US 20230231714A1

(19) **United States**

(12) **Patent Application Publication**

GERMOUTY

(10) **Pub. No.: US 2023/0231714 A1**

(43) **Pub. Date: Jul. 20, 2023**

(54) **METHOD AND SYSTEM FOR A VERIFIABLE IDENTITY BASED ENCRYPTION (VIBE) USING CERTIFICATE-LESS AUTHENTICATION ENCRYPTION (CLAE)**

(71) Applicant: **VIBE Cybersecurity Inc.**, Panama City (PA)

(72) Inventor: **Paul GERMOUTY**, Limoges (FR)

(21) Appl. No.: **18/002,492**

(22) PCT Filed: **Jul. 7, 2020**

(86) PCT No.: **PCT/IB2020/000499**

§ 371 (c)(1),
(2) Date: **Dec. 20, 2022**

Publication Classification

(51) **Int. Cl.**

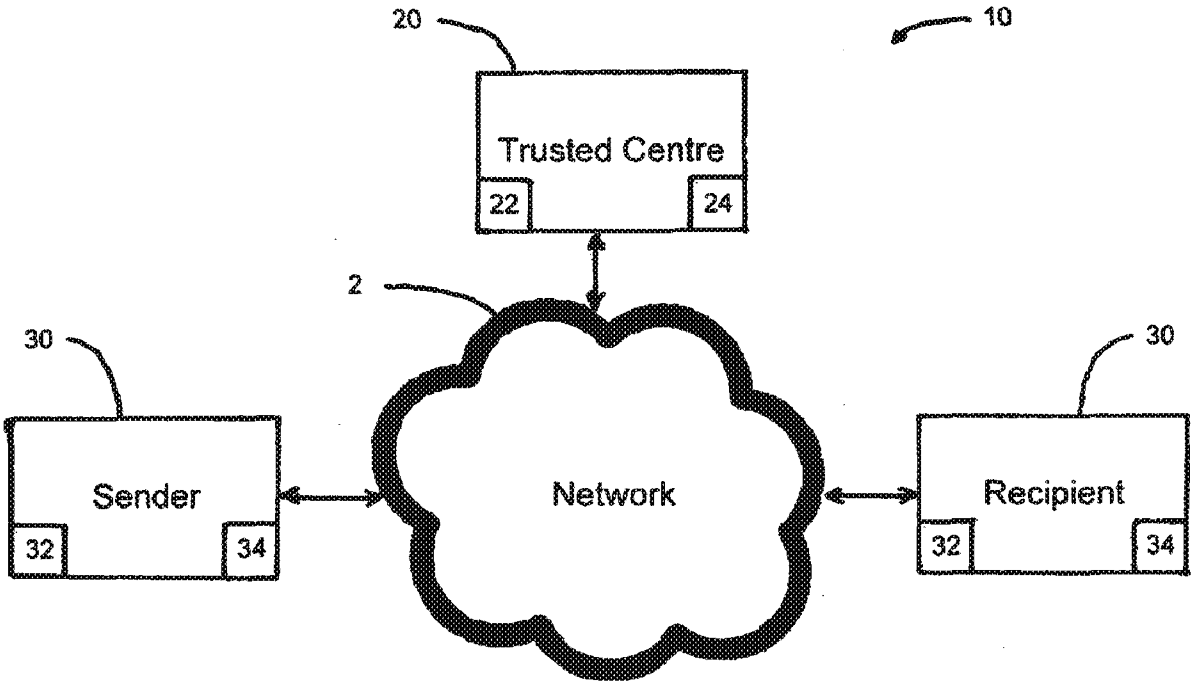
H04L 9/32	(2006.01)
H04L 9/00	(2006.01)
H04L 9/06	(2006.01)
H04L 9/30	(2006.01)

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

CPC ***H04L 9/321*** (2013.01); ***H04L 9/006*** (2013.01); ***H04L 9/0618*** (2013.01); ***H04L 9/3073*** (2013.01); ***H04L 9/0643*** (2013.01)

(57) **ABSTRACT**

Solutions of verifying a plurality of public parameters from a Trusted Centre (TC) in an identity-based encryption and signature system prior to encrypting a plaintext message by a sender having a sender identity string. The method may include identification of the Trusted Centre by a TC identity string, the Trusted Centre having a master public encryption key based on the TC identity string; determination if the sender has a sender private key and the public parameters for the Trusted Centre including the master public key of the Trusted Centre and a bilinear map; and verification of the public parameters using the TC identity string prior to encrypting the plaintext message into a ciphertext by comparing values of the bilinear map calculated with variables comprising the sender private key and the master public key. The ciphertext may include an authentication component for authenticating the sender once the ciphertext is received and decrypted by the recipient using the identity string of the sender and the private key of the recipient. Enables a signature scheme from the same parameters and private keys, the signature is forged using the private key of the signer, the message and the public parameters, the verification is done using the public parameters, the identity of the signer, the signature and the message.


20
10
Trusted Centre
22
24
2
30
30
Sender
32
34
Network
Recipient
32
34