Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 3, 2018

J. Peterson
Neustar
R. Barnes
Mozilla

October 30, 2017

ACME Identifiers and Challenges for Telephone Numbers
draft-ietf-acme-telephone-01.txt

Abstract

This document specifies identifiers and challenges required to enable the Automated Certificate Management Environment (ACME) to issue certificate for telephonoe numbers.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

ACME [I-D.ietf-acme-acme] is a mechanism for automating certificate management on the Internet. It enables administrative entities to prove effective control over resources like domain names, and automtes the process of generating and issuing certificates.

The STIR problem statement [RFC7340] identifies the need for Internet credentials that can attest authority for telephone numbers in order to detect impersonation, which is currently an enabler for common attacks associated with illegal robocalling, voicemail hacking, and swatting. These credentials are used to sign PASSporTs [I-D.ietf-stir-passport], which may be carried in using protocols such as SIP [I-D.ietf-stir-rfc4474bis] or delivered outside of the signaling channel of call setup [I-D.ietf-stir-oob]. Currently, the only defined credentials for this purpose are the certificates specified in [I-D.ietf-stir-certificates].

[I-D.ietf-stir-certificates] describes certificate extensions suitable for associating telephone numbers with certificates. To help enable certificate authorities to issue certificates with these extensions, this specification defines extensions to ACME suitable to enable certificate authorities to validate effective control of numbering resources and to issue corresponding certificates.

Note that the aim of the initial challenges specified in this document is not to prove the assignment and delegation of resources in the telephone network: it is instead to establish whether Internet-enabled entites have effective control over the devices associated with those resources. Such credentials are not mutually exclusive with credentials delegated from national authorities, and

future versions of this specification will explore issuance of those credentials as well. For the purposes of a call set-up protocol like SIP, there may be multiple attestations (for example, multiple SIP Identity header fields) signed by different parties.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in [RFC2119].

3. Telephone Number Identifier Type

In order to issue certificates for telephone numbers with ACME, a new ACME identifier type for telephone numbers is required for use in ACME authorization objects. The baseline ACME specification only defines one type of identifier, for a fully-qualified domain name ("dns"). This document thus defines a new ACME identifier type for telephone numbers ("tn"). This represents a telephone number, specifically a number of the type that is specified in the TN Authorization List certificate extension of [I-D.ietf-stir-certificates] for E164Number.

```
{
  "status": "valid",
  "expires": "2015-03-01T14:09:00Z",
  "identifier": {
    "type": "tn",
    "value": "2125551212"
  },
  "challenges": [
    {
      "type": "sms-link-00",
      "status": "valid",
      "validated": "2014-12-01T12:05:00Z",
      "keyAuthorization": "SXQe-2XODaDxNR...vb29HhjjLPSggwiE"
    }
  ]
}
```

4. Challenges for Telephone Numbers

Proving that a device on the Internet has effective control over a telephone number is not as easy as proving control over an Internet resources like a DNS zone or a resource on the web. Issuing certificates for telephone numbers is perhaps most closely analogous to certificates for email addresses: end user control over an email

address boils down to the capabilities to read and send email associated with that address. While a user typically has control over an email address for a long period of time, control over email addresses can change when users leave companies or other institutions, and addresses may subsequently end up in the control of another party. Moreover, while it is relatively easy to spoof the sender of any email address, as it unfortunately is with telephone numbers, it is harder to intercept traffic to a target email address or telephone number.

The likely challenges for proving effective control over a telephone number therefore rely largely on routing some kind of secret to the telephone number in question and requesting that the receiving device play that secret back to the ACME server. The Short Message Service (SMS) provides a key building block for challenges because of its ability to route a secret addressed to a telephone number to a user-controlled device. However, because of the diverse capabilities of Internet-connected devices that control telephone numbers, an SMS could be used in different ways for different challenges. Some devices will be able to interrogate their operating system to learn their own telephone number, for example, while others cannot. Some devices will be able to receive a text message and suppress it from being rendered to the user, while others cannot.

Because the assignment of numbering resources can change over time, demonstrations of effective control must be regularly refreshed -- though again, because of the diverse capabilities of the devices involved, different schemes for refreshing the challenge, ones that require less direct user supervision, may be available to some devices and not others.

4.1. Service Provider Validation

Communications Service Providers (CSPs) can delegate authority over numbers to their customers, and those CSPs who support ACME can then help customers to acquire certificates for those numbering resources with ACME. The system of [I-D.ietf-acme-service-provider] for example gives a mechanism that allows service providers to acquire certificates corresponding to a Service Provider Code (SPC) as defined in [I-D.ietf-stir-certificates]. Once service providers have certificates for SPCs, those could be leveraged to enable number acquisition flows compatible with those shown in [I-D.ietf-modern-problem-framework], by using a token mechanism such as the one described in [I-D.peterson-acme-authority-token].

[TBD token type registration and format]

The token must contain the delegated telephone number or number range, the SPC of the CSP, a nonce, the signature of the CSP with its SPC credential, and a link to a resource where relying parties can acquire the SPC credential.

