Use Cases of Implicit AKE with Sender and Receiver ID binding

Dan Forsberg

Nokia Research Center

2006-10-20

T-110.7290 Research Seminar on Network Security

Outline

- Overview of IBC AKE with an example related work
- Implicit Sender and Receiver ID binding protocol (new)
- Use cases (new)
- Next steps

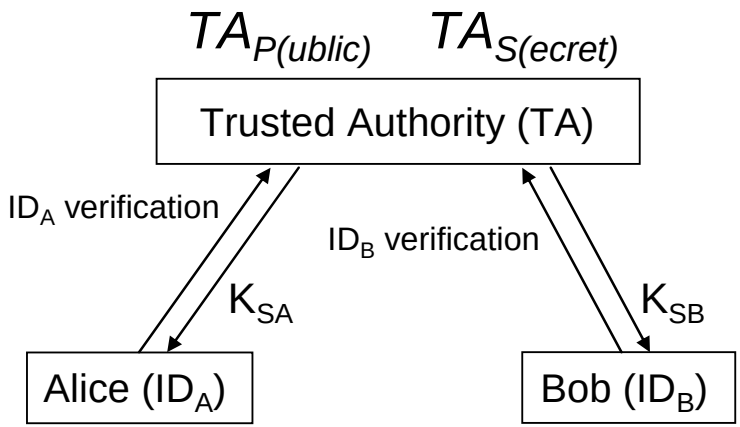
Overview of IBC AKE

Identity Based Cryptography (IBC)

- Public key authentication system
- Public key is based on user's identity information (*e.g. email address*)
- First IBC based scheme was developed by Adi Shamir in 1984 [SHAMIR]
  - Allowed users to verify digital signatures using only user's public identity information
- Later IBC based encryption and signature protocols based on pairings (and quadratic residues)

IBC – Initialization

- In an IBC system there exist a Trusted Authority (TA) in a role of a Private Key Generator (PKG)
- In initialization phase the TA creates public TA_P and secret (private) TA_S master parameters
- Users choose their identity as their public key K_P, authenticate to the TA, which provides corresponding secret (private) key K_S for them



$K_{PA} = F_1(\text{“alice@example.com”}, TA_P)$
$K_{SA} = F_2(\text{“alice@example.com”}, TA_S)$

$K_{PB} = F_1(\text{“bob@example.com”}, TA_P)$
$K_{SB} = F_2(\text{“alice@example.com”}, TA_S)$

IBC AKE

- AKE is used for data confidentiality protection (encryption) and source verification (integrity)
- Implicit authentication in IBC based on:
  1. the fact that receivers public identity is her public key
  2. assumption that TA has verified that the claimed identity belongs to the correct user before issuing secret (private) key
  3. assumption that receiver trusts the TA and holds the TA's public parameters (e.g. how to form public key from the identity)
- For Key Establishment multiple schemes exist
  - Pairing based (e.g. modified Weil and Tate pairing based)
  - Quadratic residue based (thought to be inefficient)

Pairing-based Cryptography

- Based on bilinear maps over groups of large prime order
- If G_1 and G_2 are two cyclic groups of some large prime order q, then $\hat{e}: G_1 \times G_1 \rightarrow G_2$ is called a bilinear map if for all a,b in Z and P,Q in G_1 we have:

$$\hat{e}(aP,bQ) = \hat{e}(P,Q)^{ab}$$

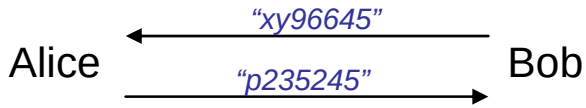
- Modified Weil and Tate pairings on supersingular elliptic curves (see more from "Identity-Based Encryption from Weil Pairing" by D. Boneh and M. Franklin)
  - Efficient to compute, non-degenerate
- Bilinear Diffie-Hellman (BDH) problem is hard:

  Given P, aP, bP, cP compute $\hat{e}(P,P)^{abc}$

“Secret handshakes from Pairing-Based Key Agreements”

D. Balfanz, G. Durfee, N. Shankar, D. Smetters, J. Staddon, and H. Wong

- Given a hash function
  $H : \{0, 1\}^* \rightarrow G_1$
- Alice with pseudonym:
  $ID_A = p235245$
  Secret key
  $K_{SA} = TA_S H(\text{“p235245-driver”})$
- Bob with pseudonym:
  $ID_B = p896645$
  Secret key
  $K_{SB} = TA_S H(\text{“xy96645-cop”})$
- Bob is a cop and stops Alice on a road
  - How does Alice verify that Bob is a cop?
- TA public parameters (TA_P) are the function H and the role based identity extension mechanism



