Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 4, No. 5. June, 2002

3GPP Security Standards

3GPP develops standards for GSM and UMTS (Wideband CDMA). They have developed a significant number of security standards for UMTS, which are listed on pages 7 and 8. The listing includes algorithms for authentication, for voice and data privacy, and for lawfully authorized electronic surveillance. All 3GPP specifications are freely available for download at:

www.3gpp.org/specs/specs.htm

Wireless Information Website

Late-breaking wireless news – both general technology news and security-specific news – is at the new website and the official home of NetStumbler software::

www.netstumbler.com

One purpose of the website is to promte the NetStumbler software – a Windows utility for 802.11b-based wireless network auditing, written by Marius Milner. However, this website is also oriented towards improving security in wireless communications. Wireless developers and groups are encouraged to assist by sending noteworthy news or by getting involved in the forums.

Book Review – "Hackproofing Your Network"

Reviewed by Peter Gregory

I think managers and above would learn a lot from Chapter 2, "The Laws of Security". This chapter is very frank, informal, and revealing, and it's not too technical for most audiences.

Ultimately, though, this is the security analyst's bible. It goes into excruciating (or should I say "delightful") detail on a wide variety of topics. Still, it's well written, and it should be easy for security practitioners to understand and use. Here is an example paragraph that makes my point about the level of detail:

> "The global offset table (GOT) is the section of an ELF program that contains the pointers to library functions used by the program. Attackers can overwrite GOT entries with pointers to shellcode that will execute when the library functions are called."

This is a valuable nugget of information – accompanied by dozens of others – for software and security engineers who want to learn more about software vulnerabilities.

One great advantage of "Hackproofing Your Network" is that it not only goes into great detail about threats and

About Wireless Security Perspectives

Price

The basic subscription price for *Wireless Security Perspectives* is $300 for one year (12 issues) for delivery by emailed PDF file or by first class mail within the US or Canada. International subscriptions are US$350 per year. The basic subscription allows for distribution to up to 10 people within one organization. Contact us for license fees to allow more readers.

We provide discounts to educational institutions and small businesses (less than 10 employees).

Back issues are available individually, or in bulk at reduced prices.

Delivery is by first class mail or by email (Acrobat PDF file).

Complete pricing information for both publications is available at:

www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

cnpaccts@cnp-wireless.com

Next Issue Due…

July 15th, 2002.

Future Topics

Radius for Wireless • IP Security • Public Keys & Wireless • Security Issues in Ad hoc Wireless Networks • Latest in Watermarking • 3G Security • Blackberry • Security for PDAs • SMS Security

Wireless Security Perspectives (ISSN 1492-806X (print) and 1492-8078 (email)) is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cresc. NW, Calgary, Alberta T2N 3W1, Canada. **Phone**: 1-800-633-5514 (+1-403-274-4749) **Fax**: +1-403-289-6658 **Email**: cnpsales@cnp-wireless.com **Web**: www.cnp-wireless.com/wsp.html **Subscriptions**: $300 for delivery in the USA or Canada, US$350 elsewhere. **Payment**: accepted by cheque, bank transfer, American Express, Diners Club, MasterCard or Visa. **Delivery**: Email or 1st class mail. **Back Issues**: Available individually for $35 in the US and Canada and US$40 elsewhere, or in bulk at reduced rates. **Discounts**: Educational and small business discount: 25% off any order. **Copies**: Each subscriber is licensed to make up to 10 copies of each issue or back issue. Call for rates to allow more copies.

Technical Editor and Illustrator: Les Owens.
Article Sourcing: Betsy Harter.
Production: Doug Scofield.
Distribution: Debbie Brandelli.
Accounts: Evelyn Goreham.
Publisher: David Crowe.

vulnerabilities, but it also includes suggested techniques for mitigating those threats and vulnerabilities.

"Hackproofing your Network", by Ryan Russell, (704 pages), was published in 2002 by Syngress Publishing.

IETF Insights

54th Meeting of IETF

The *54th meeting of the Internet Engineering Task Force (IETF)* is scheduled for the July 14th- 19th, 2002 in Yokohama, Japan.

