Group Secure Association Key Management Protocol (GSAKMP)

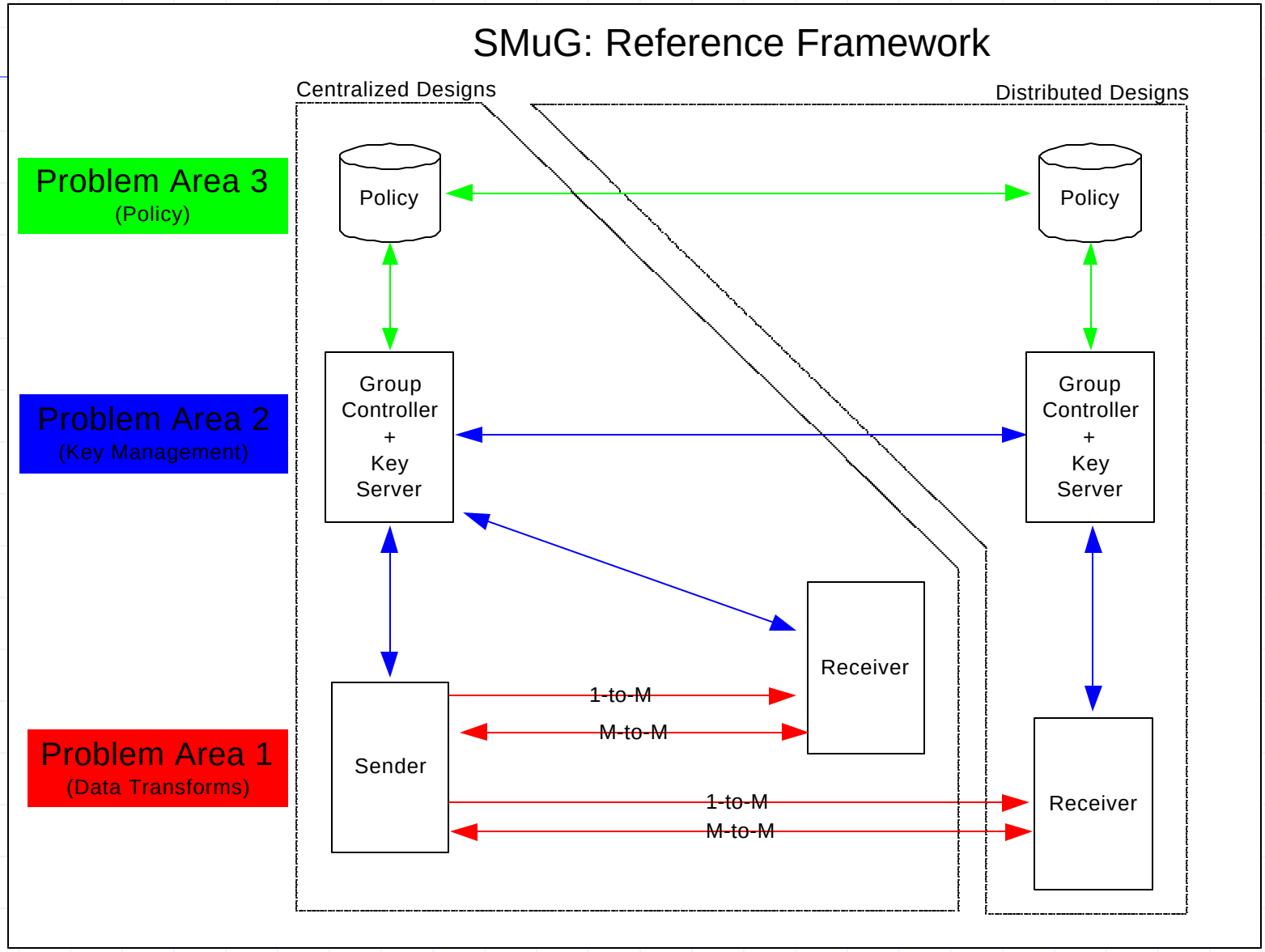
Presented by

Hugh Harney
hh@sparta.com

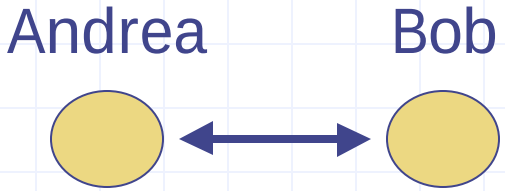
Agenda

- Framework
- GSAKMP Policy
- GSAKMP Key Management
- GSAKMP Message Structures
- Summary

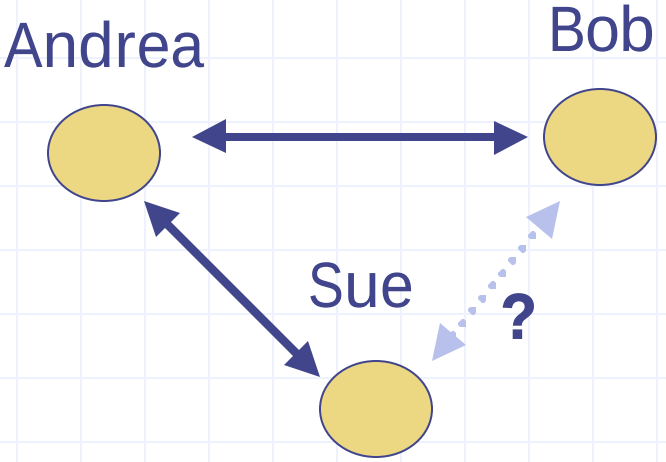
