Freescale Semiconductor
White Paper

Document Number: FSLNISTCAVP
Rev. 1.9, 03/2017

NIST Cryptographic Algorithm Validation Program (CAVP) Certifications for Freescale Cryptographic Accelerators

This document provides a consolidated list of the Cryptographic Algorithm Validation Program (CAVP) certificates obtained by the Freescale/NXP hardware crypto acceleration blocks used in PowerQUICC and QorIQ integrated communications processors as well as StarCore digital signal processors.

All products covered by this document are owned by NXP, however certificates earned under the Freescale name continue to be listed as Freescale products, while certificates earned since NXP's acquisition of Freescale are listed as NXP products.

These hardware accelerators, documented as execution units (EUs) in older products and as crypto-hardware accelerators (CHAs) in more recent devices, define the cryptographic boundary for the purposes of CAVP certification.

OEMs pursuing Cryptographic Module Validation Program (CMVP) certification on modules using Freescale/NXP devices to perform cryptographic functions may reference the Freescale/NXP's CAVP certificates in Section 1, "Certificates of validation for Freescale/NXP devices." However, it is important to note that the National Institute of Standards and Technology (NIST) requires a rationale for

Contents

freescale™

algorithm testing that is not performed on the actual cryptographic module.

For details on these requirements, see the *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program.*

NXP recommends that module developers work with their CMVP testing lab to document an acceptable rationale.

1 Certificates of validation for Freescale/NXP devices

Use the table below to locate specific certificates in this section.

Table 1. Certificates of validation for Freescale devices

Standard	Access the validated implementations (Freescale devices)	Validation number(s)
Triple DES (3DES)	csrc.nist.gov/groups/STM/cavp/documents/des/tripledesnewval.html	• 757 • 758 • 1075 • 2133 • 2378
Advanced Encryption Standard (AES)	csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html	• 962 • 1645 • 1648 • 1649 • 2490 • 2491 • 2492 • 3868 • 3869 • 3870
Secure Hash Standard (SHS)	csrc.nist.gov/groups/STM/cavp/documents/shs/shaval.htm	• 933 • 934 • 1446 • 1455 • 2108 • 2109 • 2110 • 2111 • 2112 • 3187 • 3188 • 3189 • 3192
Keyed-Hash Message Authentication Code (HMAC)	csrc.nist.gov/groups/STM/cavp/documents/mac/hmacval.html	• 537 • 538 • 967 • 1532 • 1533 • 1534 • 2511 • 2512 • 2515

Table 1. Certificates of validation for Freescale devices (continued)

Standard	Access the validated implementations (Freescale devices)	Validation number(s)
Random Number Generator (RNG)	csrc.nist.gov/groups/STM/cavp/documents/rng/rnghistoricalval.html	• 544 • 818
Deterministic Random Bit Generators (DRBG)	csrc.nist.gov/groups/STM/cavp/documents/drbg/drbgnewval.html	• 94 • 348 • 349 • 1101
RSA algorithms (RSA)	csrc.nist.gov/groups/STM/cavp/documents/dss/rsanewval.html	• 465 • 466 • 813 • 1428 • 1429 • 1430 • 1431 • 1432 • 1433 • 1434 • 2398 • 2399 • 2400 • 2401 • 2402
	csrc.nist.gov/groups/STM/cavp/documents/dss/dsanewval.html	• 516 • 769 • 770 • 771 • 772 • 773 • 774 • 775 • 1179 • 1180 • 1181 • 1182 • 1183

Table 1. Certificates of validation for Freescale devices (continued)

Standard	Access the validated implementations (Freescale devices)	Validation number(s)
DSA Certificate 775	csrc.nist.gov/groups/STM/cavp/documents/dss/ecdsanewval.html	• 209 • 418 • 419 • 420 • 421 • 422 • 423 • 424 • 1064 • 1065 • 1066 • 1067 • 1068
Key agreement and key derivation functions	csrc.nist.gov/groups/STM/cavp/documents/components/componentnewval.html	• 271 • 273 • 275 • 277 • 279 • 281 • 283 • 272 • 274 • 276 • 278 • 280 • 282 • 284 • 1119 • 1121 • 1123 • 1125 • 1127 • 1118 • 1120 • 1122 • 1124 • 1126

1.1 Triple DES (3DES)

Table 2. 3DES Certificate 757

Validation No.	757
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DEU 2.0.0
Operational Environment	Freescale Semiconductor MPC8548E

Validation No.	757
Val.Date	12/18/2008
Description/ Notes	TECB(e/d; KO 1,2); TCBC(e/d; KO 1,2) Freescale's DEU r2.0.0 is included in multiple PowerQUICC integrated communications processors and StarCore DSPs, including: MPC8548E, MPC8547E, MPC8545E, MPC8543E, MPC8568E, MPC8567E, MPC8533E, MPC8544E, MSC8144E, MPC8323E, MPC8321E, MPC8313E, MPC8349EA, MPC8347EA, MPC8343EA, MPC8360E, and MPC8358E.

Table 3. 3DES Certificate 758

Validation No.	758
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DEU 3.0.0
Operational Environment	Freescale Semiconductor MPC8572E
Val.Date	12/18/2008
Description/ Notes	TECB(e/d; KO 1,2) TCBC(e/d; KO 1,2) TOFB(e/d; KO 1,2) Freescale's DEU r3.0.0 is included in multiple PowerQUICC and QorIQ integrated communications processors and StarCore DSPs, including: MPC8379E, MPC8378E, MPC8377E, MPC8572E, MPC8571E, MPC8536E, MPC8315E, MPC8314E, MPC8569E, P2020, P2010, P1020, P1011, P1021, P1012, P1022, P1013, P1024, P1015, P1025, P1016, MSC8156E, and MSC8154E.

Table 4. 3DES Certificate 1075

Validation No.	1075
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DESA 0.0
Operational Environment	Freescale Semiconductor P4080 Rev. 2 silicon

Validation No.	1075
Val.Date	05/24/2011
Description/ Notes	TECB(e/d; KO 1,2) TCBC(e/d; KO 1,2) TOFB(e/d; KO 1,2) TCFB(e/d; KO 1,2; 64b) Freescale's DESA 0.0 is included in multiple QorIQ integrated communications processors, including: P4080 (all silicon revisions), P4040 (all silicon revisions), P5020, P5040 (all silicon revisions), P3041, P2041, P2040, P1010, P1023, T4240 (all silicon revisions), T2080, T1040, and QorIQ Qonverge products B4860, BSC9131, and BSC9132.

Table 5. 3DES Certificate 2133

Validation No.	2133
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DESA 0.1
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	02/12/2016
Description/ Notes	TECB(e/d; KO 1,2) TCBC(e/d; KO 1,2) TOFB(e/d; KO 1,2) TCFB(e/d; KO 1,2; 64b) NXP's DESA 0.1 is included in multiple QorIQ integrated communications processors, including: LS1012A, LS1023A, LS1043A, LS1044A, LS1048A, LS1084A, LS1088A, LS2040A, LS2045,A LS2080A, LS2085A.

Table 6. 3DES Certificate 2378

Validation No.	2378
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DESA 0.2
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	03/06/17
Description/ Notes	TECB(e/d; KO 1,2) TCBC(e/d; KO 1,2) TOFB(e/d; KO 1,2) TCFB(e/d; KO 1,2; 64b) NXP's DESA 0.2 is included in multiple QorIQ integrated communications processors, including: LS1026A, LS1046A, LS2044A, LS2048A, LS2084A, LS2088A.

1.2 Advanced Encryption Standard (AES)

Table 7. AES Certificate 962

Validation No.	962
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	AESU 2.1.5
Operational Environment	Freescale Semiconductor MPC8548E
Val.Date	12/18/2008
Description/ Notes	ECB (e/d; 128,256) CBC(e/d; 128,256); CTR (ext only; 128,256) CCM (KS: 128, 256) – Assoc. Data Len Range: 0 - 32 – Payload Length Range: 1 - 32 – Nonce Length(s): 7, 8, 9, 10, 11, 12, 13 – Tag Length(s): 8, 12, 16 Freescale's AESU r2.1.5 is included in multiple PowerQUICC integrated communications processors and StarCore DSPs, including: MPC8548E, MPC8547E, MPC8545E, MPC8543E, MPC8568E, MPC8567E, MPC8533E, MPC8544E, MSC8144E, MPC8323E, MPC8321E, MPC8313E, MPC8349EA, MPC8347EA, MPC8343EA, MPC8360E, and MPC8358E.

Table 8. AES Certificate 963

Validation No.	963
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	AESU 3.0.0
Operational Environment	Freescale Semiconductor MPC8572E

Validation No.	963
Val.Date	12/18/2008
Description/ Notes	ECB (e/d; 128,256) CBC (e/d; 128,256) CFB128 (e/d; 128,256) OFB (e/d; 128,256) CTR (ext only; 128,256) CCM (KS: 128, 256) – Assoc. Data Len Range: 0 - 32 – Payload Length Range: 1 - 32 – Nonce Length(s): 7, 8, 9, 10, 11, 12, 13 – Tag Length(s): 8, 12, 16 CMAC (Generation/Verification) (KS: 128; Block Size(s) – Msg Len(s) Min: 0 Max: 2^16 – Tag Len(s) Min: 1 Max: 16) (KS: 256; Block Size(s) – Msg Len(s) Min: 0 Max: 2^16 – Tag Len(s) Min: 1 Max: 16) Freescale's AESU r3.0.0 is included in multiple PowerQUICC and QorIQ integrated communications processors and StarCore DSPs, including: MPC8379E, MPC8378E, MPC8377E, MPC8572E, MPC8571E,MPC8315E, and MPC8314E.

The AESU 3.0.0 was later also certified for GCM mode.

Table 9. AES Certificate 1645

Validation No.	1645
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	AESU 3.0.0
Operational Environment	Freescale Semiconductor MPC8572E
Val.Date	05/24/2011
Description/ Notes	GCM (KS: 128,192, 256) - Assoc. Data Len Range (B): 0 - 1024 - Plaintext Length Range (B): 0 - 1024 - IV Length(B): 1-1024 - Tag Length(s) bits: 32, 64, 96, 104, 112, 120, 128 Freescale's AESU 3.0.0 is included in multiple PowerQUICC communications processors, including: MPC8379E, MPC8378E, MPC8377E, MPC8572E, MPC8571E, MPC8315E, and MPC8314E.

Table 10. AES Certificate 1648

Validation No.	1648
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	AESU 3.0.1
Operational Environment	Freescale Semiconductor MPC8569E
Val.Date	05/24/2011
Description/ Notes	ECB(e/d; 128,192, 256) CBC (e/d; 128,192, 256) CFB128 (e/d; 128,192, 256) OFB (e/d; 128,192, 256) CTR (ext only; 128,192, 256) CCM (KS: 128,192, 256) - Assoc. Data Len Range: 0 - 32 - Payload Length Range: 0 - 32 - Nonce Length(s): 7, 8, 9, 10, 11, 12, 13 - Tag Length(s): 4, 6, 8, 10, 12, 14, 16 CMAC (Generation/Verification) (KS: 128, 192, 256; Block Size(s) - Msg Len(s) Min: 0 Max: 2^16 - Tag Len(s) Min: 1 Max: 16) GCM (KS: 128,192, 256) - Assoc. Data Len Range (B): 0 - 1024 - Plaintext Length Range (B): 0 - 1024 - IV Length(B): 1-1024 - Tag Length(s) bits: 32, 64, 96, 104, 112, 120, 128 XTS (KS: 128, 256; Data Unit Sequence Number) Data unit lengths divisible by 128, 256. Not divisible by 64, 192. Data Len(s) Min: 0 Max: 2^16 Freescale's AESU 3.0.1 is included in multiple PowerQUICC and QorIQ communications processors, and StarCore DSPs, including: MPC8536E, MPC8569E, P2020, P2010, P1020, P1011, P1021, P1012, P1022, P1013, P1024, P1015, P1025, P1016, and MSC8156.

