DOCKETED	
Docket Number:	19-OIR-01
Project Title:	Load Management Rulemaking
TN #:	237533
Document Title:	UtilityAPI Comments on Potential Amendments to the Load Management Standards
Description:	N/A
Filer:	System
Organization:	UtilityAPI, Inc.
Submitter Role:	Public
Submission Date:	4/23/2021 2:22:17 PM
Docketed Date:	4/23/2021

Comment Received From: UtilityAPI, Inc.
Submitted On: 4/23/2021
Docket Number: 19-OIR-01

UtilityAPI Comments on Potential Amendments to the Load Management Standards

Additional submitted attachment is included below.

UtilityAPI, Inc.
1212 Broadway, 16th Floor
Oakland, CA 94612
(510) 907-0009
info@utilityapi.com
https://utilityapi.com

Submitted: April 23, 2021

California Energy Commission
1516 Ninth Street, MS-29
Sacramento, CA 95814-5512

Docket No. 19-OIR-01, "Load Management Rulemaking"

Re: Comments of UtilityAPI on Potential Amendments to the Load Management Standards

Dear Commissioners:

UtilityAPI is a technology services company providing energy data access services, including implementing Green Button Connect (GBC), for both utilities and third party service providers. Additionally, UtilityAPI is vice-chair on the board of the Green Button Alliance (GBA) and actively participates in the GBA working group OpenADE, the standards body responsible for maintaining the GBC standard.

UtilityAPI strongly supports the Draft Staff Analysis of the Potential Amendments to the Load Management Standards and very much appreciates the opportunity to file comments regarding the subject.

As an experienced implementer of utility-to-third-party data access platforms, UtilityAPI would like to focus on user experience possibilities for customers and service providers for the Rate Identification Number (RIN) Access Tool. Specifically, UtilityAPI would like to expand and describe what is technically possible given existing data access standards and best practices.

1. Streamlining consent and RIN access

As described in Chapter 2-B of the Draft Staff Analysis ("Third-Party Automation Services"), Automation Service Providers (ASPs) will often have an on-device or mobile app setup interface that can guide a customer through a device setup process, and RIN consent and access functionality should be able to seamlessly integrate into that setup process. Additionally, UtilityAPI has experienced that the optimal user experience is achieved when a customer is only asked to provide a piece of information they already know without having to go look it up, such as their address, phone number, or email address (and not their utility account number, for example).

Given these assumptions, UtilityAPI would like to describe a streamlined customer experience for setting up a device and granting access to their RIN:

1. Plug in a smart device and install the app.
2. Type in their phone number when asked in the app setup process.
3. Receive a text message from the Load Serving Entity (LSE) saying if they want to share their RIN with this ASP, type in this code.
4. Type in the code.
5. Done. The RIN is shared.

Behind the scenes, here is a technical breakdown of how the app interacts with the LSE to achieve the above streamlined customer experience:

1. When installed an app can use the location functionality on the mobile device to find possible LSEs for that area (see "Streamlining finding LSEs" section below). If in a CCA territory, both CCA and IOU are returned. If not in a territory covered by a CCA, then only the IOU/municipal utility is returned.

2. The app asks the customer for a piece of identifying information they can use to try to find the customer's account at the LSE, such as the customer's address, phone number, email, or account number.

3. The app sends the provided identifying information along with the scope of data requested (i.e. the RIN) to the /verify API endpoint at each possible LSE (see "Appendix A. OTP Authorization Flow Diagrams" section below), which returns either a list of authentication options (e.g. "text code to 4**-***-***2", "email code to a*****@****.**m", etc.) or an error signifying that this is not a customer (e.g. wrong phone number). If returned a list of authentication options, the app can ask the user to select which authentication option they prefer or automatically select one and submit it to trigger the LSE to initiate the authentication attempt using that option (e.g. "text code to 4**-***-***2"). The LSE sends a One Time Passcode (OTP) to the customer via the selected authentication option (e.g. text message) along with a message summarizing the access being requested.

4. The app presents an input field so that when the customer receives the text message, they can type it in. When the customer types in the code, the app submits the code back to the LSE as verification of consent. The LSE then returns an access token that can be used to access the LSE's RIN Access Tool. Additionally, the LSE should send the customer a confirmation receipt email with a link to the authorization so that the

customer can revoke access if they change their mind later.