SMuG Framework



Policy
Group policy vs. Peer Policies



- A and B have 1st hand knowledge
- A and B are sharing their own data
- A and B participate in key creation



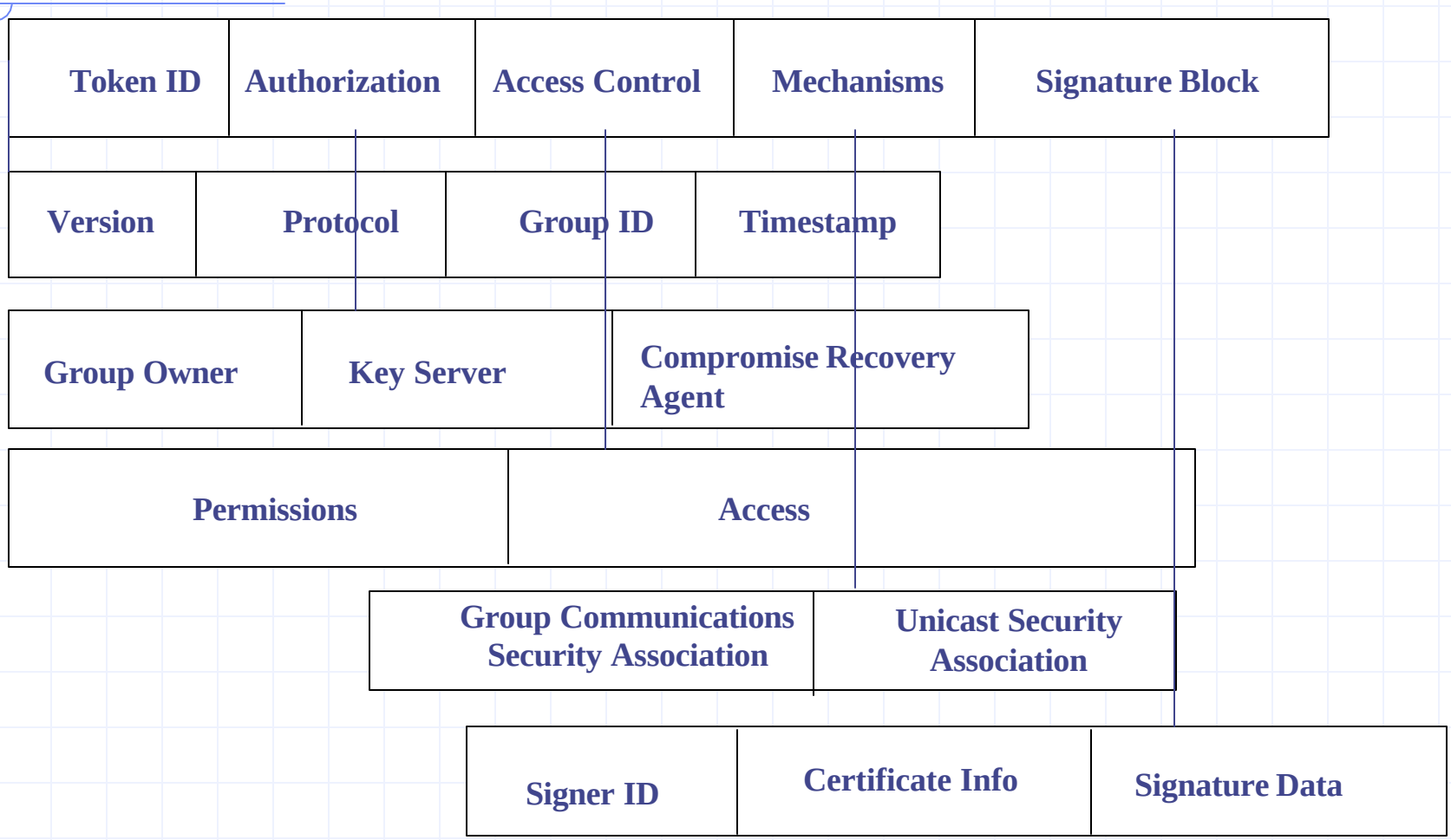
- A and B have 1st hand knowledge
- A and S have 1st hand knowledge
- B and S have never communicated

