Multicast Security (MSEC) WG

IETF-55, Atlanta, GA

Tue, Nov 19, 2002

9:00 – 11:30

MSEC Agenda

- Agenda Bashing (5min)
- Review of WG Status (T. Hardjono/R. Canetti) (15min)
- MIKEY (E. Carrara/F. Lindholm) (15min)
- MESP draft (M. Baugher) (15min)
- TESLA Overview (M. Baugher) (15min)
- Key Management Arch (L. Dondeti/M. Baugher) (15min)
- MIKEY-DHHMAC (M. Euchner) (15min)
- IPsec signatures (B. Weis) (15min)
- Updates: (20min)
  - GDOI update (B. Weis/L. Dondeti)
  - GSAKMP Update (H. Harney)
- Discussion (20min)
  - Need to update Charter

MSEC Status Review IETF-55

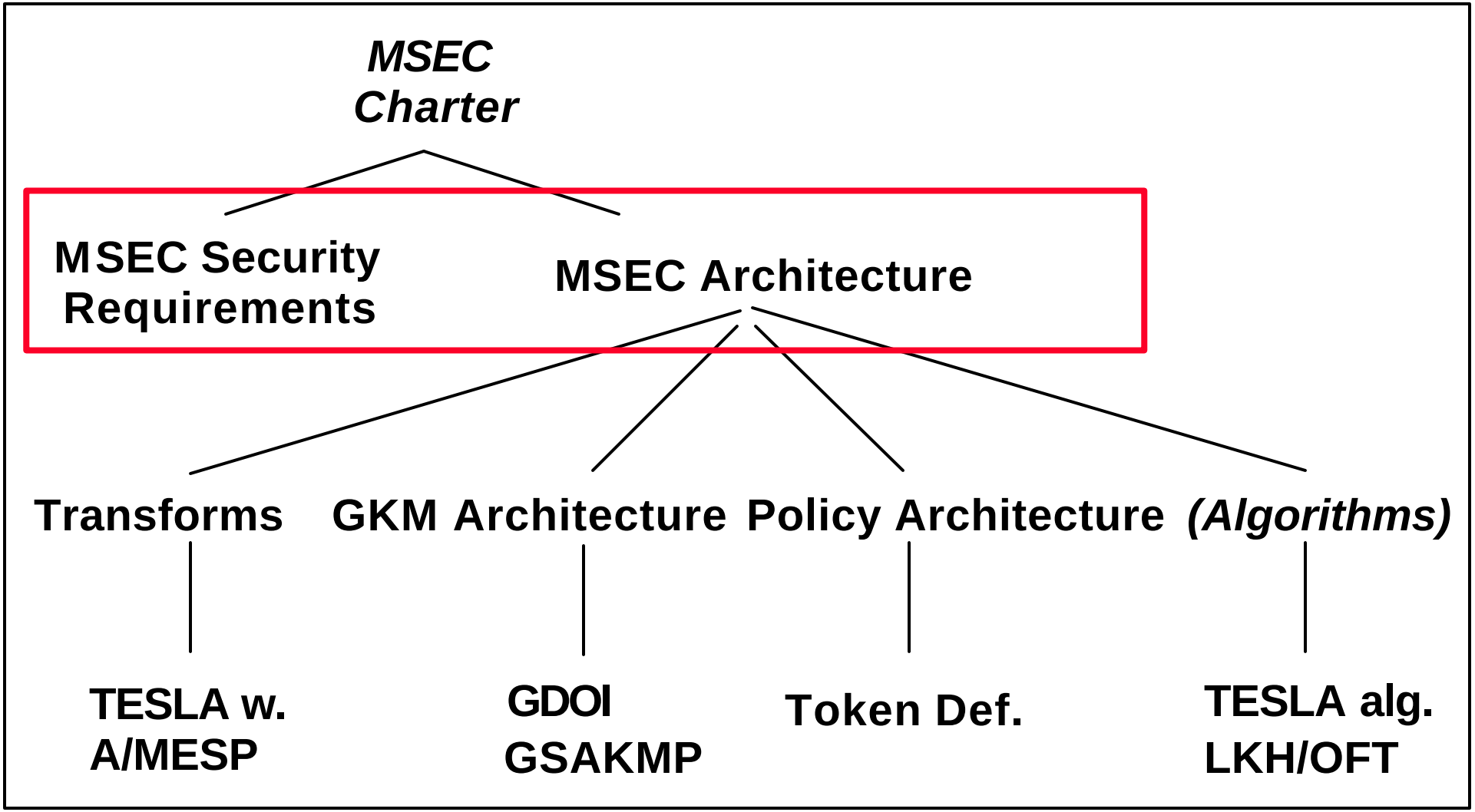
Thomas Hardjono

Non-expired MSEC documents

- Drafts:
  - draft-ietf-msec-gkmarch-03.txt
  - draft-ietf-msec-gsakmp-light-sec-01.txt
  - draft-ietf-msec-mesp-00.txt
  - draft-ietf-msec-tesla-spec-00.txt
  - Draft-ietf-msec-mikey-dhhmac-01.txt

