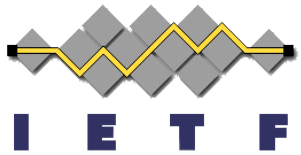
Diameter Security

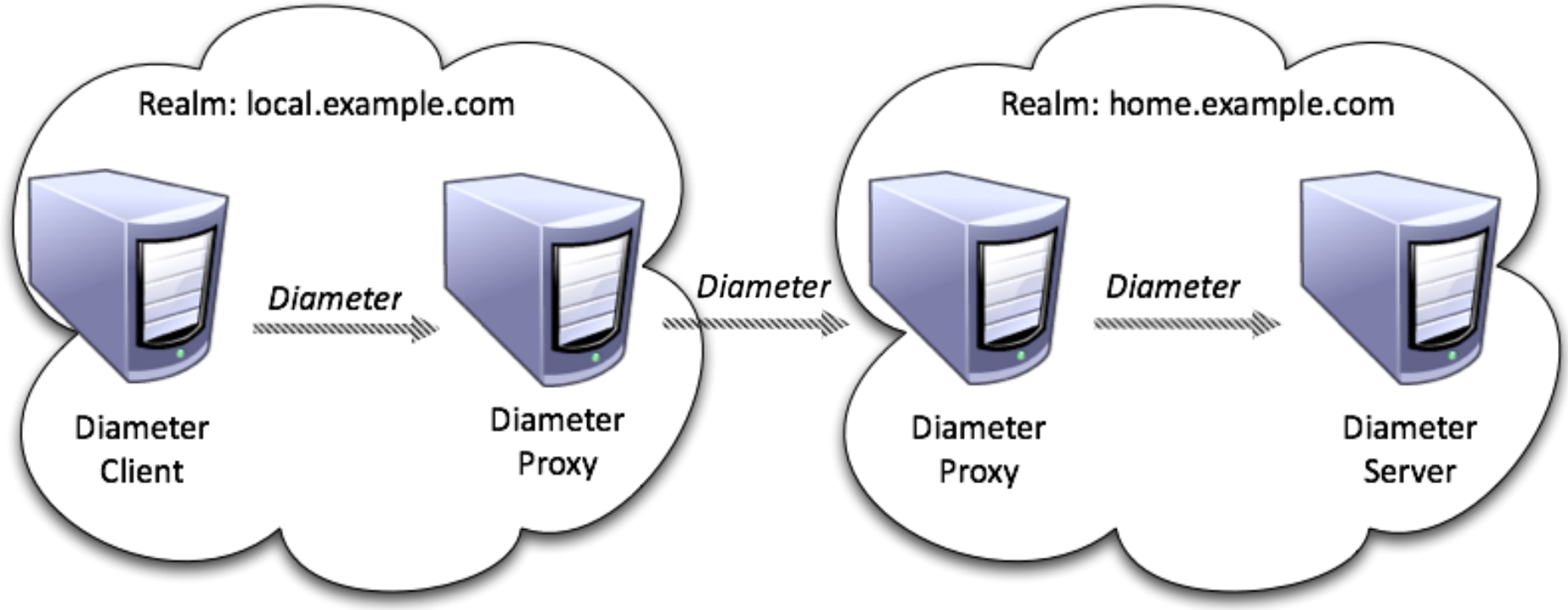
DIME WG

IETF 86

March, 2013



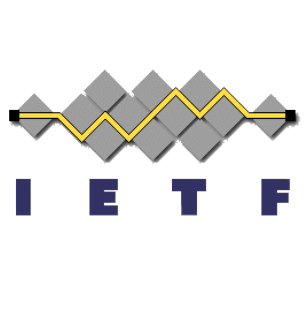
Which Scenarios do we want to cover?



Possible Examples:

- Client<->Server
- Proxy<->Proxy
- Proxy<->Server

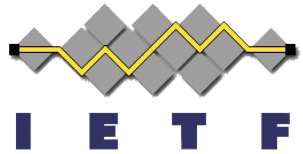
Requirements



- Crypto Agility
- Data origin authentication, integrity and confidentiality.
- Backwards compatibility with existing Diameter Applications
- Replay protection (based on timestamps)
- Selectively apply protection to certain AVPs (assuming some out-of-band agreement?)
- Mandatory to implement cryptographic algorithms
- Symmetric keys and/or asymmetric key support?
- Requirements regarding automatic key management (assumptions about PKI?)
- Support for statically provisioned keys
- How to provision long term keying material and other parameters?

