Certificate Selection API

TPAC ‘14

Options for Certificate Choice

- One certificate per origin
- One certificate per RTCPeerConnection
- (MUST have different certificates between origins to avoid SUPERCOOKIE!)

Want

- Same certificate over time
  - Stability of choice of identity allows for establishment of parallel trust
- Different certificates over time
  - Certificates per-peer or per-scenario
  - Let sites break correlation between sessions

Proposal

- Use new API to generate WebCrypto keys
- PC API generates a certificate based on those keys
- WebCrypto ensures:
  - Private keys can’t be accessed
  - Keys can be stored and retrieved

How it Works

- let theKey = RTCKeys.generate(algorithm);
- let pc = new RTCPeerConnection(
  { dtlsKeys: [theKey] });

Choosing keys

- If no keys are provided, keys are generated
- RTCPeerConnection picks a suitable key from what is presented
- It might choose several (e.g., ECDSA and RSA)
    - This maximizes interoperability