Table 11. AES Certificate 1649

Validation No.	1649
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	AESA 4.0
Operational Environment	Freescale Semiconductor P4080 Rev. 2 silicon

Validation No.	1649
Val.Date	05/24/2011
Description/ Notes	ECB(e/d; 128,192, 256) CBC (e/d; 128,192, 256) CFB128 (e/d; 128,192, 256) OFB (e/d; 128,192, 256) CTR (ext only; 128,192, 256) CCM (KS: 128,192, 256) - Assoc. Data Len Range: 0 - 32 - Payload Length Range: 0 - 32 - Nonce Length(s): 7, 8, 9, 10, 11, 12, 13 - Tag Length(s): 4, 6, 8, 10, 12, 14, 16 CMAC (Generation/Verification) (KS: 128, 192, 256; Block Size(s) - Msg Len(s) Min: 0 Max: 2^16 - Tag Len(s) Min: 1 Max: 16) GCM (KS: 128,192, 256) - Assoc. Data Len Range (B): 0 - 1024 - Plaintext Length Range (B): 0 - 1024 - IV Length(B): 1-1024 - Tag Length(s) bits: 32, 64, 96, 104, 112, 120, 128 XTS (KS: 128, 256; Data Unit Sequence Number) Data unit lengths divisible by 128, 256. Not divisible by 64, 192. Data Len(s) Min: 0 Max: 2^16 Freescale's AESA 4.0 is included in multiple QorIQ integrated communications processors, including: P4080 Rev. 2 silicon, P4040 Rev. 2 silicon, P3041, P5020, P2041, P2040, P1010, and P1023.

Table 12. AES Certificate 2490

Validation No.	2490
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	AESA 4.1
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04

Validation No.	2490
Val.Date	06/20/2013
Description/ Notes	ECB (e/d; 128,192, 256) CBC (e/d; 128,192, 256) CFB128 (e/d; 128,192, 256) OFB (e/d; 128,192, 256) CTR (ext only; 128,192, 256) CCM (KS: 128,192, 256) - Assoc. Data Len Range: 0 - 32 - Payload Length Range: 0 - 32 - Nonce Length(s): 7, 8, 9, 10, 11, 12, 13 - Tag Length(s): 4, 6, 8, 10, 12, 14, 16 CMAC (Generation/Verification) (KS: 128, 192, 256; Block Size(s) - Msg Len(s) Min: 0 Max: 2^16 - Tag Len(s) Min: 4 Max: 16) GCM (KS: 128,192, 256) - Assoc. Data Len Range supported (B): 0 - 1024; tested (0, 64, 128, 192, 1024) - Plaintext Length Range supported (B): 0 - 1024; tested (0, 64, 128, 192, 1024) - IV Length supported (B): 1-1024; tested (8, 1024) - Tag Length(s) bits: 32, 64, 96, 112,128 - OtherIVLen_Supported - GMAC_Supported XTS (KS: 128, 256; Data Unit Sequence Number) Data unit lengths divisible by 128, 256. Not divisible by 64, 192. Data Len(s) Min: 0 Max: 2^16 Freescale's AESA 4.1 is included in multiple QorIQ integrated communications processors, including: T4240 Rev. 1 and Rev. 2 silicon, T2080, T1040, and QorIQ Qonverge products B4860, BSC9131, and BSC9132.

Table 13. AES Certificate 2491

Validation No.	2491
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	AESA 4.2
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04

Validation No.	2491
Val.Date	06/20/2013
Description/ Notes	ECB (e/d; 128,192, 256) CBC (e/d; 128,192, 256) CFB128 (e/d; 128,192, 256) OFB (e/d; 128,192, 256) CTR (ext only; 128,192, 256) CCM (KS: 128,192, 256) - Assoc. Data Len Range: 0 - 32 - Payload Length Range: 0 - 32 - Nonce Length(s): 7, 8, 9, 10, 11, 12, 13 - Tag Length(s): 4, 6, 8, 10, 12, 14, 16 CMAC (Generation/Verification) (KS: 128, 192, 256; Block Size(s) - Msg Len(s) Min: 0 Max: 2^16 - Tag Len(s) Min: 4 Max: 16) GCM (KS: 128,192, 256) - Assoc. Data Len Range supported (B): 0 - 1024; tested (0, 64, 128, 192, 1024) - Plaintext Length Range supported (B): 0 - 1024; tested (0, 64, 128, 192, 1024) - IV Length supported (B): 1-1024; tested (8, 1024) - Tag Length(s) bits: 32, 64, 96, 112,128 - OtherIVLen_Supported - GMAC_Supported XTS (KS: 128, 256; Data Unit Sequence Number) Data unit lengths divisible by 128, 256. Not divisible by 64, 192. Data Len(s) Min: 0 Max: 2^16 Freescale's AESA 4.2 is included in multiple QorIQ integrated communications processors, including: P4080 Rev. 3 silicon, and P5040.

Table 14. AES Certificate 2492

Validation No.	2492
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	AESA 4.3
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04

Validation No.	2492
Val.Date	06/20/2013
Description/ Notes	ECB (e/d; 128,192, 256) CBC (e/d; 128,192, 256) CFB128 (e/d; 128,192, 256) OFB (e/d; 128,192, 256) CTR (ext only; 128,192, 256) CCM (KS: 128,192, 256) - Assoc. Data Len Range: 0 - 32 - Payload Length Range: 0 - 32 - Nonce Length(s): 7, 8, 9, 10, 11, 12, 13 - Tag Length(s): 4, 6, 8, 10, 12, 14, 16 CMAC (Generation/Verification) (KS: 128, 192, 256; Block Size(s) - Msg Len(s) Min: 0 Max: 2^16 - Tag Len(s) Min: 4 Max: 16) GCM (KS: 128,192, 256) - Assoc. Data Len Range supported (B): 0 - 1024; tested (0, 64, 128, 192, 1024) - Plaintext Length Range supported (B): 0 - 1024; tested (0, 64, 128, 192, 1024) - IV Length supported (B): 1-1024; tested (8, 1024) - Tag Length(s) bits: 32, 64, 96, 112,128 - OtherIVLen_Supported - GMAC_Supported XTS (KS: 128, 256; Data Unit Sequence Number) Data unit lengths divisible by 128, 256. Not divisible by 64, 192. Data Len(s) Min: 0 Max: 2^16 Freescale's AESA 4.3 is included in the C29x family of security co-processors.

Table 15. AES Certificate 3868

Validation No.	3868
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	AESA 4.6
Operational Environment	Cadence IES 15.10.009 Verilog simulator

Validation No.	3868
Val.Date	02/12/2016
Description/ Notes	ECB (e/d; 128,192, 256) CBC (e/d; 128,192, 256) CFB128 (e/d; 128,192, 256) OFB (e/d; 128,192, 256) CTR (ext only; 128,192, 256) CCM (KS: 128,192, 256) - Assoc. Data Len Range: 0 - 32 - Payload Length Range: 0 - 32 - Nonce Length(s): 7, 8, 9, 10, 11, 12, 13 - Tag Length(s): 4, 6, 8, 10, 12, 14, 16 CMAC (Generation/Verification) (KS: 128, 192, 256; Block Size(s) - Msg Len(s) Min: 0 Max: 2^16 - Tag Len(s) Min: 4 Max: 16) GCM (KS: 128,192, 256) - Assoc. Data Len Range supported (B): 0 - 1024; tested (0, 64, 128, 192, 1024) - Plaintext Length Range supported (B): 0 - 1024; tested (0, 64, 128, 192, 1024) - IV Length supported (B): 1-1024; tested (8, 1024) - Tag Length(s) bits: 32, 64, 96, 112,128 - OtherIVLen_Supported - GMAC_Supported XTS (KS: 128, 256; Data Unit Sequence Number) Data unit lengths divisible by 128, 256. Not divisible by 64, 192. Data Len(s) Min: 0 Max: 2^16 NXP's AESA 4.6 is included in multiple QorIQ integrated communications processors including: LS1020A, LS1021A, LS1022A.

Table 16. AES Certificate 3869

Validation No.	3869
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	AESA 4.7
Operational Environment	Cadence IES 15.10.009 Verilog simulator

Validation No.	3869
Val.Date	02/12/2016
Description/ Notes	ECB (e/d; 128,192, 256) CBC (e/d; 128,192, 256) CFB128 (e/d; 128,192, 256) OFB (e/d; 128,192, 256) CTR (ext only; 128,192, 256) CCM (KS: 128,192, 256) - Assoc. Data Len Range: 0 - 32 - Payload Length Range: 0 - 32 - Nonce Length(s): 7, 8, 9, 10, 11, 12, 13 - Tag Length(s): 4, 6, 8, 10, 12, 14, 16 CMAC (Generation/Verification) (KS: 128, 192, 256; Block Size(s) - Msg Len(s) Min: 0 Max: 2^16 - Tag Len(s) Min: 4 Max: 16) GCM (KS: 128,192, 256) - Assoc. Data Len Range supported (B): 0 - 1024; tested (0, 64, 128, 192, 1024) - Plaintext Length Range supported (B): 0 - 1024; tested (0, 64, 128, 192, 1024) - IV Length supported (B): 1-1024; tested (8, 1024) - Tag Length(s) bits: 32, 64, 96, 112,128 - OtherIVLen_Supported - GMAC_Supported XTS (KS: 128, 256; Data Unit Sequence Number) Data unit lengths divisible by 128, 256. Not divisible by 64, 192. Data Len(s) Min: 0 Max: 2^16 NXP's AESA 4.7 is included in multiple QorIQ integrated communications processors including: T1023, T1024, LS1012A, LS1026A, LS1046A, LS1044A, LS1048A, LS1084A, LS1088A, LS2040A, LS2045A, LS2080A, LS2085A, LS2044A, LS2048A, LS2084A, LS2088A.

Table 17. AES Certificate 3870

Validation No.	3870
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	AESA 4.7.1
Operational Environment	Cadence IES 15.10.009 Verilog simulator

Validation No.	3870
Val.Date	02/12/2016
Description/ Notes	ECB (e/d; 128,192, 256) CBC (e/d; 128,192, 256) CFB128 (e/d; 128,192, 256) OFB (e/d; 128,192, 256) CTR (ext only; 128,192, 256) CCM (KS: 128,192, 256) - Assoc. Data Len Range: 0 - 32 - Payload Length Range: 0 - 32 - Nonce Length(s): 7, 8, 9, 10, 11, 12, 13 - Tag Length(s): 4, 6, 8, 10, 12, 14, 16 CMAC (Generation/Verification) (KS: 128, 192, 256; Block Size(s) - Msg Len(s) Min: 0 Max: 2^16 - Tag Len(s) Min: 4 Max: 16) GCM (KS: 128,192, 256) - Assoc. Data Len Range supported (B): 0 - 1024; tested (0, 64, 128, 192, 1024) - Plaintext Length Range supported (B): 0 - 1024; tested (0, 64, 128, 192, 1024) - IV Length supported (B): 1-1024; tested (8, 1024) - Tag Length(s) bits: 32, 64, 96, 112,128 - OtherIVLen_Supported - GMAC_Supported XTS (KS: 128, 256; Data Unit Sequence Number) Data unit lengths divisible by 128, 256. Not divisible by 64, 192. Data Len(s) Min: 0 Max: 2^16 NXP's AESA 4.7.1 is included in multiple QorIQ integrated communications processors including: LS1023A, LS1043A.

1.3 Secure Hash Standard (SHS)

Table 18. SHS Certificate 933

Validation No.	933
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	Message Digest Execution Unit (MDEU) r2.1.2
Operational Environment	Freescale Semiconductor MPC8548E

Validation No.	933
Val.Date	12/18/2008
Description/ Notes	**SHA-1** (BYTE-only) **SHA-224** (BYTE-only) **SHA-256** (BYTE-only) Freescale's MDEU r2.1.2 is included in multiple PowerQUICC integrated communications processors and StarCore DSPs, including: MPC8548E, MPC8547E, MPC8545E, MPC8543E, MPC8568E, MPC8567E, MPC8533E, MPC8544E, MSC8144E, MPC8323E, MPC8321E, MPC8313E, MPC8349EA, MPC8347EA, MPC8343EA, MPC8360E, MPC8358E

Table 19. SHS Certificate 934

Validation No.	934
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	Message Digest Execution Unit (MDEU) r3.0.0
Operational Environment	Freescale Semiconductor MPC8572E
Val.Date	12/18/2008
Description/ Notes	SHA-1 (BYTE-only) SHA-224 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only) Freescale's MDEU r3.0.0 is included in multiple PowerQUICC, and QorIQ integrated communications, processors as well as StarCore DSPs, including: MPC8379E, MPC8378E, MPC8377E, MPC8572E, MPC8571E, MPC8536E, MPC8315E, MPC8314E, MPC8569E, P2020, P2010, P1020, P1011, P1021, P1012, P1022, P1013, P1024, P1015, P1025, P1016, MSC8156E, MSC8154E

Table 20. SHS Certificate 1446

Validation No.	1446
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	MDHA 2.0
Operational Environment	Freescale Semiconductor P4080 Rev. 2 silicon

Validation No.	1446
Val.Date	05/24/2011
Description/ Notes	SHA-1 (BYTE-only) SHA-224 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only) Accepts byte length of 0 for all above. HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 10, 12, 16, 20 HMAC-SHA224 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 14, 16, 20, 24, 28 HMAC-SHA256 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 16, 24, 32 HMAC-SHA384 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 24, 32, 40, 48 HMAC-SHA512 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 32, 40, 48, 56, 64 Freescale's MDHA 2.0 is included in multiple QorIQ integrated communications processors, including: P4080 Rev. 2 silicon, P4040 Rev. 2 silicon, P3041, P5020, P2041, P2040, P1010, and P1023.

