Annual Conference of ITA

ACITA 2009

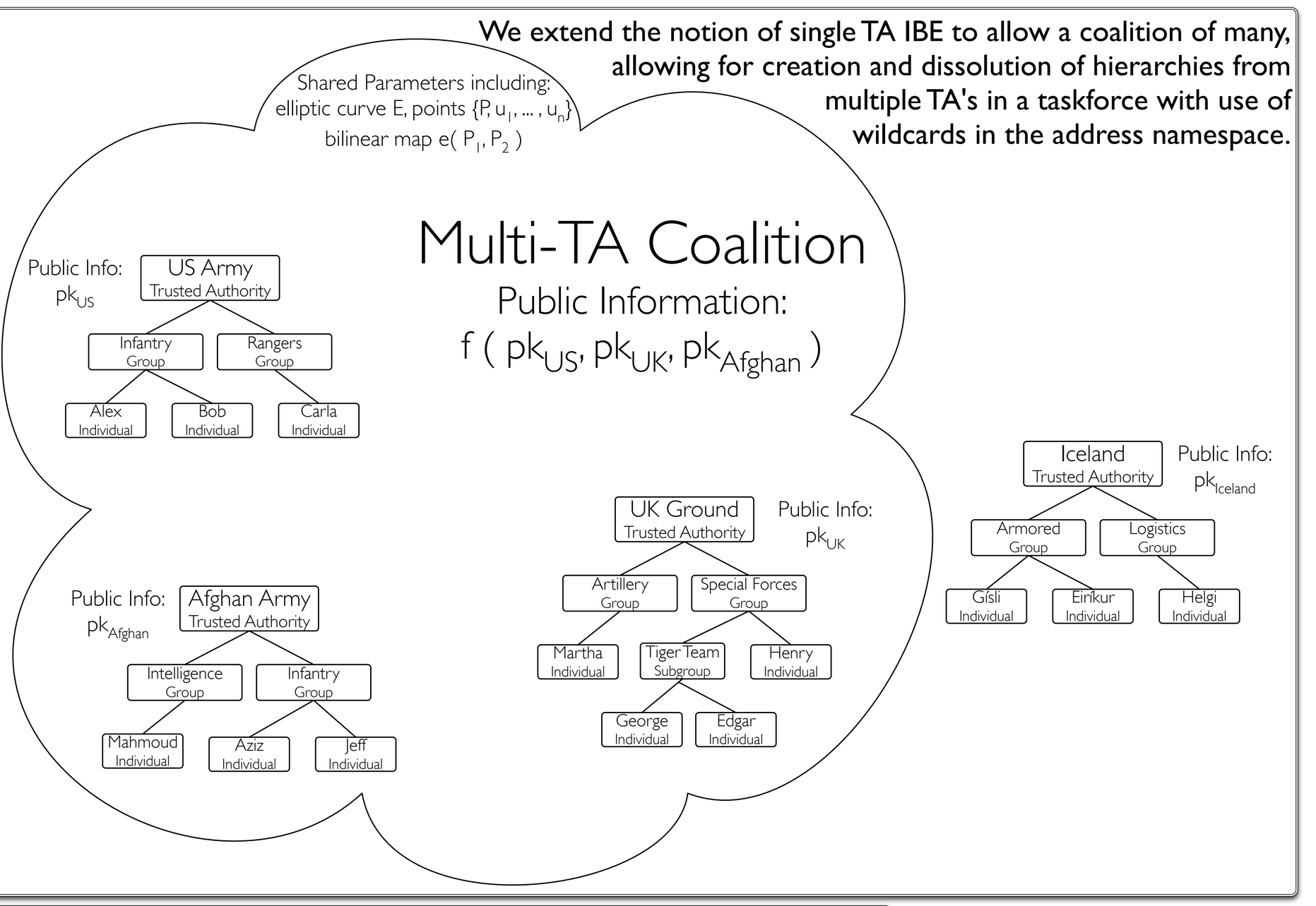
Broadcast Encryption with Multiple Trust Centers and Dynamic Coalitions

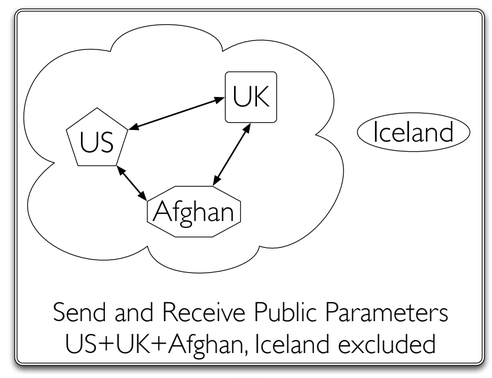
Christopher A. Seaman
Graduate Center
City University of New York

Kent D. Boklan
Queens College
City University of New York

Alex W. Dent
Royal Holloway
University of London

We extend the notion of single TA IBE to allow a coalition of many, allowing for creation and dissolution of hierarchies from multiple TA's in a taskforce with use of wildcards in the address namespace.



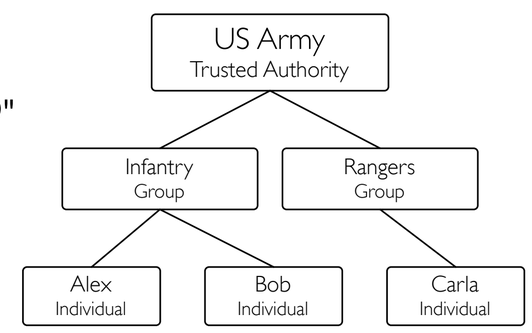


Features

- Multi-TA Identity-Based Encryption (IBE)
- No public key infrastructure (PKI)!
- Broadcast messages using wildcards
- Dynamic coalition membership
- Expelled members gain no future advantage against new coalitions

Namespace & Hierarchies

- Name reflects structure
- Old way: "Bob #123456789"
- New: (US, Infantry, Bob)
- Bob's Unit: (US, Infantry, *)



Wildcards

- One-to-many Communication
- (US, Infantry, Bob)
- (US, Infantry, *)
- (US, *, *)