



(51) International Patent Classification:

H04L 9/06 (2006.01) *G06F 21/62* (2013.01)
G06F 21/00 (2013.01) *H04L 12/701* (2013.01)

(21) International Application Number:

PCT/CA2021/050531

(22) International Filing Date:

20 April 2021 (20.04.2021)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

16/871,371 11 May 2020 (11.05.2020) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:

US 16/871,371 (CON)
Filed on 11 May 2020 (11.05.2020)

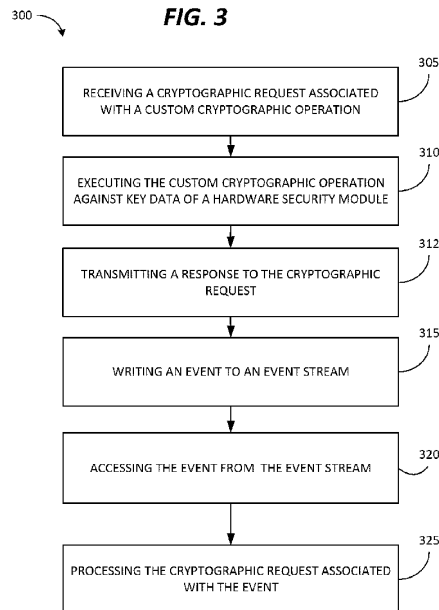
(71) Applicant: **MASTERCARD TECHNOLOGIES CANADA ULC** [CA/CA]; 475 Howe Street, 20th Floor, Vancouver, British Columbia V6C 2B3 (CA).

(72) Inventors: **FOX, Justin**; 405-11950 Harris Road, Pitt Meadows, British Columbia V3Y 0B7 (CA). **GRIMSON, Marc**; 108-1209 Jervis Street, Vancouver, British Columbia V6E 2C9 (CA).

(74) Agent: **BERESKIN & PARR LLP / S.E.N.C.R.L.**; Scotia Plaza, 40 King Street West, 40th Floor, Toronto, Ontario M5H 3Y2 (CA).

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO,

(54) Title: **HARDWARE SECURITY MODULE EXTENSION**



(57) **Abstract:** Systems and methods for providing a hardware security module extension having support for custom cryptographic operations. One system includes an application execution server providing an application execution environment. The application execution server is configured to receive a cryptographic request associated with a custom cryptographic operation and access key data from a hardware security module in response to receiving the cryptographic request. The application execution server is also configured to execute, within the application execution environment, the custom cryptographic operation against the key data from the hardware security module and transmit a response to the cryptographic request.

NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW,
SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))