Table 21. SHS Certificate 1455

Validation No.	1455
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	RNG4 4.0
Operational Environment	Freescale Semiconductor i.MX61
Val.Date	06/07/2011
Description/ Notes	SHA-256 with Prediction Resistance Support. See DRBG #94 Entropy input: 256 Nonce: 128 Personalization string: 0-256 Additional input: 0-256 This SHA implementation is part of Freescale's RNG4 4.0, which is included in the following products: i.MX6, QorIQ Qonverge processors, BSC9131 and BSC9132.

Table 22. SHS Certificate 2108

Validation No.	2108
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	MDHA 2.1
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04

Validation No.	2108
Val.Date	06/20/2013
Description/ Notes	SHA-1 (BYTE-only) SHA-224 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only) Accepts byte length of 0 for all above. Freescale's MDHA 2.1 is included in the QorIQ Qonverge processors, BSC9131 and BSC9132.

Table 23. SHS Certificate 2109

Validation No.	2109
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	MDHA 2.2
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	06/20/2013
Description/ Notes	SHA-1 (BYTE-only) SHA-224 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only) Accepts byte length of 0 for all above. Freescale's MDHA 2.2 is included in multiple QorIQ integrated communications processors, including: P4080 Rev. 3 silicon, P5040, T4240 Rev. 1 silicon, and QorIQ Qonverge products B4860 Rev. 1 silicon.

Table 24. SHS Certificate 2110

Validation No.	2110
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	MDHA 2.3
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04

Validation No.	2110
Val.Date	06/20/2013
Description/ Notes	SHA-1 (BYTE-only) SHA-224 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only) Accepts byte length of 0 for all above. Freescale's MDHA 2.3 is included in multiple QorIQ integrated communications processors, including: T4240 Rev. 2 silicon, T2080, T1040, and the C29x family of security co-processors.

Table 25. SHS Certificate 2111

Validation No.	2111
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	RNG4 4.1
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	06/20/2013
Description/ Notes	SHA-256 with Prediction Resistance Support. See DRBG #94 Entropy input: 256 Nonce: 128 Personalization string: 0-256 Additional input: 0-256 This SHA implementation is part of Freescale's RNG4 4.1, which is included in multiple QorIQ integrated communications processors, including: T4240 Rev. 1 silicon, P5040, and QorIQ Qonverge product B4860 Rev. 1 silicon.

Table 26. SHS Certificate 2112

Validation No.	2112
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	RNG4 4.2
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04

Validation No.	2112
Val.Date	06/20/2013
Description/ Notes	SHA-256 with Prediction Resistance Support. See DRBG #94 Entropy input: 256 Nonce: 128 Personalization string: 0-256 Additional input: 0-256 This SHA implementation is part of Freescale's RNG4 4.2, which is included in multiple QorIQ integrated communications processors, including: T4240 Rev. 2 silicon, T2080, T1040, and the C29x family of security co-processors

Table 27. SHS Certificate 3187

Validation No.	3187
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	MDHA 2.4
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	02/12/2016
Description/ Notes	SHA-1 (BYTE-only) SHA-224 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only) Accepts byte length of 0 for all above. NXP's MDHA 2.4 is included in multiple QorIQ integrated communications processors, including: T1023, T1024.

Table 28. SHS Certificate 3188

Validation No.	3188
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	MDHA 3.0
Operational Environment	Cadence IES 15.10.009 Verilog simulator

Validation No.	3188
Val.Date	02/12/2016
Description/ Notes	SHA-1 (BYTE-only) SHA-224 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only) Accepts byte length of 0 for all above. NXP's MDHA 3.0 is included in multiple QorIQ integrated communications processors, including: LS1023A, LS1043A, LS1026A, LS1046A, LS1044A, LS1048A, LS1084A, LS1088A, LS2040A, LS2045A, LS2080A, LS2085A, LS2044A, LS2048A, LS2084A, LS2088A..

Table 29. SHS Certificate 3189

Validation No.	3189
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	RNG4 4.3
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	02/12/2016
Description/ Notes	SHA-256 with Prediction Resistance Support. See DRBG #1101 Entropy input: 256 Nonce: 128 Personalization string: 0-256 Additional input: 0-256 This SHA implementation is part of Freescale's RNG4 4.3, which is included in multiple QorIQ integrated communications processors, including: T1023, T1024, LS1012A, LS1023A, LS1043A, LS1026A, LS1046A, LS1044A, LS1048A, LS1084A, LS1088A, LS2040A, LS2045A, LS2080A, LS2085A, LS2044A, LS2048A, LS2084A, LS2088A.

Table 30. SHS Certificate 3192

Validation No.	3192
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	MDHA 2.5
Operational Environment	Cadence IES 15.10.009 Verilog simulator

Validation No.	3192
Val.Date	02/19/2016
Description/ Notes	SHA-1 (BYTE-only) SHA-224 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only) Accepts byte length of 0 for all above. NXP's MDHA 2.5 is included in the QorIQ Layerscape integrated communications processors: LS1012A,

1.4 Keyed-Hash Message Authentication Code (HMAC)

Table 31. HMAC Certificate 537

Validation No.	537
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	Message Digest Execution Unit (DEU) r2.1.2
Operational Environment	Freescale Semiconductor MPC8548E
Val.Date	12/18/2008
Description/ Notes	HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS KS=BS KS>BS) SHS Val#933 HMAC-SHA224 (Key Size Ranges Tested: KS<BS KS=BS KS>BS) SHS Val#933 HMAC-SHA256 (Key Size Ranges Tested: KS<BS KS=BS KS>BS) SHS Val#933 Freescale's MDEU r2.1.2 is included in multiple PowerQUICC integrated communications processors and StarCore DSPs, including: MPC8548E, MPC8547E, MPC8545E, MPC8543E, MPC8568E, MPC8567E, MPC8533E, MPC8544E, MSC8144E, MPC8323E, MPC8321E, MPC8313E, MPC8349EA, MPC8347EA, MPC8343EA, MPC8360E, MPC8358E

Table 32. HMAC Certificate 538

Validation No.	538
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	Message Digest Execution Unit (DEU) r3.0.0
Operational Environment	Freescale Semiconductor MPC8572E

Validation No.	538
Val.Date	12/18/2008
Description/ Notes	HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS KS=BS KS>BS) SHS Val#934 HMAC-SHA224 (Key Size Ranges Tested: KS<BS KS=BS KS>BS) SHS Val#934 HMAC-SHA256 (Key Size Ranges Tested: KS<BS KS=BS KS>BS) SHS Val#934 HMAC-SHA384 (Key Size Ranges Tested: KS<BS KS=BS KS>BS) SHS Val#934 HMAC-SHA512 (Key Size Ranges Tested: KS<BS KS=BS KS>BS) SHS Val#934 Freescale's MDEU r3.0.0 is included in multiple PowerQUICC and QorIQ integrated communications processors and StarCore DSPs, including: MPC8379E, MPC8378E, MPC8377E, MPC8572E, MPC8571E, MPC8536E, MPC8315E, MPC8314E, MPC8569E, P2020, P2010, P1020, P1011, P1021, P1012, P1022, P1013, P1024, P1015, P1025, P1016, MSC8156E, MSC8154E

Table 33. HMAC Certificate 967

Validation No.	967
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	MDHA 2.0
Operational Environment	Freescale Semiconductor P4080 Rev. 2 silicon
Val.Date	05/24/2011
Description/ Notes	SHS Certificate Val#1446 SHA-1 (BYTE-only) SHA-224 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only) Accepts byte length of 0 for all above. HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 10,12,16,20 HMAC-SHA224 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 14,16,20,24,28 HMAC-SHA256 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 16,24,32 HMAC-SHA384 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 24,32,40,48 HMAC-SHA512 (Key Size Ranges Tested: KS<BS KS=BS KSsBS), MAC sizes 32,40,48,56,64 Freescale's MDHA 2.0 is included in multiple QorIQ integrated communications processors, including: P4080 Rev. 2 silicon, P4040 Rev. 2 silicon, P3041, P5020, P2041, P2040, P1010, and P1023.

Table 34. HMAC Certificate 1532

Validation No.	1532
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	MDHA 2.1

Validation No.	1532
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	06/20/2013
Description/ Notes	See SHS 2108. HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 10, 12, 16, 20 HMAC-SHA224 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 14, 16, 20, 24, 28 HMAC-SHA256 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 16, 24, 32 HMAC-SHA384 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 24, 32, 40, 48 HMAC-SHA512 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 32, 40, 48, 56, 64 Freescale's MDHA 2.1 is included in the BSC9131 and BSC9132 QorIQ Qonverge processors.

Table 35. HMAC Certificate 1533

Validation No.	1533
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	MDHA 2.2
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	06/20/2013
Description/ Notes	See SHS 2109. HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 10, 12, 16, 20 HMAC-SHA224 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 14, 16, 20, 24, 28 HMAC-SHA256 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 16, 24, 32 HMAC-SHA384 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 24, 32, 40, 48 HMAC-SHA512 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 32, 40, 48, 56, 64 Freescale's MDHA 2.2 is included in multiple QorIQ integrated communications processors, including: P4080 Rev. 3 silicon, P5040, T4240 Rev. 1 silicon, as well as the B4860, Rev. 1 silicon, QorIQ Qonverge processor.

Table 36. HMAC Certificate 1534

Validation No.	1534
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	MDHA 2.3
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04

Validation No.	1534
Val.Date	06/20/2013
Description/ Notes	See SHS 2110. HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 10, 12, 16, 20 HMAC-SHA224 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 14, 16, 20, 24, 28 HMAC-SHA256 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 16, 24, 32 HMAC-SHA384 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 24, 32, 40, 48 HMAC-SHA512 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 32, 40, 48, 56, 64 Freescale's MDHA 2.3 is included in multiple QorIQ integrated communications processors, including: T4240 Rev. 2 silicon, T2080, T1040, and the C29x family of security co-processors.

Table 37. HMAC Certificate 2511

Validation No.	2511
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	MDHA 2.4
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	02/12/2016
Description/ Notes	See SHS 3187. HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 10, 12, 16, 20 HMAC-SHA224 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 14, 16, 20, 24, 28 HMAC-SHA256 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 16, 24, 32 HMAC-SHA384 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 24, 32, 40, 48 HMAC-SHA512 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 32, 40, 48, 56, 64 NXP’s MDHA 2.4 is included in multiple QorIQ integrated communications processors, including: T1023, T1024.

Table 38. HMAC Certificate 2512

Validation No.	2512
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	MDHA 3.0
Operational Environment	Cadence IES 15.10.009 Verilog simulator

Validation No.	2512
Val.Date	02/12/2016
Description/ Notes	See SHS 3188. HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 10, 12, 16, 20 HMAC-SHA224 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 14, 16, 20, 24, 28 HMAC-SHA256 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 16, 24, 32 HMAC-SHA384 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 24, 32, 40, 48 HMAC-SHA512 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 32, 40, 48, 56, 64 NXP's MDHA 3.0 is included in multiple QorIQ integrated communications processors, including: LS1023A, LS1043A, LS1026A, LS1046A, LS1044A, LS1048A, LS1084A, LS1088A, LS2040A, LS2045A, LS2080A, LS2085A, LS2044A, LS2048A, LS2084A, LS2088A.

Table 39. HMAC Certificate 2515

Validation No.	2515
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	MDHA 2.5
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	02/19/2016
Description/ Notes	See SHS 3192. HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 10, 12, 16, 20 HMAC-SHA224 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 14, 16, 20, 24, 28 HMAC-SHA256 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 16, 24, 32 HMAC-SHA384 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 24, 32, 40, 48 HMAC-SHA512 (Key Size Ranges Tested: KS<BS KS=BS KS>BS), MAC sizes 32, 40, 48, 56, 64 NXP's MDHA 2.5 is included in the QorIQ Layerscape integrated communications processor: LS1012A.

