

Workgroup: COSE
Internet-Draft: draft-ietf-cose-dilithium-00
Published: 12 March 2023
Intended Status: Standards Track
Expires: 13 September 2023
Authors: M. Prorock O. Steele R. Misoczki M. Osborne
mesur.io Transmute Google IBM
C. Cloostermans
NXP

JOSE and COSE Encoding for Dilithium

Abstract

This document describes JSON and CBOR serializations for CRYSTALS Dilithium, a Post-Quantum Cryptography (PQC) based suite.

This document does not define any new cryptography, only serializations of existing cryptographic systems.

This document registers key types for JOSE and COSE, specifically LWE.

Key types in this document are specified by the cryptographic algorithm family in use by a particular algorithm as discussed in RFC7517.

This document registers signature algorithms types for JOSE and COSE, specifically CRYDI3 and others as required for use of various parameterizations of the post-quantum signature scheme CRYSTALS Dilithium.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 13 September 2023.

Copyright Notice

Copyright (c) 2023 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

- [1. Notational Conventions](#)
- [2. Terminology](#)
- [3. CRYSTALS-Dilithium](#)
 - [3.1. Overview](#)
 - [3.2. Parameters](#)
 - [3.2.1. Parameter sets](#)
 - [3.3. Core Operations](#)
 - [3.4. Using CRYDI with JOSE](#)
 - [3.4.1. CRYDI Key Representations](#)
 - [3.4.2. CRYDI Algorithms](#)
 - [3.4.3. CRYDI Signature Representation](#)
 - [3.5. Using CRYDI with COSE](#)
- [4. Security Considerations](#)
 - [4.1. Validating public keys](#)
 - [4.2. Side channel attacks](#)
 - [4.3. Randomness considerations](#)
- [5. IANA Considerations](#)
- [6. Appendix](#)
 - [6.1. Test Vectors](#)
 - [6.1.1. LWE CRYDIS](#)
- [7. Normative References](#)
- [8. Informative References](#)
- [Authors' Addresses](#)

1. Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

2. Terminology

The following terminology is used throughout this document:

PK : The public key for the signature scheme.

SK : The secret key for the signature scheme.

signature : The digital signature output.

message : The input to be signed by the signature scheme.

sha256 : The SHA-256 hash function defined in [[RFC6234](#)].

shake256 : The SHAKE256 hash function defined in [[RFC8702](#)].

3. CRYSTALS-Dilithium

3.1. Overview

This section of the document describes the lattice signature scheme CRYSTALS-Dilithium (CRYDI). The scheme is based on "Fiat-Shamir with Aborts" [Lyu09, Lyu12] utilizing a matrix of polynomials for key material, and a vector of polynomials for signatures. The parameter set is strategically chosen such that the signing algorithm is large enough to maintain zero-knowledge properties but small enough to prevent forgery of signatures. An example implementation and test vectors are provided.

CRYSTALS-Dilithium is a post-quantum approach to digital signatures that is an algorithmic approach that seeks to ensure key pair and signing properties that is a strong implementation meeting Existential Unforgeability under Chosen Message Attack (EUF-CMA) properties, while ensuring that the security levels reached meet security needs for resistance to both classical and quantum attacks. The algorithm itself is based on hard problems over module lattices, specifically Ring Learning with Errors (Ring-LWE). For all security levels the only operations required are variants of Keccak and number theoretic transforms (NTT) for the ring $Zq[X]/(X^{256}+1)$. This ensures that to increase or decrease the security level involves only the change of parameters rather than re-implementation of a related algorithm.

While based on Ring-LWE, CRYSTALS-Dilithium has less algebraic structure than direct Ring-LWE implementations and more closely resembles the unstructured lattices used in Learning with Errors (LWE). This brings a theoretical protection against future algebraic attacks on Ring-LWE that may be developed.

CRYSTALS-Dilithium, brings several advantages over other approaches to signature suites:

- *Post-quantum in nature - use of lattices and other approaches that should remain hard problems even when under attack utilizing quantum approaches
- *Simple implementation while maintaining security - a danger in many possible approaches to cryptography is that it may be possible inadvertently introduce errors in code that lead to weakness or decreases in security level
- *Signature and public key size - compared to other post-quantum approaches a reasonable key size has been achieved that also preserves desired security properties
- *Conservative parameter space - parameterization is utilized for the purposes of defining the sizes of matrices in use, and thereby the number of polynomials described by the key material.
- *Parameter set adjustment for greater security - increasing this matrix size increases the number of polynomials, and thereby the security level
- *Performance and optimization - the approach makes use of well known transforms that can be highly optimized, especially with use of hardware optimizations without being so large that it cannot be deployed in embedded or IoT environments without some degree of optimization.

The primary known disadvantage to CRYSTALS-Dilithium is the size of keys and signatures, especially as compared to classical approaches for digital signing.

3.2. Parameters

Unlike certain other approaches such as Ed25519 that have a large set of parameters, CRYSTALS-Dilithium uses distinct numbers of parameters to increase or decrease the security level according to the required level for a particular scenario. Under CRYSTALS-Dilithium, the key parameter specification determines the size of the matrix and thereby the number of polynomials that describe the lattice. For use according to this specification we do not recommend a parameter set of less than 3, which should be sufficient to maintain 128 bits of security for all known classical and quantum attacks. Under a parameter set at NIST level 3, a 6x5 matrix is utilized that thereby consists of 30 polynomials.

3.2.1. Parameter sets

Parameter sets are identified by the corresponding NIST level per the table below

NIST Level	Matrix Size	memory in bits
2	4x4	97.8
3	6x5	138.7
5	8x7	187.4

Table 1

3.3. Core Operations

Core operations used by the signature scheme should be implemented according to the details in [[CRYSTALS-Dilithium](#)]. Core operations include key generation, sign, and verify.

3.4. Using CRYDI with JOSE

This sections is based on [CBOR Object Signing and Encryption \(COSE\)](#) and [JSON Object Signing and Encryption \(JOSE\)](#)

3.4.1. CRYDI Key Representations

A new key type (kty) value "LWE" (for keys related to the family of algorithms that utilize Learning With Errors approaches to Post-quantum lattice based cryptography) is defined for public key algorithms that use base 64 encoded strings of the underlying binary material as private and public keys and that support cryptographic sponge functions. It has the following parameters:

*The parameter "kty" MUST be "LWE".

*The parameter "alg" MUST be specified, and its value MUST be one of the values specified in the table below

alg	Description
CRYDI5	CRYSTALS-Dilithium paramter set 5
CRYDI3	CRYSTALS-Dilithium paramter set 3
CRYDI2	CRYSTALS-Dilithium paramter set 2

Table 2

*The parameter "pset" MAY be specified to indicate the not only paramter set in use for the algorithm, but SHOULD also reflect the targeted NIST level for the algorithm in combination with the specified paramter set. For "alg" "CRYDI" one of the described parameter sets "2", "3", or "5" MUST be specified. Parameter set "3" or above SHOULD be used with "CRYDI" for any situation requiring at least 128bits of security against both quantum and classical attacks

*The parameter "x" MUST be present and contain the public key encoded using the base64url [[RFC4648](#)] encoding.

*The parameter "d" MUST be present for private keys and contain the private key encoded using the base64url encoding. This parameter MUST NOT be present for public keys.

Sizes of various key and signature material is as follows (for "pset" value "2")

Variable	Paramter Name	Paramter Set	Size	base64url encoded size
Signature	sig	2	3293	4393
Public Key	x	2	1952	2605
Private Key	d	2	4000	5337

Table 3

When calculating JWK Thumbprints [[RFC7638](#)], the four public key fields are included in the hash input in lexicographic order: "kty", "alg", and "x".

3.4.2. CRYDI Algorithms

In order to reduce the complexity of the key representation and signature representations we register a unique algorithm name per pset. This allows us to omit registering the pset term, and reduced the likelihood that it will be misused. These alg values are used in both key representations and signatures.

kty	alg	Paramter Set
LWE	CRYDI5	5
LWE	CRYDI3	3
LWE	CRYDI2	2

Table 4

3.4.2.1. Public Key

Per section 5.1 of [[CRYSTALS-Dilithium](#)]:

The public key, containing p and t1, is stored as the concatenation of the bit-packed representations of p and t1 in this order. Therefore, it has a size of 32 + 288 kbytes.

The public key is represented as x and encoded using base64url encoding as described in [[RFC7517](#)].

Example public key using only required fields:

===== NOTE: '\' line wrapping per RFC 8792 =====

```
{  
  "kty": "LWE",  
  "alg": "CRYDI3",  
  "x": "z7u7GwhsjnfHH3Nkrs2xvvw020Rcw5ymd1TnhRenjDdr00+nfXRVUZVy9q1\  
5zDn77zTgrIskM3WX8bqslc+B1fq12iA/wxD2jc1d6j+YjKctkGH260R7vc0YC2ZiMzw\  
zG17yebt7JkmjRbN1N+u/2fAKFLuziMcLNP6WLoWbMqxoC2X00VNAWX3QjXrCcGU23Nr\  
imtdmWz5NrP43E592Sctt5M+SV1fgQeYv8pHmtkQknE8/jr7TrgNpuiV7nXmhWHTMJ4I\  
zOGXgq43odFFthboEdKNT/enyu+VvUGoIJ6cN8C/1B6o1W1YHEaL0BEIFFbAiAhZ/vnf\  
cUYMaVPqsDJuETsjetcE32kGCD7Jkume2t068D1Ihb/2Z2JX8mkcbxFI6KrmXiRxXQj9\  
9LVn1fEzdf3Vfpes/C3omsFGqmTpLDK+AvW/SWvkDi2NKq7hL/Ayx1W2u2cqVerQZUTS\  
Z+ic6V8kZfxr3gRMnH0KuF5BtjleZ/yVvqqPjwPOZegCKE12Gd8duhcUde7CR55pil1o\  
UXy5AwgCcZTdEcJn10P0bGoots9T19gw1x4vnZCQUKVDPZuZ1gIkGqDUYXS01cNTjCMs\  
mIEmn0ZvB88jxULpb1v19HoQ3ocM2oZu4AZRt9G/L07Mwcui0uFCwtAIau+2gqNAn/Z\  
AS1010j2N0LLtAaOxoF+Ctzscrt0ZMyGHmoQ9daHkpUvEq0c08hDtLplnq3lQIIIfR0Q\  
jcNs9vNKBu87C0bjukZD+L8vV4zy8FN059MCSb9UCLwz2xvfdI1js9/J7hTGaVec8VPx\  
md42yPFrGw5Na1oefm8vW49EDmevc8AjAtwDirRBDFv9px3+5S+M6jhteSLYvpKJXQT1\  
zs1379KvIHwn9VHpA+PiUUw9TgF6xF8xWEGLN1o01Vn1xtM3givehjYxJ5p5/kBEFZI\  
DCyFzstAirJ2GadNhae+P1JFZzJwnX5jaLwzldquZwF3yTzNho4sgBA+fKqiXcgn2nw1\  
vz0Dkbxr6cMaUool0eFScU1nAz1Z39W64Ltt2nEuYs0Rx/ht2RzJxxFc21X3nLeEDFCe\  
NkNDxQFBsfpZjKKgJtXEx23mp+CbBVMrbagsLnzsAGLYbnroVmATU5Iqr6LgYBpuFs+N\  
Rkq7ZXh6CZPukMGQbc0GuNw06NBuuMNhir5ayGk1ZBiW82C7Nu0hs2pLcgNqwMtt1+Lw\  
8R96KyoSc784ZYAZ40QqvoySwmxQPBRTRJ+wB0sVpGBLTxdY9Gw3pXeXN5nao340d2ZA\  
7YEMlqcTHCAv3F8B9ew170fQ1mg6bvdMuovdVE+p0er7IAmWMRgviIzYv9sKEEqrCmuA\  
2ql5xPSbD05KRF8ZAZ2B81SCDR1nzXrQXZbXBKJivsCVQDuzxrwGE0gqRMpbk4f5GYCG\  
4i/08Knoru+jjf6wVQDYKfyZ1QUGR1XhkGUG1Xfv03r7UbJugcyjV05kbGxhoZkq0q8z\  
ZEpkefvrrNoxeoTw/z4QpjI8J1Y97GDb0mGVHbmdHugjMtVTGhVJFBbPIinmR+emt70+\  
4qOr7ywRxCvt2lziWtpPBwaf/1XDnN5Gesex1gR1YrcTRNmB808b01sxLQmxcTt4eQ0/\  
LUkas7qTJ3AQTh0fDdtIpqsthSBFy+WjSQuoXYMRcPi6M1pxJndDF32lCnL1ranV6e\  
F2ST0SYT+NwNDesMzTRmNbHUW5KAhu0k9WABTvcM5ba0Uq6i0a1NsFrcLag+KhxN6HPn\  
oobwJ/EsDi5S7TA18WrjqIhZ8x6h9eRRXerpa0w/FYk+2MpWbyp/98VE12/Ew0qAIiPp\  
e1AvUeM01RkpG64bJsmYtHuNWgcv5Qi7/eGw9ZpvB3J3G3jxvbynExqdFyDc067EKi\  
5wdxDFPuZUjkfKpekNvzQuIrqs49BzcRyMt5ndEVE21TPPFZ/R8B7Rxnb2LiK+hQc+cc9\  
pEEaWgwAOiMILcp/1CyY6Imd06RHsxf1MH7gej+hN41ka0EghI0l9kMGTLzbq5Pc8Pz\  
6F2LKTBMJWg9o/0blvilMH9EPblcLeF/bR1AZTUD6ZFdi2TxN6Epn3QVqeG/qPm1EBTF\  
Gw1V92m6/08Dd6zI1HPqwKbkHx4F567owofKHaM2imin0yVUpwxoRJru1RHMCB3tn8C4\  
ZpFl+sGV3Gip3tK1S7PKQkTqI6DMwxEbdrvtdY1sHzagpclLDisA/yFT4RR2m3VNJR9P\  
6Nx3teqN1eg6RXmD/M1KCdWr1cjz/6yeIQYwbr9CjItY/tLQX2gtAR1SX0h99UUBVv+Z\  
E03VOZ+EcsC781SB9G/6n6CFz1bk/HgAF+cu0yMbGnEM8W3mTUsP4JBACwk5w0XWNNQ\  
DWVEdgzuLGhPq+hYExDjVZrLElhkH8YgZA+7RXXUZHM/joNOGHUhlpUG/bFo3ktnaILCu\  
xSOXMubDC3VcitFFHsGK1svtcERDFxk1HA8pGa59jT0do6n3wEbnBDU1soKNFtpmcVke\  
U13XpvuoW3BgCwJzBUCWvPs47DJRgGx011bSaEYYlhTVaaShcvzgz46Akq0+Q7TjckDP\  
/8uzsSQk0AbuhxWFQpSiBP80Z/U="}
```

Example public key including optional fields:

