Creating Identity Solutions^{SM}

InCharge Systems, Inc.
1128 20th Street
West Des Moines, IA 50265

VIA ECFS

July 3, 2013

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, S.W., Room TW-A325
Washington, D.C. 20554

Re: GN Docket No. 13-5

Dear Ms. Dortch:

InCharge Systems (ICS) hereby submits these comments in response to the Commission's Technology Transitions Policy Task Force (TTPTF) public notice[1] seeking comment on several potential trials. The scope of the potential trials includes technology trials for VoIP interconnection and additional trials.

ICS proposes that signing and validation related to phone numbers should be part of these trials. ICS further believes such trials should identify and clarify potential regulatory and policy issues resulting from the use of signing and validation that directly impact calling end users, called end users, and network elements that perform the signing and validation functions.

1. Signing and Validation Related to Phone Numbers

When a public/private key pair is associated with a phone number, many benefits become possible. In particular, secure caller identification can be provided when signing is performed at call origination and when subsequent validation can be performed anywhere along the call path. This capability could be used to mitigate spoofing/impersonation when dealing with threats such as robocalling, swatting, and vishing.

Using techniques similar to those described in RFC 4474,[2] ICS demonstrated the feasibility of such an approach in 2009 at the IIT VoIP Conference.[3] SIP calls using a phone number were signed at origination. Validation was able to tell if a call had been signed or not, or if the signature was valid or not. To support this, key pairs were generated for a set of phone numbers.

[1] *Technology Transitions Policy Task Force Seeks Comment on Potential Trials*, GN Docket No. 13-5, Public Notice, DA 13-1016 (Technology Transitions Policy Task Force, May 10, 2012), http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-13-1016A1.pdf.

[2] RFC 4474, *Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)*, J. Peterson, C. Jennings, August 2006, http://tools.ietf.org/html/rfc4474.

[3] *Authenticated Identities within SIP Call Control: Interoperability Test Results*. See the conference schedule at http://www.cvent.com/events/5th-annual-voip-conference-and-expo/custom-22-31a8c7fea5b54da799ab8e110eae0312.aspx.

When a SIP call was originated, its locally stored private key was used for signing, and the corresponding public certificate used for validation was retrieved from a web server. As a result of this and other work, ICS submitted comments to the Commision advocating the use of cryptographic signing and validation for calls, which were included in its 2011 report to Congress on Caller Identification Information in Successor or Replacement Technologies.[4]

There is a lot of current interest in secure call origination, secure telephone identity, and call signing and validation.[5, 6, 7, 8, 9] ICS believes that the time is now right for the Commission to be actively involved in this area by including a trial of signing and validation related to phone numbers in the potential trials being considered.

2. Proposed Trials

Many technical issues related to secure telephone identity can be found in discussions on the mailing list of the IETF's "STIR" activity.[10] The next meeting of the IETF begins at the end of July 2013 and is likely to lead to a new Working Group and the development of protocol documents. This work could help resolve a number of technical issues.

ICS believes that the TTPTF should consider trials with lower technical complexity in order to focus on related objectives that do not depend on how certain technical issues are resolved. These are the objectives that ICS proposes for such a trial.

- First, it is necessary to demonstrate that signing and validation are not only feasible but practical, and that these functions be exercised in a number of configurations and scenarios.

- Second, it is useful to identify the ranges of related issues that arise, non-technical as well as technical, and which stakeholders are likely to be involved.

- Third, it is desirable to identify areas for policy recommendations and any needed regulatory work so that the overall implementation of a framework for secure telephone identity can be successful.

[4] FCC's Report to Congress, *Caller Identification Information in Successor or Replacement Technologies*, June 22, 2011, Par. 43, Par. 44, and Note 88, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-11-1089A1.pdf.

[5] FCC Technological Advisory Council (TAC) Meeting Presentation, September 24, 2012, pgs. 38 and 52, http://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting92412/TAC-9-24-12-Presentations.pdf.

[6] *Secure Call Origin Identification*, A. Cooper, H. Tschofenig, J. Peterson, B. Aboba, November 30, 2012, https://datatracker.ietf.org/doc/draft-cooper-iab-secure-origin/.

[7] *Secure Origin Identification: Problem Statement, Requirements, and Roadmap*, Jon Peterson, Henning Schulzrinne, Hannes Tschofenig, May 27, 2013, https://datatracker.ietf.org/doc/draft-peterson-secure-origin-ps/.

