STIR Out-of-band Mechanism

draft-rescorla-stir-fallback

Eric Rescorla

ekr@rtfm.com

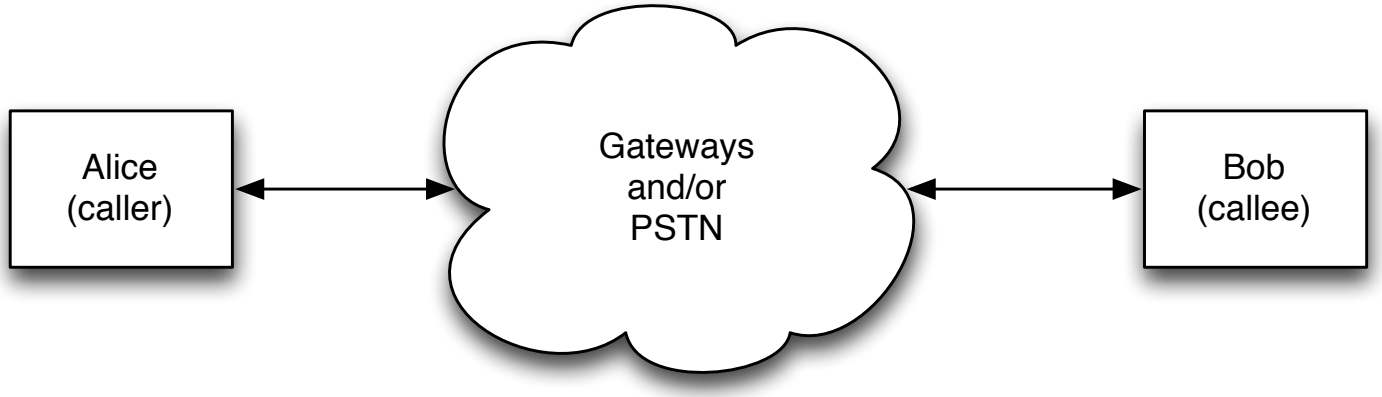
IETF 87

July 30, 2013

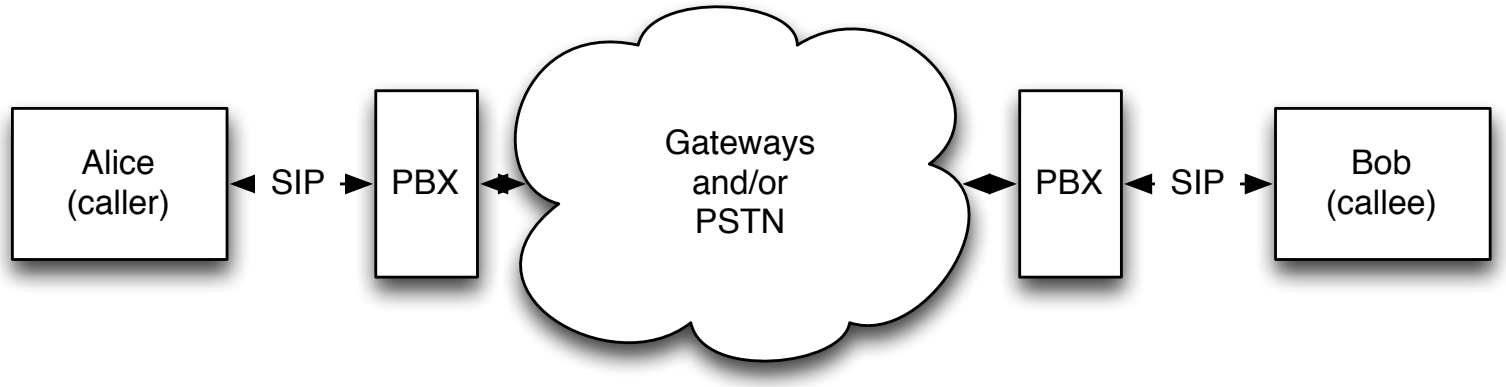
Assumptions

- We care about IP-PSTN and PSTN-PSTN
  - This means in-band is insufficient
- User is serviced by a programmable device
  - User has a smartphone, softphone, etc.
  - User has a dumb phone but is serviced by a programmable gateway
- Very restricted channel between endpoints
  - Entities other than carriers can't change telephone signaling
- We don't expect service providers to change immediately
  - Need a system which works with *no* SP changes

