ABFAB Multihop Federations
draft-mrw-abfab-multihop-fed-01.txt

Margaret Wasserman
mrw@painless-security.com

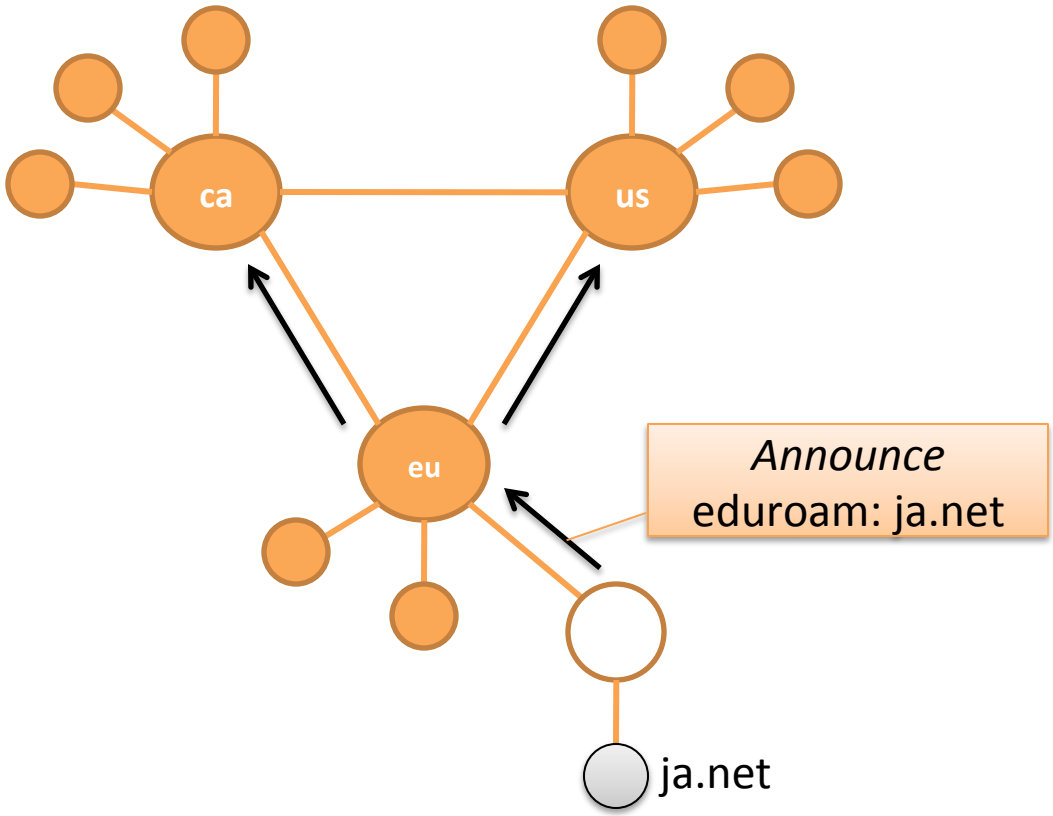
Why Am I Here?

- Published new draft on how to support a Multihop Federations in ABFAB
  - draft-mrw-abfab-multihop-fed-01.txt
- Presenting new technical work we are doing on top of the core ABFAB framework
  - This work is not in the ABFAB charter (yet)
  - Not asking the WG to adopt this work (yet)
- Here to get your feedback/comments

