

SIP
Internet-Draft
Intended status: Standards Track
Expires: August 21, 2008

K. Darilion
enum.at
H. Tschofenig
Nokia Siemens Networks
February 18, 2008

E.164 Ownership using Public Keys stored in ENUM
draft-darilion-sip-e164-enum-00.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on August 21, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

To determine which domain is allowed to claim ownership of a certain telephone number is difficult. This may cause problems when to authenticate endpoints that use telephone number URIs and domain names in their From address. This document investigates a proposal that stores a public key below the corresponding ENUM tree in the DNS. The verifier can determine ownership by performing an ENUM lookup to retrieve the public key from the DNS and to use it for

Internet-Draft

E.164 Ownership using ENUM

February 2008

verifying the signature created as part of the SIP Identity mechanism.

This document is a contribution to the ongoing discussion on [RFC 4474](#) when used in combination with E.164 numbers.

Table of Contents

1.	Introduction	3
2.	Terminology	4
3.	ENUM	5
3.1.	User ENUM	5
3.2.	Infrastructure ENUM	5
3.3.	Private ENUM trees	5
4.	Authentication Service Behavior	6
5.	Verifier Behavior	6
6.	Considerations for User Agent	8
7.	Considerations for Proxy Servers	8
8.	Examples	8
9.	Caching and Scalability	9
10.	Privacy Considerations	10
11.	Security Considerations	10
12.	IANA Considerations	11
12.1.	TBD 'Unable to retrieve Public Key from DNS' Response Code	11
12.2.	URI Scheme Registration	11
13.	Acknowledgments	11
14.	References	12
14.1.	Normative References	12

14.2. Informative References	12
Authors' Addresses	12
Intellectual Property and Copyright Statements	14

[1.](#) Introduction

[RFC 4474](#) [3] defines a mechanism whereby an authentication service authenticates a SIP UAC (possibly by sending a Digest authentication challenge) and verifies whether he or she is authorized to use the identity that is populated in the From header field. The authentication service then computes a hash over some particular headers, including the From header field and the bodies in the message. This hash is signed with the certificate for the domain and inserted in the 'Identity' header field in the SIP message.

The proxy, as the holder of the private key of its domain, is asserting that the originator of this request has been authenticated and that a specific user is authorized to claim the identity (the SIP address-of-record) that appears in the From header field. The proxy also inserts a companion header field, Identity-Info, that tells the verifying party how to acquire its certificate, in case it is not yet known already.

When the verifier receives the SIP message, it verifies the signature provided in the Identity header, and thus can determine whether the domain indicated by the host portion of the AoR in the From header field authenticated the user, and permitted the user to assert that From header field value.

The use of phone numbers with SIP was introduced with the TEL URL scheme [5] whereby domain names were not used with the phone numbers. SIP URIs always have domain names. In SIP [2], a translation between SIP URIs and TEL URLs is described: when translating from a SIP URI to a TEL URL, the domain name from the SIP URI is simply dropped. When translating in the other direction (or simply generating a SIP URI from an E.164 number) it is not clear how to populate the domain name.

When SIP Identity [3] is applied to E.164 numbers [8] then there is the question what the identity assertion actually means.

Additionally, the usage of the domain for an E.164 number is not useful as described in [7]. This document does not make use of a domain field attached to an E.164 number.

The authors of this document do not claim that the question of what ownership of E.164 numbers means is sufficiently well understood at this point to be fully confident that any solution actually helps to improve the current state-of-the-art. In fact, the entire end-to-end security story when a call originates in the PSTN and terminates somewhere on the Internet may weaken the security of the call to such an extent that additional security

Darilion & Tschofenig Expires August 21, 2008

[Page 3]

Internet-Draft

E.164 Ownership using ENUM

February 2008

mechanisms applied to the communication on the Internet leg of the call may not improve the overall security based on "security is as good as the weakest link". However, strawman proposals (like this one) might help to better understand the different forms of E.164 address ownership. The authors have received a large number of interesting comments after distributing an initial proposal.