$K_A = \hat{e}(H(\text{“xy96645-cop”}), K_{SA})$
$= \hat{e}(H(\text{“xy96645-cop”}), TA_S H(\text{“p235245-driver”}))$
$= \hat{e}(H(\text{“xy96645-cop”}), H(\text{“p235245-driver”}))^{TAs}$

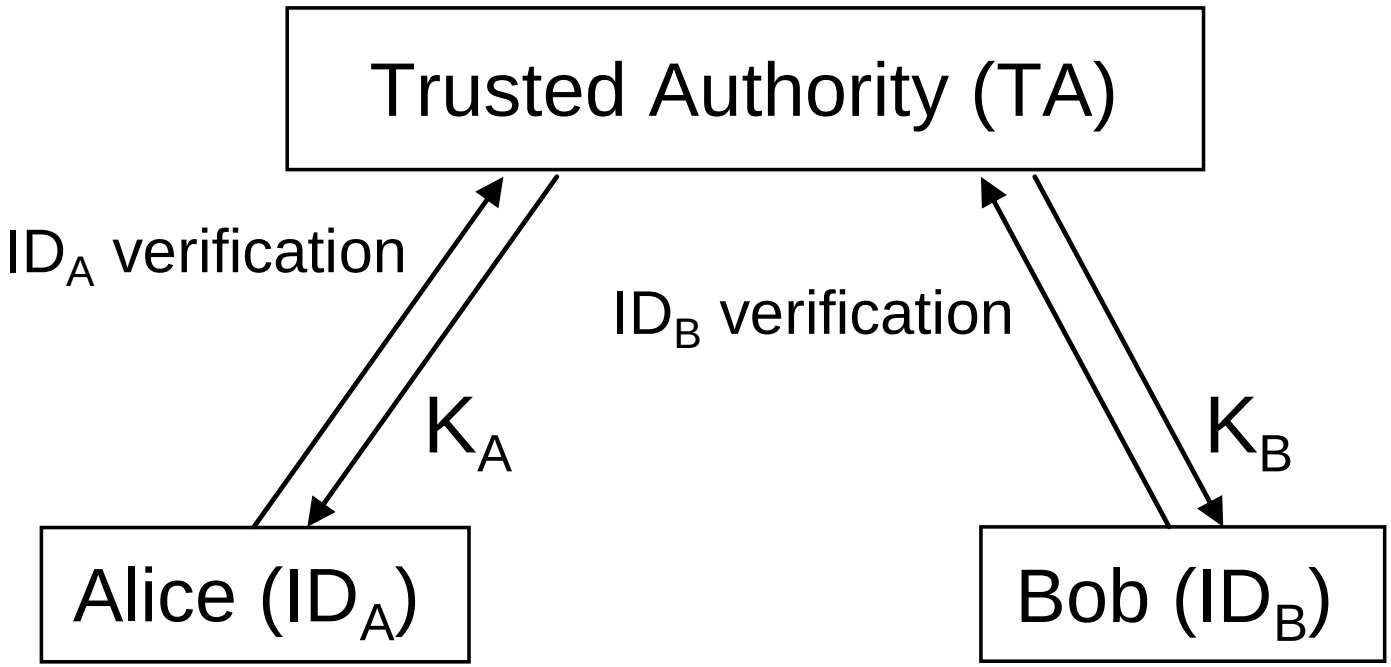
$K_B = \hat{e}(K_{SB}, H(\text{“p235245-driver”}))$
$= \hat{e}(TA_S H(\text{“xy96645-cop”}), H(\text{“p235245-driver”}))$
$= \hat{e}(H(\text{“xy96645-cop”}), H(\text{“p235245-driver”}))^{TAs}$

