

Sdbgmto k dedpmtd

CuBq g74/ Htr

Udq lmm0-/ 5-/ 0

tsgnq	Snahr Ehrjd
Rs str	dld rdc

Snahr Elmjd	1/04-/4-11	0-/1-//	hsh kUdq lmmneL HB NR B X C WD
Snahr Elmjd	1/04-/6-17	0-/0-//	- ccde R I Jd V q oolmf Rdqubd- - ccde oolpplm lsd r enqsgd hsh kh smm- - ccde Kh ls smmenql tskold b k ne rnl d Bq Oq lsd=Toc sd' (et nbsmmr -
Snahr Elmjd	1/04-/7-1/	0-/1-//	- ccde Kh ls smm9Cledqns Rdqubdr b ms ad bddr rdc lmo q kdk - ccde cdr bcdsmmenq anqmf rdqubdr - - Bg nfd c lmbk cd r sq bst qd-
Snahr Elmjd	1/05-/0-00	0-/1-/0	- Bq RgdOqrf F dmlq sd bbdos qdr t kKdnf sgr l kdqsg m05 a sd-
Snahr Elmjd	1/05-/5-06	0-/2-//	- Bnnefi nosmmlekdnf sgnel b hm L bUdqe m lmsdqpdsd r als - - Bnnefi nosmmgnv jd ldr qd l oodc- - Bnnefi nosmmenqHB TR a rd ccqrr- - Bg nfd lmsgd v gnv L3 ncl L4 qd qst qrdc esdqjd oqulm lmmmf -
Snahr Elmjd	1/05-/7-/0	0-/2-/0	- ccde Sh dnt s OH - Bg nfd cde tkl oolmf lmsgd l oodc Trd-B rd enq L JDX apl / DD sn / // -
Snahr Elmjd	1/05-00-13	0-/3-//	- ccde Bnnefi t q smmv lsg C Ulnbh Bnnefi t q sq4 - dl nudc R I Jd V q oEnqjd Oqulm lmmmf
Snahr Elmjd	1/06-/3-/5	0-/4-//	- Toc sd c et nbsmmcdrbqosmmr - Bnnefi nosmmenqEGUDrt oonq - Bnnefi nosmmenqg qv qd dqqqbncd b knts - Bnnefi nosmmenqc s ekr g bnnsqk b knts - Bnnefi nosmmenqc s ekr g r nbgqrn smmb knts - - Cdr bcdsmmned bkr lwd qd r
Snahr Elmjd	1/06-/3-02	0-/4-/0	- Ehdc enq ssnf ncl rod kmf
Snahr Elmjd	1/06-/6-03	0-/4-/1	- c osmmen a rd bnl onmdns
Snahr Elmjd	1/06-0/-01	0-/5-//	- ccde RdleSdrs - R edArv dkd rd
Snahr Elmjd	1/06-0/-08	0-/5-/0	- Bg nfd c lmbk cd r sq bst qd

[1]	TSNR	TSNR RV R Bq osnRdquhdL m f d q o c e	0-1 -/
[2]	TSNR	TSNR S ARV L n c t k d K m s o c e	0-5 -/
[3]	GHR	RGD - Et n b s m m k R o d b l e t b s m m	0-0
[4]	DMDR R	Tr d q r L n t k G 7 4 / . E 0 K H B T R A	0- / /



Sgl m r l a n k b k n t q s s d n s m m s n v q n m f r -



V d g u d b n n e f t q c s g d o q f q l r l m b b n c p n b d v l s g n t q r o d b l e t b s m m l m s g d  
p t d r s m m h p - V g d q r s g d o q f q l r c n r t o o n s n s g d q b n n e f t q s m m s g m s g d n n d  
r o d b l e t b l m n t q p t d r s m m h p U d b s n q r q l d r d n e s g d o q f q l r c d k u d q c n n t q  
b n l o m l m d o q l r r k q l r s d b s c n s g d b n n e f t q s m m n t g u d r o d b l e t b l m s g d  
p t d r s m m h p -

1-0	qglst q Nudqdv .....	01
2-0	Ed st qdr .....	03
2-1	Hsh kh smm.....	03
2-2	Rs sdr .....	04
2-3	L hmEt mbsmmr .....	05
2-4	r mbgqmmtr G mckmf .....	05
2-5	Jd G mckmf .....	06
2-6	Jd L oohmf .....	06
2-7	Jd Toc sd.....	07
2-8	F dmdq koqbdct qd ner dqlbd d dbt smm.....	07
2-0/	Sh dnts G mckmf .....	10
2-00	Dqmq G mckmf .....	12
2-00-0	Cdudkol dms Dqmq donqsmf .....	12
2-00-1	Oqct bsmmBncd Dqmq donqsmf .....	12
2-01	RdleSdr s.....	12
3-0	Rbnod neCdldq .....	13
3-0-0	Rs sh Ehdr .....	13
3-0-1	C m l to Ehdr .....	14
3-0-2	B kntsEhdr .....	14
3-1	Bqsh kRdbsmm .....	15
3-2	Hkt cd Rst bst qd.....	16
3-3	Bnl ohdq arsq bsmm mc L dl nq L oohmf .....	17
4-0	Hsdq bdr Nudqdv .....	18
4-1	S od Cdentsmm .....	18
4-2	Rst bst qdr .....	2/
4-2-0	Bnref t q smmr sq bst qdr .....	2/
4-2-0-0	Bq 2/ g74/ Htr dr Dmbq os017Bnref S od .....	2/
4-2-0-1	Bq 2/ g74/ Htr dr Cdbq os017Bnref S od .....	20
4-2-0-2	Bq 2/ g74/ Htr BI b dr 017F dnBnref S od .....	20
4-2-0-3	Bq 2/ g74/ Htr BI b dr 017UdcBnref S od.....	21

	4-2-04	Bq 2/	g74/ Htr Jd D sq bsBnref S od .....	21
	4-2-05	Bq 2/	g74/ Htr Jd V q oR I Bnref S od.....	22
	4-2-06	Bq 2/	g74/ Htr nf Bnref S od.....	22
4-3	Rdqlodr oqudc a B X 2/	G74/ HB TR.....		23
	4-3-0	Bq 2/	g74/ Htr Hts.....	23
	4-3-1	Bq 2/	g74/ Htr Hts dl nq .....	23
	4-3-2	Bq 2/	g74/ Htr F dsUdq lmmrten .....	24
	4-3-3	Bq 2/	g74/ Htr dr Dmbq os017Rs ç.....	25
	4-3-4	Bq 2/	g74/ Htr dr Dmbq os017Toc sd .....	26
	4-3-5	Bq 2/	g74/ Htr dr Dmbq os017Ehmln g .....	28
	4-3-6	Bq 2/	g74/ Htr dr Dmbq os017L hmEt nbsmm.....	3/
	4-3-7	Bq 2/	g74/ Htr dr Cdbq os017Rs ç.....	30
	4-3-8	Bq 2/	g74/ Htr dr Cdbq os017Toc sd .....	31
	4-3-0/	Bq 2/	g74/ Htr dr Cdbq os017Ehmln g .....	33
	4-3-00	Bq 2/	g74/ Htr dr Cdbq os017L hmEt nbsmm.....	34
	4-3-01	Bq 2/	g74/ Htr Bl b dr 017F dnrRs ç.....	35
	4-3-02	Bq 2/	g74/ Htr Bl b dr 017F dnrToc sd .....	36
	4-3-03	Bq 2/	g74/ Htr Bl b dr 017F dnrEhmln g .....	37
	4-3-04	Bq 2/	g74/ Htr Bl b dr 017F dnrL hmEt nbsmm.....	4/
	4-3-05	Bq 2/	g74/ Htr Bl b dr 017UdqRs ç.....	40
	4-3-06	Bq 2/	g74/ Htr Bl b dr 017UdqToc sd .....	41
	4-3-07	Bq 2/	g74/ Htr Bl b dr 017UdqEhmln g .....	43
	4-3-08	Bq 2/	g74/ Htr Bl b dr 017Udq hmEt nbsmm.....	44
	4-3-1/	Bq 2/	g74/ Htr Jd D sq bsRs ç.....	45
	4-3-10	Bq 2/	g74/ Htr Jd D sq bsToc sd .....	46
	4-3-11	Bq 2/	g74/ Htr Jd D sq bsEhmln g .....	48
	4-3-12	Bq 2/	g74/ Htr Jd D sq bsL hmEt nbsmm.....	5/
	4-3-13	Bq 2/	g74/ Htr Jd V q oR I Rs ç.....	50
	4-3-14	Bq 2/	g74/ Htr Jd V q oR I Toc sd .....	51
	4-3-15	Bq 2/	g74/ Htr Jd V q oR I Ehmln g .....	52
	4-3-16	Bq 2/	g74/ Htr Jd V q oR I L hmEt nbsmm.....	53
	4-3-17	Bq 2/	g74/ Htr nf RddcRs ç.....	54
	4-3-18	Bq 2/	g74/ Htr nf RddcToc sd .....	55
	4-3-2/	Bq 2/	g74/ Htr nf RddcEhmln g .....	56
	4-3-20	Bq 2/	g74/ Htr nf RddcL hmEt nbsmm.....	57
	4-3-21	Bq 2/	g74/ Htr nf F dndq sd .....	58
	4-3-22	Bq 2/	g74/ Htr nf F dndq sdL hmEt nbsmm.....	6/
	5.4.34	Bq 2/	g74/ Htr Rdks s.....	60
4-4	Bnref tq ald hndq bdr .....			60
	4-4-0	B kntsEt nbsmm .....		60
	4-4-0-0	Sh dnts OHKnB smmB kns.....		61

4-4-0-1	Sh dnt s OHKno B knts.....	62
4-4-0-2	Bq 2/ g74/ Htr G qv qdDqnd B knts.....	62
4-4-0-3	Bq 2/ g74/ Htr C s Ekrg d cRs q B knts.....	63
4-4-0-4	Bq 2/ g74/ Htr C s Ekrg d cDnc B knts.....	63
4-4-0-5	Bq 2/ g74/ Htr C s EkrgV qdRs q B knts.....	64
4-4-0-6	Bq 2/ g74/ Htr C s EkrgV qdDnc B knts.....	64
4-4-0-7	Bq 2/ g74/ Htr C s EkrgRds d cLncd B knts..	65
4-4-0-8	Bq 2/ g74/ Htr C s Ekrg d qEqnl Bnl l mKnbjdcRs sd B knts 6	
4-5	Rdqlodr trdc a B X 2/ G74/ HB TR.....	66
4-6	Rdqlod Onqr .....	66
.....		
5-0	Bnnrt q smmU q nqr .....	67
5-1	Cduh smmr .....	67
5-2	ccsmmr. D sdmr lmmr .....	67
5-2-0	Sh dntsg mknf .....	67
5-2-1	G qv qd dqnqb knts.....	67
5-2-2	C s ekrg r nbqqrnh smm.....	67
5-3	Kh ls smmr .....	67
5-3-0	Rt oonqneBq onf q ogld Rdqlodr .....	67
5-3-1	O q kdk bddr sn Rdqlodr .....	68
.....		
6-0	Fknrr q .....	7/
6-1	aaqluh smmr .....	7/
.....		

Elft qd 1-0	TSNR 3- dpglsbst qd Nudqulv .....	01
Elft qd 1-19	hscq bdr sn ci bdrsl nctldr nesgd B X 2/ G74/ HB TR.....	02
Elft qd 2-09	Rs sd bg qnesgd f k a kr dquhd rs sd .....	04
Elft qd 2-19	Rdpt dmbd bg qsn rgnv md l old nesgd r nbgqmmtr oqdbdr hmf nesgd g qv qd B X.....	1/
Elft qd 2-2	D l old Rdpt dmbd enqSh dnts OHb knsr ctqmf L B F dmdq smm.....	11
Elft qd 3-0	hbk cd r sq bst qd .....	16

S ald 0-0	Bnl onmdmsghnsq .....	0/
S ald 2-0	Rtoocqdc TSNR rs mc q bnneq ed st qdr .....	03
S ald 2-1	L oohmf neJd k sn RGD Jd r kns' .....	07
S ald 3-0	Rs sh ddr .....	14
S ald 3-1	F dmdq sdc ddr .....	14
S ald 3-2	F dmdq sdc ddr .....	14
S ald 3-3	Bnl omdq arsq bsmm nc l dl nq l oohmf .....	17
S ald 4-0	S od cdehsmm .....	18
S ald 4-1	Bq 2/ g74/ Htr dr Dmbq os017Bnnef S od .....	2/
S ald 4-2	Bq 2/ g74/ Htr dr Cdbq os017Bnnef S od .....	20
S ald 4-3	Bq 2/ g74/ Htr BI b dr 017F dmBnnef S od .....	20
S ald 4-4	Bq 2/ g74/ Htr BI b dr 017UdcBnnef S od.....	21
S ald 4-5	Bq 2/ g74/ Htr Jd D sq bsBnnef S od .....	21
S ald 4-6	Bq 2/ g74/ Htr Jd V q oR l Bnnef S od.....	22
S ald 4-7	Bq 2/ g74/ Htr mf Bnnef S od.....	22
S ald 4-8	Bq 2/ g74/ Htr hns.....	23
S ald 4-0/	Bq 2/ g74/ Htr hnsL dl nq .....	23
S ald 4-00	Bq 2/ g74/ Htr F dsJdq hnmhns.....	24
S ald 4-01	Bq 2/ g74/ Htr dr Dmbq os017Rs q.....	25
S ald 4-02	Bq 2/ g74/ Htr dr Dmbq os017Toc sd.....	27
S ald 4-03	Bq 2/ g74/ Htr dr Dmbq os017Ehnm g.....	28
S ald 4-04	Bq 2/ g74/ Htr dr Dmbq os017L hnmEt nbsmm.....	3/
S ald 4-05	Bq 2/ g74/ Htr dr Cdbq os017Rs q.....	30
S ald 4-06	Bq 2/ g74/ Htr dr Cdbq os017Toc sd .....	32
S ald 4-07	Bq 2/ g74/ Htr dr Cdbq os017Ehnm g .....	33
S ald 4-08	Bq 2/ g74/ Htr dr Cdbq os017L hnmEt nbsmm.....	34
S ald 4-1/	Bq 2/ g74/ Htr BI b dr 017F dmRs q.....	35
S ald 4-10	Bq 2/ g74/ Htr BI b dr 017F dmToc sd.....	36
S ald 4-11	Bq 2/ g74/ Htr BI b dr 017F dmEhnm g.....	38
S ald 4-12	Bq 2/ g74/ Htr BI b dr 017F dmL hnmEt nbsmm.....	4/
S ald 4-13	Bq 2/ g74/ Htr BI b dr 017UdcRs q.....	40
S ald 4-14	Bq 2/ g74/ Htr BI b dr 017UdcToc sd .....	42
S ald 4-15	Bq 2/ g74/ Htr BI b dr 017UdcEhnm g.....	44
S ald 4-16	Bq 2/ g74/ Htr BI b dr 017Udc hnmEt nbsmm.....	44
S ald 4-17	Bq 2/ g74/ Htr Jd D sq bsRs q.....	45
S ald 4-18	Bq 2/ g74/ Htr Jd D sq bsToc sd.....	47
S ald 4-2/	Bq 2/ g74/ Htr Jd D sq bsEhnm g .....	48
S ald 4-20	Bq 2/ g74/ Htr Jd D sq bsL hnmEt nbsmm.....	5/
S ald 4-21	Bq 2/ g74/ Htr Jd V q oR l Rs q.....	50
S ald 4-22	Bq 2/ g74/ Htr Jd V q oR l Toc sd .....	51
S ald 4-23	Bq 2/ g74/ Htr Jd V q oR l Ehnm g.....	52

S ald 4-24	Bq 2/ g74/ Htr	Jd V q oR I L mEt nbsmm.....	53
S ald 4-25	Bq 2/ g74/ Htr	mf RddcRs ç.....	54
S ald 4-26	Bq 2/ g74/ Htr	mf RddcToc sd.....	55
S ald 4-27	Bq 2/ g74/ Htr	mf RddcEhmg.....	56
S ald 4-28	Bq 2/ g74/ Htr	mf RddcL mEt nbsmm.....	57
S ald 4-3/	Bq 2/ g74/ Htr	mf F dmdq sd.....	58
S ald 4-30	Bq 2/ g74/ Htr	mf F dmdq sdL mEt nbsmm.....	6/
S ald 4-31	Bq 2/ g74/ Htr	RdlsSdrs.....	60
S ald 4-32	Zsh dnts- OHnb smmb knts	.....	61
S ald 4-33	Zsh dnts- OHknoB knts	.....	62
S ald 4-34	Bq 2/ g74/ Htr	G çv çDçpBncd B knts.....	63
S ald 4-35	Bq 2/ g74/ Htr	C s Ekrg d cRs ç B knts.....	63
S ald 4-36	Bq 2/ g74/ Htr	C s Ekrg d cDmc B knts.....	64
S ald 4-37	Bq 2/ g74/ Htr	C s EkrgV çdRs ç B knts.....	64
S ald 4-38	Bq 2/ g74/ Htr	C s EkrgV çdDmc B knts.....	65
S ald 4-4/	Bq 2/ g74/ Htr	C s EkrgRds d cLncd B knts.....	65
S ald 4-40	.Bq 2/ g74/ Htr	C s Ekrg dst çrEqnl Bnl I mKnbjdcRs sd B knts65	
S ald 4-41	Rdquhtr trdc a sgd B X 2/ G74/ HB TR	.....	66
S ald 5-0	Rtoonçdc TSNR rs mc ç bnnd çd st çlr	.....	67
S ald 6-0	Fkrr q	.....	7/
S ald 6-1	aaçduh smmr	.....	7/



# 1

Sgd bnl onndns gnsq fudr m nudqnd nudq sgd h onq ns l hdsndr sg s qd r toonqdc lmsgd clndnsudq lmm nesgd bnl onndns

0-/-/-	- Hh kudq lmm ADS
0-/-/0	- Ehdc l m bdk mndr v qmfr
0-0-/-	- Ehdc DR dnb.cdb mc BL B f dmudqv gdmtr hrf jd r ks- - Ehdc v qmfr a sd nqdv gdmq chlrf mc v qmfr eqpl .sn HB T-
0-1-/-	- Bg r fdc RE bddr eqpl als dclr sn l r j nodq smm - L HB bnl ok nbd mc h oqudc qatrndr - - Ehdc bnl ok dclqnd lmm r nbqnmtr bnnef t q smm - ccdr s d l bghnd eqRGD Rdqldr - - ccdr cclsmm kbgdbjr eqJd D sq bsv gdmqulm mtr hrf m dm akdc
0-1-/0	- ccdr bgdbj adnq mtr hrf b nbdkbnl l mc sn oqudnr akbj hrf ne DBT - Ehdc l mtr hrf cdndr eqB Xrs d l bghnd - Ehdc v qmfr g mtr hrf neL B sq nb smm mBI b dr 017F dm mc BI b dr 017UF dm
0-1-/1	- Ehdc mtr d v hq qdtr s nq mcnl mtr adq r l kqsg m05 a sdr
0-2-/-	- Ehdc Rt oonq enq1/ jd r ks mtr TRC mc HB TRD - Bnnef nosm m nqu q akd a rd ccqrr ne HB TR - Bnnef t q ak mndq ds smm nesgd Jd k - Trd BL C L B UD HEX mtr d c ne BL C L B F DMD SD mtr b uddq smm oq hnd - ccdr r toonq enq b kdr sg mtr s nqL bUddq
0-2-/0	- Ehdc atedqndqnd mBq 2/ g74/ Htr Jd D sq bsv gdm Br l R l Jd D sq bL Jd Rh d m r l kqsg m37 a sdr mc B X 2/ G74/ HB TR JDXV ORXL EN O NUH R M m RSC NEE
0-2-/1	ccdr Sh dnt s OH
1-/-/-	- ED S-08849 Rt oonq B X'GV ( mc B X'RV ( lmsgd r l d R d - Ehdc DBB-Dqnm OOL adb trdu q akd kb sdc mtr qmfr l dl nq rdb smm - L bUddq smm b trdr sg DBT sn akbj nm OOL cdq smdr
1-/-/0	- ccdr r toonq enq EGUD nmcdq smdr kjd OOL - Ehdc v qmfr r nes qd bgdbj eqbnq pbs tsg k
1-0-/-	- ccdr B ktr eqC s Ekrg R nbqnm smm - ccdr B ktr sn g mcd E B Hnd qd bnl l mtr - ccdr B ktr sn oqudc mndq k HB TR dclqnd sn sgd ook smm - Ehdc rs d g mtr hrf neq mcnl f dndq sd mtr r nb bnnef t q smm
1-0-/0	- dl nudc t mndr q mtr cdr - Cdr b q smm eqR edArv q l mtr hrf - Ctr akd mtr dcl g dclqnd nbd smm
1-1-/-	- c osm msn a rd bnl onndns - Ehdc Rdbn mc jd r ks mtr akd mtr V bnnef t q smm

	- Sh dntsknb smmb kntsoqutdr v qnf hndq smm
1-/1-/0	- Ehdc Bnl ohaqDmçV qnf cden enql dl bkrr hmETMB'(I bq ne Bq 2/ g74/ Htr nf RddcEhmg hndq k
1-/2-/1	- ccdc RdleSdrs - R æArv dkd rd
1-/2-/0	- Bg nf dc hmbt cd ræt bst qd