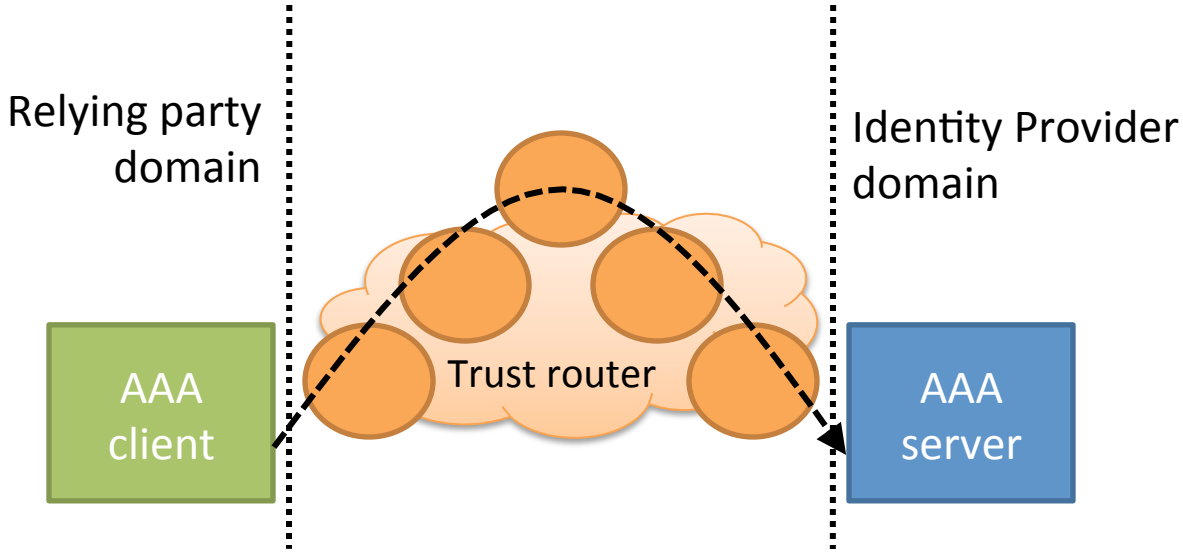
Multihop Federations

- Draft describes a mechanism for establishing trust across a multihop ABFAB federation
  - Where not all AAA Clients and Servers are connected via a single AAA server
  - Replaces current multihop AAA substrate with manual configuration at every hop
- Introduces a new ABFAB entity called the Trust Router
  - Trust router and KNP are combined to provide support for multihop federations

Trust router protocol

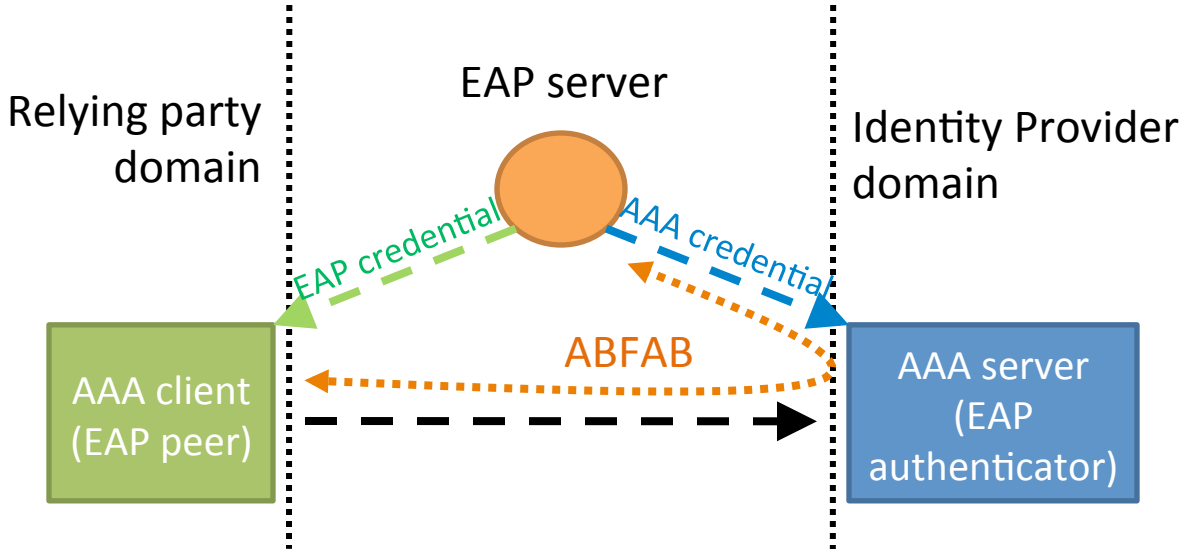


RADIUS substrate



- **Trust Router allows path selection through the AAA fabric**
- **But, static configuration is still required at each hop for trust establishment**

