Updates to Adaptive DNS Discovery

draft-pauly-dprive-adaptive-dns-privacy

Tommy Pauly, Eric Kinnear, Patrick McManus, Chris Wood
ADD
IETF 107, March 2020, Virtually Vancouver

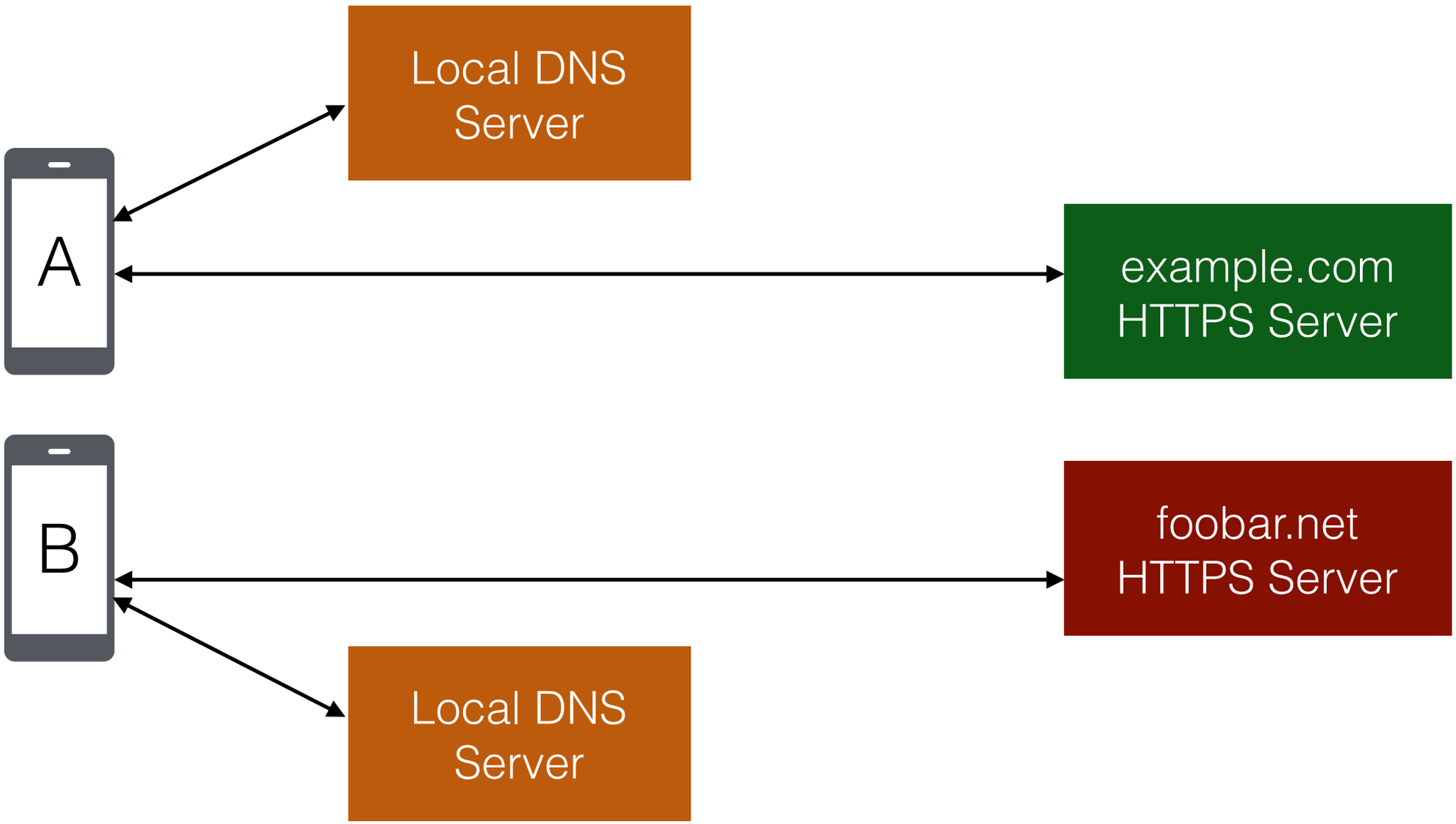
Goals

Resolver discovery (local or remote)

