

Manual

Golden Reader Tool

Implemented by secunet Security Networks AG



based on ePassportAPI 2.1

Version 2.9

Installations

Just unzip the GoldenReader.zip archive to a separate directory and start the executable file “GoldenReader.exe”.

System Requirements

- Windows 2000, Windows XP
- 64MB memory
- 10MB free disk space
- Resolution: 1024x768 pixels
- Supported RF-Readers:
 - o PC/SC compatible readers
 - o Philips Pegoda
 - o Integrated Engineering Smart-ID
 - o Feig USB Series (Beta)
- Supported MRZ Readers:
 - o Rochford Thompson RTE6701 with PS/2 keyboard interface
 - o Desko MPR 7310 O (USB)
 - o Desko MPR 7010 O (PS/2)

Main Dialog

The main dialog of the GRT is divided into several parts described below.



Figure 1: GRT Main Dialog

Dialog Areas

1 - Personal Data

Within this area all data stored in data group 1 (DG1 according to [ICAO Doc 9303]) is displayed.

2 - Printed MRZ

Within this area the machine readable zone (MRZ) lines are displayed, if a BAC or EAC protected passport has to be read. The lines must be entered manually in a special dialog (see 4 - “Read BAC/EAC”, page 7) or submitted by an OCR/Stripe reader (see “System Requirements” at the beginning of this document). This data does not represent the data stored on the chip.

③ - Chip Data

Within this area several chip parameters are displayed:

UID: Unique Identifier of the build-in chip
ATR/ATS: Answer to Reset/Answer to Select
[ISO/IEC 14443]: ISO 14443 chip type (Type A or Type B)
Reading time: Total time for reading all possible stored data on chip in seconds. Time measurement starts when reading the first data, chip initialisation is not included.

④ - Logging

Within this window the GRT logs several high level messages. A detailed protocol can be written to disk (see 9 - “Options” button, page 10).

⑤ - Picture

The picture area displays the pictures stored in data group 2 (DG2 according to [ICAO Doc 9303]) and data group 3 (DG3 according to [ICAO Doc 9303]) if present. Use the arrow keys to switch between the different pictures. Double-click the picture to display the current data in original size and aspect ratio.

⑥ - Access Control

Within this area all currently supported access control mechanisms are displayed. Every access method can have one of the following three states:



Access condition not set or processed.

Access condition successfully set.

Setting up access condition failed. See protocol file and protocol window for details.

The following access control methods are supported:

- **BAC (Basic Access Control)** as described in [ICAO Doc 9303]
- **EAC (Extended Access Control)** as described in [BSI TR-03110]
- **Chip Authentication** as described in [BSI TR-03110]
- **Terminal Authentication** as described in [BSI TR-03110]
- **Active Authentication** as described in [ICAO Doc 9303]

7 - Passive Authentication

Within this area the status of the passive authentication procedure is displayed (if available). One of the following states is displayed for each element:



Status not set or processed.



Status successfully verified.



Verification of status failed. See protocol file and protocol window for details.

The Certificate Chain can also have this state:



Status basically verified, but no more valid or not valid according to shell model.

The following signature and hash value states are displayed:

- **Signature EF.SOD:** Indicates, if the Signature of the EF.SOD file could be verified. If possible, the corresponding signature algorithm is displayed.
- **Certificate-Chain:** Indicates, if the certificate chain of the SOD signature could be verified.
- **Revocation:** Indicates, if the revocation status of the SOD signature certificate could be checked.

There is also a line of blocks indicating the verification of the separate data groups stored on the passport. The first block indicates the status of DG1, the second indicates the status of DG2 etc. up to DG16.



