

Network Working Group
Internet-Draft
Intended status: Informational
Expires: March 11, 2011

L. Morand
France Telecom - Orange
September 7, 2010

Hypertext Transfer Protocol (HTTP) Digest Authentication Using GSM 2G
Authentication and Key Agreement (AKA)
draft-morand-http-digest-2g-aka-01

Abstract

This memo specifies a one-time password generation mechanism for Hypertext Transfer Protocol (HTTP) Digest access authentication based on Global System for Mobile Communications (GSM) authentication and key generation functions A3 and A8, also known as GSM AKA or 2G AKA. The HTTP Authentication Framework includes two authentication schemes: Basic and Digest. Both schemes employ a shared secret based mechanism for access authentication. The GSM AKA mechanism performs user authentication and session key distribution in GSM and Universal Mobile Telecommunications System (UMTS) networks. GSM AKA is a challenge-response based mechanism that uses symmetric cryptography.

Requirements Language

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 [RFC 2119](#) [[RFC2119](#)].

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on March 11, 2011.

Copyright Notice

Internet-Draft

HTTP Digest 2G AKA

September 2010

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](http://trustee.ietf.org/license-info) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction and Motivation	3
2.	Requirements Language	3
3.	Terminology	4
4.	GSM 2G AKA Mechanism Overview	4
5.	Specification of Digest 2G AKA	6
5.1.	Algorithm Directive	6
5.2.	Creating a Challenge	7
5.3.	Client Authentication	7
5.4.	Server Authentication	8
6.	Example of Digest 2G AKA operations	8
7.	IANA Considerations	10
8.	Security Considerations	11
8.1.	Authentication of Clients using Digest 2G AKA	11
8.2.	Limited Use of Nonce Values	11
8.3.	Multiple Authentication Schemes and Algorithms	12
8.4.	Online Dictionary Attacks	12
8.5.	Session Protection	12
8.6.	Replay Protection	13
8.7.	Mutual Authentication	13
8.8.	Flooding the Authentication Centre	13
8.9.	AKA Security	13
9.	Acknowledgements	14
10.	References	14
10.1.	Normative References	14
10.2.	Informative References	14
	Author's Address	14

1. Introduction and Motivation

The Hypertext Transfer Protocol (HTTP) Authentication Framework, described in [[RFC2617](#)], includes two authentication schemes: Basic and Digest. Both schemes employ a shared secret based mechanism for access authentication. The Basic scheme is inherently insecure in that it transmits user credentials in plain text. The Digest scheme improves security by hiding user credentials with cryptographic hashes, and additionally by providing limited message integrity.

The 2G AKA functions [[TS55.205](#)] perform authentication and session key distribution in Global System for Mobile Communication (GSM) and Universal Mobile Telecommunications System (UMTS) networks. 2G AKA is a challenge-response based mechanism that uses symmetric cryptography. GSM AKA is typically run in a GSM Subscriber Identity Module (SIM), which resides in a smart card like device that also provides tamper resistant storage of shared secrets. The 3G Authentication and Key Agreement (AKA) mechanism, also known as UMTS AKA, relying on the use of the UMTS Subscriber Identity Module (USIM) instead of the GSM SIM, is most closely associated with UMTS; however, mobile operators commonly distribute GSM SIMs with UMTS mobile phones, resulting in the use of GSM 2G AKA in place of UMTS AKA.

This document specifies a mapping of GSM AKA parameters onto HTTP Digest authentication. In essence, this mapping enables the usage of GSM 2G AKA as a one-time password generation mechanism for Digest authentication.

This document is based heavily on [[RFC3310](#)] which specified a mapping of Authentication and Key Agreement (AKA) onto HTTP Digest authentication. While Digest AKA can be generally used when the mobile phones are equipped with a UMTS SIM card, it may be useful for mobile operators who have not yet fully deployed USIMs and have still millions of SIMs deployed in the network. Digest 2G AKA allows access to applications in a more secure way than would be possible

with the use of passwords or with GSM without enhancements.

Moreover, as the Session Initiation Protocol (SIP) [[RFC3261](#)] Authentication Framework closely follows the HTTP Authentication Framework, Digest 2G AKA is directly applicable to SIP as well as to any other embodiment of HTTP Digest.

