

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: September 6, 2018

J. Peterson  
Neustar  
C. Wendt  
Comcast  
March 5, 2018

Using Telephone Related Information (TeRI) with the Distributed Registry  
Protocol (DRiP)  
[draft-peterson-modern-drip-teri-00.txt](#)

## Abstract

The Distributed Registry Protocol (DRiP) allows a set of nodes to implement a decentralized registry function. This document explores how Telephone Related Information (TeRI) Records can be shared by DRiP, and a decentralized registry approaches the operations necessary to assign, provision, and route for telephone numbers.

## 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 <https://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 September 6, 2018.

## Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://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

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Terminology . . . . .	<a href="#">3</a>
<a href="#">3.</a>	Use Cases . . . . .	<a href="#">3</a>
<a href="#">3.1.</a>	Assumptions . . . . .	<a href="#">3</a>
<a href="#">3.2.</a>	CSP Acquires a Block . . . . .	<a href="#">4</a>
<a href="#">3.3.</a>	CSP Acquires a Single Number . . . . .	<a href="#">4</a>
<a href="#">3.4.</a>	CSP Assigns a Single Number within its Block . . . . .	<a href="#">5</a>
<a href="#">3.5.</a>	Number Porting . . . . .	<a href="#">5</a>
<a href="#">4.</a>	Identity Elements in TeRI . . . . .	<a href="#">6</a>
<a href="#">5.</a>	Acknowledgments . . . . .	<a href="#">6</a>
<a href="#">6.</a>	IANA Considerations . . . . .	<a href="#">6</a>
<a href="#">7.</a>	Security Considerations . . . . .	<a href="#">6</a>
<a href="#">8.</a>	Informative References . . . . .	<a href="#">6</a>
	Authors' Addresses . . . . .	<a href="#">8</a>

## [1.](#) Introduction

The Distributed Registry Protocol (DRiP) [[I-D.wendt-modern-drip](#)] is a protocol that enables a distributed set of nodes to synchronize information in real-time with a minimal amount of delay. DRiP assumes a peer-to-peer gossip network that shares key-value pairs. The protocol is intended to carry information related to personal communication, including identifiers like telephone numbers and related identity information about the participants in communication.

The Telephone Related Information [[I-D.peterson-modern-teri](#)] information model provides a framework for distributing Records that convey service or administrative data about telephone numbers. TeRI Records are signed by entities such as CSPs or Registrars who possess credentials which enable relying parties to trust that Records have been created or modified by the appropriate parties for a particular telephone number, such as STIR [[RFC8226](#)] certificates. In TeRI parlance, anyone holding such a credential attesting authority over telephone number resources is called an "Authority." TeRI Records containing service data provide routing information for telephone numbers, and may be retrieved from local caches, remote services, or even a distributed network, as relying parties trust Authorities rather than services. The TeRI Record format therefore seems suitable for distribution via DRiP.

Following the MODERN framework [[I-D.ietf-modern-problem-framework](#)], TeRI usages for centralized registries support three fundamental operations on telephone numbers: acquisition, management, and



retrieval. There are at a high level a couple of potential ways to approach using TeRI with DRiP: for example, the gossip protocol could be used as a transport layer to pass client-server requests to what is effectively a centralized Authority that actually creates and signs TeRI Records; or, more interestingly, nodes in the gossip network might all act as Authorities, possessing credentials that enable them to create and sign TeRI Records themselves and then vote on their validity to prevent conflicts and race conditions. The possibility of a decentralized registry based on the latter principle largely motivates this exploration of the intersection between TeRI and DRiP.

This initial draft explores some key use cases for TeRI over DRiP, and how they differ from the use cases already given in the baseline MODERN framework [[I-D.ietf-modern-problem-framework](#)].

## **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. Use Cases**

### **3.1. Assumptions**

It is assumed in the MODERN system that before any actor can interact with a Registry, a Credential Authority provides certificate credentials to individual actors corresponding to their identity and role: such as the CSPs and Users of the MODERN framework [[I-D.ietf-modern-problem-framework](#)]. For the purposes of this document, we assume those credentials are STIR [[RFC8226](#)] certificates associated with telephone number blocks that can be managed by the distributed Registry.

These use cases explore the possibility that there could be more than one distinct administrative entity who holds credentials authorizing them to generate TeRI Records for the same numbering resources: effectively, that set of Authorities functions as a distributed Registry. Imagine, for example, that in the North American Numbering Plan an experimental area code were created that enabled any CSP authorized by the distributed Registry to reserve a new telephone number on a first come first serve basis - with some policy controls.

For these use cases we assume that a policy governs the acquisition of telephone numbers in the distributed Registry. For example, there could be a financial cost of acquiring numbers that goes up



dramatically if CSPs acquire resources too greedily; or alternatively, there could be some policy enforcement of the ratio of allocated to assigned numbers a CSP has claimed to maintain an agreed reasonable level of number inventory per CSP. In the DRiP gossip network, there could moreover be a "policy node" that simply votes "no" when new TeRI Records that conflict with the policy are propagated. These initial use cases are however "sunny day" cases where we assume that CSPs scrupulously adhere to policy.

### **3.2. CSP Acquires a Block**

In the following case, a CSP performs acquires a block of telephone numbers, placing it under their control using their credentials.

First, assume that a Numbering Authority has unallocated number blocks that are eligible for allocation, and that these resources have been made available to the distributed Registry.