===== NOTE: '\' line wrapping per RFC 8792 =====

```
{  
  "kid": "key-0",  
  "kty": "LWE",  
  "alg": "CRYDI3",  
  "key_ops": ["verify"],  
  "x": "z7u7GwhsjjnfhH3Nkrs2xvvw020Rcw5ymd1TnhRenjDdr00+nfXRVUZVy9q1\  
5zDn77zTgrIskM3WX8bqslc+B1fq12iA/wxD2jc1d6j+YjKctkGH260R7vc0YC2ZiMzW\  
zG17yebt7JkmjRbN1N+u/2fAKFLuziMcLNP6WLobMqxoC2X00VNAWX3QjXrCcGU23Nr\  
imtdmWz5NrP43E592Sctt5M+SVlfgQeYv8pHmtkQknE8/jr7TrgNpuiv7nXmhWHTMJ4I\  
zOGXgq43odFFthboEdKNT/enyu+VvUGoIJ6cN8C/1B6o1W1YHEaLOBEIFFbAiAhZ/vnf\  
cUYMaVPqsDJuETsjetcE32kGCD7Jkume2t068D1Ihb/2Z2JX8mkcbxFI6KrmXiRxXQj9\  
9LVn1fEzdf3Vfpcs/C3omsFGqmTpLDK+AvW/SWvkDi2NKq7hL/Ayx1W2u2cqVERQZUTS\  
Z+ic6V8kZfxr3gRMnH0KuF5Btj1eZ/yVvqqPjwPOZegCKE12Gd8duhcUde7CR55pil1o\  
UXy5AwgCcZTdEcJn10PObGoots9T19gw1x4vnZCQUKVDPZuZ1gIkGqDUYS01cNTjCMs\  
mFEmn0ZvB88jxULpb1v19HoQ3ocM2oZu4AZRt9G/L07Mwcui0uFCwtAIau+2gqNAn/Z\  
AS1010j2N0LLtAaOxoF+Ctzscrt0ZMyGHmoQ9daHkpUvEq0c08hDtLplnq31QIIIfr0Q\  
jcNs9vNKBu87C0bjukZD+L8vv4zy8FN059MCSb9UCLwz2xvfdI1js9/J7hTGaVec8VPx\  
md42yPFrGw5Na1oefm8vw49EDmevc8AjAtwDirRBDFv9px3+5S+M6jhteSLYvpKJXQT1\  
zs1379KviHwn9VHpA+PiUUw9TgF6xF8xWEWSN1o01Vn1xtM3givehjYxJ5p5/kBEFZI\  
DCyFzstAirJ2GadNhae+P1JFZZJWnX5jaLwzldquZwF3yTzNho4sgBA+fKqiXcgn2nw1\  
vz0Dkbxr6cMaUool0eFScU1nAz1Z39W64LtT2nEuYs0Rx/ht2RzJxxFc21X3nLeEDFCe\  
NkNDxQFBSpZjKKgJtXEx23mp+CbBVMrbagsLnzsAGLYbnroVmATU5Iqr6LgYBpuFs+N\  
Rkq7ZXh6CZPukMGQbc0GuNw06NBuuMNhir5ayGk1ZBiW82C7Nu0hs2pLcgNqWMtt1+Lw\  
8R96KyoSc784ZYAZ40QqvoySwmxQPBRTRJ+wB0sVpGBLTxdY9Gw3pXeXN5nao340d2ZA\  
7YEMlqcTHCAv3F8B9ewl70fQ1mg6bvdMuovdVE+p0er7IAmWMRgviTzYv9sKEEQrCmuu\  
2ql5xPSbD05Krf8ZAZ2B81SCDR1nzXrQXzbXBkJivsCVQDuzxrwGE0gqRMpbk4f5GYCG\  
4i/08Knoru+jjf6wVQDYKfyz1QUGR1XHkGUG1Xfv03r7UbJugycjV05kbGxhoZkq0q8z\  
ZEpkefvrrNoxeotw/z4QpjI8J1Y97Gdb0mGVHbmdHugjMtVTGhVJFBbPIinmR+emt70+\  
4qOr7ywRxCvt2lziWtpPBwaf/1XDnN5Gesex1gR1YrcTRNmB808b01sxLQmxcTt4eQ0/\\  
LUkas7qTJ3AQTh0fDdtIpqksthSBFy+WjSQuXCYMRcPi6M1pxJndDF321CnL1ranV6e\  
F2ST0SYT+NwNDesMzTRmNbHUW5KAhu0k9WABTvcM5ba0Uq6i0a1NsFrcLag+KhxN6HPn\  
oobwJ/EsDi5S7TA18WrjqIhZ8x6h9eRRXerpa0w/FYk+2MpWByp/98VE12/Ew0qAIiPp\  
e1AvUeM01RkpG64bJsmYtHuNWgcv5Qiy7/eGw9ZpvB3J3G3jxvbynExqdFyDc067EKi\  
5wdxDFPuZUjkfKpekNvzQuIrqs49BzcRyMt5ndEVE21TPPFZ/R8B7Rxnb2LiK+hQc+cc9\  
pEEaWgwA0iMILcp/1CyY6Imd06RHsxf1MH7gej+hN41kaoEghI0l9kMGTLzbq5Pc8Pz\  
6F2LKTBMJWg9o/0blvilMH9EPblcLeF/bR1AZTUD6ZFdi2TxN6Epn3QVqeG/qPm1EBTF\  
Gw1V92m6/08Dd6zI1HPqwKbkHx4F567owofKHam2imin0yVUpwxoRJru1RHMCB3tn8C4\  
ZpFl+sGV3Gip3tKls7PKQkTqI6DMwxEbdrvtdY1sHZagpc1LDisA/yFT4RR2m3VNJR9P\  
6Nx3teqN1eg6RXmD/M1KCdWr1cjZ/6yeIQYwbr9CjItY/tLQX2gtAR1SX0h99UUBVv+Z\  
E03VOZ+EcsC781SB9G/6n6CFz1bk/HgAF+cu0yMbGnEM8W3mTUsps4JBACwk5w0XWNNQ\  
DWEdgzuLGhPq+hYExDjVzrLElhkh8YgZA+7RXXUZHM/joNOGHUhPUG/bFo3ktnaILCu\  
xs0XMUbDC3VcitFFHsGK1svtcERDFxk1HA8pGa59jT0do6n3wEbnBDU1soKNFtpmcVke\  
U13XpvuoW3BgCwJzBUCWvPs47DJRgGx011bSaEYY1hTVaaShcvzgz46Akq0+Q7TjckDP\  
/8uzsSQk0AbuhxWFQpSiBP80Z/U=""  
}
```

3.4.2.2. Private Key

Per section 5.1 of [[CRYSTALS-Dilithium](#)]:

The secret key contains p, K, tr, s_1, s_2 and t_0 and is also stored as a bit-packed representation of these quantities in the given order. Consequently, a secret key requires $64 + 48 + 32((k+1) * \text{dlog}(2n+1)e + 14k)$ bytes. For the weak, medium and high security level this is equal to $112 + 576k + 128l$ bytes. With the very high security parameters one needs $112 + 544k + 96l = 3856$ bytes.

The private key is represented as d and encoded using base64url encoding as described in [[RFC7517](#)].

Example private key using only required fields:

===== NOTE: '\' line wrapping per RFC 8792 =====

```
{  
  "kty": "LWE",  
  "alg": "CRYDI3",  
  "x": "z7u7GwhsjnfHH3Nkrs2xvvw020Rcw5ymd1TnhRenjDdr00+nfXRVUZVy9q1\  
5zDn77zTgrIskM3WX8bqslc+B1fq12iA/wxD2jc1d6j+YjKctkGH260R7vc0YC2ZiMzw\  
zG17yebt7JkmjRbN1N+u/2fAKFLuziMcLNP6WLoWbMqxoC2X00VNAWX3QjXrCcGU23Nr\  
imtdmWz5NrP43E592Sctt5M+SV1fgQeYv8pHmtkQknE8/jr7TrgNpuiV7nXmhWHTMJ4I\  
zOGXgq43odFFthboEdKNT/enyu+VvUGoIJ6cN8C/1B6o1W1YHEaL0BEIFFbAiAhZ/vnf\  
cUYMaVPqsDJuETsjetcE32kGCD7Jkume2t068D1Ihb/2Z2JX8mkcbxFI6KrmXiRxXQj9\  
9LVn1fEzdf3Vfpes/C3omsFGqmTpLDK+AvW/SWvkDi2NKq7hL/Ayx1W2u2cqVerQZUTS\  
Z+ic6V8kZfxr3gRMnH0KuF5BtjleZ/yVvqqPjwPOZegCKEl2Gd8duhcUde7CR55pil1o\  
UXy5AwgCcZTdEcJn10P0bGoots9T19gw1x4vnZCQUKVDPZuZ1gIkGqDUYXS01cNTjCMs\  
mIEmn0ZvB88jxULpb1v19HoQ3ocM2oZu4AZRt9G/L07Mwcui0uFCwtAIau+2gqNAn/Z\  
AS1010j2N0LLtAaOxoF+Ctzscrt0ZMyGHmoQ9daHkpUvEq0c08hDtLplnq3lQIIIfR0Q\  
jcNs9vNKBu87C0bjukZD+L8vV4zy8FN059MCSb9UCLwz2xvfdI1js9/J7hTGaVec8VPx\  
md42yPFrGw5Na1oefm8vW49EDmevc8AjAtwDirRBDFv9pX3+5S+M6jhteSLYvpKJXQT1\  
zs1379KvIHwn9VHpA+PiUUw9TgF6xF8xWEGLN1o01Vn1xtM3givehjYxJ5p5/kBEFZI\  
DCyFzstAirJ2GadNhae+P1JFZzJwnX5jaLwzldquZwF3yTzNho4sgBA+fKqiXcgn2nw1\  
vz0Dkbxr6cMaUool0eFScU1nAz1Z39W64Ltt2nEuYs0Rx/ht2RzJxxFc21X3nLeEDFCe\  
NkNDxQFBSpZjKKgJtXEx23mp+CbBVMrbagsLnzsAGLYbnroVmATU5Iqr6LgYBpuFs+N\  
Rkq7ZXh6CZPukMGQbc0GuNw06NBuuMNhir5ayGk1ZBiW82C7Nu0hs2pLcgNqwMtt1+Lw\  
8R96KyoSc784ZYAZ40QqvoySwmxQPBRTRJ+wB0sVpGBLTxdY9Gw3pXeXN5nao340d2ZA\  
7YEMlqcTHCAv3F8B9ew170fQ1mg6bvdMuovdVE+p0er7IAmWMRgviIzYv9sKEEqrCmuA\  
2ql5xPSbD05KRF8AZZ2B81SCDR1nzXrQXZbXBkJivsCVQDuzxrwGE0gqRMpbk4f5GYCG\  
4i/08Knoru+jjf6wVQDYKfyz1QUGR1XhkGUG1Xfv03r7UbJugcyjV05kbGxhoZkq0q8z\  
ZEpkefvrrNoxeoTw/z4QpjI8J1Y97GDb0mGVHbmdHugjMtVTGhVJFBbPIinmR+emt70+\  
4qOr7ywRxCvt2lziWtpPBwaf/1XDnN5Gesex1gR1YrcTRNmB808b01sxLQmxcTt4eQ0/\  
LUkas7qTJ3AQTh0fDdtIpqstthsBFy+WjSQuoXYMRcPi6M1pxJndDF32lCnL1ranV6e\  
F2ST0SYT+NwNDesMzTRmNbHUW5KAhu0k9WABTvcM5ba0Uq6i0a1NsFrcLag+KhxN6HPn\  
oobwJ/EsDi5S7TA18WrjqIhZ8x6h9eRRXerpa0w/FYk+2MpWbyp/98VE12/Ew0qAIiPp\  
e1AvUeM01RkpG64bJsmYtHuNWgcv5Qi7/eGw9ZpvB3J3G3jxvbynExqdFyDc067EKi\  
5wdxFPuZUjkfKpekNvzQuIrqs49BzcRyMt5ndEVE21TPPFZ/R8B7Rxnb2LiK+hQc+cc9\  
pEEaWgwAOiMILcp/1Cy6I0d06RHsxf1MH7gej+hN41ka0EghI0l9kMGTLzbq5Pc8Pz\  
6F2LKTBMJWg9o/0blvilMH9EPblcLeF/bR1AZTUD6ZFd12TxN6Epn3QVqeG/qPm1EBTF\  
Gw1V92m6/08Dd6zI1HPqwKbkHx4F567owofKHaM2imin0yVUpwxoRJru1RHMCB3tn8C4\  
ZpFl+sGV3Gip3tK1S7PKQkTqI6DMwxEbdrvtdY1sHzagpclLDisA/yFT4RR2m3VNJR9P\  
6Nx3teqN1eg6RXmD/M1KCdWr1cjz/6yeIQYwbr9CjItY/tLQX2gtAR1SX0h99UUBVv+z\  
E03VOZ+EcsC781SB9G/6n6CFz1bk/HgAF+cu0yMbGnEM8W3mTUsP4JBACwk5w0XWNNQ\  
DWVEdgzuLGhPq+hYExDjVZrLElhkH8YgZA+7RXXUZHM/joNOGHUhPUG/bFo3ktnaILCu\  
xSOXMubDC3VcitFFHsGK1svtcERDFxk1HA8pGa59jT0do6n3wEbnBDU1soKNFtpmcVke\  
U13XpvuoW3BgCwJzBUCWvPs47DJRgGx011bSaEYYlhTVaaShcvzgz46Akq0+Q7TjckDP\  
/8uzssSqk0AbuhxWFQpSiBP80Z/U=",  
  "d": "z7u7GwhsjnfHH3Nkrs2xvvw020Rcw5ymd1TnhRenjDUBgL6Fk1HURz5btM5\  
yrI5FQdWk+U2srVuSmfDV7EYG897mUFY35Z0WQ0mZ9XvI0KCh+GFF0k56b5F0Fq6xnV8\  
UDQnFyY2JREU0HdiUjcUNxA1YXR3QiQ0BkE1AUBmFE0AUHZGBzQAU2dxVIgTQRV3U3g4\  
GGiISEYQhHRSWDIBQ2Z3UIIwdsV1EWhwBTYiWGI3VmJVI1UIU2REdUhHBoJ2gRhFUThy\  
BSQnhBIGI1AoMVB2MCNhUXQiNUGCKHgzUmQxU3dEgBhmQyIQgmFjdxY1dCJgGBSEB4Ij\"
```