- WG Last Call:
  - draft-ietf-msec-gdoi-06.txt
  - draft-ietf-msec-mikey-05.txt

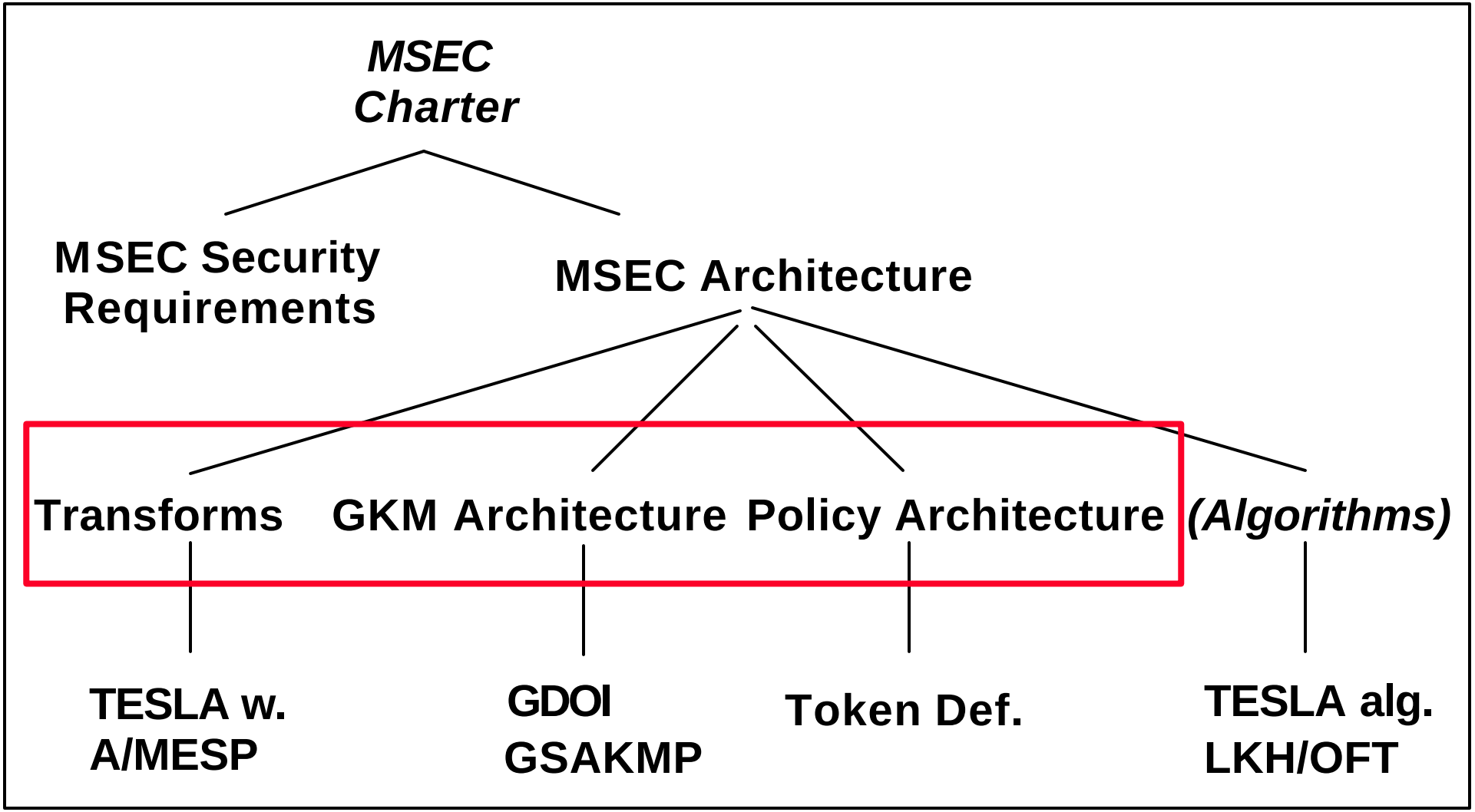
MSEC drafts tree



High-Level Drafts

- MSEC Requirements
  - (Based on *draft-irtf-smug-taxonomy-01.txt*)
  - Owner: Canetti et. Al.
  - Aim: Informational
  - Status: (upcoming)
- MSEC Architecture
  - Currently: *draft-ietf-msec-arch-00.txt*
  - Owner: Hardjono/Weis
  - Aim: Informational
  - Status: Work in Progress

