**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

---

**BEFORE THE PATENT TRIAL AND APPEAL BOARD**

---

ERICSSON INC.,

Petitioner,

v.

KONINKLIJKE KPN N.V.,

Patent Owner.

---

Case No. IPR2023-00902

Patent 9,438,572

---

# DECLARATION OF DR. ANGELOS KEROMYTIS IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 9,438,572

# TABLE OF CONTENTS

**Page**


**LIST OF EXHIBITS AND APPENDICES** ..... **vi**

**I. INTRODUCTION** ..... **1**

**II. SUMMARY OF OPINIONS** ..... **2**

**III. QUALIFICATIONS AND EXPERIENCE** ..... **2**

A. Education and Work Experience ..... 2

B. Compensation ..... 9

C. Documents and Other Materials Relied Upon ..... 9

**IV. STATEMENT OF LEGAL PRINCIPLES** ..... **10**

A. Claim Construction ..... 10

B. Anticipation ..... 11

C. Obviousness ..... 11

**V. TECHNOLOGY BACKGROUND OF THE '572 Patent** ..... **13**

A. A Brief History of Cryptography ..... 14

**VI. OVERVIEW OF THE '572 PATENT** ..... **24**

A. Prosecution History ..... 27

B. The '572 Patent Claims ..... 29

C. Priority Date ..... 33

D. Claim Construction ..... 34

**VII. LEVEL OF ORDINARY SKILL IN THE ART** ..... **34**

**VIII. IDENTIFICATION OF THE PRIOR ART AND SUMMARY OF OPINIONS** ..... **38**

A. Summary of WO 2012/112124 A1 ("*Teo*") ..... 38

B. Summary of U.S. Patent Application Publication No. 2013/0067552 ("*Hawkes*") ..... 47

C. Summary of RFC 4279 ..... 48

D. Summary of U.S. Patent Application Publication No. 2001/0019614 (*Madoukh*) ..... 50

**TABLE OF CONTENTS**
(continued)

**Page**


E. Summary of S3-070234 ....51

F. Summary of U.S. Patent Application Publication No. 2007/0171910 ("*Kumar*") ....52

G. Summary of U.S. Patent Application Publication No. 2009/0016524 ("*Park*") ....52

H. Summary of U.S. Patent Application Publication No. 2009/0181643 ("*Thakare*") ....53

I. A POSITA's Motivation to Combine *Teo* with *Madoukh* ....53

J. Reasonable Expectation of Success ....55

K. A POSITA's Motivation to Combine *Teo* with *Madoukh* and *Hawkes* ....55

L. Reasonable Expectation of Success ....58

M. **A POSITA's Motivation** to Combine *Teo* with *Madoukh* and RFC 4279 ....59

N. Reasonable Expectation of Success ....61

O. **A POSITA's Motivation** to Combine *Teo* with *Madoukh*, RFC 4279, and *Kumar* ....62

P. Reasonable Expectation of Success ....64

Q. **A POSITA's Motivation** to Combine *Teo* with *Madoukh* and S3-070234 ....65

R. Reasonable Expectation of Success ....66

S. **A POSITA's Motivation** to Combine *Teo* with *Madoukh* and *Thakare* ....67

T. Reasonable Expectation of Success ....68

**IX. UNPATENTABILITY OF THE '572 PATENT CLAIMS ....69**

A. Ground 1: Claims 1-2 and 14 are Unpatentable as they are Rendered Obvious by *Teo* in view of *Madoukh*. ....69

1. Claim 1 ....69

**TABLE OF CONTENTS**
(continued)

**Page**


2. Claim 2. Method according to claim 1, wherein the preloading the initiation key comprises providing the initiation key to each of the mobile devices via the mobile network when each respective mobile device is connected to the mobile network. ....94

3. Claim 14. Method according to claim 1, wherein the key agreement procedure comprises: a three-pass authentication procedure; or a use of the initiation key to encrypt a message exchange between the mobile devices for obtaining a shared secret, and a Diffie-Hellman key exchange procedure which is initiated based on the shared secret. ....95

B. Ground 2: Claims 3-5 and 15-17 are Unpatentable as they are Rendered Obvious by *Teo* in view of *Madoukh* and *Hawkes* ....98

1. Claim 3. Method according to claim 1, wherein the preloading the initiation key comprises storing the initiation key in a secure storage area of each respective mobile device. ....98

2. Claim 4. Method according to claim 3, wherein the secure storage area is provided by a trusted computing subsystem of each respective mobile device. ....100

3. Claim 5. Method according to claim 4, wherein at least one of the group of: verifying the validity of the initiation key, and using the initiation key in performing the key agreement procedure, is performed by the trusted computing subsystem. ....101

4. Claim 15 ....102

5. Claim 16 ....105

6. Claim 17 ....108

C. Ground 3: Claims 6-9 are Unpatentable as they are Rendered Obvious by *Teo* in view of *Madoukh* and RFC 4279 ....110

1. Claim 6. ....110

**TABLE OF CONTENTS**
(continued)

**Page**


2. Claim 7. ..... 114

3. Claim 8. Method according to claim 6, further comprising disabling or removing the initiation key from the set of initiation keys after use in establishing the D2D communication session. ..... 115

4. Claim 9. Method according to claim 6, wherein the set of validity periods is constituted at least in part by different but overlapping validity periods. ..... 117

D. Ground 4: Claim 10 is Unpatentable as it is Rendered Obvious by *Teo* in view of *Madoukh*, RFC 4279, and *Kumar* ..... 118

1. Claim 10. Method according to claim 1, wherein the initiation key is associated with a virtual network identity, and wherein the verifying the validity of the initiation key further comprises determining a match of the virtual network identity on each of the mobile devices via the D2D communication channel ..... 118

E. Ground 5: Claims 11-12 are are Unpatentable as they are Rendered Obvious by *Teo* in view of *Madoukh* and S3-070234 ..... 120

1. Claim 11. Method according to claim 1, wherein the initiation key is associated with a usage count for limiting a number of uses of the initiation key, and wherein the verifying the validity of the initiation key is further based on the usage count. ..... 120

2. Claim 12. Method according to claim 11, further comprising adjusting the usage count after use of the initiation key in establishing the D2D communication session. ..... 121

F. Ground 5: Claim 13 is Unpatentable as it is Rendered Obvious by *Teo* in view of *Madoukh* and *Thakare* ..... 122

1. Claim 13. Method according to claim 1, further comprising requesting a further initiation key via the mobile network if the key agreement procedure fails in providing the session key. ..... 122

**TABLE OF CONTENTS**
(continued)

**Page**

**X. CONCLUSION .....123**
**XI. DECLARATION .....123**



ERICSSON EXHIBIT 1003, Page 6

## LIST OF EXHIBITS AND APPENDICES

| Exhibit No.[1] | Description |
|---|---|
| **1001** | U.S. Patent No. 9,438,572 B2 ("the '572 Patent") |
| **1002** | Prosecution File History for the '572 Patent |
| **1005** | WO 2012/112124 A1 to *Teo* ("*Teo*") |
| **1006** | U.S. Patent Application Pub. No. 2013/0067552 to *Hawkes* ("*Hawkes*") |
| **1007** | RFC 4279 |
| **1008** | Claim Listing |
| **1009** | Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C," Wiley & Sons (Second Edition), 1996 |
| **1010** | Reserved |
| **1011** | U.S. Patent Application Pub. No. 2001/0019614 to Madoukh |
| **1012** | Reserved |
| **1013** | S3-070272, "Comments to 'Key Refresh in SAE/LTE'," 3GPP TSG SA WG3 Security – SA3#46b, 28-29, March, 2007 |
| **1014** | ETSI TS 133 110 v10.1.0 (2011-07) |
| **1015** | RFC 2409 |
| **1016** | U.S. Patent Application Pub. No. 2007/0171910 to Kumar ("*Kumar*") |
| **1017** | U.S. Patent Application Pub. No. 2009/0016524 to Park ("*Park*") |
| **1018** | U.S. Patent Application Pub. No. 2009/0181643 to Thakare ("*Thakare*") |
| **1019** | Declaration of Craig Bishop |
| **1020** | U.S. Patent No. 6,879,825 to Daly |
| **Appendix No.** | **Description** |
| **1** | https://datatracker.ietf.org/doc/rfc4279/history/ |
| **2** | Excerpts of https://www.rfc-editor.org/rfc-index.html |
| **3** | February 19, 2006 capture of http://www.rfc-editor.org/rfc/rfc4279.txt |

[1] Citations to patents are made by column and line cite; citations to patent publications are made by paragraph number; citations to Exhibit 1002 are made with reference to the Bates-stamped pagination; citations to other exhibits are made to the page number of the document itself.

I, Angelos Keromytis, Ph.D., hereby declare as follows:

## I. INTRODUCTION

1. I am currently a Professor, John H. Weitnauer Technology Transition Endowed Chair, and Georgia Research Alliance (GRA) Eminent Scholar at the Georgia Institute of Technology (Georgia Tech), and an elected Fellow of the Institute of Electrical and Electronics Engineers (IEEE) and the Association for Computing Machinery (ACM) for my contributions to cybersecurity.

2. I have been engaged by Petitioner to investigate and opine on certain issues relating to U.S. Patent No. 9,438,572 to Norp et al. (EX1001, "the '572 Patent").

3. I understand that the '572 Patent is assigned to Koninklijke KPN N.V. ("KPN"). KPN is also referred to as the "Patent Owner" in this document.

4. In this declaration, I will discuss the technology related to the '572 Patent, including an overview of that technology as it was known at the time of the earliest priority date claimed by the '572 Patent, which I have been informed is September 6, 2012. This overview of the technology provides some of the bases for my opinions with respect to the '572 Patent.

5. This declaration is based on the information currently available to me. To the extent that additional information becomes available, I reserve the right to continue my investigation and study.

6. In forming my opinions, I have relied on information and evidence identified in this declaration, including, without limitation, the '572 Patent, the prosecution history of the '572 Patent, and prior art including the references and other materials mentioned throughout my declaration below. I have also relied on my own experience and expertise in the technologies and systems that were already in use prior to September 6, 2012.

## II. SUMMARY OF OPINIONS

7. The '572 patent generally relates to "a method for establishing a device-to-device (D2D) communication session between mobile devices." *See* EX1001, 1:12-14. As I will discuss below in more detail, challenged claims 1-17 of the '572 Patent were not patentable as of the claimed priority date.

8. It is my opinion that challenged claims 1-17 are obvious in light of the prior art discussed below.

## III. QUALIFICATIONS AND EXPERIENCE

### A. Education and Work Experience

9. I have significant experience and familiarity with computer and network security, and have been working in this field since 1993.

10. I am currently a Professor, John H. Weitnauer Technology Transition Endowed Chair, and Georgia Research Alliance (GRA) Eminent Scholar at Georgia Tech. I am also an elected Fellow of both the Institute of Electrical and

Electronics Engineers (IEEE) and the Association for Computing Machinery (ACM), premier international professional organizations in the fields of engineering and computing, whose respective bylaws limit the number of Fellows to less than 1% of global membership. I received my M.Sc. and Ph.D. degrees in Computer Science, both from the University of Pennsylvania. My Ph.D. dissertation work was on the topic of secure access control for distributed systems and, in particular, on the management of trust in distributed computer networks.

11. I received my B.Sc. in Computer Science from the University of Crete, in Greece, in 1996. During my undergraduate studies, I worked as system administrator in the Computing Center at the University of Crete. Following that, I worked as network engineer at the first commercial Internet Service Provider (ISP) in Greece, FORTHnet SA, where I was exposed to many network security issues.

12. I have actively participated in the Internet Engineering Task Force (IETF), a standards-setting body for the Internet, since 1995. In the late 1990s and early 2000s, my work with the IETF was primarily within the Internet Protocol Security (IPsec) Working Group. In addition to contributing to the specification of the IPsec standards, I wrote the first implementation of the Photuris key management protocol (now RFC 2522). I also contributed to the first open-source implementation of the ISAKMP/IKE key management protocol (now RFC 2409), for the open-source BSD operating system, and developed the first such

implementation for the Linux operating system. My Linux implementation, named Pluto, was adopted by the Federal National Institute of Standards and Technology (NIST) in 1999. In addition, my implementation of IPsec for the open-source OpenBSD operating system is currently used by many companies and governments around the world, and serves as the basis for several commercial products that employ cryptographic communications. In 1999, I architected and implemented the first open-source framework for supporting hardware cryptographic accelerators. This framework is used in the open-source OpenBSD, NetBSD, FreeBSD, and Linux operating systems. My work in implementing firewalls and other cryptographic and network protocols has resulted in commercial systems and publications in refereed technical conferences and academic journals. I served as Working Group Secretary for the IETF IPsec Working Group (2003-2005) and as Security Area Advisor to the IETF at large (2003-2008).

13. I joined Columbia University in 2001, where I worked first as an Assistant and then (starting in 2005) as an Associate Professor of Computer Science. I received tenure in 2008. At Columbia, I founded the Network Security Lab (NSL) and worked with a large group of graduate and postgraduate students in the area of cybersecurity. My past students now work in this field as university professors, as technical researchers for research laboratories, or as engineers for telecommunications, software, and cybersecurity companies.

14. In 2013, I took a leave of absence from Columbia to serve as a Program Director at the National Science Foundation (NSF). My primary responsibility was with the Secure and Trustworthy Cyberspace (SaTC) program, which is the primary NSF source of funding for academic research in cybersecurity across the country. As a Program Director, I was responsible for coordination across the Government and for making funding decision pertaining to fundamental research projects on cybersecurity. I also helped create new initiatives, such as the Resilient Interdependent Infrastructure Processes and Systems (RIPS) program, the NSF/Intel Partnership on Cyber-Physical System Security and Privacy, and the Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) track within SaTC.

15. In 2014, I moved to the role of Program Manager with the Defense Advanced Research Projects Agency (DARPA), which is part of the Department of Defense. Over a period of 53 months, I conceived, launched, and managed 5 new major research programs in the area of cybersecurity; I also managed an additional 4 cybersecurity programs that were already in progress. The total budget of all programs and efforts I created or managed exceeds 500 million US dollars, and the work done under those programs has been (and is being) used by various elements of the Department of Defense, Intelligence Community, federal law enforcement, and other parts of the US Government and international partners, as well as private

companies and non-profits. For my work, I received the DARPA Superior Public Service Medal and other awards/tokens of recognition.

16. I have received federal, state, and corporate sponsorship to conduct cybersecurity research from the Department of Defense, the National Security Agency, the Defense Advanced Research Projects Agency , the National Science Foundation, the Department of Homeland Security, the Air Force, the Office for Naval Research, the Army Research Office, the Department of the Interior, the National Reconnaissance Office, New York State, Google, Intel, Cisco, and others. In my twenty two years as a professor, I have received over 78 million dollars to support my research in cybersecurity. I also regularly teach courses on cybersecurity, in addition to more general courses in computer science.

17. l have published over 300 technical papers in refereed journals, conferences, and workshops, all of which are directed to various areas of cybersecurity. I have authored or coauthored three books, and contributed chapters for many other books that relate to cybersecurity. Between 1999 and 2010, I drafted or co-drafted seven standards documents that were published as Internet Request for Comments (RFCs). Several of these RFCs are directly related to network security. For example, RFC 6042 relates to transport layer security; RFC 5708, RFC 2792, and RFC 2704 relate to key signature and encoding for trust management; and RFC 3586 relates to IP security policy requirements.

Additionally, I am a co-inventor on 61 issued U.S. patents. Most of these patents are related to network and systems security.

18. I have chaired several international technical conferences and workshops in cybersecurity, including, for example, the International Conference on Financial Cryptography and Data Security (FC), USENIX Security Symposium, ACM Computer and Communication Security (CCS), and the New Security Paradigms Workshop (NSPW). I have also served in over 100 technical program committees for such events. From 2004-2010, I served as Associate Editor tor the premier technical journal on cybersecurity-the ACM Transactions on Information and Systems Security (TISSEC). Additionally, I have served on several advisory workshops to the United States Government on cybersecurity, including, among others, the Office of the Director of National Intelligence (ODNI)/National Security Agency (NSA) Invitational Workshop on Computational Cybersecurity in Compromised Environments (C3E) (several times between 2011 and 2022), the Office of Naval Research (ONR) Workshop on Host Computer Security (2010), the Intelligence Community Technical Exchange on Moving Target (2010), Lockheed Martin Future Security Threats Workshop (2009), and the ARO/FSTC Workshop on AI for Security and Security for AI (2023). In 2022, I co-chaired the US Open-Source Security Initiative Workshop, organized by the Office of Management and the Budget (OMB), the National Science Foundation, and the

National Institute for Standards and Technology (NIST). In 2020-2021, I served on the Georgia Secretary of State's Bipartisan Task Force for Safe, Secure, and Accessible Elections.

19. In addition to this work, I have cofounded four companies in cybersecurity. One company, StackSafe Inc. (formerly Revive Systems Inc.), was a provider of a virtualized preproduction staging environment that includes automated testing, analysis, and reporting tor IT operations teams. I was with this company from its founding in 2005 until 2009. The second company, Allure Security Technologies (founded in 2010), develops deception-based solutions for detecting and mitigating the malicious cyber-insider threat, commercializing technology developed at Columbia University with support from DHS and DARPA grants and a DARPA SBIR contract. The third company, Voreas Laboratories Incorporated (founded in 2018), provides cybersecurity services focused on threat detection and attribution via network analytics. The fourth company, Aether Argus Incorporated (founded in 2019), is developing technology for ensuring supply chain security and enabling runtime attestation for embedded and critical infrastructure devices using unintended electromagnetic emissions. I am currently serving as President and CEO for both Voreas Laboratories and Aether Argus.

20. Because of my background, training, and experience, I am qualified as an expert to explain the background of the technology encompassed by the '572 Patent as well as to opine on the validity of the claims of the '572 Patent in view of the prior art references discussed herein.

21. My curriculum vitae, which is attached to this declaration as Exhibit 1004, provides more details on my background and technical qualifications.

### B. Compensation

22. I am being compensated for the services I am providing in connection with this petition for *inter partes* review of the '572 Patent at the rate of $600 per hour. The compensation is not contingent upon my performance, the outcome of these *inter partes* review proceeding, or any other proceeding, or any issues involved in or related to the *inter partes* review.

### C. Documents and Other Materials Relied Upon

23. The documents on which I rely for the opinions expressed in this declaration are referenced in the section entitled LIST OF EXHIBITS AND APPENDICES above. I also rely on any other references specifically identified in this declaration, in their entirety, even if only portions of these documents are discussed here in an exemplary fashion.

# IV. STATEMENT OF LEGAL PRINCIPLES

## A. Claim Construction

24. I have been informed that in an IPR proceeding, the challenged claims are generally given their ordinary and customary meaning in view of the specification and the prosecution history as it would have been understood by one of ordinary skill in the art at the time of the alleged invention.

25. I also understand that the claims should be construed consistent with the patent's intrinsic record, which includes the patent itself as well as the patent's prosecution history.

26. Moreover, I understand that extrinsic evidence (including, for example, technical dictionaries and treatises) may shed light on the meaning claim terms would have to one of ordinary skill in the art. I also understand that, where extrinsic evidence conflicts with the intrinsic record, the intrinsic record governs the meaning of claim terms.

27. Further, I understand that conditional language in an apparatus claim does not render the claim indefinite because the structural elements that carry out conditional steps remain present regardless of whether or not the conditions for carrying out the step(s) is (are) met.

### B. Anticipation

28. I have been informed that a patent claim is invalid if it is anticipated by prior art. I have been informed that anticipation requires a finding that a single prior art reference discloses each limitation of a claim as the limitations are arranged in the claim. I have been informed that a prior art reference's disclosures may be express or inherent. I have been informed that a limitation is inherently disclosed by a prior art reference if the reference necessarily includes the limitation in question.

### C. Obviousness

29. I have also been informed that obviousness is a basis for invalidity of a patent. Specifically, I understand that where a prior art reference discloses less than all of the limitations of a given patent claim, that patent claim is invalid if the differences between the claimed subject matter and the prior art reference are such that the claimed subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the relevant art. Obviousness can be based on a single prior art reference or a combination of references that teach all limitations of the claimed invention.

30. I have been informed that a claim is not obvious merely because each limitation was independently known in the prior art. I also have been informed

that hindsight reasoning is not an appropriate basis for combining references to form an obviousness combination.

31. I understand that obviousness is not driven by a rigid formula, but is instead a flexible inquiry that reflects the fact that a person of ordinary skill in the art exercising ordinary creativity may find a variety of reasons to combine the teachings of different references. I understand that a non-exclusive list of possible factors that may give a person of ordinary skill in the art a reason to combine references includes any one or more of the following:

- Whether combining elements according to known methods yields predictable results;
- Whether simple substitution of known elements obtains predictable results;
- How use of known techniques improves similar methods in the same way;
- Whether applying known techniques to known methods ready for improvement yields predictable results;
- Whether one can choose from a finite number of identified, predictable solutions, with a reasonable expectation of success;

- How known work in one field of endeavor prompts variations for use in the same field; and
- Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to combine prior art reference teachings to arrive at the claimed invention.

32. I have been informed that obviousness also requires that the combination could have been made with a reasonable expectation of success. I have been informed that absolute predictability is not required; however, at least some degree of predictability is required. I have been informed that predictability is determined at the time the invention was made.

## V. TECHNOLOGY BACKGROUND OF THE '572 PATENT

33. I have been asked to provide some context to the technology related to the '572 Patent and the prior art. I understand that the relevant timeframe is September 6, 2012, and below I provide background on how the various technologies were developed and operating up to that time frame.[2]

[2] This technology background is intended to provide an introduction to the technology covered by the '572 Patent. My shortened explanations to introduce these concepts for purposes of understanding the claims of the '572 Patent and the prior art discussed in this Declaration are not intended to, and do not, provide a complete explanation of this technology.

### A. A Brief History of Cryptography

34. In modern telecommunications and computer networks, security of communications is primarily ensured through the use of cryptographic algorithms (such as Advanced Encryption Standard (AES), hash-based message authentication code (HMAC), and Rivet-Shamir-Adleman (RSA)), and the security protocols (such as Secure Socket Layer (SSL)/Transport Layer Security (TLS) and IPsec) that use these algorithms as building blocks.

35. One of the fundamental concepts behind modern cryptography, referred to as Kerckhoff's Principle, is that a cryptosystem (*e.g.*, cryptographic algorithm) should be secure even if everything about the system, except the cryptographic key, is public knowledge (including to potential attackers). Cryptographic keys are meant to be relatively long and chosen as randomly as possible, such that an attacker cannot simply try to guess the correct key by trial-and-error (which is also referred to as brute force search). Modern cryptographic algorithms are designed to be secure against a large and ever-evolving set of cryptanalytic attacks, under an assumption that the only piece of information an attacker does not know is the cryptographic key(s) used.

36. While there exist many types of cryptographic algorithms, the ones most relevant to the matter at issue relate to encryption and integrity protection.

37. In simple terms, encryption algorithms use an encryption key to transform data (often referred to as "plaintext") into a form (called "ciphertext") that is unintelligible to an attacker or anyone who does not possess a corresponding decryption key. EX1009, 1. The data can be a file, a packet, or most any other type of data. Algorithms where the encryption key and the decryption key are the same are referred to as symmetric encryption or, more simply, "secret key" encryption algorithms. *Id*., 4. An example of such algorithm is AES, which is a US Federal Standard and widely used worldwide, including by protocols such as SSL/TLS and IPsec. In the context of network communications, the challenge in the use of such algorithms is to ensure that two users or computers that wish to communicate can both possess the same secret key, without an attacker being able to get ahold of it. Further in the context of securing network communications, an attacker may not be able to view the contents of said encrypted communications, but they may be able to modify the ciphertext before it is received by the intended recipient. Absent any other measures, such as message integrity codes discussed below, this would cause the message plaintext as decrypted by the recipient to be garbled, albeit largely in uncontrolled/unpredicted (by the attacker) ways. Because this can cause unexpected problems, most network security protocols that provide data encryption also use integrity protection.

38. Algorithms where the encryption and decryption keys are different (but typically interdependent through complex mathematical relationships) are referred to as asymmetric encryption algorithms; the subset of these algorithms where the encryption key can be publicly released to anyone without endangering the secrecy of the corresponding decryption key are referred to as "public key" encryption algorithms. *Id*., 4-5. An example of such a public key encryption algorithm is RSA, which can be used by anyone who knows a recipient's public key to encrypt a message such that only the recipient (who holds the corresponding private key used for decryption) can decrypt the encrypted message ciphertext. Note that in this case, not even the sender can decrypt the ciphertext they generated.

39. Integrity protection algorithms (sometimes informally also referred to as "authentication algorithms") use an integrity protection key (which, confusingly, is sometimes also informally referred to as an encryption key, even though no encryption may actually be taking place) to compute a secure summary, often referred to as a "digest," "integrity code," or "authentication code," of a piece of data (such as a message that will be transmitted over the network). *Id*., 30-31. Anyone with a corresponding integrity verification key can then verify this digest or authentication code and have a cryptographic assurance that the data (and the digest) have not been modified by someone not in possession of the integrity

protection key. *Id*. Where the integrity protection key and the integrity verification key are the same, we have symmetric key message digests; these are the most common way of protecting large volumes of data and in time-sensitive applications, *e.g.*, protecting network communications using SSL/TLS and IPsec. Where the integrity protection key and the integrity verification key are different, and where the verification key can be released publicly, we have a digital signature algorithm: the holder of the integrity protection key ("private key") can "sign" a piece of data that anyone can verify using the corresponding public key. The RSA algorithm can be and is used in this fashion in a number of settings, including in SSL/TLS, IPsec, and secure email. Note that there exist digital signature algorithms that are designed so they cannot be used for encryption (*e.g.,* the DSA algorithm).