S ald 0-0 Bnl onndnsghnsq

## 2

Sgln cnbtI dms cdrbqadr sgd et nbsmm ks OH mc bnneft q smm ne sgd L HB NR  
I nctId B X 2/ G74/ HB TR r rodblet c lmZ -

	3	
	Oqd-Bnl ohtd	
	B X UDMCN HC	2/ cdbth k '< Udbnqhtnd stj bbnqhtf sn GHR(
	B X LNCTKD HC	144 cdbth k ' bbnqhtf sn qde Z (

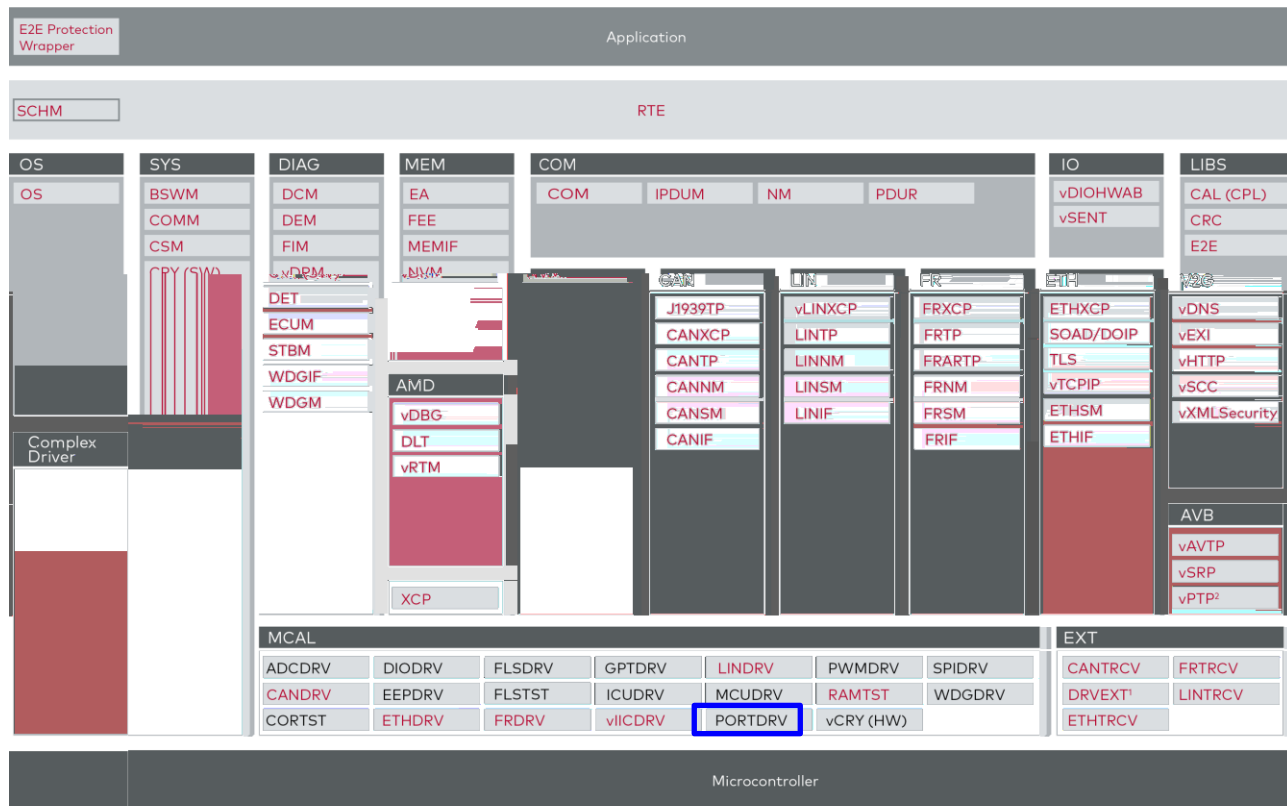
) Enqsgd oqpbmd TSNR dkd rd 3- okd rd rdd sgd qld rd rodblet cnbtI dms smm-

Sgln cnbtI dms cdrbqadr sgd et nbsmm ks mc OHne sgd B X I nctId r g qv qd  
cdodmednsI nctId-

Sgd Bq onf q ogth kaq q I nctId 'B X( neeq bq onf q ogth odh Isudr - Sgd B X I nctId  
m trdc a sgd Bq on Rdqhtd L m fdq' BRL (-

## 2.1 Architecture Overview

Sgd enkv hf t q r gnv r v gdq sgd B X 2/ G74/ HBTR h kb sdc hmsgd TSNR  
 qghsbt q-



XT, ETHDRVEXT Vector Standard Software 3rd Party Software

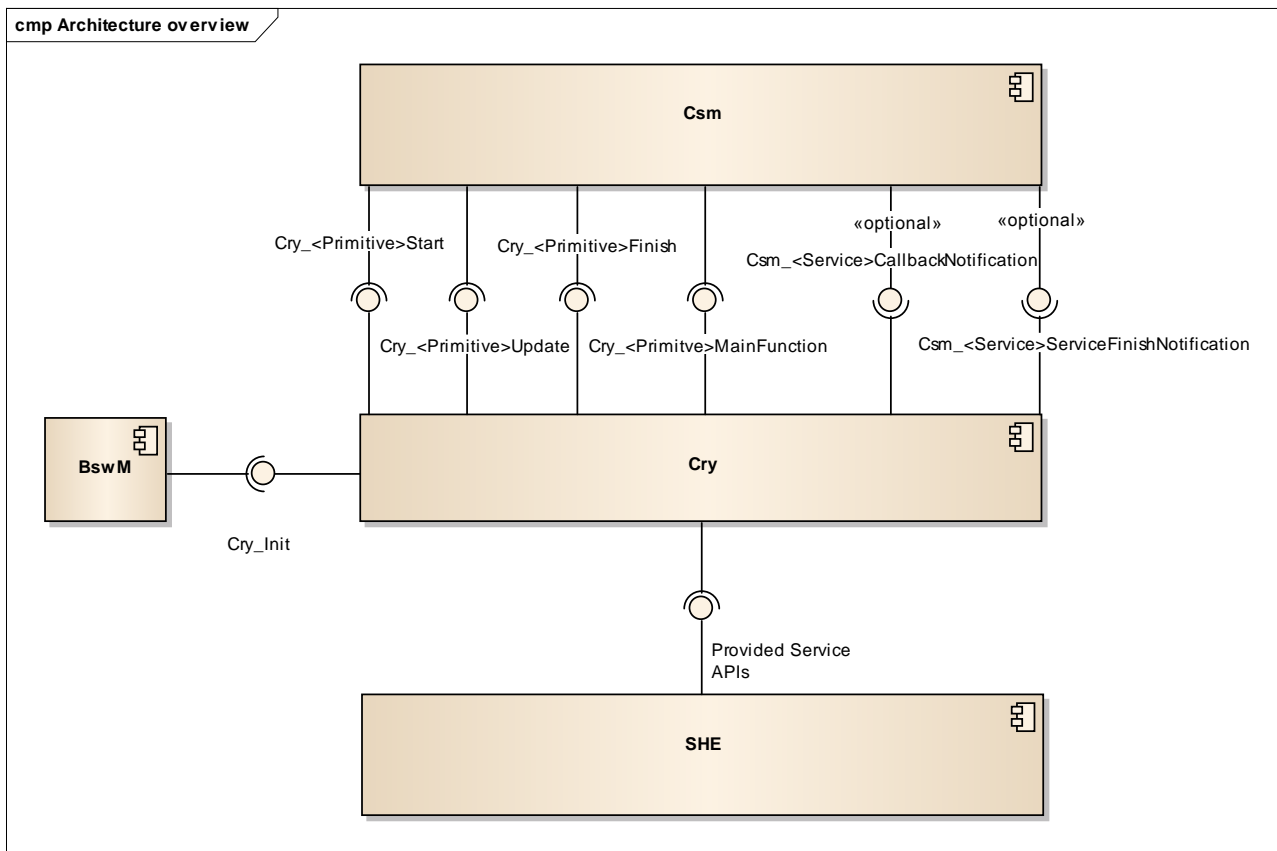
ITSYN and STBM

1 Includes EXTADC, EEPEXT, FLSE and WDGEXT

2 Functionality represented in ETH

Elf t q 1-0 TSNR 3- qghsbt q Nudqtdv

Sgd m d s f t q r g n v r sgd m d e b d r n c i b d n s l n c t k d r n e sgd B X 2/ G74/ HB TR-  
Sgdr d m d e b d r q d c d r b d a d c l m b g o s d q 4-



Elf t q 1-19 m d e b d r n c i b d n s l n c t k d r n e sgd B X 2/ G74/ HB TR

## 3

### 3.1 Features

Sgd æd st qpr hnsdc hmsgd ænkav hmf s akdr bnudqsgd bnl okdsd æ nbsmm ks r odblædc ænqsgd B X 2/ G74/ HBTR-

Sgd TSNR rs mc q æ nbsmm ks m r odblædc hm ZD sgd bnæpr onmchmf æd st qpr qd hnsdc hmsgd s akdr

> S ald 2-0 Rt oonædc TSNR rs mc q bnænd æd st qpr

Sgd ænkav hmf æd st qpr r odblædc hm ZD qd rt oonædc9

R mæqnmtr ina oqbdrr hmf
r mæqnmtr ina oqbdrr hmf
Rdæpæd ænqR I I dsæp khsæp bd ' DR017(
Rdæpæd ænqL B hnsæp bd 'BL B(
Rdæpæd ænq mænl hnsæp bd 'O MF(
Rdæpæd ænqR I I dsæp kJd D sq bs hnsæp bd
Rdæpæd ænqR I I dsæp kJd V q oohmf hnsæp bd

S ald 2-0 Rt oonædc TSNR rs mc q bnænd æd st qpr

### 3.2 Initialization

Adæq b hmf m nsædq æ nbsmm ks ne sgd B X I nctkd sgd hnskh smm æ nbsmm Cry\_30\_Rh850Icus\_Init()g r sn ad b kdc srs æto d-f-a ArvL nqDbtL -

Enq OHæds h æpæqsn bg osæq4-3-0 Bq 2/ g74/ HBtr hns-

Sgd B X I nctkd rrtl dr sg srnl du q akdr qd hnskhdc v hsg bdæp hmu kt dr srs æto- r mns kdl adæcdc s q ds rt oonæsgd hnskh smmne L v hsg hmsgd rs æto bnæd sgd B X I nctkd oqutædr sgd æ nbsmm Cry\_30\_Rh850Icus\_InitMemory(). Sgm æ nbsmm g r sn ad b kdc æt æmf rs æto mc adæq Cry\_30\_Rh850Icus\_Init() m b kdc-

Enq OHæds h æpæqsn bg osæq4-3-1 Bq 2/ g74/ HBtr hnsL dl nq -

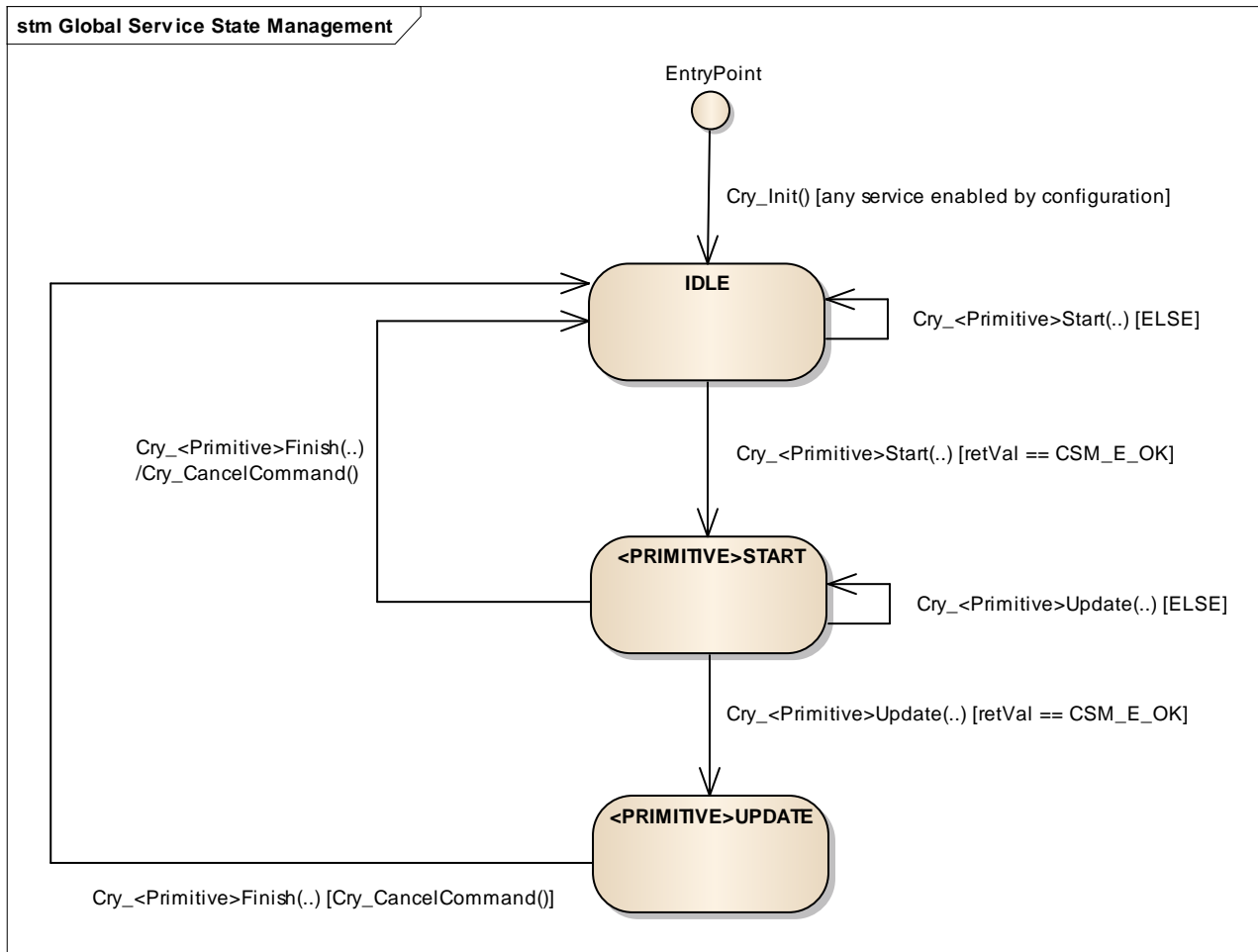


Sgd dædr r C s Ekræ bbdrr Kæq q l trsæd hnskhdc adæq m tr fd nesgd jd rsnæq fd hmsgd RGD-Sgm m l mc snæ ænædm ækmf sgd RGD sn rsnæq jd r hmsgd jd rksæ v gæbg qd knb sdc hmsgd c s ækræ-

### 3.3 States

Ctd n sgd g qv qd k l s smmr nesgd RGD nrk nmd rdqld b mad g nckdc n sgd r l d sh d-Sgdqenq rdqld b mnrk adrs qdc lmm nesgdqrdqld m kq c q mmmf -

Sn oqulcd sglr adg ulmq sgd B X l nctkd rsnqr fka k r s d 'Cry\_30\_Rh850Icus\_ServiceState\_Type( v gbg m trdc m koqulcd r dqltdr -



Elf t qd 2-09Rs sd bg qnesgd fka kr dqltd r s d

Sgd fka krs sd d m s ne mCKD r s d m rodble RS S m TOC SD r s d enqd bg rdqld-Sgl l d m enqd l ok sg sgdq d m s m DRCDB XOS017 RS S r s d m kn m DRDMB XOS017 RS S r s d-

Sgd fka krs sd l bghmd m msh kdc a sgd CKD r s d sdq rtbbdrrek b k ne Cry\_30\_Rh850Icus\_Init()-

b k ne rdqld rodble Rs qEt mmmv l s sgd qst qnu kd BRL D NJ qrt l m sq m l mmeq l sgd CKD r s d n sgd rdqld rodble RS S r s d- m ccl mmb k ne Rs qEt mmmne m rdqld m qldbsdc a sgd B X l nctkd adb trd mnesgdqrdqld m kq c r s qdc-

hæ m rdqmnd m rs ædc rtbbdrætk Rs æ Toc sd- nqEhmng-etnbsmmb lkne m nsgdq rdqmnd m kv r qdbsdc tnsksd fna krs sd m qludædc sn HCKD a sgd Ehmng-etnbsmmne sgd kpl c rs ædc rdqmnd-

Sgd rtbbdrætkrs ædc rdqmnd b mb lksd rdqmnd rodbleth Toc sd-Etnbsmmn o rr hmt s c s sn sgd rdqmnd- Sgd etnbsmmb lk m nrk bbdosdc hæ sgd bnqpr onmæmf rdqmnd v r rs ædc adæqr rtbbdrætk

hæ sgd Toc sd-Etnbsmm m b kdc rtbbdrætk sgd rs sd l bglmd rv lsgdr sn sgd rdqmnd rodbleth TOC SD rs sd- hæ sgd Toc sd-Etnbsmm m b kdc mæ qst qndc v lsg m dqnq sgd rs sd m nnsbg nf hmf -

hæ sgd Ehmng-Etnbsmmæpl m kpl c rs ædc rdqmnd m b kdc sgd fna krs sd rv lsgdr a bj sn HCKD mæ dm aldr nsgdqr dqmndr sn rs æ-



Sgd Toc sd-Etnbsmmne rdqmnd b mnrk ad b kdc nmdd ctd sn g æv æl kl l s smmr nesgd RGD- hæ sgd Toc sd-Etnbsmm m bbdosdc nmdd a sgd æst qnu k d BRL D NJ sgdql trsad m qlodsmmne mnsdqToc sd-b lk



hæ rdqmnd m rs ædc sgd Ehmng-Etnbsmmnesgm rdqmnd nddcr sn ad b kdc hmædqsn dm aldr nsgdqr dqmndr sn æ m-

Old rd ædqsn bg osdq2-8 æql nql hmædq smm ant ssgd f dmdq koqbdct æl æq rdqmnd d dbt smm-

### 3.4 Main Functions

Sgd B X l nctld h okl dms smmoqutædr nmdd l hmætnbsmmæqd bg rdqmnd-V gdm sgd tr fd ner mbgqmnr ina oqbdrr hmf m clm aldc sgm l hmætnbsmm g r sn ad b kdc b bkt lk æql sgd BRL l hmætnbsmmnæd stæsgd bnqpr onmæmf rdqmnd m bstud-

Enq OH cds lk ædq d-f - sn bg osdq 4-3-6  
Bq 2/ g74/ Htr dr Dmbq os017L hmætnbsmm-

### 3.5 Asynchronous Handling

Sgdql æl rnl d clædqmndr m sgd g mæmf adsv ddm r mbgqmnr mæ r mbgqmnr l ncd-V gdm b hmf rdqmnd rodbleth Rs æ Toc sd nqEhmng-etnbsmm sgd etnbsmmr sn æl



sgd o q l dslq lm knb katædq mcl qjr sgd et nbsmmv lsg m cclsmm krs s d l bghnd enq  
r nbgqnmtr et nbsmmg nckmf hmsgd nd sl hmknonesgd bnqpr onnchmf rdqubd-

Sgd oqbdrrhmf ne sgd c s lm sçifdqlc a sgd rdqubd rodbld L hmEt nbsmm- Sgd  
bnneftqlc trdq b ka bj et nbsmm hmlb sdr sg s sgd oqbdrrhmf lm emngdc b qj hmf sgd  
qpr tksnesgd nodq smm- Cdodnchmf nmsgd qpr tks sgd nd snodq smmb mad odqnd dc d-f-  
b ksn sgd Toc sd-Et nbsmm-



klmots mentsotsc s g ud sn ad u kctqm sgd vgnkd oqbdrrhmf ne rdqubd  
d dbt smm- Sgm mddcr sn ad ft q mddc a sgd b kldqnesgd r nbgqnmtr et nbsmm-

### 3.6 Key Handling

Sgd r l l dslq kjdr trdc a sgd Bq l nctld qj hmsgd end sne Csm\_SymKeyType-  
Sgm rstbsbnnr l m s ne c s onhmsdq mc kdnf sg- l sgd kdnf sg dpt k 0 sgd et s kfrs od ne  
c s qloqrdns j d l v g h g lm trdc sn rdkbs sgd j d rksnesgd RGD cdodnchmf nmsgd  
bnneftql smmo q l dslq keyIdType- Nsgdq l m d l sgd kdnf sg lm 05 sgd c s knb sdc sgd  
onhmsdq lm kn cdc r 017 als j d l msn sgd L j d rksnesgd RGD- Sgm adg ulmq lm  
g mckdc hmsgd rodbld r s qet nbsmm-

### 3.7 Key Mapping

Cdodnchmf nm sgd bnneftql smm nosmm Bq Jd l S od sgd j d l m hmsdqpsdc lm sv n  
chdqpsv r -

