



EXECUTIVE SUMMARY

T-Systems GEI GmbH, BU ITC Security

Rabinstrasse 8, D-53111 Bonn

GERMANY

confirms the Security Test and Firmware Review
of the Discretix Crypto Coprocessor

developed by

Discretix Technologies Ltd.

43 Hamelacha Street

Beit Etgarim, poleg Industrial Zone, 42502 Netanya

ISRAEL

with the following result:

The firmware has been found to have no major defects and is of very good quality. The security evaluation concludes that the software includes effective and state of the art protection measures (both algorithmic and specific coding) for the handling of cryptographic keys and other security relevant data. See the summary below for minor conspicuousnesses.

The investigated implementation of the cryptographic mechanisms (PKI-engine and DES-engine) are not found to be vulnerable to side channel analysis including simple power analysis (SPA), differential power analysis (DPA), timing analysis (TA) and fault analysis (FA).

The evaluators invested for their investigation several months, high expertise and special equipment. The judgment is based on the assumption that the target hardware guarantees a secure environment.

Product Version

- CryptoCell firmware image date Mar 23 2003 for EVB1_B on CPU: ARM Integrator - ARM940T (ARM), VxWorks: 5.4.1, BSP version: 1.2/1

Methods

Hardware

- The implemented cryptographic mechanisms (PKI-engine and DES-engine) were investigated using side channel analysis including simple power analysis (SPA), differential power analysis (DPA), timing analysis (TA) and fault analysis (FA).
- The physical random number generator (TRNG) was investigated using statistical tests (according to FIPS 140-2, NIST 800-22 and Common Criteria AIS31 P2) as well as analytical tests.

Firmware

- The security functions and mechanisms of the Discretix crypto coprocessor firmware were analysed and checked by a source code evaluation.
- The sources were evaluated using “code walk through”. The identified sensitive routines were analysed completely in a single step (line by line) process.
- The evaluators had access to the complete software of the security module.

General aspects of the investigations

- It was checked that security functions do not have unwanted side effects, they are executable in defined states only, they always finish in a well defined state and that no hidden functionality is implemented.
- It was checked that sensitive information (keys) cannot be compromised in an unintended manner and whether sensitive information is only kept in clear as long as needed and erased afterwards.
- The correct implementation of the access control mechanisms and of the memory management was checked.
- The correct and efficient implementation of the relevant specified security functions was verified. It was checked whether each function checks the boundaries of the memory areas as specified.

Summary side channel analysis

The DES implementation of the ASIC device of Discretix does not leak secret information. Significant correlation on the correct key values could not be found. The test set-up used a special software that triggers the DES execution. The net time used for the analysis was approximately 70 hours.

Both the standard RSA implementation and the CRT RSA implementation of the ASIC device of Discretix did not lead to a significant key disclosure. The test set-up used a special software that allows to load a given RSA key. The net time used for the analysis was approximately 150 hours.

The cornerstone of the elliptic curve cryptography (ECC) implementation is the scalar multiplication of a curve point where the scalar is secret and the point consisting of two coordinates is publicly known. The analysis was carried out with known scalar. **By SPA it was only possible to reveal the structure and some data dependent details of the implemented algorithm, but not the secret scalar itself.**

The evaluators got hints from the power trace to look on the probable ECC calculation area but did not succeed in finding proofs for it. The significance of the found signals is unclear. Since there is no fixed secret key, DPA is not applicable.

The test set-up used a special software that triggers the ECC execution. The net time used for the analysis was approximately 150 hours.

All measurements were carried out directly at the core voltage of the ASIC. The price of the whole equipment used was EURO 30.000,-.

Summary TRNG analysis

The statistical distribution of the physical random number generator (sources RND0 and RND1 of the ASIC device) differs significantly from the equal distribution.

The design of the Discretix pseudo random number generator is cryptographically strong. The loss of seed entropy does not allow an attacker to gain useful information about the resulting pseudo random numbers.

Summary firmware review

The firmware is of good quality. It is well structured and the cryptographic core functionality is implemented efficiently and secure.

The evaluators did not find any firmware code part which could disclose or modify sensitive data by software malfunction.

Within the cryptographic calculation routines no security risk was found. There are effective countermeasures implemented against SPA/DPA, TA and FA.

But note that the following functions could be exposed to side channel analysis and/or related attacks:

- **The implementation of the PIN check is potentially vulnerable to glitch attacks. The evaluators recommend a re-implementation of the PIN check.**

With the following functions no actual risk was found but there could be a potential risk:

- The comparison of two long numbers is not time invariant.
- A block wise copy function is used for copying sensitive data and might be used to learn the Hamming weight of secret PKI keys in the target environment (the evaluators did not succeed with this on the evaluation board).

Remarks

It was not the aim of the evaluation to prove the correctness of the overall functionality or the absence of all undesired side effects. This evaluation rather aims to detect flaws or errors that could be used for attacks against the security of the system.

The complete results of the evaluation can be found in the following reports:

Security Test and Firmware Review of the Discretix Crypto Coprocessor, Part 1, Hardware Random Number Generator,- Version 1.0 -, T-Systems GEI GmbH, January 31, 2003.

Security Review, Topic: Discretix Random Number Generator, Properties of the ANSI X.931 – 1998 pseudo random number generator using the Discretix RNG seeding, T-Systems GEI GmbH, May 22, 2003

Security Test and Firmware Review of the Discretix Crypto Coprocessor, Part 2, Side Channel Analysis of the DES and RSA Implementation, - Version 1.0 -, T-Systems GEI GmbH, April 01, 2003

Security Test and Firmware Review of the Discretix Crypto Coprocessor, Part 3, Side Channel Analysis of the ECC Implementation, - Version 1.1 -, T-Systems GEI GmbH, May 13, 2003

Security Test and Firmware Review of the Discretix Crypto Coprocessor, Part 4, Firmware Review, - Version 1.0 -, T-Systems GEI GmbH, August 12, 2003

Bonn, 12th August 2003

T-Systems GEI GmbH, BU ITC Security

The evaluators

Joachim Klein

Guntram Wicke