# Internet Infrastructure Security Panel

Symposium on Network and Distributed System Security

February 10, 1997

# Internet Infrastructure Security

- Panelists
  - Steve Bellovin - AT&T Research
  - Olafur Gudmundsson - TIS
  - Paul Lambert - Oracle
  - Russ Mundy - TIS

# What Gives (or Doesn't Give) the Internet Infrastructure Security?

- Interaction Between "Internet Pieces"
- Dominated By Protocols - Examples
  - Internet Protocol
  - Routing
  - Name Service
  - Network Management
  - etc, etc, etc,
- Software Implementing & Executing the Protocols

# Internet Infrastructure Security Requires (at least)

- Support for Security Mechanisms in Protocols
  - Standards are Crucial
- Implementation and Use of Security Mechanisms in Software of “Internet Pieces”
- Policies and Correct Usage

# Are All Internet Related Protocols Infrastructure? (one view)

- Infrastructure
  - OSPF, BGP, (add your favorite routing protocol(s))
  - DNS
  - ARP
  - SNMP
  - IP
  - ISAKMP/Oakley
  - DHCP
- Probably Not??
  - TCP
  - HTTP
  - FTP
  - Telnet
  - ....

# Are All Internet Related Protocols Infrastructure? (another view)

- Everything Needed for MY Job

  An Example:

  – Email is Infrastructure to end users

  – TCP is Infrastructure to Email Developers

  – IP is Infrastructure to Multicast Developers and Users

# Internet Infrastructure Security How Much Is There??

- Some Today BUT More is Coming
- Emerging Protocol Standards
- Experimental & Reference Software Implementations

  Examples

  – IPSEC / ISAKMP / OAKLEY

  – DNSSEC

  – SNMP-NG

# SNMP - Next Generation

Symposium on Network and
Distributed System Security

February 10, 1997

# SNMP ADVISORY TEAM Background

- Chartered After 36th IETF
- Security and Administrative Framework Evolution for SNMP Advisory Team (AKA **Advisory Team**)
- Principal Goal: Identify Single Approach for SNMP-NG That Can Move to Open Working Group

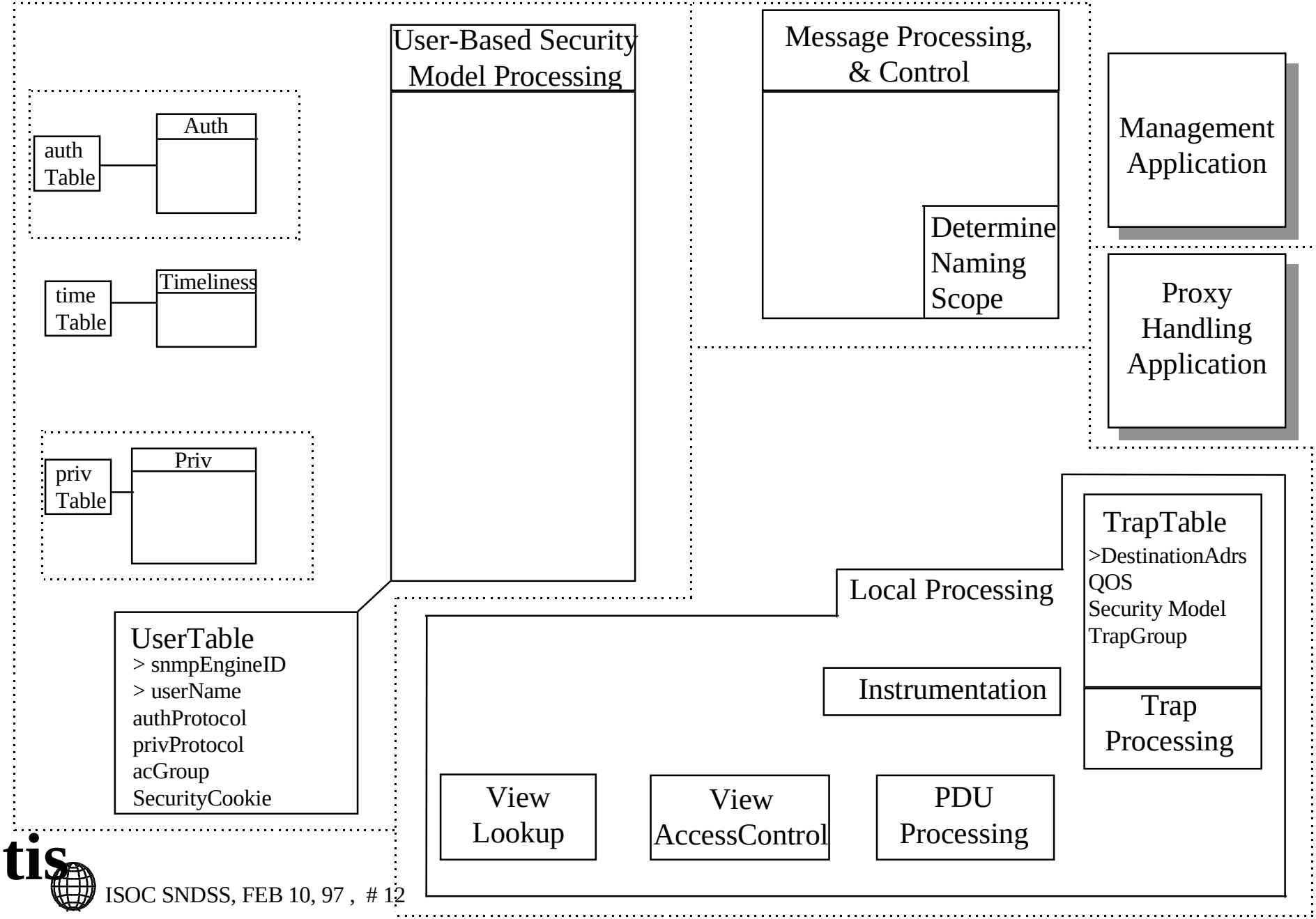
# SNMP ADVISORY TEAM Approach Highlights

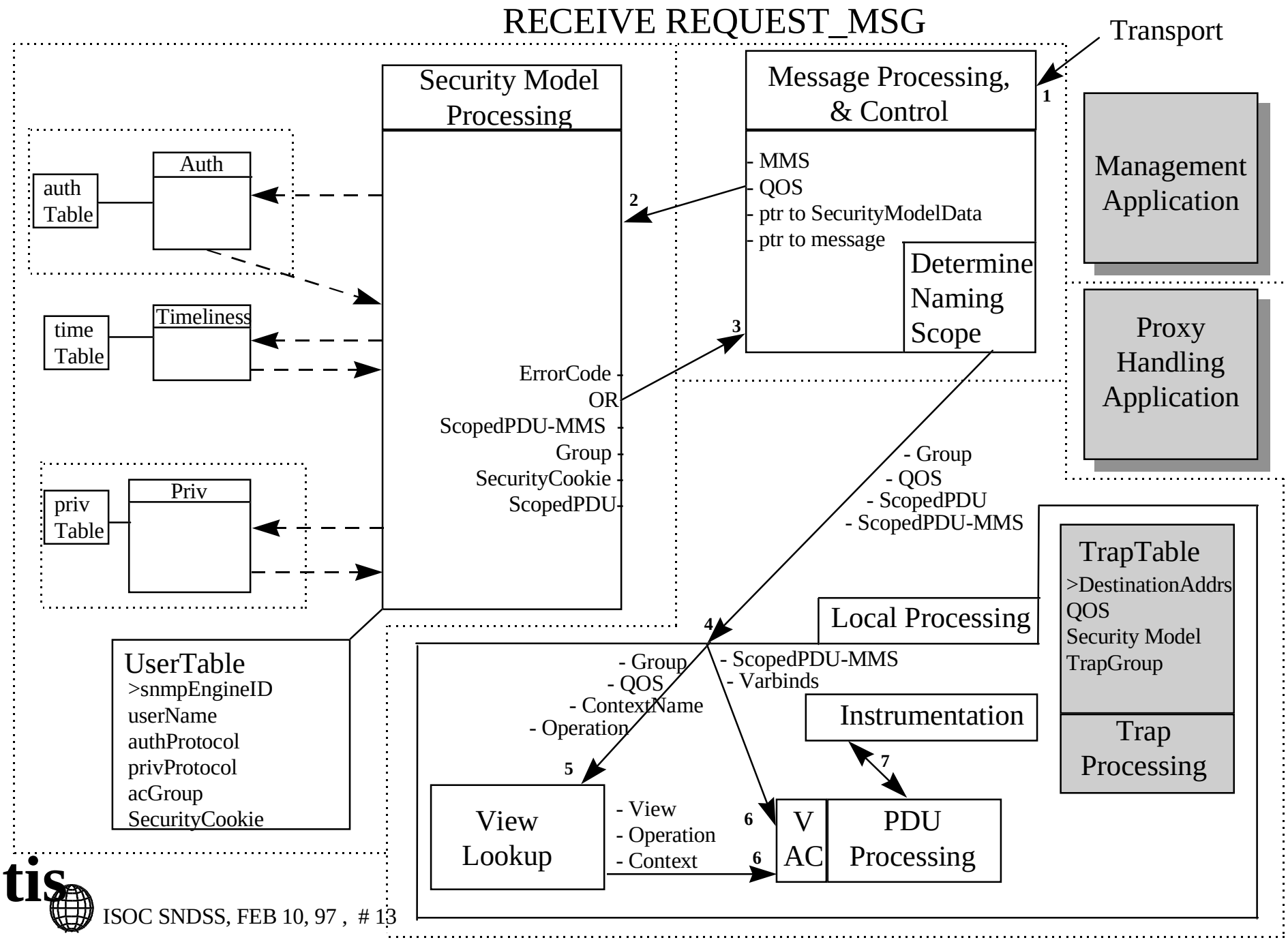
- Used As Much From Existing Technology Base as Practical
- Constrained to Requirements of Existing v2* & USEC Proposals
- Did Not Choose One “Winner”
- Identified a Set of Modules and Interfaces that Perform Required Functions

