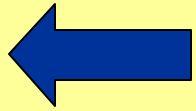
Group DOI for ISAKMP

<draft-irtf-smug-gdoi-01.txt>

Mark Baugher (PassEdge)
Thomas Hardjono (Nortel)
Hugh Harney (SPARTA)
Brian Weis (Cisco)

Group DOI for ISAKMP

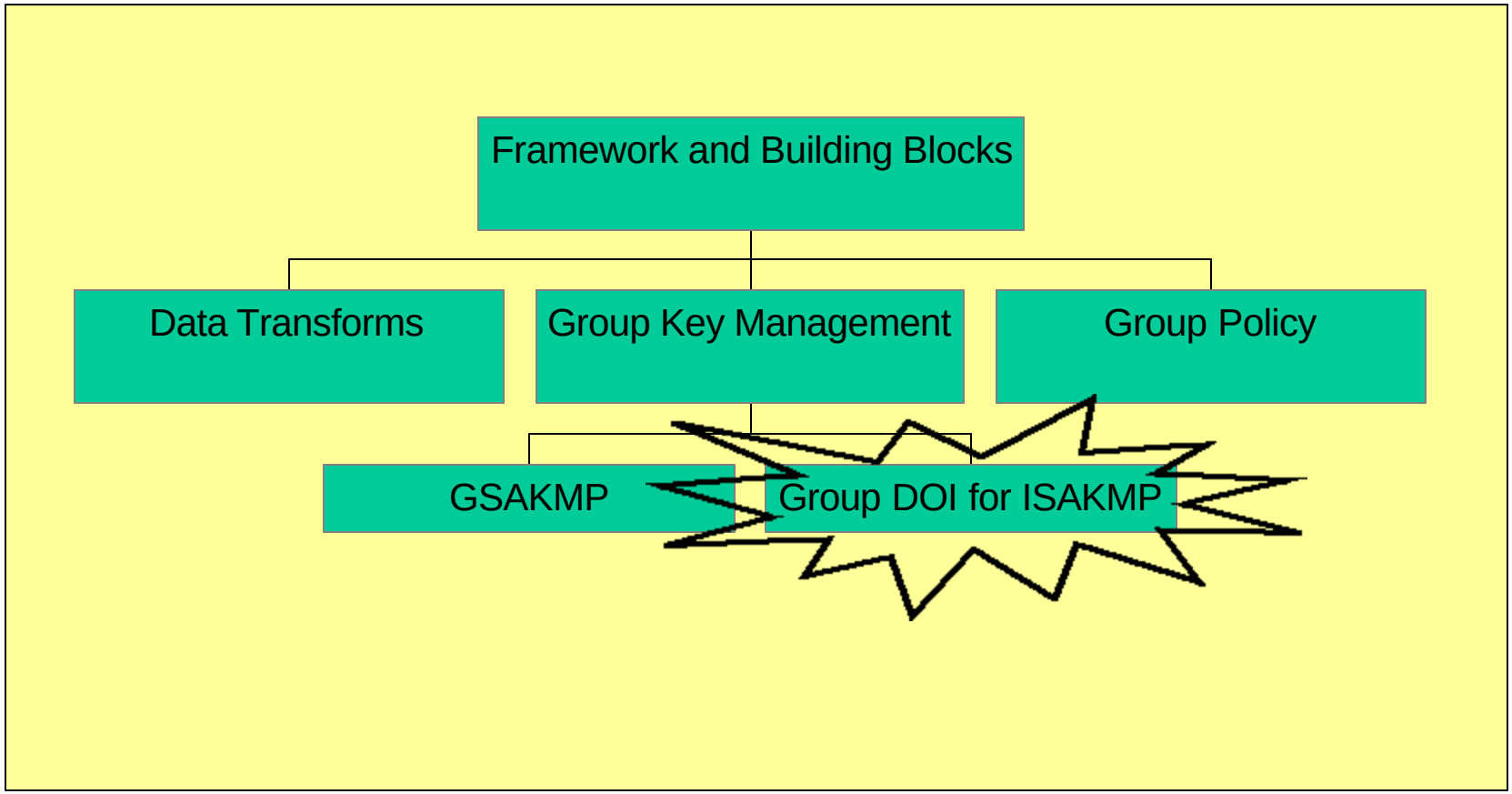
Background Concepts 

Group DOI Flows & Payloads

Proof of Concept Testing

Current Status & Future Plans

SMUG Building Block Framework



Motivation for GDOI

- There will be a need for systems to protect both group and unicast traffic.
- Having two independent key mgmt frameworks on one system is unnecessarily complex.
- Many systems have implemented ISAKMP and IKE for unicast key mgmt.
- We believe that this environment can be used for group key mgmt.

ISAKMP (RFC 2408)

- General framework for key management
- Defines payloads for authentication, policy negotiation, and key generation.
- Defines basic key mgmt exchanges.
- Primarily used by IKE, but not restricted to IKE. E.g., KINK drafts use some ISAKMP payloads.

Domains of Interpretation

- ISAKMP provides for multiple domains of interpretation (DOIs)
- RFC 2407 defines one DOI for IPSEC
- Other DOIs can be easily defined for ISAKMP.

IPSEC DOI (RFC 2407) & IKE (RFC 2409)

- IPSEC DOI defines IPSEC-specific payloads and policy definitions
- IKE defines exchanges in two phases:
  - IKE Phase 1 sets up a “secure channel” between IKE peers.
  - IKE Phase 2 negotiates specific IPSEC policy.

IKE Phase 1

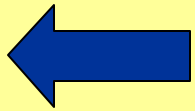
- Authenticates the peer.
- Negotiates “secure channel” policy.

IKE Phase 1 services

- IKE Phase 1 provides the following security services for subsequent exchanges:
  - *Confidentiality* -- encryption of exchange payloads
  - *Integrity* -- HASH payload provides an HMAC
  - *Replay protection* -- NONCE payload provides liveliness proof
  - *Generation of Phase 2 keying material*