Basic Setting



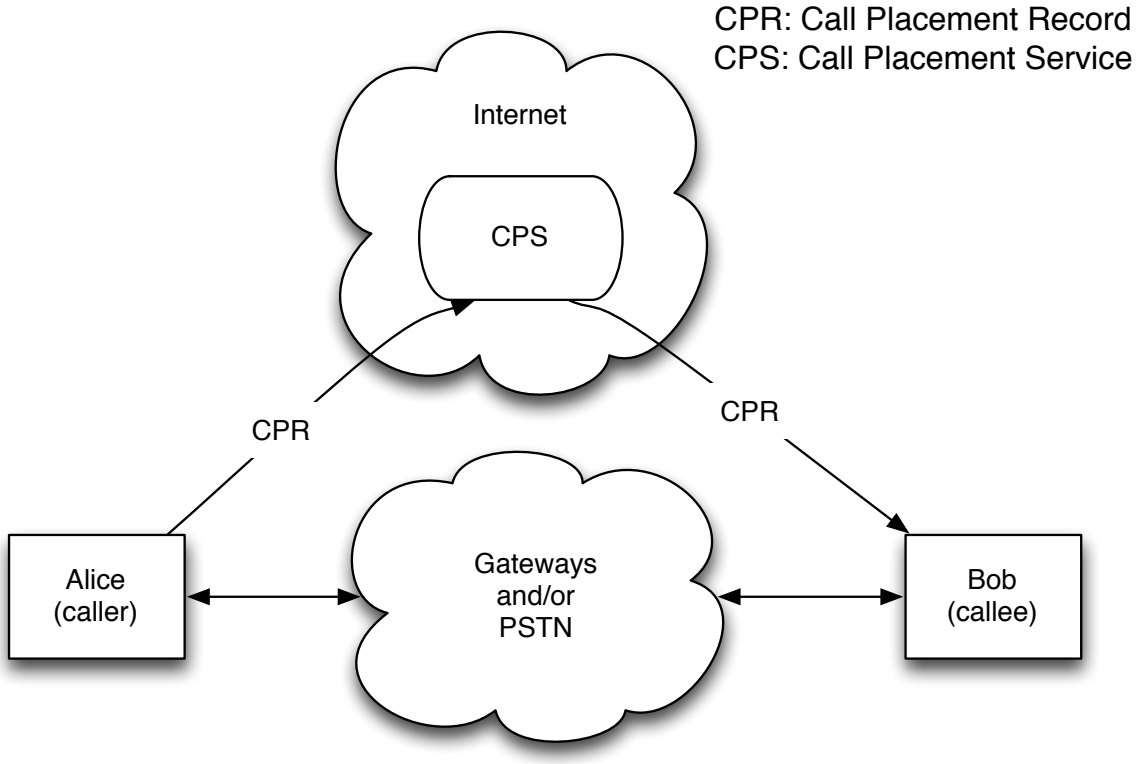
Alternate Setting



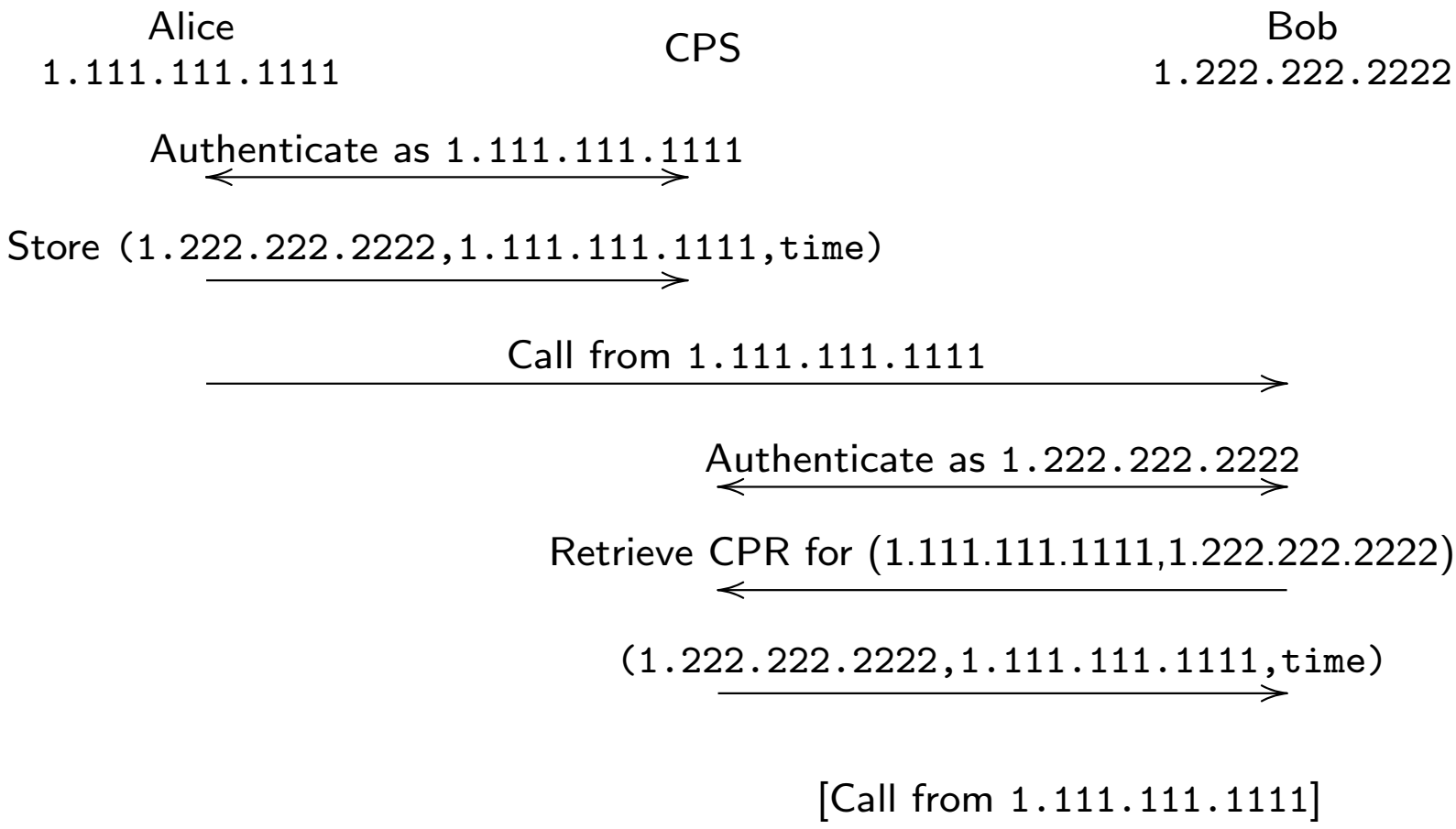
Credentials

- This assumes that each phone number is associated with credentials
  - May be assigned to endpoint, PBX, gateway, ...
  - Or all of the above jointly
- Exact provisioning mechanism is unspecified
  - May be either authoritative or third-party