$K_A == K_B$

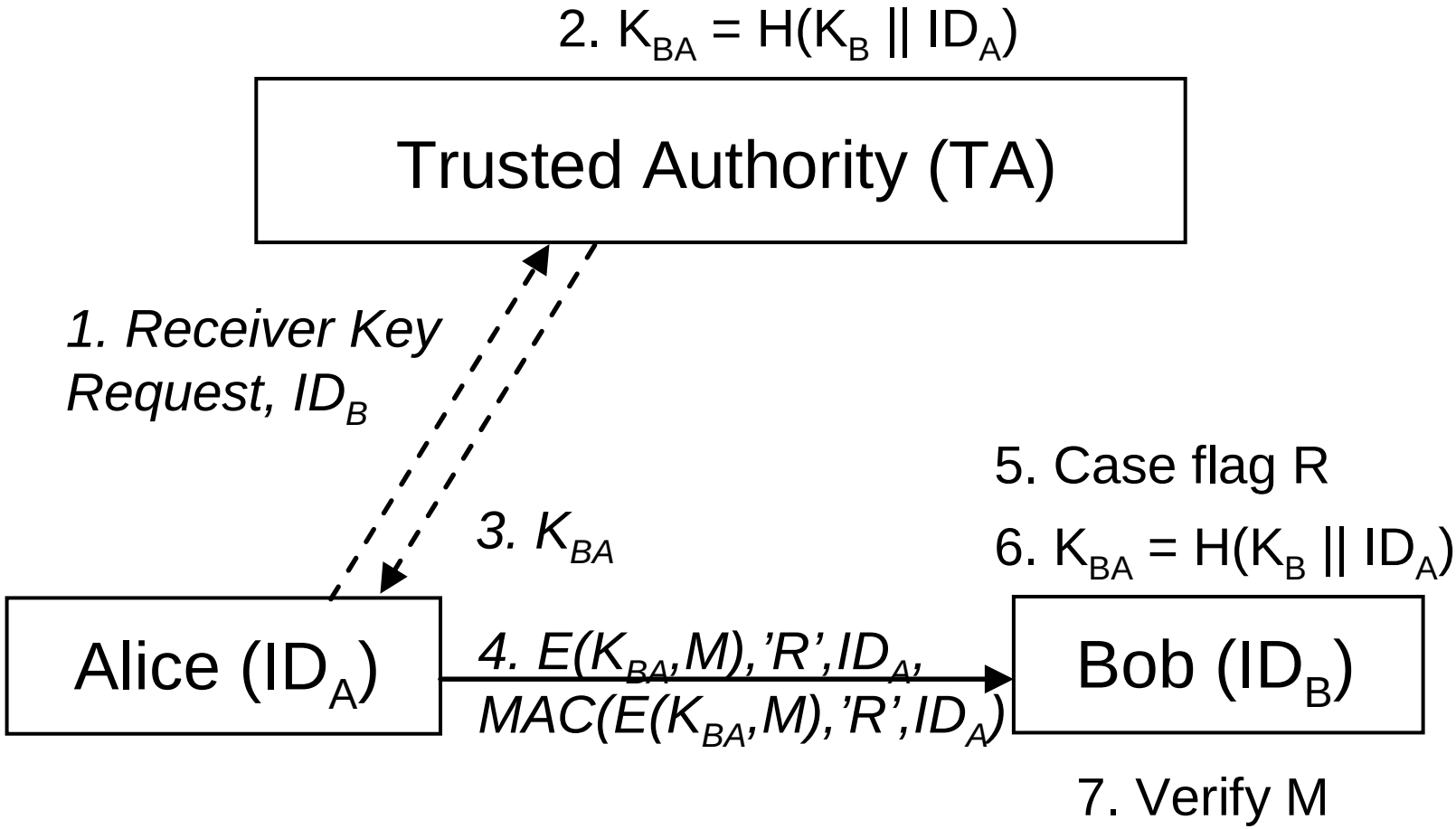
- $\hat{e}(aP,bQ) = \hat{e}(P,Q)^{ab}$
- Calculating $\hat{e}(P,Q)^{ab}$ is a difficult BDH problem

Implicit Sender and Receiver ID Binding Protocol (new)