CEJ0MBGIQWRRN3QjRmRSQWQIJgNjcjdnlJhJIU1M1JRp1NmF4dwhHIIIdEYYcAhEc1BQ\JjESAiBwBQYzYlAIiocBcoZFcGVka2SDMCVTBjgzCAAzNnQGYHI1VwJzYxQRckBIZBV4\VxZmZiV1YXgHFRNjdDEFIYVOFIvDhcniINEhhIURjg0cxJ0SCIWUUvCHJzdDUTASciAW\UiJAg1IoQkIwNjM1cwACZxcHZVJAh4EnNnWAZVVoBjNnNEcicTdyEEUHBVFjETETNjd0\YUFmFDVXNUCHFVJoE2A1VwFhMzc0dQckMYJUaBJ0JkUBdyd1AnZiJ3hYYkWAgYR1Vzid\BERVh1NQAFIGWIhUZXCEQxITHyR1FIGNTKAcwdRNBDYEd2RVEwUDMzWAhNQEEMYAS\hUSCgTJ3ViDXU1FBFxKvhVCCZEABjQCAxFGNkhHQzM1YSSHn1EBEmJkgWZCVwZHSVD\GDZzRCQiNhE3IghDhSFoBYCHNFVHMxZAZTSGAVMUQkhBKIFRQEVB0cHNGEiJVScQQh\hzQiBzKBRY4Q0R2MVUldwVCIKQYEEgFYEREY2NERyFVdHJzdAZHBmhdSCFIgh1IwGB\AxNzFjEoUWFCF4AhZRJSER0EETHxAGYBJTgUcUdFJB0FRmcVYnZUUFCAY1AnZEZBVThs\ECBQYBNGeAdzQ3KGhIE3ZiFxQoVCgQBjEFdFcIV0IAaFcgi0iAgAUVQAhEInQWE CY1I4\E2U0MkAXQSZkdSRRc2I4BjEiSGd4hgQEEDcTRmhFd3MBMmY2gERxNwiISAvkFVETGccI\gYhzRXByGBgzKGvXJuhoGEY1hgFmZwgmEWYwvoIsd4V1hid4VUMHgSZXhXUSAcgmJ3Eg\MQIzIDITHwRSARQhFB2QQBjEgIoEHN1BhMcIiIBU1ZWChdBMyZFQoQ2UUJXJCFnZyFD\RTFUUTQoQmUjB0aHJXJHeDz1JGBCExATEUEDg3BTACHWImN0AwcFB3IUgBEARxVUREdX\QzhVBEBBF4UgcRhCg4gUcoRkdYCAIUQBRUJUYjFjEBYUhSBjIyV2cXBcckEiMic1N4ED\gDUGVSCHhCYURXcQB10Dg4hDJFJ3J1d2gyYnQYclRjE3VwCQNXYBYn0GhYFoU2dHATAw\0EeBUGQjJhcDgUJTRXBXJ3IAejExhXeEEmgHIAAGdjUVBndnI2FCAVcyV4cxIyZ2dYE1\ZEiHcYJYCaCcXQXJCaER1coIDRWJkcSnHEVF3JGOCQkYWyKcndRA1QTh0MFgzIyVocYJY\cWIAFRNiE1VAUECBI3MzQiZkUhR1cid1NSAXFXN0gUNnRCV0ISNmYnB3NIzYMIQWEVVz\E1EohnQyKBNoY1ccmdjVYiGhvU1A0CHMTZIURBgR4aIJwJQJ1IDMYhwNGNwiGcIBUdA\NXMBETUgICJyMkMIN1BAIAB4gEMDUwhndFJKQDEgRRMld4EzhRM0ZhGAYHMgZ4NhEEhn\U2I2VicBBXZUFUNoczcmBzBnUEBxUwcdg4RHUXZS0EzogABRAISVEAzdoQhRmBgEWYE\Z4U1dgQ2gjjgQUjMScgIIFQR3YFczhTyob1IiVCYGBAVmVAFIdhRmZ1InhwdTRjJjNhVx\IzcWgjF1FCaCh1IWUySIaDFwAWV3RAIxg2QWYgAYMujP7wmw0wPp7Uk13L1Ka1Y/6dN4\dBriAYS8JnkVq6pPeBf07ccX95SrVfA07EX7RVEYyhVR9QOQyEpLBUMcfcfnHCZWM0o\OBF7BXiWMR9BQo4ybtpJGKQ+IzyCKUJVRhZ+uae182qYcBKFMd00zXi08kAa98eUy6SR\pPfKPD6D+xXgtJ0FWtYnp1Jy2aIG3HqmItHoSdVIvccGkf94gpVWTMeJQsQpgq7dAJiJ\5J0MQjk7JIhCIZxb4T8sQHzA55MFfV7Hus/8FUX7Nfin1JRmc2zHL/7kdfCFSwG67iw\U4ob2kTwdkZPv0L+d3e+A0E0PiJ4vVJA0jhWm02fIFNvFhNqPh0MSiSkatPGbSVdqQ1\PsG6C+1YqMrTM7KFr4hTQM8a3+tA0sImMjXSSPDkVeuJFq1rw642SJJx8yZTXVe8g75D\ZTYghbeX5LLzaVkt9mzs7cW16Zy+C3MwnWDrGQ6hUDxYaYjp7SOGJHepcmVV214oD6nw\5QprgpGTxVcdXQU00fhKwerYDko0Ij+uqk7NYDv0t8zANphYcE3v+6yVFyYh3eg7DyRj\riZIcbaG91ySv2iRRC+cWaymH6xuqaHRwZu/p962/u8/c3rITJzCoVc+0bnZ5oItZFBelAYFhLBx7PvPdBULXyCqmtk0tnT/jnaCUVxtGeaIeQmmeM4yPq3d5uWBf0vIyuPmfBSKd\Y0NETGlsaoQuqFp0kCmQdMVZKh3UZ8A0jw22LlqaZlrUf0akb0fs7le2HT47KV9y0JHC\tec9tjHUEBVmma504AofGcVXLbkqKv+Soax9GooHV0v+uxa8iwjAdTZKtqwKnKDx4jar\+zotCsYi4BuB2JbkjnHG6NL7ubN+aKnwnzznMKQZIh2Q7vSRYKTM8j90GLq7IP8q2NS\oc7it//eAvb4oF6LaY7qebxQ6ROXCSRrrXgpo+pw31tfuUCuGzAxD4+wMzu3dlXsivhJ\PNTEjI/V6GmkR1fZ9XnYfj8SILETwk03dMFJh3LmUwkbRV+C3ml2GzjgQVTkvP82KDBL\Dar9iKyPkJnMnK9Ix/StVyJbGAtGp4jHnp+PSjz9ja4qI9jVrjGgIUQhw0DnI0fnplUn\Qhz3F9MQXmplSPvFw8M0xkUKsAcxQvxZgb5LkYByZ0Zr0/iphwhnE6zQuOva+8uTyBX/\B9VR24tUITvlhy7SS6JrULrvTA+d/ZCiqKRx61iF6pU3BoC8fgA9D/AifiQnPz0SI5kx\FJfdTz1LWMju1QKBHFvRFLE9eFD0rnwAGx7Pgpvc/KrLqVmcmj/96TYtoedp/iW4asfY\c2vs+GVyxVoumIdFPHJpencwbE/nizNvDaJCIh1iIqgXzDsI8bENh2B9cutDWX+bshZSC\jSQb9YkGN+MoNiJ1XmQHSJdyFPhzWPibdS/1pS90ppPWIY+PpL0fzDSGFFWswQ4q5Phc\pLWHx5lw9KSye+T86p6kadnBBTLTyfn0dG7Np09QKQObMN60MnybkVGx5nH9yLJ1F1mV\0H+k0VZIKm4UzYV+RYfqqXYtMqTQxeQ1U7L7o0H+6viErxuKj5rs3i+r1rdFEcAGgCoq\0mixATHISAHi2eSV5fk3r5xMkKSwwPIRuMt50+kk1RPu0LohTj7G1CnL602xwBdQMTUx\

4Jq5JBWnfB+U4D9n0si1DwikIhpauy0oBeawo4iFQiWVLwjeeQvY6zj66170xsPHjZXg\ uCitsWfp5MYV3cLTkb80uCM/xhp4Y0Edobt6x3k1FD8vh8g3YAG0Xe/U+Iz3k1npCt2\ R0Q21GQa0JM14nbQr3tqTLoXv4szaErFp/Xw05Cnt9DsBzN5DNrmfF6EDcfVf/hn8v9a\ wrg6Rfv8Jpys1YFpwLanhb3Wz+x1yaDsa54Id1FOFnyBxv8GppbFrMpVFx/nLAXGIocc\ WjcRKs0tBJUW/IoXeK0MPUD1wHR4dqUCEXsoexHjiNe5sH+akr6UID0bF70hhupBoiY9\ AzVxi5zXf2VdafyQrkGfKz4BEUKiqcaajHr1CF9ZJ+Mjdmfr3z0xyCmCAWir5ZL0BXDj\ T7sYCV3QjCz4a2mGvee9Ix9kSLapCq90UMAxnTLjJGQM/d1pgjDsjsCZX5wKdsnMs79\ 60Z75BGDOC1dDINj4f5kHZmwvcmw/04mi/1RPBUABXse3Up3eJQ0X2haZPqmy0+2PZTF\ exku9pETHtKcfSdRe1oJLmlB34JSogRmNp1eBxakcIL09huiFVtGVZng/pC/ryoJ/T9q\ 9w4aV5H+4u2dHc29Vb77SasxCdRH0sDaLaPpesRXsrdJwjbiz0gzR1Ix+83o07NuhE+C\ kKf07cZMrFm8r8g1M1zDiFrTf3RTusMtIW6CV1VuTROZFnqqaR5yeYPprpSELtQHSwz\ U5AaY5Qd8tbky5ec+2/QkX0+cdyWhQUuBRpibwpRpD3x1yTgT4E91cwTFpvSLk54ZHf+\ D3EsZf0PYMN6d4jVdh9iv+0tCebnfMqp65wY26YBopSLtCXXb1anU1RPlzPzRq99yKnt\ FM7gK1XnBAZoZBBqCyZw90HWmttIFWcm14Wd5BxF9uZh2Y8gtcN8UKWHv43tsNBa7j/T\ ikIBskIVI/6EqvyPW4YTdyz2V8RKHN5XcdpdwFaVhgSJMC4I6Bm0Lwenhkma17Sd247q\ uCtEow8qh+w7Jk4SxrmvJxd5sBnvz150KEaHPeWNNJw00bWEDT+0ZzzD8vMN1/GkbbB3\ s7UfcJXZbRu7HtQ+wHIblBKVstX3hMonra+k6wS9KPhcAaC3IjZ7ZApSedKk1sW1SuDg\ 148Yw2/cyS3LvmISQn9KPwK7yEpNQnV0vurn3ZFOG00eDjsXujI+xIrRia5GQ1yb31ma\ nJnf2PdHcMmVr0wu41MGno7a14nMRdnXkBu8bV0p8wF6Toz59hBJ3a/F+mP4/a19Ixra\ wiVVeEPgoi9QQ9NcLgQEFCoskA+EpcLK0FxV2rYI9JFNF/nDxP5nmGtnkmlFaLo+pleH\ CJYS00TGKQr6X+Y65N011x5nNwsnwkIukCodoSt4Givdoe/S9JNiu8tw+jTBae2hNr9c\ glErCNKDYe1+T+Ldyr9rf0Km9LKNyTBsodgF4KI/hFh9IV/i55DTWtqjpN0eQnPTB3/6\ +7KzTfSE9il5UMcP3zKKC2mAQvtyYxF3k0m24ZTwPs2LAPJkr/xtPH3BnGE/UfUDmvDS\ TBp9m049Nh9oDZvI4HKsY8auiyENk0ys67F9GTHh0YM0FgHyP5qk4/IR5YC3lnq7xx6i\ owebEJAY63htMytq+xd3cJyZR01wBU0qvSpd/A=="
}

Example private key using optional fields:

===== NOTE: '\' line wrapping per RFC 8792 =====

```
{  
    "kid": "key-0",  
    "kty": "LWE",  
    "alg": "CRYDI3",  
    "key_ops": ["sign"],  
    "x": "z7u7GwhsjjnfhH3Nkrs2xvw020Rcw5ymd1TnhRenjDdr00+nfXRVUZV  
y9q1\\  
5zDn77zTgrIskM3WX8bqslc+B1fq12iA/wxD2jc1d6j+YjKctkGH260R7vc0YC2ZiMzW\\  
zG17yebt7JkmjRbN1N+u/2fAKFLuziMcLNP6WLobMqxoC2X00VNAWX3QjXrCcGU23Nr\\  
imtdmWz5NrP43E592Sctt5M+SVlfgQeYv8pHmtkQknE8/jr7TrgNpuiv7nXmhWHTMJ4I\\  
zOGXgq43odFFthboEdKNT/enyu+VvUGoIJ6cN8C/1B6o1W1YHEaLOBEIFFbAiAhZ/vnf\\  
cUYMaVPqsDJuETsjetcE32kGCD7Jkume2t068D1Ihb/2Z2JX8mkcbxFI6KrmXiRxXQj9\\  
9LVn1fEzdf3Vfpc/C3omsFGqmTpLDK+A  
v/SWvkDi2NKq7hL/Ayx1W2u2cqVERQZUTS\\  
Z+ic6V8kZfxr3gRMnH0KuF5BtjleZ/yVvqqPjwPOZegCKE12Gd8duhcUde7CR55pil1o\\  
UXy5AwgCcZTdEcJn10P0bGoots9T19gw1x4vnZCQUKVDPZuZ1gIkGqDUYS01cNTjCMs\\  
mFEmn0ZvB88jxULpb1v19HoQ3ocM2oZu4AZRt9G/L07Mwcui0uFCwtAIau+2gqNAn/Z\\  
AS1010j2N0LLtAa0xoF+Ctzscrt0ZMyGHmoQ9daHkpUvEq0c08hDtLplnq31QIIIfr0Q\\  
jcNs9vNKBu87C0bjukZD+L8vv4zy8FN059MCSb9UCLwz2xvfdI1js9/J7hTGaVec8VPx\\  
md42yPFrGw5Na1oefm8vw49EDmevc8AjAtwDirRBDFv9px3+5S+M6jhteSLYvpKJXQT1\\  
zs1379KviHwn9VHpA+PiUUw9TgF6xF8xWEGSN1001Vn1xtM3givehjYxJ5p5/kBEFZI\\  
DCyFzstAirJ2GadNhae+P1JFZZJWnX5jaLwzldquZwF3yTzNho4sgBA+fKqiXcgn2nw1\\  
vz0Dkbxr6cMaUool0eFScu1nAz1Z39W64Lt2nEuYs0Rx/ht2RzJxxFc21X3nLeEDFCe\\  
NkNDxQFBSpZjKKgtjXEx23mp+CbBVMrbagsLnzsAGLYbnroVmATU5Iqr6LgYBpuFs+N\\  
Rkq7ZXh6CZPukMGQbc0GuNw06NBuuMNhir5ayGk1ZBiW82C7Nu0hs2pLcgNqWMtt1+Lw\\  
8R96KyoSc784ZYAZ40QqvoySwmxQPBRTRJ+wB0sVpGBLTxdY9Gw3pXeXN5nao340d2ZA\\  
7YEMlqcTHCAv3F8B9ewl70fQ1mg6bvdMuovdVE+p0er7IAmWMRgviTzYv9sKEEQrCmu\\  
2ql5xPSbD05Krf8ZAZ2B81SCDR1nzXrQXzbXBkJivsCVQDuzxrwGE0gqRMpbk4f5GYCG\\  
4i/08Knoru+jjf6wVQDYKfyz1QUGR1XHkGUG1Xfv03r7UbJugycjV05kbGxhoZkq0q8z\\  
ZEpkefvrrNoxeotw/z4QpjI8J1Y97Gdb0mGVHbmdHugjMtVTGhVJFBBPIinmR+emt70+\\  
4qOr7ywRxCvt2lziWtpPBwaf/1XDnN5Gesex1gR1YrcTRNmB808b01sxLQmxct4eQ0/\\  
LUkas7qTJ3AQTh0fDdtIpqksthSBFy+WjSQuXCYMRcPi6M1pxJndDF321CnL1ranV6e\\  
F2ST0SYT+NwNDesMzTRmNbHUW5KAhu0k9WABTvcM5ba0Uq6i0a1NsFrcLag+KhxN6HPn\\  
oobwJ/EsDi5S7TA18WrjqIhZ8x6h9eRRXerpa0w/FYk+2MpWbyp/98VE12/Ew0qAIiPp\\  
e1AvUeM01RkpG64bJsmYtHuNWgcv5Qiy7/eGw9ZpvB3J3G3jxvbynExqdFyDc067EKi\\  
5wxDfPuZUjkfKpekNvzQuIrqs49BzcRyMt5ndEVE21TPPFZ/R8B7Rxnb2LiK+hQc+cc9\\  
pEEawgwAOiMILcp/1CyY6Imd06RHsxf1MH7gej+hN41kaoEghI019kMGTLzbq5Pc8Pz\\  
6F2LKTBMJWg9o/0blvilMH9EPblcLeF/bR1AZTUD6ZFdi2TxN6Epn3QVqeG/qPm1EBTF\\  
Gw1V92m6/08Dd6zI1HPqwKbkHx4F567owofKHaM2imin0yVUpwxoRJru1RHMCB3tn8C4\\  
ZpFl+sGV3Gip3tKls7PKQkTqI6DMwxEbdrvtdY1sHZagpc1LDisA/yFT4RR2m3VNJR9P\\  
6Nx3teqN1eg6RXmD/M1KCdWr1cjZ/6yeIQYwbr9CjItY/tLQX2gtAR1SX0h99UUBVv+z\\  
E03VOZ+EcsC781SB9G/6n6CFz1bk/HgAF+cu0yMbGnEM8W3mTUsps4JBACwk5w0XWNNQ\\  
DWEdgzuLGhPq+hYExDjVzrLElhkh8YgZA+7RXXUZHM/joNOGHUhPUG/bFo3ktnaILCu\\  
xs0XMUbDC3VcitFFHsGK1svtcERDFxk1HA8pGa59jT0do6n3wEbnBDU1soKNFtpmcVke\\  
U13XpvuoW3BgCwJzBUCWvPs47DJRgGx011bSaEYY1hTVaaShcvzgz46Akq0+Q7TjckDP\\  
/8uzsSQk0AbuhxWFQpSiBP80Z/U=",  
    "d": "z7u7GwhsjjnfhH3Nkrs2xvw020Rcw5ymd1TnhRenjDUBgLFk1HURz5btM5\\  
yrI5FQdwk+U2srVuSmfDV7EY897mUFY35Z0WQ0mZ9XvI0KCh+GFF0k56b5F0Fq6xnV8\\  
UDQnFyY2JREUOHdiUjcUNxA1YxR3QiQ0BKE1AUBmFEOAUHZGBzQAU2dxVIgTQRV3U3g4\\
```