1.5 Random Number Generator (RNG)

Table 40. RNG Certificate 544

Validation No.	544
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	Random Number Generator (RNG-B, r3.1.0)
Operational Environment	Synopsys Vera 6.3.30 simulation environment

Validation No.	544
Val.Date	12/18/2008
Description/ Notes	FIPS 186-2 General Purpose [(x-Original); (SHA-1)] Freescale's Deterministic Random Number Generator-B, revision 3.1.0 completed certification in a simulation environment. The hardware implementation is included in multiple PowerQUICC and QorIQ integrated communications processors and StarCore DSPs, including: MPC8569E, MPC8536E, P2020, P2010, P2020, P2010, P1020, P1011, P1021, P1012, P1022, P1013, P1024, P1015, P1025, P1016, MSC8156E, MSC8154E

NOTE: RNG-B revision 3.1.0 testing

Within the cryptographic boundary, the RNG-B revision 3.1.0, which is used in all of the products listed above, is identical. Outside the core RNG-B logic, there are differences in the seed-loading procedure between the MPC8569E, MPC8536E, P2020, P2010, MSC8156E, and the P1020, P1011, P1021, P1012, P1022, P1013, P1024, P1015, P1025, P1016. Developers planning to conduct RNG-B r3.1.0 testing using a known seed are advised to contact Freescale for the proper seed-loading procedure for the MPC8569E, MPC8536E, P2020, P2010, and MSC8156E.

Table 41. RNG Certificate 818

Validation No.	818
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	Random Number Generator (RNG-B, r2.1.0)
Operational Environment	Freescale Semiconductor P4080 Rev. 2 silicon
Val.Date	11/16/2010
Description/ Notes	FIPS 186-2 General Purpose [(x-Original); (SHA-1)] Freescale's RNG-B 2.1.0 is included in multiple QorIQ integrated communications processors and StarCore DSPs, including: P4080 Rev. 2 and Rev. 3 silicon, P4040 Rev. 2 and Rev. 3 silicon, P3041, P5020, P2041, P2040, P1010, and P1023.

1.6 Deterministic Random Bit Generators (DRBG)

NOTE

Deterministic random number generators, as specified in *Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, are listed separately.

Table 42. DRBG Certificate 94

Validation No.	94
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	RNG4 4.0
Operational Environment	Freescale Semiconductor i.MX61
Val.Date	06/07/2011
Description/ Notes	SHA-256 with Prediction Resistance Support. SHS 1455 Entropy input: 256 Nonce: 128 Personalization string: 0-256 Additional input: 0-256 Freescale's RNG4 4.0 is included in i.MX media processors, and in the BSC9131 and BSC9132 QorIQ Qonverge processors.

Table 43. DRBG Certificate 348

Validation No.	348
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	RNG4 4.1
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	06/20/2013
Description/ Notes	SHA-256 with Prediction Resistance Support. SHS 2111. Entropy input: 256 Nonce: 128 Personalization string: 0-256 Additional input: 0-256 Freescale's RNG4 4.1 is included in multiple QorIQ integrated communications processors, including: T4240 Rev. 1 silicon, and P5040 as well as the B4860, Rev. 1 silicon, QorIQ Qonverge processor.

Table 44. DRBG Certificate 349

Validation No.	349
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	RNG4 4.2
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04

Validation No.	349
Val.Date	06/20/2013
Description/ Notes	SHA-256 with Prediction Resistance Support. SHS 2112. Entropy input: 256 Nonce: 128 Personalization string: 0-256 Additional input: 0-256 Freescale''s RNG4 4.2 is included in multiple QorIQ integrated communications processors, including: T4240 Rev. 2 silicon, T2080, T1040, and the C29x family of security co-processors.

Table 45. DRBG Certificate 1101

Validation No.	1101
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	RNG4 4.3
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	02/12/2016
Description/ Notes	SHA-256 with Prediction Resistance Support. SHS 3189. Entropy input: 256 Nonce: 128 Personalization string: 0-256 Additional input: 0-256 NXP's RNG4 4.3 is included in multiple QorIQ integrated communications processors, including: T1023, T1024, LS1012A, LS1023A, LS1043A, LS1026A, LS1046A, LS1044A, LS1048A, LS1084A, LS1088A, LS2040A, LS2045A, LS2080A, LS2085A, LS2044A, LS2048A, LS2084A, LS2088A.

1.7 RSA algorithms (RSA)

Table 46. RSA Certificate 465

Validation No.	465
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	Public Key Execution Unit (PKEU) r2.1.2
Operational Environment	Freescale Semiconductor MPC8548E

Validation No.	465
Val.Date	12/18/2008
Description/ Notes	ALG [RSASSA-PKCS1_V1_5] SIG(gen); SIG(ver); 1024 , 1536 , 2048 SHS: SHA-1 Val#933 , SHA-256 Val#933 Freescale's PKEU r2.1.2 is included in multiple PowerQUICC integrated communications processors and StarCore DSPs, including: MPC8548E, MPC8547E, MPC8545E, MPC8543E, MPC8568E, MPC8567E, MPC8533E, MPC8544E, MSC8144E, MPC8323E, MPC8321E, MPC8313E, MPC8349EA, MPC8347EA, MPC8343EA, MPC8360E, MPC8358E

Table 47. RSA Certificate 466

Validation No.	466
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	Public Key Execution Unit (PKEU) r3.0.0
Operational Environment	Freescale Semiconductor MPC8572E
Val.Date	12/18/2008
Description/ Notes	ALG[RSASSA-PKCS1_V1_5] SIG(gen); SIG(ver); 1024 , 1536 , 2048 , 3072 , 4096 SHS: SHA-1 Val#934 , SHA-256 Val#934 , SHA-384 Val#934 , SHA-512 Val#934 Freescale's PKEU r3.0.0 is included in multiple PowerQUICC and QorIQ integrated communications processors and StarCore DSPs, including: MPC8379E, MPC8378E, MPC8377E, MPC8572E, MPC8571E, MPC8536E, MPC8315E, MPC8314E, MPC8569E, P2020, P2010, P1020, P1011, P1021, P1012, P1022, P1013, P1024, P1015, P1025, P1016, MSC8156E, MSC8154E

Table 48. RSA Certificate 813

Validation No.	813
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	PKHA-XT 0.1
Operational Environment	Freescale Semiconductor P4080r2

Validation No.	813
Val.Date	05/24/2011
Description/ Notes	ALG[RSASSA-PKCS1_V1_5] SIG(gen); SIG(ver); 1024 , 1536 , 2048 , 3072 , 4096 SHS with MDHA 2.0: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 Freescale's PKHA-XT 0.1 is included in multiple QorIQ integrated communications processors, including: P4080 Rev. 2 silicon, P4040 Rev. 2 silicon, P3041, P5020, P2041, P2040, P1010, and P1023.

The following RSA certificates include FIPS 186-3 Key Generation, a feature not available in previous implementations, which are sign/verify only. The cryptographic boundary, and definition of the certified implementation, for RSA key gen operations includes multiple “engines” within the SEC block; in specific, the Descriptor Controller (DECO), PKHA, RNG, and MDHA. A Freescale QorIQ, QorIQ Qonverge, or C29x product is only listed if it contains the tested combination of these engines.

Table 49. RSA Certificate 1428

Validation No.	1428
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 11200121
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	12/20/2013
Description/ Notes	FIPS186-3: 186-3KEY(gen): FIPS186-3_Random_e PGM(ProbRandom: (2048 , 3072) PPTT:(C.2 , C.3) PGM(ProbPrimeCondition): 1024 , 2048 , 3072 PPTT:(C.2 , C.3) ALG[RSASSA-PKCS1_V1_5] SIG(gen) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) SIG(Ver) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) FIPS186_3 Component Test: (SignGenModExp_PKCS15_SHA1 SHA224 SHA256) SHA Val#1446 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs plus Descriptor Controller: DECO 1.1, MDHA 2.0, PKHA-XT0.1, RNGB 2.1. Freescale's DMPR 11200121 is included in multiple QorIQ integrated communications processors, including: P3041, P2041, P2040, P5020, P5010, and P1010.

Table 50. RSA Certificate 1429

Validation No.	1429
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 12211040
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	12/20/2013
Description/ Notes	FIPS186-3: 186-3KEY(gen): FIPS186-3_Random_e PGM(ProbRandom: (2048 , 3072) PPTT:(C.2 , C.3) PGM(ProbPrimeCondition): 1024 , 2048 , 3072 PPTT:(C.2 , C.3) ALG[RSASSA-PKCS1_V1_5] SIG(gen) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) SIG(Ver) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) FIPS186_3 Component Test: (SignGenModExp_PKCS15_SHA1 SHA224 SHA256) SHA Val#2108 DRBG: Val# 94 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 1.2, MDHA 2.1, PKHA-SD32 1.0, RNGB 4.0. Freescale's DMPR 12211040 is included in the BSC9131 and BSC9132 QorIQ Qonverge processors.

Table 51. RSA Certificate 1430

Validation No.	1430
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 13221121
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04

Validation No.	1430
Val.Date	12/20/2013
Description/ Notes	FIPS186-3: 186-3KEY(gen): FIPS186-3_Random_e PGM(ProbRandom: (2048 , 3072) PPTT:(C.2 , C.3) PGM(ProbPrimeCondition): 1024 , 2048 , 3072 PPTT:(C.2 , C.3) ALG[RSASSA-PKCS1_V1_5] SIG(gen) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) SIG(Ver) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) FIPS186_3 Component Test: (SignGenModExp_PKCS15_SHA1 SHA224 SHA256) SHA Val#2109 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 1.3, MDHA 2.2, PKHA-SD32 1.1, RNGB 2.1. Freescale's DMPR 13221121 is included in the P4080, Rev. 3 silicon, QorIQ integrated communications processor.

Table 52. RSA Certificate 1431

Validation No.	1431
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 20222141
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	12/20/2013
Description/ Notes	FIPS186-3: 186-3KEY(gen): FIPS186-3_Random_e PGM(ProbRandom: (2048 , 3072) PPTT:(C.2 , C.3) PGM(ProbPrimeCondition): 1024 , 2048 , 3072 PPTT:(C.2 , C.3) ALG[RSASSA-PKCS1_V1_5] SIG(gen) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) SIG(Ver) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) FIPS186_3 Component Test: (SignGenModExp_PKCS15_SHA1 SHA224 SHA256) SHA Val#2109 DRBG: Val# 348 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 2.0, MDHA 2.2, PKHA-SD64 2.1, RNG4 4.1. Freescale's DMPR 20222141 is included in multiple QorIQ integrated communications processors and co-processors, including: P5040, P5021, T4240 Rev. 1 silicon, T4160 Rev. 1 silicon, and B4860.

Table 53. RSA Certificate 1432

Validation No.	1432
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 30231242
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	12/20/2013
Description/ Notes	FIPS186-3: 186-3KEY(gen): FIPS186-3_Random_e PGM(ProbRandom: (2048 , 3072) PPTT:(C.2 , C.3) PGM(ProbPrimeCondition): 1024 , 2048 , 3072 PPTT:(C.2 , C.3) ALG[RSASSA-PKCS1_V1_5] SIG(gen) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) SIG(Ver) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) FIPS186_3 Component Test: (SignGenModExp_PKCS15_SHA1 SHA224 SHA256) SHA Val#2110 DRBG: Val# 349 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 3.0, MDHA 2.3, PKHA-SD32 1.2, RNG4 4.2. Freescale's DMPR 30231242 is included in the T1040 QorIQ integrated communications processor.

Table 54. RSA Certificate 1433

Validation No.	1433
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 30232242
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04

Validation No.	1433
Val.Date	12/20/2013
Description/ Notes	FIPS186-3: 186-3KEY(gen): FIPS186-3_Random_e PGM(ProbRandom: (2048 , 3072) PPTT:(C.2 , C.3) PGM(ProbPrimeCondition): 1024 , 2048 , 3072 PPTT:(C.2 , C.3) ALG[RSASSA-PKCS1_V1_5] SIG(gen) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) SIG(Ver) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) FIPS186_3 Component Test: (SignGenModExp_PKCS15_SHA1 SHA224 SHA256) SHA Val#2110 DRBG: Val# 349 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 3.0, MDHA 2.3, PKHA-SD64 2.2, RNG4 4.2. Freescale's DMPR 30232242 is included in the T2080 QorIQ integrated communications processor.