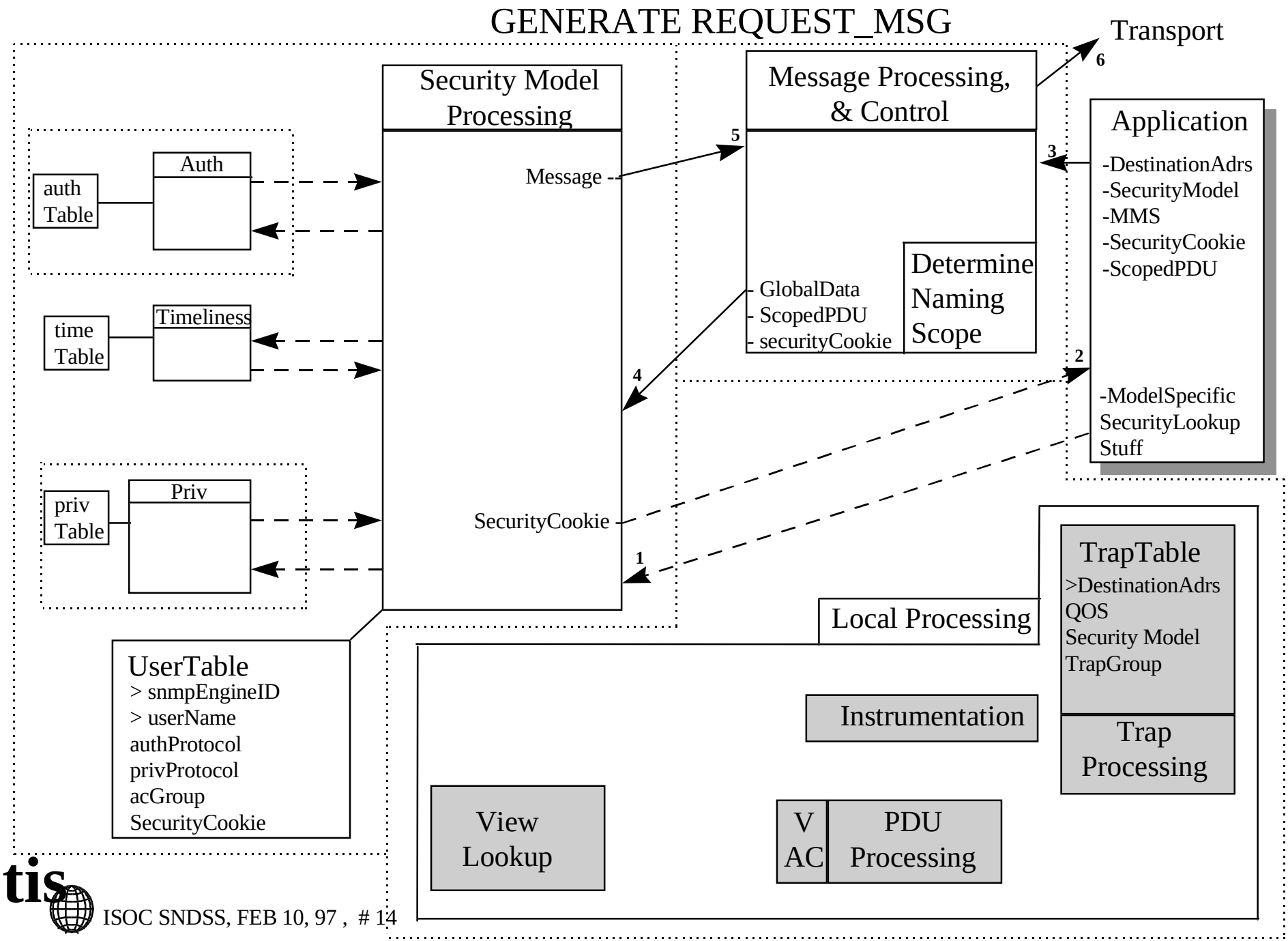
# SNMP ADVISORY TEAM Approach Highlights (cont)

- Approach Emphasizes Modularity
- Documents Expected to Follow the Modularity
- It Is Not Necessarily Expected that Implementations Will Choose To Follow Strict Modularity
- Currently Defined Security Services (Integrity & Confidentiality) Are Sufficient

# USER-BASED SNMP-NG MODULES & SUB-MODULES




RECEIVE REQUEST_MSG
Transport
Security Model Processing
Message Processing, & Control
1
- MMS
- QOS
- ptr to SecurityModelData
- ptr to message
Determine Naming Scope
Management Application
Proxy Handling Application
2
3
Auth
auth Table
Timeliness
time Table
Priv
priv Table
ErrorCode
OR
ScopedPDU-MMS
Group
SecurityCookie
ScopedPDU
- Group
- QOS
- ScopedPDU
- ScopedPDU-MMS
TrapTable
>DestinationAddrs
QOS
Security Model
TrapGroup
Trap Processing
Local Processing
4
UserTable
>snmpEngineID
userName
authProtocol
privProtocol
acGroup
SecurityCookie
- Group
- QOS
- ContextName
- Operation
- ScopedPDU-MMS
- Varbinds
Instrumentation
5
7
View Lookup
- View
- Operation
- Context
6
6
V AC
PDU Processing


GENERATE REQUEST_MSG
Transport
6
Security Model Processing
Message Processing, & Control
Application
-DestinationAdrs
-SecurityModel
-MMS
-SecurityCookie
-ScopedPDU
5
3
Message
Auth
auth Table
Timeliness
time Table
Priv
priv Table
GlobalData
- ScopedPDU
- securityCookie
Determine Naming Scope
4
2
-ModelSpecific SecurityLookup Stuff
SecurityCookie
1
TrapTable
>DestinationAdrs
QOS
Security Model
TrapGroup
Local Processing
Instrumentation
Trap Processing
UserTable
> snmpEngineID
> userName
authProtocol
privProtocol
acGroup
SecurityCookie
View Lookup
V AC
PDU Processing

# SNMP ADVISORY TEAM
# Process Recommendations

- Re-Charter “standard” Working Group
- Develop Revised Documents With “Cut & Paste” Approach
- Plan Face-to-Face Meeting (or 2) Prior to April IETF
- Have I-D(s) Prepared Prior to April IETF

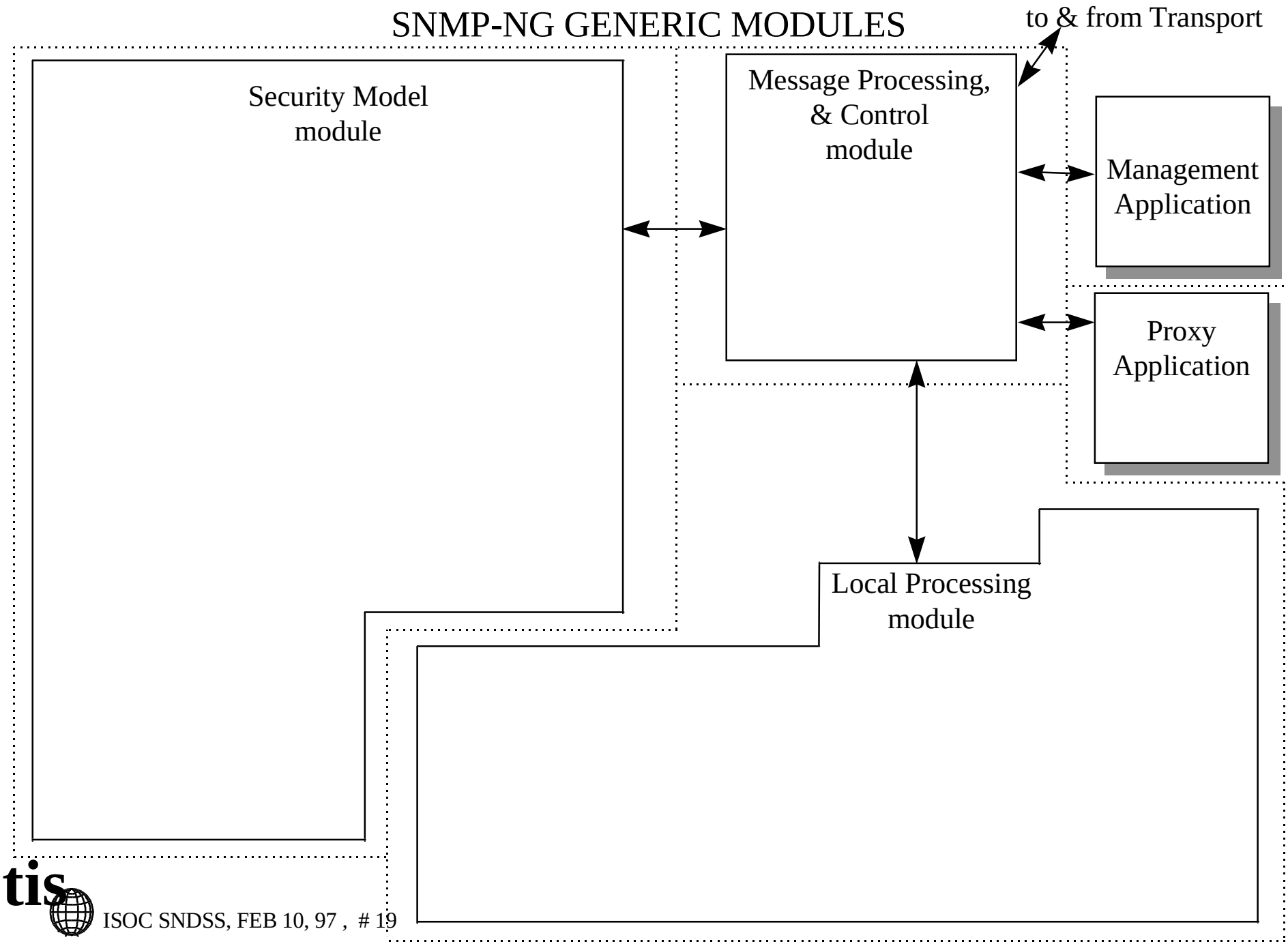
# THANK YOU

# Backup Slides

# SNMP ADVISORY TEAM Members

- David Harrington
- Jeff Johnson
- David Levi
- John Linn
- Russ Mundy
- Shawn Routhier
- Glenn Waters
- Bert Wijnen