5. The app uses the access token to query the RIN Access Tool (a Green Button Connect API can act as the RIN Access Tool) and obtain the customer's RIN. Additionally, if originally requested in the scope of access, ongoing access to the RIN can be provided using the same customer experience, so that if a customer changes their rate, the app can adjust the smart device's behavior accordingly.

There are multiple benefits of this streamlined customer experience:

- The customer does not need to know their LSE.
- The customer never has to leave the app setup interface.
- The customer can revoke access at any time.
- The ASP does not need to know whether the customer is bundled or unbundled.
- The final RIN data retrieval is compatible with existing GBC API implementations.
- The process supports multi-meter access for commercial customers.
- The process supports optional additional data fields (e.g. RIN + monthly usage).
- The process supports ongoing access for monitoring the RIN for changes.

The above described streamlined customer experience builds off of existing standards. The Green Button Connect standard can be used to transfer the RIN once a customer has consented, and customer authentication uses One Time Passcodes (OTPs), which is commonly used in other industries such as banking and mobile app verification.

2. Streamlining finding LSEs

In order to streamline the development process for ASPs, UtilityAPI suggests that a central API or database be created that allows registered ASPs to look up what LSEs are available at a given location (latitude, longitude). This allows an ASP to narrow down the possible LSEs to involve in the initial verification lookup step based on a customer's location, which can be provided using a mobile phone's GPS or the customer inputting their address or zip code. If an LSE-by-location is not made available, ASPs may resort to attempting the initial step of the OTP authorization flow across all LSEs (i.e. all CCAs, IOUs, and participating municipal utilities), which will create significant yet unneeded traffic on the LSE verification APIs.

For a central API method, a central entity (perhaps the CEC) would need to operate and maintain an API endpoint to which registered ASPs could make requests with location information (latitude, longitude) and receive back a list of participating LSEs at that location. The advantage of this method is that ASPs would not need to develop their own geospatial query system. The disadvantage of this is that a central API needs to be able to scale to large

amounts of simultaneous requests, since it can potentially be queried for every smart energy device setup across the state.

For a central database method, registered ASPs would be able to, on a regular basis, copy a database of geospatial shape files that represent the territories of all participating CCAs, IOUs, and municipal utilities. The advantage of this method is that day-to-day lookup queries would be done internally by each ASP, so no central system would have to handle the traffic. The disadvantage of this is that each ASP would need to set up their own parsing and geospatial query system to be able to use the database shape files.

Closing

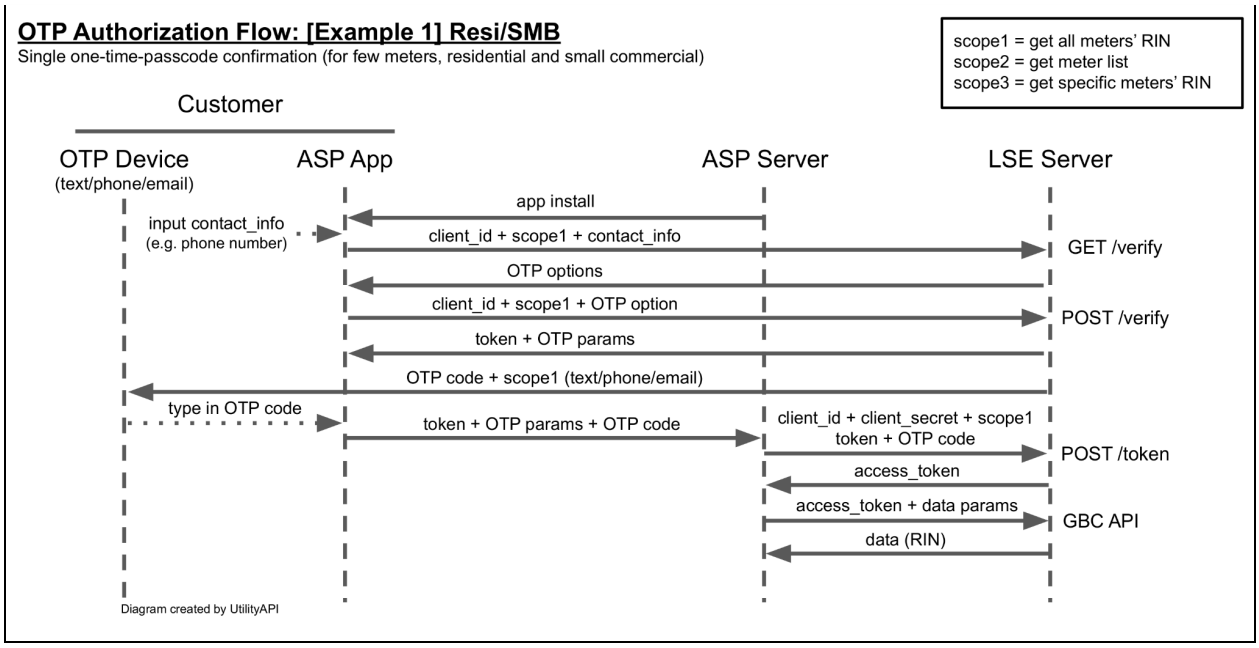
UtilityAPI again thanks the Commission for the opportunity to provide comments, enthusiastically supports the development of an RIN Access Tool and MIDAS database and API, and hopes that staff and the Commission find the above descriptions of possible streamlined customer authorization experiences helpful.