This document investigates the ability to store a public key in the ENUM database. The private key corresponding to that public key is then used by the authentication service to compute the digital signature for the 'Identity' header. Additionally, an indication is provided for the verifier inside the Identity-Info header so that it is apparent that the public key is not available at a given URI but rather in the DNS used by ENUM. When the verifier receives a SIP message that contains the 'Identity' header instead of obtaining the certificate it performs a DNS lookup to determine the public key used for the specific E.164 number. Possessing the public key stored with the E.164 number allows verification of the digital signature.

From a design point of view we would like to make the following note:

This document does not define new SIP headers. Instead, it re-uses existing headers from the SIP Identity specification. The 'Identity-Info' header is reused to convey a so-called selector and the ENUM root. Both are required for the verification procedure. The selector allows the authentication service to support multiple concurrent public keys per signing domain and the ENUM root allows to use different ENUM trees. This document

suggests to store the selector and the ENUM root as a URI in the 'Identity-Info' even though a new and more flexible header is already required by the SIP SAML specification.

To summarize the proposed changes; this document suggests an alternative method for storing public keys, namely one based on the DNS in relationship to the ENUM database. This method is conceptually similar to the approach used by DKIM [4]. As a consequence, the mechanism to look-up the public key by the verifier is different to the one proposed in [3]. The suggested modifications are intentionally kept at a minimum and only applicable when an E.164 number is signed by an authentication service.

[2.](#) Terminology

In this document, several words are used to signify the requirements of the specification. These words are often capitalized. 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 [1].

[3.](#) ENUM

ENUM comes in different deployment variations. The incentives for storing public keys in ENUM with these deployments are different. Mostly, they can be distinguished by the root domain and whether access is restricted or unrestricted.

[3.1.](#) User ENUM

User ENUM is defined in [6]. It uses the root domain e164.arpa and access is not restricted. The right to provision DNS records is given to the user of the corresponding E.164 number.

Use cases for putting the public key into user ENUM are the following. A user who has registered its E.164 number into ENUM and has its own SIP infrastructure (like companies have) or users utilizing their own open SIP infrastructure (similar to users running an SMTP server).

[3.2.](#) Infrastructure ENUM

There is no exact definition for Infrastructure ENUM (also called Carrier ENUM). Infrastructure ENUM is often understood as a public accessible ENUM tree (for example ie164.arpa) where the "carrier-of-record" (the carrier which provide telephony service to the end-user) is allowed to provision the DNS records. It can also be seen as federations of private ENUM.

The use case for infrastructure ENUM is similar to user ENUM except that now carriers are able to relate the "carrier of record" to the E.164 number. For example, if a call is routed from carrier A to carrier B via transit carrier T, T will trust A and B will trust T. There is no way for B to verify that the caller is really allowed to use the indicated caller id.

[3.3.](#) Private ENUM trees

Private ENUM trees choose just any available domain as root domain (e.g., e164.example.com) and provide ENUM services below this root domain. Whether access is restricted or not, and the policy for provisioning of DNS records, is defined by the holder of that domain. An example of a private ENUM tree with restricted access is the 3GPP ENUM tree (e164enum.net).

Use cases are similar to before, except that the owner of the root domain can decide who is allowed to use the ENUM tree. Furthermore, private ENUM trees can be used if user ENUM is not available in the respective country (for example by using nrenum.net).

The main drawback of this proposal is the fact that public ENUM does not enjoy a lot of deployment (see <http://enumdata.org/>). This document is, however, particularly useful for environments that make use of public ENUM. Private and infrastructure ENUM only need SIP Identity alike mechanisms when interacting with the "external" world since they follow a sort of wallet garden model with a chain-of-trust. There is non-neglectable deployment incentive challenge. As such, this proposal will live or die with the ability to come up with a lucrative deployment story.

[4.](#) Authentication Service Behavior

The authentication service behavior proposed in this document is almost identical to the authentication service described in [\[3\]](#).

