US 20240214390A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2024/0214390 A1

Smith et al. (43) Pub. Date: Jun. 27, 2024

(54) SUPPLY CHAIN ATTESTATION TRANSPARENCY AND AUTHORIZATION

(71) Applicant: **Intel Corporation**, Santa Clara, CA (US)

(72) Inventors: **Ned M. Smith**, Beaverton, OR (US); **Rajesh Poornachandran**, Portland, OR (US); **Sunil K. Cheruvu**, Tempe, AZ (US)

(73) Assignee: **Intel Corporation**, Santa Clara, CA (US)

(21) Appl. No.: **18/146,687**

(22) Filed: **Dec. 27, 2022**

Publication Classification

(51) **Int. Cl.**
H04L 9/40 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/126*** (2013.01); ***H04L 63/1416*** (2013.01)

(57) **ABSTRACT**

The technology described herein includes receiving a first reference integrity manifest (RIM) and a first proto-RIM from a first endorser, the first endorser asserting authority, by the first RIM and the first proto-RIM, to supply first attestation reference values for a computing device; storing the first proto-RIM in a RIM transparency database; notarizing the first proto-RIM; and providing the first RIM and the notarized first proto-RIM to a verifier of the computing device.