SNMPv3

TUTORIAL T4 - PART 2
PRESENTED AT NOMS'2004
SEOUL, KOREA
19 APRIL 2004

AIKO PRAS
UNIVERSITY OF TWENTE
THE NETHERLANDS

pras@cs.utwente.nl
http://wwwhome.cs.utwente.nl/~pras

SNMPv3

OVERVIEW:

DESIGN DECISIONS

ARCHITECTURE

SNMP MESSAGE STRUCTURE

SECURE COMMUNICATION
- USER SECURITY MODEL (USM)

ACCESS CONTROL
- VIEW BASED ACCESS CONTROL MODEL (VACM)

RFCs

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

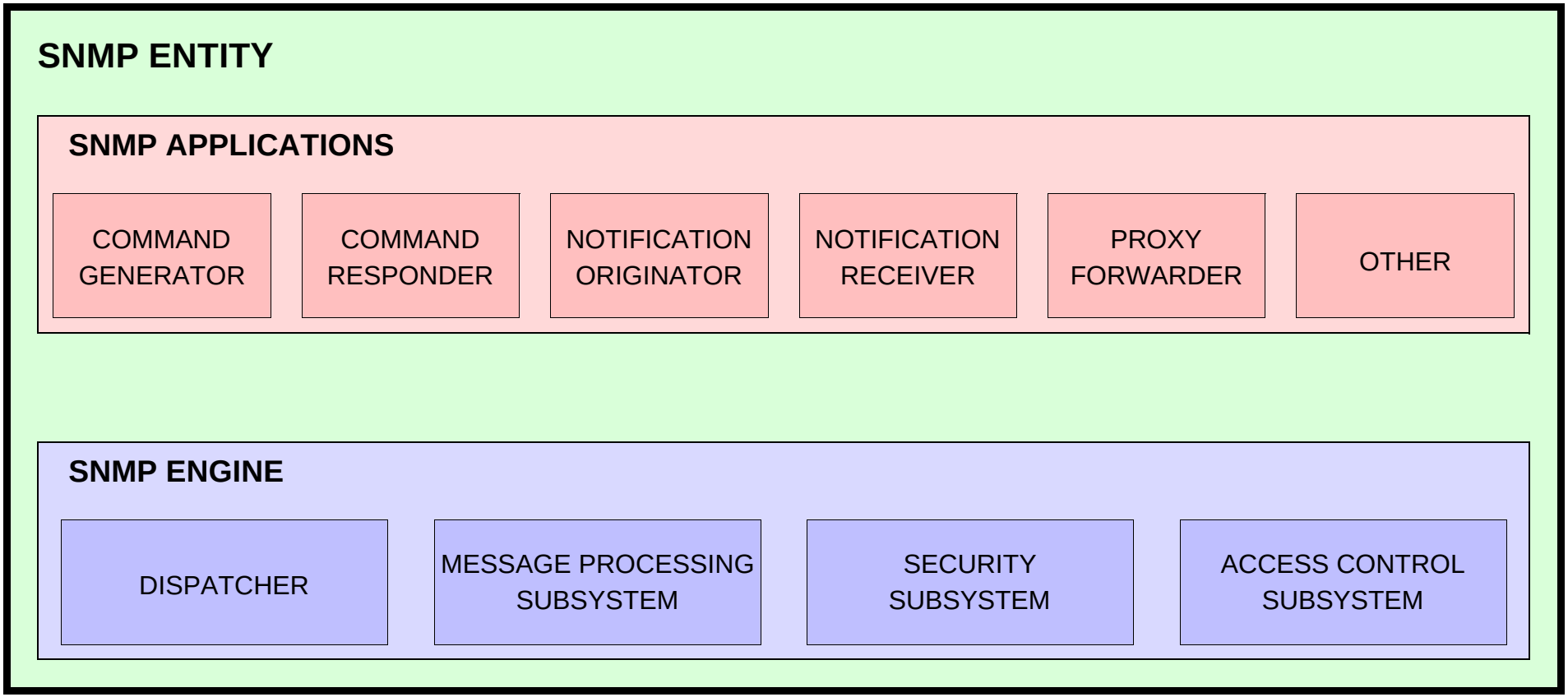
KEEP SNMP AS SIMPLE AS POSSIBLE

ALLOW FOR MINIMAL IMPLEMENTATIONS

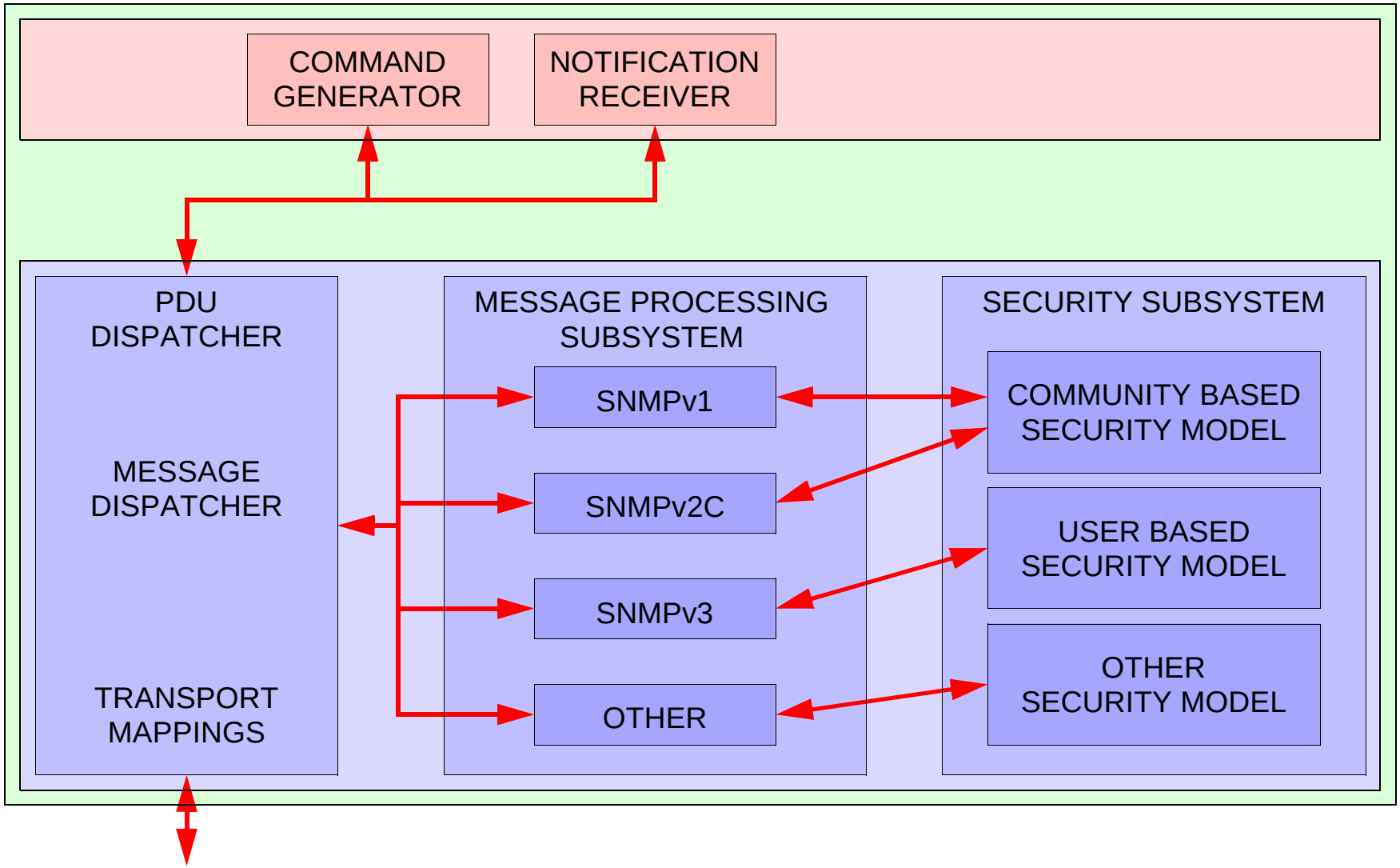
SUPPORT ALSO THE MORE COMPLEX FEATURES,
WHICH ARE REQUIRED IN LARGE NETWORKS

RE-USE EXISTING SPECIFICATIONS, WHENEVER POSSIBLE

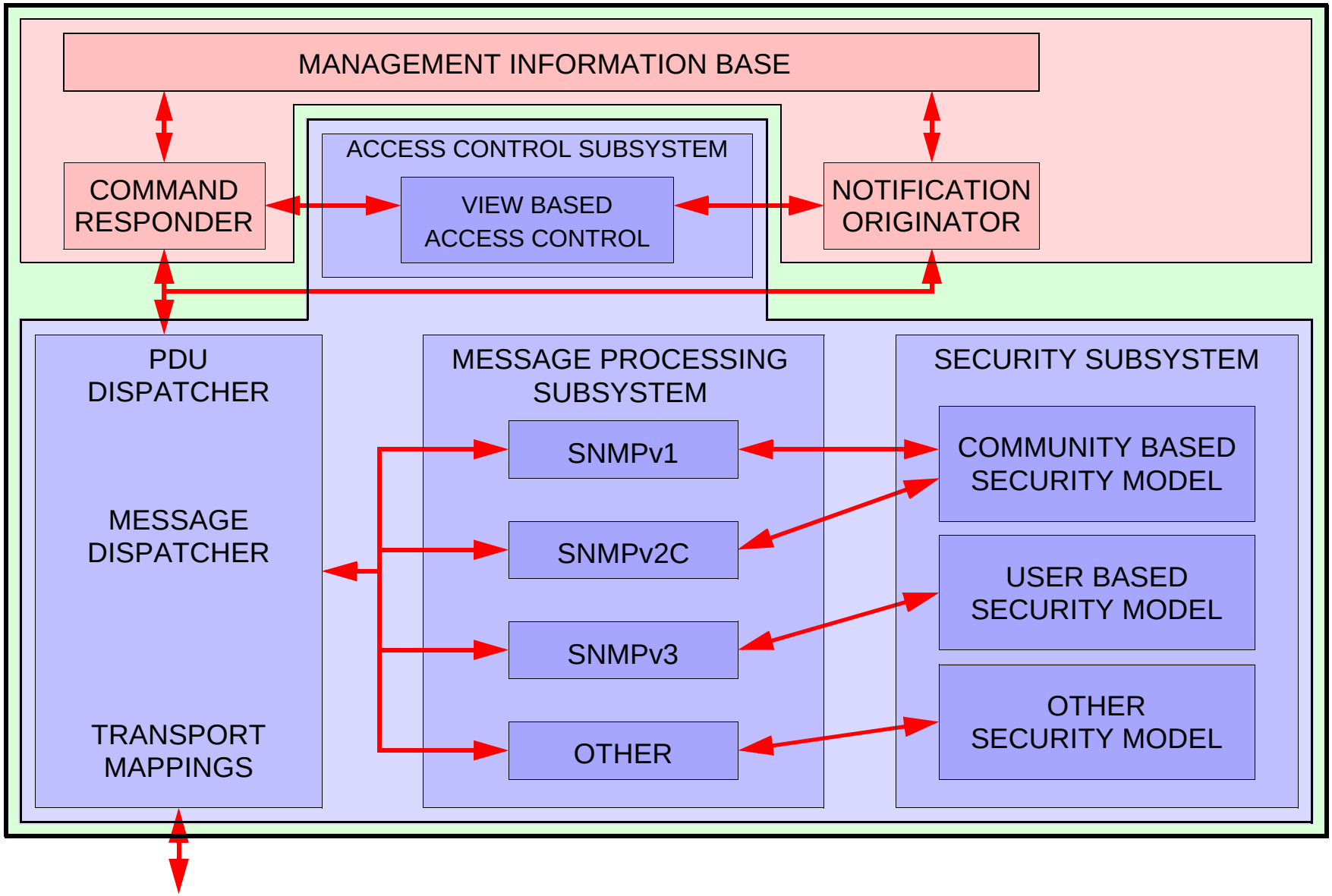
SNMPv3 ARCHITECTURE



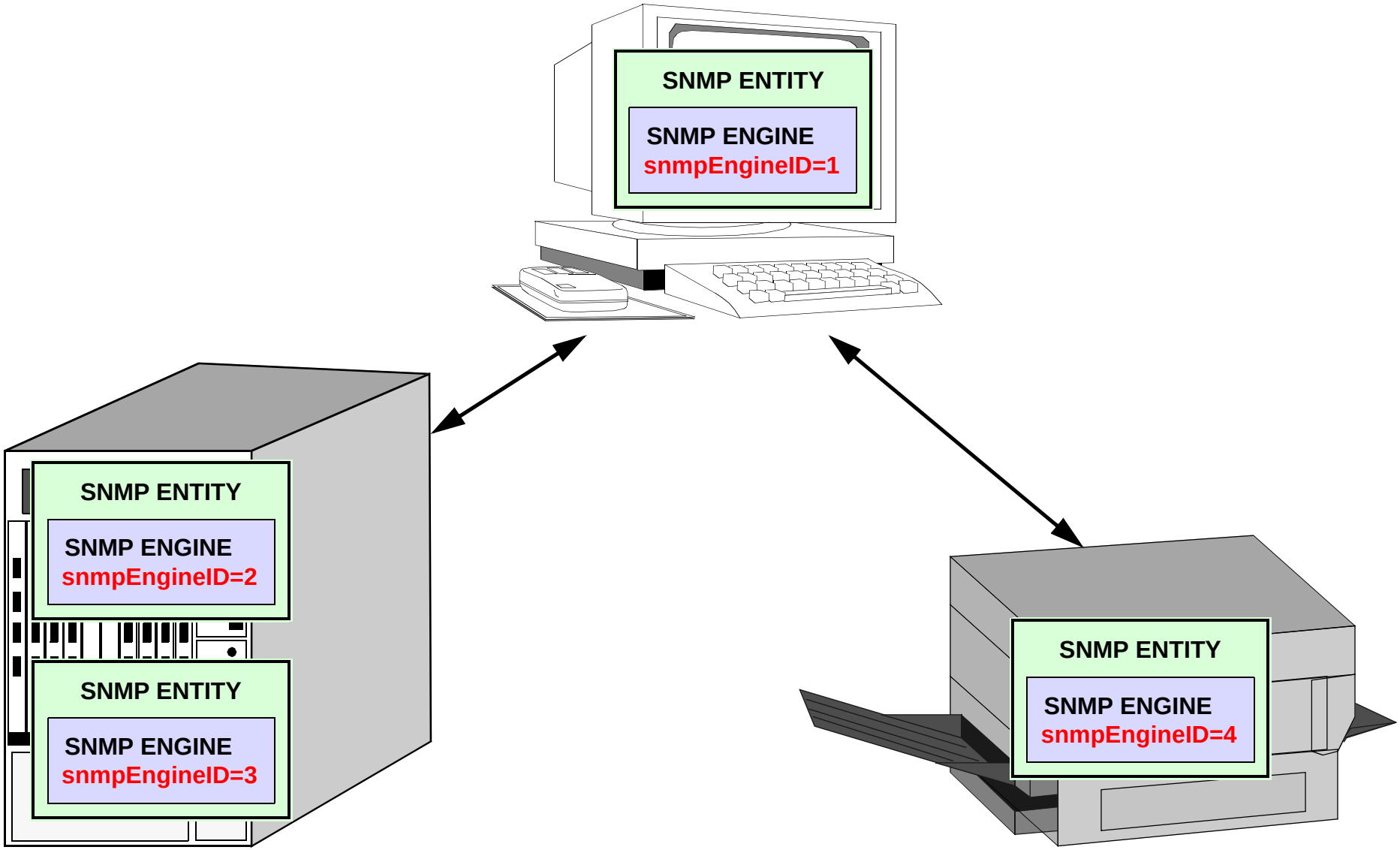
SNMPv3 ARCHITECTURE: MANAGER



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