Then, a CSP participating in the distributed Registry declares its intention to allocate one such block of Numbers. In centralized MODERN architectures, the CSP would send a TeRI acquisition operation query to the Registry, and receive a Record for the Block (along with associated credentials) from the Registry response. In this distributed architecture, the CSP simply creates a new administrative TeRI Record for the block and signs it with its own credential. It then propagates that Record through the gossip network. If no node in the network votes against the Record, it is cached by all nodes, and that Record becomes a new administrative Record for that block.

Note that per the MODERN framework [[I-D.ietf-modern-problem-framework](#)], a CSP can act directly as a Registrar itself, or it can use a third-party Registrar to effect these transactions.

### **3.3. CSP Acquires a Single Number**

In the following case, a CSP acquires a single available number in a block. Imagine, for example, that a new freephone area code 8yy were allocated in the North American Numbering Plan that allowed any Responsible Organization to acquire numbers on a first-come-first-serve basis under some governing policy.

First, assume that there are numbers under 8yy available for assignment.

Then, a CSP acting as a RespOrg participating in the distributed Registry declares its intention to allocate and assign a number to a customer. In this distributed architecture, the CSP simply creates a



new administrative TeRI Record for the individual TN and signs it with its own credential, marking it as assigned. It then propagates that Record through the gossip network. If no node in the network votes against the Record, it is cached by all nodes, and that Record becomes a new administrative Record for that block.

#### **3.4. CSP Assigns a Single Number within its Block**

In the following case, a CSP had already allocated a block to itself per [Section 3.2](#). Now, it intends to assign a single number in that block.

In centralized MODERN architectures, the CSP would contact the Registry with a TeRI management operation, notifying the Registry that the number's status had changed to assigned. In this distributed Registry, the CSP creates a new TeRI record for that individual number, marking it as assigned, signs it, and then propagates that Record through the gossip network.

The same would apply for marking a sub-block within the block as assigned: the CSP creates a new TeRI record for that individual sub-block, marking it as assigned, signs it, and then propagates that Record through the gossip network.

#### **3.5. Number Porting**

The most difficult use cases for the distributed Registry are ones where control of resources has been allocated or assigned to one CSP but must now move to a new CSP. Number portability is the most common cause of this, though various other business reasons might result in changes of control over allocated and/or assigned numbers.

Suppose that CSP B has allocated and assigned a block to itself, and that TeRI records for that block are cached throughout the gossip network. Now, CSP A declares its intention to assign a particular TN within the block of CSP B. CSP A does so by creating a new TeRI Record for the number which CSP A signs, allocating the number to itself and marking it as assigned. As this Record propagates through the gossip network, CSP B recognizes this transaction and does not vote "no", in effect authorizing the transfer. If CSP B's customer were not porting the number to CSP A, then CSP B would vote "no."

From a policy oversight perspective, this could require a "policy node" or similar actor in the network to make sure it is not abused.





#### **4. Identity Elements in TeRI**

[Future versions of this specification will explore extensions to baseline TeRI for DRiP use cases.]

#### **5. Acknowledgments**

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

#### **6. IANA Considerations**

This document contains no instructions for the IANA.

#### **7. Security Considerations**

TBD.

#### **8. Informative References**

[I-D.ietf-acme-acme]

Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", [draft-ietf-acme-acme-09](#) (work in progress), December 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-02](#) (work in progress), October 2017.

[I-D.ietf-acme-star]

Sheffer, Y., Lopez, D., Dios, O., Pastor, A., and T. Fossati, "Support for Short-Term, Automatically-Renewed (STAR) Certificates in Automated Certificate Management Environment (ACME)", [draft-ietf-acme-star-03](#) (work in progress), March 2018.

[I-D.ietf-acme-telephone]

Peterson, J. and R. Barnes, "ACME Identifiers and Challenges for Telephone Numbers", [draft-ietf-acme-telephone-01](#) (work in progress), October 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-18](#) (work in progress), December 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.

[I-D.peterson-modern-teri]

Peterson, J., "An Architecture and Information Model for Telephone-Related Information (TeRI)", [draft-peterson-modern-teri-03](#) (work in progress), July 2017.

[I-D.rescorla-stir-fallback]

Rescorla, E. and J. Peterson, "STIR Out of Band Architecture and Use Cases", [draft-rescorla-stir-fallback-02](#) (work in progress), June 2017.

[I-D.wendt-modern-drip]

Wendt, C. and H. Bellur, "Distributed Registry Protocol (DRiP)", [draft-wendt-modern-drip-02](#) (work in progress), July 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>>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", [RFC 7515](#), DOI 10.17487/RFC7515, May 2015, <<https://www.rfc-editor.org/info/rfc7515>>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", [RFC 7519](#), DOI 10.17487/RFC7519, May 2015, <<https://www.rfc-editor.org/info/rfc7519>>.



[RFC8226] Peterson, J. and S. Turner, "Secure Telephone Identity Credentials: Certificates", [RFC 8226](https://www.rfc-editor.org/info/rfc8226), DOI 10.17487/RFC8226, February 2018, <<https://www.rfc-editor.org/info/rfc8226>>.

#### Authors' Addresses

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

Email: [jon.peterson@neustar.biz](mailto:jon.peterson@neustar.biz)

Chris Wendt  
Comcast  
One Comcast Center  
Philadelphia, PA 19103  
USA

Email: [chris-ietf@chriswendt.net](mailto:chris-ietf@chriswendt.net)

