Manual

Golden Reader Tool

Implemented by secunet Security Networks AG

based on ePassportAPI

Version 2.7.0

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:
    - PC/SC compatible readers
    - Philips Pegoda
    - Integrated Engineering Smart-ID
    - NMDA Tx-PR-400 series
    - Feig USB Series (Beta)
- Supported MRZ Readers:
    - Rochford Thompson RTE6701 with PS/2 keyboard interface

Main Dialog

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

Figure 1: GRT Main Dialog

Dialog Areas

❶ - Personal Data

Within this area all data stored in data group 1 (DG1) is displayed.

❷ - 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 “Read BAC/EAC”) or submitted by an OCR/Stripe reader (e.g. Rochford Thompson RTE6701). This data does not represent the data stored on the chip.

❸ - 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-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.

❹ - Logging

Within this window the GRT logs several high level messages. A detailed protocol is written to disk (see "Options" button).

❺ - 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 Technical Report "PKI for Machine Readable Travel Documents offering ICC Read-Only Access", Version 1.1.
- **EAC (Extended Access Control)** as described in BSI Technical Report "Advanced security mechanisms for Machine Readable Travel Documents" , Version 0.9.
- **Chip Authentication** as described in BSI Technical Report "Advanced security mechanisms for Machine Readable Travel Documents" , Version 0.9.
- **Terminal Authentication** as described in BSI Technical Report "Advanced security mechanisms for Machine Readable Travel Documents" , Version 0.9.
- **Active Authentication** as described in ICAO Technical Report "PKI for Machine Readable Travel Documents offering ICC Read-Only Access", Version 1.1.

❻ - Passive Authentication

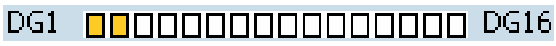
Within this area the status of the passive authentication procedure is displayed (if available). One of the following states is displayed for each element:

	Status not set or processed.
	Status successfully verified.
	Verification of status failed. See protocol file and protocol window for details.

The 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 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

Picture
The picture area displays the picture stored in data group 2 (DG2) and data group 3 (DG3) if present. Use the arrow keys to switch between the different pictures.

Buttons

Within the “Operation” frame several buttons are placed to configure and to use the GRT.

① - Autodetect

Using this button the GRT tries to detect if an unprotected, BAC or EAC protected passport is placed on the reader. If it detects a BAC or EAC protected ePassport, it automatically pops up the MRZ Dialog (see “Read BAC/EAC”).

② - 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.

③ - 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 2: MRZ Dialog

The GRT stores previously entered MRZ lines in the registry to avoid retyping already entered MRZ lines.

④ - Read from Disk

Using this button the GRT reads binary data groups from disk.