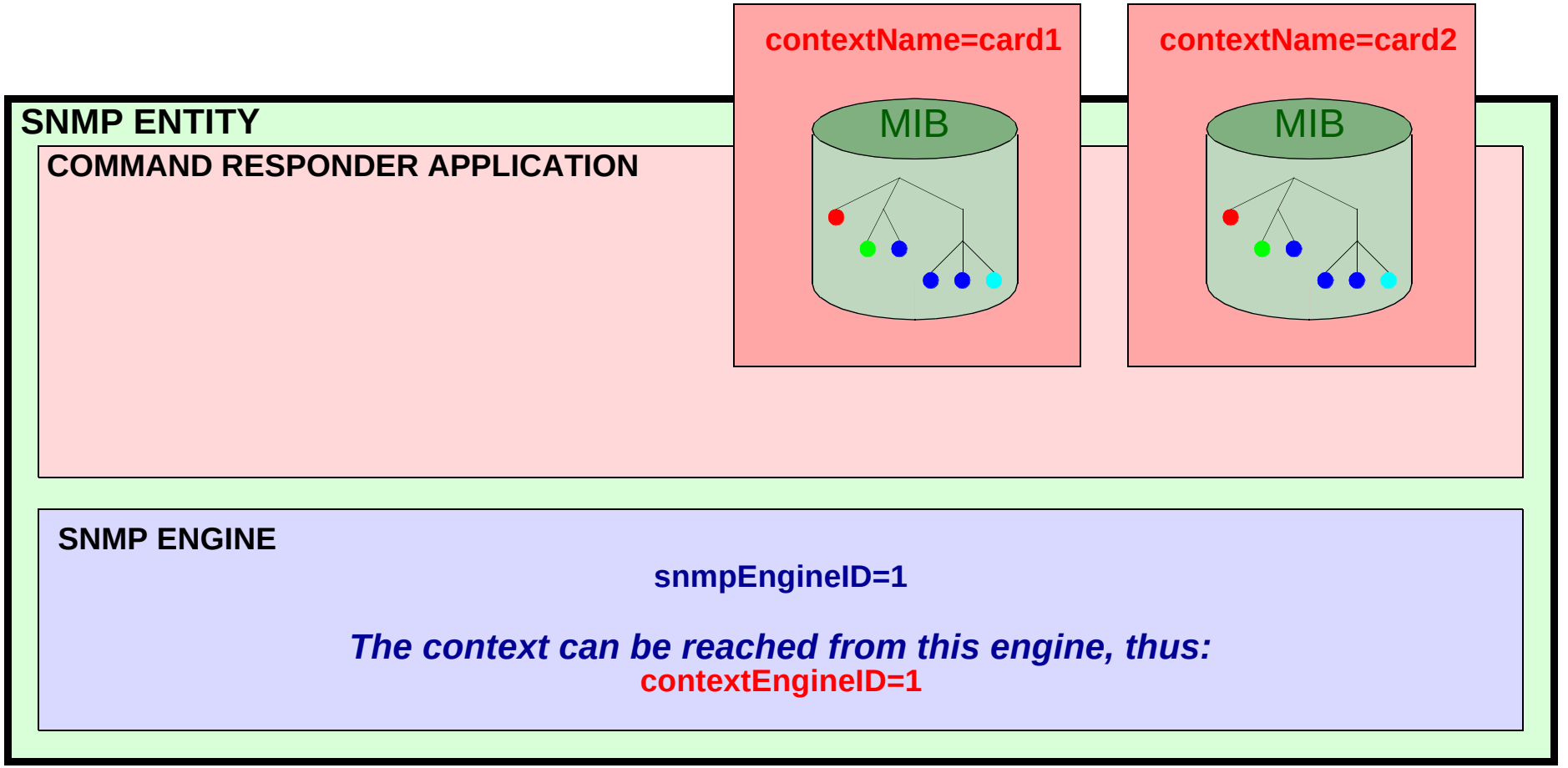
TEXTUAL CONVENTION DEFINED IN SNMP FRAMEWORK MIB

CONCEPTS: snmpEngineID

THE TERM EngineID IS FREQUENTLY USED

SnmpEngineID	The textual convention.
snmpEngineID	The identifier of an SNMP engine.
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 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 communi-cate.
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



