US 20230231715A1

(19) United States
(12) Patent Application Publication
Le Saint et al.

(10) Pub. No.: US 2023/0231715 A1
(43) Pub. Date: Jul. 20, 2023

(54) METHODS FOR SECURE CRYPTOGRAM GENERATION

(71) Applicant: **Visa International Service Association**, San Francisco, CA (US)

(72) Inventors: **Eric Le Saint**, Los Altos, CA (US); **James Gordon**, Lafayette, CA (US); **Roopesh Joshi**, San Ramon, CA (US)

(73) Assignee: **Visa International Service Association**, San Francisco, CA (US)

(21) Appl. No.: **18/156,933**

(22) Filed: **Jan. 19, 2023**

Related U.S. Application Data

(63) Continuation of application No. 17/308,749, filed on May 5, 2021, now Pat. No. 11,588,637, which is a continuation of application No. 16/443,610, filed on Jun. 17, 2019, now Pat. No. 11,032,075, which is a continuation of application No. 15/723,001, filed on Oct. 2, 2017, now Pat. No. 10,389,533, which is a continuation of application No. 14/841,589, filed on Aug. 31, 2015, now Pat. No. 9,813,245.

(60) Provisional application No. 62/044,172, filed on Aug. 29, 2014.

Publication Classification

(51) **Int. Cl.**

H04L 9/32	(2006.01)
H04L 9/08	(2006.01)
H04L 9/14	(2006.01)
H04L 9/40	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 9/321*** (2013.01); ***H04L 9/14*** (2013.01); ***H04L 9/0841*** (2013.01); ***H04L 9/0861*** (2013.01); ***H04L 9/0891*** (2013.01); ***H04L 63/061*** (2013.01)

(57) ABSTRACT

A computer-implemented method performed by a user device is provided. The computer-implemented method includes receiving a message including an encrypted credential from a server computer; determining a response shared secret using a private key and a server public key; decrypting the encrypted credential using the response shared secret to determine a credential; obtaining a key derivation parameter from the credential; determining a first cryptogram key using the key derivation parameter; generating a first cryptogram using the first cryptogram key; and sending the first cryptogram to a second computer.