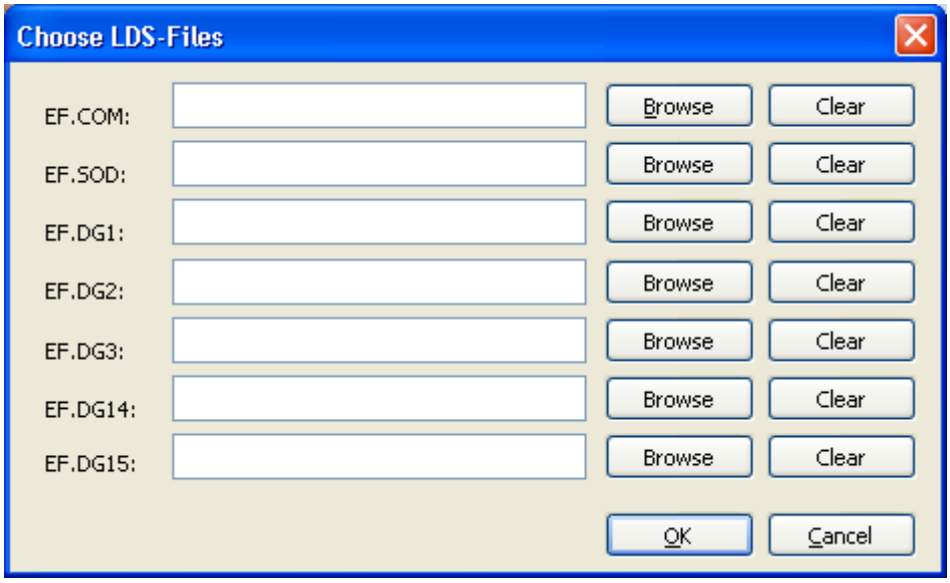


Figure 3: LDS File Dialog

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.

⑤ - 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 have to 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 “Read BAC/EAC”).

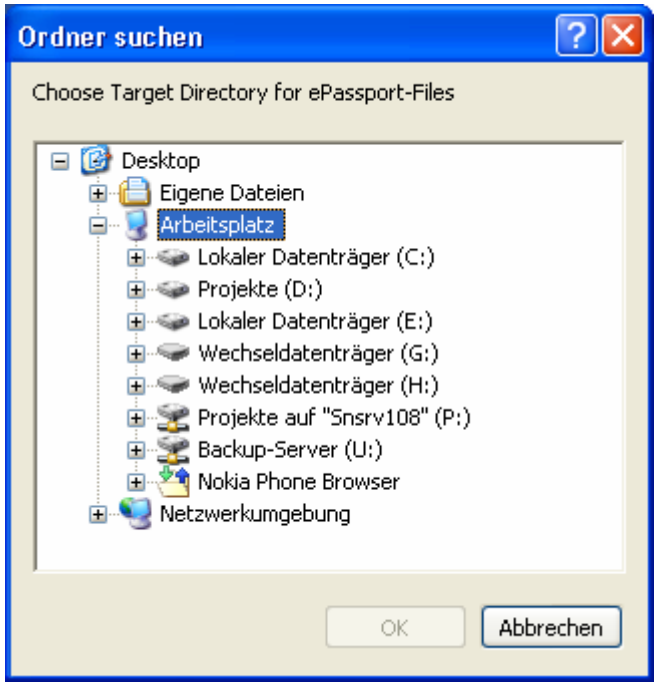


Figure 4: Place to store Datagroups

Within this directory the GRT automatically stores the following files (if available 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

⑥ - Reset Display

This button sets all display elements to default.

⑦ - About…

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

⑧ - Options

Here the user can change several settings of the GRT as described below.

