Tab 1

SPDX Security Meeting - November 4, 2025

Attendees:

- Rose Judge
- Karsten Klein
- Steven Carbno
- Victor Lu

SPDX Security Meeting - October 28, 2025

Attendees:

- Rose Judge
- Alfred Strauch
- Steven Carbno
- Victor Lu

Notes:

-

SPDX Security Meeting - October 21, 2025

Attendees:

- Rose Judge
- Alfred Strauch
- Steven Carbno

Notes:

- Discussed and built the model proposal for signature and certificate

SPDX Security Meeting - October 14, 2025

Attendees:

- Rose Judge
- Alfred Strauch
- Steven Carbno
- Karsten Klein

Notes:

- Discussed and built out the model proposal for signature and certificate

SPDX Security Meeting - September 30, 2025

Attendees:

- Rose Judge
- Alfred Strauch
- Steven Carbno
- Victor Lu

Notes:

- Going over work that Steven has done to materialize the concepts we have been discussing: Key, keyTypeSpecification,

SPDX Security Meeting - September 30, 2025

Attendees:

- Rose Judge
- Alfred Strauch
- Steven Carbno

Notes:

- Discussion around a new “Key” class (child class of File)
- CDX uses https://cyberphone.github.io/doc/security/jsf.html
- Prefeerence to not get into the description of the key itself, but use a name that can be looked up and referenced
- Private vs public key
    - Shouldn’t be encouraging transmitting any private key information but we may still need a private key element that would have a verification method but no other metadata
    - Would need publicKey and privateKey
    - publicKey classes: RSA, EC curve, etc (look at https://datatracker.ietf.org/doc/html/rfc7517)
    -

SPDX Security Meeting - September 23, 2025

Attendees:

- Rose Judge
- Alfred Strauch
- Steven Carbno
- Karsten Klein

Notes:

- We are going to create a new class called “Cryptography” (working title) to capture an instance of the cryptography algorithm list element
    - The parameter set has details about it, like key size,
    - This cryptography class will have a inUse or canSupoport relationship FROM a package
- canSupport → hypothetical security defects in crypto algorithms which may need patching
- inUse → has start time and end time to denote when a package used which signature/key/cryptography method
- How to anticipate combined algorithms? →
- Should this class be in the security profile? Consensus is yes
- https://github.com/stevenc-stb/spdx-3-model/blob/Profile-Security/model/Security/Classes/Cryptography.md
- Rename Cryptography class to Crytogrpahy Algorithm. Suggest changing the crypto-algorithm list to mirror this to avoid any confusion with crypto currency
- Object signature specifically for objects that are of a graph. SPDX signature can include objects. Important to have signatures of anything. Must be able to secure all your objects with signatures.

SPDX Security Meeting - September 16, 2025

Attendees:

- Rose Judge
- Steven Carbno
- Alfred Strauch

Notes:

-

SPDX Security Meeting - August 19, 2025

Attendees:

- Rose Judge
- Steven Carbno
- Alfred Strauch

Notes:

- Discussing comments on: https://github.com/spdx/spdx-3-model/issues/1065
- Discussion from tech call: two profiles for 1) Hardware 2) Supply Chain (hw/sw)
- What's the difference between a certificate and the info if we want to sign something?
- Do we want to treat a signature as a separate form of artifact
- Certificate is more like a key; signature is an application of the key
- Certificate vs signature:
    - Certificate: a document stating that an agent is the owner of a given private key
    - Signature: a cryptographic process that authenticates the origin and integrity of a digital document; the output; application that is using a cryptographic algorithm
    - Key Element
- Can you have a certificate displaced by another certificate?
- Certificate lifestyle stage shouldn't be in the certificate because you can't edit it.
- Let's model the scenarios next week (i.e. real work examples)

SPDX Security Meeting - August 12, 2025

Attendees:

- Rose Judge
- Steven Carbno
- Victor Lu
- Karsten Klein
- Alfred Strauch

Notes:

- Requirements drawio presentation from Steven about Signature requirements
- What do we want in a certificate? Certificate can be used as a signature. Subclass of File/SoftwareArtifact
    - serialNumber
    - subjectName
    - issuerName: Issued on behalf of an element
    - notValidBefore
    - notValidAfter
    - signatureAlgorithmRef
    - subjectPublicKey

        - certificateFormat
        - certificateExtension
        - Fingerprint
        - certificateState
        - activationDate
        - deactivationDate
        - revocationDate
        - destructionDate
        - certificateExtensions
- Can use a certificate for a signature
- Certificate is for proof and verification of any info that has been utilized
- Child of annotation – InUseCryptography (params=CryptographyName [string] and parameter [dictionary entry]) which could refer to the cryptography algorithm
    - How to specify *where* the algorithm is being used? TBD
- Need to cross check with FuSA and Operations group
-

SPDX Security Meeting - August 5, 2025

Attendees:

- Rose Judge
- Alfred Strauch
- Steven Carbno
- Karsten Klein
- Victor Lu
-

Notes:

- Internal signature vs external signature: when we represent the full data set - maybe we don't copy the entire signature in.
- How do we represent the external document - i.e. web certificate x509 - this technically exists as af ile somewhere but we want to bring in attributes so we don't have to bring in the actual file to the spdx model but have enough metadata to validate the signature for an artifact. To verify it wasn't tampered with.
    - Can either send the verification to an engine
- Do we need to include links to public keys or do we just say this is a certificate
- It will be complex to sign an SPDX node - in order to sign it we need to be able to serialize that node - digital signature in a bundle will be different than an element.
- Requirements:
    - 1) we must be able to repeat the signature process - must be able to verify the signature of the document and the knowledge about how to do the algorithm
- We should create a formal set of requirements next meeting
- How to make note of trust in the key relationship

