November 2021

LEVERAGING RICH CALL DATA TO ENHANCE CUSTOMER EXPERIENCE

Kaustubh Inamdar

Gonzalo Salgueiro

Sreekanth Narayanan

LEVERAGING RICH CALL DATA TO ENHANCE CUSTOMER EXPERIENCE

AUTHORS:
Kaustubh Inamdar
Gonzalo Salgueiro
Sreekanth Narayanan

ABSTRACT

Secure Telephony Identity Revisited (STIR) is an effort currently being utilized to provide cryptographic assurance of caller Identity in an effort to combat robocalls and impersonation attacks. The STIR framework can be used to transport additional claims during the course of a call. These additional claims, known as Rich Call Data (RCD), may be leveraged to embed useful, context-driven information. In particular, techniques presented herein provide an overarching framework through which companies that have a technical support division can advertise a set of RCD keys that would allow callers to avoid having to navigate interactive voice response (IVR) menus, specify support contract numbers, provide device serial numbers, and explain the specifics of assistance required. By advertising a set of required RCD keys, support organizations can expect to receive RCD calls from their customers. On parsing the key set present within an RCD STIR claim, systems can route calls to the appropriate tech support representatives or automatically open support cases.

DETAILED DESCRIPTION

Many service providers or equipment manufacturers have a technical services arm that helps in assisting customers with product queries, product configuration, device replacement, solution integration, among others. However, in most cases, customers often have to navigate through a complex set of interactive voice response (IVR) menus and, often times, may even have to verbally describe their problem to a "front line" individual before they speak to someone that that can help them from a technical stand point.

Regardless of the quality of technical support obtained, customers typically have to spend a significant amount of time navigating pre-established controls before they are able

to get their problem solved. This, of course, is non-optimal and can negatively impact customer experience.

This proposal leverages Rich Call Data (RCD) within a Secure Telephony Identity Revisited (STIR) framework to provide techniques through which the customer support experience can be made more fluid.

The STIR framework can be leveraged to transport RCD, which is typically embedded as an "RCD" claim in a standard Personal Assertion Token (PASSporT), from a caller to a callee. RCD transported from a caller to a callee must include a 'nam' key, as defined in https://datatracker.ietf.org/doc/draft-ietf-stir-passport-rcd. Additionally, for a more extensive set of key-value pairs, the fields specified in https://tools.ietf.org/html/draft-ietf-sipcore-callinfo-rcd-01 and Internet Engineering Task Force (IETF) Request For Comments (RFC) 7095 may be leveraged.

Techniques of this proposal provide an overarching framework through which companies that have a technical support division can advertise a set of RCD keys that would allow callers to avoid having to navigate IVR menus, specify support contract numbers, provide device serial numbers, and explain the specifics of assistance required. By advertising a set of required RCD keys, support organizations can expect to receive RCD calls from their customers. On parsing the key set present within an RCD STIR claim, systems can route calls to the appropriate tech support representatives or automatically open support cases.

Techniques of this proposal can be explained through the use of various core tenets involving various example entities, as follows:

1. CompanyABC: A large multi-national corporation that has several departments, many of which are central to engineering/infrastructure.
2. Company123: An equipment manufacturer of storage devices.
3. Company456: An equipment manufacturer of network load balancers.
4. DepartmentXYZ: A department within CompanyABC that is responsible for network infrastructure rollout for CompanyABC.

To realize features of this proposal, consider that a STIR authentication service operating in Company ABC is responsible for signing PASSporTs for calls originating from CompanyABC. Additionally, consider that the calls that originate from Company ABC, in addition to the standard PASSporT claims of calling/called number and Issued At Time, also include RCD. Further, consider that members of DepartmentXYZ initiate support calls to support teams of Company123 and Company456 to ensure the upkeep of certain infrastructure assets.

The telephony infrastructures belonging to both Company123 and Company456 may support the STIR framework and, subsequently, use this framework as a basis for receiving calls containing RCD. Additionally, it is assumed that both companies require different key-value pairs that are to be communicated as part of RCD to ensure a smooth customer experience. For example, Company123 may require the following key-value pairs as part of RCD: 'fn', 'tel', 'email', 'title', 'role', and 'org'.