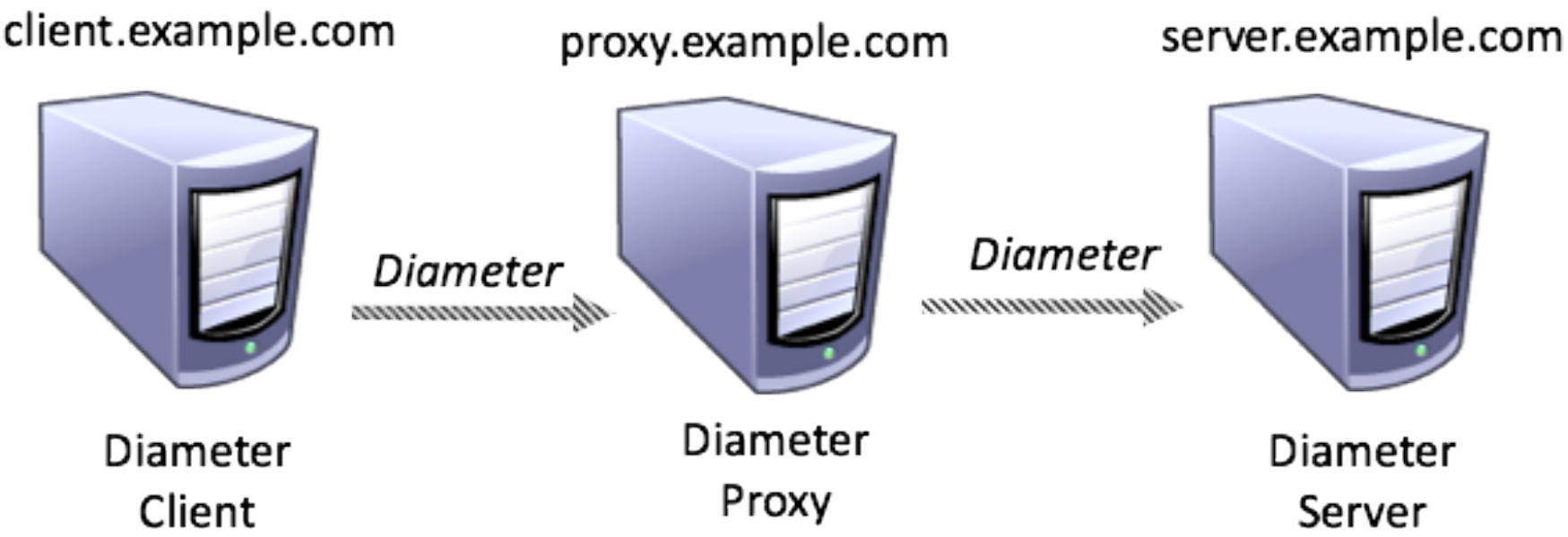
Keying Database

draft-tschofenig-dime-keying-database-00.txt

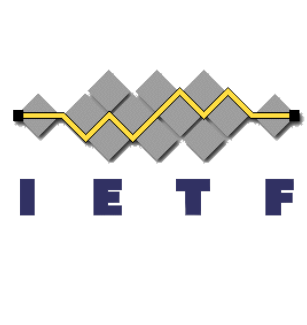


- Describes a conceptual model for a keying database
  - Sending side: what AVPs to protect, and what keys / algorithms to use.
  - Receiving side: select the appropriate security association for verifying the protected AVPs.
- Idea inspired by draft-ietf-karp-crypto-key-table and IPsec
- Diameter uses a number of databases already, e.g., realm based routing table.

Examples


client.example.com
proxy.example.com
server.example.com
Diameter
Diameter
Diameter
Client
Diameter
Proxy
Diameter
Server

Example #1: Symmetric Key



Entry from the keying database at the Diameter client.

KeyName: abc123

DestinationHost: server.example.com

ApplicationID: *

AVPCodeList: *

AlgID: HMAC-SHA1-96

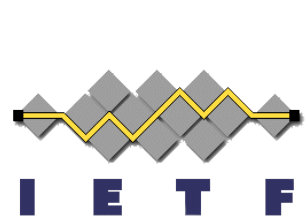
KeyType: SymmetricKey

Key: 617CAA833BEF64D88E45

Direction: out

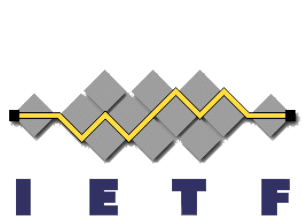
SendNotAfter: 201302142000Z

Example #1: Symmetric Key



Key Name	Dst Host	AppID	AVP Code List	KeyType	Key	Dir	Send Not After	AlgID
abc123	server.example.com	*	*	Symm. Key	617C…8E45	out	20130214200Z	HMAC SHA196

Example #2: Asymmetric Key



Key Name	Dst Host	AppID	AVP Code List	KeyType	Key	Dir	Send Not After	AlgID
abc123	server.example.com	*	*	Asymm. Key	61…45	out	20130214200Z	RS256

Feedback?