40. A relevant concept is that of a hash function. In computer science, hash functions are functions that take inputs of arbitrary length and produce fixed-size outputs. Inherent in this definition is the fact that there are many (possibly infinite) inputs that will produce the same output. While hash functions have several uses and accordingly differing requirements, cry*ptographic hash functions* have several important properties. First, they are designed so it is difficult given a specific output (usually called "digest") to find the input that produced it; in fact, they are designed to make it difficult to find *any* input that produces that specific

digest. *See* EX1009, 30-31. More generally, cryptographic hash functions are designed to make it difficult (the proper term is "computationally intractable or infeasible") to produce a specific output, except by trial-and-error (also referred to as brute force search). Examples of cryptographic hash functions include MD5, SHA256, and SHA512. Typical output (digest) sizes for cryptographic hash functions are 128, 256, and 512 bits; this means that one would expect (absent some cryptanalytic attack against the algorithm) to try respectively $2^{128}$, $2^{256}$, or $2^{512}$ different potential inputs to produce desired digest, making such an undertaking latter effectively impossible with current technology. Another property of a good cryptographic function is that an arbitrary change of even a single bit in the input data should produce drastic and "unpredictable" (*i.e.,* not computable without actually running the hash function over the modified input data) in the digest output. *Id*. Because of these properties, cryptographic hash functions serve many roles in computer and network security, including for computing digests of data transmitted over the network in conjunction with a cryptographic key.

41. In the context of network security, message (*e.g.*, packet) integrity using symmetric key digests is typically implemented by a sender computing the digest using an algorithm such as the SHA256 cryptographic hash function over a pre-agreed upon arrangement of the data to be protected and the integrity protection key. A simple example for denoting this is as:

MAC = SHA256(K, Data)

where MAC is the "Message Authentication Code" digest produced by the application of the SHA256 algorithm on the key K and the Data. *See id*., 30-31, 455-456. A more detailed example would be

$$MAC = HMAC\text{-}SHA256_K(Data\ Field\ 1 \mid Data\ Field\ 2 \mid \ldots \mid Data\ Field\ N)$$

which indicates that the MAC is produced by using the HMAC-SHA256 algorithm (which uses SHA256 in a particular structure) and the key K over the concatenation of distinct data objects. The sender would then transmit the data and the MAC to the recipient. Note that encryption may or may not be used, depending on the needs to protect the confidentiality of the data; in most modern security protocols, encryption and message integrity are used together. In the simplest scenario, the data and the MAC are transmitted unencrypted, which means that an attacker can also view them. Upon receipt, the receiver that holds the same key K can compute the same digest over the data received and compare their computed MAC value with the received MAC. *Id*. If the two are identical, then they can be confident that an attacker did not tamper with the contents of the message or the received MAC. *Id*. Had an attacker done so, the computed and the received MACs would not match. *Id*. Furthermore, because an attacker does not know the key K, they should not be able to modify the transmitted data and compute a valid substitute MAC for the modified data.

42. From a practical viewpoint, it is not possible to establish symmetric secret keys between any two pairs of devices that might want to communicate at some point in the future, as the number of such keys would be equal to the square of the number of devices. As a contrived example, each human being would need to prearrange (and maintain the security of) a secret key with each other human being; since there are approximately 8,000,000,000 humans on the planet, we would need a total of 64,000,000,000,000,000,000 (64 quintillion) secret keys in total; the situation becomes even less practical when we are considering computers and other digital devices. Although at first glance public key algorithms would appear to address this issue, other challenges arise (*e.g.*, ensuring the veracity of the association of an identity to a public key, or the significantly worse performance of public key algorithms compared to symmetric key algorithms that makes them unsuitable for encrypting large amounts of data or for time-sensitive applications).

43. Furthermore, prudent cryptographic engineering seeks to limit the amount of data encrypted or integrity-protected with any given key, so as to minimize the amount of material (*e.g.*, ciphertexts, or even plaintext/ciphertext pairs) that an attacker may have collected by eavesdropping or by compromising one of the endpoints, to make cryptanalytic attacks harder. EX1009, 183-184. Thus, it is common practice, as we discuss below, to establish encryption keys as

needed, and to limit their use as much as possible. Such temporary encryption or integrity-protection keys are often referred to as "session keys", because they are used only in the context of a communication session (*e.g.*, some well-defined period of time, or a specific number of packets or messages exchanged between the two parties). *See, e.g., id.*, 33-34. The definition of "session" is typically tied to the underlying network communication protocol(s) and is used rather flexibly by those skilled in the art, yet typically implying some notion of limited use.

44. When both encryption and integrity protection are used in the same protocol, it is common cryptographic practice to use different session keys for the encryption and integrity protection, to avoid certain types of potential cryptanalytic attacks. For the same reasons, different session keys may also be used in the different directions of the communication. Thus, a particular communication (*e.g.*, a bidirectional network connection) between two hosts may employ a total of four keys for data protection, *i.e.*, two in each direction, one each for encryption and integrity protection. One common way to do so is to somehow (discussed below) establish a "master" or "pre-master" session key, and to derive session subkeys for specific uses using an agreed-upon process, which is typically defined as part of the security protocol specification. As specific examples, both SSL/TLS and IPsec follow this process.

45. As discussed above, both practicalities and prudent cryptographic engineering dictate the use of some mechanism for establishing limited-use cryptographic keys (*i.e.*, session keys) between two networked entities that may not have previously communicated. As it pertains to the subject matter at hand, we will constrain our conversation to the situation where only symmetric key cryptography is used. In this scenario, for two parties to be able to securely establish session keys to protect their communications, they need the help of a mutually trusted third party (TTP). The TTP must be axiomatically trusted because it has knowledge and control of all cryptographic material and can impersonate any entity in the system (which also means it can ultimately decrypt all messages and forge arbitrary messages to any entity). Such TTPs, also sometimes referred to as Key Distribution Centers (KDCs) as in the case of the widely used Kerberos protocol, are implemented as secure servers with which each authorized network entity (user, computer, *etc*.) shares a "long term" secret key. *See, e.g.*, EX1009, 47-48, 566. The KDC is then used to "make introductions" between the two parties that wish to communicate, typically also assisting in the process of establishing a session key between them. The parties can then use the session key as-is or can use it to negotiate/establish session subkeys, as discussed earlier or as done in Kerberos.

46. Other relevant considerations that come in play in the context of network security involve entity authentication and liveness.

47. Entity authentication refers to the assurance of one entity in a secure communication that their correspondent is really who they believe and intend to communicate with. This is typically reduced to one entity proving to the other that it is the holder of a cryptographic key only they could know. For example, if a KDC is used to distribute session keys to two communicating parties, then, after this session key distribution has occurred, each party could generate a message digest over some arbitrarily chosen piece of data using the just-received session key and send it to the other party. Correct verification of the received message digest would imply that the sender (*i.e.*, corresponding party) is the intended communication peer, because only they could have generated the message and corresponding digest. *See id*., 30-31. Inherent in entity authentication is typically some type of entity identification, whether that is done by network address (*e.g.*, an IP address) or through some other type of identifier (*e.g.*, a domain name, a username, or even a random sequence of bits such as a Universally Unique Identifier, or UUID).

48. However, an attacker could have recorded a previous message exchange and tried to replay messages from it, in order to convince one of the parties that the other is present and wishing to communicate. Aside from relying on

the randomness of the selected session key(s), some of the techniques used include relying on a notion of a synchronized time (wherein all entities are assumed to know what the current time is, within some tolerances) and/or to include in the message digest computation some random data that was contributed by both parties, and to check that said values were "recently" (*e.g.*, as part of the current communication session) provided to the other party. These values are often called "nonces" (a term which, according to some cryptographic folklore, comes from the phrase "number used once"), and are a common staple of cryptographic protocols to ensure liveness, *i.e.*, an assurance that the messages being exchanged are "fresh" and correspond to the current session.

## VI. OVERVIEW OF THE '572 PATENT

49. The '572 Patent is titled "Telecommunications network and method of transferring user data in signaling messages from a communication unit to a data processing centre." EX1001, cover. The '572 patent claims priority to a PCT application that was filed on Oct. 28, 2009. The '572 patent has 4 independent claims and 13 dependent claims.

50. The '572 Patent is directed to "a method for establishing a device-to-device (D2D) communication session between mobile devices." EX1001, 1:12-14. The '572 Patent explains that D2D communications "offers advantages such as, e.g., enabling mobile communication between users outside a range of the mobile

network, reducing of load from the base stations and/or from the core nodes of the mobile network, etc." *Id.*, 1:52-56. However, the '572 Patent states that existing telecommunications networks have "no or only limited control over the D2D communication," and that it is desirable to have "more control over the D2D communication between mobile devices which are connectable to a mobile network." *Id.*, 2:11-25.

51. Claim 1 of the '572 Patent is representative, and recites:

> 1. Method for establishing a device-to-device (D2D) communication session between mobile devices which are mutually connectable via a D2D communication channel and individually connectable to a mobile network, comprising:
>
> preloading an initiation key on each of the mobile devices, the initiation key being associated with a validity period; and on each of the mobile devices:
>
> verifying a validity of the initiation key based on a current time;
>
> requesting a further initiation key via the mobile network if no initiation key is deemed valid;
>
> if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel, the key agreement procedure resulting in the session key based on a match of the respective initiation keys used by each of the mobile devices; and
>
> establishing the D2D communication session over the D2D communication channel based on the session key.

52. The '572 Patent states that the claimed "*key agreement procedure*" is a procedure performed between the mobile devices "via the D2D communication channel, e.g., by exchanging messages between the mobile devices, with the

messages together constituting the key agreement procedure." *Id.*, 3:64-4:5. This key agreement procedure results in a valid session key "provided that each respective mobile device uses the same initiation key in the key agreement procedure." *Id.*, 4:8-13. For example, the '572 Patent explains that the initiation key may be used to generate the session key. *Id.*, 8:62-9:3. And "[t]he session key constitutes a key used for cryptographically protecting messages in a communication session." *Id.*, 4:13-15. When a "D2D communication session" is established, "messages, such as those of a voice or video transmission between the mobile devices, are cryptographically protected using the session key." *Id.*, 4:18-23.

53. The '572 Patent explains that the initiation key "is associated with a validity period," which "indicates a period of time in which the initiation key is deemed to be valid for use in establishing the D2D communication session." *Id.*, 3:47-54. The mobile devices holding the initiation key will check the current time when a D2D communication session is requested; if the current time is "in the validity period, the initiation key is used in performing a key agreement procedure between the mobile devices." *Id.*, 3:54-63. Thus, "the initiation key essentially functions as an authorization token in that a mobile device needs the initiation key to establish the D2D communication session," and the validity period associated

with the initiation key offers "a time-based control mechanism" for D2D sessions. *Id.*, 4:28-30.

54. Further, the initiation key is "preloaded" in that it is loaded "on a mobile device before establishing the D2D communication session. For example, the initiation key may be loaded on the mobile device before a request is received to establish the D2D communication session." *Id.*, 3:32-39. This preloading of the initiation key allows the mobile devices to "autonomously establish the D2D communication session, i.e., without a need for contacting 3rd parties." *Id.*, 4:57-59

A. **Prosecution History**

55. The PCT application that led to the '572 Patent was filed as a national stage entry in the U.S. on February 27, 2015. EX1002, 356 (transmittal of application). The Patent Office issued a first office action on December 20, 2015, in which the Examiner rejected then-pending claims 18-34. *Id.*, 88-104. The Examiner rejected Claims 18-27 and 30-34 over U.S. Patent Publication 2013/0013926 to Hakola in view of U.S. Patent Publication 2013/0227655 to Vanderveen. *Id.*, 93-100, and rejected claims 28-29 over Hakola in view of Vanderveen and U.S. Patent Publication 2009/00320102 to Ou. *Id.*, 100-101. In response to the Office Action, applicant filed an amendment to the claims on March 16, 2016, to specify that the recited "key agreement procedure" results in a

session key "*based on a match of the respective initiation keys* used by each of the mobile devices":

> 18. Method for establishing a device-to-device (D2D) communication session between mobile devices which are mutually connectable via a D2D communication channel and individually connectable to a mobile network, comprising:
>
> preloading an initiation key on each of the mobile devices, the initiation key being associated with a validity period ; and on each of the mobile devices;
>
> verifying a validity of the initiation key based on a current time;
>
> if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel, the key agreement procedure resulting in the session key **based on a match of the respective initiation keys** ~~**if the initiation key**~~ used by each of the mobile devices ~~**matches**~~; and
>
> establishing the D2D communication session over the D2D communication channel based on the session key.

*Id.*, 66. In the remarks accompanying this amendment, applicant argued that Hakola "discloses different keys for each mobile device"—thus, Hakola fails to teach "preloading an initiation key on each of the mobile devices," and "the key agreement procedure resulting in the session key based on a match of the respective initiation keys used by each of the mobile devices." *Id.*, 72-73 (emphasis original).

56. The Examiner found these remarks persuasive and issued a notice of allowance on May 11, 2016. *Id.*, 25. The Examiner also suggested an additional amendment adding the claim limitation "*requesting a further initiation key via the*

*mobile network if no initiation key is deemed valid*," which applicant authorized. *Id.*, 30-31, 40.

### B. The '572 Patent Claims

57. The '572 Patent includes seventeen claims: four independent claims and thirteen dependent claims. Independent claim 1 is directed to a method for establishing a device-to-device communication session, and independent claims 15, 16, and 17 are very similar but directed to a non-transitory computer-readable medium (claim 15), a mobile device (claim 16), or a mobile network (claim 17).

58. I understand that Petitioner is challenging claims 1-17 in their petition. Here is a table listing the claims challenged in the petition on a limitation-by-limitation basis.

| Claim Element | Claim Language |
|---|---|
| **Independent Claim 1** | |
| [1p] | Method for establishing a device-to-device (D2D) communication session between mobile devices which are mutually connectable via a D2D communication channel and individually connectable to a mobile network, comprising: |
| [1a] | preloading an initiation key on each of the mobile devices, the initiation key being associated with a validity period; |
| [1b] | and on each of the mobile devices: verifying a validity of the initiation key based on a current time; |
| [1c] | requesting a further initiation key via the mobile network if no initiation key is deemed valid; |
| [1d] | if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel, |

| | |
|---|---|
| [1e] | the key agreement procedure resulting in the session key based on a match of the respective initiation keys used by each of the mobile devices; |
| [1f] | and establishing the D2D communication session over the D2D communication channel based on the session key. |
| 2 | Method according to claim 1, wherein the preloading the initiation key comprises providing the initiation key to each of the mobile devices via the mobile network when each respective mobile device is connected to the mobile network. |
| 3 | Method according to claim 1, wherein the preloading the initiation key comprises storing the initiation key in a secure storage area of each respective mobile device. |
| 4 | Method according to claim 3, wherein the secure storage area is provided by a trusted computing subsystem of each respective mobile device. |
| 5 | Method according to claim 4, wherein at least one of the group of: verifying the validity of the initiation key, and using the initiation key in performing the key agreement procedure, is performed by the trusted computing subsystem. |
| [6a] | Method according to claim 1, further comprising: preloading a set of initiation keys on each of the mobile devices, the set of initiation keys key being associated with a respective set of validity periods; |
| [6b] | and performing a key synchronization procedure between the mobile devices over the D2D communication channel for selecting a matching one of the set of initiation keys on each of the mobile devices as the initiation key. |
| [7a] | Method according to claim 6, further comprising: preloading a set of key identifiers on each of the mobile devices, each of the set of key identifiers identifying a respective one of the set of initiation keys; |
| [7b] | and performing the key synchronization procedure based on an exchange of one or more of the set of key identifiers between the mobile devices. |
| 8 | Method according to claim 6, further comprising disabling or removing the initiation key from the set of |

| | |
|---|---|
| | initiation keys after use in establishing the D2D communication session. |
| 9 | Method according to claim 6, wherein the set of validity periods is constituted at least in part by different but overlapping validity periods. |
| 10 | Method according to claim 1, wherein the initiation key is associated with a virtual network identity, and wherein the verifying the validity of the initiation key further comprises determining a match of the virtual network identity on each of the mobile devices via the D2D communication channel. |
| 11 | Method according to claim 1, wherein the initiation key is associated with a usage count for limiting a number of uses of the initiation key, and wherein the verifying the validity of the initiation key is further based on the usage count. |
| 12 | Method according to claim 11, further comprising adjusting the usage count after use of the initiation key in establishing the D2D communication session. |
| 13 | Method according to claim 1, further comprising requesting a further initiation key via the mobile network if the key agreement procedure fails in providing the session key. |
| 14 | Method according to claim 1, wherein the key agreement procedure comprises: a three-pass authentication procedure; or a use of the initiation key to encrypt a message exchange between the mobile devices for obtaining a shared secret, and a Diffie-Hellman key exchange procedure which is initiated based on the shared secret. |
| **Independent Claim 15** | |
| [15p] | A non-transitory computer-readable medium configured to store instructions for, upon execution of the instructions on a mobile device, causing the mobile device to establish a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to a mobile network, by: |

| | |
|---|---|
| [15a] | storing an initiation key which is provided during a preloading procedure, the initiation key being associated with a validity period; |
| [15b] | verifying a validity of the initiation key based on a current time; |
| [15c] | requesting a further initiation key via the mobile network if no initiation key is deemed valid; |
| [15d] | if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by the mobile device matches an initiation key used by the further mobile device; |
| [15e] | and establishing the D2D communication session over the D2D communication channel based on the session key. |
| **Independent Claim 16** | |
| [16p] | Mobile device for establishing a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to a mobile network, the mobile device comprising: |
| [16a] | a storage area for storing an initiation key which is provided during a preloading procedure, the initiation key being associated with a validity period; |
| [16b] | and a computing subsystem for: |
| [16c] | verifying a validity of the initiation key based on a current time; |
| [16d] | requesting a further initiation key via the mobile network if no initiation key is deemed valid; |
| [16e] | if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by the mobile device matches an initiation key used by the further mobile device; |

| | |
|---|---|
| [16f] | and a mobile subsystem for establishing the D2D communication session over the D2D communication channel based on the session key. |
| **Independent Claim 17** | |
| [17p] | Mobile network arranged for preloading an initiation key on a mobile device when the mobile device is connected to the mobile network, the initiation key being associated with a validity period, the mobile device for establishing a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to the mobile network, the mobile device comprising: |
| [17a] | a computing subsystem for: |
| [17b] | verifying a validity of the initiation key based on a current time; |
| [17c] | requesting a further initiation key via the mobile network if no initiation key is deemed valid; |
| [17d] | if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by the mobile device matches an initiation key used by the further mobile device; |
| [17e] | and a mobile subsystem for establishing the D2D communication session over the D2D communication channel based on the session key. |

### C. Priority Date

59. I understand that the Petitioner assumes without conceding that under pre-AIA § 102(b) the date of the first priority application filed "in the United States" was September 6, 2012.

### D. Claim Construction

60. In my opinion, all of the claim terms in the '572 Patent should be given their plain and ordinary meaning, as a POSITA would understand them in light of the specification and file history of the '572 Patent at the priority date which I understand to be September 6, 2012. Except as otherwise noted, I have applied such a plain and ordinary meaning in my analysis of the claims. I reserve the right to offer additional opinions on claim construction in response to arguments that may be made by Patent Owner.

## VII. LEVEL OF ORDINARY SKILL IN THE ART

61. I understand that the claims and specification of a patent must be read and construed through the eyes of a person of ordinary skill in the art ("POSITA") at the time of the priority date of the claims.

62. I have also been advised that to determine the appropriate level of a person having ordinary skill in the art, the following factors may be considered: (a) the types of problems encountered by those working in the field and prior art solutions thereto; (b) the sophistication of the technology in question, and the rapidity with which innovations occur in the field; (c) the educational level of active workers in the field; and (d) the educational level of the inventors.

63. Based on my education and experience, I am familiar with the level of knowledge that a person of ordinary skill would have possessed during the relevant time period.

64. ***First***, turning to the types of problems and prior art solutions in the art, the "Field of Invention" to the specification of the '572 Patent states that "the invention relates to a method for establishing a device-to-device (D2D) communication session between mobile devices." EX1001, 1:12-14. The "Abstract" of the '572 Patent further explains that the patent is directed to utilizing keys (*e.g.*, an "initiation key" and a "session key") for establishing a D2D communication session. *Id.*, Abstract.

65. ***Second***, turning to the sophistication of the technology and the rapidity with which innovations occur in the field, the technical specifications that governed the functionality of cellular networks and their security protocols at the time of the alleged invention required education and experience in cellular communications technology to understand. A person skilled in the art would have been monitoring these developments. *See*, *e.g.*, EX1001, 1:57-2:7 ("An example of a mobile communication standard which enables mobile communication between mobile devices both via the mobile network as well as via the aforementioned D2D communication is Terrestrial Trunked Radio (TETRA). Another example of such

a mobile communication standard is Global System for Mobile Communications (GSM). … Yet another example is Long Term Evolution (LTE).").

66. ***Third***, with respect to the educational level of active workers in the field, I personally observed that the individuals that participated in development and implementation of networking systems, including their security protocol, typically had at least a bachelor's degree in electrical engineering, computer science, or a related discipline and at least 2-4 years of experience working in the network security industry or in academic research in the field of network security.

67. ***Fourth***, turning to the educational level of the named inventors, the '572 Patent names three inventors: Antonius Norp, Frank Fransen, and Sander De Kievit. I am not personally acquainted with these individuals, but here is a summary of the information I located from a LinkedIn profile that I reasonably believe to be associated with Antonius Norp, Frank Fransen, and Sander De Kievit:

- Antonius (Toon) Norp's profile indicates that he has worked in the field of mobile communications since 1991, by 2012 he had over 21 years' experience in mobile communications. He also appears to have an M.Sc. degree from Eindhoven University of Technology. https://www.linkedin.com/in/toon-norp-2496a4/
- Frank Fransen's profile indicates that he has worked in the field of information security and security of mobile communication systems

since 1995, by 2012 he had over 17 years' experience in mobile communications and the security thereof. He also appears to have M.Sc. and B.Sc. degrees respectively from Eindhoven University of Technology and Amsterdam University of Applied Sciences. https://www.linkedin.com/in/frank-fransen-a6249a/

- Sander de Kievit's profile indicates that he has worked in the field of security of mobile communication systems since 2010, by 2012 he had over 2 years' experience in mobile communications and the security thereof. He also appears to have degrees from Lieden University (B.Sc. and M.Sc.) and Utrecht University (B.Sc.). https://www.linkedin.com/in/sanderdekievit/

68. In my opinion, a person of ordinary skill in the art at the time of the alleged invention of the '572 Patent (September 6, 2012) would have had a degree in electrical engineering, computer science, or a similar discipline, with at least three years of relevant industry or research experience, including designing or implementing network systems. A POSITA would also have familiarity with the standards and protocols relating to mobile communications and the security of such communications. This definition is approximate, and more education may substitute for industry experience or vice versa.

69. In addition, in my opinion, while a person of ordinary skill in the art would have some familiarity with such underlying technologies, that familiarity would need only be sufficient to utilize the technology in connection with a broader system and method. For example, a person of ordinary skill in the art would be aware of signaling messages used in telecommunications systems and the type of data included in those signaling messages.

70. Based on my educational and employment background, I am qualified to provide opinions concerning what a POSITA would have known and understood by September 6, 2012. Indeed, as reflected in my qualifications above, I am more than qualified as a person of ordinary skill in the art as of the relevant date of the '572 Patent.

## VIII. IDENTIFICATION OF THE PRIOR ART AND SUMMARY OF OPINIONS

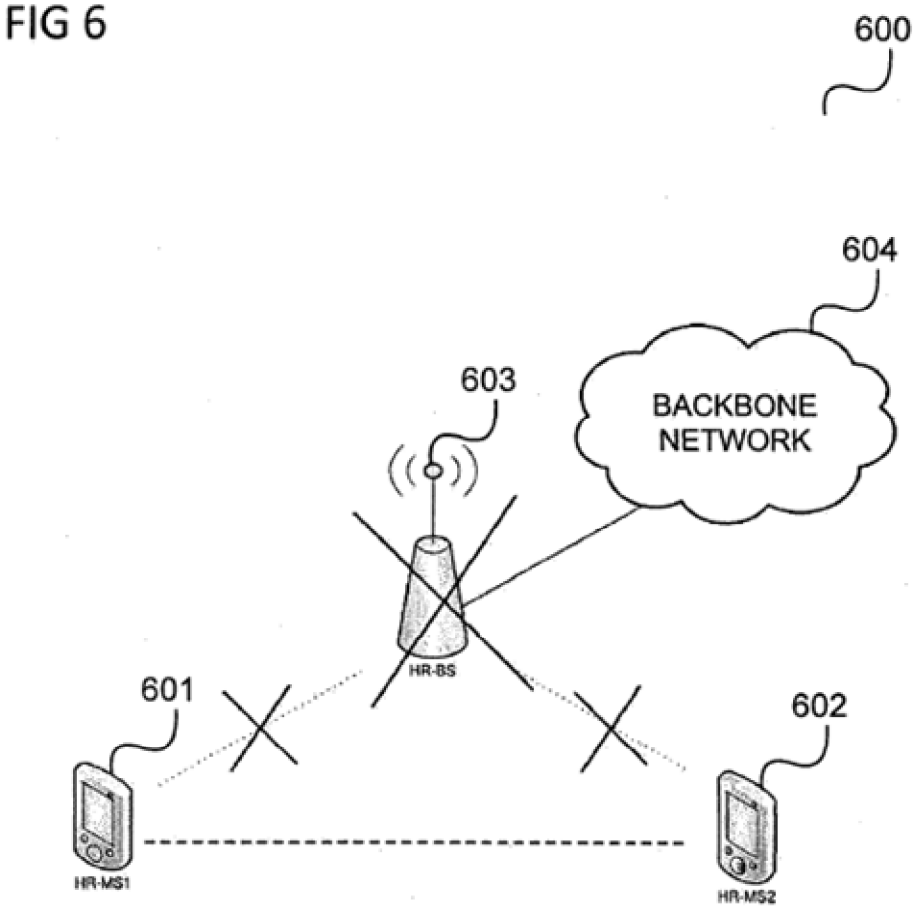
71. As explained below, it is my opinion that the following prior art references, at least in the combinations outlined below, disclose all technical features of challenged claims 1-6 and 9-25 of the '572 Patent, thus rendering them unpatentable.

