SNMP V3

Eng. Maha Jeha

Simple Web

SNMPv3

1. OVERVIEW:
2. DESIGN DECISIONS
3. ARCHITECTURE
4. SNMP MESSAGE STRUCTURE
5. SECURE COMMUNICATION
    1. USER SECURITY MODEL (USM)
6. ACCESS CONTROL
    1. VIEW BASED ACCESS CONTROL MODEL (VACM)
7. IMPLEMENTATIONS
8. RFCs

Simple Web

DESIGN DECISIONS

ADDRESS THE NEED FOR SECURY SET SUPPORT

DEFINE AN ARCHITECTURE THAT ALLOWS FOR LONGEVITY OF SNMP

ALLOW THAT DIFFERENT PORTIONS OF THE ARCHITECTURE MOVE AT DIFFERENT SPEEDS TOWARDS STANDARD STATUS

ALLOW FOR FUTURE EXTENSIONS

KEEP SNMP AS SIMPLE AS POSSIBLE

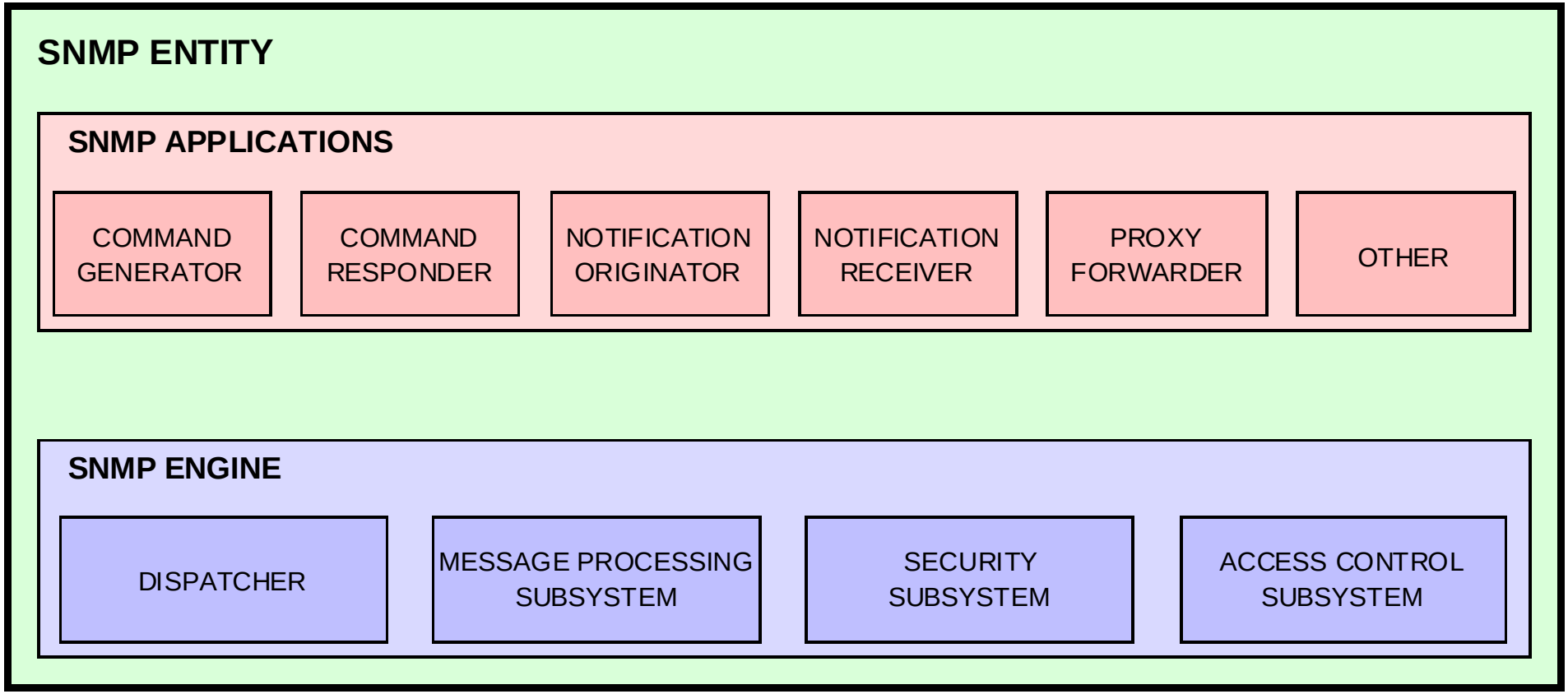
ALLOW FOR MINIMAL IMPLEMENTATIONS

SUPPORT ALSO THE MORE COMPLEX FEATURES, WHICH ARE REQUIRED IN LARGE NETWORKS

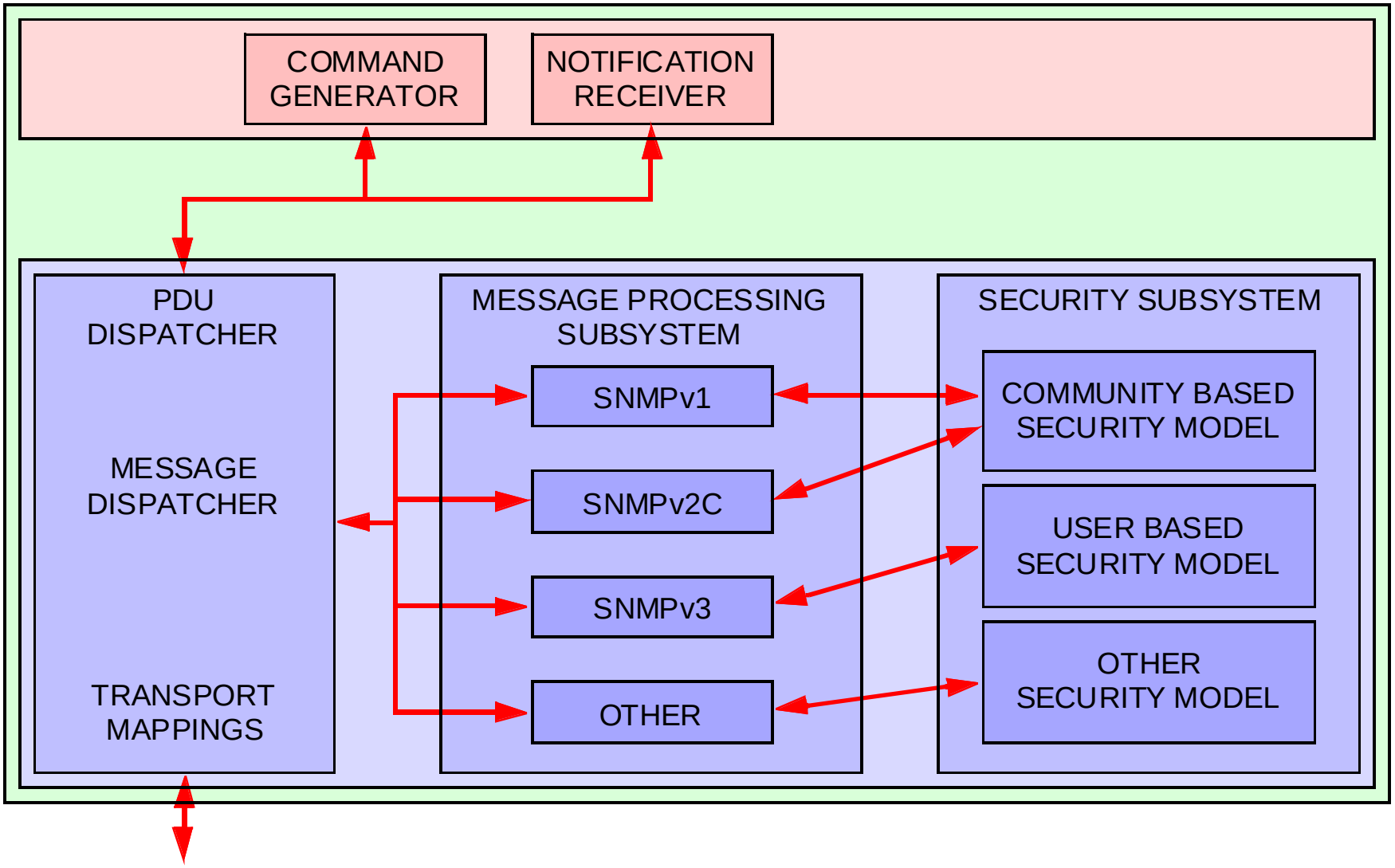
RE-USE EXISTING SPECIFICATIONS, WHENEVER POSSIBLE