GGIISYEYQhHRSWDIBQ2Z3UIIWdSV1EWhwBTYiWGI3VmJVI1UIU2REdUhHBoJ2gRhFUThy\BSQnhBIGI1AoMVB2MCNhUXQiNUGCKHgzUmQxU3dEgBhmQyIQgmFjdxY1dCJgGBSEB4Ij\CEJ0MBGIQWRRN3QjRmRSQWQIjgNjcjdnlJhJIU1M1Jrd1NmF4dwhHIIdEYYcAhEc1BQ\JjESAiBwBQYzY1AIlocBcoZFcGVKA2SDMCVTBjgzCAAzNnQGYHI1VwJzYxQRckBIZBV4\VxZmZiV1YXgHFRNjDEFIYVOFIVdhcnIINehhIURjg0cxJ0SCIWYUUVCJzdDUTASciAw\UiJAgliQkIwNjMlcwACZxcHZVJAh4EnNnWAZVVoBjNnNEcicTdyEEUHBVFjETETNjd0\YUFmFDVXNUcHFVJoE2A1VwFhMzc0dQckMYJuaBJ0JkUBdyd1AnZiJ3hYYkWAgYR1VziD\BERVh1NQAFIGWIhUZXCEQxITHyR1FIGNTKAcwdRNBGDYEd2RVEwUDMzWAhnQEEMYAS\hUSCgTJ3VIdXU1FBFxFkhVCCZEABJjQCAxFGNkhHQzM1YSSHn1EBEmJkgWZCVwZHRSD\GDZzRCQinhE3IghDhSFoBYCHNFVHMxzAZTSGAVMUQkhBKIFRQEVB0cHNGEiJVScQqh\hzQiBzKBRYRY4Q0R2MVU1dwVCIkQYEEgFYEREY2NERyFvdHJzdAZHbmhdSCFIgh1IwGB\AxNzFjEoUWFcf4AhZRJSER0EETHxAGYBJTgUcUdFJB0FRmcVYnZUUFcAY1AnZEZBVThs\ECBQYBNGeAdzQ3KGhIE3ZiFxQoVCgQbjEFdFcIV0IAaFcgi0iAgAUvQAhEInQWEcy1I4\E2U0MkAXQSZkdSRrc2I4BjEiSGd4hgQEEdctrmhFd3MBMmY2gERxNwiISAvkFVETGCCi\gYhzRXByGBgzkGVXJUhoGEY1hgFmZwgmEWywVoISd4V1hid4VUMHgSZXhXUsaCgmJ3Eg\MQIzIDITHwRSARQhBFB2QQBjEgioEHN1BhMciiIBU1ZwChdBMyZFQoQ2UUJxJCFnZyFD\RTFUUTQoQmUjB0aHJXJHeDz1JGBCExATEUEDg3BTachWImN0AWcFB3IugBEARxVUREdX\QzhVBEBBF4UgcRhCg4gUcoRkdYCAIUQBRUJUYjFjEBYuhsBjIyV2cXBcYckEiMic1N4ED\gDUGVSCHhCYURXcQB10Dg4hDJFJ3J1d2gyYnQYclRjE3VwCQNXJBYh0GhYFo2dHATAw\0EeBUGqjJhcDgUJTRBXJ3IAejEXhXeEEmghIAAGdjUVBndnI2FCAVcyV4cxIyZ2dYE1\ZEihcYJYacCcXQXJCaER1coIDRWjkcsnhEVF3JG0CQkYwYkndRA1QTh0MFgzIyVocYJY\cwiAFRNiE1VAUECBI3MzQizkUhR1cid1NSAXFXN0gUNnRCV0ISNmYnB3NIZyMIQWEVVz\E1EohnQyKBNoY1cCdmdjVYiGhv1A0CHMTZIURBgR4aIJwJQJ1IDMYhwNGNwiGcIBUdA\NxbETUgICJyMkMIN1BAIAB4gEMDUwhndFjkQDEgRRMld4EzhRM0ZhGAYHMgZ4NhEEhn\U2I2VicBBXZUFUNoczcmBzBnUEBxUwcDg4RHUXZS0EZogABHRAISVEAzdoQhRmBgEWYE\Z4U1dgQ2gjgQUjMScgIIFQR3YFcZhTYoB1IiVCYGBAVmVAFIdhRmZ1InhwdTRjJjNhVx\IzcWgjFlFCaChlIWUySiADFwAW3RAIxg2QwYgAYMuJp7wmw0wPp7ukl3L1Ka1Y/6dN4\dBriAYS8JnkVq6pPeBf07ccX95SrVfa07EX7RVEyyhVR9Q0QyEpLBUMcfcfnHCZWM0o\OBF7BXiWMR9BQo4ybtPJGKQ+IzyCKUJVRhZ+uae182qYcBKFMd00zXi08kAa98eUy6SR\pFfKPD6D+xXgtJ0FwtYnp1Jy2aIG3HqMiTHoSdVIVccGkf94gpVWTMeJQsQpgq7dAJiJ\5J0MQjk7JIHcIzxb4T8sQHzA55MFvM7Hus/8FUX7NfIN1JRmc2zHL/7kdfCFSwG67iW\U4ob2kTwdkzPv0L+d3e+A0E0PiJ4vVJA0jhwM02fIFNvFhNqPh0MSiSkatPGbSVdqQ1\PsG6C+1YqMrTM7KFr4hTQM8a3+tA0sImMjXSSPDkVeuJFq1rw642SJJx8yZTXVe8g75D\ZTYghbeX5LLzaVkt9mzs7cW16Zy+C3MwnWDrGQ6hUDxYaYJp7S0GJHepcmVV214oD6nw\5QprgpGIxVcdXQU00fhKwerYDko0Ij+uqk7NYDv0t8zANphYcE3v+6yVFyYh3eg7DyRj\rIzIcbaG91ySv2iRRC+cWaymH6xuqaHRwZu/p962/u8/c3rITJzCoVc+0bnZ5oItZFBelAYFhLBx7PvPdBULXyCqmtk0tnT/jnaCUVxtGeaIeQmmeM4yPq3d5ulwBf0vIyuPmfBSKd\Y0NETGlsaoQuqFp0kCmQdMVZKh3UZ8A0jw22LlqaZlrUf0akb0fs7le2HT47KV9y0JHC\tec9tjHUEBVmma504AofGcVXLbkqKv+Soax9GooHOv0+uxa8iwjAdTZKtqwKnKDx4jar\+zotCsYi4BuB2JbkjnHG6NL7ubN+aNKnwnzznMKQZih2Q7vSRYKTm8j90GLq7IP8q2NS\oc7iT//eAvb4oF6LaY7qebxQ6ROXCSRrrXgpo+pw3ltfuUCuGzAx4+wMZU3d1XsivhJ\PnTejI/V6GmkR1fZ9XnYfj8SILETwk03dMFJh3LmUwkbRV+C3mL2GzjgQVTkvP82KDBL\Dar9iKyPkJnMnK9Ix/StVjBGAtpGp4jHnp+PSjz9ja4qI9jVRjGgIUQhw0DnI0fnplUn\Qhz3F9MQXMPPLSPvFw8M0xkUKsAcxQvxZGb5LkYByZ0Zr0/ippwhnE6zQuOva+8uTyBX/\B9VR24tUITvlhy7SS6JrULrvTA+d/ZCiqKRx61iF6pU3BoC8fgA9D/AifiQnPz0SI5kx\FFfdTz1LWMju1QKBHFvRFLE9eFD0rnwAGx7Pgpvc/KrLqvmcnj/96TYtoedp/iw4asfy\c2vs+GVyxVoumIdFPHJpencWbE/niZnVDaJCih1ioggXzDsI8bENh2B9cutDWX+bsHZSC\jSQb9YKGN+MoNiJ1xmQHSJDyfPhzWPibdS/lpS90ppPWIY+PpL0fzDSGFFWswQ4q5Phc\pLWhx5lw9Ksye+T86p6kadnBBTLTyfn0dg7Np09QKQ0bMN60MnybkVGx5nH9yLJ1F1mV\

0H+K0VZIKm4UzYV+RYfqqXYtMqTQxeQ1U7L7o0H+6viEr xuKj5rS3i+r1rdfECAGgCoq\0mixATHISAHi2eSV5fk3r5xMkKSwwPIRuMt50+kk1RPuO LohTj7G1CnL602xwBdQMTUx\4Jq5JBWnfB+U4D9n0si1Dw iKihpaUy0oBeawo4iFQiWVlwjeeQvY6zj66170XsPHjZxg\uCitsWfp5MYV3cLTkb80uCM/xhp4Y0Edobt6x3k1FD8vbh8g3YAG0Xe/U+Iz3k1npCt2\R0Q21GQa0JM14nbQr3tqTLoXv4szaEr fP/Xw05Cnt9DsBzN5DNrmff6EDcfVf/hn8v9a\wrg6Rfv8Jpys1YFpwLanhb3Wz+x1yaDsa54Id1F0FnyBxv8GppbFrMpVFx/nLAXGIocc\WjcRKs0tBJUW/IoXeKOMPUD1wHR4dqUCEXsoexHJiNe5sH+akr6UID0bF70hhupBoiY9\AzVXi5zXF2VdafyQrkGfKz4BEUkiqcajHr1CF9ZJ+Mjdmfr3z0xyCmCAwir5ZLOBXDj\T7sYCV3QjCz4a2mGvee9Ix9kSLapCq90UMAxnTLjJGQM/dlpgjDsj sCZX5wKdsnMs79\60Z75BGDOC1dDINj4f5kHZmw wcmw/04mi/1RPBUABXse3Up3eJQ0X2haZPqmY0+2PZTF\exku9pETHTKcfSdRe1oJLmlB34JSogRmNp1eBxakcIL09huiFVtGVZng/pC/ryoJ/T9q\9w4aV5H+4u2dHc29Vb77SasxCdRH0sDaLaPpesRXsrdJwjbiz0gzR1Ix+83o07NuhE+C\kF07czMrFm8r8g1M1zDiFrTf3RTusMtiW6CV1VuTROPZFngqaR5yeYPprpSELtQHSwz\U5AaY5Qd8tbky5ec+2/QkX0+cdyWhQuuBRpibwpRpD3x1yTgT4E91cwTFpvSLk54ZHf+\D3EsZf0PYMN6d4jVdh9iv+0tCebnfMqp65wY26YBopSLtCXXb1anU1RP1zPzRq99yKnt\FM7gK1XnBAZoZBBqCyZw90HWmttIFWcm14Wd5BxF9uZh2Y8gtcN8UKWHv43tsNBa7j/T\ikIBSkIVI/6EqvyPW4YTdyz2V8RKHN5XcdpdwFaVhgSJMC4I6Bm0Lwenhkma17Sd247q\uCtEow8qh+w7Jk4SxrmvJxd5sBnvz150KEaHPeWNNJw00bwEDT+0ZzzD8vMN1/GkbbB3\s7UfcJXZbRu7HtQ+wHIblBKvstX3hMonra+k6wS9KPhcAaC3IjZ7ZApSedKk1sW1SuDg\148YW2/cyS3LvmISQn9KPWK7yEpNQnV0vurn3ZFOGO0eDjsXuji+xIrRia5GQ1yb31ma\nJnf2PdHcMmVr0wu41MGno7a14nMRdnXkBu8bV0p8wF6Toz59hBJ3a/F+mP4/a19Ixra\wiVVeEPgoi9QQ9NcLgQEFCoskA+EpcLK0FxV2rYI9JFNF/nDxP5nmGtnkmlFaLo+pleH\CJYS00TGKQr6X+Y65N011x5nNwsnWkIUkCodoSt4Givdoe/S9JNiu8tW+jTBae2hNr9c\g1ErCNKDYe1+T+Ldyr9rf0Km9LKNyTBsodgF4KI/hFh9IV/i55DTwtqjpN0eQnPTB3/6\+7KzTfSE9i15UMcP3zKKC2mAQvtyYxF3k0m24ZTwPs2LAPJkr/xtPH3BnGE/UfUDmvDS\TBp9m049Nh9oDZvI4HKsY8auiyENk0ys67F9GTHh0YM0FgHyP5qk4/IR5YC31nq7xx6i\owebEJAy63htMytq+xd3cJyZR01wBU0qvSpd/A=="}

}

3.4.3. CRYDI Signature Representation

For the purpose of using the CRYSTALS-Dilithium Signature Algorithm (CRYDI) for signing data using "JSON Web Signature (JWS)" [[RFC7515](#)], algorithm "CRYDI" is defined here, to be applied as the value of the "alg" parameter.

The following key subtypes are defined here for use with CRYDI:

"paramter"	CRYDI Paramter Set
5	CRYDI5
3	CRYDI3
2	CRYDI2

Table 5

The key type used with these keys is "LWE" and the algorithm used for signing is "CRYDI". These subtypes MUST NOT be used for key agreement.

The CRYDI variant used is determined by the subtype of the key (CRYDI3 for "pset 3" and CRYDI2 for "pset 2").

Implementations need to check that the key type is "LWE" for JOSE and that the pset of the key is a valid subtype when creating a signature.

The CRYDI digital signature is generated as follows:

1. Generate a digital signature of the JWS Signing Input using CRYDI with the desired private key, as described in [Section 3.2](#). The signature bit string is the concatenation of a bit packed representation of z and encodings of h and c in this order.
2. The resulting octet sequence is the JWS Signature.

When using a JWK for this algorithm, the following checks are made:

*The "kty" field MUST be present, and it MUST be "LWE" for JOSE.

*The "alg" field MUST be present, and it MUST represent the algorithm and parameter set.

*If the "key_ops" field is present, it MUST include "sign" when creating an CRYDI signature.

*If the "key_ops" field is present, it MUST include "verify" when verifying an CRYDI signature.

*If the JWK "use" field is present, its value MUST be "sig".

Example signature using only required fields, represented in compact form:

```
eyJhbGciOiJQUzM4NCIsImtpZCI6ImJpbGJvLmJhZ2dpbnNAaG9iYml0b24uZX  
hhbXBsZSJ9
```

```
SXTigJlzIGEgZGFuZ2Vyb3VzIGJ1c2luZXNzLCBGcm9kbywgZ29pbmcgb3V0IH  
1vdXIgZG9vcI4gWW91IHN0ZXAgb250byB0aGUgcm9hZCwgYW5kIGlmIH1vdSBk  
b24ndCBrZWVwIH1vdXIgZmVldCwgdGhlcmXigJlzIG5vIGtub3dpbmcd2h1cm  
UgeW91IG1pZ2h0IGJ1IHN3ZXB0IG9mZiB0by4
```

```
cu22eBqkYDKgIlTpzDXGvaFfz6WGoz7fUDcfT0kk0y42miAh2qyBzk1xEsnk2I  
pN6-tPid6Vrk1HkqsGqDqHCdP608TTB5dDDIt1lVo6_10LPpcbUrhiUSMxbbXU  
vdvWXzg-UD8biiReQFlfz28zGWVsdiNAUf8ZnyPEgVFn442ZdNqiVJRmBqrYRX  
e8P_ijQ7p8Vdz0TTrxUeT3lm8d9shnr2lfJT8ImUjvAA2Xez2Mlp8cBE5awDzT  
0qI0n6uiP1aCN_2_jLAeQTlqRHtfa64QQSUmFAAjVKPbByi7xho0uT0cbH510a  
6GYmJUAfmWjwZ6oD4ifKo8DYM-X72Eaw
```

The same example decoded for readability:

