

SECURE COMMUNICATION FOR AD-HOC, FEDERATED GROUPS

Andreas Sjöholm
andreas@axiomatics.com

Axiomatics AB
Swedish Institute of Computer Science

Babak Sadighi
Axiomatics AB
SICS

Ludwig Seitz
SICS

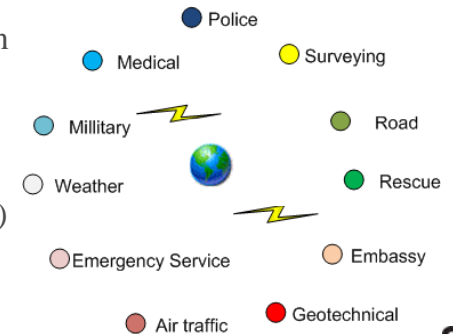
SCENARIO

Severe accident



• Group collaboration goal

• Can involve many organizations (nodes)



THE EMERGING EVERNET

A federated collaborative group

- An in common goal
- No intra-knowledge between nodes
- Dynamic infrastructure and group composition
- Uses the Evernet as medium

PROBLEM

- How can confidentiality and integrity be ensured?
- Who may join a group?

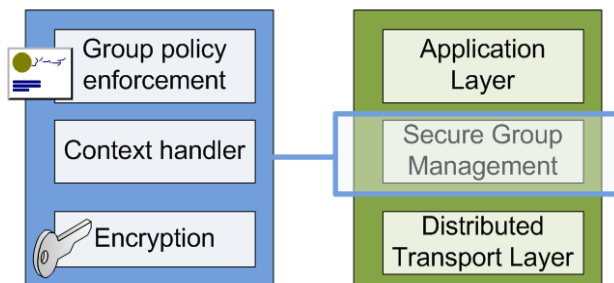
The ad-hoc and federal structure of the group worsen the situation.

A MIDDLEWARE SOLUTION

Group policy enforcement

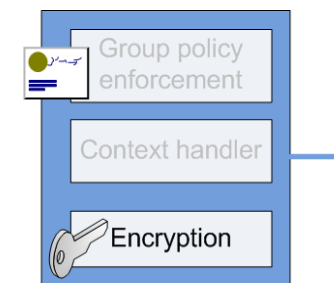
Context handler

Encryption/ Integrity



GROUP KEY DISTRIBUTION

- Contributory / Key dealer / TTP ?
- Symmetric / Asymmetric ?

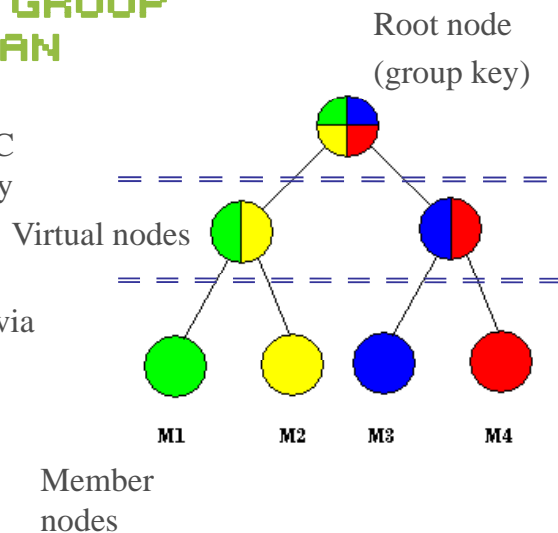


- Computational and decisional group key secrecy
- Implicit key authentication

TREE-BASED GROUP DIFFIE-HELLMAN

Proposed in 2004 at UC Irvine and UC Berkeley

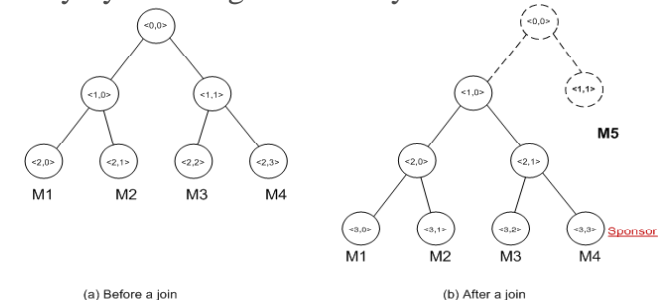
Apply two part DH recursively to a group via binary tree



TGDH

DH :

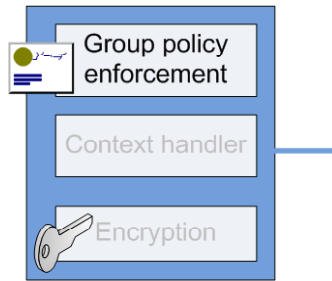
Two nodes (siblings) can compute an in common (parent) secret key by knowing its own key and the other's blinded key.