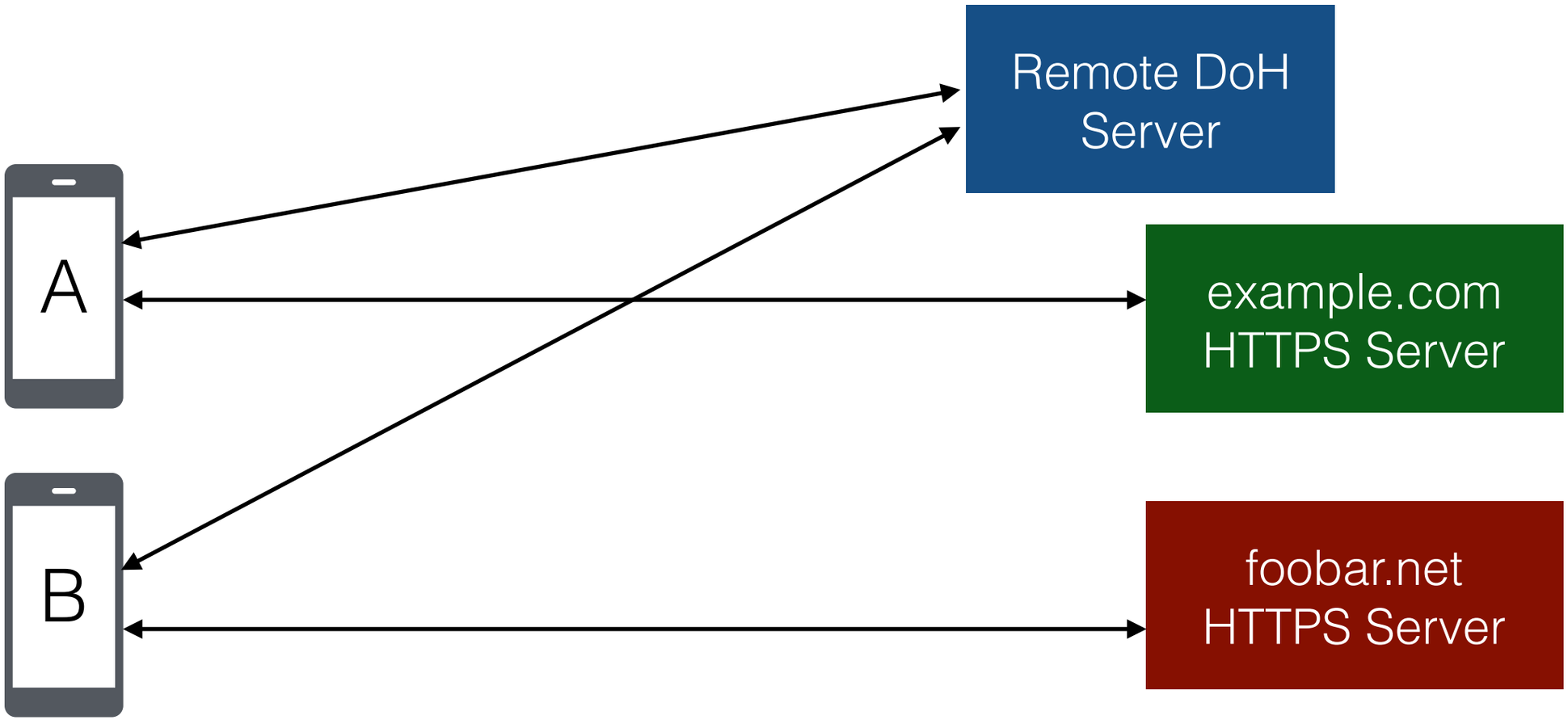
Resolver information

- When should a client use this resolver?
- Are there any special capabilities of this resolver?

