1. Grant name: JWS Grant

2. Challenge Definition*:*

2.1. Donor(s): ____Microsoft_____

2.2. Challenge Owner(s): __Claims and Credentials WG_______________

2.2.1. If a working group, current chairs: _________________

2.3. Work can be contributed to by:
___ [pre-approved] grantee(s) only (**mini-grant** mode)
_X_ [pre-approved] grantee(s) with help from DIF membership (**work item** mode)
___ any eligible member* (**open bounty** mode)

2.4. Payment options (select only one):

2.4.1. ___ Winner takes it all

2.4.2. ___ At discretion of submission judges

2.4.3. _X_ Itemized in Success Criteria and/or Additional Details section

2.5. Scope:

Lead or co-lead an iteration of this conformance test definitions and test suite implementing the test definitions that gets it to a major version release by the end of 2021. Implementations of the JSON Web Signature 2020 specification (https://w3c-ccg.github.io/lds-jws2020/) are to be tested. Both positive and negative tests and tests for both producers and consumers are to be included. Testing pertinent criteria from the Verifiable Credentials and DID specifications may be performed if those drafting the test criteria believe that including these tests will improve interoperability. Where the underlying specifications are deemed to contain ambiguities, it is within scope of the work for the test definitions and test suite to resolve those ambiguities in ways that promote interoperability. The tests may designate support for some algorithms as being required - particularly some of those registered in the IANA JSON Web Signature and Encryption Algorithms Registry at https://www.iana.org/assignments/jose/jose.xhtml#web-signature-encryption-algorithms - and may designate support for other algorithms as being optional - particularly those that have not gone through IETF review.
Note that the DIF working group owning this challenge is responsible for vetting and approving the test definitions, whereas the selected contractor for the challenge is responsible for writing tests implementing the test definitions.

(Define a problem space, set of problems, or stakeholders whose needs are unlikely to be met otherwise, without defining one specific technical or business problem)

2.6. Rationale for Community Benefit

Interoperability tests for ***JsonWebKey2020*** and ***JsonWebSignature2020*** will advance interoperation of implementations using these cryptographic formats, including those used with Verifiable Credentials and DIDs.

(Define how this challenge benefits the whole DIF community, even if short-term benefits are unevenly distributed)

2.7. Success Criteria:

The tests cover the feature areas of https://w3c-ccg.github.io/lds-jws2020/, for both producers and consumers of relevant JWKs and JWSs. Both positive tests (such as verification of correct signatures) and negative tests (such as rejection of bad signatures) are included. At least three independent implementations of both producers and consumers are used to “test the tests”. Ideally, the tests will cover all the signature algorithms registered in the IANA JSON Web Signature and Encryption Algorithms registry at https://www.iana.org/assignments/jose/jose.xhtml#web-signature-encryption-algorithms, but a core set of at least three of the most commonly used algorithms would be minimally acceptable.
(*aka Definition of “done”, test vectors, description of needed test fixtures, etc.)*

2.8. Dependency Limitations:

No pre-existing limitations beyond conformance to the relevant specifications are known to exist.(*are there requirements or limitations on the dependencies of submissions, or their licensing? Can a submission depend on closed-source, or copyleft-licensed libraries? Be explicit about cryptographic maturity or regulatory approval if application.)*

2.9. Additional Details Section:

See https://openid.net/wordpress-content/uploads/2018/06/OpenID-Connect-Conformance-Profiles.pdf for examples of test definitions for OpenID Connect conformance tests. Note that there are negative and positive tests and some tests are mandatory whereas others are designated as optional. A similar tabular test definition format could be used.
Test definitions could also be modelled after and/or borrowed from other test suites with similar goals, including those for Linked Data Signatures and particularly conformance tests for Verifiable Credentials and DIDs. If it served DIF’s goal of greater interoperability and alignment across standards bodies, the DIF Steering Committee could consider donating the resulting test suite to another organization.(*Mention here any relevant specifications, bibliography, external criteria of success such as criteria for consideration in a registry or standards process, etc)*