[2.](#) Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this

Morand

Expires March 11, 2011

[Page 3]

Internet-Draft

HTTP Digest 2G AKA

September 2010

document are to be interpreted as described in [[RFC2119](#)].

[3.](#) Terminology

This section explains the terminology used in this document.

AuC Authentication Center.

AKA Authentication and Key Agreement.

GSM Global System for Mobile Communication.

IMS IP Multimedia Subsystem.

ISIM IMS Subscriber Identity Module.

Kc Cypher Key. Ki Subscriber Key.

RAND Random Challenge.

SIM Subscriber Identity Module.

SRES Signed Authentication Response.

UMTS Universal Mobile Telecommunications System.

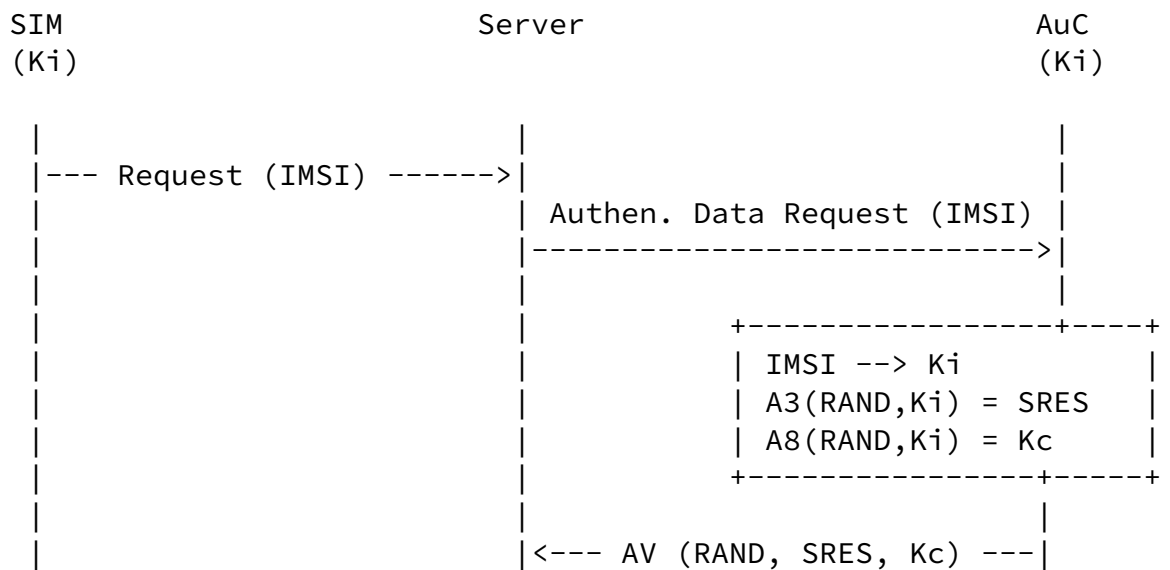
USIM UMTS Subscriber Identity Module.

4. GSM 2G AKA Mechanism Overview

This chapter describes the GSM AKA mechanism based on a shared secret key (Ki) and the use of A3/A8 algorithms:

1. A shared secret Ki is established beforehand between the SIM and the Authentication Center (AuC). The secret is stored in the SIM, which resides on a smart card like, tamper resistant device.
2. The AuC of the home network produces an authentication vector (AV), based on the shared secret Ki and a generated random value (RAND). Using Ki and RAND, the A3 algorithm is used for calculating the expected response (SRES) and the A8 algorithm is used for calculating the ciphering key Kc.

3. The authentication vector (RAND, SRES, Kc) is downloaded to a server. Optionally, the server can also download a batch of AVs, containing more than one authentication vector generated by adding different RAND values.
4. The server creates an authentication request, which contains the random challenge RAND.
5. The authentication request is delivered to the client.
6. The client produces a signed authentication response RES, using the shared secret Ki and the random challenge RAND.
7. The authentication response RES is delivered to the server.
8. The server compares the authentication response RES with the expected response SRES. If the two match, the user has been successfully authenticated, and the session key Kc can be used for protecting further communication between the client and the server



