

# **Release Notes**

## **Golden Reader Tool**



**Version 2.7.3**

**Version 2.7.3 (08.06.2006):**

- bugfix RSA keyhandling in “Terminal Authentication” (EAC)
- several changes from Interop-Test Berlin

**Version 2.7.2 (17.05.2006):**

- bugfix extended Le/Lc handling in secure messaging

**Version 2.7.1 (11.05.2006):**

- bugfix RSA keyhandling in “Terminal Authentication” (EAC)
- support for salt length parameter in RSA-PSS

**Version 2.7.0 (20.04.2006):**

- EAC Version 1.0 support (see TR-03110 for details), final
- selectable Datagroups
- bugfix “Active Authentication” (A4 instead of A6)
- minor bugfixes

**Version 2.6.1 beta (02.02.2006):**

- support for DG3 according to ISO 19794-4 FDIS
- fix Active Authentication to support other cases than  $I^* = J^*$

**Version 2.6.0 (16.01.2006):**

- support for EAC based on EAC-Spec 0.9
- native implementation of FEIG USB reader family (Beta)
- Minor changes from Singapore Testing

EAC specification work is still in progress. EAC implementation is not final!

**Version 2.5.0 (23.09.2005):**

- face lifting of user interface due to new features
- support for new ISO-Face/Finger/Iris-Tags (old ones still supported)
- support for certificate chains
- support for data group 3
- experimental implementation of EAC based on EAC-Spec 0.86b (key-material for Chip-Authentication in DG14)
- minor bug fixes

EAC specification work is still in progress. EAC implementation is not final!

**Version 2.2.0 (14.03.2005):**

- more convenience for MRZ Dialog (stores previously entered MRZ data)
- bug fix when reading invalid or empty data groups
- shortcuts added for convenience with stripe readers (reading procedure is triggered when passport is plunged)
- fixed crash with passports returning invalid size of data within secure messaging
- average real reading speed displayed in log

**Version 2.1.9 (09.03.2005):**

- Bugfixes while testing in Tsukuba (Japan)

**Version 2.1.8 (04.03.2005):**

- Additional shortcuts for ReadBAC

#### **Version 2.1.7 (28.02.2005):**

- Support for some special interpretations of the B1-Read-Binary command (major topic, see below!)
- Changed one error message to be more specific
- Basics for Extended Access control (internal)

We also discovered one major topic which has to be discussed by chip card and chip operating vendors:

The prior GRT had some problems reading certain passport sample with a 34k DG2. Today we received such a passport and were able to find the reason for this problem: The passport handles the ReadBinary command with odd instruction byte (b1) different from the chips we have seen so far. The problem occurs while reading the very last bytes of DG2. If there for example 0x50 bytes left to read, we request 0x52 bytes in the le byte of the ReadBinary command. We do this, because we need 0x50 data bytes and one byte for tag 0x53 and one length byte. One example passport now returns 0x52 data bytes plus an additional tag and length byte, so it returns in total 0x54 bytes. The bug in the GRT was that it doesn't expect to receive more bytes than requested. This issue is fixed now. However, I think we should discuss whether this is legal behaviour.

#### **Version 2.1.6 (25.02.2005):**

- Type B implementation for Philips Pegoda
- Shortcuts for buttons

#### **Version 2.1.5 (22.02.2005):**

- Minor Bugfix in NMDA driver
- new Option (Disable Highspeed) for better reliability (only effects Philips Pegoda at the moment)
- internal support of XML-Parameterset
- bugfix for anticollision with BAC passports
- minor memory leak closed
- UID/ATR/Iso14443-Type display if supported by drivers
- removed some elements out of the package which are not used any more
- removed UT-Version of GRT to keep the package smaller

#### **Version 2.1.2 (16.02.2005):**

- Support for DG15 and Active Authentication
- Anti-collision Support for Philips Pegoda (only!)
- ECC-Bugfix
- SFI-Option active/selectable again
- Optical MRZ will be updated, if entered
- some minor optical changes

#### **Version 2.1.0 (10.02.2005):**

- First tests for AntiCollision with Philips Pegoda

#### **Version 2.0.2 (09.02.2005):**

- Support for RSA-PSS (Japanese Test Set)
- Support for 3 line MRZ data in DG1 (ID Card Netherlands)
- Support for "Australian interpretation" of RSA Signature

- Bugfix in reading card data > 32k
- ECDSA is currently under discussion again. It's implemented but in a different way.

**Version 2.0.0 PublicBeta (28.01.2005):**

- Based on ePassportAPI
- New Design
- The UT-Version is the "Un-Themed"-Version of the Golden Reader, it uses standard dialog items and windows routines. The regular exe is the blue themed dialog shown in London. There are still some optical bugs to fix in the themed dialog version when NOT running it with Windows XP! So if you have any problems with the normal one try the \_UT-Version.

**Version 1.5.7 (07.01.2005):**

- For PC/SC-Readers the number of maximal requested response bytes was wrong. Therefore the tool had problems reading BAC-ePassports with PC/SC driver based reader hardware.

**Version 1.5.5 (09.12.2004):**

- Changes made in Baltimore testing integrated (stability)

**Version 1.5.1 (16.11.2004):**

- Bugfix for some PC/SC drivers

**Version 1.5.0 (12.10.2004):**

- Integration CV-ACT library
- Bugfixing ECDSA

**Version 1.4.3 (16.09.2004):**

- Internal fixes

**Version 1.4.2 (10.09.2004):**

- Bugfixing IE-Reader

**Version 1.4.0 (20.08.2004):**

- Integration IE-Reader
- Integration ECDSA

**Version 1.3.1 (19.08.2004):**

- Bugfixing ACG

**Version 1.3.0 (18.08.2004):**

- Integration of ACG reader (ASCII interface)

**Version 1.1.1 (03.08.2004):**

- display of additional data
- SFI-Usage can be switched on or off
- UID's and ATR/ATS is logged into file
- added different Philips SCComm.dll to avoid reader problems with certain Firmware Versions
- several internal changes

**Version 1.0.0 (09.07.2004):**

- first internal release
- base for Morgantown tests