- Who owns the data?
- How can S trust B? B trust S?
- Was the A to B key exchange as strong As the A to S exchange?
- Will A and B protect the data equally?
- Is A authorized to distribute key?
- Is A controlling the group?

GSAKMP Features

- Layered approach
  - Additional functionality vs. re-engineering
- Full policy specification and dissemination
  - Authenticated policy token
- Distributed Key Management
  - Security infrastructure discovery
  - Push or Pull operation
  - Optional fields for high grade security
- Ubiquitous policy enforcement
  - Access control
  - Authorizations
  - Mechanism specifications
- Rekey
  - Logical Key Hierarchy
- Proof of concept source code is available - FREE

GSAKMP Policy Token (Generic)



GSAKMP Policy

IPSEC example Token ID Field

- Token ID
  - Token version
    - GSAKMP v1.0
    - ANTIGONE v1.0
  - Protocol ID
    - IP Multicast
      - Group Name
        - IPV4
        - Multicast Addr: 224.0.0.7
        - Group #: abcd
        - Source Address: aaa.bbb.ccc.ddd
    - Reliable IP Multi
  - Life date
    - 1 day
- Authorizations
- Access Control
- Mechanisms
- Signature Block

GSAKMP Policy

IPSEC example: Authorizations Field

Token ID

Authorizations

Access Control

Mechanisms

Signature Block

Group Owner

Subject Name
/C=US/ST=MD/L=Columbia/
O=SPARTA,Inc./
CN=Jane Owner
(Opt Serial #)
1234….
PKI Information

Root Cert Type(s)
X.509 v3-DSS-SHA1
Key length
1024
Root CA
/C=US/ST=MD/L=Columbia/
O=SPARTA,Inc./CN =John Root

GC/KS

Subject Name
(Opt) Serial #
PKI Information

Root Cert Type(s)
X.509 v3-DSS-SHA1
Key length
1024
Root CA
/C=US/ST=MD/L=Columbia/
O=SPARTA,Inc./CN = Sally Member