The meaning of the colors is similar to the ones above:

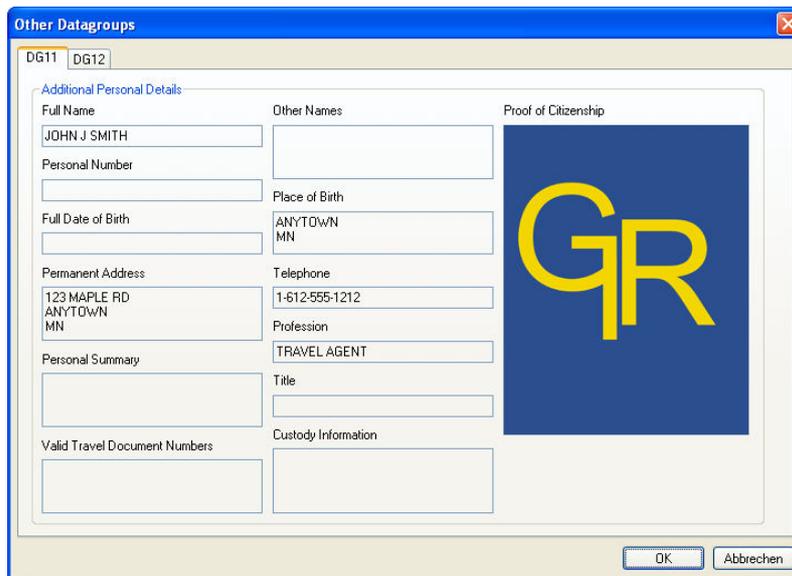
- File not present
- File present, hash status not checked
- File present, hash status successfully checked
- File present, hash verification failed

Buttons

Below the Picture and within the “Operation” frame several buttons are placed to configure and to use the GRT.

① - Show Other Datagroups

This button shows a dialog presenting the contents of data groups 11 and 12 (according to [ICAO Doc 9303]), if existing, read from the passport:

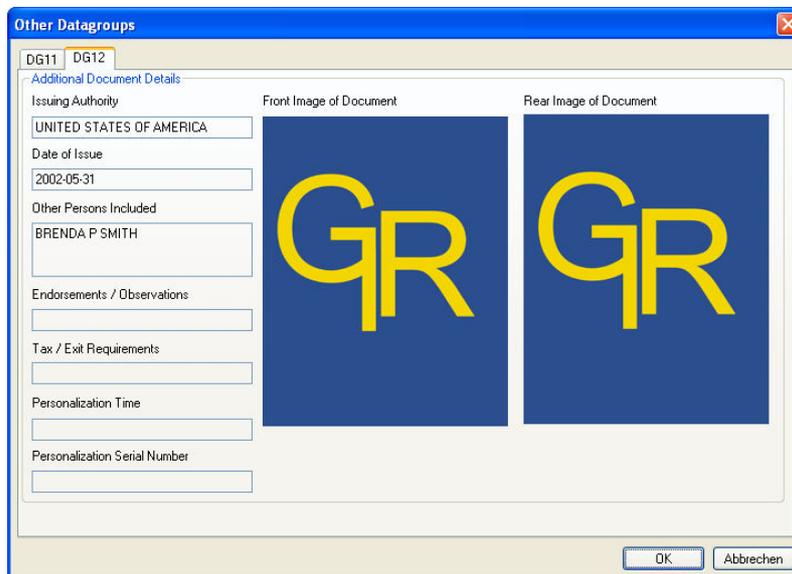


The screenshot shows a dialog box titled "Other Datagroups" with tabs for "DG11" and "DG12". The "Additional Personal Details" section contains the following fields:

Field	Value
Full Name	JOHN J SMITH
Personal Number	
Full Date of Birth	
Permanent Address	123 MAPLE RD ANYTOWN MN
Personal Summary	
Valid Travel Document Numbers	
Other Names	
Place of Birth	ANYTOWN MN
Telephone	1-612-555-1212
Profession	TRAVEL AGENT
Title	
Custody Information	
Proof of Citizenship	Image of a blue passport page with the yellow "GR" logo.

Buttons: OK, Abbrechen

Figure 2 : Data group 11



The screenshot shows a dialog box titled "Other Datagroups" with tabs for "DG11" and "DG12". The "Additional Document Details" section contains the following fields:

Field	Value
Issuing Authority	UNITED STATES OF AMERICA
Date of Issue	2002-05-31
Other Persons Included	BRENDA P SMITH
Endorsements / Observations	
Tax / Exit Requirements	
Personalization Time	
Personalization Serial Number	
Front Image of Document	Image of a blue passport page with the yellow "GR" logo.
Rear Image of Document	Image of a blue passport page with the yellow "GR" logo.

