Updates in this revision

§3. Indication of pre-negotiated parameters

§4.5. WebCrypto use case

§5. Summary of requirements
§3. Indication of pre-negotiated parameters

• Sometimes two parties are exchanging many objects, so they pre-negotiate parameters
  – In principle, just omit the pre-negotiated fields
  – Variety of ways this can go wrong

• Requirement to either:
  – Provide all parameters, or
  – Indicate that parameters
§4.5. WebCrypto use case

• Protect API constraints on keys as they’re communicated to/from a browser
  – Exportable = false: Keys check in, but they don’t come out

• Wrap keys with attributes so that they can’t be tampered with en route
§5. Summary of requirements

• Summary of requirements from elsewhere
  – Functional: Formats, encodings
  – Security: Key management, validation, negotiation
  – Desiderata: WebCrypto compatibility, no canonicalization
Next Steps

• Submit as draft-ietf-jose-use-cases
• Reviews
• WGLC?