For more information, visit:

www.ietf.org/meetings/IETF-54.html

Some sessions of interest at the 54th meeting include:

I. SUNDAY, July 14th, 2002:

Security Tutorial
(3 - 5 PM)

II. MONDAY, July 15th, 2002:

IP Routing for Wireless/Mobile Hosts Working Group
(5:30 - 7:30 PM)

III. TUESDAY, July 16th, 2002:

Provider Provisioned Virtual Private Networks Working Group
(9 - 11:30 AM)

Kerberos Working Group
(2:15 - 3:15 PM)

IV. WEDNESDAY, July 17th, 2002:

Mobile Ad-hoc Networks Working Group
and
Internet Emergency Preparedness Working Group
(9 - 11:30 AM)

Public-Key Infrastructure (X.509) Working Group
and
Session Initiation Protocol Working Group
(1 - 3 PM);

IP Security Protocol Working Group
(3:30 - 5:30 PM)

For a Good Chuckle...

www.cnp-wireless.com/acronyms.html

…has a collection of humorous definitions for common telecom and computer acronyms. If you suspect that one has been contributed by a competitor to belittle your favorite technology, get back at them by submitting your own barb directed at theirs!

Other IETF Insights

Several new Internet-Drafts are available from the on-line Internet-Drafts directories. These are draft work items of the Public-Key Infrastructure (X.509) Working Group of the IETF.

I. Internet X.509 PKI Permanent Identifier

Authors: D. Pinkas, T. Gindin

Filename: draft-ietf-pkix-pi-05.txt

Date: June 17th, 2002

Upcoming Fraud and Security Events

The following are some upcoming conferences and security events that may be of interest to the wireless and network security practitioners.

SANS Motor City
8th- 13th July 2002
Marriott Renaissance Center Hotel
Detroit, MI
www.sans.org/MotorCity

Wireless2002 -The 14th International Conference on Wireless Communications
8th- 10th July 2002
Coast Plaza Hotel
Calgary, Alberta, CA
www.cal.trlabs.ca/wireless

Optimizing End-to-end Revenue Assurance Strategies
8th- 10th July 2002
Marriott Hotel Lisbon
Lisbon, Portugal
www.iir-conferences.com

GOVSEC-The Government Security Expo and Conference
23rd- 25th July 2002
Washington Convention Center
Washington, DC
www.govsecinfo.com

Identity Fraud 2002
24th- 26th July 2002
Merchant Court Hotel
Sydney, Australia
www.marcusevansconferences.com

Blackhat Briefing - USA 2002
31st July - 1st August 2002
Caesars Palace
Las Vegas, NV
www.blackhat.com/html/bh-link/briefings.html

Internet Untethered - Denver Wireless Trade Show/Seminar
6th August 2002
Venue TBD
Denver, CO
www.angelbeat.com/Denver86.shtml

RAWCON2002 - IEEE Radio and Wireless Conference
11th- 14th August 2002
Hilton Boston Back Bay
Boston, MA
rawcon.org

Sector 5-The Global Summit Exploring Cyber Terrorism and the Targets of Critical Infrastructures
21st- 23rd August 2002
Grand Hyatt Washington
Washington, DC
sector5.biz

This document (Internet X.509 PKI) defines a new form of name, called permanent identifier, that may be included in the subjectAltName extension of a public key certificate issued to an entity.

The permanent identifier is an optional feature that may be used by a CA to indicate that the certificate relates to the same entity, even if the name or the affiliation of that entity stored in the subject or another name form in the subjectAltName extension has changed.

The subject name, carried in the subject field, is only unique for each subject entity certified by the one CA, as defined by the issuer name field. Also, the new name form can carry a name that is unique for each subject entity certified by a CA.

II. Attribute Certificate Policies Extension

Authors: C. Francis, D. Pinkas

Filename: draft-ietf-pkix-acpolicies-extn-00.txt

Date: June 12th, 2002

This document describes a certificate extension to explicitly state the attribute certificate policies that apply to the attributes contained in the certificate containing that extension.

It also defines two certificate extensions that may be used to indicate the location of the public or private repositories where the certificate is being stored.

III. Wireless LAN Certificate Extensions

Authors: R. Housley, T. Moore

Filename: draft-ietf-pkix-wlan-extns-00.txt

Date: June 12th, 2002

This document defines two Extensible Authentication Protocol (EAP) extended key usage values and a certificate extension to carry Wireless LAN (WLAN) System Service identifiers (SSIDs).