### A. Summary of WO 2012/112124 A1 ("*Teo*")

72. WO 2012/112124 A1 to Teo ("*Teo*") is titled "Communication Terminal and Method for Performing Communication." *Teo* was filed as

International Application Number PCT/SG2012/000045 on February 14, 2012, designated the United States, and was filed and published in English. EX1005, Codes 22, 25, 26. *Teo* has an international publication date of August 23, 2012. *Id.*, Code 43. I understand that *Teo* qualifies as prior art under at least (pre-AIA) 35 U.S.C. §§ 102(a) and 102(e). I understand *Teo* qualifies as prior art under at least 35 U.S.C. § 102(a)(1).

73. *Teo* describes establishing a direct communication session between mobile devices. *Teo* explains that high reliability (HR) telecommunications networks may require mobile stations to "communicate directly with each other in the event of network failure." EX1005, 1:15-18. Such direct communication may be needed "in the event of a disaster where in the backbone network is destroyed" and rescue teams "would have to communicate directly with each other without a backbone network in order to provide disaster recovery." *Id.*, 1:18-23. Figure 6 of *Teo*, copied and annotated below, illustrates such a backbone network failure:




*Id.*, Fig. 6, 19:29-20:4 ("In normal operation, the base station 603 provides coverage for the mobile terminals 601, 602 such that the mobile terminals 601, 602 can communicate via the base station 603. For this embodiment, it is assumed that the base station 603 is not available for providing communication between the mobile terminals 601, 602. For example, the backbone network 604 has failed.").

74. To facilitate direct communication between mobile devices, *Teo* discloses a system and method for "setting up communication between a communication terminal of a cellular mobile communication system and another communication terminal of the cellular mobile communication system." *Id.*, 8:1-4.

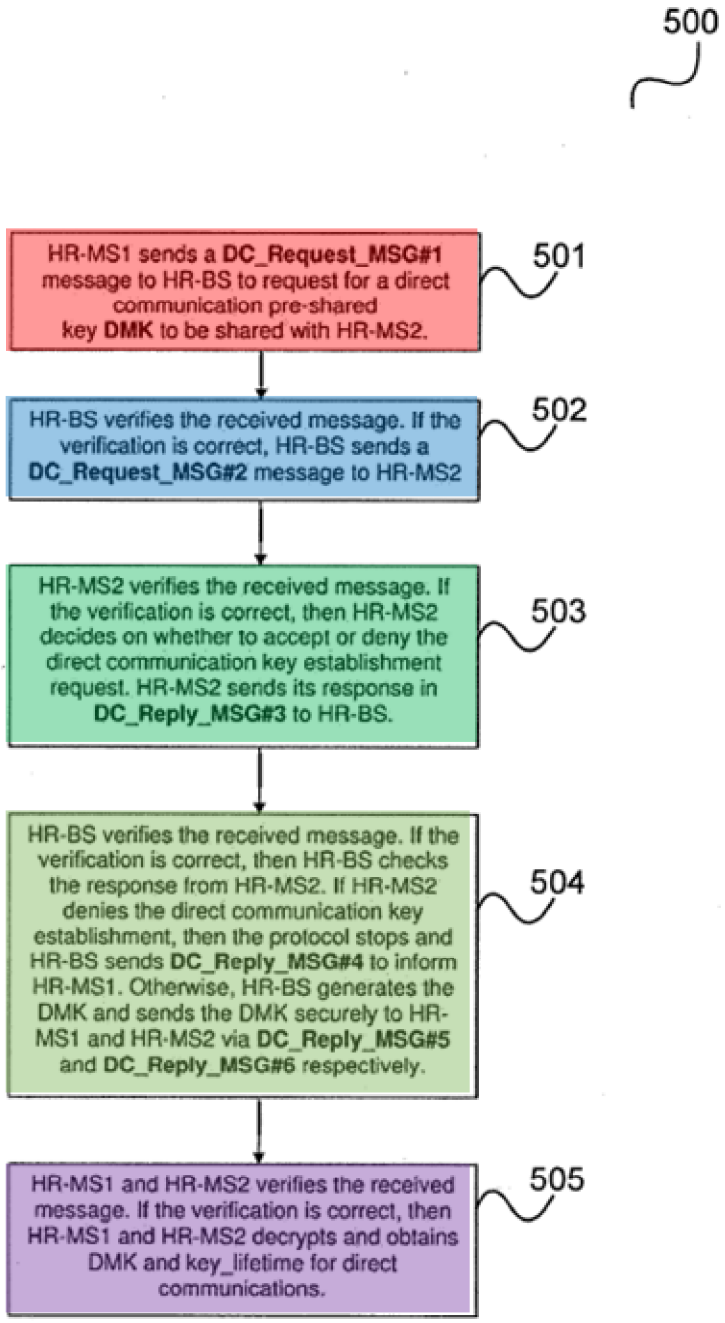
*Teo* explains that this communication is "secure" because the messages exchanged between the communication terminals are encrypted according to an encryption key. *Id.*, 8:17-21 ("In 2002, secure communication between the communication terminal and the other communication terminal is performed via the radio interface between the communication terminal and the other communication terminal using the determined encryption key.").

75. *Teo* describes "three AKE [Authenticated Key Exchange] protocols for Mutual Authentication of HR-MS [high reliability mobile station] and data security for Direct Communications," which are used to determine the encryption key. *Id.*, 18:7-10. One such protocol is referred to as the "Pre-shared key scenario…where it is assumed that HR-MS1 and HR-MS2 shares a key prior to direct communications." *Id.*, 18:10-19:3. In accordance with the pre-shared key scenario (also referred to as the "pre-shared key approach," *see* EX1005, 37:14-16) the mobile communication terminals that want to establish a direct communication must first receive the pre-shared key, called "DMK" (Direct Communications Master Key). *Id.*, 31:6-15 ("In the following, the pre-shared key approach according to one embodiment is described with reference to figures 6, 16 and 12. It is assumed that HR-MS1 601, 701 and HR-MS2 602, 702 have already established a pre-shared key DMK using one of the methods previously described, such as with the aid of the Network Infrastructure for example using the approach

as described above with reference to figures 3, 4 and 5, or some other method and wish to communicate directly."), 62:29-30.

76. In one example, *Teo* describes that the mobile communication terminals wanting to directly communicate receive the DMK from the base station to which the mobile communication terminals are connected. 13:4-14:19 (describing the base station HR-BS generating the DMK and transmitting the DMK to two mobile communication terminals, HR-MS1 and HR-MS2). Figure 5 of *Teo* is a flow diagram that describes how the pre-shared DMK is obtained according to this example:

FIG 5




*Id.*, Fig. 5 (highlighting added).

77. First, a first mobile communication terminal (*i.e.*, HR-MS1) sends a first message to a base station (*i.e.*, HR-BS) requesting a "direct communication pre-shared key DMK to be shared with" a second mobile communication terminal

(*i.e.*, HR-MS2). *Id.*, 11:12-17, Fig. 5 (Step 501). HR-BS then sends a second message to HR-MS2 to inform HR-MS2 of the HR-MS1's request. *Id.*, 12:1-7, Fig. 5 (Step 502). If HR-MS2 accepts the request, HR-MS2 sends a response message back to HR-BS informing HR-BS of the acceptance. *Id.*, 12:15-13:2, Fig. 5 (Step 503). HR-BS then "generates the DMK" and sends the DMK to both HR-MS1 and HR-MS2 in encrypted messages. *Id.*, 13:4-14:19, Fig. 5 (Step 504). HR-MS1 and HR-MS2 each decrypt the message it received from HR-BS and "obtains DMK and its lifetime key_lifetime." *Id.*, 14:21-15:2, Fig. 5 (Step 505).

78. As will be discussed in more detail below, *Teo*'s "pre-shared key DMK" corresponds to the claimed "*initiation key*," and its "key_lifetime" parameter corresponds to the claimed "*validity period*."

79. Once the mobile communication terminals (*e.g.*, HR-MS1 and HR-MS2) receive the DMK, they are able to establish direct communication should the backbone network fail, for example. If direct communication is desired, the first mobile communication terminal generates a set of new keys using the pre-shared DMK it received from the base station—DAK, DCMAC, and DTEK. EX1005, 32:16-21 ("Step 1201: In 1603, HR-MS1 1601 selects a nonce $N_{HR\text{-}MS1}$ and uses the shared DMK and computes DAK…, the DCMAC… and DTEK…."). The DAK is derived from the DMK. *Id.*, 37:23-25 ("DAK is derived from DMK and belongs to a pair of HR-MSs."), 32:17-18 ("DAK = Dot16KDF(DMK, HR-MS1Addr | HR-

MS2Addr | 'DAK', 160)"). The DCMAC and DTEK are then derived from the DAK. *Id.*, 38:1-7 ("The DCMAC-DTEK prekey is derived from DAK and is used to derive other keys: Direct Communication Cipher-based Message Authentication Code (DCMAC) key; Direct communication Traffic Encryption (DTEK) Key)"), 32:19 ("DCMAC = Dot16KDF(DAK, 'DCMAC_KEYS', 128)"), 32:21 ("DTEK = DOT16KDF(DAK, 'DTEK_KEY', 128")). The first mobile communication terminal then generates a "message digest," $\theta_{HR\text{-}MS1}$, which is "calculated using the DCMAC key," and sends $\theta_{HR\text{-}MS1}$ to the second mobile communication terminal.

80. The second mobile communication terminal then uses the pre-shared DMK received from the base station to generate its own set of DAK, DCMAC, and DTEK. *Id.*, 33:1-7 (In 1606, HR-MS2…uses the shared DMK and computes DAK…, DCMAC…, DTEK."). The second mobile communication terminal then "uses DCMAC to check $\theta_{HR\text{-}MS1}$." *Id.*, 33:7-8. A successful check indicates that the first and second mobile communication terminals possess the same DMK and that the terminals have computed the same DAK, DCMAC, and DTEK. That is, if both HR-MS1 and HR-MS2 start with the same DMK, they will each compute the same DAK, DCMAC, and DTEK keys. If their DMKs differ, the DAK, DCMAC, and DTEK keys will be different and the message digests (*e.g.*, $\theta_{HR\text{-}MS1}$) will not be verifiable by either terminal. If $\theta_{HR\text{-}MS1}$ is successfully verified, the second mobile communication terminal computes a second message digest, $\theta_{HR\text{-}MS2}$, using its

DCMAC key and sends $\theta_{HR\text{-}MS2}$ to the first communication terminal. EX1005, 33:8-24, 36 (explaining that $\theta_{HR\text{-}MS2}$ is a "[m]essage digest calculated using DCMAC key.").

81. Upon receiving the $\theta_{HR\text{-}MS2}$ and successfully verifying it, the first mobile communication terminal generates a third message digest, $\theta_{HR\text{-}MS1}'$, using its DCMAC key and sends $\theta_{HR\text{-}MS1}'$ to the second communication terminal. *Id.*, 33:30-34:15, 36 (explaining that $\theta_{HR\text{-}MS1}'$ is a "[m]essage digest calculated using DCMAC key"). When the second communication terminal successfully checks $\theta_{HR\text{-}MS1}'$, the second mobile communication terminal is "ready for direct communications with" the first mobile communication terminal. *Id.*, 34:19-21.

82. *Teo* explains that the keys generated by the mobile communication terminals—DAK, DCMAC, and DTEK—are used for direct communications. For example, the DTEK is "used to encrypt data in direct communications." *Id.*, 38:24-25. Accordingly, a POSITA would have recognized the DTEK as the "encryption key" that facilitates secure direct communication between the mobile communication terminals. EX1005, 8:17-21 ("In 2002, secure communication between the communication terminal and the other communication terminal is performed via the radio interface between the communication terminal and the other communication terminal using the determined encryption key.").

### B. Summary of U.S. Patent Application Publication No. 2013/0067552 ("*Hawkes*")

83. United States Patent Application Publication No. 2013/0067552 to *Hawkes* ("*Hawkes*"), titled "MDN-less SMS messaging (network solution) for wireless M2M application," was filed as Application No. 13/288/949 on November 3, 2011. I understand that *Hawkes* qualifies as prior art under at least (pre-AIA) 35 U.S.C. §102(e). I understand *Hawkes* qualifies as prior art under at least 35 U.S.C. § 102(a)(2).

84. *Hawkes* is directed to a system for managing security credentials associated with a mobile device, where the security credential is later used to authenticate the mobile device for secure user plane location (SUPL) services. EX1006, Abstract. *Hawkes* explains that the security credential may comprise a "device certificate" that includes a public key and a device identifier. *Id.*, [0032]. *Hawkes* describes hardware components that store the security credential. For example, *Hawkes* explains that the security credential may be stored in a "universal integrated circuit card (UICC)," which may include a "secure storage area." *Id.*, [0098], [1278]. *Hawkes* also describes the hardware components that facilitate wireless communication with other entities, such as a "system-in-package or system-on-chip device (*e.g.*, a mobile station modem (MSM))" that includes

components such as a processor, a display controller, a memory, and a wireless controller. Id, [0099]-[0100].

### C. Summary of RFC 4279

85. RFC 4279 is a standards-track document entitled "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)," that was submitted by Nokia and Siemens to the Internet Engineering Task Force (IETF) for consideration of standardizing the protocols described therein.

86. To obtain this document, I directed a web browser to URL: https://www.rfc-editor.org/rfc/rfc4279. I selected the "PDF" link, which directed me to the following URL: https://www.rfc-editor.org/rfc/pdfrfc/rfc4279.txt.pdf. I then saved the PDF version of this file, which was downloaded as "rfc4279.txt.pdf". A true and correct copy of this PDF file is provided as Exhibit 1007.

87. According to the IETF webpage tracking the history of RFC 4279 (https://datatracker.ietf.org/doc/rfc4279/history/; Appendix 1), RFC 4279 was originally published on December 6, 2005, as evidenced by the publish date corresponding to that file:

| | | |
|---|---|---|
| 2005-12-06 | 09 Amy Vezza | State Changes to **RFC Published** from **RFC Ed Queue** by **Amy Vezza** |
| 2005-12-06 | 09 Amy Vezza | [Note]: 'RFC 4279' added by Amy Vezza |
| 2005-12-05 | 09 (System) | RFC published |

Further, the Index for all Requests for Comment ("RFC"), published by the IETF since 1969 through 2023, is available at https://www.rfc-editor.org/rfc-index.html (Appendix 2). The Index lists all RFCs from RFC1 through RFC9411 and provides the following "Key to Citations": "Following the number are the title, the author list, and the publication date." Appendix 2, 1. Based on the Index's key to citations, December 2005 is the publication date of RFC 4279:

4279 **Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)** P. Eronen, H. Tschofenig [ December 2005 ] (TXT, HTML) (Updated-By RFC8996) (Status: PROPOSED STANDARD) (Stream: IETF, Area: sec, WG: tls) (DOI: 10.17487/RFC4279)

*Id*., 2. Further, the Internet Archive captured and archived a published copy of RFC 4279 on February 19, 2006, confirming its publication as of at least that date. Appendix 3.

88. In the course of my professional and academic career, I have worked closely on IETF standards, and I have every reason to believe that "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)," (*i.e.*, RFC 4279) was published before the '572 Patent's September 6, 2012, priority date. In addition, I recognize that Exhibit 1007 is a true and correct copy of "Pre-Shared Key

Ciphersuites for Transport Layer Security (TLS)," (*i.e.*, RFC 4279) as it existed on or before the'572 Patent's September 6, 2012, priority date.

89. Thus, I understand that RFC 4279 qualifies as prior art under at least (pre-AIA) 35 U.S.C. §§ 102(a) and 102(b). I understand RFC 4279 qualifies as prior art under at least 35 U.S.C. § 102(a)(1).

90. RFC 4279 describes protocols to support authentication of clients using the TLS protocol based on pre-shared keys (PSKs). When using PSK-based authentication, the client and server must first agree to a particular PSK that is to be used, which is necessary because "[b]oth clients and servers may have pre-shared keys with several different parties." EX100S, 4-5. Accordingly, the client may send a "PSK identity" to the server, thereby "indicat[ing] which key to use." *Id.*, 5. If the server does not recognize the PSK identity, it may respond with an alert message. *Id.*, 6.

### D. Summary of U.S. Patent Application Publication No. 2001/0019614 (*Madoukh*)

91. United States Patent Application Publication No. 2001/0019614 to Madoukh ("*Madoukh*") was filed as Application No. 09/693,605 on October 20, 2000. *Madoukh* was published on September 6, 2001. I understand *Madoukh* qualifies as prior art under at least (pre-AIA) 35 U.S.C. §§ 102(a), 102(b), and

102(e). I understand *Madoukh* qualifies as prior art under at least 35 U.S.C. § 102(a)(1).

92. *Madoukh* describes a computer system that includes a number of components for managing encrypted data, security information, and keys. EX1011, Abstract. For example, the disclosed computer system "includes a key lifetime manager operable to monitor encryption key expiration dates and request new encryption keys upon the expiration of old encryption keys." *Id*., [0007].

E. **Summary of S3-070234**

93. Document number S3-070234 to 3GPP TSG SA WG3 Security meeting #46b ("S3-070234") is a 3GPP standards submission submitted by Nokia and Siemens to 3GPP. S3-070234 was published on March 21, 2007. EX1019, ¶¶ 45-52. I understand that S3-070234 qualifies as prior art under at least (pre-AIA) 35 U.S.C. §§ 102(a) and 102(b). I understand S3-070234 qualifies as prior art under at least 35 U.S.C. § 102(a)(1).

94. S3-070234 describes implementing "counters related to limiting key usage, e.g. to limit the number of key derivations from one parent key." EX1013, 1-2.

### F. Summary of U.S. Patent Application Publication No. 2007/0171910 ("*Kumar*")

95. United States Patent Application Publication No. 2007/0171910 to Kumar ("*Kumar*") was filed as Application No. 11/538,222 on October 3, 2006. *Kumar* was published on July 26, 2007. I understand that *Kumar* qualifies as prior art under at least (pre-AIA) 35 U.S.C. §§ 102(a), 102(b), and 102(e). I understand *Kumar* qualifies as prior art under at least 35 U.S.C. § 102(a)(1).

96. *Kumar* describes peer-to-peer communication in an ad-hoc wireless network using pre-shared keys to generate session keys. EX1016, Abstract. Kumar explains that the pre-shared keys may be associated with a service set identifier (SSID), which identifies an 802.11 wireless network. *Id*., [0057], Fig. 2.

### G. Summary of U.S. Patent Application Publication No. 2009/0016524 ("*Park*")

97. United States Patent Application Publication No. 2009/0016524 to Park ("*Park*") was filed as Application No. 12/147,967 on June 27, 2008. *Park* was published on January 15, 2009. I understand that *Park* qualifies as prior art under at least (pre-AIA) 35 U.S.C. §§ 102(a), 102(b), and 102(e). I understand *Park* qualifies as prior art under at least 35 U.S.C. § 102(a)(1).

98. *Park* describes distributing keys within an ad-hoc peer-to-peer network, wherein the keys may have different validity periods (*e.g.*, one month, six

hours, one hour), after which the key expires. EX1017, Abstract, [0050], [0052], [0059], [0064].

### H. Summary of U.S. Patent Application Publication No. 2009/0181643 ("*Thakare*")

99. United States Patent Application Publication No. 2009/0181643 to Thakare ("*Thakare*") was filed as Application No. 12/255,509 on October 21, 2008. *Thakare* was published on July 16, 2009. I understand that *Thakare* qualifies as prior art under at least (pre-AIA) 35 U.S.C. §§ 102(a), 102(b), and 102(e). I understand *Thakare* qualifies as prior art under at least 35 U.S.C. § 102(a)(1).

100. *Thakare* describes packet-based communication wherein data packets are encrypted according to an encryption key. EX1018, [0008], [0032]. *Thakare* explains that a new encryption key may be requested if data packets are not successfully authenticated. *Id*., [0008]-[0009].

### I. A POSITA's Motivation to Combine *Teo* with *Madoukh*

101. It is my opinion that there are a number of reasons why a POSITA would have been motivated to combine *Teo* with *Madoukh* at the time of the alleged invention and would have had a reasonable expectation of success in doing so.

102. *Teo* discloses a system wherein two mobile communication terminals receive both a pre-shared key DMK and the DMK's lifetime, "key_lifetime." EX1005, 13:19-15:2. *Madoukh* discloses a computer system that "includes a key lifetime manager operable to monitor encryption key expiration dates and request new encryption keys upon the expiration of old encryption keys," as well as "deactivate the expired keys." EX1011, [0007]-[0008].

103. A POSITA would have been motivated to combine *Teo*'s system for receiving and using keys with associated lifetimes with *Madoukh*'s "key lifetime manager" for monitoring the expiration of keys, requesting new keys when old keys have expired, and deactivating expired keys. Such a combination would have involved combining prior art elements according to known methods to yield predictable results. A POSITA would have understood that *Madoukh*'s key lifetime manager could be implemented in any device that stores keys with some designated lifetime, such as *Teo*'s mobile communication terminals. The combination of *Teo* with *Madoukh* would have been predictable and foreseeable because the combination merely involves incorporating known features that are explicitly disclosed by *Madoukh* and would have been understood by a POSITA as likely present if not explicitly disclosed by *Teo*. A POSITA would have understood that *Teo*'s DMK would expire (as indicated by the key_lifetime value associated with the DMK) and one would need to implement a component for

tracking the DMK's expiration, requesting a new DMK upon such expiration, and deactivating the expired DMK, such as *Madoukh*'s key lifetime manager.

### J. Reasonable Expectation of Success

**104.** It is my opinion that a POSITA would have reasonably expected success when combining *Teo* with *Madoukh*. As discussed above in Section VIII.I, a POSITA would have recognized that *Madoukh*'s key lifetime manager could be implemented in any device that stores keys with some designated lifetime, such as *Teo*'s mobile communication terminals. A POSITA would have understood that *Teo*'s terminals would need to some sort of component for managing DMKs and their lifetime, as it is a fundamental aspect of cryptographic key management that keys should expire and be replaced. *See* EX1009, 183 ("No encryption key should be used for an indefinite period. It should expire automatically like passports and licenses."). Thus, a POSITA would have reasonably expected success in implementing the key lifetime manager as detailed by *Madoukh*.

### K. A POSITA's Motivation to Combine *Teo* with *Madoukh* and *Hawkes*

105. As I discussed above in Section VIII.I, A POSITA would have been motivated to combine *Teo* with *Madoukh.* It is my opinion that a POSITA would have been motivated to further combine these references with *Hawkes.*

106. *Teo* discloses a system and method for establishing direct communications between mobile communication terminals. In accordance with this method and system, *Teo* describes sending to the mobile communication terminals a "pre-shared" direct communication master key (DMK). The mobile communication terminals use the DMK to generate additional keys, such as the DAK, DCMAC, and DTEK, which are used to ensure the security of direct communications.

107. *Hawkes* discloses a system for managing security credentials in a telecommunications network. *Hawkes* explains that its system includes one or more mobile devices that may access secure user plane location (SUPL) services offered by the network. The mobile devices include memory components that securely store authorization credentials, such as public keys, needed to verify a mobile device's access to the SUPL services. For example, *Hawkes* states that its mobile device include a "card interface 1170" that is configured to "accommodate a card 1172 (e.g., a subscriber Identity module (SIM) card, a universal integrated circuit card (UICC), or other card) storing security credential(s)" of the mobile device. EX1006, [0098]; *See* also *id.*, [0032] (describing that the UICC may store "security credentials of the mobile device" such as a "device certificate" that includes a "public key 124 and a device Identifier").

108. *Hawkes* further discloses a "system-in-package or system-on-chip device (*e.g.*, a mobile station modem (MSM))" that includes components such as a processor, a display controller, a memory, and a wireless controller. *Id.*, [0099]. *Hawkes* explains that these components are used to facilitate the transmission of data. EX1006, [0100].

109. A POSITA would have been motivated to combine *Teo*'s system for establishing direct communication between mobile communication terminals with *Hawkes*' memory and processor components. Such a combination would have involved combining prior art elements according to known methods to yield predictable results. *Hawkes* discloses mobile devices that include memory components like the UICC for securely storing security credentials, such as public keys, as well as a system-on-chip device that facilitates transmission of data. EX1006, [0032], [0098]-[0099]. A POSITA would have understood that these memory and processor components could be implemented in any mobile device that stores information and exchanges messages with other devices, such as *Teo*'s mobile communication terminals. This understanding would have been apparent in light of Hawkes' teaching that these components are included in a "wireless communication device" such as "mobile device 120." EX1006, [0096]. The combination of *Teo* with *Hawkes* would have been predictable and foreseeable because the combination merely involves incorporating known features that are

explicitly disclosed by *Hawkes* and would have been understood by a POSITA as likely present if not explicitly disclosed by *Teo*. The combination is predictable, at least in part because elements of the combined system would each perform similar functions they had been known to perform prior to the combination. For example, *Teo*'s mobile communication devices would still perform the same functions, including receiving a pre-shared key DMK, for generation of additional encryption keys, as it did prior to the combination with *Hawkes*.