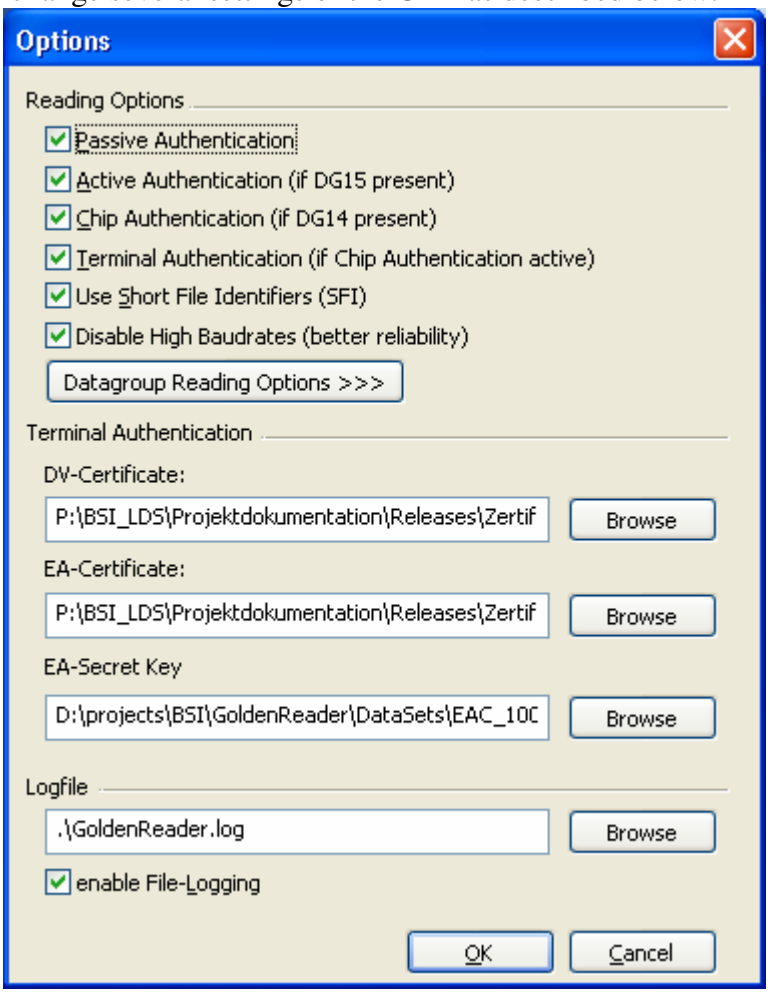


Figure 5: GRT Options

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 authenticaton 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, the GRT proceeds normally. When deactivated, the terminal authentication mechanism is never performed, regardless if chip authentication had been performed or not. Normally 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**

Disable High Baudrates – In some cases and with some readers the GRT supports transfer rates up to 848kbps. If the passport behaves unstable at these high transfer rates, the user can reduce transfer speed by activating this setting. **Default: Deactivated**

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

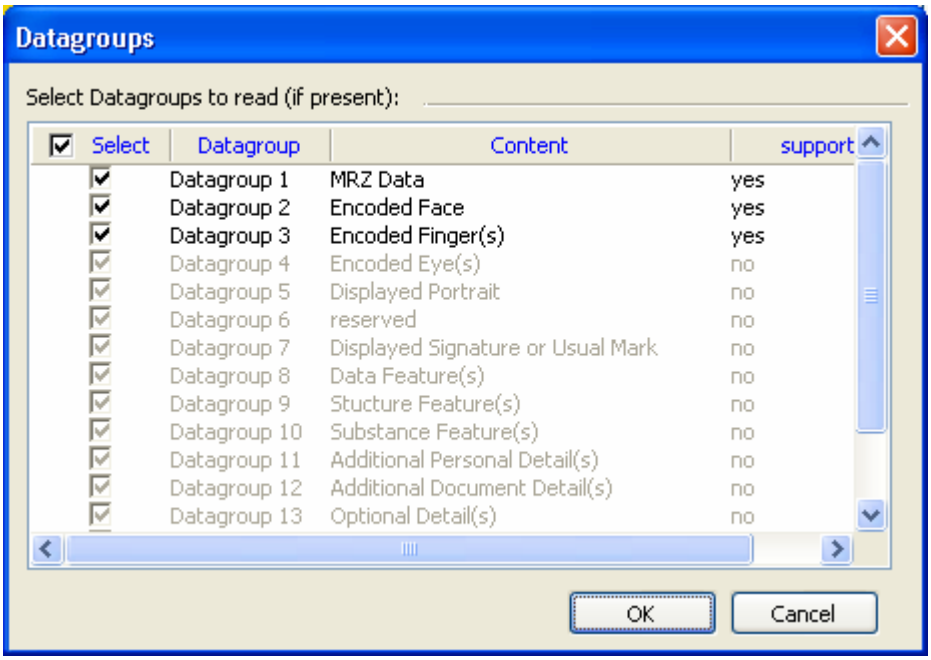


Figure 6: Supported Datagroups

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

Terminal Authentication

The terminal authentication mechanism needs some additional parameters (certificates and keys) to be performed correctly (see BSI Technical Report "Advanced security mechanisms for Machine Readable Travel Documents", Version 0.9, for technical details). These parameters have to be available in separate files. The corresponding file names can be entered within the "Terminal Authentication" section.