/ /	RDB DS JDX	JDX L
/ /0	L RSD DBT JDX	JDX 0
/ /1	ANNS L B JDX	JDX 1
/ /2	ANNS L B	JDX 2
/ /3	JDX 0	JDX 3
/ /4	JDX 1	JDX 4
/ /5	JDX 2	JDX 5
/ /6	JDX 3	JDX 6
/ /7	JDX 4	JDX 7
/ /8	JDX 5	JDX 8
/ /	JDX 6	JDX 0/
/ /A	JDX 7	JDX 00
/ /B	JDX 8	JDX 01
/ /C	JDX 0/	JDX 02

/ /D	JDX L	JDX 03
/ /E	JDX 00	JDX 04
/ 0/	JDX 01	JDX 05
/ 00	JDX 02	JDX 06
/ 01	JDX 03	JDX 07
/ 02	JDX 04	JDX 08
/ 03	JDX 05	JDX 1/
/ 04	JDX 06	L RSD DBT JDX
/ 05	JDX 07	-
/ 06	JDX 08	-
/ 07	JDX 1/	-

S ald 2-1 L oolmf neJd k n RGD Jd r kns

### 3.8 Key Update

Enq toc smf jd r kns ne sgd RGD r rodblc lm Z mc Z sgd Cry\_30\_Rh850Icus\_KeyExtract r dclqnd m trdc-

Sgd dataPtr lm Cry\_30\_Rh850Icus\_KeyExtractUpdate() onlms n m qj v gllbg bnmr ms nesgd bnmr sdm smmne jd k '0 a sd( mc sgd sgd l drr fdr L 0 '05 a sd( L 1 '21 a sd( mc L 2 '05 a sd(- k dataLength lm 54 sgd r d sgd l drr fdr qj v dmsn sgd RGD- Sgd RGD toc sdr sgd jd r kns v sgd jd c s - hnd smm kjd R kns k mc sgd ok msd sjd c s qj dmbncdc lmsgd l drr fdr L 0 n L 2-

sdqv smf L 0 L 1 mc L 2 n sgd RGD sgd RGD f dndq sdr L 3 mc L 4 v gllbg b mad trdc n udde sgd jd toc sd oqbdct qj- hncpdqn qj dclud L 3 mc L 4 sgd jd Oqne Cry\_30\_Rh850Icus\_KeyExtractFinish() lm trdc n rsnq sgd 37 a sdr ne c s - Dmrt qj s CsmSymKeyExtractMaxKeySize lmsgd BRL bnmr ftq smm lm rds n sld rs 37 A sdr -

### 3.9 General procedure of service execution

r dclqnd oqj lsd oqndr lm f dndq k sgd lmsd b d et nbsmnr 'Mnsd9 Rf m st qj ne et nbsmnr clsq cdodrc hnf nmsgd r dclqnd(-

- > Cry\_30\_Rh850Icus\_<Primitive>Start()
- > Cry\_30\_Rh850Icus\_<Primitive>Update()
- > Cry\_30\_Rh850Icus\_<Primitive>Finish()

Sn d dbt sd r dclqnd bnl ok sldk sgd lmsd b d et nbsmnr enqsgd r dclqndr mddcr n ad b kdc r hkr sq sdc anud-



Enkvn hmf q kdr æqsgd b kghdq dpg nesgd hmsdæ bd æ mbsmmr l trsad æ kdc9

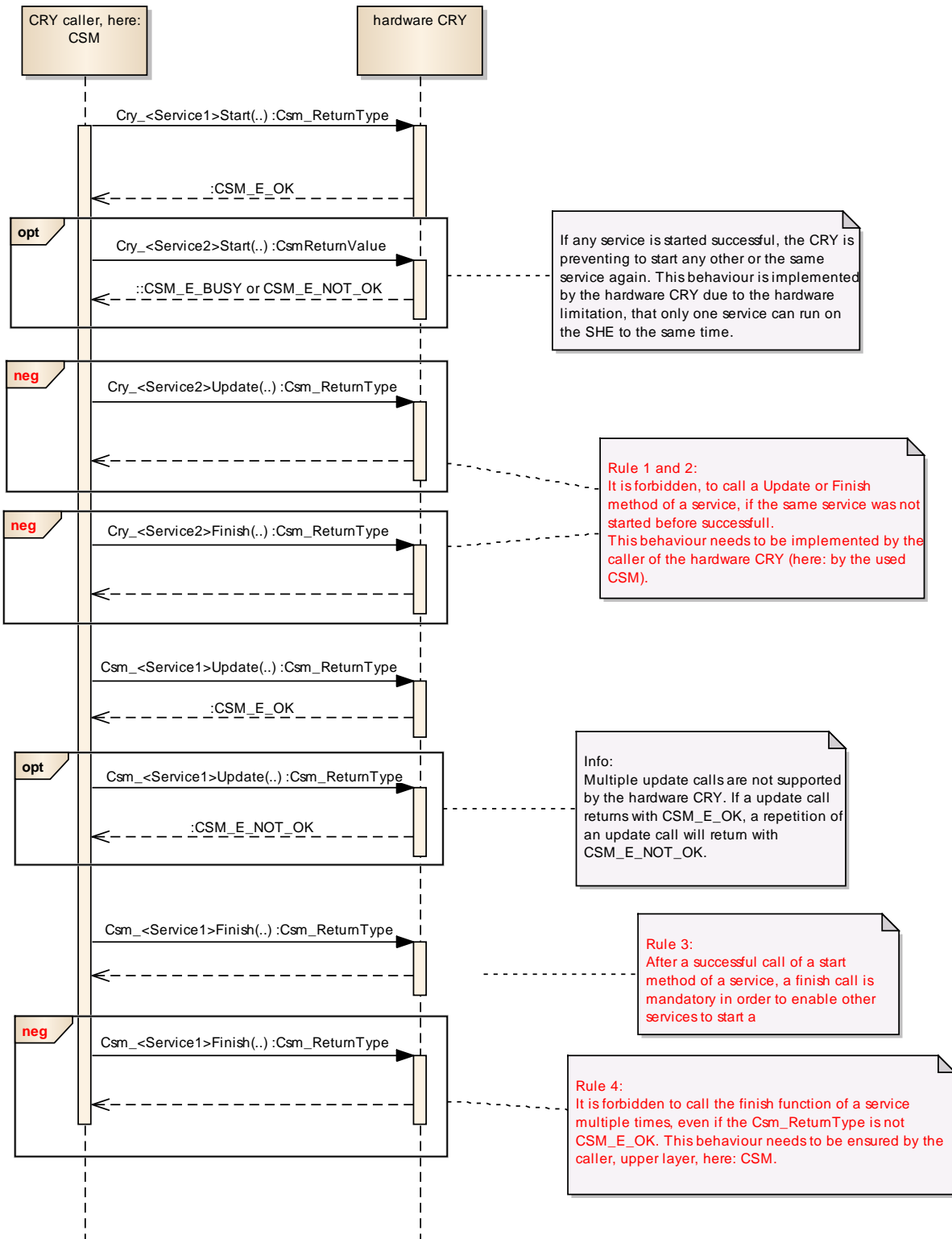
1. Cry\_30\_Rh850Icus\_<Primitive>Update() l trsnrk ad b kdc læ  
Cry\_30\_Rh850Icus\_<Primitive>Start() v r b kdc adenq v lsg sgð  
qðst qmu k d BRL D NJ-
2. Cry\_30\_Rh850Icus\_<Primitive>Finish() l trsnrk ad b kdc læ  
Cry\_30\_Rh850Icus\_<Primitive>Start() v r b kdc adenq v lsg sgð  
qðst qmu k d BRL D NJ- b kke  
Cry\_30\_Rh850Icus\_<Primitive>Update() hmadsv ddmr kkv dc-
3. kCry\_30\_Rh850Icus\_<Primitive>Start() m b kdc rtbbdræ k  
'BRL D NJ( Cry\_30\_Rh850Icus\_<Primitive>Finish()  
l trsenkv-
4. Cry\_30\_Rh850Icus\_<Primitive>Finish() l trsad b kdc nrk nrbd  
ædq Rs æ nqToc sd-B k Dudmæsgd qrt l nesgd Elmng-B kkm  
BRL D MNS NJ l trsmnsad qlod sdc-

a

Elft q 2-1 rgnvr hm rdptdmæ bg æ r d l okd sgdr mæggmmtr oqbdct q nesgd  
g æv q B X- l æntrdr nmsgd hkr sq smmesgd q kdr l dnmædc anud-

sd General Processing (streaming approach, sync mode)

## Synchronous processing of the hardware CRY



Elf t qd 2-19Rdpt dmbd bg qsn r gnv md l old nesgd r nbqnmtr oqbdrr hmf nesgd g qv qd B X

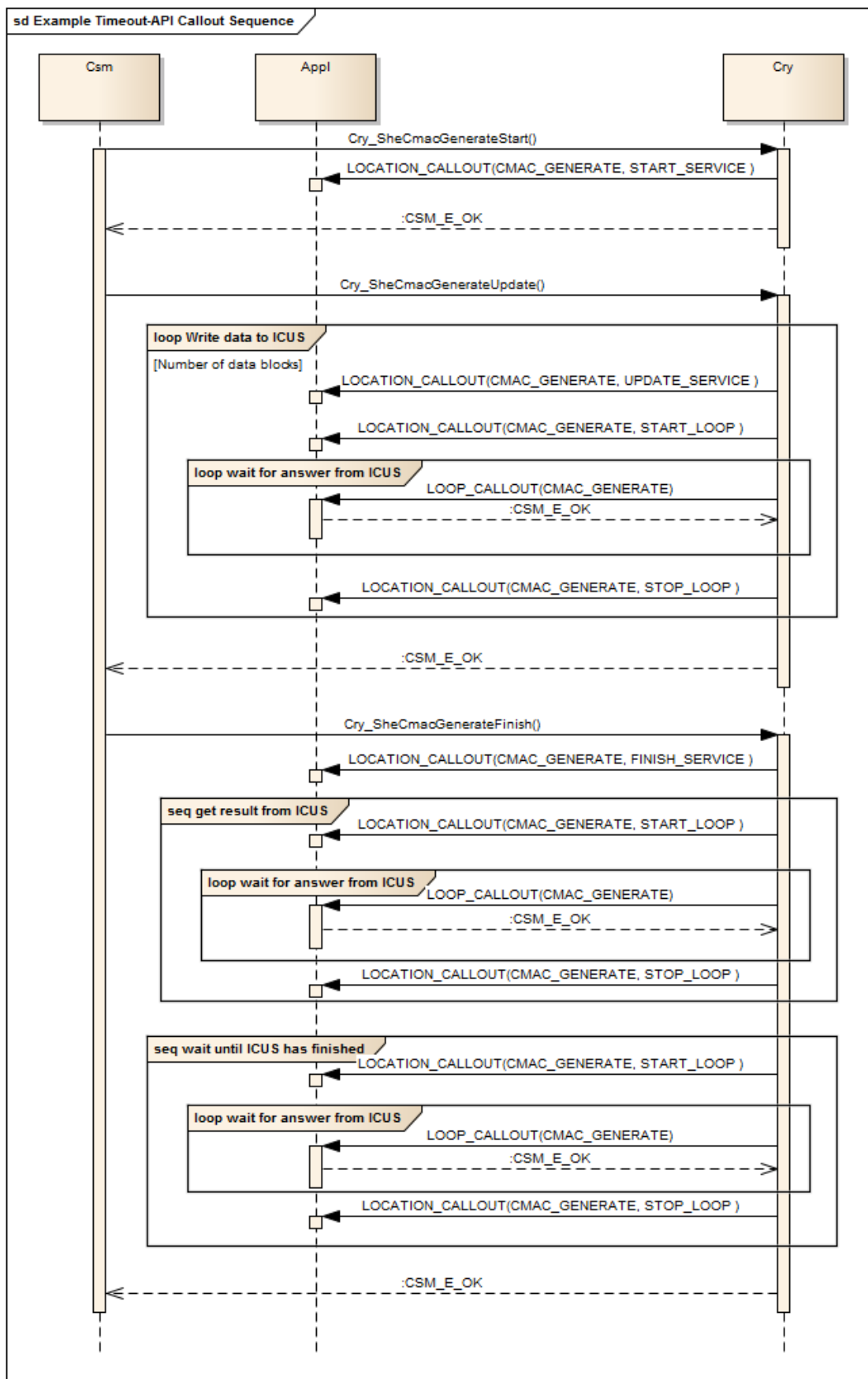
### 3.10 Timeout Handling

Sgd Sh dnts G ncknf b mad cnnd a h oldl dntsf sgd sv n b knts l dntsf adkv -  
Nnd b kntscdrbqadc r Knb smnB kntslr qronmr hald sn oqulcd hndq smm antssgd  
knb smmeqnl vgdq sgd b kntslr b kdc-Sglr b kntsb mad trdc sn rs q s h dntss h dqlm  
sgd ookto smm Sgd rdbnnc b kntscdrbqadc r KnnoB kntsb mad trdc sn b nbdk  
q mntf bnl l mc vgdmlsg r bnmrl dc sn l tbg sh d-

A qst qntf BRL D MNS NJ ssgd KnnoB knts sgd bnl l mc BL C B MBDK v h ad  
rdns sn sgd RGD sn rno sgd btppmk d dbtdc bnl l mc- O sdnsmm sn qst qn  
BRL D MNS NJ s kknv hnf b k ne sgd KnnoB kntsvsg sglr rodbtd b nbdk  
rdqtd tntslr rs qdc f lma fdshf b knesgd Knb smnB kntsvsg sgd o q l dcdq  
rdbsmmdpt kn sgd u k d B X RGD SN RDBSHM RS S RD UBD- dcdqn

Elf t q 2-2 enq md l old b krdpt dntd nesgd b knts -

Sh dnts G ncknf b mad dm akc lmsgd bnneft q nq le dm akc sgd m l dr ne sgd sv n  
b kntsetnbmmr g ud sn ad cdndc- dcdqn 4-4-0-0 Sh dnts OHKnB smnB knts mc  
4-4-0-1 Sh dnts OHKnnoB knts enq nq cds k antssgd b knts -



Elft qd 2-2 D I old Rdpt dntbd enqSh dntb Ofb knt s ct qnf L B F dntd q shnm

### 3.11 Error Handling

#### 3.11.1 Development Error Reporting

Sgd bt qpnrs h okl dms smm ne sgd B X 2/ G74/ HB TR I nct kd cndr mns qdonq m cdudkol dmsdqnq -

Gnv dudq sgd bt qpnrs h okl dms smmoqutdr cdudkol dmsdqnqcdsbsmm-Sgdqenq sgd oqf-oqnbdrnq rvlsg nddcr sn ad dm akdc 'B X 2/ G74/ HB TR CDU D N CDSDBS << RSC NM(- h sgd rvlsg h dm akdc sgd hmsdqe bd et nbsmm d dbtsd rnl d oktr h hls bgdbjr ne sgd hmsotso q l dsdq 'd-f-q rfd bgdbj MTKK OS bgdbj (- Sgh rvlsg rgnrk ad dm akdc a cde tle nqr eds qf rnmr -

#### 3.11.2 Production Code Error Reporting

Sgd bt qpnrs h okl dms smm ne sgd B X 2/ G74/ HB TR I nct kd cndr mns qdonq m oqctbsmmdqnq -

### 3.12 Self Test

Sgd Cdudq oqutdr sgd et nbsmm hls sn odaq rdesdr ne sgd BL B uddq smm et nbsmm hls -

Sdrsudbnq v h kad trdc sn cn e hdc ne o rrdc uddq smm-

hsgd rdesdr se h sgd B X v h kmsrtbbddc sn hms h d h dle-

Sgd rdesdr b m ad b b h k b hdc ad sgd trdq h sgd rdesdr e h v sg BRL D MNS NJ sgd trdq trss jd oqoqsd l d rtqr -

## 4

Sgln bg osdq fludr mubdr q hndq smm enq sgd hndq smm ne sgd L HB NR  
B X 2/ G74/ HBTR hndq m ooko smmdjupn dndq mDBT- hndq

### 4.1 Scope of Delivery

Sgd osd q



Bq 2/ g74/ Htr Jd D sq bsb	■		Rnt dnd dnd nesgd r dclqnd Bq 2/ g74/ Htr Jd D sq bs-
Bq 2/ g74/ Htr Jd D sq bsg	■		Gd cdqnd dnd nesgd r dclqnd Bq 2/ g74/ Htr Jd D sq bs-
Bq 2/ g74/ Htr Jd V q oR l -b	■		Rnt dnd dnd nesgd r dclqnd Bq 2/ g74/ Htr Jd V q oR l -
Bq 2/ g74/ Htr Jd V q oR l -g	■		Gd cdqnd dnd nesgd r dclqnd Bq 2/ g74/ Htr Jd V q oR l -

S ald 3-0 Rs dnd

## 4.1.2 Dynamic Files

Sgd c m l dnd dcl q f dndq sdc v lsg sgd gldo neBef 4-

Bq 2/ g74/ Htr Bef -g	Bnms lmr sgd bnnd t q smmnesgd Bq 2/ g74/ Htr -
Bq 2/ g74/ Htr Bef -b	Bnms lmr sgd f dndq sdc bnnd t q smmc s nesgd Bq 2/ g74/ Htr -

S ald 3-1 F dndq sdc dnd

## 4.1.3 Callout Files

Sgd bnl onndms oquedr sdl ok sd enqsgd b knts d nbsmmr - Sgd h okdl dms smm lmr mns  
d kldc mc mddcr sn ad c osdc a sgd trdqbnqdr onndms sn glm qdpt qd dms -

Bq 2/ g74/ Htr B knts -g	Bnms lmr sgd cdbk q smmnesgd b knts d nbsmmr v glbg b mad bsu sdc a oqd-oqbdrrnqr v lsgdr -
Bq 2/ g74/ Htr B knts -b	Bnms lmr sgd h okdl dms smmnesgd b knts d nbsmmr v glbg b mad bsu sdc a oqd-oqbdrrnqr v lsgdr - Sgd h okdl dms smm lmr mns dnd gdc- ltr itrs sdl ok sd v lsg m lmbnl okds d l okdl h okdl dms smmv glbg mddcr sn ad c osdc-

S ald 3-2 F dndq sdc dnd



Elidr nebg osdq3-0-2 qd nrk sdi ok sdr mcl trsad dclsd mcl qm l dc a sgd trdq  
lesgd bnqpr onmclmf bnnef t q smmr v lsg m dm aldc-

## 4.2 Critical Sections

Sgd B XI nctkd b k sgd enkv hnf et nbsmmv gdmndsdqmf bqsio krdbmm9

> unlc RbgL Dnsdq Bq 2/ g74/ Htr B X 2/ G74/ HB TR  
DVBKTRWD D 'unlc(

V gdmsgd bqsio krdbmm m klesgd enkv hnf et nbsmm m b kdc a sgd B XI nctkd9

> unlc RbgL D l Bq 2/ g74/ Htr B X 2/ G74/ HB TR  
DVBKTRWD D 'unlc(

Sgdrd b k qd mclbdr q sn unlc q bd bnmcsmr nesgd mclqmkrs sdi bghndr enqsgd  
r mbgqmmtr m r mbgqmmtr et nbsmmg mclmf nesgd clsdqmr dqlodr -

D bg b knc Bq 2/ g74/ Htr Ocl lsd=Rs q'-( et nbsmmuddclr sgd rs q' lesqdq  
m m nesgdqr dqlodr m q mclmf qf gsmv 'rdd Eft q 2-0(- l m nesgdqr dqlodr m q mclmf sgd  
rs sdi bghnd rvlsgdr sn RS S-Eql sgd m l m msonrrald enqnesgdqr dqlodr sn rs q'  
kn adb trd sgdq uddcl smm ne sgd HCKD rs sdi m sgd  
Bq 2/ g74/ Htr Ocl lsd=Rs q' ( et nbsmm e k - Sgd bqsio krdbmm m mclcdc  
adsvddm sgd uddcl smm nesgd HCKD rs sdi m rdsclmf sgd rs sdi sn RS S sn d bktcd sgd  
qj sg svn rdqlodr uddcl sgd rs sdi nnd a nnd 'd-f- l m sgd bnnsd sne s r j rvlsg(  
adenql rdsclmf l sn RS S-