Simple Web

SNMPv3 ARCHITECTURE

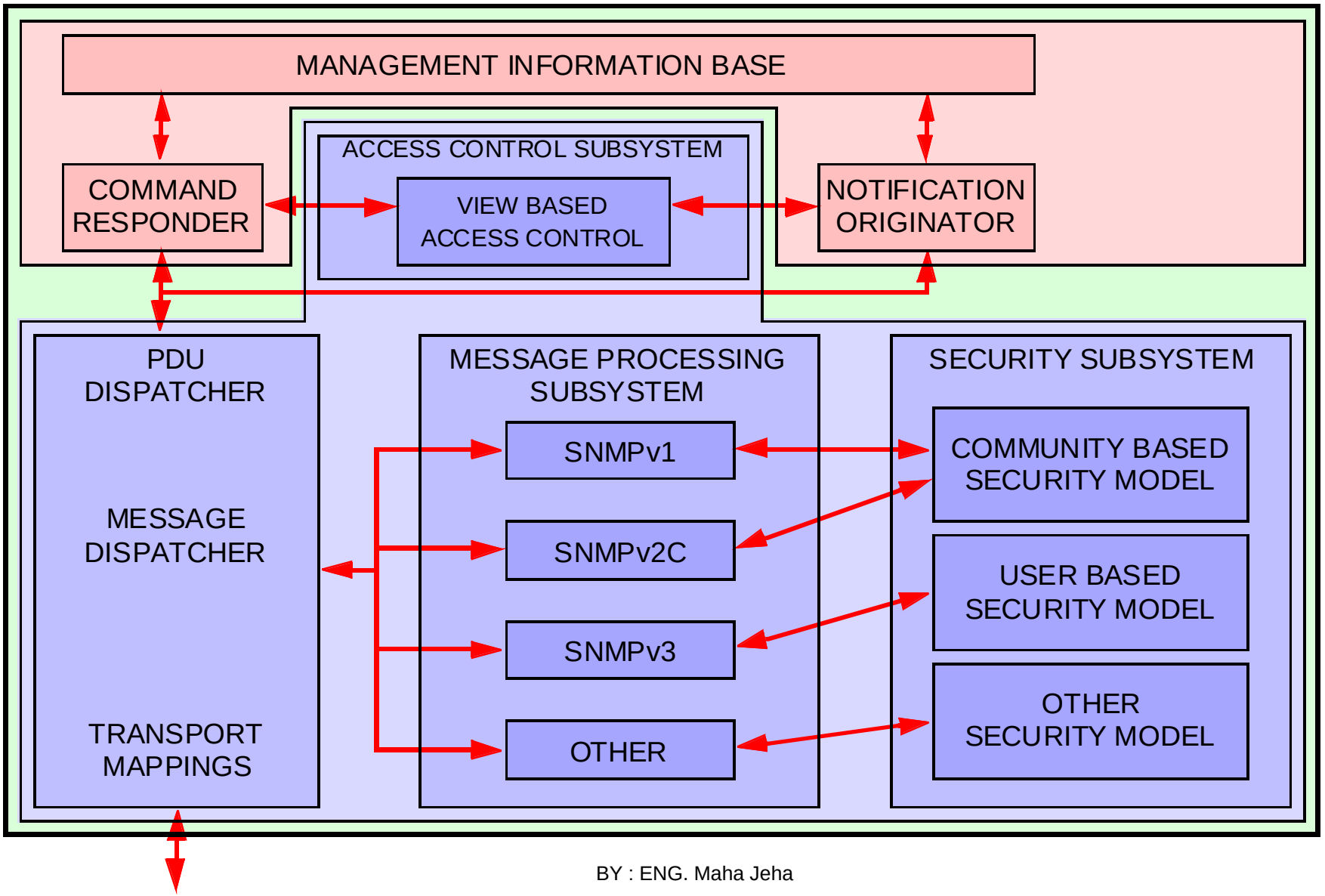


SNMPv3 ARCHITECTURE: MANAGER

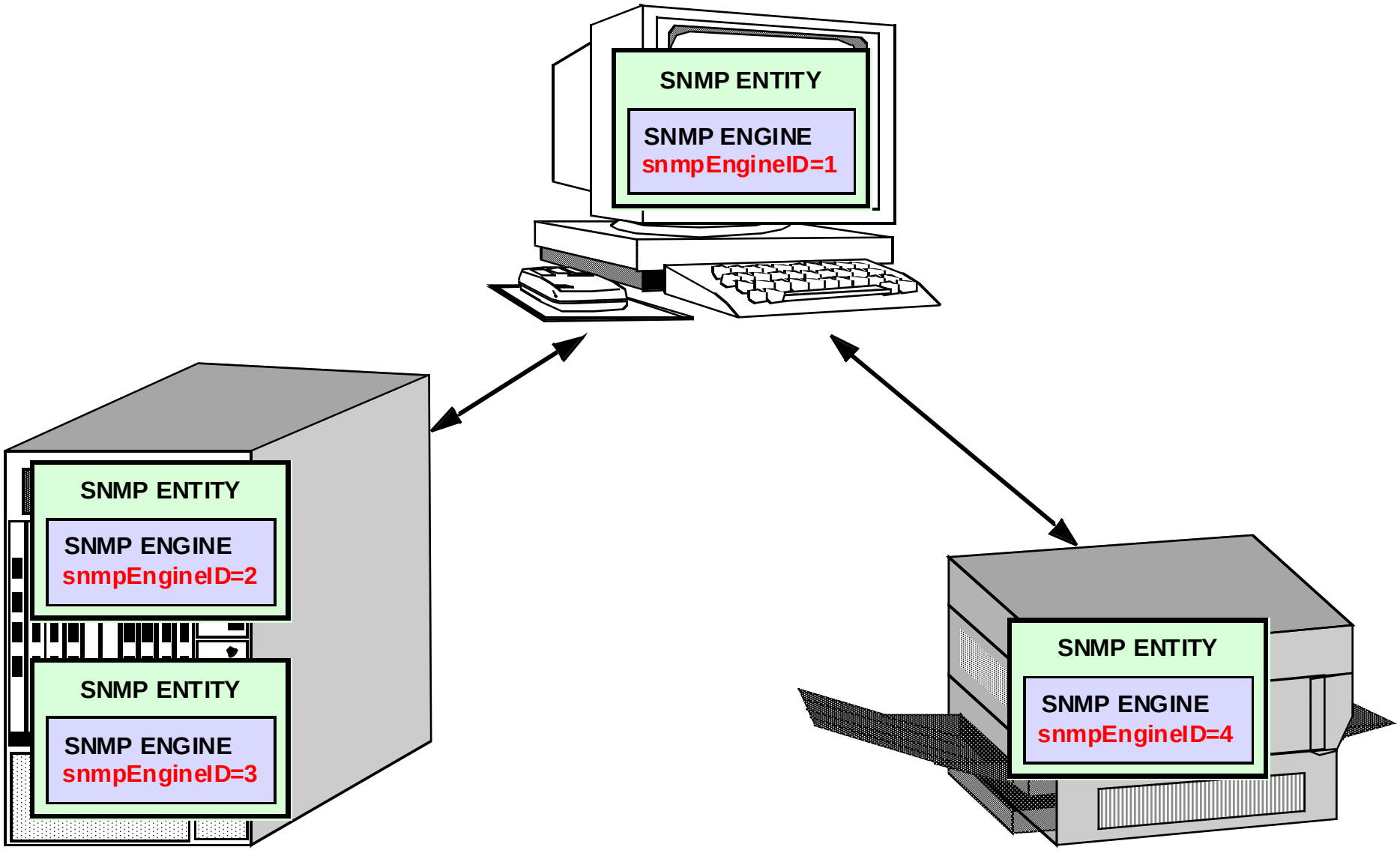


Simple Web

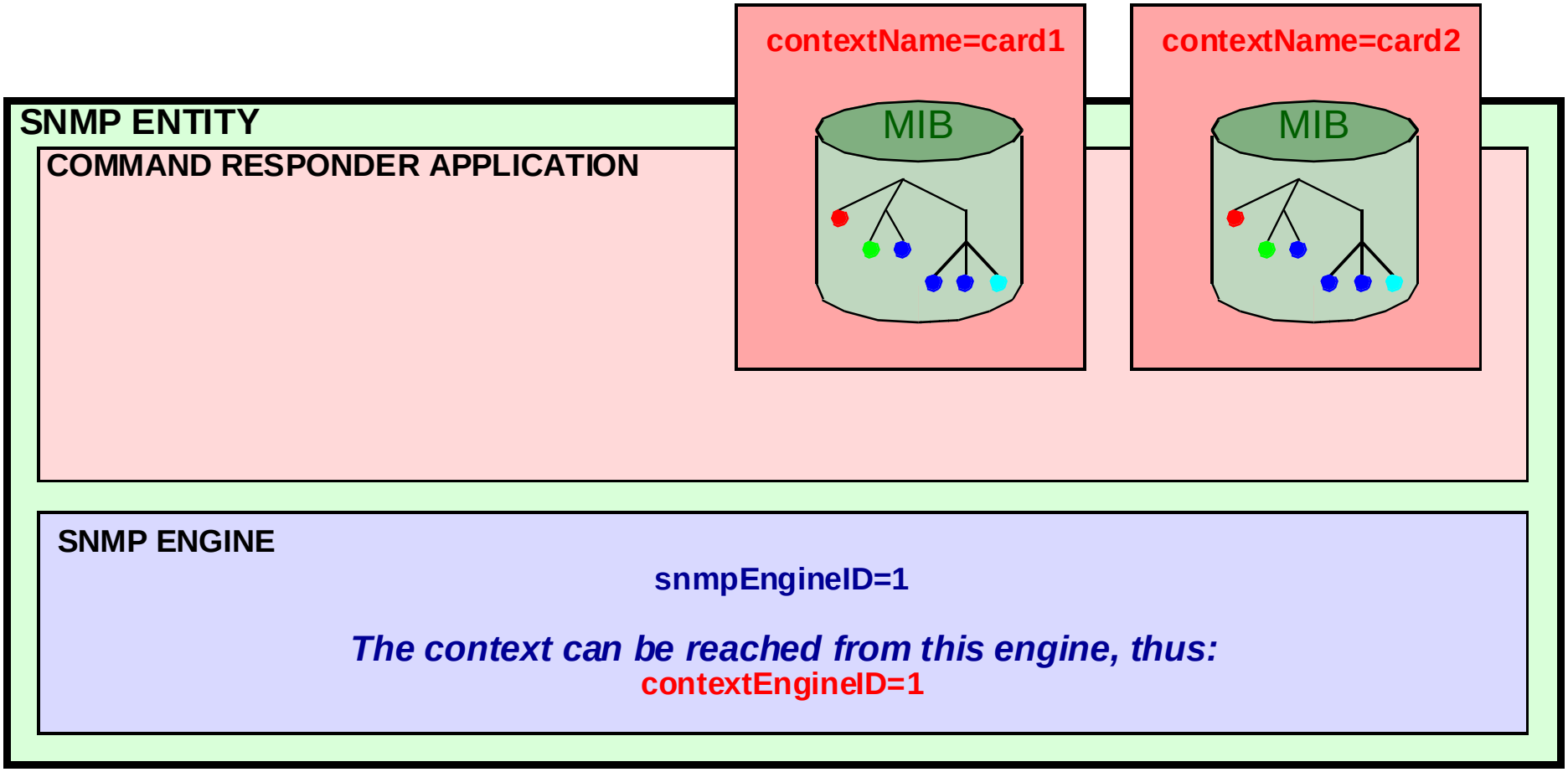
SNMPv3 ARCHITECTURE: AGENT



CONCEPTS: snmpEngineID

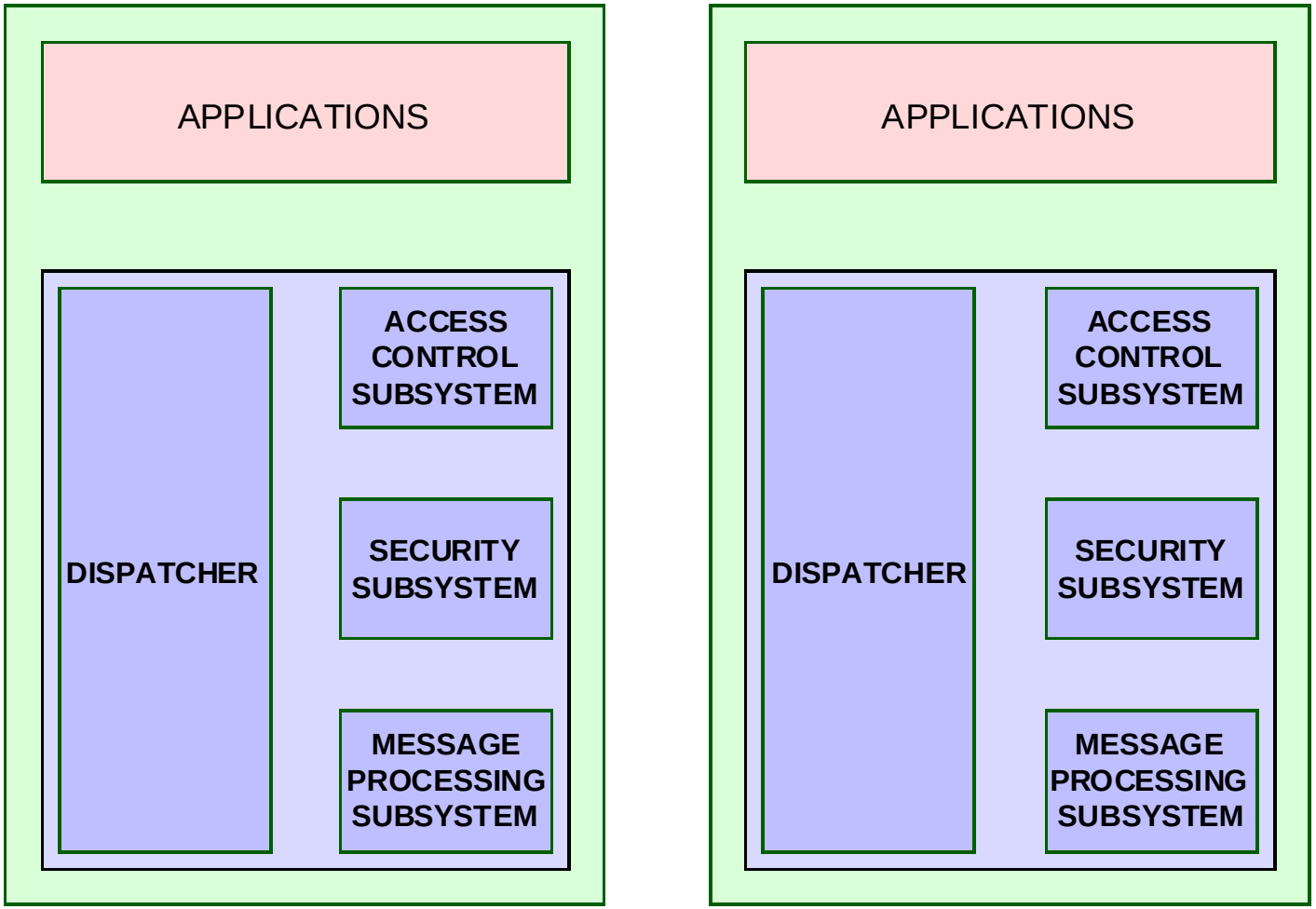


CONCEPTS: Context



Simple Web

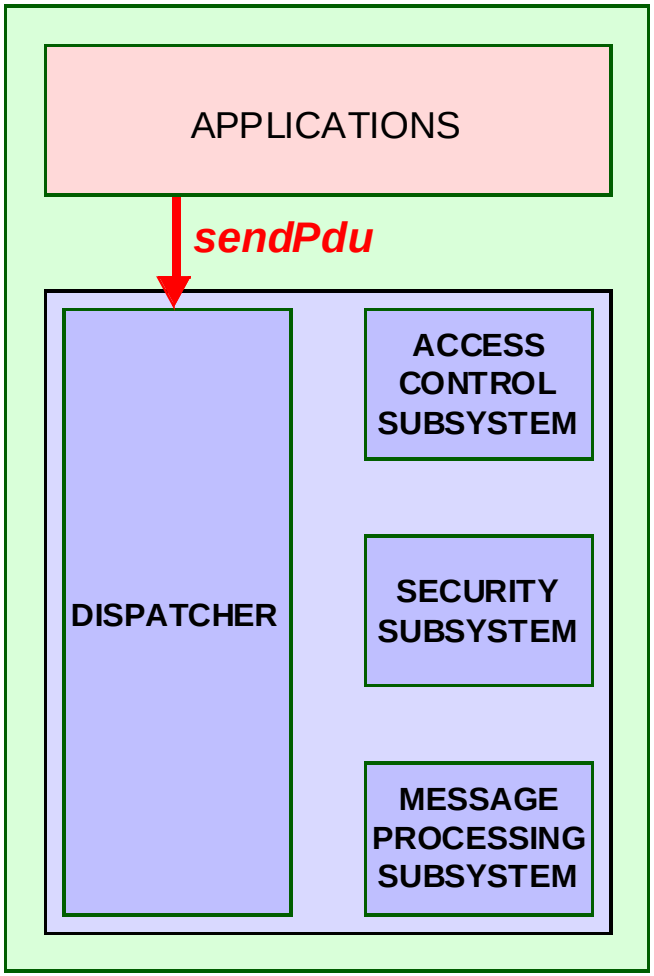
PRIMITIVES BETWEEN MODULES

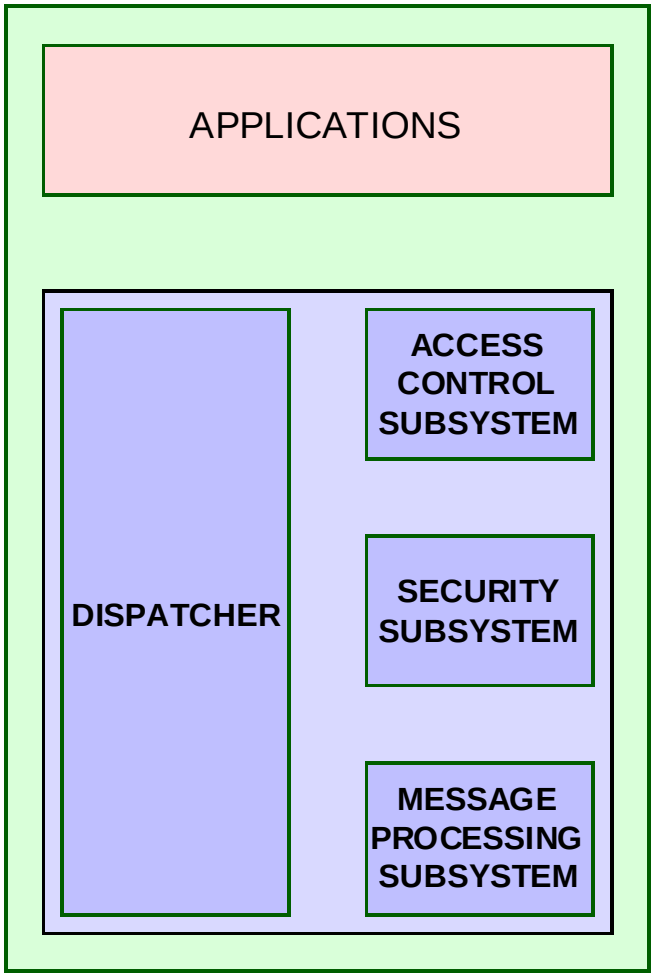


Parameters
contextEngineID
contextName
destTransportAddress
destTransportDomain
expectResponse
globalData
maxMessageSize
maxSizeResponseScopedPDU
messageProcessingModel
outgoingMessage
outgoingMessageLength
PDU
pduType
pduVersion
scopedPDU
stateReference
statusInformation
securityEngineID
securityLevel
securityModel
securityName
securityParameters
securityStateReference
sendPduHandle
transportAddress
transportDomain
variableName
viewType
wholeMsg
wholeMsgLength

Simple Web

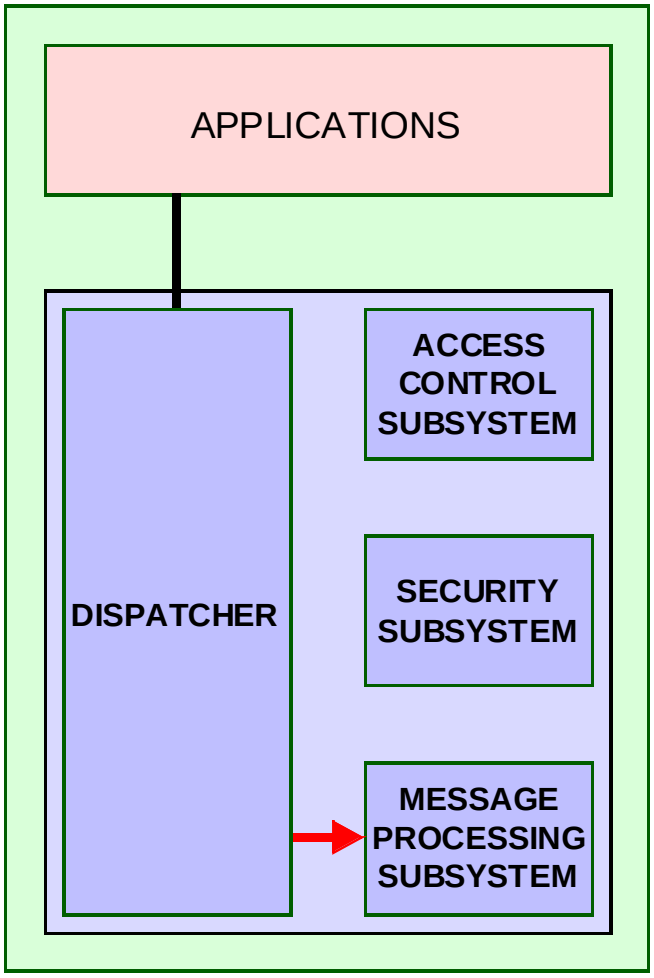
sendPdu



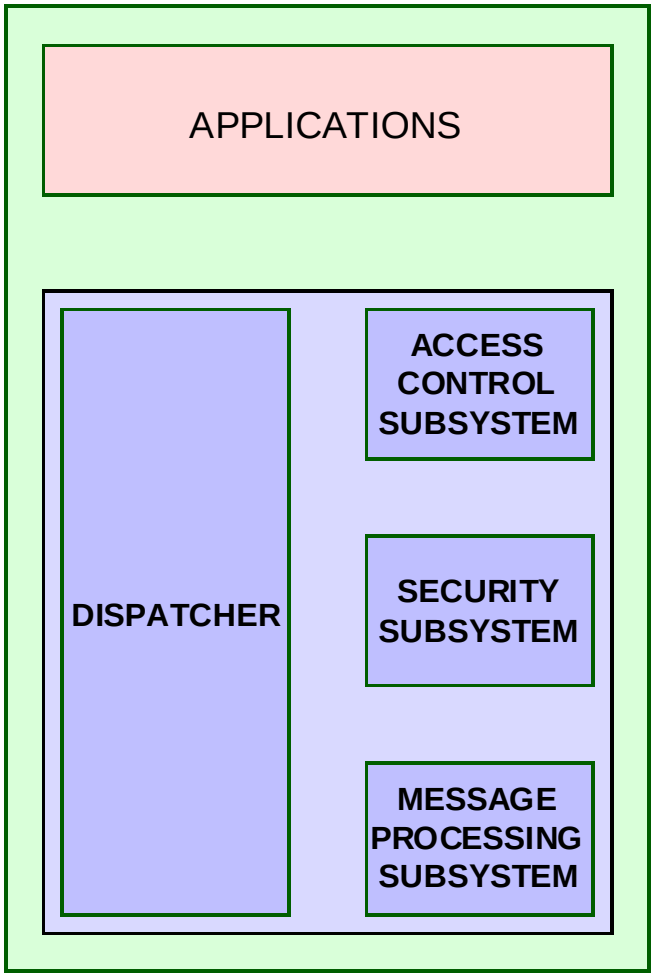


Parameters
contextEngineID
contextName
destTransportAddress
destTransportDomain
expectResponse
globalData
maxMessageSize
maxSizeResponseScopedPDU
messageProcessingModel
outgoingMessage
outgoingMessageLength
PDU
pduType
pduVersion
scopedPDU
stateReference
statusInformation
securityEngineID
securityLevel
securityModel
securityName
securityParameters
securityStateReference
sendPduHandle
transportAddress
transportDomain
variableName
viewType
wholeMsg
wholeMsgLength

