

## All.Net Analyst Report and Newsletter

### Welcome to our Analyst Report and Newsletter

#### Attestation for Attribution

A lot of work has been done in the area of supply chain to allow for attribution through attestation. I thought it might be time to clarify a bit.

#### Attribution and causality

Attribution can be understood as associating actions with actors. This is conceptually a case of causality clarification. Causality associates a cause to an effect operating through a mechanism ( $C \rightarrow^M E$ ). Attribution, on the other hand, associates a causal agent (an actor) to an effect (an action) ( $C \rightarrow E$ ). Note the lack of mechanism. Fred wrote this article. If true, it is an attribution of the article to its author. But it is not a causal chain indicating the mechanism(s) by which this happened to a level of granularity. And of course the granularity of mechanism can go to the depth of current physics and the number of resulting links in the causal chain to too many to count.

#### Attestation as a surrogate with responsibility

Attestation is testimony to what happened and/or how it happened. How it came to be, how it came to me, what I did with it. I attest to it, and as a result, I take responsibility for the truth of what I have attested to. An Attributer takes Responsibility for an Effect ( $A \rightarrow^R E$ ) When I attest to the fact that I wrote this article, I can do it in many ways.

This article is self-attesting, except of course if you copy it and change the name, you are attesting to your authorship, so independently verifying the authorship is potentially problematic. Of course by me putting my name on it, I am taking responsibility for it, but if you write something else and put my name on it, it is a false attestation, potentially making me responsible for your acts. Per the encyclopedia Britannica (online)<sup>1</sup>

**diplomatics**, the study of documents. The term is derived from the Greek word diploma, meaning “doubled” or “folded.” Besides the documents of legal and administrative import with which it is properly concerned, diplomatics also includes the study of other records, such as bills, reports, cartularies, registers, and rolls. Diplomats is therefore a basic, and not simply an auxiliary, historical science.

Diplomatic analysis is how we assert attribution to a desired level of certainty, and digital diplomatics is the version of this for the digital legal world.<sup>2</sup> Current attestation channels in the digital world use cryptographic hash functions in blockchains or similar methods to create bills of material that support automation, and distribution and authorship sources use these methods to claim authorship and responsibility in supply chain. They predominantly supply a digital signature as part of a sequence of signatures distributed across multiple repositories.

- The signature presents a ‘hard-to-forge’ association between a ‘document’ and a sequence of bits.
- The distributed ledger uses redundancy to fix the association in sequence (and time)

<sup>1</sup> <https://www.britannica.com/topic/diplomatics>

<sup>2</sup> See F. Cohen “Digital Forensic Evidence Examination” – available under Books at <http://all.net>

## Limitations of Attestation for Attribution

Those who know me know that I point out the limitations of such things. It is part of the engineering disease I have that prevents me from overselling, and as a result, makes me a lower performing sales person in most contexts.

I started talking about attribution through attestation, and along the way I identified the following limitations (even if I didn't explicitly state them at the time):

- Attribution ( $C \rightarrow E$ ) is not causality ( $C \rightarrow^M E$ ) and both are inherently limited in granularity.
- Attestation ( $A \rightarrow^R E$ ) is not attribution ( $C \rightarrow E$ ), but is rather just a claim of attribution.
- Attestation is limited by the honesty, information available to, and expertise (knowledge, skills, training, education, and experience) of the responsible party (R).
- The responsibility (R) for the attestation ( $A \rightarrow^R E$ ) may not reflect reality, so unless they appear in person, we don't know for sure who or what the attester is...
- ... or was: R can change with time ( $R'$ ), typically a custodian of records for an entity.
- The mechanisms of digital attestation (bills of material or similar means) are subject limitations on use control, in that the mechanisms used may be used by others than the asserted responsible party ( $R \neq \bar{R}$ ).
- The mechanisms of attestation ( $\rightarrow^R$ ) may be otherwise subverted, unreliable, forged, and so forth.

So it should now be apparent that Attestation for Attribution has substantial limitations.

## So what?

So does everything and everyone else.

In managing your risk (uncertainty about the future), you can now take into account these limitations. And you should do the same thing for the alternatives. So what are the alternatives in the digital world today?

- **Do nothing** and suffer the consequences of unlimited lies, deceptions, and corruption.
- **Rely on the kindness of strangers** to keep you well informed and grounded in reality.
- **Do it all yourself** and hope you can separate the wheat from the chaff.
- **Wait till it breaks** and try to fix it.

If you want to know if I authored it, you can look at all.net where I keep copies of most of it. I also keep redundant copies and backups, and of course while I am alive, you can invite me to come and attest to it. I do all of these for different situations, and likely so should you.

## Conclusions

Attestation channels are increasingly available for the digital world. This ranges from DBOM (digital) and SBOM (software) bills of materials, to archival methods as they evolve over time, to narrative integrity techniques being increasingly and rapidly deployed in Canada as a World leader. And of course, keep reading the material at all.net and our other distribution channels for my self-attested views.