Network Working Group
INTERNET-DRAFT
Expires: April 2001

Rolf Blom, Ericsson
Elisabetta Carrara, Ericsson
Mats Naslund, Ericsson
Sweden
November 15, 2000

Conversational Multimedia Security in 3G Networks
<draft-blom-cmsec-3g-00.txt>

Status of this memo

Abstract

As emerging real-time services on the Internet, such as Voice over IP (VoIP), increase their visibility, a security framework has to be provided. In particular, confidentiality is a main concern in the multimedia scenario.

To support full flexibility of the services, a solution with IP all the way (to the terminal) is believed to offer advantages, if technically and economically feasible. Therefore, new requirements have to be met on cellular access networks, and this has an impact on the security solutions.

This document investigates requirements that a security scheme for such applications should fulfill when used in a cellular environment. The focus is mainly on the confidentiality of the media session, in particular within the conversational multimedia scenario, which proves to be the most demanding one.

The highlighted keypoints are the necessity of a trade-off between security and cost to end up with an attractive service, and the support of profiles.

TABLE OF CONTENTS

1. Introduction

Emerging real-time services in the Internet, such as VoIP [WMGL], pose new requirements on cellular access networks, as described in [WL00]. The main concern is to take into consideration the

characteristics of the radio link to end up with a service, which

could be as attractive as today's circuit switched service in terms of cost and speech quality.

Moreover, there is a strong need to add a security framework to multimedia scenarios. In particular, increasing interest in the end-to-end (e2e) confidentiality of the session flow has been showed by several parties. While IPsec [KA98] is generally envisaged as becoming a widely used security solution, there are indeed cases where its usage as e2e functionality has implications, as lately pointed out in the document.

An aspect that should be taken into consideration mainly in the emerging real-time service scenario is the attractiveness of the service [WMGL]. A high security level will of course in many cases be a very strong argument (perhaps the strongest one) in favor of a certain solution. However, the cost of the cellular spectrum is a strong argument against some features, which are inherent to full security (e.g., added fields, and high reliability of the transmission). Therefore, we foresee the security/cost trade-off as a keypoint of the service. Profiles have to be offered to fulfill the user's expectation in the experience of the service, and any kind of compromise that shall be needed in term of security has to be explained in terms of cost for the user and/or for the operator.

The above is clearly motivated by the fact that, as the wired Internet and the wireless world merge (heterogeneous environment), new requirements have to be met, which also have an impact on the design of a security solution.

There are in general several ways to provide support for real-time services in cellular access networks. One straightforward way may be to use proxies and gateways; but such solutions pose problems for e2e security, because they often require that some entities on the transmission path between the endpoints have the ability to inspect and possibly manipulate the packets. The preferred solution is instead to transfer the IP packet e2e ('IP-all-the-way approach', [WL00] and [ROHC], sometimes also called 'All-IP scenario'), and also to support e2e security. Moreover, bypassing the air link and entering with encryption at the wired edge (where constraints are not demanding) opens trust model issues, as it requires network-assisted security. Instead, an e2e solution is the desired possibility, if feasible. This necessitates a compromise between e2e security and spectrum cost, as motivated in the following discussion.

This document does not propose a general security solution for RTP [RTP] traffic (RTP being the most likely transport protocol for the applications in question). The document instead investigates some requirements that a security scheme for RTP should fulfill, in

particular when used as the transport protocol for conversational

multimedia applications over a heterogeneous environment, such as the one described in [WL00].

Among the different security services, we investigate in particular the confidentiality of the session flow, which has to be guaranteed by use of encryption. In case of speech, confidentiality is seen as the major objective, even if authentication/integrity protection may be requested in other situations. Therefore, we concentrate mainly on confidentiality of conversational multimedia sessions over RTP in the rest of this paper.

1.1. The right security for each type of traffic

Security can be entered at many layers of the stack, providing different protection levels. Going towards an All-IP scenario, IPsec turns out to be a natural choice, ranging from a very general framework to a fine-granular security. However, for certain types of traffic the employment of IPsec does not appear to be the most suitable one. This statement is motivated by the requirement of offering an attractive service with a reasonable level of security, and is further discussed in Section 3.

We describe in the following the requirements of the RTP session in a conversational multimedia scenario, which proves to be one of the most demanding types of traffic. The description highlights the reasons why application security seems to be the feasible choice. Some other real-time (video) and streaming types of traffic show more relaxed requirements (see Section 6).