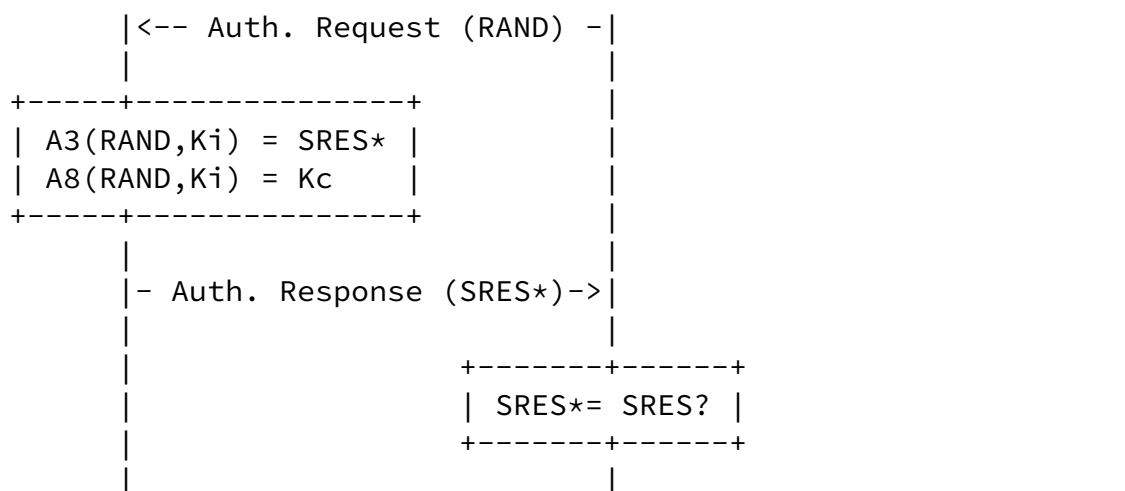


Figure 1. GSM 2G AKA overview

5. Specification of Digest 2G AKA

In general, the Digest GSM AKA operation is identical to the Digest operation in [RFC2617]. This chapter specifies the parts in which Digest 2G AKA extends the Digest operation. The notation used in the Augmented BNF definitions for the new and modified syntax elements in this section is as used in SIP [RFC3261], and any elements not defined in this section are as defined in SIP and the documents to which it refers.

5.1. Algorithm Directive

In order to direct the client into using 2G AKA for authentication instead of the standard password system, the RFC 2617 defined algorithm directive is overloaded in Digest 2G AKA:

```
algorithm = "algorithm" EQUAL ( 2GAKA-namespace / algorithm-value )
```

```
2GAKA-namespace = "2GAKA" "-" algorithm-value
```

```
algorithm-value = ( "MD5" / "MD5-sess" / token )
```

algorithm

A string indicating the algorithm used in producing the digest and the checksum. If the directive is not understood, the nonce SHOULD be ignored, and another challenge (if one is present) should be used instead. Reuse of the same SRES value in authenticating subsequent requests and responses is NOT RECOMMENDED. An SRES value SHOULD only be used as a one-time password, and algorithms such as "MD5-sess", which limit the amount of material hashed with a single key, by producing a session key for authentication, SHOULD NOT be used.

[5.2.](#) Creating a Challenge

In order to deliver the GSM AKA authentication challenge to the client in Digest 2G AKA, the nonce directive defined in [\[RFC2617\]](#) is extended:

```
nonce = "nonce" EQUAL ( 2GAKA-nonce / nonce-value )
```

```
2GAKA-nonce = LDQUOTE 2GAKA-nonce-value RDQUOTE
```

```
2GAKA-nonce-value = <base64 encoding of RAND>
```

nonce

A parameter which is populated with the Base64 [\[RFC2045\]](#) encoding of the 2G AKA authentication random challenge RAND.

[5.3.](#) Client Authentication

When a client receives a Digest 2G AKA authentication challenge, it extracts the RAND from the "nonce" parameter and runs the A3-A8 algorithms with the RAND challenge and shared secret Ki.

The resulting A3-A8 SRES parameter is treated as a "password" when calculating the response directive of [\[RFC2617\]](#). Due to the fact that the SRES parameter is 32 bits and the response directive of [\[RFC2617\]](#) is defined as 32 hex digits, SRES is encoded in the low order (i.e. rightmost) 32 bits of "response", padded with leading zeroes.

Example:

SRES="000000000000000000000000000000007018d8a1"

[5.4.](#) Server Authentication

With Digest 2G AKA, the server MUST use the expected response SRES received in the authentication vector as "password" when calculating the "response-auth" of the "Authentication-Info" header defined in [\[RFC2617\]](#).