RadSec with ABFAB



- **Allows trust to be established using ABFAB, not PKI**
- **However, not all AAA clients and AAA servers in a large federation will be connected via a single AAA server**

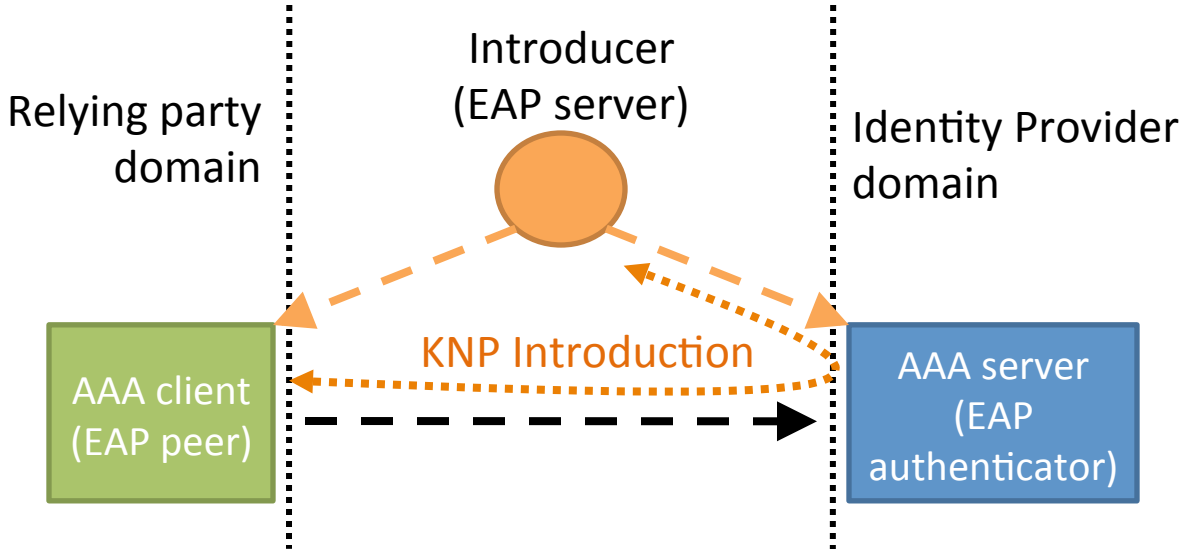
Key Negotiation Protocol

- KNP enables a RadSec client and server to dynamically establish a short-lived credential for a subsequent RadSec connection.

- KNP uses EAP authentication of credentials issued to the AAA client by an EAP server that is also trusted by the AAA server.

- The EAP server is called the ‘Introducer’. The process of establishing the RadSec credential between AAA client and server is called ‘Introduction’.

