Instructions for IDCard

David Llewellyn-Jones
david@flypig.co.uk
http://www.flypig.co.uk/
7th October 2002

Introduction

This document provides general instructions for use of the programs !IDCard and IDCard.exe along with the associated example data. The purpose of these programs is to provide an example system for the techniques described in the document 'Liberty, Security, Identity' (**LSI.pdf**), which in turn is intended as a response to the government's 'Entitlement Cards and Identity Fraud - A Consultation Paper' (July 2002).

Brief Overview

This section provides a brief description which will allow you to run and try the IDCard example program without getting overly involved with the details. For a more thorough explanation, see the sections which follow this one.

To run the program under Windows (2000 or XP recommended), run the **IDCard.exe** executable on the CD. Under RISC OS, run the **!IDCard** application. The data will be verified (indicated by 'SUCCESSFUL' messages), after which you will be given a number of options. To choose one of the options, press one of the number keys between 1 and 7.

To verify the name stored on the card, select option 1, then type in the name which you believe the data to refer to. In this case, the correct name is 'David Llewellyn-Jones'. The verification will only succeed if the exact punctuation and capitalisation is used.

The other options generally work in a similar way, although you' ll need to re-run the program every time you want to try one of them out as it quits itself automatically once each action has been performed.

Running the program

The program is provided in two executable formats. One is for use under RISC OS, the other for use under Windows. Once running, the two act in essentially the same way (they have been produced from the same source code), however getting them to run does differs slightly between the two platforms.

RISC OS

To run the RISC OS version you require a computer running RISC OS. Begin by opening the CD filer window by clicking on the CD icon at the bottom left of the screen (on the icon bar). A directory display will appear. To run the program simply double click the **!IDCard** icon in the directory display.

Windows

We recommend using a recent version of Windows, such as Windows 2000 or XP. The program will work with earlier versions, but this has not been fully tested and

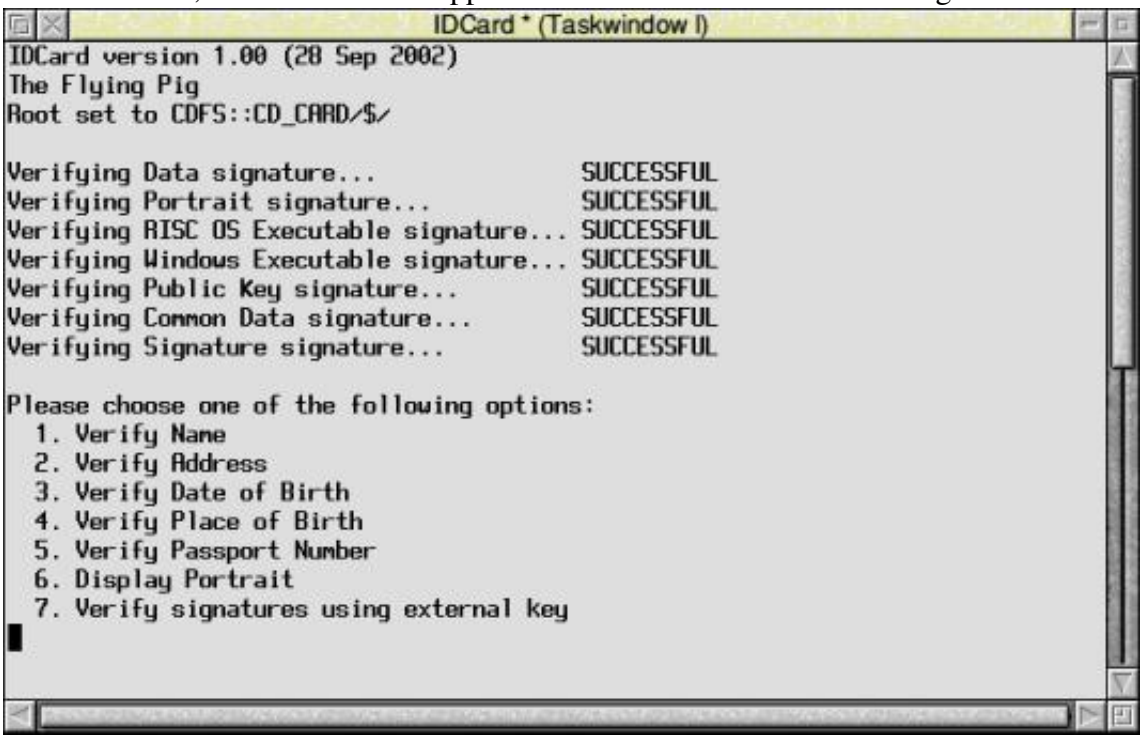
certain operations may not work correctly.

The program is set to autorun once the CD is placed in the CD drive, however this can be disabled via the computer's configuration options. If disabled, the program may be run by choosing 'Run' from the Start menu. A box will appear, where you can enter the text '**D:\IDCard.exe**'. If your CD drive is not mapped to the D drive, then swap the initial D with the appropriate drive letter.