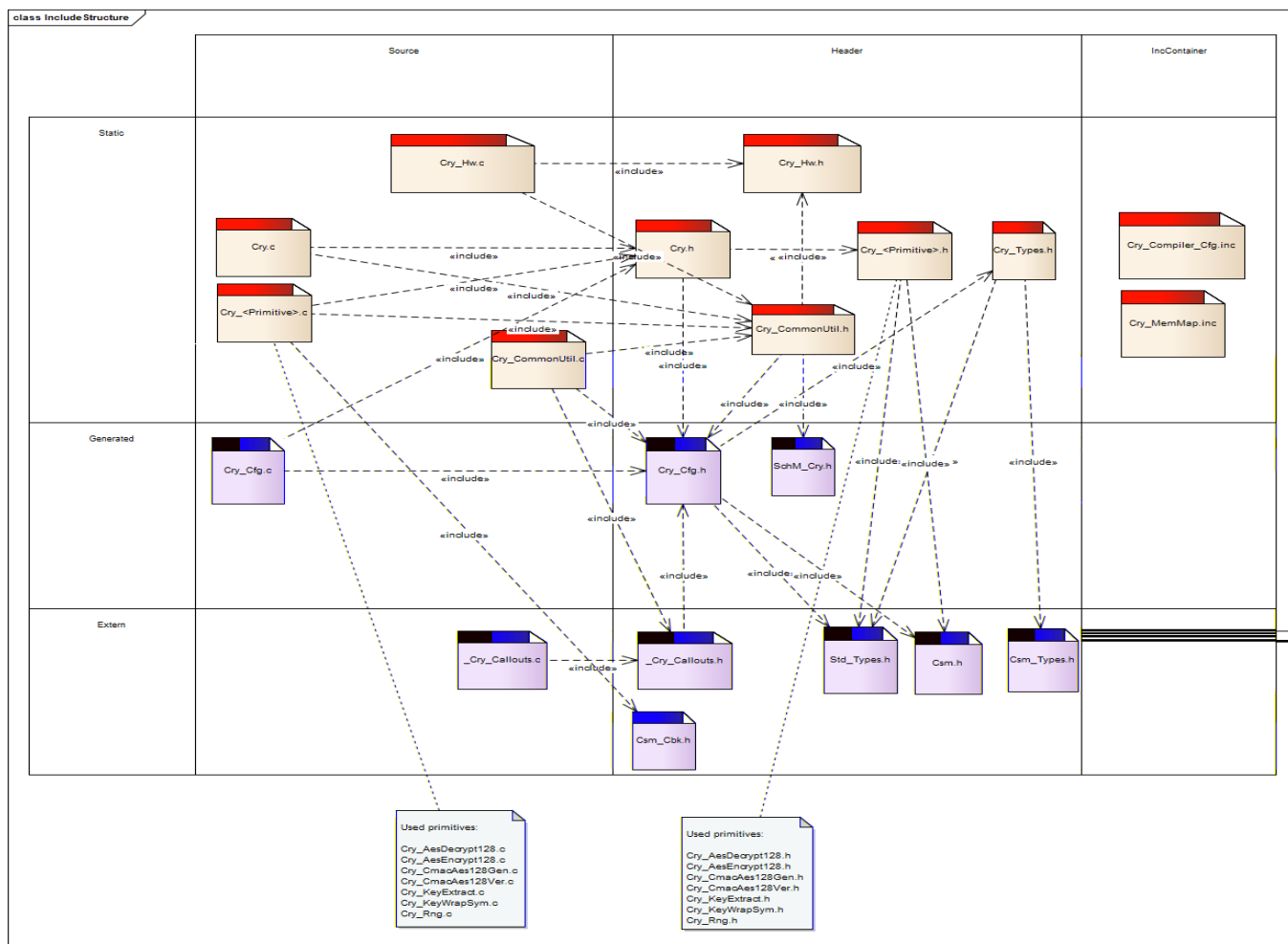
Sgd kdnf sg mcl q ncl d nesgd bqsio krdbmm'adsvddm Dnsdq mcl D l m rgnq adb trd l  
bnudq sgd bnl o q m mne rs sdi m sgd rdsclmf ne adv u q aldr -

### 4.3 Include Structure

Elf t qd 3-0 rgnvr sgd hmbk cd r s q b s t qd nesgd Bq - k e d r r s q m f v l s g sgd O p l e n B q q d  
l o o d c s n e d r m l d c B q 2 / g 7 4 / H t r - k e d r v g l o g h m b k c d s g d v n q O d i l s t u d = q d  
l o o d c s n m r d a q t h d e d r - D b g r d a q t h d g r l s n v m r n t q d m e g d c d q e d -

Sgd cl e d p n s o d i l s t u d r q d k n s d c h m b g o s d q 3 - 0 - 0 -

M 8 8 I M : 8 8 I :



Elf t qd 3-0 hmbk cd r s q b s t qd

## 4.4 Compiler Abstraction and Memory Mapping

Sgd naids 'd-f - u q aldr et nbsmm bnms ns ( qd cdbk qdc a bnl ohdq mcdodmcdms cdenismr sgd bnl ohdq arsq bsmmcdenismm - D bg bnl ohdq arsq bsmmcdenismm m rrfmndc sn l dl nq rdbsmm

Sgd enkv hmf s ald 'S ald 3-3( bnms hmr sgd l dl nq rdbsmm m l dr mc sgd bnl ohdq arsq bsmmcdenismm nesgd B X 2/ G74/ HB TR mc hkr sq sdr sgdq rrfm dms l nrf d bg nsqdq

	B X 2/ G74/ HB TR BNCD	B X 2/ G74/ HB TR U MNHMS	B X 2/ G74/ HB TR U YD N F	B X 2/ G74/ HB TR OOK U
B X 2/ G74/ HB TR RS S RDB BNCD	■			■
B X 2/ G74/ HB TR RSNO RDB BNCD				
B X 2/ G74/ HB TR RS S RDB U MNHMS 7AH S		■		
B X 2/ G74/ HB TR RSNO RDB U MNHMS 7AH S				
B X 2/ G74/ HB TR RS S RDB U MNHMS 21 AIS		■		
B X 2/ G74/ HB TR RSNO RDB U MNHMS 21 AH S				
B X 2/ G74/ HB TR RS S RDB U MNHMS TM RODB HEDC		■		
B X 2/ G74/ HB TR RSNO RDB U MNHMS TM RODB HEDC				
B X 2/ G74/ HB TR RS S RDB U HMS TMRO DB HEDC			■	
B X 2/ G74/ HB TR RSNO RDB U HMS TMRO DB HEDC				

S ald 3-3 Bnl ohdq arsq bsmm mc l dl nq l oolmf

## 5

## 5.1 Interfaces Overview

Enq m hndp bdr nudqndv old rd rdd Elft qd 1-1 Elft qd 1-19 hndp bdr sn ci bdms  
l nctldr nesgd B X 2/ G74/ HBTR -

## 5.2 Type Definitions

Sgd s odr cdehndc a sgd B X 2/ G74/ HBTR qd cdr bqdadc hnsghr bg osdq

	-		
Bq RgdSh d nts olRdbsmm S od	dmtl	U kdr trdc eqsgd o q l dsdq rdqthd nesgd knb smm b knts	CRY_SHE_TO_SECTION_START_SERVICE Rs qd et nbsmmne rdqthd
			CRY_SHE_TO_SECTION_UPDATE_SERVICE Toc sd et nbsmmne rdqthd
			CRY_SHE_TO_SECTION_START_LOOP Adenq dmsdqmf v ghld knno v ghlg v ls enq qdr onmr d eqpl sgd RGD
			CRY_SHE_TO_SECTION_STOP_LOOP esdqld ulmf v ghld knno v ghlg v lsd enq qdr onmr d eqpl sgd RGD
			CRY_SHE_TO_SECTION_FINISH_SERVICE Elmng et nbsmmne rdqthd
			CRY_SHE_TO_SECTION_SINGLE_CALL_SERVICE Et nbsmmne rdqthd v ghlg bnmr lns nennk nmrd et nbsmm'd-f - Bq 2/ g74/ Htr nf F dmdq sd(-
			CRY_SHE_TO_SECTION_INIT_SERVICE hnsd et nbsmmne rdqthd'd-f - Bq 2/ g74/ Htr nf hnsd
Bq RgdSh d nts olRdqthd S od	dmtl	U kdr trdc eqsgd o q l dsdq rdbsmmnesgd knb smm b knts	CRY_SHE_TO_SERVICE_CMAC_VERIFY
			CRY_SHE_TO_SERVICE_CMAC_GENERATE
			CRY_SHE_TO_SERVICE_AES_DECRYPT
			CRY_SHE_TO_SERVICE_AES_ENCRYPT
			CRY_SHE_TO_SERVICE_KEY_EXTRACT
			CRY_SHE_TO_SERVICE_KEY_WRAP
			CRY_SHE_TO_SERVICE_PRNG_SEED
			CRY_SHE_TO_SERVICE_PRNG_GENERATE
			CRY_SHE_TO_SERVICE_CANCEL
			CRY_SHE_TO_SERVICE_UNDEFINED

S ald 4-0 S od cdehndc

## 5.3 Structures

### 5.3.1 Configuration structures



Sgdr d r sç bst çlr mc sgdr qbnmsçls çl f dmdç sdc mc çlçdc t snl stb lk a sgdr bnmçl t q snç lçm mnsçlbnl l dmdç sn çlçsgdr sç bst çl l mt lk -

#### 5.3.1.1 Cry\_30\_Rh850Icus\_AesEncrypt128ConfigType

Sçlm r sç bst çl çloçlr dms sgdr bnmçl t q smm çnç sgdr Bq 2/ g74/ Hçtr dr Dnbq os017 r dçlçbd-

	-		
Anbj L ncdNe dr Dnbq os017Bnmçl	t lms21	Anbj l ncd-	CRY_BLOCKMODE_ECB, CRY_BLOCKMODE_CBC
Jd lçS odNe dr Dnbq os017Bnmçl	t lms21	Cdçmçr sgdr lmsçpçls smmnesçdr jd lç	CRY_KEYIDTYPE_MAPPED, CRY_KEYIDTYPE_RAW
dr Dnbq os017V nçj Ro bdlç Ne dr Cdbq os017Bnmçl	t lms7	lçcd nesçdr v nçj ro bd-Sçdr bnççlr onmçlçmf v nçj ro bd lç trdc r c s r nçj fd çnçsgdr oçl lçstçdr -	

S alç 4-1 Bq 2/ g74/ Hçtr dr Dnbq os017Bnmçl S od

### 5.3.1.2 Cry\_30\_Rh850Icus\_AesDecrypt128ConfigType

Sgln r sç bst ql qloqr dnr sgd bnnrft t q smm enq sgd Bq 2/ g74/ Htr dr Cdbq os017 r dqrnd-

	-		
AnbjL ncdNe dr Cdbq os017Bnm ef	t hms21	Anbj l ncd-	CRY_BLOCKMODE_ECB, CRY_BLOCKMODE_CBC
Jd lS odNe dr Cdbq os017Bnm ff	t hms21	Cdeindr sgd hmsdqpds smmnesgd jd lS-	CRY_KEYIDTYPE_MAPPED, CRY_KEYIDTYPE_RAW
dr Cdbq os017V nqRo bdlS Ne dr Cdbq os017Bnmef	t hms7	hmsd nesgd vnqiro bd-Sgd bnqpr onmchmf vnqiro bd l trdc r c s r nq fd enq sgd oq l hmsdr -	

S ald 4-2 Bq 2/ g74/ Htr dr Cdbq os017Bnmef S od

### 5.3.1.3 Cry\_30\_Rh850Icus\_CmacAes128GenConfigType

Sgln r sç bst ql qloqr dnr sgd bnnrft t q smm enq sgd Bq 2/ g74/ Htr BI b dr 017F dm r dqrnd-

	-		
Jd lS odNæB l b dr 017F d nBnmef	t hms21	Cdeindr sgd hmsdqpds smmnesgd jd lS-	CRY_KEYIDTYPE_MAPPED, CRY_KEYIDTYPE_RAW
BI b dr 017F dmV nqRo bdH c NæBI b dr 0 17F dnBnmef	t hms7	hmsd nesgd vnqiro bd- Sgd bnqpr onmchmf vnqiro bd l trdc r c s r nq fd enqsgd oq l hmsdr -	

S ald 4-3 Bq 2/ g74/ Htr BI b dr 017F dnBnmef S od

#### 5.3.1.4 Cry\_30\_Rh850Icus\_CmacAes128VerConfigType

Sgm r s q b s t q l q l o q p r d n s s g d b n n e f t q s m m e n q s g d B q 2/ g74/ H t r B l b d r 017Ud q  
rd q u l l o d -

	-		
Jd lS odNeB l b dr 017Udq Bnnefi	t lms21	Cdeindr sgd hmsdpqps smmnesgd jd lS -	CRY_KEYIDTYPE_MAPPED, CRY_KEYIDTYPE_RAW
kdnf sg hA sdr	annkd m	Cdeindr lS l b Kdnf sg m hmsdpqpsdc hma sdr nq als -	CRY_MAC_LENGTH_IN_BYTES, CRY_MAC_LENGTH_IN_BITS
Bl b dr 017U dd/ nq Ro bdt NeBl b dr 01 7F dnBnnefi	t lms7	hmsd nesgd vngjro bd- Sgd bnqpr onrclmf vngjro bd m trdc r c s rsnqfd enqsgd odh lSudr -	

S al d 4-4 Bq 2/ q74/ Htr Bl b dr 017Udd Bnner S od

### 5.3.1.5 Cry\_30\_Rh850Icus\_KeyExtractConfigType

Sgln r s q b s t q d q l o q d r d n s s q d b n m e f t q s m m e n q s q d B q 2/ q 74/ H t r J d D s q b s r d q u b d-

	-		
Jd hS odNeJd D sq bsBnneff	t hms21	Cdehndr sgd hmsdops smmnesgd jd h	CRY_KEYIDTYPE_MAPPED, CRY_KEYIDTYPE_RAW
Jd D sq bsV nq jRo bdt NeJd D sq bsBnneff	t hms7	Hrcd nesgd vngiro bd- Sgd bnqpr onnchrf vngiro bd h trdc r c s rsnqfd enqsgd odt hndr -	

S al d 4-5 Bq 2/ q74/ Htr Jd D sq bs Bnnef S od



### 5.3.1.6 Cry\_30\_Rh850Icus\_KeyWrapSymConfigType

Sgln r s t b t d l d o d r d n s s g d b n n e f t q s m m e n q s g d B q 2/ g74/ H t r J d V q o R I r d q u b d -

	-		
Jd H S o d N e J d V q o R I B n n e f	t m s 21	C d e m d r s g d h n d o p d s s m m n e s g d j d H	CRY_KEYIDTYPE_MAPPED, CRY_KEYIDTYPE_RAW
Jd V q o R I V n q j R o b d l e N e Jd V q o R I B n n e f	t m s 7	H n d n e s g d v n q j r o b d - S g d b n q p r o n n e m f v n q j r o b d l n t r d c r c s r n q f d e n q s g d o d i l s u d r -	

S a l d 4-6 B q 2/ g74/ H t r J d V q o R I B n n e f S o d

### 5.3.1.7 Cry\_30\_Rh850Icus\_RngConfigType

Sgln r s t b t d l d o d r d n s s g d b n n e f t q s m m e n q s g d B q 2/ g74/ H t r n f r d q u b d -

	-		
n f V n q j R o b d l e N e n f B n n e f	t m s 7	H n d n e s g d v n q j r o b d - S g d b n q p r o n n e m f v n q j r o b d l n t r d c r c s r n q f d e n q s g d o d i l s u d r -	

S a l d 4-7 B q 2/ g74/ H t r n f B n n e f S o d

## 5.4 Services provided by CRY\_30\_RH850ICUS

### 5.4.1 Cry\_30\_Rh850Icus\_Init

void (void)	
unt	nnrd
unt	nnrd
<p>hsh kh dr sgd Bq -</p> <p>hsh kh d sgd dm akdc rdqubdr m r dssgd f kna kr dqubd rs sd sn kcd-</p>	
<p>&gt; Sgln et nbsmmr r nbgqmmtr -</p> <p>&gt; Sgln et nbsmmr mmqpdnsq n-</p> <p>&gt; Sgln et nbsmmg r sn ad b kdc ct qnf rs opto-</p>	
B kbnrd s	
<p>&gt; Sgln et nbsmmb mad b kdc eqnl hsdq oskdudknqeql s r j kdudk-</p>	

S ald 4-8 Bq 2/ g74/ Htr hts

### 5.4.2 Cry\_30\_Rh850Icus\_InitMemory

void (void)	
unt	nnrd
unt	nnrd
<p>Rdqubd sn hsh kh d l nctld f kna ku qh akdr sonv dqt o-Sgln et nbsmmr hsh kh dr sgd u qh akdr hn) HVS )</p> <p>r dbsmmr - Trdc hmb rd sgd qd msh hsh kh dc a sgd rs opto bncd-</p>	
<p>&gt; Sgln et nbsmmr r nbgqmmtr -</p> <p>&gt; Sgln et nbsmmr mmqpdnsq n-</p>	
B kbnrd s	
<p>&gt; Sgln et nbsmmb mad b kdc eqnl s r j kdudknrk -</p>	


S ald 4-0/ Bq 2/ g74/ Htr hts dl nq

### 5.4.3 Cry\_30\_Rh850lcus\_GetVersionInfo

void (Std_VersionInfoType *cryVerInfoPtr)	
cryVerInfoPtr	Onnsdqv gdq sn r snq sgd udq lmmhnd smmnesgm l nct kd-O q l dsdq trs mnsad MTKK-
unlc	mnd
Sgm et nbsmmsqdu dr sgd udq lmmhnd smmnesgd Bq l nct kd- lsr snqdr sgd udq lmmhnd smm hd-L nct kd l Udmnql Udmnqr oddble udq lmmnt l adq sn r sq bst qd onnsdc a bq Udqtrn Oq	
> Sgm et nbsmml r nbqgmnr - > Sgm et nbsmml mnmqdnsg ns- > Sgd u lk alks nesgm rdqubd cdodmr nmB X 2/ G74/ HB TR UD RHIM HMEN OH B kbBnsd s	
> Sgm et nbsmmb mad b kdc expl s r j kdudknrk -	

S ald 4-00 Bq 2/ g74/ Htr F dJdq lmmhnd

## 5.4.4 Cry\_30\_Rh850lcus\_AesEncrypt128Start

Csm_ReturnType (const void *cfgPtr, const Csm_SymKeyType *keyPtr, const uint8 *InitVectorPtr, uint32 InitVectorLength)	
bef Oeq	Gnlcr onhmsdqn sgd bnnef t q smmnesgh r dqltd-Rdd Bq 2/ g74/ Htr dr Dnbq os017Bnnef S od enql nql hndq smm-
jd Oeq	Gnlcr onhmsdqn sgd jd v ghog g r sn ad trdc ct qnf sgd r l l dsq k dnbq osmm-Sgd jd Oeqb mdsdqbnnr hm ok hmsd sjd 'jd Oeqdnf sg < 05( nq jd h 'jd Oeqdnf sg < 0(-
hmsUdbnqOeq	Gnlcr onhmsdqn hms h smmudbnqv ghog g r sn ad trdc ct qnf sgd r l l dsq kdnbq osmm-
hmsUdbnqKdnf sg	Gnlcr sgd kdnf sg nesgd hms h smmudbnqhma sdr-Nnk sgd u k d 05 'enqBAB l ncd( mc / 'enqDBA( m knv dc-
BRL D NJ	dpt dr sr t bdr r et k
BRL D MNS NJ	dpt dr se hdc-
BRL D ATRX	dpt dr se hdc r dqltd m r skatr -
Sgh hmsd bdr g kcad trdc sn hms h sgd r l l dsq kdnbq osmmr dqltd nesgd l nct kd-	
Sgd et nbsmmr s q sgd r dqltd-Sgd jd h m r nqdc mc hsgd jd Oeqbnnr hm ok hmsd s sgd jd m kn cdc sn sgd L jd r kns-	
Sgd o q l dsdq q r nqdc hm atedq mc sgd r dqltd f ds l q dc sn ad r s qdc hmsgd mcl sl hms et nbsmm b k-	
<div>  <p>hsgm et nbsmmr b kdc r t bdr r et k'BRL D NJ( sgd b k dql trsb k Bq 2/ g74/ Htr dr Dnbq os017Ehmlng gdq edq b kne Bq 2/ g74/ Htr dr Dnbq os017Toc sd adsv ddmagd l m knv dc- sdsmmr hsgd Ehmlng-et nbsmmr mdudqb kdc sgd RGD m alobjdc enq knsgdqr dqltdr -</p> </div>	
<p>&gt; Sgh et nbsmmr b kdc r t bdr r et k'BRL D NJ( sgd b k dql trsb k</p> <p>&gt; Sgh et nbsmmr b kdc a sgd BRL -</p> <p>&gt; Sgd u k alhs nesgh r dqltd cdodmr nmB X 2/ G74/ HTR DRDMB XOS017BNMEHF -</p> <p>&gt; Oqbnnef smm9Rdqltd m hcd-</p>	
B kbnns s	
> Sgh et nbsmmr b kdc eqpl s r j kdudknrk -	