Table 55. RSA Certificate 1434

Validation No.	1434
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 30233242
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	12/20/2013
Description/ Notes	FIPS186-3: 186-3KEY(gen): FIPS186-3_Random_e PGM(ProbRandom: (2048 , 3072) PPTT:(C.2 , C.3) PGM(ProbPrimeCondition): 1024 , 2048 , 3072 PPTT:(C.2 , C.3) ALG[RSASSA-PKCS1_V1_5] SIG(gen) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) SIG(Ver) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) FIPS186_3 Component Test: (SignGenModExp_PKCS15_SHA1 SHA224 SHA256) SHA Val#2110 DRBG: Val# 349 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 3.0, MDHA 2.3, PKHA-SD128 3.2, RNG4 4.2. Freescale's DMPR 30233242 is included in multiple QorIQ integrated communications processors and co-processors, including: C291, C292, C293, T4240 Rev. 2 silicon, and T4160 Rev. 2 silicon.

Table 56. RSA Certificate 2398

Validation No.	2398
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 31231342
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	03/06/2017
Description/ Notes	FIPS186-3: 186-3KEY(gen): FIPS186-3_Random_e PGM(ProbRandom: (2048 , 3072) PPTT:(C.2 , C.3) PGM(ProbPrimeCondition): 1024 , 2048 , 3072 PPTT:(C.2 , C.3) ALG[RSASSA-PKCS1_V1_5] SIG(gen) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) SIG(Ver) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) FIPS186_3 Component Test: (SignGenModExp_PKCS15_SHA1 SHA224 SHA256) SHA Val# 2110 DRBG: Val# 349 NXP’s cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 3.1, MDHA 2.3, PKHA 1.3, RNG4 4.2. DMPR 31231342 is included in multiple QorIQ integrated communications processors including: LS1020A, LS1021A, LS1022A.

Table 57. RSA Certificate 2399

Validation No.	2399
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 40303443
Operational Environment	Cadence IES 15.10.009 Verilog simulator

Validation No.	2399
Val.Date	03/06/2017
Description/ Notes	FIPS186-3: 186-3KEY(gen): FIPS186-3_Random_e PGM(ProbRandom: (2048 , 3072) PPTT:(C.2 , C.3) PGM(ProbPrimeCondition): 1024 , 2048 , 3072 PPTT:(C.2 , C.3) ALG[RSASSA-PKCS1_V1_5] SIG(gen) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) SIG(Ver) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) FIPS186_3 Component Test: (SignGenModExp_PKCS15_SHA1 SHA224 SHA256) SHA Val# 3188; DRBG Val# 1101 NXP's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 4.0, MDHA 3.0, PKHA 3.4, RNG4 4.3. DMPR 40303443 is included in multiple QorIQ integrated communications processors including: LS2040A, LS2045A, LS2080A, LS2085A, LS2044A, LS2048A, LS2084A, LS2088A.

Table 58. RSA Certificate 2400

Validation No.	2400
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 40241443
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	03/06/2017
Description/ Notes	FIPS186-3: 186-3KEY(gen): FIPS186-3_Random_e PGM(ProbRandom: (2048 , 3072) PPTT:(C.2 , C.3) PGM(ProbPrimeCondition): 1024 , 2048 , 3072 PPTT:(C.2 , C.3) ALG[RSASSA-PKCS1_V1_5] SIG(gen) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) SIG(Ver) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) FIPS186_3 Component Test: (SignGenModExp_PKCS15_SHA1 SHA224 SHA256) SHA Val# 3187; DRBG Val# 1101 NXP's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 4.0, MDHA 2.4, PKHA 1.4, RNG4 4.3. DMPR 40241443 is included in multiple QorIQ integrated communications processors including: T1023, T1024.

Table 59. RSA Certificate 2401

Validation No.	2401
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 40251443
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	03/06/2017
Description/ Notes	FIPS186-3: 186-3KEY(gen): FIPS186-3_Random_e PGM(ProbRandom: (2048 , 3072) PPTT:(C.2 , C.3) PGM(ProbPrimeCondition): 1024 , 2048 , 3072 PPTT:(C.2 , C.3) ALG[RSASSA-PKCS1_V1_5] SIG(gen) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) SIG(Ver) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) FIPS186_3 Component Test: (SignGenModExp_PKCS15_SHA1 SHA224 SHA256) SHA Val# 3192; DRBG Val# 1101 NXP’s cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 4.0, MDHA 2.5, PKHA 1.4, RNG4 4.3. DMPR 40251443 is included in the QorIQ integrated communications processor: LS1012A.

Table 60. RSA Certificate 2402

Validation No.	2402
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 40301443
Operational Environment	Cadence IES 15.10.009 Verilog simulator

Validation No.	2402
Val.Date	03/06/2017
Description/ Notes	FIPS186-3: 186-3KEY(gen): FIPS186-3_Random_e PGM(ProbRandom: (2048 , 3072) PPTT:(C.2 , C.3) PGM(ProbPrimeCondition): 1024 , 2048 , 3072 PPTT:(C.2 , C.3) ALG[RSASSA-PKCS1_V1_5] SIG(gen) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) SIG(Ver) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) FIPS186_3 Component Test: (SignGenModExp_PKCS15_SHA1 SHA224 SHA256) SHA Val# 3188; DRBG Val# 1101 NXP's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 4.0, MDHA 3.0, PKHA 1.4, RNG4 4.3. DMPR 40301443 is included in multiple QorIQ integrated communications processors, including: LS1023A, LS1043A, LS1026A, LS1046A, LS1044A, LS1048A, LS1084A, LS1088A.

1.8 Digital Signature Algorithms (DSA)

The cryptographic boundary, and definition of the certified implementation, for DSA operations includes multiple "engines" within the SEC block, specifically the Descriptor Controller (DECO), PKHA, RNG, and MDHA. A Freescale/NXP QorIQ, QorIQ Qonverge, or C29x product is only listed if it contains the tested combination of these engines.

Table 61. DSA Certificate 516

Validation No.	516
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DHSA 0A10
Operational Environment	Freescale Semiconductor P4080r2
Val.Date	05/24/2011
Description/ Notes	FIPS186-2: KEYGEN(Y) MOD(1024); SIG(gen) MOD(1024); SIG(ver) MOD(1024); SHS: Val# 1446 RNG: Val# 818 Freescale's DSHA 0A10 is included in multiple QorIQ integrated communications processor, including: P4080 Rev. 2 silicon, P4040 Rev. 2 silicon, and P1023.

Table 62. DSA Certificate 769

Validation No.	769
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 11200121
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	06/20/2013
Description/ Notes	FIPS186-4: Key Pair: [(2048,224) ; (2048,256) ; (3072,256)] SIG(gen)PARMS TESTED: [(2048,224) SHA(224 , 256 , 384 , 512); (2048,256) SHA(224 , 256 , 384 , 512); (3072,256) SHA(224 , 256 , 384 , 512);] SIG(ver)PARMS TESTED: [(1024,160) SHA(1 , 224 , 256 , 384 , 512); (2048,224) SHA(1 , 224 , 256 , 384 , 512); (2048,256) SHA(1 , 224 , 256 , 384 , 512); (3072,256) SHA(1 , 224 , 256 , 384 , 512)] SHS: Val# 1446 RNG: Val# 818 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 1.1, MDHA 2.0, PKHA-XT0.1, RNGB 2.1. Freescale's DMPR 11200121 is included in multiple QorIQ integrated communications processor, including: P3041, P2041, P2040, P5020, P5010, and P1010.

Table 63. DSA Certificate 770

Validation No.	770
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 12211040
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	06/20/2013
Description/ Notes	FIPS186-4: Key Pair: [(2048,224) ; (2048,256) ; (3072,256)] SIG(gen)PARMS TESTED: [(2048,224) SHA(224 , 256 , 384 , 512); (2048,256) SHA(224 , 256 , 384 , 512); (3072,256) SHA(224 , 256 , 384 , 512);] SIG(ver)PARMS TESTED: [(1024,160) SHA(1 , 224 , 256 , 384 , 512); (2048,224) SHA(1 , 224 , 256 , 384 , 512); (2048,256) SHA(1 , 224 , 256 , 384 , 512); (3072,256) SHA(1 , 224 , 256 , 384 , 512)] SHS: Val# 2108 RNG: Val# 94 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 1.2, MDHA 2.1, PKHA-SD32 1.0, RNGB 4.0. Freescale's DMPR 12211040 is included in the QorIQ Qonverge processors, BSC9131 and BSC9132.

Table 64. DSA Certificate 771

Validation No.	771
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 13221121
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	06/20/2013
Description/ Notes	FIPS186-4: Key Pair: [(2048,224) ; (2048,256) ; (3072,256)] SIG(gen)PARMS TESTED: [(2048,224) SHA(224 , 256 , 384 , 512); (2048,256) SHA(224 , 256 , 384 , 512); (3072,256) SHA(224 , 256 , 384 , 512);] SIG(ver)PARMS TESTED: [(1024,160) SHA(1 , 224 , 256 , 384 , 512); (2048,224) SHA(1 , 224 , 256 , 384 , 512); (2048,256) SHA(1 , 224 , 256 , 384 , 512); (3072,256) SHA(1 , 224 , 256 , 384 , 512)] SHS: Val# 2109 RNG: Val# 818 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 1.3, MDHA 2.2, PKHA-SD32 1.1, RNGB 2.1. Freescale's DMPR 13221121 is included in the P4080, Rev. 3 silicon, QorIQ integrated communications processors.

Table 65. DSA Certificate 772

Validation No.	772
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 20222141
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	06/20/2013
Description/ Notes	FIPS186-4: Key Pair: [(2048,224) ; (2048,256) ; (3072,256)] SIG(gen)PARMS TESTED: [(2048,224) SHA(224 , 256 , 384 , 512); (2048,256) SHA(224 , 256 , 384 , 512); (3072,256) SHA(224 , 256 , 384 , 512);] SIG(ver)PARMS TESTED: [(1024,160) SHA(1 , 224 , 256 , 384 , 512); (2048,224) SHA(1 , 224 , 256 , 384 , 512); (2048,256) SHA(1 , 224 , 256 , 384 , 512); (3072,256) SHA(1 , 224 , 256 , 384 , 512)] SHS: Val# 2109 DRBG: Val# 348 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 2.0, MDHA 2.2, PKHA-SD64 2.1, RNG4 4.1. Freescale's DMPR 20222141 is included in multiple QorIQ integrated communications processors and co-processors, including: P5040, P5021, T4240 Rev. 1 silicon, T4160 Rev. 1 silicon, and B4860.

Table 66. DSA Certificate 773

Validation No.	773
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 30233242
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	06/20/2013
Description/ Notes	FIPS186-4: Key Pair: [(2048,224) ; (2048,256) ; (3072,256)] SIG(gen)PARMS TESTED: [(2048,224) SHA(224 , 256 , 384 , 512); (2048,256) SHA(224 , 256 , 384 , 512); (3072,256) SHA(224 , 256 , 384 , 512);] SIG(ver)PARMS TESTED: [(1024,160) SHA(1 , 224 , 256 , 384 , 512); (2048,224) SHA(1 , 224 , 256 , 384 , 512); (2048,256) SHA(1 , 224 , 256 , 384 , 512); (3072,256) SHA(1 , 224 , 256 , 384 , 512)] SHS: Val# 2110 DRBG: Val# 349 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 3.0, MDHA 2.3, PKHA-SD128 3.2, RNG4 4.2. Freescale's DMPR 30233242 is included in multiple QorIQ integrated communications processors and co-processors, including: C291, C292, C293, T4240 Rev. 2 silicon, and T4160 Rev. 2 silicon.

Table 67. DSA Certificate 774

Validation No.	774
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 30231242
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	06/20/2013
Description/ Notes	FIPS186-4: Key Pair: [(2048,224) ; (2048,256) ; (3072,256)] SIG(gen)PARMS TESTED: [(2048,224) SHA(224 , 256 , 384 , 512); (2048,256) SHA(224 , 256 , 384 , 512); (3072,256) SHA(224 , 256 , 384 , 512);] SIG(ver)PARMS TESTED: [(1024,160) SHA(1 , 224 , 256 , 384 , 512); (2048,224) SHA(1 , 224 , 256 , 384 , 512); (2048,256) SHA(1 , 224 , 256 , 384 , 512); (3072,256) SHA(1 , 224 , 256 , 384 , 512)] SHS: Val# 2110 DRBG: Val# 349 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 3.0, MDHA 2.3, PKHA-SD32 1.2, RNG4 4.2. Freescale's DMPR 30231242 is included in the T2080 QorIQ integrated communications processors.