[8] *Authenticated Identity Management in the Session Initiation Protocol (SIP)*, J. Peterson, C. Jennings, E.K. Rescorla, May 29, 2013, https://datatracker.ietf.org/doc/draft-jennings-dispatch-rfc4474bis/.

[9] *Source Identity (Origin Authentication)*, Henning Schulzrinne, May 31, 2013, http://www.cs.columbia.edu/~hgs/papers/2013/2013-source-identity.pptx.

[10] Secure Telephone Identity Revisited (STIR) BoF, scheduled for IETF 87, Draft Charter: http://www.ietf.org/mail-archive/web/stir/current/msg00200.html, Mailing List: https://www.ietf.org/mailman/listinfo/stir.

Therefore, ICS proposes that, at a minimum, a single neutral entity should initially operate a database for proposed trials of signing and validation, the database should store the E.164 phone numbers to be used in the trials along with the public certificates associated with those numbers, and that the database be web-accessible.

Trial participants whose network elements or end devices act as call originators using phone numbers would populate this database and would sign calls using private keys whose corresponding public certificates can be retrieved from the database. Any trial participant that has a network element along the call path, or who acts as a called end user or call handling entity, would then have the option to attempt to validate a potentially signed call by fetching the certificate associated with the called number from the database and extracting the public key.

It is important that all stakeholders agree that technical, operational, and administrative matters related to such a trial are for the trial only and are not intended to preclude or favor how things will progress after the trial.

It is also important that trial participants agree on test plans and procedures, and that they agree to provide test reports, including issues identified and lessons learned, in order to document the results of the trial.

In particular, it is highly desirable that issues relating to the signing and validation functions that involve end users and network elements be identified and considered. This data would be useful in the development of policy recommendations.

3. End Users and Network Elements

End users – the calling and called parties – will be affected by whatever changes are made to the systems they use and rely on. In its earlier demonstration of feasibility, ICS identified several issues impacting end users that required decisions to be made when signing and validation functions were performed. For the demonstration, ICS chose to complete all valid calls and to route invalid calls to a recorded voice announcement. Those preferences are just a sample of the decisions that will be embodied in systems that sign and validate calls.

- How a called party chooses to respond to an incoming call would depend on the result of the validation of the call, the capabilities of the end user’s device, and the terminating provider’s services. An end user might prefer to receive all incoming calls as long as there is an indication (such as a tone or brief announcement, or a displayed icon or message) if a call is unsigned or if validation fails. Another end user might choose to have all invalid calls blocked.

- How a calling party deals with a validation result may depend on things beyond that caller’s control. What kind of notification would be given to a caller whose call’s validation fails? What course(s) of action would a caller have if the originating carrier or service provider was unable to sign a call?

For network elements, decisions about call handling and notifications will be based on the results of their signing or validation actions.

- If a network element fails to successfully sign a call, how if at all should it indicate that status, and how is the call handled? Who if anyone should be notified?

- If a network element fails to validate a signed call, again, how if at all should it indicate that status, how is the call handled, and who if anyone should be notified?

- How should a network element handle an unsigned call?

These are examples of issues that are not necessarily or entirely technical. ICS believes that these issues show the need for work to develop policy guidelines. ICS further believes that a trial of signing and validation based on phone numbers used to make calls is an effective way to gather data that would be used to develop those policy guidelines.

Without sufficient policy guidelines (and such regulation as may be needed) for signing and validation related to phone numbers, there is a clear danger of call handling and notification decisions being implemented and configured in a piecemeal and uncoordinated fashion. This would impair interoperability and degrade end user experience, which are just two of the potential negative consequences of failing to address these issues.

4. Conclusion

InCharge Systems believes the current proceeding offers the Commission a unique and timely opportunity to address issues related to signing and validation of calls related to phone numbers. This opportunity is afforded by the TTPTF's public notice seeking comments on technology and additional trials.

ICS strongly urges that a trial such as the one described above be conducted, that the data collected include call handling and notification issues affecting end users and network elements, and that policy recommendations and guidelines be developed to address these issues.

Thank you.

Respectfully submitted,

/s/ Michael D. Hamilton

Michael D. Hamilton, President
InCharge Systems, Inc.
1128 20th Street
West Des Moines, Iowa 50265
mikehamilton@inchargesys.com
+1.515.224.9600