New Wireless Security Book

Another favorite among 802.11b WLAN practitioners is the new text from O'Reilly:

> "802.11 Wireless Networks: The Definitive Guide Creating and Administering Wireless Networks"

By Matthew Gast

April 2002

0-596-00183-5, Order Number: 1835

464 pages

A practical guide for wireless network planning, analysis, deployment and troubleshooting.

The cost of the book is:

$44.95 US $69.95 CA £31.95 UK

www.oreilly.com/catalog/802dot11

Fraud And Security Patent News

The US Patent and Trademark Office (USPTO) recently granted the following fraud and security patents. These may be of interest to some of our wireless security practitioners. Each patent includes the patent number, the invention title – linked to its corresponding USPTO webpage, a brief description, the inventor(s), and the assignee (owner). All of these patents were granted within the last three months.

With the listings below, one can see *who* is doing *what* in the world of inventions. Moreover, it is often instructive to read issued patents, since they include patent claims, specifications, illustrations, detailed descriptions and cited references. Patents often include other references, and these are sometimes useful to broaden one's perspective of wireless communications and security.

US Patent: 6,405,203

Method and program product for preventing unauthorized users from using the content of an electronic storage medium

A system, method, and article of manufacture is provided for tracking the distribution of content electronically. First, an electronic storage medium tracking identifier is incorporated onto an electronic storage medium and stored on a database. Next, a package tracking identifier is situated onto a package in which the electronic storage medium is stored. The electronic storage medium is then tracked while being shipped between various entities using the tracking identifier on the package. Further, the electronic storage medium may be identified using the tracking identifier on the electronic storage medium in order to afford various advertising, security, support, or retail-related features.

Issued: June 11, 2002

Inventor: Todd Collart

Assignee: Research Investment Network, Inc. (Irvine, CA)

US Patent: 6,405,029

Wireless prepaid telephone system with dispensable instruments

A telecommunication system incorporates individual station instruments simplified by wireless operation, voice dialing, prepaid accounting and out-call operation, all enabled by cooperative system operation including supporting central equipment. Wireless operation of the central equipment involves a multiple port wireless platform along with other units for interfacing a multitude of mobile station instruments simultaneously for interactive audio communication to: Regulate control, monitor and record operations of the instruments, and bridge communication with selected remote terminals through the public switched telephone network. Message capability, emergency abort to an operator station and security features supplement the basic system.

Issued: June 11, 2002

Inventor: Bryard Nilsson

Assignee: Same

US Patent: 6,401,203

Method for automatic handling of certificate and key-based processes

A method, system and program for automatic administration and management of a plurality of certificates and/or cryptographic keys. Each key is associated with a set of attributes so that the set of attributes is specific both to a user or group of users and to a particular use to which the key is intended to be put. Each user can automatically conduct any legitimate operation or process related to any certificate/key and/or group of certificates/keys, by virtue of the associated set of attributes.

Issued: June 4, 2002

Inventor: Dan Eigeles

Assignee: Same

US Patent: 6,400,967

Mobile keyless telephone instruments and wireless telecommunications system having voice dialing and voice programming capabilities

A telecommunication system incorporating individual station instruments simplified by wireless operation, voice dialing, prepaid, and custom-programmed operating characteristics, all enabled by cooperative operation with supporting central equipment. Wireless operation of the central equipment involves a multiple port wireless platform, along with other units for interfacing a multitude of mobile station instruments simultaneously for interactive audio communication to program the operating characteristics as with respect to language, out call, anti-fraud, and available data, as well as to regulate, control, monitor, and record operations of the instruments, and bridge communication with selected remote terminals through the public switched telephone network. Message capability, rapid dialing, emergency abort to an operator station, and security features supplement the basic system.

Issued: June 4, 2002

Inventor: Bryard Nilsson

Assignee: Same

US Patent: 6,400,827

Methods for hiding in-band digital data in images and video

Frames of video and image data are processed to convey plural bits of hidden auxiliary data. The auxiliary data can be used for identification purposes, for device control (disabling video recording and the like), etc. The claimed arrangement uses a data embedding technique wherein the value of single pixels of the video or image data are influenced by the values of several of the bits of auxiliary data. A great variety of other techniques and applications are also detailed.

