US011115395B2

(12) **United States Patent**
Kurdziel et al.

(10) **Patent No.: US 11,115,395 B2**
(45) **Date of Patent: Sep. 7, 2021**

(54) **CROSS-DOMAIN INFORMATION TRANSFER SYSTEM AND ASSOCIATED METHODS**

(71) Applicant: **HARRIS GLOBAL COMMUNICATIONS, INC.**, Albany, NY (US)

(72) Inventors: **Michael T. Kurdziel**, Rochester, NY (US); **Steven M. Farris**, Webster, NY (US); **Peter Bajorski**, Fairport, NY (US); **Alan R. Kaminsky**, Rochester, NY (US); **Marcin Lukowiak**, Rochester, NY (US); **Stanislaw P. Radziszowski**, West Henrietta, NY (US)

(73) Assignee: **HARRIS GLOBAL COMMUNICATIONS, INC.**, Albany, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 54 days.

(21) Appl. No.: **16/519,098**

(22) Filed: **Jul. 23, 2019**

(65) **Prior Publication Data**

US 2021/0029097 A1 Jan. 28, 2021

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 9/06 (2006.01)
(Continued)

(52) **U.S. Cl.**
CPC ***H04L 63/0442*** (2013.01); ***H04L 9/0631*** (2013.01); ***H04L 9/083*** (2013.01); ***H04L 9/088*** (2013.01); ***H04L 9/3252*** (2013.01)

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

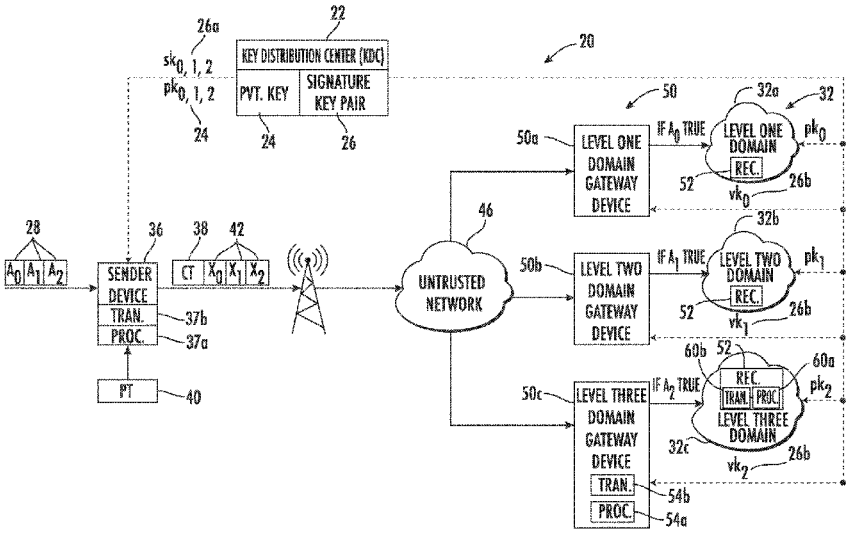
5,481,613 A 1/1996 Ford et al.
8,634,563 B2 1/2014 Vaikuntanathan et al.
(Continued)

OTHER PUBLICATIONS

Kent, "IP encapsulating security payload (ESP)", The Internet Society, Dec. 2005, pp. 1-44.
(Continued)

Primary Examiner — Eleni A Shiferaw
Assistant Examiner — Bassam A Noaman
(74) *Attorney, Agent, or Firm* — Allen, Dyer, Doppelt + Gilchrist, P.A. Attorneys at Law

(57) **ABSTRACT**

A cross-domain information transfer system includes a key distribution center that generates private encryption keys and a signature key pair as a secret signing and secret verifying key for an attribute associated with a given domain. A sender device generates ciphertext from plaintext based upon the private encryption key, appends an attribute for a given domain to the ciphertext, generates ciphertext with a concealed attribute based upon the secret signing key and broadcasts the ciphertext with the concealed attribute. Domain gateway devices each receive a respective secret verifying key for an associated attribute, receive the ciphertext with the concealed attribute from the untrusted network, and use the secret verifying key to determine if the concealed attribute matches the attribute associated with the domain gateway device, and, when so, pass the ciphertext to at least one receiver device coupled with the domain gateway device.

12 Claims, 5 Drawing Sheets