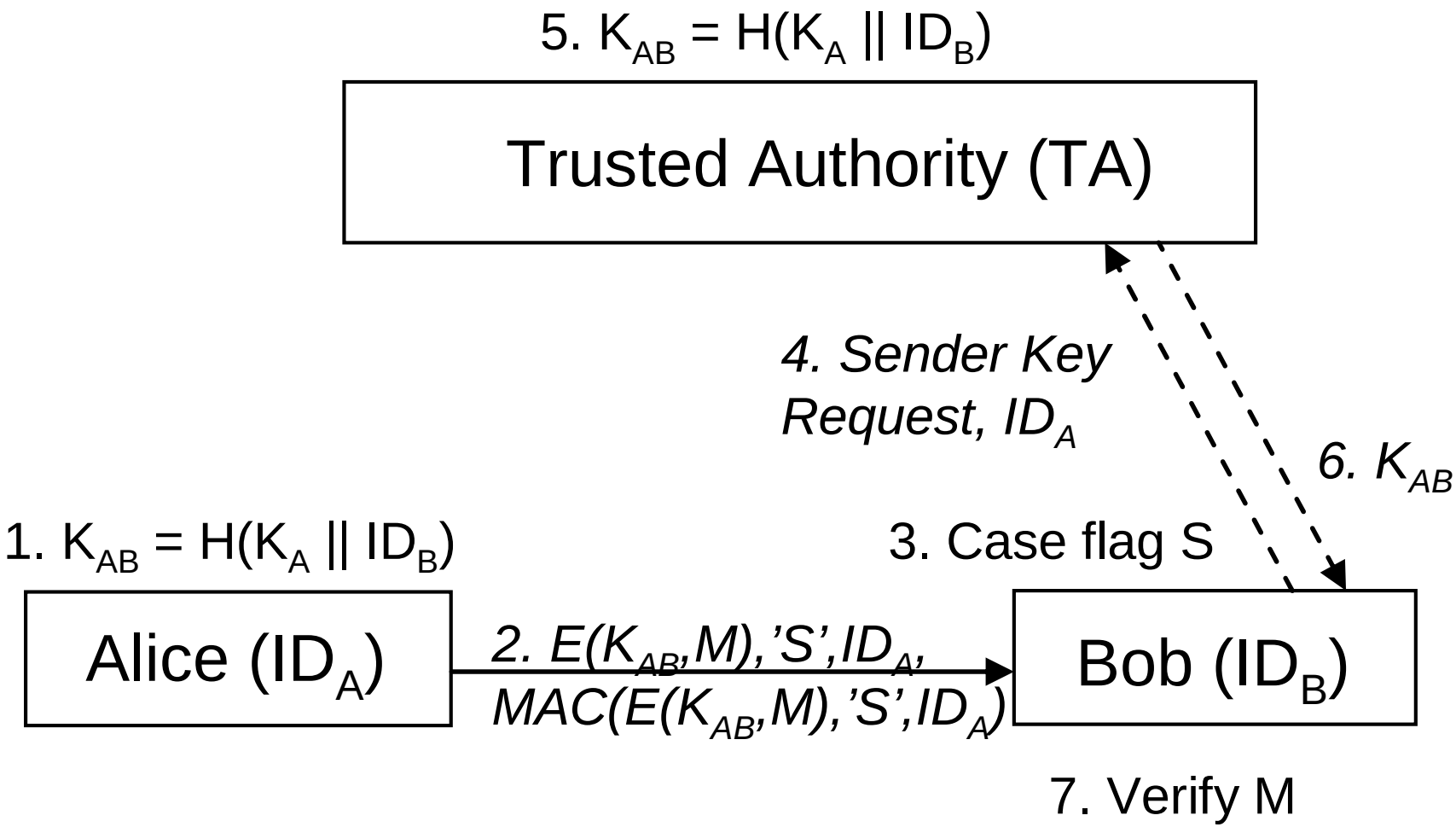
Initialization with Symmetric Keys



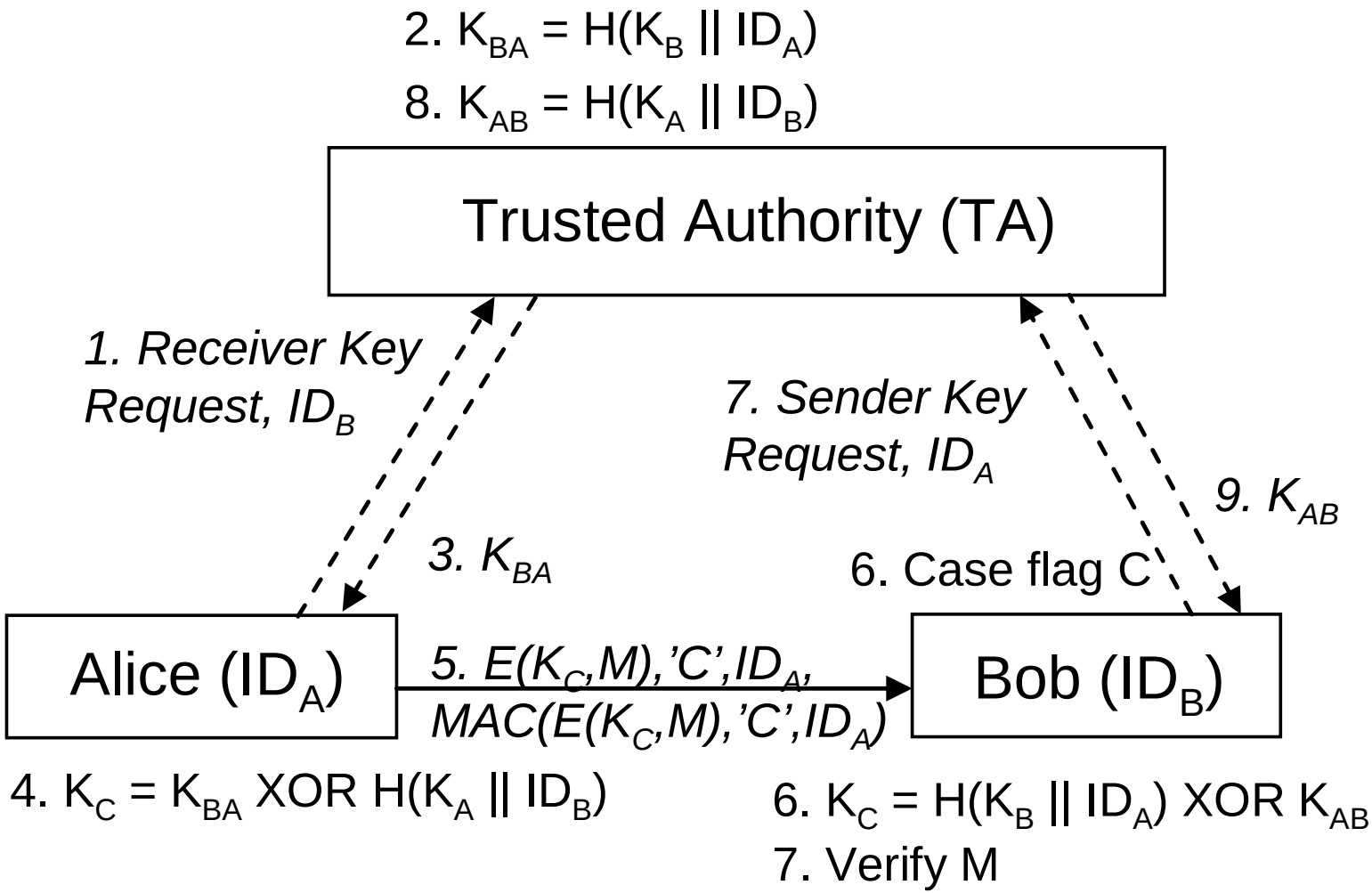
Sender ID (S-ID) Binding



Receiver ID (R-ID) Binding



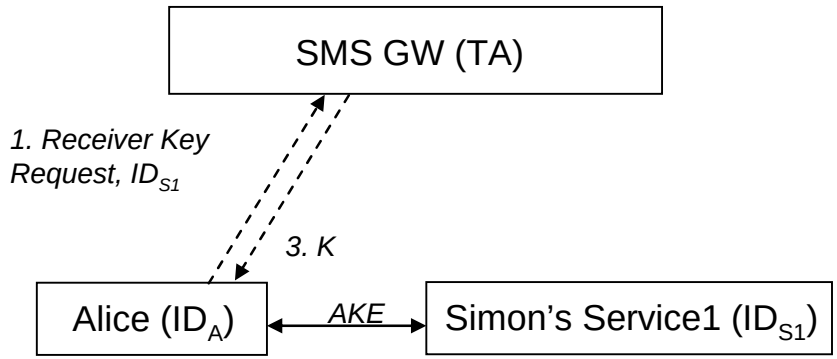
Combined R-ID and S-ID Binding



New Use Cases?