===== NOTE: '\\\' line wrapping per RFC 8792 =====

```
{  
  "header": { "alg": "CRYDI3", "kid": "did:example:123#key-0" },  
  "payload": "It's a dangerous business, Frodo, going out your door.\\"  
\\ You step onto the road, and if you don't keep your feet, there's\\  
\\ no knowing where you might be swept off to.",  
  "signature": "2As8T1AHenWzLuTojcAYFDnT05n4bmDGIWenHqoXVizL7311HtVg\\  
\\7PEJHYmpc1fIvFNrm0xJt0asD5bQk3ZY8WuEQDUjsn4j+zbyob8MPQI5u3p5ZkqlLhg\\  
\\6Q8p1q0Hd5voY4a78vNxFJpYsETc0bECAft196z5hml2VjuDBqI7W4ju/iDKambJIDz\\  
\\NLyGyInNyPcHj1fBP7aCf0qGBA0QrWuVgrAkdeM+uH6djaXW25+FeU14Lg1u0IBPrcj\\  
\\ZJ04M07j7BmiuHJD74QG/ifVqnvr4z2a1MwHjjR7nPPr2CIKpuRthSpNwYVTRSN3mM\\  
\\v0GjVLyaqhJpmUmewhjaQCi3iP7c59yKatGYjLPPEapsbN7ypIo1Bod/R2PZR0zeool\\  
\\d9k30VmGsVLkJ40EIFn1A8epv+bJISApZWrGuU6NPB8vr4UB2D9DRd8zwvd/vI0Bwdq\\  
\\nfg1X4x181We8Tnd+21UC9n4zUb+KQlo9RR14fxE0t9g5a0IzCwjAN+Oz8vqJ/ZwgH\\  
\\zZotZNF+nZehFPcPLM3dpouKEI391VH3QQ6VTYfbMW9wGJ6UnylxZFEzNCnMFF9Qhs\\  
\\7Xehy4yEDgJBFYIvbTRCFd+EbzBwQAnLKsm7UXXBR7HdusJMHtkwdffGziWJBTf1UsG\\  
\\tqaCF1bvXgbcCSe0XGhc0QkQKwwj3kNwY9/hnhH1bn7kyySqaI+W4Ph3pKwRb38sCS/\\  
\\Gb3ryptI8zez0JR+1ClWnu18noJjGincZq7jCGMiMCRFpzUV6rpY/FiM26IpZ8M9ShF\\  
\\BHsTN7KGpyIqG6Yc3GzOJ/4ir7V3I3wYguK7iBUiuTM+OKwxtM75carZJPX/21kn2Hh\\  
\\TC+JVb2/yaHS2oDr1CwQosNhA/cB/cm+YmYgHc3KQwrZ/3Axr6weUSrWJ8qv+vJ5QKK\\  
\\a1+CLrkVGJX6vh+ps1NB5EV9yyMhBXAbBjZ3K+dGed3G7Vj/qF2kbnIUlSiEp1f6Lsh\\  
\\XASuVLTU6qG0rTaCMYKwaAc5R0wAgyZmPXu0UwyCtNFb0+S73uX5/N2drrUPdXiURw+\\  
\\luFKCtaNimU8myoz6YkoY234kz8pedST8eqBZAioe8HeYEktZSAyYov4YfLgkqHqJG6\\  
\\ycD2uA33kwnMim+jg/hIrWAIYYP9R90KECTvFR877RtfFgfn3+tZjWlmsxHZ5pNsTIA\\  
\\dNR+VmNpoUzkQ0dgHuFLztyAnCaumL38LHYHFhj2boa0zYsMGw8WtpEQ3+BNgoanNax\\  
\\dJ5THRRmhvMS3EdwanERimsZ6ZjdK8uchuVhytNiiKvBwEFWYIyoK9uUMBoEfDje4DX\\  
\\wIAefXYCqPK8eXhL+9qDLxAD1DQbCu+Ey3whX/r4r2Q61+34HpRrn3g5ok+Gt0/3ni9\\  
\\dYiIYpcXYfhMGDoXJLZ3IMkK7L6e5u4/Wye7lot2B5ekSGRrkLkjv+bTIkppxbTU4Pi\\  
\\n40qbD91sRzw2/GzZmJsfcaKbj5dhoNWyh5cZr1PqsxMI5EdXSxJ69Vwf8e+h4iPoB\\  
\\YS1JnUjhicVws1pA1rdAvTkAsVY8rC22e09Hxzkb/E7bt3iLDpekbbQaghZ31AwDv5\\  
\\KEG72bBbXIYHzPvhJzrls2LR0XKTJvd8tAx0SdxQD0t8tE2eKpmWZ38MJfRIxt2Rzo1\\  
\\p+bpKrR++pMLRrpViekVpZ1/t1EojImN05rLqxZhLxvZ0yDfcT37jc1oqire527/Y9L\\  
\\3k894eHNYCxxjb0LGGPDeLutSEX+afHZLNbd93Qa5VTmLwsPxEW/Erua6nXUrAR/87P\\  
\\0gIyce3h3s15jzCXsQm/i0Dgyn7PTe05ksQCFRPiyXq5xgiXGKGGkqTGg280hdby+1N\\  
\\DPnNHU2J0F6GLTqwK3qGbBLzDGIMR2sePGpxZ/pecoX7yn5bT0f4iY10CyLo5nEgSeb\\  
\\JdBjh0ZU+QodLRN0cnenLmP1oNK2yCuT9uIA1Wh9C1CLhBiE0foIs9/r1W1XHPiPsX7\\  
\\c21w+B1IPfzUX1cVdndnNo4Xdh19CH1tYJDLr8LfeuYnz+bnaFlqEUryTc8zU14A+qB\\  
\\SIDDDjefCbmDsTrdqzGT2J89MKVi0ogy3qJzyt3jo04xq+Q30Gjb0FJikyJEqUm8BmX\\  
\\d3ctGfzsEr+5w7fDRco40/tDQUSH0q0W0sPkhuellqKDziJXwhPQI42miVN2A4+0AS4\\  
\\f2uTgpDNn1gIfH2+d0CkBj1hZeA1Tgrp8FHQxca05kut6cTLrL7CSBqINa7Khe1zyxa\\  
\\PZG/tXUk+iv0BYT92b7CRNmg1qhE0G8V3q3QrB6EePYa1WxRQ7ij4rRcQwcj66A1hZ5\\  
\\KjDUVJh+02cZTFrv97wM/im3vb3dbiSxAiQExSa2KATfLI2oS+y7R1RNJ+9nF/vTaFc\\  
\\0HOdKfmUJAukAcyk/h0Quvdaf9jxEcstj95mva+HkIqPuFifidlvgiafKr4fHzryp1h\\  
\\g7QUtDRU2a4BRfzclz6PK0BFV3xVI7qoQbKEqQyldv8mZRd0LBRKprxHW7PdUquth2V\\  
\\GEmZ4UuCYXT11UweBx2W91HrQX+xaKAjTu6oLYIOvmFVCUr4mCrYRcLZnzw0RcsqIl4\\  
\\G88x8r5aeill4lsQZ03kNotR4n0qzFVRU2+EX07QJFm+NKxB7aRZ5oH+dSy+Ye6aMeg\\  
\\Epv491LU0LVnZNMBP2eUhoEo0gimmZGtUobjRdLuYyNiJfJzVkjwF3gYQtY59zb+46N\\  
\\SzvWUqpFUG80Vswns8GNAQ5hfLoH80GGohT+UvoqvptEXhiAAFstT/EQrHLZrYpXHJI\\
```

\YaICW+6uo9ixL0oWkfI0H1YaXyNkaFKHQ5ZbPaP45dbWq/dqXdrRe2YU8AqdjCxyyzo\
\lyZR6zH9wHj0k1AI0HvnKZ/B2v4bS8YAtNZ1zgKb0vM4qqSIFETfr8N4yItuemHEznP\
\prD7Gr6W2VCS/0FXnQt5y0QC8z4ffrnnngwPjcZfsCRSkntQB1q6Cx8KU0ipf+Rh0vs\
\HnNN3qJZmxz6YCvo2M7fxJtyRvm34UEVaj8QKXrmzX70Y9rDl6wEhhvSThaeq4dcfAC\
\vczGXWgCLB10gl+Iz6hVDTgCx7bC2BQ2oHtzSDc+v/UuJewvVaIL9tn4CtMzu86f3zc\
\fTN2zke5alNpoJP9A+mkbcfy0aD6yFcн3nw2ueFDsssRg1ZcS5CuјNeylAwxRYaNSmu\
\zDzMygHu0CTxfGEG2c63J32HKG4Ds58SK7HSD58jgScBv+QjBUAGSJozFG9y7yIF5R\
\kd74aSJMYmuzow2UnGayR9yM50NbW1brD4wNyJHqDIroCUvrL8zu24ErFWDKy6VaZ0m\
\ggPvX38Ix0IPnE+Pm0tRGr+ua9r9z047TtEoAdjIEtwQuNem0S1fqeVx2Fd1TmKc5+v\
\cxMsnuEKQiewTbviLdIWHTz4snU/dt77cxQEfwks3pu31kCLyLbpickMrn1nELafNBg\
\RbwEqGTT0i24Kz/kvC5RYr2USuHKksZxPfgx7Y00pY3IbemF011EmnG9odSwnVcww+\
\9/IlevZHuw1qqTxZu1re/AMfqhKgaD8XiwuKxPZQqo7Z6jj3y0ugAVWY0w/88bAX02k\
\deVc0mG53sKH9ChLg35LdPrpLgHeFjIHJ27L9ucqUw70Pu58vRJUnYDey997y57k1vh\
\9RwPkNvIs269v6s/xfg9VM9N4aY4X25EWCxchMWlH9LMamYF6JTP0v7v00cdHycmX5D\
\EnwqspYYNomVpJ100xgMA09oy1E4dhg3IJo+fJgL9rg0xJ4INTJ0g/9tUz21LPI3c1c\
\D5pPs/y0zy0cF9f6ahaYxMDk/nfout2FGmoesMCaTN11JngYYC5H95cDeMwErm6ppSU\
\woCqut45noJq0VS4V3PKfASIfuUwP3vgFKo+82Wy3dqEr+sBAsve44CKQ8Tq1GLYjet\
\L3xugCk10uaGh6TFqj2X/vJ1X0W00uyvzt62fxeQ4es0rs4LdRxkjbKT2I2p6rQA1Bi\
\GaZLvOuccQh7NST7BEJBy8QUrPV10vPmCNGQrKS6a1C/JNFLaxmsP4CPQqwrQ3fg2ia\
\qQRol0htD+UFjWUBXrQdrs48b9TdLHmbPHPbG6+Zeuci87kJ/zJyjHA0SYUP6awkfga\
\ckilUppo0oNIC9/qsVr21FIWI09+UwnIFR9nNFPzgbqw/cMOC/uWA00sGS8ADQ/rePO\
\fTxX0mfkvI2YeTdiIayy+uwUxoLdz90DGhUysP+JGU9kZTqYNJYsjC40gLXS+qKCYai\
\oW/leFs1fdP6SH+E24p00JARU/f/ZajcMMXAwQdIVe0o7jvDhMydne90/18fcwpNVN0\
\tswhRsnW4uMCSAAAAAAAAAAAAAAAAAAAAAAIEBMZHyE=""
}

3.5. Using CRYDI with COSE

The approach taken here matches the work done to support secp256k1 in JOSE and COSE in [[RFC8812](#)].

The following tables map terms between JOSE and COSE for signatures.

Name	Value	Description	Recommended
CRYDI5	TBD	CRYSTALS-Dilithium with parameter set 5	No
CRYDI3	TBD	CRYSTALS-Dilithium with parameter set 3	No
CRYDI2	TBD	CRYSTALS-Dilithium with parameter set 2	No

Table 6

The following tables map terms between JOSE and COSE for key types.

Name	Value	Description	Recommended
LWE	TBD	kty for Learning with Errors based Signatures	No

Table 7

4. Security Considerations

The following considerations SHOULD apply to all parameter sets described in this specification, unless otherwise noted.

Care should be taken to ensure "kty" and intended use match, the algorithms described in this document share many properties with other cryptographic approaches from related families that are used for purposes other than digital signatures.

4.1. Validating public keys

All algorithms in that operate on public keys require first validating those keys. For the sign, verify and proof schemes, the use of KeyValidate is REQUIRED.

4.2. Side channel attacks

Implementations of the signing algorithm SHOULD protect the secret key from side-channel attacks. Multiple best practices exist to protect against side-channel attacks. Any implementation of the CRYSTALS-Dilithium signing algorithms SHOULD utilize the following best practices at a minimum:

*Constant timing - the implementation should ensure that constant time is utilized in operations

*Sequence and memory access persistence - the implementation SHOULD execute the exact same sequence of instructions (at a machine level) with the exact same memory access independent of which polynomial is being operated on.

- *Uniform sampling - uniform sampling is the default in CRYSTALS-Dilithium to prevent information leakage, however care should be given in implementations to preserve the property of uniform sampling in implementation.
- *Secrecy of S1 - utmost care must be given to protection of S1 and to prevent information or power leakage. As is the case with most proposed lattice based approaches to date, forgery and other attacks may succeed, for example, with Dilithium through [leakage of S1](#) through side channel mechanisms.

4.3. Randomness considerations

It is recommended that the all nonces are from a trusted source of randomness.

5. IANA Considerations

The following has NOT YET been added to the "JSON Web Key Types" registry:

- *Name: "LWE"
- *Description: LWE family post-quantum signature algorithm key pairs
- *JOSE Implementation Requirements: Optional
- *Change Controller: IESG
- *Specification Document(s): Section 3.1 of this document (TBD)

The following has NOT YET been added to the "JSON Web Key Parameters" registry:

- *Parameter Name: "pset"
- *Parameter Description: The parameter set of the crypto system
- *Parameter Information Class: Public
- *Used with "kty" Value(s): "LWE"
- *Change Controller: IESG
- *Specification Document(s): Section 2 of this document (TBD)

The following has NOT YET been added to the "JSON Web Key Parameters" registry:

- *Parameter Name: "d"
- *Parameter Description: The private key
- *Parameter Information Class: Private
- *Used with "kty" Value(s): "LWE"
- *Change Controller: IESG
- *Specification Document(s): Section 2 of RFC 8037

The following has NOT YET been added to the "JSON Web Key Parameters" registry:

```
*Parameter Name: "x"  
*Parameter Description: The public key  
*Parameter Information Class: Public  
*Used with "kty" Value(s): "LWE"  
*Change Controller: IESG  
*Specification Document(s): Section 2 of RFC 8037
```

The following has NOT YET been added to the "JSON Web Signature and Encryption Algorithms" registry:

```
*Algorithm Name: "CRYDI2"  
*Algorithm Description: CRYDI2 signature algorithms  
*Algorithm Usage Location(s): "alg"  
*JOSE Implementation Requirements: Optional  
*Change Controller: IESG  
*Specification Document(s): Section 3.1 of this document (TBD)  
*Algorithm Analysis Documents(s): (TBD)
```

The following has NOT YET been added to the "JSON Web Signature and Encryption Algorithms" registry:

```
*Algorithm Name: "CRYDI3"  
*Algorithm Description: CRYDI3 signature algorithms  
*Algorithm Usage Location(s): "alg"  
*JOSE Implementation Requirements: Optional  
*Change Controller: IESG  
*Specification Document(s): Section 3.1 of this document (TBD)  
*Algorithm Analysis Documents(s): (TBD)
```

The following has NOT YET been added to the "JSON Web Signature and Encryption Algorithms" registry:

```
*Algorithm Name: "CRYDI5"  
*Algorithm Description: CRYDI5 signature algorithms  
*Algorithm Usage Location(s): "alg"  
*JOSE Implementation Requirements: Optional  
*Change Controller: IESG  
*Specification Document(s): Section 3.1 of this document (TBD)  
*Algorithm Analysis Documents(s): (TBD)
```

6. Appendix

- * JSON Web Signature (JWS) - [RFC7515](#)
- * JSON Web Encryption (JWE) - [RFC7516](#)
- * JSON Web Key (JWK) - [RFC7517](#)
- * JSON Web Algorithms (JWA) - [RFC7518](#)
- * JSON Web Token (JWT) - [RFC7519](#)

* JSON Web Key Thumbprint - [RFC7638](#)
* JWS Unencoded Payload Option - [RFC7797](#)
* CFRG Elliptic Curve ECDH and Signatures - [RFC8037](#)
* CRYSTALS-Dilithium - [Dilithium](#)