Rekey Control

Subject Name
(Opt) Serial #
PKI Information

GSAKMP Policy

IPSEC example: Access Control Field

Token ID

Authorizations

Access Control

- permissions
  - Security level 1
  - Security level 2
  - Security level 3
  - Etc.
- access Control List
  - /C=US/ST=MD/L=Columbia/O=SPARTA,Inc./CN = Grumpy Member
  - /C=US/ST=MD/L=Columbia/O=SPARTA,Inc./CN = Doc Member
  - /C=US/ST=MD/L=Columbia/O=SPARTA,Inc./CN = Sneezy Member
  - Etc.
- Access Control Rules
  - Distinguished name must be in member Database
  - AND
  - Distinguished name must not be on bad guy list

Mechanisms

Signature Block

GSAKMP Policy

IPSEC example: Mechanisms Field

- Token ID
- Authorizations
- Access Control
- Mechanisms
  - Unicast
    - **Peer SA**
    - Security Protocol
    - Key Length
    - Key Creation Method
    - **Group Establishment Messages**
    - Key encryption algorithm
    - Signature
    - Key creation method
  - Group Data Comms
    - **SPI:** mandatory for group
    - **Security Protocol**
      - **AH**
      - **ESP**
      - **IPSec (none)**
    - **Key Length**
    - **Key Creation Method**
    - **Group Source Authentication**
  - Group Management
    - Key encryption algorithm
    - Rekey method
    - Signature
    - Data channel exceptions
- Signature Block

Direction
in
out

ESP Algorithm
3 DES
(See DOI)

ESP Authentication
hmac-sha
(See DOI)

Encapsulation Mode
tunnel
transport

SA Life
time
bytes

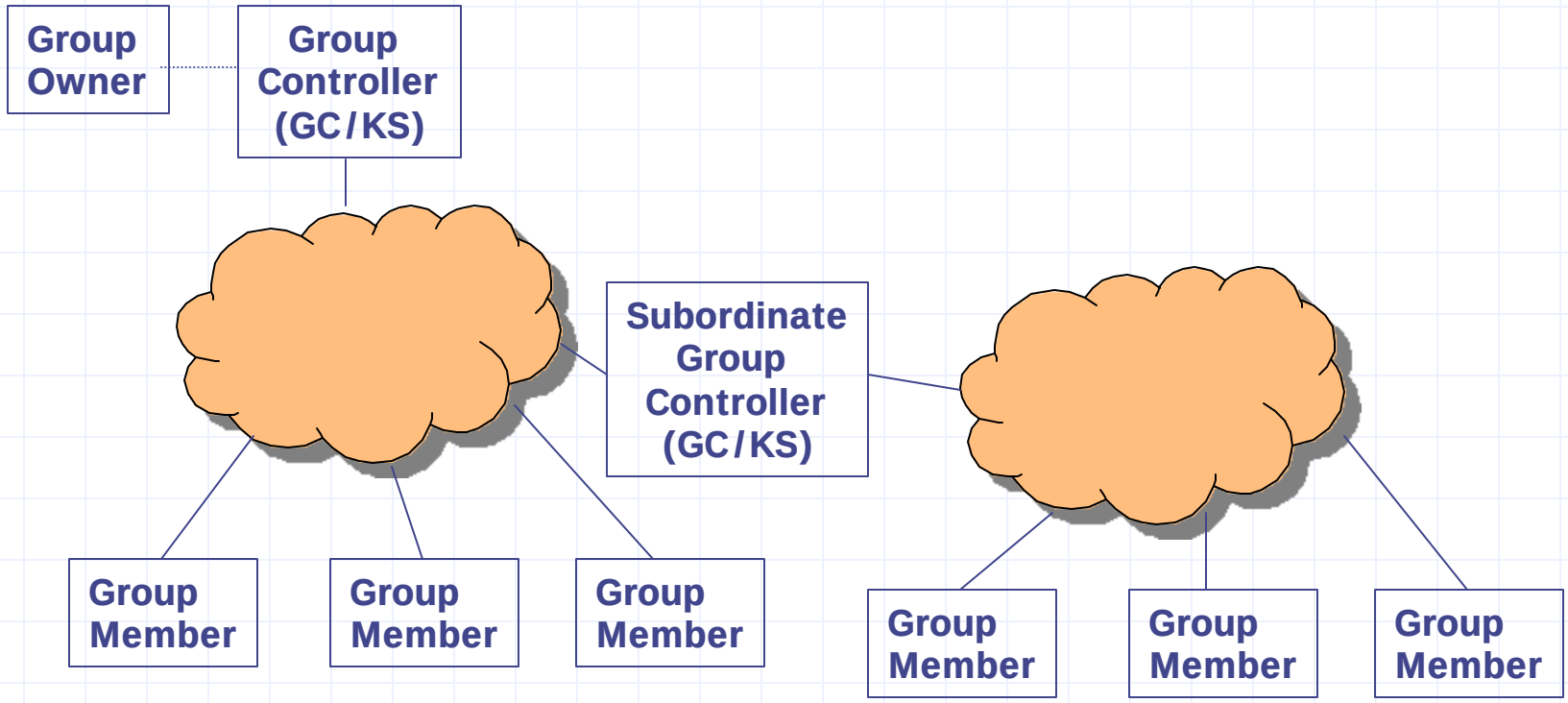
Selectors
source address: 111.222.333.444
(destination port):
(group ID): 4 byte?
(security label):