prepareOutgoingMessage



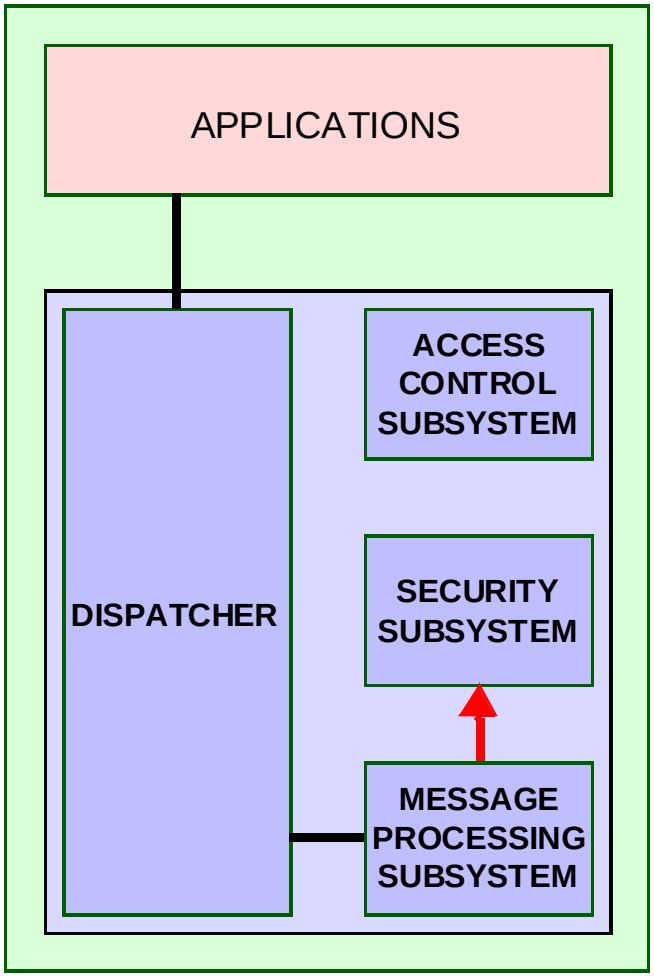
prepareOutgoingMessage

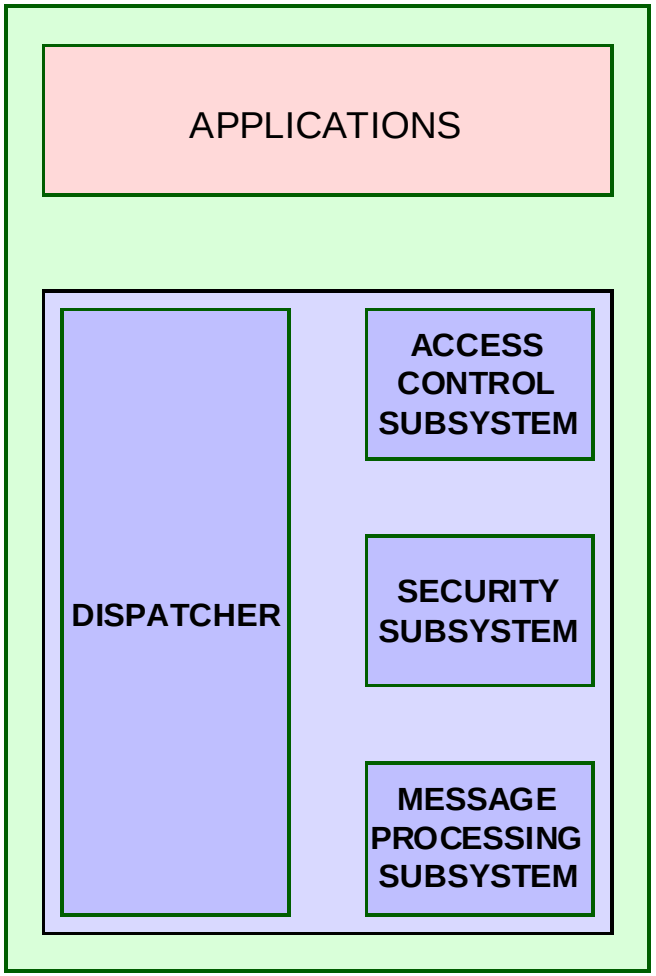


Parameters
contextEngineID
contextName
destTransportAddress
destTransportDomain
expectResponse
globalData
maxMessageSize
maxSizeResponseScopedPDU
messageProcessingModel
outgoingMessage
outgoingMessageLength
PDU
pduType
pduVersion
scopedPDU
stateReference
statusInformation
securityEngineID
securityLevel
securityModel
securityName
securityParameters
securityStateReference
sendPduHandle
transportAddress
transportDomain
variableName
viewType
wholeMsg
wholeMsgLength

Simple Web

generateRequestMsg



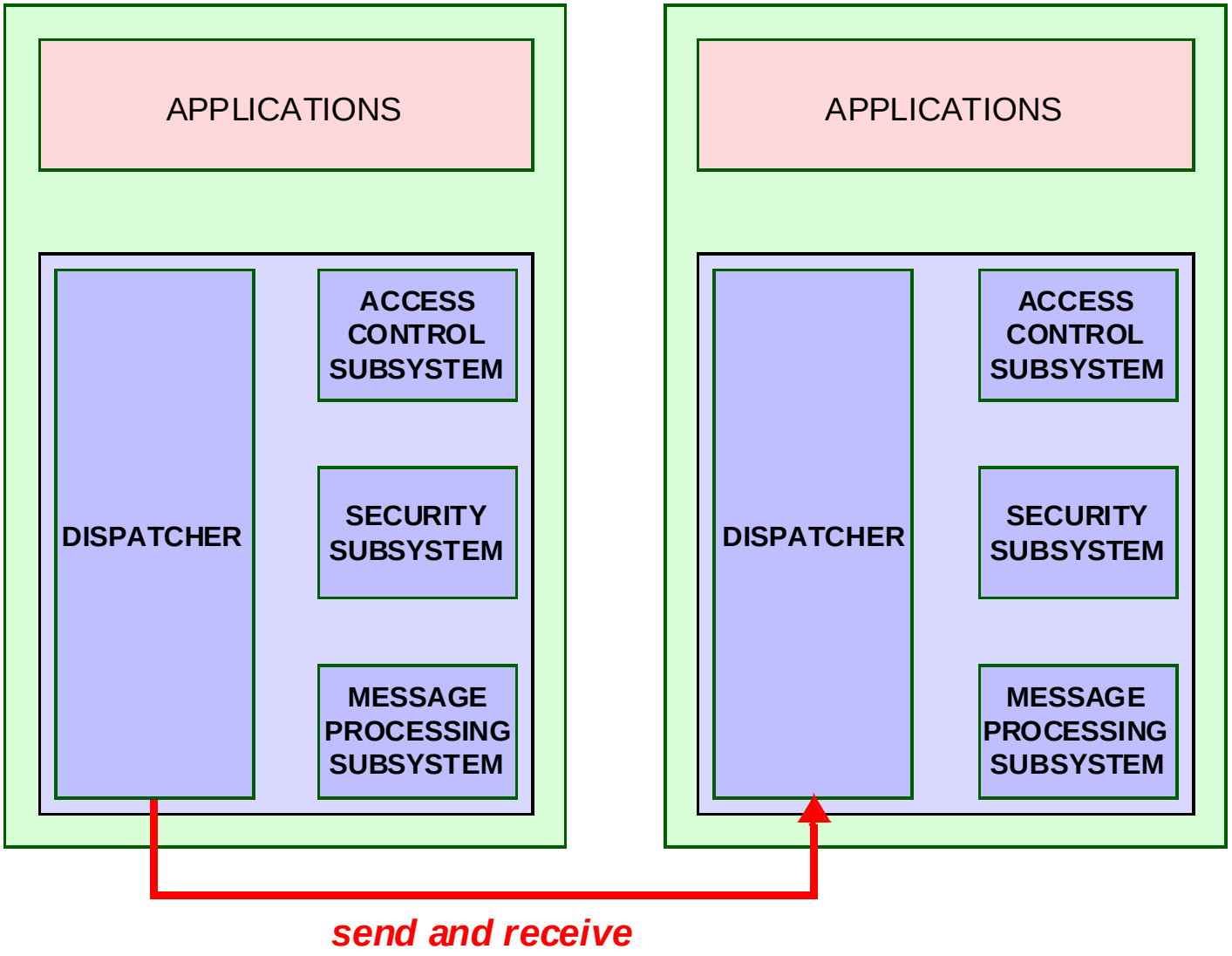


generateRequestMsg

Parameters
contextEngineID
contextName
destTransportAddress
destTransportDomain
expectResponse
globalData
maxMessageSize
maxSizeResponseScopedPDU
messageProcessingModel
outgoingMessage
outgoingMessageLength
PDU
pduType
pduVersion
scopedPDU
stateReference
statusInformation
securityEngineID
securityLevel
securityModel
securityName
securityParameters
securityStateReference
sendPduHandle
transportAddress
transportDomain
variableName
viewType
wholeMsg
wholeMsgLength

Simple Web

send / receive

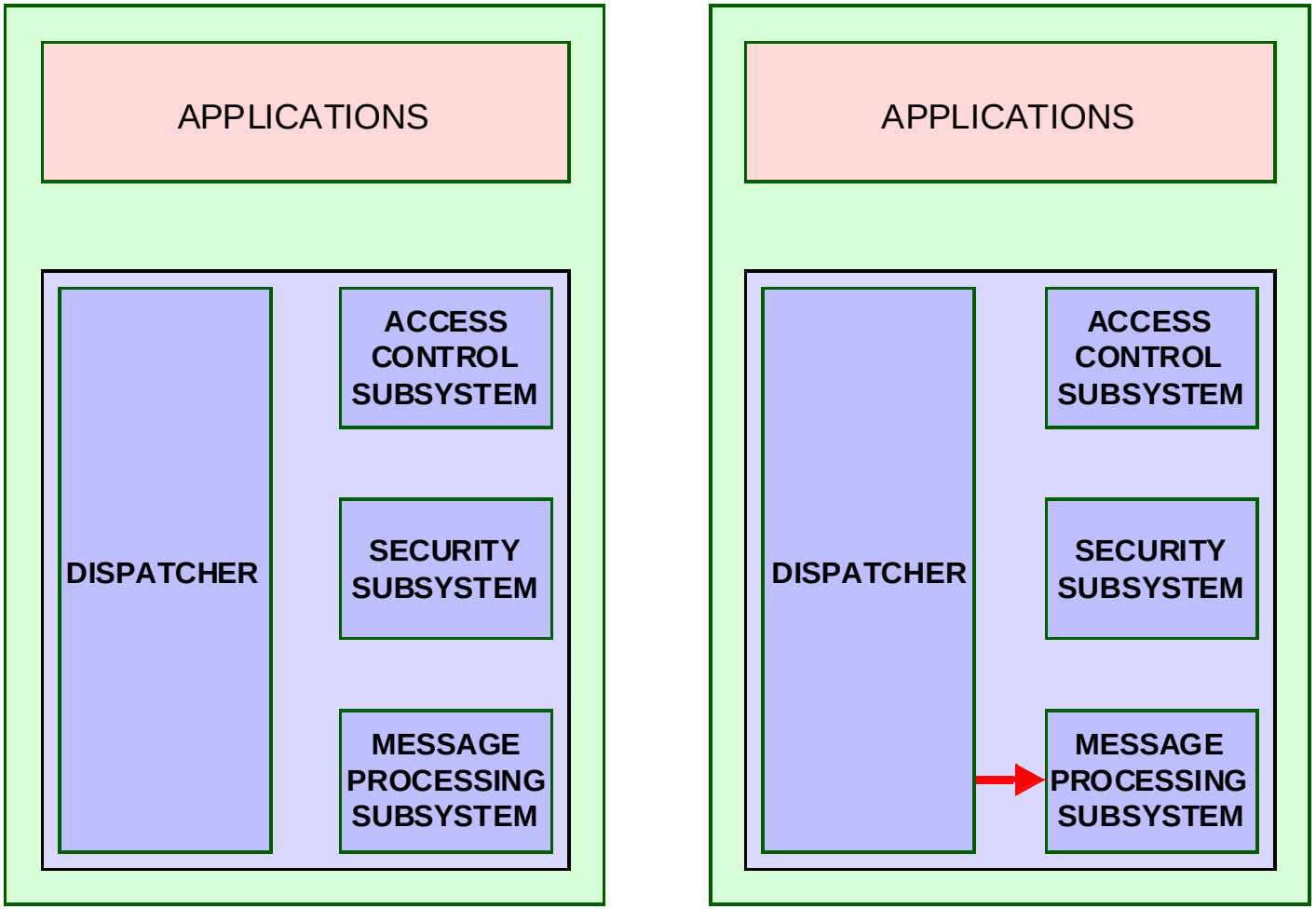


Parameters
contextEngineID
contextName
destTransportAddress
destTransportDomain
expectResponse
globalData
maxMessageSize
maxSizeResponseScopedPDU
messageProcessingModel
outgoingMessage
outgoingMessageLength
PDU
pduType
pduVersion
scopedPDU
stateReference
statusInformation
securityEngineID
securityLevel
securityModel
securityName
securityParameters
securityStateReference
sendPduHandle
transportAddress
transportDomain
variableName
viewType
wholeMsg
wholeMsgLength