It is also possible to run the program by opening Windows Explorer and double clicking on the CD drive icon. You may then have to click on the **IDCard.exe** executable, depending on your configuration settings.

Using the program

Once run, a window should appear with text similar to the following[1]:



The seven lines which begin with the word 'Verifying' show that checks have been undertaken to ensure that the data is correctly signed using the card issuer's private key. If any of these were to fail, it would indicate that the data had been tampered with in some way. Note however that under RISC OS, the ImageFS[2] application is known to cause problems with the verification of the Portrait signature. It is recommended that ImageFS[2] is turned off before !IDCard is used.

Assuming the verifications are successful, you will be presented with seven options:

1. Verify Name;
2. Verify Address;
3. Verify Date of Birth;
4. Verify Place of Birth;
5. Verify Passport Number;
6. Display Portrait;

[1] The colours and general appearance will probably be slightly different.

7. Verify Signature using external key.

Choose one of the options by selecting the appropriate number on the keyboard between 1 and 7.

Options 1-5 all act in the same way: you will be presented with the opportunity to enter the data to verify. For example, if you select option 1 a prompt will appear asking you to 'Enter Name'. Normally you would enter the name of the cardholder. The example data is set up with my details, so entering my name will produce a successful verification:-

```
Enter Name:
David Llewellyn-Jones
     Verification was SUCCESSFUL

Finished
```

You may want to try this along with some other incorrect names. Only the correct name (with the correct capitalization) will produce a 'Successful' outcome. The same applies to the other data on the card. You might want to try the following:

Name:	David Llewellyn-Jones
Address:	67 Lodge Hill Road, Selly Oak, Birmingham, B29 6NL, UK
D.o.B:	1st April 1976
Place o. B:	Rochford

Be careful to enter the details exactly as they are given here, including the correct capitals and punctuation. Any deviation from these will result in an unsuccessful verification.

Choosing option 6 will display the digital version of the photograph held on the card. The photograph is stored in jpeg format and jpeg viewers can be found in the Utilities directory if there is not already one available on your computer.

The final option (option 7) allows you to verify the signatures using an external key. In general it would not be sensible to use the signature stored on the card to verify that the data originated with the card issuer. Instead, greater security can be obtained if the card issuer's public key is supplied with the card checking software. This option allows you to enter a public key stored in a different place to verify the data on the card. The public key file kept on the card is called **public.dss**, but on choosing option 7 you can enter the filename of any other version of this key, after which the signatures will be checked using the given external key.

Additional functions

As well as verifying the data held on the card, the programs may also be used to generate new cards. To do this you will require access to the card issuer's private key. If you do not have such access, you might want to generate your own.

To generate a new public-private key pair, run the program using the **-g** switch. To do this, open a DOS window or taskwindow and enter the full pathname for the program with the switch added at the end. Under RISC OS this would be:

```
CDFS::CD_CARD.$.!Idcard.!RunImage -g
```

whilst under Windows this might be:

```
D:\IDCard.exe -g
```

You may be asked to enter a 'root path'. This is just a working directory, and you

should enter the path of a directory where you would be happy for the program to save the generated keys to. The root directory *must* contain the file **common.dss**, so you may wish to copy this file into an empty directory before you begin.

Once you have generated a public-private key pair, creating new card data can be achieved by executing the program using the **-i** switch. Hence under RISC OS you might enter the following into a taskwindow:

```
CDFS::CD_CARD.$.!Idcard.!RunImage -i
```

whilst under Windows you might enter the following into a DOS window:

```
D:\IDCard.exe -k
```

Again, you may be prompted for a root path, in which case follow the same guidelines as given above for key generation. As long as a root path can be established you will be prompted for all of the information which is to be held on the card. Enter the details desired, pressing return after each. At the end you will be prompted for a private key file. Enter the full pathname of the private key which you generated earlier. This will usually have a leafname of **private.dss**. You may also wish to add an image to your designated root directory, to constitute the photograph of the cardholder which will be stored on the card. You must name the file **portrait.jpg** and a signature for the file will then also be produced at this point.

This completes the process. The files which have been generated in the root directory constitute the files needed to be included on any ID card.

Acknowledgements

The executables have been compiled using the excellent MIRACL multi-precission maths library. For more information about this please visit http://indigo.ie/~mscott.

Further Information

Additional information can be obtained by reading the file **!IDCard\!Help**. C Source code has also been provided in the file **!IDCard\Source.c**, which can be compiled under the gcc compiler for RISC OS. The **Utilities\WinSrc.zip** archive contains a fill Visual C++ dsp setup for compilation under Windows. Although untested, compiling for other platforms should be relatively straightforward.

For anything else, feel free to contact me or visit my website:

David Llewellyn-Jones
llewelld@for.mat.bham.ac.uk
http://www.mat.bham.ac.uk/llewelld/