Thus, the authentication service behavior is identical to the description in Section 5 of [\[3\]](#) when TEL URIs are used with the following addition for step 4:

When a TEL URI scheme is used in context of SIP Identity then the 'Identity-Info' header field does not contain a URI pointing to a certificate but rather contains the DomainKeys selector and the ENOM root domain since the procedure described in [Section 5](#) allows the verifier to determine the location of the public key associated with a particular TEL URI.

The mechanism for storing a public key in the DNS is re-used from DKIM [\[4\]](#).

[5.](#) Verifier Behavior

When a verifier receives a SIP message containing an Identity-Info header, it may inspect the signature to verify the identity of the sender of the message. Typically, the results of a verification are provided as input to an authorization process which is outside the scope of this document. If an Identity-Info header is not present in a request, and one is required by either local policy (for example, based on a per-sending-domain policy, or a per-sending-user policy) or remote policy, then 'Use Identity Header' response code MUST be sent.

The steps executed by the verifier are outlined in Section 6 of [\[3\]](#) with the exception that step 1 is different primarily because SIP Identity relies on certificates whereas this document stores public keys in the DNS. The following paragraph replaces the text in [Section 6/step 1](#) of [\[3\]](#). This document does not make use of the 'Unsupported Certificate' and the 'Bad Identity-Info' response code.

Step 1:

The verifier MUST obtain the ENUM root domain from the Identity-Info header and apply local policies to find out if the specified ENUM root domain points to a trusted ENUM tree. If the specified ENUM tree is not trusted, the verifier has to cancel the signature verification and the message MUST be treated like an unsigned message.

Step 2:

The verifier MUST acquire the public key for the signing domain. This document suggests to store the public key in the DNS.

This document is only applicable for the usage of tel URIs in the From: header. When the tel URI contains a 'global-number', i.e., a phone number in E.164 format starting with the '+' sign, the domain for retrieving the public key will be constructed according to the following algorithm:

1. remove the 'visual-separators' and all parameters from the tel URI
2. remove the leading "+" sign
3. put dots (".") between each digit
4. reverse the order of the digits
5. append the ENUM root domain (for example ".e164.arpa") to the end
6. prepend the string "_domainkey."
7. prepend the selector

For example, given the tel URI "tel:+43-1-5056416-36;mobile=false", the selector "2008-02" and the root domain ".e164.arpa", the domain under which the public key is stored is:

2008-02._domainkey.6.3.6.1.4.6.5.0.5.1.3.4.e164.arpa

Non global-numbers cannot be stored in ENUM and thus they cannot be used in the From: header when signing the request by the authentication service.

The 'Unable to retrieve Public Key from DNS' response code is used

when an error in fetching the public key from the DNS occurs.

6. Considerations for User Agent

There are no additional considerations beyond those described in Section 8 of [\[3\]](#).

7. Considerations for Proxy Servers

There are no additional considerations beyond those described in Section 8 of [\[3\]](#).

8. Examples

The following message exchange highlights the interaction.