[6.](#) Example of Digest 2G AKA operations

Figure 2 below describes a message flow describing a Digest 2G AKA process of authenticating a SIP request, namely the SIP REGISTER request.

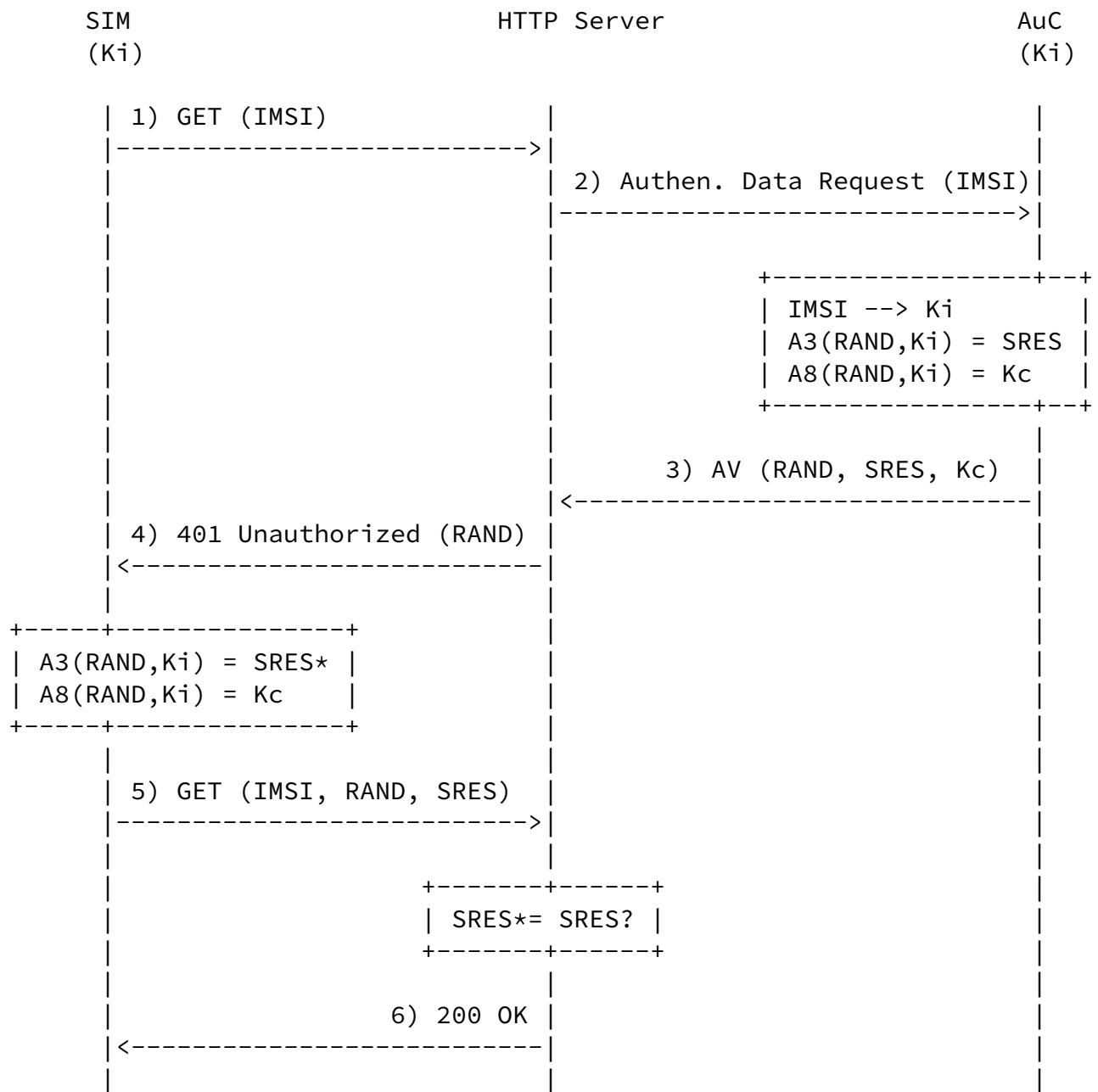


Figure 2: Message flow representing a successful authentication

1) Initial request

```

GET / HTTP/1.1
Authorization: Digest
  username="user1_private@home1.net",
  realm="service1.home1.net",