BY : ENG. Maha Jeha

Simple Web

prepareDataElements

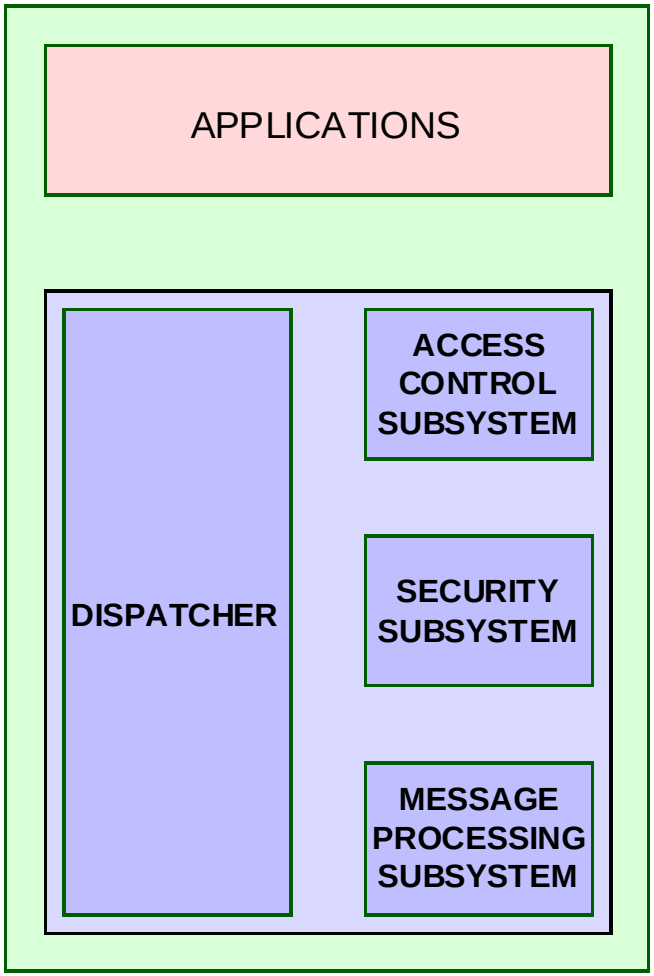


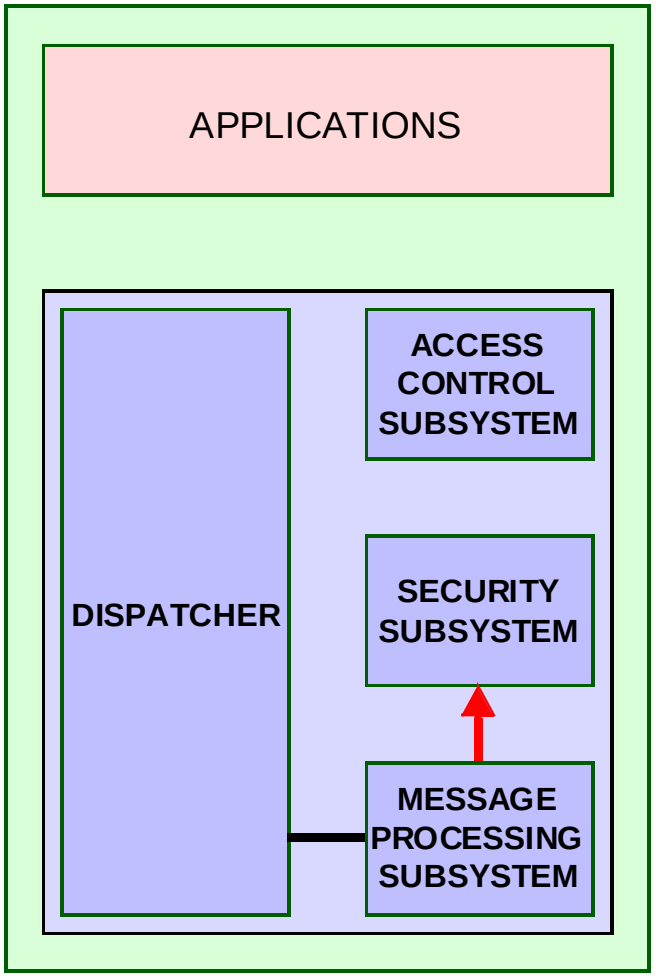
prepareDataElements

Parameters
contextEngineID
contextName
destTransportAddress
destTransportDomain
expectResponse
globalData
maxMessageSize
maxSizeResponseScopedPDU
messageProcessingModel
outgoingMessage
outgoingMessageLength
PDU
pduType
pduVersion
scopedPDU
stateReference
statusInformation
securityEngineID
securityLevel
securityModel
securityName
securityParameters
securityStateReference
sendPduHandle
transportAddress
transportDomain
variableName
viewType
wholeMsg
wholeMsgLength

Simple Web

processIncomingMsg



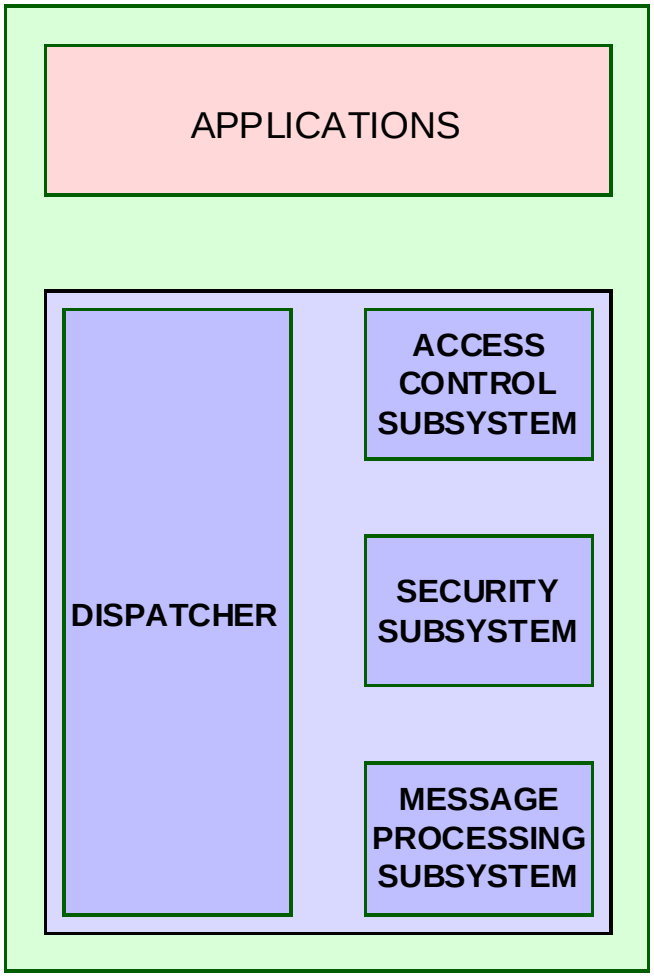


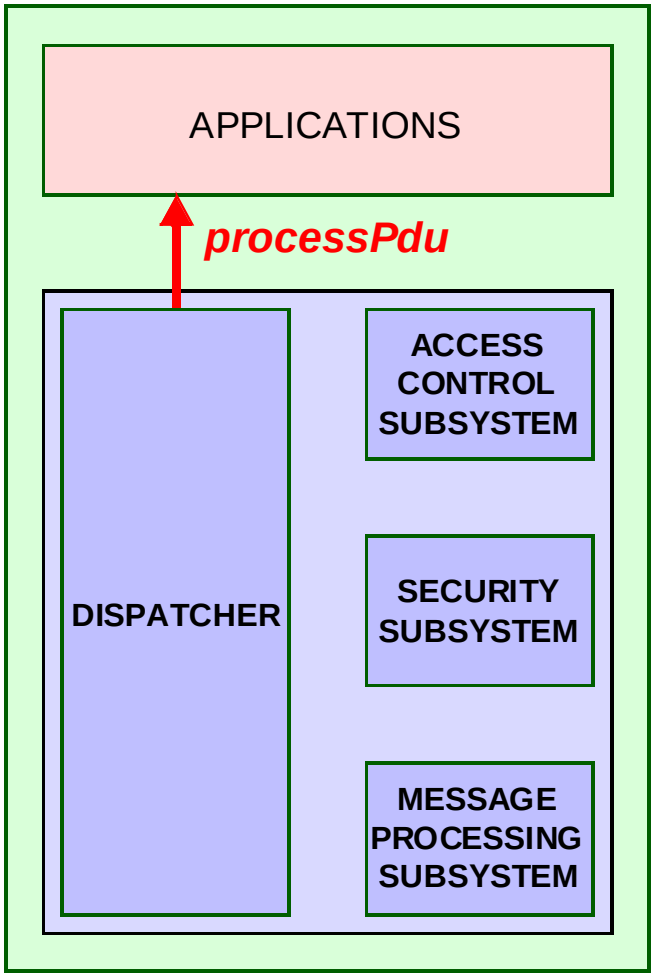
processIncomingMsg

Parameters
contextEngineID
contextName
destTransportAddress
destTransportDomain
expectResponse
globalData
maxMessageSize
maxSizeResponseScopedPDU
messageProcessingModel
outgoingMessage
outgoingMessageLength
PDU
pduType
pduVersion
scopedPDU
stateReference
statusInformation
securityEngineID
securityLevel
securityModel
securityName
securityParameters
securityStateReference
sendPduHandle
transportAddress
transportDomain
variableName
viewType
wholeMsg
wholeMsgLength

Simple Web

processPd

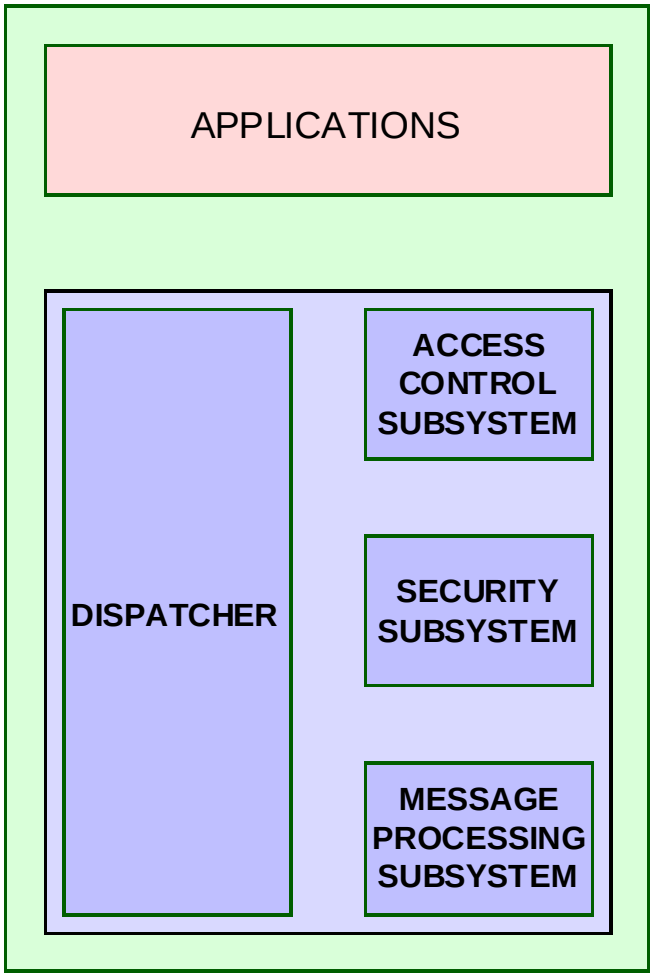


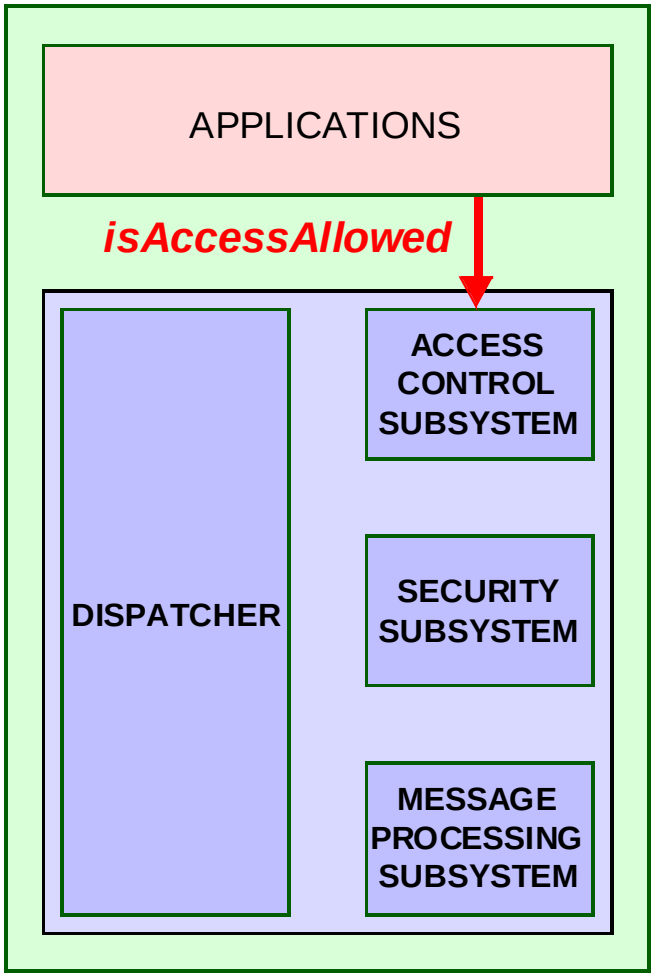


Parameters
contextEngineID
contextName
destTransportAddress
destTransportDomain
expectResponse
globalData
maxMessageSize
maxSizeResponseScopedPDU
messageProcessingModel
outgoingMessage
outgoingMessageLength
PDU
pduType
pduVersion
scopedPDU
stateReference
statusInformation
securityEngineID
securityLevel
securityModel
securityName
securityParameters
securityStateReference
sendPduHandle
transportAddress
transportDomain
variableName
viewType
wholeMsg
wholeMsgLength

Simple Web

isAccessAllowed

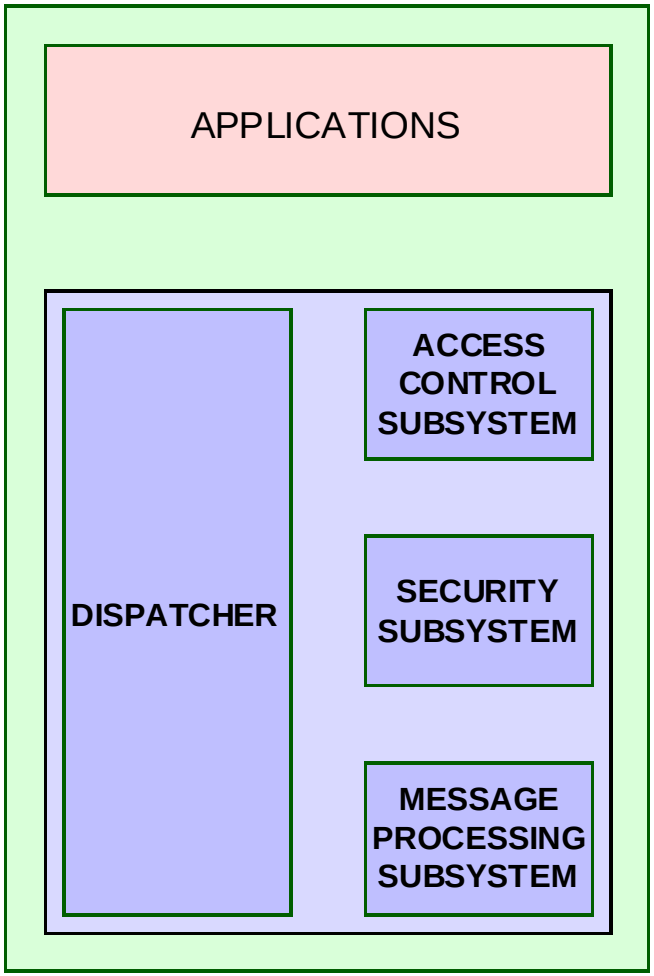


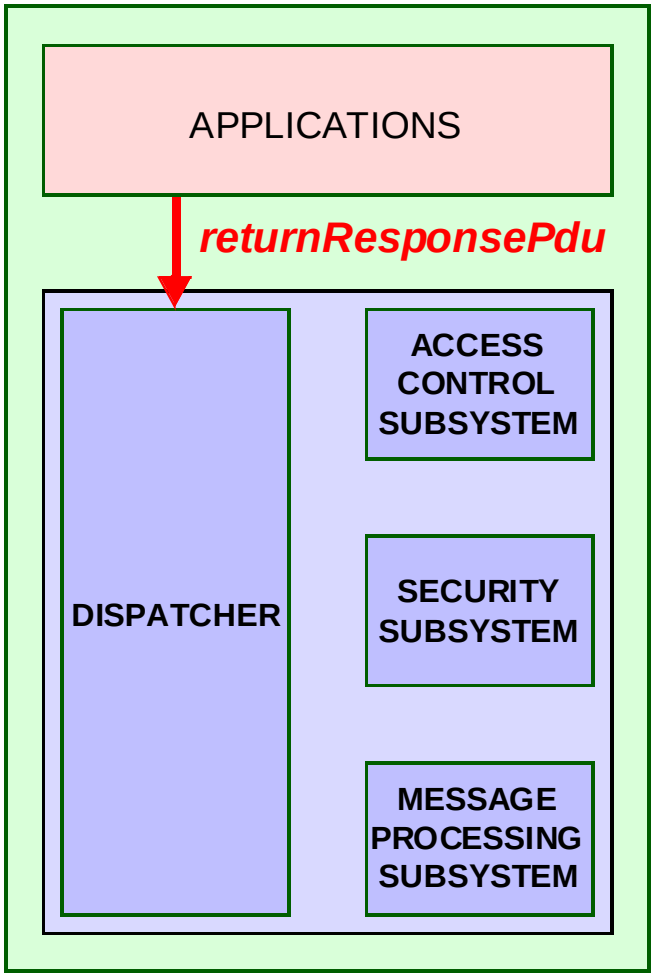


Parameters
contextEngineID
contextName
destTransportAddress
destTransportDomain
expectResponse
globalData
maxMessageSize
maxSizeResponseScopedPDU
messageProcessingModel
outgoingMessage
outgoingMessageLength
PDU
pduType
pduVersion
scopedPDU
stateReference
statusInformation
securityEngineID
securityLevel
securityModel
securityName
securityParameters
securityStateReference
sendPduHandle
transportAddress
transportDomain
variableName
viewType
wholeMsg
wholeMsgLength

