SNMPv3

OVERVIEW:

DESIGN DECISIONS

ARCHITECTURE

SNMP MESSAGE STRUCTURE

SECURE COMMUNICATION
- USER SECURITY MODEL (USM)

ACCESS CONTROL
- VIEW BASED ACCESS CONTROL MODEL (VACM)

RFCs

Copyright © 2005 by *Aiko Pras*
These sheets may be used for educational purposes

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

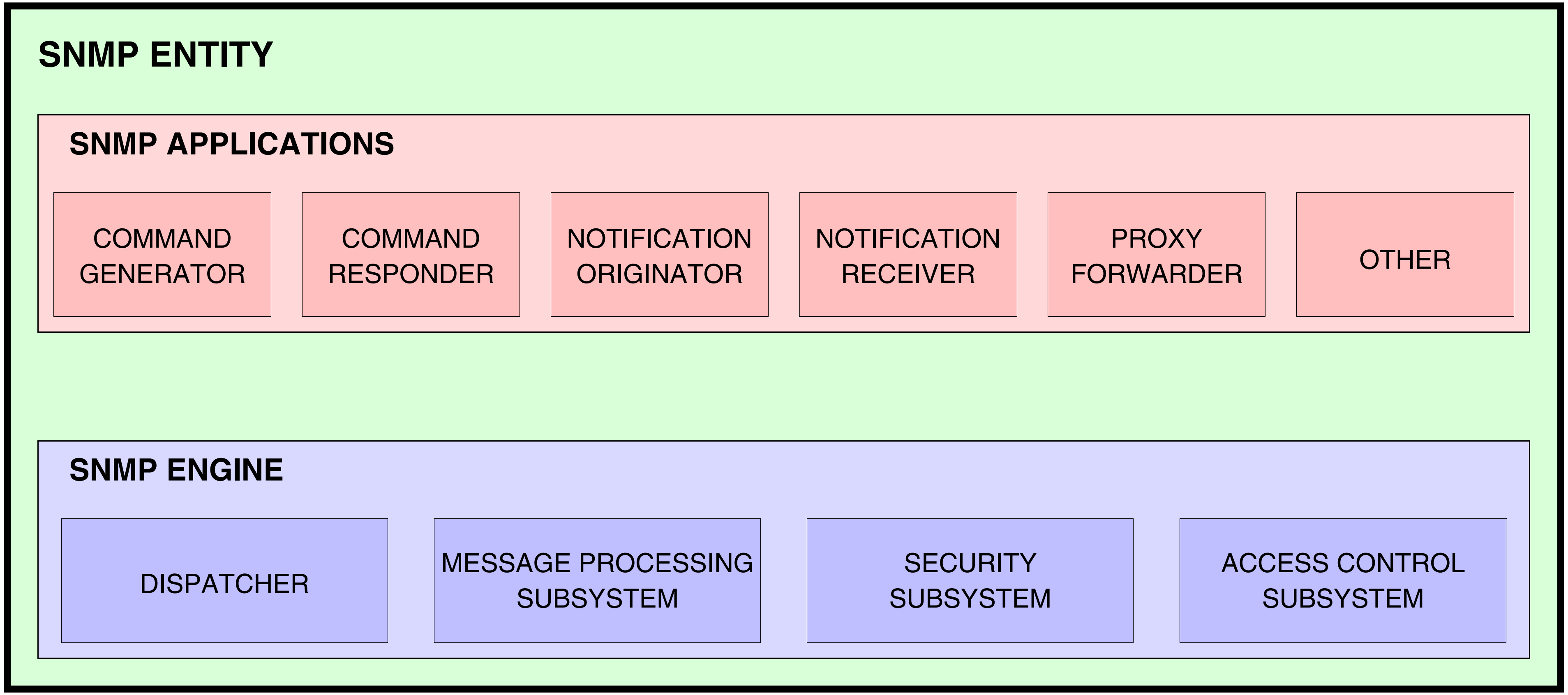
KEEP SNMP AS SIMPLE AS POSSIBLE

ALLOW FOR MINIMAL IMPLEMENTATIONS

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

RE-USE EXISTING SPECIFICATIONS, WHENEVER POSSIBLE

SNMPv3 ARCHITECTURE



SNMP ENTITY

SNMP APPLICATIONS

COMMAND GENERATOR

COMMAND RESPONDER

NOTIFICATION ORIGINATOR

NOTIFICATION RECEIVER

PROXY FORWARDER

OTHER

SNMP ENGINE

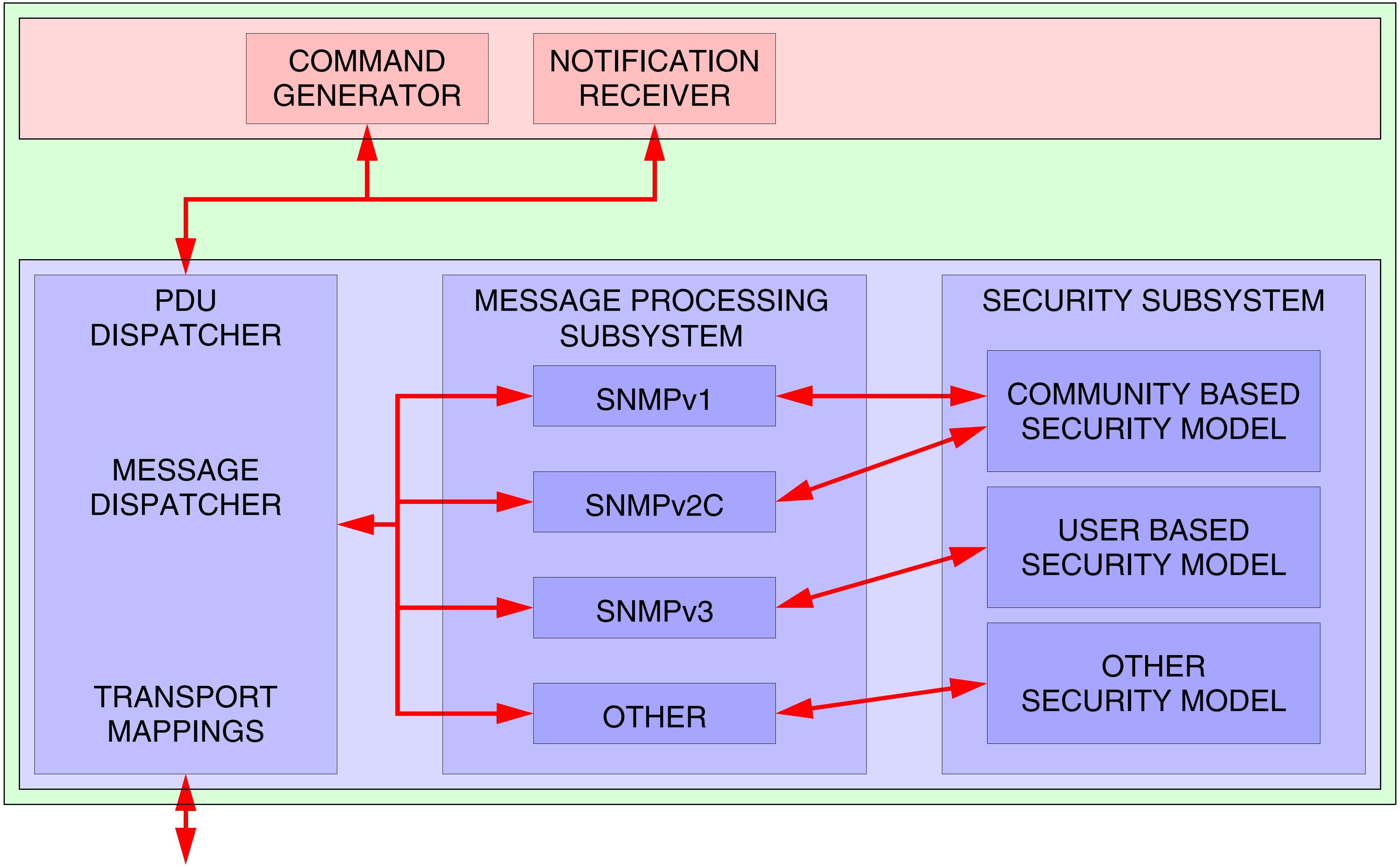
DISPATCHER

MESSAGE PROCESSING SUBSYSTEM

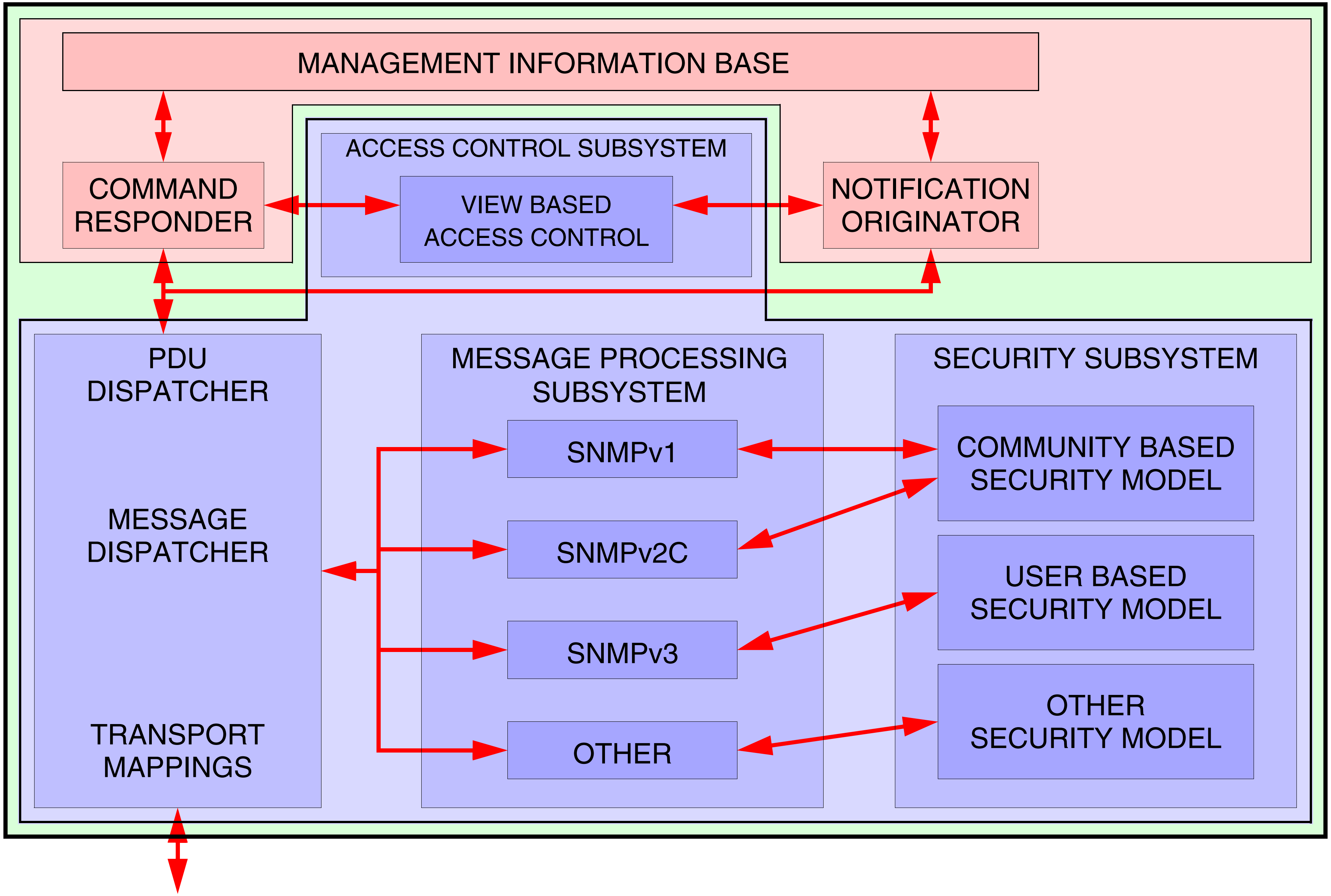
SECURITY SUBSYSTEM

ACCESS CONTROL SUBSYSTEM

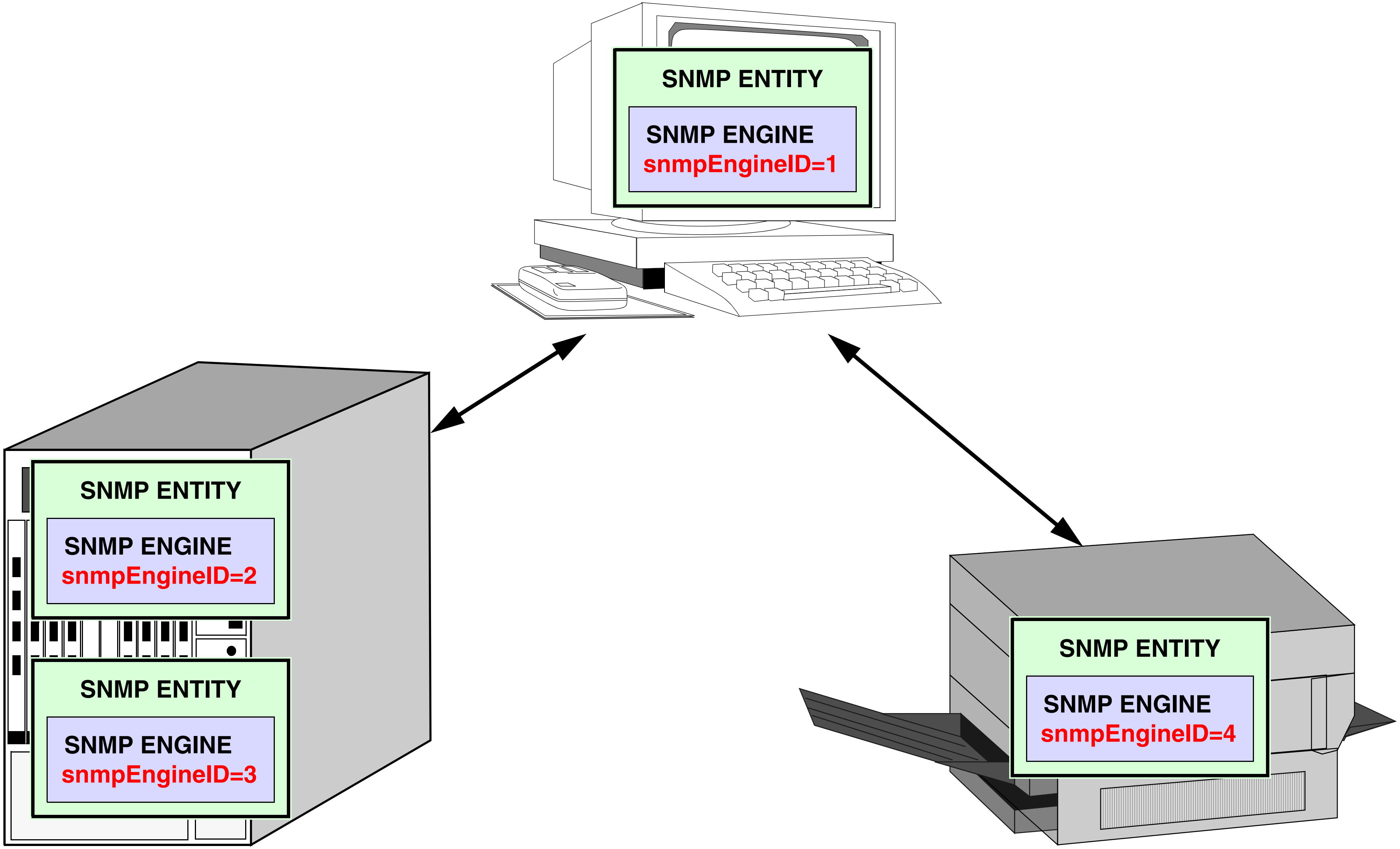
SNMPv3 ARCHITECTURE: MANAGER



SNMPv3 ARCHITECTURE: AGENT



CONCEPTS: snmpEngineID



CONCEPTS: snmpEngineID

SYNTAX DEFINED VIA TEXTUAL CONVENTION

OCTET STRING (5..32)