GSAKMP Policy

IPSEC example: Signature Block Field

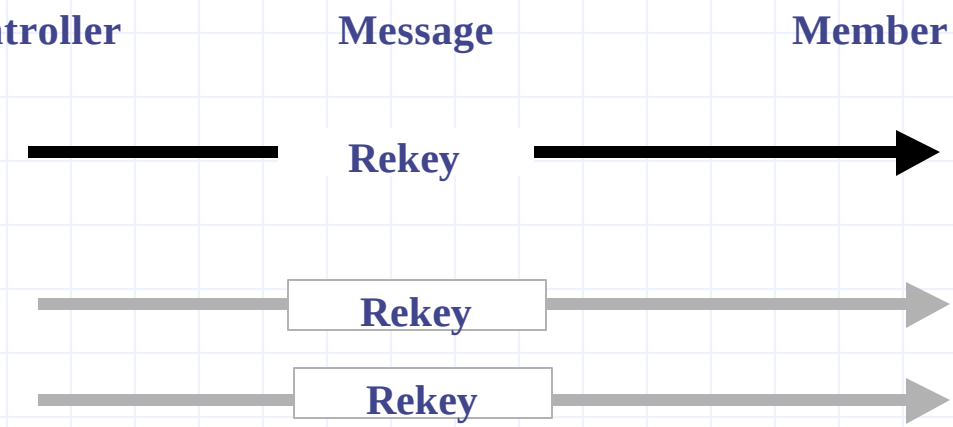
- Token ID
- Authorizations
- Access Control
- Mechanisms
- Signature Block
  - Signature Information
    Algorithm: DSS
    Hash: SHA1
  - Signature Data

GSAKMP Key Management - Group Establishment Architecture



GSAKMP Key Management Establishment messages

GSAKMP Key Management Rekey



Request to join

- Message Name : Request to Join
- Dissection : {HDR, GrpID, Nonce_I, GSA RQ} SigM, [CertM]
- Payload Types : GSAKMP Header, Nonce, Notification, Signature, [Certificate], [Certificate Request], [Vendor ID], [Identification], [Authorization]

- SigM : Signature of Group Member
- CertM : Certificate of Group Member
- {}SigX :Indicates minimum fields used in Signature
- [ ] : Indicate an optional data item

