MSEC Status Review

Thomas Hardjono

IETF-52, Salt Lake City

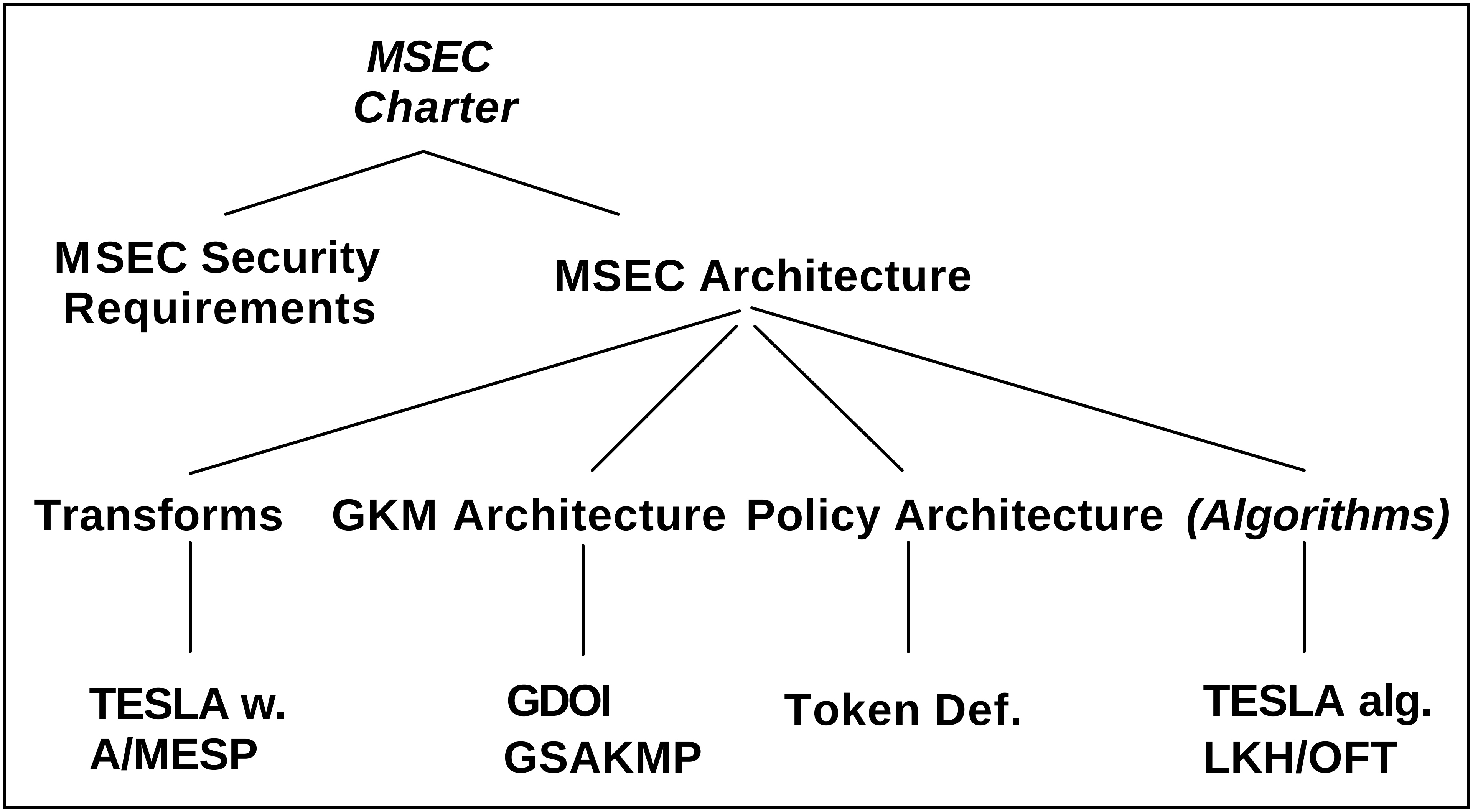
Fri, Dec 14, 2001

9:00 – 11:30

Review of WG Status

- Charter
  - Has a specific set of deliverables
  - Has an approximate completion date
  - 3 general types of documents:
    - High level or framework drafts
    - Architecture/functionalities drafts
    - Protocols and Algorithms drafts
- Charter is open to additional work
  - MIKEY
  - Group Management Security
  - Others

MSEC Drafts Tree



MSEC Charter

MSEC Security Requirements

MSEC Architecture

Transforms

GKM Architecture

Policy Architecture

(Algorithms)

TESLA w. A/MESP

GDOI GSAKMP

Token Def.

TESLA alg. LKH/OFT

High-Level Drafts

- Security Requirements
  - Based on *draft-irtf-smug-taxonomy-01.txt*
  - Owner: Canetti
  - Aim: Informational
  - Status: in writing
- MSEC Architecture
  - Based on *draft-irtf-smug-framework-01.txt*
  - Owner: Hardjono/Baugher
  - Aim: Standards Track
  - Status: in writing

Architecture/Functionalities

- Data Transforms (A/MESP):
  - Based on *draft-irtf-smug-data-transforms-00.txt*
  - Owner: Canetti
  - Aim: Standards
  - Status: expired in SMuG, will be updated and submitted to MSEC
- Group Key Management Architecture
  - Based on *draft-ietf-msec-gkmarch-01.txt*
  - Owner: Baugher/Dondeti/Canetti
  - Aim: Standards
  - Status: v.01/current

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, though GSAKMP carries some policy-related items
  - Comments:
    - Need to investigate relationship of group-security-policy with other WGs in the IETF
    - Needs someone to drive this. (See last slide)

Protocols & Algorithms

- Group DOI (GDOI):
  - Based on *draft-ietf-msec-gdoi-02.txt*
  - Owner: Weis et al.
  - Status: v.02/current
- GSAKMP & GSAKMP-Light
  - Based on:
    - *draft-ietf-msec-gsakmp-sec-00.txt*
    - *draft-ietf-msec-gsakmp-light-sec-00.txt*
  - Owner: Harney et al.
  - Status: v.00/current

Protocols & Algorithms (cont)

- TESLA with A/MESP:
  - Specific usage of TESLA with A/MESP
  - Owner: Canetti/Perrig
  - Status: to be written
- TESLA algorithm
  - Based on *draft-irtf-smug-tesla-00.txt*
  - Owner: Perrig/Canetti
  - Status:
    - Expired, will be submitted to MSEC
    - Focus on algorithm only, independent of any transport or implementation

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

Other Issues

- Group Policy:
  - Different types of policy:
    - Membership policies for groups (cf. MAGMA)
    - Security mechanisms policies (for different components, e.g. Cat-1, Cat-2, Cat-3, etc.)
    - Policies for managing GCKSs
    - Rules for bootstrapping a group
    - Rules for disaster recovery (e.g. dead groups)
  - Need overall architecture for these policies
  - Need way to make these policies known to the appropriate consumers (announcement)
  - Should policy be driven by applications of group security

END