Group DOI for ISAKMP

Background Concepts

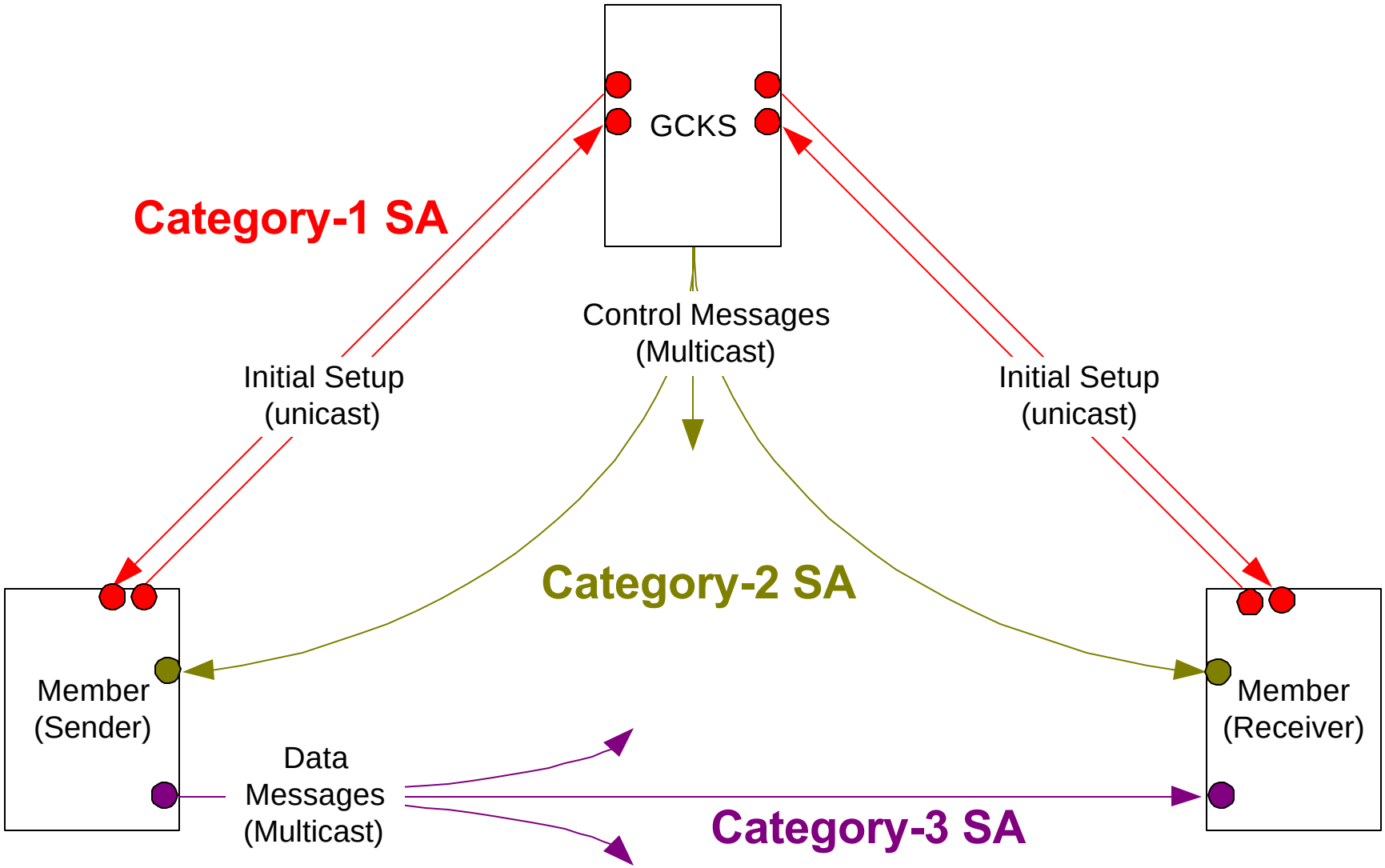
Group DOI Flows & Payloads 

Proof of Concept Testing

Current Status & Future Plans

Group DOI Overview

- Defines a temporary DOI number for ISAKMP and group policy definitions.
- Defines a new Category-1 SA (“Pull”) exchange for initial group key mgmt. This is sent through the IKE “secure channel”.
- Defines a Category-2 SA (“Push”) exchange for subsequent key updates. This exchange can be multicasted for efficiency.