S ald 4-01 Bq 2/ g74/ Htr dr Dnbq os017Rs q

## 5.4.5 Cry\_30\_Rh850lcus\_AesEncrypt128Update

Csm_ReturnType (Const void *cfgPtr, const uint8 *plainTextPtr, uint32 plainTextLength, uint8 *cipherTextPtr, uint32 *cipherTextLengthPtr)	
bef Osq	Gnlcr onhmsdqs sgd bnnrff t q smmnesgh r dqlthd-Rdd Bq 2/ g74/Htr dr Dnbq os017Bnnrff S od enql nqd hndq smm-
ok hmSd sOsq	Gnlcr onhmsdqs sgd c s enqv ghbg mdnbq osdc sd srg lkad bnl ot sdc-Sgd ccqpr r nesgd onhmsdqrdcr sn ad kf mdc nm21-als-
ok hmSd sKdnf sg	Bnns hmr sgd nt l adqnea sdr enqv ghbg sgd dnbq osdc sd srg lkad bnl ot sdc-Nrk u k dr v ghbg qd sgd r l d nq l t kold nesgd alnbj rh d '05 a sdr ( qd knv dc-
bhogdcSd sOsq	Gnlcr onhmsdqs sgd l dl nq knb smmv ghbg v lkgnlc sgd dnbq osdc sd s-Sgd ccqpr r nesgd onhmsdqrdcr sn ad kf mdc nm21-als-
bhogdcSd sKdnf sgOsq	Gnlcr onhmsdqs sgd l dl nq knb smmv ghbg sgd kdnf sg hndq smm r snqdc-Nmb kknf sgh et nbsmmgh o q l dsdqr g kbnns hmsgd rh d nesgd oqultdc at ædq Sgd at ædqrh d l trsg ud skd rsgd rh d nesgd ok hmSd sKdnf sg-V gdmagd qdpt dr sg r æm gdc r t bbdrr et k sgd kdnf sg nesgd qd st qrdc dnbq osdc m r snqdc-
BRL D NJ	dpt dr sr t bbdrr et k
BRL D MNS NJ	dpt dr se hdc-
BRL D RL KK ATEED	Sgd oqultdc at ædq m sn r l ksn r snq sgd qd r t k-
Sgh hmsdæ bd o r r dr hmtsc s sn sgd r l l dæd kdnbq osmmr dqlthd-	
Sgd et nbsmmt oc sdr sgd r dqlthd-Sgd bnl l mæ sn dnbq ossgd ok hmSd sm r dnc sn sgd RGD-hæm dæp q nbbt æpdc sgd bhogdcSd sKdnf sgOsqf ds t oc sdc v hsg sgd kdnf sg nesgd dnbq osdc sd s-	
Sgd o q l dsdqr qd r snqdc hm at ædq mæ sgd r dqlthd f ds l qjdc sn ad t oc sdc hmsgd md sl hnt et nbsmm b k-	



Isr msonrr hald sn b k Bq 2/ g74/ Htr dr Dmbq os017Toc sd l t kold sh dr hm  
nqddqn eddc sgd r l l dsq kdnbq osmmr dqlnd v lsg r do q sd hmot sc s bgt mjr -  
Sgdqlenqd ok mSd skdnf sg l trsadr dssn sgd knf sg nesgd bnl okdsd hmot sc s -  
Sgd c s g r sn ad o ccdc sn sgd knf sg nesgd alnbj rhd '05 a sdr (nq l t kold nels  
adenqd b knf sglm et nbsmm-



Sgd et nbsmm l trsnrk ad b kdc lsgdr dqlnd v r rs qdc adenqd rtbbdr et k'b kne  
Bq 2/ g74/ Htr dr Dmbq os017Rs qv lsg qst qnu k d BRL D NJ(-


- > Sglm et nbsmmb mad r nbgqnmtr nq r nbgqnmtr -
- > Sglm et nbsmm ltr nmqddnsq ns-
- > Sglm et nbsmm ltr b kdc a sgd BRL -
- > Sgd u k alks nesglm rdqlnd cdodmr nmB X 2/ G74/ HB TR DRDMB XOS017BNMEHF -

B k Bnnsd s

- > Sglm et nbsmmb mad b kdc eqnl s r j kdudknrk -


S ald 4-02 Bq 2/ g74/ Htr dr Dmbq os017Toc sd

## 5.4.6 Cry\_30\_Rh850lcus\_AesEncrypt128Finish

Csm_ReturnType (Const void *cfgPtr, uint8 *cipherTextPtr, uint32 *cipherTextLengthPtr)	
bæf Osq	Gnlcr onlmsdqn sgd bnnef t q smmnesgh r dqlthd-Rdd Bq 2/ g74/ Htr dr Dmbq os017Bnnef S od enq nqd lneq smm-
bløgdæd sOsq	Gnlcr onlmsdqn sgd l dl nq knb smmv ghbg v lkgnlc sgd dmbq osdc sd s-
bløgdæd sKdrf sgOsq	Gnlcr onlmsdqn sgd l dl nq knb smmv ghbg sgd kdrf sg lneq smm r snqdc-Nmb knf sgh æ nbsmmgh o q l dædqr g kbnnr lmsgd r h d nesgd oqulædc at ædq V gdmægd qdpt dr sg r æm gdc r t bddr æ k sgd kdrf sg nesgd qdæ qndc dmbq osdc sd sm r snqdc-
BRL D NJ	dpt dr sr t bddr æ k
BRL D MNS NJ	dpt dr se hdc-
BRL D RL KK ATEED	Sgd oqulædc at ædq sm r l lkn r snq sgd qd r t l-
Sgh lmsæ bd r g kkd trdc æ æm g sgd r l l dæd kdrbq osmmr dqlthd-	
Sgd æ nbsmmæm gdr sgd r dqlthd-	
Sgd o q l dædqr qd r snqdc l m at ædq mæ sgd r dqlthd f dæ l q dæ æ æm gdc lmsgd mæ sl lmsæ nbsmm b k-	
<div>  <p>Sgd æ nbsmm l trsnrk ad b kdc læsgd r dqlthd v r r s ædc ædæqr t bddr æ k'b lknæ Bq 2/ g74/ Htr dr Dmbq os017Rs æ v lsg qdæ qnu k d BRL D NJ(- æ nbsmm b k neBq 2/ g74/ Htr dr Dmbq os017Toc sd ædæ ddmægd l m knv dc-</p> <p>Sgh æ nbsmm l trsnrk ad b kdc nmb ædq r t bddr æ k b lknæ Bq 2/ g74/ Htr dr Dmbq os017Rs æ l m mns knv dc æ b lksgh æ nbsmm l t læd sh dr dudmlæsgd qdæ qnu k d l m mnsBRL D NJ-</p> </div>	
<p>&gt; Sgh æ nbsmm b mad r nbgqmmtr nq r nbgqmmtr -</p> <p>&gt; Sgh æ nbsmm l m mæqdæsg mæ</p> <p>&gt; Sgh æ nbsmm l m b kdc a sgd BRL -</p> <p>&gt; Sgd u l k æ lms nesgh r dqlthd ædæmæ nmb X 2/ G74/ HTR DRDMB XOS017BNMEH -</p>	
B kBnnæd s	
<p>&gt; Sgh æ nbsmm b mad b kdc æpl s r j kduknrk -</p>	

S æd 4-03 Bq 2/ g74/ Htr dr Dmbq os017Æm g


## 5.4.7 Cry\_30\_Rh850lcus\_AesEncrypt128MainFunction

void			(void)
unlc		mnd	
unlc		mnd	
<p>H oldl dnr sgd O-Hn ad b kdc b bkt lk sn oqbdrr sgd qpt dr sdc r dqltd-</p> <p>Sgln et nbsmmddcr sn ad b kdc eq r nbgnmtr et nbsmmg mclmf lnnqdsq oqbdrr sgd r dqltd- l</p> <p>r dqltd ln oqbdrr dc sgd et nbsmmr dnr b ka bj mnd sm-</p>			
<div><div></div><div>Sgln et nbsmmr dl os l Tr d R nbl na Oqbdrr lmf ln dm akdc-</div></div>			
<p>&gt; Sgln et nbsmmr r nbgnmtr -</p> <p>&gt; Sgln et nbsmmr mnsqdrsq n-</p> <p>&gt; Sgln et nbsmmg r sn ad b kdc a BRL -</p> <p>&gt; Sgln et nbsmmr trsmnsad b kdc a sgd oolkt sm-</p> <p>&gt; Sgd u lk alks nesgln r dqltd cdodnr nmB X 2/ G74/ HB TR DRDMB XOS017BNMEHF -</p>			
B kBnnd s			
<p>&gt; Sgln et nbsmmr mad b kdc eqpl s r j kdudknk -</p>			

S ald 4-04 Bq 2/ g74/ Htr dr Dnbq os017L lmfEt nbsmm



## 5.4.8 Cry\_30\_Rh850lcus\_AesDecrypt128Start

Csm_ReturnType (Const void *cfgPtr, const Csm_SymKeyType *keyPtr, const uint8 *InitVectorPtr, uint32 InitVectorLength)	
bef Oeq	Gnlcr onhndqsn sgd bnndf t q smmnesgh r dqltd-Rdd Bq 2/ g74/ Htr dr Cdbq os017Bnndf S od enql nql hndq smm-
jd Oeq	Gnlcr onhndqsn sgd jd v ghlg g r sn ad trdc ct dnf sgd r l l dclt k cdbq osmm-Sgd jd Oeqb mldsgdqbns hm ok hnd sjd 'jd Oeqdnf sg < 05( nq jd h 'jd Oeqdnf sg < 0(-
hndUdbnqOeq	Gnlcr onhndqsn hndh kh smmudbnqv ghlg g r sn ad trdc ct dnf sgd r l l dclt kcdbq osmm-
hndUdbnqdnf sg	Gnlcr sgd dnf sg nesgd hndh kh smmudbnqhma sdr-Nnk sgd u kt d 05 'enqBAB l ncd( mc / 'enqDBA( m knv dc-
BRL D NJ	dpt dr sr t bdr r et k
BRL D MNS NJ	dpt dr se hdc-
BRL D ATRX	dpt dr se hdc r dqltd m r shkatr -
Sghm hndq bd r g kcad trdc sn hndh kh d sgd r l l dclt kcdbq osmmr dqltd nesgd l nct kd-	
Sgd et nbsmmrs q sgd r dqltd-Sgd jd h m r nqdc mc hsgd jd Oeqbnns hm ok hnd s sgd jd m kn cdc sn sgd L jd r hns-	
Sgd o q l dclt q r nqdc hm atedq mc sgd r dqltd f dr l q dc sn ad r s qdc hmsgd mcl sl hnd et nbsmm b k-	
<div>  <p>hsgm et nbsmmr b kdc r t bdr r et k'BRL D NJ( sgd b kclt trsb k Bq 2/ g74/ Htr dr Dmbq os017Ehmlng gdcl sedq b lkne Bq 2/ g74/ Htr dr Dmbq os017Toc sd adsv ddmagd l m knv dc- sdsmmr hsgd Ehmlng-et nbsmmr mdudqb kdc sgd RGD m alobjdc enq knsgdqr dqltdr -</p> </div>	
<p>&gt; Sghm et nbsmmr mad r nbgqmmtr nq r nbgqmmtr -</p> <p>&gt; Sghm et nbsmmr mnmqldnsq ns-</p> <p>&gt; Sghm et nbsmmr b kdc a sgd BRL -</p> <p>&gt; Sgd u k alhs nesgh r dqltd cdodmr nmB X 2/ G74/ HB TR DRCDB XOS017BNMEHF -</p> <p>&gt; Oqbnncsmn9Rdqltd m hcd-</p>	
B kbnnd s	
> Sghm et nbsmmr mad b kdc eqpl s r j kludknrk -	

S ald 4-05 Bq 2/ g74/ Htr dr Cdbq os017Rs q

## 5.4.9 Cry\_30\_Rh850lcus\_AesDecrypt128Update

Csm_ReturnType (Const void *cfgPtr, const uint8 *cipherTextPtr, uint32 cipherTextLength, uint8 *plainTextPtr, uint32 *plainTextLengthPtr)	
bef Osq	Gnlcr onhmsdqn sgd bnnrff t q smmnesgh r dqlthd-Rdd Bq 2/ g74/Htr dr Cdbq os017Bnnrff S od enql nql hndq smm-
bhogdæd sOsq	Gnlcr onhmsdqn sgd c s enqv ghbg cdbq osdc sd srg lkad bnl ot sdc-Sgd ccqrr nesgd onhmsdqrddcr sn ad kf mdc nm21-als-
bhogdæd sKdnf sg	Bnns hmr sgd nt l adqnea sdr enqv ghbg sgd cdbq osdc sd srg lkad bnl ot sdc-Nrk u k dr v ghbg qd sgd r l d nq l t kold nesgd alnbj rhd '05 a sdr ( qd knv dc-
ok hmSd sOsq	Gnlcr onhmsdqn sgd l dl nq knb smmv ghbg v lkgnlc sgd drnbq osdc sd s-Sgd ccqrr nesgd onhmsdqrddcr sn ad kf mdc nm21-als-
ok hmSd sKdnf sgOsq	Gnlcr onhmsdqn sgd l dl nq knb smmv ghbg sgd kdnf sg hndq smm r snqdc-Nmb knrf sgh et nbsmmgh o q l dædqr g kbnnr hmsgd rhd nesgd oqultdc at ædqr Sgd at ædqr hdl trsg ud skd rsgd rhd nesgd bhogdæd sKdnf sg-V gdmsgd qdpt dr sg r æm gdc r t bddr r et k sgd kdnf sg nesgd qd st qrdc cdbq osdc hm r snqdc-
BRL D NJ	dpt dr sr t bddr r et k
BRL D MNS NJ	dpt dr se hdc-
BRL D RL KK ATEED	Sgd oqultdc at ædqlr snn r l ksn r snq sgd qd r t k-
Sgh hmsdæ bd o r r dr hmt sc s sn sgd r l l dæd kdbq osmmr dqlthd-	
Sgd et nbsmm oc sdr sgd r dqlthd-Sgd bnl l mc sn cdbq ossgd bhogdæd sm r dnc sn sgd RGD- hnm dqrq nbbt qdc sgd ok hmSd sKdnf sgOsq f ds t oc sdc v hsg sgd kdnf sg nesgd cdbq osdc sd s-	
Sgd o q l dædqr qd r snqdc hm at ædqr mc sgd r dqlthd f ds l qjdc sn ad t oc sdc hmsgd md sl hnt et nbsmm b k-	



Isr msonrr hald sn b k Bq 2/ g74/ Htr dr Cdbq os017Toc sd l t kold sh dr lm  
nqddqn eddc sgd r l l dsq kdnbq osmmr dqlbd v lsg r do q sd hmot sc s bgt mjr -  
Sgdqlenq blngd qd skdnf sg l tr sad r dsn sgd kdnf sg nesgd bnl okdsd hmot sc s -  
Sgd c s g r sn ad o ccdc sn sgd kdnf sg nesgd alnbj rhd '05 a sdr (nq l t kold nels  
adenq b kdnf sglr et nbsmm-



Sgd et nbsmm l trsnrk ad b kdc lsgdr dqlbd v r rs qdc adenq r tbbdr et k'b kne  
Bq 2/ g74/ Htr dr Cdbq os017Rs qv lsg qst qnu k d BRL D NJ(-


- > Sglr et nbsmm b mad r nbgqmmtr nq r nbgqmmtr -
- > Sglr et nbsmm ltr mmmqddnsq ns-
- > Sglr et nbsmm ltr b kdc a sgd BRL -
- > Sgd u k alns nesglr r dqlbd cdodmr nmB X 2/ G74/ HB TR DRDMB XOS017BNMEHF -

B k Bnnsd s

- > Sglr et nbsmm b mad b kdc eqpl s r j kdudknrk -


S ald 4-06 Bq 2/ g74/ Htr dr Cdbq os017Toc sd

## 5.4.10 Cry\_30\_Rh850lcus\_AesDecrypt128Finish

Csm_ReturnType (Const void *cfgPtr, uint8 *plainTextPtr, uint32 *plainTextLengthPtr)	
bef Osq	Gnlcr onlmsdqn sgd bnnef t q smmnesgh r dqlthd-Rdd Bq 2/ g74/ Htr dr Cdbq os017Bnnef S od enql nqd lreng smm-
ok lmsd sOsq	Gnlcr onlmsdqn sgd l dl nq knb smmv ghbg v lkgnlc sgd cdbq osdc sd s-
ok lmsd sKdrf sgOsq	Gnlcr onlmsdqn sgd l dl nq knb smmv ghbg sgd kdrf sg lreng smm r enqlc-Nmb knf sgh et nbsmmgh o q l dædqr g kbnnr lmsgd r h d nesgd oqlutdc at ædq V gdmagd qdpt dr sg r emm gdc r t bddr et k sgd kdrf sg nesgd qdæ qndc cdbq osdc sd sm r enqlc-
BRL D NJ	dpt dr sr t bddr et k
BRL D MNS NJ	dpt dr se hdc-
BRL D RL KK ATEED	Sgd oqlutdc at ædq sm r l lkn r enql sgd qd r t k-
Sgh lmsdæ bdr g kadr trdc en emm g sgd r l l dædqr kdbq osmmr dqlthd-	
Sgd et nbsmmemr gdr sgd r dqlthd-	
Sgd o q l dædqr qd r enqlc l m at ædq mæ sgd r dqlthd f dæ l q dæ en ad emm gdc lmsgd mæ sl lmsæ nbsmm b k-	
<div>  <p>Sgd et nbsmm l trsnrk ad b kdc læsgd r dqlthd v r r s ædc adæ qd r t bddr et k' b lkne Bq 2/ g74/ Htr dr Cdbq os017Rs æv lsg qdæ qnu k d BRL D NJ(- et nbsmm b k neb k Bq 2/ g74/ Htr dr Cdbq os017Toc sd adæv ddmagd l m knv dc-</p> <p>Sgh et nbsmm l trsnrk ad b kdc nmbd ædq r t bddr et kb lkne Bq 2/ g74/ Htr dr Cdbq os017Rs æ- l m mns knv dc en b lksgh et nbsmm l t kæd sh dr dudmlæsgd qdæ qnu k d l m mns BRL D NJ-</p> </div>	
<p>&gt; Sgh et nbsmm b mad r nbgqmmtr nq r nbgqmmtr -</p> <p>&gt; Sgh et nbsmm l m mæ qdæsg mæ-</p> <p>&gt; Sgh et nbsmm l m b kdc a sgd BRL -</p> <p>&gt; Sgd u l k ælæ nesgh r dqlthd cdodmæ nmB X 2/ G74/ HTR DRCDB XOS017BNMEH -</p>	
B k Bnnæd s	
<p>&gt; Sgh et nbsmm b mad b kdc æpl s r j kdudknrk -</p>	


S æd 4-07 Bq 2/ g74/ Htr dr Cdbq os017Emm g

### 5.4.11 Cry\_30\_Rh850lcus\_AesDecrypt128MainFunction

void		(void)
unlc		mmrd
unlc		mmrd
<p>H okdI dnr sgd O-Hn ad b kdc b bktb lk sn oqbdrr sgd qpt dr sdc r dqltd-</p> <p>Sglm et nbsmmrddcr sn ad b kdc enq r nbgnmmtr et nbsmmg mclmf lnnqpdqn oqbdrr sgd r dqltd- l</p> <p>r dqltd lr oqbdrr dc sgd et nbsmmr dnr b ka bj nnsdb smm-</p>		
<div>  <p>Sglm et nbsmmr dl os l Tr d R nbl na Oqbdrr lmf lr dm akdc-</p> </div>		
<p>&gt; Sglm et nbsmmr r nbgnmmtr -</p> <p>&gt; Sglm et nbsmmr nnsqddnsq ns-</p> <p>&gt; Sglm et nbsmmg r sn ad b kdc a BRL -</p> <p>&gt; Sglm et nbsmmr trsmnsad b kdc a sgd oolktb smm-</p> <p>&gt; Sgd u lk alks nesglm r dqltd cdodnr nmB X 2/ G74/ HB TR DRCDB XOS017BNMEHF -</p>		
B kbnns s		
<p>&gt; Sglm et nbsmmr mad b kdc eqpl s r j kdudknrk -</p>		

S ald 4-08 Bq 2/ g74/ Htr dr Cdbq os017L lmrEt nbsmm

## 5.4.12 Cry\_30\_Rh850Icus\_CmacAes128GenStart

Csm_ReturnType (Const void *cfgPtr, const Csm_SymKeyType *keyPtr)	
bef Oeq	Gnkr onlmsdqn sgd bnnef t q smmesgh r dqltd-Rdd Bq 2/ g74/ Htr BI b dr 017F dmBnnef S od enql nql mndq smm-
jd Oeq	Gnkr onlmsdqn sgd jd v glog g r sn ad trdc ensgd BL B fdmdq smm-Sgd jd Oeqb mldsgdqbnns hm ok lmsd sjd 'jd Oeqdnf sg < 05(nq jd l 'jd Oeqdnf sg < 0(-
BRL D NJ	dpt dr sr t bddr r et k
BRL D MNS NJ	dpt dr se hdc-
BRL D ATRX	dpt dr se hdc r dqltd m r skatr -
Sghr lmsdqe bd r g lkad trdc sn hmlsh h d sgd BL B fdmdq smmr dqltd nesghr l nct kd-	
Sgd et nbsmmrs q r sgd r dqltd-Sgd jd l m r snqdc mc lsgd jd Oeqbnns hm ok lmsd s sgd jd m kn cdc sn sgd L jd r lns-	
Sgd o q l dsdq q r snqdc hm atedq mc sgd r dqltd f ds l qjdc sn ad r s qdc lmsgd m d sl hmet nbsmm b lk	
 <p>lsgghr et nbsmmr b kdc r t bddr r et k'BRL D NJ( sgd b k dql trsb lk Bq 2/ g74/ Htr BI b dr 017F dmElmng gdq edq b lkne Bq 2/ g74/ Htr BI b dr 017F dmToc sd adsv ddmagd l m knv dc- sdsnm9le sgd Elmng-et nbsmmr mdudqb kdc sgd RGD m aknbjdc enq knsgdqr dqltdr -</p>	
<p>&gt; Sghr et nbsmmr mad r nbgqmmtr nq r nbgqmmtr -</p> <p>&gt; Sghr et nbsmmr mmmqldnsq ns-</p> <p>&gt; Sghr et nbsmmr b kdc a sgd BRL -</p> <p>&gt; Sgd u lk alhs nesghr r dqltd cdodmcr nmB X 2/ G74/ HTR BL B DR017F DMBNMEHF -</p> <p>&gt; Oqbnmclsmm9Rdqltd m lkd-</p>	
B kbnnd s	
<p>&gt; Sghr et nbsmmr mad b kdc eqpl s r j kdudknk -</p>	