2. Requirements for the encryption scheme

As underlined in [WL00], there is the need of an appropriate design of the link layer protocol based on radio requirements, and of some link layer enhancements to support real-time traffic. This poses specific requirements on the encryption scheme to be used, which we briefly outline in the following, in relation to conversational audio traffic.

2.1. Encryption and Bit Error Rate

A first aspect is the interaction between the bit error rate (BER) and the chosen encryption algorithm. Some modes of encryption result in error propagation, that is, a single bit error in the transmitted ciphertext causes multiple bit errors in the deciphered message (in block ciphers, at least one entire block, e.g. 64 bits, is turned into "random noise"). This error propagation is a very undesired feature that should be minimized/eliminated in a VoIP scenario, not

to degrade quality. Therefore, the encryption algorithm is requested

to be error-robust. [FC] provides a good overview about the relation between encryption and BER.

- The encryption algorithm must be error-robust (error propagation should be avoided).

2.2. Encryption and Efficiency

Efficiency plays an important role in real-time services. The overall delay budget has to be reduced to achieve acceptable performance in terms of service quality and spectrum efficiency, therefore a particular concern is the processing time required by the encryption/decryption engine that contributes to the overall delay.

Another aspect affecting the efficiency requirements is that the security solution has also to take into account that the encryption endpoints may be small, lightweight mobile (wireless) terminals often with limited computational resources.

- The encryption algorithm must be fast, and has to be implemented in thin clients.

2.3. Encryption and Heterogeneous Environments

In an e2e solution for a heterogeneous environment, different types of networks pose different constraints to be taken into account in the overall solution. As an example, the unreliable nature of IP per-se means packet-loss and non-ordered delivery, while the air-link shows other characteristics (discussed throughout the paper). These are features of the media, which the encryption scheme has to deal with.

- The encryption scheme needs to show a "fast-forward/rewind" property.

2.4. Selective (Payload) Encryption

Furthermore, [WL00] stresses the need for protocol enhancements to solve the issues posed on the radio network by real-time traffic.

The flows should be identified and demultiplexed over appropriate radio channels for efficient transmission. There may be different ways to implement this kind of identification, one being e.g. snooping on the traffic in the attempt of classifying it. This implies in general the necessity of accessing some parts of the packet (i.e., the IP/UDP/RTP headers may be enough for a good guess) by intermediate nodes. This scenario breaks the e2e confidentiality, unless a compromise is accepted, and specific parts of the packet are left accessible. If e2e confidentiality is the objective, it is

likely that e2e encryption can cover only a part of the IP datagram, in case optimization/manipulation need access to some parts of the

datagram. The disclosure of more fields in the packet may open higher chance of attacks, but should be justified by the need of said trade-off.

In the previous scenario (an intermediate node requires access to the packet, e.g., transcoder or any kind of payload-manipulating proxy), it is up to the trust model to define the way security has to be handled between entities. As said, we do not investigate the proxy approach.

- The encryption scheme should be possible to apply selectively to different portions of the payload.

2.5. Security and Bandwidth

The cost of cellular access links poses the need of careful bandwidth usage.

In general, the number of bytes added by encryption should be minimized: a right compromise between encryption and bandwidth usage has to be reached. Schemes limiting message-size expansion and added fields (e.g., dedicated headers and padding) should be preferred. Authentication and/or integrity protection, if used, add several bytes; therefore, an analysis of their impact should be performed.

- Message-size expansion and added fields should be limited

2.5.1. Encryption and Header Compression

Optimization of the protocol headers is needed for real-time transmission [VOIPOW, SH00], that is, header compression is to be performed when cost is a concern. [ROHC] has developed a robust header compression scheme particularly suitable for lossy links. It develops a link-layer header compression scheme working (with maximum compression rate) over the IP-UDP-RTP headers to be performed on the air link for spectrum usage optimization. [VOIPOW] reports that the capacity drops only 10% with respect to the circuit-switched reference case, once the IP(v4)/UDP/RTP header is compressed. This should be compared with a capacity drop to less than 50%, if the complete header is sent over the air interface.

- If both e2e encryption and header compression are to be applied, the former has to be done in a way not to obstruct the latter.

