Provenance record container and signing format

GitHub repo with code

https://github.com/icebreakerone/provenance

Script which generated these examples:
https://github.com/icebreakerone/provenance/blob/experiments/provenance.py

Example encoded record

In these examples, the container and signatures are “real” and have been generated by code, but the data in the steps is just an indication of what it might look like. Long chunks of base64 encoded data have been abbreviated for clarity. Since we use EC crypto, the signatures are relatively compact, and haven’t been abbreviated very much.

Key:

Base64 encoded JSON step
Signature information

```
[
  [
    "eyJpZCI6IlVSZDB3Z3MiLCJ0eXBlIjoidHJhbnNmZXIiLCJmcm9tIjoiaHR0cHM6……..MyOjU2WiJ9",
    "eyJpZCI6Iml0SU5zR3RVIiwidHlwZSI6InJlY2VpcHQiLCJmcm9tIjoiaHR0cH……..jE2OjMxWiJ9",
    [
      "123456",  <- certificate serial number
      "2024-10-17T12:16:31Z",  <- timestamp of signature
      "MEUCIQDNk3nS64bmGvMJwfdVWfyGuheGDEbB8-b5Ur2H9Iat9gIgc…….eGO3GvzH2EJut707lA="
    ]
  ],
  "eyJpZCI6IndiZ29VRCIsInR5cGUiOiJwcm9jZXNzIiwicHJvY2VzcyI6Imh0dHBzOi8v……6MzFaIn0=",
  [
    "98765",
    "2024-10-17T12:16:31Z",
    "MEUCIQCwEGqRtRRiyMP42rJjMUzN7HN7r-WER0yhwiVre5bM3gIgR7eZ_o2sJFEy……..LN-17m6Mow="
  ]
]
```

This is the transport format. The structure is inspired by JWS, and the crypto pretty much just copied, but it has nested containers and adds certificate information.

The first container is included in the top level container, and is included in the final signature.

The serial number of the certificate is an integer, but it might be a long one, so it's string encoded. JSON just loves to round large integers.

Signature generation

This container format uses arrays and position, rather than dictionaries with nice names. This means the algorithm to generate the bytes to sign is very simple and unambiguous. A prettier format will mean implementations are much more complex.

The signed data for the final signature in the above is, without abbreviations:


```
%.eyJpZCI6IlVSZDB3Z3MiLCJ0eXBlIjoidHJhbnNmZXIiLCJmcm9tIjoiaHR0cHM6Ly
9kaXJlY3RvcnkuZXN0Zi5pYjEub3JnL21lbWJlci8yODc2MSIsInNvdXJjZSI6eyJlbm
Rwb2ludCI6Imh0dHBzOi8vYXBpNjUuZXhhbXBsZS5jb20vZW5lcmd5IiwicGFyYW1ldG
VycyI6eyJmcm9tIjoiMjAyNC0wOS0xNlQwMDowMDowMFoiLCJ0byI6IjIwMjQtMDktMT
ZUMTI6MDA6MDBaIn0sInBlcm1pc3Npb24iOnsiZW5jb2RlZCI6InBlcm1pc3Npb24gcm
Vjb3JkIn19LCJ0aW1lc3RhbXAiOiIyMDI0LTA5LTE2VDE1OjMyOjU2WiJ9.eyJpZCI6I
ml0SU5zR3RVIiwidHlwZSI6InJlY2VpcHQiLCJmcm9tIjoiaHR0cHM6Ly9kaXJlY3Rvc
nkuZXN0Zi5pYjEub3JnL21lbWJlci8yMzczNDYiLCJvZiI6IlVSZDB3Z3MiLCJ0aW1lc
3RhbXAiOiIyMDI0LTEwLTE3VDEyOjE2OjMxWiJ9.%.123456.2024-10-17T12:16:31
Z.MEUCIQDNk3nS64bmGvMJwfdVWfyGuheGDEbB8-b5Ur2H9Iat9gIgcc2pic-3xTTMdb
ceXEM7MKBjReGO3GvzH2EJut707lA=.&.&.eyJpZCI6IndiZ29VRCIsInR5cGUiOiJwc
m9jZXNzIiwicHJvY2VzcyI6Imh0dHBzOi8vZGlyZWN0b3J5LmVzdGYuaWIxLm9yZy9zY
2hlbWUvZWxlY3RyaWNpdHkvcHJvY2Vzcy9lbWlzc2lvbnMtcmVwb3J0Iiwib2YiOiJpd
ElOc0d0VSIsInRpbWVzdGFtcCI6IjIwMjQtMTAtMTdUMTI6MTY6MzFaIn0=.98765.20
24-10-17T12:16:31Z
```


% marks the beginning of an array.
& marks the end of an array.
. joins the strings together.