Respectfully submitted,

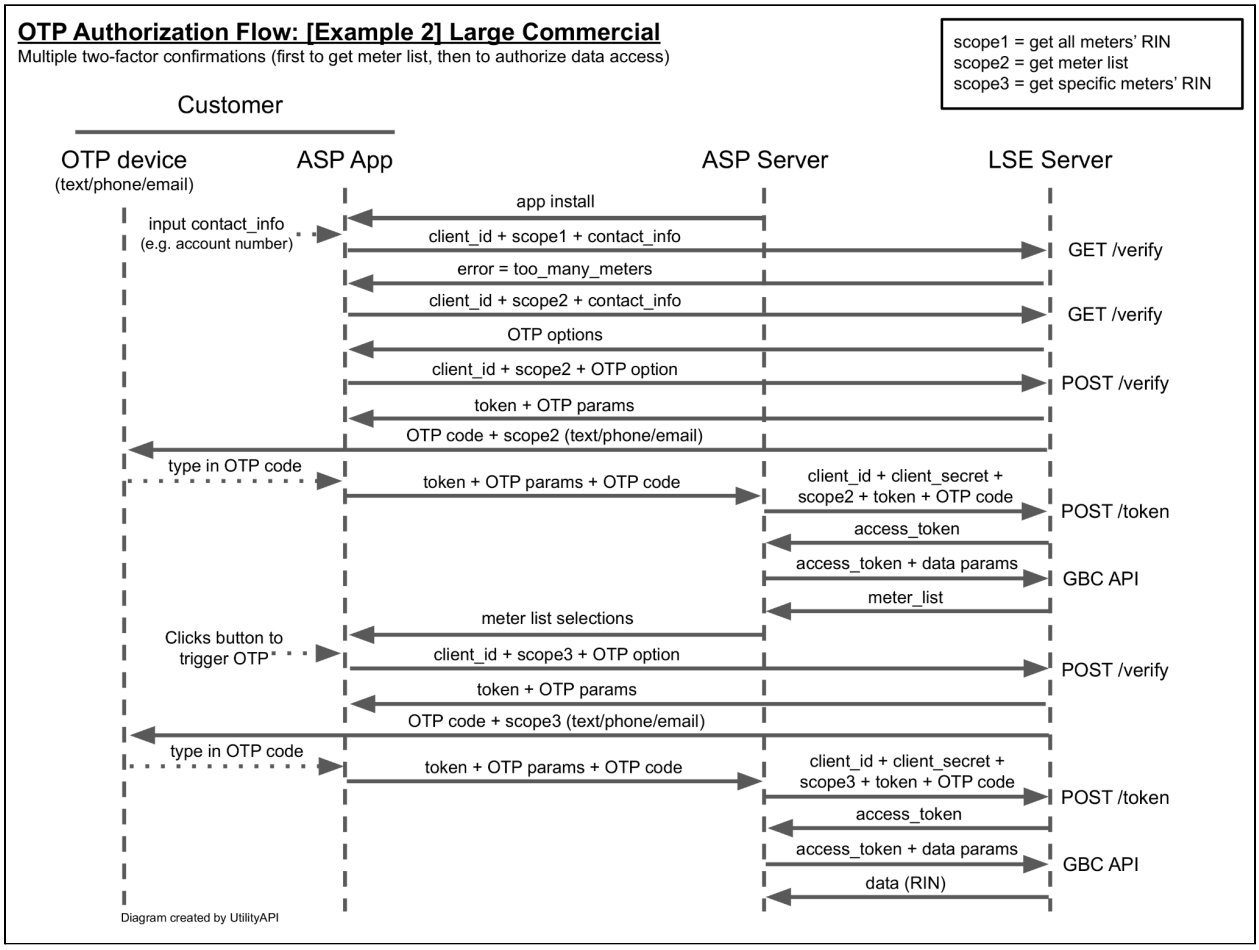
_____/s/_____
Daniel Roesler
Chief Technology Officer and Founder
UtilityAPI, Inc.
1212 Broadway, 16th Floor
Oakland, CA 94612
Tel: (510) 907-0009
Email: daniel@utilityapi.com