MODULES OF THE SNMPv3 ARCHITECTURE

DISPATCHER AND MESSAGE PROCESSING MODULE

- SNMPv3 MESSAGE STRUCTURE
- snmpMPDMIB
- RFC 3412

APPLICATIONS

- snmpTargetMIB
- snmpNotificationMIB
- snmpProxyMIB
- RFC 3413

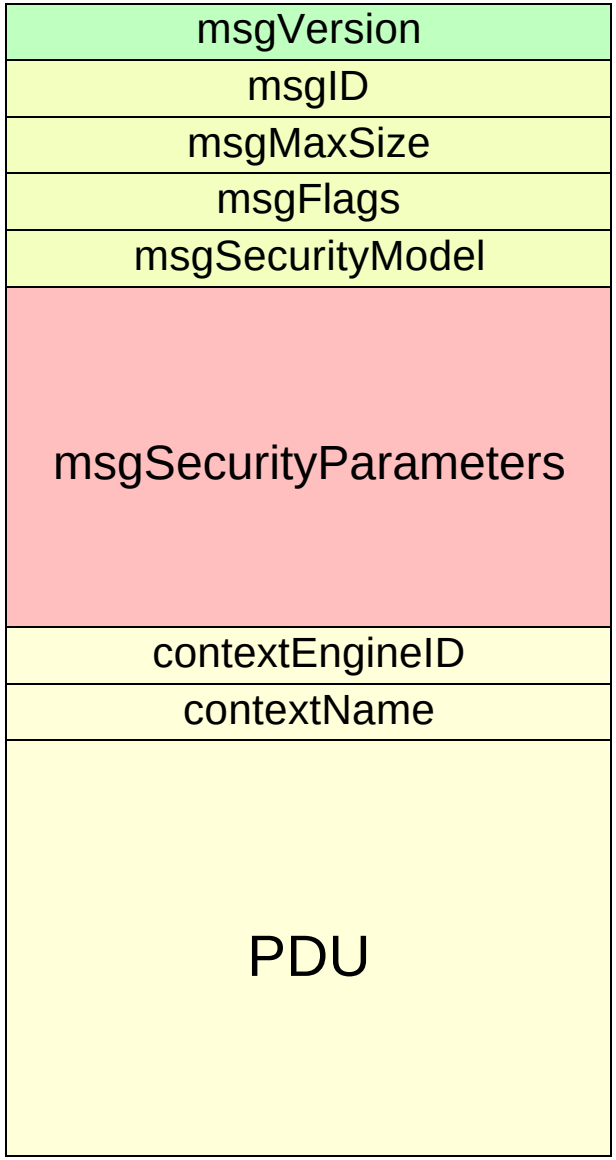
SECURITY SUBSYSTEM

- USER BASED SECURITY MODEL
- snmpUsmMIB
- RFC 3414

ACCESS CONTROL SUBSYSTEM

- VIEW BASED ACCESS CONTROL MODEL
- snmpVacmMIB
