
GlobalPlatform Card Card Benchmark

Version 1.0

Member Release

July 1, 2007

Document Reference: GPC_GUI_008



Copyright © 2007 GlobalPlatform Inc. All Rights Reserved.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights or other intellectual property rights of which they may be aware which might be infringed by the implementation of the specification set forth in this document, and to provide supporting documentation. The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Table of contents

1. INTRODUCTION

- 1.1. EXECUTIVE SUMMARY
- 1.2. NORMATIVE REFERENCES
- 1.3. TERMINOLOGY AND DEFINITIONS
- 1.4. ABBREVIATIONS AND NOTATIONS
- 1.5. CONVENTIONS

2. EXECUTION SPEED EVALUATION

- 2.1. GENERAL COMMENTS
- 2.2. IMPLEMENTATION

3. RESPONSE TIMING FUNCTIONALITY

DESCRIPTION

- 3.1. GET
- 3.2. PUT
- 3.3. PUTGET

4. GP PROCESSING PERFORMANCE

- 4.1. TEST APPLET DESCRIPTION
- 4.2. INITIALIZE
- 4.3. PROCESSING_PERFORMANCE
- 4.4. FACTORIAL
- 4.5. PRIME_NUMBER
- 4.6. SUM
- 4.7. LOOP_WHILE
- 4.8. LOOP_FOR
- 4.9. LOOP_DO_WHILE
- 4.10. ARRAY_FILLNONATOMIC
- 4.11. ARRAY_COPYNONATOMIC
- 4.12. ARRAY_FILLPAGESIZE

5. GLOBALPLATFORM IMPLEMENTATION CHARACTERISTICS BENCHMARK

TEST APPLET DESCRIPTION

- 5.1. TXBUF_RAW TRANSACTION BUFFER SIZE RAW
- 5.2. TXBUF_BYTE TRANSACTION BUFFER SIZE FOR BYTES
- 5.3. TXBUF_SHORT TRANSACTION BUFFER SIZE FOR SHORTS
- 5.4. JAVA_STACK_1
- 5.5. JAVA_STACK_2

6. GP CRYPTO BENCHMARK

TEST APPLET DESCRIPTION

- 6.1. INITIALIZE
- 6.2. ENCRYPT_DES
- 6.3. ENCRYPT_3DES
- 6.4. DECRYPT_DES
- 6.5. DECRYPT_3DES
- 6.6. CALC_MAC_DES

Copyright © 2007 GlobalPlatform Inc. All Rights Reserved.

The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

- 6.7. CALC_RETAIL_MAC_3DES
- 6.8. CALC_MAC_3DES
- 6.9. PRIV_RSA_512
- 6.10. PUB_RSA_512
- 6.11. PRIV_RSA_1024
- 6.12. PUB_RSA_1024
- 6.13. SIGN_RSA_PKCS1
- 6.14. KEY_GEN_RSA_1024

7. GP API V2.1.1 BENCHMARK

TEST APPLET DESCRIPTION

- 7.1. GP_INIT_UPDATE
- 7.2. GP_EXT_AUTH
- 7.3. GP_DECRYPT
- 7.4. GP_ENCRYPT
- 7.5. GP_UNWRAP_DECRYPT
- 7.6. GP_WRAP

8. GP API V2.0.1' BENCHMARK

TEST APPLET DESCRIPTION

- 8.1. GP_INIT_UPDATE
- 8.2. GP_EXT_AUTH
- 8.3. GP_DECRYPT_VERIFY_KEY
- 8.4. GP_UNWRAP
- 8.5. GP_CLOSE

9. PACKAGE GPIMPLEMENTATIONCHARACTERISTICS

10. PACKAGE GPPROCESSINGPERFORMANCE

11. PACKAGE GPIMPLEMENTATIONCHARACTERISTICS

12. PACKAGE GPCRYPTOBENCHMARK

13. PACKAGE GPAPI211ERROR! BOOKMARK NOT DEFINED.

14. PACKAGE GPAPI201