W3C WebCrypto Request to JOSE for JWK Private and Symmetric Key Representations

Mike Jones
November 7, 2012
W3C WebCrypto Use Case

• W3C WebCrypto WG developing JavaScript APIs for crypto operations
  – Intended to enable efficient JavaScript JOSE implementations, among other scenarios
• Some WebCrypto APIs use key representations
  – Including JWKs
• Currently an asymmetry for JWK
  – Other formats can represent public, private, and symmetric keys
  – JWK only defines public key representation
WebCrypto Request to JOSE

• WebCrypto WG requests that JOSE define and standardize representations for all three types of keys:
  – Public
  – Private
  – Symmetric

• They will likely use the IANA registry to define the remaining two if we don’t
Decision Needed by JOSE WG

• Do we want to define the additional representations?
• Potential starting point already exists:
  – draft-jones-jose-json-private-key