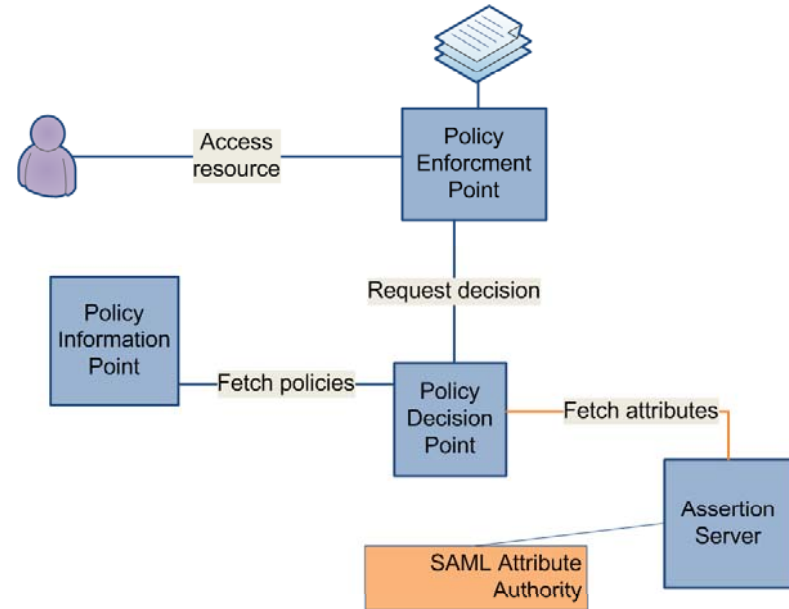
TGDH:

A member (leaf) can compute the master key, $k<0,0>$, by knowing all ancestors' keys and knowing the blinded keys of all ancestors' direct siblings.

ACCESS CONTROL AND TRUST

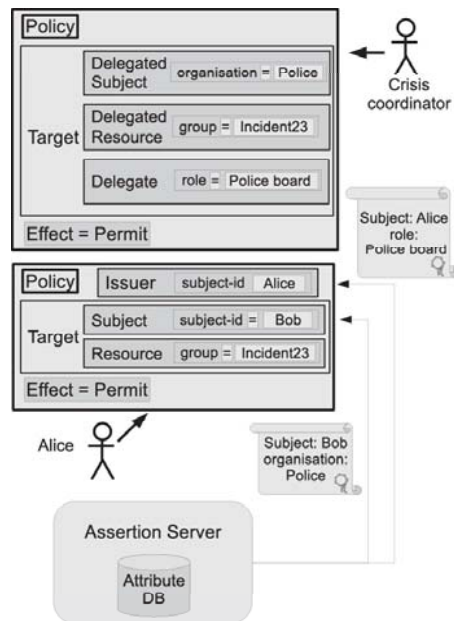


XACML – eXtensible Access Control Markup Language
 SAML – Secure Assertion Markup Language
 Assertion Server
 PKI