6.1. Test Vectors

6.1.1. LWE CRYDIS

6.1.1.1. publicKeyJwk

{"kty":"LWE","alg":"CRYDI5","x":"lgNFI62eq4YKxuvpMl2V9SVtGV5z_vQQZe\iCziAVcFMuUUzjpbwrd7uKHrBtxNPWsLI1fYKmM5SM-0LeoDII-GNQYJfm3QRt9133P\A0yJpbeLidJg6e4UAIZJQx-KbKrIVqk6F42P8WmhDWxgc5xJZXUabUtMHV-irm9pMP8\kjrlRFuIenHS_YYj3RrX9yeAZKmD6YJsROVMEprjR1B7u0QxJYX1WNNRD5AEiGL8TKF\oxb0g-qDIP-M6ubjuKZqlhd3_-z1bLJDVKN_uh9hsI1qpghW7niD1dxKBAU1dyELqn\WzvadJyhKTt3KevLOWGuPJGc927VgDnTVSvai0W0bZu3wHEup5PxsqymxGEuJGkiY6Q\zl15KWzr4jdhq-_HpknGUjg2LbC0Q-f5raUm27vkT8E17A3i-ar5Jhd91hfXpGJ4Ui6\amgeTedhqJCK0zTrEF12ecwQ9ERhjdsksC8XMDe21QS1W-AyHfntg2oPeC702q0E46J\MG_OUcLtMo3ShprY1VF930bswsozfX6mmwqinQvYSpDAC7HHd39mp6CwJu10auoPi7H\DEAb0aS0-qUgdh8WOPgyCEe0GJ_Hpl7sokVq5dXtbV4458_zDtc-pUcX7C8J30UgLfn\KsZze0xQhgqkk0nG56CTleN_9u4rfwQzQZBH5ofr_biWhgr05HZ-UdjL4ezxPUIGW7M_HwktpowTnXfV4-6HTF16jqmH-Am05XJ1wjP44IbRMNK5m-vH0BJj6ELGiDuNQoia\hKHS_-L0A0-7d2IxcpVuNWZfz1SvHzC4XPht21p01_Rp9vu7obwG1FRrnLx1IrWcK6n\R3ux8oDJTM3H8J4cdRgZKaPM9_1BMhamWnpCXFThwRWshaTapgnLEfExpMjikdho-SP\8DH6yddFrV-S1_1Z8re1vD5CUXh50Ec0epvnDYK5deW-Jqh6e_wGG1rwD7d9XZK9hKQ\oX1cYPsfkdgRIBywrD1bMIs7pyu5PVNSR39HD5woExp1y5bKgCaJDF-tBS11tGQV11U\pzENPHMi6fTCsv00tEuvPZJkDvE-osJ_3Aj9eTdK1lJDD1YzSKu2Uodc96vaH3bXJW\05iBprV6h-nG6MuQuXirUNiG9h8nQ7MmaJ_Jdr58_cBChxYZRu1zaJcSwpTecAtktv3\R-Yp2Lc7LxebwbEa19598X7CQtyS4RoUKorLOX4FkuXp1JZduQbM2QftVqA6ufBkFH2\3Axy_fZooaz0oBM8YYBAIqJAs2Ya1iLfrdqo42rDL0K_VxmVGqctqKhM0etvM2nf8\vbdsosmionB4d2Ur3no0AvZzbHcmIdHFg-EgJzfoIAhgKdH1zsN_AwEC9CFAp0dPwdi\MUsoPhkWNAsf9hmnEX-Izx057IyxE_ilki9smuR6f2Nku23279NaZHBmIpmpU1tryg\SZ0i8yssFqKCDpRZwVV83F1Wcg3pnGsh9HXHC7rqI3-TB0_KxbTEmgKVspoido3T12Z\9Dx-9Jawe6rd7g1lheM0z1BWEfHFwwDTr5TxhE0o59zATIAJu4DxWkkFFQj4iXMYP-R\ha8QxNe82yUXoJGJ04F-C7N1xXJ64d0PoW0JNeDyM71iqtAQQgR6TNzVJv0b97E4W1\AAC2gYfXGS8k0awcTyewdytjXs8fqw0PJ3or2HZK1jnXZloGeSJILxHOQt12PDM2k-w\0KZ1CPzbzjqQwQdg9CZ1F02b1Kus142T20jUy1xsDGg4vaF-_IYuc07js31adyf90GZ\sMeoLqrwE1txMYJSk9SWSkjpL0csNDHH_sh591101ogQk6QoUIf_1Ma-hg7EWKJAkP2\w2NsxPqr8vIAcdyC0_t5b6XpYcp7gkZiVxFn8tSrlofZbyW-zT1gp1gVEMhrWK5tIBZ\gE2ftMnG-AGekLYFD3aMzF3YZIDa3-Fs-_YBojx4pt0LCa8mXMUTj9s0KTXyB3BhYA\V7n8MDBRYITV17KMkLrY9vU1uhkxzSrNnBtSewEXf8Q4sGv2wEJjRJZyNPQzGtXRHnr\FKwCG3TVk1Cwc1d5C2Ttwh5HbtMtCBxTkAchRgRZshMwyVjnUiPn4rcGA-5XP6n8EZM\x0Po9vYkFuvb83GSB1g56jNCKGNStA-ZP33KKw_U8zdGz1fKX5xGvWrTU1MkhTST-aX\DHqpKjFTPU2M3wfraj371fYK42rUYR-viKHyRXVH221DI6Ke-s1rKQxzSSHjSUB13ID\ehTfB-pk1L_JqIabpAk_hLkSthbvsim1M8PUkiw30zzKQqScYiMxl_Ns3yvoahiWDh0\x038smAiws9FjgI71mRywBGGj4z21HTwfMAwWbzbl0MqZ4AW4zN6e-pMSfnPl-jF9\2C-FcXG58UQuBociY7Jwpg1XvWrVsTo3I8Qedzp1RYVV8qu3TQCCiCLom-U0wehbPdE\hp3ugI2nYjVggbk2QwseoRISKEylu1J_vveItZCkinsK5Cy5g90D59Ym4WzpdXjtRIP\k1ilfyLYcFwgdnNVLSNk1hb1iHgde9rghyzaUkEDdQwjfjXu8BsjsKABdVyJwqF2r3g\5U1K300F8Et7n36y3RBxIx1fqpCD-G-tePQ0zkbYwRouMC5P7Ws_Qj1WPAq9vIVF\WYDmRcXN4PKLb94q0Qu8Ev2MffffDKDTvuPWU33Uv0d3KbzKd3Jyfpq62WbeXEr_JgJ6\x442fEawx4gh9tq1XFQ4Wb9GzTuGz_hLkpCd0Qd7snxiHPSxYq0jd9g81YcsQK0hw_\dHcuSKyxxIAmI2MwLmGp6YnhY_JrfuUpZ1jfwcSCuqrzEvAS7CDvwzJ6-PAi2X043ou\SP1-CGg9JS5hIiiIR5hpW3-Fqq2t0eqv7fFn_fAGyEtpHWDXkLJDTDcIzL2eU2umYur\dbPyn09J99cEW3MU956D6LbmgRWK6lxQ5m539KMP7D4KQPPDt6CRA3YqAzzw-Vga8zd\2UxphCk0RsaAs8pBihHwwe4ZhQ15qolmFKtQT2chnqVkn6nmpQmH3Th13Xgf0R1Byq-\bTEcwboD_vYorb6HHyv9ciM0qh4g7tgmiphuR5b6LiVywqxrMAN13cU8TiNIveY9A\fbS6qJMshNi61lkux4wnM6fpENDxCvRVCCyLB4NhS57fYddsTPiGZ6w1PeS_2Be8J9h\IN1g_yLmN8C1-9dgSx3yYYJZ4MGBNzxtbQIYcdH0_1mraXouf7hkhHAVbDPEcpCfUxt\

\mAI8h1Yy-Pq1fjQTHoaEm9XaVe0SQfN6EsrbcXF2zjrG2uJuglRRM-IoWhleeMc1lv8\
\wCi33fB2KJhNo-iTK1hFYQms06qJyxusPu5Bmc11EzONbBuH0eIHxzWBFoZ5o4ziz3A\
\C1sD7eTc5-bF9enC-6J70zRTx6mft5GwF8-FkQFJdqulPfgnr-_TYQZScKHW0Iki8kp\
\TUTr"}

6.1.1.2. `privateKeyJwk`

{"kty":"LWE","alg":"CRYDI5","x":"lgNFI62eq4YKxuvpMl2V9SVtGV5z_vQQZe\iCziAVcFMuUUzjpbwrd7uKHrBtxNPWsLI1fYKmM5SM-0LeoDII-GNQYJfm3QRt9133P\A0yJpbeLidJg6e4UAIZJQx-KbKrIVqk6F42P8WmhDWxgc5xJZXUabUtMHV-irm9pMP8\kjrlRFuIenHS_YYj3RrX9yeAZKmD6YJsROVMEprjR1B7u0QxJYX1WNNRD5AEiGL8TKF\oxb0g-qDIP-M6ubjuKZqlhd3_-z1bLJDVKN_uh9hsI1qpghW7niD1dxKBAU1dyELqn\WzvadJyhKTt3KevLOWGuPJGc927VgDnTVSvai0W0bZu3wHEup5PxqsymxGEuJGkiY6Q\zl15KWzr4jdhq-_HpknGUjg2LbC0Q-f5raUm27vkT8E17A3i-ar5Jhd91hfXpGJ4Ui6\amgeTedhqJCK0zTrEF12ecwQ9ERhjdsksC8XMDe21QS1W-AyHfntg2oPeC702q0E46J\MG_OUcLtMo3ShprY1VF930bswsozfX6mmwqinQvYSpDAC7HHd39mp6CwJu10auoPi7H\DEAb0aS0-qUgdh8WOPgyCEe0GJ_Hpl7sokVq5dXtbV4458_zDtc-pUcX7C8J30UgLfn\KsZze0xQhgqkk0nG56CTleN_9u4rfwQzQZBH5ofr_biWhgr05HZ-UdjL4ezxPUIGW7M_HwktpowTnXfV4-6HTF16jqmH-Am05XJ1wjP44IbRMNK5m-vH0BJj6ELGiDuNQoia\hKHS_-L0A0-7d2IxcpVuNWZfz1SvHzC4XPht21p01_Rp9vu7obwG1FRrnLx1IrWcK6n\R3ux8oDJTM3H8J4cdRgZKaPM9_1BMhamWnpCXFThwRWshaTapgnLEfExpMjikdho-SP\8DH6yddFrV-S1_1Z8re1vD5CUXh50Ec0epvnDYK5deW-Jqh6e_wGG1rwD7d9XZK9hKQ\o1cYPsfkdgRIBywrD1bMIs7pyu5PVNSR39HD5woExp1y5bKgCaJDF-tBS11tGQV11U\pzENPHMi6fTCsv00tEuvPZJkDvE-osJ_3Aj9eTdK1lJDD1YzSKu2Uodc96vaH3bXJW\05iBprV6h-nG6MuQuXirUNiG9h8nQ7MmaJ_Jdr58_cBChxYZRu1zaJcSwpTecAtktv3\R-Yp2Lc7LxebwbEa19598X7CQtyS4RoUKorLOX4FkuXp1JZduQbM2QftVqA6ufBkFH2\3Axy_fZooaz0oBM8YYBAIqJAs2Ya1iLfrdqo42rDL0K_VxmVGqctqKhM0etvM2nf8\vbdsosmionB4d2Ur3no0AvZzbHcmIdHFg-EgJzfoIAhgKdH1zsN_AwEC9CFAp0dPwdi\MUsoPhkWNAsf9hmnEX-Izx057IyxE_ilki9smuR6f2Nku23279NaZHBmIpmpU1tryg\SZ0i8yssFqKCDpRZwVV83F1Wcg3pnGsh9HXHC7rqI3-TB0_KxbTEmgKVspoido3T12Z\9Dx-9Jawe6rd7g1lheM0z1BWEfHFwwDTr5TxhE0o59zATIAJu4DxWkkFFQj4iXMYP-R\ha8QxNe82yUXoJGJ04F-C7N1xXJ64d0PoW0JNeDyM71iqtAQQgR6TNzVJv0b97E4W1\AAC2gYfXGS8k0awcTyewdytjXs8fqw0PJ3or2HZK1jnXZloGeSJILxHOQt12PDM2k-w\0KZ1CPzbzjqQwQdg9CZ1F02b1Kus142T20jUy1xsDGg4vaF-_IYuc07js31adyf90GZ\sMeoLqrwE1txMYJSk9SWSkjpL0csNDHH_sh591101ogQk6QoUIf_1Ma-hg7EWKJAkP2\w2Nsxpqr8vIAcdyC0_t5b6XpYcp7gkZiVxFn8tSrlofZbyW-zT1gp1gVEMhrWK5tIBZ\gE2ftMnG-AGekLYFD3aMzF3YZIDa3-Fs-_YB0jx4pt0LCa8mXMUTj9s0KTXyB3BhYA\V7n8MDBRYITV17KMkLrY9vU1uhkxzSrNnBtSewEXf8Q4sGv2wEJjRJZyNPQzGtXRHnr\FKwCG3TVk1Cwc1d5C2Ttwh5HbtMtCBxTkAchRgRZshMwyVjnUiPn4rcGA-5XP6n8EZM\x0Po9vYkfuvb83GSB1g56jNCKGNStA-ZP33KKw_U8zdGz1fKX5xGvWrTU1MkhTST-aX\DHqpKjFTPU2M3wfraij371fYK42rUYR-viKHyRXVH221DI6Ke-s1rKQxzSSHjSUB13ID\ehTfb-pk1L_JqIabpAk_hLkSthbvsim1M8PUkiw30zzKQqScYiMxl_Ns3yvoahiWDh0\x038smAiws9FjgI71mRywBGGj4z21HTwfMAwWbzbl0MqZ4AW4zN6e-pMSfnPl-jF9\2C-FcXG58UQuBociY7Jwpg1XvWrVsTo3I8Qedzp1RYVV8qu3TQCCiCLom-U0wehbPdE\hp3ugI2nYjVggbk2QwseoRISKEylu1J_vveItZCkinsK5Cy5g90D59Ym4WzpdXjtRIP\k1i1fyLYcFwgdnNVLSNk1hb1iHgde9rghyzaUkEDdQwjfjXu8BsjsKABdVyJwqF2r3g\VV5U1K300F8Et7n36y3RBxIx1fqpCD-G-tePQ0zkbYwRouMC5P7Ws_Qj1WPAq9vIVF\WYDmRcXN4PKLb94q0Qu8Ev2MffffDKDTvuPWU33Uv0d3KbzKd3Jyfpq62WbeXEr_JgJ6\x0442fEawx4gh9tq1XFQ4Wb9GzTuGz_hLkpCd0Qd7snxiHPSxYq0jd9g81YcsQK0hw_\dHcuSKyxxIAmI2MwLmGp6YnhY_JrfuUpZ1jfwcSCuqrzEvAS7CDvwzJ6-PAi2X043ou\SP1-CGg9JS5hIiiIR5hpW3-Fqq2t0eqv7fFn_fAGyEtpHWDXkLJDTDcIzL2eU2umYur\dpyn09J99cEW3MU956D6LbmgRWK6lxQ5m539KMP7D4KQPPDt6CRA3YqAzzw-Vga8zd\2UxphCk0RsaAs8pBihHwwe4ZhQ15qolmFKtQT2chnqVkn6nmpQmH3Th13Xgf0R1Byq-\bTEcwboD_vYorb6HHyv9ciM0qh4g7tgmiphuR5b6LiVywqxrMAN13cU8TiNIveY9A\fbs6qJMshNi61lkux4wnM6fpENDxCvRVCCyLB4NhS57fYddsTPiGZ6w1PeS_2Be8J9h\IN1g_yLmN8C1-9dgSx3yYYJZ4MGBNzxtbQIYcdH0_1mraXouf7hkhHAVbDPEcpCfUxt\

