

System and methods for uicc-based secure communication US 20150222631 A1

Walter Cooper Chastain, Stephen Emille Chin

ABSTRACT

A system that incorporates the subject disclosure may include instructions which when executed cause a device processor to perform operations comprising sending a service request to a remote management server; receiving from the management server an authentication management function and an encryption key generator for execution by a secure element and an encryption engine for execution by a secure device processor, sending a request to establish a communication session with a remote device; and communicating with the remote device via a channel established using an application server. The secure element and the secure device processor authenticate each other using a mutual authentication keyset. The secure element, the secure device processor and the device processor each have a security level associated therewith; the security level associated with the secure device processor is intermediate between that of the secure element and that of the device processor. Other embodiments are disclosed.

Reference

- 1 ["3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Characteristics of the Universal Subscriber Identity Module \(USIM\) application"](#), Release 11, 2012.
- 2 ["3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Remote APDU Structure for \(U\)SIM Toolkit applications"](#), Release 10, 2012.
- 3 ["3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Secured packet structure for \(Universal\) Subscriber Identity Module \(U\)SIM Toolkit applications"](#), Release 10, 2012.
- 4 ["3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; UICC-terminal interface; Physical and logical characteristics"](#), Release 10, 2011.
- 5 ["3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Universal Subscriber Identity Module \(USIM\) Application Toolkit \(USAT\)"](#), Release 11, 2012.
- 6 ["GlobalPlatform Card Confidential Card Content Management Card Specification v2.2-Amendment A"](#), 2011.
- 7 ["GlobalPlatform Card Contactless Services Card Specification v2.2-Amendment C"](#), 2012.
- 8 ["GlobalPlatform Card Remote Application Management over HTTP Card Specification v2.2-Amendment B"](#), 2012.
- 9 ["GlobalPlatform Card Security Upgrade for Card Content Management Card Specification v 2.2-Amendment E"](#), 2011.
- 10 ["GlobalPlatform Card Specification"](#), Version 2.2.1, 2011.
- 11 ["GlobalPlatform Card Technology Secure Channel Protocol 03 Card Specification v 2.2-Amendment D"](#), 2009.
- 12 ["GlobalPlatform Device Secure Element Remote Application Management"](#), May 2011.

Reference

- 13 ["GlobalPlatform Device Technology Secure Element Access Control"](#), Version 1.0, May 2012.
- 14 ["GlobalPlatform Device Technology TEE System Architecture"](#), Dec. 2011.
- 15 ["GlobalPlatform Key Management System"](#), Functional Requirements, Nov. 2003.
- 16 ["GlobalPlatform System Messaging Specification for Management of Mobile-NFC Services"](#), Feb. 2011.
- 17 ["Over-The-Air Platform Security Review"](#), Mandiant Intelligent Information Security, 6 pgs., Aug. 17, 2010.
- 18 Farhat, Farshid, Somayeh Salimi, and Ahmad Salahi. ["Private Identification, Authentication and Key Agreement Protocol with Security Mode Setup"](#) IACR Cryptology ePrint Archive 2011 (2011): 45.
- 19 ["Reprogrammable SIMs: Technology, Evolution and Implications"](#), csmg, Sep. 25, 2012.
- 20 ["Secure Authentication for Mobile Internet Services"](#)-Sim Alliance, Dec. 2011 <http://simalliance.org/wp-content/uploads/2015/03/12-01-01-WP-SIMAllianceSecureAuthentication-EN-V1.1.pdf>.
- 21 ["Smart Cards; Card Application Toolkit \(CAT\)"](#), Release 11, 2012.
- 22 ["Smart Cards; ETSI numbering system for telecommunication application providers"](#), Release 11, 2011.
- 23 ["Smart Cards; Machine to Machine UICC; Physical and logical characteristics"](#), Release 9, 2011.
- 24 ["Smart Cards; Remote APDU structure for UICC based applications"](#), Release 11, 2012.
- 25 ["Smart Cards; Secured packet structure for UICC based applications"](#), Release 11, 2012.
- 26 ["Smart Cards; Security mechanisms for UICC based Applications-Functional requirements"](#), Release 8, 2008.
- 27 ["Smart Cards; UICC Application Programming Interface \(UICC API\) for Java Card\(TM\)"](#), Release 9, 2012.
- 28 ["Smart Cards; UICC Application Programming Interface \(UICC API\) for Java Card™"](#), Release 9, 2012.
- 29 ["Smart Cards; UICC-Terminal Interface; Physical and logical characteristics"](#), Release 10, 2011, 179 pages.
- 30 ["The OTA Platform in the World of LTE"](#), 14 pgs., Jan. 2011.
- 31 ["Universal Mobile Telecommunications System \(UMTS\); UICC-terminal interface; Physical and logical characteristics"](#), Release 10, 2011.
- 32 Chen, ["An efficient end-to-end security mechanism for IP multimedia subsystem"](#), Computer Communications, 2008, vol. 31.18, pp. 4259-4268.
- 33 Dodson, Ben et al., ["Snap2Pass: Consumer-Friendly Challenge-Response Authentication with a Phone"](#), <http://prpl.stanford.edu/papers/soups10j.pdf>, Apr. 30, 2010.
- 34 Global Platform, ["Secure Element Remote Application Management"](#), Version 1.0, May 2011.

Reference

-
- 35 Imhontu, et al., "[A survey on near field communication in mobile phones & PDAs](#)", Dissertation Halmstad University, 2010. <http://hh.diva-portal.org/smash/get/diva2:385433/FULLTEXT01>.
-
- 36 Kim, Jong-Min et al., "[A Study of Coupons issuance System Considering of User Convenience Based on NFC](#)", 3rd International Conference on Computer Science and Information Technology (ICCSIT'2013) Jan. 4-5, 2013 Bali (Indonesia). <http://pscentre.org/images/extraimages/113118.pdf>.
-
- 37 Kounelis, Ioannis et al., "[Secure Middleware for Mobile Phones and UICC Applications](#)", Mobile Wireless Middleware, Operating Systems, and Applications, Springer Berlin Heidelberg, 2012, 143-152.
-
- 38 Kounelis, Ioannis et al., "[Security of service requests for cloud based m-commerce](#)", MIPRO, 2012 Proceedings of the 35th International Convention, IEEE, 2012.
-
- 39 Meyerstein, et al., "[Security Aspects of Smart Cards vs. Embedded Security in Machine-to-Machine \(M2M\) Advanced Mobile Network Applications](#)", InterDigital Communications Corporation LLC, First International ICST Conference: MobiSec 2009, Security and Privacy in Mobile Information and Communication Systems, p. 214-225, Jun. 3-5, 2009.
-
- 40 Nagalakshmi, et al., "[Modified Protocols for Internet Key Exchange \(IKE\) Using Public Encryption and Signature Keys](#)", Information Technology: New Generations (ITNG), 2011 Eighth International Conference on, 2011, pp. 376, 381.
-
- 41 Zhang, et al., "[Cryptographic Key Agreement Protocol Simulation](#)", Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on, 2010, pp. 418, 419.
-

[System and methods for UICC-based secure communication](#)

[SYSTEM AND METHODS FOR UICC-BASED SECURE COMMUNICATION 20150222631](#)

[System and methods for UICC-based secure communication US 9461993 B2](#)

[System and methods for uicc-based secure communication US 20150222631 A1](#)