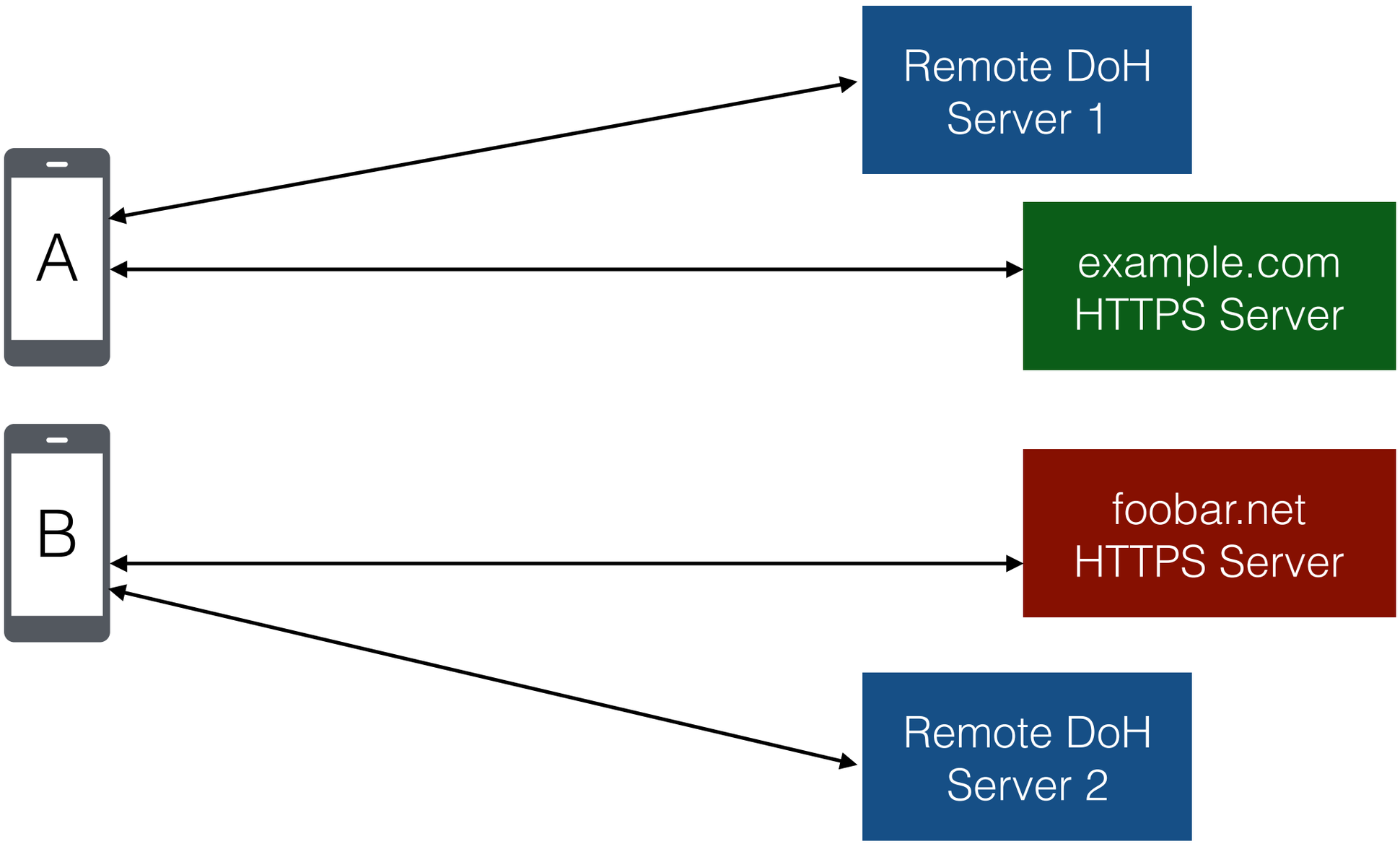
Status Quo Model



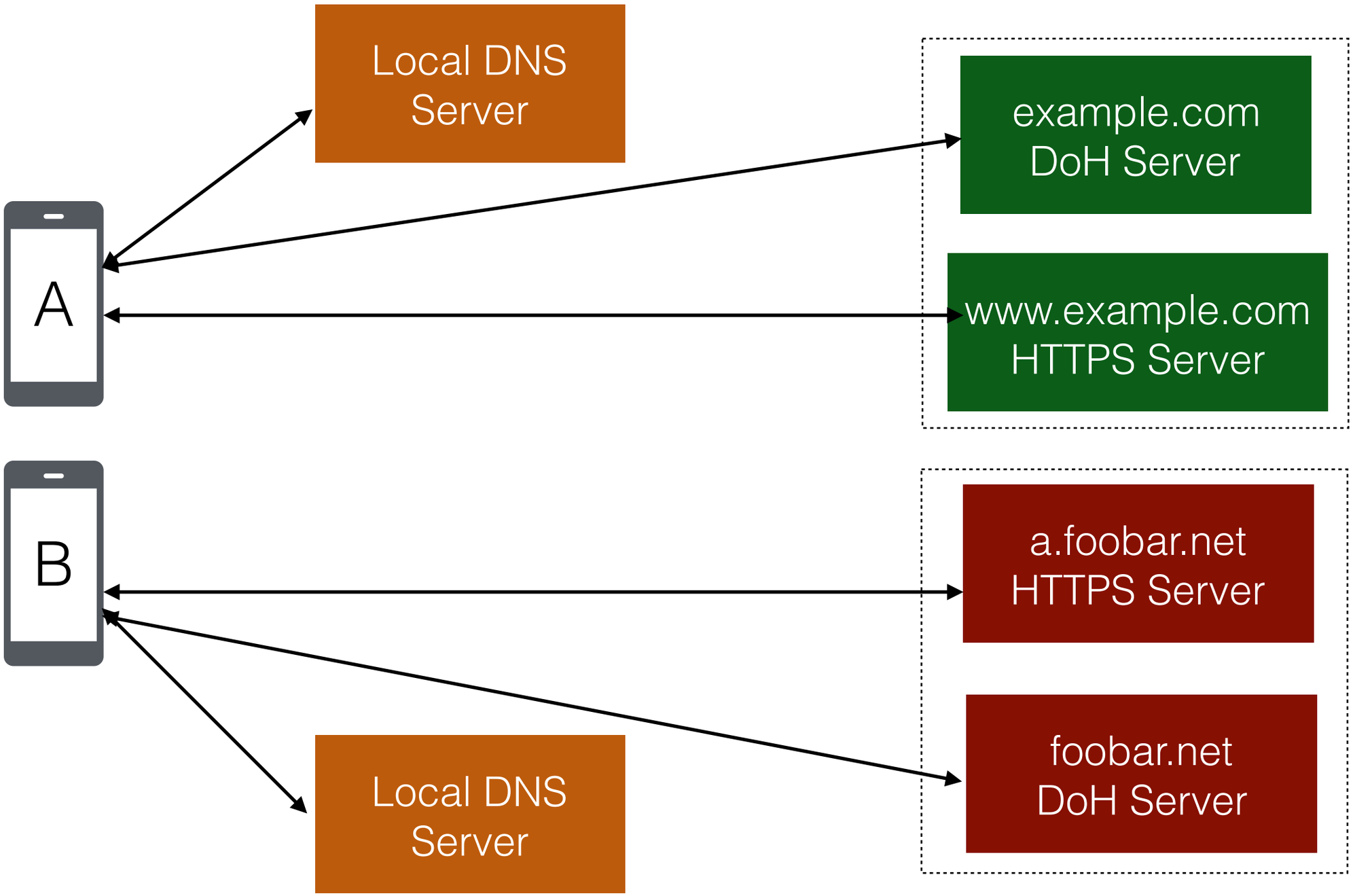
Trusted Remote Resolver Model



Multiple Trusted Remote Resolver Model



Designated Remote Resolver Model



Why designate resolvers for domains?

Having the same “entity” terminate TLS/HTTPS connections also terminate DoH has several benefits:

Reduction of the number of entities that see traffic from a given client IP address associated with a hostname

While the entity *can* see many clients accessing a given name, it sees those same clients in TLS connections

It becomes easier to deploy shared servers that allow DoH connections to be reused for later HTTP traffic

Discovery of Resolvers

Remote resolvers advertised in DNS Records

- Extend HTTPSSVC to include DoH URI Template
- Same mechanism as Encrypted TLS Client Hello (ECHO)
- Involves DNS bootstrapping (local resolver / TRR / oblivious)

Local resolvers advertised in PvD info from RA

Resolver Information

Access a well-known URI to fetch remote configuration as a Provisioning Domain JSON blob

For `https://example-dns.org/dns-query`, info is at `https://example-dns.org/.well-known/pvd/dns-query`

JSON information can include the DoH URI template, which is useful for finding DoH for local PvDs

Supports identifying domains used for split DNS, or other extensible behavior properties

Validating Designation

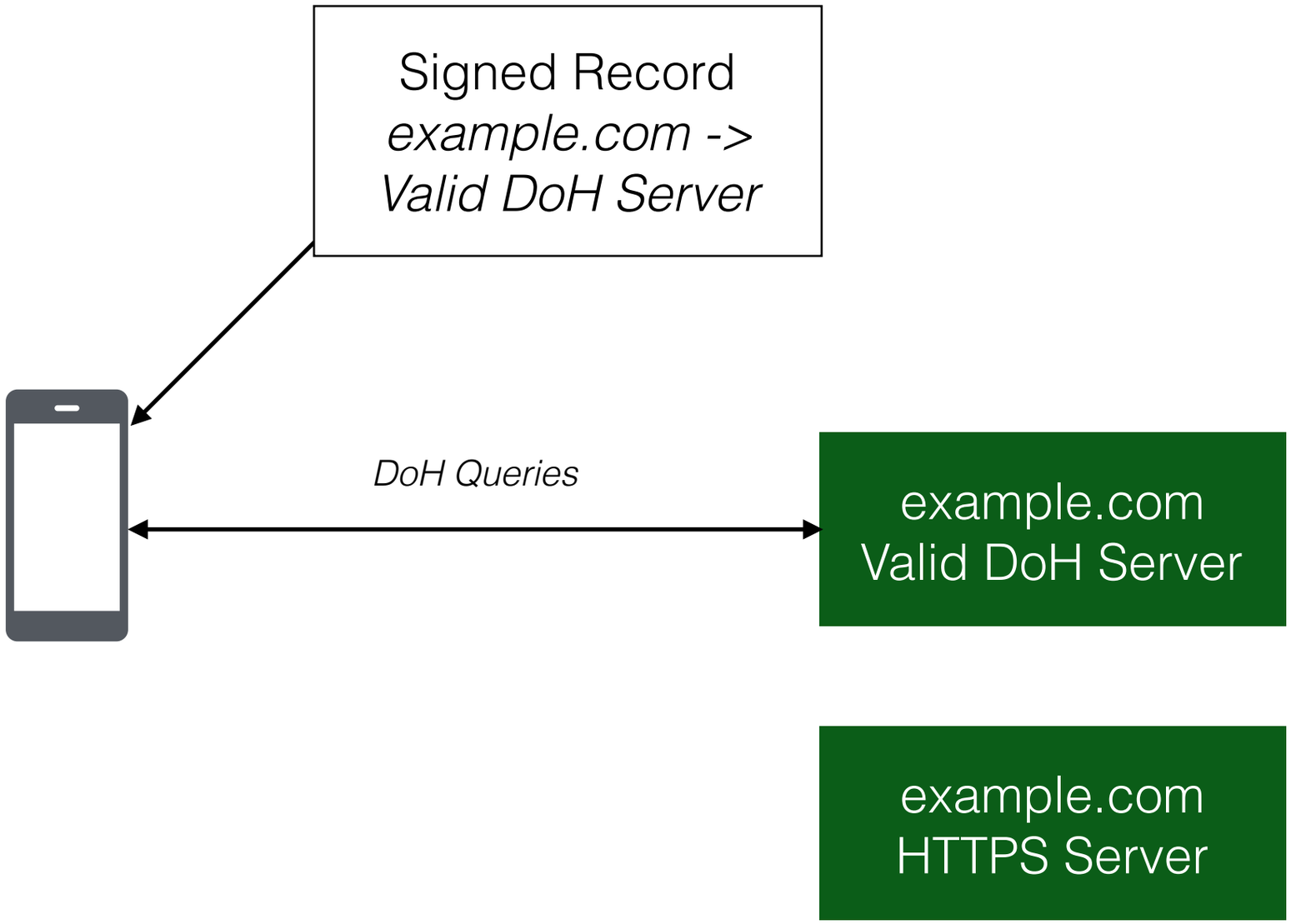
DNSSEC-signed DNS records that designate a DoH server for a given name establish a trusted relationship