Simple Web

returnResponsePdu

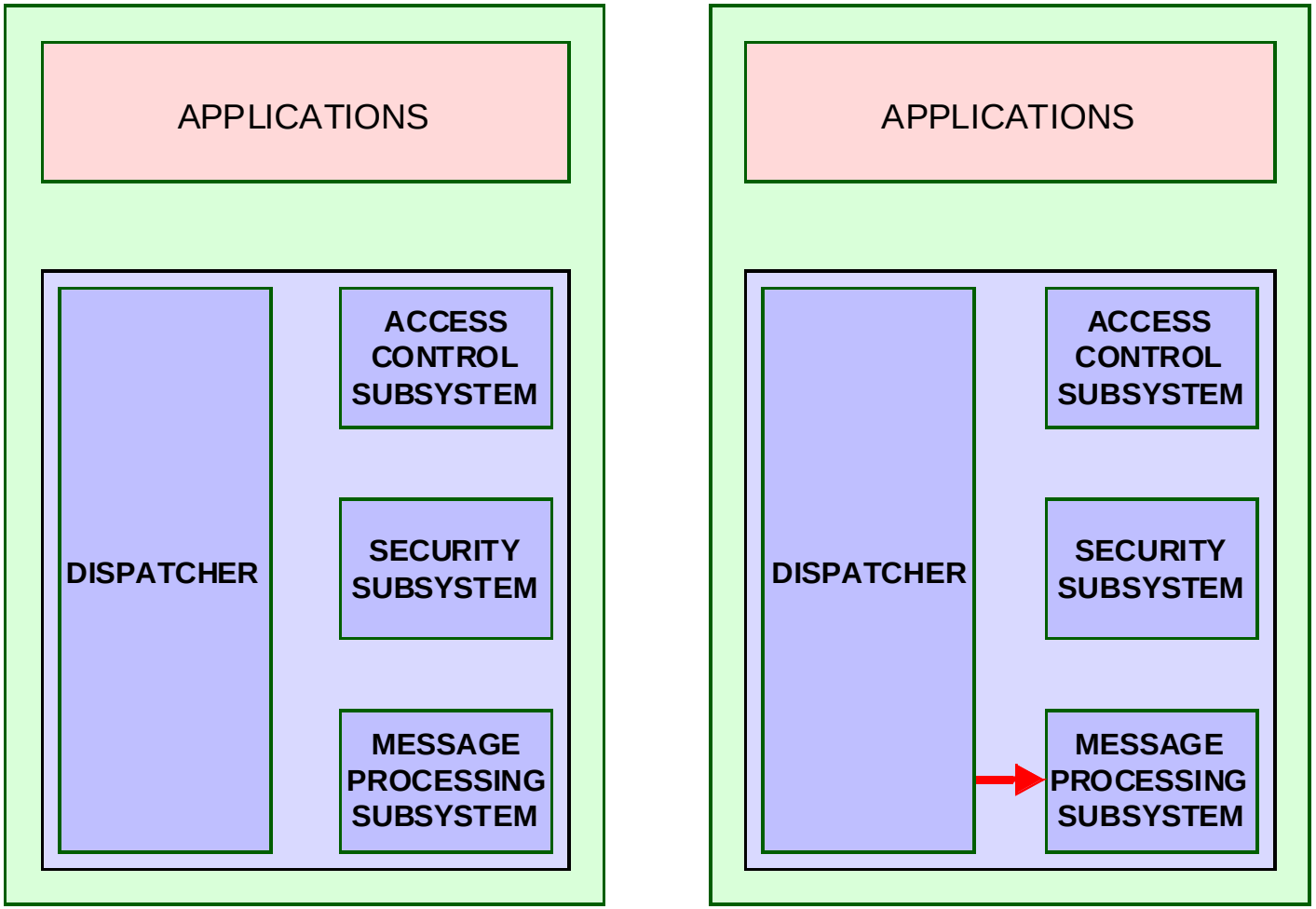




Parameters
contextEngineID
contextName
destTransportAddress
destTransportDomain
expectResponse
globalData
maxMessageSize
maxSizeResponseScopedPDU
messageProcessingModel
outgoingMessage
outgoingMessageLength
PDU
pduType
pduVersion
scopedPDU
stateReference
statusInformation
securityEngineID
securityLevel
securityModel
securityName
securityParameters
securityStateReference
sendPduHandle
transportAddress
transportDomain
variableName
viewType
wholeMsg
wholeMsgLength

Simple Web

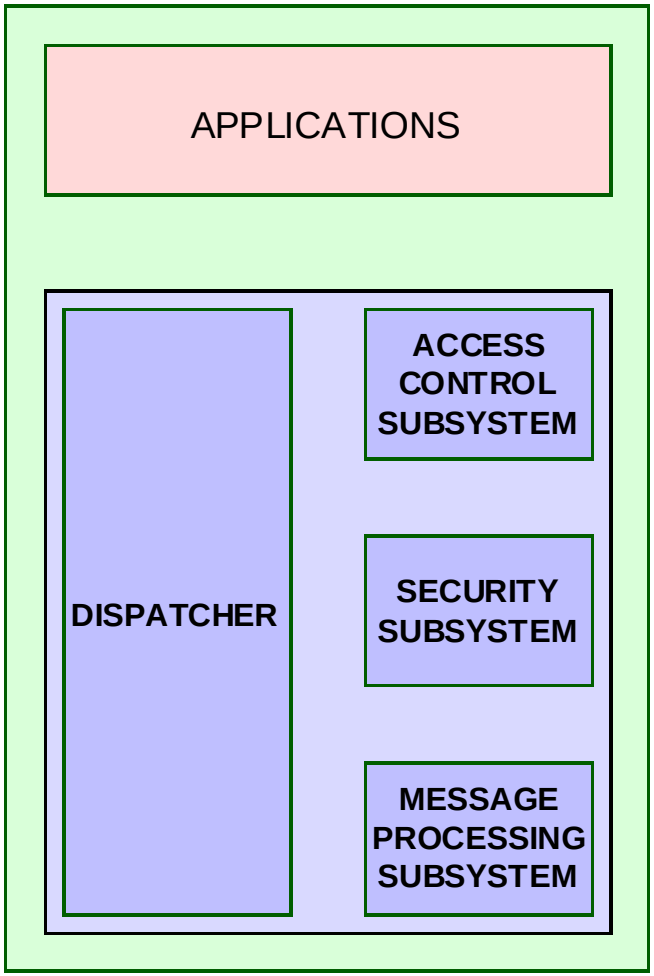
prepareResponseMessage

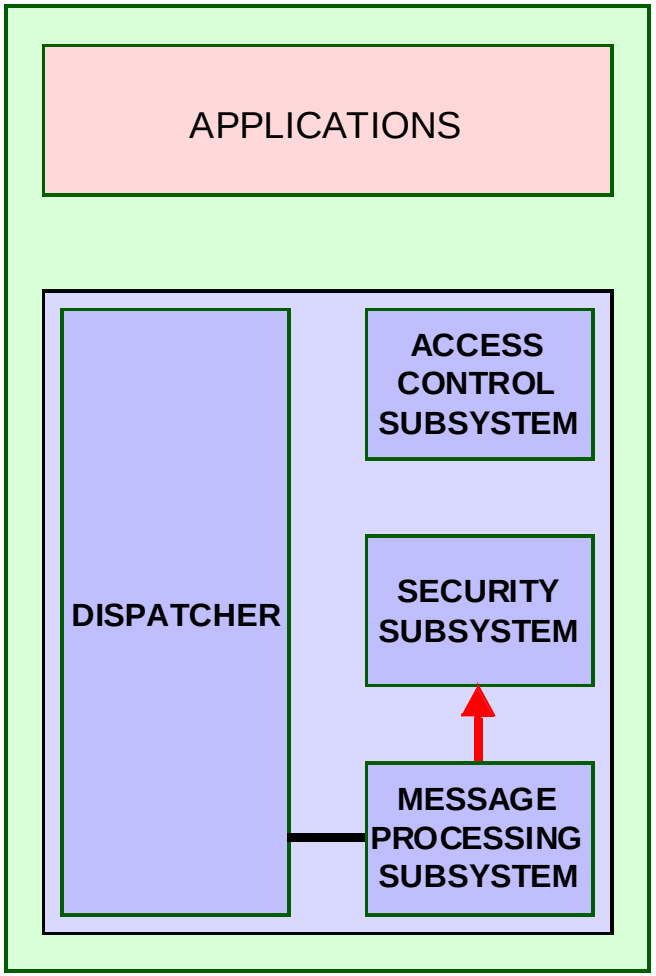


prepareResponseMessage

Parameters
contextEngineID
contextName
destTransportAddress
destTransportDomain
expectResponse
globalData
maxMessageSize
maxSizeResponseScopedPDU
messageProcessingModel
outgoingMessage
outgoingMessageLength
PDU
pduType
pduVersion
scopedPDU
stateReference
statusInformation
securityEngineID
securityLevel
securityModel
securityName
securityParameters
securityStateReference
sendPduHandle
transportAddress
transportDomain
variableName
viewType
wholeMsg
wholeMsgLength

generateResponseMsg



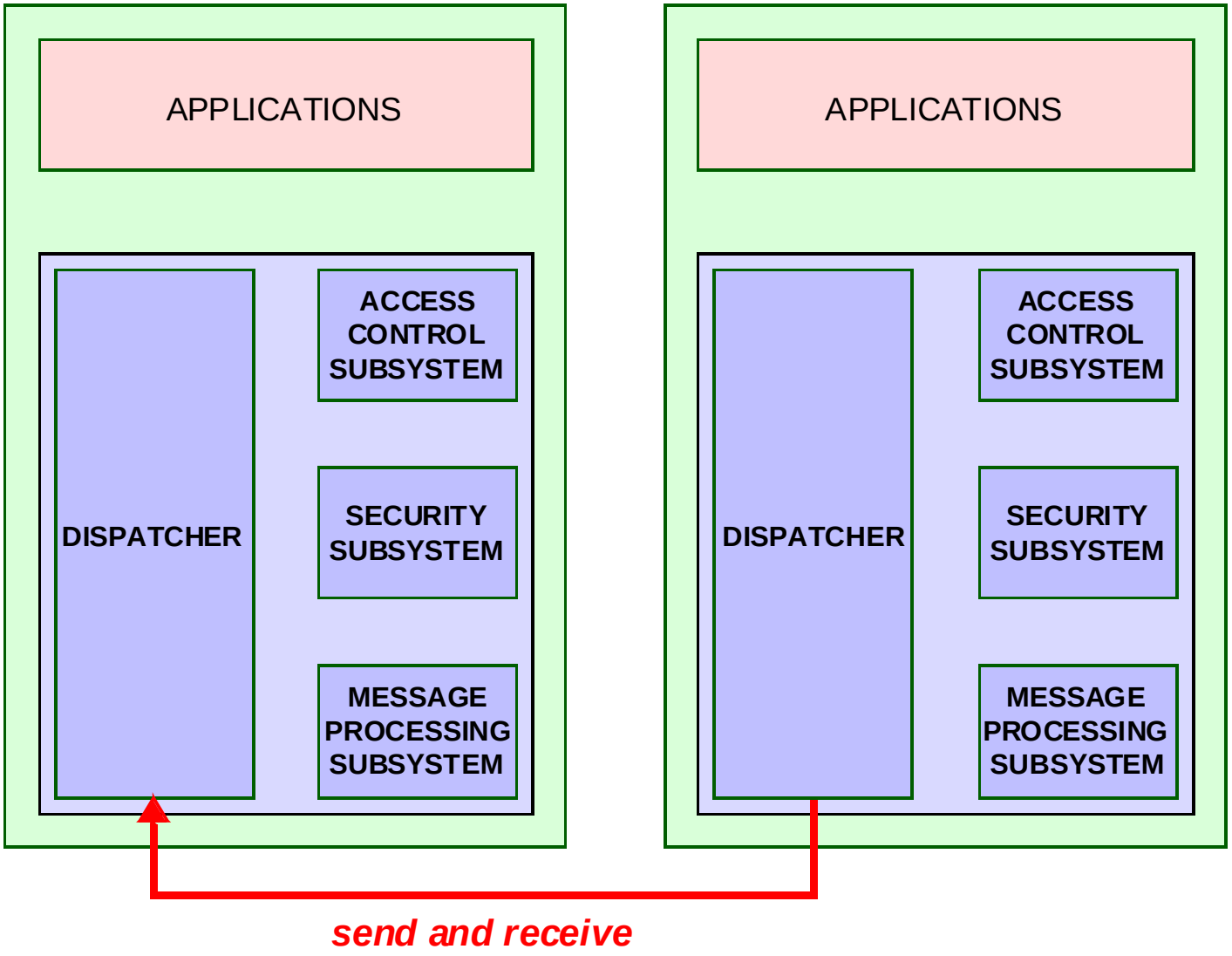


generateResponseMsg

Parameters
contextEngineID
contextName
destTransportAddress
destTransportDomain
expectResponse
globalData
maxMessageSize
maxSizeResponseScopedPDU
messageProcessingModel
outgoingMessage
outgoingMessageLength
PDU
pduType
pduVersion
scopedPDU
stateReference
statusInformation
securityEngineID
securityLevel
securityModel
securityName
securityParameters
securityStateReference
sendPduHandle
transportAddress
transportDomain
variableName
viewType
wholeMsg
wholeMsgLength