\mAI8h1Yy-Pq1fjQTHoaEm9XaVe0SQfN6EsrbcXF2zjrG2uJuglRRM-IoWhleeMc1lv8\\wCi33fb2KJhNo-iTK1hFYQms06qJyxusPu5Bmc11EzONbBuH0eIHxzWBfOz5o4ziz3A\\C1sD7eTc5-bF9enC-6J70zRTx6mft5GwF8-FkQFJdqulPfgnr-_TYQZScKHW0Iki8kp\\TUTr", "d": "lgNFI62eq4YKxuvpM12V9SVtGV5z_vQQZeiiCziAVcFVyXwhRDnGPXKI\\-p70KAxRHm3Z7G8D21xfkTEWs04DNJgttnqBBjiKbqrqLXMEK5vvJe5W96PyYrlTbImN\\DBL6yQ0ZIYBYJm4YtmygJAakg2bQoyRAwIzMgIpBBkAgAFJMg1MgMUBgEYoqhGUOMma\\R1oDABmgCKGhmN3IgQI4KECMExwBBNwoR1khQpYbYwHKMFkaQtoaRgysBQm4YE1CYgQ\\7hBAcaEAgoGHLAskqRB00CQVKCMIKhx2wZkYAJKEQGNiihogoQoEQYKAYCISxJxWLhx\\GZU1kkRFISQwGiVNA4WBJDCM0cZFE6VBGSWAwjKFWsSNUaYIRBAMgFhWSAuYjaISMg\\MowIlw0B1oThlpLCRJDIqHAQAwzGzBMcRSRQNHCJywABJCCJsIbwNyIiIJEFiw0hwEj\\Nug4RgSgAB2iAsgpRtYgC01IAtHAIuUqIA3IIJ3MggyyBgGkWMm8QAhBaAgCJMScQkw\\QCFk5RNxJRFCqkgHDVmwhEBAFNnEQoo5YJyYBRg4QgCAiF4ZiNCRkgJIls24hB2UhP\\YsYBwkjtUrYx4TCG07Y1IDguXAZhAgwRY4QRgYBsoaiBA0JAKJCQ04Ask4IByyhiigK\\BE8GQnAIAjAIp2Sh1ERCCGEsUiJtkoiQErhpsYAxJAUEWggEbKNoiIkEyM1TCBI4j\\ZOXJAJ0cZsIkiADDIIGAJByBCFQwIuzLJQIKBIAyMAIUZZJLB1QAJhicJtVMRpSARpg\\LQAIrZI0iAiMygl5MRpUpSF2aAJokYAwgRQIJBtAyhRkhhQhZGEieKSIAsEbUwwjCE\\0iQgVBBCCZRJWJRwC0ZG0SZ12rBBGKgo5CJEArFwSzBAG0h1kJQMGgclwgQm2AIqETE\\kSYgtCLQpELFBGAIewBhEysRQ2UgCkwgJgbhg2IYtFCZqEBZxoBJ0pJIBjERpSahAwb\\iMTKKIyihqwJKFGhCMwkBSUTaRiLSnjAKJoihwGchAy7JgAoYtSShyg8YNIEKI2hYhI\\hdycUVJ3CCSVIJgSDINsKMkJCEoEYFACURwYBxQagJoIIIazFBRMZxmCguIjMxo6KJ\\U0AB07aN0qqQgzhtHKg1CwYKCCZsUAhh1DY0gUYMSzaB1ERBDEKpw7YtGgNOUqYFC6J\\h2ZQNCQaBWCIhozIKDDhpZChuRIKA5AaFIhiREUlQJMAN1AZR1KhQYUJyGiFgGUdqQw\\BS3Ijh1CiGyoIFI7MApJKFWkANCzYSygQ1kSgpnsKSBIkIqYiIFBLAKICGMwrQJYCAkI\\acEisACyoJkCBQKQkIg4xZMECbGkphTBtgtDQpcQwJigAwCAWGIpEBIhaEXDYIuR1\\gAKBIaeQEoUglMgMgCZCGpcwwpQp2YKMyqaRCKhQowQB0YBBhBghC71QRDYpFAghS8C\\IAyc1GDmSFCEQ2aaNgEBsygRBpBaFIRMs4xgMCUJgArVkJ3AJoEbKxCSBI4haCI5VJ1J\\RQYyAFgSYJAUDjjAAqSyZRCgIQYiZJywYkUIaEAzYJwahBSwZ0iTgk4YpEcmmCyFhE\\wIxEjFy4jYQwTJwkAQEUqJMxChuDIkhCibJiAhGmCB0gxQJTBJukzYkm4JomUZtHDeG\\CAhpS6QkABUswMIFS6QgShgpmKYpwASE2hYIiwBIAzVgkERNZAY1GA1Fg0BMQQRRWyi\\OkohJERITYjhEE0NwkREmJBFggWIk0BhRBBOSgBNYRZFkoITAJghARTIwVxmZaQch\\RpXBAMijJMYAhkTQwibIxwTRCA8dNIJjgW5KNDJYAEliMoSCIGqZBVKAgsURTxDgMx\\Dgk4IYgFCCewhaG45IwY5CNzKJQIAUKBEQeArmHCBJWDggm4YsyUAkUMQ1XKAtwiJS\\FKIMUjBpYgAJA8BFwzgIG0aRVBCIASBBYIhkFLMgGCMqI0WCEjgAAJbtCzhBCSUQiyR\\uUEItYkaK2agNAEqm4ESREhNmIreMAXYuETZpEyJBUAJuJBRu7kh_85-NnVU1ybdxVd\\53EqwXd5rJr3r9DUZ9en2KzzPDgzcTPEbfQk6JsroofVPkTLuv91Qj4vyeB31IohvBL\\bh8fqaYioveZBPNbp2I_J9RfRRCxdSXau28NFtYfc5aeDMhfOM_UKqIIu-hUZntGUNR\\NxS58X2hiJPFORu5EjJDMagA9tjYrRggbZuWkcpf67But2NMG68zIj27rB3tb3NwPzf\\zr1PJ0uVn0q17uZr5HozPSJMHqUjfJFxemLxLnPfYfIyxkMj1KT_WsvQiWacudZKFwK6\\Ijh18Pwp7wBXeF2zzDfZkpMtRKNeQxLGeJ5RCWqcW40FIOfzkV1p-fckThXER0UXJL\\j_50d5_KhaZP022eM3MM0AvDhg3ZcoKKGI0xtL9WGS3Cg5xMrtiJ0wN42YehXxGUN8\\NYZL3nuFSS0zs1Dq3SmQ6dM-SzsAB1oYw9g-DB07Y2xcPsNzH6Qvc0c6oa9t0JK9RYF\\BySCyH9ZSCwfij1FFD81Zgd8ociINCpu8BFV0Wpn0cYdRwmzX6czabmaVwCdGcBfCIB\\8kNw28PZhYmrzkgF3Ti8qDTCrZFMay1knaS0qRX3NDWIEs4fU_rYiMKsYi9dIEmXqPj\\zknXYi-Sj21mjxliPWZkt1Iqbh7d14i-1C4c9WA5HCXPSPNa8VRb-dmVjdZ9ZBv1YzU\\BiaRLfxwx6pbds1ldhxDgFFBc8J9eDsH_-9dQgDmgGrgrgQgNI9It1ZwpvrTLb-n3YZmo\\Zhcd0mWgTZnuMRSCmWPTj_2iHgtqX-EHj0h0jqXXfu7t54FMSgyKYMiu8q1_xm_Xztg\\CPjE8tkCq1bAXZ-Vw4MXTf0ks9tiiUMExVLzT7hEgTVreY0qB_oToZVd_BVJqvbcNDe\\GBp3Sd8q2VdWr_X3ISmr1Sbacl7loRwsVE1Eea6a_unR2Cpk9M_j9wMXAR_-0pnY0s0\\GJKv9_1mWEMc8393npbg5P7I7cTS6bJ0pcopRX2mlwof_QB65633bf51FBpmJ7qI-9e\\

\iEz0EJ4o46RNo990ZEEJ6z7HLCE_IJJwnnRQbaNUPymZhoJ7ALMTxU-TODBL1jots-_\\
\2ZJPbS_yI0nx7sD1Gk4IqF39TDWUhqEdDbXR3laEJHTfeCezn32UBDuz_Jp3y16nSrwl\\
\htiFk-gZPfHf-6cz8C1QCV7ezl_Hiwif1F2RSVT3ZNkkisfkvRnwJpK_RS5H8jvvMR3\\
\uVUE3MLVKznPg7Y5cbUERoCL_6DE6FHpZqPa6H0WKg7SE3bZpXbQiTnfo17kZqpYBCo\\
\KBjDkHhzQgMNNa-11Z2Pdzkumgz_vo1Z08WuK2pNg47c44Yenm2RBxvag1KsI8ZWSK_n\\
\Xia9yzygQHVh2h89MV2z1bynRinC5VysJ5KG1Zya_0jgL0mX0D1MG2m6mwmQ50zHeJe\\
\ymk87uzKJDfdACrUSRR1VyBF04Fxe2fd158q1ofIrI6S1juh0gb@wPryCy5Izh4aaP\\
\gSpGYG706Eddi_8pdmIluxr7eSkwIqsQCT0eLYtXDmOWMmh5W4QDBZHrV_iA7nNM1PW\\
\fynapnsoyiCewwqIeForRRbYEenMHUd5ksFYH1LtAbsqvB9oIm98crCkN3V0eWg8Tzti\\
\f11S8Jqd5G5QY8CdvxXzh5Ae0IUzieddqZd0trBhswRDpaM7n61vPt3wurgDgHktFJn1\\
\VVQtgIEqjMFP_1wfRdWaVSCgd5ekSvuPmYdjatIp3v0N5uyj_GqkCU0098X7NcyWfBA\\
\gGtbTmn5yl25HFqPsLyGND0suzXj0eNX9N4e01u7d-Z57-9ba04sEJ1sHQ3PGTwc6Sa\\
\Y1BR-EF79WZBES9VI0AE1kSkdMHIAVAQ9-JJxxJgNbdcWLbmrhd5-fwtEKRYRoA9L00\\
\pe6ry1kBv3u0MqAKn7uneUrvADZmHxrVgAP1TV401YBdq0iz5QfauvgCM-V4S16D3Rd\\
\Nr8KwbY0uqSVI2Jc12AAbcwBTMDq1AkpxIXU8xE_LYjjXXaBhKbtvtN3Qh712ge-d7RD\\
\DxePpqafroQoa4KO_-YyfNgnIEG01Vwp3sZPenUnq2tEpgDAUIXcy2zMH4G5CmU_0zb\\
\fh9iT97h5K3LLG7JnM_E-jneyE06KkyIH1vEUC5J4PC84ixuWqr7xNNfE2URYmh1E_s\\
\VX5UZobF2MYRsOfb6dtVfojyliw_IN2n3KmggyfVmVnQE11XPC7dyN9gXfheu3agxDnw\\
\UjqbRj79oQdxmXHOhzE2JzhcglyD9BSPyfRH8o1PnP86LRAVGaYUm8HILZ0ESEJ3PYq\\
\P8K-uVY2P4Po81bHgnFtH9U680jlqZ65rs1K5IKLctRZ7i58m055jXAaEMpf0g-91Zy\\
\imJKJ09DeZ6-sI66y2hw7ofAUk9ZboFxYntIQkulbIrncUILwvDxTCHCy4QPX1hMVgc\\
\6YF_vIrQFINILZ8tyYgqaoJ1Md9YQEnGM9fqIWkcZtj4X1zJ-wFRxg_VxoT3thIHduo\\
\kd0p5WGmuY5kmpa0CmYG6ZZLYJMGsYzf-80Zm3t_4_AHZwCPXfui8kCFOP_0EJSvlWo\\
\X_baoet6d4-u342BjgHnd9a2u0HqaZY_YHwdy3LxEvrusMxUqqUhjIPZfJJGhopUV0y\\
\KRxyP6nFMY8Z4rAs5fkrtURL2mj0fDJBAW0o6i1tBTyscVfSHBayMffby2g1DPzmH21\\
\ksAffowLRxo7pRm6TLXAjxTr4Rk-7CLQt8zURy8rdy815xvAEvtCweMeyWqjMDzJjI3\\
\fx3jMr6Sjw_yQ7J0Z1VPBLa5APNJkt8ilKST01w_gQMPIoVDZSAdnmj1q1EytPfxfDDq\\
\CeC6166qDuox07hOoHTrGZ1ztsduZsN7J81Rckp5AuBupmD3pQKeWRDKgoMxluTrt60\\
\V_7HtORNg-NCiWSejw0YGrboqyShJ5efIV9vzmh6-N1X6y5s0GShHgiWIo8xYFdshP-\\
\i1wzUo0AmPTaBiLHDjb0M7keH8HEpfmqnRwfIDZQ3T9xHIQXHcQYa8ggRGkAhcijr_x\\
\qdYN58YmNDRR5IKAPisnfe6jRxhIQxE4Pvphmpq4pRRTD98Ui6AXbuMEQuzqHJe2506\\
\tgYIrveMsY2dtUziMr5QzXdaAvWBj2o60n1kWh2ucFATTjHipHLfs-tsMova-XIKYo\\
\VfJ3MeX3nxQhbMGzYhKT9YMNQR7Yo0nYcBraTia3bprcStwTySzgUP314ybRQJrcso\\
\nwIVkl1C7XSaxKJhznwViTgpCSBwctn46yHMrlvvqNt8TCwClKk-8_OFsNxBhSjFxZC\\
\Y6zq-HaQe0HP59tDDEuUAjkgcfGNh5Aj_JGrz1WVnyDvrXGXZ6BpzqPbJJypjXukZpv\\
\U3yCcPNYVRKI1stKFC43rN2XMQS_-K0NwGxbrHUiG01ApRg21AcLNjXQu01_H5IMPP\\
\fUMPwXZrLNIVBmJjTny1I8uNwBmU1WRF-2v_jfdVqPvdHztw3xodwszuZmzgMvMVL11\\
\sa78QCoZAqBEPqYE0xvw199r1TPhnqHYM5Az41CWBY1co1AkCTfBpcBxKE9QdpvpIPH\\
\U1diCScJfEq1f3A_pMr-HrWrmpnk-KXRBgogRp4Hjezk9HyhxTfQA00RcPQPuDvx fu1\\
\EIVMhar4TdujfA30hQeigoXbRG9bC4fTJ6q3LiHAQRNgMzGIfwAZfgyTQXuAst4BvmH\\
\cS45n-dl2eeye8i7gi5V0vnfqCdhzCMGHh9gt1Vg50stA93xBPLJVudYcwUDitSHSS3\\
\AmakHXG8YHY0ZuIJFvj_UtiMC7k4YMMf6ZTz0U2F7wmNgIdp1I-UqKPitk5BIWZbDpx\\
\jSwyfjty5bfM4lsONII38-TFGF6cWnWC-QC1BhxYsn18cUFzwoEish0PK4iy0pMvpYr\\
\kfivcXzDYPfpWBEKE4BRcfRqrs4w5TK_zqLbt9tv8V_CLnJXEYmJrIdF6tVyIf2bGPK\\
\p58YF8QuPjJArNc4qVC1R9yyKs7hxNb4wLaWsDQPYEY1bJeTJ8TsCPM7mSvp7F3weqi\\
\AwbLAd5f8girEKeYSjx0j1K3zWb0BL7u_07a8kJZYkt7L9sn5jnGumeLedvab0cWP-1\\
\g6hCjHn1BvVpI66sp04i90ZSVMEpcXWWUUMrxG373uuZ1AqVbQu6mYuMJNwavv4hf53\\
\GwPRytC46rfTLIDv0BKvTLRpGCQsWxqWw-IHAYLWoT00IZ695xePq5z03o-Sek-Kxj\\
\UgGg91tIm74KuaMYIrMQCyNDv_-Qdj_OEDAxRj2V4w5TS3c04Dy2IPftmSj0xivXS8s\\

\YJQNsncI1tXA2-di2gyvsr6qf2ae91QpCa0P3vW9golEge04Mq6lo4VAzaNrmPJhell\ \aQyE_NsYEfJhvI9EAAAbg4Q28Dg1GSxErZHd4tgy82nRqlYdPFzjGUvYFzS4lePnQ"}}