An ACME server supporting the Service Provider Validation for telephone number certificates must have some way to determine whether or not a telephone number falls within a particular SPC. This may involve consulting a local or external database that maps SPCs to TNs. Without this check, CSPs would be able to issue credentials for numbers owned by other CSPs. The order should only be validated if the telephone number in the order actually falls under the SPC that signed the token.

4.2. Web-Based Telephone Number Routability Validation

With web-based telephone number routability validation, the client in an ACME transaction proves its control over a telephone number by proving that it can receive traffic sent to that number over the PSTN. The ACME server challenges the client to dereference a URL containing a token that is sent to the client over SMS. Typically that token will be embedded in a URL that the end user will visit in order to be guided to a web resource that will enable account creation with the CA. By allowing a user action to complete the challenge, this validation method supports the use of ACME with SMS endpoints that do not support automated response to challenges.

type (required, string): The string "sms-link-00"

token (required, string): A random value that uniquely identifies the challenge. This value MUST have at least 128 bits of entropy, in order to prevent an attacker from guessing it. It MUST NOT contain any characters outside the URL-safe Base64 alphabet and MUST NOT contain any padding characters ("=").

```
{
  "type": "sms-link-00",
}
```

A client's response to this challenge simply acknowledges that it is ready to receive the validation SMS from the server.

On receiving a response, the server sends an SMS message to the TN being validated containing a URL that the client must have a user access in order to complete the challenge. This URL is intended to be opened in a web browser so that the user can have an interaction with the CA; it is not sufficient for the client to simply send a GET request to the URL.

To validate an "sms-link" challenge, the server verifies that a user has visited the URL included in the SMS message and completed any steps specified there.

Because SMS return routability tests are becoming more common in two-factor authentication systems, they have also become an attractive target for attackers to try to compromise. Using short-lived certificates for this function, and requiring the client to perform this validation repeatedly, would help to mitigate associated risks.

4.3. Advanced Routability Validation

Future versions of this specification will explore ways to increase the automation of the challenge process when the client device has an application capable of creating ACME accounts and requesting certificates to be issued. This will likely follow the token / key-authorization pattern of the challenges defined for DNS names, except that the token and key authoriation will be passed in SMS instead of HTTP, TLS, or DNS.

4.4. Authority-Based Validation

Future versions of this specification will also explore ways that various numbering authorities could attest ownership over numbering resources, and ways that the assignees of numbers could coordinate with those authorities to satisfy ACME challenges and receive certificates. This would likely work much the same way as the Service Provider case in Section 4.1.

4.5. Telephone Number Range Validation

Future versions of this specification will explore ways to validate bulk allocations of telephone numbers such as those used by IP PBXs.

5. Acknowledgments

We would like to thank you for your contributions to this problem statement and framework.

6. IANA Considerations

Future versions of this specification will include registrations for the ACME Identifier type and ACME Challenge type registries here.

7. Security Considerations

TBD.

8. Informative References

[I-D.ietf-acme-acme]
Barnes, R., Hoffman-Andrews, J., and J. Kasten, "Automatic Certificate Management Environment (ACME)", draft-ietf-acme-acme-07 (work in progress), June 2017.

[I-D.ietf-acme-service-provider]
Barnes, M. and C. Wendt, "ACME Identifiers and Challenges for VoIP Service Providers", draft-ietf-acme-service-provider-01 (work in progress), July 2017.

[I-D.ietf-acme-star]
Sheffer, Y., Lopez, D., Dios, O., Pastor, A., and T. Fossati, "Use of Short-Term, Automatically-Renewed (STAR) Certificates to Delegate Authority over Web Sites", draft-ietf-acme-star-00 (work in progress), June 2017.

[I-D.ietf-modern-problem-framework]
Peterson, J. and T. McGarry, "Modern Problem Statement, Use Cases, and Framework", draft-ietf-modern-problem-framework-03 (work in progress), July 2017.

[I-D.ietf-stir-certificates]
Peterson, J. and S. Turner, "Secure Telephone Identity Credentials: Certificates", draft-ietf-stir-certificates-14 (work in progress), May 2017.

[I-D.ietf-stir-oob]
Rescorla, E. and J. Peterson, "STIR Out of Band Architecture and Use Cases", draft-ietf-stir-oob-00 (work in progress), July 2017.

[I-D.ietf-stir-passport]
Wendt, C. and J. Peterson, "Personal Assertion Token (PASSporT)", draft-ietf-stir-passport-11 (work in progress), February 2017.

[I-D.ietf-stir-rfc4474bis]
Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", draft-ietf-stir-rfc4474bis-16 (work in progress), February 2017.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7340] Peterson, J., Schulzrinne, H., and H. Tschofenig, "Secure Telephone Identity Problem Statement and Requirements", RFC 7340, DOI 10.17487/RFC7340, September 2014, <https://www.rfc-editor.org/info/rfc7340>.

Authors' Addresses

Jon Peterson
Neustar, Inc.
1800 Sutter St Suite 570
Concord, CA 94520
US

Email: jon.peterson@neustar.biz

Richard Barnes
Mozilla

Email: rlb@ipv.sx