Table 68. DSA Certificate 775

Validation No.	775
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 30232242
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	06/20/2013
Description/ Notes	FIPS186-4: Key Pair: [(2048,224) ; (2048,256) ; (3072,256)] SIG(gen)PARMS TESTED: [(2048,224) SHA(224 , 256 , 384 , 512); (2048,256) SHA(224 , 256 , 384 , 512); (3072,256) SHA(224 , 256 , 384 , 512);] SIG(ver)PARMS TESTED: [(1024,160) SHA(1 , 224 , 256 , 384 , 512); (2048,224) SHA(1 , 224 , 256 , 384 , 512); (2048,256) SHA(1 , 224 , 256 , 384 , 512); (3072,256) SHA(1 , 224 , 256 , 384 , 512)] SHS: Val# 2110 DRBG: Val# 349 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 3.0, MDHA 2.3, PKHA-SD64 2.2, RNG4 4.2. Freescale's DMPR 30232242 is included in the T2080 QorIQ integrated communications processors.

Table 69. DSA Certificate 1179

Validation No.	1179
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 31231342
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	03/06/2017
Description/ Notes	FIPS186-4: Key Pair: [(2048,224) ; (2048,256) ; (3072,256)] SIG(gen)PARMS TESTED: [(2048,224) SHA(224 , 256 , 384 , 512); (2048,256) SHA(224 , 256 , 384 , 512); (3072,256) SHA(224 , 256 , 384 , 512);] SIG(ver)PARMS TESTED: [(1024,160) SHA(1 , 224 , 256 , 384 , 512); (2048,224) SHA(1 , 224 , 256 , 384 , 512); (2048,256) SHA(1 , 224 , 256 , 384 , 512); (3072,256) SHA(1 , 224 , 256 , 384 , 512)] SHS: Val# 2110 DRBG: Val# 349 NXP’s cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 3.1, MDHA 2.3, PKHA 1.3, RNG4 4.2. DMPR 31231342 is included in multiple QorIQ integrated communications processors including: LS1020A, LS1021A, LS1022A.

Table 70. DSA Certificate 1180

Validation No.	1180
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 40303443
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	03/06/2017
Description/ Notes	FIPS186-4: Key Pair: [(2048,224) ; (2048,256) ; (3072,256)] SIG(gen)PARMS TESTED: [(2048,224) SHA(224 , 256 , 384 , 512); (2048,256) SHA(224 , 256 , 384 , 512); (3072,256) SHA(224 , 256 , 384 , 512);] SIG(ver)PARMS TESTED: [(1024,160) SHA(1 , 224 , 256 , 384 , 512); (2048,224) SHA(1 , 224 , 256 , 384 , 512); (2048,256) SHA(1 , 224 , 256 , 384 , 512); (3072,256) SHA(1 , 224 , 256 , 384 , 512)] SHS: Val# 3188 DRBG: Val# 1101 NXP's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 4.0, MDHA 3.0, PKHA 3.4, RNG4 4.3. DMPR 40303443 is included in multiple QorIQ integrated communications processors including: LS2040A, LS2045A, LS2080A, LS2085A, LS2044A, LS2048A, LS2084A, LS2088A.

Table 71. DSA Certificate 1181

Validation No.	1181
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 40241443
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	03/06/2017
Description/ Notes	FIPS186-4: Key Pair: [(2048,224) ; (2048,256) ; (3072,256)] SIG(gen)PARMS TESTED: [(2048,224) SHA(224 , 256 , 384 , 512); (2048,256) SHA(224 , 256 , 384 , 512); (3072,256) SHA(224 , 256 , 384 , 512);] SIG(ver)PARMS TESTED: [(1024,160) SHA(1 , 224 , 256 , 384 , 512); (2048,224) SHA(1 , 224 , 256 , 384 , 512); (2048,256) SHA(1 , 224 , 256 , 384 , 512); (3072,256) SHA(1 , 224 , 256 , 384 , 512)] SHS: Val# 3187 DRBG: Val# 1101 NXP's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 4.0, MDHA 2.4, PKHA 1.4, RNG4 4.3. DMPR 40241443 is included in multiple QorIQ integrated communications processors including: T1023, T1024.

Table 72. DSA Certificate 1182

Validation No.	1182
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 40251443
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	03/06/2017
Description/ Notes	FIPS186-4: Key Pair: [(2048,224) ; (2048,256) ; (3072,256)] SIG(gen)PARMS TESTED: [(2048,224) SHA(224 , 256 , 384 , 512); (2048,256) SHA(224 , 256 , 384 , 512); (3072,256) SHA(224 , 256 , 384 , 512);] SIG(ver)PARMS TESTED: [(1024,160) SHA(1 , 224 , 256 , 384 , 512); (2048,224) SHA(1 , 224 , 256 , 384 , 512); (2048,256) SHA(1 , 224 , 256 , 384 , 512); (3072,256) SHA(1 , 224 , 256 , 384 , 512)] SHS: Val# 3192 DRBG: Val# 1101 NXP's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 4.0, MDHA 2.5, PKHA 1.4, RNG4 4.3. DMPR 40251443 is included in the QorIQ integrated communications processor: LS1012A.

Table 73. DSA Certificate 1183

Validation No.	1183
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 40301443
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	03/06/2017
Description/ Notes	FIPS186-4: Key Pair: [(2048,224) ; (2048,256) ; (3072,256)] SIG(gen)PARMS TESTED: [(2048,224) SHA(224 , 256 , 384 , 512); (2048,256) SHA(224 , 256 , 384 , 512); (3072,256) SHA(224 , 256 , 384 , 512);] SIG(ver)PARMS TESTED: [(1024,160) SHA(1 , 224 , 256 , 384 , 512); (2048,224) SHA(1 , 224 , 256 , 384 , 512); (2048,256) SHA(1 , 224 , 256 , 384 , 512); (3072,256) SHA(1 , 224 , 256 , 384 , 512)] SHS: Val# 3188 DRBG: Val# 1101 NXP's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 4.0, MDHA 3.0, PKHA 1.4, RNG4 4.3. DMPR 40301443 is included in multiple QorIQ integrated communications processors, including: LS1023A, LS1043A, LS1026A, LS1046A, LS1044A, LS1048A, LS1084A, LS1088A.

1.9 Elliptic Curve Digital Signature Algorithm (ECDSA)

The cryptographic boundary, and definition of the certified implementation, for ECDSA operations includes multiple “engines” within the SEC block, specifically the Descriptor Controller (DECO), PKHA, RNG, and MDHA. A Freescale/NXP QorIQ, QorIQ Qonverge, or C29x product is only listed if it contains the tested combination of these engines.

Table 74. ECDSA Certificate 209

Validation No.	209
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DHSA 0A10
Operational Environment	Freescale Semiconductor P4080 Rev. 2 silicon
Val.Date	05/24/2011
Description/ Notes	ECDSA Key Pair, SIG(gen); SIG(ver); P: 192, 224, 256, 384, 521 K: 163, 233, 283, 409, 571 B: 163, 233, 283, 409, 571 SHS: Val# 1446 RNG: Val# 818 Freescale"s DSHA 0A10 is included in multiple QorIQ integrated communications processors, including: P4080 Rev. 2 silicon, P4040 Rev. 2 silicon, and P1023.

Table 75. ECDSA Certificate 418

Validation No.	418
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 11200121
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04

Validation No.	418
Val.Date	06/20/2013
Description/ Notes	FIPS186-4: PKG: CURVES(P-192 K-163 B-163) SigGen: CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224:(SHA-1) P-256:(SHA-1) P-384:(SHA-1) P-521: K-163: (SHA-1, 224, 256, 384, 512) K-233:(SHA-1) K-283:(SHA-1) K-409:(SHA-1) K-571:(SHA-1) B-163: (SHA-1, 224, 256, 384, 512) B-233:(SHA-1) B-283:(SHA-1) B-409:(SHA-1) B-571:(SHA-1)) SHS: Val#1446 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 1.1, MDHA 2.0, PKHA-XT0.1, RNGB 2.1. Freescale's DMPR 11200121 is included in multiple QorIQ integrated communications processors, including: P3041, P2041, P2040, P5020, P5010, and P1010.

Table 76. ECDSA Certificate 419

Validation No.	419
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 12211040
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	06/20/2013
Description/ Notes	FIPS186-4: PKG: CURVES(P-192 K-163 B-163) SigGen: CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224:(SHA-1) P-256:(SHA-1) P-384:(SHA-1) P-521: K-163: (SHA-1, 224, 256, 384, 512) K-233:(SHA-1) K-283:(SHA-1) K-409:(SHA-1) K-571:(SHA-1) B-163: (SHA-1, 224, 256, 384, 512) B-233:(SHA-1) B-283:(SHA-1) B-409:(SHA-1) B-571:(SHA-1)) SHS: Val#2108 DRBG: Val# 94 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 1.2, MDHA 2.1, PKHA-SD32 1.0, RNGB 4.0. Freescale's DMPR 12211040 is included in the BSC9131 and BSC9132 QorIQ Qonverge processors.

Table 77. ECDSA Certificate 420

Validation No.	420
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 13221121
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04

Validation No.	420
Val.Date	06/20/2013
Description/ Notes	FIPS186-4: PKG: CURVES(P-192 K-163 B-163) SigGen: CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224:(SHA-1) P-256:(SHA-1) P-384:(SHA-1) P-521: K-163: (SHA-1, 224, 256, 384, 512) K-233:(SHA-1) K-283:(SHA-1) K-409:(SHA-1) K-571:(SHA-1) B-163: (SHA-1, 224, 256, 384, 512) B-233:(SHA-1) B-283:(SHA-1) B-409:(SHA-1) B-571:(SHA-1)) SHS: Val#2109 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 1.3, MDHA 2.2, PKHA-SD32 1.1, RNGB 2.1. Freescale's DMPR 13221121 is included in the P4080, Rev. 3 silicon, QorIQ integrated communications processor.

Table 78. ECDSA Certificate 421

Validation No.	421
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 20222141
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	06/20/2013
Description/ Notes	FIPS186-4: PKG: CURVES(P-192 K-163 B-163) SigGen: CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224:(SHA-1) P-256:(SHA-1) P-384:(SHA-1) P-521: K-163: (SHA-1, 224, 256, 384, 512) K-233:(SHA-1) K-283:(SHA-1) K-409:(SHA-1) K-571:(SHA-1) B-163: (SHA-1, 224, 256, 384, 512) B-233:(SHA-1) B-283:(SHA-1) B-409:(SHA-1) B-571:(SHA-1)) SHS: Val#2109 DRBG: Val# 348 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 2.0, MDHA 2.2, PKHA-SD64 2.1, RNG4 4.1. Freescale's DMPR 20222141 is included in multiple QorIQ integrated communications processor and co-processors, including: P5040, P5021, T4240 Rev. 1 silicon, T4160 Rev. 1 silicon, and B4860.

Table 79. ECDSA Certificate 422

Validation No.	422
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 30233242
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04

Validation No.	422
Val.Date	06/20/2013
Description/ Notes	FIPS186-4: PKG: CURVES(P-192 K-163 B-163) SigGen: CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224:(SHA-1) P-256:(SHA-1) P-384:(SHA-1) P-521: K-163: (SHA-1, 224, 256, 384, 512) K-233:(SHA-1) K-283:(SHA-1) K-409:(SHA-1) K-571:(SHA-1) B-163: (SHA-1, 224, 256, 384, 512) B-233:(SHA-1) B-283:(SHA-1) B-409:(SHA-1) B-571:(SHA-1)) SHS: Val#2110 DRBG: Val# 349 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs plus Descriptor Controller: DECO 3.0, MDHA 2.3, PKHA-SD128 3.2, RNG4 4.2. Freescale's DMPR 30233242 is included in multiple QorIQ integrated communications processor and co-processors, including: C291, C292, C293, T4240 Rev. 2 silicon, and T4160 Rev. 2 silicon.