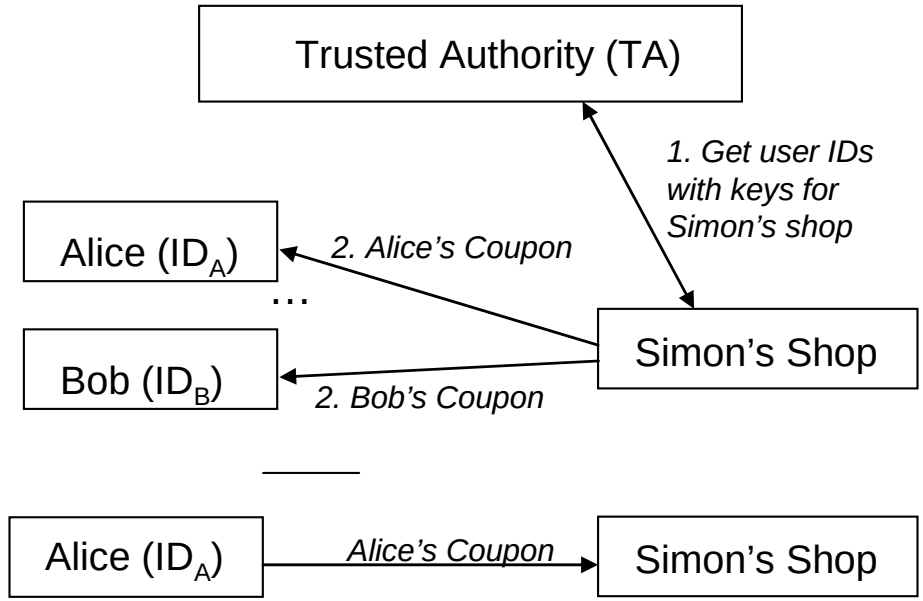
“SMS gw as Trusted Authority”
(S-ID Binding)

- Alice and Bob register to the SMS gw (TA) and both get their own shared keys
- Simon registers as well and provides a service in the Internet - “Simon’s Shop”. Simon gets his own shared key from the TA as well
- Alice and Bob send SMS messages to the TA with the “Simon’s Shop” service ID and get their PIN codes for the service access
- Alice and Bob login into Simon’s Shop with their phone numbers as their identities and using their PIN codes as passwords



“Personal Coupon Offers”
(R-ID Binding)

- Alice and Bob register to the SMS gw (TA) and both get their own shared keys. *They also register to the Personal Coupon offer (push) service.*
- Simon registers as well and provides a service in the Internet - “Simon’s Shop”. Simon gets his own shared key from the TA as well
- Simon asks phone numbers along with authentication keys from the TA so that he can send personalized offer coupons. *Simon signs the offers with his own secret key without ID binding*.
- Alice and Bob both get their encrypted coupon offers, which only they can open with their own keys.
- Showing the coupon in Simon’s shop desk they get personal discounts (cashier machine checks the signature)



“PSK-TLS with S-ID Binding”