Invitation

- **Message Name : Invitation to Join**
- **Dissection : {HDR, GrpID, Policy Token, (Nonce_R, Nonce_C) OR Nonce_I, [Key Creation], GSA RQ}SigC, [CertC], [SigSC], [CertSC]**
- **Payload Types : GSAKMP Header, Policy Token, Nonce, Notification, Signature, [Certificate], [Signature], [Certificate], [Key Creation], [Certificate Request], [Vendor ID], [Identification], [Authorization]**

- **SigC : Signature of Group Controller**
- **SigSC : Signature of Subordinate Group Controller**
- **CertC : Certificate of Group Controller**
- **CertSC : Certificate of Subordinate Group Controller {}**
- **SigX :Indicates minimum fields used in Signature [] : Indicate an optional data item**

Invitation Response

- **Message Name : Invitation Response**
- **Dissection : {HDR, GrpID, (Nonce_R, Nonce_C) OR Nonce_C, [ID_R], [Key Creation], GSA RS}SigM, [CertM]**
- **Payload Types : GSAKMP Header, Nonce, [Identification], Notification, Signature, [Key Creation], [Certificate], [Vendor ID], [Authorization]**

- **SigM : Signature of Group Member**
- **CertM : Certificate of Group Member**
- **{}SigX :Indicates minimum fields used in Signature**
- **[] : Indicate an optional data item**

Key download over SA

- **Message Name : Key Download**
- **Dissection : {HDR, GrpID, Nonce_C, ID_R, [(]Key Data[)*]}SigC, [SigSC], [CertSC]**
- **Payload Types : GSAKMP Header, Nonce, Identification, Key Download, Signature, [Authorization], [Vendor ID] SigC : Signature of Group Controller**

- **SigSC : Signature of Subordinate Group Controller**
- **CertC : Certificate of Group Controller**
- **CertSC : Certificate of Subordinate Group Controller**
- **{}SigX :Indicates minimum fields used in Signature**
- **[] : Indicate an optional data item**
- **(data)* : Indicates encrypted information**

Key download insufficient SA

Definition Message Name : Key Download

- **Dissection : {HDR, GrpID, Nonce_C, ID_R, (Key Data)*}SigC, [SigSC], [CertSC]**
- **Payload Types : GSAKMP Header, Nonce, Identification, Key Download, Signature, [Authorization], [Vendor ID]**

- **SigC : Signature of Group Controller**
- **SigSC : Signature of Subordinate Group Controller**
- **CertC : Certificate of Group Controller**
- **CertSC : Certificate of Subordinate Group Controller**
- **{}SigX :Indicates minimum fields used in Signature**
- **[] : Indicate an optional data item**
- **(data)* : Indicates encrypted information**

Acknowledgement

- **Message Name : Acknowledgment**
- **Dissection : {HDR, GrpID, Nonce_C, [ID_R], ACK}SigM, [CertM]**
- **Payload Types : GSAKMP Header, Nonce, [Identification], Notification, Signature, [Certificate], [Vendor ID], [Identification], [Authorization]**

- **SigM : Signature of Group Member**
- **CertM : Certificate of Group Member**
- **{}SigX :Indicates minimum fields used in Signature**
- **[] : Indicate an optional data item**

Rekey

- Message Name : Rekey Event
- Dissection : {HDR, GrpID, [Policy Token], Rekey Array}SigC, [CertC]
- Payload Types : GSAKMP Header, [Policy Token], Rekey Event, Signature, [Certificate], [Vendor ID]

- SigC : Signature of Group Controller
- CertC : Certificate of Group Controller
- {}SigX :Indicates minimum fields used in Signature
- [] : Indicate an optional data item

Closing Remarks

- GSAKMP has a free release
- ftp://ftp.sparta.com/pub/columbia/gsakmp

- hh@sparta.com