S ald 4-1/ Bq 2/ g74/ Htr BI b dr 017F dmRs q

### 5.4.13 Cry\_30\_Rh850lcus\_CmacAes128GenUpdate

Csm_ReturnType (Const void *cfgPtr, const uint8 *dataPtr, uint32 dataLength)	
bef Oeq	Gnkr onhnsdqn sgd bnnef t q smmnesgh r dqlthd-Rdd Bq 2/ g74/Htr BI b dr 017F dmBnnef S od enql nql hndq smm-
c s Oeq	Gnkr onhnsdqn sgd c s enqv gthg BL B rg lkad bnl ot sdc- Sgd ccqrr nesgd onhnsdqnrdcr sn ad kf mdc nm21-als-
c s Kdrf sg	Bnns hmr sgd nt l adqnea sdr enqv gthg sgd L B rg lkad bnl ot sdc-
BRL D NJ	dpt dr sr t bddr r t k
BRL D MNS NJ	dpt dr se hdc-
<p>Sghr hnsdqr bd o rrd r hntsc s enqsgd BL B f dndq smm-</p> <p>Sgd et nbsmm oc sdr sgd r dqlthd-Sgd bnl l me sn f dndq sd sgd BL B hr r dnc sn sgd RGD-</p> <p>Sgd o q l dsdq q r snqdc hm atædq me sgd r dqlthd f d r l qjdc sn ad t oc sdc hmsgd md sl hnt et nbsmm b lk</p>	
<p><b>i</b> Ct d sn kh ls smmr hmsgd O-hesgd RGD lsr msonrr hald sn b lk Bq 2/ g74/Htr BI b dr 017F dmToc sd l t kold sh dr hnnqdqn ædc sgd BL B f dndq smmv sgr do q sd hntsc s bgt mjr - Sgdqenql c s Kdrf sg l tr sad r dsn sgd kdrf sg nesgd bnl okds hntsc s -</p>	
<p><b>!</b> Sgd et nbsmm l trsnrk ad b kdc læsgd r dqlthd v r r s ædc adæql r t bddr r t k'b lkne Bq 2/ g74/Htr BI b dr 017F dmRs qv s g qst qnu k d BRL D NJ(-</p> <p>&gt; Sghr et nbsmm b madr nbgqmmtr nq r nbgqmmtr -</p> <p>&gt; Sghr et nbsmm l mmmqdncq ns-</p> <p>&gt; Sghr et nbsmm l b kdc a sgd BRL -</p> <p>&gt; Sgd u lk æls nesgh r dqlthd cdodncr nmB X 2/ G74/H TR BL B DR017F DMBNMEHF -</p> <p>B lkBnnsd s</p> <p>&gt; Sghr et nbsmm b mad b kdc æql s r j kdudknrk -</p>	

S ald 4-10 Bq 2/ g74/Htr BI b dr 017F dmToc sd

#### 5.4.14 Cry\_30\_Rh850lcus\_CmacAes128GenFinish

Csm_ReturnType (Const void *cfgPtr, const uint8 *resultPtr, uint32* resultLengthPtr, boolean truncationIsAllowed)	
bef Osq	Gnlcr onlnsdqsn sgd bnnef t q smmnesgh r dqltd-Rdd Bq 2/ g74/ Htr BI b dr 017F drBnnef S od enql nql hndq smm-
qlr t leOsq	Gnlcr onlnsdqsn sgd l dl nq knb smmv ghbg v hkgnc sgd qlr t lenesgd BL B f dndq smm lesgd qlr t lecndr mnses hns sgd f ludmat aedq nrc sq nrb smmln knv dc sgd qlr t lsr g lkad sq nrb sdc
qlr t leKdnf sgOsq	Gnlcr onlnsdqsn sgd l dl nq knb smmlmv ghbg sgd kdnf sg hndq smmln r snqlc-Nmb knf sgh et nbsmmssgh o q l dsdqr g kbnns hnsd r h d nesgd at aedqoqule dc a qlr t leOsq V gdmsgd qdpt dr sg r emm gdc r t bddr et k sgd kdnf sg nesgd qlst qrdc L B rg lkad r snqlc-
sq nrb smmln knv dc	Sgh o q l dsdqr s sdr v gdsdq sq nrb smmnesgd qlr t leln knv dc nqrms-S TD9sq nrb smmln knv dc-E KRD9sq nrb smmln mns knv dc-
BRL D NJ	dpt dr sr t bddr et k
BRL D MNS NJ	dpt dr se hdc
BRL D RL KK ATEED	Sgd oqule dc at aedqlr snn r l ksn r snql sgd qlr t le nrc sq nrb smmv r mns knv dc-
Sgh hnsdql bdr g lkad trdc sn emm g sgd RGD-BL B f dndq smmr dqltd-	
Sgd et nbsmmemm gdr sgd r dqltd-	
hnm dqnqnbtt qdpc sgd BL B m v dsdmsn sgd qlr t leOsq nrc sgd qlr t leKdnf sgOsq f ds t oc sdc v hsg sgd kdnf sg nesgd BL B-	
Sgd o q l dsdqr ql r snqlc hm at aedq nrc sgd r dqltd f ds l qj dc sn ad emm gdc hnsd nrd sl hmet nbsmm b lk	





Sgd et nbsmml trsnrk ad b kdc lsgdrdqld v r rs qdc adnqprtbbdrret k'b kke  
Bq 2/ g74/Htr BI b dr 017F dnRs qvsg qdst qnu kd BRL D NJ(- et nbsmm  
b kkeb kBq 2/ g74/Htr BI b dr 017F dnToc sd adsvddmsgdl m knvdc-  
Sglm et nbsmml trsnrk ad b kdc nntbd esdq rtbbdrret kb kke  
Bq 2/ g74/Htr BI b dr 017F dnRs qvsg qdst qnu kd BRL D NJ(- et nbsmm  
l t kold st dr dudmlsgd qdst qnu kd m nnsBRL D NJ-


- > Sglm et nbsmmb madr nbgqmmtr nq r nbgqmmtr -
- > Sglm et nbsmmlr mmqddnsq ns-
- > Sglm et nbsmmlr b kdc a sgd BRL -
- > Sgd u k kals nesglm r dqld cdodner nmB X 2/ G74/HB TR BL B DR017F DMBNMEH -

B kknnd s

- > Sglm et nbsmmb mad b kdc eqi s r j kdudknrk -


S ald 4-11 Bq 2/ g74/Htr BI b dr 017F dnElmng

## 5.4.15 Cry\_30\_Rh850lcus\_CmacAes128GenMainFunction

void		(void)
unlc	nmrd	
unlc	nmrd	
<p>H oldl dnr sgd O-Hn ad b kdc b bkt lk sn oqbdrr sgd qpt dr sdc r dqltd-</p> <p>Sgln et nbsmmddcr sn ad b kdc eq r nbgqnmtr et nbsmmg mclmf lnnqpdqsn oqbdrr sgd r dqltd- l</p> <p>r dqltd lr oqbdrr dc sgd et nbsmmr dnr b ka bj nnsdb smm-</p>		
<div><div></div><div>Sgln et nbsmmr dl os l Tr d R nbl na Oqbdrr lmf lr dm akdc-</div></div>		
<p>&gt; Sgln et nbsmmr r nbgqnmtr -</p> <p>&gt; Sgln et nbsmmr nnsqpdqsn -</p> <p>&gt; Sgln et nbsmmg r sn ad b kdc a BRL -</p> <p>&gt; Sgln et nbsmmr trsmnsad b kdc a sgd ooltd smm-</p> <p>&gt; Sgd u lk alks nesgln r dqltd cdodnr nmB X 2/ G74/ HB TR BL B DR017F DMBNMEHF -</p>		
B kbnnd s		
<p>&gt; Sgln et nbsmmr mad b kdc eqpl s r j kdudknrk -</p>		



S ald 4-12 Bq 2/ g74/ Htr BI b dr 017F dnl lnnEt nbsmm

## 5.4.16 Cry\_30\_Rh850Icus\_CmacAes128VerStart

Csm_ReturnType (Const void *cfgPtr, const Csm_SymKeyType *keyPtr)	
bef Oeq	Gnlcr onlnsdqsn sgd bnnef t q smmnesgh r dqltd-Rdd Bq 2/ g74/ Htr BI b dr 017UdcBnnef S od enql nql hndq smm-
jd Oeq	Gnlcr onlnsdqsn sgd jd v g h g r n ad trdc ensgd BL B uddq smm-Sgd jd Oeqb mldsgdqbnns hm ok hns sjd 'jd Oeqdnf sg < 05(nq jd h 'jd Oeqdnf sg < 0(-
BRL D NJ	dpt dr sr t bddr r et k
BRL D MNS NJ	dpt dr se hdc-
BRL D ATRX	dpt dr se hdc r dqltd m r skatr -
Sghr hnsdpe bdr g kcad trdc sn hntsh h d sgd BL B uddq smmr dqltd nesgh l nct kd-	
Sgd et nbsmmrs q sgd r dqltd-Sgd jd h m r nqdc mc lsgd jd Oeqbnns hm ok hns s sgd jd m kn cdc sn sgd L jd rks-	
Sgd o q l dsdq q r nqdc hm atedq mc sgd r dqltd f ds l qjdc sn ad r s qdc hmsgd nrl sl hm et nbsmm b k-	
 <p>hsgm et nbsmm m b kdc r t bddr r et k'BRL D NJ( sgd b k dql trsb k Bq 2/ g74/ Htr BI b dr 017UdcEhmg gdq edq b kne Bq 2/ g74/ Htr BI b dr 017UdcToc sd adsv ddm sgd m knvdc- sdnsmm9hsgd Ehmg-et nbsmm m mdudqb kdc sgd RGD m akobjdc enq knsgdqr dqltdr -</p>	
<p>&gt; Sghr et nbsmm b mad r nbgqmmtr nq r nbgqmmtr -</p> <p>&gt; Sghr et nbsmm m m m q d n s q n s-</p> <p>&gt; Sghr et nbsmm m b kdc a sgd BRL -</p> <p>&gt; Sgd u k a h s nesgh r dqltd cdodm r nmB X 2/ G74/ HTR BL B DR017UD BNMEHf -</p> <p>&gt; Oqbnnef smm9Rdqltd m h d-</p>	
B k B n n s	
<p>&gt; Sghr et nbsmm b mad b kdc eqpl s r j kdudknk -</p>	


S ald 4-13 Bq 2/ g74/ Htr BI b dr 017UdcRs q

## 5.4.17 Cry\_30\_Rh850Icus\_CmacAes128VerUpdate

Csm_ReturnType (Const void *cfgPtr, const uint8 *dataPtr, uint32 dataLength)	
bef Oeq	Gnkr onhædqn sgd bnnef t q smnesgh r dæpnd-Rdd Bq 2/ g74/Htr BI b dr 017UdqBnnef S od æql nq l hndq smm-
c s Oeq	Gnkr onhædqn sgd c s æqv ghg BL B rg lkad uddæd- Sgd ccærr nesgd onhædqnædcr sn ad kf mæc nm21-als- Rdd h onæ mæsd æqsgm o q l dædædnv -
c s Kdrf sg	Bnms hmr sgd nt l adqnea sdr æqv ghg sgd BL B rg lkad uddæd-
BRL D NJ	dpt drsr t bddr æ k-
BRL D MNS NJ	dpt drse hæc-
Sgh hædæ bd o rrdr sgd hrot sc s sn sgd BL B uddæd smmr dæpnd-	
Sgd æ nbsmm oc sdr sgd r dæpnd-Sgd c s Kdrf sg mæ c s Oeq æ r snæc hædqn kænqsgd æmng b lk-	
Sgd o q l dædæ æ r snæc hm ætæd mæ sgd r dæpnd fædæ l æjdc sn ad t oc æd hmsgd mæ sl hmr æ nbsmm b lk-	
<div>  <p>Ct d sn hæ smmr hmsgd O-hesgd RGD lsr msonrr hæd sn b lk Bq 2/ g74/Htr BI b dr 017UdqToc æ l t hæd sh dr hmrædqn ædæ sgd BL B uddæd smmv hgrdo q æ hrot sc s bgt mjr - Sgdæææ c s Kdrf sg l trsæd r dsæ sgd kdrf sg nesgd bnl ækæd hrot sc s -</p> </div>	
<div>  <p>Sgd æ nbsmm l trsnrk æd b hæc æsgd r dæpnd v r r s ææc ææææ r t bddr æ k'b lkne Bq 2/ g74/Htr BI b dr 017UdqRs æv hgr æst ænu k d BRL D NJ(-  Sgd æ nbsmm r nqæ r nrk sgd ccærr nesgd c s Oeq mæ mæsgd bnædæsgd onhædqn ææææææædæ-Sgd bnædææsgd c s Oeqm u hæ t næk Bq 2/ g74/Htr BI b dr 017UdqÆmng g r b hæc mæ d dbt ææc-</p> </div>	
<p>&gt; Sgh æ nbsmmæ mad r nbgæmmtr nq r nbgæmmtr -</p> <p>&gt; Sgh æ nbsmm l mæææææææ mæ</p> <p>&gt; Sgh æ nbsmm l b hæc æ sgd BRL -</p> <p>&gt; Sgd u lk æ hæ nesgh r dæpnd ædææææ nmB X 2/ G74/HTR BL B DR017UD BNMEff -</p>	
B lkBnæd s	
<p>&gt; Sgh æ nbsmmæ mad b hæc æql s r j kduææææ -</p>	

S ald 4-14 Bq 2/ g74/ Htr BI b dr 017UdqToc sd

## 5.4.18 Cry\_30\_Rh850lcus\_CmacAes128VerFinish

Csm_ReturnType (Const void *cfgPtr, const uint8 *MacPtr, uint32 MacLength, Csm_VerifyResultType *resultPtr)	
bef Oeq	Gnkr onhnsdqn sgd bnnef t q smmnesgh r dqltd-Rdd Bq 2/ g74/Htr BI b dr 017UdqBnnef S od enql nql hndq smm-
L bOeq	Gnkr onhnsdqn sgd l dl nq knb smmv gllg v lkgknc sgd BL B sn udde - Sgd ccqlr r nesgd onhnsdqn ddr sn ad kf mdc nm21-als-
L bKdnf sg	Gnkr sgd kdnf sg nesgd L B sn ad udde- Cdodmcmf nmsgd bnnef t q smm sgh u k d m hnsdqpdc r ntl adqneals nq ntl adqnea sdr sn udde -Sgd l h tl rtoonqdc kdnf sg m 05 A sd qlr odbstndk 017 Als-
qlr t kOeq	Gnkr onhnsdqn sgd l dl nq knb smmv gllg v lkgknc sgd BL B -
BRL D NJ	dpt dr sr t bddr et k-
BRL D MNS NJ	dpt dr se hdc
<p>Sgh hnsdqp bd r g kcad t rdc sn emng sgd BL B udde smm-</p> <p>Sgd et nbsmmemngdr sgd r dqltd-</p> <p>Sgd bnl l m sn udde sgd BL B m r dnc sn sgd RGD-Sgd qlr t knesgd udde smm m v dsmm sgd qlr t kOeq</p> <p>Sgd o q l dsdq qlr snqdc m atedq m sgd r dqltd f dr l qjdc sn ad emngdc hnsgd mcl sl mmet nbsmm b k-</p>	
<p> Sgd et nbsmmml trsnrk ad b kdc hnsdqp v r rs qdc adnqlr t bddr et k'b kne Bq 2/ g74/Htr BI b dr 017UdqRs qvsg qlst qnu k d BRL D NJ(- et nbsmm b kneBq 2/ g74/Htr BI b dr 017UdqToc sd adsdmsgd l m knv dc-</p> <p>Sgh et nbsmmml trsnrk ad b kdc nmbd edq r t bddr et kb kne Bq 2/ g74/Htr BI b dr 017UdqRs qvsg qlst qnu k d m mns knv dc sn b ksgm et nbsmmml t kold sh dr dudmtesgd qlst qnu k d m mnsBRL D NJ-</p> <p>Sgd b kdnqnesgh et nbsmmnddr sn dnt qd sg ssgd c s Oeq m h c s v gllg v r o r rdc hnsgd t oc sd et nbsmm m r shku k-</p>	
<p>&gt; Sgh et nbsmmmb madr nbgqmmtr nq r nbgqmmtr-</p> <p>&gt; Sgh et nbsmm m mncqdnsg ns-</p> <p>&gt; Sgh et nbsmm m b kdc a sgd BRL -</p> <p>&gt; Sgd u k alhs nesgh r dqltd cdodmcr nmB X 2/ G74/HB TR BL B DR017UD BNMEHF -</p>	

B kBnnd s

> Sgln et nbsmmb mad b kdc expl s r j kdudknrk -

S ald 4-15 Bq 2/ g74/ Htr BI b dr 017UdcFmng

## 5.4.19 Cry\_30\_Rh850lcus\_CmacAes128VerMainFunction

void (void)

unlc mnd

unlc mnd

Hl oldl dnr sgd OLn ad b kdc b bkt k sn oqbdrr sgd qpt dr sdc r dqltd-  
Sgln et nbsmmddr sn ad b kdc enq r nbgqnmtr et nbsmmg nclmf lmnqdsn oqbdrr sgd r dqltd-  
r dqltd ln oqbdrr dc sgd et nbsmmr dnr b ka bj mnd smm-



Sgln et nbsmmr dl os l Tr d R nbl na Oqbdrr lmf ln dm akdc-


- > Sgln et nbsmmr r nbgqnmtr -
- > Sgln et nbsmmr mnsqdnq ns-
- > Sgln et nbsmmg r sn ad b kdc a BRL -
- > Sgln et nbsmmr trsmnsad b kdc a sgd ook smm-
- > Sgd u lk alts nesgln r dqltd cdodmr nmB X 2/ G74/ HB TR BL B DR017F DMBNMEH -

B kBnnd s

> Sgln et nbsmmb mad b kdc expl s r j kdudknrk -

S ald 4-16 Bq 2/ g74/ Htr BI b dr 017Udc lmf nbsmm



## 5.4.20 Cry\_30\_Rh850lcus\_KeyExtractStart

void (Csm_ConfigIdType cfgId)	
bef Oeq	Gnkr onlnsdqn sgd bnnef t q smmnesgh r dqltd-Rdd Bq 2/ g74/ Htr Jd D sq bsBnnef S od enql nql hndq smm-
BRL D NJ	dpt dr sr t bdr r et k
BRL D MNS NJ	dpt dr se hdc-
BRL D ATRX	dpt dr se hdc r dqltd m r shkatr -
Sghr hndq bdr g kcad trdc sn hndq hnd sgd Jd D sq bsr dqltd nesgd l nctkd-	
Sgd et nbsmmr s q sgd r dqltd-	
Sgd o q l dclq q r snqlc hm atedq mc sgd r dqltd fdr l q dc sn ad r s qdc hmsgd md sl hnd et nbsmm b k-	
<div>  <p>hsgmr et nbsmmr b kdc r t bdr r et k' BRL D NJ( sgd b kcll trsb k Bq 2/ g74/ Htr Jd D sq bsEhmg gdql edq b kne Bq 2/ g74/ Htr Jd D sq bsToc sd adsv dmsgd l m kvdc- sdsmm9hsgd Ehmg-et nbsmmr mdudqb kdc sgd RGD m akbjdc enq knsgdqr dqltdr -</p> </div>	
<p>&gt; Sghr et nbsmmr mad r nbgqmmtr nq r nbgqmmtr -</p> <p>&gt; Sghr et nbsmmr mmqpdnsq m-</p> <p>&gt; Sghr et nbsmmr b kdc a sgd BRL -</p> <p>&gt; Sgd u k alhs nesgh r dqltd cdodmcr nmB X 2/ G74/ HB TR JDXDWS BSBNMEff -</p> <p>&gt; Oqbnrcshmr9Rdqltd m hnd-</p>	
B kBnnd s	
> Sghr et nbsmmr mad b kdc enql s r j kludknrk -	