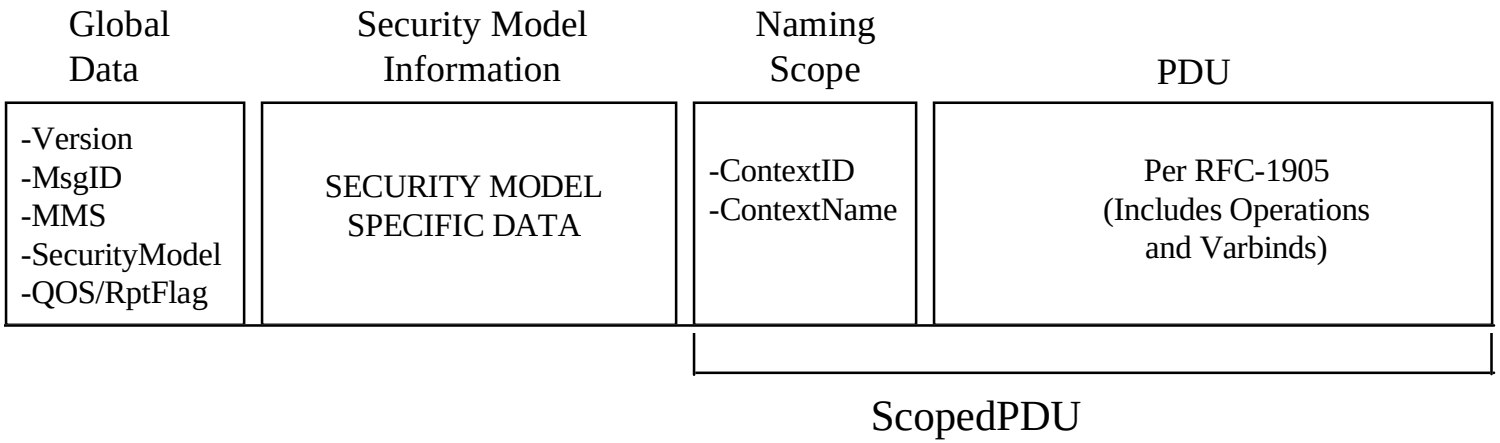
# SNMP-NG GENERIC MODULES



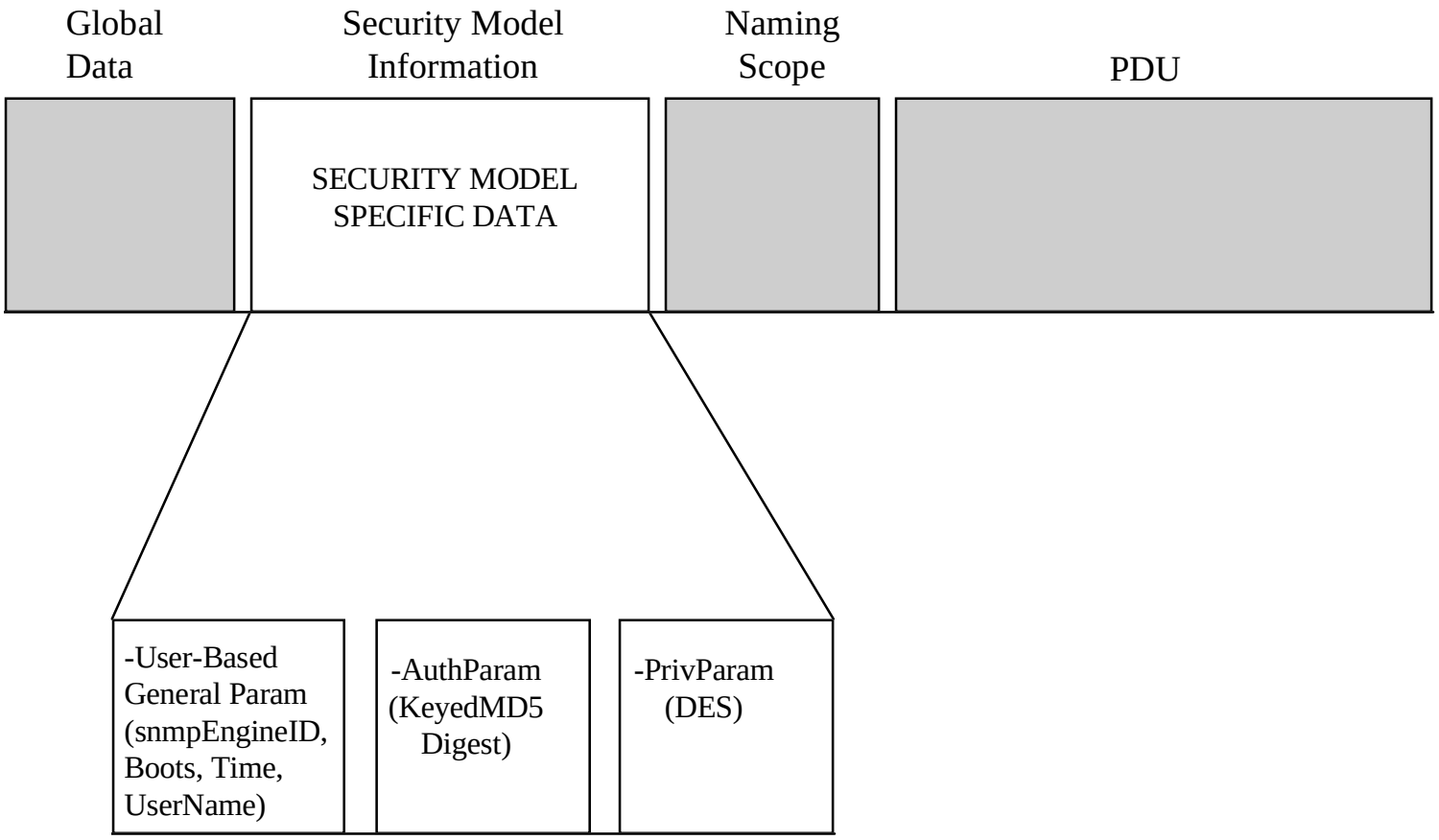
# SNMP Advisory Team

## Message Format Illustrations

# SNMP-NG MESSAGE FORMAT

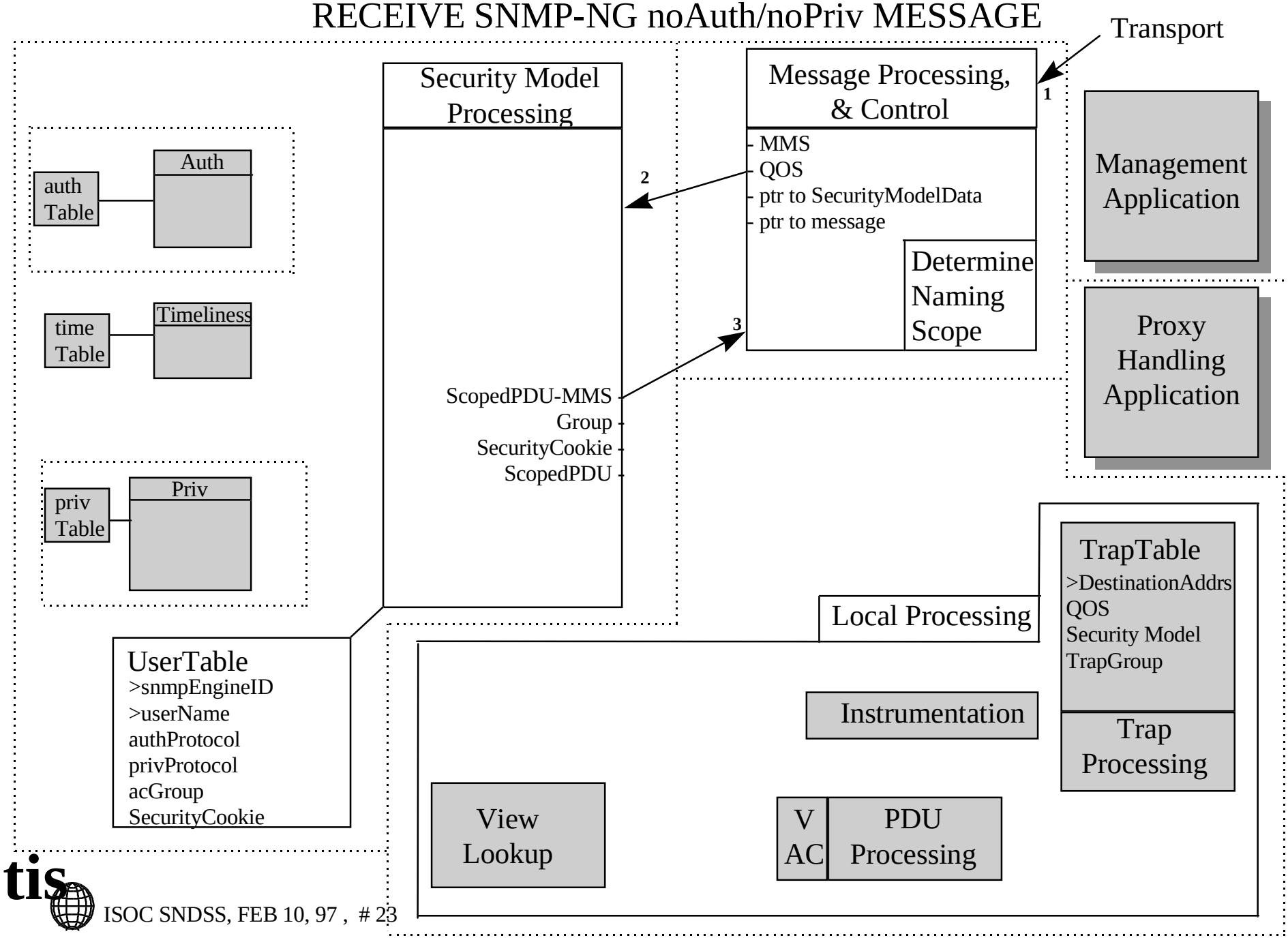


# SNMP-NG MESSAGE FORMAT
# User-Based