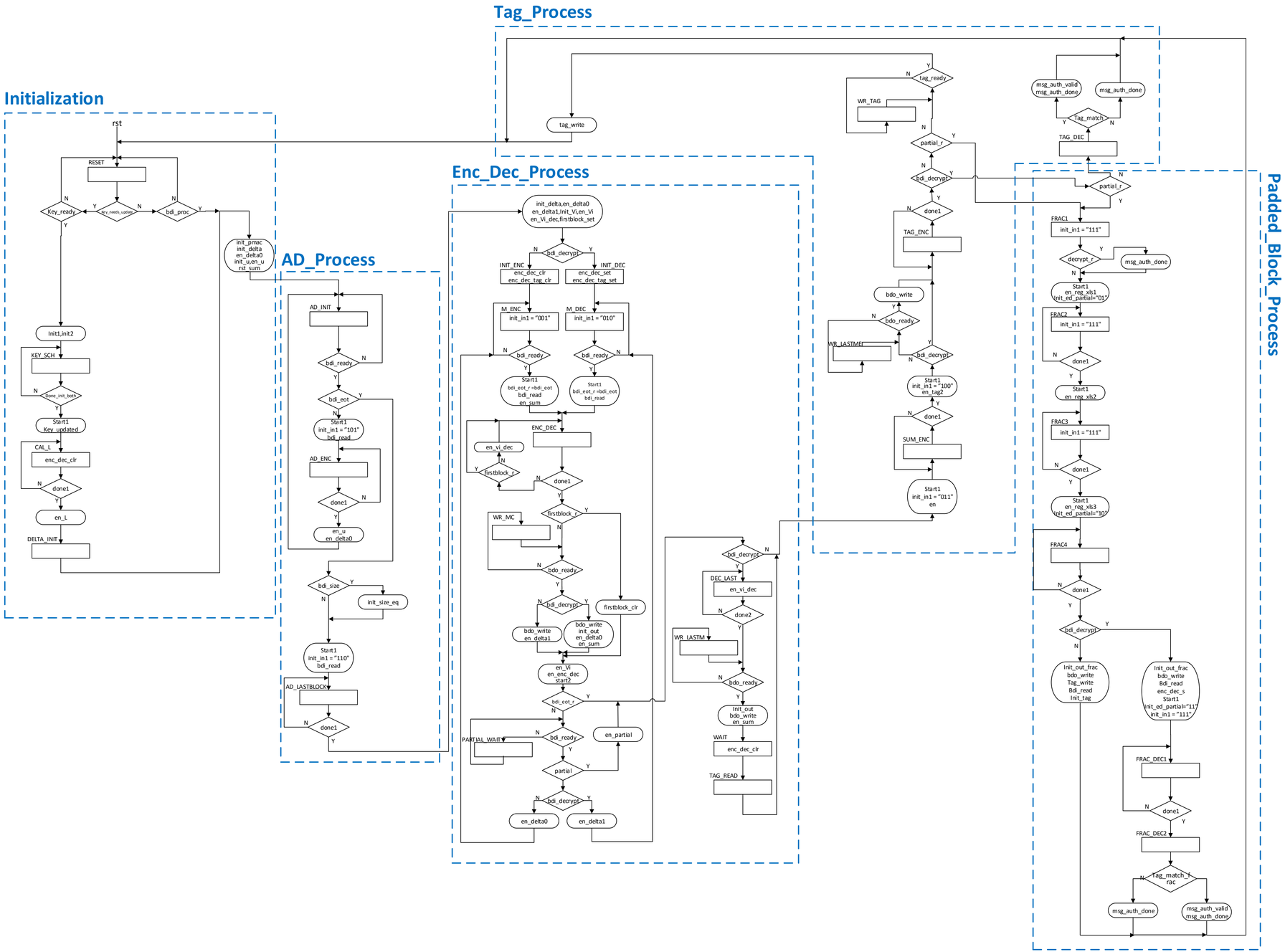

Initialization
rst
RESET
Key_ready
key_needs_update
bdi_proc
init_pmac
init_delta
en_delta0
init_u,en_u
rst_sum
Init1,init2
KEY_SCH
Done_init_both
Start1
Key_updated
CAL_L
enc_dec_clr
done1
en_L
DELTA_INIT
AD_Process
AD_INIT
bdi_ready
bdi_eot
Start1
init_in1 = "101"
bdi_read
AD_ENC
done1
en_u
en_delta0
bdi_size
init_size_eq
Start1
init_in1 = "110"
bdi_read
AD_LASTBLOCK
done1
Enc_Dec_Process
init_delta,en_delta0
en_delta1,Init_Vi,en_Vi
en_Vi_dec,firstblock_set
bdi_decrypt
INIT_ENC
enc_dec_clr
enc_dec_tag_clr
INIT_DEC
enc_dec_set
enc_dec_tag_set
M_ENC
init_in1 = "001"
M_DEC
init_in1 = "010"
bdi_ready
Start1
bdi_eot_r =bdi_eot
bdi_read
en_sum
Start1
bdi_eot_r =bdi_eot
bdi_read
ENC_DEC
en_vi_dec
firstblock_r
done1
WR_MC
bdo_ready
bdi_decrypt
firstblock_clr
bdo_write
en_delta1
bdo_write
init_out
en_delta0
en_sum
en_Vi
en_enc_dec
start2
bdi_eot_r
PARTIAL_WAIT
bdi_ready
en_partial
partial
bdi_decrypt
en_delta0
en_delta1
bdi_decrypt
DEC_LAST
en_vi_dec
done2
WR_LASTM
bdo_ready
Init_out
bdo_write
en_sum
WAIT
enc_dec_clr
TAG_READ
Tag_Process
tag_write
tag_ready
WR_TAG
partial_r
bdi_decrypt
done1
TAG_ENC
bdo_write
bdo_ready
WR_LASTMEI
bdi_decrypt
Start1
init_in1 = "100"
en_tag2
done1
SUM_ENC
Start1
init_in1 = "011"
en
msg_auth_valid
msg_auth_done
msg_auth_done
Tag_match
TAG_DEC
Padded_Block_Process
partial_r
FRAC1
init_in1 = "111"
decrypt_r
msg_auth_done
Start1
en_reg_xls1
init_ed_partial="01"
FRAC2
init_in1 = "111"
done1
Start1
en_reg_xls2
FRAC3
init_in1 = "111"
done1
Start1
en_reg_xls3
init_ed_partial="10"
FRAC4
done1
bdi_decrypt
Init_out_frac
bdo_write
Tag_write
Bdi_read
Init_tag
Init_out_frac
bdo_write
Bdi_read
enc_dec_s
Start1
init_ed_partial="11"
init_in1 = "111"
FRAC_DEC1
done1
FRAC_DEC2
Tag_match_frac
msg_auth_done
msg_auth_valid
msg_auth_done