### L. Reasonable Expectation of Success

110. As I discuss above in Section VIII.J, a POSITA would have had a reasonable expectation of success in combining *Teo* with *Madoukh.* It is my opinion that a POSITA would have reasonably expected success in further combining these references with *Hawkes.* As discussed above in Section VIII.K, a POSITA would have recognized that the components taught by *Hawkes*, such as the UICC and the system-on-chip device, could be implemented in any mobile device that stores information and exchanges messages with other devices, such as *Teo*'s mobile communication terminals. Such an understanding would have been readily apparent in light of *Hawkes*' inclusion of these components in a "wireless communication device" such as "mobile device 120." EX1006, [0096]. A POSITA would have understood that *Teo*'s mobile communication terminals would need to implement memory and communication components to operate as

disclosed in *Teo*, and therefore would have reasonably expected success in implementing the memory and processor components expressly detailed by *Hawkes*.

111. As an example embodiment of operation, a POSITA would have implemented *Teo*'s teachings according to *Hawkes*' teachings such that *Teo*'s mobile communication terminals (*e.g.*, HR-MS1 and HR-MS2) would have comprised the memory components and the system-on-chip components taught by *Hawkes*, such as a card interface, a UICC, and a wireless controller. A POSITA would have understood that upon receiving the pre-shared key, DMK, from the base station, the mobile communication terminals would have stored the DMK in their respective memory components. Further, a POSITA would have understood that the components of the system-on-chip device, such as the wireless controller, would have facilitated communication between the mobile communication devices for establishing a D2D communication session.

### M. A POSITA's Motivation to Combine *Teo* with *Madoukh* and RFC 4279

112. As I discussed above in Section VIII.I, A POSITA would have been motivated to combine *Teo* with *Madoukh.* It is my opinion that a POSITA would have been motivated to further combine these references with RFC 4279.

113. *Teo* discloses a system and method for establishing direct communications between mobile communication terminals. In accordance with this method and system, *Teo* explains that its system may be applied, for example, "in the event of a disaster where the backbone network is destroyed" such that "[t]he rescue teams (*e.g.* firemen and police officers) would have to communicate directly with each other without a backbone network in order to provide disaster recovery." EX1005, 1:18-23. *Teo* describes facilitating the direct communications between mobile communication terminals by sending to the mobile communication terminals a "pre-shared" direct communication master key (DMK). EX1005, 7:24-27, 10:19-28.

114. RFC 4279 describes "how to use symmetric keys (later called pre-shared keys or PSKs), shared in advance among the communicating parties, to establish a TLS [Transport Layer Security] connection" between a client and a server. EX1007, 2. RFC 4279 explains that "[b]oth clients and servers may have pre-shared keys with several different parties." *Id.*, 5. Accordingly, RFC 4279 discloses a procedure whereby the client and server agree on the pre-shared key that they wish to use for a TLS connection. *Id.*, 4-5. In particular, RFC 4279 explains that after the client and server agree to use pre-shared key authentication, the client includes "PSK identity" information in a "ClientKeyExchange message," which thereby "indicates which key to use." *Id.*

115. A POSITA would have been motivated to modify *Teo*'s procedure for establishing direct communications between mobile communication terminals based on a pre-shared key DMK to include a procedure whereby the mobile communication terminals agree on the pre-shared DMK to be used as taught by RFC 4279. Including a procedure for mobile communication terminals to agree on a pre-shared key for later use would have been a matter of common sense and a needed step in a communications system. A POSITA would have recognized that the mobile communication terminals operating according to *Teo*'s system could receive several pre-shared DMKs, as suggested by *Teo*, which envisions a communications environment wherein several "firemen and police officers," for example, would need to communicate directly with each other. EX1005, 1:20-23. Accordingly, a POSITA would have recognized the need for implementing a system that allows the mobile communication terminals to agree on a pre-shared key DMK before attempting to establish a direct communication session. Such a system would allow for a more efficient coordination of pre-shared keys between mobile communication terminals, as the terminals could avoid having to perform wasteful trial-and-error procedures for selecting a common pre-shared key.

### N. Reasonable Expectation of Success

116. As I discussed above in Section VIII.J, a POSITA would have reasonably expected success in combining *Teo* with *Madoukh*. It is my opinion

that a POSITA would have been motivated to further combine these references with *Hawkes*. Both *Teo* and RFC 4279 relate to the use and management of pre-shared keys, and a POSITA would have recognized that the procedure for identifying pre-shared keys using a generic "PSK identifier" for agreement between entities could be applied in any system where two entities have pre-shared keys, as in *Teo*. Although RFC 4279 describes its procedure in the context of TLS connection setup between a client and a server, nothing in RFC 4279 restricts the application of its teachings to any particular system or environment, and a POSITA would have had a reasonable expectation of success in applying RFC 4279's procedure, which generally teaches how to choose a particular key between two entities that have received several keys, in the context of *Teo*'s device-to-device communication system, which suggests the sharing of several keys amongst several mobile terminals. Such a modification would not have involved undue experimentation and instead would have required only basic network programming ability.

### O. A POSITA's Motivation to Combine *Teo* with *Madoukh*, RFC 4279, and *Kumar*

117. As I discussed above in Section VIII.M, A POSITA would have been motivated to combine *Teo* with *Madoukh* and RFC 4279. It is my opinion that a

POSITA would have been motivated to further combine these references with *Kumar*.

118. *Teo* describes sending a "pre-shared" direct communication master key (DMK) that is used to facilitate the direct communications between mobile communication terminals. EX1005, 7:24-27, 10:19-28. RFC 4279 discloses a procedure whereby a client device includes "PSK identity" information in a "ClientKeyExchange message" sent to a server, which thereby "indicates which key to use" for a Transport Layer Security connection. EX1007, 4-5. And *Kumar* describes associating a "Preshare Key" (PSK) with an "SSID," which identifies an 802.11 wireless network associated with the PSK. EX1016, Fig. 2, [0057].

119. A POSITA would have been motivated to modify the *Teo*-*Madoukh*-RFC 4279 combination with *Kumar* such that RFC 4279's "PSK identity" is implemented using *Kumar*'s SSID value. Such a combination would have involved a simple substitution of one known element for another to obtain predictable results. A POSITA would have recognized RFC 4279's "PSK identity" to be a generic value that anonymously identifies a "preshare[d] key," such as *Teo*'s DMK, and could take any value that distinguishes one key from another, such as *Kumar*'s SSID value, which identifies a wireless network with which a key is associated. Indeed, as shown in Figure 2 of *Kumar*, different SSID values are associated with different "Preshare Key[s]." EX1016, Fig. 2.

120. A POSITA would have recognized that applying such a basic technique, using an SSID value associated with a key to identify the key, would have yielded predictable results and an improved system, such as mobile communication terminals that can efficiently identify a pre-shared key (e.g., DMK) to establish direct communication by exchanging SSID values associated with the pre-shared key.

P. **Reasonable Expectation of Success**

121. As I discussed above in Section VIII.J, a POSITA would have reasonably expected success in combining *Teo* with *Madoukh* and RFC 4279. It is my opinion that a POSITA would have reasonably expected success when further combining these references with *Kumar*.

122. *Teo*, *Madoukh*, RFC 4279, and *Kumar* all relate to the use and management of keys, and a POSITA would have recognized that the procedure for identifying pre-shared keys using a generic "PSK identifier" could use any value that distinguishes one key from another, such as *Kumar*'s SSID value. *See* EX1016, Fig. 2 (associating different SSID values with different "Preshare Key[s]"). Such a modification would not have involved undue experimentation and instead would have required only basic network security design ability.

### Q. A POSITA's Motivation to Combine *Teo* with *Madoukh* and S3-070234

123. As I discussed above in Section VIII.I, A POSITA would have been motivated to combine *Teo* with *Madoukh*. It is my opinion that a POSITA would have been motivated to further combine these references with S3-070234.

124. *Teo* describes sending a pre-shared key, DMK, to mobile communication terminals to facilitate their direct communication. EX1005, 7:24-27, 10:19-28. As discussed above in Ground 1, the DMK is associated with a lifetime that indicates when the DMK expires. *See supra*, Section IX.A.1.b. The mobile communication terminals use the DMK to generate additional keys, such as the DAK, DCMAC, and DTEK, which are used to ensure the security of direct communications. *Id*., 37:4-38:25. S3-070234 describes various proposals for increasing the security and integrity of cryptographic keys used in encryption. EX1013, 1. One such proposal is implementing "counters related to limiting key usage, e.g. to limit the number of key derivations from one parent key." *Id*., 1-2. In combination, the *Teo-Madoukh*-S3-070234 combination teaches a mobile communication terminal that uses a counter to limit the number of times the DMK is derived into other keys, such as the DAK.

125. A POSITA would have been motivated to combine *Teo*'s system wherein a pre-shared key DMK is used to derive other keys with S3-070234's

usage-based counter for limiting the number of key derivations of a parent key. Such limiting of the DMK's use would have been a matter of common sense to a POSITA. It is a well-known principle in cryptographic key management that the severity of a key being compromised increases the more often the key is used. EX1009, 183 ("The longer a key is used, the greater the loss if the key is compromised. If a key is used only to encrypt a single budgetary document on a file server, then the loss of the key means only the compromise of that document. If the same key is used to encrypt all the budgetary information on the file server, then its loss is much more devastating."). While the DMK's lifetime offers a time-based mechanism to limit the overuse of the DMK, a POSITA would have recognized that security concerns arise when the DMK is used many times before the lifetime expires. Accordingly, a POSITA would have been motivated to seek out additional methods for limiting a DMK's exposure, such as S3-070234 method for counting key usage.

### R. Reasonable Expectation of Success

126. As I discussed above in Section VIII.J, a POSITA would have reasonably expected success in combining *Teo* with *Madoukh*. It is my opinion that a POSITA would have been motivated to further combine these references with S3-070234.

127. A POSITA would have understood that S3-070234's method for limiting the number of derivations of a parent key could be implemented in any device that uses a parent key to derive additional keys, such as *Teo*'s mobile communication terminals that use the DMK to derive the DAK, DCMAC, and DTEK. Such a modification would not have involved undue experimentation and instead would have required only basic network security design ability. The combination of *Teo* with S3-070234 would have been predictable and foreseeable because the combination merely involves incorporating known features that are explicitly disclosed by S3-070234. The combination is predictable, at least in part because elements of the combined system would each perform similar functions they had been known to perform prior to the combination. For example, *Teo*'s terminals would still perform the same functions, including receiving a pre-shared key, DMK, for generating additional encryption keys and establishing a D2D communication session, as they did prior to the combination with S3-070234.

### S. A POSITA's Motivation to Combine *Teo* with *Madoukh* and *Thakare*

128. As I discussed above in Section VIII.I, A POSITA would have been motivated to combine *Teo* with *Madoukh.* It is my opinion that a POSITA would have been motivated to further combine these references with *Thakare*.

129. *Teo* teaches receiving a pre-shared key DMK from a base station and using the DMK to generate additional keys, such as the DAK, DCMAC, and DTEK, that are used during a direct communication session. EX1005, 13:19-15:2, 32:16-21, 33:1-8, 38:24-25. A POSITA implementing such a procedure would have recognized that errors (*e.g.*, transmission errors or message decryption errors) may occur and prevent the additional keys from being generated. A POSITA thus would have been motivated to seek out solutions to correct for such errors. A natural and common sense solution would have been to request a new DMK from the base station and to reattempt generating the additional keys with the new DMK, and a POSITA would have searched for and implemented such solutions—like *Thakare*'s concept of requesting a new encryption key for generating encrypted data packets—to address such errors.

T. **Reasonable Expectation of Success**

130. As I discussed above in Section VIII.J, a POSITA would have reasonably expected success in combining *Teo* with *Madoukh*. It is my opinion that a POSITA would have been motivated to further combine these references with *Thakare*.

131. A POSITA would have recognized that *Thakare*'s process of requesting a new key upon encountering errors in the using the key was a complementary process to the concepts relied upon in *Teo*. As an example

embodiment of operation, a POSITA would have implemented *Thakare*'s teachings according to *Teo*'s mobile communication terminals (*e.g.*, HR-MS1 and HR-MS2) such that the terminals would have simply requested a new DMK from the base station (*e.g.*, HR-BS) upon detecting that the "pre-shared key approach" for generating additional keys (*e.g.*, DAK, DCMAC, and DTEK) failed. That modification—requesting a new DMK from the base station upon determining that the DMK has failed in generating the additional keys—would have involved basic design skill and would not have required any undue experimentation, as such tasks were well-known at the time of invention.

## IX. UNPATENTABILITY OF THE '572 PATENT CLAIMS

### A. Ground 1: Claims 1-2 and 14 are Unpatentable as they are Rendered Obvious by *Teo* in view of *Madoukh*.

132. In my opinion, claims 1-2 and 14 are rendered obvious by *Teo* in view of *Madoukh*.

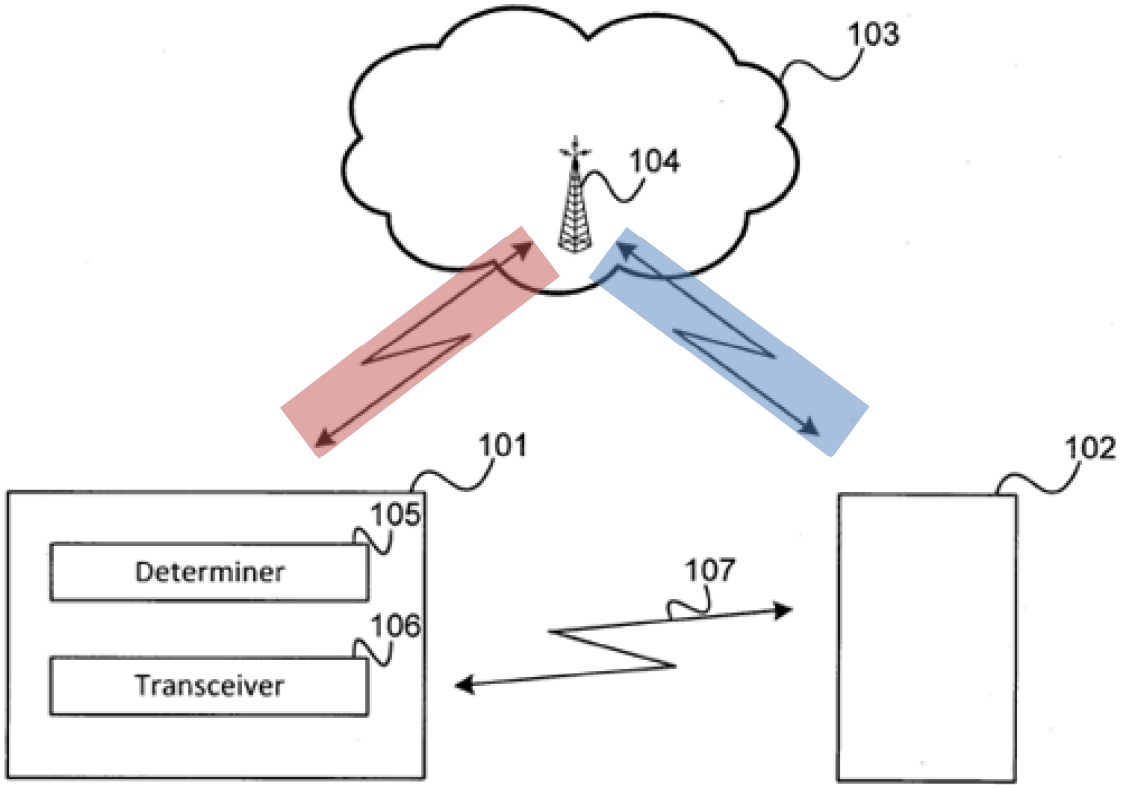
#### 1. Claim 1

**a. [1p] Method for establishing a device-to-device (D2D) communication session between mobile devices which are mutually connectable via a D2D communication channel and individually connectable to a mobile network, comprising:**

133. To the extent the preamble is limiting, *Teo* discloses the preamble. *Teo* discloses "a method for setting up a communication between a communication

terminal of a cellular mobile communication system and another communication terminal of the cellular mobile communication system." EX1005, 8:1-4. *Teo*'s cellular mobile communication system comprises "communication terminal 101, another communication terminal 102 and a communication network 103 for providing a communication connection between the communication terminal and the other communication terminal via at least one base station 104 of the communication network." *Id.*, 4:11-17. The "communication terminal 101 is a (mobile) communication terminal." EX1005, 4:10-11. The communication terminals comprise a "determiner 105 configured to determine an encryption key for secure communication between the communication terminal 101 and the other communication terminal 102 via a radio interface 107 between the communication terminal 101 and the other communication terminal 102." *Id.*, 4:19-24. The communication terminals also comprise "a transceiver configured to perform secure communication" between the two communication terminals via the radio interface. *Id.*, 4:26-31. Figure 1 of *Teo*, copied and annotated below, shows an example of *Teo*'s cellular mobile communication system:

FIG 1




EX1005, Fig. 1 (annotated)

134. *Teo*'s communication terminals disclose "*mobile devices*." As discussed above, *Teo* explains that "communication terminal 101 is a (mobile) communication terminal." EX1005, 4:10-11. A POSITA would have understood the other communication terminals described in *Teo* (*e.g.*, "communication terminal 102") to also be "(mobile) communication terminal[s]." *See* EX1005, 10:4-6 (describing a communication system that comprises "a first mobile terminal…[and] a second mobile terminal."). And *Teo*'s communication terminals (*i.e.*, "*mobile devices*") are "*mutually connectable via a D2D communication*

*channel*," at least because these communication terminals are able to directly communicate with each other via a radio interface. EX1005, 4:26-30 ("The communication terminal 101 further comprises a transceiver 106 configured to ***perform secure communication with the other communication terminals [102] via the radio interface 107 between the communication terminal 101 and the other communication terminal 102***." (emphasis added)), 5:11-13 ("According to an embodiment ***the secure communication is direct communication between the communication terminal and the other communication terminal***." (emphasis added)). Because *Teo*'s radio interface 107 facilitates direct communication between the communication terminals, the radio interface discloses "*a D2D communication channel*."

135. *Teo*'s communication terminals (*i.e.*, "*mobile devices*") are "*individually connectable to a mobile network*," at least because these communication terminals are each connected to communication network 103 via base station 104. As shown above in annotated Figure 1 of *Teo*, communication terminal 101 is connected with communication network 103 via a first connection with base station 104 (as indicated by the arrow annotated with a red box), and communication terminal 102 is connected with communication network 103 via a second connection with base station 104 (as indicated by the arrow annotated with a blue box).

136. *Teo*'s method for setting up direct communication between the communication terminals discloses a "[*m*]*ethod for establishing a device-to-device (D2D) communication session between mobile devices*." *Teo*'s method includes, in a first step, determining an encryption key for secure communication. *Id.*, 8:12-15, Fig. 2 (step 201). In a second step, the communication terminals perform secure communication with each other via the radio interface between the two communication terminals by using the determined encryption key. *Id.*, 8:17-21, Fig. 2 (step 202). As discussed above, "the secure communication is ***direct communication*** between the communication terminal and the other communication terminal." *Id.*, 5:11-13 (emphasis added). Thus, *Teo* discloses this claim element.

137. For at least these reasons, *Teo* discloses the preamble.

**b. [1a] preloading an initiation key on each of the mobile devices, the initiation key being associated with a validity period;**

138. *Teo* discloses Claim Element [1a] through at least its disclosure of loading a "pre-shared key DMK" and a "lifetime of DMK" parameter associated with it to different mobile communication terminals.

139. As discussed above with reference to Claim Element [1p], *Teo* discloses a method for setting up direct communication between mobile communication terminals. *Teo* explains that this direct communication is secure

because the messages exchanged by the mobile communication terminals are encrypted according to an "encryption key." EX1005, 8:17-21. *Teo* explains that the mobile communication terminals are given a pre-shared key, DMK (Direct Communication Master Key), which is used to derive the encryption key, DTEK. *Id.*, 37:20-23 ("The DMK may be used as a source for keying materials required by upper layers. DAK is derived from DMK and belongs to a pair of HR-MSs."), 38:1-7 ("The DCMAC-DTEK prekey is derived from DAK and is used to derive other keys:…Direct Communication Traffic Encryption (DTEK) Key.").

140. *Teo* explains that the mobile communication terminals, in one embodiment, obtain the pre-shared DMK from the base station to which the mobile communication terminals are connected. Figure 5 of *Teo* is a flow diagram that describes how the pre-shared DMK is obtained according to this embodiment. First, a first mobile communication terminal (*i.e.*, HR-MS1) sends a first message (*i.e.*, DC_Request_MSG#1) to a base station (*i.e.*, HR-BS) requesting a "direct communication pre-shared key DMK to be shared with" a second mobile communication terminal (*i.e.*, HR-MS2). *Id.*, 11:12-17, Fig. 5 (Step 501). HR-BS then sends a second message (*i.e.*, DC_Request_MSG#2) to HR-MS2 to inform HR-MS2 of the HR-MS1's request. *Id.*, 12:1-7, Fig. 5 (Step 502). HR-MS2 may then send a response message (*i.e.*, DC_REPLY_MSG#3) back to HR-BS informing HR-BS that HR-MS2 accepts the request for direct communication. *Id.*,

12:15-13:2, Fig. 5 (Step 503). Upon receiving the response message and determining that the HR-MS2 has accepted the request for direct communication, HR-BS "generates the DMK" and sends the DMK to both HR-MS1 and HR-MS2 in encrypted messages DC_REPLY_MSG#5 and DC_REPLY_MSG#6, respectively. *Id.*, 13:4-14:19, Fig. 5 (Step 504). HR-MS1 and HR-MS2 each decrypt the message it received from HR-BS and "obtains DMK and its lifetime key_lifetime." *Id.*, 14:21-15:2, Fig. 5 (Step 505).

141. *Teo*'s DMK is an "*initiation key*" because the mobile communication terminals (*e.g.*, HR-MS1 and HR-MS2) establish direct communication with each other based on the DMK that they previously received from the mobile network (*e.g.*, base station HR-BS). As will be discussed in more detail below with respect to Claim Element [1d], *Teo* describes how the DMK is used to derive another key, the DTEK, that is used to encrypt messages during direct communication between the mobile communication terminals. *See*, *e.g.*, *id.*, 37:20-23 ("The DMK may be used as a source for keying materials required by upper layers. DAK is derived from DMK and belongs to a pair of HR-MSs."), 38:1-7 ("The DCMAC-DTEK prekey is derived from DAK and is used to derive other keys:…Direct Communication Traffic Encryption (DTEK) Key."), 38:24-25 (describing that the DTEK is "used to encrypt data in direct communications"). The DMK is therefore an "*initiation key*" because it initiates the mobile communication terminals' ability

to directly communicate with each other by facilitating the generation of other information necessary for direct communication, such as the DTEK. This is consistent with the '572 Patent, which states that "*initiation key*" "essentially functions as an authorization token in that a mobile device needs the initiation key to establish the D2D communication session." EX1001, 4:28-30.

142. *Teo*'s DMK is "*preload*[*ed*]" because it is obtained by the communication terminals before a direct communication session is established. Indeed, *Teo* refers to the DMK as a "***pre-shared*** key DMK." EX1005, 10:27-28 (emphasis added). In one embodiment, *Teo* describes that the mobile communication terminals may establish a direct communication only after they obtain the DMK. *See*, *e.g.*, *id.*, 18:7-19:3 (referring the "Pre-shared key scenario…where it is assumed that HR-MS1 and HR-MS2 shares a key ***prior to direct communications."*** (emphasis added)); 63:9-13 ("Finally, the third autonomous AKE solution is used in the event where two HR-MSs that wish[] to establish direct communications with each other autonomously have already established a pre-shared key DMK using the network-aided AKE protocol described above."). As discussed above, this is because other keying materials used during the direct communication are derived from the DMK. *See id.*, 37:20-25. This is consistent with the '572 Patent, which states that "the term preloading

refers to a loading of the initiation key on a mobile device before establishing the D2D communication session." EX1001, 3:34-37.

143. And *Teo*'s DMK is "*preload*[*ed*]…*on each of the mobile devices*" because the base station transmits the same DMK to each of the two mobile communication terminals. As discussed above, *Teo* explains that the base station "generates ***the*** DMK" and sends the DMK to both HR-MS1 and HR-MS2 in encrypted messages. *Id.*, 13:4-14:19 (emphasis added), Fig. 5 (Step 504). As will be discussed in more detail below with regard to Claim Element [1d], the same DMK being loaded to each of the mobile communication terminals allows the terminals to establish direct communication with each other. *See infra*, Section IX.A.1.e.

144. Finally, *Teo*'s DMK is "*associated with a validity period*" because the DMK has an associated lifetime, "key_lifetime." As described above, when the mobile stations decrypt the messages from the base station containing the DMK, the mobile stations obtain both the DMK "and its lifetime key_lifetime." *Id.*, 14:25-26, 15:1-2. The mobile stations also receive timestamps from the base station (*i.e.*, $T_{HR\text{-}BS}'$ and $T_{HR\text{-}BS}''$) in the messages containing the DMK values (*i.e.*, DC_REPLY_MSG#5 and DC_REPLY_MSG#6). *Id.*, 13:19-14:19, 17 (showing $T_{HR\text{-}BS}'$ in DC_REPLY_MSG#5 sent to HR-MS1), 18 (showing $T_{HR\text{-}BS}''$ in DC_REPLY_MSG#6 sent to HR-MS2). It would be manifestly obvious to a

POSITA that the DMK is valid from the period starting at the time indicated by the received timestamp through the expiration of the DMK's lifetime as indicated by the "key_lifetime" value. *See*, *e.g.*, EX1009, Section 8.10 ("No encryption key should be used for an indefinite period. It should expire automatically like passports and licenses. …***For any cryptographic application, there must be a policy that determines the permitted lifetime of a key***." (emphasis added)); *see also* EX1015, 35 (showing that a "Life Type" parameter's value defines the lifetime of a Security Association (SA) in seconds), 5 (defining Security Association as a "set of policy and key(s) used to protect information"). This understanding is consistent with the '572 Patent, which states that the "validity period indicates a period in time in which the initiation key is deemed to be valid for use in establishing the D2D communication session." EX1001, 3:52-54.