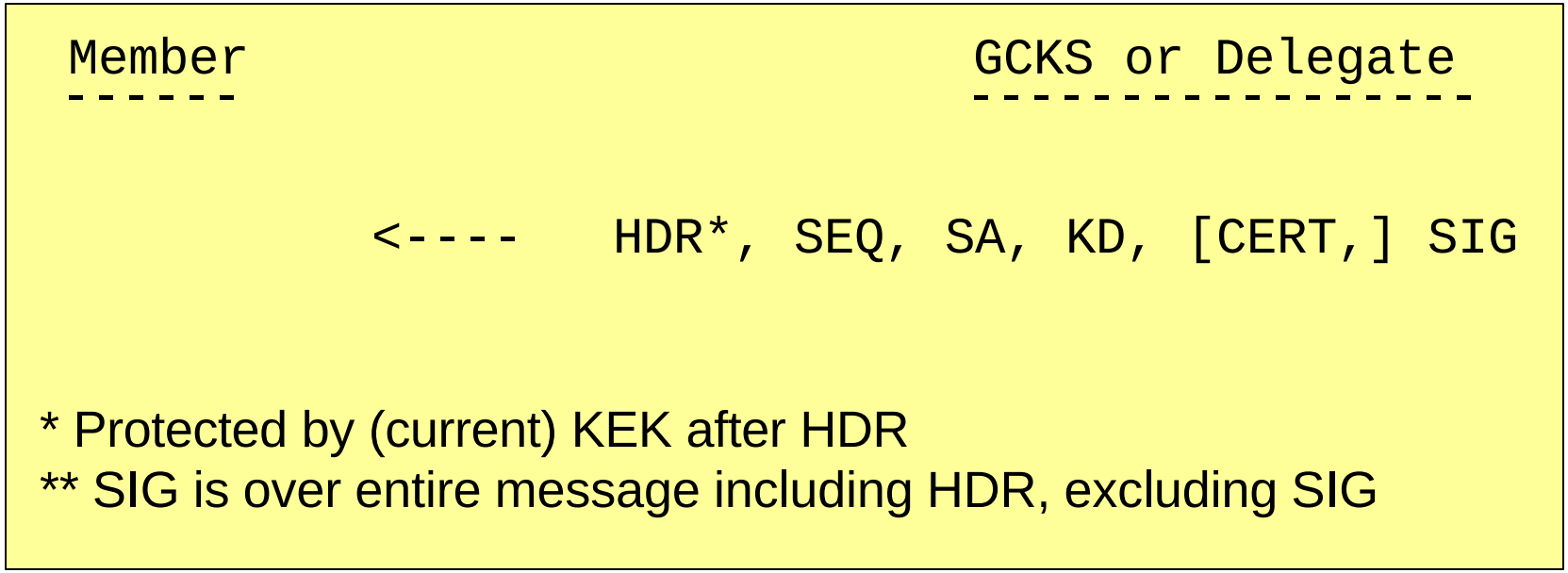

GCKS
Category-1 SA
Control Messages
(Multicast)
Initial Setup
(unicast)
Initial Setup
(unicast)
Category-2 SA
Member
(Sender)
Member
(Receiver)
Data
Messages
(Multicast)
Category-3 SA

“Pull” Protocol

```
Initiator (Member)                  Responder (GCKS)
-----------------                   ----------------

HDR*, HASH(1), Ni, ID       -->

                            <--     HDR*, HASH(2), Nr, SA

HDR*, HASH(3) [, KE_I]      -->
         [,CERT] [,POP_I]

                            <--     HDR*, HASH(4), [KE_R,] SEQ, KD
                                                    [,CERT] [,POP_R]

* Protected by IKE Phase 1 SA Hashes, encryption occurs after HDR
```

```
  HASH(1) = prf(SKEYID_a, M-ID | Ni | ID)
  HASH(2) = prf(SKEYID_a, M-ID | Ni_b | Nr | SA)
  HASH(3) = prf(SKEYID_a, M-ID | Ni_b | Nr_b [ | KE_I ] [| POP_I])
  HASH(4) = prf(SKEYID_a, M-ID | Ni_b | Nr_b [ | KE_R ] | SEQ | KD [| POP_R])
```

“Push” Message



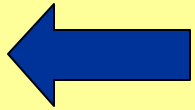
The “cookie pair” in the ISAKMP HDR acts as a SPI which identifies the group.

Group DOI for ISAKMP

Background Concepts

Group DOI Flows & Payloads

Proof of Concept Testing



Current Status & Future Plans

Proof of Concepts

- We started with the assertion that it would be reasonable to add GDOI to an IKE implementation.
- But is it really?
- A proof of concept test was done using the freely available *isakmpd* package.

Prototyping with isakmpd

- *isakmpd* is very modular, focused around DOI-specific functions.
- *isakmpd* has a well-defined state machine.
- New policy configuration statements can be added without affecting existing code.

Prototyping Results

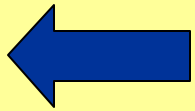
- The Group DOI “pull” exchange was added to *isakmpd* in less than 2,000 lines of code.
- This represents < 10% increase in overall code size.
- Less than 400 (out of 28,000) existing lines were modified, nearly all to accommodate multiple DOIs.

Group DOI for ISAKMP

Background Concepts

Group DOI Flows & Payloads

Proof of Concept Testing

Current Status & Future Plans 

Current status

- Latest draft:

  http://www.securemulticast.org/draft-irtf-smug-gdoi-01.txt
- Two independent implementations being written (Cisco and Nortel).
- Group DOI protocol specification under evaluation by Catherine Meadows, NRL.

Future Plans

- Revise the draft as necessary.
  - Fix inconsistencies
  - Investigate features necessary to support large groups.
- Complete the reference implementations and test with multicast applications.
  - Show interoperable implementations.
  - Add support for LKH key trees for scalability.