Issued: June 4, 2002

Inventor: Geoffrey Rhoads

Assignee: Digimarc Corporation (Tualatin, OR)

US Patent: 6,396,916

Clip-on fraud prevention method and apparatus

Description of fraud prevention in a telecommunications network using call initiation equipment including intelligence capable of authentication. In order to initiate a call via a telecommunications network, the call initiation equipment sends authentication data to an adjunct platform. The adjunct platform uses the authentication data to determine if the call initiation equipment is authorized to use the customer wireline that interconnects the call initiation equipment to the telecommunications network.

Issued: May 28, 2002

Inventor: David Jordan

Assignee: MCI Communications Corporation (Washington, DC)

US Patent: 6,393,563

Temporary digital signature method and system

A digital signature system that employs a temporary digital ID signed by using a private key, so that the digital ID can be used as a proxy for a specific period of time and for a specific purpose. When a signature is requested by a server application, a user does not use his or her private key, but employs a temporary key generated using the private key. A temporary certificate for the temporary key is signed using the user's private key. The temporary certificate includes information concerning the period of time during which the temporary certificate is valid and information concerning the purpose for which it is to be used.

Upon receipt of a request from an application that a document be signed, a client transmits to the server a document signed using the temporary key, the temporary certificate and a user's certificate. First, the server examines the signature; second, it determines whether the temporary certificate is still effective, i.e. whether the period of time during which it is valid has expired and whether the certificate is for another application; and third, it confirms that the temporary certificate has been signed by an authenticated user. Finally, the server validates the user's certificate.

Issued: May 21, 2002

Inventors: Hiroshi Maruyama and Naohiko Uramoto

Assignee: International Business Machines Corporation (Armonk, NY)

US Patent: 6,393,283

Wireless communications system and method of operation for reducing fraud

The wireless communications system includes a home carrier and a HLR memory, associated with the home carrier, for storing a number of Home Locator Records defining the level of service to be provided to the individual subscribers of the home carrier. The Home Locator Record is at least initially configured to prohibit call termination of the respective subscriber outside of the predetermined service area of the home carrier. However, the wireless communications system also includes reconfiguring devices for at least temporarily reconfiguring the Home Locator Record of a respective subscriber in response to a request for communications service involving the subscriber who has roamed outside of the predetermined service area of the home carrier if the subscriber has prepaid for the requested services. Once reconfigured, the wireless communications system can provide the Home Locator Record of the respective subscriber to a serving carrier via IS-41 (Rev. A) messaging. The reconfigured Home Locator Record serves as the roaming subscriber's Visitor Locator Record which, in turn, authorizes the requested wireless communications service. Once the requested service has been ended, either upon completion of the call or upon exhaustion of the

prepaid services, the reconfiguring devices reset the Home Locator Record of the respective subscriber such that the Home Locator Record again prohibits call termination with the subscriber outside of the service area of the home carrier, thus protecting the wireless communications system from fraud.

Issued: May 21, 2002

Inventor: Joseph Morgan

Assignee: AT&T Corp. (New York, NY)

US Patent: 6,393,270

Network authentication method for over-the-air activation

A method for authenticating a cellular service provider during over-the-air activation of a mobile station, which includes the steps of programming an A-key value into the mobile station and providing the A-key value to the service provider. The mobile station requests over-the-air activation by transmitting a registration request to the service provider. The service provider verifies billing information and generates two random numbers. The service provider then performs a first CAVE algorithm using the provided A-key value and the first random number to generate a first shared secret data value. The service provider performs a second CAVE algorithm using the first shared secret data value and the second random number to produce a first authentication value. The service provider then transmits the first and second random numbers, along with the authentication value, to the mobile station. The mobile station performs a third CAVE algorithm using the first random number and its programmed A-key value to generate a second shared secret data value. Next, the mobile station performs a fourth CAVE algorithm using the second random number and the second shared secret data value to generate a second authentication value. The mobile station then compares the first and the second authentication values to determine if the correct service provider is activating the mobile station.