THE VALUE OF snmpEngineID MAY BE DETERMINED BY:

- HUMAN OPERATOR
- AUTOMATIC ALGORITHM

AUTOMATIC ALGORITHM USES:

- PRIVATE ENTERPRISE NUMBER
- IPv4 ADDRESS / IPv6 ADDRESS / MAC ADDRESS

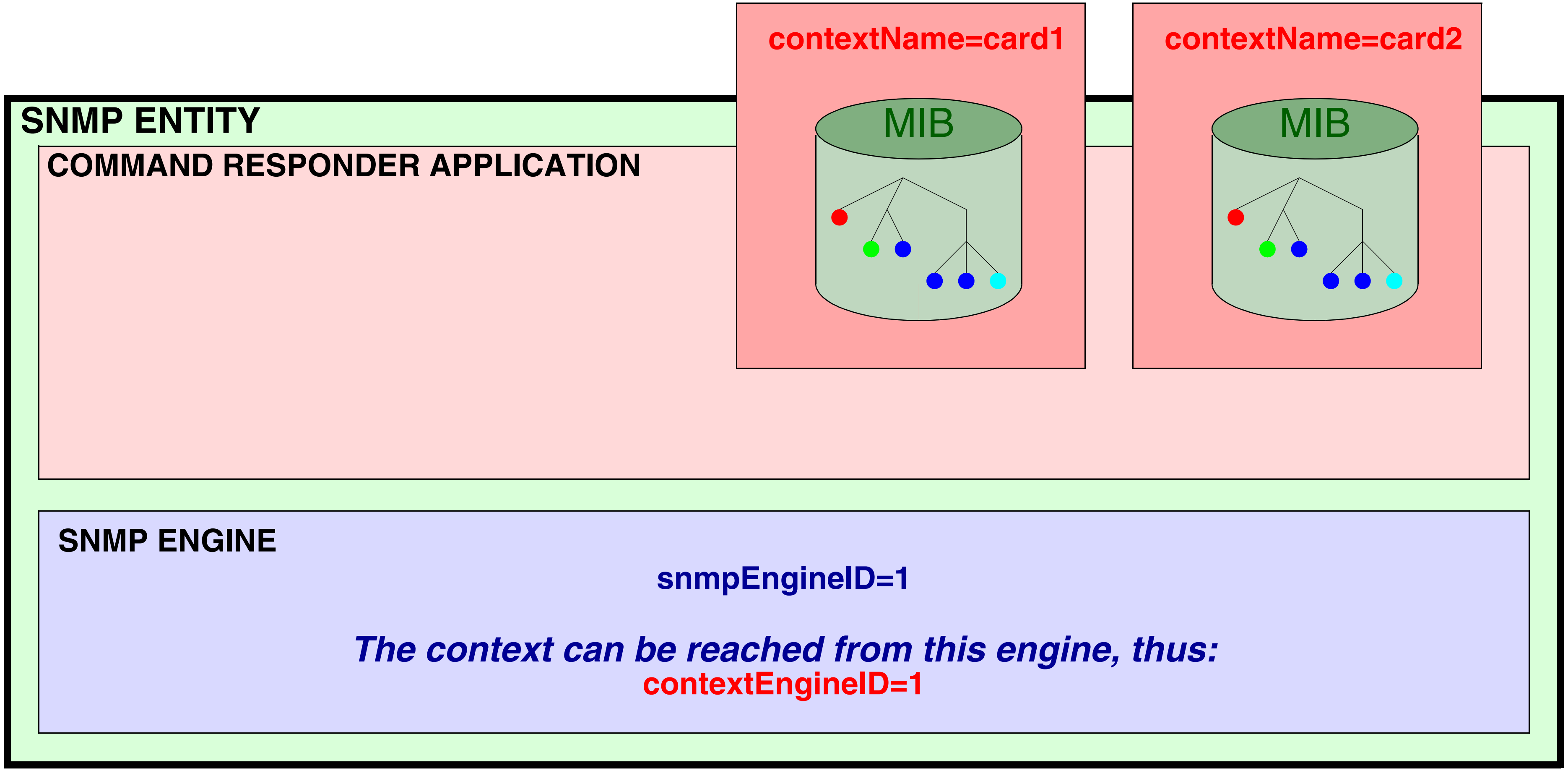
TEXTUAL CONVENTION DEFINED IN SNMP FRAMEWORK MIB

CONCEPTS: snmpEngineID

THE TERM EngineID IS FREQUENTLY USED

snmpEngineID	The identifier of an SNMP engine.
SnmpEngineID	The textual convention.
securityEngineID	Parameter of primitives in the architecture. The *authoritative* SNMP entity (which is the receiver of a confirmed PDU, the sender of a trap).
contextEngineID	Parameter of primitives in the architecture, and Parameter in messages. Identifies the engine associated with the data.
msgAuthoritativeEngineID	Parameter in messages. USM security parameter.
usmUserEngineID	An object in the snmpUsmMIB. In a simple agent, this is the agent's own snmpEngineID. It may also be the snmpEngineID of a remote SNMP engine with which this user can communicate.
usmStatsUnknownEngineID	An object in the snmpUsmMIB.
snmpCommunityContextEngineID	An object in the communityMIB.
entLogicalContextEngineID	An object in the entityMIB.
snmpProxyContextEngineID	An object in the proxyMIB.

CONCEPTS: Context



SNMP ENTITY

COMMAND RESPONDER APPLICATION

contextName=card1

contextName=card2

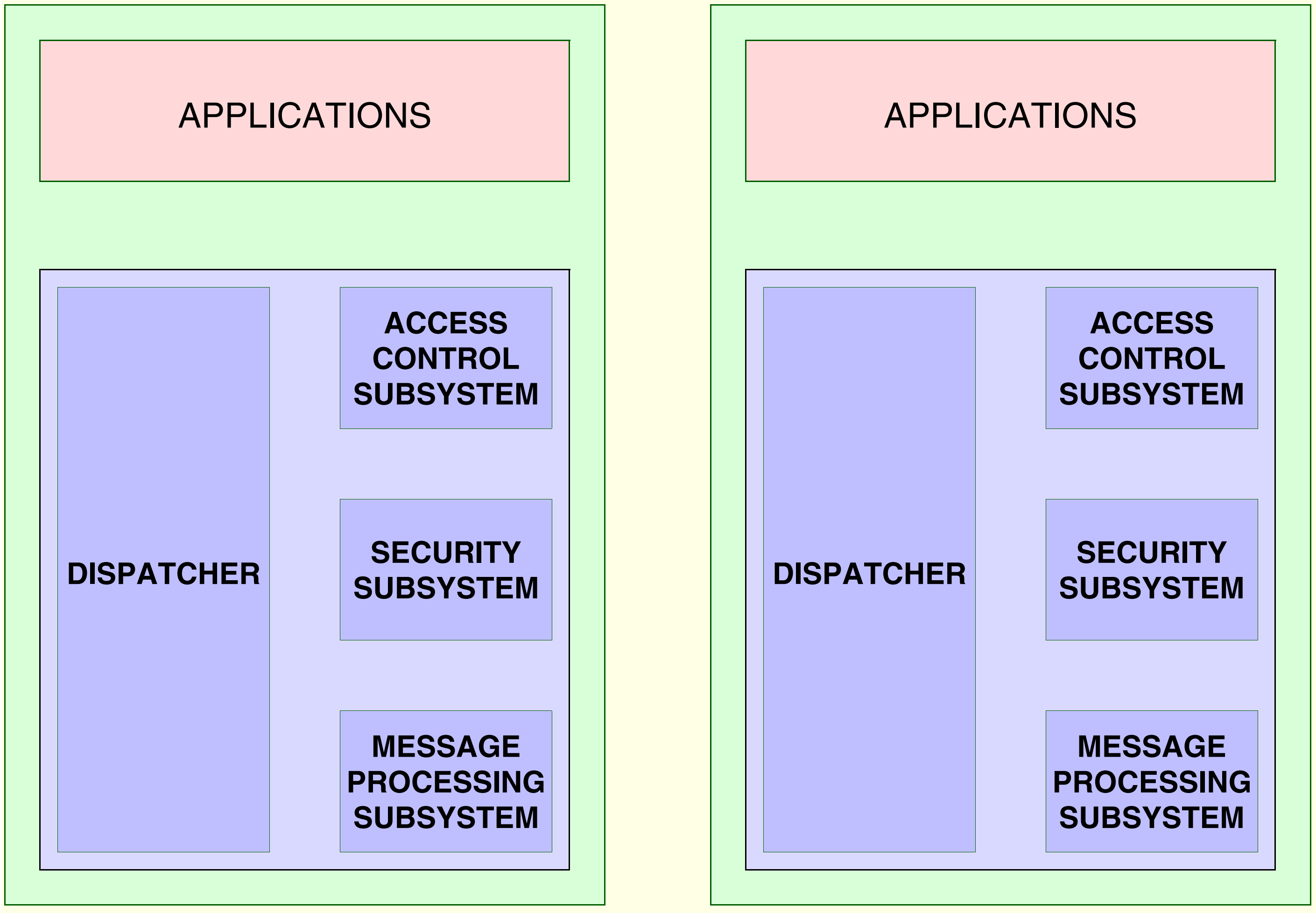
SNMP ENGINE

snmpEngineID=1

The context can be reached from this engine, thus:

