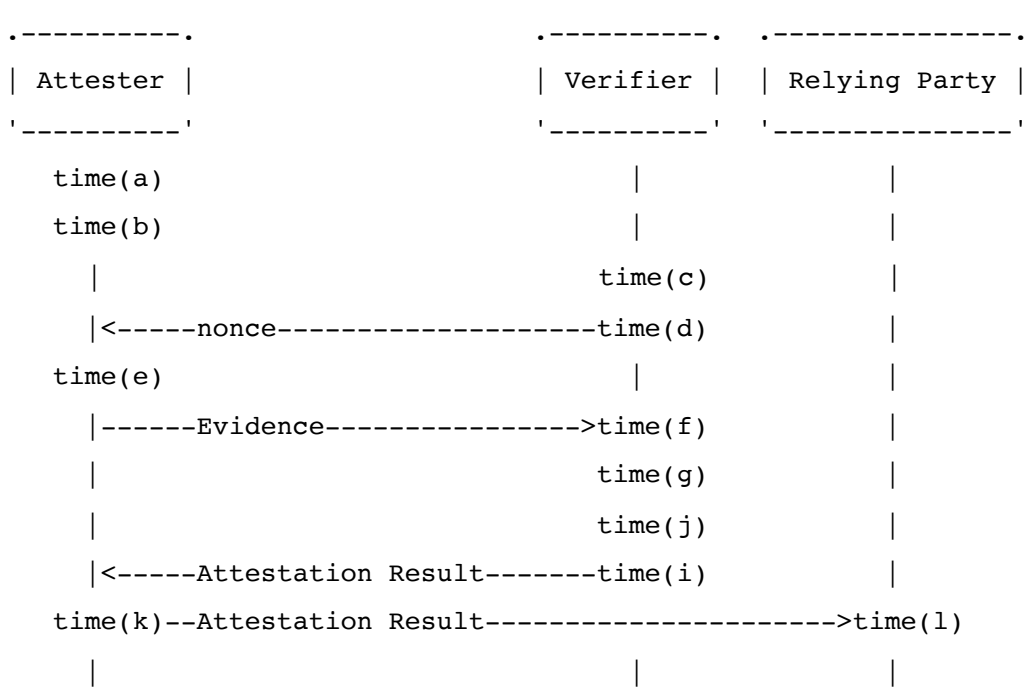
# IETF RATS Timestamps in EAT

Remote ATtestation ProcedureS (rats) WG Virtual Meeting: 2020-03-31

Laurence Lundblade

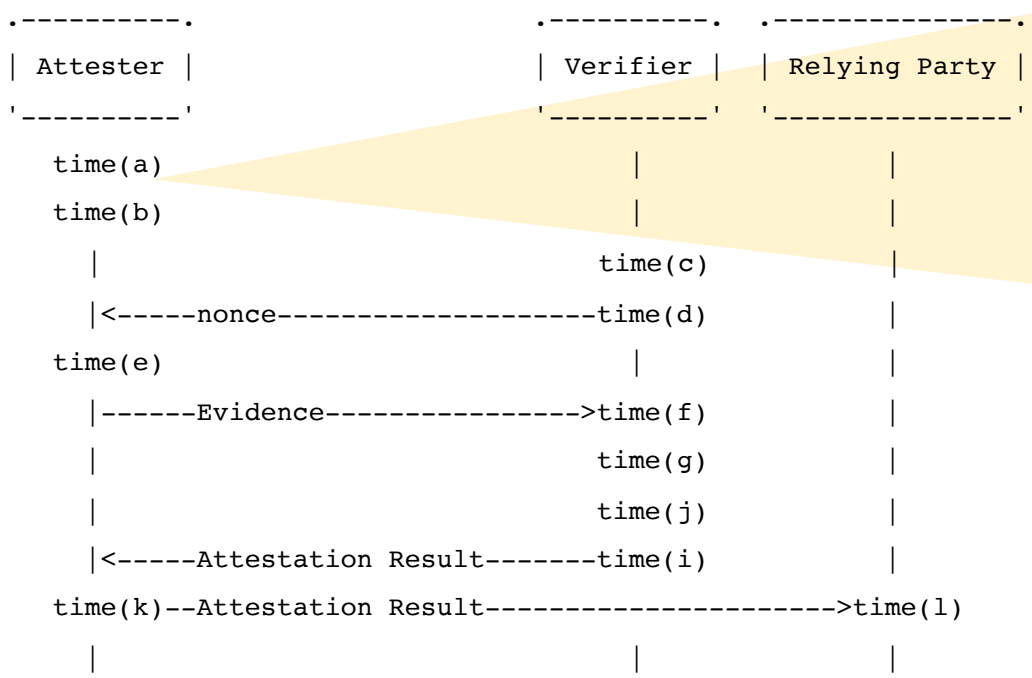
# Base Diagram




- Simple composite of some of Eric's passport model diagrams
- Assumes attester is simply reflecting the attestation results at time(k); there is no signing then

| id | name | strawman definition |
|---|---|---|
| time(a) | Time of claim generation | When a particular claim was created, or when any values within that claim change |
| time(b) | Time of Attester awareness | When an Attester or Attester Component receives a claim |
| time(c) | Time of nonce generation | When a random number not predictable to an Attester is generated |
| time(d) | Time of nonce delivery | When the random number becomes known to Attester |
| time(e) | Time of Attester assembly | When an Attester marshals Evidence. This Evidence typically consists of one or more sets of claims. Each set might be signed by signed by an Attester Component. Additionally some new claims might be generated as part of this assembly. |
| time(f) | Time of Verifier Receipt | When a set of Evidence is received by a Verifier |
| time(g) | Time of Results | When Attestation Results were generated by a Verifier |
| time(h) | Time of Results expiry | When a Verifier states that a specific instance of Attestation Results should no longer be accepted |
| time(i) | Time of Results delivery | When Attestation Results are pushed from a Verifier |