```

```
nonce="",  
uri="/",
```

```
response=""
```

- 2) Request to the AuC for 2G AKA authentication vector (AV) for the given IMSI
- 3) Response from the AuC providing 2G AKA AV (RAND, SRES, Kc) associated with the IMSI
- 4) Response containing a challenge

```
HTTP/1.1 401 Unauthorized  
WWW-Authenticate: Digest  
    realm="service1.home1.net",  
    nonce="base64(RAND)",  
    qop="auth,auth-int",  
    opaque="6dae728da9089dab9112373c9f0a9731",  
    algorithm=2GAKA-MD5
```

- 5) Request containing credentials

```
GET / HTTP/1.1  
Authorization: Digest  
    username="user1_private@home1.net",  
    realm="service1.home1.net",  
    nonce="base64(RAND)",  
    uri="/",  
    nc=00000001,  
    cnonce="0b8f29d6",  
    response="6629fae49393a05397450978507c4ef1",  
    opaque="6dae728da9089dab9112373c9f0a9731",  
    algorithm=2GAKA-MD5
```

- 6) Successful response

```
HTTP/1.1 200 OK  
Authentication-Info:  
    qop=auth-int,  
    rspauth="6629fae49394a05397450978507c4ef1",  
    cnonce="6629fae49393a05397450978507c4ef1",
```

```
nc=00000001,  
opaque="6dae728da9089dab9112373c9f0a9731",  
nonce="base64(RAND)"
```

7. IANA Considerations

This document has no actions for IANA.

Morand

Expires March 11, 2011

[Page 10]

Internet-Draft

HTTP Digest 2G AKA

September 2010

Note to RFC Editor: this section may be removed on publication as an RFC.

8. Security Considerations

In general, Digest 2G AKA is vulnerable to the same security threats as HTTP authentication [[RFC2617](#)]. This chapter discusses the relevant exceptions.

8.1. Authentication of Clients using Digest 2G AKA

2G AKA is typically -- though this isn't a theoretical limitation -- run on a SIM application that usually resides in a tamper resistant smart card. Interfaces to the SIM exist, which enable the host device to request authentication to be performed on the card. However, these interfaces do not allow access to the long-term secret outside the SIM, and the authentication can only be performed if the device accessing the SIM has knowledge of a PIN code, shared between the user and the SIM. Such PIN codes are typically obtained from user input, and are usually required when the device is powered on.

The use of tamper resistant cards with secure interfaces implies that Digest 2G AKA is typically more secure than regular Digest implementations, as neither possession of the host device nor Trojan Horses in the software give access to the long-term secret. Where a PIN scheme is used, the user is also authenticated when the device is powered on. However, there may be a difference in the resulting security of Digest 2G AKA, compared to traditional Digest implementations, depending on whether those implementations cache/store passwords that are received from the user.

[8.2.](#) Limited Use of Nonce Values

The Digest scheme uses server-specified nonce values to seed the generation of the request-digest value. The server is free to construct the nonce in such a way that it may only be used from a particular client, for a particular resource, for a limited period of time or number of uses, or any other restrictions. Doing so strengthens the protection provided against, for example, replay attacks.

Digest 2G AKA limits the applicability of a nonce value to a particular SIM. Typically, the SIM is accessible only to one client device at a time. However, the nonce values are strong and secure even though limited to a particular SIM. Additionally, this requires that the server is provided with the client identity before an authentication challenge can be generated. If a client identity is

Morand

Expires March 11, 2011

[Page 11]

Internet-Draft

HTTP Digest 2G AKA

September 2010

not available, an additional round trip is needed to acquire it.

[8.3.](#) Multiple Authentication Schemes and Algorithms

In HTTP authentication, a user agent **MUST** choose the strongest authentication scheme it understands and request credentials from the user, based upon that challenge.

In general, using passwords generated by Digest 2G AKA with other HTTP authentication schemes is not recommended even though the realm values or protection domains would coincide. In these cases, a password should be requested from the end-user instead. Digest 2G AKA passwords **MUST NOT** be re-used with such HTTP authentication schemes, which send the password in the clear. In particular, 2G AKA passwords must not be re-used with HTTP Basic.