Additionally, Company123 may also require a support contract identifier that is held by DepartmentXYZ of CompanyABC. Company456, on the other hand, requires the same information sets as Company123, but also requires the following:

a) The identifier of the device for which technical support is being requested; and
b) The type of service being requested - namely service types such as, Configuration, Troubleshooting, or Design Verification.

Different companies would typically require different keys (fields) as part of RCD to be able to provide superior customer experience. Therefore, in order to discern the required key set as part of RCD, these companies can provide an Application Programming Interface (API) or publish a Uniform Resource Locator (URL) that, when de-referenced, can provide external entities the key set required as part of RCD.

At the very least, the support organization of any company would require a "service contract identifier" to identify the company or the team within a company from which a person is calling. If there are several devices attached to a service contract identifier - for example, 100 switches, 1000 IP phones, 800 headsets, etc. a provision should exist that is capable of identifying a particular device in question. Additionally, a mechanism should exist to determine, at a high-level, the category of assistance being sought by callers.

Accordingly, this proposal provides that additional elements can be added to the standard set of vCard/jCard elements, namely:

a) contract - an element that denotes the service contract number;
b) device identifier/serial number - a unique identifier provided to a device at the time of manufacturing; and
c) service - a string denoting the category of assistance required - for example: 'configuration' or 'design'.

Figure 1, below, illustrates various example details associated with an example vCard displaying various fields, as discussed above.

```
["vcard",
    [
      ["version", {}, "text", "4.0"],
      ["contract", {}, "text", ["12345678"],
      ["device/PID", {}, "text", "ABCDEF1234"],
      ["service", {}, "text", "Configuration Assistance"],
    ]
  ]
```

Figure 1: Example vCard Displaying Selected Fields

When someone from DepartmentXYZ of CompanyABC originates a call to mainline support number of Company456, based on the calling and called number, a call processing node within the enterprise network such as a single board computer (SBC), mints a PASSporT containing RCD claims such that the key set is populated according to the requirements published (e.g., via an API or URL) by Company456. This key set can be obtained by the SBC during the dial plan configuration phase or manually entered by an administrator. Alternatively, the SBC can redirect the call to a third-party application that can be configured to gather RCD key sets for different numbers over telephony networks and, subsequently, populate RCD claims in accordance with the required key sets.

In order to populate the key set required in the PASSporT, entities such as SBCs or third-party applications may have to consult a database(s) in some instances, for example, to obtain richer details about the caller, such as the title of caller, the role of the caller, the photo of the caller, service contract number, etc.

The PASSporT may be signed by the SBC (assuming it is the node populating RCD information) or the third-party application (if the application is the one populating RCD information). To ensure that the PASSporT claims are trusted by third-party intermediaries, including telecommunication system operators, the PASSporT should be signed using credentials from delegate certificates, such that these certificates are rooted to a trusted Certificate Authority (CA).

There could be situations in which the entity signing PASSporTs in the enterprise network of CompanyABC might be different that the entity populating RCD information. For example, there could be a lookup service that is responsible for two functions: a) Filling in the RCD information according to the required key set for a called number; and b) Providing a publicly accessible URL (included as the value of the 'jcl' claim of RCD), which when de-referenced is a jCard.

However, in order to ensure that the lookup service populates the jCard/RCD to comply with certain pre-established policies, specifically around what are allowed/permitted values, an 'rcdi' claim may be included in the PASSporT and can be set to be equal to one of the 'permitted values' (*see*, Section 8 of RFC 8226) contained in the certificate used to sign the PASSporT. More succinctly, the credential used to sign the PASSporT may be derived from a certificate that has the 'mustInclude' and 'permittedValues' extensions. The certificate has a 'mustInclude' for the 'rcd' and 'rcdi' claims. Additionally, the 'permittedValues' can contain multiple possible entries to allow for variability.

Such a construct may provide various benefits, including:

a) When the SBC signs the PASSporT, if the value of the 'rcdi' claim is not equal to one of the 'permittedValues' listed in the certificate, the call can be rejected at the source.
b) Restriction at the source, namely the enterprise network, can be enforced to allow only authorized personnel to make calls and reference support contract numbers.

After the PASSporT is minted and communicated to the destination network/device, either via either in-band or out-of-band STIR, the call makes it way to the destination,

namely Company456. Once the call arrives at Company456, we assume that the verification checks pass, especially when considering the lookup service and construct, as specified above. Once verification succeeds, the verification service on Company456 can send the key values obtained from the RCD PASSporT to backend systems via interfaces such as APIs to determine the fate of the call.