Buttons: OK, Abbrechen

Figure 3: Data group 12

If the passport read does not contain DG11 or DG12, the following dialog is shown:

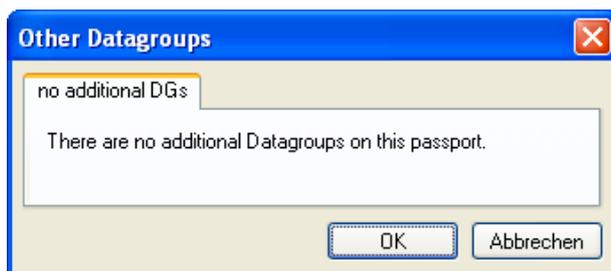


Figure 4: No additional data groups

② - Autodetect

If this button is pressed the GRT uses a special passport detection mode. If the passport is not BAC protected, reading will start immediately. If the passport is BAC (or EAC) protected, the MRZ has to be entered before reading starts.

The GRT checks the entered MRZ with the passport(s) activated in the RF-field whenever there are multiple passports in the field. It will then automatically select the correct passport and read the corresponding data.

③ - Read

Using this button the GRT tries to read an unprotected ePassport placed on the reader. If the error message “Security conditions not fulfilled” shows up, the passport is protected by BAC or EAC. Use the “Autodetect” or “Read BAC/EAC” button instead.

④ - Read BAC/EAC

Using this button the GRT tries to read a BAC or EAC protected passport. At first, the MRZ dialog shows up and the user has to enter the MRZ lines of the passport. The access key is derived from this MRZ. The tool automatically identifies if the passport is protected by BAC or by EAC.

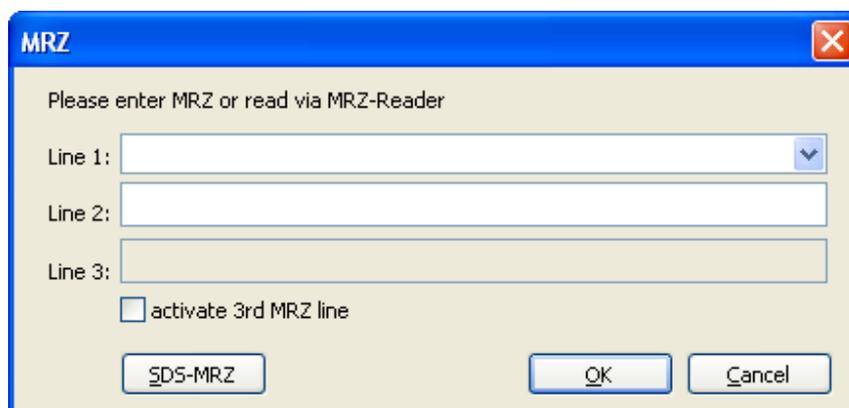


Figure 5: MRZ Dialog

The GRT stores previously entered MRZ lines in the registry to avoid retyping already entered MRZ lines. For ID-Cards with a three-line MRZ the check box “activate 3rd MRZ line” has to be activated. The GRT automatically extracts the required information from the 3rd line.

⑤ - Read from Disk

Using this button the GRT displays the following window where files of binary data groups can be chosen to be read from disk.