2.6. Encryption and Unequal Error Protection

Unequal Error Protection (UEP) might be added to reduce the frame error rate (FER) for the audio stream, by taking into consideration the fact that different bits in a frame of encoded speech show a

varying sensitivity to errors. UEP results in the division of the application payload into different classes, which are protected in

different ways according to their importance. When encryption is applied, attention has to be paid in keeping the independence of the classes. The influence that an error in a certain bit has to a class it does not belong to may be against the definition of UEP itself.

- The encryption scheme should not interfere with the use of UEP.

3. A suitable encryption scheme

3.1. IPsec Applicability

IPsec is a protocol suite used to secure communication at the network layer, and is one of the most promising security schemes for the All-IP scenario. Its two protocols are the Authentication Header [AH] and the Encapsulating Security Payload [ESP]. Below, we analyse the applicability of IPsec according to the requirements described previously.

Applicability of ESP within the real-time scenario raises some considerations. ESP in transport mode is the one used for e2e encryption and preferred for reduced header overhead. However, ESP in transport mode has the major disadvantage to hide the UDP and RTP headers, giving them the cryptographic randomness that obstructs a proper header compression (which normally works at the link layer, i.e. [ROHC]). [ROHC] has developed profiles to compress ESP, treating the two cases in which ESP is implementing the NULL algorithm (only authentication, therefore header compression can work on all headers), and encrypting algorithms other than NULL (where compression only works up to the ESP header). The objective here is confidentiality, therefore the interest is in the latter case. The fact that full header compression (IP/UDP/RTP headers) cannot be performed implies that the service's cost for the session increases. A profile may require ESP in the case the user is willing to pay for it, and in that case the ROHC profiles may be applied, providing a limited increase in the efficiency. Otherwise, we envisage the encryption of only the RTP payload to be the right compromise to make the service attractive for larger user groups (it allows the most efficient header compression profile), still providing confidentiality of the media traffic.

[MF00] has recently specified the use of an additive stream cipher within the context of ESP, whose features satisfy several of the requirements previously outlined. In particular, advantages showed are speed, reduced packet expansion, and random-access property (the keystream can be entered at any point, to solve out-of-order delivery). These features could make the Stream Cipher ESP suitable for real-time traffic requirements, except for header compression

whose absence would actually have an impact in terms of cost. In case ESP is required by the user profile, we recommend the use of said Stream Cipher ESP.

In ESP transport mode, the header compression could work only on the IP header and similarly on the ESP header. Since compression has to be performed before encryption, it is possible to apply tunneling to accommodate them. Full header compression can be performed, followed by IPsec insertion, coupled with an appropriate tunneling protocol (e.g., GRE or L2TP over PPP). However, this would end up having to support e2e header compression, and it would also result in header overhead. As a general rule, tunneling should be avoided in wireless environments. Thus, we conclude not to examine this alternative any further.

We note that the IPsec non-suitability for several applications has been raised before, most prominently by the Transport Friendly IPsec BOF, that promoted selective encryption of the packet. Some similar proposals for multi-layer payload protection have been presented elsewhere. This kind of proposals could provide some of the necessary modifications to promote the applicability of IPsec to our scenario, but none of them has lead to work in the standard.

AH also opens some considerations, which extend to other kinds of cryptographic authentication as well (e.g., ESP with NULL encryption algorithm, or simply a MAC at the application layer). Typically, the authentication data (Integrity Check Value, or ICV, in the AH glossary) consists of an uncompressible field, i.e. 160/128-bit field when SHA1 [SHA] or MD5 [MD5] are used (typically truncated to 96 bits [HMAC]). It results in obvious bandwidth consumption, which turns out in cost. Moreover, the necessity of delivering all frames to the application, e.g. a speech decoder, regardless of bit errors, motivated by the lossy and expensive nature of a cellular access link, encounters a problem once authentication/integrity protection is requested. In fact, a single bit error, either in the data portion of the packet or in the MAC portion, would cause the integrity check to fail, and the packet to be dropped. This is wasteful, as most audio/video encoding schemes will produce acceptable quality from the user point of view, even in the presence of a few bit errors. Hence, to what extent integrity should be pursued is not always obvious. Again, security/cost/usability must be weighed against one another. We discuss this further in a later section (Section 5).

3.2. Conversational Multimedia

The above indicates that the conversational multimedia scenario over a wireless link poses specific (sometimes delicate) issues for the encryption scheme (and other security primitives, see Section 5), due mainly to the properties of the air link. We argue that these issues are not fully taken into consideration by existing solutions,

tailored for a fixed, reliable transport medium, and the use of more powerful platforms.