Appendix A. OTP Authorization Flow Diagrams

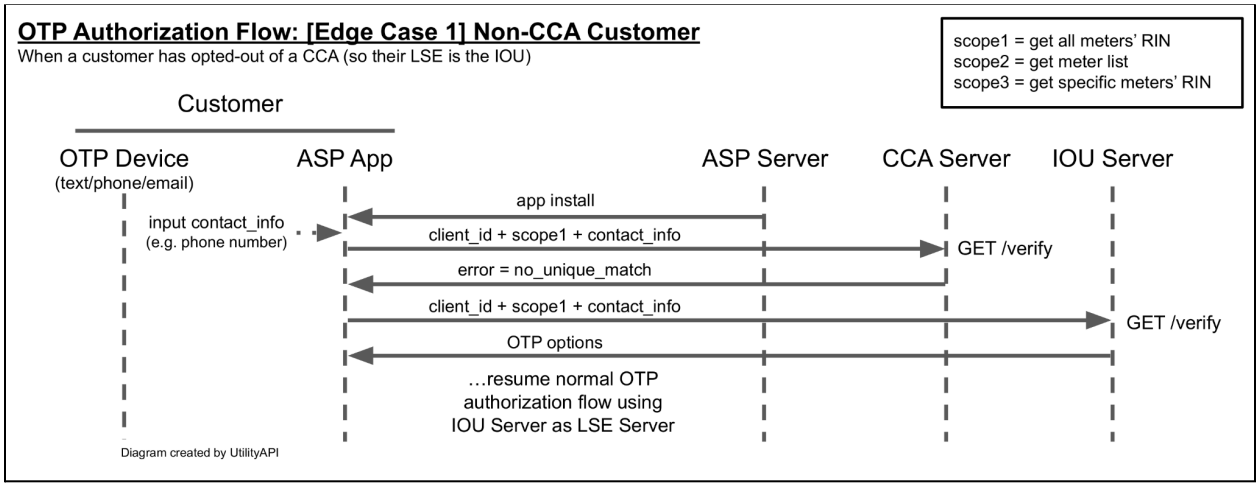
Below are technical handshake diagrams illustrating how an OTP Authorization system can work in various scenarios.