| time(j) | Time of passport assembly | Time when Evidence that includes Attestation Results is assembled in a format digestible by a Relying Party |
| time(k) | Time of Evidence to Relying Party | When an Attester pushes Evidence to a Relying Party. This evidence could potentially include a Verifier's Attestation Results. |
| time(l) | Time of Relying Party receipt | When the Relying party receives Evidence from an Attester. |

# Acquisition Time




- Simple composite of some of Eric's diagrams
- Assumes attester is simply reflecting the attestation results at time(k); there is no signing then

| id | name | strawman definition |
|---|---|---|
| time(a) | Time of claim generation | When a particular claim was created, or when any values within that claim change |

- Examples: GPS fix acquired; SW measurement taken
- May happen long before attester is involved in turning data into a claim. For example the GPS subsystem may intrinsically cache locations and report them with time stamps

- Handle this in EAT with claim-specific timestamps as only a minority of claims will work this way.
- No need for general means to associate an acquisition time with any arbitrary claim
- Individual claims must be modified
- The proposal for location:

```
location-type = {
    latitude => number,
    longitude => number,
    ? altitude => number,
    ? accuracy => number,
    ? altitude-accuracy => number,
    ? heading => number,
    ? speed => number,
    ? timestamp => time-int,
    ? age => uint
}
```