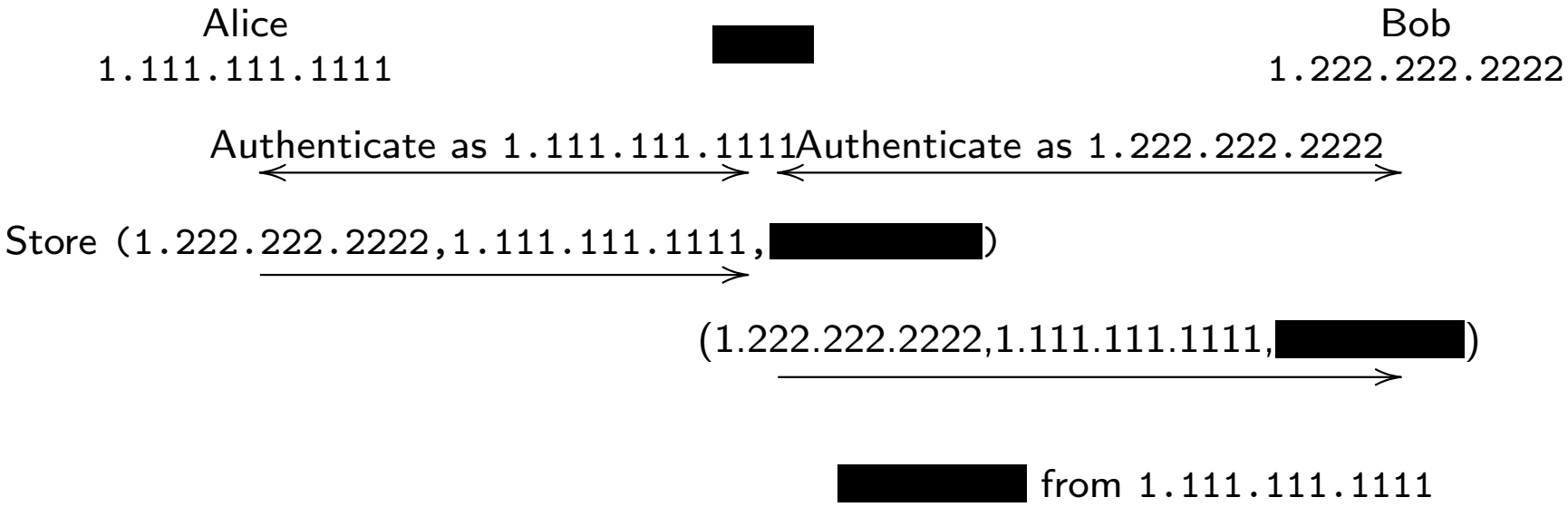
System Architecture



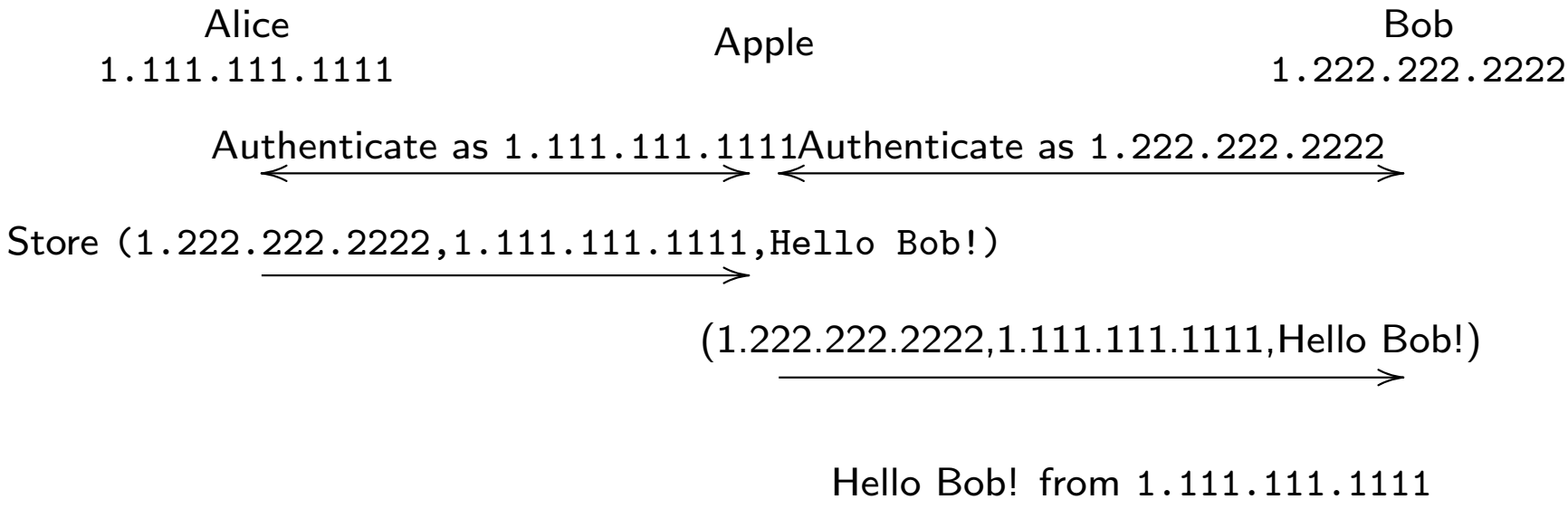
Call Flow

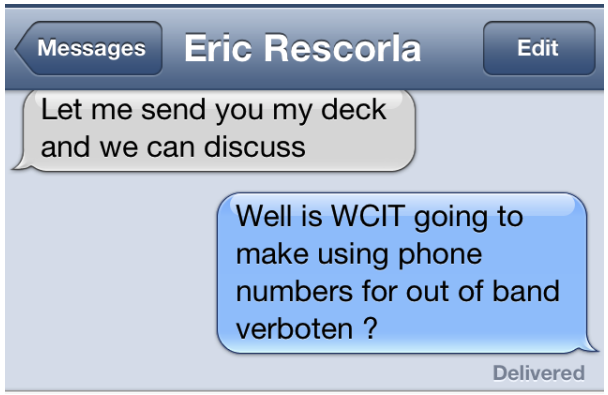

Alice
1.111.111.1111
CPS
Bob
1.222.222.2222
Authenticate as 1.111.111.1111
Store (1.222.222.2222,1.111.111.1111,time)
Call from 1.111.111.1111
Authenticate as 1.222.222.2222
Retrieve CPR for (1.111.111.1111,1.222.222.2222)
(1.222.222.2222,1.111.111.1111,time)
[Call from 1.111.111.1111]

Don't I know you from somewhere?



Oh, yeah, that's right





Relationship to In-band

- Can use the same credentials
  - Out-of-band requirements are a subset of in-band (maybe a proper subset)
- CPR can be based on the inline signature block
  - May need to carry some of the headers
- Mechanisms can be used independently
- Receiver should accept calls with either In-band or Out-of-band validation

Questions?

Backup Slides

Fine Print I: Privacy

- CPS learns about every call
  - Not totally optimal
- Third parties don't learn about calls
- There is a bunch of crypto we can deploy here
  - But not really relevant for this discussion
  - See the draft

Fine Print II: Performance

- Concerns raised about timeliness of message delivery
  - Primarily about connection setup
  - These seem premature at this stage, but....
- Caller can set up a connection ahead of time
  - When user invokes dialer app
- Callee probably has to set up connection in real-time
  - But this is reasonably fast (3-5 RTT even with HTTPS)