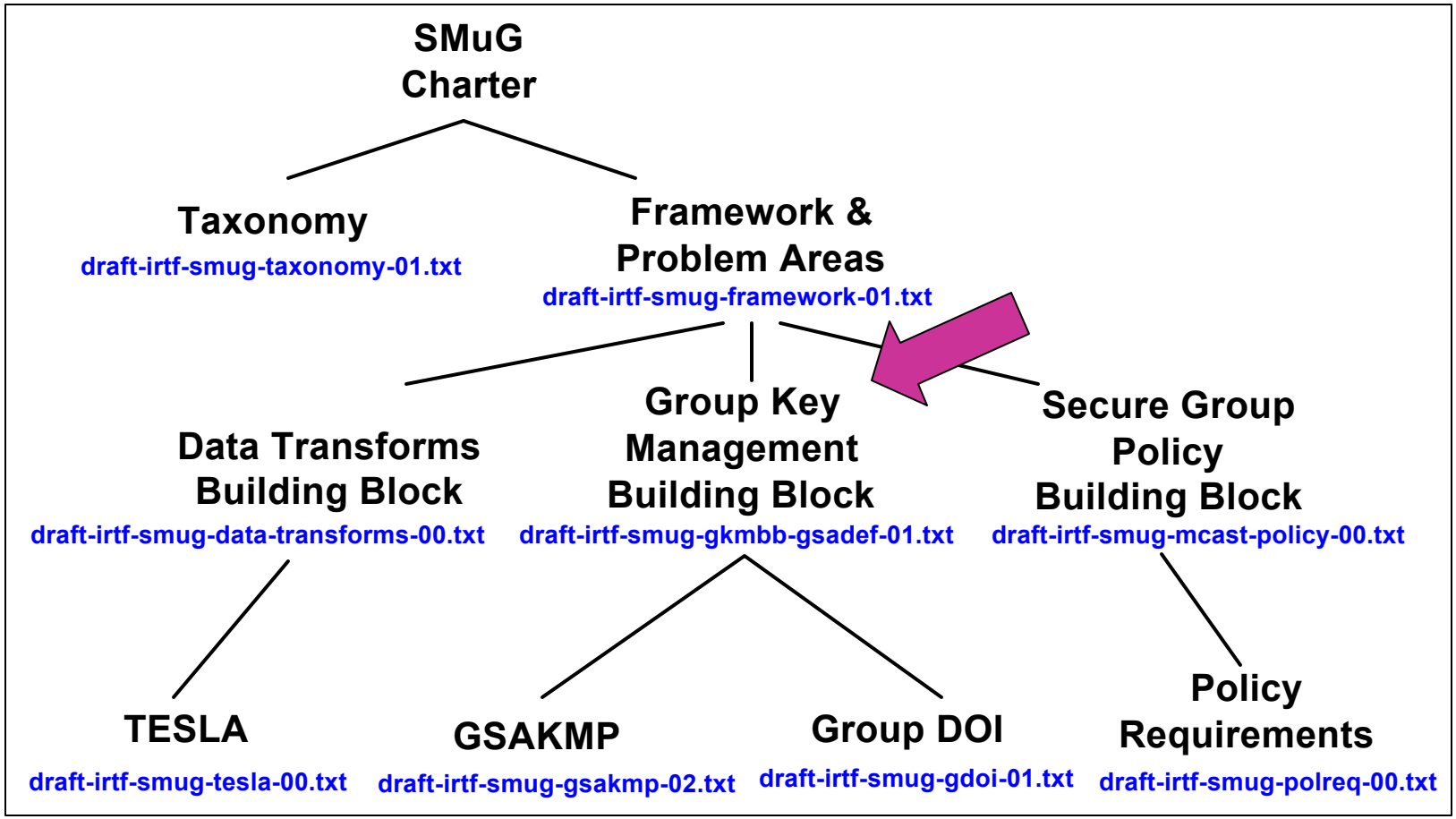
GKM Building Block: Group Security Association Definition

<draft-irtf-smug-gkmbb-gsadef-00.txt>

Hugh Harney (Sparta)
Mark Baugher (PassEdge)
Thomas Hardjono (Nortel)

(You Are Here)