The serial of the certificate used to sign and the timestamp are included in the signed data. The serial is not strictly needed, but is best practise in include, but the timestamp is required so that it cannot be altered without breaking the signature.

This signing scheme follows the same general design of JWS, which joins base64 encoded data with a . None of the possible values includes % & or .

As this record includes steps signed by someone else, their signature is also included in the data to be signed.

Decoded record

The library generates a decoded structure. In the process of decoding, signatures are verified, certificate chains, validity times and root are verified. The decoded output includes information about the signer from the certificates. It (probably) doesn't need to be repeated in the steps.

Key

Data in the base64 encoded JSON steps (indicative, not specced out yet)
Identity of the member who added the step to the record (from certificate)
Identities of the members who are including/relying on the step (from cert)


```
[
  {
    "id": "URd0wgs",
    "type": "transfer",
    "from": "https://directory.estf.ib1.org/member/28761",
    "source": {
      "endpoint": "https://api65.example.com/energy",
      "parameters": {
        "from": "2024-09-16T00:00:00Z",
        "to": "2024-09-16T12:00:00Z"
      },
      "permission": {
        "encoded": "permission record"
      }
    },
    "timestamp": "2024-09-16T15:32:56Z",
    ".signature": {
      "signed": {
        "member": "https://directory.estf.ib1.org/member/2876152",
        "application":
           "https://directory.estf.ib1.org/scheme/electricty/application/38936455",
        "roles": [
          "https://registry.estf.ib1.org/scheme/electricty/role/supply-voltage-reader",
          "https://registry.estf.ib1.org/scheme/electricty/role/reporter"
        ]
      },
      "includedBy": [
        {
          "member": "https://directory.estf.ib1.org/member/81524",
          "application":
"https://directory.estf.ib1.org/scheme/electricty/application/26241",
          "roles": [
            "https://registry.estf.ib1.org/scheme/electricty/role/consumption-reader",
            "https://registry.estf.ib1.org/scheme/electricty/role/reporter"
          ]
        }
      ]
    }
  },
  {
```

```
    "id": "itINsGtU",
    "type": "receipt",
    "from": "https://directory.estf.ib1.org/member/237346",
    "of": "URd0wgs",
    "timestamp": "2024-10-17T12:16:31Z",
    ".signature": {
      "signed": {
        "member": "https://directory.estf.ib1.org/member/2876152",
        "application":
              "https://directory.estf.ib1.org/scheme/electricty/application/38936455",
        "roles": [
          "https://registry.estf.ib1.org/scheme/electricty/role/supply-voltage-reader",
          "https://registry.estf.ib1.org/scheme/electricty/role/reporter"
        ]
      },
      "includedBy": [
        {
          "member": "https://directory.estf.ib1.org/member/81524",
          "application":
              "https://directory.estf.ib1.org/scheme/electricty/application/26241",
          "roles": [
            "https://registry.estf.ib1.org/scheme/electricty/role/consumption-reader",
            "https://registry.estf.ib1.org/scheme/electricty/role/reporter"
          ]
        }
      ]
    }
  },
  {
    "id": "wbgoUD",
    "type": "process",
    "process":
       “https://directory.estf.ib1.org/scheme/electricity/process/emissions-report",
    "of": "itINsGtU",
    "timestamp": "2024-10-17T12:16:31Z",
    ".signature": {
      "signed": {
        "member": "https://directory.estf.ib1.org/member/81524",
        "application":
              "https://directory.estf.ib1.org/scheme/electricty/application/26241",
        "roles": [
          "https://registry.estf.ib1.org/scheme/electricty/role/consumption-reader",
          "https://registry.estf.ib1.org/scheme/electricty/role/reporter"
        ]
      },
      "includedBy": []
    }
  }
]
```