These backend systems, on obtaining key values, are able to then decide where the calls are to be routed, for example, to a designated expert based on the device type and problem code or can determine if a support case is to be opened with the appropriate key words and problem description. In one instance, the problem description may be obtained from the 'crn' claim of PASSporT.

Figure 2, below, illustrates various example details associated with an example operational flow following the various operations as discussed above.

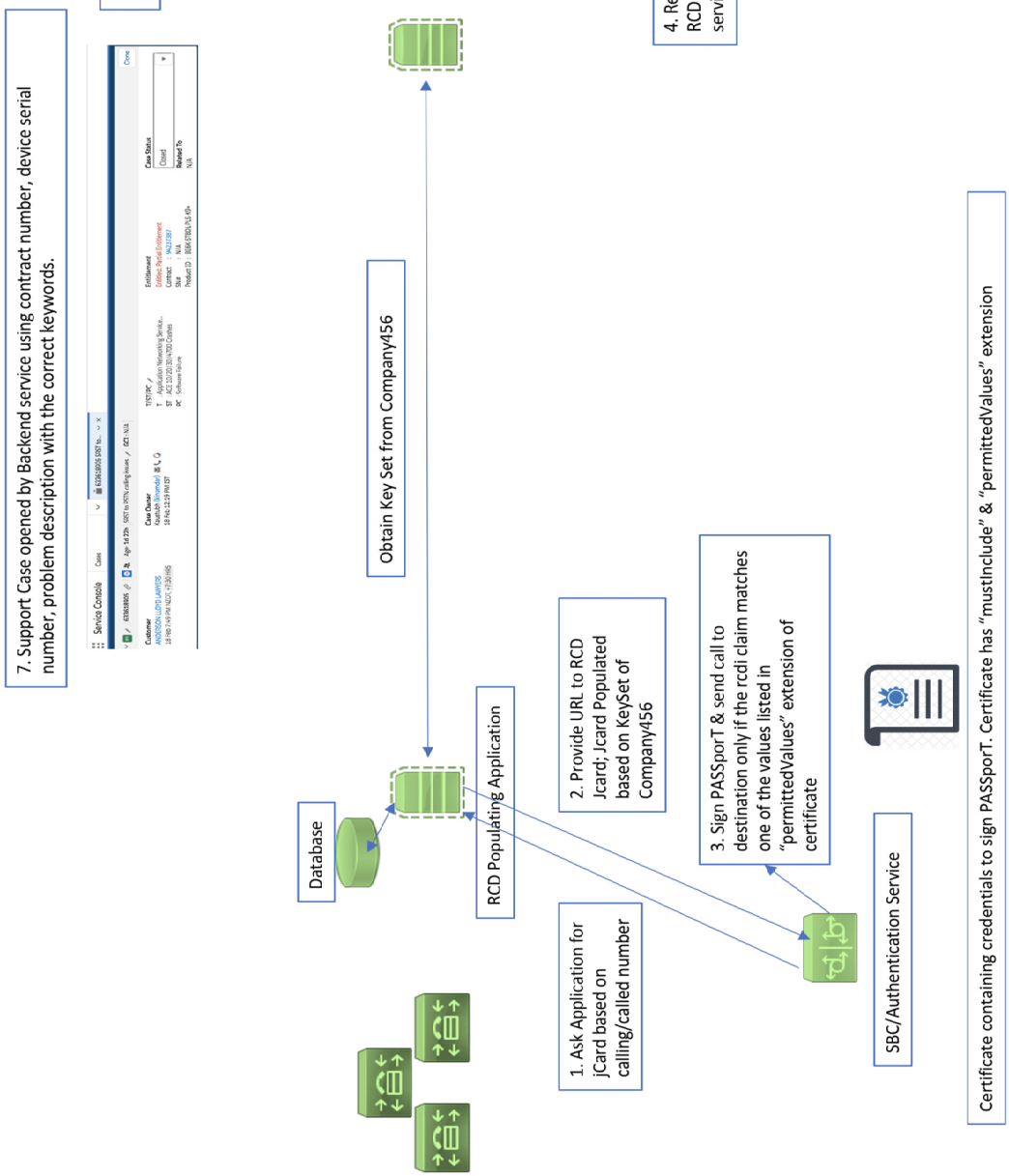

Figure 2: Example Operational Flow