Simple Web

send / receive

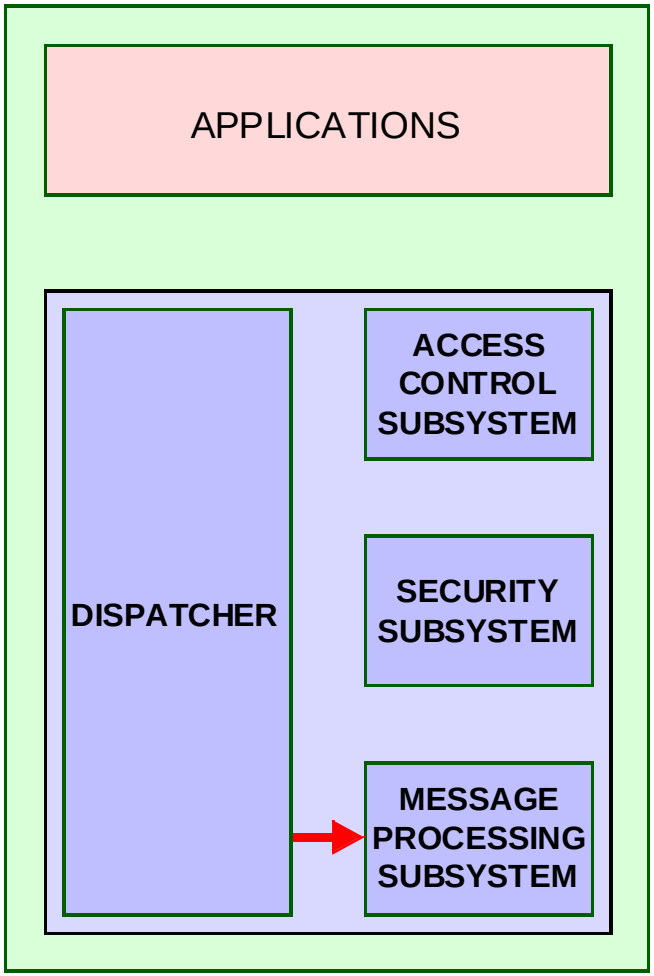


Parameters
contextEngineID
contextName
destTransportAddress
destTransportDomain
expectResponse
globalData
maxMessageSize
maxSizeResponseScopedPDU
messageProcessingModel
outgoingMessage
outgoingMessageLength
PDU
pduType
pduVersion
scopedPDU
stateReference
statusInformation
securityEngineID
securityLevel
securityModel
securityName
securityParameters
securityStateReference
sendPduHandle
transportAddress
transportDomain
variableName
viewType
wholeMsg
wholeMsgLength

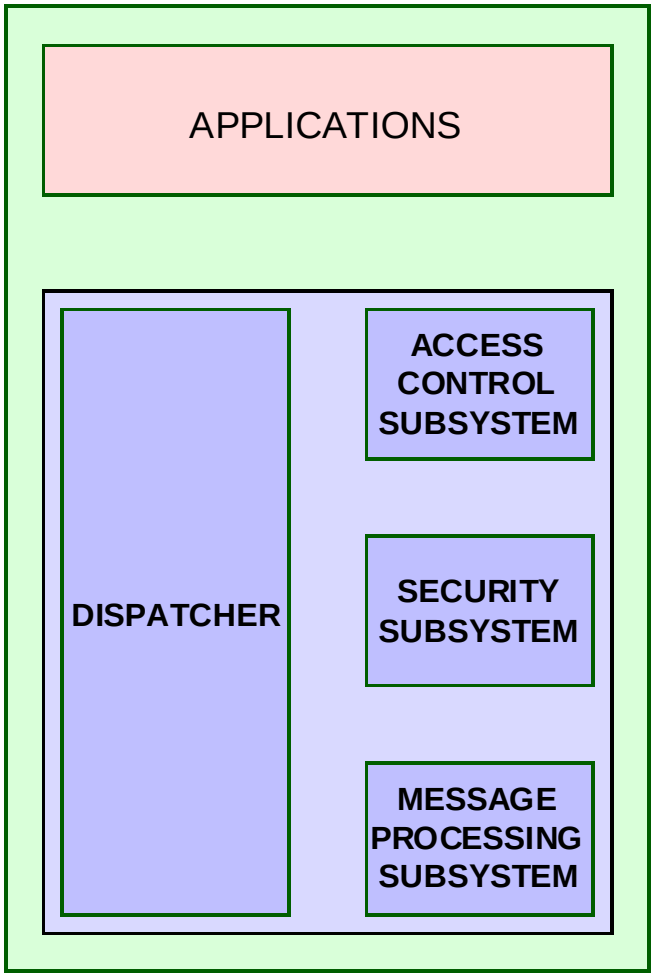
BY : ENG. Maha Jeha

Simple Web

prepareDataElements



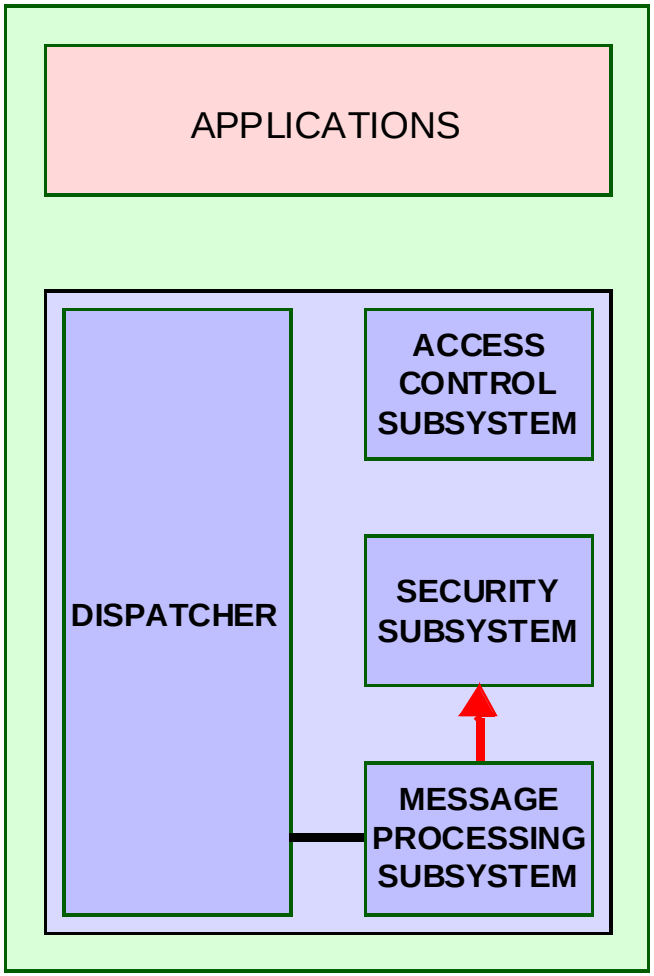
prepareDataElements

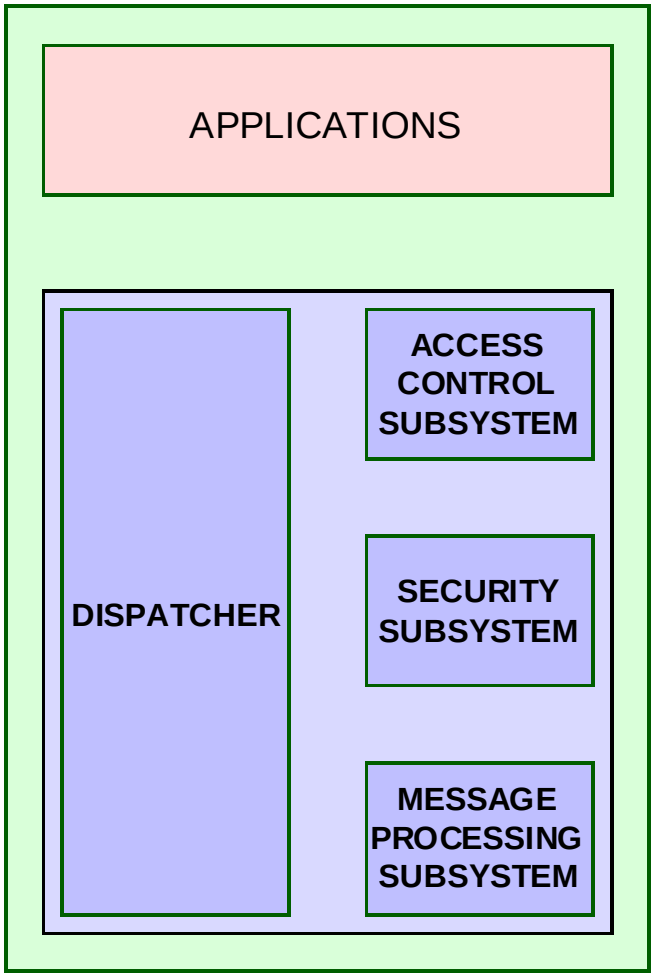


Parameters
contextEngineID
contextName
destTransportAddress
destTransportDomain
expectResponse
globalData
maxMessageSize
maxSizeResponseScopedPDU
messageProcessingModel
outgoingMessage
outgoingMessageLength
PDU
pduType
pduVersion
scopedPDU
stateReference
statusInformation
securityEngineID
securityLevel
securityModel
securityName
securityParameters
securityStateReference
sendPduHandle
transportAddress
transportDomain
variableName
viewType
wholeMsg
wholeMsgLength

Simple Web

processIncomingMsg



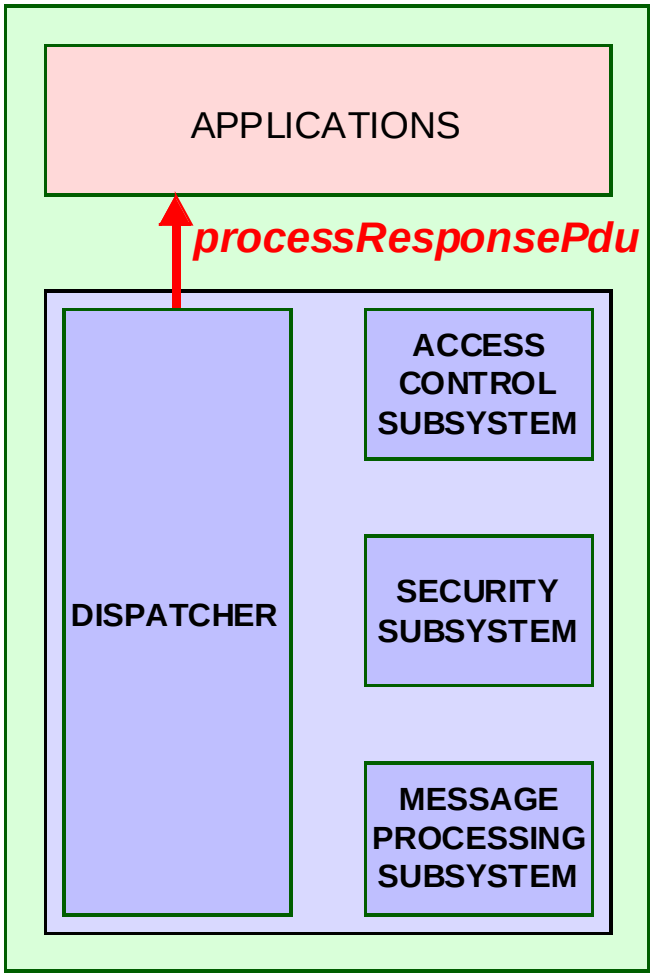


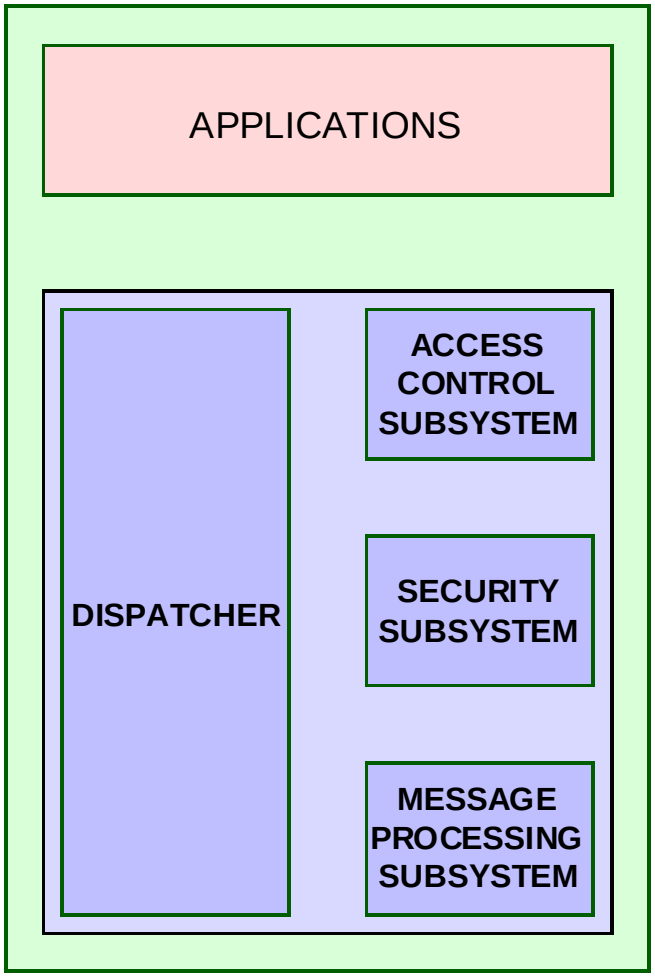
processIncomingMsg

Parameters
contextEngineID
contextName
destTransportAddress
destTransportDomain
expectResponse
globalData
maxMessageSize
maxSizeResponseScopedPDU
messageProcessingModel
outgoingMessage
outgoingMessageLength
PDU
pduType
pduVersion
scopedPDU
stateReference
statusInformation
securityEngineID
securityLevel
securityModel
securityName
securityParameters
securityStateReference
sendPduHandle
transportAddress
transportDomain
variableName
viewType
wholeMsg
wholeMsgLength

Simple Web

processResponsePdu





Parameters
contextEngineID
contextName
destTransportAddress
destTransportDomain
expectResponse
globalData
maxMessageSize
maxSizeResponseScopedPDU
messageProcessingModel
outgoingMessage
outgoingMessageLength
PDU
pduType
pduVersion
scopedPDU
stateReference
statusInformation
securityEngineID
securityLevel
securityModel
securityName
securityParameters
securityStateReference
sendPduHandle
transportAddress
transportDomain
variableName
viewType
wholeMsg
wholeMsgLength