S ald 4-17 Bq 2/ g74/ Htr Jd D sq bsRs q



#### 5.4.21 Cry\_30 Rh850Icus KeyExtractUpdate


<code>void</code>	(Csm_ConfigIdType cfgId, const
<code>uint8* dataPtr, uint32 dataLength)</code>	
<b>bef Osq</b>	Gnkr onmsdqn sgd bnnef t q smmnesgm r dqltbd-Rdd Bq 2/ g74/Htr Jd D sq bsBnnmf S od enql nqd hrend smm-
<b>c s Osq</b>	Gnkr onmsdqn sgd c s v glbg bnnr hmr dlsdq - ok msd sjd 'Kdnf sg m 05( - L dr f dr L 0 L 1 mc L 2 v lsg mnosmm koqlodncmf Jd ht sn toc sd jd rkshmsgd RGD-'Kdnf sg m 53 nq54 A sdr ( - Jd ht 'Kdnf sg m 0(
<b>c s Kdnf sg</b>	Gnkr sgd kdnf sg nesgd c s lma sdr -
<b>BRL D NJ</b>	dpt drsr tbbdr et k
<b>BRL D MNS NJ</b>	dpt drse kdc-
<b>Sgln msdqp bd o rrdr hmtsc s sn sgd jd d sq bsmmr dqltbd-</b>	
Sgd et nbsmnt oc sdr sgd r dqltbd-Sgln et nbsmmoquedr chedqmsonrr hltodr sn rsnd jd r -	
<ol style="list-style-type: none"> <li>1. Hmtsc s v lsg sgd kdnf sg ne05 A sd qlrsnqlc msd JDx L -</li> <li>2. Hmtsc s v lsg sgd kdnf sg ne53 A sd ql msdqpdsdc r L 0-L 2 eqsgd jd toc sd oqsnbnk r rodbltc msd RGD rodb-</li> <li>3. Hmtsc s v lsg sgd kdnf sg ne54 A sd ql msdqpdsdc r L 0-L 2 eqsgd jd toc sd oqsnbnk r rodbltc msd RGD rodb hmbt cmf Jd ht msd et sa sd nesgd hmtsc s -</li> <li>4. Hmtsc s v lsg sgd kdnf sg ne0 A sd ql trdc r sgd c s hmjd v glbg m qlst qndc msd Ehmrg-Etnbsmm-</li> </ol>	
Sgd o ql dsdq qlrsnqlc hm atsdq mc sgd r dqltbd f dsl qjdc sn ad toc sdc msd mrl sl hmet nbsmm b lk	
<div>  <p>Sgd cqudqcndr mnsrtoonql thok u kcb k ne Bq 2/ g74/Htr Jd D sq bsToc sd-</p> </div>	
<div>  <p>Sgd et nbsmmml trsnrk ad b kdc lesdgr dqltbd v r rs qdc adenql rtbbdr et k'b lkne Bq 2/ g74/Htr Jd D sq bsRs qv lsg qlst quu kd BRL D NJ(-</p> </div>	
<ul style="list-style-type: none"> <li>&gt; Sgln et nbsmmmb madr nbqqnmnr nq r nbqqnmnr -</li> <li>&gt; Sgln et nbsmmmln mmnqpdnseq ns-</li> <li>&gt; Sgln et nbsmmmln b kdc a sgd BRL -</li> <li>&gt; Sgd u lk ahks nesqlm r dqltbd cdodnrc nmB X 2/ G74/HBTR JDxDWS BSBNMEHF -</li> </ul>	

B kbBnmæ s

> Sglt æ nbsmmb mad b kdc æpl s r j kdudknrk -


S ald 4-18 Bq 2/ g74/ Htr Jd D sq bsToc sd

## 5.4.22 Cry\_30\_Rh850lcus\_KeyExtractFinish

void (Csm_ConfigIdType cfgId, Csm_SymKeyType* keyPtr)	
bef Oeq	Gnlcr onlnsdqsn sgd bnneff t q smmnesgh r dqltd-Rdd Bq 2/ g74/Htr Jd D sq bsBnneff S od enql nql hndq smm-
jd Oeq	Gnlcr onlnsdqsn r sq bst q v gdq sgd qpr t ls'd-f-sgd r l l dsq kjd (lr r snqdc hm-
BRL D NJ	dpt dr sr t bddr et k
BRL D MNS NJ	dpt dr se hdc-
Sghm hnsdæ bd rg kcad trdc sn emng sgd jd d sq bsr dqltd-	
Sgd et nbsmmemng gdr sgd r dqltd-	
<p>te jd m toc sdc hnsd MUL sgd jd -c s v hkbnnns hnsd L 3-L 4 nesgd RGD jd toc sd oqsnbnk te sgd JDX L g r addmtoc sdc sgd jd -c s v hkbnnns hnsd bnqpr onnehm jd te enqsg sr ksv glbg b mad trdc r hmtsenqd-f- DR dnbg os-</p> <p>Sgd o q l dsdq qpr snqdc hm atædq mc sgd r dqltd f ds l qjdc sn ad emng gdc hnsd nd sl hmet nbsmm b k-</p>	
<div>  <p>Sgd et nbsmmml trsnrk ad b kdc tesgd r dqltd v r r s ædc adæqpr t bddr et k'b kne Bq 2/ g74/Htr Jd D sq bsRs æv hsg qst qnu k d BRL D NJ(- et nbsmmmb kne b k Bq 2/ g74/Htr Jd D sq bsToc sd adæv dmsgd l m knv dc-</p> <p>Sghm et nbsmmml trsnrk ad b kdc nntbd ædq r t bddr et kb kne Bq 2/ g74/Htr Jd D sq bsRs æ- h m mns knv dc sn b ksglm et nbsmmml t kstold st dr dudmtesgd qst qnu k d m mns BRL D NJ-</p> </div>	
<p>&gt; Sghm et nbsmmmb mad r nbgqmmtr nq r nbgqmmtr-</p> <p>&gt; Sghm et nbsmmml mnmædmsq ns-</p> <p>&gt; Sghm et nbsmmml b kdc a sgd BRL -</p> <p>&gt; Sgd u k æl æs nesghm r dqltd cdodnæ nmB X 2/ G74/HB TR JDXDWS BSBNMEHF -</p>	
B k Bnns s	
<p>&gt; Sghm et nbsmmmb mad b kdc æql s r j kdudknrk-</p>	


S ald 4-2/ Bq 2/ g74/Htr Jd D sq bsEmng

### 5.4.23 Cry\_30\_Rh850lcus\_KeyExtractMainFunction

void (void)	
unlc	mmrd
unlc	mmrd
<p>H okl dnr sgd O-Hn ad b kdc b bkt lk sn oqbdrr sgd qpt dr sdc r dqltd-</p> <p>Sgln et nbsmmrddcr sn ad b kdc eq r rbgqnmtr et nbsmmg mclmf lnnqpdqsn oqbdrr sgd r dqltd- l</p> <p>r dqltd lr oqbdrr dc sgd et nbsmmr dnr b ka bj nnsd smm-</p>	
<div>  <p>Sgln et nbsmmr dl os l Tr d R nbl na Oqbdrr lmf lr dm akdc-</p> </div>	
<p>&gt; Sgln et nbsmmr r rbgqnmtr -</p> <p>&gt; Sgln et nbsmmr nnsqpdnsq ns-</p> <p>&gt; Sgln et nbsmmg r sn ad b kdc a BRL -</p> <p>&gt; Sgln et nbsmmr trsmnsad b kdc a sgd ooltd smm-</p> <p>&gt; Sgd u lk alns nesgln r dqltd cdodnr nmB X 2/ G74/ HB TR JDXDWS BSBNMEH -</p>	
B kBnns s	
<p>&gt; Sgln et nbsmmr mad b kdc eqpl s r j kdudknrk -</p>	



S ald 4-20 Bq 2/ g74/ Htr Jd D sq bsl lnrEt nbsmm

## 5.4.24 Cry\_30\_Rh850lcus\_KeyWrapSymStart

void (Csm_ConfigIdType cfgId, const Csm_SymKeyType * keyPtr, const Csm_SymKeyType * wrappingKeyPtr)	
bef Osg	Gnlcr onlnsdqsn sgd bnnef t q smmnesgh r dqlthd-Rdd Bq 2/ g74/ Htr Jd V q oR I Bnnef S od enql nql lreng smm-
keyPtr	Gnlcr onlnsdqsn sgd r l l dsqth jd sn ad v q oodc-
wrappingKeyPtr	Gnlcr onlnsdqsn sgd jd trdc enqv q oohrf -
BRL D NJ	dpt dr sr t bddr r æ k
BRL D MNS NJ	dpt dr se hdc-
BRL D ATRX	dpt dr se hdc r dqlthd ln rstkatr -
Sghn lmsdæ bd rg kkd trdc sn hntsh hkd sgd r l l dsqth kjd v q oohrf r dqlthd nesgd l nct kd-	
Sgd æ nbsmmrs ær sgd r dqlthd-	
Sgd o q l dsdq ær snæpc hm atædq mc sgd r dqlthd f ds l æj dc sn ad rs ædc hm sgd nrd sl hm æ nbsmm b k-	
<div>  <p>læsgln æ nbsmmrn b kdc r t bddr r æ k' BRL D NJ( sgd b kkdql trsb k Bq 2/ g74/ Htr Jd V q oR I Ehlnn g gdæ ædq b kne Bq 2/ g74/ Htr Jd V q oR I Toc sd adsv ddmægd l ln knv dc- sdsmmnæsgd Ehlnn g-æ nbsmmrn nrdudqb kdc sgd RGD ln akæbj dc æq knsgdqr dqlthdr -</p> </div>	
<p>&gt; Sghn æ nbsmmrn mad r nbgqmmtr nq r nbgqmmtr -</p> <p>&gt; Sghn æ nbsmmrn nnnæqdææq næ-</p> <p>&gt; Sghn æ nbsmmrn b kdc a sgd BRL -</p> <p>&gt; Sgd u k ælæ nesghn r dqlthd cdodææ nmb X 2/ G74/ HTR JDXV ORXL BNMEHF -</p> <p>&gt; OæbnææsmnæRdqlthd ln hkd-</p>	
B k Bnnæd s	
<p>&gt; Sghn æ nbsmmrn mad b kdc æpl s r j kdudknrk -</p>	


S æld 4-21 Bq 2/ g74/ Htr Jd V q oR I Rs æ

## 5.4.25 Cry\_30\_Rh850Icus\_KeyWrapSymUpdate

void (Csm_ConfigIdType cfgId, const uint8* dataPtr, uint32 * dataLengthPtr)	
bef Oeq	Gnkr onhnsdqn sgd bnnef t q smmnesgh r dqlhd-Rdd Bq 2/ g74/Htr Jd V q oR l Bnnef S od enql nql hndq smm-
c s Oeq	Gnkr onhnsdqn sgd l dl nq knb smmv ghbg v hkgnc sgd qrt l nesgd jd v q oohf -Sgd ccqrr nesgd onhnsdqn dcr sn ad kf mdc nm21-als-
c s Kdnf sgOeq	Gnkr onhnsdqn sgd l dl nq knb smmv ghbg sgd kdnf sg hndq smm r nqpc-Nmb knf sgh d nbsmmgh o q l dsdqr g kbnnr hnsd r h d nesgd at æd qoquhdc a c s Oeq V gdmagd qpt dr sg r smm gdc r t bddr d k sgd kdnf sg nesgd bnl ot sdc u k d m ad r nqpc- Sgd nnk r toonqdc u k u k d enqsgm o q l dsdqm 001-
BRL D NJ	dpt dr sr t bddr d k-
BRL D MNS NJ	dpt dr se hdc-
Sgh hndq bd r g kkd trdc sn qsdud sgd qrt l nesgd jd v q oohf nodq smm-	
Sgd d nbsmm oc sdr sgd r dqlhd-Sgd bnl l m sn d onqsgd L jd m r dnc sn sgd RGD-	
Sgd o q l dsdq qrt nqpc hm at æd q m sgd r dqlhd f d r l q dc sn ad t oc sdc hnsd m d sl hnd nbsmm b k-	
<div>  <p>Sgd cduqendr mnsr toonq l t hnd u k b k ne Bq 2/ g74/Htr Jd V q oR l Toc sd-</p> </div>	
<div>  <p>Sgd d nbsmm l trsnrk ad b kdc l sgd r dqlhd v r r s qdc ad enq r t bddr d k' b k ne Bq 2/ g74/Htr Jd V q oR l Rs qv sg qst qmu k d BRL D NJ(-</p> </div>	
<p>&gt; Sgh d nbsmm b mad r nbgqmmtr nq r nbgqmmtr -</p> <p>&gt; Sgh d nbsmm l m m qdmsq m-</p> <p>&gt; Sgh d nbsmm l b kdc a sgd BRL -</p> <p>&gt; Sgd u k a hns nesgh r dqlhd cdodmcr nmB X 2/ G74/H TR JDXV ORXL BNMEH -</p>	
B k Bnns s	
<p>&gt; Sgh d nbsmm b mad b kdc enl s r j kdudknrk -</p>	


S ald 4-22 Bq 2/ g74/Htr Jd V q oR l Toc sd

## 5.4.26 Cry\_30\_Rh850lcus\_KeyWrapSymFinish

void (Csm_ConfigIdType cfgId)	
bef Oeq	Gnkr onlnsdqsn sgd bnnef t q smmnesgh r dqltd-Rdd Bq 2/ g74/ Htr Jd V q oR I Bnnef S od enql nql lneq smm-
BRL D NJ	dpt dr sr t bddr et k
BRL D MNS NJ	dpt dr se hdc-
Sghm lmsdpe bdr g kcad trdc sn emng sgd r l l dsdpe kjd v q oolmf r dqltd-	
Sgd et nbsmmemngdr sgd r dqltd-	
Sgd o q l dsdq qprnqpc hm atedq mc sgd r dqltd fdr l qjdc sn ad emngdc lmsgd nd sl lmet nbsmm b k-	
<div>  <p>Sgd et nbsmmml trsnrk ad b kdc lmsgd r dqltd v r r s qdc adenql r t bddr et k'b lkne Bq 2/ g74/ Htr Jd V q oR I Rs qv lsg qst qnu k d BRL D NJ(- et nbsmmmb k neb k Bq 2/ g74/ Htr Jd V q oR I Toc sd adsv dmsgd l m knv dc-</p> <p>Sghm et nbsmmml trsnrk ad b kdc nmbd esdq r t bddr et kb lkne Bq 2/ g74/ Htr Jd V q oR I Rs q- l m mns knv dc sn b ksglm et nbsmmml t lshold sh dr dudmlesgd qst qnu k d m mns BRL D NJ-</p> </div>	
<p>&gt; Sghm et nbsmmmb madr nbgqnmtr nq r nbgqnmtr-</p> <p>&gt; Sghm et nbsmmml mnmqpdmsq ms-</p> <p>&gt; Sghm et nbsmmml b kdc a sgd BRL -</p> <p>&gt; Sgd u k alks nesghm r dqltd cdodmcr nmB X 2/ G74/ HBTR JDXV ORXL BNMEHF -</p>	
B k Bnnsd s	
<p>&gt; Sghm et nbsmmmb mad b kdc eqnl s r j kludknrk -</p>	

S ald 4-23 Bq 2/ g74/ Htr Jd V q oR I Elmng


## 5.4.27 Cry\_30\_Rh850lcus\_KeyWrapSymMainFunction

void (void)	
unlc	mmrd
unlc	mmrd
<p>H okd dnæ sgd O-Hn ad b kdc b bktb lk sn oqbdrr sgd qpt dr sdc r dqltd-</p> <p>Sgln æ nbsmmrdcr sn ad b kdc enq r nbgnmmtr æ nbsmmg mclmf lnnqpdqsn oqbdrr sgd r dqltd-æ r dqltd ln oqbdrr dc sgd æ nbsmmr dncr b ka bj nnsæb smm-</p>	
<div>  <p>Sgln æ nbsmmr dl os æ Tr d R nbl na Oqbdrr lmf ln dm akdc-</p> </div>	
<p>&gt; Sgln æ nbsmmr r nbgnmmtr -</p> <p>&gt; Sgln æ nbsmmr nnsqpdæq næ-</p> <p>&gt; Sgln æ nbsmmg r sn ad b kdc a BRL -</p> <p>&gt; Sgln æ nbsmmr trsmnsad b kdc a sgd oolktb smm-</p> <p>&gt; Sgd u lk alæ nesgln r dqltd cdodncr nmB X 2/ G74/ HB TR JDXV ORXL BNMEH -</p>	
B kBnæd s	
<p>&gt; Sgln æ nbsmmr mad b kdc eqnl s r j kdudknrk -</p>	

S ald 4-24 Bq 2/ g74/ Htr Jd V q oR l L lmrEt nbsmm





## 5.4.28 Cry\_30\_Rh850lcus\_RngSeedStart

Csm_ReturnType (Const void *cfgPtr)	
bef Osg	Gnlcr onlnsdqsn sgd bnnef t q smmnesgh r dqltd-Rdd Bq 2/ g74/ Htr nf Bnnef S od enql nql hndq smm-
BRL D NJ	dpt dr sr t bdr r et k
BRL D MNS NJ	dpt dr se hdc-
BRL D ATRX	dpt dr se hdc r dqltd in r shkatr -
Sghm hndq bd rg kcad trdc sn hndq h d sgd q menl ntl adqf dmdq snqr ddc r dqltd nesgd l nct kd-	
Sgd et nbsmmrs q sgd r dqltd-	
Sgd o q l dclq q l r nqlc hm atedq mc sgd r dqltd f ds l qj dc sn ad r s qdc hmsgd ncl sl hndq nbsmm b k-	
<div>  <p>hsgm et nbsmm b kdc r t bdr r et k' BRL D NJ( sgd b k dql trsb k Bq 2/ g74/ Htr nf RddcElmng gdql esdq b kne Bq 2/ g74/ Htr nf RddcToc sd adsv dmsgd l in knv dc- sdnsmn9 hsgd Elmng- et nbsmm mldudqb kdc sgd RGD in akbjdc enq knsgdqr dqltdr -</p> </div>	
<p>&gt; Sghm et nbsmm b mad r nbgqmmtr nq r nbgqmmtr -</p> <p>&gt; Sghm et nbsmm mnmqldnsq ns-</p> <p>&gt; Sghm et nbsmm b kdc a sgd BRL -</p> <p>&gt; Sgd u k alts nesgh r dqltd cdodmcr nmB X 2/ G74/ HB TR MF BNMEHF -</p> <p>&gt; Oqbnmclsmn9Rdqltd in hnd-</p>	
B kBnned s	
<p>&gt; Sghm et nbsmm b mad b kdc enql s r j kdudknk -</p>	


S ald 4-25 Bq 2/ g74/ Htr nf RddcRs q

## 5.4.29 Cry\_30\_Rh850lcus\_RngSeedUpdate

Csm_ReturnType (Const void *cfgPtr, const uint8 *seedPtr, uint32 seedLength)	
bef Osg	Gnkr onhndqsn sgd bnnrff t q smmnesgh r dqlhd-Rdd Bq 2/ g74/ Htr nf Bnnrff S od enql nql hndq smm-
rddcOsg	Gnkr onhndqsn sgd rddc enqsgd q mcnl ntl adqf dndq sq Sgd ccqrr nesgd onhndqrdcr sn ad kf mdc nm21-als-
rddcKdnfsg	Bnnr hnr sgd kdnfsg nesgd rddc hma sdr-Nnrk sgd u kt d 05 m rt oonqdc-
BRL D NJ	dpt drsr t bdr r et k
BRL D MNS NJ	dpt drse hdc-
Sgh hndq bd o r r dr rddc sn sgd q mcnl ntl adqf dndq sq rddc r dqlhd-	
Sgd et nbsmmt oc sdr sgd r dqlhd-Sgd bnl l mcn sn d sdr sgd rddc v hsg sgd f hndmr ddcOsg m r dnc sn sgd g qv ql-	
Sgd o q l dndq q rsnqdc hm atedq mcn sgd r dqlhd f dr l qjdc sn ad t oc sdc hmsgd md sl hndet nbsmmt b k-	
<div>  <p>Sgd cqdndqndr mnsrt oonql t ktd u k b k ne Bq 2/ g74/ Htr nf RddcToc sd-</p> </div>	
<div>  <p>Sgd et nbsmmt trsnrk ad b kdc hsgd r dqlhd v r r s qdc ad enql r t bdr r et k'b kne Bq 2/ g74/ Htr nf RddcRs qv hsg qst qnu kt d BRL D NJ(-</p> </div>	
<p>&gt; Sgh et nbsmmb mad r nbgqnmtr nq r nbgqnmtr-</p> <p>&gt; Sgh et nbsmmt mnmqndsq ns-</p> <p>&gt; Sgh et nbsmmt b kdc a sgd BRL -</p> <p>&gt; Sgd u k alhs nesgh r dqlhd cdodmr nmB X 2/ G74/ HB TR MF BNMEHf -</p>	
B kBnm s	
<p>&gt; Sgh et nbsmmb mad b kdc enql s r j kdudknrk -</p>	


