

# SPICE SD-CWT

draft-ietf-spice-sd-cwt-07

M. Prorock , O. Steele , H. Birkholz , R. Mahy, M. Jones  
IETF 125 Shenzhen  
18 March 2026 — Session II



# Agenda

- Changes since IETF 124
- Open Issues
- Next Steps

# Changes since IETF 124

45 issues closed  
30 PRs merged  
-06 and -07 published



# Changes between -05 and -06

Issue	PR	Description
153	155	Add additional implementation
11	157	<b>Added Decoy Digests</b>
161	163	Added support for CWT Claims protected header
146	“	Added CBOR data model and encoding restrictions
164	“	Discuss +sd-cwt suffix
166	167	Move SD-CWT Definition before the differences section
165	168	Split issued and pre-issued payload definitions
144	171	<b>define To Be Decoy tag</b>
158	177	<b>redefine To Be Decoy tag</b>
179	180	<b>change To Be Decoy tag number to assigned value</b>
159	173	add multiple hash support to script
137	169	IANA expert reviewer suggestions 17.1 and 17.3
154	“	<b>change CDDL, script to use IANA values</b>
133	“	<b>reflect what is legal in which context in CDDL</b>
-	“	add optional vct claim to CDDL
131	175	explain time constraints between KBT and CWT
174	176	regenerate examples with IANA-assigned values
178	182	<b>restrict dates to 2<sup>-53</sup>..2<sup>53</sup></b>
170	181	explain that array length can change in Validated Disclosed Claims Set
154	-	IANA early allocation



# Changes between -06 and -07 (1/2)

Issue	PR	Description
210	-	Misread of text about +sd-cwt suffix
213	241	Holders also care about decoys
207	239	Make floating point range clear for dates
208	240	Explain gap in CBOR simple values
192	246	Include Figure numbers and titles
234	“	duplicate of 192
195	244	Rename “custom” claims in examples
203	242	Explain some CBOR-acrana
186	238	<b>Make CDDL consistent with IANA section</b> (off by zero error)
214	“	Clarify that presentations don't include TBR and TBD
247	250	<b>Allow use of cti instead of iat by Holder</b>
184	“	IANA Early Allocation of To Be Decoy (Done)
187	251	Inspired by, rather than based on SD-JWT
188	“	SD-CWT is generic container, not specific credential type
190	“	Move normative language formerly in Section 1.1
193	“	Reformat Boxes in Figures 2 and 3
194	“	Move Figures 2 and 3 into overview section



# Changes between -06 and -07 (2/2)

Issue	PR	Description
197	“	Add note about handling of empty disclosure array
199	“	Reword language about `typ`
202	“	Clarify claim “name” in CBOR
216	“	Replace lowercase must
230	252	Remove threat model section
227	253	Remove inflated promises about KT
217	257	Explain purpose of integer in To Be Decoy
205	254	Add disclosure of decoys section
205	256	Point to relevant security discuss in decoy section
215	-	wontfix. time constraints are needed since we have 2 related tokens
189	251	<b>Partial Fix:</b> Choose claims to blind/unblind
211	“	<b>Partial Fix:</b> Explain why cnf claim is there; KBT/CWT wrapping

Thank you Martin for the review

# Summary of Normative Changes

## -06

- Added **Decoy Digests** (PR#157)
- Defined a new **To Be Decoy tag** (62) to request a decoy on a pre-issued Claims Set (PR#171/177/180)
- Update to use the IANA-assigned values (PR#169)
- **Change the CDDL** to be more precise and only allow tags and simple values in the correct context (pre-issuance, issued CWT, presented CWT, KBT) (PR#169)
- Dates have to be between  $2^{-53}$  and  $2^{53}$  (PR#182)

## -07

- Make To Be Decoy integer consistent in CDDL with text (PR#238)
- In a KBT, the Holder can use cti instead of iat (ex: if they don't have a clock) (PR#250)

# Decoy Digests

- Decoy Digests are additional blinded claims that obfuscate the number of claims in a map or array. (PR#157)
- The “To Be Decoy” tag 62 is used pre-issuance to request a decoy in a location in a map or array (PR#171/177/180)

```
/countries array/ 98: [  
  /redacted country = "fr" /  
  60(h'dc5f753b66acd89d78481039934a86cc  
    14f9959c64c4037dea3f872b9a8453f1')  
  /decoy country #1 /  
  60(h'3f80963a1246b412d6567f2a5ca446fd  
    19a01dd8cfc291bed69e8c575c5abfb8')  
],  
/ redacted_claim_keys / simple(59) : [  
  / redacted claim 500 (= true) /  
  h'bd0fd88127b3071ff5433eef59a5e3c5  
    f18341f25c5bd119c41fd34802a9797b'  
  / decoy claim #2 /  
  h'eeec970897a5b9108f24f44751baedab  
    b53a1f3d241ab6b60c9f309f114ecf88'  
]
```

```
{  
  ...  
  /component origin countries/ 607: [  
    58("de"),  
    58("ph"),  
    62(1),      # add two decoys in this array  
    62(2)  
  ],  
  62(3): null, # add a decoy in this map  
  62(4): null, # add a second decoy in the same map  
  ...  
}
```

