BK Profiling Report

This product is subject to EU export restrictions according to Council Regulation (EC) No. 428/2009, dual-use control category 5D002.

BK v2.8.2

Doc version 1.1
Status Approved
Reference IID-BK-PR

For internal use by customer only

Confidential

www.intrinsic-id.com

This product is subject to EU export restrictions according to Council Regulation (EC) No. 428/2009, dual-use control category 5D002.

This document contains information which is proprietary and confidential to Intrinsic ID B.V. and is intended for internal use only. The document is provided with the express understanding that the recipient will not divulge its content to other parties or otherwise misappropriate the information contained herein. Please destroy this document if you are not the intended recipient. Thank you.

Overview

This document contains the profiling results of BK v2.8.2 for several of its configurations on a variety of embedded platforms. The table of contents below provides links to the dedicated sections for these combinations.

Table of Contents

1. Platform STM32L476RG-NUCLEO (M4)

Device	STM32L476RG-NUCLEO
Core	M4
Compiler	arm gcc
Branch	feature/BK-1986
Commit	989f3088556b8c65e7f6082edf0d089bd1f04333
Timestamp	2020-10-27 - 07:22

1.1. Configuration Pro-256

Core	Cortex-M4
Flavor	Pro-256 (intl.ref: pki_256)
Code Size	20.0 kBytes

Function Profiling

Function	Cycle count	Stack (Bytes)	Remark
bk_compute_public_from_private_key	2718824	1312	
bk_create_csr	5388250	1504	
bk_create_private_key	235433	1064	
bk_create_selfsigned_certificate	5408437	1512	
bk_derive_public_key	2423989	1048	P256
bk_ecdh_shared_secret	2720649	1328	
bk_ecdsa_sign	2936744	1552	
bk_ecdsa_verify	3026521	1744	
bk_enroll	401373	1784	
bk_generate_cryptogram	5259659	1680	
bk_generate_random	78036	616	32
bk_get_key	28797	712	S_256
bk_get_private_key	127204	936	P256 RANDOM
bk_get_public_key_from_cryptogram	579	28	
bk_init	99520	624	
bk_process_cryptogram	2825570	1552	
bk_start	545044	1936	
bk_stop	254	8	
bk_unwrap	125127	1184	
bk_wrap	125312	840	

1.2. Configuration Plus-256

Core	Cortex-M4
Flavor	Plus-256 (intl.ref: plus_256)
Code Size	8.4 kBytes

Function Profiling

Function	Cycle count	Stack (Bytes)	Remark
bk_enroll	402167	1776	
bk_generate_random	78280	616	32
bk_get_key	28864	712	S_256
bk_get_private_key	137976	1016	P256 RANDOM
bk_init	99598	624	
bk_start	545902	1928	
bk_stop	254	8	
bk_unwrap	125390	1168	
bk_wrap	125605	800	

1.3. Configuration Safe-256

Core	Cortex-M4
Flavor	Safe-256 (intl.ref: safe_256)
Code Size	6.8 kBytes

Function Profiling

Function	Cycle count	Stack (Bytes)	Remark
bk_enroll	373843	1736	
bk_generate_random	78292	616	32
bk_get_key	29046	712	S_256
bk_get_private_key	137951	1016	P256 RANDOM
bk_init	99598	624	
bk_start	515390	1888	
bk_stop	180	8	

1.4. Configuration Pro-128

Core	Cortex-M4
Flavor	Pro-128 (intl.ref: pki_128)
Code Size	19.9 kBytes

Function Profiling

Function	Cycle count	Stack (Bytes)	Remark
bk_compute_public_from_private_key	2687391	1208	
bk_create_csr	5370679	1400	
bk_create_private_key	221591	1064	
bk_create_selfsigned_certificate	5371025	1408	
bk_derive_public_key	2421616	1056	P256
bk_ecdh_shared_secret	2683543	1224	
bk_ecdsa_sign	2928427	1448	
bk_ecdsa_verify	3054498	1640	
bk_enroll	294493	1432	
bk_generate_cryptogram	5208337	1576	
bk_generate_random	78338	624	32
bk_get_key	24251	704	S_128
bk_get_private_key	127274	936	P256 RANDOM
bk_get_public_key_from_cryptogram	642	28	
bk_init	69874	616	
bk_process_cryptogram	2793392	1448	
bk_start	395365	1544	
bk_stop	157	8	
bk_unwrap	117541	1080	
bk_wrap	117735	816	

1.5. Configuration Plus-128

Core	Cortex-M4
Flavor	Plus-128 (intl.ref: plus_128)
Code Size	8.5 kBytes

Function Profiling

Function	Cycle count	Stack (Bytes)	Remark
bk_enroll	293795	1424	
bk_generate_random	78052	616	32
bk_get_key	24173	696	S_128
bk_get_private_key	137365	1008	P256 RANDOM
bk_init	69846	616	
bk_start	394557	1536	
bk_stop	158	8	
bk_unwrap	117091	1096	
bk_wrap	117313	808	