MODULES OF THE SNMPv3 ARCHITECTURE

DISPATCHER AND MESSAGE PROCESSING MODULE

- SNMPv3 MESSAGE STRUCTURE
- snmpMPDMIB
- RFC 2572

APPLICATIONS

- snmpTargetMIB
- snmpNotificationMIB
- snmpProxyMIB
- RFC 2573

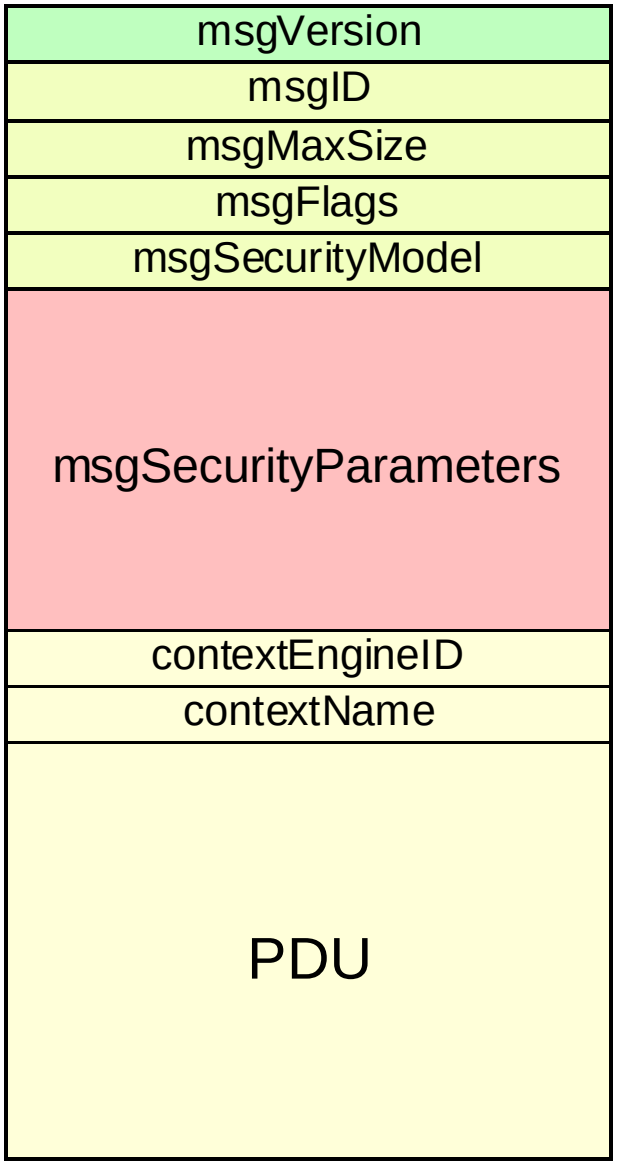
SECURITY SUBSYSTEM

- USER BASED SECURITY MODEL
- snmpUsmMIB
- RFC 2574

ACCESS CONTROL SUBSYSTEM

- VIEW BASED ACCESS CONTROL MODEL
- snmpVacmMIB
- RFC 2575

SNMPv3 MESSAGE STRUCTURE



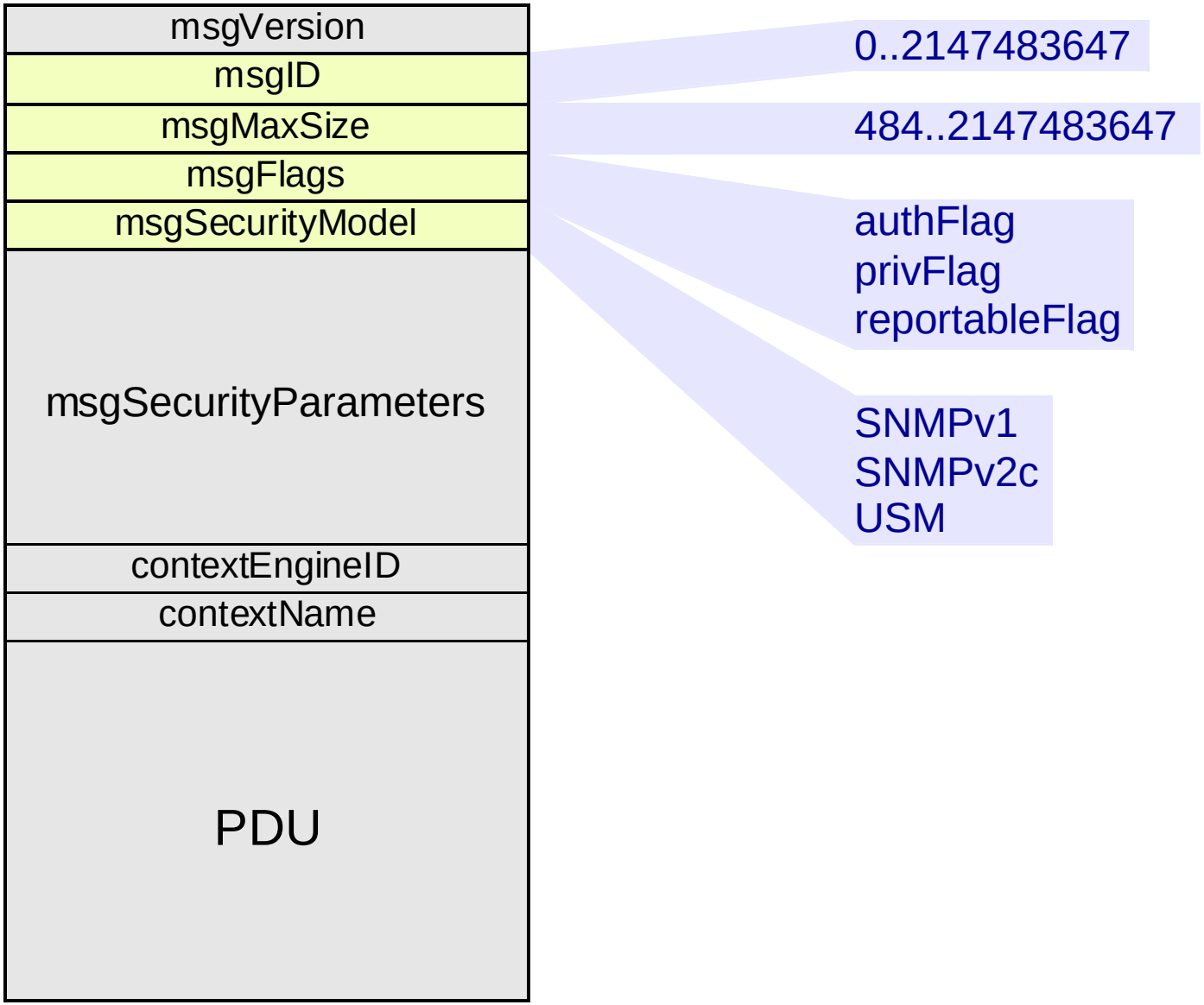
USED BY MESSAGE PROCESSING SUBSYSTEM

USED BY SNMPv3 PROCESSING MODULE

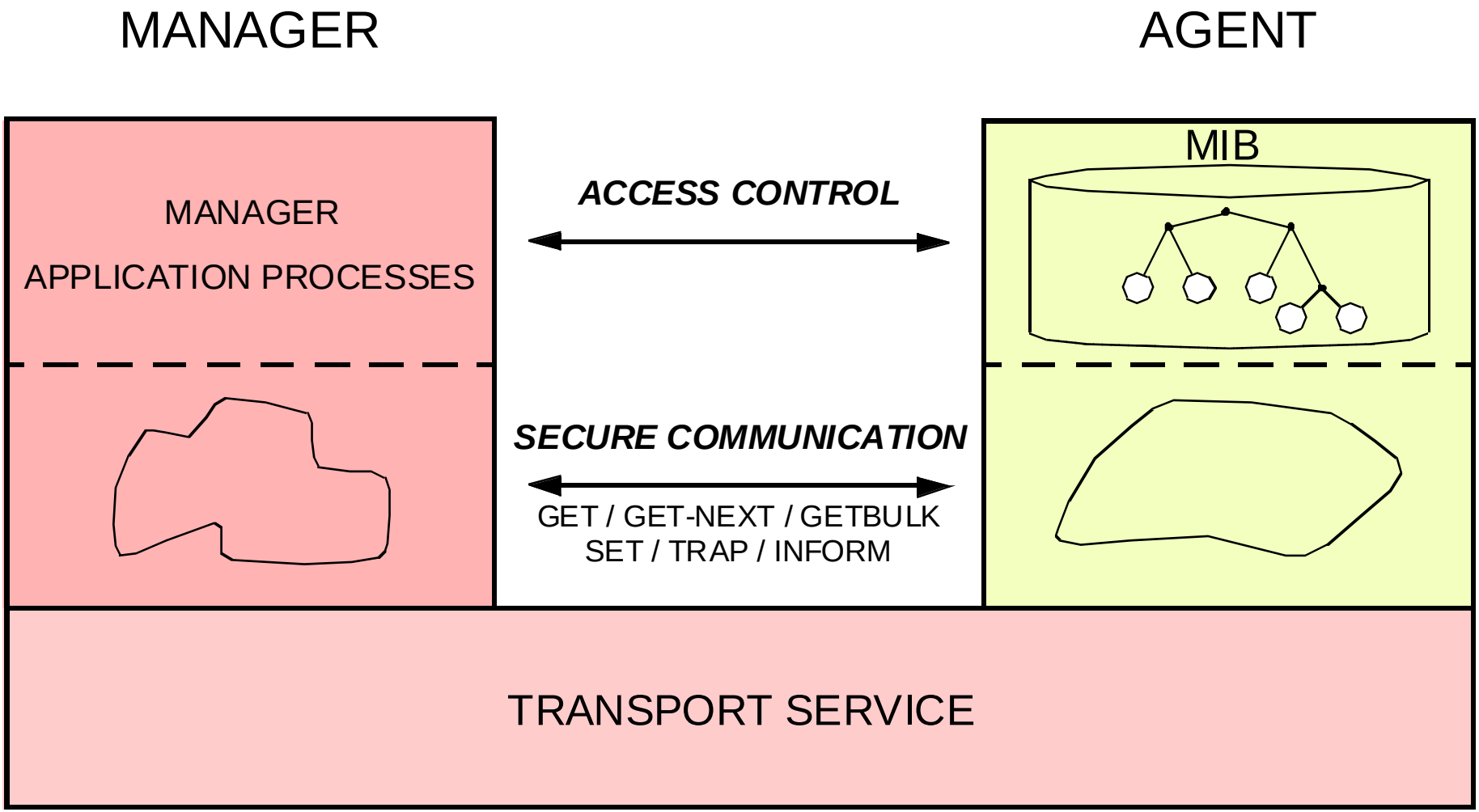
USED BY SECURITY SUBSYSTEM

USED BY ACCESS CONTROL SUBSYSTEM AND APPLICATIONS

SNMPv3 PROCESSING MODULE PARAMETERS



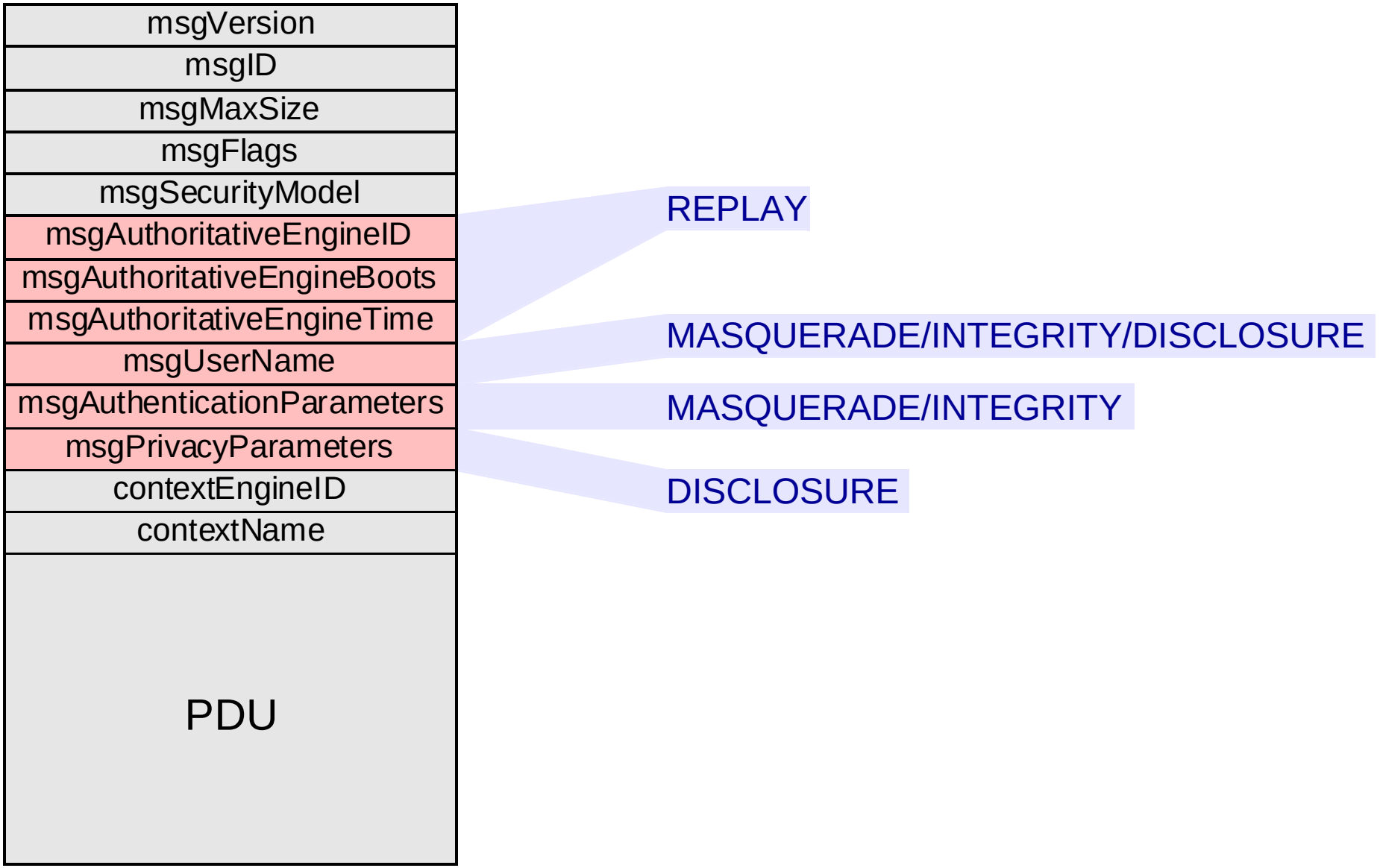
SECURE COMMUNICATION VERSUS ACCESS CONTROL



USM: SECURITY THREATS

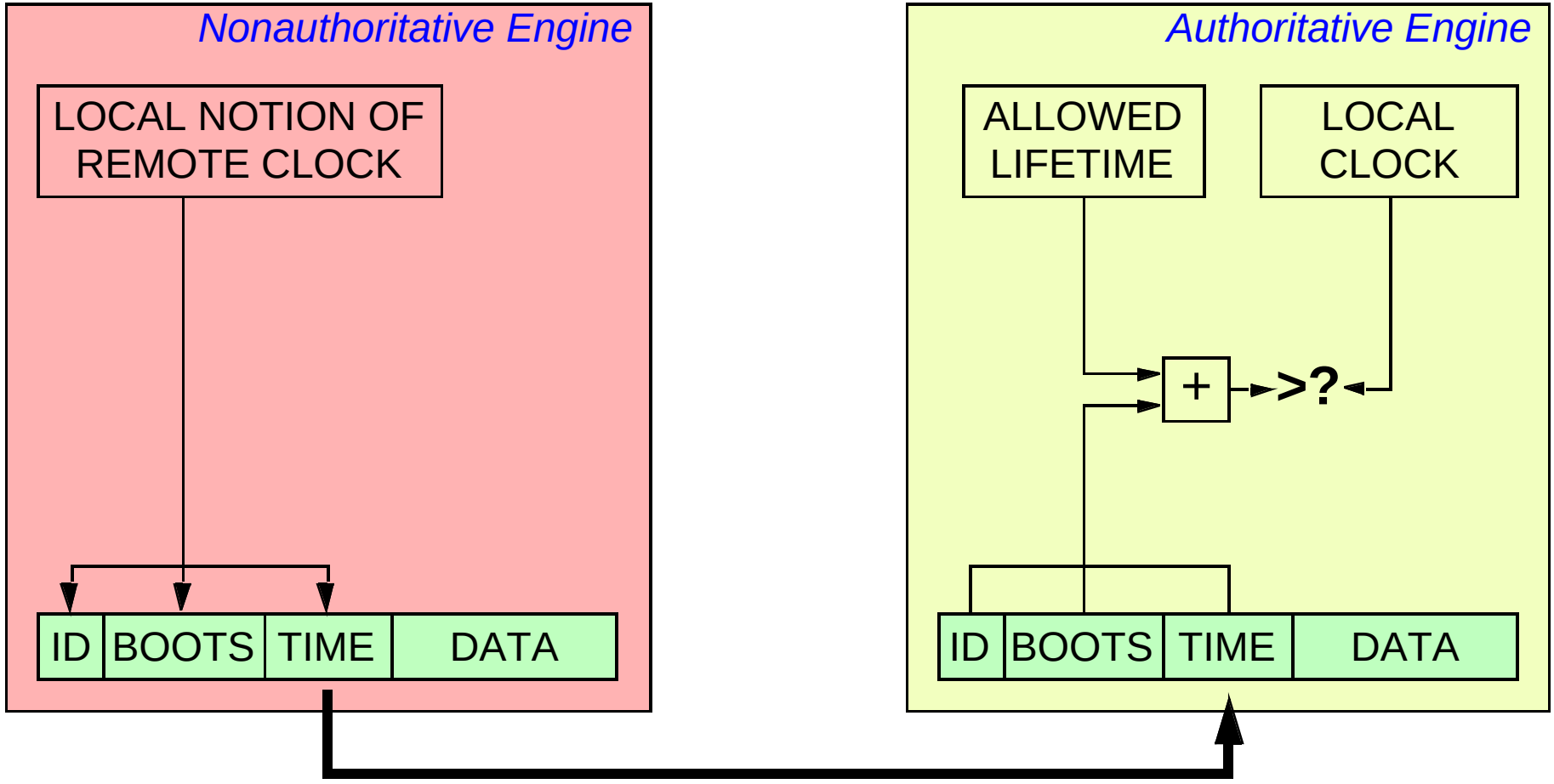
THREAT	ADDRESSED?	MECHANISM
REPLAY	YES	TIME STAMP
MASQUERADE	YES	MD5 / SHA-1
INTEGRITY	YES	(MD5 / SHA-1)
DISCLOSURE	YES	DES
DENIAL OF SERVICE	YES	
TRAFFIC ANALYSIS	YES	