Table 80. ECDSA Certificate 423

Validation No.	423
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 30231242
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	06/20/2013
Description/ Notes	FIPS186-4: PKG: CURVES(P-192 K-163 B-163) SigGen: CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224:(SHA-1) P-256:(SHA-1) P-384:(SHA-1) P-521: K-163: (SHA-1, 224, 256, 384, 512) K-233:(SHA-1) K-283:(SHA-1) K-409:(SHA-1) K-571:(SHA-1) B-163: (SHA-1, 224, 256, 384, 512) B-233:(SHA-1) B-283:(SHA-1) B-409:(SHA-1) B-571:(SHA-1)) SHS: Val#2110 DRBG: Val# 349 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 3.0, MDHA 2.3, PKHA-SD32 1.2, RNG4 4.2. Freescale's DMPR 30231242 is included in the T1040 QorIQ integrated communications processor.

Table 81. ECDSA Certificate 424

Validation No.	424
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 30232242
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04

Validation No.	424
Val.Date	06/20/2013
Description/ Notes	FIPS186-4: PKG: CURVES(P-192 K-163 B-163) SigGen: CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224:(SHA-1) P-256:(SHA-1) P-384:(SHA-1) P-521: K-163: (SHA-1, 224, 256, 384, 512) K-233:(SHA-1) K-283:(SHA-1) K-409:(SHA-1) K-571:(SHA-1) B-163: (SHA-1, 224, 256, 384, 512) B-233:(SHA-1) B-283:(SHA-1) B-409:(SHA-1) B-571:(SHA-1)) SHS: Val#2110 DRBG: Val# 349 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 3.0, MDHA 2.3, PKHA-SD64 2.2, RNG4 4.2. Freescale's DMPR 30232242 is included in the T2080 QorIQ integrated communications processor.

Table 82. ECDSA Certificate 1064

Validation No.	1064
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 31231342
Operational Environment	***Chronologic VCS simulator, vcs D-2010.06-04***
Val.Date	***12/20/2013***
Description/ Notes	FIPS186-4: PKG: CURVES(P-192 K-163 B-163) SigGen: CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224:(SHA-1) P-256:(SHA-1) P-384:(SHA-1) P-521: K-163: (SHA-1, 224, 256, 384, 512) K-233:(SHA-1) K-283:(SHA-1) K-409:(SHA-1) K-571:(SHA-1) B-163: (SHA-1, 224, 256, 384, 512) B-233:(SHA-1) B-283:(SHA-1) B-409:(SHA-1) B-571:(SHA-1)) SHS: Val# 2110 DRBG: Val# 349 NXP’s cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 3.1, MDHA 2.3, PKHA 1.3, RNG4 4.2. DMPR 31231342 is included in multiple QorIQ integrated communications processors including: LS1020A, LS1021A, LS1022A.

Table 83. ECDSA Certificate 1065

Validation No.	1065
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 40303443
Operational Environment	Cadence IES 15.10.009 Verilog simulator

Validation No.	1065
Val.Date	03/06/2017
Description/ Notes	FIPS186-4: PKG: CURVES(P-192 K-163 B-163) SigGen: CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224:(SHA-1) P-256:(SHA-1) P-384:(SHA-1) P-521: K-163: (SHA-1, 224, 256, 384, 512) K-233:(SHA-1) K-283:(SHA-1) K-409:(SHA-1) K-571:(SHA-1) B-163: (SHA-1, 224, 256, 384, 512) B-233:(SHA-1) B-283:(SHA-1) B-409:(SHA-1) B-571:(SHA-1)) SHS: Val# 3188 DRBG: Val# 1101 NXP's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 4.0, MDHA 3.0, PKHA 3.4, RNG4 4.3. DMPR 40303443 is included in multiple QorIQ integrated communications processors including: LS2040A, LS2045A, LS2080A, LS2085A, LS2044A, LS2048A, LS2084A, LS2088A.

Table 84. ECDSA Certificate 1066

Validation No.	1066
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 40241443
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	03/06/2017
Description/ Notes	FIPS186-4: PKG: CURVES(P-192 K-163 B-163) SigGen: CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224:(SHA-1) P-256:(SHA-1) P-384:(SHA-1) P-521: K-163: (SHA-1, 224, 256, 384, 512) K-233:(SHA-1) K-283:(SHA-1) K-409:(SHA-1) K-571:(SHA-1) B-163: (SHA-1, 224, 256, 384, 512) B-233:(SHA-1) B-283:(SHA-1) B-409:(SHA-1) B-571:(SHA-1)) SHS: Val# 3187 DRBG: Val# 1101 NXP's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 4.0, MDHA 2.4, PKHA 1.4, RNG4 4.3. DMPR 40241443 is included in multiple QorIQ integrated communications processors including: T1023, T1024.

Table 85. ECDSA Certificate 1067

Validation No.	1067
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 40251443
Operational Environment	Cadence IES 15.10.009 Verilog simulator

Validation No.	1067
Val.Date	03/06/2017
Description/ Notes	FIPS186-4: PKG: CURVES(P-192 K-163 B-163) SigGen: CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224:(SHA-1) P-256:(SHA-1) P-384:(SHA-1) P-521: K-163: (SHA-1, 224, 256, 384, 512) K-233:(SHA-1) K-283:(SHA-1) K-409:(SHA-1) K-571:(SHA-1) B-163: (SHA-1, 224, 256, 384, 512) B-233:(SHA-1) B-283:(SHA-1) B-409:(SHA-1) B-571:(SHA-1)) SHS: Val# 3192 DRBG: Val# 1101 NXP's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 4.0, MDHA 2.5, PKHA 1.4, RNG4 4.3. DMPR 40251443 is included in the QorIQ integrated communications processor: LS1012A.

Table 86. ECDSA Certificate 1068

Validation No.	1068
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 40301443
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	03/06/2017
Description/ Notes	FIPS186-4: PKG: CURVES(P-192 K-163 B-163) SigGen: CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224:(SHA-1) P-256:(SHA-1) P-384:(SHA-1) P-521: K-163: (SHA-1, 224, 256, 384, 512) K-233:(SHA-1) K-283:(SHA-1) K-409:(SHA-1) K-571:(SHA-1) B-163: (SHA-1, 224, 256, 384, 512) B-233:(SHA-1) B-283:(SHA-1) B-409:(SHA-1) B-571:(SHA-1)) SHS: Val# 3188 DRBG: Val# 1101 NXP's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 4.0, MDHA 3.0, PKHA 1.4, RNG4 4.3. DMPR 40301443 is included in multiple QorIQ integrated communications processors, including: LS1023A, LS1043A, LS1026A, LS1046A, LS1044A, LS1048A, LS1084A, LS1088A.

1.10 Key agreement and key derivation functions

The cryptographic boundary and definition of the certified implementation for pair-wise key establishment schemes using discrete logarithm cryptography and application-specific key derivation functions includes multiple "engines" within the SEC block, specifically the Descriptor Controller (DECO), PKHA, RNG, and MDHA. A Freescale/NXP QorIQ, QorIQ Qonverge, or C29x product is only listed if it contains the tested combination of these engines.

Freescale's application-specific key derivation functions and pair-wise key establishment schemes using discrete logarithm cryptography certificates are located at the following address: csrc.nist.gov/groups/STM/cavp/documents/components/componentnewval.html

1.10.1 Pair-wise key establishment schemes using discrete logarithm cryptography

Table 87. CVL Certificate 271, ECC

Validation No.	271
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 11200121
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	05/30/2014
Description/ Notes	SP800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Section 5.7.1.2: ECC CDH Primitive Curves tested: P-224 P-256 P-384 P-521 K-233 K-283 K-409 K-571 B-233 B-283 B-409 B-571 Freescale's cryptographic boundary for DSA, ECDSA, RSA, KAS and ASKDF includes the following CHAs plus Descriptor Controller: DECO 1.1, MDHA 2.0, PKHA-XT0.1, RNGB 2.1. Freescale's DMPR11200121 is included in multiple QorIQ integrated communications processors, including: P3041, P2041, P2040, P5020, P5010, and P1010.

Table 88. CVL Certificate 273, ECC

Validation No.	273
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 12211040
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	05/30/2014
Description/ Notes	SP800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Section 5.7.1.2: ECC CDH Primitive Curves tested: P-224 P-256 P-384 P-521 K-233 K-283 K-409 K-571 B-233 B-283 B-409 B-571 Freescale's cryptographic boundary for DSA, ECDSA, RSA, KAS and ASKDF includes the following CHAs plus Descriptor Controller: DECO 1.2, MDHA 2.1, PKHA-SD32 1.0, RNGB 4.0. Freescale's DMPR 12211040 is included in the QorIQ integrated communications processors: BSC9131 and BSC9132.

Table 89. CVL Certificate 275, ECC

Validation No.	275
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 13221121
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	05/30/2014
Description/ Notes	SP800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Section 5.7.1.2: ECC CDH Primitive Curves tested: P-224 P-256 P-384 P-521 K-233 K-283 K-409 K-571 B-233 B-283 B-409 B-571 Freescale's cryptographic boundary for DSA, ECDSA, RSA, KAS and ASKDF includes the following CHAs plus Descriptor Controller: DECO 1.3, MDHA 2.2, PKHA-SD32 1.1, RNGB 2.1. Freescale's DMPR 13221121 is included in the P4080, Rev. 3 silicon, QorIQ integrated communications processors.

Table 90. CVL Certificate 277, ECC

Validation No.	277
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 30233242
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	05/30/2014
Description/ Notes	SP800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Section 5.7.1.2: ECC CDH Primitive Curves tested: P-224 P-256 P-384 P-521 K-233 K-283 K-409 K-571 B-233 B-283 B-409 B-571 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs plus Descriptor Controller: DECO 3.0, MDHA 2.3, PKHA-SD128 3.2, RNG4 4.2. Freescale's DMPR 30233242 is included in multiple QorIQ integrated communications processors and co-processors, including: C291, C292, C293, T4240 Rev. 2 silicon, and T4160 Rev. 2 silicon.

Table 91. CVL Certificate 279, ECC

Validation No.	279
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR DMPR 30231242
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04

Validation No.	279
Val.Date	05/30/2014
Description/ Notes	SP800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Section 5.7.1.2: ECC CDH Primitive Curves tested: P-224 P-256 P-384 P-521 K-233 K-283 K-409 K-571 B-233 B-283 B-409 B-571 Freescale's cryptographic boundary for DSA, ECDSA, RSA, KAS and ASKDF includes the following CHAs and Descriptor Controller: DECO 3.0, MDHA 2.3, PKHA-SD32 1.2, RNG4 4.2. Freescale's DMPR30231242 is included in the T1040 QorIQ integrated communications processors.

Table 92. CVL Certificate 281, ECC

Validation No.	281
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 30232242
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	05/30/2014
Description/ Notes	SP800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Section 5.7.1.2: ECC CDH Primitive Curves tested: P-224 P-256 P-384 P-521 K-233 K-283 K-409 K-571 B-233 B-283 B-409 B-571 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs plus Descriptor Controller: DECO 3.0, MDHA 2.3, PKHA-SD64 2.2, RNG4 4.2. Freescale's DMPR 30232242 is included in the QorIQ T2080 integrated communications processors.

Table 93. CVL Certificate 283, ECC

Validation No.	283
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 20222141
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	05/30/2014
Description/ Notes	SP800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Section 5.7.1.2: ECC CDH Primitive Curves tested: P-224 P-256 P-384 P-521 K-233 K-283 K-409 K-571 B-233 B-283 B-409 B-571 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs plus Descriptor Controller: DECO 2.0, MDHA 2.2, PKHA-SD64 2.1, RNG4 4.1. Freescale's DMPR 20222141 is included in multiple QorIQ integrated communications processors and co-processors, including: P5040, P5021, T4240 Rev. 1 silicon, T4160 Rev. 1 silicon, and B4860.

Table 94. CVL Certificate 1119, ECC

Validation No.	1119
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 31231342
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	03/06/2017
Description/ Notes	SP800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Section 5.7.1.2: ECC CDH Primitive Curves tested: P-224 P-256 P-384 P-521 K-233 K-283 K-409 K-571 B-233 B-283 B-409 B-571 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs plus Descriptor Controller: DECO 3.1, MDHA 2.3, PKHA 1.3, RNG4 4.2. Freescale's DMPR 31231342 is included in multiple QorIQ integrated communications processors and co-processors, including: LS1020A, LS1021A, LS1022A.

Table 95. CVL Certificate 1121, ECC

Validation No.	1121
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 40303443
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	03/06/2017
Description/ Notes	SP800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Section 5.7.1.2: ECC CDH Primitive Curves tested: P-224 P-256 P-384 P-521 K-233 K-283 K-409 K-571 B-233 B-283 B-409 B-571 NXP’s cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 4.0, MDHA 3.0, PKHA 3.4, RNG4 4.3. DMPR 40303443 is included in multiple QorIQ integrated communications processors including: LS2040A, LS2045A, LS2080A, LS2085A, LS2044A, LS2048A, LS2084A, LS2088A.

