The following items remain to be done in this draft:

TBD

No IANA actions are required by this specification.
9.1 Normative References


[RFC4627] Crockford, D., "The application/json Media Type for JavaScript Object Notation (JSON)," RFC 4627, July 2006


9.2 Informative References


Appendix A. Acknowledgements

A JSON representation for RSA public keys was previously introduced in [MagicSignatures].

Appendix B. Document History

-02 Editorial changes to have this spec better match the JWT, JWS, and JWE specs.
No normative changes.

-01 Changed algorithm member value for Elliptic Curve keys from ECDSA to EC, since Elliptic Curve keys can be used with more algorithms than just the Elliptic Curve Digital Signature Algorithm (ECDSA). Added OPTIONAL use member to identify intended key usage, especially since the same Elliptic Curve key should not be used for both signing and encryption operations.

-00 Created first version based upon decisions made at the Internet Identity Workshop (IIW), as documented at http://self-issued.info/?p=390.

Author's Address

Michael B. Jones
Microsoft
Email: mbj@microsoft.com
URI: http://self-issued.info/MagicSignatures