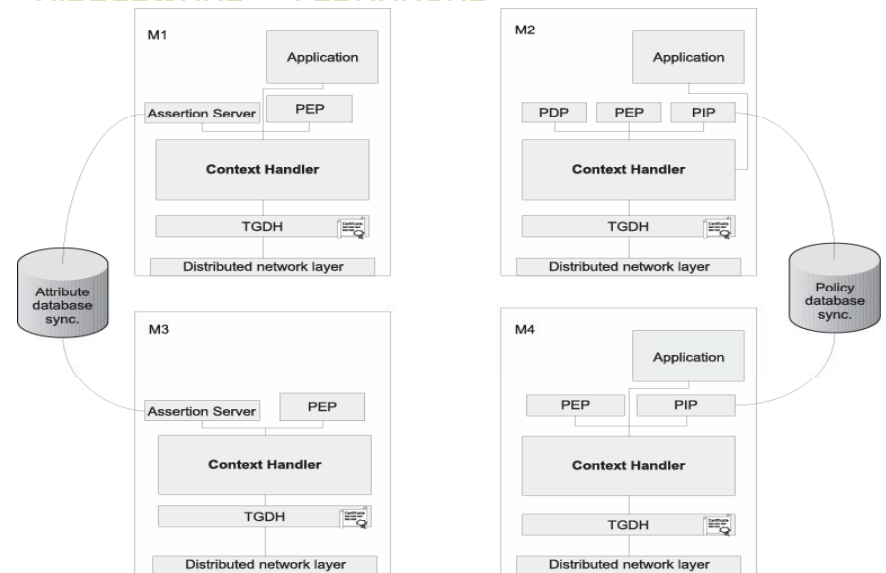


ATTRIBUTE ASSERTION & DELEGATION

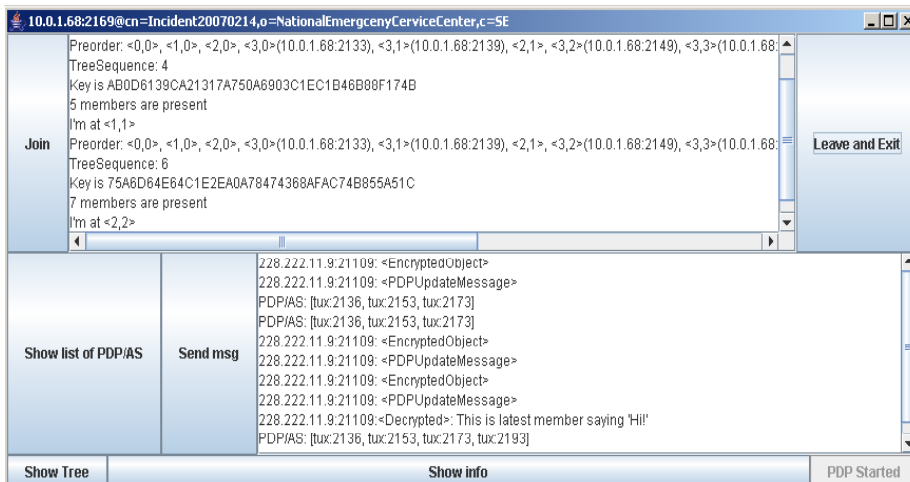
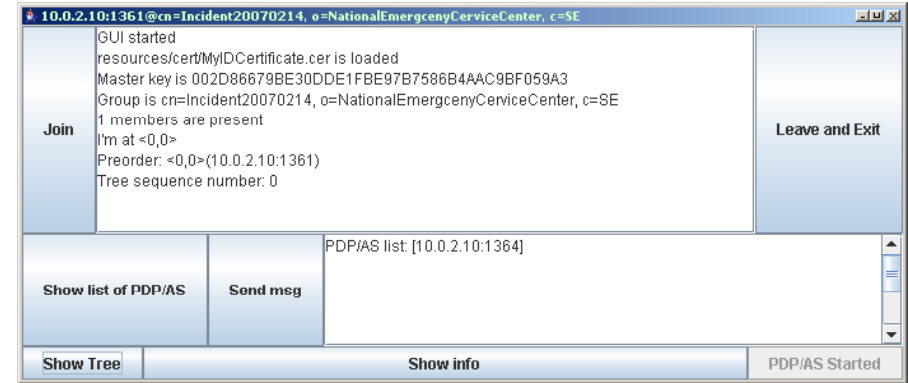
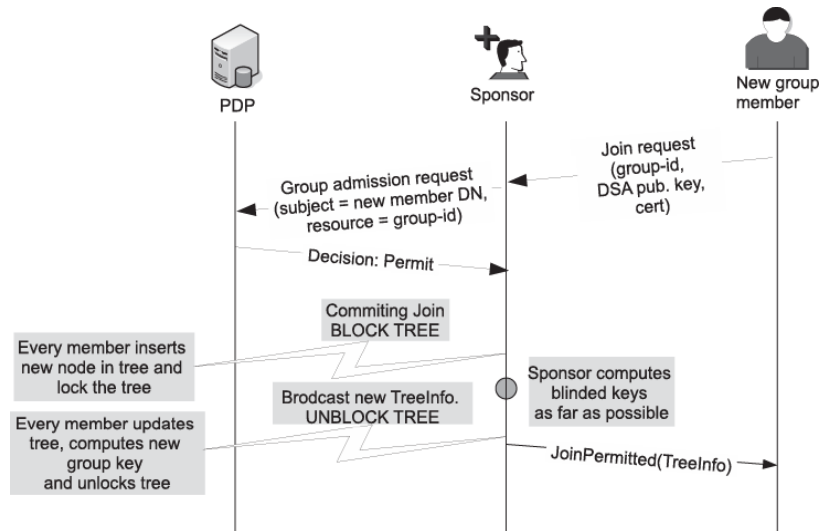
1. CC delegates resource *group: incident123*
2. Alice has attribute *role: Police Board*
3. Alice creates administrative policy targeting Bob
4. Bob can access group



MIDDLEWARE - TGDHXACML



JOIN EVENT



DISCUSSION

- XACML/SAML too excessive
- Block-free TGDH
- Sync of data (policies, assertions)
- Questions?