Table 96. CVL Certificate 1123, ECC

Validation No.	1123
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 40241443
Operational Environment	Cadence IES 15.10.009 Verilog simulator

Validation No.	1123
Val.Date	03/06/2017
Description/ Notes	SP800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Section 5.7.1.2: ECC CDH Primitive Curves tested: P-224 P-256 P-384 P-521 K-233 K-283 K-409 K-571 B-233 B-283 B-409 B-571 NXP's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 4.0, MDHA 2.4, PKHA 1.4, RNG4 4.3. DMPR 40241443 is included in multiple QorIQ integrated communications processors including: T1023, T024.

Table 97. CVL Certificate 1125, ECC

Validation No.	1125
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 40251443
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	03/06/2017
Description/ Notes	SP800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Section 5.7.1.2: ECC CDH Primitive Curves tested: P-224 P-256 P-384 P-521 K-233 K-283 K-409 K-571 B-233 B-283 B-409 B-571 NXP's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 4.0, MDHA 2.5, PKHA 1.4, RNG4 4.3. DMPR 40251443 is included in the QorIQ integrated communications processor: LS012A.

Table 98. CVL Certificate 1127, ECC

Validation No.	1127
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 40301443
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	03/06/2017
Description/ Notes	SP800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Section 5.7.1.2: ECC CDH Primitive Curves tested: P-224 P-256 P-384 P-521 K-233 K-283 K-409 K-571 B-233 B-283 B-409 B-571 NXP's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 4.0, MDHA 3.0, PKHA 1.4, RNG4 4.3. DMPR 40301443 is included in multiple QorIQ integrated communications processors, including: LS1023A, LS1043A, LS1026A, LS1046A, LS1044A, LS1048A, LS1084A, LS1088A.

1.10.2 Application-specific key derivation functions

Table 99. CVL Certificate 272, KDF-135

Validation No.	272
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 11200121
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	05/30/2014
Description/ Notes	SP800-135: Recommendation for Existing Application-Specific Key Derivation Functions; Section 4.2: TLS TLS(TLS1.0/1.1 TLS1.2 (SHA 256 , 384)) SHA Val#1446 HMAC Val#967 Freescale's cryptographic boundary for DSA, ECDSA, RSA, KAS and ASKDF includes the following CHAs plus Descriptor Controller: DECO 1.1, MDHA 2.0, PKHA-XT0.1, RNGB 2.1. Freescale's DMPR11200121 is included in multiple QorIQ integrated communications processors, including: P3041, P2041, P2040, P5020, P5010, and P1010.

Table 100. CVL Certificate 274, KDF-135

Validation No.	274
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 12211040
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	05/30/2014
Description/ Notes	SP800-135: Recommendation for Existing Application-Specific Key Derivation Functions; Section 4.2: TLS TLS(TLS1.0/1.1 TLS1.2 (SHA 256 , 384)) SHA Val#2108 HMAC Val#1532 Freescale's cryptographic boundary for DSA, ECDSA, RSA, KAS and ASKDF includes the following CHAs plus Descriptor Controller: DECO 1.2, MDHA 2.1, PKHA-SD32 1.0, RNGB 4.0. Freescale's DMPR 12211040 is included in the QorIQ Integrated Communications Processors: BSC9131 and BSC9132.

Table 101. CVL Certificate 276, KDF-135

Validation No.	276
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 13221121

Validation No.	276
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	05/30/2014
Description/ Notes	SP800-135: Recommendation for Existing Application-Specific Key Derivation Functions; Section 4.2: TLS TLS(TLS1.0/1.1 TLS1.2 (SHA 256 , 384)) SHA Val#2109 HMAC Val#1533 Freescale's cryptographic boundary for DSA, ECDSA, RSA, KAS and ASKDF includes the following CHAs plus Descriptor Controller: DECO 1.3, MDHA 2.2, PKHA-SD32 1.1, RNGB 2.1. Freescale's DMPR13221121 is included in the P4080, Rev. 3 silicon, QorIQ integrated communications processor.

Table 102. CVL Certificate 278, KDF-135

Validation No.	278
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 30233242
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	05/30/2014
Description/ Notes	SP800-135: Recommendation for Existing Application-Specific Key Derivation Functions; Section 4.2: TLS and Section 4.1.2: IKEv2 TLS(TLS1.0/1.1 TLS1.2 (SHA 256 , 384)) SHA Val#2110 HMAC Val#1534 IKEv2((224 (SHA 1 , 256 , 384 , 512)) (384 (SHA 1 , 256 , 384 , 512)) (384 (SHA 1 , 256 , 384 , 512)) SHA Val#2110 HMAC Val#1534 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs plus Descriptor Controller: DECO 3.0, MDHA 2.3, PKHA-SD128 3.2, RNG4 4.2. Freescale's DMPR 30233242 is included in multiple QorIQ integrated communications processors and co-processors, including: C291, C292, C293, T4240 Rev. 2 silicon, and T4160 Rev. 2 silicon.

Table 103. CVL Certificate 280, KDF-135

Validation No.	280
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR DMPR 30231242
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04

Validation No.	280
Val.Date	05/30/2014
Description/ Notes	SP800-135: Recommendation for Existing Application-Specific Key Derivation Functions; Section 4.2: TLS and Section 4.1.2: IKEv2 TLS(TLS1.0/1.1 TLS1.2 (SHA 256 , 384)) SHA Val#2110 HMAC Val#1534 IKEv2((224 (SHA 1 , 256 , 384 , 512)) (4096 (SHA 1 , 256 , 384 , 512)) (384 (SHA 1 , 256 , 384 , 512)) SHA Val#2110 HMAC Val#1534 Freescale's cryptographic boundary for DSA, ECDSA, RSA, KAS and ASKDF includes the following CHAs and Descriptor Controller: DECO 3.0, MDHA 2.3, PKHA-SD32 1.2, RNG4 4.2. Freescale's 30231242 is included in the T1040 QorIQ integrated communications processor.

Table 104. CVL Certificate 282, KDF-135

Validation No.	282
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 30232242
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04
Val.Date	05/30/2014
Description/ Notes	SP800-135: Recommendation for Existing Application-Specific Key Derivation Functions; Section 4.2: TLS and Section 4.1.2: IKEv2 TLS(TLS1.0/1.1 TLS1.2 (SHA 256 , 384)) SHA Val#2110 HMAC Val#1534 IKEv2((224 (SHA 1 , 256 , 384 , 512)) (4096 (SHA 1 , 256 , 384 , 512)) (384 (SHA 1 , 256 , 384 , 512)) SHA Val#2110 HMAC Val#1534 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 3.0, MDHA 2.3, PKHA-SD64 2.2, RNG4 4.2. Freescale's DMPR 30232242 is included in the T2080 QorIQ integrated communications processor.

Table 105. CVL Certificate 284, KDF-135

Validation No.	284
Vendor	Freescale Semiconductor _____ Geoff Waters 7700 W.Parmer Lane _____ TEL: 512-996-5815 Austin, TX 78729 USA
Implementation	DMPR 20222141
Operational Environment	Chronologic VCS simulator, vcs D-2010.06-04

Validation No.	284
Val.Date	05/30/2014
Description/ Notes	SP800-135: Recommendation for Existing Application-Specific Key Derivation Functions; Section 4.2: TLS TLS(TLS1.0/1.1 TLS1.2 (SHA 256 , 384)) SHA Val#2109 HMAC Val#1533 Freescale's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 2.0, MDHA 2.2, PKHA-SD64 2.1, RNG4 4.1. Freescale's DMPR 20222141 is included in multiple QorIQ integrated communications processors and co-processors, including: P5040, P5021, T4240 Rev. 1 silicon, T4160 Rev. 1 silicon, and B4860.

Table 106. CVL Certificate 1118, KDF-135

Validation No.	1118
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 31231342
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	03/06/2017
Description/ Notes	SP800-135: Recommendation for Existing Application-Specific Key Derivation Functions; Section 4.2: TLS TLS(TLS1.0/1.1 TLS1.2 (SHA 256 , 384)) SHA Val#2109 HMAC Val#1533 NXP's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 3.1, MDHA 2.3, PKHA 1.3, RNG4 4.2. NXP’s DMPR 31231342 is included in multiple QorIQ integrated communications processors and co-processors, including: LS1020A, LS1021A, LS1022A.

Table 107. CVL Certificate 1120, KDF-135

Validation No.	1120
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 40303443
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	03/06/2017
Description/ Notes	SP800-135: Recommendation for Existing Application-Specific Key Derivation Functions; Section 4.2: TLS TLS(TLS1.0/1.1 TLS1.2 (SHA 256 , 384)) SHA Val#2109 HMAC Val#1533 NXP's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 4.0, MDHA 3.0, PKHA 3.4, RNG4 4.3. NXP’s DMPR 40303443 is included in multiple QorIQ integrated communications processors and co-processors, including: LS2040A, LS2045A, LS2080A, LS2085A, LS2044A, LS2048A, LS2084A, LS2088A.

Table 108. CVL Certificate 1122, KDF-135

Validation No.	1122
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 40241443
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	03/06/2017
Description/ Notes	SP800-135: Recommendation for Existing Application-Specific Key Derivation Functions; Section 4.2: TLS TLS(TLS1.0/1.1 TLS1.2 (SHA 256 , 384)) SHA Val#2109 HMAC Val#1533 NXP's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 4.0, MDHA 2.4, PKHA 1.4, RNG4 4.3. NXP’s DMPR 40241443 is included in multiple QorIQ integrated communications processors and co-processors, including: T1023, T024.

Table 109. CVL Certificate 1124, KDF-135

Validation No.	1124
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 40251443
Operational Environment	Cadence IES 15.10.009 Verilog simulator
Val.Date	03/06/2017
Description/ Notes	SP800-135: Recommendation for Existing Application-Specific Key Derivation Functions; Section 4.2: TLS TLS(TLS1.0/1.1 TLS1.2 (SHA 256 , 384)) SHA Val#2109 HMAC Val#1533 NXP's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 4.0, MDHA 2.5, PKHA 1.4, RNG4 4.3. NXP’s DMPR 40251443 is included in the QorIQ integrated communications processor: LS1012A.

Table 110. CVL Certificate 1126, KDF-135

Validation No.	1126
Vendor	NXP Semiconductor _____ Geoff Waters 6501 W.William Cannon Drive_____ TEL: 512-895-2069 Austin, TX 78735 USA
Implementation	DMPR 40301443
Operational Environment	Cadence IES 15.10.009 Verilog simulator

Validation No.	1126
Val.Date	03/06/2017
Description/ Notes	SP800-135: Recommendation for Existing Application-Specific Key Derivation Functions; Section 4.2: TLS TLS(TLS1.0/1.1 TLS1.2 (SHA 256 , 384)) SHA Val#2109 HMAC Val#1533 NXP's cryptographic boundary for DSA, ECDSA and RSA includes the following CHAs and Descriptor Controller: DECO 4.0, MDHA 3.0, PKHA 1.4, RNG4 4.3. DMPR 40301443 is included in multiple QorIQ integrated communications processors, including: LS1023A, LS1043A, LS1026A, LS1046A, LS1044A, LS1048A, LS1084A, LS1088A.

2 Revision history

This table provides a revision history for this document.

Table 111. Revision history

Revision	Date	Substantive change(s)
1.9	03/2017	• Added new certificates in each section.
1.8	10/2016	• Updated links to NIST CAVP validation lists
1.7	03/2015	• Added device part numbers (P1024, P1015, P1025, P1016) to some certificates.”
1.6	07/2014	• Added Section 1.10, “Key agreement and key derivation functions.” • Fixed minor typos throughout document. Corrected dates from 2103 to 2013. • Updated PSC9131 and PSC9132 to BSC9131 and BSC9132, respectively. • Removed Section 1 heading “CAVP-to-CMVP mapping.” • Added Table 1, “Certificates of validation for Freescale devices.”
1.5	01/2014	• Reorganized RNG certifications so that they appear before asymmetric crypto certifications. • Added new certificates in each section.
1.4	03/2012	• Updated part numbers associated with various certificates. • Added RNG certificate #818.
1.3	06/2011	Added new certificates in each section.
1.2	09/2010	Reformatted document for clarity.
1.1	08/2010	Updated part numbers.
1.0	04/2010	Initial public release