KNP Introduction

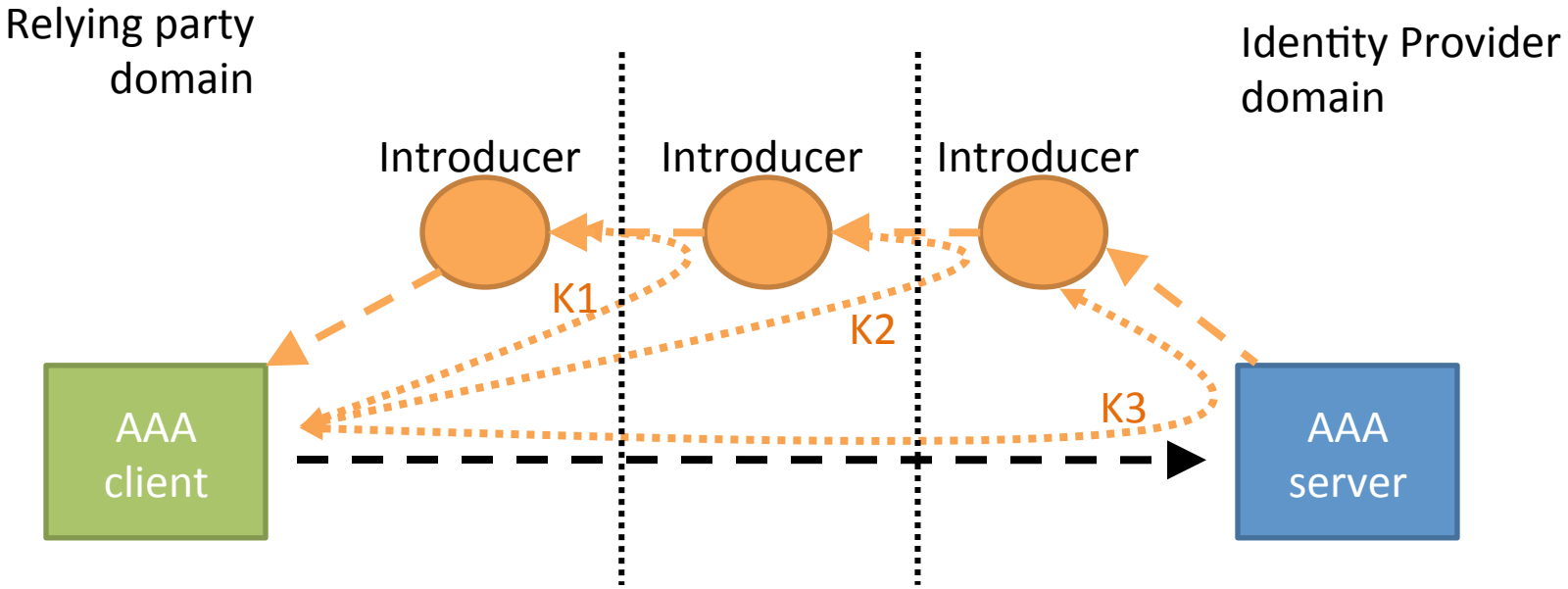


When an AAA Client and a AAA Server are connected via a single KNP Introducer, this is referred to as a Trust Link

Transitive operation

- Not all AAA nodes share a common Introducer.
- An Introducer can also be party as AAA client or server to an Introduction.
- This enables transitive introduction: the AAA client recurses along a path of Introducers to the AAA server.

Transitive Use of KNP



- **When a AAA Client can reach a AAA Server through a chain of KNP Introducers, this is a Trust Path**
- **How does the RP know what path to traverse? It asks it's local Trust Router!**

Trust Link

- A Trust Link represents an available KNP hop between a Trust Router and and another Trust Router or a AAA Server
- A Trust Link is an assertion that a Trust Router is willing to provide temporary identities to access another element in the ABFAB system
  - Another Trust Router
  - Or a AAA Server (Radius, RadSec or Diameter)
- Shown as a realm name and realm name (type), separated by an arrow
  - A->B(T) indicates there is a Trust Link from realm A to a Trust Router in realm B
  - ja.net -> oxford.ac.uk(R) indicates there is a Trust Link from ja.net to a AAA Server in oxford.ac.uk

Trust Path

- A Trust Path is a series of KNP hops that can be used to reach a AAA server in a destination realm
- Each KNP hop is called a Trust Link
- Shown as series of realms and types, connected by arrows
  - Currently defined types are Trust Router (T) or AAA Server (R)
  - Example: A -> B(T) -> C(T) -> D(T) -> D(R)

Trust Router Functions

- Trust Router Protocol
  - Distributes information about available Trust Links in the network
  - Calculates a tree of Trust Paths to reach target destinations
- Trust Path Query
  - Provide “best” path to a destination realm in response to queries from local RPs
- Temporary Identity Request
  - Provision temporary identities that RPs can use to reach the next hop in the Trust Path, in response to KNP requests from RPs
  - AKA, serve as a KNP Introducer

Trust Router Protocol

- Exchange information about Trust Links between Trust Routers
  - Trust Links are unidirectional and of a specific type
    - A -> B(T) does not imply A -> B(R), B -> A(T) or B -> A(R)
  - Realm names are not necessarily hierarchical, but they may be
    - example-u.ac.uk is not necessarily reached via .uk or .ac.uk
- Tree of available Trust Paths rooted in local realm is calculated by each Trust Router