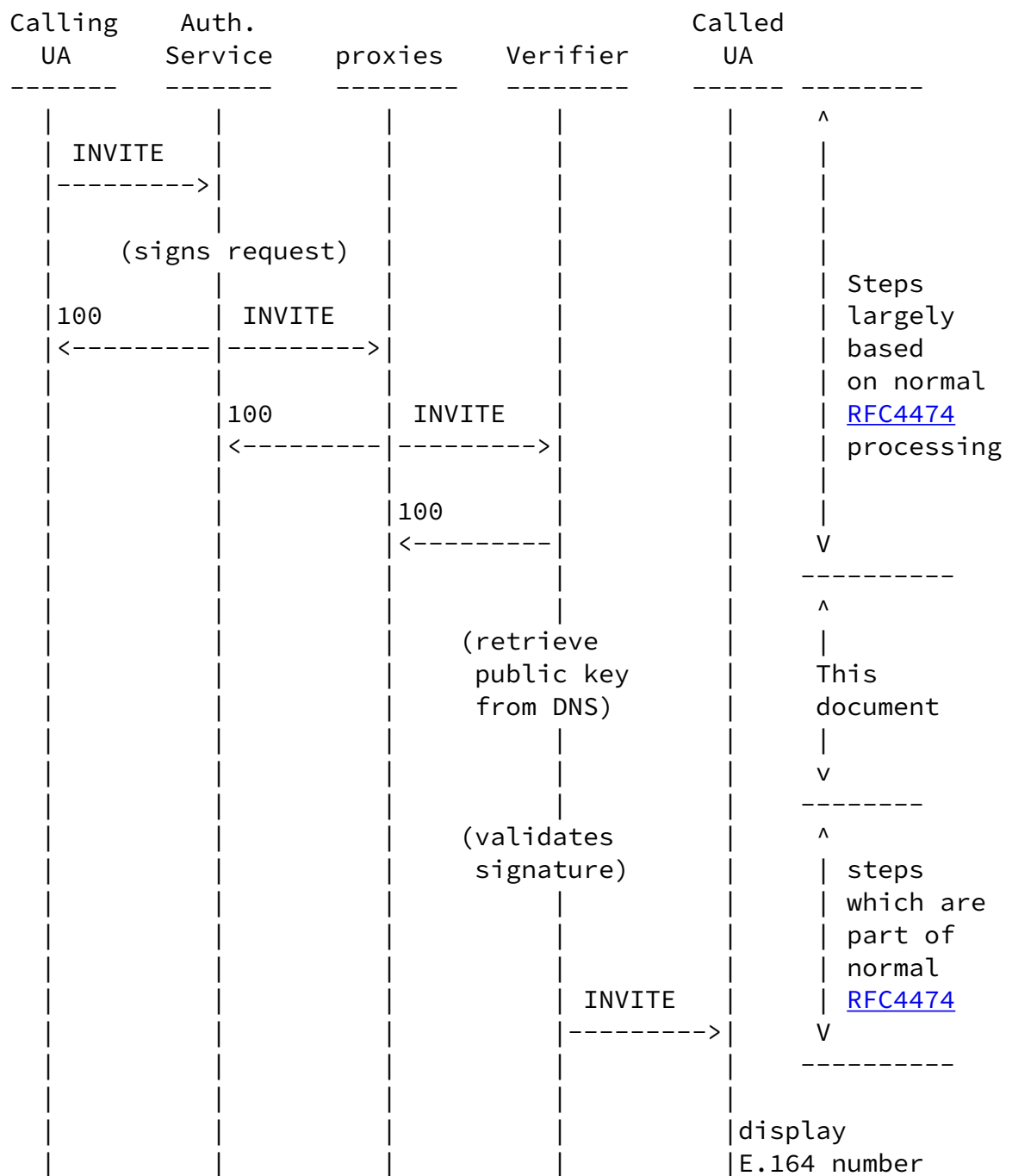


Figure 1: Example Exchange

9. Caching and Scalability

When the verifier needs to determine the public key of a specific E.164 number then it needs to perform a DNS lookup. This lookup might be cached in the DNS but the lookup is specific for a certain

E.164 number and not for a domain. The verifier may cache the public key corresponding to a particular E.164 number but there is no

guarantee that the same key will be used by any other E.164 number. Furthermore, a specific E.164 number may have multiple public keys associated with it based on the selector concept that is useful when revocating keys or when delegating the signing process.

10. Privacy Considerations

The mechanism presented in this draft is compatible with the standard SIP practices for privacy, described in [RFC 3323](#) [9] and also with the privacy considerations of [RFC 4474](#) [3].

11. Security Considerations

The mechanism described in this document has different authorization properties than [RFC 4474](#) [3]. A SIP message (including the 'Identity' and the 'Identity-Info' header) with an E.164 number in the From: header field has the following property (if successfully processed by the verifier):

The entity that uses the private key for creating the SIP Identity header is authorized to attach the corresponding public key to the ENUM database of the respective E.164 number used during the lookup.