**c. [1b] and on each of the mobile devices: verifying a validity of the initiation key based on a current time;**

145. *Teo* renders obvious Claim Element [1b] in light of *Madoukh*. As discussed above, *Teo* teaches that its pre-shared DMK (*i.e.*, the "initiation key") has an associated lifetime, "key_lifetime." EX1005, 14:21-15:2, Fig. 5 (Step 505). And *Madoukh* discloses a "key lifetime manager operable to monitor encryption key expiration dates and request new encryption keys upon the expiration of old encryption keys." EX1011, [0007].

146. A POSITA would have understood that *Teo*'s "key_lifetime" reflects the duration for which the DMK is valid. *See supra*, Section IX.A.1.b. Accordingly, a POSITA would have understood that in implementing *Teo*, one would need to verify the validity of the DMK based on the current time before using the DMK. And it would have been obvious to use the teachings of *Madoukh* in doing so. Thus, a POSITA would have found it obvious to implement *Madoukh*'s key lifetime manager to monitor whether *Teo*'s DMK has expired by checking whether the current time falls within the range of the DMK's lifetime (*i.e.*, the time period starting at the time of the received timestamp (*e.g.*, $T_{HR\text{-}BS}'$) through the expiration of the associated "key_lifetime"). A POSITA would have understood that when the key lifetime manager determines that the DMK is not expired because the current time falls within the DMK's lifetime, the DMK has been verified as valid (*i.e.*, not expired).

147. And a POSITA would have understood that each mobile communication terminal that receives a DMK and associated key_lifetime value from a base station (*e.g.*, HR-MS1 and HR-MS2) would have performed this verification to validate the DMK before using it.

148. Thus, *Teo* renders obvious this claim element in view of *Madoukh*. This combination would have been obvious for the additional reasons explained above in Sections VIII.I-J.

**d. [1c] requesting a further initiation key via the mobile network if no initiation key is deemed valid;**

149. *Teo* renders obvious Claim Element [1c] in light of *Madoukh*. The *Teo*-*Madoukh* combination renders obvious verifying the validity of *Teo*'s DMKs by using a key lifetime manager (as taught by *Madoukh*) to compare the current time to the DMKs' lifetime, "key_lifetime." *See supra*, Section IX.A.1.c. *Makoukh* also explains that the key lifetime manager is operable to "request new encryption keys upon the expiration of old encryption keys." EX1011, [0007]. It would have been obvious to a POSITA to implement *Madoukh*'s key lifetime manager in *Teo*'s mobile communication terminals such that the terminals request a new DMK from the base station (*e.g.*, HR-BS) upon determining that a currently-held DMK has expired (*i.e.*, is not "*deemed valid*") (as disclosed by *Madoukh*). This implementation would have been obvious because a POSITA would have recognized that *Teo*'s DMKs would eventually expire and thus need to be replaced. *See* EX1009, 183 ("No encryption key should be used for an indefinite period. It should expire automatically like passports and licenses."). And because *Teo* teaches that the base station is part of a "communication network" that provides service to mobile terminals, a POSITA would have understood that this request would be made "*via the mobile network*." EX1005, 4:14-17.

150. Further, it would have been obvious to a POSITA that both mobile communication terminals (*e.g.*, both HR-MS1 and HR-MS2) would have requested a new DMK upon determining that a currently-held DMK is expired. As discussed above with reference to Claim Element [1a], *Teo* teaches that the base station transmits the same DMK value and associated lifetime, key_lifetime, to the two mobile communication terminals that agree to establish direct communication. *See supra*, Section IX.A.1.b. Because both mobile communication terminals would have received the same key_lifetime value, a POSITA would have understood that both mobile communication terminals would detect the expiration of the DMK at the same or similar times. Accordingly, a POSITA would have understood that when the DMK expires, both mobile communication terminals would have determined that the DMK is no longer valid and would therefore have requested a new DMK value from the base station.

151. Thus, the *Teo-Madoukh* combination renders obvious Claim Element [1c]. This combination would have been obvious for the additional reasons explained above in Sections VIII.I-J.

**e. [1d] if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel,**

152. The *Teo-Madoukh* combination renders obvious this claim element, at least through its disclosure of generating an encryption key, DTEK. As discussed above, *Teo* discloses a method for establishing direct communication between two mobile communication terminals. *See supra*, Section IX.A.1.a; EX1005, 5:11-13, 8:1-4. Establishing the direct communication involves generating an encryption key, which later encrypts the direct communications to ensure their security. *See supra*, Section IX.A.1.a; EX1005, 8:17-21, 38:24-25. *Teo* discloses "three AKE [Authenticated Key Exchange] protocols for Mutual Authentication of HR-MS and data security for Direct Communications," which involve generating the encryption key. EX1005, 18:7-19:3. One such protocol, referred to as the "pre-shared key approach," occurs when the two mobile communication terminals wishing to establish direct communication (*e.g.*, HR-MS1 and HR-MS2) have already received a pre-shared DMK (*e.g.*, as described above with reference to Claim Element [1a]). *Id.*, 18:10-19:3, 31:6-18, Fig. 12 (showing a flow diagram of the "pre-shared key approach"), Fig. 16 (showing a message flow diagram of the "pre-shared key approach").

153. In the pre-shared key approach, a first mobile communication terminal (*e.g.*, HR-MS1) uses its pre-shared DMK to compute three new keys: DAK, DCMAC, and DTEK. EX1005, 32:16-21 ("Step 1201: In 1603, HR-MS1 1601 selects a nonce $N_{HR\text{-}MS1}$ and uses the shared DMK and computes DAK…, the DCMAC… and DTEK…."), Fig. 12 (Step 1201). *Teo* explains that the DAK is derived from the DMK. *Id.*, 37:23-25 ("DAK is derived from DMK and belongs to a pair of HR-MSs."), 32:17-18 ("DAK = Dot16KDF(DMK, HR-MS1Addr | HR-MS2Addr | 'DAK', 160)"). The DCMAC and DTEK are then derived from the DAK. *Id.*, 38:1-7 ("The DCMAC-DTEK prekey is derived from DAK and is used to derive other keys: Direct Communication Cipher-based Message Authentication Code (DCMAC) key; Direct communication Traffic Encryption (DTEK) Key)"), 32:19 ("DCMAC = Dot16KDF(DAK, 'DCMAC_KEYS', 128)"), 32:21 ("DTEK = DOT16KDF(DAK, 'DTEK_KEY', 128")). The first mobile communication terminal then generates a "message digest," $\theta_{HR\text{-}MS1}$, which is "calculated using the DCMAC key," and sends $\theta_{HR\text{-}MS1}$ to the second mobile communication terminal (*e.g.*, HR-MS2) in a message called "DirectComms_KeyAgreement_MSG_#1." *Id.*, 32:23-30 ("DirectComms_KeyAgreement_MSG_#1 = NHR-MS1 | DMK_Sequence_No | DAKID | Key_lifetime | **$\theta_{HR\text{-}MS1}$**." (emphasis added)), 35 (explaining that $\theta_{HR\text{-}MS1}$ is a "[m]essage digest calculated using DCMAC key.").

154. Upon receiving the "DirectComms_KeyAgreement_MSG_#1" message, the second communication terminal uses the pre-shared DMK to compute its own set of DAK, DCMAC, and DTEK. *Id.*, 33:1-7 (In 1606, HR-MS2…uses the shared DMK and computes DAK…, DCMAC…, DTEK."), Fig. 12 (Step 1202). The second communication terminal uses the same functions to compute DAK, DCMAC, and DTEK as those used by the first mobile communication terminal. *See id.*, 32:17-21 ("DAK = Dot16KDF(**DMK**, HR-MS1Addr | HR-MS2Addr | "DAK", 160)" (emphasis added); "DCMAC = Dot16KDF(**DAK**, "DCMAC_KEYS", 128)" (emphasis added); "DTEK = DOT16KDF(DAK, "DTEK_KEY", 128)); 33:5-7 (showing the same functions used by HR-MS2 to compute DAK and DCMAC, respectively). Thus, because the first and second communication terminals have received the same DMK value, a POSITA would have understood that the second communication terminal generates the same DAK, DCMAC, and DTEK values as those generated by the first mobile communication terminal.

155. The second mobile communication terminal then "uses DCMAC to check $\theta_{HR\text{-}MS1}$," which the second mobile communication terminal received in the "DirectComms_KeyAgreement_MSG_#1" message. *Id.*, 33:7-8. A POSITA would have understood that the second mobile communication terminal "check[s] $\theta_{HR\text{-}MS1}$" by independently computing $\theta_{HR\text{-}MS1}$ using the DCMAC calculated by the

second communication terminal, consistent with the DCMAC's intended use for message authentication. *See* EX1005, 38:14-16 ("The DCMAC key is derived from DAK and used for message authentication for the messages sent during direct communications."). Because the DCMAC held by the first and second communication terminal are expected to have the same value (because these keys are derived from the DAK, which is derived from the pre-shared DMK), a POSITA would have understood that the second mobile communication terminal would have successfully checked $\theta_{HR\text{-}MS1}$ if it its independent calculation of $\theta_{HR\text{-}MS1}$ matched the value received from the first mobile communication terminal, thereby indicating that the two mobile communication terminals share the same DMK value and have generated the same DAK, DCMAC, and DTEK keys.

156. After verifying the received $\theta_{HR\text{-}MS1}$, the second mobile communication terminal computes a second message digest, $\theta_{HR\text{-}MS2}$. EX1005, 33:8-12. Like $\theta_{HR\text{-}MS1}$, $\theta_{HR\text{-}MS2}$ is calculated "using DCMAC key." *Id.*, 36 (explaining that $\theta_{HR\text{-}MS2}$ is a "[m]essage digest calculated using DCMAC key."). The second mobile communication terminal then sends $\theta_{HR\text{-}MS2}$ to the first mobile communication terminal in a message called "DirectComms_KeyAgreement_MSG_#2." *Id.*, 33:14-24 ("DirectComms_KeyAgreement_MSG_#2 = $N_{HR\text{-}MS1}$ | $N_{HR\text{-}MS2}$ | DAKID | DMK_Sequence_No | DC_Security_Parameters | **$\theta_{HR\text{-}MS2}$**." (emphasis added)).

The second mobile communication terminal also includes its security capabilities in the DirectComms_KeyAgreement_MSG_#2 message. *Id.*, 33:14-24 ("DirectComms_KeyAgreement_MSG_#2 = $N_{HR\text{-}MS1}$ | $N_{HR\text{-}MS2}$ | DAKID | DMK_Sequence_No | **DC_Security_Parameters** | $\theta_{HR\text{-}MS2}$." (emphasis added)); 36 (explaining that the "DC_Security_Parameters" notation indicates "[t]he requesting HR-MS's security capabilities").

157. Upon receiving the "DirectComms_KeyAgreement_MSG_#2" message, the first communication terminal "checks DAKID and $\theta_{HR\text{-}MS2}$." *Id.*, 33:27-30, Fig. 12 (Step 1203). Similar to the scenario discussed above wherein the second communication terminal "uses DMCAC to check $\theta_{HR\text{-}MS1}$," a POSITA would have understood that the first communication terminal "checks" $\theta_{HR\text{-}MS2}$ by independently computing $\theta_{HR\text{-}MS2}$ (which was generated based on the DCMAC value calculated by the second communication terminal) with its own DCMAC value. A POSITA would have understood the "check" to be successful if the independently-computed and the received $\theta_{HR\text{-}MS2}$ values are the same, which would only occur if the DCMAC value used by the second communication terminal to generate $\theta_{HR\text{-}MS2}$ matches the DCMAC value calculated by the first communication module (as discussed above with reference to Step 1201 in *Teo*). Upon a successful check, the first communication terminal generates a new message digest, $\theta_{HR\text{-}MS1}'$, which is "calculated using the DCMAC key." EX1005,

33:30-34:3, 36 (explaining that $\theta_{HR\text{-}MS1}'$ is a "[m]essage digest calculated using DCMAC key"). The first communication terminal then sends $\theta_{HR\text{-}MS1}'$ to the second communication terminal in a message called "DirectComms_KeyAgreement_MSG_#3." *Id.*, 34:5-15 ("DirectComms_KeyAgreement_MSG_#3 = $N_{HR\text{-}MS1}$ | $N_{HR\text{-}MS2}$ | DMK_Sequence_No | DC_SAID | DC_Security_Parameters | **$\theta_{HR\text{-}MS1}'$**." (emphasis added)). The second communication terminal also includes its security capabilities in the DirectComms_KeyAgreement_MSG_#3 message. *Id.*, ("DirectComms_KeyAgreement_MSG_#3 = $N_{HR\text{-}MS1}$ | $N_{HR\text{-}MS2}$ | DMK_Sequence_No | DC_DAID | **DC_Security_Parameters** | $\theta_{HR\text{-}MS1}'$." (emphasis added)); 36 (explaining that the "DC_Security_Parameters" notation indicates "[t]he supporting HR-MS's security capabilities").

158. Upon receiving the "DirectComms_KeyAgreement_MSG_#3" message, the second communication terminal "checks the received nonces for freshness and $\theta_{HR\text{-}MS1}'$." *Id.*, 34:17-19, Fig. 12 (Step 1204). Similar to the scenarios discussed above, a POSITA would have understood that the first communication terminal "checks" $\theta_{HR\text{-}MS1}'$ by independently computing $\theta_{HR\text{-}MS1}'$ (which was generated based on the DCMAC value calculated by the first communication terminal) with its own DCMAC value. A POSITA would have understood the "check" to be successful if the independently-computed and the

received $\theta_{HR\text{-}MS1}'$ values are the same, which would only occur if the DCMAC value used by the first communication terminal to generate $\theta_{HR\text{-}MS1}'$ matches the DCMAC value calculated by the second communication module (as discussed above with reference to Step 1202 in *Teo*). Upon a successful check, the second communication terminal "applies the negotiated security parameters and is ready for direct communications with HR-MS1" (*i.e.*, the first mobile communication terminal). EX1005, 34:19-21.

159. *Teo*'s pre-shared key approach just discussed discloses "*generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel*," as recited in Claim 1. As discussed above, *Teo* describes how the mobile communication terminals (*e.g.*, HR-MS1 and HR-MS2) use the DMK (*i.e.*, the "*initiation key*", *see* Claim Element [1a] above) to generate a DTEK (*i.e.*, the "*session key*") during the pre-shared key approach. EX1005, 32:17-18 ("DAK = Dot16KDF(**DMK**, HR-MS1Addr | HR-MS2Addr | 'DAK', 160)" (emphasis added)), 38:1-7 ("The DCMAC-DTEK prekey is derived from DAK and is used to derive other keys:…Direct Communication Traffic Encryption (DTEK) Key."), 32:21 ("DTEK = DOT16KDF(**DAK**, 'DTEK_KEY', 128") (emphasis added)). A POSITA would have understood *Teo*'s pre-shared key approach to be a "*key agreement procedure*" because the pre-shared key approach involves the two

mobile communication terminals agreeing to keys used for direct communications (*i.e.*, DAK, DCMAC, and DTEK) by confirming that the two mobile communication terminals have generated the same keys. Indeed, the messages exchanged during this procedure, called "DirectComms_**KeyAgreement**" messages (emphasis added), confirm that the pre-shared key approach would be considered a "*key agreement procedure*." EX1005, 32:23-30, 33:14-24, 34:5-15.

160. Further, *Teo* explains that the DTEK "is used to encrypt data in direct communications." *Id.*, 38:24-25. Accordingly, a POSITA would have understood the DTEK to be a "session key" because it facilitates a direct communication session between the two mobile communication terminals. This role in encrypting data in direct communications between the mobile communication terminals is consistent with the '572 Patent's description of the "session key." *See* EX1001, 4:13-17 ("The session key constitutes a key used for cryptographically protecting messages in a communication session, ***such as confidentiality protection using encryption*** or integrity protection using message authentication codes." (emphasis added)).

161. *Teo* discloses that the "encryption key" (*i.e.*, DTEK) is determined "by exchanging messages with the other communication terminal via the radio interface between the communication terminal and the other communication terminal" (*i.e.*, via "*the D2D communication channel*"). EX1005, 5:23-27. Thus,

*Teo*'s disclosure of the mobile communication terminals generating the DTEK (*i.e.*, "*session key*") during the pre-shared key approach (*i.e.*, "*key agreement procedure*") based on the pre-shared DMK (*i.e.*, "*initiation key*") teaches "*generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel*."

162. A POSITA would have understood that the pre-shared key approach discussed above would have occurred only after the mobile communication terminals determine that the DMK (*i.e.*, the "*initiation key*") is valid, *e.g.*, based on comparing the current time with the DMK's key_lifetime relative to the time stamp indicating the start of DMK's validity period (*e.g.*, $T_{HR\text{-}BS}'$). *See supra*, Sections IX.A.1.c-d. Thus, a POSITA would have understood that the pre-shared key approach is performed only "*if the initiation key is deemed valid*," as recited in Claim 1.

**f. [1e] the key agreement procedure resulting in the session key based on a match of the respective initiation keys used by each of the mobile devices;**

163. *Teo* discloses this claim element. As discussed above with reference to Claim Element [1d], during the pre-shared key approach, both of the mobile communication terminals use the pre-shared DMK to generate additional keys—the DAK, DCMAC, and DTEK. *See supra*, Section IX.A.1.e; *see* EX1005,

EX1005, 32:16-21 ("Step 1201: In 1603, HR-MS1 1601 selects a nonce $N_{HR\text{-}MS1}$ and uses the shared DMK and computes DAK…, the DCMAC… and DTEK…."), 33:1-7 (In 1606, HR-MS2…uses the shared DMK and computes DAK…, DCMAC…, DTEK."), 38:1-6 ("The DCMAC-DTEK prekey is derived from DAK and is used to derive other keys: Direct Communication Cipher-based Message Authentication Code (DCMAC) key."). The DCMAC is used to generate and verify message digests (*e.g.*, $\theta_{HR\text{-}MS1}$, $\theta_{HR\text{-}MS2}$, and $\theta_{HR\text{-}MS1}'$) sent by one mobile communication terminal to the other. *See supra*, Section IX.A.1.e; EX1005, 35 (explaining that $\theta_{HR\text{-}MS1}$ is a "[m]essage digest calculated using DCMAC key."), 36 (explaining that $\theta_{HR\text{-}MS2}$ is a "[m]essage digest calculated using DCMAC key" and that $\theta_{HR\text{-}MS1}'$ is a "[m]essage digest calculated using DCMAC key"), 37:7-8 (explaining that the second mobile communication terminal "uses DCMAC to check $\theta_{HR\text{-}MS1}$"). Upon receiving a message digest, a mobile communication terminal "checks" the message digest and continues with the pre-shared key approach upon successful verification. EX1005, 33:1-12, 33:27-34:3, 34:17-24.

164. A POSITA would have understood that these message digests are verified by the receiving mobile communication terminal only if said receiving mobile communication terminal has generated the same DCMAC value as the DCMAC value used to generate the message digest at the sending mobile communication terminal. *See supra*, Section IX.A.1.e; EX1005, 37:7-8

(explaining that the second mobile communication terminal "uses DCMAC to check $\theta_{HR\text{-}MS1}$"). Therefore, a POSITA would have understood that successful verification of these message digests indicates that the mobile communication terminals have received and used matching DMK values, because the DMK is used to generate the DAK, which is then used to generate the DCMAC. EX1005, 37:23-25 ("DAK is derived from DMK and belongs to a pair of HR-MSs."). The DCMAC and DTEK are then derived from the DAK. *Id.*, 38:1-6 ("The DCMAC-DTEK prekey is derived from DAK and is used to derive other keys: Direct Communication Cipher-based Message Authentication Code (DCMAC) key…").

165. Thus, a POSITA would have understood that the mobile communication terminals would successfully complete *Teo*'s pre-shared key approach only if the DMKs held by each of said mobile communication terminals matched. If the DMKs did not match, a POSITA would have understood that the various keys generated from it would be different in each mobile communication terminal, and the "checks" made by the mobile communication terminals on the received message digests (*e.g.*, $\theta_{HR\text{-}MS1}$, $\theta_{HR\text{-}MS2}$, and $\theta_{HR\text{-}MS1}'$) would have failed. Accordingly, *Teo*'s pre-shared key approach to generating the DTEK (*i.e.*, the "*session key*") results in a valid DTEK only when the DMK (*i.e.*, the "*initiation key*") held by each mobile communication terminal is the same value (*i.e.*, "*match*[*es*]"). *Teo* therefore renders obvious this claim element.

**g. [1f] establishing the D2D communication session over the D2D communication channel based on the session key.**

166. *Teo* discloses this claim element. As discussed above with reference to Claim Element [1p], *Teo* generally discloses a two-step method wherein (1) an encryption key for secure direct communication is determined and (2) mobile communication terminals perform secure direct communication with each other based on the determined encryption key. *See supra*, Section IX.A.1.a; *see also* EX1005, 8:12-21. As discussed above with reference to Claim Element [1d], *Teo* discloses the generation of the DTEK (*i.e.*, the "*session key*"), during a key agreement procedure between two mobile communication terminals. *Teo* explains that the DTEK is "used to encrypt data in direct communications." EX1005, 38:24-25. A POSITA would have therefore understood *Teo*'s DTEK to be the "encryption key" used during secure communication between the mobile communication terminals. And as discussed above with reference to Claim Element [1p], *Teo* discloses that the secure direct communication between the two mobile communication terminals occurs via a radio interface between the two communication terminals (*i.e.*, the "D2D communication channel"). *See supra*, Section IX.A.1.a.

167. Thus, *Teo* discloses establishing a secure direct communication between mobile communication terminals (*i.e.*, "*establishing the D2D*

*communication session*") via a radio interface between the two communication terminals (*i.e.*, "*over the D2D communication channel*") based on a determined encryption key, DTEK (*i.e.*, "*based on the session key*"). *Teo* therefore discloses this claim element.

2. **Claim 2. Method according to claim 1, wherein the preloading the initiation key comprises providing the initiation key to each of the mobile devices via the mobile network when each respective mobile device is connected to the mobile network.**

168. *Teo* discloses Claim 2. As discussed above with reference to Claim Element [1a], *Teo* discloses a process whereby two mobile communication terminals (*e.g.*, HR-MS1 and HR-MS2) obtain a "pre-shared key DMK" (*i.e.*, an "*initiation key*") from a base station after the mobile communication terminals agree to establish direct communication with each other. *See supra*, Section IX.A.1.b. Because *Teo* teaches that the base station is part of the "communication network" of *Teo*, a POSITA would have understood that the DMK is provided "*via the mobile network*." EX1005, 4:14-17 ("a communication network 103 for providing a communication connection between the communication terminal and the other communication terminal via at least ***one base station 104 of the communication network***" (emphasis added)). And a POSITA would have understood that the base station's ability to send the DMK to the mobile communication terminals indicates that the base station provides the DMK (*i.e.*,

the initiation key) "*when each respective mobile device is connected to the mobile network*." If the mobile communication terminals were not connected to the base station (*i.e.*, the "*mobile network*"), the base station would be unable to send any messages, such as the messages that contain the DMK, to the mobile communication terminals.

169. Thus, *Teo*'s disclosure of a base station sending a "pre-shared DMK" to two mobile communication terminals teaches Claim 2.

3. **Claim 14. Method according to claim 1, wherein the key agreement procedure comprises: a three-pass authentication procedure; or a use of the initiation key to encrypt a message exchange between the mobile devices for obtaining a shared secret, and a Diffie-Hellman key exchange procedure which is initiated based on the shared secret.**

170. *Teo* discloses Claim 14, at least because *Teo* teaches "*wherein the key agreement procedure comprises: a three-pass authentication procedure*."[3] As discussed above with reference to Claim Element [1d], *Teo* discloses a "pre-shared key approach" (*i.e.*, "*key agreement procedure*") whereby two mobile communication terminals exchange "message digests" in three separate messages (*i.e.*, "DirectComms_KeyAgreement_MSG_#1,"
"DirectComms_KeyAgreement_MSG_#2, and

[3] I do not address the alternative limitation, "*or a use of the initiation key to encrypt a message exchange between the mobile devices for obtaining a shared secret, and a Diffie-Hellman key exchange procedure which is initiated based on the shared secret*."

"DirectComms_KeyAgreement_MSG_#3") and subsequently checking the message digests to authorize direct communication with each other. *See supra*, Section IX.A.1.e; *see also* EX1005, 32:26-33, 33:17-30, 34:8-19. A POSITA would have understood that a successful check indicates that the terminals have generated the same DCMAC, which indicates that the terminals have received the same DMK and are thereby authenticating each other for direct communication. *See supra*, Section IX.A.1.e. *Teo*'s pre-shared key approach comprises "*a three-pass authentication procedure*" at least because the pre-shared key approach includes the exchange of three messages between the two mobile communication terminals to authenticate the terminals for direct communication.