Security Framework

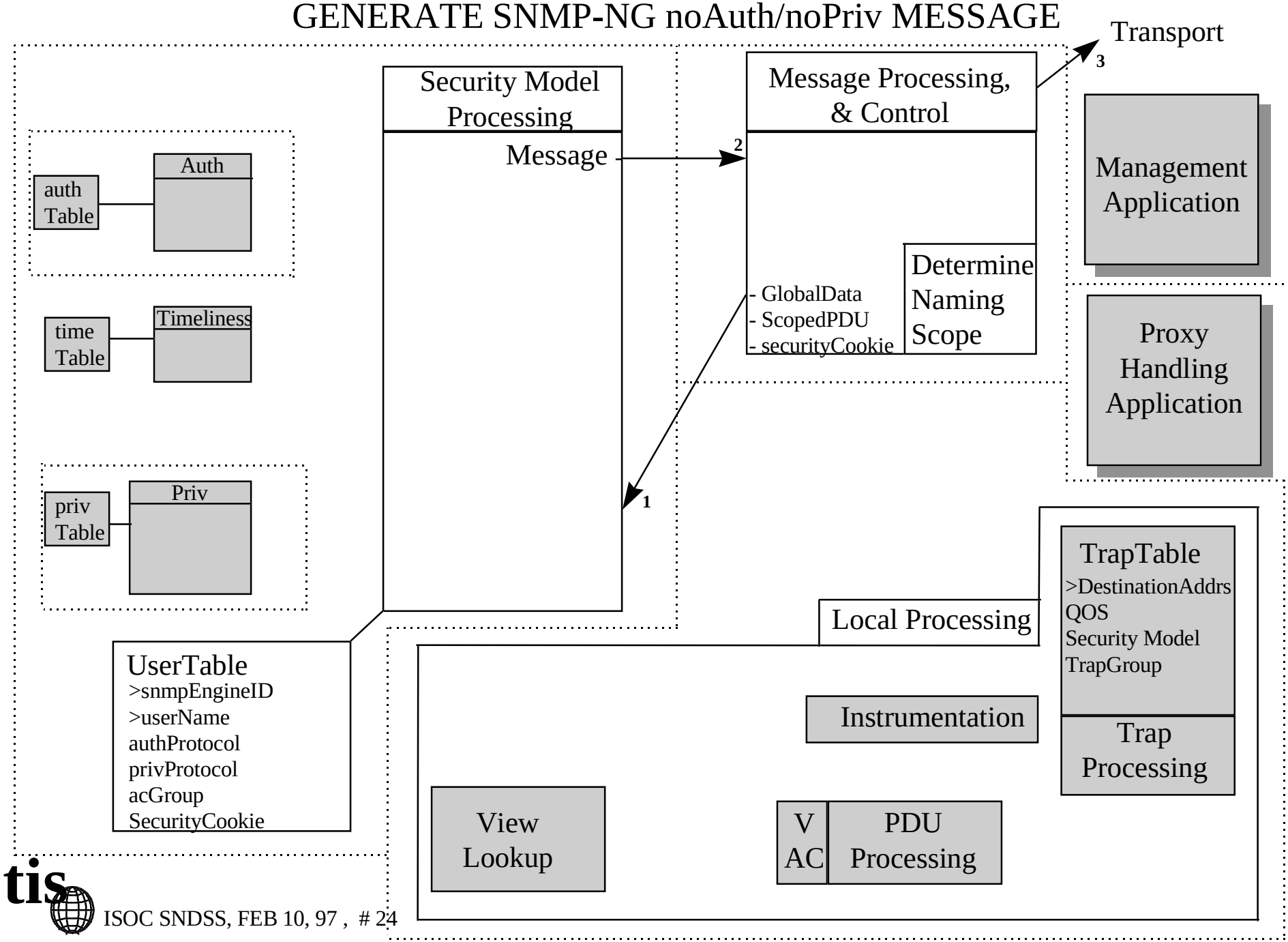



User-Based Security Framework
Model Information

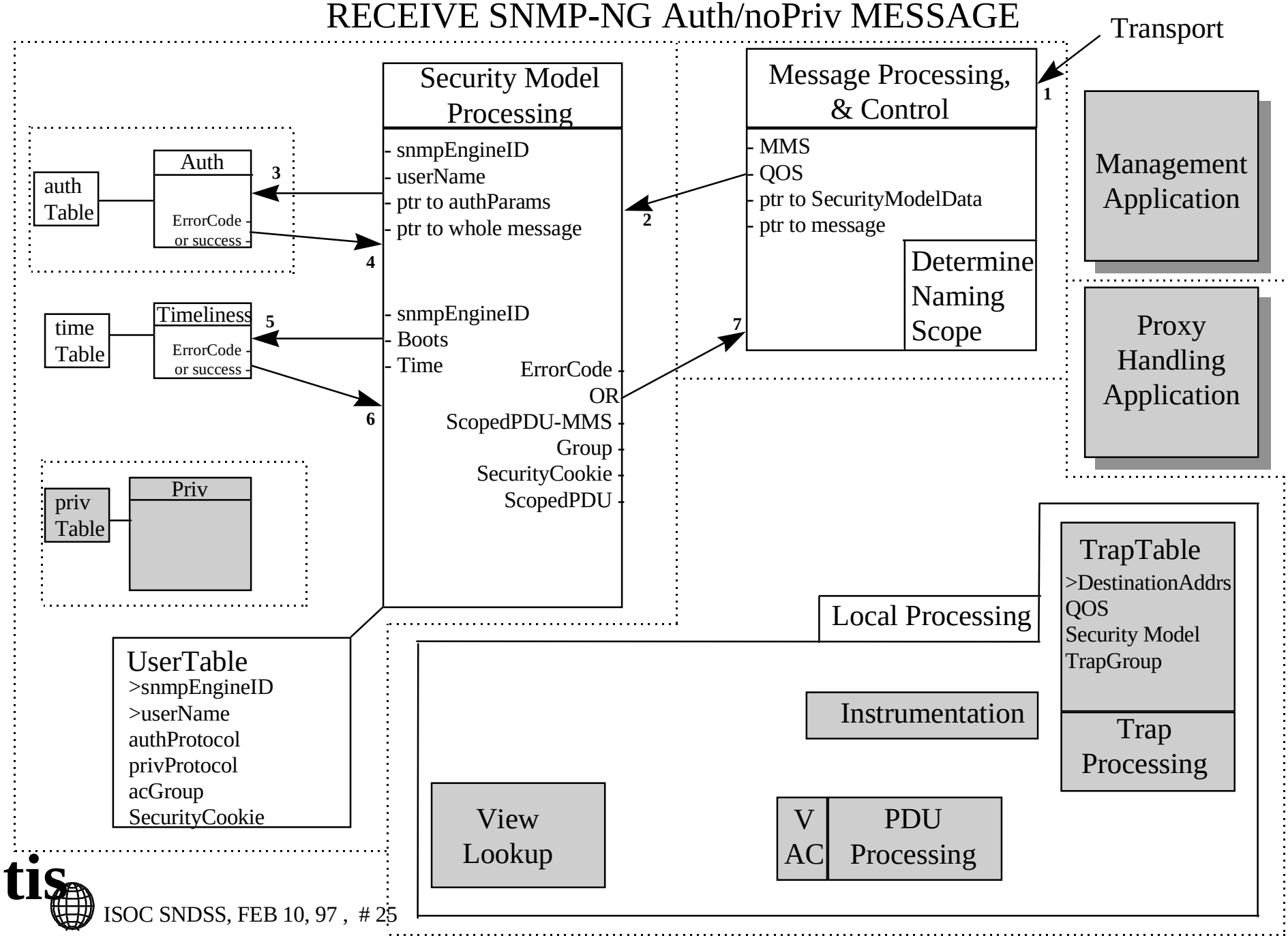
# RECEIVE SNMP-NG noAuth/noPriv MESSAGE



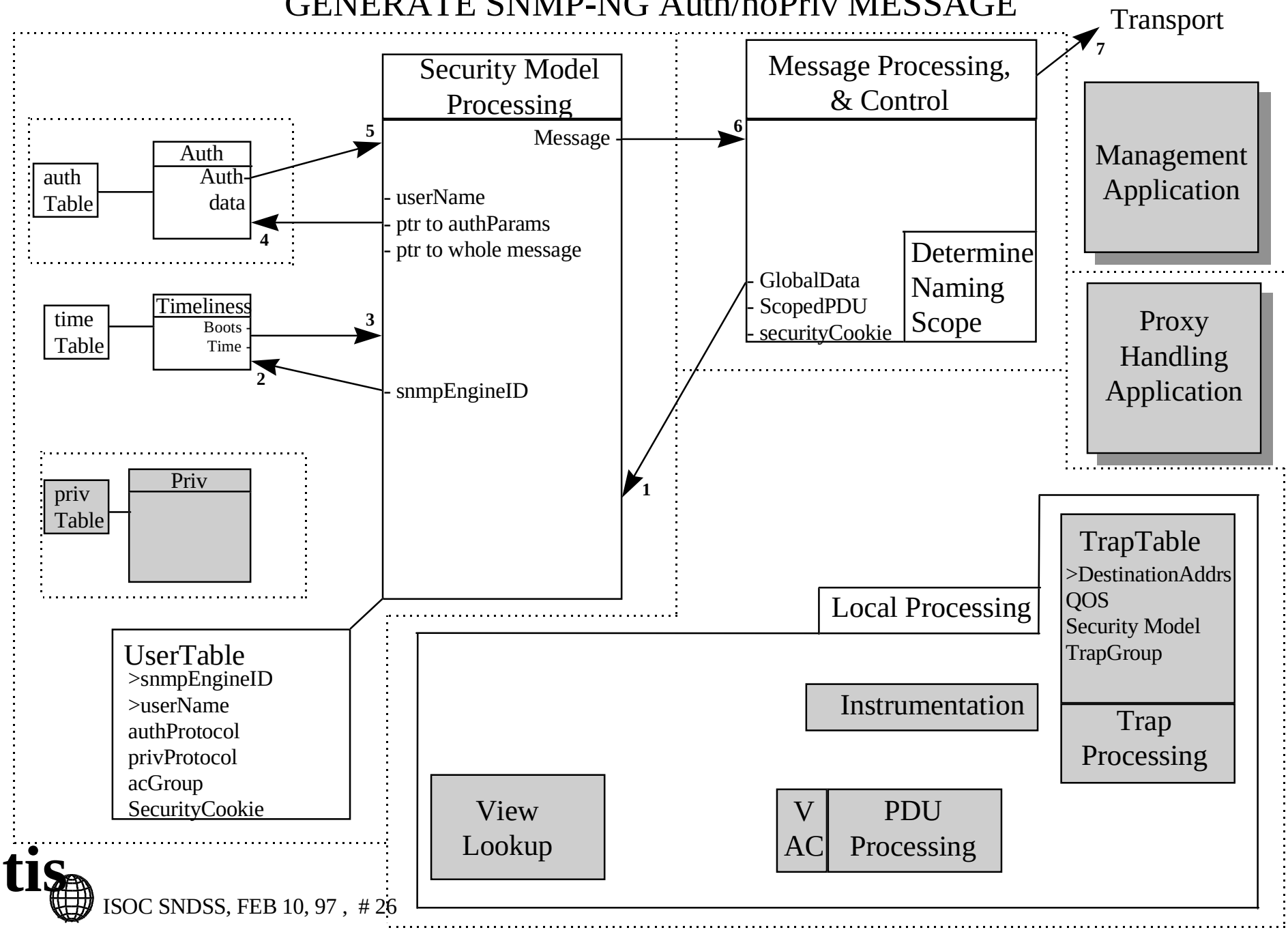
# GENERATE SNMP-NG noAuth/noPriv MESSAGE