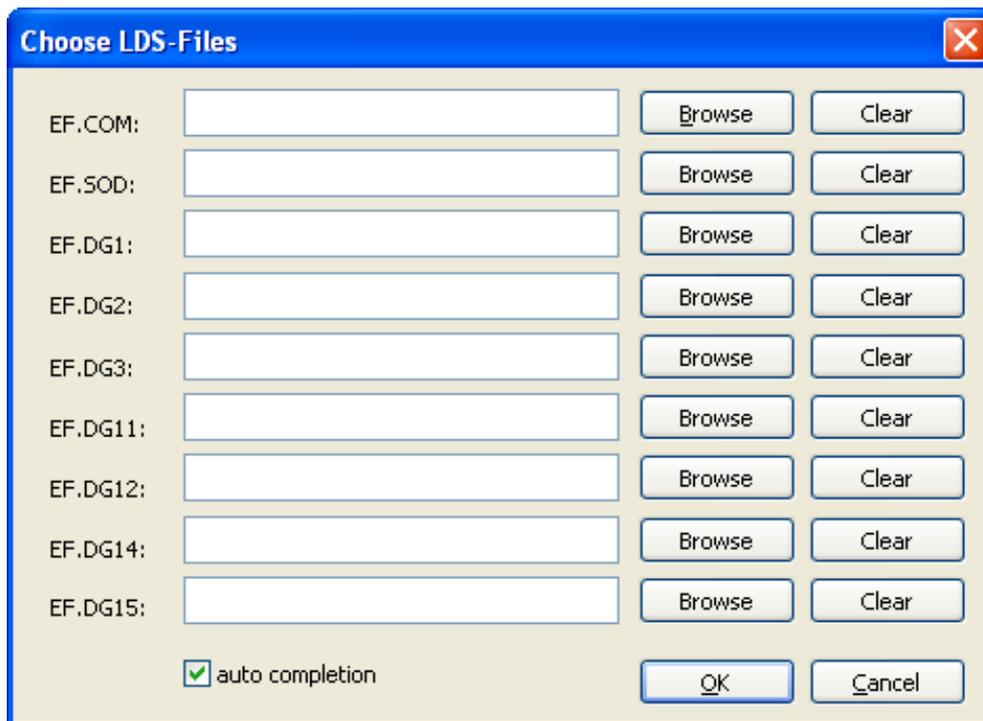


Figure 6: LDS File Dialog

The GRT supports reading the files EF.COM, EF.DG1, EF.DG2, EF.DG3, EF.DG14, EF.DG15 and EF.SOD from disk. The user can enter the filenames directly or use the browse buttons instead. The GRT automatically fills all paths as soon as one filename has been browsed. The GRT uses the same filenames as described in “Write to Disk”. With the “Clear” button a path to a file can be cleared automatically. Empty filenames will not be processed.

⑥ - Write to Disk

Using this button the GRT reads the currently placed passport and writes all data groups found to disk. At first the user has to select a directory where the files will be stored. The GRT proceeds like using the “Autodetect” button; if a BAC or EAC protected passport is found, the MRZ dialog pops up automatically (see 4 - “Read BAC/EAC”, page 7).



Figure 7: Place to store Data groups

Within this chosen directory the GRT automatically stores the following files (if available on the passport). The GRT also extracts some data from the files stored on the passport. The following file names are used:

Filename	Content
Datagroup1.bin	Content of DG1
Datagroup2.bin	Content of DG2
Datagroup3.bin	Content of DG3
Datagroup14.bin	Content of DG14
Datagroup15.bin	Content of DG15
EF_COM.bin	Content of EF_COM
EF_SOD.bin	Content of EF_SOD
DocumentSigner_extr.cer	Document signer certificate extracted from EF_SOD
FaceImage.jpg/.jp2	Face image extracted from DG2
FingerImage*.wsq	Fingerprint images extracted from DG3

* = <number of biometric template>_<number of image>_<position of finger> - (one file for each fingerprint image)

7 - Reset Display

This button sets all display elements to default.

8 - About...

This button shows the dialog with the version number and copyright information.

9 - Options

Here the user can change several settings of the GRT as described below. All settings are saved in the registry and will be still set if the GRT is started again. The Certificates and Key for Terminal Authentication are saved in two files located in the same directory as the executable file.