SPDX Security Meeting - July 29, 2025

Attendees:

- Rose Judge
- Alfred Strauch
- Steven Carbno
- Bob Martin
-

Notes:

- Debrief signature presentation during the tech call today
- Signatures going to be critical for compliance and CRA
- Need an ability to represent a signature in SPDX
- Signature will also need to be used in Functional Safety profile
- Signature is evidence - lack thereof is evidence as well
-

SPDX Security Meeting - July 22, 2025

Attendees:

- Rose Judge
- Alfred Strauch
- Steven Carbno
-

Notes:

- Would like to introduce a concept of a digital/cryptographic signature on a package.
- Cryptography group is deciding what a cryptographic algorithm is
- Want to declare that an organization signed a piece of software using a certain cryptographic algorithm
- Security profile has to guarantee that something is secure
    - Cryptology/cryptographic signature achieves this
- CryptographicMethod could be a child class of model/Core/Classes/IntegrityMethod.md
- Would it also make sense to say that a signature is a subclass of IntegrityMethod
- Digital signature is a type of cryptographic method
- Not sure if it would a type of IntegrityMethod since a signature can combine an integrity method
- Digital signatures - a form of annotation rather than considering it a hash method: https://github.com/spdx/spdx-3-model/blob/546a2fe32e9515cde8b3a04bc855e8286028fe47/model/Core/Classes/Annotation.md?plain=1#L12

- For now create an annotation type that is a signature - Add ‘signature’ to https://github.com/spdx/spdx-3-model/blob/546a2fe32e9515cde8b3a04bc855e8286028fe47/model/Core/Vocabularies/AnnotationType.md#L4
    - Definition: <Alfred and Steven will send to me>.. A validation process
    - Maybe start by opened
    - 1) annotation
    - 2) “signature” sub class of integrity method (if we put it off of element instead, could be better for relationships to and from as well - evidencefor)
        - Signature value
        - Signature identification algorithm
        - Public Key
        - Agent that did the signature (signer)
        - Signature timestamp
    - 3) some combo of the two?
- Comment could be the actual signature values?
- Could signature be the statement property of annotation?
- Subject is the element we point to - that would be the file or piece of software that gets signed.
- contentType could be empty since optional
- Until we want to start representing signing keys this may be the way to go
- Potentially has CRA requirements.
- Could be 3.1 or later

SPDX Security Meeting - July 15, 2025

Attendees:

- Rose Judge
- Alfred Strauch
- Karsten Klein
- Steven Carbno
- Bob Martin

Notes:

- Still discussing the “exploited” category in the
- The exploited means something different than exploit - the catalog say that there’s known exploits against this particular CVE “in the wild”. For kev, of all the CVEs out there these are what bad actors are leveraging so patch these first.

- “Indicates whether a CVE is known to have an exploit…” in https://github.com/spdx/spdx-3-model/blob/develop/model/Security/Properties/exploited.md
    - What does it mean to leave it out? It is “in” the catalog just by creating the ExploitCatalogVulnAssessmentRelationship
    - Ideally we would create a default value and if not defined set it to true.
    - Or we want to be able to say “we made an assessment and this vulnerability is NOT in this exploit catalog”
- Anything in the current description of the profile that we want to revise for 3.1? This is the opportunity to tighten descriptions or elaborate
-

SPDX Security Meeting - June 24, 2025

Attendees:
- Rose Judge
- Victor Lu
- Alfred Strauch
- Steven Carbno

Notes:
- Went through the security issue backlog and discussed individually. Left comments summarizing what we discussed. Particularly on:
    - https://github.com/spdx/spdx-3-model/issues/439
    - https://github.com/spdx/spdx-3-model/issues/652
    -

SPDX Security Meeting - June 24, 2025

Attendees:
- Rose Judge
- Bob Martin
- Alfred Strauch
- Steven Carbno
- Karsten Klein

- Dick Brooks
- Ilan Schifter
- Victor Lu

Notes:
- Discussing https://github.com/spdx/spdx-3-model/issues/861
- Mostly worked directly in the code. PR opened for others to comment on with hopes of presenting next week at the tech call: https://github.com/spdx/spdx-3-model/pull/1034

SPDX Security Meeting - June 10, 2025

Attendees:
- Rose Judge
- Bob Martin
- Victor Lu
- Alfred Strauch
- Steven Carbno

Notes:
- Discussing https://github.com/spdx/spdx-3-model/issues/861:
- Having a security contact would support implementation of RFC 9116 section 2.5.3 as part of the SPDX metadata.
- What is a property of a contact point for a package? Class of contact points? Types of contacts.. Would that satisfy this need?
- Relationship to a package. Contact could be a time window and change over time.
- New contact class, field could be type of contact (i.e. agent or organization). Also have the field that you would want to connect with.
- FuSA might also want a contact
- What profile should this contact class belong to? Core
- This is the place to start the potential repair process.
- Do we treat it as an agent object or a separate contact?
- What is a vulnerability lifecycle? What does that look like? This is a part of that.
- Consumer, community and software perspective.
- Want a contact with a type (email, phone number, contact point)
- Can use an agent with relationship between an agent
- Agent can be used - it is the role
- Can agents have external identifier types?
- https://arxiv.org/abs/2505.19301
- https://datatracker.ietf.org/doc/draft-parecki-oauth-identity-assertion-authz-grant/
- Example: company (AMD), has companies in multiple countries and multiple types of locations (factory 1, factory 2) May have multiple roles at multiple locations - need a method for determining the purpose in determining
- Summary of meeting aded as comment in the issue we discussed: