**BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA**

Application of Pacific Gas and Electric Company for Recovery of Costs to Implement Electric Rule 24 Direct Participation Demand Response (U 39 E)	Application No. 14-06-001 (Filed June 2, 2014
And Related Matters	Application No. 14-06-002 Application No. 14-06-003

STATUS REPORT ORDERED BY THE ASSIGNED COMMISSIONER'S OFFICE DURING DISCUSSIONS AT THE OCTOBER 5, 2016 CLICK-THROUGH WORKSHOP

SHIRLEY A. WOO
DARREN P. ROACH

Pacific Gas and Electric Company
77 Beale Street, B30A
San Francisco, CA 94105
Telephone: (415) 973-2248
Facsimile: (415) 973-5520
E-Mail: SAW0@pge.com

Attorneys for
PACIFIC GAS AND ELECTRIC COMPANY

Dated: October 12, 2016

**BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA**

Application of Pacific Gas and Electric Company for Recovery of Costs to Implement Electric Rule 24 Direct Participation Demand Response (U 39 E)	Application No. 14-06-001 (Filed June 2, 2014
And Related Matters	Application No. 14-06-002 Application No. 14-06-003

STATUS REPORT ORDERED BY THE ASSIGNED COMMISSIONER'S OFFICE DURING DISCUSSIONS AT THE OCTOBER 5, 2016 CLICK-THROUGH WORKSHOP

Pursuant to the verbal instructions from the Assigned Commissioner's office at the click-through workshop for the customer authentication and authorization process for Electric Rules 24 and 32[1/] noticed in the Commission's calendar and held October 5, 2016, Pacific Gas and Electric Company, on behalf of the workshop participants who have contributed to the status report, is serving a status report on Solutions 1 and 3, which were discussed at the workshop.[2/] The status report will be served on parties to R.13-09-011 as well as A.14-06-001, et seq.

Workshop participants who have contributed to the status report include EnergyHub, Inc., Mission:data Coalition, Inc., OhmConnect, Inc., Olivine, Inc., Chai Energy, Inc., San Diego Gas & Electric Company, Southern California Edison Company, and Pacific Gas and Electric Company. While this report provides a consolidated description of the informal status of the click-through working group, it does not in any way indicate that the two sets of parties (the utilities and the DRPs) agree with the views expressed by the other group of parties, or have formed a consensus regarding Solution 1 versus Solution 3.

[1/] Rule 32 is San Diego Gas & Electric's rule number. Rule 24 is the number for Southern California Edison and PG&E.

[2/] The status report was due October 11, 2016. However, Energy Division staff granted a 1-day extension.

The status report follows the template which Energy Division staff provided at the workshop. The status report accompanies this notice. It may also be accessed electronically by following the instructions below:

1) Go to: https://pgera.azurewebsites.net/Regulation/search
2) Click on "Search for Public Case Documents"
3) Select "Demand Response OIR 2013 [R.13-09-011]" or "Demand Response Rule 24 Cost Recovery [A.14-06-001] from the dropdown menu
4) Select 10/12/2016 and PG&E as the party to narrow the search criteria
5) Click Search

Respectfully Submitted,

SHIRLEY A. WOO
DARREN P. ROACH

By: /s/ *Shirley A. Woo*
SHIRLEY A. WOO

Pacific Gas and Electric Company
77 Beale Street
San Francisco, CA 94105
Telephone: (415) 973-2248
Facsimile: (415) 973-5520
E-Mail: SAW0@pge.com

Attorney for
PACIFIC GAS AND ELECTRIC COMPANY

Dated: October 12, 2016

Streamlining and Simplification of Direct Participation Enrollment Process (Click-Through) Working Group Informal Status Report (Consolidated Comments from Utilities & DRPs/Interested Parties)

1. Description of Solutions 1 and 3

The demand response parties (DRPs), with the support of interested parties, proposed three solutions that meet their needs, based on the guiding principles the DRPs proposed. The working group has already ruled out the second solution, and what has been named API Solution 1 (Solution 1) and OAuth Solution 3 (Solution 3) remain as potential solutions that could be implemented together or alone. Both options stand on the foundational grounding that the utilities have the responsibility to authenticate the customer to ensure compliance with the Commission's privacy rules.

The following two options support utility authentication but vary in terms of customer experience, technical requirements, implementation time, and ratepayer cost:

Solution 1: The customer would begin on the third party DRP site, and provide specific customer information via a browser that is sent directly to the utility. The information would be authenticated by the utility's back-end systems. Once authenticated, the customer would authorize release of data on the DRP site and the parameters would be sent to the utility to complete the process. The authentication and authorization steps could, at the option of the DRP, be completed on a single screen. The customer does not leave the DRP website during this process; however, this solution requires the utilities to build one, or possibly two, custom API endpoints to authenticate the customer's identity and authorization of data release to the DRPs.

Solution 3: The customer would begin on the third party DRP site, but then be directed to log into the utility site, where existing utility privacy controls exist to authenticate the customer. Once authentication is completed, the customer authorizes the release of their data and is redirected back to the DRP site to complete the process. While the process starts and ends on the DRP's website, the customer provides their authentication and authorization information directly on the utility website, utilizing enhancements to simplify and streamline an existing Green Button Connect (GBC) system[1], which is an international, industry standards-based solution.

While this report provides a consolidated description of the informal status of the click-through working group, it does not in any way indicate that the two sets of parties (the utilities and the DRPs) agree with the views expressed by the other group of parties, or have formed a consensus regarding Solution 1 versus Solution 3.

2. Introduction

a. Utility Introduction:

Below are the pros and cons for each option as identified by the utilities and the DRPs. This assessment attempts to consider different aspects of each option ranging from (but not limited to) ensuring that a solution is secure, customer friendly, and supports privacy rules.

[1] SDG&E may use a different industry standards-based system outside of GBC.

The utilities are not able, at this time, to provide cost estimates for either option. The estimation process will require clear business requirements which have not yet been obtained as part of the workshop process.

In addition, the utilities clarify that these solutions are provided in the context of Rule 24 (for SCE and PG&E) and Rule 32 (for SDG&E), which establishes the terms, conditions, and procedures for third parties to obtain retail customer information for direct participation in the CAISO wholesale market and to register retail customers in the CAISO demand response system and in DR resources. Although the utilities view Demand Response (DR) and Rule 24/32 as a platform to help transform a multitude of distributed energy resource (DER) end-use technologies, for e.g. energy storage, into grid-responsive loads that serve the evolving needs of the grid, going beyond the scope of the click through workshops with the time available would not be fruitful. Work for other DER initiatives that the Commission is addressing is not being coordinated with the staff resources involved in Rule 24/32 and will require a lot of consultation with participants in the IDER/DER processes, (as an example), to understand what is occurring with other aspects on the DER side, and identify similarities and differences.

Please note that the utilities have not been provided the opportunity to review and discuss the DRP appendices E, F, G and H, and first saw them when they were sent after close of business on October 11, 2016, and have not been able to address them in the status report.

b. DRP Introduction:

Through the workshops, the parties have made progress to reach broad agreement on the following areas:

- Authentication and Authorization will occur in real-time, instantaneously
- The IOUs will authenticate in any scenario and will offer multiple types of credentials (e.g. login credentials and/or zip-code+AcctID).
- Certain improvements to streamline the user experience of an OAuth solution, such as decreasing the number of required screens
- DRPs will be involved prior to any IOU changes to the authentication/authorization screens
- More collaborative work is needed to arrive at sufficiently detailed technical specifications of both Solutions 1 and 3
- There are myriad finer points where there is also progress – for example, efforts are being made to streamline an electronic DRP form and to agree upon a full data set

Please note that the DRPs have not been provided the opportunity to review and discuss the Utility's appendix A, and first saw it when they were sent after close of business on October 7, 2016, and have not been able to address them in the status report.

3. Price and Implementation of Solution 1

Utility Pros	Utility Cons
• Customer Experience: The customer is never redirected to another site during the process.	• Authentication and Authorization: Customer provides confidential authentication information on the third party's website,