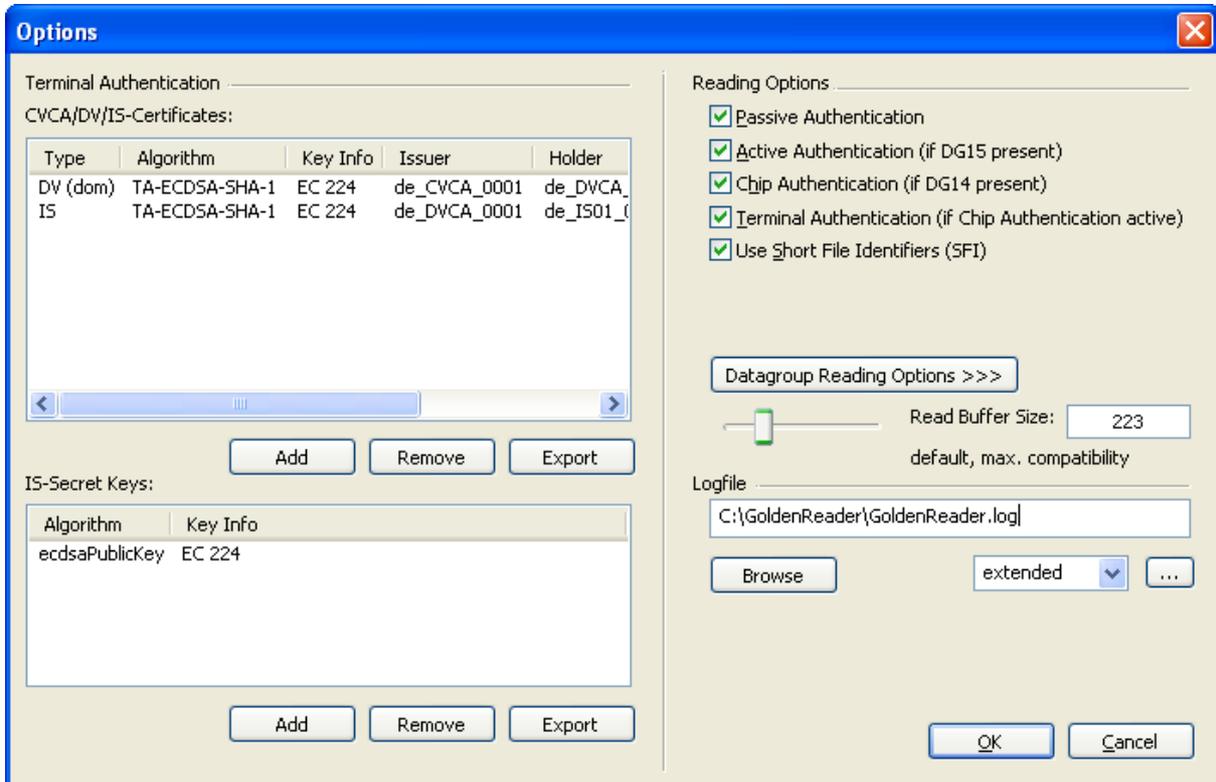


Figure 8: GRT Options

Terminal Authentication

The Terminal Authentication mechanism needs several certificates and keys to be performed correctly ([BSI TR-03110] for technical details). In this part of the dialog these certificates and keys can be imported from files and exported to files. With the “Remove”-button they also can be deleted from the GRT’s certificate list. .

CVCA/DV/IS-Certificates - any number of CV-, DV- and IS-certificates can be imported to this list. For Terminal Authentication at least one DV- and one IS-certificate is needed, for Trust Point Update several CV-certificates may be required (see [BSI TR-03110]). During the Terminal Authentication process, the GRT builds automatically the appropriate certificate chain, based on the information read from the EF.CVCA file.

IS-Secret-Keys - Any number PKCS#8-encoded secret keys can be imported here. However, if multiple keys with the same algorithm and the same size are present, the first one in the list is always used for the Terminal Authentication process.

Reading Options

Passive Authentication – When activated, the GRT reads and checks the signature of the EF.SOD file. It also checks the hash values of the stored data groups. When deactivated, EF.SOD is not read and hash values are not checked. This increases reading speed but reduces security. **Default: Activated**

Active Authentication – When activated and the GRT finds DG15 on the passport, it performs the complete Active Authentication procedure as described in ICAO Technical Report “PKI for Machine Readable Travel Documents offering ICC Read-Only Access“, Version 1.1. If DG15 is not present, the GRT proceeds normally. When deactivated, the Active Authentication mechanism is never performed, regardless if DG15 is present or not.

Default: Activated

Chip Authentication – When activated and the GRT finds DG14 on the passport, it performs the Chip Authentication procedure (first step of the EAC mechanism). If DG14 is not present, the GRT proceeds normally. When deactivated, the Chip Authentication mechanism and Terminal Authentication mechanism are never performed, regardless if DG14 is present or not.

Default: Activated

Terminal Authentication – When activated and the GRT already processed the Chip Authentication on the passport, it performs the Terminal Authentication procedure (second step of the EAC mechanism). If Chip Authentication has not been processed, according to [BSI TR-03110] Terminal Authentication will also be not processed and EAC protected data can not be read. When deactivated, the Terminal Authentication mechanism is never performed, regardless if Chip Authentication had been performed or not. If the passport implements EAC correctly, this case will lead to an error when trying to read EAC protected data groups.