- RFC 3415

SNMPv3 MESSAGE STRUCTURE



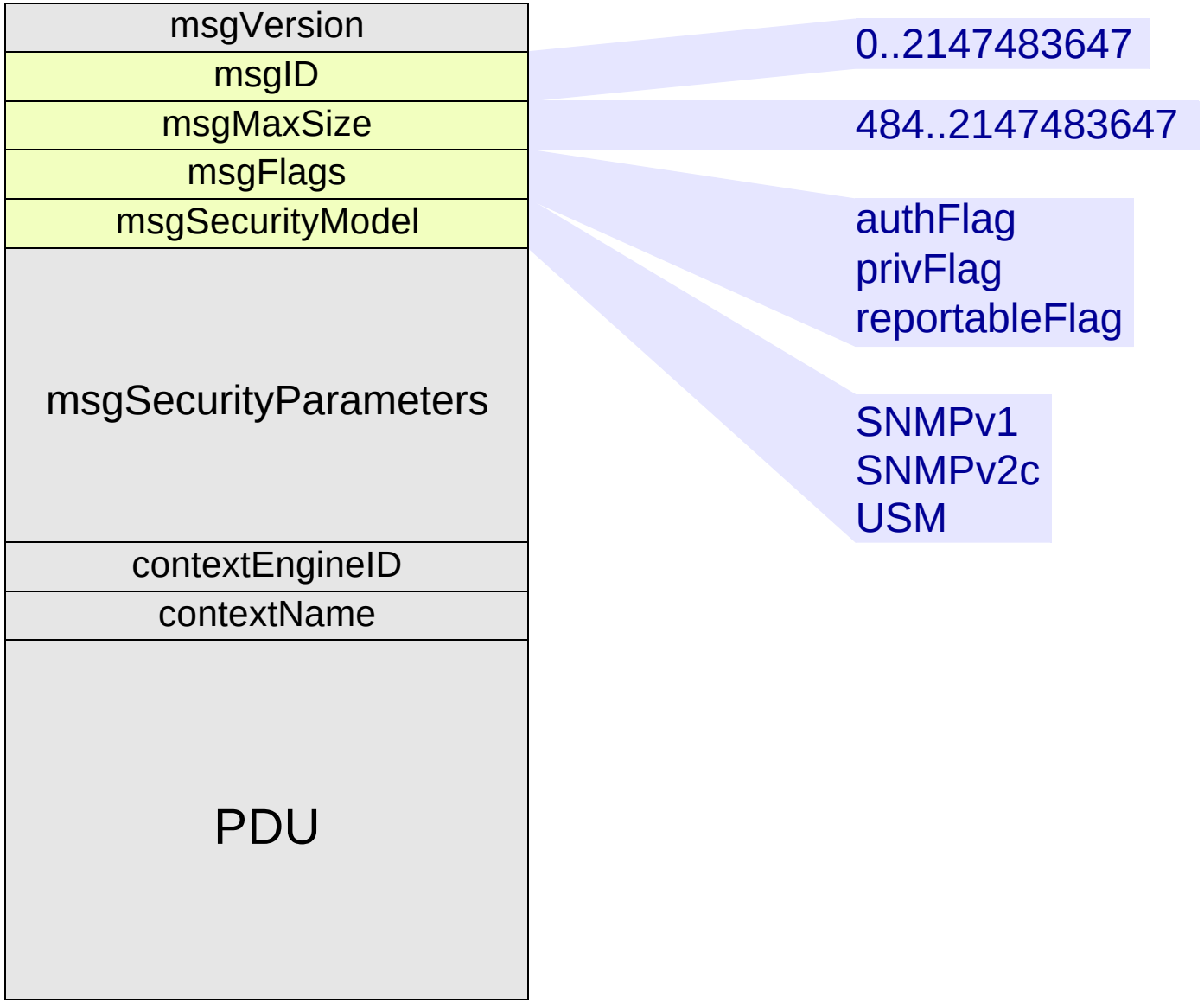
USED BY MESSAGE PROCESSING SUBSYSTEM

USED BY SNMPv3 PROCESSING MODULE

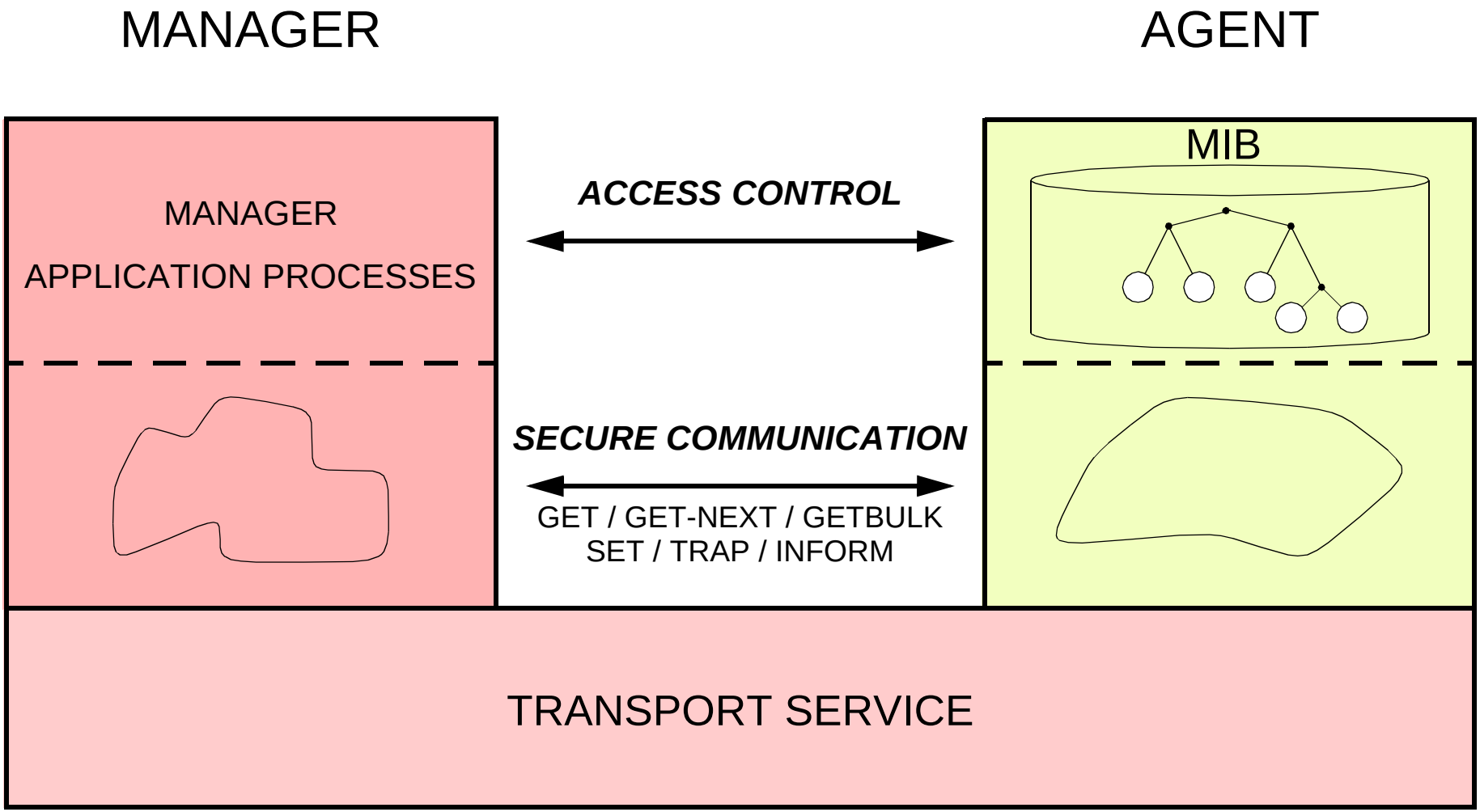
USED BY SECURITY SUBSYSTEM

USED BY ACCESS CONTROL SUBSYSTEM
AND APPLICATIONS

SNMPv3 PROCESSING MODULE PARAMETERS



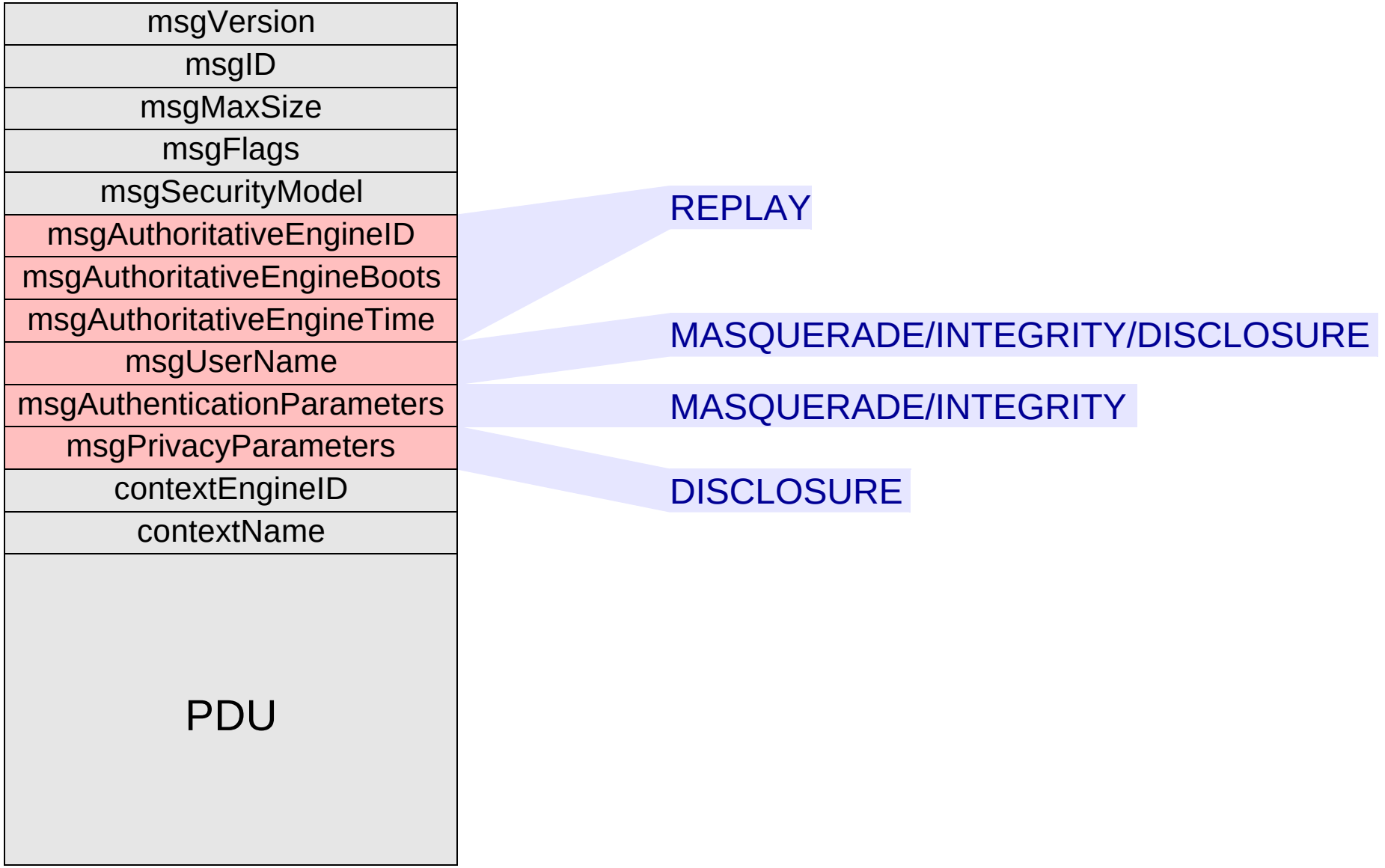
SECURE COMMUNICATION VERSUS ACCESS CONTROL