contextEngineID=1

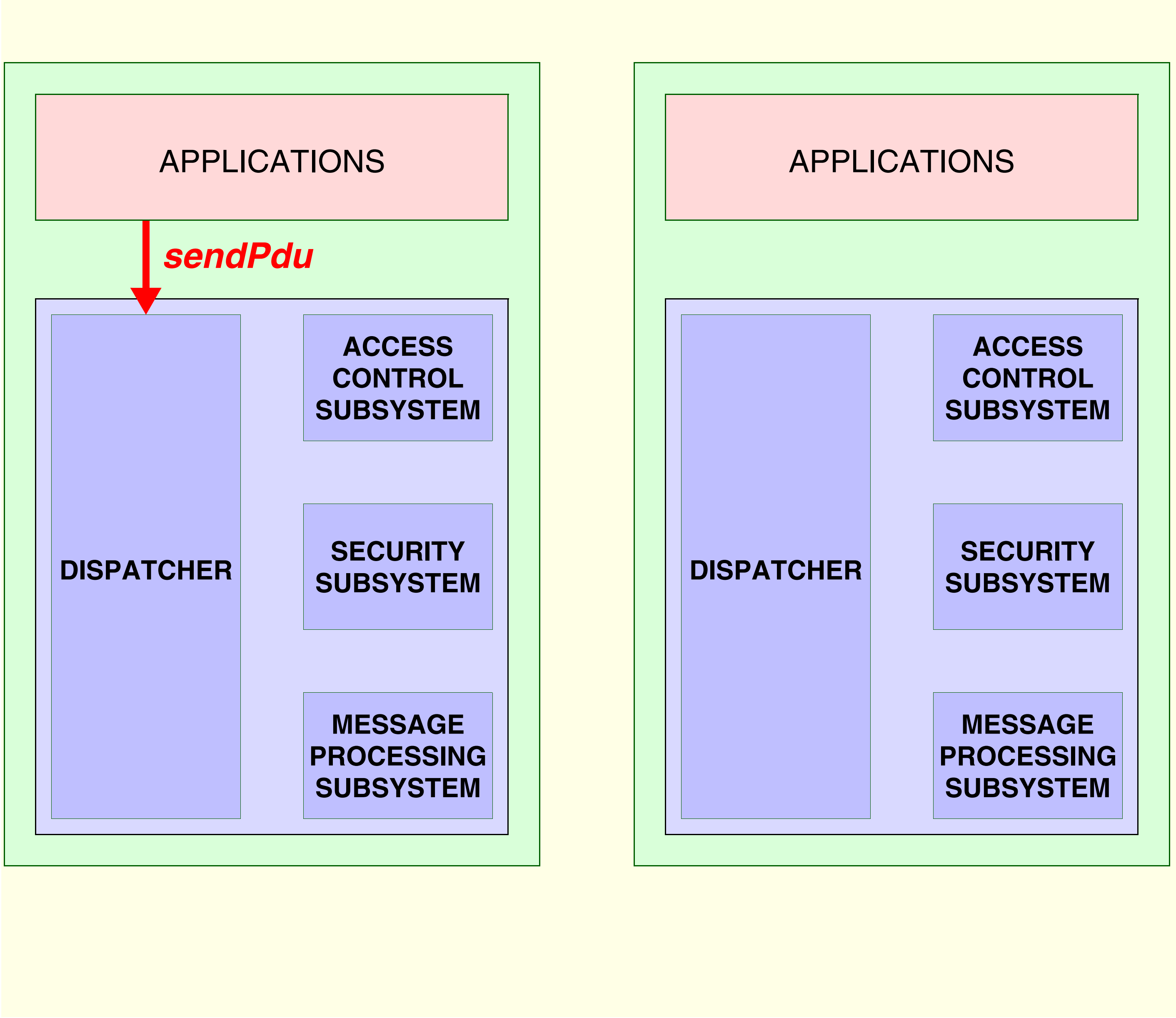
PRIMITIVES BETWEEN MODULES



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

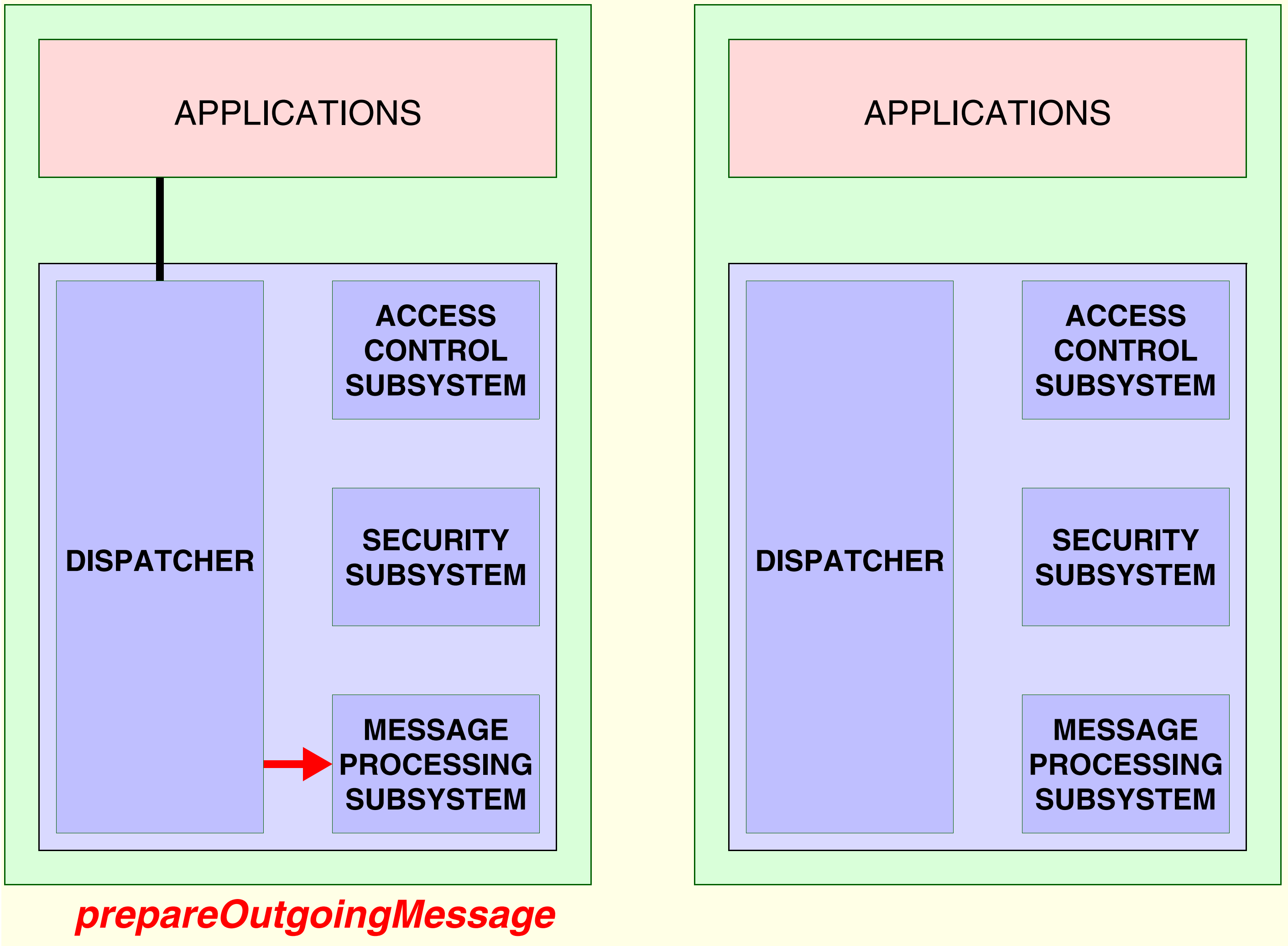
sendPdu



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

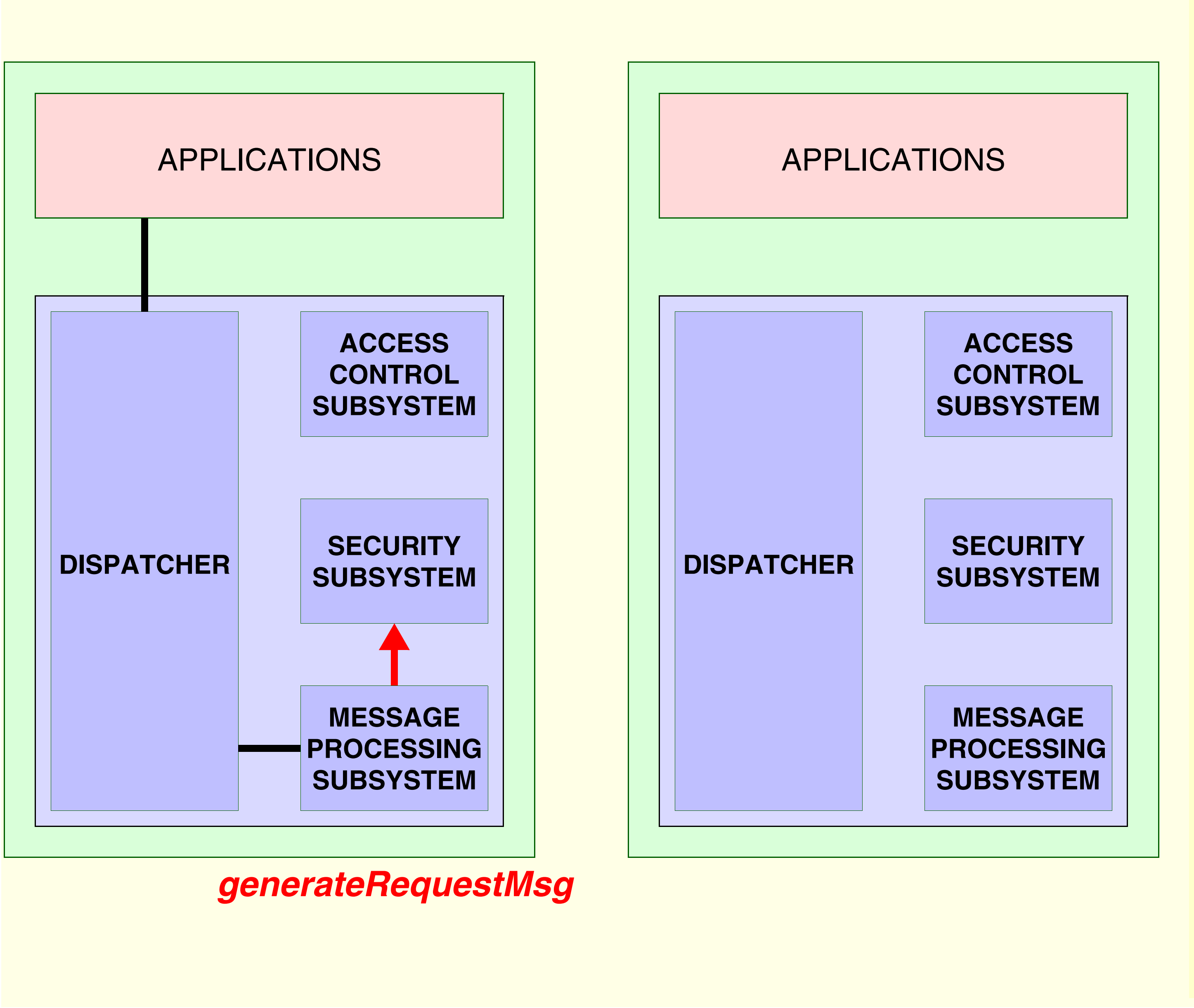
prepareOutgoingMessage



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

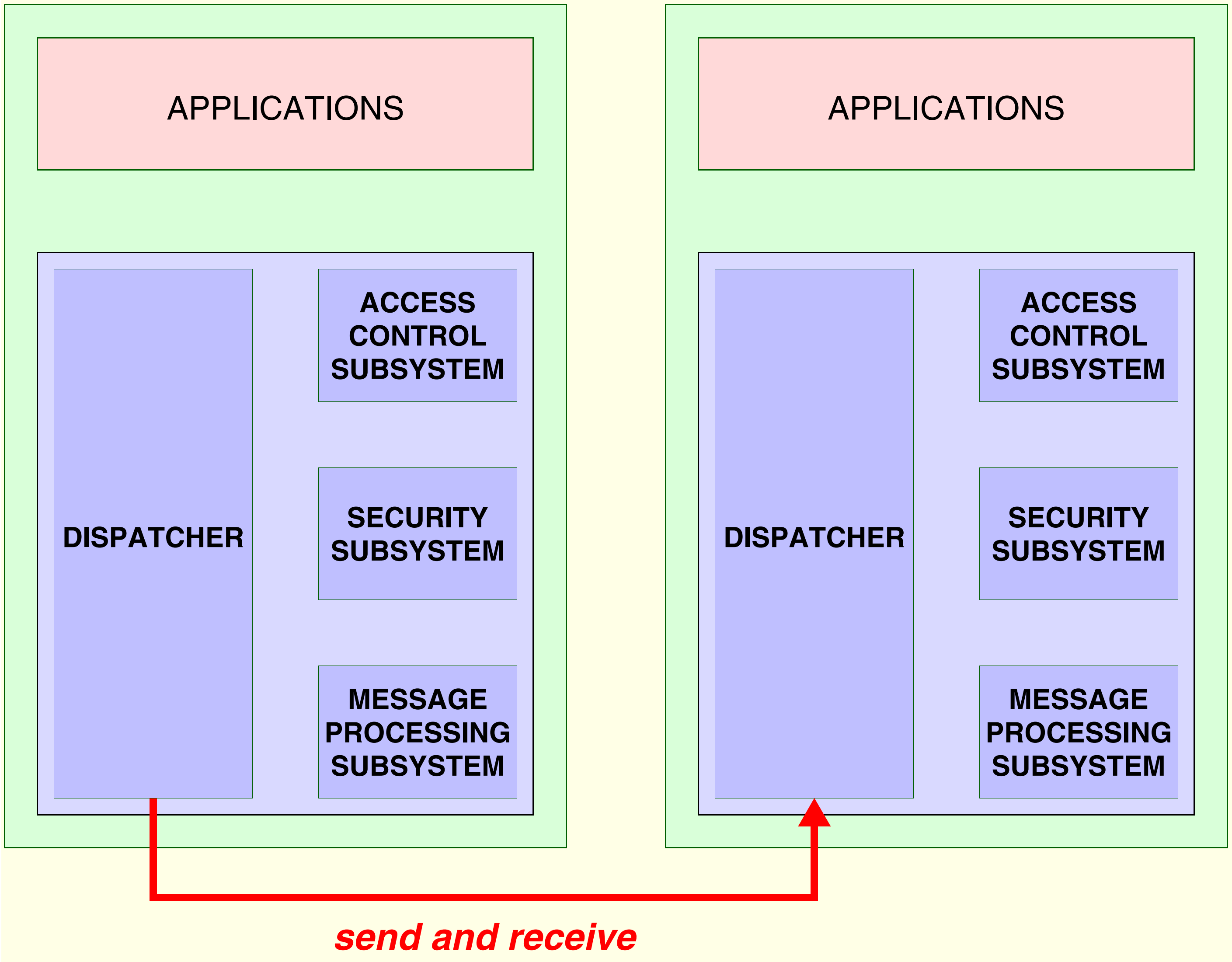
generateRequestMsg



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

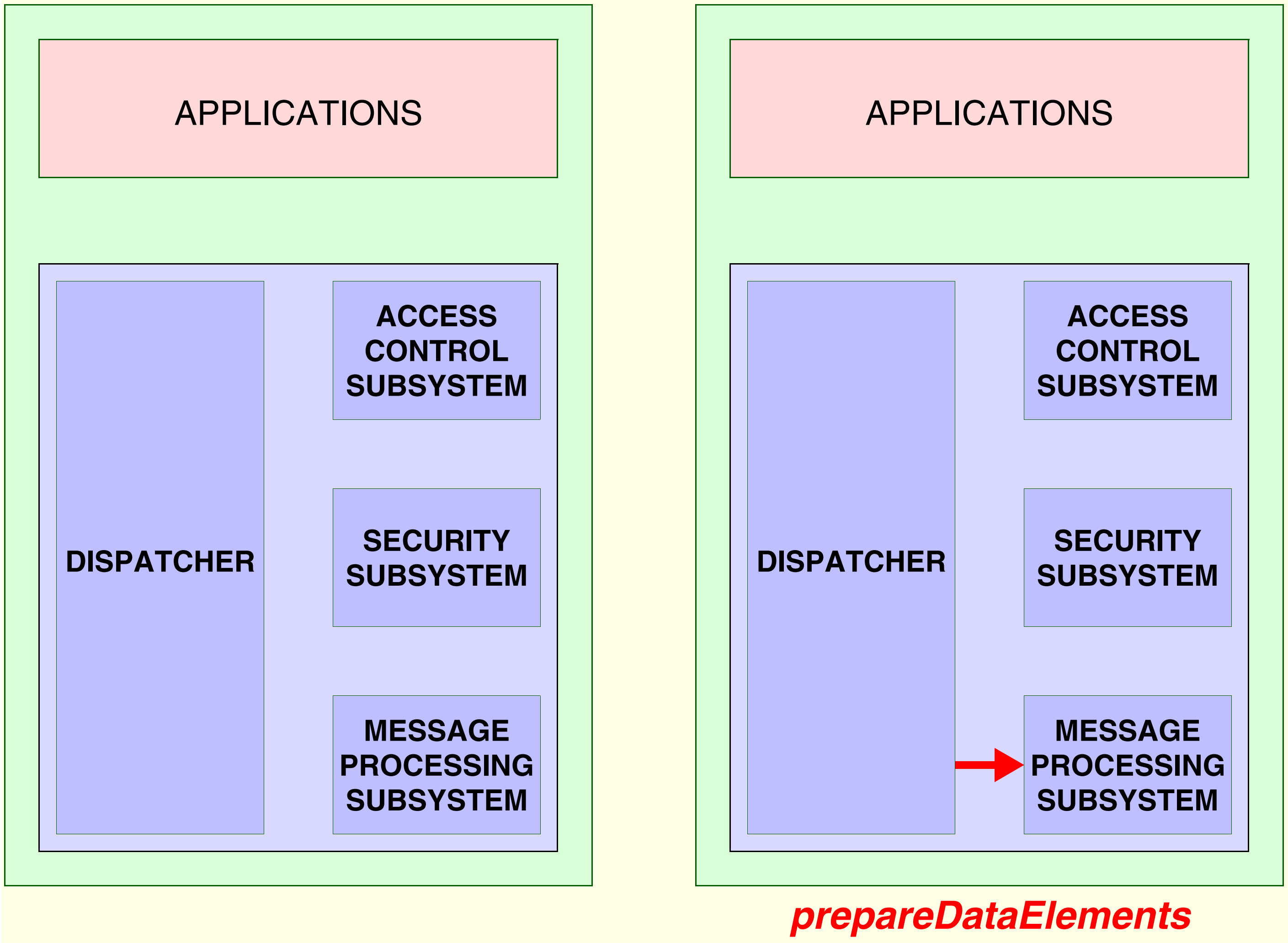
send / receive



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

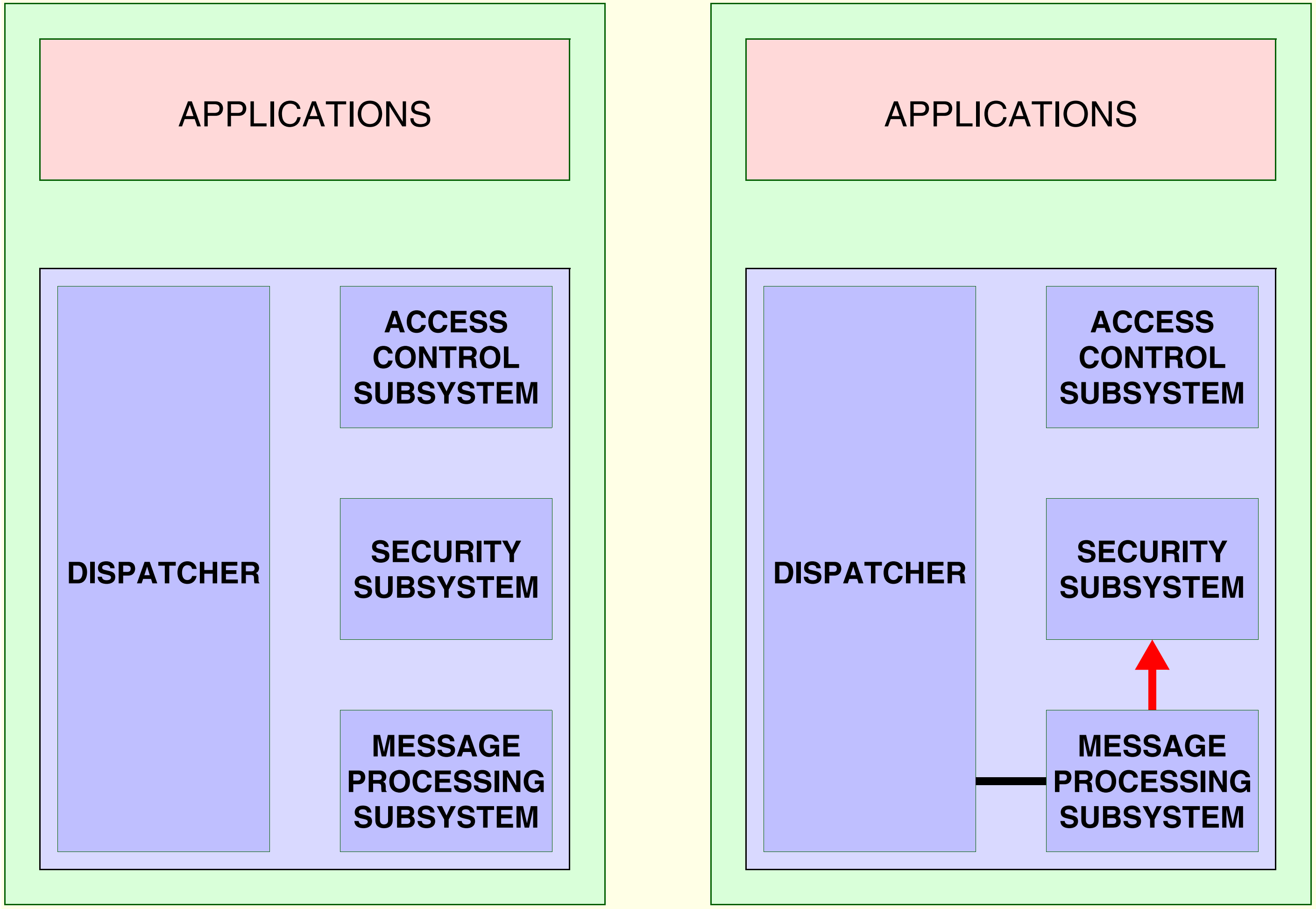
prepareDataElements



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