Default: Activated

Use Short File Identifiers (SFI) – Some ePassports do not support the usage of Short File Identifiers (SFIs). To be able to read them nevertheless, SFIs can be deactivated here. It is not recommended to deactivate this setting. ePassports not supporting SFIs do not comply with ICAO Technical Report “Development of a Logical Data Structure – LDS“ Version 1.7!

Default: Activated

Datagroup Reading Options – The GRT by default reads all data groups present on the ePass, which are supported by the GRT. If some of these data groups should not be read, deactivate them in the following dialog.

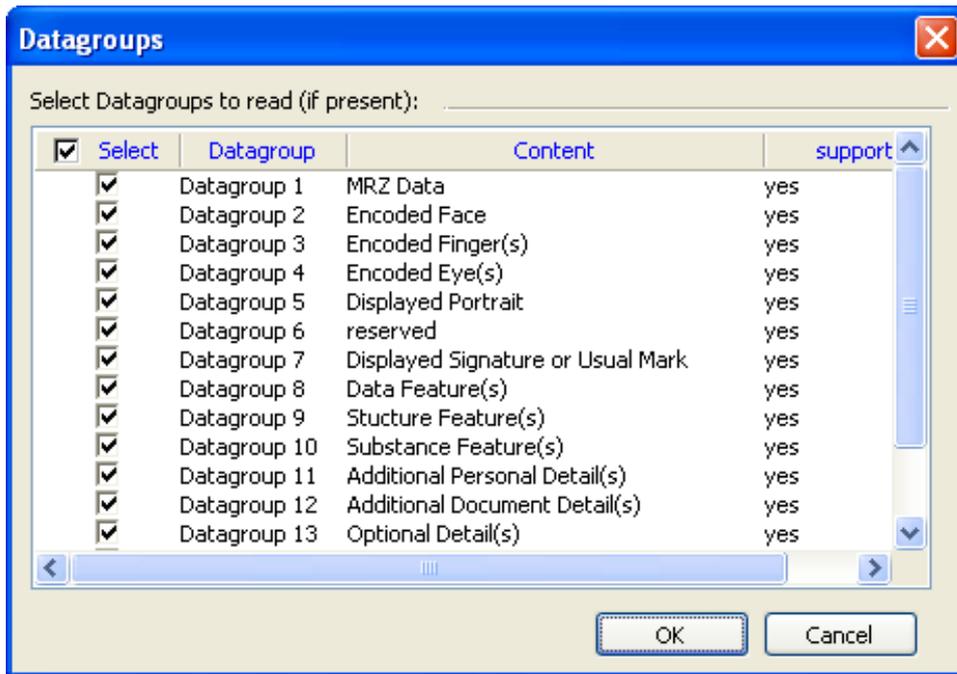


Figure 9: Supported Data groups

Selected data groups will be read, if present. Data groups not supported by the current version of the GRT are grayed.

Read Buffer Size – The size of the buffer used to receive the data read by the Read Binary APDUs can be configured. The default value is 223 which works with most reading devices. However the overall transfer speed can be increased by using larger buffer sizes. Of course this has to be supported by both the reader and the chip. If a buffer size larger than 255 bytes is configured, the extended length mechanism is used by the GRT. **Default: 223**

Logfile

The GRT records several messages in a logfile. This protocol is very extensive because all APDUs are logged. Within this area the logging can be configured and the location for the protocol can be chosen.

Log Sources – The GRT application generates log messages itself and passes on log messages from the ePassport API. Both sources can be selected separately from each other for the logging.

Log Content - There are some predefined log settings (“off”, “brief”, “normal”, “extended”). Via the “...” button, the logging can be configured manually by enabling log lines of a specific type:



Figure 10: Detailed logging options

The following table lists all kind of messages that are logged by GRT:

kind of log messages	log settings required					
	normal				debug	
	config	operations	authentication	performance	keys	APDUs
search for electronic passport reader DLLs	x					
search for optical MRZ reader DLLs	x					
length of APDUs				x		
data of plain APDUs						x
data of encrypted SM-APDUs					x	x
data of decrypted SM-APDUs					x	x
MRZ					x	
BAC keys					x	
BAC result			x			
AA details (algorithm)			x			
AA keys			x		x	
AA result			x			
SM-parameters					x	
performed operations		x				
operation errors		x				
LDS file sizes				x		
LDS file reading times				x		
LDS encoding warnings		x				
LDS encoding errors		x				
results of hash value checks			x			
passive authentication results			x			
CA details (algorithm)			x			
CA keys			x		x	
CA result			x			
TA details (chain, algorithm)			x			
TA keys			x		x	
TA result			x			

10 - Configuration

The “Configuration” dialog includes the management of RF readers and CSCA-certificates.