4. Encryption Methods Overview

There are two main flavors of ciphers: block ciphers and stream ciphers. In the following, we analyze some of the main aspects of these two flavors to determine their applicability to the conversational multimedia scenario. For more information, we refer to [MvOV].

4.1. Stream Ciphers

An additive stream cipher is a cipher that generates a pseudo-random string of bits (the keystream), and encrypts by adding it modulo 2 to the plaintext. Decryption is obtained adding the keystream to the ciphertext, modulo 2. The operation has to be performed bitwise, that is, synchronization has to be guaranteed to correctly decrypt. In the remainder of the document, stream ciphers refer to additive stream ciphers.

Stream ciphers offer valuable advantages over block ciphers. They generally provide faster ciphers and do not expand the protected message as instead some other methods do by e.g. requiring padding. This makes stream ciphers particularly suitable in scenarios where time and bandwidth are two valuable aspects.

Regarding the specific conversational multimedia data features, error propagation is not an issue, since one-bit error in the transmitted ciphertext results exactly in one-bit error in the recovered message. UEP can be used without problems, since the effect of encryption is local to every single bit and does not influence bits belonging to other classes.

The main issue that stream ciphers pose is the synchronization of the keystream. Moreover, in an e2e solution, the unreliability of IP as transport gives the necessity for encryption to deal with out-of-order delivery and loss of packets. State-caching mechanisms are possible to overcome the out-of-order problem, but they are complex, expensive in terms of time, and may be vulnerable to denial of service attacks [MF00]. Many stream ciphers, e.g. the alleged RC4 [SC96], cannot overcome the problem, while SEAL [SEAL] can. We say that a cipher that efficiently (in constant time) enables forward advance/backward rewind to any position in the keystream has the random-access property.

4.2. Block Ciphers

Block ciphers operate on larger blocks of plaintext and ciphertext.

There are mainly two modes. Electronic Codebook (ECB) mode operates

on each block independently, which eliminates problems of synchronization. Cipher Block Chaining (CBC) mode instead, feeds the previous ciphered block into the current block. Generally speaking, ECB is not secure in the strongest sense of the word (regardless of what block cipher is used), while CBC can be (if the block cipher is idealized) [BDJR].

Block ciphers have some features which deprecate their use with the RTP-type traffic.

Error propagation is not desired, as stated above. [WL00] underlines that cellular telephony systems require delivery of all frames to the speech decoder to guarantee an acceptable speech quality. With block ciphers, a single bit error in transmisssion affects an entire block in ECB mode, and even propagates to the following block with CBC mode. Given the current requirement for the BER target over the air link, this may negatively influence the resulting speech quality.

Managing out-of-order delivering and loss of packets then is not simple in CBC mode. The former may require state-caching mechanisms with the problem already underlined, and the latter may give error propagation in feedback mode.

The applicability of UEP is not straightforward. A bit ends up influencing other classes it does not belong to, when CBC mode is used. Even worse, the cipher chaining propagates occurring errors, which may end up in high importance classes of bits if the encryption/decryption of packets is not kept independent from each other.

ECB can keep the independence of the classes, needed to perform UEP. However, to achieve this, padding may be required for each class to "fill out" a multiple of the block size. The resulting waste in bits, which depends on the class sizes, is in many cases unacceptable.

4.3. Block Ciphers used as Stream Ciphers

It is possible to use block ciphers to realize stream ciphers; they can offer the same advantages as pure stream ciphers, except generally the same high speed. Examples are block ciphers in Output-Feedback (OFB) mode, and Counter mode. We do not consider Cipher Feedback (CFB) mode (that can be implemented to give a self-synchronizing stream cipher), since it gives error propagation and, perhaps even worse, since its self-synchronization may be lost due to recurring bit errors.

Counter mode has the advantage that the keystream can be directly entered at any point independent of the previous states (random-

access property). This is not a feature of pure OFB mode.