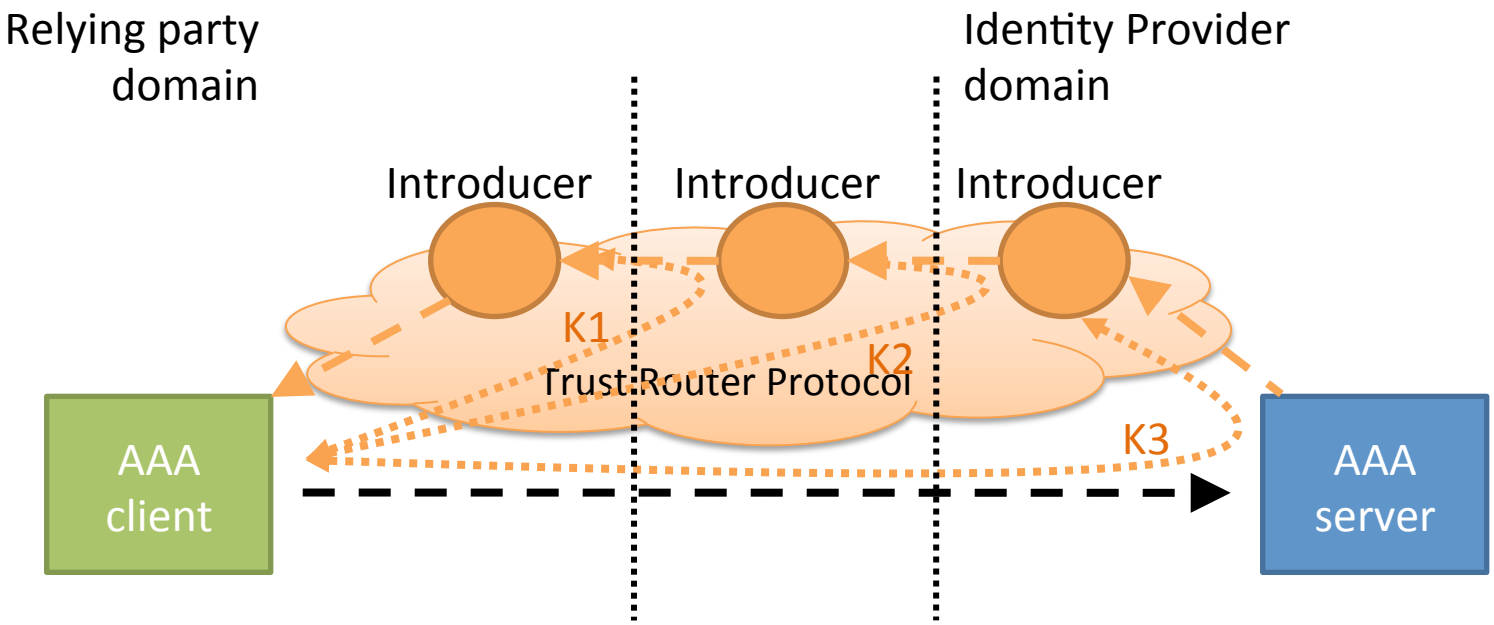
Trust Path Query

- Generated by an RP to request a Trust Path to reach a AAA server in a destination realm
- When a Trust Path Query is received, the Trust Router:
  - Authenticates the RP, and checks local policy to determine whether or not to reply
  - Searches its tree of Trust Paths to find the best path to reach the destination
  - Returns the best path, if found, to the RP

Temporary Identity Request

- The RP issues a Temporary Identity Request to obtain an identity that will be used to traverse each link in the Trust Path
  - The existence of the Trust Link implies that a Temporary Identity Request will be granted

ABFAB Multihop Federation



- **Uses ABFAB, KNP and Trust Routers to allow RPs to reach AAA Servers in all destination realms that can be reached through a transitive Trust Path across the federation**
- **Minimal per-hop configuration, as needed to define one-to-one trust relationships and express local policy**

This Week

- Presented Trust Router concept in RADEXT and OpsArea
  - Received constructive feedback
  - No major objections raised from the AAA community, but there was some discussion about alternative solutions

Questions? Feedback?

- Questions about what we are proposing?
- Feedback on this proposal?