(11) **EP 2 863 329 A8**

(12) CORRECTED EUROPEAN PATENT APPLICATION

(15) Correction information:

Corrected version no 1 (W1 A1)

Corrections, see

Bibliography INID code(s) 71

(48) Corrigendum issued on:

17.02.2016 Bulletin 2016/07

(43) Date of publication:

22.04.2015 Bulletin 2015/17

(21) Application number: 14186453.8

(22) Date of filing: 25.09.2014

(84) Designated Contracting States:

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated Extension States:

BA ME

(30) Priority: 21.10.2013 US 201314059442

(71) Applicant: Intel Corporation Santa Clara, CA 95054 (US) (51) Int Cl.:

G06F 21/44 (2013.01)

G06F 21/57 (2013.01)

(72) Inventors:

 Martin, Jason Beaverton, OR 97007 (US)

 Lal, Reshma Hillsboro, OR 97124 (US)

 Nemiroff, Daniel Folsom, CA 95630 (US)

(74) Representative: Hufton, David Alan

HGF Limited Fountain Precinct Balm Green

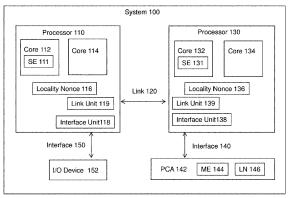
Sheffield S1 2JA (GB)

(54) Establishing physical locality between secure execution environments

(57) Embodiments of an invention for establishing physical locality between secure execution environments are disclosed. In one embodiment, a processor includes a storage location and an execution core. The storage location is to store a locality nonce. The execution core

is to execute a first instruction to create a secure execution environment. The execution core is also to execute, from within the secure execution environment, a second instruction to read the locality nonce from the storage location.

FIGURE 1



EP 2 863 329 A8