171. This understanding is consistent with the '572 Patent, which characterizes Figure 7 of the '572 Patent, copied and annotated below, as example of the "three-pass authentication procedure."

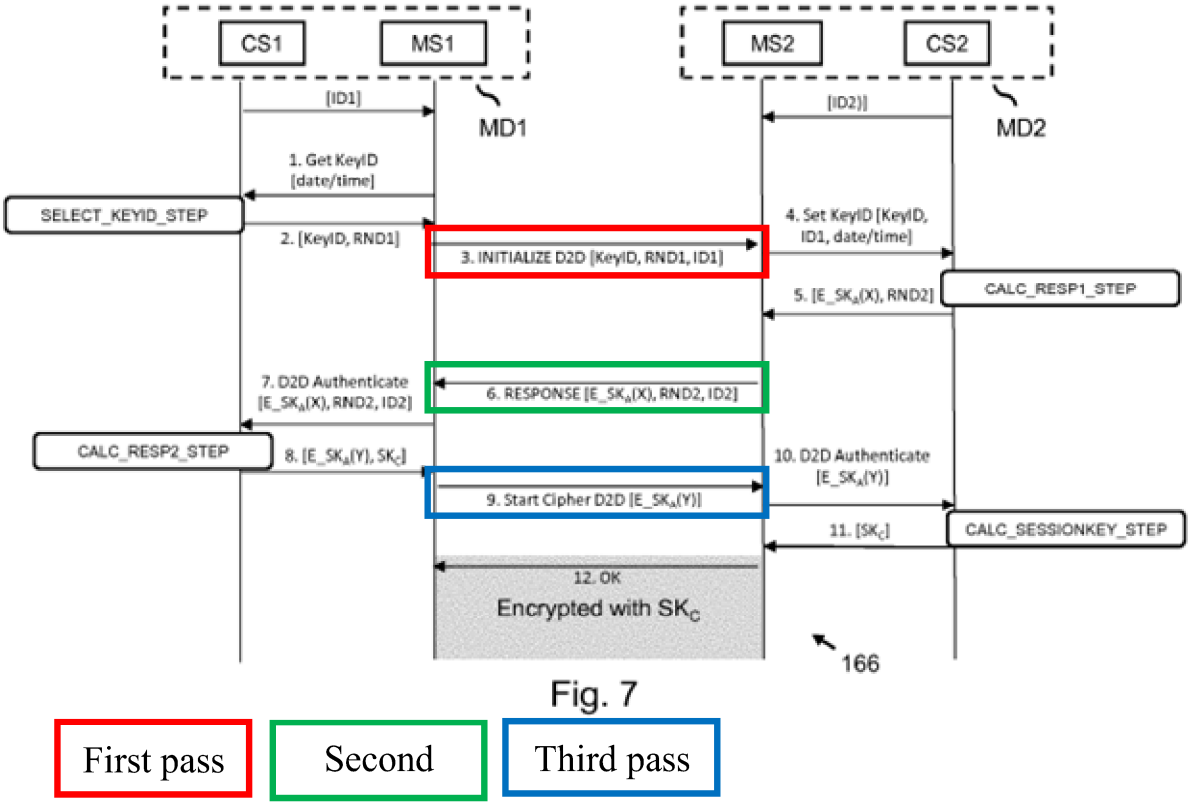



Fig. 7

First pass | Second | Third pass

172. EX1001, Fig. 7 (annotations added), 13:64-14:6. As shown, Figure 7, like *Teo*, involves the exchange of three messages between mobile devices attempting to authenticate each other for D2D communication. The '572 Patent's characterization of this procedure as a "three-pass authentication procedure" is consistent with a POSITA's understanding that a "three-pass" procedure is one in which three messages of the authentication protocol are exchanged. *See, e.g.*, EX1009, 516-517 (describing the well-known Shamir's ***three-pass*** protocol which involves the exchange of three messages).

173. *Teo* therefore discloses Claim 14.

### B. Ground 2: Claims 3-5 and 15-17 are Unpatentable as they are Rendered Obvious by *Teo* in view of *Madoukh* and *Hawkes*

174. It is my opinion *Teo* in view of *Madoukh* and *Hawkes* renders obvious claims 3-5 and 15-17.

#### 1. Claim 3. Method according to claim 1, wherein the preloading the initiation key comprises storing the initiation key in a secure storage area of each respective mobile device.

175. The *Teo-Madoukh-Hawkes* combination discloses Claim 3. As discussed above in Section IX.A with reference to Claim 1, *Teo* discloses mobile communication terminals (*i.e.*, "*mobile device*[*s*]") that receive a pre-shared key, DMK, from a base station. *See supra*, Section IX.A.1.b. *Hawkes* discloses a mobile device that stores security credentials, such as a "public key," in a "universal integrated circuit card (UICC)." EX1006, [0098] ("The card interface 1170 may be configured to accommodate a card 1172 (e.g., a Subscriber Identity module (SIM) card, a universal integrated circuit card (UICC), or other card) storing security credential(s) of the device 1100."), [0032] (describing a "public key" as being a part of a "security credential"). *Hawkes* further explains that the UICC may include a "secure storage area." *See id.*, [1278] ("If the H-SLP address can not be found in the ***secure storage area of the UICC*** (USIM/SIM),…" (emphasis added)).

176. A POSITA would have understood that the *Teo-Madoukh-Hawkes* combination discloses mobile communication terminals that each include UICCs for storing the pre-shared DMK (*i.e.*, the "*initiation key*") after the DMK is received from the base station. A POSITA would have understood that the received DMK could have been stored in the "secure storage area" location of the respective UICCs (*i.e.*, in the secure storage area of the first mobile communication terminal's UICC, and in the secure storage area of the second mobile communication terminal's UICC), as taught by *Hawkes*, because *Hawkes* teaches using the UICC to store keys. A POSITA would have been motivated to store the DMK in the "secure storage area" of the UICC to prevent the DMK from being stolen or otherwise compromised, thereby increasing the security of any subsequent direct communication. This understanding is confirmed by the '572 Patent, which describes "storing the initiation key in a secure storage area of each respective mobile device," where "[t]he secure storage area provided by such a trusted computing subsystem, *e.g.*, ***the memory of the UICC***, is well suited for securely storing the initiation key on the mobile device." EX1001, 5:22-25 (emphasis added).

177. The *Teo-Madoukh-Hawkes* combination discloses Claim 3. This combination would have been obvious for the additional reasons explained above in Sections VIII.K-L.

### 2. Claim 4. Method according to claim 3, wherein the secure storage area is provided by a trusted computing subsystem of each respective mobile device.

178. The *Teo-Madoukh-Hawkes* combination discloses Claim 4. As discussed above with respect to Claim 3, *Hawkes* discloses a UICC that includes a "secure storage area," which a POSITA would have understood could be used to store a key, such as *Teo*'s DMK. *See supra*, Section IX.C.1. *Hawkes*' UICC discloses a "*trusted computing subsystem*." A POSITA would have understood the UICC to be a well-known component used in mobile devices to not only securely store sensitive information, but also to perform computations with that information. *See* EX1014, 5 (describing the UICC as a "smart card" that has "a primary role of storing credentials and performing sensitive cryptographic computations"). Accordingly, a POSITA would have understood the UICC to be a "*trusted computing subsystem*." This understanding is confirmed by the '572 Patent, which acknowledges that a UICC is "[a]n example of a removable trusted computing subsystem." EX1001, 5:17-22. Thus, the *Teo-Madoukh-Hawkes* combination discloses Claim 4. This combination would have been obvious for the additional reasons explained above in Sections VIII.K-L.

3. **Claim 5. Method according to claim 4, wherein at least one of the group of: verifying the validity of the initiation key, and using the initiation key in performing the key agreement procedure, is performed by the trusted computing subsystem.**

179. The *Teo-Madoukh-Hawkes* combination renders obvious Claim 5. As discussed above with reference to Claim 4, the UICC disclosed by *Hawkes* is a well-known component that is used for "storing credentials and performing sensitive cryptographic computations" (emphasis added). *See supra*, Section IX.B.2; *see also* EX1014, 5. Under the *Teo-Madoukh-Hawkes* combination, it would have been obvious to a POSITA that the UICC would have verified the validity of the DMK (*i.e.*, "*initiation key*") and performed the pre-shared key approach for generating an encryption key (*i.e.*, "*performing a key agreement procedure*") as discussed above with reference to Claim 1. Because these operations involve the use of the security-sensitive pre-shared key DMK, a POSITA would have found it obvious to use the UICC, which was well known for "performing sensitive cryptographic computations." *See* EX1014, 5. Thus, the *Teo-Madoukh-Hawkes* combination renders obvious Claim 5. This combination would have been obvious for the additional reasons explained above in Sections VIII.K-L.

4. **Claim 15**

**a. [15p] A non-transitory computer-readable medium configured to store instructions for, upon execution of the instructions on a mobile device, causing the mobile device to establish a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to a mobile network, by:**

180. If the preamble is limiting, the *Teo-Madoukh-Hawkes* combination discloses the preamble. The Petition explains above in Claim Element [1p] how *Teo* discloses a "[*m*]*ethod for establishing a device-to-device (D2D) communication between mobile devices which are mutually connectable via a D2D communication channel and indiv*id*ually connectable to a mobile network*." The only difference between Claim Element [1p] and Claim Element [15p] is that this element adds that a mobile device includes "[*a*] *non-transitory computer-readable medium configured to store instructions for, upon execution of the instructions on a mobile device, causing the mobile device to establish a device-to-device (D2D) communication session with a further mobile device,…*" This element was well known.

181. *Teo*'s mobile communication terminals store a pre-shared key DMK (*i.e.*, "*initiation key*") and perform a "pre-shared key approach" (*i.e.*, "*key agreement procedure*") to establish an encryption key DTEK (*i.e.*, "*session key*").

*See* Claim Elements [1p]-[1f]. A POSITA would have known that a mobile communication terminal is a hardware component in a communications network. For example, *Teo* describes the mobile communication terminals (also referred to as "mobile stations") could be used by rescue teams to directly communicate with each other in the event of a disaster, suggesting that the terminals are mobile phones or similar hardware devices that facilitate direct communication between people. *See* EX1005, 1:14-23; *see also id*., Figs. 3, 6, 9 (generally depicting the mobile communication terminals (*i.e.*, "HR-MSs") as mobile telephone-like hardware devices); *see also* EX1020, 9:5-14 (describing a mobile station (MS) as a "phone").

182. And a POSITA would have known that a mobile communication terminal would have required a non-transitory memory (*e.g.*, SD card) storing instructions that would have allowed the mobile communications terminal to perform its task. *See* EX1006, [0032], [0098]; EX1014, 5 (explaining that *Hawkes*' UICC would have been understood to be a component that performs the memory functions); *see also* EX1020, 5:53-6:16, Fig. 3 (describing that programmable memory and non-programmable read-only memory (ROM) provide "stored program control" that drives a mobile station's operations). Accordingly, a POSITA would have known that the mobile communications terminals in *Teo* had a non-transitory memory storing instructions that, when executed on the mobile

communications terminal, would have allowed the mobile communications terminal to perform its tasks.

**b. [15a] storing an initiation key which is provided during a preloading procedure, the initiation key being associated with a validity period;**

183. *See* Claim Element [1a] and Claim 3.

**c. [15b] verifying a validity of the initiation key based on a current time;**

184. *See* Claim Element [1b].

**d. [15c] requesting a further initiation key via the mobile network if no initiation key is deemed valid;**

185. *See* Claim Element [1c].

**e. [15d] if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by the mobile device matches an initiation key used by the further mobile device; and**

186. *See* Claim Elements [1d]-[1e].

**f. [15e] establishing the D2D communication session over the D2D communication channel based on the session key.**

187. *See* Claim Element [1f].

5. **Claim 16**

**a. [16p] Mobile device for establishing a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to a mobile network, the mobile device comprising:**

188. If the preamble is limiting, the *Teo-Madoukh-Hawkes* combination discloses the preamble. Claim Element [16p]'s recitation of "[*m*]*obile device for establishing a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and indiv*id*ually connectable to a mobile network, the mobile device comprising*," corresponds to Claim Element [1p]'s recitation of "*mobile devices which are mutually connectable via a D2D communication channel and indiv*id*ually connectable to a mobile network*" and is disclosed for the same reasons explained in Claim Element [1p]. *See* Claim Element [1p].

**b. [16a] a storage area for storing an initiation key which is provided during a preloading procedure, the initiation key being associated with a validity period; and**

189. *See* Claim Element [1a] and Claim 3.

**c. [16b] a computing subsystem for:**

190. *See* Claim 5.

**d. [16c] verifying a validity of the initiation key based on a current time;**

191. *See* Claim 5 and Claim Element [1b].

**e. [16d] requesting a further initiation key via the mobile network if no initiation key is deemed valid;**

192. *See* Claim 5 and Claim Element [1c].

**f. [16e] if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by the mobile device matches an initiation key used by the further mobile device; and**

193. *See* Claim Elements [1d]-[1e].

**g. [16f] a mobile subsystem for establishing the D2D communication session over the D2D communication channel based on the session key.**

194. I explain above in Claim Element [1f] how *Teo* discloses "*establishing the D2D communication session over the D2D communication channel based on the session key*." The only difference between Claim Element [1f] and Claim Element [16f] is that this element adds that the "*establishing*" is performed by "*a mobile subsystem*." This element was well known.

195. *Teo*'s mobile communication terminals establish a direct communication session with each other based on a computed encryption key,

DTEK (*i.e.*, "session key"). *See* Claim Element [1f]. A POSITA would have known that a mobile communication terminal is a hardware component in a communications network. For example, *Teo* describes the mobile communication terminals (also referred to as "mobile stations") could be used by rescue teams to directly communicate with each other in the event of a disaster, suggesting that the terminals are mobile phones or similar hardware devices that facilitate direct communication between people. *See* EX1005, 1:14-23; *see also id.*, Figs. 3, 6, 9 (generally depicting the mobile communication terminals (*i.e.*, "HR-MSs") as mobile telephone-like hardware devices); *see also* EX1020, 9:5-14 (describing a mobile station (MS) as a "phone").

196. And a POSITA would have known and that a mobile communication terminal (also referred to as a "mobile station") would have would have required a subsystem that facilitates the exchange of messages necessary to establish the direct communication session. *See, e.g.*, EX1020, 6:3-12, Fig. 3 (describing that a mobile station includes an antenna, transceiver, and processor that allow wireless communication). It would have been obvious to a POSITA that *Hawkes*' system-on-chip device and the components included therein (*e.g.*, the wireless controller, processor, and memory), which are taught by *Hawkes* as facilitating the transmission of data, teaches such a subsystem. EX1006, [0098]-[0100]. Accordingly, a POSITA would have known that *Teo*'s mobile communication

terminals would include "a mobile subsystem" for establishing a direct communication session between the mobile communication terminals. This understanding is confirmed by the '572 Patent, which explains that "[a]n example of a mobile subsystem is a mobile System on a Chip (SoC) comprising an application processor, a display processor, one or more modems, an integrated LTE radio." EX1001, 9:15-18

6. **Claim 17**

**a. [17p] Mobile network arranged for preloading an initiation key on a mobile device when the mobile device is connected to the mobile network, the initiation key being associated with a validity period, the mobile device for establishing a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to the mobile network, the mobile device comprising:**

197. If the preamble is limiting, the *Teo-Madoukh-Hawkes* combination discloses the preamble. I explain above in Claim Element [1p] how *Teo* discloses a "[*m*]*ethod for establishing a device-to-device (D2D) communication between mobile devices which are mutually connectable via a D2D communication channel and indiv*id*ually connectable to a mobile network*." The Petition explains above in Claim Element [1a] how *Teo* discloses "*preloading an initiation key on each of the mobile devices, the initiation key being associated with a validity period*." The

Petition explains above in Claim 2 how *Teo* discloses "*wherein the preloading the initiation key comprises provi*d*ing the initiation key to each of the mobile devices via the mobile network when each respective mobile device is connected to the mobile network*." Claim Element [17p] is written from the perspective of the "[m]obile network" that is "arranged for preloading an initiation key"; this "[m]obile network" corresponds to the "mobile network" of Claim Element [1p]. Thus, Claim Element [17p] is disclosed for the same reasons explained in Claim Elements [1p] and [1a] and Claim 2.

**b. [17a] a computing subsystem for:**

198. *See* Claim 5 and Claim Element [16b].

**c. [17b] verifying a validity of the initiation key based on a current time;**

199. *See* Claim 5 and Claim Elements [1b] and [16c].

**d. [17c] requesting a further initiation key via the mobile network if no initiation key is deemed valid;**

200. *See* Claim 5 and Claim Elements [1c] and [16d].

**e. [17d] if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by the mobile device matches an initiation key used by the further mobile device; and**

201. *See* Claim Elements [1d]-[1e].

**f. [17c] a mobile subsystem for establishing the D2D communication session over the D2D communication channel based on the session key.**

202. *See* Claim Elements [1f] and [16f].

### C. Ground 3: Claims 6-9 are Unpatentable as they are Rendered Obvious by *Teo* in view of *Madoukh* and RFC 4279

In my opinion, *Teo* in view of *Madoukh* and RFC 4279 renders obvious Claims 6-9.

#### 1. Claim 6.

**a. [6a] Method according to claim 1, further comprising: preloading a set of initiation keys on each of the mobile devices, the set of initiation keys key being associated with a respective set of validity periods; and**

203. The *Teo*-*Madoukh*-RFC 4279 combination renders obvious this claim element. As discussed above with reference to Claim Element [1a], *Teo* discloses a base station (*e.g.*, HR-BS) sending a pre-shared DMK (*i.e.*, "initiation key") and

its associated "key_lifetime" to two mobile communication terminals (*e.g.* HR-MS1 and HR-MS2). *See supra*, Section IX.A.1.b. *Teo* explains that its system may be applied when several emergency rescue personnel need to directly communicate with each other in the event of a disaster, for example. It would have been obvious to a POSITA that in such a scenario, there would be many mobile communication terminals that would need to communicate with each other. Accordingly, a POSITA would have found it obvious that *Teo*'s base station would have transmitted several pre-shared DMKs (*i.e.*, "preloading a set of initiation keys") to the mobile communication terminals to facilitate their direct communication with each other. *See* EX1007, 5 ("Both clients and servers may have pre-shared keys with several different parties.")). And it would have been obvious to a POSITA that each of the respective keys sent by the base station would have its own "key_lifetime" value and, therefore, its own "validity period" indicated by the time period between the time stamp included in the message carrying the pre-shared DMK (and the associated key_lifetime) and the expiration of the key_lifetime value.

204. The *Teo*-*Madoukh*-RFC 4279 combination therefore renders obvious this claim element. This combination would have been obvious for the additional reasons discussed above in Sections VIII.M-N.

**b. [6b] performing a key synchronization procedure between the mobile devices over the D2D communication channel for selecting a matching one of the set of initiation keys on each of the mobile devices as the initiation key.**

205. The *Teo*-*Madoukh*-RFC 4279 combination renders obvious this claim element. RFC 4279 describes a "PSK [pre-shared key] Key Exchange Algorithm" whereby a client seeking to establish a TLS communication with a server indicates the pre-shared key that should be used for communication establishment. EX1007, 4-5. In particular, RFC 4279 explains that "[b]oth clients and servers may have pre-shared keys with several different parties." *Id.* Accordingly, the "client indicates which key to use" to establish a TLS connection by "including a 'PSK identity' in the ClientExchange message" sent from the client to the server. *Id.*, 4-5, 1 (explaining that pre-shared keys are used to establish a TLS connection). RFC 4279 explains that if the server does not recognize the "PSK identity," the server can send an alert message back to the client. *Id.*, 5. A POSITA would have understood that if the server does recognize the PSK identity, the server would understand that it possesses (*e.g.*, it has received) the same pre-shared key as the one selected by the client and that it can commence TLS connection establishment with the client.

206. A POSITA would have understood that the *Teo*-RFC 4279 combination teaches a system whereby a base station transmits both a set of pre-

shared DMKs and a set of "PSK identities" associated with the pre-shared DMKs to mobile terminals, where each pre-shared DMK is associated with a "PSK identity" that identifies the pre-shared DMK, as taught by RFC 4279. EX1007, 4-5. When a first mobile communication terminal wishes to establish a direct communication session with a second mobile communication terminal, the first terminal will transmit to the second terminal the "PSK identity" associated with the pre-shared DMK that the first terminal wants to use during the pre-shared key approach for generating a DTEK, as suggested by RFC4279. *See* EX1007, 4-5. Upon receiving the "PSK identity," the second terminal will determine if it received a pre-shared DMK associated with the received "PSK identity;" if a positive determination is made (*e.g.*, by determining that the second terminal has a pre-shared DMK with an associated "PSK identity" that matches the "PSK identity" received from the first terminal), the second terminal would determine that the first and second terminals have received matching pre-shared DMKs and that they may proceed with the pre-shared key approach for generating an encryption key as described in *Teo*. *See* EX1007, 4-5.

207. A POSITA would have understood that this procedure whereby the mobile terminals agree to a pre-shared DMK for future use discloses a "key synchronization procedure between the mobile devices." Further, it would have been obvious to a POSITA that this agreement procedure would occur via direct

communication between the mobile terminals (as suggested by RFC 4279), thereby rendering obvious "over the D2D communication channel." And because the agreement procedure would result in the mobile terminals each agreeing to use the same pre-shared DMK from the several received pre-shared DMKs, the *Teo-Madoukh*-RFC 4279 combination renders obvious "for selecting a matching one of the set of initiation keys on each of the mobile devices as the initiation key." This combination would have been obvious for the additional reasons discussed above in Sections VIII.M-N.

2. **Claim 7.**

**a. [7a] Method according to claim 6, further comprising: preloading a set of key identifiers on each of the mobile devices, each of the set of key identifiers identifying a respective one of the set of initiation keys; and**

208. As discussed above with reference to Claim Element [6a], the *Teo-Madoukh*-RFC 4279 combination renders obvious a system wherein a base station sends a set of "PSK Identities" that are associated with, and uniquely identify, a set of pre-shared DMKs. *See supra*, Section IX.C.1.a. For the same reasons discussed above with reference to Claim Element [6a], the *Teo-Madoukh*-RFC 4279 combination renders obvious Claim Element [7a]. This combination would have been obvious for the additional reasons discussed above in Sections VIII.M-N.

**b. [7b] performing the key synchronization procedure based on an exchange of one or more of the set of key identifiers between the mobile devices.**

209. As discussed above with reference to Claim Element [6b], the *Teo-Madoukh*-RFC 4279 combination renders obvious a system wherein a first mobile communication terminal and a second mobile communication terminal agree to a common pre-shared DMK based on the exchange of a "PSK identifier" associated with a selected pre-shared DMK. *See supra*, Section IX.C.1.b. For the same reasons discussed above with reference to Claim Element [6b], the *Teo-Madoukh*-RFC 4279 combination renders obvious Claim Element [7b]. This combination would have been obvious for the additional reasons discussed above in Sections VIII.M-N.

3. **Claim 8. Method according to claim 6, further comprising disabling or removing the initiation key from the set of initiation keys after use in establishing the D2D communication session.**

210. The *Teo-Madoukh*-RFC 4279 combination renders obvious Claim 8. As discussed above in Ground 1, a POSITA would have found it obvious to implement *Madoukh*'s key lifetime manager to monitor the lifetime of *Teo*'s DMK (*i.e.*, "*initiation key*"), and deactivate the DMK after it expires. *See supra*, Sections VIII.I-J; EX1011, [0008] ("…the key lifetime manager is operable to flag the expired keys ***and to change or deactivate the expired keys***…." (emphasis added)).

And it would have been obvious to a POSITA that in the emergency scenario described in *Teo*, there would be many mobile communication terminals that would need to communicate with each other, and, therefore, that several pre-shared DMKs (*i.e.*, a "*set of initiation keys*") would be transmitted to the terminals to facilitate their direct communication with each other. *See supra*, Section IX.C.1.a. A POSITA would have understood that when direct communication between terminals is desired in such a scenario, one of the several DMKs would be selected for establishing direct communication. Further, a POSITA would have understood that after the DMK is used to establish direct communication, the DMK would eventually expire (*i.e.*, as indicated by the expiration of the DMK's "key_lifetime"). *See* EX1009, 183 ("No encryption key should be used for an indefinite period. It should expire automatically like passports and licenses.").

211. It would have been obvious to a POSITA that in such a scenario, one could implement *Madoukh*'s key lifetime manager to flag and "deactivate" a DMK after the DMK is used and expires, as taught by *Madoukh*. A POSITA would have understood that the deactivated DMK is "*disable*[*ed*]" from further use. The *Teo*-*Madoukh*-RFC 4279 combination therefore renders obvious Claim 8. This combination would have been obvious for the additional reasons discussed above in Sections VIII.M-N.

#### 4. Claim 9. Method according to claim 6, wherein the set of validity periods is constituted at least in part by different but overlapping validity periods.

212. The *Teo-Madoukh*-RFC 4279 combination renders obvious Claim 9. As discussed above with reference to Claim 6, it would have been obvious to a POSITA that the *Teo-Madoukh*-RFC 4279 combination renders obvious preloading a set of DMKs (*i.e.*, "*initiation keys*") and associated key_lifetime values on each of *Teo*'s mobile communication terminals (*i.e.*, "*mobile devices*"). *See supra*, Section IX.C.1. A POSITA would have considered in a natural occurrence in a system that deploys several DMKs with a corresponding set of "*validity periods*" (*i.e.*, the time periods extending from the time indicated by the time stamp of the received messages from the base station through the end of the key_lifetime value), that the set of validity periods would include some different but overlapping time periods. *Park*, for example, describes such an occurrence. *Park* discloses that a set of keys may be generated with different validity periods (*e.g.*, one year, one month, six hours, three hours, or one hour), and distributed simultaneously such that the different validity periods overlap. EX1017, [0050], [0052], [0059], [0064]. Thus, the *Teo-Madoukh*-RFC 4279 combination renders obvious Claim 9. This combination would have been obvious for the reasons discussed above in Sections VIII.M-N.