SMuG Charter
Taxonomy
draft-irtf-smug-taxonomy-01.txt
Framework & Problem Areas
draft-irtf-smug-framework-01.txt
Data Transforms Building Block
draft-irtf-smug-data-transforms-00.txt
Group Key Management Building Block
draft-irtf-smug-gkmbb-gsadef-01.txt
Secure Group Policy Building Block
draft-irtf-smug-mcast-policy-00.txt
TESLA
draft-irtf-smug-tesla-00.txt
GSAKMP
draft-irtf-smug-gsakmp-02.txt
Group DOI
draft-irtf-smug-gdoi-01.txt
Policy Requirements
draft-irtf-smug-polreq-00.txt

Background & Requirements

- Key management for groups more complex than for point-to-point:
  - Type of application
  - 1-to-M or M-to-M
  - Scalability requirements
  - Group size & membership dynamicity:
    - small interactive groups, dynamic, minimal latency
    - large "broadcast" groups with users > 100K
- Two core components of GKMBB:
  - Group-key determination algorithm (eg. LKH)
  - Group Security Association management

Some Existing Work

- Algorithms: Wallner, Wong et al, LKH, OFT,...
- RFC 1949 (Ballardie)
- RFC 2093, 2094 on GKMP (Harney et al)
- NARK, MARKS (Briscoe et al)
- Cliques (Tsudik et al)
- Antigone (Umich)
- DCCM (NAI labs)
- VersaKey
- Iolus
- KHIP
- Others

Properties of Key Exchange

- Protection against various attacks:
  - man-in-the-middle, conn. hijacking, replay, etc.
- Diff protection levels in key establishment:
  - transforms, optional PFS, id protect, etc.
- Alternate authentication mechanisms:
  - shared key, PKI, public key, etc
- Forward migration path:
  - New transforms, new exchanges
- A single key management framework to support the establishment of SAs

Security Association (SA)

- An SA has selectors:
  - e.g. source and destination transport addresses
- An SA has properties:
  - e.g. security parameter index (SPI) or cookie pair, and identities.
- An SA has cryptographic policy:
  - e.g. algorithms, modes, key lifetimes, and key lengths for authentication/confidentiality.
- An SA has keys:
  - e.g. authentication, encryption and signing keys.