# More precise CDDL (PR#169)

```
; CWT claim legal values only
safe_map = { * label => safe_value }

safe_value =
  int / tstr / bstr /
  [ * safe_value ] /
  safe_map /
  #6.<safe_tag>(safe_value) / #7.<safe_simple> / float

; legal values in issued SD-CWT
issued_sd_cwt_map = {
  ? redacted_claim_keys ^ => [ * bstr ],
  * label => issued_sd_cwt_value
}

issued_array_element = redacted_claim_element / issued_sd_cwt_value

issued_sd_cwt_value =
  int / tstr / bstr /
  [ * issued_array_element ] /
  issued_sd_cwt_map /
  #6.<safe_tag>(issued_sd_cwt_value) / #7.<safe_simple> / float

; legal values in claim set sent to Issuer
preissuance_label = label /
  #6.<TO_BE_REDACTED_TAGNUM>(label) /
  #6.<TO_BE_DECOY_TAGNUM>(uint .gt 0)

preissuance_map = { * preissuance_label => preissuance_value }

preissuance_value =
  int / tstr / bstr /
  [ * preissuance_value ] /
  preissuance_map /
  #6.<safe_tag>(preissuance_value) / #7.<safe_simple> / float
```

## What keys can go in a claims set CBOR map?

- **KBT:** “safe” = text string / int
- **Issued CWT:** safe / simple59
- **Pre-issued:** safe / to-be-redacted tag / to-be-decoy tag
- No nested tags

# Changes since -07

- Issue #212 (PR#258) **Partially done**: Replaced claim requirements with table. Fine tune wording and push new PR.

# Open Issues/PRs

# Open Issues and PRs: Part 1 (Just Do It)

## Ready for Review:

PR#259 - rewording on uniqueness of decoy integers

PR#260 - Issues #218 and #220 (AEAD nonce size and AAD)

PR#261 - Issue #224 (Who can exploit the lack of canonical encoding)

PR#262 - Issue #209 (Stronger normative language in 6.3 and 6.5)

## Partially Done:

Issue #212 (PR#258) Fine tune wording and push new PR.

PR#204 rewording about nesting - accept PR, reword PR, or close

## Issues Ready to Address:

#191 Orié            Add more about linkability

#222 Rohan        Maybe remove section 16.7 first two lines

#226 Orié            Authenticate user public keys

#249 Rohan        Add COSE key thumbprint URIs in Appendix C

# Open Issues: Part 2 (Discuss)

#255 Redacted or Blinded or Both? (slide)

#198 Nonce usage (slide)

#219/236 AEAD or not? (slide)

#221 Include VCT registration for parity w/SD-JWT?

#233 Include RATS appendix?

#229 Requirements on disclosure (wording of 16.2)

#232 KBT/CWT bindings (wording of 16.5)

# Globally Replace "redacted" with "blinded" ?

## #255

- Currently we use a mixture of both terms. Generally using redacted as an adjective, and blind, unblind, and disclose as verbs.
- Redact — “to obscure part of a document for legal or security purposes”. Common in non-technical context. No such word as “unredacted”.
- Blind — “to cause to be unable to see”. Common in cryptography and testing contexts. “Unblinded” is a word.
- IANA early registration uses “To Be Redacted”.
- What do we want to do?

# "redacted" vs. "blinded" example 1

## Terms ⇨

Blinded Claim Hash: A hash digest of a Salted Disclosed Claim.

Blinded Claim: Any **Redacted** Claim Key or **Redacted** Claim Element that has been replaced in the CWT payload by a Blinded Claim Hash.

**Redacted** Claim Key: The hash of a claim **redacted** from a map data structure.

**Redacted** Claim Element: The hash of an element **redacted** from an array data structure.

Presented Disclosed Claims Set: The CBOR map containing zero or more **Redacted** Claim Keys or **Redacted** Claim Elements.