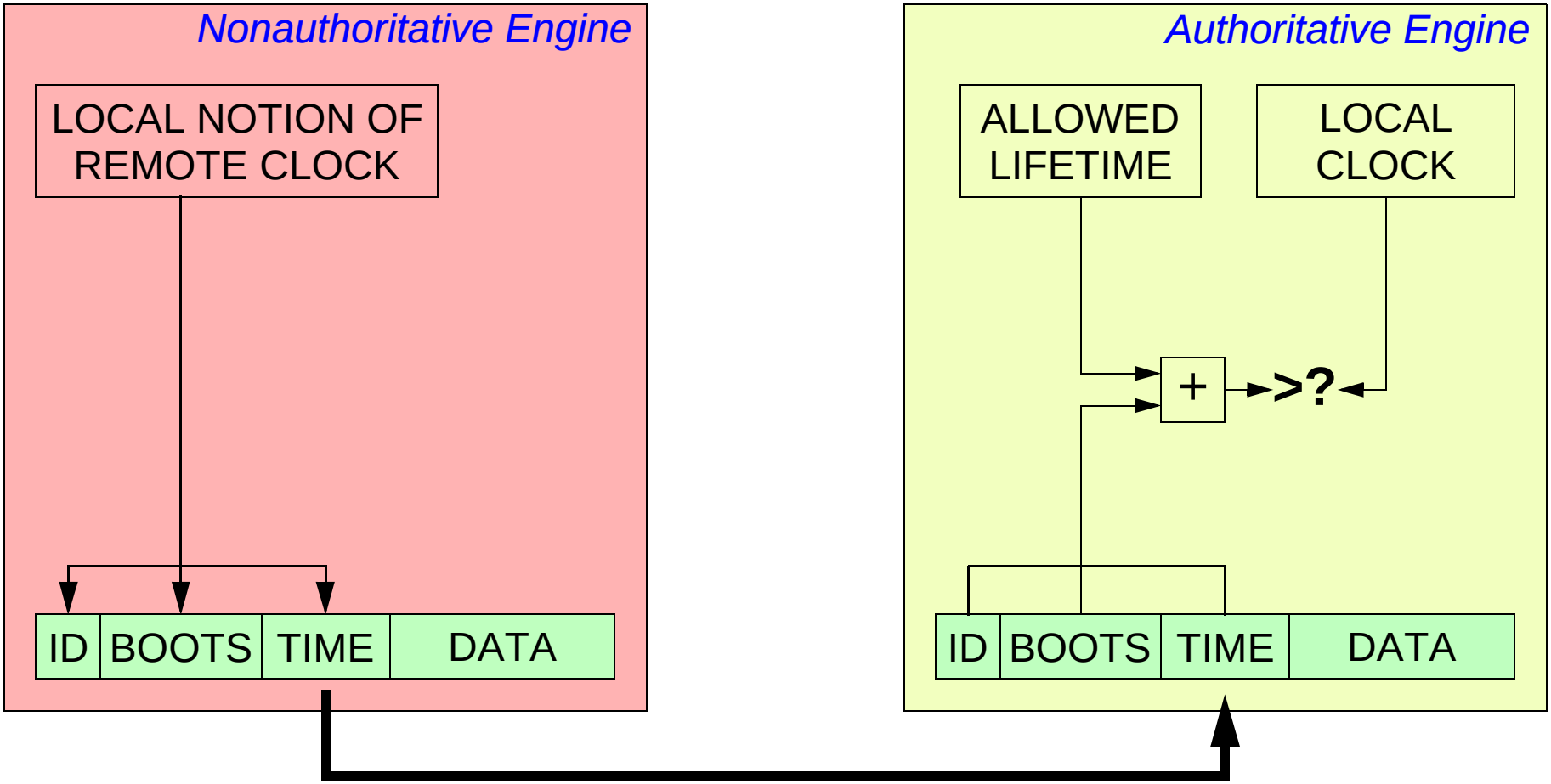
USM: SECURITY THREATS

THREAT	ADDRESSED?	MECHANISM
REPLAY	YES	TIME STAMP
MASQUERADE	YES	MD5 / SHA-1
INTEGRITY	YES	(MD5 / SHA-1)
DISCLOSURE	YES	DES
DENIAL OF SERVICE	NO	
TRAFFIC ANALYSIS	NO	