processIncomingMsg

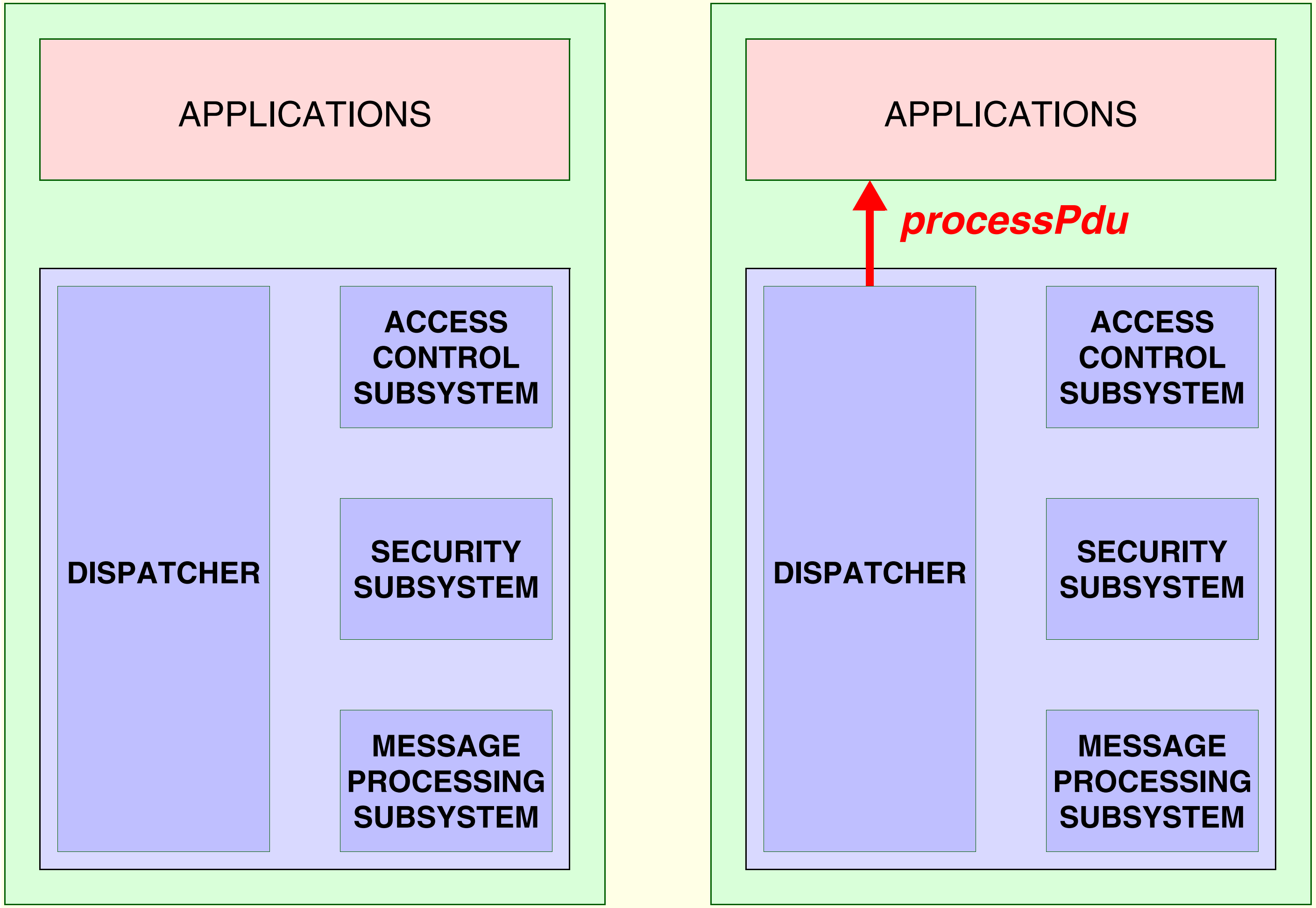


processIncomingMsg

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

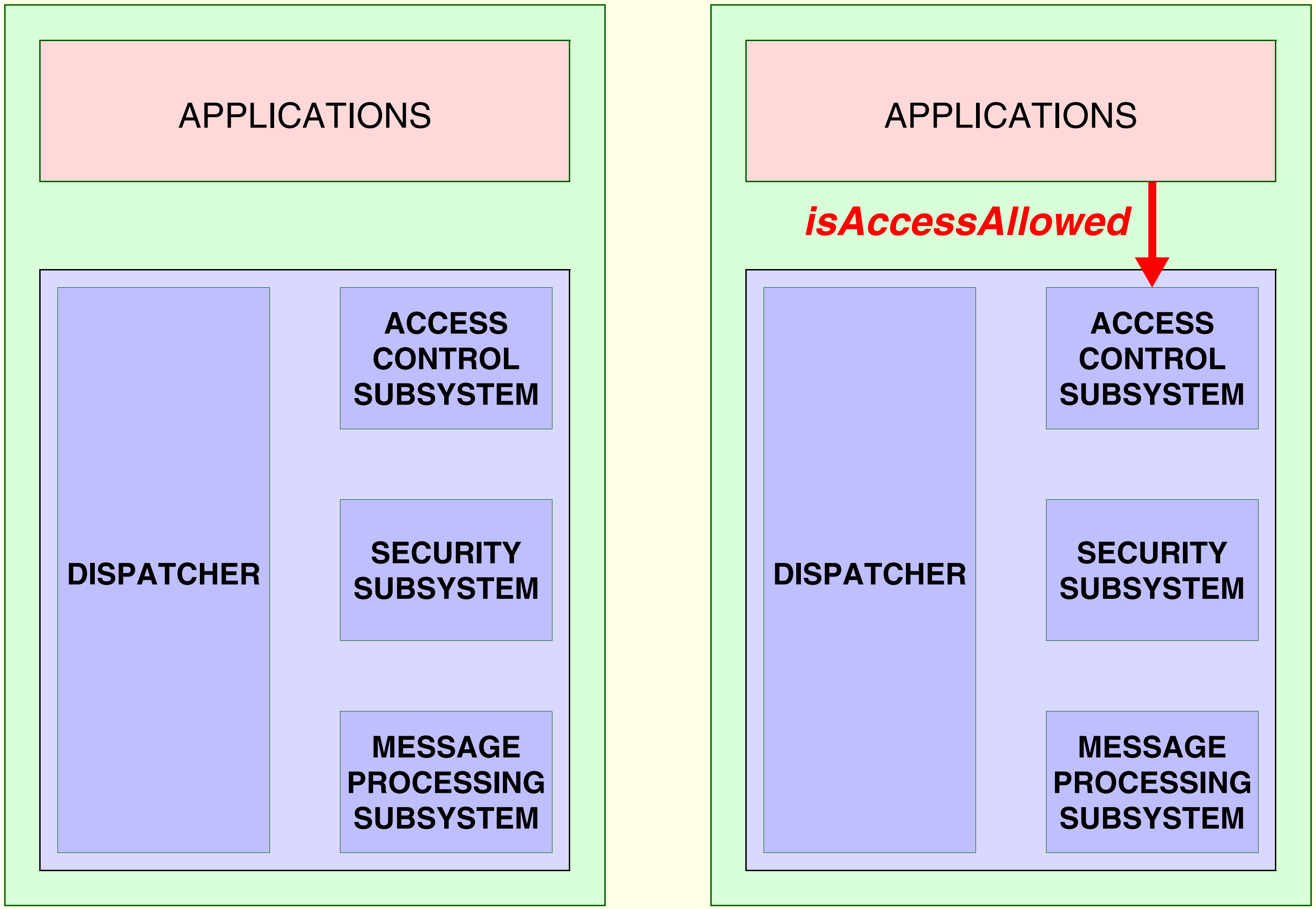
processPdu



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

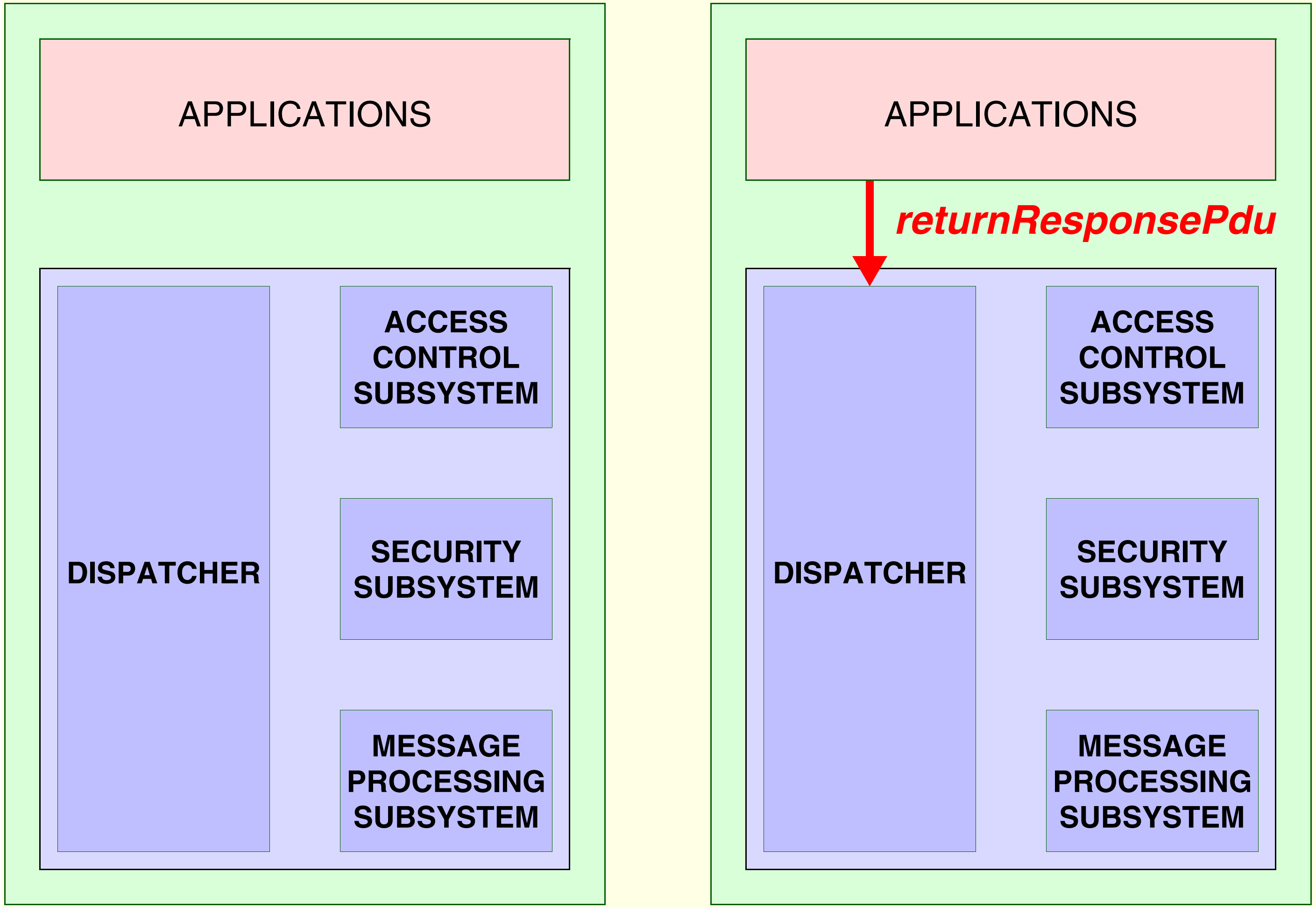
isAccessAllowed



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

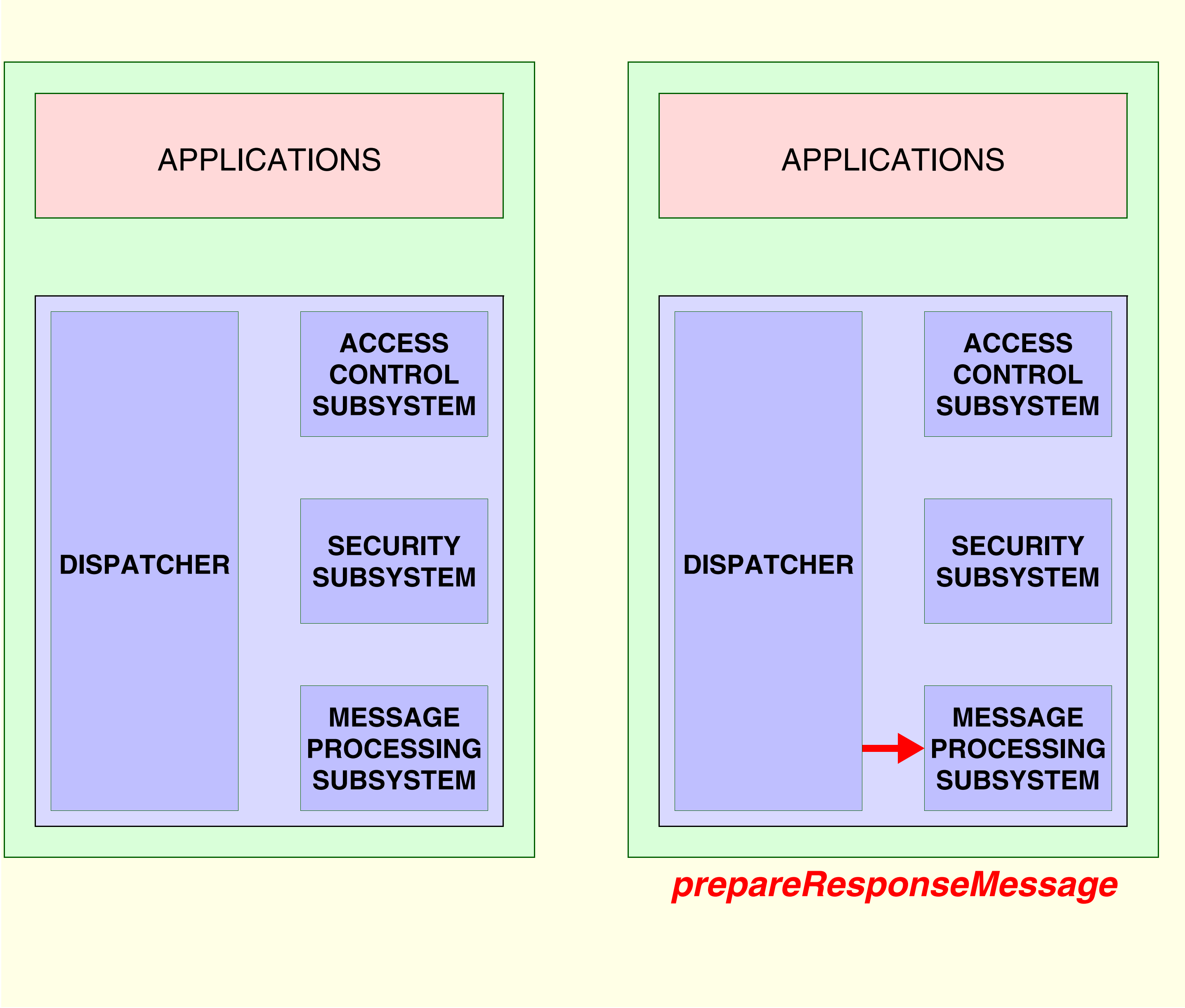
returnResponsePdu



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

prepareResponseMessage

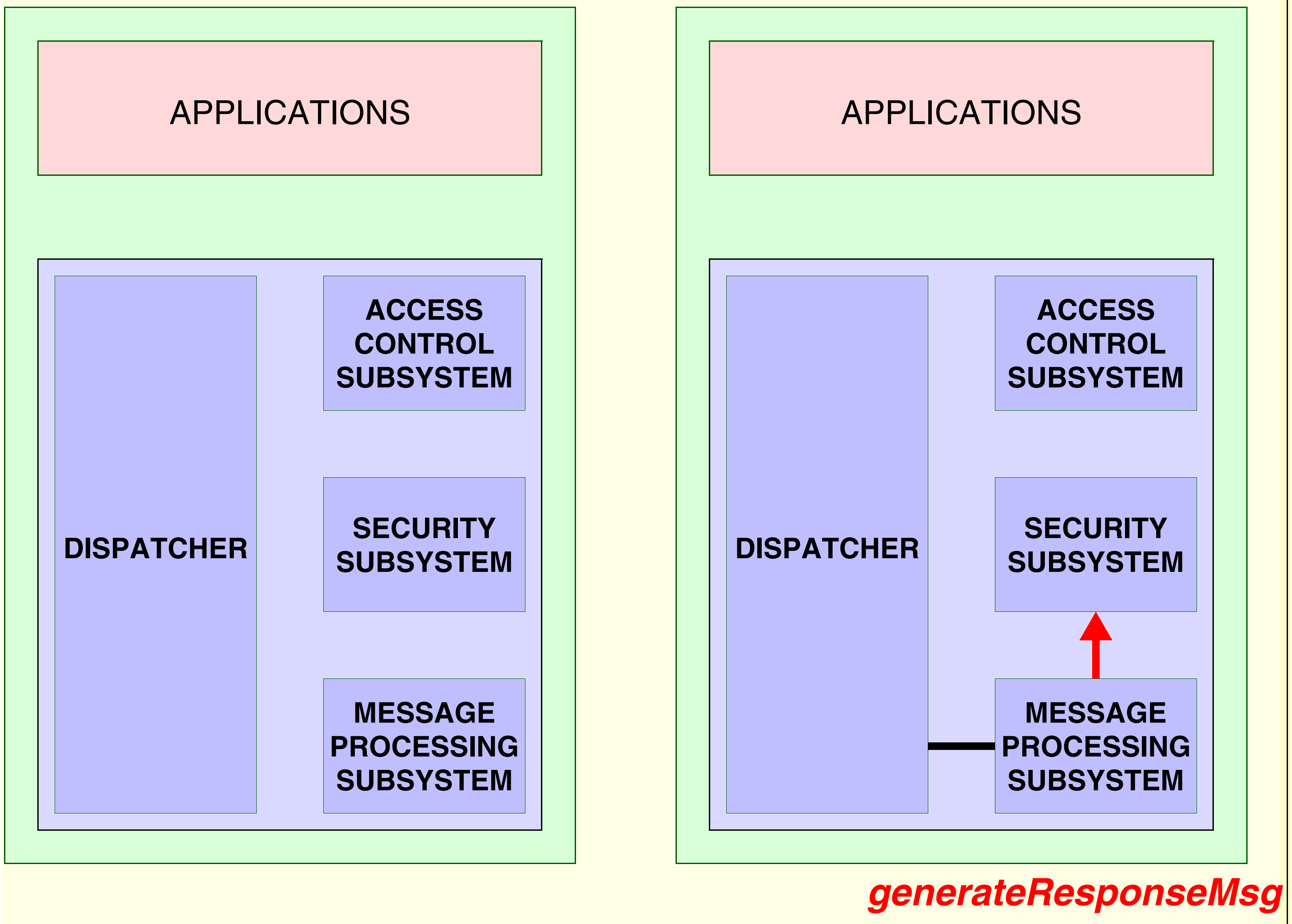


prepareResponseMessage

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

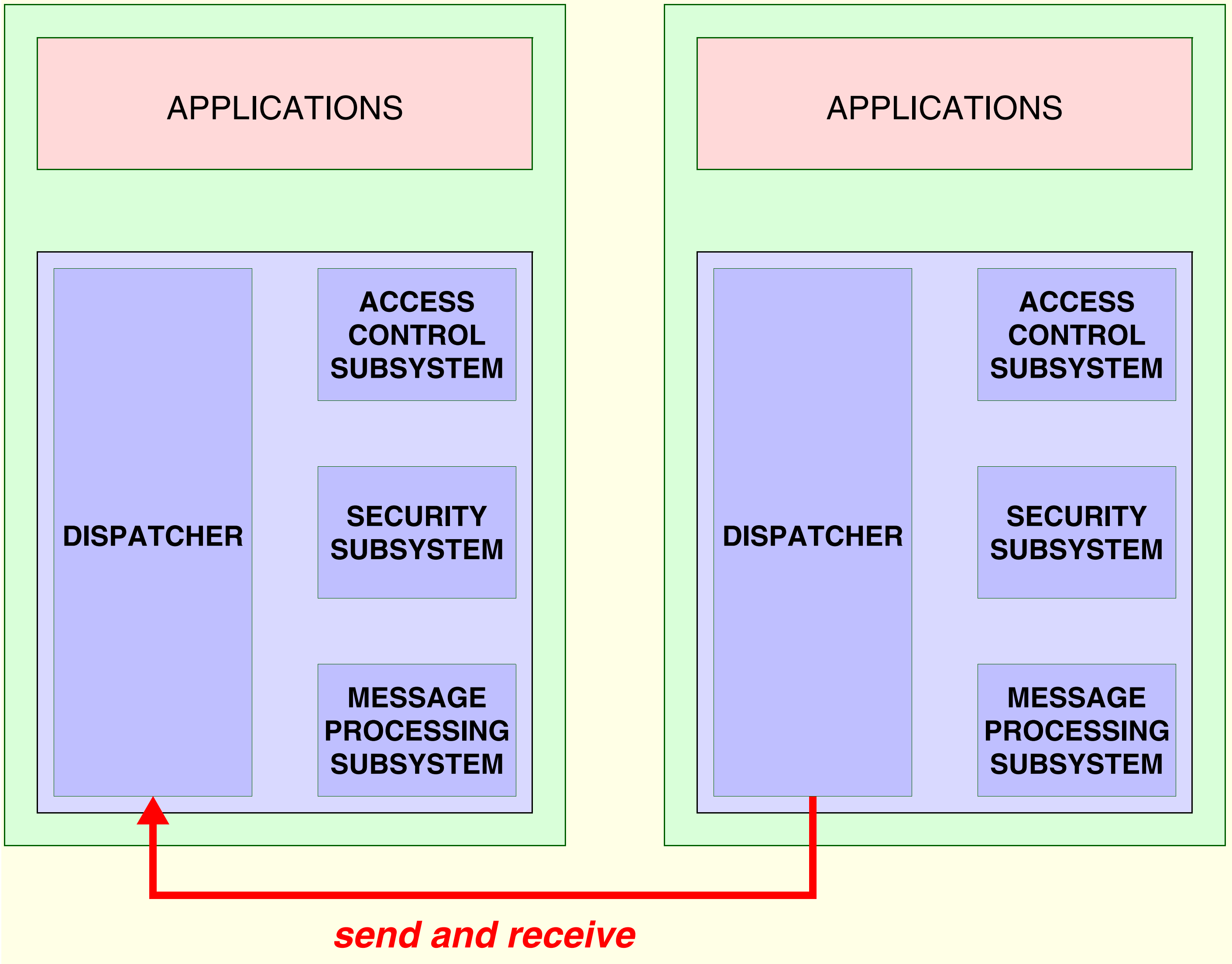
generateResponseMsg