### D. Ground 4: Claim 10 is Unpatentable as it is Rendered Obvious by *Teo* in view of *Madoukh*, RFC 4279, and *Kumar*

213. It is my opinion that *Teo* in view of *Madoukh*, RFC 4279, and *Kumar* renders obvious Claim 10.

#### 1. Claim 10. Method according to claim 1, wherein the initiation key is associated with a virtual network identity, and wherein the verifying the validity of the initiation key further comprises determining a match of the virtual network identity on each of the mobile devices via the D2D communication channel.

214. The *Teo-Madoukh*-RFC 4279- *Kumar* combination renders obvious Claim 10. As discussed above with respect to Claim 6, The *Teo-Madoukh*-RFC 4279 combination teaches a system wherein mobile communication terminals exchange a "PSK identity" associated with a pre-shared DMK (*i.e.*, "*initiation key*") to confirm that the terminals have received the same DMK (which may be used to establish direct communication between the terminals). *See supra*, Section IX.C.1. And *Kumar* teaches associating a "Preshare Key" (PSK) with an SSID value, which identifies a wireless network with which the PSK is associated. EX1016, Fig. 2, [0057]. A POSITA would have understood that the *Teo-Madoukh*-RFC 4279-*Kumar* combination teaches associating *Teo*'s DMK with a wireless network identity (*e.g.*, SSID, as taught by *Kumar*), and exchanging that associated network identity in place of RFC 4279's "PSK identity" to verify that the terminals have received the same DMK (*i.e.*, the DMK associated with the

exchanged network identity), as taught by RFC 4279. When implemented in such a manner, the network identity (*e.g.*, SSID) teaches "*a virtual network identity*," which the '572 Patent describes simply as an identifier that identifies a network with which an initiation key is associated. EX1001, 10:40-51. Accordingly, *Teo-Madoukh*-RFC 4279-*Kumar* combination renders obvious "*wherein the initiation key is associated with a virtual network identity*."

215. And as discussed above with reference to Claim 6, the *Teo-Madoukh*-RFC 4279 combination teaches that the mobile communication terminals exchange the "PSK identity" to confirm that both terminals have received the same DMK, thereby verifying that the associated DMK is valid for generating a DTEK. *See supra*, Section IX.C.1. A POSITA would have recognized that this verification would operate in the same manner when the "PSK identity" is implemented as a network identity (*e.g.*, SSID), as taught by *Kumar* and described above. Thus, the *Teo-Madoukh*-RFC 4279-*Kumar* combination renders obvious "*verifying the validity of the initiation key further comprises determining a match of the virtual network identity on each of the mobile devices via the D2D communication channel*" at least for the same reasons discussed above with reference to Claim [6b]. This combination would have been obvious for the additional reasons discussed above in Sections VIII.O-P.

### E. Ground 5: Claims 11-12 are are Unpatentable as they are Rendered Obvious by *Teo* in view of *Madoukh* and S3-070234

216. It is my opinion that Claims 11 and 12 are rendered obvious by *Teo* in view of *Madoukh* and S3-070234.

#### 1. Claim 11. Method according to claim 1, wherein the initiation key is associated with a usage count for limiting a number of uses of the initiation key, and wherein the verifying the validity of the initiation key is further based on the usage count.

217. The *Teo-Madoukh*-S3-070234 combination renders obvious Claim 11. *Teo* describes mobile communication terminals using a pre-shared key DMK to derive additional keys (*e.g.*, DAK). *See supra*, Section IX.A.1.b. S3-070234 describes implementing "counters related to limiting key usage, e.g. to limit the number of key derivations from one parent key." EX1013, 1-2. A POSITA would have found it obvious to implement S3-070234's usage-based counter in *Teo*'s mobile communication terminal such that the terminal counts the number of times the DMK is used to derive additional keys and limits the usage of the DMK based on that count.

218. Accordingly, it would have been obvious to a POSITA that before a mobile communication terminal uses a pre-shared DMK, the terminal would check the counter associated with the DMK to confirm that a threshold number of uses has not been exceeded. A POSITA would have understood that this check, along

with checking whether the DMK's lifetime has expired as discussed above with reference to Claim Elements [1a] and [1b], would ensure that the DMK is valid for use. Thus, the *Teo-Madoukh*-S3-070234 combination renders obvious Claim 11. This combination would have been obvious for the additional reasons discussed above in Sections VIII.Q-R.

2. **Claim 12. Method according to claim 11, further comprising adjusting the usage count after use of the initiation key in establishing the D2D communication session.**

219. As discussed above with reference to Claim 11, a POSITA would have found it obvious to modify *Teo*'s mobile communication terminal such that it counts the number of times a DMK (*i.e.,* "*initiation key*") is used to derive additional keys and limits the usage of the DMK based on that count (as taught by S3-070234). A POSITA would have considered updating (*i.e.*, "*adjusting*") the counter whenever the DMK is used to derive additional keys (*e.g.*, the DAK) to be an obvious step in implementing S3-070234's usage-based counter. Without this updating, the DMK's usage would not be accurately counted and limited in the manner suggested by S3-070234. *Id.*; EX1013, 1-2. Thus, the *Teo-Madoukh*-S3-070234 combination renders obvious Claim 12. This combination would have been obvious for the additional reasons discussed above in Sections VIII.Q-R.

## F. Ground 5: Claim 13 is Unpatentable as it is Rendered Obvious by *Teo* in view of *Madoukh* and *Thakare*

220. It is my opinion that Claim 13 is rendered obvious by *Teo* in view of *Madoukh* and *Thakare*.

### 1. Claim 13. Method according to claim 1, further comprising requesting a further initiation key via the mobile network if the key agreement procedure fails in providing the session key.

221. The *Teo-Madoukh-Thakare* combination renders obvious Claim 13. *Teo* teaches mobile communication terminals receiving, from a base station (*i.e.*, a component of a "*mobile network*"), a pre-shared key DMK (*i.e.*, "*initiation key*"), which is used in a pre-shared key approach (*i.e.*, "*key agreement procedure*") to generate a DTEK (*i.e.*, "*session key*"). *See supra*, Section IX.A.1. *Thakare* teaches requesting a new encryption key upon determining that data packets encrypted with the encryption key are not successfully authenticated. EX1018, [0009]. A POSITA would have found it obvious to implement *Thakare*'s process of requesting a new key upon encountering errors in the using the key into *Teo*'s system such that *Teo*'s terminals request a new DMK upon determining that pre-shared key approach fails in generating the DTEK. When facing such a failure, a POSITA would have recognized that a limited number of obvious options were available, and a POSITA would have considered requesting a new DMK to be one such common-sense response. *See, e.g.*, EX1011, [0007] (discussing requesting

new keys upon expiration of old keys). The *Teo-Madoukh-Thakare* combination therefore renders obvious Claim 13. This combination would have been obvious for the additional reasons discussed above in Sections VIII.S-T.

## X. CONCLUSION

222. The challenged claims of the '572 Patent do not claim a novel or non-obvious invention. For all of the reasons explained above, the identified combinations render all of the challenged claims obvious.

## XI. DECLARATION

223. I hereby declare that all the statements made in this Declaration are of my own knowledge and true; that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. § 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Executed in Atlanta, Georgia on May 12, 2023.

/ / Angelos Keromytis /
Angelos Keromytis

# Appendix 1

# Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)
## RFC 4279



## Revision differences

**From revision**

draft-ietf-tls-psk-09 (2005-06-22)

**To revision**

RFC 4279 (2005-12-05)

**Diff format**

Side-by-side | Before-after | Change bars | Inline

## Document history

Search

| Date | Rev. | By | Action |
|---|---|---|---|
| 2015-10-14 | 09 | (System) | Notify list changed from ekr@networkresonance.com, pasi.eronen@nokia.com, hannes.tschofenig@siemens.com to ekr@networkresonance.com |
| 2012-08-22 | 09 | (System) | post-migration administrative database adjustment to the Yes position for Sam Hartman |
| 2012-08-22 | 09 | (System) | post-migration administrative database adjustment to the No Objection position for David Kessens |
| 2005-12-06 | 09 | Amy Vezza | State Changes to **RFC Published** from **RFC Ed Queue** by **Amy Vezza** |
| 2005-12-06 | 09 | Amy Vezza | [Note]: 'RFC 4279' added by Amy Vezza |
| 2005-12-05 | 09 | (System) | RFC published |
| 2005-06-30 | 09 | Amy Vezza | State Changes to **RFC Ed Queue** from **Approved-announcement sent** by **Amy Vezza** |
| 2005-06-24 | 09 | Amy Vezza | IESG state changed to **Approved-announcement sent** |
| 2005-06-24 | 09 | Amy Vezza | IESG has approved the document |
| 2005-06-24 | 09 | Amy Vezza | Closed "Approve" ballot |
| 2005-06-23 | 09 | Russ Housley | State Changes to **Approved-announcement to be sent** from **IESG Evaluation::AD Followup** by **Russ Housley** |
| 2005-06-23 | 09 | Sam Hartman | [Ballot Position Update] Position for Sam Hartman has been changed to Yes from Discuss by Sam Hartman |
| 2005-06-22 | 09 | (System) | New version available: **draft-ietf-tls-psk-09.txt** |
| 2005-06-09 | 09 | Amy Vezza | State Changes to **IESG Evaluation::AD Followup** from **IESG Evaluation** by **Amy Vezza** |

| | | | |
|---|---|---|---|
| 09 | | Kessens | |
| 2005-06-08 | 09 | (System) | State Changes to **IESG Evaluation** from **IESG Evaluation - Defer** by **system** |
| 2005-06-07 | 09 | Sam Hartman | [Ballot discuss]<br>I sent a question to the tls working group about two issues:<br><br>1) labeling of identities<br><br>2) internationalization of identities.<br><br>Hearing nothing. I ... |
| 2005-06-07 | 09 | Sam Hartman | [Ballot Position Update] New position, Discuss, has been recorded for Sam Hartman by Sam Hartman |
| 2005-06-03 | 09 | Ted Hardie | [Ballot comment]<br>The document says:<br><br>IANA does not currently have a registry for TLS-related numbers, so<br>there are no IANA actions associated with ... |
| 2005-05-27 | 09 | (System) | Removed from agenda for telechat - 2005-05-26 |
| 2005-05-26 | 09 | Sam Hartman | State Changes to **IESG Evaluation - Defer** from **IESG Evaluation** by **Sam Hartman** |
| 2005-05-26 | 09 | Allison Mankin | [Ballot comment]<br>Glad to see this, it has been needed. It might be useful to state that examples of identities form<br>a very partial list ... |
| 2005-05-26 | 09 | Allison Mankin | [Ballot Position Update] New position, Yes, has been recorded for Allison Mankin by Allison Mankin |
| 2005-05-26 | 09 | Margaret Cullen | [Ballot Position Update] New position, No Objection, has been recorded for Margaret Wasserman by Margaret Wasserman |
| 2005-05-26 | 09 | Mark Townsley | [Ballot Position Update] New position, No Objection, has been recorded for Mark Townsley by Mark Townsley |
| 2005-05-26 | 09 | Bill Fenner | [Ballot Position Update] New position, No Objection, has been recorded for Bill Fenner by Bill Fenner |
| 2005-05-25 | 09 | David Kessens | [Ballot discuss]<br>I think the following comments that I received from the ops directorate should be addressed:<br><br>The document says in Section 5:<br><br>"To improve ... |
| 2005-05-25 | 09 | David Kessens | [Ballot Position Update] Position for David Kessens has been changed to Discuss from No Objection by David Kessens |
| 2005-05-25 | 09 | Alex Zinin | [Ballot Position Update] New position, No Objection, has been recorded for Alex Zinin by Alex Zinin |
| 2005-05-25 | 09 | David Kessens | [Ballot Position Update] New position, No Objection, has been recorded for David Kessens by David Kessens |
| 2005-05-25 | 09 | Jon Peterson | [Ballot Position Update] New position, No Objection, has been recorded for Jon Peterson by Jon Peterson |
| 2005-05-25 | 09 | Bert Wijnen | [Ballot Position Update] Position for Bert Wijnen has been changed to No Objection from Undefined by Bert Wijnen |

| | | | |
|---|---|---|---|
| 25 | | | sect 5.1 has as first bullet:<br><br>o IPv4 addresses are sent as dotted-decimal strings (e.g., "192.0.1.2"), not as 32-bit ... |
| 2005-05-25 | 09 | Bert Wijnen | [Ballot Position Update] New position, Undefined, has been recorded for Bert Wijnen by Bert Wijnen |
| 2005-05-25 | 09 | Michelle Cotton | IANA Comments:<br>Ack Ted's comments.<br>Are the authors sure that they do not want to have this registry published on the IANA website? If so, ... |
| 2005-05-24 | 09 | Scott Hollenbeck | [Ballot Position Update] New position, No Objection, has been recorded for Scott Hollenbeck by Scott Hollenbeck |
| 2005-05-23 | 09 | Ted Hardie | [Ballot comment]<br>The document says:<br><br>IANA does not currently have a registry for TLS-related numbers, so there are no IANA actions associated with ... |
| 2005-05-23 | 09 | Ted Hardie | [Ballot Position Update] New position, No Objection, has been recorded for Ted Hardie by Ted Hardie |
| 2005-05-20 | 09 | Brian Carpenter | [Ballot Position Update] New position, No Objection, has been recorded for Brian Carpenter by Brian Carpenter |
| 2005-05-18 | 09 | Russ Housley | Placed on agenda for telechat - 2005-05-26 by Russ Housley |
| 2005-05-18 | 09 | Russ Housley | [Ballot Position Update] New position, Yes, has been recorded for Russ Housley |
| 2005-05-18 | 09 | Russ Housley | Ballot has been issued by Russ Housley |
| 2005-05-18 | 09 | Russ Housley | Created "Approve" ballot |
| 2005-05-18 | 09 | Russ Housley | State Changes to **IESG Evaluation** from **Waiting for AD Go-Ahead::AD Followup** by **Russ Housley** |
| 2005-05-18 | 09 | Russ Housley | State Change Notice email list have been change to **ekr@networkresonance.com**, **pasi.eronen@nokia.com**, **hannes.tschofenig@siemens.com** from treese@acm.org, ekr@networkresonance.com, pasi.eronen@nokia.com, hannes.tschofenig@siemens.com |
| 2005-04-26 | 09 | (System) | Sub state has been changed to **AD Follow up** from New Id Needed |
| 2005-04-26 | 08 | (System) | New version available: **draft-ietf-tls-psk-08.txt** |
| 2005-04-03 | 09 | Russ Housley | State Changes to **Waiting for AD Go-Ahead::Revised ID Needed** from **Waiting for AD Go-Ahead** by **Russ Housley** |
| 2005-04-03 | 09 | Russ Housley | State Change Notice email list have been change to **treese@acm.org**, **ekr@networkresonance.com**, **pasi.eronen@nokia.com**, **hannes.tschofenig@siemens.com** from treese@acm.org, ekr@rtfm.com, pasi.eronen@nokia.com, hannes.tschofenig@siemens.com |
| 2005-04-01 | 09 | (System) | State has been changed to **Waiting for AD Go-Ahead** from **In Last Call** by system |
| 2005-03-18 | 09 | Amy Vezza | Last call sent |
| 2005-03-18 | 09 | Amy Vezza | State Changes to **In Last Call** from **Last Call Requested** by **Amy Vezza** |
| 2005-03-17 | 09 | Russ Housley | State Changes to **Last Call Requested** from **AD Evaluation::AD Followup** by **Russ Housley** |

| | | | |
|---|---|---|---|
| 17 | | | |
| 2005-03-17 | 09 | (System) | Ballot writeup text was added |
| 2005-03-17 | 09 | (System) | Last call text was added |
| 2005-03-17 | 09 | (System) | Ballot approval text was added |
| 2005-03-16 | 09 | (System) | Sub state has been changed to **AD Follow up** from New Id Needed |
| 2005-03-16 | 07 | (System) | New version available: **draft-ietf-tls-psk-07.txt** |
| 2005-03-06 | 09 | Russ Housley | State Changes to **AD Evaluation::Revised ID Needed** from **AD Evaluation** by **Russ Housley** |
| 2005-02-23 | 06 | (System) | New version available: **draft-ietf-tls-psk-06.txt** |
| 2005-01-04 | 09 | Russ Housley | State Changes to **AD Evaluation** from **Publication Requested** by **Russ Housley** |
| 2004-12-20 | 09 | Russ Housley | Draft Added by Russ Housley in state Publication Requested |
| 2004-12-17 | 05 | (System) | New version available: **draft-ietf-tls-psk-05.txt** |
| 2004-11-29 | 04 | (System) | New version available: **draft-ietf-tls-psk-04.txt** |
| 2004-11-18 | 03 | (System) | New version available: **draft-ietf-tls-psk-03.txt** |
| 2004-10-06 | 02 | (System) | New version available: **draft-ietf-tls-psk-02.txt** |
| 2004-08-18 | 01 | (System) | New version available: **draft-ietf-tls-psk-01.txt** |
| 2004-06-04 | 00 | (System) | New version available: **draft-ietf-tls-psk-00.txt** |

# Appendix 2

# RFC Index

CREATED ON: May - 12 - 2023

This file contains citations for all RFCs in numeric order. RFC citations appear in this format:

| Num | Information |
|---|---|
| #### | **Title of RFC** Author list [ Month Year ] (Format) (Obsoletes xxxx) (Obsoleted-By xxxx) (Updates xxxx) (Updated-By xxxx) (Also zzz##) (Status: status) (Stream: stream) (DOI: doi)<br><br>or #### Not Issued. |

For example:

| Num | Information |
|---|---|
| 5234 | **Augmented BNF for Syntax Specifications: ABNF** D. Crocker, P. Overell [ January 2008 ] (TXT, HTML) (Obsoletes RFC4234) (Also STD0068) (Status: INTERNET STANDARD) (Stream: IETF, WG: NON WORKING GROUP) (DOI: 10.17487/RFC5234) |

## Key to Citations

- #### is the RFC number.
- Following the number are the title, the author list, and the publication date.
- The format follows in parentheses. One or more of the following formats are listed: text (TXT), PostScript (PS), Portable Document Format (PDF), HTML, XML.
- "Obsoletes xxxx" refers to other RFCs that this one replaces.
- "Obsoleted-By xxxx" refers to RFCs that have replaced this one.
- "Updates xxxx" refers to other RFCs that this one merely updates but does not replace.
- "Updated-By xxxx" refers to RFCs that have updated but not replaced this one.
- "(Also zzz##)" gives pointer(s) to equivalent sub-series documents, if any. Here zzz is one of the sub-series designators STD, BCP, or FYI. In a few cases, the Also field points to an equivalent number in some other document series.
- The Status field gives the document's current status (see RFC 2026 and RFC 6410).
- The Stream field gives the document's stream (see RFC 4844), followed by Area and WG when relevant.
- The DOI field gives the Digital Object Identifier.

See the RFC Editor Web page for more information.

# RFC Index

Num Information

0001 **Host Software** S. Crocker [ April 1969 ] (TXT, HTML) (Status: UNKNOWN) (Stream: Legacy) (DOI: 10.17487/RFC0001)

0002 **Host software** B. Duvall [ April 1969 ] (TXT, PDF, HTML) (Status: UNKNOWN) (Stream: Legacy) (DOI: 10.17487/RFC0002)

10.17487/RFC4273)

4274 **BGP-4 Protocol Analysis** D. Meyer, K. Patel [ January 2006 ] (TXT, HTML) (Status: INFORMATIONAL) (Stream: IETF, Area: rtg, WG: idr) (DOI: 10.17487/RFC4274)

4275 **BGP-4 MIB Implementation Survey** S. Hares, D. Hares [ January 2006 ] (TXT, HTML) (Status: INFORMATIONAL) (Stream: IETF, Area: rtg, WG: idr) (DOI: 10.17487/RFC4275)

4276 **BGP-4 Implementation Report** S. Hares, A. Retana [ January 2006 ] (TXT, HTML) (Status: INFORMATIONAL) (Stream: IETF, Area: rtg, WG: idr) (DOI: 10.17487/RFC4276)

4277 **Experience with the BGP-4 Protocol** D. McPherson, K. Patel [ January 2006 ] (TXT, HTML) (Status: INFORMATIONAL) (Stream: IETF, Area: rtg, WG: idr) (DOI: 10.17487/RFC4277)

4278 **Standards Maturity Variance Regarding the TCP MD5 Signature Option (RFC 2385) and the BGP-4 Specification** S. Bellovin, A. Zinin [ January 2006 ] (TXT, HTML) (Status: INFORMATIONAL) (Stream: IETF, WG: IESG) (DOI: 10.17487/RFC4278)

4279 **Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)** P. Eronen, H. Tschofenig [ December 2005 ] (TXT, HTML) (Updated-By RFC8996) (Status: PROPOSED STANDARD) (Stream: IETF, Area: sec, WG: tls) (DOI: 10.17487/RFC4279)

4280 **Dynamic Host Configuration Protocol (DHCP) Options for Broadcast and Multicast Control Servers** K. Chowdhury, P. Yegani, L. Madour [ November 2005 ] (TXT, HTML) (Status: PROPOSED STANDARD) (Stream: IETF, Area: int, WG: dhc) (DOI: 10.17487/RFC4280)

4281 **The Codecs Parameter for "Bucket" Media Types** R. Gellens, D. Singer, P. Frojdh [ November 2005 ] (TXT, HTML) (Obsoleted-By RFC6381) (Status: PROPOSED STANDARD) (Stream: IETF, WG: NON WORKING GROUP) (DOI: 10.17487/RFC4281)

4282 **The Network Access Identifier** B. Aboba, M. Beadles, J. Arkko, P. Eronen [ December 2005 ] (TXT, HTML) (Obsoletes RFC2486) (Obsoleted-By RFC7542) (Status: PROPOSED STANDARD) (Stream: IETF, Area: sec, WG: radext) (DOI: 10.17487/RFC4282)

4283 **Mobile Node Identifier Option for Mobile IPv6 (MIPv6)** A. Patel, K. Leung, M. Khalil, H. Akhtar, K. Chowdhury [ November 2005 ] (TXT, HTML) (Status: PROPOSED STANDARD) (Stream: IETF, Area: int, WG: mip6) (DOI: 10.17487/RFC4283)

4284 **Identity Selection Hints for the Extensible Authentication Protocol (EAP)** F. Adrangi, V. Lortz, F. Bari, P. Eronen [ January 2006 ] (TXT, HTML) (Status: INFORMATIONAL) (Stream: IETF, WG: NON WORKING GROUP) (DOI: 10.17487/RFC4284)

4285 **Authentication Protocol for Mobile IPv6** A. Patel, K. Leung, M. Khalil, H. Akhtar, K. Chowdhury [ January 2006 ] (TXT, HTML) (Status: INFORMATIONAL) (Stream: IETF, Area: int, WG: mip6) (DOI: 10.17487/RFC4285)

4286 **Multicast Router Discovery** B. Haberman, J. Martin [ December 2005 ] (TXT, HTML) (Status: PROPOSED STANDARD) (Stream: IETF, Area: int, WG: magma) (DOI: 10.17487/RFC4286)

4287 **The Atom Syndication Format** M. Nottingham, R. Sayre [ December 2005 ] (TXT, HTML) (Updated-By RFC5988) (Status: PROPOSED STANDARD) (Stream: IETF, Area: app, WG: atompub) (DOI: 10.17487/RFC4287)

4288 **Media Type Specifications and Registration Procedures** N. Freed, J. Klensin [ December 2005 ] (TXT, HTML) (Obsoletes RFC2048) (Obsoleted-By RFC6838) (Status: BEST CURRENT PRACTICE) (Stream: IETF, WG: NON WORKING GROUP) (DOI: 10.17487/RFC4288)

4289 **Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures** N. Freed, J. Klensin [ December 2005 ] (TXT, HTML) (Obsoletes RFC2048) (Also BCP0013) (Status: BEST CURRENT PRACTICE) (Stream: IETF, WG: NON WORKING GROUP) (DOI: 10.17487/RFC4289)

4290 **Suggested Practices for Registration of Internationalized Domain Names (IDN)** J. Klensin [ December 2005 ] (TXT, HTML) (Status: INFORMATIONAL) (Stream: INDEPENDENT) (DOI: 10.17487/RFC4290)

4291 **IP Version 6 Addressing Architecture** R. Hinden, S. Deering [ February 2006 ] (TXT, HTML) (Obsoletes RFC3513) (Updated-By RFC5952, RFC6052, RFC7136, RFC7346, RFC7371, RFC8064) (Status: DRAFT STANDARD) (Stream: IETF, Area: int, WG: ipv6) (DOI: 10.17487/RFC4291)

# Appendix 3

The Wayback Machine - https://web.archive.org/web/20060219221316/http://www.rfc-editor.org:80/rfc/rfc4279.txt

Network Working Group
Request for Comments: 4279
Category: Standards Track

P. Eronen, Ed.
Nokia
H. Tschofenig, Ed.
Siemens
December 2005

# Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)

## Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

## Copyright Notice

Copyright (C) The Internet Society (2005).

## Abstract

This document specifies three sets of new ciphersuites for the Transport Layer Security (TLS) protocol to support authentication based on pre-shared keys (PSKs). These pre-shared keys are symmetric keys, shared in advance among the communicating parties. The first set of ciphersuites uses only symmetric key operations for authentication. The second set uses a Diffie-Hellman exchange authenticated with a pre-shared key, and the third set combines public key authentication of the server with pre-shared key authentication of the client.