The same principle must be applied within a scheme if several algorithms are supported. A client receiving an HTTP Digest challenge with several available algorithms **MUST** choose the strongest algorithm it understands. For example, Digest with "2GAKA-MD5" would be stronger than Digest with "MD5".

[8.4.](#) Online Dictionary Attacks

Since user-selected passwords are typically quite simple, it has been

proposed that servers should not accept passwords for HTTP Digest which are in the dictionary [[RFC2617](#)]. This potential threat does not exist in HTTP Digest 2G AKA because the algorithm will use SIM originated passwords. However, the end-user must still be careful with PIN codes. Even though HTTP Digest 2G AKA password requests are never displayed to the end-user, the end-user will be authenticated to the SIM via a PIN code. Commonly known initial PIN codes are typically installed to the SIM during manufacturing and if the end-users do not change them, there is a danger than an unauthorized user may be able to use the device. Naturally this requires that the unauthorized user has access to the physical device, and that the end-user has not changed the initial PIN code. For this reason, end-users are strongly encouraged to change their PIN codes when they receive a SIM.

[8.5.](#) Session Protection

Digest 2G AKA is able to generate an additional session key for integrity (Kc) protection. Even though this document does not specify the use of these additional keys, they may be used for creating additional security within HTTP authentication or some other security mechanisms.

[8.6.](#) Replay Protection

The generation of RAND used as one-time or very limited-use nonces and the use of the integrity protection of qop=auth-int will limit the possibility of replay attacks.

In GSM, the network is allowed to re-use the RAND challenge in consecutive authentication exchanges. This is not allowed in Digest 2G AKA. The server is mandated to use fresh triplets (RAND challenges) in consecutive authentication exchanges. Digest 2G AKA does not mandate any means for the client to check if the RANDs are fresh, so the security of the scheme leans on the secrecy of the triplets. However, the peer MAY employ implementation-specific mechanisms to remember some of the previously used RANDs, and the client MAY check the freshness of the server's RANDs.

[8.7.](#) Mutual Authentication

With Digest 2G AKA, network authentication is performed only after UE authentication, in contrary to Digest AKA [[RFC3310](#)] in which the UE authenticates the network before responding to the challenge. To prevent an impersonation attack of the server to the UE, the authentication of the server to the UE SHOULD be improved by protecting the communication with TLS. An attacker succeeds only if he can break both, the certificate-based TLS authentication to the UE and mutual authentication provided by HTTP Digest using a password derived from GSM procedures. One way to break TLS is to compromise the certificate.

[8.8.](#) Flooding the Authentication Centre

The server typically obtains authentication vectors from the Authentication Centre (AuC). Digest 2G AKA introduces a new usage for the AuC. The protocols between the server and the AuC are out of the scope of this document. However, it should be noted that a malicious client may generate a lot of protocol requests to mount a denial of service attack. The server implementation SHOULD take this into account and SHOULD take steps to limit the traffic that it generates towards the AuC, preventing the attacker from flooding the AuC and from extending the denial of service attack from Digest 2G AKA to other users of the AuC.

[8.9.](#) AKA Security

Evolutions of GSM networks, specifically Universal Mobile Telecommunications System (UMTS) and IP Multimedia System (IMS) networks, use an enhanced shared secret based mechanism for authentication known as Authentication and Key Agreement (AKA). In

these networks, AKA is typically run in a UMTS Services Identity Module (USIM) or IP Multimedia Services Identity Module (ISIM). GSM phones can also be equipped with a USIM or ISIM. In that case, Digest AKA as described in [[RFC3310](#)] is used for authentication as opposed to Digest 2G AKA.

[9.](#) Acknowledgements

This memo is based on an initial draft written by Brett Wallis ([draft-ietf-http-digest-auth-a3a8-01](#)).

10. References

10.1. Normative References

- [RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", [RFC 2045](#), November 1996.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2617] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", [RFC 2617](#), June 1999.

10.2. Informative References

- [RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", [RFC 3261](#), June 2002.
- [RFC3310] Niemi, A., Arkko, J., and V. Torvinen, "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)", [RFC 3310](#), September 2002.
- [TS55.205] "Specification of the GSM- MILENAGE algorithms (Release 9)", December 2009.

38-40 rue du general Leclerc
Issy-Les-Moulineaux Cedex 9 92794
France

Phone: +33 1 4529 6257

Email: lionel.morand@orange-ftgroup.com