be stored on a smart card.

The next deliverable [D22] described how the security obtained by this vocal check could be enhanced quite a lot by switching from a single to multiple password verification system. It was shown that the separation increases by increasing the number of passwords.

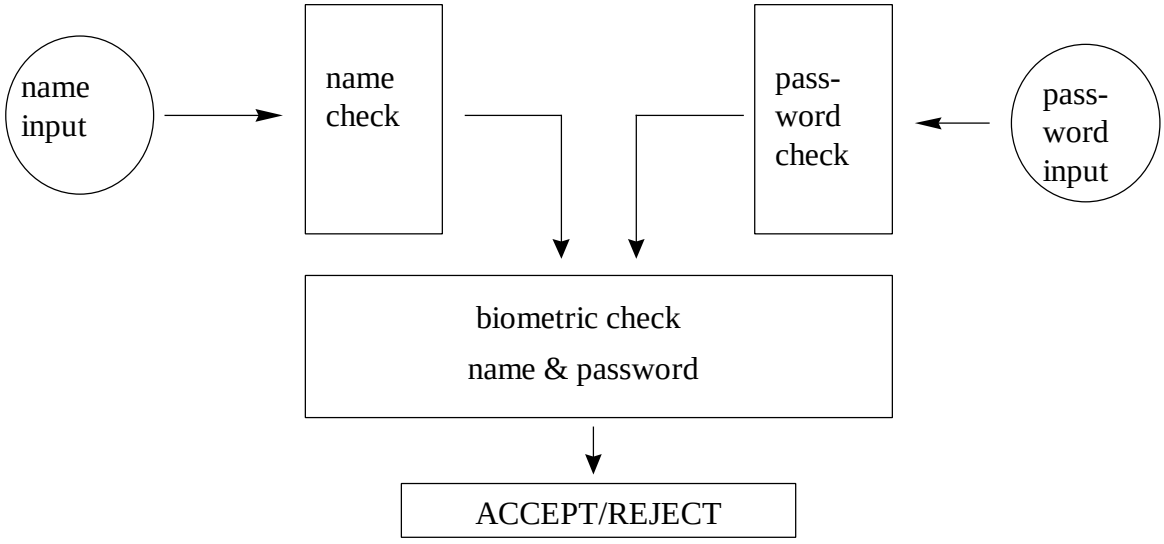
In this demonstration, we have made a real-time implementation of such a multiple password verification system.

In order to keep the system as user-friendly as possible, we opted for a dual password verification system in this demonstration.

More specifically the user is prompted to give his/her name, together with a user-defined password system.

The demonstration includes a full training session, the storage of the voice prints onto the smart card, the retrieval of data from the smart card, and the verification process.

4. IMPLEMENTATION OF THE DEMONSTRATION



In the current implementation a dual password verification system is used. To make the system attractive to the user however, he or she will be asked to utter their name and than to speak the user-chosen password.

Within in the system however, the user's name will be treated in completely the same way as the user's password. During the training session, the user has complete freedom to chose the so-called 'name' input. He or she can use their proper name (first + last name), or use a nickname. A minimum length constraint of 0.8 seconds is used on the speech input. The voice prints of the name response and the password response are stored on the Smart Card.

At verification time, the user will again be prompted for their name (or nickname) and their password. A dual password verification session as described in [D22] is then invoked.

For each password the user is given three attempts, with possible exit functions after the first and second trial. This in order to enhance the user friendliness. In general *bona fide* users will require fewer attempts than impostors. A maximum of three attempts are used to check a single password (whether the user's name or password), and the scores of the different passwords of the complete session are combined in order to make the final accept/reject decision.

5. SYSTEM SETUP

Hardware setup:

The hardware system consists of a PC system, with a built-in or add-on sound card of the Soundblaster type, an external microphone and an external smart card terminal, with the corresponding smart cards. The smart card terminal is connected to the PC via a serial port.

Software setup:

The architecture of the demonstration has a modular setup. At the high level there is a scripting language, enabling the setup of flexible scenarios. The script is build up by several states, each state enabling a specific low-level function. The low-level functions are enabled by the linkage of the appropriate DLL functions.

The parsing of a script file by the script engine will result in a network of states being created. The set of states is organized as a final state machine.

The following states have been defined:

- Initialize
- Terminate
- Abort
- Prompt
- Acquisition
- Train
- Verify
- Store VoicePrint
- Retrieve VoicePrint

The script tool will be provided by a vocal user interface. This system gives the necessary prompts to the user. These prompts include a welcome prompt, a request to insert the smart card, and the necessary prompts to utter the names and passwords. During the training session, a vocal feedback system replays the user's input in order to give him or her feedback on the recording quality. After the verification session, the decision is also given verbally.

6. CONCLUSION

The deliverable D23 of WP2.7 of the ASPeCT project illustrates the feasibility of the implementation of a multiple password voice verification system, generating voiceprints small enough to comply with the storage constraints of currently available smart cards. All the functionality of the verification system is illustrated, including on-line training of the voice prints, the actual storage on the smart card, the retrieval of a voice print from the card, and the user identity check.

7. REFERENCES

[D21] ACTS AC095 ASPeCT Deliverable D21. *Algorithms for single password user verification*. AC095/L&H/W27/DS/I/21/1. February 1997.

[D22] ACTS AC095 ASPeCT Deliverable D22. *Algorithms for multiple password user verification*. AC095/L&H/W27/DS/I/21/1. June 1997.