Issued: May 21, 2002

Inventors: Mark Austin and Stephen Hardin

Assignee: Bellsouth Intellectual Property Corp.

US Patent: 6,393,127

Method for transferring an encryption key

Encryption keys are transferred by obtaining a public and private key pair from a source device. The public key is transmitted from the source device to a target device. The target obtains a traffic key stored within the target device. The traffic key is encrypted within the target device using the public key. The encrypted traffic key is transmitted to the source device where it is decrypted using the private key. The replacement encryption key(s) is(are) encrypted using the traffic key by the source device forming an encrypted replacement key message which contains a target slot identification for each of the replacement encryption keys. The encrypted replacement key message is transmitted to the target device where the replacement encryption key(s) is(are) recovered. The replacement encryption key(s) is(are) then stored at the target device in an identified target slot. The public, private, and traffic keys may then be erased from the source and target devices, as appropriate.

Issued: May 21, 2002

Inventor: Dean Vogler

Assignee: Motorola, Inc. (Schaumburg, Il)

US Patent: 6,390,367

Fraud prevention arrangement

A self-service terminal is described. The terminal comprises a user interface and at least one proximity sensor located adjacent the user interface, such that the sensor may detect foreign objects placed in contact with – or in close proximity to – the user interface. A fraud prevention arrangement, and a method of detecting fraud at an SST, are also described.

Issued: May 21, 2002

Inventor: Alistair Doig

Assignee: NCR Corporation (Dayton, OH)

US Patent: 6,389,136

Auto-recoverable and auto-certifiable cryptosystems with RSA or factoring-based keys

A method is provided for an escrow cryptosystem that is: Essentially overhead-free; does not require a cryptographic tamper-proof hardware implementation (i.e. can be done in software); is publicly verifiable; and cannot be used subliminally to enable a shadow public key system. The keys generated are based on composite numbers (like RSA keys).

> Note: A shadow public key system is an unescrowed public key system that is publicly displayed in a covert fashion.

The keys generated by the method are auto-recoverable and auto-certifiable (abbreviated as ARC). The ARC Cryptosystem is based on a key generation mechanism that outputs a public/private key pair, and a certificate of proof that the key is recoverable by the escrow authorities. Each generated public/private key pair can be verified efficiently to be escrowed properly by anyone. The verification procedure does not use the private key. Hence, the general public has an efficient way of making sure that any given individual's private key is escrowed properly, and the trusted authorities will be able to access the private key if needed.

Since the verification can be performed by anyone, there is no need for a special trusted entity, known in the art as a "trusted third party". Furthermore, the system is designed so that its internals can be made publicly scrutinizable (e.g. it can be distributed in source code form). This differs from many schemes which require that the escrowing device be tamper-proof hardware. The system is efficient, and it can be implemented as a "drop-in" replacement to an RSA or Rabin cryptosystem. The system is applicable for law-enforcement, file systems, e-mail systems, certified e-mail systems, and any scenario in which public key cryptography can be employed and where private keys, or information encrypted under public keys, need to be recoverable. Another aspect of the system is the possibility to organize it in a hierarchical tree structure, where each element in the

tree is an escrow authority (or authorities) capable to recover keys and/or information encrypted under these keys within the subtree rooted at the authority (or authorities) and only within this subtree.

Issued: May 14, 2002

Inventors: Adam Young and Marcel Yung

Assignee: Same

US Patent: 6,385,316

Method and apparatus for encrypting data in a wireless communication system

In a communications system, this is a method of transforming a set of message signals representing a message. It comprises the steps of:

1. Encoding one of the set of message signals in accordance with a first keyed transformation;
2. Encoding of the one of the set of message signals in accordance with at least one additional keyed transformation;
3. Encoding of the one of the set of message signals in accordance with a self-inverting transformation in which at least one of the set of message sgnals is altered;
4. Encoding of the one of the set of message signals in accordance with at least one additional inverse-keyed transformation, wherein each of the at least one additional inverse keyed transformation is a corresponding inverse of at least one additional keyed transformation;
5. Encoding the one of the set of message signals in accordance with first inverse keyed transformation, wherein the first inverse keyed transformation is the inverse of the first keyed transformation.