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

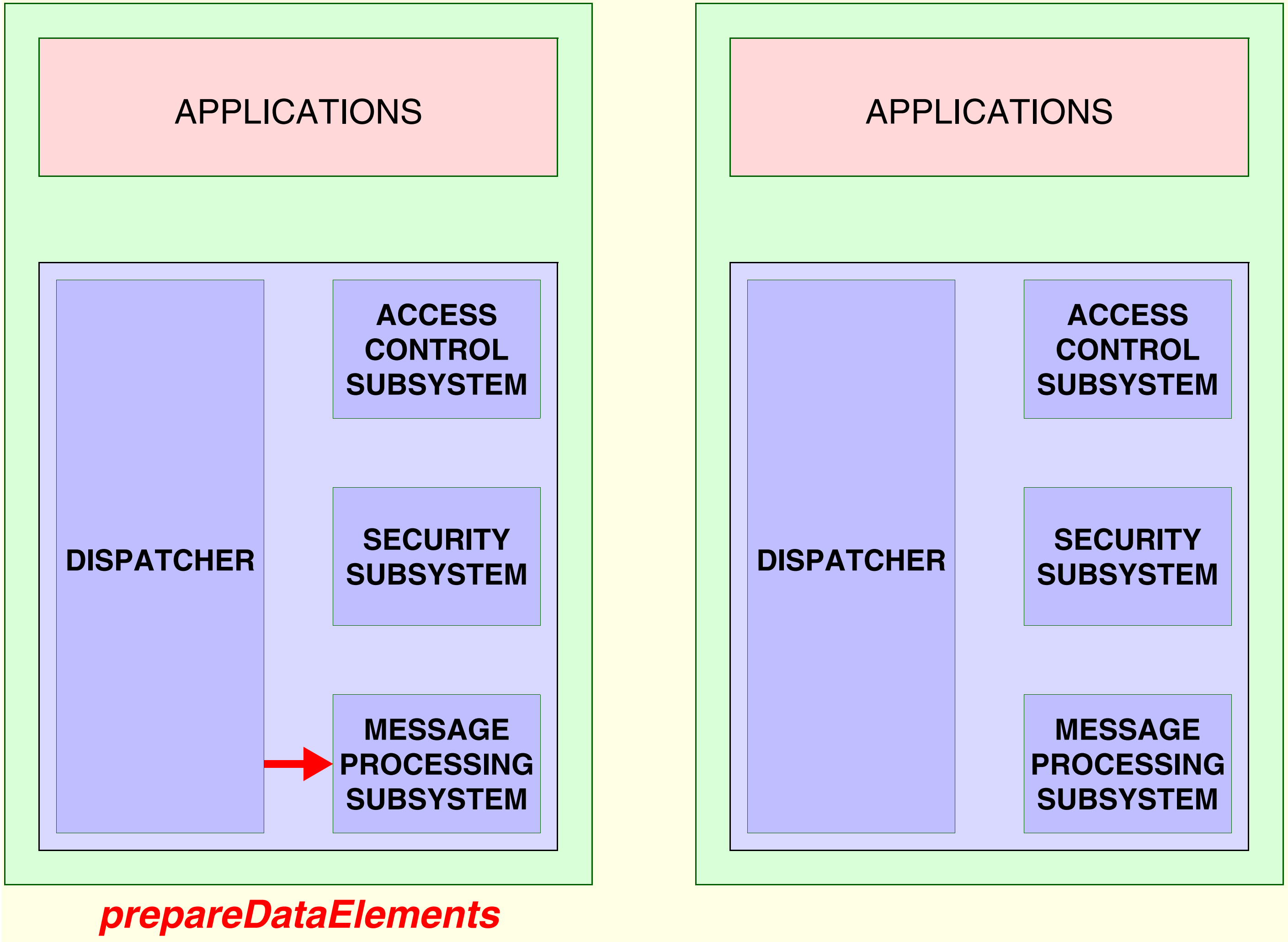
send / receive



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

prepareDataElements

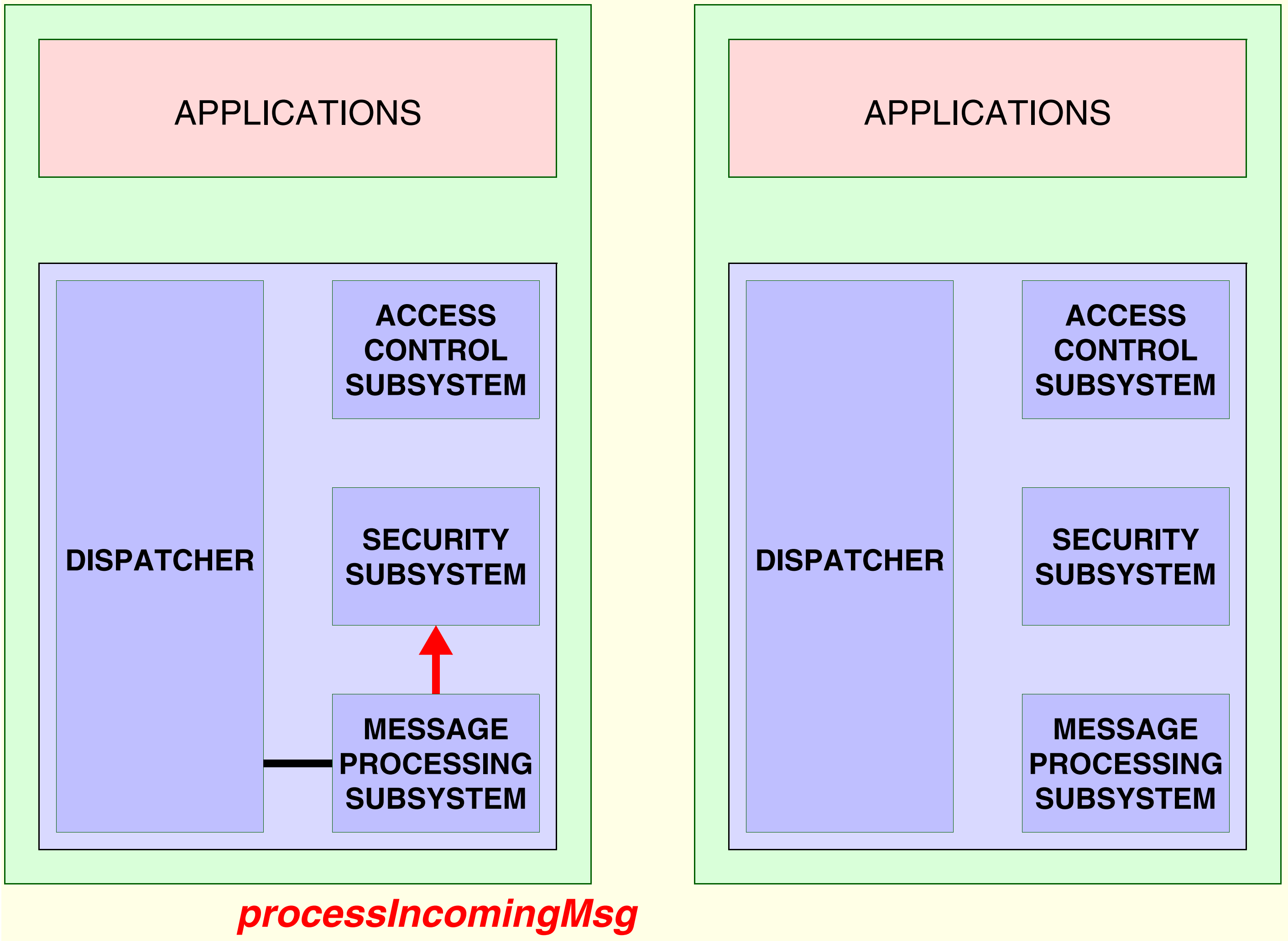


prepareDataElements

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

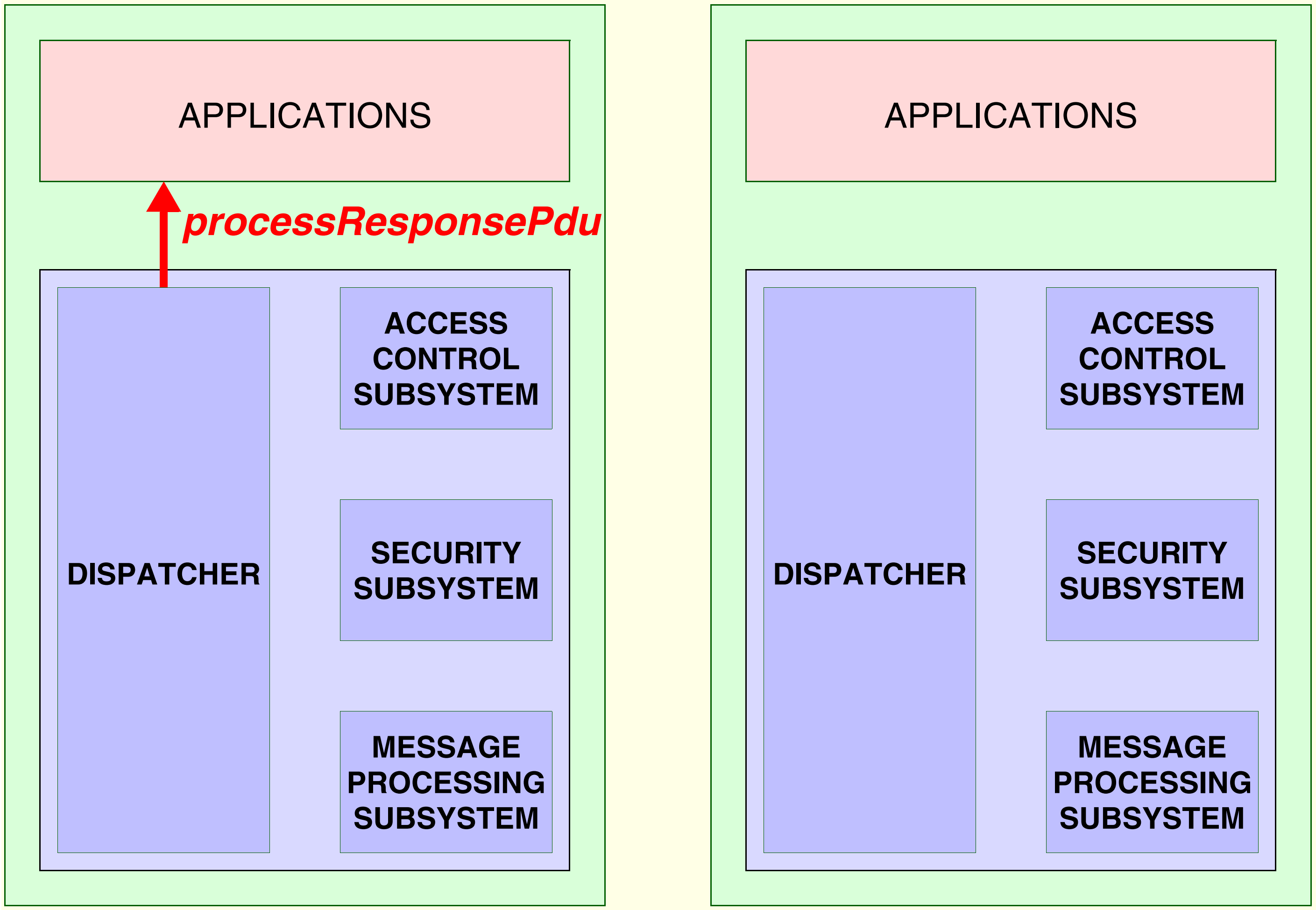
processIncomingMsg



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

processResponsePdu



APPLICATIONS

processResponsePdu

DISPATCHER

ACCESS CONTROL SUBSYSTEM

SECURITY SUBSYSTEM

MESSAGE PROCESSING SUBSYSTEM

APPLICATIONS

DISPATCHER

ACCESS CONTROL SUBSYSTEM

SECURITY SUBSYSTEM

MESSAGE PROCESSING SUBSYSTEM

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