Discussion on age versus timestamp on next slide

# Timestamp / age for Acquisition Time

## Timestamp

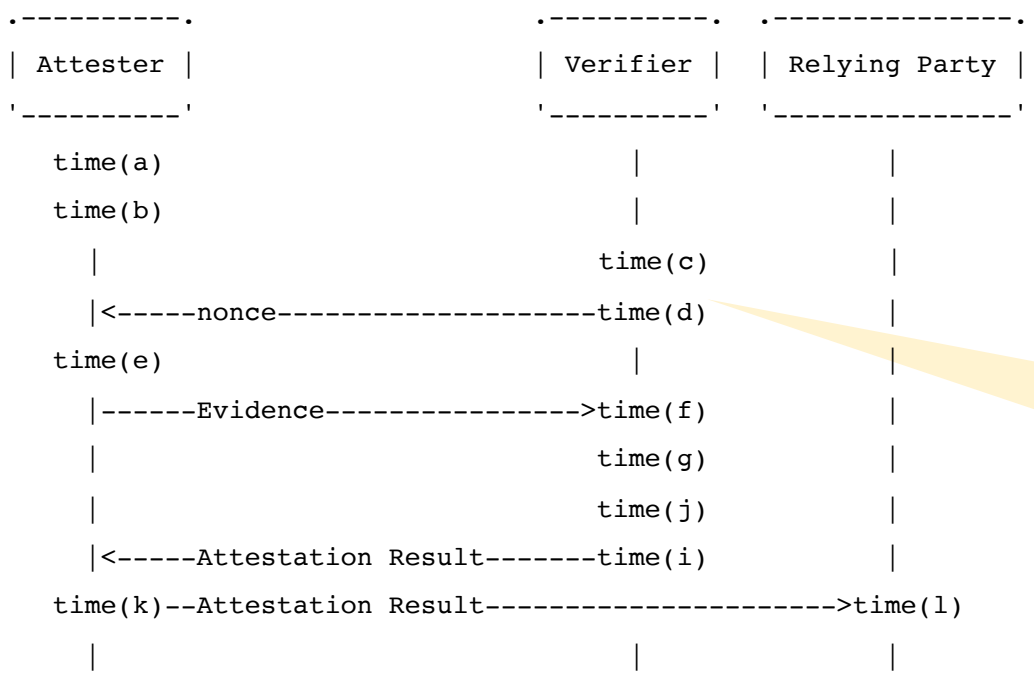
- Absolute time based on UTC/UNIX Epoch time; CBOR tag 1
- Preferred to age
- Disallow floating-point values

## Age

- Alternate for devices that don’t have a clock or whose clock is unset
- Device must have a ticker to measure elapsed time; an uptime ticker will work
- Is elapsed time between acquisition and token assembly; between time(a) and time(e)
- Verifier can compute the range of the absolute time of acquisition from time(d), nonce generation and time(f), evidence receipt. If window is small, this can be quite accurate

# Nonce

| id | name | strawman definition |
|---|---|---|
| time(c) | Time of nonce generation | When a random number not predictable to an Attester is generated |
| time(d) | Time of nonce delivery | When the random number becomes known to Attester |