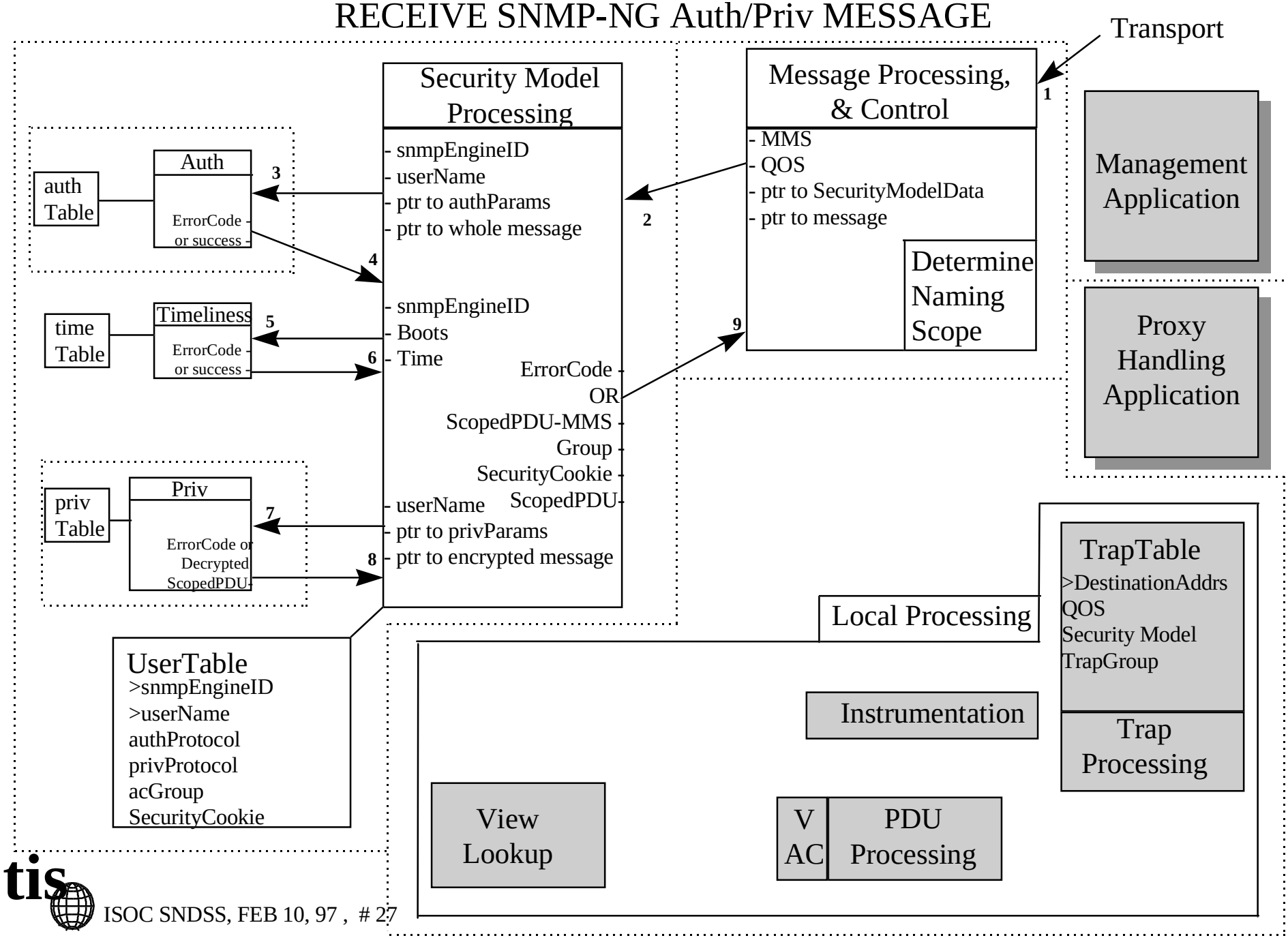
# RECEIVE SNMP-NG Auth/noPriv MESSAGE



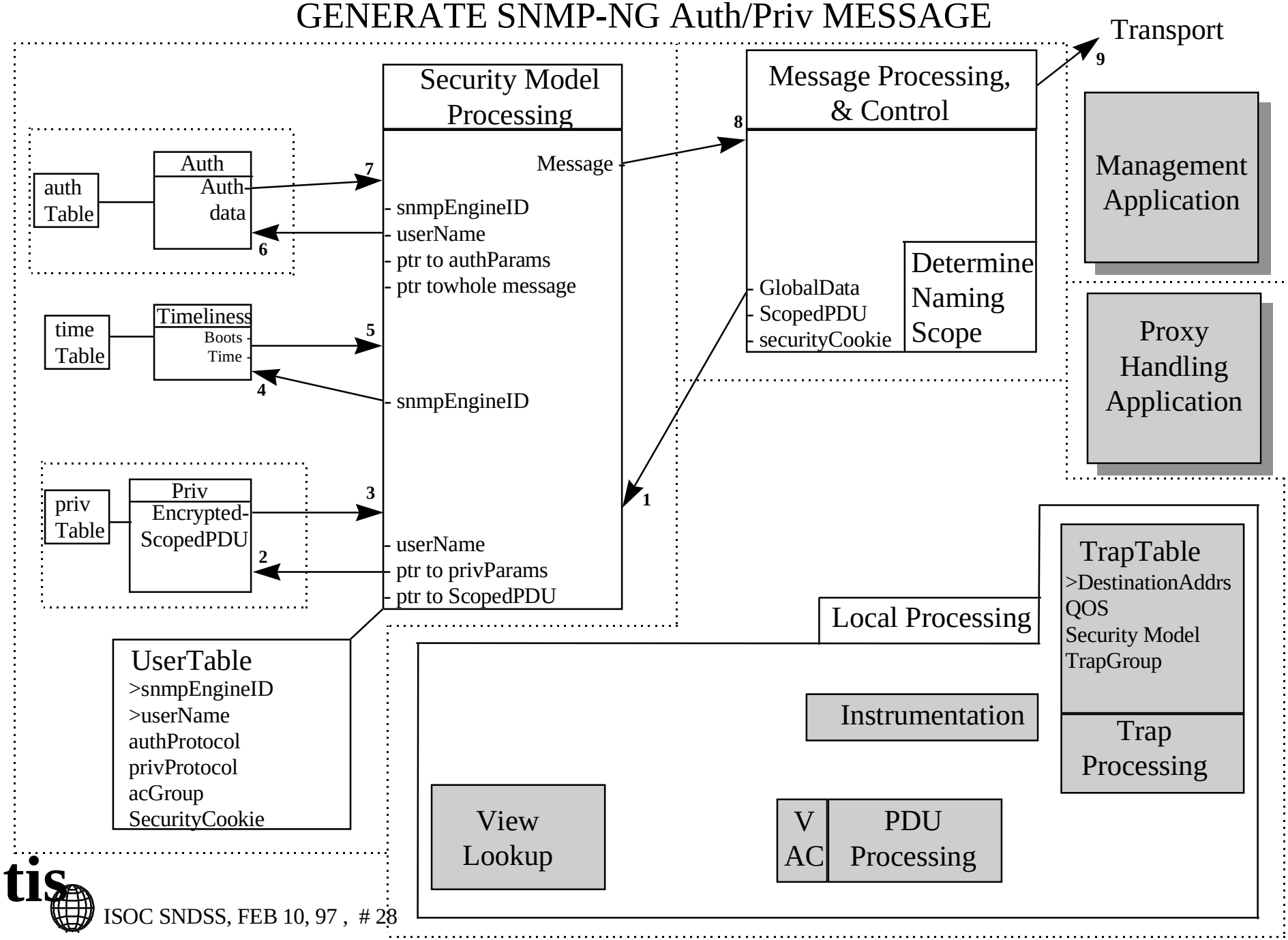
# GENERATE SNMP-NG Auth/noPriv MESSAGE



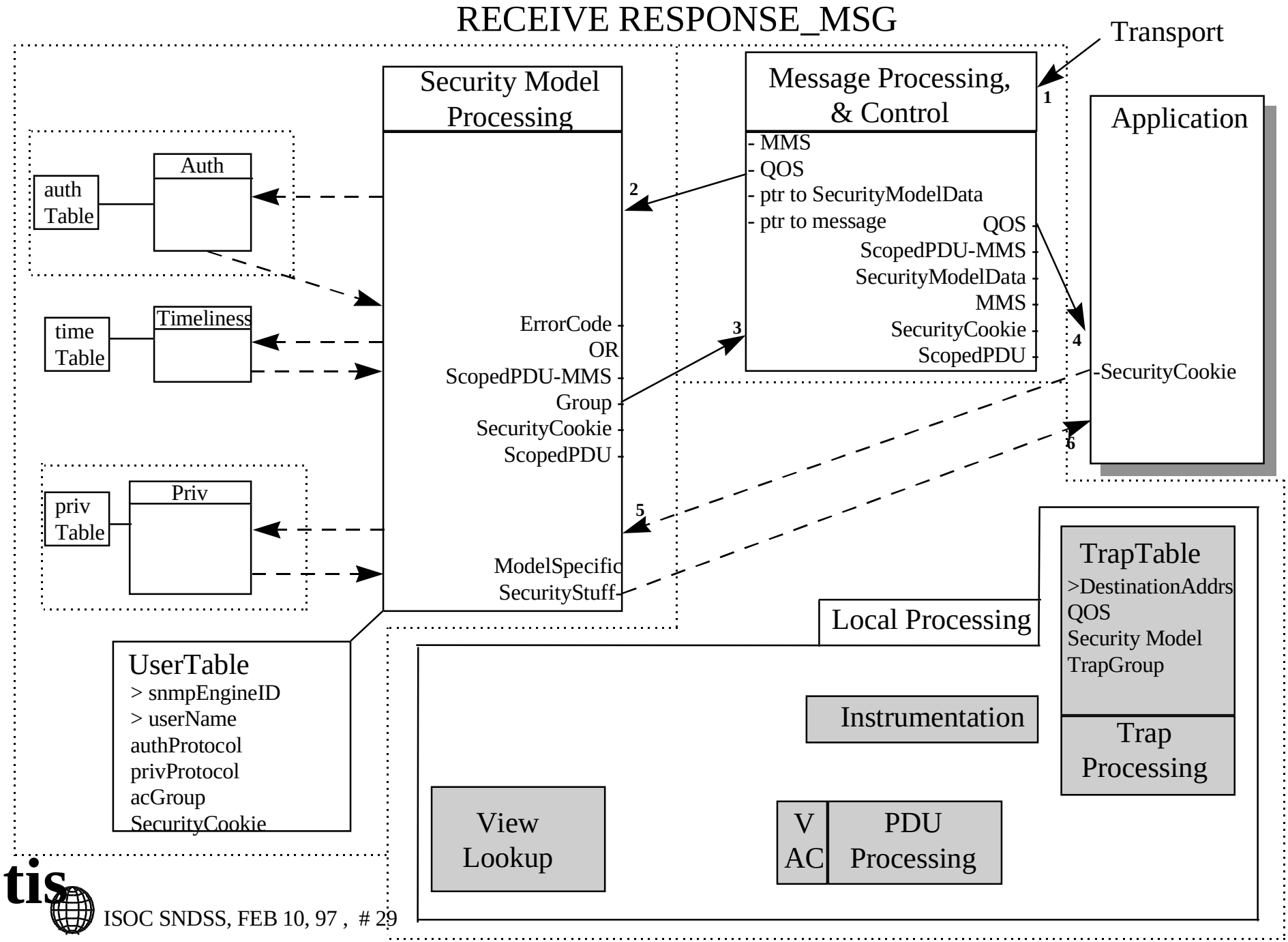
# RECEIVE SNMP-NG Auth/Priv MESSAGE

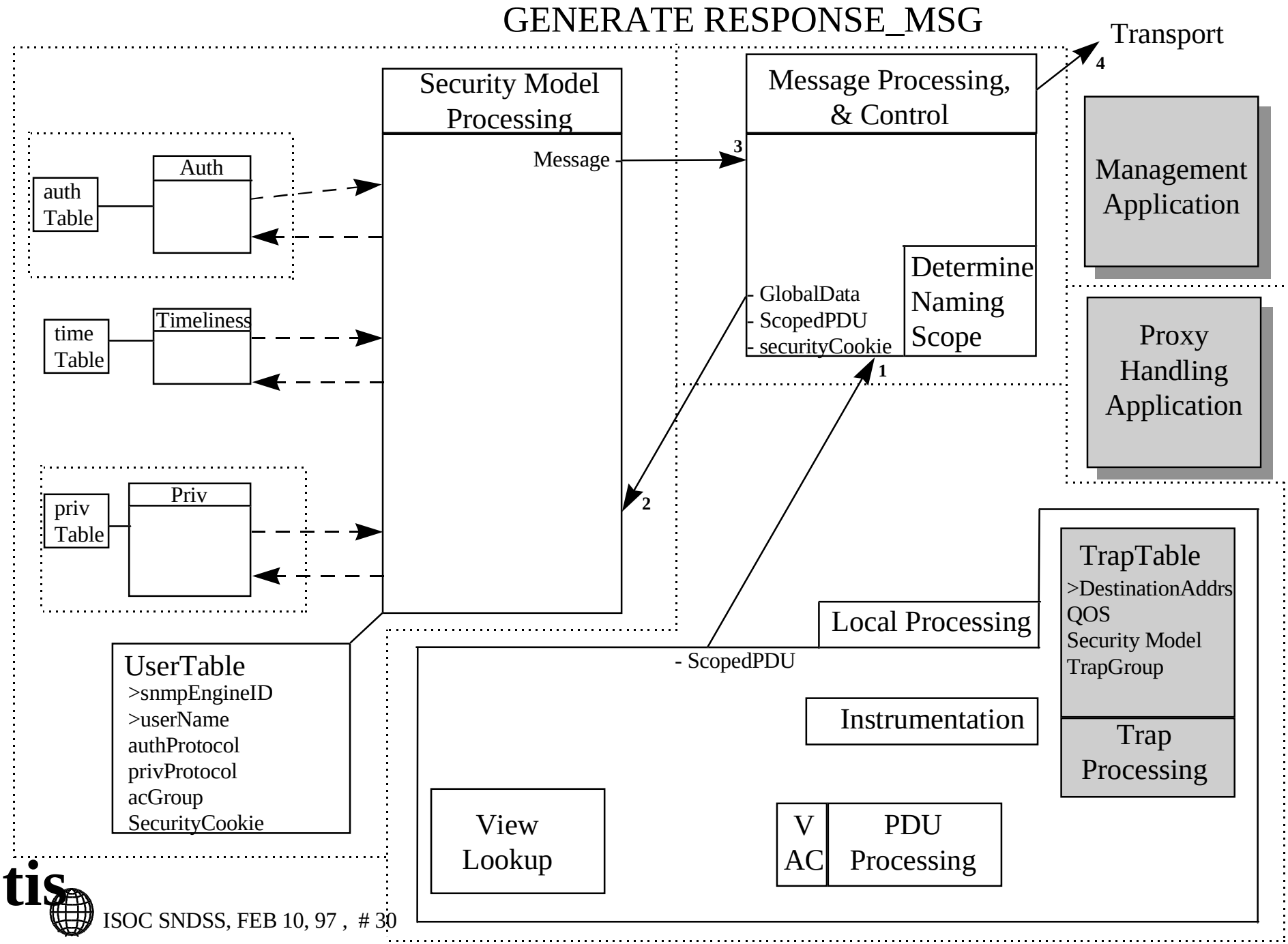


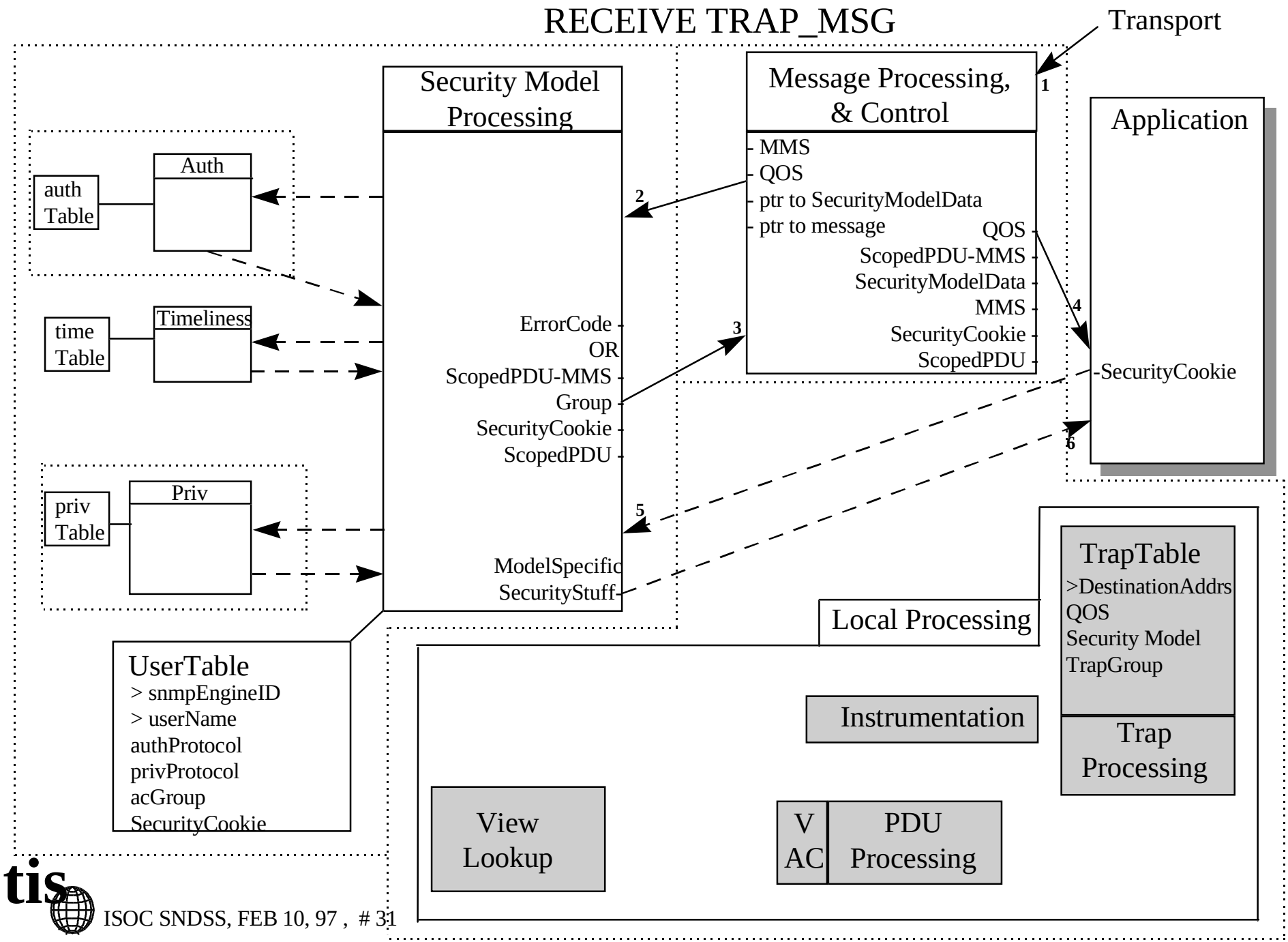
# GENERATE SNMP-NG Auth/Priv MESSAGE

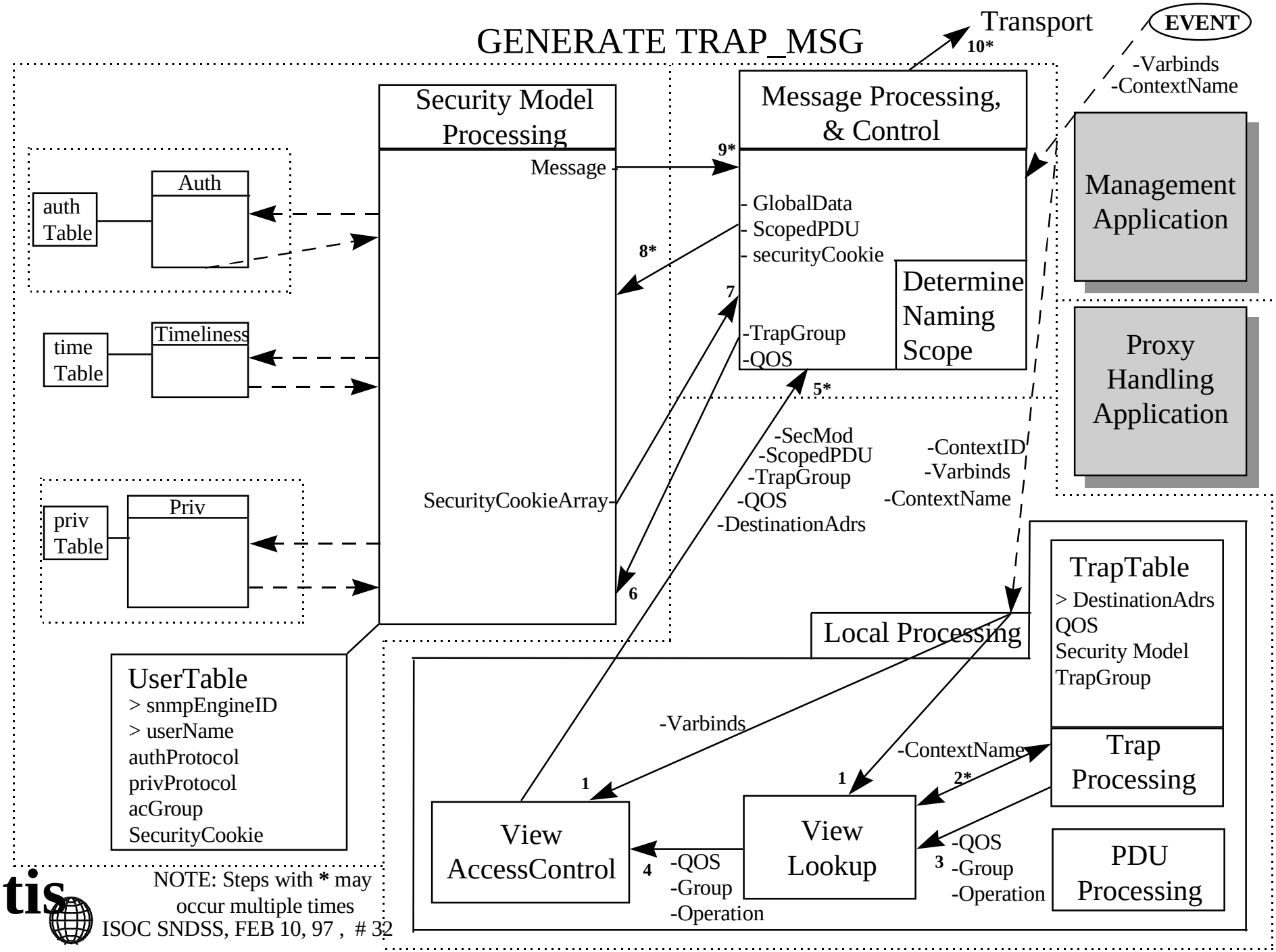


# RECEIVE RESPONSE_MSG

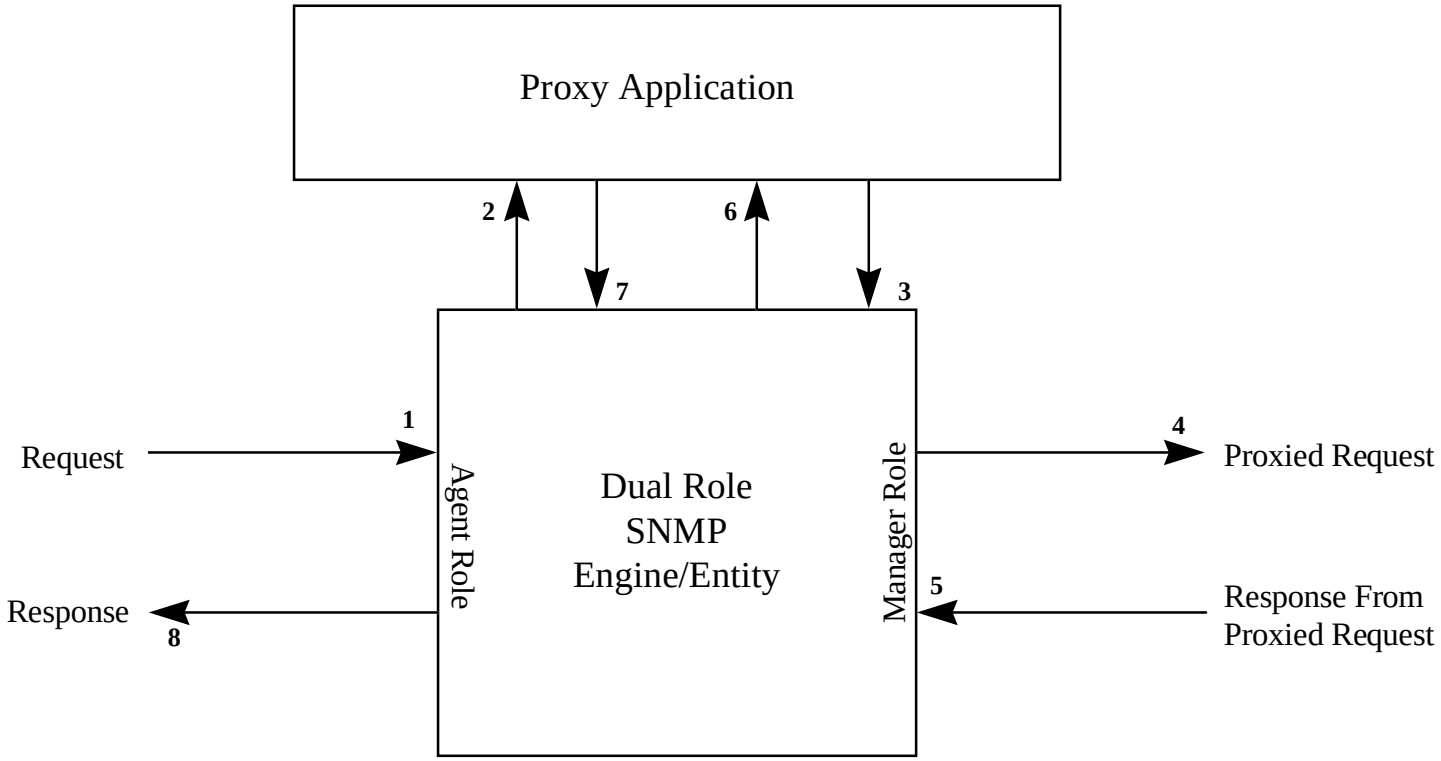



GENERATE RESPONSE_MSG
Transport
4
Security Model Processing
Message Processing, & Control
Message
3
Management Application
Auth
auth Table
Timeliness