	Stream	Block	Block as Stream (OFB)
Error-robustness	yes	no	yes
Speed *	very high	high	high
Out-of-order and loss resistance	yes**	some	yes***
Absence of message size expansion	yes	no	yes
UEP friendliness	yes	no	yes

* it is a general observation, there might be block ciphers with a speed comparable to certain (slow) stream ciphers
** it is true for some stream ciphers, for ex. SEAL. It is not true for example for RC4
*** it is not a feature of pure OFB, but it may be for revised OFB modes

Table 1: Convenience of encryption schemes for conversational multimedia

4.4. Applicability of the encryption scheme to conversational multimedia

We conclude from the previous discussion that from the encryption point of view a fast stream cipher with the random-access property appears to be suitable for conversational multimedia traffic. This stream cipher, in turn, can be derived from a block cipher in a suitable mode. Table 1 summarizes some relevant parameters, which are meaningful to the comparison. In particular, we refer to [BC00], which suggests the use of a variant of OFB.

Moreover, for the motivations presented in Section 2, we also believe that a straighforward way to provide media confidentiality and to allow needed optimization like full header compression, is to apply encryption only on the RTP payload. [RTP] itself foresees encryption methods leaving the headers in clear. We refer to [BC00] for a proposal specifying such a method, and fulfilling the requirements highlightened in the current document.

For many applications, there will be an extra level of security added, for instance by the air interface for a mobile phone. Though

not an e2e solution, this may sometimes, at least partly, compensate for a different level of security at the application layer.

5. Integrity Protection

Integrity and message authentication may be chosen independently of confidentiality. There are several aspects that question their applicability to conversational multimedia traffic.

First of all, they are typically performed using a keyed hash as a MAC (whatever layer in the stack they are applied on) that translates into additional (uncompressible) bytes to be bound to the single packet. Popular functions like SHA1 and MD5 produce an output of 160/128 bits, often truncated to 96 bits, which increases the overhead for packets, especially for short packets like those for voice transmission (6-32 bytes of speech payload, [SW00]). Such an impact on capacity should be strongly motivated.

The biggest problem is related to the impact given by errors. [WL00] states that the BER over the radio link may be on the order of 10e-3, when retransmission is not used. Furthermore, [WL00] identifies as a necessary improvement for the radio link the requirement 'no dropped packets due to bit errors in the payload'. The reason for this is that the codec itself can manage errors in the payload, often maintaining reasonable speech quality. A single bit error in the authentication verification process causes the packet to be dropped. This single error can be present either in the data portion or in the MAC field of the packet. Therefore, authentication of the payload may lead highly degraded speech quality.

Replay attacks seem hard to perform, for the nature of conversational multimedia traffic. If then an attacker knows the codec (with a stream cipher, the information may be gained by observing the packet length), he could for example perform bit inversion. However, in general it seems hard to perform modifications which could lead to something harmful and meaningful, while it may cause mainly degradation of the quality and Denial-of-Service (DoS), which anyway authentication cannot prevent, only detect. [BC00] reports further analysis.

We conclude therefore that, even if (strong) authentication is required from the security point of view, whether or not to actually use it, and at what level of security (number of bits for the MAC) depends on the security need vs. the channel characteristics. It is again up to the user profile to require its correct usage.

6. Video and Streaming

Conversational video shows characteristics and requirements similar

to conversational voice, for the channel described in [WL00].

Streaming traffic shows more relaxed requirements. Packets have bigger sizes, and retransmission is performed. Therefore, the choice of the encryption algorithm and the security scheme seem less critical, as does authentication (assuming the overhead is acceptable). Header compression should be performed anyway, but the gain is not so remarkable as it is in the case of short packets.

7. Security considerations

Most of the discussion has been focused on security issues, with a main concern on confidentiality.

We underline the open challenge with respect to DoS attacks, which appear the most feasible and harmful attacks in this scenario.

Moreover, we foresee the need for a careful key management design behind this security framework. Bandwidth usage and time restrictions (e.g. round-trip time has impact on service behavior) impose strict requirements on the key management as well.

Real-time Transport Control Protocol (RTCP) security is not investigated in this version of the document.

8. Conclusions

Real-time services in the Internet need to be coupled with security. The ambition is to employ a solution with IP all the way, and to offer a service as attractive as the circuit switched one is already today. This leads to new issues, mainly posed by the cellular access networks.

The document has highlighted the need for a trade-off between security and cost as a paradigm for 3G networks, and promotes the use of security profiles.

Requirements for encryption in the conversational multimedia scenario have mainly been addressed. The high spectrum cost induced by the use of IPsec and the need of full header compression motivate the choice of placing encryption at the RTP layer. Message authentication and integrity may have impact on the bandwidth usage and on the quality of the service, thus their proper usage is an issue.