MSEC drafts tree



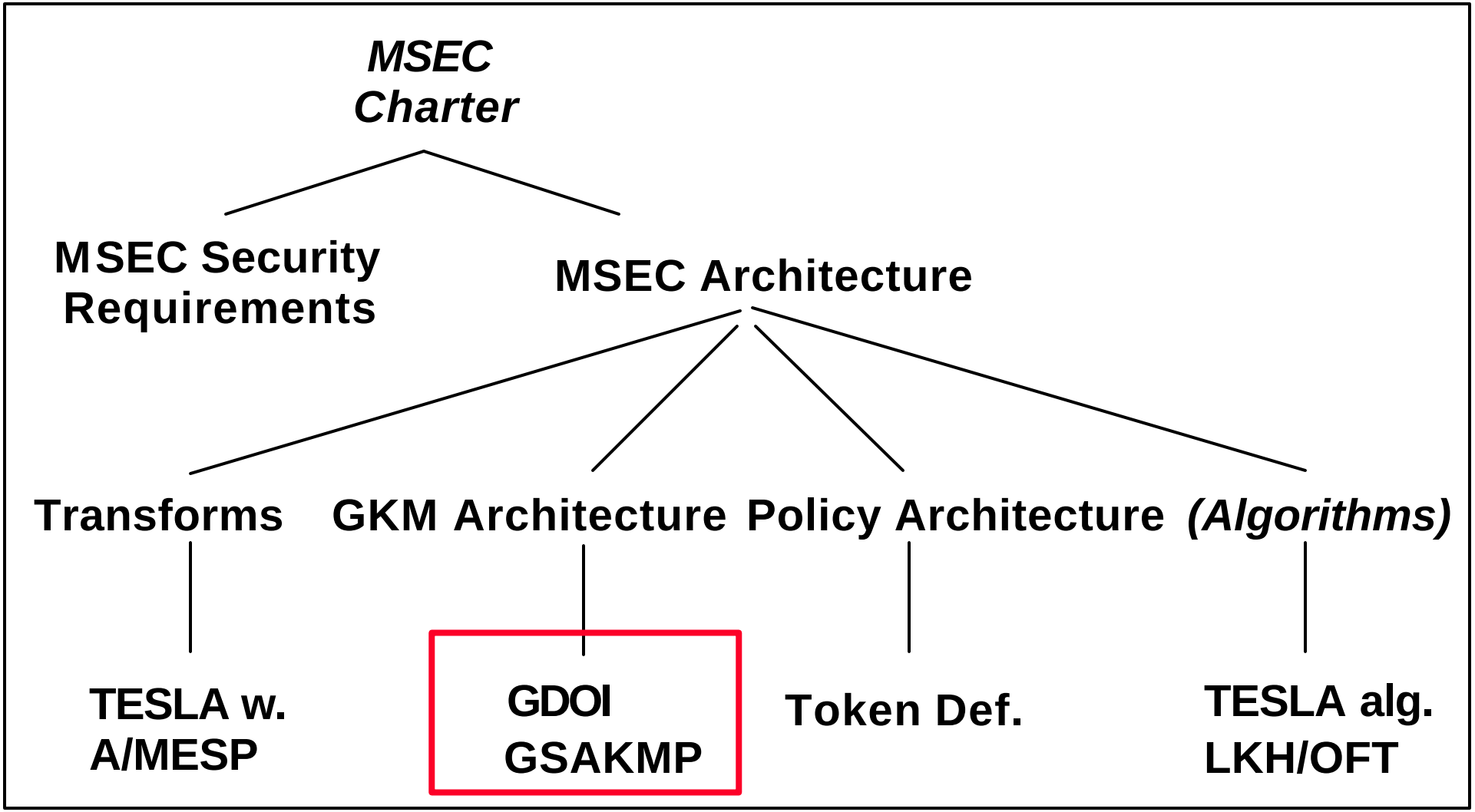
Architecture/Functionalities

- Multicast ESP (MESP):
  - Currently: *draft-ietf-msec-mesp-00.txt*
  - Owner: Canetti et. Al.
  - Aim: Standards
  - Status: Work in Progress
- Group Key Management Architecture
  - Currently: *draft-ietf-msec-gkmarch-03.txt*
  - Owner: Baugher et. Al.
  - Aim: Standards
  - Status: Work in Progress

Architecture/Functionalities (cont)

- Group Security Policy Architecture
  - Based on:
    - *draft-irtf-smug-polreq-00.txt*
    - *draft-irtf-smug-mcast-policy-00.txt*
    - *draft-ietf-msec-gspt-01.txt*
  - Owner: ?
  - Status:
    - Only GSPT draft has been submitted to MSEC
      - Expired
  - Comments:
    - Need to investigate relationship of group-security-policy with other WGs in the IETF
    - Needs someone to drive this. (See last slide)