1.6. Configuration Safe-128

Core	Cortex-M4
Flavor	Safe-128 (intl.ref: safe_128)
Code Size	6.8 kBytes

Function Profiling

Function	Cycle count	Stack (Bytes)	Remark
bk_enroll	269972	1392	
bk_generate_random	78039	616	32
bk_get_key	24161	688	S_128
bk_get_private_key	137321	1008	P256 RANDOM
bk_init	69838	616	
bk_start	371788	1504	
bk_stop	115	8	

2. Platform STM32F207ZG-NUCLEO (M3)

Device	STM32F207ZG-NUCLEO
Core	M3
Compiler	arm gcc
Branch	feature/BK-1986
Commit	989f3088556b8c65e7f6082edf0d089bd1f04333
Timestamp	2020-10-27 - 07:22

2.1. Configuration Pro-256

Core	Cortex-M3
Flavor	Pro-256 (intl.ref: pki_256)
Code Size	20.9 kBytes

Function Profiling

Function	Cycle count	Stack (Bytes)	Remark
bk_compute_public_from_private_key	5115829	1320	
bk_create_csr	10215332	1512	
bk_create_private_key	256369	1064	
bk_create_selfsigned_certificate	10236384	1520	
bk_derive_public_key	4800634	1048	P256
bk_ecdh_shared_secret	5119918	1336	
bk_ecdsa_sign	5383688	1560	
bk_ecdsa_verify	5755857	1752	
bk_enroll	421335	1784	
bk_generate_cryptogram	10043620	1688	
bk_generate_random	81816	616	32
bk_get_key	30651	712	S_256
bk_get_private_key	140480	936	P256 RANDOM
bk_get_public_key_from_cryptogram	654	28	
bk_init	106197	616	
bk_process_cryptogram	5230718	1560	
bk_start	683219	1936	
bk_stop	255	8	
bk_unwrap	132635	1192	
bk_wrap	132836	840	

2.2. Configuration Plus-256

Core	Cortex-M3
Flavor	Plus-256 (intl.ref: plus_256)
Code Size	8.3 kBytes

Function Profiling

Function	Cycle count	Stack (Bytes)	Remark
bk_enroll	422111	1776	
bk_generate_random	82047	616	32
bk_get_key	30717	712	S_256
bk_get_private_key	153042	1016	P256 RANDOM
bk_init	106276	616	
bk_start	682278	1928	
bk_stop	255	8	
bk_unwrap	132888	1168	
bk_wrap	133106	800	

2.3. Configuration Safe-256

Core	Cortex-M3
Flavor	Safe-256 (intl.ref: safe_256)
Code Size	6.7 kBytes

Function Profiling

Function	Cycle count	Stack (Bytes)	Remark
bk_enroll	392817	1736	
bk_generate_random	82041	616	32
bk_get_key	30904	712	S_256
bk_get_private_key	153004	1016	P256 RANDOM
bk_init	106278	616	
bk_start	654775	1888	
bk_stop	182	8	

2.4. Configuration Pro-128

Core	Cortex-M3
Flavor	Pro-128 (intl.ref: pki_128)
Code Size	20.9 kBytes

Function Profiling

Function	Cycle count	Stack (Bytes)	Remark
bk_compute_public_from_private_key	5134544	1216	
bk_create_csr	10298911	1408	
bk_create_private_key	240779	1064	
bk_create_selfsigned_certificate	10297723	1416	
bk_derive_public_key	4851959	1064	P256
bk_ecdh_shared_secret	5131860	1232	
bk_ecdsa_sign	5424026	1456	
bk_ecdsa_verify	5881039	1648	
bk_enroll	308821	1432	
bk_generate_cryptogram	10092851	1584	
bk_generate_random	82142	632	32
bk_get_key	25672	704	S_128
bk_get_private_key	140252	944	P256 RANDOM
bk_get_public_key_from_cryptogram	718	28	
bk_init	74560	616	
bk_process_cryptogram	5248377	1456	
bk_start	487971	1544	
bk_stop	159	8	
bk_unwrap	124225	1088	
bk_wrap	124440	824	

2.5. Configuration Plus-128

Core	Cortex-M3
Flavor	Plus-128 (intl.ref: plus_128)
Code Size	8.4 kBytes

Function Profiling

Function	Cycle count	Stack (Bytes)	Remark
bk_enroll	308084	1424	
bk_generate_random	81835	624	32
bk_get_key	25590	696	S_128
bk_get_private_key	152387	1016	P256 RANDOM
bk_init	74531	616	
bk_start	488333	1536	
bk_stop	159	8	
bk_unwrap	123758	1104	
bk_wrap	123989	816	