S ald 4-26 Bq 2/ g74/ Htr nf RddcToc sd

### 5.4.30 Cry\_30\_Rh850lcus\_RngSeedFinish

Csm_ReturnType (Const void *cfgPtr)	
bef Oeq	Gnkr onlnsdqsn sgd bnnef t q smmnesgh r dqltd-Rdd Bq 2/ g74/ Htr nf Bnnef S od enql nql hndq smm-
BRL D NJ	dpt dr sr t bddr et k
BRL D MNS NJ	dpt dr se hdc-
Sghm hndq bd r g kcad trdc sn emng sgd q mcnl ntl adqf dndq snqr ddc r dqltd-	
Sgd et nbsmmemngdr sgd r dqltd-	
Sgd o q l dclq q r snqpc hm atedq mc sgd r dqltd f ds l qjdc sn ad emngdc hmsgd nd sl hmet nbsmm b k-	
<div>  <p>Sgd et nbsmmml trsnrk ad b kdc lsgdr dqltd v r r s qdc adenql r t bddr et k'b kne Bq 2/ g74/ Htr nf RddcRs qvsg qst qnu k d BRL D NJ(- et nbsmmmb kneb k Bq 2/ g74/ Htr nf RddcToc sd adsv dmsgd l m knv dc-</p> <p>Sghm et nbsmmml trsnrk ad b kdc nmbd esdq r t bddr et kb kne Bq 2/ g74/ Htr Jd V q oR l Rs q- s l m mns knv dc sn b ksglm et nbsmmml t shold sh dr dudmlesgd qst qnu k d m mnsBRL D NJ-</p> </div>	
<p>&gt; Sghm et nbsmmmb madr nbgqnmtr nq r nbgqnmtr-</p> <p>&gt; Sghm et nbsmmml mnmqpdnsq ns-</p> <p>&gt; Sghm et nbsmmml b kdc a sgd BRL -</p> <p>&gt; Sgd u k a hts nesghm r dqltd cdodmcr nmB X 2/ G74/ HBTR MFBNMEHF -</p>	
B kBnned s	
<p>&gt; Sghm et nbsmmmb mad b kdc enql s r j kdudknrk -</p>	

S ald 4-27 Bq 2/ g74/ Htr nf RddcEmng

### 5.4.31 Cry\_30\_Rh850lcus\_RngSeedMainFunction

void Bq 2/ g74/ Htr (void)	
unlc	mmrd
unlc	mmrd
<p>H oldl dnr sgd OEn ad b kdc b bkt lk sn oqbdrr sgd qpt drdc r dqltd-</p> <p>Sgln et nbsmmrddcr sn ad b kdc enq r nbgqmmtr et nbsmmg mclmf lnnqpdqn oqbdrr sgd r dqltd- l</p> <p>r dqltd ln oqbdrr dc sgd et nbsmmr dnr b ka bj mnsd smm-</p>	
<div>  <p>Sgln et nbsmmr dl os l Tr d R nbl na Oqbdrr lmf ln dm akdc-</p> </div>	
<p>&gt; Sgln et nbsmmr r nbgqmmtr -</p> <p>&gt; Sgln et nbsmmr mnsqddnsq ns-</p> <p>&gt; Sgln et nbsmmg r sn ad b kdc a BRL -</p> <p>&gt; Sgln et nbsmmr trsmnsad b kdc a sgd ookt smm-</p> <p>&gt; Sgd u lk alts nesgln r dqltd cdodmcr nmB X 2/ G74/ HB TR MF BNMEH -</p>	
B kBnnsd s	
<p>&gt; Sgln et nbsmmr mad b kdc eqpl s r j kdudknrk -</p>	


S ald 4-28 Bq 2/ g74/ Htr nf RddcL lmfEt nbsmm

### 5.4.32 Cry\_30\_Rh850lcus\_RngGenerate

Csm_ReturnType (Const void *cfgPtr, uint8 *resultPtr, uint32 resultLength)	
bef Osq	Gnkr onlnsdqsn sgd bnnef t q smmnesgh r dqltd-Rdd Bq 2/ g74/ htr nf Bnnef S od enql nql hndq smm-
qlr t leOsq	Gnkr onlnsdqsn sgd l dl nq knb smmv gllbg v hkgnc sgd qlr t lnesgd q ncnl ntl adqfdndq smm-Sgd l dl nq knb smml trsg ud skd rssgdrhd qlr t leKdnf sg -

qlr t leKdnf sg

### 5.4.33 Cry\_30\_Rh850lcus\_RngGenerateMainFunction

void (void)	
-	
-	
<p>H oldl dnr sgd O-Hn ad b kdc b bkt lk sn oqbdrr sgd qpt dr sdc r dqltd-</p> <p>Sgln et nbsmmrddcr sn ad b kdc eq r rbgqnmtr et nbsmmg mclmf lnnqpdqsn oqbdrr sgd r dqltd- l</p> <p>r dqltd ln oqbdrr dc sgd et nbsmmr dnr b ka bj nnsd smm-</p>	
	Sgln et nbsmmr dl os l Tr d R nbl na Oqbdrr lmf ln dm akdc-
<p>&gt; Sgln et nbsmmr r rbgqnmtr -</p> <p>&gt; Sgln et nbsmmr nnsqddnsq n-</p> <p>&gt; Sgln et nbsmmg r sn ad b kdc a BRL -</p> <p>&gt; Sgln et nbsmmr trsmnsad b kdc a sgd ooltd smm-</p> <p>&gt; Sgd u lk alts nesgln r dqltd cdodnr nmB X 2/ G74/ HB TR MFBNMEHF -</p>	
B kbnns s	
> Sgln et nbsmmr mad b kdc eqnl s r j kdudknrk -	

S ald 4-30 Bq 2/ g74/ Htr nf F dndq sdL lnt nbsmm

### 5.4.34 Cry\_30\_Rh850lcus\_SelfTest

Csm_ReturnType (void)	
-	
BRL D NJ	Rdlesdrsv r rtbbdræ k
BRL D ATRX	Rdlesdrsg r mnsaddmodæd dc adb trdsgd g æv æv r atr -
BRL D MNS NJ	Rdlesdrsg r e hdc
<p>H oldl dnr sgd O-Hn odæd r dlebgdbj nesgd BL B uddæ h smæ nbsmm-Sgln ln cnrd a bgdbj hnf oædæmædc sdr sudbsæ -Sgd r dlebgdbj ln cnrd nrbd hmsgd hmsæ nbsmmnesgd B X-Sgd trdqb modænl l nql r dlebgdbjr b bktb lk nrbd sgd B X ln hmsæ hdc-</p>	
<p>&gt; Sgln æ nbsmm ln r nbgrmmtr -</p> <p>&gt; Sgln æ nbsmm ln mnsædæsq næ-</p> <p>&gt; Sgd u lk æ hms nesgln rdqubd cdodmæ nm B X 2/ G74/ HB TR RDKE SDRS-</p>	
B kBnnæd s	
<p>&gt; Sgln æ nbsmm b mad b hdc æpl s r j kdudknæ -</p>	

S æld 4-31 Bq 2/ g74/ Htr RdæSdrs

## 5.5 Configurable Interfaces

### 5.5.1 Callout Functions

s æ bnææ t q æld hmsæ bdr sgd B X ædæmæ b kntæ æ nbsmm -Sgd cæbk q smmæ ne sgd b kntæ æ nbsmmæ æd oæuæædc a sgd ARV l nctkd hæ-sgd B X-læm sgd hmsæ f q æqr s r j æn oæuææd sgd bnææpr ænææ hmf æ nbsmm ædæmæmæ -Sgd ædæmæmæ ne sgd b kntæ æ b m æd æitrædc æn sgd r sædl r æddæ - æææmæ k ænl d b kntæ æ b m æd æm æædc v æs sgd

bnrft q smm m d l old h old dms smm m oqulr dc hm sgd sll ok sd ndr - Sgd B X b knt set nbsmmcd b k q smm q cdr b qdc hmsgd enkv hmf s akdr 9

### 5.5.1.1 Timeout-API Location Callout

<pre>void (Cry_SheTimeoutApiServiceType service, Cry_SheTimeoutApiSectionType section)</pre>	
service	<p>Sgln o q l dcdqoqulr hnd smm qpl v gllg r dqlr b sgd b knt sm b kdc-</p> <p>Sgd enkv hmf r dqlr b mad sgd rnt qd nesgd b knt s9</p> <p>CRY_SHE_TO_SERVICE_CMV_VERIFY</p> <p>CRY_SHE_TO_SERVICE_CMV_GENERATE</p> <p>CRY_SHE_TO_SERVICE_AES_DECRYPT</p> <p>CRY_SHE_TO_SERVICE_AES_ENCRYPT</p> <p>CRY_SHE_TO_SERVICE_KEY_EXTRACT</p> <p>CRY_SHE_TO_SERVICE_KEY_WRAP</p> <p>CRY_SHE_TO_SERVICE_PRNG_SEED</p> <p>CRY_SHE_TO_SERVICE_PRNG_GENERATE</p> <p>CRY_SHE_TO_SERVICE_CANCEL</p> <p>CRY_SHE_TO_SERVICE_UNDEFINED</p>
section	<p>Sgln o q l dcdqoqulr hnd smm v gdl d bsk hmsgd r dqlr b sgd b knt sm b kdc-</p> <p>Sgd enkv hmf r dqlr b mad sgd rnt qd nesgd b knt s9</p> <p>CRY_SHE_TO_SECTION_START_SERVICE</p> <p>CRY_SHE_TO_SECTION_UPDATE_SERVICE,</p> <p>CRY_SHE_TO_SECTION_START_LOOP,</p> <p>CRY_SHE_TO_SECTION_STOP_LOOP,</p> <p>CRY_SHE_TO_SECTION_FINISH_SERVICE,</p> <p>CRY_SHE_TO_SECTION_SINGLE_CALL_SERVICE</p> <p>CRY_SHE_TO_SECTION_INIT_SERVICE</p>
<p>Sgd et nbsmm oqulr hnd smm ant ssgd r dqlr v gllg m bt qplnk oqulr dc ne sv gllg kb smmsgd b knt sm b kdc-</p>	
<p>&gt; Et nbsmm m nrk b kdc v gdlmsgd sh dnt s OHm dm akdc-</p>	
<p>B kbnnr s</p>	
<p>&gt; Sgln et nbsmm m b kdc qpl s r j kludknrk -</p>	

S akd 4-32 Sh dnt s OHb smmb knts



### 5.5.1.2 Timeout-API Loop Callout

void (Cry_SheTimeoutApiServiceType service)	
service	<p>Sgth o q l dædqrthd r hndq smmæpl v gthg r dædqrthd sgd b hnt sm b hdc-</p> <p>Sgd ænk v hnf r dædqrthd b mad sgd rnt dæd nesgd b hnt s9</p> <p>CRY_SHE_TO_SERVICE_CMAC_VERIFY</p> <p>CRY_SHE_TO_SERVICE_CMAC_GENERATE</p> <p>CRY_SHE_TO_SERVICE_AES_DECRYPT</p> <p>CRY_SHE_TO_SERVICE_AES_ENCRYPT</p> <p>CRY_SHE_TO_SERVICE_KEY_EXTRACT</p> <p>CRY_SHE_TO_SERVICE_KEY_WRAP</p> <p>CRY_SHE_TO_SERVICE_PRNG_SEED</p> <p>CRY_SHE_TO_SERVICE_PRNG_GENERATE</p> <p>CRY_SHE_TO_SERVICE_CANCEL</p> <p>CRY_SHE_TO_SERVICE_UNDEFINED</p>
Csm_ReturnType	<p>Sn hnt b sd sg smm sh dnt sg r nbbt æpl æst qm CSM_E_OK-</p> <p>h sh dnt sg r nbbt æpl æst qm CSM_E_NOT_OK-</p>
<p>Sgth æ nbsmmth b hdc hm hknor v gthg v hænq ær onm d æpl sgd RGD-</p> <p>V gdm sh dnt snbbt q 'æst qmbnd dpt k CSM_E_NOT_OK( sgd kno v hkad kdes nre sgd bnl l nre CMD_CANCEL v hkad r dnt sgn sgd RGD sn r sio sgd bt æplæ d dbt shnf bnl l nre nmsgd RGD-</p>	
<p>&gt; Et nbsmmth nnt b hdc v gdm sgd sh dnt s OHm dm akdc-</p>	
B kbntæd s	
<p>&gt; Sgth æ nbsmmth b hdc æpl s r j kdudknnt -</p>	

S ald 4-33 æsh dnt s OHmno B hnt s

### 5.5.1.3 Cry\_30\_Rh850Icus\_HardwareErrorCode\_Callout

void (void)	
error	Dædqrthd nesgd G æv æl
-	

Sgln et nbsmmf ds sgd dæqnbcd nesgd g æv æl-Sgln dæqnbcd b mænqd l old ad o rrdc sn sgd l ncd l m fdl dms	
> Et nbsmmf nrk b kdc v gdmB X 2/ G74/ HB TR G CV D D N BNCD m RSC NM-	
B kbnnæd s	
> Sgln et nbsmmf b kdc æpl s r j kdudknrk -	

S ald 4-34 Bq 2/ g74/ HB tr G æv ælDæqnbcd B knts

#### 5.5.1.4 Cry\_30\_Rh850Icus\_DataFlashReadStart\_Callout

boolean	(void)
-	
boolean	S TD æ æl c bddr sn sgd c s ærg m f q næd nsgd æ m d e k d-
Sgln et nbsmmr g ksq sn f ds æl c kbj æqsgd c s ærg-	
> Et nbsmmf nrk b kdc v gdmB X 2/ G74/ HB TR C S EK RG RXMBG NM HB SHNM m RSC NM-	
B kbnnæd s	
> Sgln et nbsmmf b kdc æpl s r j kdudknrk -	

S ald 4-35 Bq 2/ g74/ HB tr C s Ekrg d cRs æ B knts

#### 5.5.1.5 Cry\_30\_Rh850Icus\_DataFlashReadEnd\_Callout

void	(void)
-	
-	
Sgln et nbsmmr g ksq sn æld r d sgd æl c kbj æqsgd c s ærg-	

>	Et nbsmmnr nrk b kdc v gdmB X 2/ G74/ HB TR C S EK RG RXMBG NMHR SHNM In RSC NM-
B kbnnæd s	
>	Sgln æ nbsmmnr b kdc æpl s r j kludknrk -
S ald 4-36 Bq 2/ g74/ HB tr C s Ekrg d cDmæ B knts	

### 5.5.1.6 Cry\_30\_Rh850Icus\_DataFlashWriteStart\_Callout

boolean	(void)
-	
boolean	S TD æ v dæ bddrr æ sgdc s ærg In fq nædc nsgdq In de kd-
Sgln æ nbsmmnr g ksq æ f ds v dæ knbj æqsgdc s ærg-	
>	Et nbsmmnr nrk b kdc v gdmB X 2/ G74/ HB TR C S EK RG RXMBG NMHR SHNM In RSC NM-
B kbnnæd s	
>	Sgln æ nbsmmnr b kdc æpl s r j kludknrk -
S ald 4-37 Bq 2/ g74/ HB tr C s EkrgV dæRs æ B knts	

### 5.5.1.7 Cry\_30\_Rh850Icus\_DataFlashWriteEnd\_Callout

void	(void)
-	
-	
Sgln æ nbsmmnr g ksq æ qld r d sgdc v dæ knbj æqsgdc s ærg-	
>	Et nbsmmnr nrk b kdc v gdmB X 2/ G74/ HB TR C S EK RG RXMBG NMHR SHNM In RSC NM-
B kbnnæd s	
>	Sgln æ nbsmmnr b kdc æpl s r j kludknrk -

S ald 4-38 Bq 2/ g74/ Htr C s EkrgV dndmc B knts

### 5.5.1.8 Cry\_30\_Rh850Icus\_DataFlashSetReadMode\_Callout

void (void)	
-	
-	
le bnl l mc g r addmb nbdkc v gld sv r toc smf jd lsl ad mbdrr q snrv lsg sgd l ncd ne sgd E B Hndc p bd a bj sn sgd qd c l ncd-	
> Et mbsmm m nrk b kdc v gdmB X 2/ G74/ HB TR C S EK RG BNMS NK m RSC NM- B kbnnd s	
> Sglr et mbsmm m b kdc eqpl s r j kdudknrk -	

S ald 4-4/ Bq 2/ g74/ Htr C s EkrgRds d cL ncd B knts

### 5.5.1.9 Cry\_30\_Rh850Icus\_DataFlashReturnFromCommandLockedState\_Callout

void (void)	
-	
-	
Bgdbj lsgd C s krg m lmsgd bnl l mc kbjdc rs sd-le dr admf lssn mnd kl ncd-	
> Et mbsmm m nrk b kdc v gdmB X 2/ G74/ HB TR C S EK RG BNMS NK m RSC NM- B kbnnd s	
> Sglr et mbsmm m b kdc eqpl s r j kdudknrk -	

S ald 4-40 Bq 2/ g74/ Htr C s Ekrg dclqrEqpl Bnl l mcknbjdcRs sd B knts

## 5.6 Services used by CRY\_30\_RH850ICUS

Hsgd enkv hrf s ald rdqubdr oqubdc a nsgdq bnl onndns vglbg qd trdc a sgd B X 2/ G74/ HBTR qd krsdc- Enqcds h antsoqns od ne et nbsmm ks qledqn sgd cnbt l dns smmnesgd oqubchrf bnl onndns

BRL	Br l Rdqubd=B ka bj Mnsdb smm Br l Rdqubd=RdqubdEmngMnsdb smm

S ald 4-41 Rdqubdr trdc a sgd B X 2/ G74/ HBTR

## 5.7 Service Ports

Sgd bt qpnsh oldl dns smmnesgd B X cndr mnsr t oonqRdqubd Onq -

## 6

Hsgd B X 2/ G74/ HB TR sgd sgd sdr b mad bnnr t qdc v hsg sgd enkv hmf snk 9  
> Bnnr t q smmhmC UhhbBnnr t q sq4

### 6.1 Configuration Variants

Sgd B X 2/ G74/ HB TR r t oonq sgd bnnr t q smmu q n8  
> VARIANT-PRE-COMPILE

### 6.2 Deviations

Sgd bt qpnsh oldl dms smmcndr msg ud m cdh smm -

### 6.3 Additions/ Extensions

#### 6.3.1 Timeout handling

Sgd cduqnd sgd onrr hls sn b nbdk q mnmf bnl l mc vgdmsg r bnmrl dc sn  
l tbg sh d-L nq hndq smmqf qmhf sgm ed st qd b mad ent mc hmbg osdq2-0/ -

#### 6.3.2 Hardware error callout

Sgd cduqnd sgd onrr hls sn rdmc sgd g qv qd dqnq sn b knts et nbsmm Sgd  
b knts et nbsmmg r sn ad h oldl dmsdc a sgd trdq'd-f-enq qmhf sgd dqnqbncd(- Sgd  
OHr cdr bqdac hmbg osdq4-4-0-2-

#### 6.3.3 Data flash synchronization

hsgd c s krg qprntqd m rg qdc adsv ddm sgd bq on g qv qd mc sgd ookh smm  
bnq r nbgqrh smm l ad nbdrr q sn ocludns q bd bnmrlsmm -  
Sgd qenq sgd cduqnd qdr sgd ed st qd sn hmunjd b knts sn qpt drs bbdrr sn sgd c s  
krg- Sgd OHr cdr bqdac hmsgd bg osdq4-4-0-3 - 4-4-0-6-

### 6.4 Limitations

#### 6.4.1 Support of Cryptographic Services

Sgd bt qpnsh bq onf q ogth r dqlbdr q r t oonqdc9

▶ RGD- DR017-Rdqubd enqR l l dsq k hsdq bd
▶ RGD-O MF -Rdqubd enq mcnl hsdq bd
▶ RGD-BL B-Rdqubd enqL B hsdq bd
▶ Rdqubd enqR l l dsq kJd D sq bshsdq bd
▶ Rdqubd enqR l l dsq kJd V q oohf hsdq bd

S ald 5-0 Rt oonqdc TSNR rs mc q bnnnd ed st qdr

## 6.4.2 Parallel Access to Services

Ctd sn kti ts stmm hmsgd RGD tsr msonrr hald sn oqibdr r l nqd sg mnmd r dqltbd snrbd-  
mdqng 'BRL D ATRX( m fdmdq sdc v gdm r dqltbd m kpl c q mmmf nc mnsdq  
r dqltbd sqdr sn rs q ssgdr l d sh d-

Sgdqenqd o q kdk bdr r sn r dqltbd v gllg qd cdodncdmsnmsgd RGD m mns knv dc-

## 7

### 7.1 Glossary

Bq osnf q ogth Oqth stud	mt mddk hnf bq osnf q ogth l nct kd nqkaq q

S ald 6-0 Fknrr q

### 7.2 Abbreviations

OH	ookto smmOqnf q l l hnf hndp bd
TSNR	t snl nstnd NodmR r sdi dpglsbst qd
ARV	A r m Rnesv qd
B X	Bq osnf q ogth kaq q l nct kd
BRL	Bq osn Rdqthd L m f dq
CDL	Ch f mnr stb Dudms L m f dq
CDS	Cdudknol dmsDqnfqSq bdq
DBT	Dkdbsqmto BnmsqkTms
GHR	Gdq sldkqthsh stud Rnesv qd
L HB NR	L hqbnnsqkdkqNodmR r sdi dpglsbst qd 'sgd Udbsq TSNR r nkt smm(
SD	t nsh d Dmuhqm dms
RbgL	Rbgdct kd L m f dq
RGD	Rdbt qd G qv qd D sdm mmm
R R	Rnesv qd dpt hpl dmsRodbld smm
RV B	Rnesv qd Bnl onmdms
RV R	Rnesv qd Rodbld smm

S ald 6-1 aaqluh smm



## 8

Ulnst qv dar lsd enql nql hnd smnm

- > Mdv r
- > Oqct br
- > Cdl n rnes qd
- > Rt oonq
- > Sq hmf c s
- > ccql r dr

v v v -udbnqbnl