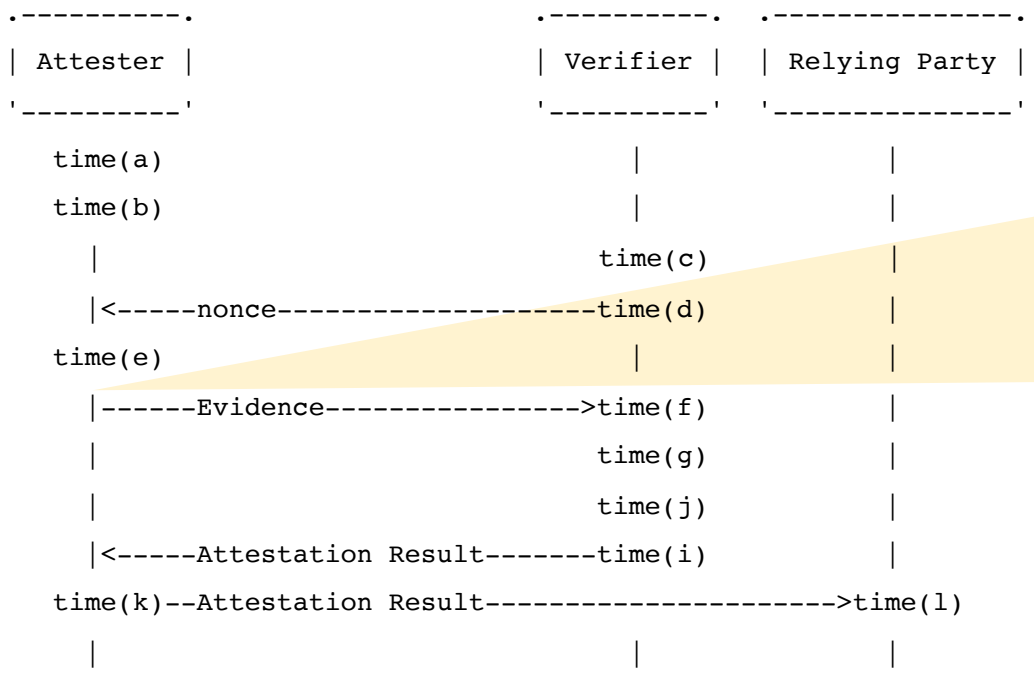



- No need to record time(c) or time(d) in a token

- Simple composite of some of Eric's diagrams
- Assumes attester is simply reflecting the attestation results at time(k); there is no signing then

# Token Creation

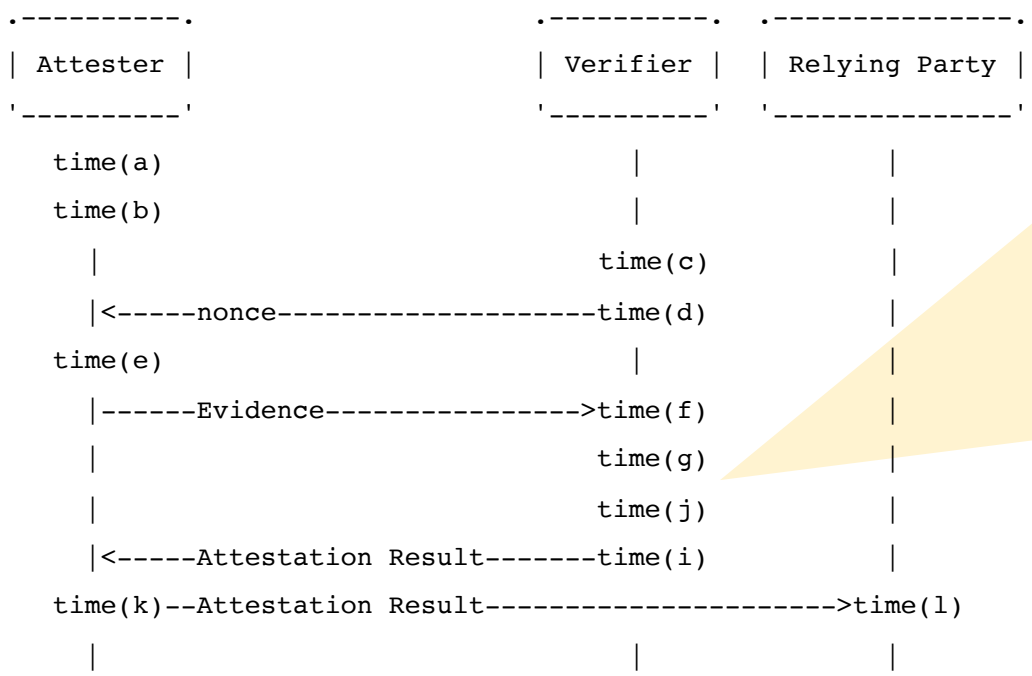
| id | name | strawman definition |
|---|---|---|
| time(b) | Time of Attester awareness | When an Attester or Attester Component receives a claim |
| time(e) | Time of Attester assembly | When an Attester marshals Evidence. This Evidence typically consists of one or more sets of claims. Each set might be signed by signed by an Attester Component. Additionally some new claims might be generated as part of this assembly. |




- Simple composite of some of Eric's diagrams
- Assumes attester is simply reflecting the attestation results at time(k); there is no signing then

- This the time that all claims are formatted and the signature is applied.
- The IssuedAt or "iat" claims from CWT / JWT can be used for this
- It is always an absolute time, never an "age"
- If the device has no clock or the clock is unset, then this claim is omitted and the Verifier has to go by time(c) and time(f) to establish range.
- Assumption is made that time(b) and time(e) are the same. That there is no caching of data inside the attester.

