



(19) **United States**

(12) **Patent Application Publication**
Borgatti et al.

(10) **Pub. No.: US 2024/0214195 A1**

(43) **Pub. Date: Jun. 27, 2024**

(54) **SYSTEMS AND METHODS FOR
ENTANGLED AUTHENTICATION OF
BIOSENSORS AND BIOSENSOR OUTPUTS**

Publication Classification

(51) **Int. Cl.**
H04L 9/08 (2006.01)
G06F 21/32 (2006.01)
(52) **U.S. Cl.**
CPC **H04L 9/0866** (2013.01); **G06F 21/32**
(2013.01)

(71) Applicants: **HID Global Corp.**, Austin, TX (US);
HID Czech s.r.o., Prague (CZ); **HID**
Global Taiwan Ltd., Taipei (CN)

(72) Inventors: **Michele Borgatti**, Bologna (IT); **Vito**
Fabrizio, Berkeley, CA (US); **Marco**
Mancini, Prague (CZ)

(21) Appl. No.: **18/557,672**

(22) PCT Filed: **Apr. 29, 2022**

(86) PCT No.: **PCT/US2022/072007**

§ 371 (c)(1),

(2) Date: **Oct. 27, 2023**

Related U.S. Application Data

(60) Provisional application No. 63/201,463, filed on Apr.
30, 2021.

(57) **ABSTRACT**

Disclosed herein are systems and methods for entangled authentication of biometric sensors and biometric-sensor outputs. In an embodiment, a secure-biometric-sensor system includes a biometric sensor and a secure element physically bound to one another. The sensor is communicatively interposed between a host and the secure element. The sensor receives a cryptographic challenge from the host and forwards it to the secure element. The sensor captures a biometric reading and transmits it to the host. The sensor receives, from the secure element, a challenge response that includes a shared secret between the host and the secure element. The sensor generates a cryptographically entangled token from a predetermined combination of the shared secret and data specific to the captured biometric reading, and transmits the cryptographically entangled token to the host for use by the host in attempting to authenticate the biometric reading as having been captured by the sensor.