- RFC 3412
- SNMPv3 MESSAGE STRUCTURE
- snmpMPDMIB

APPLICATIONS

- RFC 3413
- snmpTargetMIB
- snmpNotificationMIB
- snmpProxyMIB

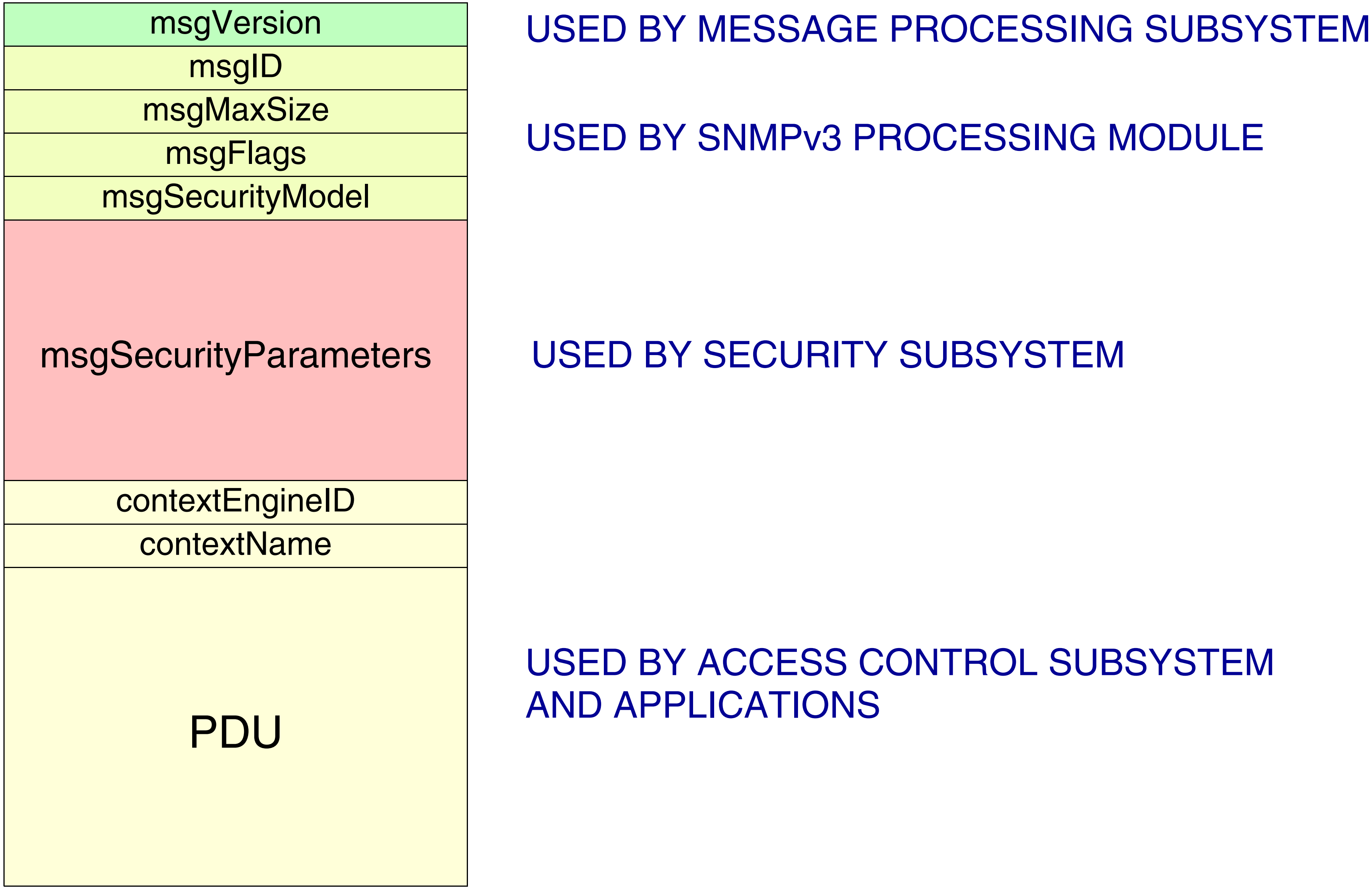
SECURITY SUBSYSTEM

- RFC 3414
- USER BASED SECURITY MODEL
- snmpUsmMIB

ACCESS CONTROL SUBSYSTEM

- RFC 3415
- VIEW BASED ACCESS CONTROL MODEL
- snmpVacmMIB

SNMPv3 MESSAGE STRUCTURE



msgVersion

msgID

msgMaxSize

msgFlags

msgSecurityModel

msgSecurityParameters

contextEngineID

contextName

PDU

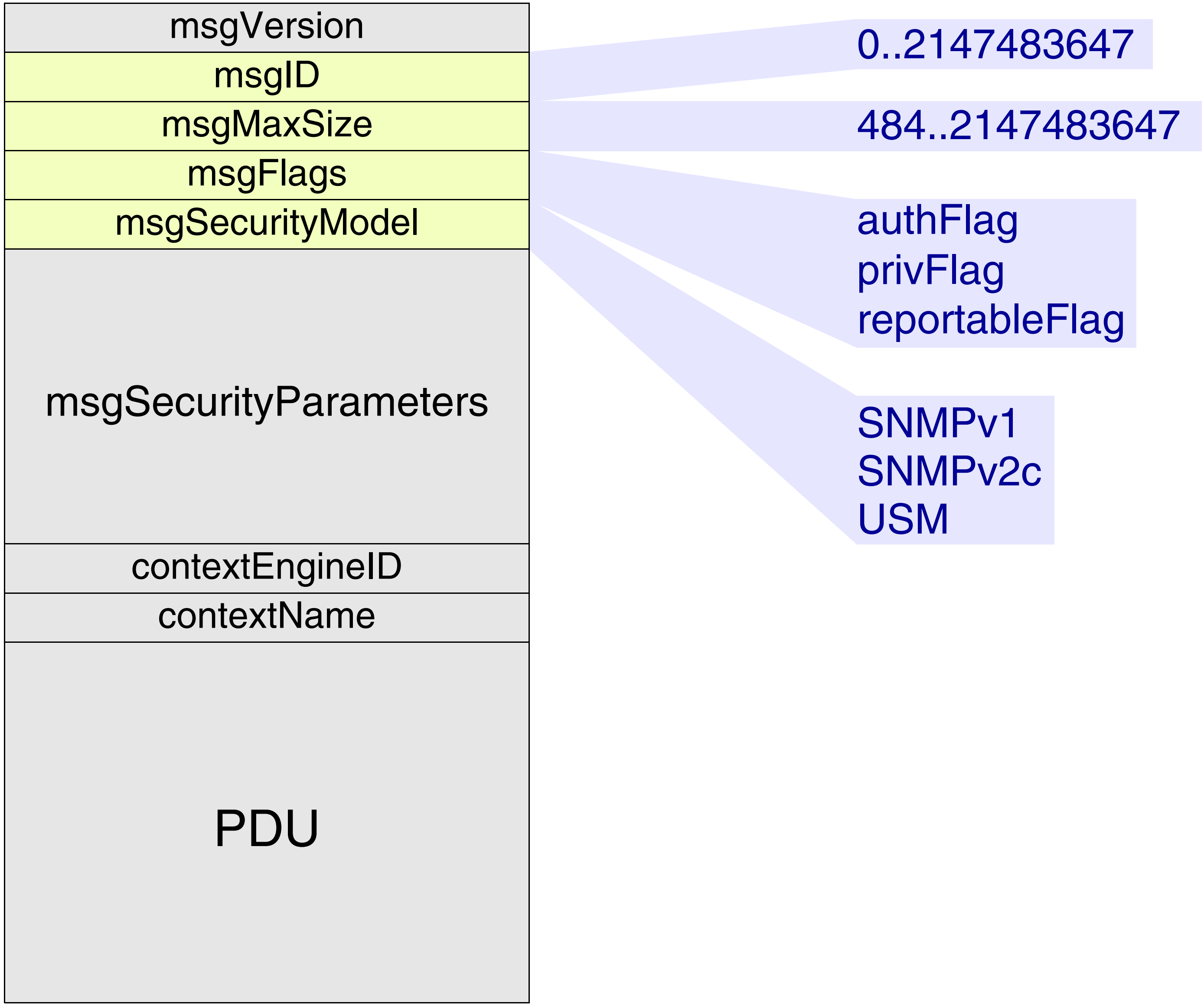
USED BY MESSAGE PROCESSING SUBSYSTEM

USED BY SNMPv3 PROCESSING MODULE

USED BY SECURITY SUBSYSTEM

USED BY ACCESS CONTROL SUBSYSTEM
AND APPLICATIONS

SNMPv3 PROCESSING MODULE PARAMETERS