A stream cipher (possibly based on a block cipher) with certain features (listed in the document) seems to properly fulfill the requirements needed by the encryption algorithm for conversational multimedia traffic.

9. Acknowledgments

We would like to thank Lars Westberg, Morgan Lindqvist, and Luigi D'Antonio for their work and assistance. Krister Svanbro, Johan Sjoberg, and Magnus Westerlund provided significant help. Thanks to Jari Arkko, Luis Barriga, and Andras Mahes for their valuable comments.

10. Author's Addresses

Rolf Blom
Ericsson Research
Stockholm, Sweden
Tel: +46 8 58531707
EMail: rolf.blom@era.ericsson.se

Elisabetta Carrara
Ericsson Research
Stockholm, Sweden
Tel: +46 8 50877040
EMail: elisabetta.carrara@era.ericsson.se

Mats Naslund
Ericsson Research
Stockholm, Sweden
Tel: +46 8 58533739
EMail: mats.naslund@era.ericsson.se

11. References

[AH] Kent, S., and Atkinson, R., "IP Authentication Header", RFC 2402, November 1998.

[BC00] Blom, R., Carrara, E., Naslund, M., Norrman, K., "RTP Encryption in 3G Networks", IETF draft, November 2000

[BDJR] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway: "A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation", in proceedings of the 38th IEEE FOCS, 1997.

[ESP] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[FC] Ferland, G., Chouinard, J., "Error Rate Performance Analysis of Stream and Block Ciphers in a Digital Mobile Communication Channel," Int. Conf. Vehicle Navigation and Information Systems, Oslo, Norway, 1992.

[HMAC] Madson, C., and Glenn, R., "The Use of HMAC-MD5-96 within ESP

and AH", RFC 2403, and "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404

[KA98] Kent, S., and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[MD5] Rivest, R.,"MD5 Digest Algorithm", RFC 1321, April 1992.

[MvOV] Menezes, A., van Oorschot, P., and Vanstone, S, "Handbook of Applied Cryptography", CRC Press 1997.

[MF00] McGrew, D., Fluhrer, S.R., Peyravian, M., "The Stream Cipher Encapsulating Security Payload", Internet Draft, draft-mcgrew-ipsec-scesp-01.txt, July 2000

[ROHC] Burmeister, C., Clanton, C., Degermark, M., Fukushima, H., Hannu, H., Jonsson, L-E., Hakenberg, R., Koren, T., Le, K., Liu, Z., Martensson, A., Miyazaki, A., Svanbro, K., Wiebke, T., Zheng, H., "RObust Header Compression (ROHC)", Internet Draft, October 2000

[RTP] Schulzrinne, H., Casner, S., Frederick, R., Jacobson, V., "RTP: A Transport Protocol for Real-time Applications", RFC 1889, January 1996.

[SC96] Schneier, B., "Applied Cryptography. Protocols, Algorithms, and Source Code in C", John Wiley and Sons, 2nd edition, 1996

[SHA] NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995. http://csrc.nist.gov/fips/fip180-1.ps

[SH00] Svanbro, K., Hannu, H., Jonsson, L-E, and Degermark, M., "Wireless Real-time IP Services Enabled by Header Compression", Proceedings of IEEE VTC Spring 2000, Tokyo, June 2000

[VOIPOW] Svanbro, K., Wiorek, J., and Olin, B., "Voice-over-IP-over-wireless", Proc. PIMRC 2000, London, Sept. 2000

[SEAL] Rogaway, P., and Coppersmith, D., "A Software-Optimized Encryption Algorithm", Journal of Cryptology, vol. 11(4), 1998, 273-287

[SW00] Sjoberg, J., Westerlund, M., Lakaniemi, A., Koskelainen, P., Wimmer, B., and Fingscheidt, T., "RTP payload format for AMR", IETF, August 2000

[WL00] Westberg, L., Lindqvist, M., "Real-time Traffic over Cellular Access Networks", Internet Draft, draft-westberg-real-time-

[WMGL] Wang, J., McCann, P., Gorrepati, P.B., and Liu, C-Z., "Wireless Voice-over-IP and Implications for Third-Generation Network Design", Bell Labs Technical Journal, Vol.3, No.3, July-September 1998.

This Internet-Draft expires in April 2001.