# Public Key-derived secrets for MAC-based signatures

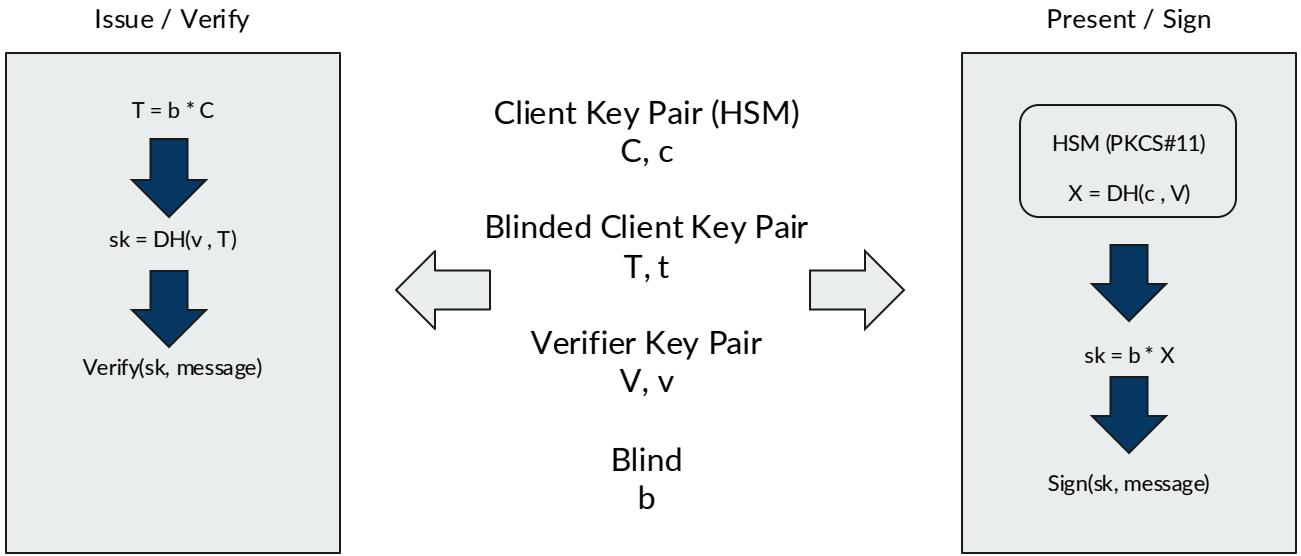
draft-bastian-jose-pkdh-01

Stefan Santesson, Micha Kraus
Paul Bastian, Peter Lee Altmann (not present)

IETF 124

# Motivation

## SD-JWT – Supporting fully specified HMAC signatures (as mDoc do)



# Key proof with blinded key

- Relevant for EU wallets (eIDAS) providing verifiable presentations bound to blinded PoP keys
- Relevant for use with SD-JWT as verifiable presentation format
- Can be done with ECDSA, but requires modified HSM (add then sign)
- HMAC signatures allows use of standard PKCS#11 HSM (Diffie-Hellman)
- HMAC signatures natively supported by mDoc / mDL (ISO 18013)
    - Fully specifies HMAC key derivation from public signer key
- HMAC signatures supported by SD-JWT
    - Key derivation from public signer key is NOT defined

# The pkdh JOSE header parameters


```
{
  "typ":"JWT",
  "alg":"ECDH-P256+HKDF-SHA256+HS256",
  "pkdh":{
    "pkp":{
      "jwk":{
        "kty":"EC",
        "crv":"P-256",
        "x":"f83OJ3D2xF1Bg8vub9tLe1gHMzV76e8Tus9uPHvRVEU",
        "y":"x_FEzRu9m36HLN_tue659LNpXW6pCyStikYjKIWI5a0"
      }
    },
    "pkr":{
      "jwk":{
        "kty":"EC",
        "crv":"P-256",
        "x":"vWV4vmRT8HV9QAkbZJAWrvjOV0NfNOzkzq92apq8yjk",
        "y":"XGJRplhubKDv6cFA7e9-yn7F89UUwt57JVLAOS1tpXE"
      }
    },
    "info":"PKDH-v1",
    "salt": "V2hhdCBhIHNhbHQ="
  }
}
```

# Since last IETF

- Presentation of Designated Verifier Signatures at IETF 121 and IETF 123
- Changed name to Public Key Derived HMAC for JOSE (PKDH)
- Changed generic algorithm names to Fully Specified Algorithms
- Removed suite parameter from the “pkdh” header parameter
- Removed options
  - No selectable key lengths (Use HMAC default)
  - No suite based generic structure for key derivation parameters
- Specified base algorithm for P-256, SHA-256 HKDF, SHA-256 HMAC
  - ECDH-P256+HKDF-SHA256+HS256

# Outstanding issues

- More algorithm profiles?
- Salt
  - Achieving unique signing keys per signature
  - Default salt value derivation
    - Bound to signed document?
    - Allow custom salt?
- Algorithm identifier syntax – Derive basic config from name?
  - Eg. ECDH-P256+HKDF-SHA256+HS256
- IANA considerations
- Examples

# Next steps

- Call for adoption
- Complete work within JOSE

# Links

Datatracker -> https://datatracker.ietf.org/doc/draft-bastian-jose-pkdh
Git Repository -> https://github.com/paulbastian/draft-bastian-jose-pkdh
Current Editors Copy -> https://paulbastian.github.io/draft-bastian-jose-pkdh/draft-bastian-jose-pkdh.html