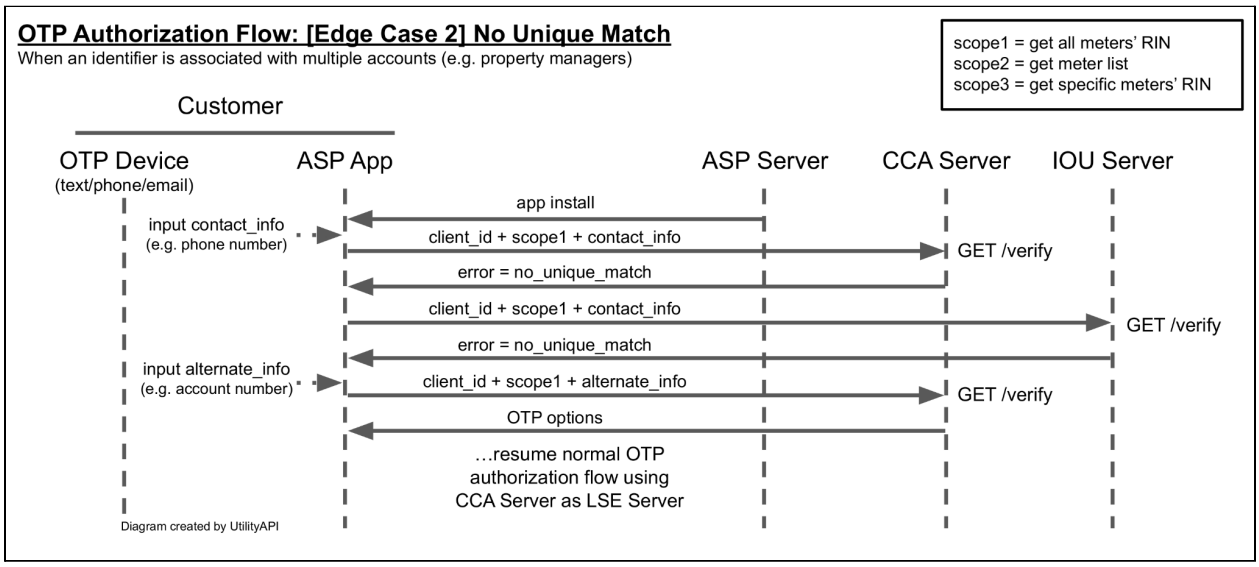
Example 1: Typical authorization flow for residential and small commercial customers with only a few services.



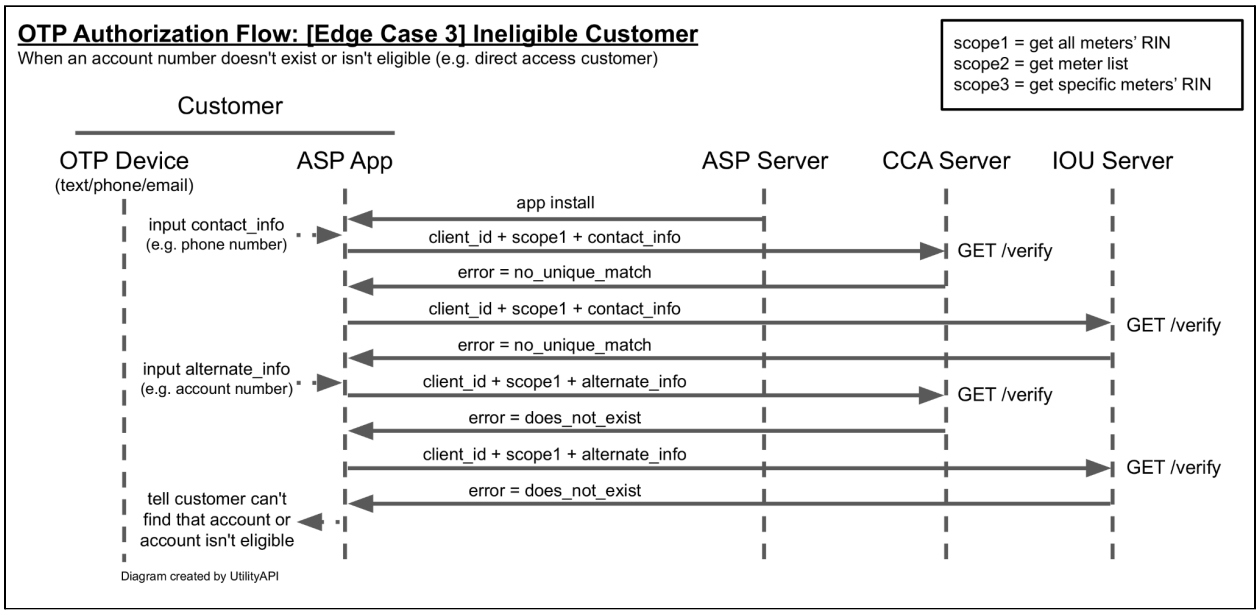
Example 2: Authorization flow for large commercial customers that have many services and need to authorize access for only a few of them.



Edge Case 1: Initial authorization flow for a residential customer who has opt-ed out of a CCA, but should still be able to share RIN access via the IOU.



Edge Case 2: Authorization flow showing how apps can fallback to asking for the account number in situations where the initial provided information (e.g. phone number or email) is not unique, which is common for multi-account customers such as property managers.



Edge Case 3: Authorization flow showing the error experience for a customer who either doesn't have a correct account number or the account number is not eligible for RIN access (e.g. they are a direct access customer).