time Table
Priv
priv Table
- GlobalData
- ScopedPDU
- securityCookie
Determine Naming Scope
1
2
Proxy Handling Application
TrapTable
>DestinationAddrs
QOS
Security Model
TrapGroup
Local Processing
- ScopedPDU
Instrumentation
Trap Processing
UserTable
>snmpEngineID
>userName
authProtocol
privProtocol
acGroup
SecurityCookie
View Lookup
V AC
PDU Processing

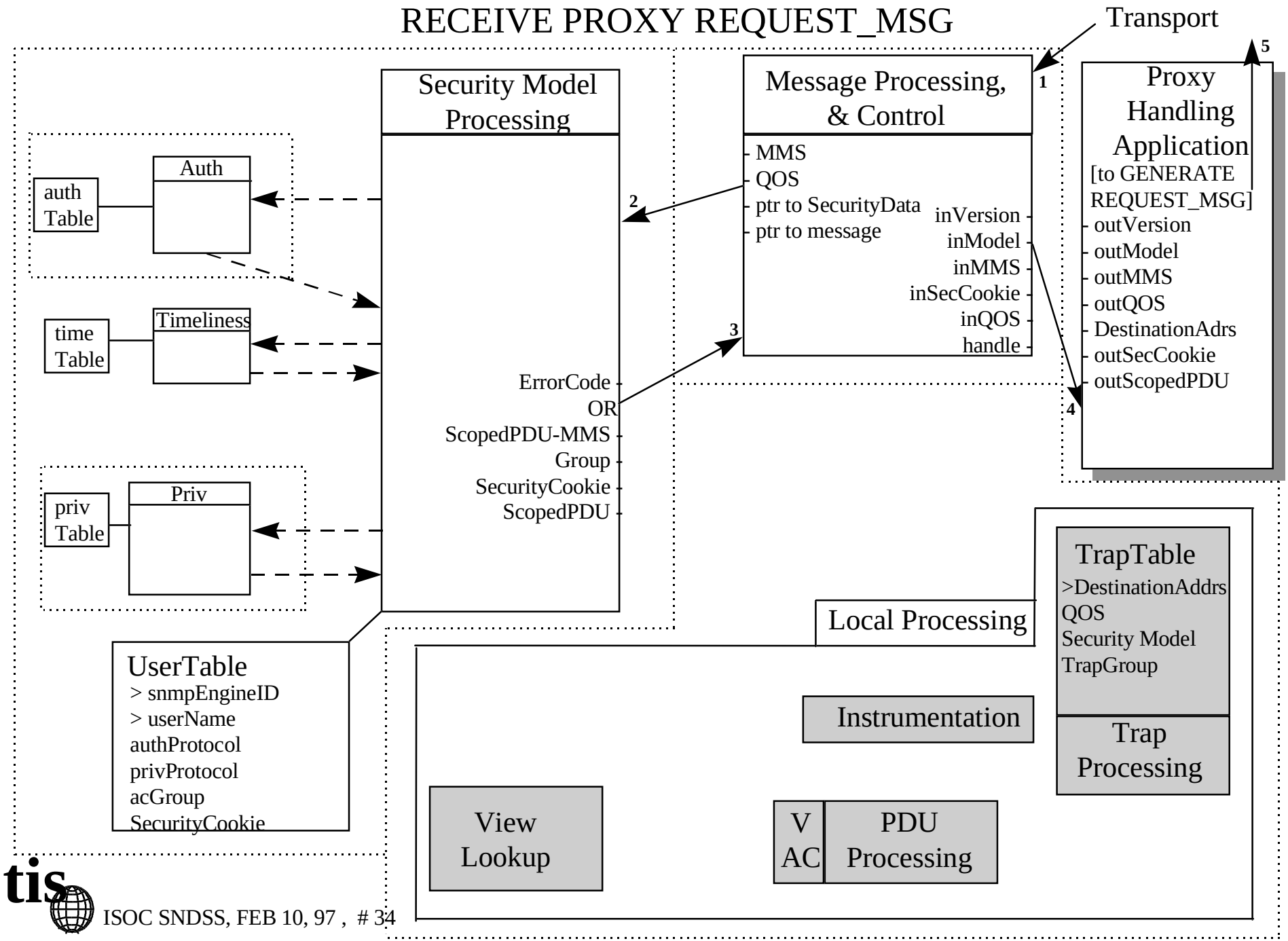

RECEIVE TRAP_MSG
Transport
Security Model Processing
Message Processing, & Control
Application
MMS
QOS
ptr to SecurityModelData
ptr to message
QOS
ScopedPDU-MMS
SecurityModelData
MMS
SecurityCookie
ScopedPDU
-SecurityCookie