msgVersion

msgID

msgMaxSize

msgFlags

msgSecurityModel

msgSecurityParameters

contextEngineID

contextName

PDU

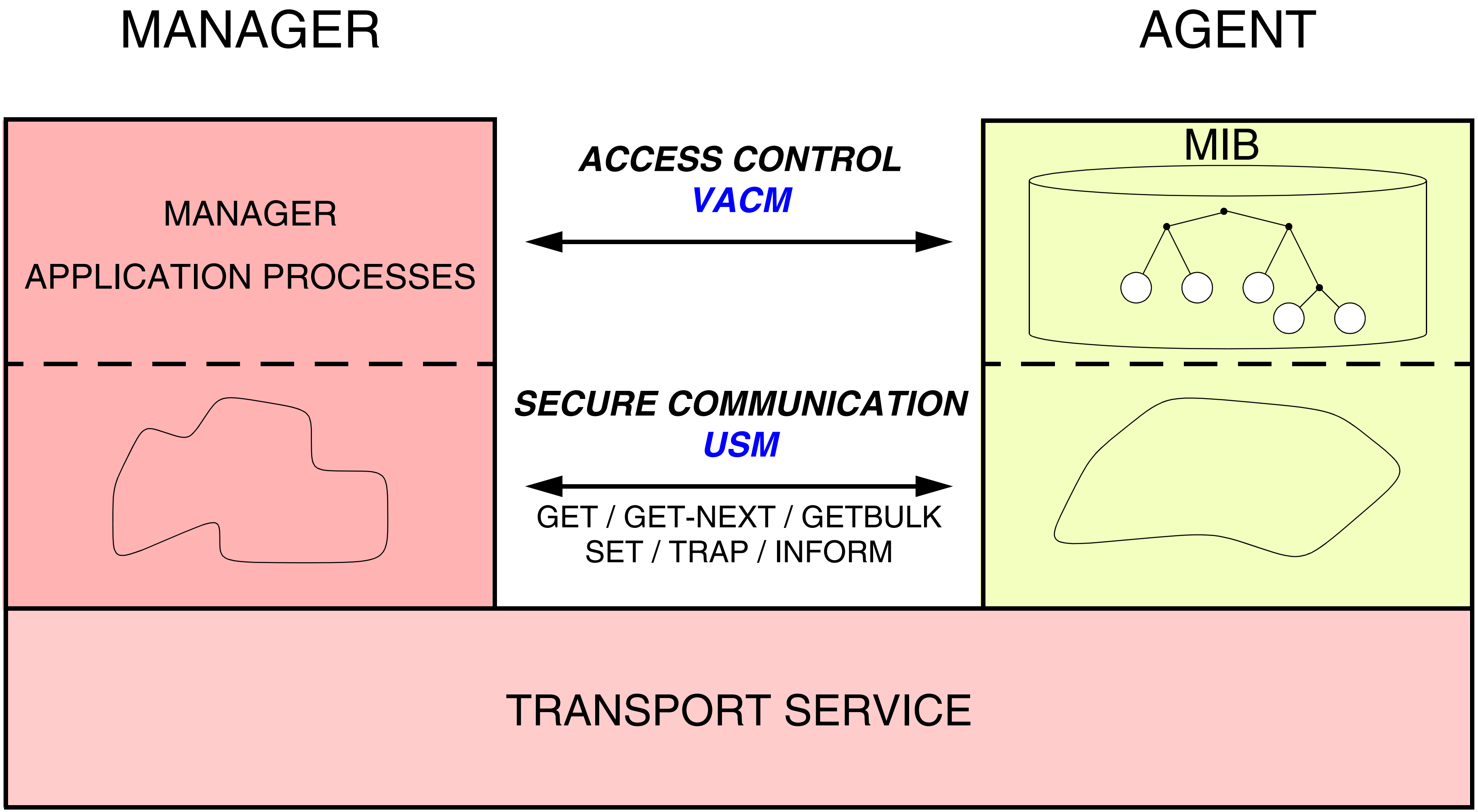
0..2147483647

484..2147483647

authFlag
privFlag
reportableFlag

SNMPv1
SNMPv2c
USM

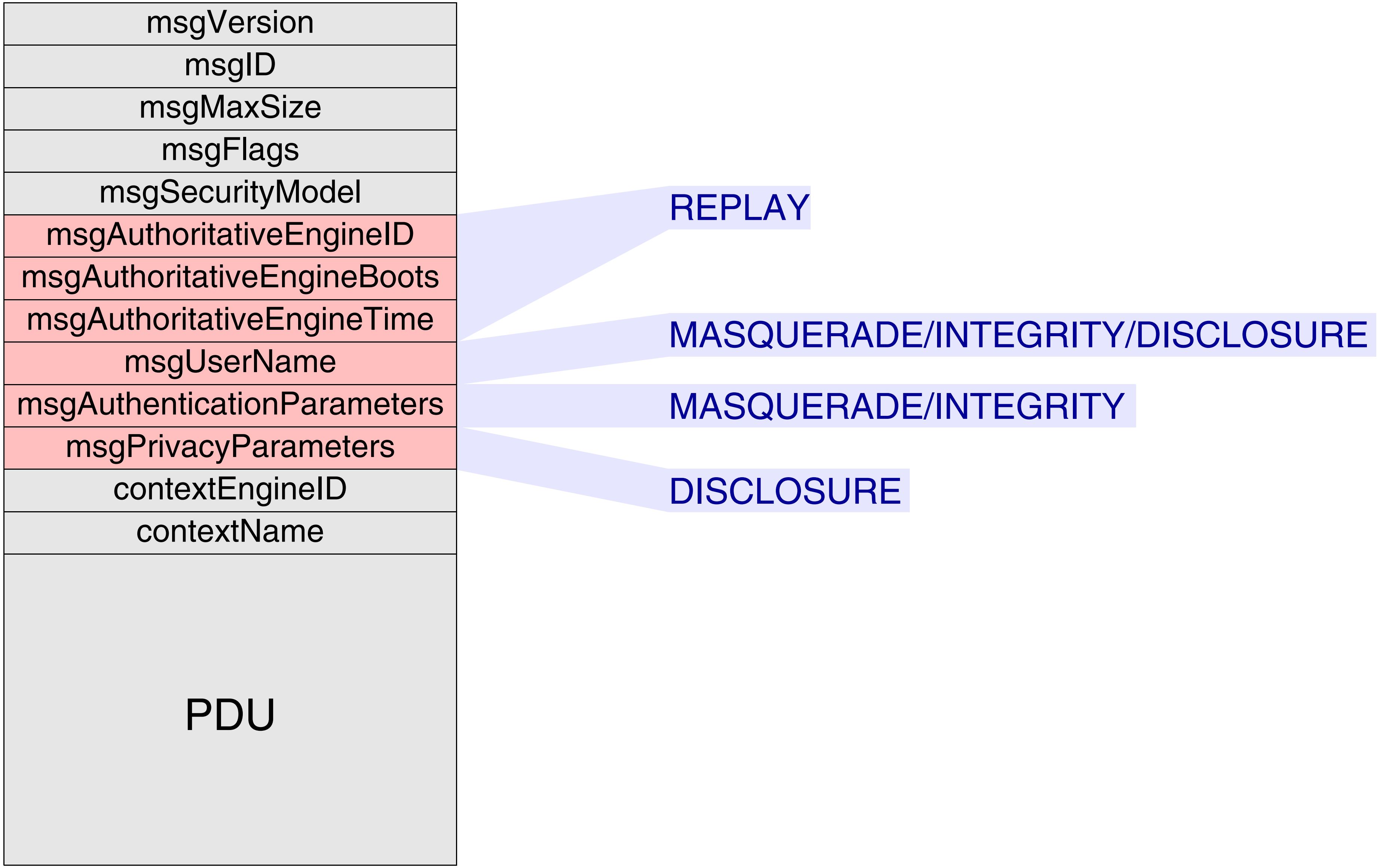
SECURE COMMUNICATION VERSUS ACCESS CONTROL



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	NO	
TRAFFIC ANALYSIS	NO	

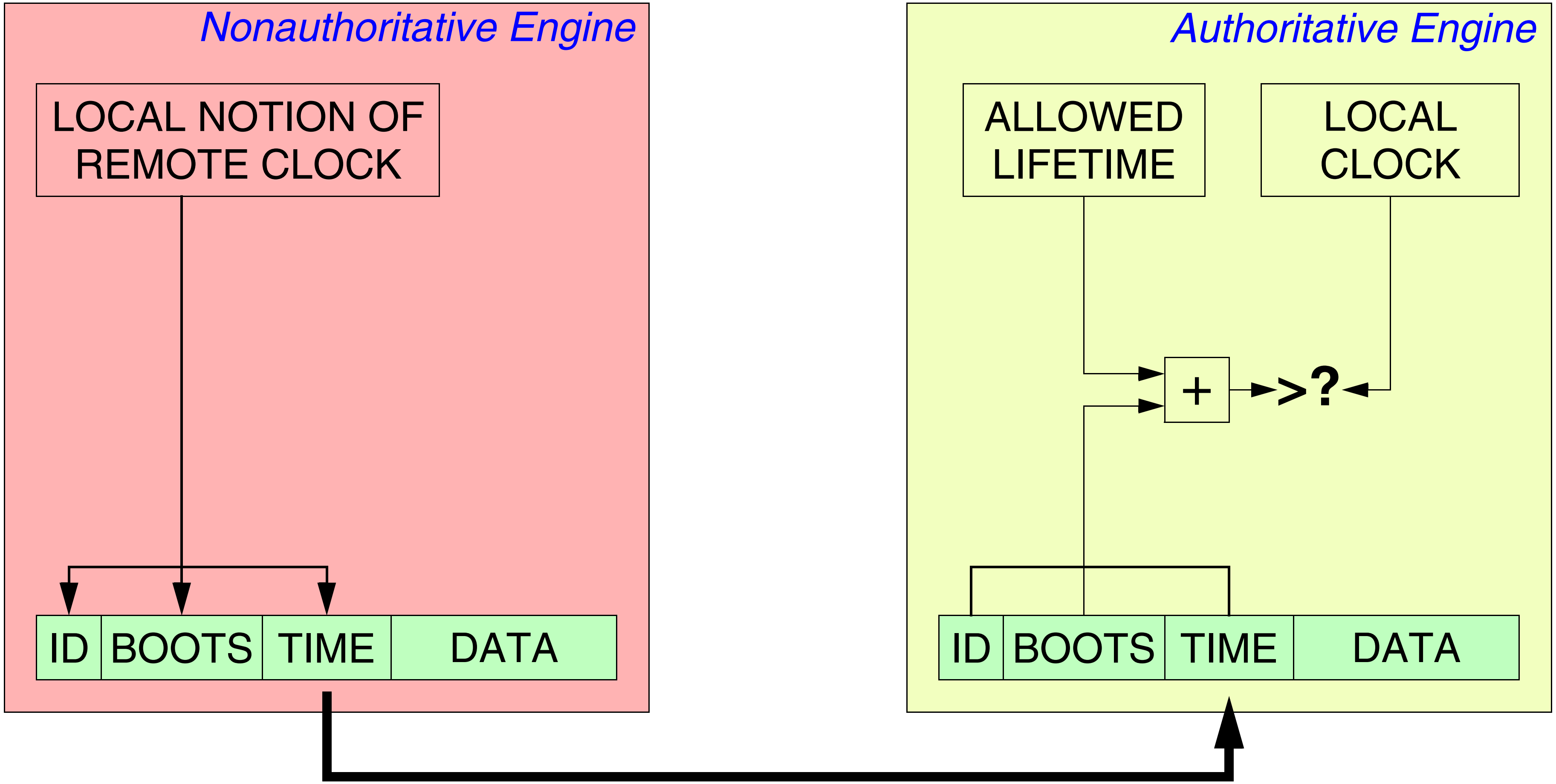
USM MESSAGE STRUCTURE



msgVersion
msgID
msgMaxSize
msgFlags
msgSecurityModel
msgAuthoritativeEngineID
msgAuthoritativeEngineBoots
msgAuthoritativeEngineTime
msgUserName
msgAuthenticationParameters
msgPrivacyParameters
contextEngineID
contextName
PDU