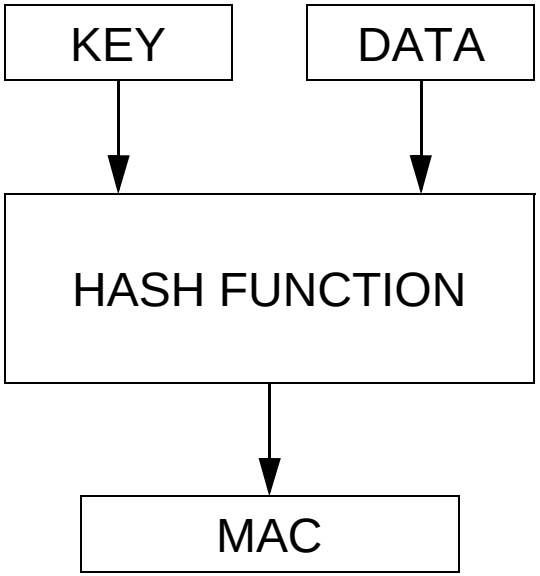
USM MESSAGE STRUCTURE



IDEA BEHIND REPLAY PROTECTION

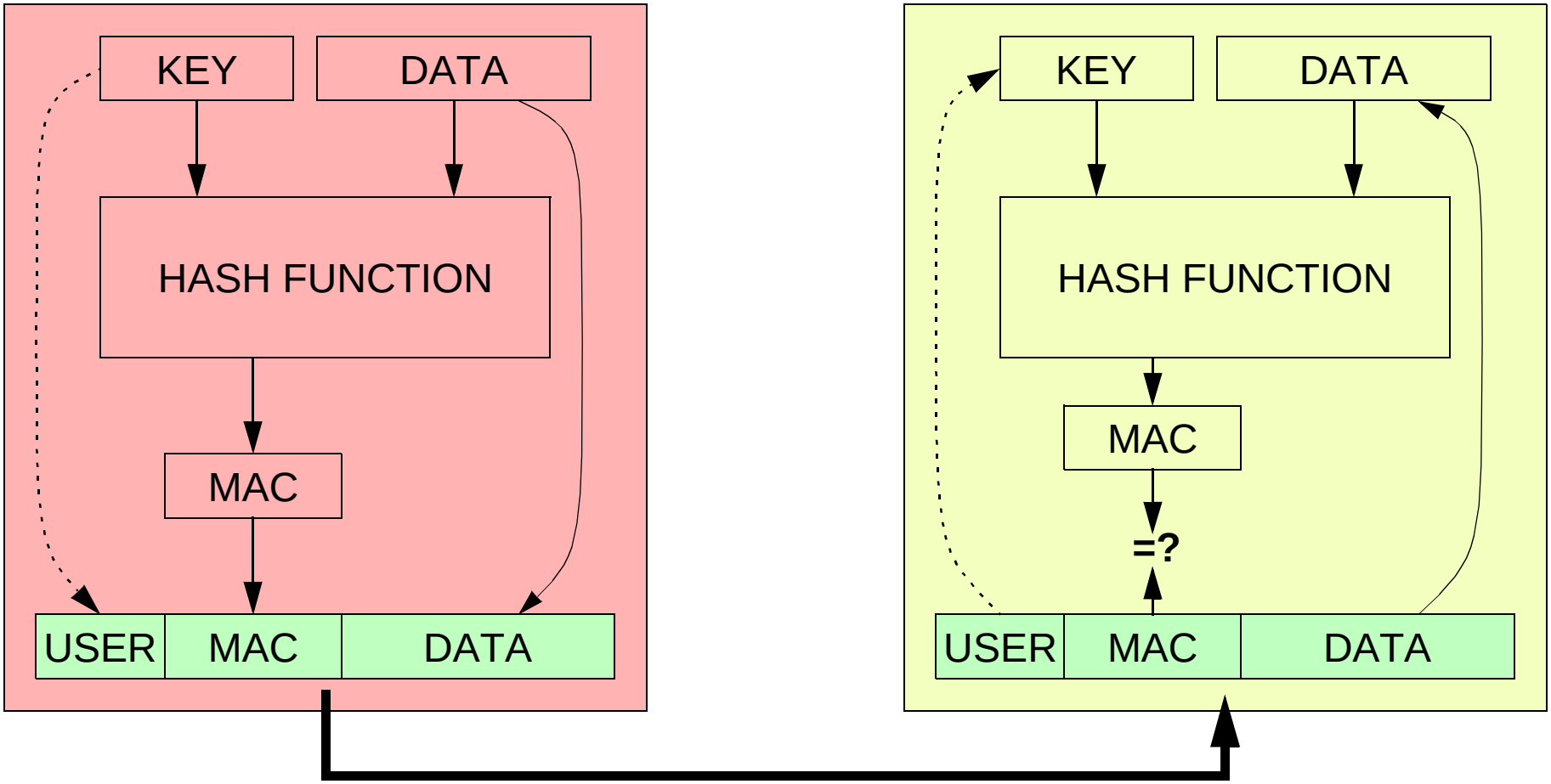


IDEA BEHIND DATA INTEGRITY AND AUTHENTICATION

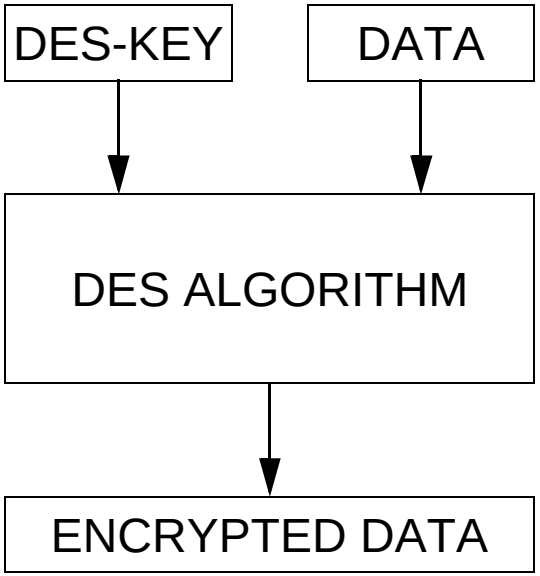


ADD THE MESSAGE AUTHENTICATION CODE (MAC) TO THE DATA
AND SEND THE RESULT

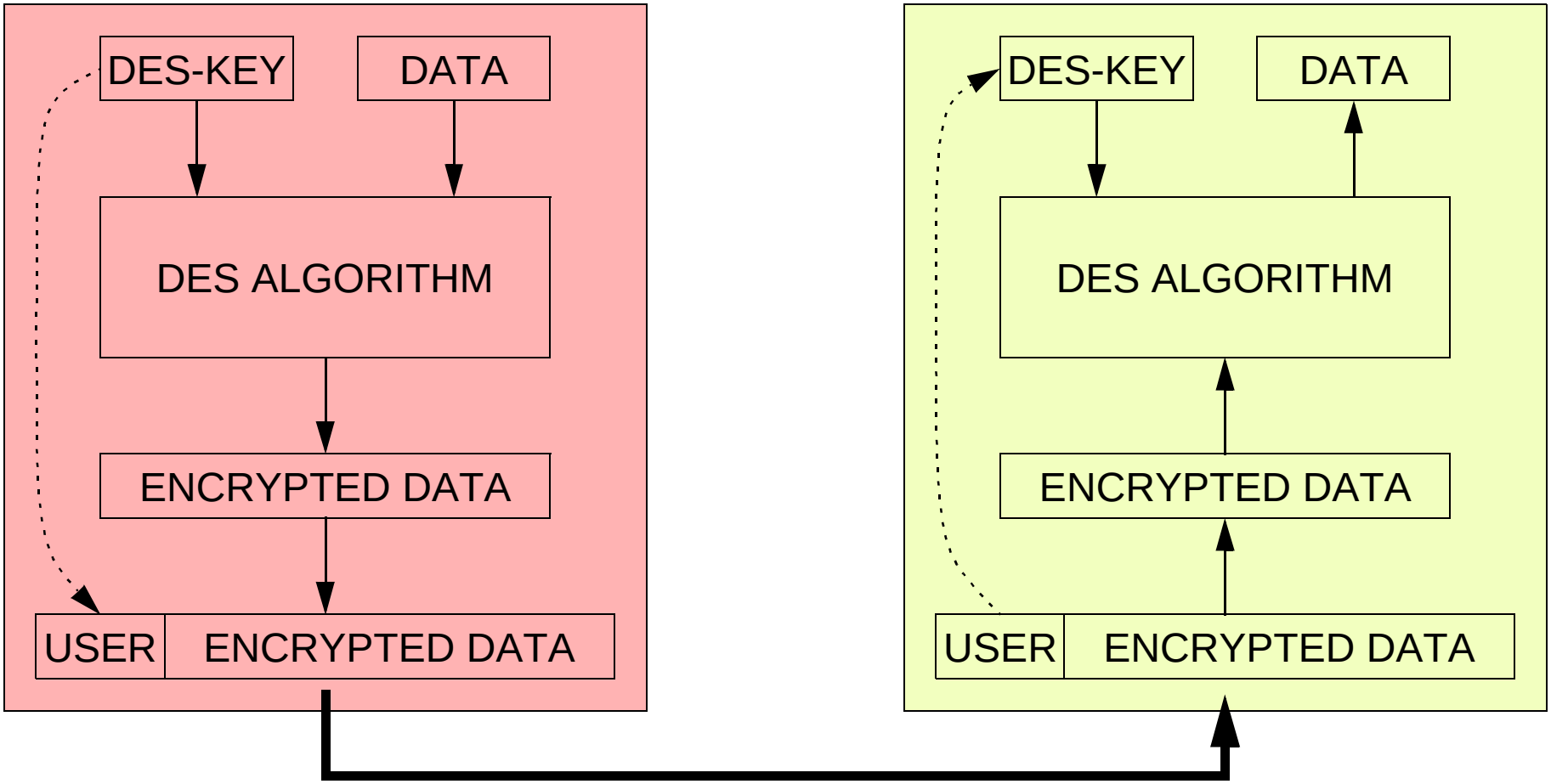
IDEA BEHIND AUTHENTICATION



IDEA BEHIND THE DATA CONFIDENTIALITY (DES)