ERICSSON EXHIBIT 1003, Page 140

The Wayback Machine - https://web.archive.org/web/20060219221316/http://www.rfc-editor.org:80/rfc/rfc4279.txt



Table of Contents

1. Introduction ....2
1.1. Applicability Statement ....3
1.2. Conventions Used in This Document ....4
2. PSK Key Exchange Algorithm ....4
3. DHE_PSK Key Exchange Algorithm ....6
4. RSA_PSK Key Exchange Algorithm ....7
5. Conformance Requirements ....8
5.1. PSK Identity Encoding ....8
5.2. Identity Hint ....9
5.3. Requirements for TLS Implementations ....9
5.4. Requirements for Management Interfaces ....9
6. IANA Considerations ....10
7. Security Considerations ....10
7.1. Perfect Forward Secrecy (PFS) ....10
7.2. Brute-Force and Dictionary Attacks ....10
7.3. Identity Privacy ....11
7.4. Implementation Notes ....11
8. Acknowledgements ....11
9. References ....12
9.1. Normative References ....12
9.2. Informative References ....12

## 1. Introduction

Usually, TLS uses public key certificates [TLS] or Kerberos [KERB] for authentication. This document describes how to use symmetric keys (later called pre-shared keys or PSKs), shared in advance among the communicating parties, to establish a TLS connection.

There are basically two reasons why one might want to do this:

- First, using pre-shared keys can, depending on the ciphersuite, avoid the need for public key operations. This is useful if TLS is used in performance-constrained environments with limited CPU power.

- Second, pre-shared keys may be more convenient from a key management point of view. For instance, in closed environments where the connections are mostly configured manually in advance, it may be easier to configure a PSK than to use certificates. Another case is when the parties already have a mechanism for setting up a shared secret key, and that mechanism could be used to "bootstrap" a key for authenticating a TLS connection.

ERICSSON EXHIBIT 1003, Page 141

The Wayback Machine - https://web.archive.org/web/20060219221316/http://www.rfc-editor.org:80/rfc/rfc4279.txt



This document specifies three sets of new ciphersuites for TLS. These ciphersuites use new key exchange algorithms, and reuse existing cipher and MAC algorithms from [TLS] and [AES]. A summary of these ciphersuites is shown below.

| CipherSuite | Key Exchange | Cipher | Hash |
|---|---|---|---|
| TLS_PSK_WITH_RC4_128_SHA | PSK | RC4_128 | SHA |
| TLS_PSK_WITH_3DES_EDE_CBC_SHA | PSK | 3DES_EDE_CBC | SHA |
| TLS_PSK_WITH_AES_128_CBC_SHA | PSK | AES_128_CBC | SHA |
| TLS_PSK_WITH_AES_256_CBC_SHA | PSK | AES_256_CBC | SHA |
| TLS_DHE_PSK_WITH_RC4_128_SHA | DHE_PSK | RC4_128 | SHA |
| TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA | DHE_PSK | 3DES_EDE_CBC | SHA |
| TLS_DHE_PSK_WITH_AES_128_CBC_SHA | DHE_PSK | AES_128_CBC | SHA |
| TLS_DHE_PSK_WITH_AES_256_CBC_SHA | DHE_PSK | AES_256_CBC | SHA |
| TLS_RSA_PSK_WITH_RC4_128_SHA | RSA_PSK | RC4_128 | SHA |
| TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA | RSA_PSK | 3DES_EDE_CBC | SHA |
| TLS_RSA_PSK_WITH_AES_128_CBC_SHA | RSA_PSK | AES_128_CBC | SHA |
| TLS_RSA_PSK_WITH_AES_256_CBC_SHA | RSA_PSK | AES_256_CBC | SHA |

The ciphersuites in Section 2 (with PSK key exchange algorithm) use only symmetric key algorithms and are thus especially suitable for performance-constrained environments.

The ciphersuites in Section 3 (with DHE_PSK key exchange algorithm) use a PSK to authenticate a Diffie-Hellman exchange. These ciphersuites protect against dictionary attacks by passive eavesdroppers (but not active attackers) and also provide Perfect Forward Secrecy (PFS).

The ciphersuites in Section 4 (with RSA_PSK key exchange algorithm) combine public-key-based authentication of the server (using RSA and certificates) with mutual authentication using a PSK.

## 1.1. Applicability Statement

The ciphersuites defined in this document are intended for a rather limited set of applications, usually involving only a very small number of clients and servers. Even in such environments, other alternatives may be more appropriate.

If the main goal is to avoid Public-Key Infrastructures (PKIs), another possibility worth considering is using self-signed certificates with public key fingerprints. Instead of manually configuring a shared secret in, for instance, some configuration file, a fingerprint (hash) of the other party's public key (or certificate) could be placed there instead.

ERICSSON EXHIBIT 1003, Page 142

The Wayback Machine - https://web.archive.org/web/20060219221316/http://www.rfc-editor.org:80/rfc/rfc4279.txt


It is also possible to use the SRP (Secure Remote Password) ciphersuites for shared secret authentication [SRP]. SRP was designed to be used with passwords, and it incorporates protection against dictionary attacks. However, it is computationally more expensive than the PSK ciphersuites in Section 2.

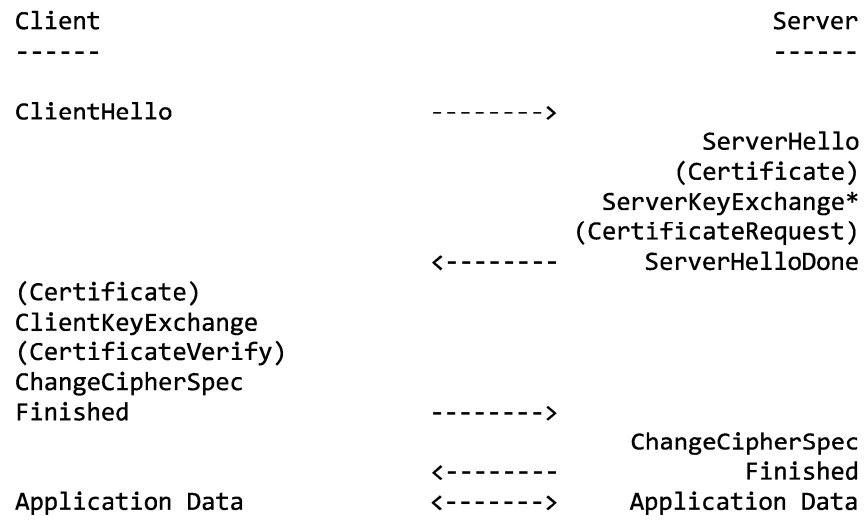
### 1.2. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [KEYWORDS].

## 2. PSK Key Exchange Algorithm

This section defines the PSK key exchange algorithm and associated ciphersuites. These ciphersuites use only symmetric key algorithms.

It is assumed that the reader is familiar with the ordinary TLS handshake, shown below. The elements in parenthesis are not included when the PSK key exchange algorithm is used, and "*" indicates a situation-dependent message that is not always sent.




The client indicates its willingness to use pre-shared key authentication by including one or more PSK ciphersuites in the ClientHello message. If the TLS server also wants to use pre-shared keys, it selects one of the PSK ciphersuites, places the selected ciphersuite in the ServerHello message, and includes an appropriate ServerKeyExchange message (see below). The Certificate and CertificateRequest payloads are omitted from the response.

ERICSSON EXHIBIT 1003, Page 143

The Wayback Machine - https://web.archive.org/web/20060219221316/http://www.rfc-editor.org:80/rfc/rfc4279.txt



Both clients and servers may have pre-shared keys with several different parties. The client indicates which key to use by including a "PSK identity" in the ClientKeyExchange message (note that unlike in [SHAREDKEYS], the session_id field in ClientHello message keeps its usual meaning). To help the client in selecting which identity to use, the server can provide a "PSK identity hint" in the ServerKeyExchange message. If no hint is provided, the ServerKeyExchange message is omitted. See Section 5 for a more detailed description of these fields.

The format of the ServerKeyExchange and ClientKeyExchange messages is shown below.

```
   struct {
       select (KeyExchangeAlgorithm) {
           /* other cases for rsa, diffie_hellman, etc. */
           case psk:  /* NEW */
               opaque psk_identity_hint<0..2^16-1>;
       };
   } ServerKeyExchange;

   struct {
       select (KeyExchangeAlgorithm) {
           /* other cases for rsa, diffie_hellman, etc. */
           case psk:   /* NEW */
               opaque psk_identity<0..2^16-1>;
       } exchange_keys;
   } ClientKeyExchange;
```

The premaster secret is formed as follows: if the PSK is N octets long, concatenate a uint16 with the value N, N zero octets, a second uint16 with the value N, and the PSK itself.

Note 1: All the ciphersuites in this document share the same general structure for the premaster secret, namely,

```
      struct {
          opaque other_secret<0..2^16-1>;
          opaque psk<0..2^16-1>;
      };
```

Here "other_secret" either is zeroes (plain PSK case) or comes from the Diffie-Hellman or RSA exchange (DHE_PSK and RSA_PSK, respectively). See Sections 3 and 4 for a more detailed description.

Note 2: Using zeroes for "other_secret" effectively means that only the HMAC-SHA1 part (but not the HMAC-MD5 part) of the TLS PRF

ERICSSON EXHIBIT 1003, Page 144

The Wayback Machine - https://web.archive.org/web/20060219221316/http://www.rfc-editor.org:80/rfc/rfc4279.txt


is used when constructing the master secret. This was considered more elegant from an analytical viewpoint than, for instance, using the same key for both the HMAC-MD5 and HMAC-SHA1 parts. See [KRAWCZYK] for a more detailed rationale.

The TLS handshake is authenticated using the Finished messages as usual.

If the server does not recognize the PSK identity, it MAY respond with an "unknown_psk_identity" alert message. Alternatively, if the server wishes to hide the fact that the PSK identity was not known, it MAY continue the protocol as if the PSK identity existed but the key was incorrect: that is, respond with a "decrypt_error" alert.

## 3. DHE_PSK Key Exchange Algorithm

This section defines additional ciphersuites that use a PSK to authenticate a Diffie-Hellman exchange. These ciphersuites give some additional protection against dictionary attacks and also provide Perfect Forward Secrecy (PFS). See Section 7 for discussion of related security considerations.

When these ciphersuites are used, the ServerKeyExchange and ClientKeyExchange messages also include the Diffie-Hellman parameters. The PSK identity and identity hint fields have the same meaning as in the previous section (note that the ServerKeyExchange message is always sent, even if no PSK identity hint is provided).

The format of the ServerKeyExchange and ClientKeyExchange messages is shown below.

```
   struct {
       select (KeyExchangeAlgorithm) {
           /* other cases for rsa, diffie_hellman, etc. */
           case diffie_hellman_psk:  /* NEW */
               opaque psk_identity_hint<0..2^16-1>;
               ServerDHParams params;
       };
   } ServerKeyExchange;

   struct {
       select (KeyExchangeAlgorithm) {
           /* other cases for rsa, diffie_hellman, etc. */
           case diffie_hellman_psk:   /* NEW */
               opaque psk_identity<0..2^16-1>;
               ClientDiffieHellmanPublic public;
       } exchange_keys;
   } ClientKeyExchange;
```

ERICSSON EXHIBIT 1003, Page 145

The Wayback Machine - https://web.archive.org/web/20060219221316/http://www.rfc-editor.org:80/rfc/rfc4279.txt



The premaster secret is formed as follows. First, perform the Diffie-Hellman computation in the same way as for other Diffie-Hellman-based ciphersuites in [TLS]. Let Z be the value produced by this computation (with leading zero bytes stripped as in other Diffie-Hellman-based ciphersuites). Concatenate a uint16 containing the length of Z (in octets), Z itself, a uint16 containing the length of the PSK (in octets), and the PSK itself.

This corresponds to the general structure for the premaster secrets (see Note 1 in Section 2) in this document, with "other_secret" containing Z.

## 4. RSA_PSK Key Exchange Algorithm

The ciphersuites in this section use RSA and certificates to authenticate the server, in addition to using a PSK.

As in normal RSA ciphersuites, the server must send a Certificate message. The format of the ServerKeyExchange and ClientKeyExchange messages is shown below. If no PSK identity hint is provided, the ServerKeyExchange message is omitted.

```
   struct {
       select (KeyExchangeAlgorithm) {
           /* other cases for rsa, diffie_hellman, etc. */
           case rsa_psk:  /* NEW */
               opaque psk_identity_hint<0..2^16-1>;
       };
   } ServerKeyExchange;

   struct {
       select (KeyExchangeAlgorithm) {
           /* other cases for rsa, diffie_hellman, etc. */
           case rsa_psk:   /* NEW */
               opaque psk_identity<0..2^16-1>;
               EncryptedPreMasterSecret;
       } exchange_keys;
   } ClientKeyExchange;
```

The EncryptedPreMasterSecret field sent from the client to the server contains a 2-byte version number and a 46-byte random value, encrypted using the server's RSA public key as described in Section 7.4.7.1 of [TLS]. The actual premaster secret is formed by both parties as follows: concatenate a uint16 with the value 48, the 2-byte version number and the 46-byte random value, a uint16 containing the length of the PSK (in octets), and the PSK itself. (The premaster secret is thus 52 octets longer than the PSK.)

ERICSSON EXHIBIT 1003, Page 146

The Wayback Machine - https://web.archive.org/web/20060219221316/http://www.rfc-editor.org:80/rfc/rfc4279.txt



This corresponds to the general structure for the premaster secrets (see Note 1 in Section 2) in this document, with "other_secret" containing both the 2-byte version number and the 46-byte random value.

Neither the normal RSA ciphersuites nor these RSA_PSK ciphersuites themselves specify what the certificates contain (in addition to the RSA public key), or how the certificates are to be validated. In particular, it is possible to use the RSA_PSK ciphersuites with unvalidated self-signed certificates to provide somewhat similar protection against dictionary attacks, as the DHE_PSK ciphersuites define in Section 3.

## 5. Conformance Requirements

It is expected that different types of identities are useful for different applications running over TLS. This document does not therefore mandate the use of any particular type of identity (such as IPv4 address or Fully Qualified Domain Name (FQDN)).

However, the TLS client and server clearly have to agree on the identities and keys to be used. To improve interoperability, this document places requirements on how the identity is encoded in the protocol, and what kinds of identities and keys implementations have to support.

The requirements for implementations are divided into two categories, requirements for TLS implementations and management interfaces. In this context, "TLS implementation" refers to a TLS library or module that is intended to be used for several different purposes, while "management interface" would typically be implemented by a particular application that uses TLS.

This document does not specify how the server stores the keys and identities, or how exactly it finds the key corresponding to the identity it receives. For instance, if the identity is a domain name, it might be appropriate to do a case-insensitive lookup. It is RECOMMENDED that before looking up the key, the server processes the PSK identity with a stringprep profile [STRINGPREP] appropriate for the identity in question (such as Nameprep [NAMEPREP] for components of domain names or SASLprep for usernames [SASLPREP]).

### 5.1. PSK Identity Encoding

The PSK identity MUST be first converted to a character string, and then encoded to octets using UTF-8 [UTF8]. For instance,

ERICSSON EXHIBIT 1003, Page 147

The Wayback Machine - https://web.archive.org/web/20060219221316/http://www.rfc-editor.org:80/rfc/rfc4279.txt



- IPv4 addresses are sent as dotted-decimal strings (e.g., "192.0.2.1"), not as 32-bit integers in network byte order.

- Domain names are sent in their usual text form [DNS] (e.g., "www.example.com" or "embedded\.dot.example.net"), not in DNS protocol format.

- X.500 Distinguished Names are sent in their string representation [LDAPDN], not as BER-encoded ASN.1.

This encoding is clearly not optimal for many types of identities. It was chosen to avoid identity-type-specific parsing and encoding code in implementations where the identity is configured by a person using some kind of management interface. Requiring such identity-type-specific code would also increase the chances for interoperability problems resulting from different implementations supporting different identity types.

### 5.2. Identity Hint

In the absence of an application profile specification specifying otherwise, servers SHOULD NOT provide an identity hint and clients MUST ignore the identity hint field. Applications that do use this field MUST specify its contents, how the value is chosen by the TLS server, and what the TLS client is expected to do with the value.

### 5.3. Requirements for TLS Implementations

TLS implementations supporting these ciphersuites MUST support arbitrary PSK identities up to 128 octets in length, and arbitrary PSKs up to 64 octets in length. Supporting longer identities and keys is RECOMMENDED.

### 5.4. Requirements for Management Interfaces

In the absence of an application profile specification specifying otherwise, a management interface for entering the PSK and/or PSK identity MUST support the following:

- Entering PSK identities consisting of up to 128 printable Unicode characters. Supporting as wide a character repertoire and as long identities as feasible is RECOMMENDED.

- Entering PSKs up to 64 octets in length as ASCII strings and in hexadecimal encoding.

ERICSSON EXHIBIT 1003, Page 148

The Wayback Machine - https://web.archive.org/web/20060219221316/http://www.rfc-editor.org:80/rfc/rfc4279.txt



## 6. IANA Considerations

IANA does not currently have a registry for TLS ciphersuite or alert numbers, so there are no IANA actions associated with this document.

For easier reference in the future, the ciphersuite numbers defined in this document are summarized below.

```
CipherSuite TLS_PSK_WITH_RC4_128_SHA          = { 0x00, 0x8A };
CipherSuite TLS_PSK_WITH_3DES_EDE_CBC_SHA     = { 0x00, 0x8B };
CipherSuite TLS_PSK_WITH_AES_128_CBC_SHA      = { 0x00, 0x8C };
CipherSuite TLS_PSK_WITH_AES_256_CBC_SHA      = { 0x00, 0x8D };
CipherSuite TLS_DHE_PSK_WITH_RC4_128_SHA      = { 0x00, 0x8E };
CipherSuite TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA = { 0x00, 0x8F };
CipherSuite TLS_DHE_PSK_WITH_AES_128_CBC_SHA  = { 0x00, 0x90 };
CipherSuite TLS_DHE_PSK_WITH_AES_256_CBC_SHA  = { 0x00, 0x91 };
CipherSuite TLS_RSA_PSK_WITH_RC4_128_SHA      = { 0x00, 0x92 };
CipherSuite TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA = { 0x00, 0x93 };
CipherSuite TLS_RSA_PSK_WITH_AES_128_CBC_SHA  = { 0x00, 0x94 };
CipherSuite TLS_RSA_PSK_WITH_AES_256_CBC_SHA  = { 0x00, 0x95 };
```

This document also defines a new TLS alert message, unknown_psk_identity(115).

## 7. Security Considerations

As with all schemes involving shared keys, special care should be taken to protect the shared values and to limit their exposure over time.

### 7.1. Perfect Forward Secrecy (PFS)

The PSK and RSA_PSK ciphersuites defined in this document do not provide Perfect Forward Secrecy (PFS). That is, if the shared secret key (in PSK ciphersuites), or both the shared secret key and the RSA private key (in RSA_PSK ciphersuites), is somehow compromised, an attacker can decrypt old conversations.

The DHE_PSK ciphersuites provide Perfect Forward Secrecy if a fresh Diffie-Hellman private key is generated for each handshake.

### 7.2. Brute-Force and Dictionary Attacks

Use of a fixed shared secret of limited entropy (for example, a PSK that is relatively short, or was chosen by a human and thus may contain less entropy than its length would imply) may allow an attacker to perform a brute-force or dictionary attack to recover the secret. This may be either an off-line attack (against a captured

ERICSSON EXHIBIT 1003, Page 149

The Wayback Machine - https://web.archive.org/web/20060219221316/http://www.rfc-editor.org:80/rfc/rfc4279.txt



TLS handshake messages) or an on-line attack where the attacker attempts to connect to the server and tries different keys.

For the PSK ciphersuites, an attacker can get the information required for an off-line attack by eavesdropping on a TLS handshake, or by getting a valid client to attempt connection with the attacker (by tricking the client to connect to the wrong address, or by intercepting a connection attempt to the correct address, for instance).

For the DHE_PSK ciphersuites, an attacker can obtain the information by getting a valid client to attempt connection with the attacker. Passive eavesdropping alone is not sufficient.

For the RSA_PSK ciphersuites, only the server (authenticated using RSA and certificates) can obtain sufficient information for an off-line attack.

It is RECOMMENDED that implementations that allow the administrator to manually configure the PSK also provide a functionality for generating a new random PSK, taking [RANDOMNESS] into account.

### 7.3. Identity Privacy

The PSK identity is sent in cleartext. Although using a user name or other similar string as the PSK identity is the most straightforward option, it may lead to problems in some environments since an eavesdropper is able to identify the communicating parties. Even when the identity does not reveal any information itself, reusing the same identity over time may eventually allow an attacker to perform traffic analysis to identify the parties. It should be noted that this is no worse than client certificates, since they are also sent in cleartext.

### 7.4. Implementation Notes

The implementation notes in [TLS11] about correct implementation and use of RSA (including Section 7.4.7.1) and Diffie-Hellman (including Appendix F.1.1.3) apply to the DHE_PSK and RSA_PSK ciphersuites as well.

## 8. Acknowledgements

The protocol defined in this document is heavily based on work by Tim Dierks and Peter Gutmann, and borrows some text from [SHAREDKEYS] and [AES]. The DHE_PSK and RSA_PSK ciphersuites are based on earlier work in [KEYEX].

ERICSSON EXHIBIT 1003, Page 150

The Wayback Machine - https://web.archive.org/web/20060219221316/http://www.rfc-editor.org:80/rfc/rfc4279.txt



Valuable feedback was also provided by Bernard Aboba, Lakshminath Dondeti, Philip Ginzboorg, Peter Gutmann, Sam Hartman, Russ Housley, David Jablon, Nikos Mavroyanopoulos, Bodo Moeller, Eric Rescorla, and Mika Tervonen.

When the first version of this document was almost ready, the authors learned that something similar had been proposed already in 1996 [PASSAUTH]. However, this document is not intended for web password authentication, but rather for other uses of TLS.

## 9. References

### 9.1. Normative References

[AES] Chown, P., "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)", RFC 3268, June 2002.

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RANDOMNESS] Eastlake, D., 3rd, Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, June 2005.

[TLS] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[UTF8] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

### 9.2. Informative References

[DNS] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[KERB] Medvinsky, A. and M. Hur, "Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)", RFC 2712, October 1999.

[KEYEX] Badra, M., Cherkaoui, O., Hajjeh, I. and A. Serhrouchni, "Pre-Shared-Key key Exchange methods for TLS", Work in Progress, August 2004.

[KRAWCZYK] Krawczyk, H., "Re: TLS shared keys PRF", message on ietf-tls@lists.certicom.com mailing list 2004-01-13, http://www.imc.org/ietf-tls/mail-archive/msg04098.html.

ERICSSON EXHIBIT 1003, Page 151

The Wayback Machine - https://web.archive.org/web/20060219221316/http://www.rfc-editor.org:80/rfc/rfc4279.txt


[LDAPDN] Zeilenga, K., "LDAP: String Representation of Distinguished Names", Work in Progress, February 2005.

[NAMEPREP] Hoffman, P. and M. Blanchet, "Nameprep: A Stringprep Profile for Internationalized Domain Names (IDN)", RFC 3491, March 2003.

[PASSAUTH] Simon, D., "Addition of Shared Key Authentication to Transport Layer Security (TLS)", Work in Progress, November 1996.

[SASLPREP] Zeilenga, K., "SASLprep: Stringprep Profile for User Names and Passwords", RFC 4013, February 2005.

[SHAREDKEYS] Gutmann, P., "Use of Shared Keys in the TLS Protocol", Work in Progress, October 2003.

[SRP] Taylor, D., Wu, T., Mavroyanopoulos, N. and T. Perrin, "Using SRP for TLS Authentication", Work in Progress, March 2005.

[STRINGPREP] Hoffman, P. and M. Blanchet, "Preparation of Internationalized Strings ("stringprep")", RFC 3454, December 2002.

[TLS11] Dierks, T. and E. Rescorla, "The TLS Protocol Version 1.1", Work in Progress, June 2005.

## Authors' and Contributors' Addresses

Pasi Eronen
Nokia Research Center
P.O. Box 407
FIN-00045 Nokia Group
Finland

EMail: pasi.eronen@nokia.com

Hannes Tschofenig
Siemens
Otto-Hahn-Ring 6
Munich, Bayern 81739
Germany

EMail: Hannes.Tschofenig@siemens.com

ERICSSON EXHIBIT 1003, Page 152

The Wayback Machine - https://web.archive.org/web/20060219221316/http://www.rfc-editor.org:80/rfc/rfc4279.txt



Mohamad Badra
ENST Paris
46 rue Barrault
75634 Paris
France

EMail: Mohamad.Badra@enst.fr

Omar Cherkaoui
UQAM University
Montreal (Quebec)
Canada

EMail: cherkaoui.omar@uqam.ca

Ibrahim Hajjeh
ESRGroups
17 passage Barrault
75013 Paris
France

EMail: Ibrahim.Hajjeh@esrgroups.org

Ahmed Serhrouchni
ENST Paris
46 rue Barrault
75634 Paris
France

EMail: Ahmed.Serhrouchni@enst.fr

ERICSSON EXHIBIT 1003, Page 153

The Wayback Machine - https://web.archive.org/web/20060219221316/http://www.rfc-editor.org:80/rfc/rfc4279.txt



## Full Copyright Statement

Copyright (C) The Internet Society (2005).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

## Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.



ERICSSON EXHIBIT 1003, Page 154