Auth
auth Table
Timeliness
time Table
Priv
priv Table
ErrorCode
OR
ScopedPDU-MMS
Group
SecurityCookie
ScopedPDU
ModelSpecific
SecurityStuff
1
2
3
4
5
6
UserTable
> snmpEngineID
> userName
authProtocol
privProtocol
acGroup
SecurityCookie
Local Processing
TrapTable
>DestinationAddrs
QOS
Security Model
TrapGroup
Instrumentation
Trap Processing
View Lookup
V AC
PDU Processing


GENERATE TRAP_MSG
Transport
EVENT
-Varbinds
-ContextName
10*
Security Model Processing
Message Processing, & Control
Management Application
Proxy Handling Application
Message
9*
- GlobalData
- ScopedPDU
- securityCookie
8*
7
Determine Naming Scope
-TrapGroup
-QOS
5*
Auth
auth Table
Timeliness
time Table
Priv
priv Table
SecurityCookieArray
6
-SecMod
-ScopedPDU
-TrapGroup
-QOS
-DestinationAdrs
-ContextID
-Varbinds
-ContextName
TrapTable
> DestinationAdrs
QOS
Security Model
TrapGroup
Local Processing
UserTable
> snmpEngineID
> userName
authProtocol
privProtocol
acGroup
SecurityCookie
-Varbinds
-ContextName
1
1
2*
Trap Processing
View AccessControl
View Lookup
PDU Processing
4
-QOS
-Group
-Operation
3
-QOS
-Group
-Operation
NOTE: Steps with * may occur multiple times

# PROXY PROCESSING
## Overview



# RECEIVE PROXY REQUEST_MSG



# RECEIVE PROXY RESPONSE_MSG