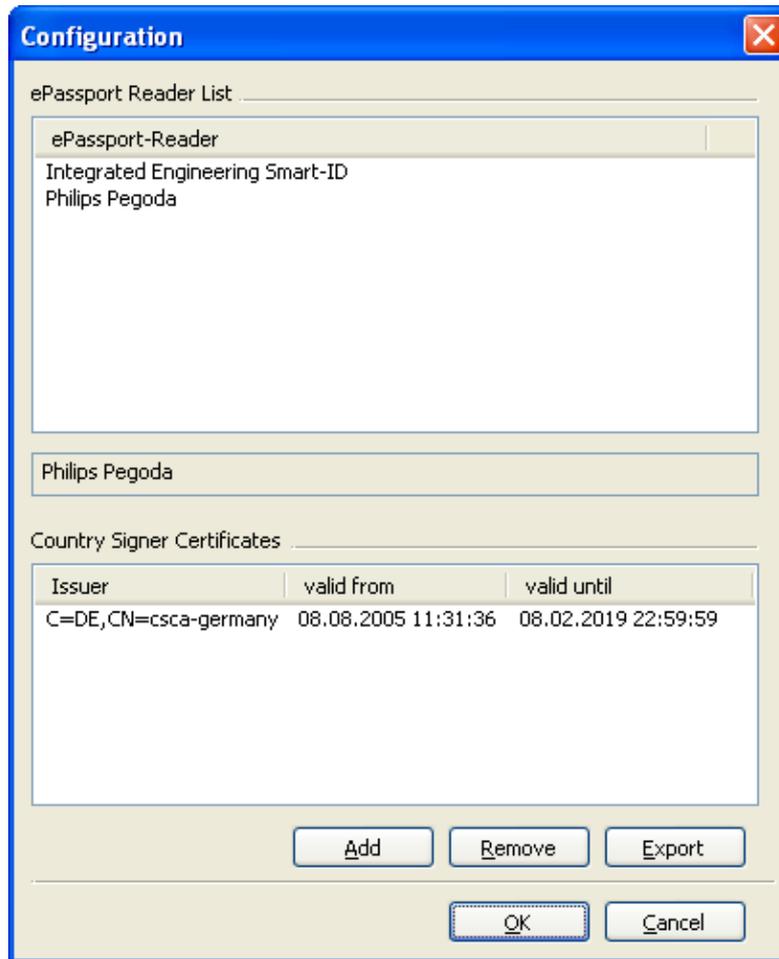


Figure 11: GRT RF Readers

ePassport Reader List – Within this dialog the connected RF Reader which will be used can be selected. The GRT supports the following readers:

- All PC/SC V1.1 compatible readers
- Integrated Engineering Smart ID, native interface
- Philips Pegoda, native interface
- Feig USB Series (Beta)

Country Signer Certificates – Here the certificates used for the certificate chain verification can be managed. For adding country signing certificates use the “Add” button. All der-encoded X.509 certificates are supported. Certificates stored in this list are usually self signed and will be processed as trusted certificates within the check of the certificate chain verification.

Certificates can be removed by the “Remove” button and stored back on disk using the “Export” button.

11 - Close

This button terminates the GRT.

References

- [BSI TR-03110] BSI Technical Report TR-03110, “Advanced security mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC)”, Version 1.01 and 1.1.
- [ICAO Doc 9303] ICAO. Machine readable passport. In Doc 9303, „Machine Readable Travel Documents“, volume 2: Specifications for Electronically Enabled Passports with Biometric Identification Capabilities. ICAO, sixth edition, 2006.
- [ISO/IEC 14443] ISO/IEC 14443, „Identification cards - Contactless integrated circuit(s) cards - Proximity cards“.