# Results Creation




- Simple composite of some of Eric's diagrams
- Assumes attester is simply reflecting the attestation results at time(k); there is no signing then

| id | name | strawman definition |
|---|---|---|
| time(f) | Time of Verifier Receipt | When a set of Evidence is received by a Verifier |
| time(g) | Time of Results | When Attestation Results were generated by a Verifier |
| time(h) | Time of Results expiry | When a Verifier states that a specific instance of Attestation Results should no longer be accepted |
| time(i) | Time of Results delivery | When Attestation Results are pushed from a Verifier |
| time(j) | Time of passport assembly | Time when Evidence that includes Attestation Results is assembled in a format digestible by a Relying Party |

- Assumption is that the Attestation Results is in EAT format
- Assumption that the "passport" is just an EAT-format Attestation Result
- Assumption is that the Attester just relays the unmodified Attestation Result to the Relying Party.

- Time(g) and time(j) are assumed to be the same, the time at which the attestation result / passport is created and signed.

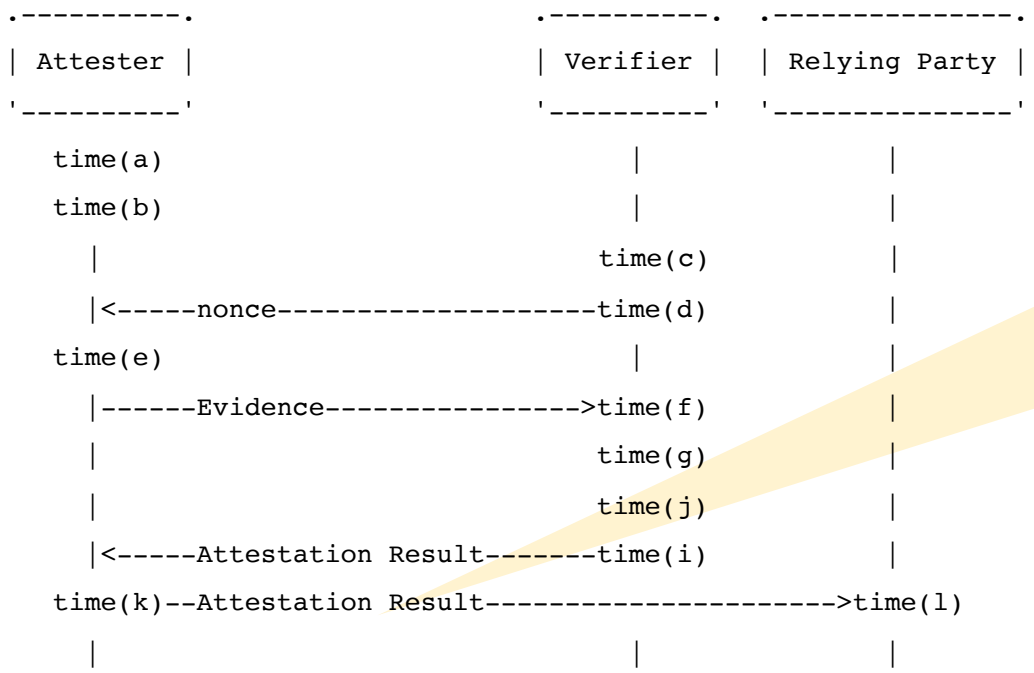
- The CWT/JWT IssuedAt time, "iat" claim is used to record this
  - Hmmmm, how to distinguish time(e) from time(g)? They should both be in the results as the relying party will care about both.

- The CWT/JWT Expiration claim is used to record time(h)

- No need to record time(f) or time(i) in the Attestation Results

# Results Delivery

| id | name | strawman definition |
|---|---|---|
| time(k) | Time of Evidence to Relying Party | When an Attester pushes Evidence to a Relying Party. This evidence could potentially include a Verifier's Attestation Results. |
| time(l) | Time of Relying Party receipt | When the Relying party receives Evidence from an Attester. |




- No need to record time(k) or time(l) in the Attestation Results
- Also, no possibility to record time(k) or time(l) in the Attestation Results as it can't be modified once it leaves the Verifier.

- Simple composite of some of Eric's diagrams
- Assumes attester is simply reflecting the attestation results at time(k); there is no signing then