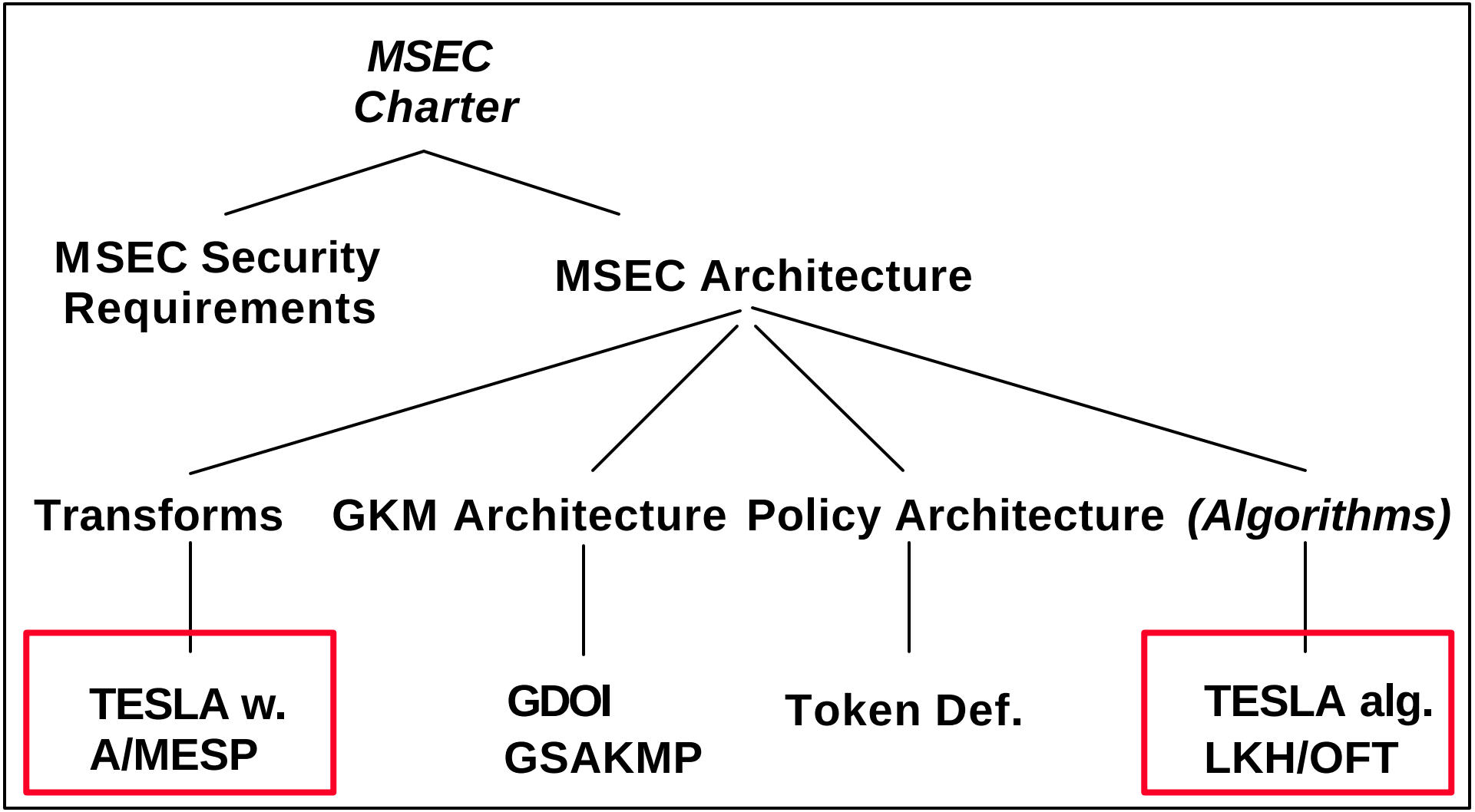
MSEC drafts tree



GKM Protocols

- Group DOI (GDOI):
  - Currently: *draft-ietf-msec-gdoi-06.txt*
  - Owner: Weis et al.
  - Aim: Standards
  - Status: finished Last Call (issued 1/18/2002)
- MIKEY
  - Currently: *draft-ietf-msec-mikey-05.txt*
  - Owner: Lindholm et al.
  - Aim: Standards
  - Status: finished Last Call (issued 8/28/2002)
- GSAKMP-Light
  - Currently: *draft-ietf-msec-gsakmp-light-sec-01.txt*
  - Owner: Harney et al.
  - Aim: Standards
  - Status: Work in Progress

MSEC drafts tree



Protocols & Algorithms (cont)

- TESLA with A/MESP:
  - Specific usage of TESLA with A/MESP
  - Owner: Canetti/Perrig
  - Status: to be submitted to MSEC (?)
- TESLA algorithm
  - Currently: *draft-ietf-msec-tesla-spec-00.txt*
  - Owner: Perrig/Canetti
  - Aim: Standards
  - Status: Work in Progress
- DHHMAC for MIKEY
  - Currently: *draft-ietf-msec-dhhmac-00.txt*
  - Owner: Euchner
  - Aim: Informational or Standards
  - Status: Work in Progress

Protocols & Algorithms (cont)

- LKH/OFT algorithm:
  - Based on:
    - *draft-irtf-smug-groupkeymgmt-oft-00.txt (OFT)*
    - *draft-harney-sparta-lkhp-sec-00.txt (LKH)*
  - Owner: Dondeti/McGrew
  - Status:
    - to be written; algorithm only, independent of any key management protocols
- Policy Token definition & structure
  - Based on *draft-ietf-msec-gspt-01.txt*
  - Status:
    - GSAKMP PT may not cover all info required for session and membership management
  - Owner: open?, maybe based on GSAKMP policy token

Open Issues

- GSAKMP to Informational:
  - Background & supplement for implementers of GSAKMP-Light
  - Preserved for historical purposes
  - Maybe of interest to external (non-IETF) organizations

END