2.6. Configuration Safe-128

Core	Cortex-M3
Flavor	Safe-128 (intl.ref: safe_128)
Code Size	6.7 kBytes

Function Profiling

Function	Cycle count	Stack (Bytes)	Remark
bk_enroll	283397	1392	
bk_generate_random	81828	624	32
bk_get_key	25590	688	S_128
bk_get_private_key	152349	1016	P256 RANDOM
bk_init	74530	616	
bk_start	462141	1504	
bk_stop	118	8	

3. Platform STM32_B-L072Z-LRWAN1 (M0+)

Device	STM32_B-L072Z-LRWAN1
Core	M0+
Compiler	arm gcc
Branch	feature/BK-1986
Commit	989f3088556b8c65e7f6082edf0d089bd1f04333
Timestamp	2020-10-27 - 07:22

3.1. Configuration Pro-256

Core	CORTEX-M0+
Flavor	Pro-256 (intl.ref: pki_256)
Code Size	19.8 kBytes

Function Profiling

Function	Cycle count	Stack (Bytes)	Remark
bk_compute_public_from_private_key	12974729	1344	
bk_create_csr	25771456	1528	
bk_create_private_key	348080	1088	
bk_create_selfsigned_certificate	25799304	1528	
bk_derive_public_key	12514125	1072	P256
bk_ecdh_shared_secret	12984533	1360	
bk_ecdsa_sign	13221207	1576	
bk_ecdsa_verify	14565815	1768	
bk_enroll	582094	1776	
bk_generate_cryptogram	25679496	1696	
bk_generate_random	115456	632	32
bk_get_key	43505	720	S_256
bk_get_private_key	173485	1008	P256 RANDOM
bk_get_public_key_from_cryptogram	765	48	
bk_init	149140	608	
bk_process_cryptogram	13153032	1576	
bk_start	918023	1944	
bk_stop	364	16	
bk_unwrap	199530	1224	
bk_wrap	199671	864	

3.2. Configuration Plus-256

Core	CORTEX-M0+
Flavor	Plus-256 (intl.ref: plus_256)
Code Size	8.5 kBytes

Function Profiling

Function	Cycle count	Stack (Bytes)	Remark
bk_enroll	582065	1768	
bk_generate_random	115428	632	32
bk_get_key	43498	720	S_256
bk_get_private_key	187666	1072	P256 RANDOM
bk_init	149150	616	
bk_start	917956	1936	
bk_stop	364	16	
bk_unwrap	199423	1192	
bk_wrap	199566	808	

3.3. Configuration Safe-256

Core	CORTEX-M0+
Flavor	Safe-256 (intl.ref: safe_256)
Code Size	6.9 kBytes

Function Profiling

Function	Cycle count	Stack (Bytes)	Remark
bk_enroll	538660	1736	
bk_generate_random	115415	632	32
bk_get_key	45197	720	S_256
bk_get_private_key	187652	1024	P256 RANDOM
bk_init	149150	616	
bk_start	874551	1904	
bk_stop	258	16	

3.4. Configuration Pro-128

Core	CORTEX-M0+
Flavor	Pro-128 (intl.ref: pki_128)
Code Size	19.7 kBytes

Function Profiling

Function	Cycle count	Stack (Bytes)	Remark
bk_compute_public_from_private_key	12941876	1248	
bk_create_csr	25767051	1432	
bk_create_private_key	326628	1064	
bk_create_selfsigned_certificate	25770890	1432	
bk_derive_public_key	12522267	1072	P256
bk_ecdh_shared_secret	12945678	1264	
bk_ecdsa_sign	13217205	1480	
bk_ecdsa_verify	14804564	1672	
bk_enroll	427382	1424	
bk_generate_cryptogram	25635697	1600	
bk_generate_random	115480	632	32
bk_get_key	36203	696	S_128
bk_get_private_key	173130	992	P256 RANDOM
bk_get_public_key_from_cryptogram	765	48	
bk_init	104729	616	
bk_process_cryptogram	13121048	1480	
bk_start	661657	1544	
bk_stop	232	16	
bk_unwrap	187803	1128	
bk_wrap	188101	832	

3.5. Configuration Plus-128

Core	CORTEX-M0+
Flavor	Plus-128 (intl.ref: plus_128)
Code Size	8.4 kBytes

Function Profiling

Function	Cycle count	Stack (Bytes)	Remark
bk_enroll	427359	1424	
bk_generate_random	115464	632	32
bk_get_key	36198	696	S_128
bk_get_private_key	185560	1064	P256 RANDOM
bk_init	104731	632	
bk_start	661619	1544	
bk_stop	232	16	
bk_unwrap	187719	1136	
bk_wrap	187998	816	

3.6. Configuration Safe-128

Core	CORTEX-M0+
Flavor	Safe-128 (intl.ref: safe_128)
Code Size	6.8 kBytes

Function Profiling

Function	Cycle count	Stack (Bytes)	Remark
bk_enroll	391670	1392	
bk_generate_random	115451	632	32
bk_get_key	37059	696	S_128
bk_get_private_key	185507	1016	P256 RANDOM
bk_init	104458	632	
bk_start	626122	1512	
bk_stop	168	16	