Validated Disclosed Claims Set: The CBOR map containing all mandatory to disclose claims signed by the Issuer, all selectively disclosed claims presented by the Holder, and omitting all undisclosed instances of **Redacted** Claim Keys and **Redacted** Claim Element claims that are present in the original SD-CWT.

## Section 3.2



Some of the claims are **redacted** in the payload. The corresponding *disclosure* is communicated in the unprotected header in the `sd_claims` header parameter. For example, the `inspector_license_number` claim is a Salted Disclosed Claim, consisting of a per-disclosure random salt, the Claim Key, and Claim Value.

# "redacted" vs. "blinded": example 2

## Section 3.2 ⇨

## Section 11.1



### 11.1. To Be Redacted Tag Definition

In order to indicate specific claims that the Holder would like to be redacted in a Claim Set, this specification defines a new CBOR tag "To Be Redacted". The tag can be used by a library to automatically convert a Claim Set with "To Be Redacted" tags into a) a new Claim Set containing Redacted Claim Keys and Redacted Claim Elements replacing the tagged claim keys or claim elements, and b) a set of corresponding Salted Disclosed Claims.

When used on an element in an array, the value to be redacted is present inside the tag. When used on a map key and value, the tag is placed around the map key, while the map value remains.

Examples in this draft use the To Be Redacted tag in order to distinguish their pre-issued, post-issued, and post-presented representations in EDN and CDDL.

The cryptographic hash, using the hash algorithm identified by the `sd_alg` header parameter in the protected headers, of that byte string is the Blinded Claim Hash (shown in hex). The digest value is included in the payload in a `redacted_claim_keys` field for a Redacted Claim Key (in this example), or in a named array for a Redacted Claim Element (for example, for the `redacted` claim element of `inspection_dates`).

```
d9df03da474fcb3c65771748e2e0608cf437504ecc24f450aaeacd40dd552b3f
```

Figure 8: SHA-256 hash of `inspector_license_number` disclosure

Finally, since this `redacted` claim is a map key and value, the Blinded Claim Hash is placed in a `redacted_claim_keys` array in the SD-CWT payload at the same level of hierarchy as the original claim.

```
/ redacted_claim_keys / simple(59) : [  
  / redacted_inspector_license_number /  
  h'd9df03da474fcb3c65771748e2e0608c  
    f437504ecc24f450aaeacd40dd552b3f',  
  / ... next redacted claim at the same level would go here / ],
```

Figure 9: `redacted` `inspector_license_number` claim in the issued CWT payload

Redacted claims that are array elements are handled slightly differently, as described in Section 5.1.

# Describing Nonces for Freshness #198

martinthomson opened on Jan 23 · edited by martinthomson

Edits ▾

Contributor

⋮

[This text](#) seems a little backwards:

The Holder MAY fetch a nonce from the Verifier to prevent replay, or obtain a nonce acceptable to the Verifier through a process similar to the method described in [[I-D.ietf-httpbis-unprompted-auth](#)].

Generally, a Verifier is the one that has the requirement for freshness. That means that they will want to challenge the Holder, rather than have the Holder unilaterally decide that freshness is needed.

The unprompted auth trick of using a TLS exporter is a good one, but I would instead mention exporters directly, but only in relation to describing cases where the Holder isn't actively challenged and it knows that the Verifier will need some freshness. (A nonce derived from TLS has other properties as well, but those can be a little fiddly to reason about, so I'd be inclined to avoid mention of the trick.)

In doing this, whatever you do, you should also mention the connection to the `cnonce` field. The current text doesn't mention it and you sort of have to guess.

# AEAD Encryption or Not PR#219 / 236

- Why use AEAD Encryption?
  - The algorithms are ubiquitous
  - Allows quick feedback if the decryption succeeds or fails
  - Prevents one style of attempted resource exhaustion attacks (validator needs to hold arbitrarily many possibly valid plaintexts before they can start matching disclosures to redacted claim hashes.
- Why not?
  - authentication (ex: AES-GCM) is “slow” relative to unauthenticated encryption (ex: AES-CTR).
  - Can eventually tell if decrypted disclosures all match redacted claim hashes in signed CWT.

# Open Issues: Part 2 (Discuss)

#255 Redacted or Blinded or Both? (slide)

#198 Nonce usage (slide)

#219/236 AEAD or not? (slide)

#221 Include VCT registration?

#223 Include RATS appendix?

#229 Requirements on disclosure (wording of 16.2)

#232 KBT/CWT bindings (wording of 16.5)

# Next Steps

# Next Steps

- Finish open issues
- Continue Interop testing of implementations
- WGLC, please!!