IDEA BEHIND ENCRYPTION



VIEW BASED ACCESS CONTROL MODEL

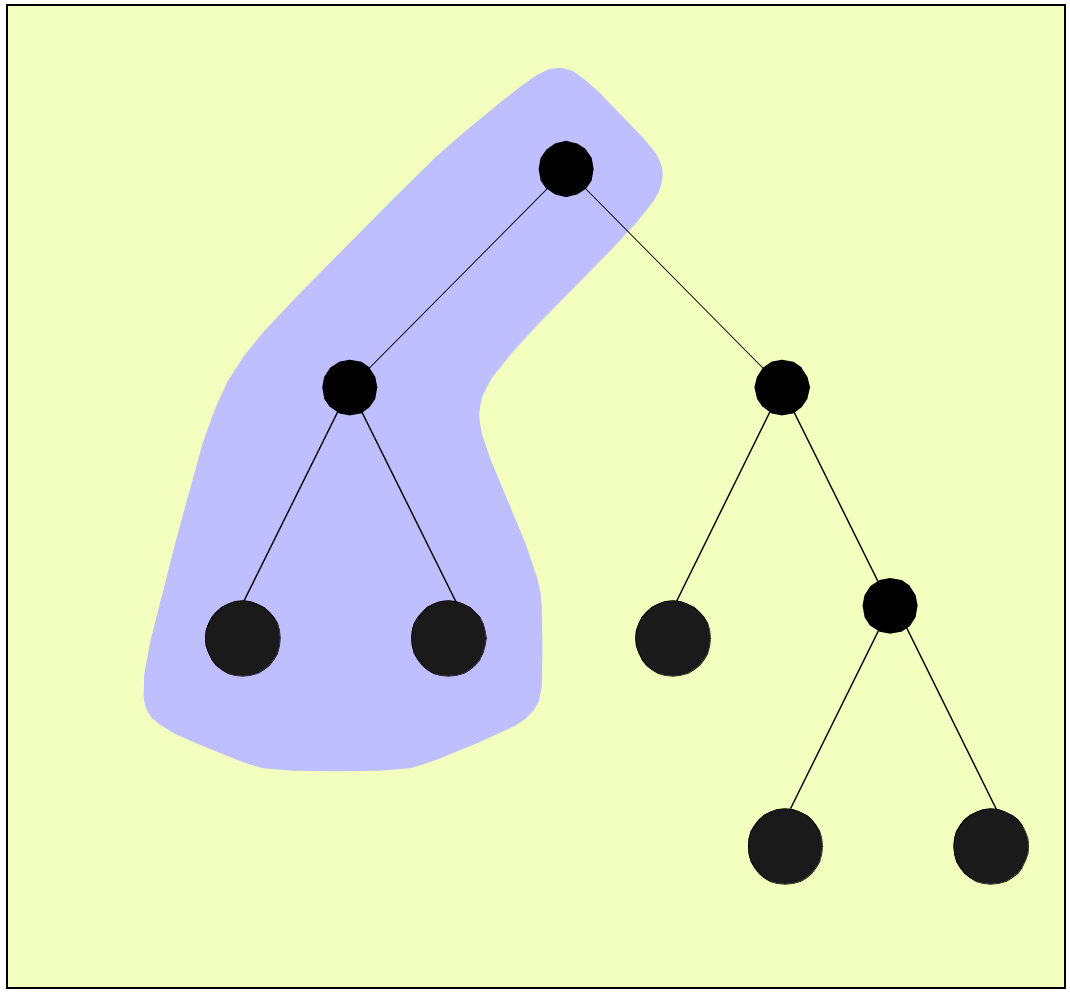
ACCESS CONTROL TABLE

MIB VIEWS

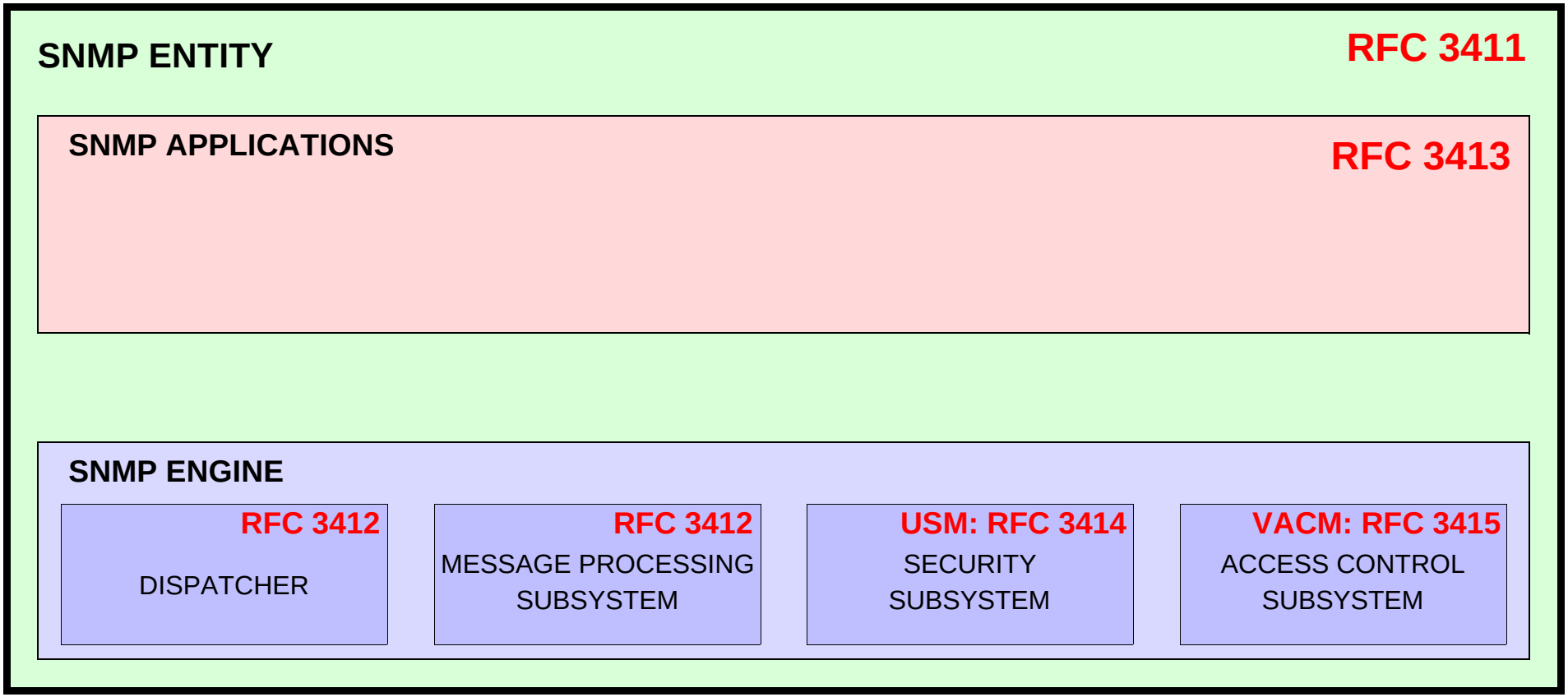
ACCESS CONTROL TABLES

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