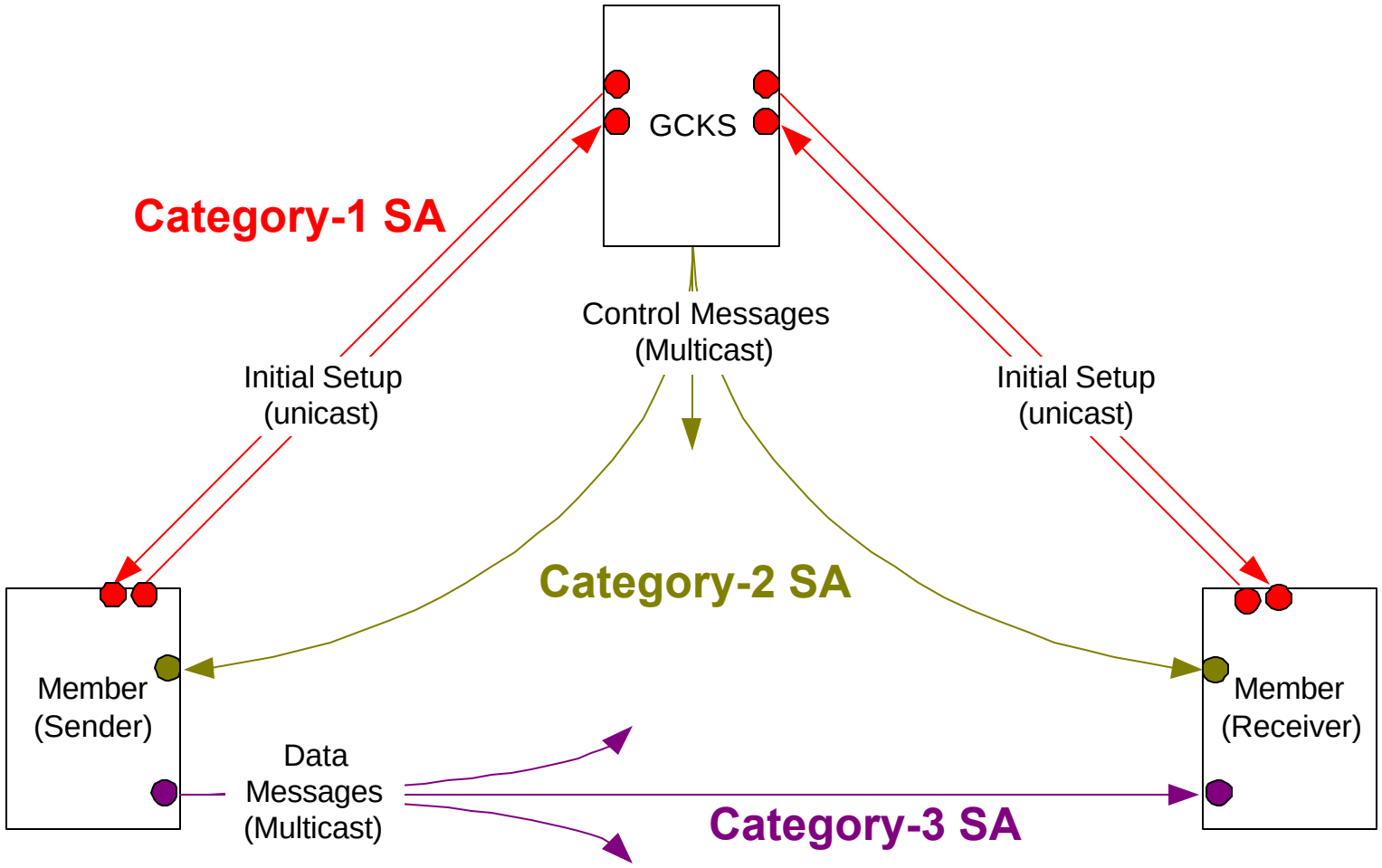
Properties of Group Key Exchange

- The previous five properties
- Support for the SMuG Framework
- Support for multiple senders where:
  - each may have a unique SA in the group
  - each share a common SA in the group
- Push/pull of keying material and policy
  - Member-initiated "pull" from the GCKS
  - GCKS-initiated "push" to the members
- Variable level of performance for group key management (latencies, rekeys, etc.)

GSA: Model & Definition

- A Group SA (GSA) is a super-set of SAs
  - A GSA has group policy attributes:
    - e.g. member credentials, back/forward rekey,…
  - A GSA has SAs as attributes
- A GSA is composed of 3 Categories of SAs
  - The three Categories of SAs are inseparable
  - An instance of a GSA has all three,
  - even if Category-2 or Category-3 is null in simple (centralized) key management protocols
- A unique Group ID identifies each group

GSA: Model & Definition



GSA: Category-1 SA

- Unicast (bi-directional) communications between the GCKS and member
- Used to protect the other elements of the GSA (i.e. Category-2 and Category-3 SAs), either in a "push" or "pull" model.
- There are as many unique Category-1 SAs as there are members in the group

GSA: Category-2 SA

- Multicast transmission of control messages from the GCKS to members
- Unidirectional
- Not negotiated:
  - GCKS is the sole point for members to obtain this Category-2 SA
  - This SA is known to GCKS and group members
- There is at least one Category-2 in a group:
  - Multiple Category-2 SAs possible
  - e.g. one for each Cat-3 (diff. types of media)

GSA: Category-3 SA

- Multicast transmission of data messages from a Sender to other group members
- Unidirectional
- Not negotiated: obtain it from the GCKS
- At least one Cat-3 SA for the Sender(s)
- Multiple sender case:
  - Unique Category-3 SA per Sender, or
  - One Category-3 SA for ALL Senders
    - Receivers filter based on GID and Source address
  - Combination of both

GSA Maintenance

- Keying material need to be updated:
  - Keys expire, compromises, joins/leaves, etc.
- Initial setup/registration from GCKS:
  - Cat-1 SA protects download of Cat-2 & Cat-3
- Cat-3 SA updates:
  - GCKS uses Cat-2 SA to multicast new Cat-3 SA
- Cat-2 SA updates: two options
  - "old" Cat-2 protects multicast of new Cat-2
    - Security concerns
  - New Cat-2 downloaded under Cat-1
    - Scalability issues

end