When using PKI infrastructure, the signature verifier trusts the certificate authority, which attest the identity of the certificate holder. Using ENUM, the signature verifier has to trust the ENUM registry and the registrars. The ENUM registrar typically has to validate that the user who tries to register an ENUM domain is the number right holder. The validation methods usually will be different between user ENUM (the validation methods can be approved by official buddies) and private ENUM trees.

It is important to note that with this proposal public keys are essentially for individual users rather than for the entire domain. As such, the authentication service needs to have access to the private keys corresponding to the respective public key. Note,

however, that there is nothing special about these key pairs as such and there is no relationship to other (long-term) asymmetric credentials potentially possessed by the user. They are rather used only as a technical vehicle to accomplished the ownership requirement described in this document.

This proposal also does not address the case where a call originates in the PSTN and enters the Internet via provider that does not possess the private key corresponding to the public key stored with

the E.164 number in the ENUM tree. This is, in some sense, desired since Caller-ID spoofing is very easy in the PSTN and is difficult to differentiate from a call that enters the Internet through a provider that has no relationship with the calling party. This asymmetric routing scenario is, however, quite common today.

Additional security considerations can be found in [\[10\]](#).

[12.](#) IANA Considerations

This document requests IANA to register a new response code.

[12.1.](#) TBD 'Unable to retrieve Public Key from DNS' Response Code

This document registers a new SIP response code, which is described in [Section 5](#). It is used when a verifier tries to retrieve the public key from the DNS and does not succeed and the DNS lookup fails. This response code is defined by the following information, which has been added to the method and response-code sub-registry under <http://www.iana.org/assignments/sip-parameters>.

Response Code Number: TBD

Default Reason Phrase: Unable to retrieve Public Key from DNS

[12.2.](#) URI Scheme Registration

[Editor's Note: A future version of this document may register a URI scheme that allows the SIP 'Identity-Info' header to be reused in order to convey parameters from the authentication service to the verifier.]

13. Acknowledgments

We would like to thank Dan Wing for raising the problems associated with E.164 number-usage in SIP Identity and the discussion during writing of this draft. Further we would like to thank Alexander Mayrhofer for his ideas in [[draft-mayrhofer-enum-domainkeys-00](#)].

We would also like to thank Kai Fischer, John Elwell, Hadriel Kaplan, David Schwartz, and Jon Peterson for their off-list comments.

14. References

Darilion & Tschofenig Expires August 21, 2008 [Page 11]

Internet-Draft E.164 Ownership using ENUM February 2008

14.1. Normative References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [2] 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.
- [3] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", [RFC 4474](#), August 2006.
- [4] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures", [RFC 4871](#), May 2007.
- [5] Schulzrinne, H., "The tel URI for Telephone Numbers", [RFC 3966](#), December 2004.
- [6] Faltstrom, P. and M. Mealling, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", [RFC 3761](#), April 2004.

14.2. Informative References

- [7] Elwell, J., "SIP E.164 Problem Statement",
[draft-elwell-sip-e164-problem-statement-00](#) (work in progress),
February 2008.
- [8] ITU-T, "The international public telecommunication numbering
plan", Recommendation E.164, May 1997.
- [9] Peterson, J., "A Privacy Mechanism for the Session Initiation
Protocol (SIP)", [RFC 3323](#), November 2002.
- [10] Schwartz, D., "E.164 Ownership Problem Statement",
Std [draft-schwartz-sip-e164-ownership-00.txt](#), Feb 2008.

Authors' Addresses

Klaus Darilion
enum.at GmbH
Karlsplatz 1/9
Wien A-1010
Austria

Phone: +43 1 5056416 36
Email: klaus.darilion@enum.at
URI: <http://www.enum.at/>

Hannes Tschofenig
Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

Phone: +358 (50) 4871445
Email: Hannes.Tschofenig@nsn.com
URI: <http://www.tschofenig.com>

Darilion & Tschofenig Expires August 21, 2008 [Page 13]

Internet-Draft E.164 Ownership using ENUM February 2008

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

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, THE IETF TRUST 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.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).