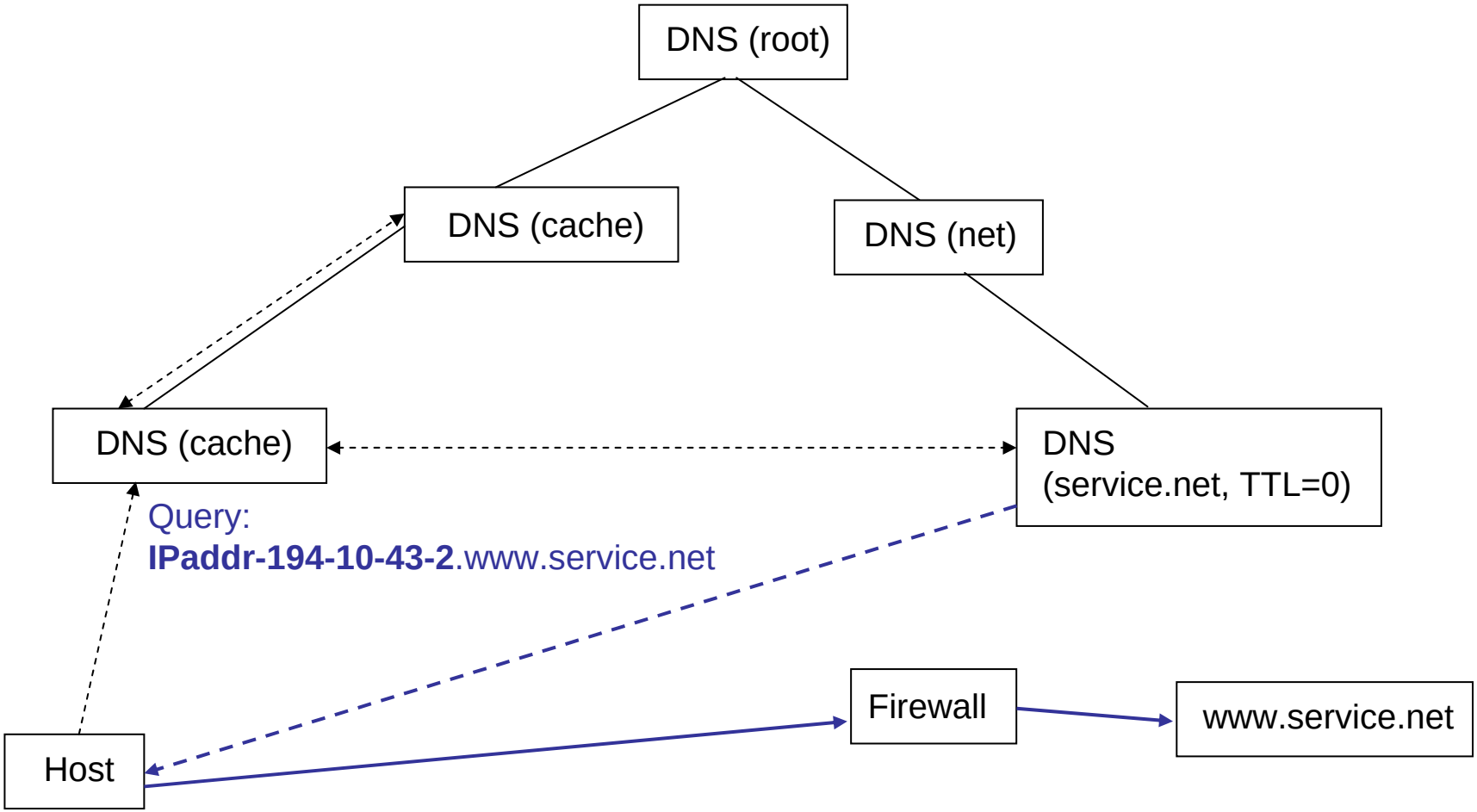
- Operations & Management (O&M) server is given a master key. The server supports PSK-TLS with S-ID Binding extension.
- Base stations are deployed into the operator’s network with S-ID pre-bound keys
- Each base station contact the O&M server and provide their identification information
- Server derives key based on the base station ID and it’s own master key

“DNS based PLA with Symmetric Keys and S-ID Binding”

- Domain master DNS as the TA. Domain firewall shares a secret with it – DNS is trusted
- Client uses R-ID based AKE
- Client add it’s own IP address (sender ID) into the DNS query
  - IPaddr-194-10-43-2.www.service.net
  - Host’s serving name server must check that the IP address is correct OR
  - the target domains master DNS must do reverse lookup query for the received IP address and compare it with the host’s DNS domain (must be same)
- Service.net domain master DNS server gets the request, takes the IP address and derives key for the client
- Client gets the key in the DNS response message and uses it to create per packet authentication headers

“DNS based PLA with Symmetric Keys and R-ID Binding”

- Firewall gets packets and authenticates based on the R-ID scheme
  - Key hierarchies allow multiple firewalls and destination hosts
  - NAT is a problem, unless NAT address is used and port also included into the DNS query
- Nothing prevents attacker from sending false queries with false IP addresses – unless the domain master DNS server sends the key directly to the IP address (or part of the key in direct response and other part in the DNS response)
- Cache is not possible, thus must TTL=0. Not a problem.


DNS (root)
DNS (cache)
DNS (net)
DNS (cache)
DNS
(service.net, TTL=0)
Query:
IPaddr-194-10-43-2.www.service.net
Firewall
www.service.net
Host

Next Steps?

FFS..

- Refine the DNS model
  - How to deliver the key securely
- Fine tune the other use cases as well
- Compare with Kerberos
- Compare to PK and IBC AKE
  - Key renewal etc.
- Security analysis
- Is there any benefit of using SID+RID variant...
- Refine the usage of one-time keys (e.g. counter used in the key derivation)
- Distributed TA

Distributed TA?