Resolver information can also identify other mechanisms for validation

Information can hint that `example.com` designates this DoH server, which can be validated using a request such as `https://example.com/.well-known/pvd`

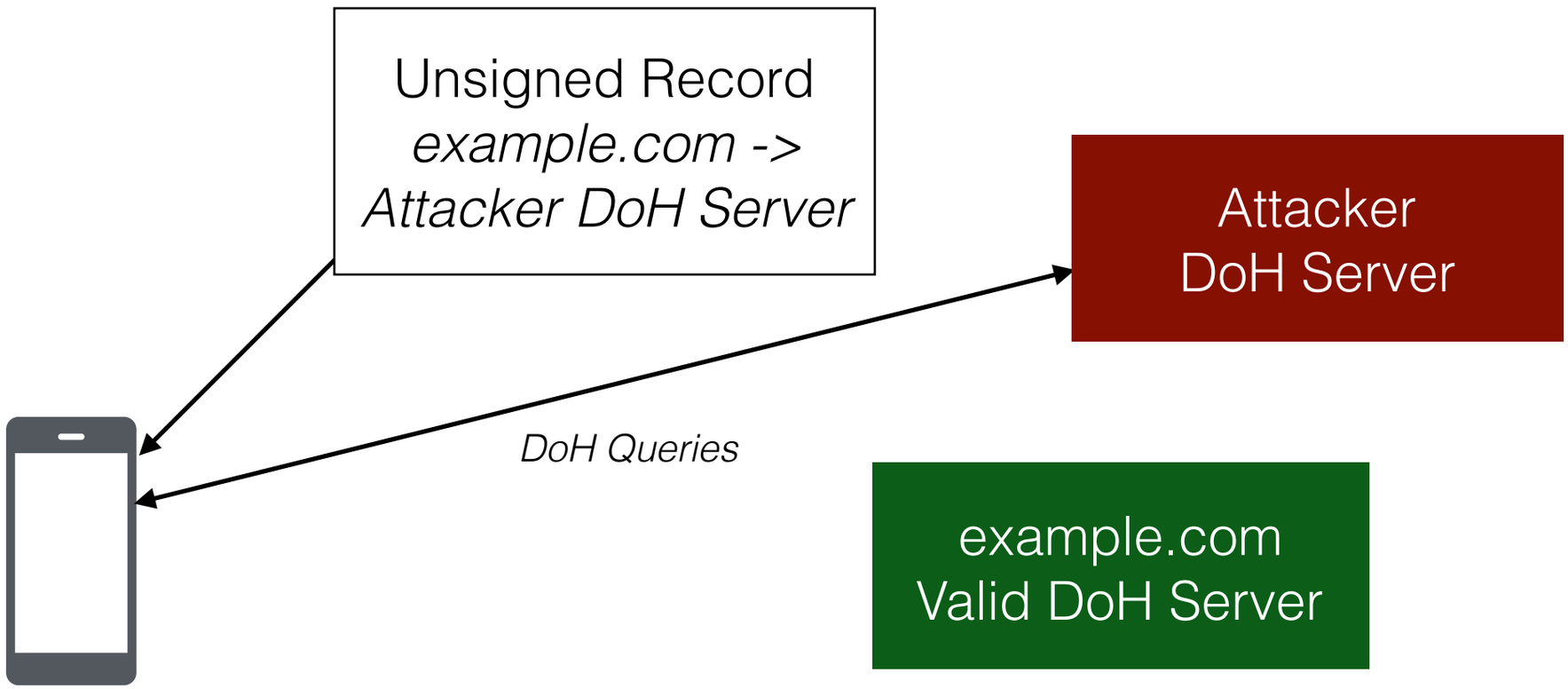
Scenarios

DNSSEC Signed Designation



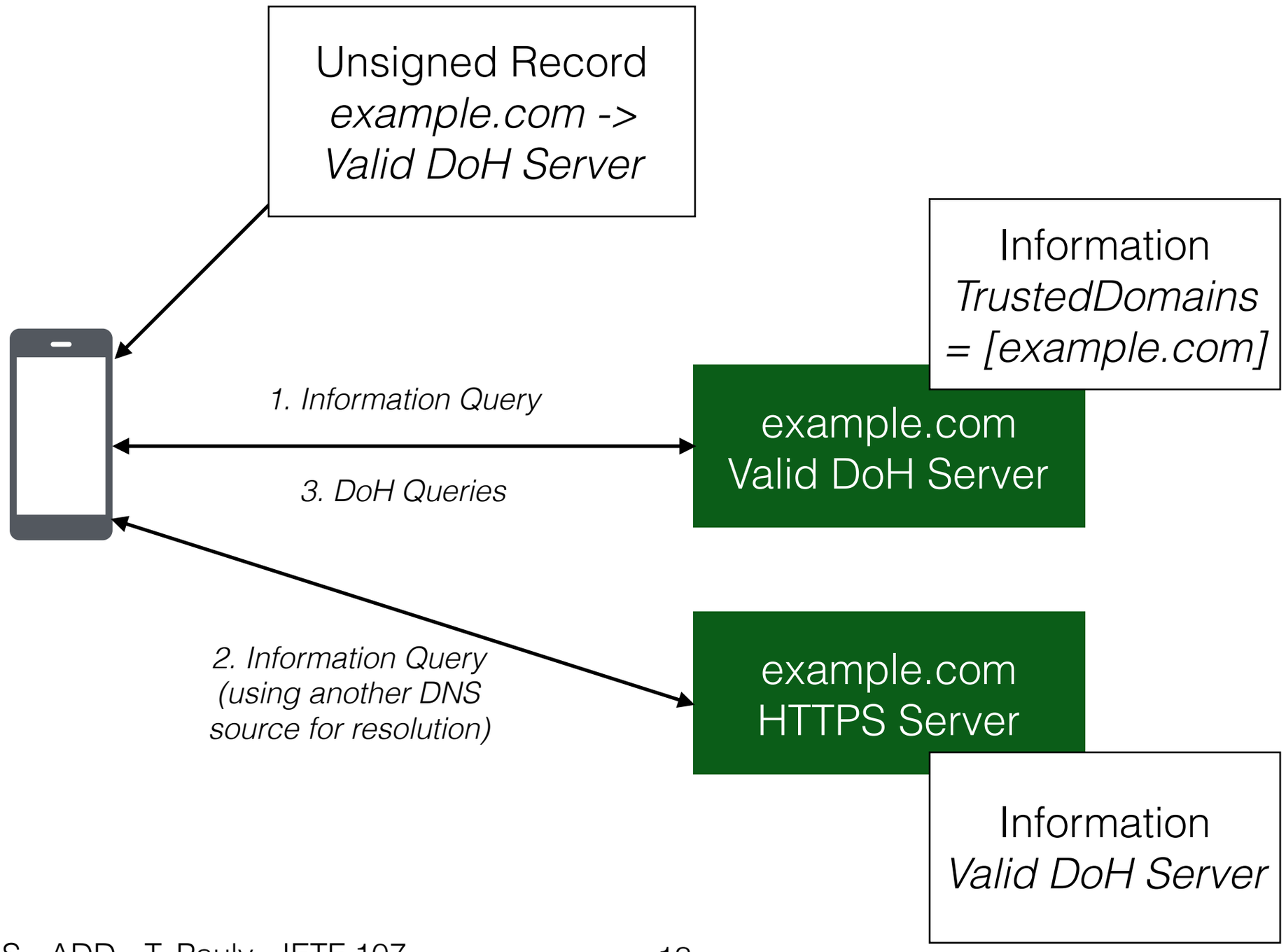
Scenarios

Unsigned Designation Attack



Scenarios

Unsigned Designation Mitigation



Scenarios

Unsigned Designation Attack Attempt