Issued: May 7, 2002

Inventor: Gregory Rose

Assignee: Qualcomm Incorporated (San Diego, CA)

US Patent: 6,378,073

Single account portable wireless financial messaging unit

A portable secure financial messaging unit including a receiver and a selective call decoder. The selective call decoder has a memory that includes a single unique selective call address corresponding with a predetermined financial transaction type. An address correlator operates to determine substantial coincidence between the single unique selective call address and a received selective call address corresponding with the predetermined financial transaction type. In response to a coincidence, a main processor and a financial transaction processor process received information to effect a financial transaction corresponding with the predetermined financial transaction type.

Issued: April 23, 2002

Inventors: Walter David, Jeff LaVell, and Victoria Leonardo

Assignee: Motorola, Inc. (Schaumburg, IL)

Further Patent Information

To obtain a complete copy of these patents, contact the US Patent and Trademark Office at the address or telephone numbers below:

General Information Services Division
U.S. Patent and Trademark Office
Crystal Plaza 3, Room 2C02
Washington, DC 20231

800-786-9199 or 703-308-4357

www.uspto.gov

3GPP Security Specifications

Wireless Security Perspectives

Editor: David.Crowe@cnp-wireless.com First publication

Note:
1. TR – 3GPP Technical Specification (Standards), TR – 3GPP Technical Report (Informational).
2. Bold Type indicates a modification since the previous publication of this information.
3. 3GPP specifications and reports can be freely obtained from http://www.3gpp.org
4. Versions 3.x.x are for Rel 99, 4.x.x for Rel 4 and 5.x.x for Rel 5 (All IP)

3G (UMTS) Security Aspect Specifications (Series 33 TS)

Specification	Title	Version
TS 33.102	**Security Architecture**	**5.0.0**
TS 33.103	**Security Integration Guidelines**	**4.2.0**
TS 33.105	**Cryptographic Algorithm requirements**	**4.1.0**
TS 33.106	**Lawful interception requirements**	**5.0.0**
TS 33.107	**Lawful interception architecture and functions**	**5.3.0**
TS 33.108	**Handover interface for lawful interception**	**5.0.0**
TS 33.120	**Security Objectives and Principles**	**4.0.0**
TS 33.200	**Network Domain Security (NDS); Mobile Application Part (MAP) application layer security**	**5.0.0**
TS 33.201	**Access Domain Security**	**none**
TS 33.203	**Access Security for IP-based services**	**5.2.0**
TS 33.210	**Network Domain Security (NDS); IP network layer**	**5.1.0**
TS 33.21U	**Security requirements**	**3.0.0**

3G (UMTS) Security Aspect Reports (Series 33 TR)

Report	Description	Version
TR 33.20U	**Security principles for UMTS**	**3.0.0**
TR 33.800	**Principles for Network Domain Security**	**5.0.0**
TR 33.900	**Guide to 3G security**	**0.4.1**
TR 33.902	**Formal Analysis of the 3G Authentication Protocol**	**4.0.0**
TR 33.903	**Access security for IP based services**	**none**
TR 33.908	**Security Algorithms Group of Experts (SAGE); General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms**	**4.0.0**
TR 33.909	**ETSI SAGE 3GPP Standards Algorithms Task Force: Report on the evaluation of 3GPP standard confidentiality and integrity algorithms**	**4.0.1**

3GPP Security Specifications (cont'd)

3G (UMTS) Security Algorithm Specifications (Series 35 TS)

Specification	Title	Version
TS 35.201	Confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	5.0.0
TS 35.202	Confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	5.0.0
TS 35.203	Confidentiality and integrity algorithms; Document 3: Implementors' test data	5.0.0
TS 35.204	Confidentiality and integrity algorithms; Document 4: Design conformance test data	5.0.0
TS 35.206	MILENAGE algorithm specification	5.0.0
TS 35.207	MILENAGE implementors' test data	5.0.0
TS 35.208	MILENAGE design conformance test data	5.0.0
TS 35.209	Summary and results of MILENAGE design and evaluation	Replaced by TR 35.909

3G (UMTS) Security Algorithm Reports (Series 35 TR)

Report	Description	Version
TR 35.205	Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General	5.0.0
TR 35.909	Report on the design and evaluation of the MILENAGE algorithm set	5.0.0