USM MESSAGE STRUCTURE

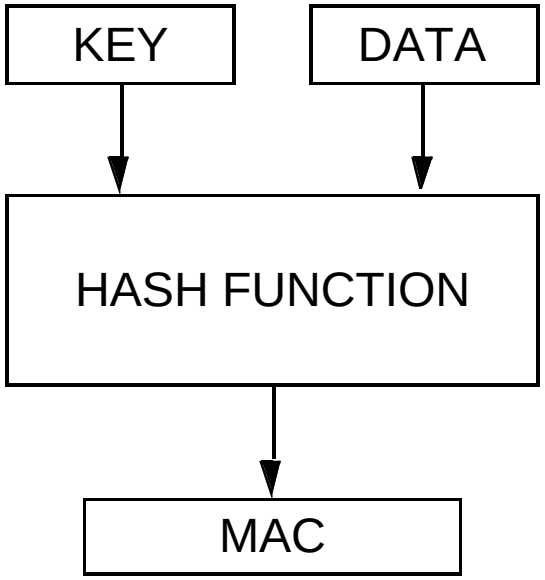


Simple Web

IDEA BEHIND REPLAY PROTECTION



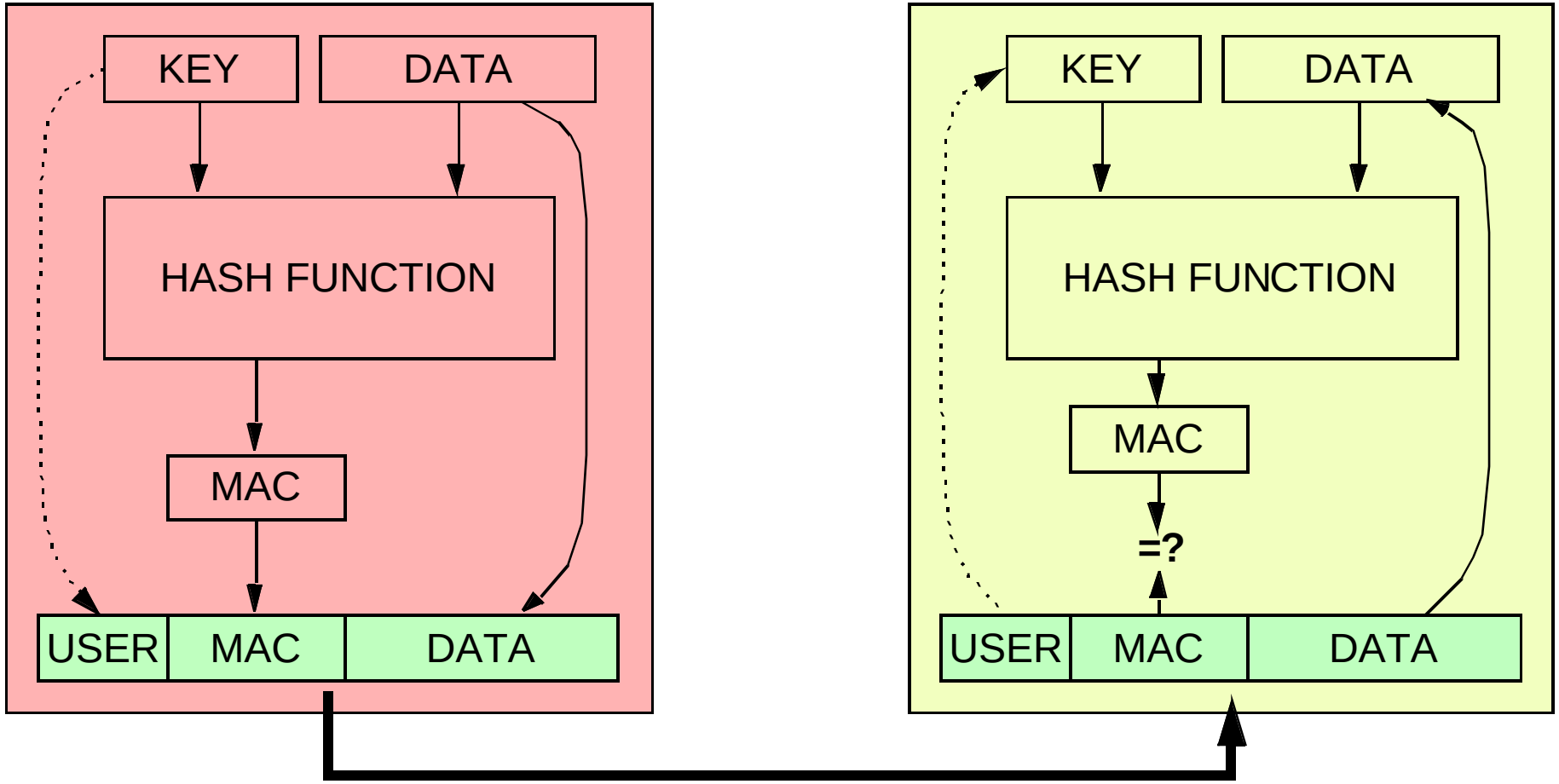
IDEA BEHIND DATA INTEGRITY AND AUTHENTICATION



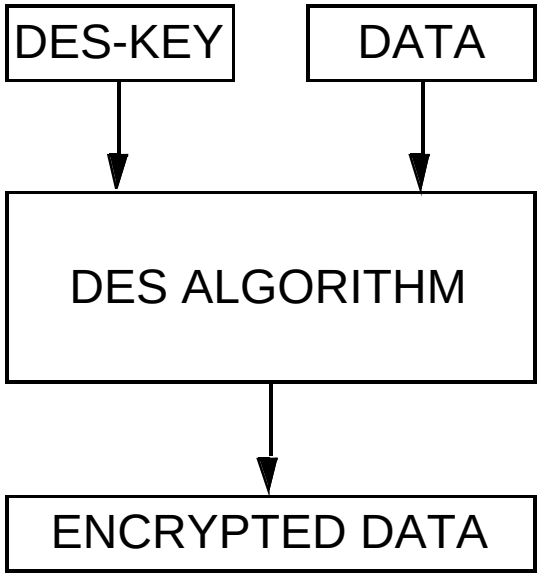
ADD THE MESSAGE AUTHENTICATION CODE (MAC) TO THE DATA AND SEND THE RESULT

Simple Web

IDEA BEHIND AUTHENTICATION

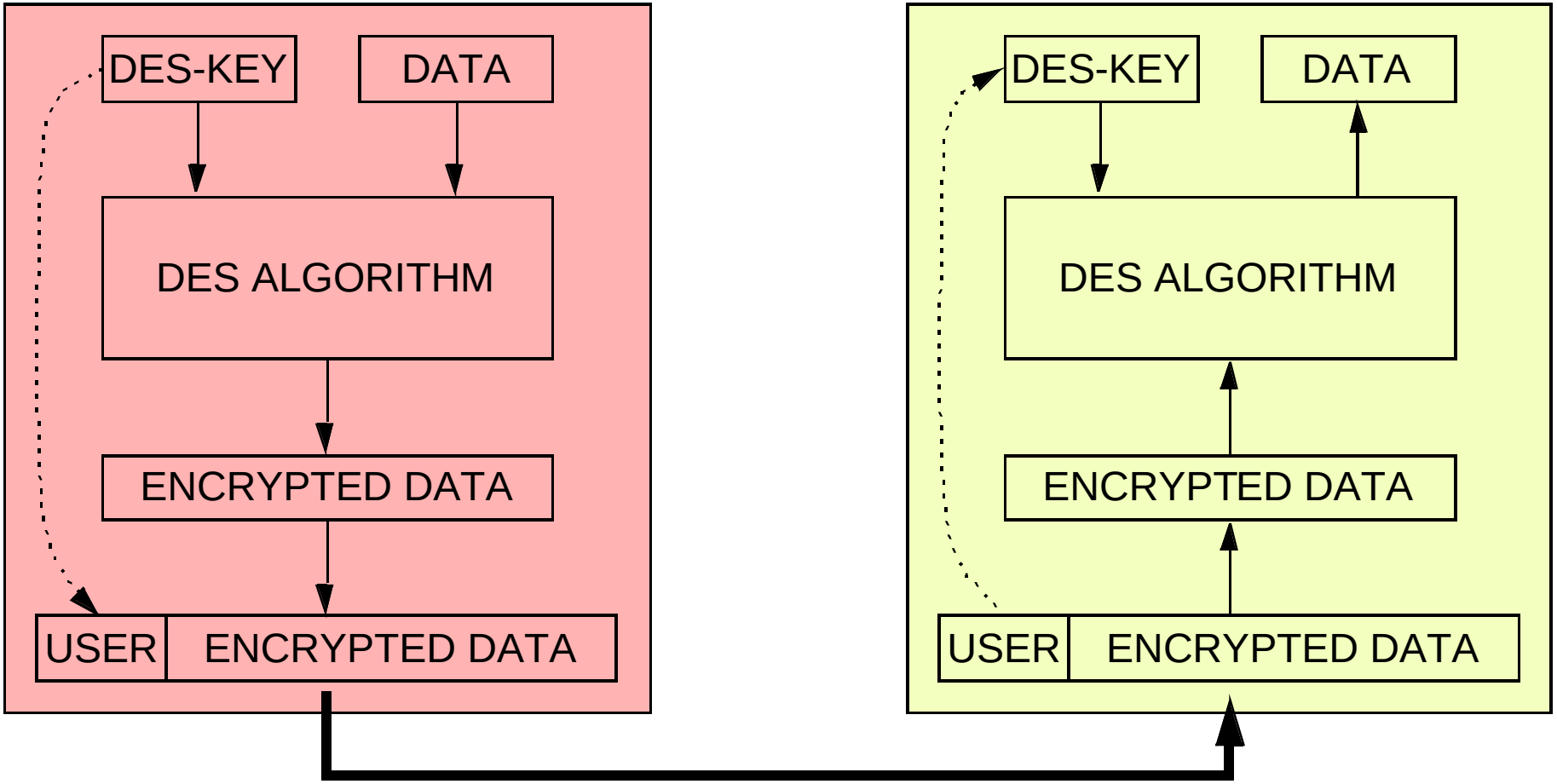


IDEA BEHIND THE DATA CONFIDENTIALITY (DES)



Simple Web

IDEA BEHIND ENCRYPTION



VIEW BASED ACCESS CONTROL MODEL

ACCESS CONTROL TABLE

MIB VIEWS

BY : ENG. Maha Jeha

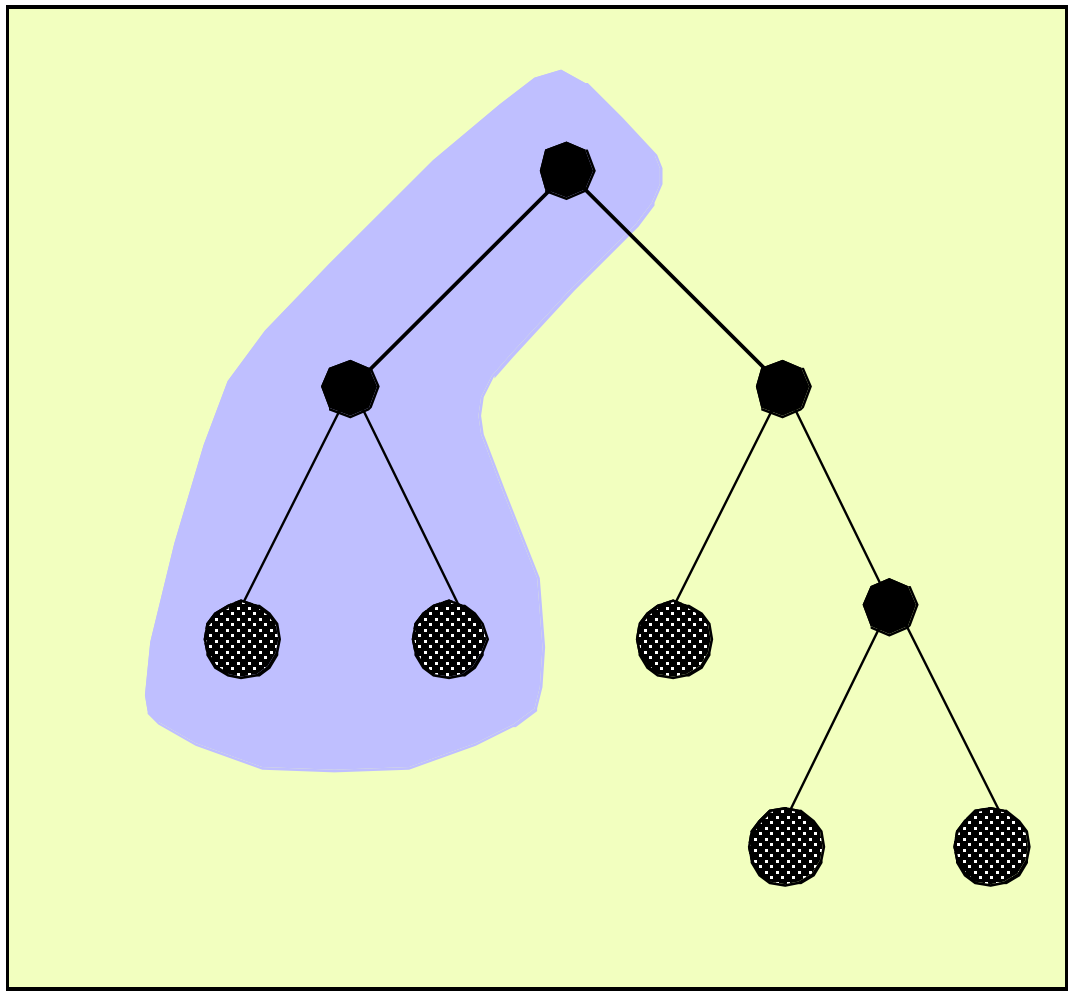
Simple Web

ACCESS CONTROL TABLES

MIB VIEW	ALLOWED OPERATIONS	ALLOWED MANAGERS	REQUIRED LEVEL OF SECURITY
Interface Table	SET	John	Authentication Encryption
Interface Table	GET / GETNEXT	John, Paul	Authentication
Systems Group	GET / GETNEXT	George	None
•••	•••	•••	•••
•••	•••	•••	•••
•••	•••	•••	•••
•••	•••	•••	•••

Simple Web

MIB VIEWS



SNMPv3 IMPLEMENTATIONS

ACE*COMM
AdventNet
BMC Software
Cisco
Epilogue
Gambit communications
Halcyon
IBM
ISI
IWL
MG-SOFT
MultiPort Corporation
SimpleSoft
SNMP Research

SNMP++
TU of Braunschweig
UCD
University of Quebec

Simple Web

SNMPv3 RFCs