6.1.1.3. jws

eyJhbGciOiJDULLESTUiFQ.OTA4NWQyYmVmNjkyODZhNmNiYjUxNjIzYzhmYTI10DYy0\ \Tk0NWNKNTVjYTcwWNjNGU2NjcwMDM5Njg5NGUwYw.8xELcU6FTHpMyTHwLqwmHJDck\ \Zdm7J6zLy1wT6Xtw5zG9qBQoCP2dBUlau1YkM7ZEcnZ09h8xEa_7L8dfiIs0dwHdb0r\ \S5-0dQ1DMbLEA8zgn8Jb12RyqH2Ehw9PsRCxp4BtyqvNZCnpV_UHykYdMvtUq2NKLt8\ \XrzfJWXcG4dzz-GddE6jJQPmKDzBQt0CsmaEwQ1_wzN-167I0mPMmzwx0JcfjerWg6H\ \4wcwMj_0WPeAe5iMygAwCIIFp72crFyLjWu3ziLojmK065UL9_a99C_YbzagwNjYc7\ \2SJYDcaDWiyajvnXfGM-e9hpM0-SeX79p-U8P1KNKBb8aPzP7LSUxrwCdf_xFPS68d\ \0QE6njannI7DbamW-LzMcrwKI6zUvdBVn0hYpM32fg2T-a0mW3KIL-aQZZ0wWH850E\ \JVeUrSVX2uaGp2eFbNY6Y_C40wByKLM50trQuSLYwzkfHu9jaTWhBfUXhkQLGy1q0\ \1xf1JpbYfe4Doy7v0XfgDEYYGVY0-1PZ78d7WyrYLxJCSQGuuG8K2u7_g2Qw0Rc5ESN\ \D4adRMMBBG0RFrJiXmn3Fem8Si2rV5k-eoT-sMs8lsQclWEHwmS38hH4IuRtsUmfxnz\ \cq-X7mljwAKB6fnnU6poZvB0ag0MFNjha76N0fmdz3HeH4dK7f9DR2wt7pw_16h20SD\ \xASLLMTeIYPVN4Vzi63KfZ23FsXcnqbAwaK4ihBC70LwUNKwfzo110SxiVX1k00eVqt\ \RiJe_VgDqxRk5sSgnaKBs_wk1PeEG1K_cXLWcxp1akyC-e5kYdu3HX1g60o5MJdFPz0\ \E4JX5LCNU5w5CrkoJSKHcyy3KHCT6vmnpyMesJWhywuGPa0iS65Q2brkwCgqq-pUCJ\ \BeyqpzSV1J-89xPhU2BE6XSorXXAhr09S_FehFw8ypNh2uS9S42U15vY4ccy-Jc6Tw\ \y4Pwqecsr7AlnSsvHDrUebItid2Pqa9DHa9gN_1zS6f-u9ne7tC7_PnYS9M5warHhDt\ \LTwm9k9z8bVtR7pHYKPWoutVtWaoI-Z0VV0vnZmKYL26gt1KJ7qUfvU0vzxNdKDhvV_\ \IqlAx9U_uQdrm0glz1F2Ia967tMA-x2xQt1NA0kcc6e8ZZew40eG0xXJgV7pYmsGtPN\ \JvATmTCcEEqJ2rzG99PNAbNgon1UWz6-X3mRBXr5Kt75wPOI_IG3-k7SjqoTuOYmn0W\ \pzaIKlsG8wL_Vk0r3x1gN3djBxuA6_LmU5RyyCP1fPB7ZtxJKSiB707IGLJBmeYVnAL\ \11-24Nvy2jXjfeQJ1J8cr0MQEglV1iCc16XKmjtg_T8m5ktTxRL0yP64jir4M8H_tkL\ \TKCW1DH51K_U7genF9aucB8ASy8Uj9X129A2ccvP58PDYsP8YHpa5wsfixDtJotfLq\ \j3wsA-baB4hdQnhhZ0-K5Qufa8TIIcyyyIuJ1iV04I0sKwMAuW0ePGrfQwksba8GiW-\ \b15CXP8jC_DptR60ULeaxLIBjtykIm_p0hL6JprKV8FAD6QFCMlyHapirma8ubLdyx9\ \p5c2STHq1UTCss8xTUyDcIz7oY_sVhk5Pe1v5HFRpBRaoaVe2pcIcgAZ2uV0P8K09ne\ \WdbB0wKxwZmlVdnCLXe-ylscsb6NvyMEDMWSrerjSv2CSFA_HHfiKYJ8BC_DPEUedv\ \nrAx4X0MGEThIUah0AoRL41gp-AKu0p01HftC2zbhHDxKeJpBS5UqTY7v8s1Tr6z1h\ \cGbLUaNzBC7U5QXxiHGZVtcn2s1W4v6i1ea0JKj72FUBt6ME9v22sGphJaDJ1iGfktr\ \LPSPAvp-6X6d0_pIbMydMyWABd-Ch9GOE4n-WX0cPUUIepm5loRUx7-dKG1MfmmU00q\ \dL1Ew_Dwn299TGGKFyDVwnNCnGGEDKEfmqJcvUOCD_i5JChe4QKwuM7wU3KB0tDhQag\ \KLbIFa-4Szitqws8fn6TaH5DCi9E8JL7r3zvsfsJwj5-951ZIKTcB057cXynNkUT6C_\ \buch1ReBj8n8mGp7ZtTNusV90MMManLzpDlizgUlwdi9Gv4rH6VqWuSndnozLKKzIdrj\ \a5iv9QuGgkuwCxkgcVC00mixik9eBxkGdXbiUz8xdyYh21RLPLmHHELqqUUZMMCQGGF\ \Bg_DhozNMT48-1mS4MdKA8FUAAu0xBPA9Qkanqh1AJQf2jnW63J-iK2A6U410cpxE\ \S2XXu51g6sgStI8iWrA8o3Xit8HenL_SNsNNk8t0_Vwa06Vj0poENkNqZS6MjSWR8y\ \nbvItMz8ANT8ZLhCA1JRxsFwG9-t3CHVb6GfsbPSe4H6UGG91y4sJ-Sbmeb19eMzxJD\ \ay2bi07C0IrRoWkAQsawu8Vbyyb8Pm40LqBgbajimBELTDSNUZNMKHFw9uR50QKXoe\ \Yaet_LCpRzAv-tj3JpC8vJYwMdPwpcheIVj0qw2abj0oNDNRFZNbCUAHLjeqEC01Nwx\ \kb1Nw_cU1Go4liuREMbgr9qqBpiELsr_qk9vIEB3Acg07TJu-fq21jQ9AdKLHtyxHwz\ \jGLER3YwW7i3qqcKcoCJbv9PPaFD4Wob3tZ_0Ki2m0KvHq8cIjyEb1xGdXt73T9cima\ \dxshgiaayVzpMUSdVdHyvAfjK2JPuemj-t3SCPN7QrPkmVhhUYCdxt3dIQ35TR4F\ \V9sp-52UckVckfLSPZmthJ2XAG_a2xt8Jnek8uhgYs1YhWkaCfbq-PVTGKLLGeDgIdc\ \W-vwzygAcMyMrH8CoSt6Zm3YL1pTaFN3eG0DJmvD7mSBcn7B_D7tQ2INEPK9YJKfjXs\ \JEFElI881p4ZkMk81Nv7k-Cs7m3Qi47HeMA6dcBLhpq30UtNCnEzgI2-S-ZIB-m9Tno\ \AenT3evvivdrK-B3Gg6n0N0xmhxM-j1H-Ad_9gio3Zqd0vIz6LSJZ6QbZmXewjCcehh\ \hiY8-iHWw3eYZ8MvxkfgcsBtkxu2jRhHYM-nftbFt6Cgd2Yu47P71K9Als81hG6gjao\ \hh_mVLq0BaHTrgQ7D0-D-9N-BJSrXWe-Ev6hx_NAQjmDuYa2ReGJnv0J1CHxeau9Bsw\ \ZzRB3EwcnlevorMhgDWSn0YmM60wGiwAswssoe17Df3wcdt-sDyPBUqVPRaXGm88GPV\

\x EJNESK6Zi920H2r6u8JehAejnr20Kt3-sCEEDIpR6K8lgo-TaMTiF8WUylUWTfpym5\\veaDqFmp_AooB_0qPLDCp1TLPetVI^mQh1T2tg0DM5AdtJuz2eQ-jog_ENCIEof070g_\\\QyTNR6RFGz1CVStRD7YGPOzz_SC0Yn_sYpMpQ39g1I0I36DXjdBOX3gcMN4esHXHHps\\\YttwxegCuGMb0AzMgG-ZGpC1YC5NH9VGAA2kXQwz1zuAQZP6N5YAMNb4jJnUqbSZ0i\\\GzN4zu7hEX1X0VwVKLr4UJ1ox1IcVXVYFO_AjaRn-V4g7EdBCqA-FrlcXmLcGKuN2U\\\ax0Gj-qLn9bP0rz2G1kQy5QXy32axxurIJRpAbA60-yclqy54jzto7fg5gn1VRggMKf\\\NP0Z9eyfQ_DmrH-60eoyJ1rDZ6NaFR4gRwCXQt00F0Wze7H1bGpbbrJbeXDbr9Lns\\\1EjHzaqyVstqpK0GcxQaDsdqNciHTo-mhKGqB2LgyQ4z4iIrcmaHEfc4NIUM_MghxPF\\\wi9w7kB8900y41LUS6dHdu2ea-W1T_0mDXXdTWOfxNXQRdTKPwSSICi8vMM0BSn4k4F\\\or7n73x5Rvzv80ocHA3GeE0By8ymVxuyRq2csGv2nAMIH2f8erKxh4Id_foQbnJyQF_\\\sMzW1Fs6PC7UtRxL16xgT7_Ynfhx-sgg38Ro_qMkwmJdBbwEPY4Vv-iu-PMKwp0XXQD_oiTjS2yuf27B729ToREZc4hUUGNnhG_6cNsCn68W-E6s-koJRG633jMcHX3Sv0IFb6\\\DP3AggcLSaFd1s2V5zR4Y6PLUZHwg9M5kQbU17zDpHwsI_ANmFMyf6KQU3XLiKq0g2k\\\cvP2RyGf5CDQk5HWVXXm7TDGv7AYPKThtU4Az00HRKN8UPjPJuOv73DRNDvxEEYV32\\\hv1EyE3AYxRGrY610rAU1xXrATJBxJypIaaYXw-HVKwVcQYbbGyNCROUWRaR0aZ4LFX\\\MCLEE1Vs7G6I7pIguDWKCY702dpaxBKDI0KbUP1VwWF1qDdJ2sH2iCYdfK20Zfx0FiU\\\uK6JSaME4a2RGaT5uC712bGxw7zuK2n16xzH861vM_KVQzTMgYQhpS7to2_xnEvrQ0H\\\ogrScf6Yd215g7NtTDMjo5GgBi1TwXudyCmGhaoFZRDcrLsyw5G0vz1o0C29Hv28ecs\\\XtkFohjNNi_1Mw7wqBDMTRsLLb0pQ_LTMOZRwIaJfsGpa7FuCwvaQ8QTDfNMX1hdMzD\\\e-gNpeW9gWU6h1w_SXEwKyqpsx0jqWnpTQLCJFW4_54HmVjQGs-0JqUoRwXEmoxQnEh\\\5F5t0AepJuDeAaSnPcJHqc1G4WAPhIY4c2Hi1GHX1zjQnkMe7wmm1K5v7zsGxh1hCt\\\pw_yCVH7_i1fb38k8XKsq2-sVNCsUWYvqAe2hVdIwv4CVNvRohkxBn9uJ-76nTxPbL3\\\jJg5uUqD8kTpAv8LD0Hf3V107tYAMh4S6gbME7dw6I3U1cKAUmkXOs_AwbskXKL801q\\\CnZ1ZRpJoMXbL1e-nT40pAHSzDTiVb9fwUF5d2aeylzQxW1ucbEhFTtJK1tGa0E1EV\\\Iz2_XfQu649ToHwsXJGiL_qLuX-v_Hc01hhm6d8_KYH1sXZm6sFVSp19QJPu5X16j6A\\\wsJ4A1k56nVzCYL47fT-c087s_parbwfH0WdTEfawf1XEKRdqvIW4bhzLE08XIligw_\\\bd26QkWXWiK0CBaz_zNFptXbYIhjb599Ew_vN4jRRdU3k_UzUJIN6-3fMCImNgb8389\\\KSzsx2VRQWN3vP1QQcs3-oxTq-dks-PIA8G_Gz07bTY1i19957dy3z9k07Z6grSNu_eY\\\pmuR0Vhsc0Cr30iXWSFpo8Vkn49MAa1Sx1pNmQKQ9n9sYCeef1Mxz6KeTBInB4E_u5_\\\mz7JjoinhYBUIRgmGiDFVe0kfToZToG7Qf6F2f3M3XTMDkQBH93RJBhRWXjd4gUIjTB\\\vMehuU1Vz57CKRo1LAbiDb4f1mCrofTmXUvsX9zv7CwNMXnPgrMwVuHYsAoRgB6sNDE\\\kTwf82i6yubpBo9ZAwtSz72LjdsQbscn35hp9-qak3ZsRhstnyApD4i16TMze7smwNb\\\doDnXKmi560P6-F2AcCNRqcDTXYZFF0C9qDVJQs1KorZ8DGuwPN1IgnuozSTVzCNhQ1\\\ZfpYEB19FL6SYKPe1XzgSQ06s-IKo_90KbMqMpPaMwgNjGMfYAKcX4Sx1FzeoVuvgms\\\5LEyJa_vib-lKbnrbwcaSj8pI_xqg8E2dBWu2YKJvcyxz7ZTF6YwySuVJHYIf0JVWsp\\\vd_LUj6ySe2NA0sMq0xceJFM6ssfHURjsUGZcQ6prm18t1AKeyWhnW1-c0ALCDyNyX\\\UozNt07kuCVFJtjEk5P9DdkdwgQaaTyErJcEA6fD3b3mfouZQ6PBQqTSAYEMrNARraA\\\78_10pZEZgone5LN3e-mhFK-NpFhteOKzV870Air3dEXVo6RodykqYCH6dberJdzdcj\\\6C0q6YRA8mdiXXcaZE6a1fkuewRTFPBd9LZojPTfqh20oo_MZ8h4qd-Ky4ixKZMWiwX\\\FAWE7JicpFC94bZqK_XQ78n9HIytd6gLh5UwIhHrShfNw0unnT0yaV4e_Abf73zxmV8\\\OryQvoaDobxAnsiEBE5B-7-QjSI-2MBm3meII1GMgz-jLtz4LoT1tBKgzx1hS83s47\\\U12S0Jt0nkstYtefZjKwsQ0Vsn3nS4ioYDn9J49tt2MEznMOKIAY3y3bypoFLlibeHN\\\pXs6A9wREKKfd1wC2ytSZ_G1x-IRBtwtWoictr7U2uY_QWSYnq2yEC8xfpmhz9kIFxx\\\ceZjN-QQna3xVZJWw3_0HDSQxatTXAA0cH3CPnLQAAAAAAAAAAAAAAAJJEB\\\ggJCox0WV5SmhiR2NpT21KRFVsbEVTVFVpZ1EuT1RBNE5XUX1zbVztTmpreU9EWmh0b\\\U5pWwpVeE5qSXpZemhtWVRJMU9EWX1PVGswTld0a05UVmpZVGN3T1d0ak5HVTJ0amN3\\\TURNNU5qZzV0R1V3Wxc

7. Normative References

[CRYSTALS-Dilithium]

Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., and D. Stehle, "CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme", 2018, <<https://doi.org/10.13154/tches.v2018.i1.238-268>>.

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.

- [RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <<https://www.rfc-editor.org/info/rfc4648>>.

- [RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <<https://www.rfc-editor.org/info/rfc7515>>.

- [RFC7517] Jones, M., "JSON Web Key (JWK)", RFC 7517, DOI 10.17487/RFC7517, May 2015, <<https://www.rfc-editor.org/info/rfc7517>>.

- [RFC7638] Jones, M. and N. Sakimura, "JSON Web Key (JWK) Thumbprint", RFC 7638, DOI 10.17487/RFC7638, September 2015, <<https://www.rfc-editor.org/info/rfc7638>>.

- [RFC8702] Kampanakis, P. and Q. Dang, "Use of the SHAKE One-Way Hash Functions in the Cryptographic Message Syntax (CMS)", RFC 8702, DOI 10.17487/RFC8702, January 2020, <<https://www.rfc-editor.org/info/rfc8702>>.

- [RFC8812] Jones, M., "CBOR Object Signing and Encryption (COSE) and JSON Object Signing and Encryption (JOSE) Registrations for Web Authentication (WebAuthn) Algorithms", RFC 8812, DOI 10.17487/RFC8812, August 2020, <<https://www.rfc-editor.org/info/rfc8812>>.

8. Informative References

- [RFC6234] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, DOI 10.17487/RFC6234, May 2011, <<https://www.rfc-editor.org/info/rfc6234>>.

Authors' Addresses

Michael Prorock

`mesur.io`

Email: mprorock@mesur.io

Orie Steele
Transmute

Email: orie@transmute.industries

Rafael Misoczki
Google

Email: rafaelmisoczki@google.com

Michael Osborne
IBM

Email: osb@zurich.ibm.com

Christine Cloostermans
NXP

Email: christine.cloostermans@nxp.com