DV-Certificate - der-encoded document verifier cv-certificate used for authentication
EA-Certificate - der-encoded extended authentication cv-certificate used for authentication
EA-Secret-Key - PKCS#8-encoded secret key matching ea-certificate for signing the authentication data

Logfile

Logfile – The GRT uses a file to record several messages. This protocol is very extensive because all APDUs are logged. Within this area the logging can be de-/activated and the location for the protocol can be chosen.

⑨ - Configuration

Within this dialog a connected RF reader can be selected and the certificates used for the certificate chain verification can be managed.

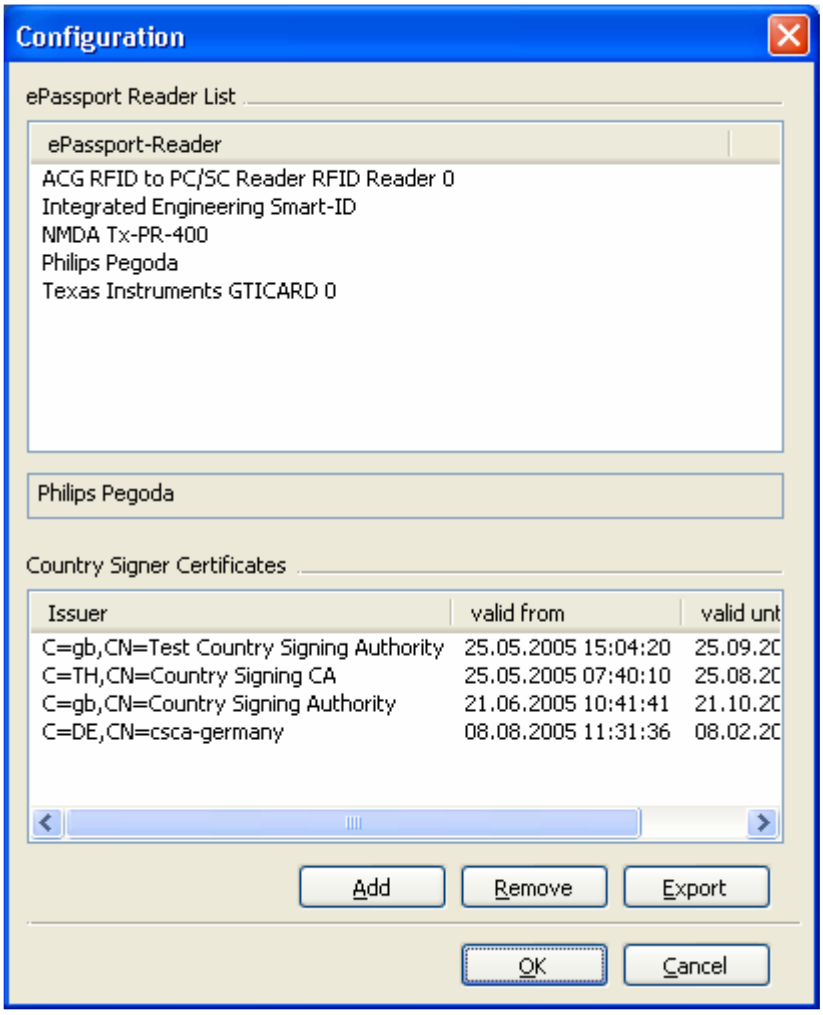


Figure 7: GRT RF Readers

The GRT supports the following readers:

- All PC/SC V1.1 compatible readers
- Integrated Engineering Smart ID, native interface
- NMDA Tx-PR-400 series, native interface
- Philips Pegoda, native interface
- Feig USB Series (Beta)

For adding country sigining certificated 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.

⑩ - Close

This button terminates the GRT.