REPLAY
MASQUERADE/INTEGRITY/DISCLOSURE
MASQUERADE/INTEGRITY
DISCLOSURE

IDEA BEHIND REPLAY PROTECTION

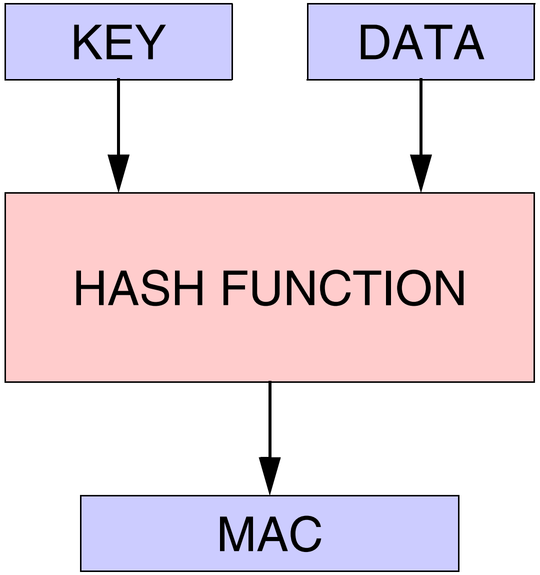


ID = msgAuthoritativeEngineID

BOOTS = msgAuthoritativeEngineBoots

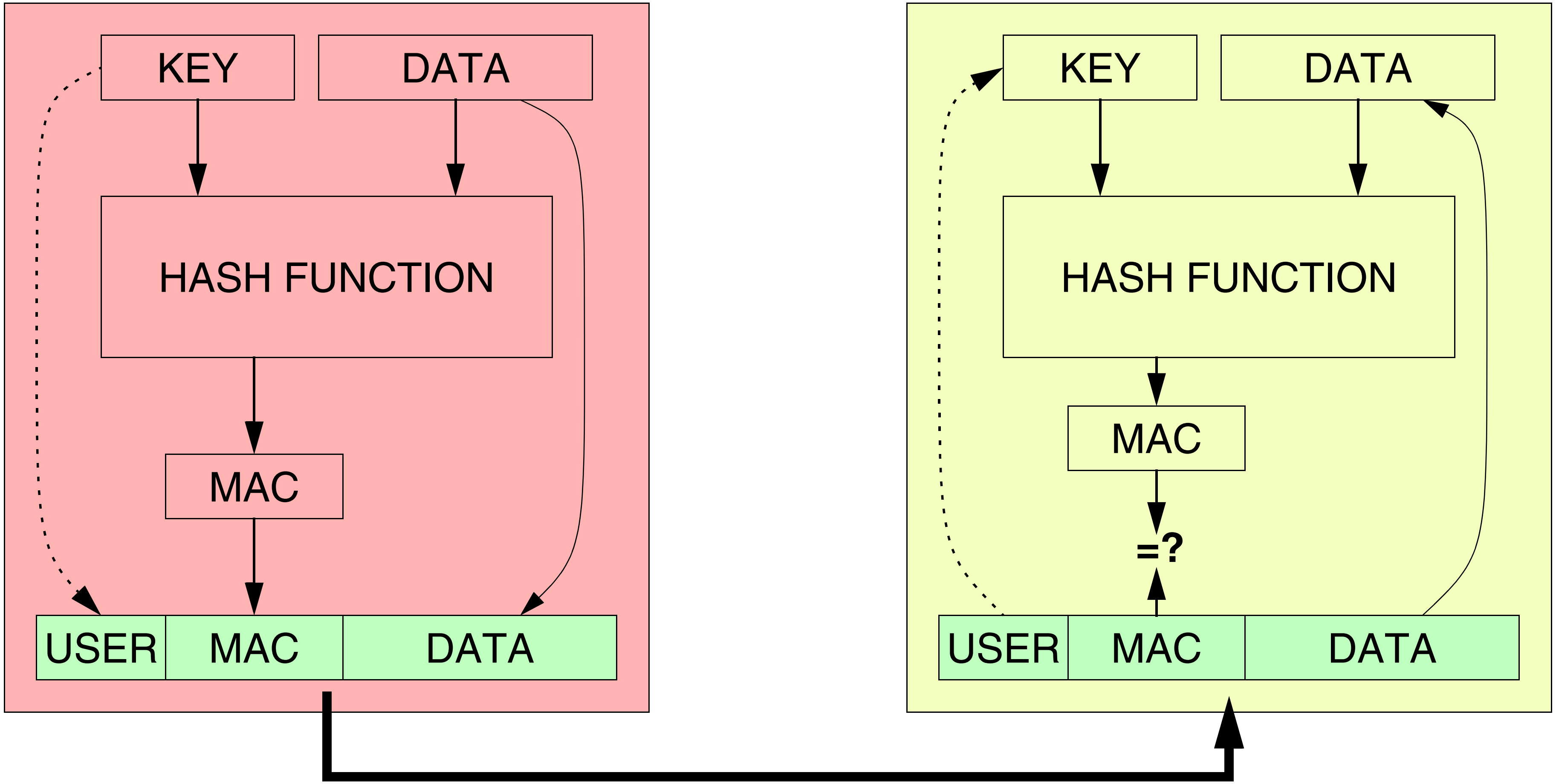
TIME = msgAuthoritativeEngineTime

IDEA BEHIND DATA INTEGRITY AND AUTHENTICATION



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

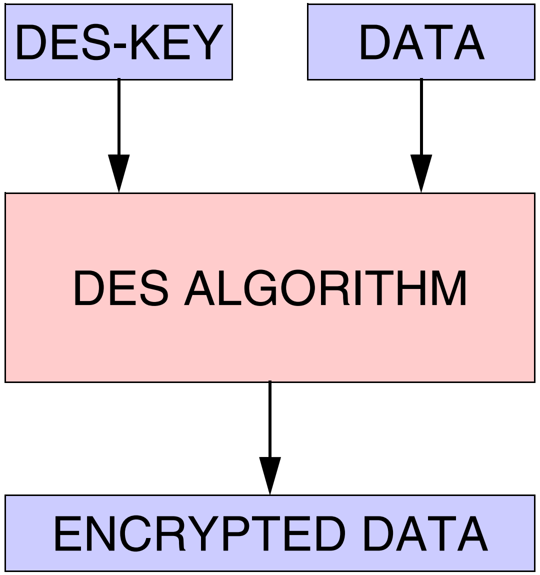
IDEA BEHIND AUTHENTICATION



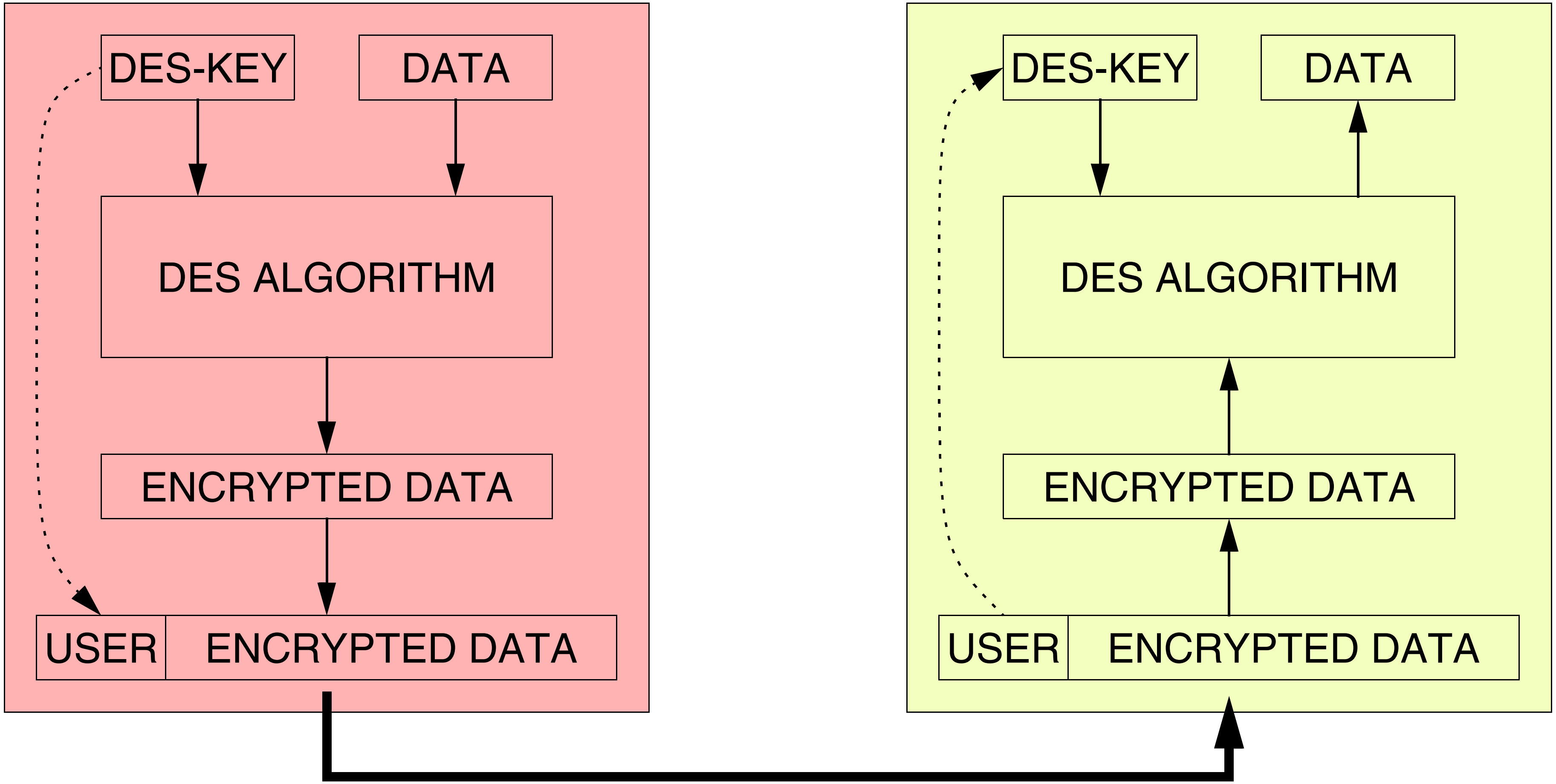
USER = msgUserName

MAC = msgAuthenticationParameters

IDEA BEHIND THE DATA CONFIDENTIALITY (DES)



IDEA BEHIND ENCRYPTION



USER = msgUserName

VIEW BASED ACCESS CONTROL MODEL

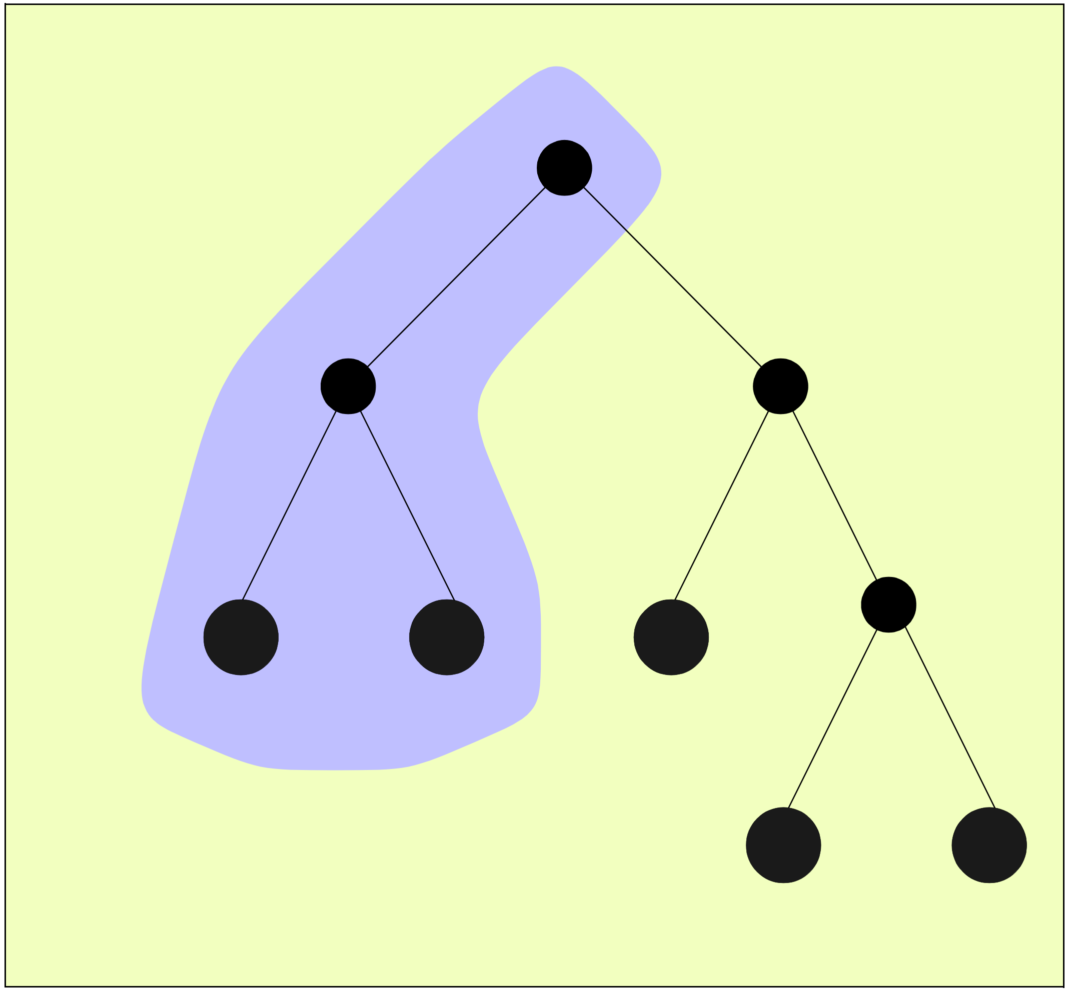
ACCESS CONTROL TABLE

MIB VIEWS

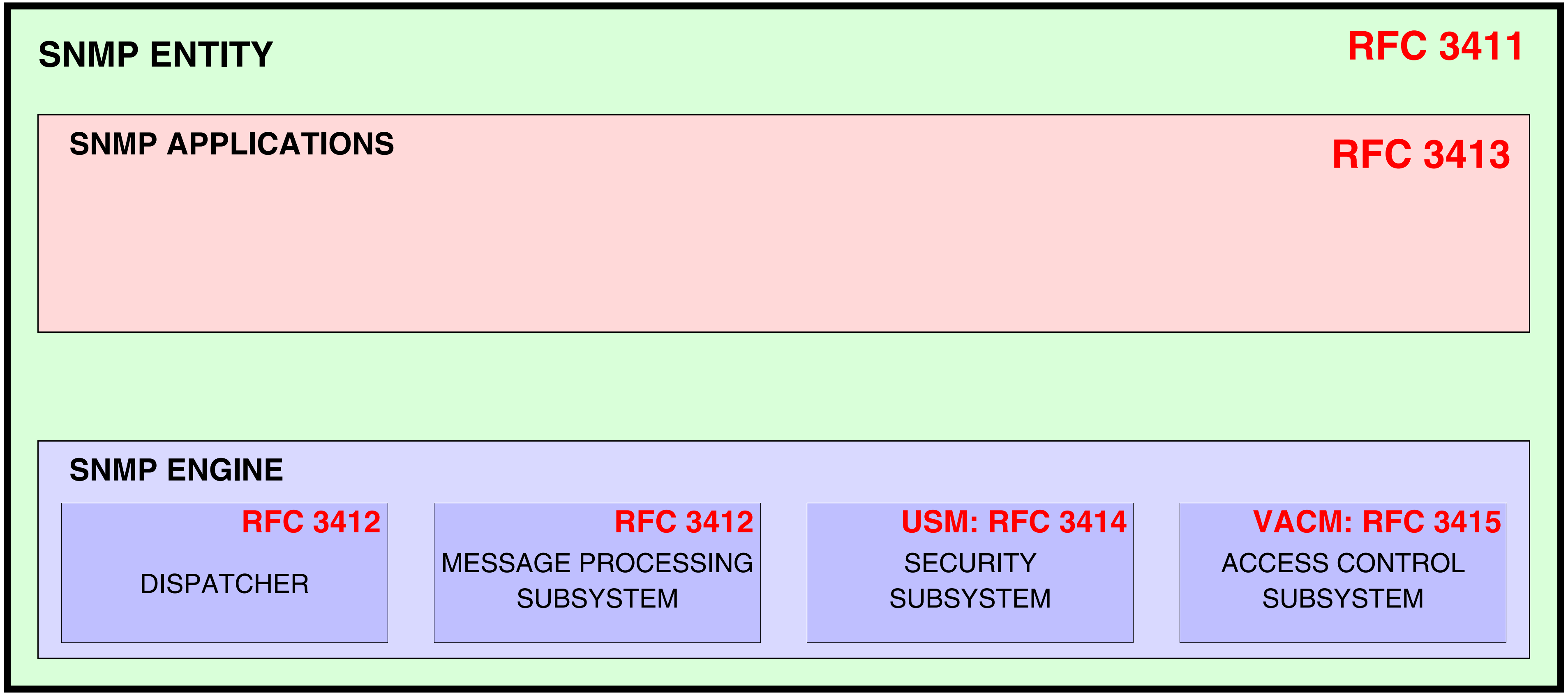
ACCESS CONTROL TABLES

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
●●●	●●●	●●●	●●●
●●●	●●●	●●●	●●●
●●●	●●●	●●●	●●●
●●●	●●●	●●●	●●●

MIB VIEWS



SNMPv3 RFCs



SNMP ENTITY

RFC 3411

SNMP APPLICATIONS

RFC 3413

SNMP ENGINE

RFC 3412

DISPATCHER

RFC 3412

MESSAGE PROCESSING SUBSYSTEM

USM: RFC 3414

SECURITY SUBSYSTEM

VACM: RFC 3415

ACCESS CONTROL SUBSYSTEM