• Testing: Requires isolated testing between the utility and the DRP if the DRP makes a change to its forms.	requiring the customer and the utility to trust that the third party's implementation of this solution does not transmit or store this information on third party servers. The customer does not really know who they are authenticating with, or that the utility is supporting this process. In addition, changes to utility authentication and authorization standards must be accommodated by each third party DRP's systems, and supporting each of these mechanisms for each DRP is very difficult and costly for ongoing utility operations and maintenance. • User Experience: Additional use cases around revocation and authorizing multiple service agreements are yet to be defined. For example, if a large commercial customer would need to list each service agreement that they'd like to select for data release, then this process could be more intensive than the check boxes that a utility website could present. • Security: Depending on how login mechanism is implemented by the DRP, the DRP may have visibility to the customer credentials being passed to the utility authentication web service. If the DRP builds the login, they can build it without assuring the utilities of the proper security, and these concerns cannot be mitigated with any guarantees. • Time and Cost: Implementation time and cost are highly variable as the utilities would need to develop new functionality across all steps of this process, including needing to design developer resources such as documentation, code and open secure API endpoints into its systems. There will be additional costs for training front-line operation employees to support customer and DRP calls and inquiries. The utilities can only say that Solution 1 would take longer and cost more than Solution 3. • This option does not accommodate a

	password reset.
DRP Pros	**DRP Cons**
• Allows ongoing innovation by DRPs in customer experience without having to seek approval of IOUs • Allows a shorter customer experience that can be accomplished in 1-2 screens, rather than 3-4 screens • Allows for alternative credentials to be provided (such as SAID+zip) rather than online utility account credentials • Allows for easy mobile device support as these technologies rapidly change over time • Solution 1 is consistent with Ordering Paragraph 8 of D.16.06-008	• Would require significant IT functions to be built and supported by both the IOUs and DRPs • May delay the availability of solutions for DRAM 2018 • May result in additional costs • May not produce a significantly improved customer experience for C&I relative to Solution 3

a. Utility Rationale:

Overall: The utilities strongly state that the "cons" on this option are overwhelming and Solution 1 should be disqualified as a result. If the DRP builds the login, they can build it without assuring the utilities of the proper security. The utilities prefer to build the login pages for this process to ensure that a customer's authentication and authorization meet the Commission's privacy rules. In addition, there remains a great deal of uncertainty around how this solution would be implemented. As a result, there remain many outstanding questions that may ultimately result in deal-breakers for the utilities.

Time and Cost: Solution 1 requires brand new functionality for the following steps of the click-through process: DRP registration, issuance of registration keys and secrets, customer authentication, customer authorization, DRP API data requests, and ongoing operations and maintenance. The utilities would need to provide what it considers extensive developer resources, for example, but not limited to, documentation and reference code to DRPs as part of this option, which is not functionality the utilities have experience or expertise in. As a result, the utilities are concerned that the initial IT project implementation and on-going support and maintenance needs are significant, particularly to support security-related concerns. While a specific time estimate is not available at this time, the utilities do not believe this option could be completed in time to support the 2018 DRAM.

Security: API Solution 1 has little implementation description and this inherent lack of detail significantly limits the utilities' ability to assess the full scope of cybersecurity risks that utilities, DRPs and customers are exposed to. (One such example is phishing attacks, whereby customers get accustomed to entering Personally Identifiable Information (PII) at third party sites where no mechanism exists to verify or validate trust of those sites.)

Generally speaking, the following aspects of Solution 1 are currently not well defined:

- Validity: Customers need the ability to verify which third party sites are actual valid DRPs (as opposed to malicious websites)

- Security: Customers, utilities and third parties need the ability to verify that Solution 1 has been fully implemented as per security requirements (e.g. third parties may inadvertently or intentionally misconfigure their implementation of the solution which compromises the security of information transmission to utilities)
- Evolving Security Threats: Utilities and third parties must be made aware of and adapt the solution to quickly address vulnerabilities and threats that are identified by the cybersecurity community.

It is therefore the opinion of the utilities that an accurate or plausible assessment of cybersecurity threat for this design pattern is not possible due to lack of detail.

b. Third Party Rationale:

Overall: While the IOUs have asked that only a single solution, Solution 3, be implemented, it would be short-sighted to do so at this juncture for the reasons described below.

- **Solution 1 enables ongoing innovation by DRPs that will reduce enrollment fatigue and increase participation in demand response.** By defining a clear interface or API between DRPs and utilities in which the entire customer experience resides on the DRP's website or mobile app, DRPs are empowered to rapidly iterate their product features to improve enrollment rates as technology changes. Solution 1 lets innovation occur by third parties, who have the capability and the incentive to improve the customer experience. In contrast, Solution 3 requires a fixed handoff to webpages controlled by the utility that cannot be improved quickly. User experience improvements in Solution 3 involve an opaque, time-consuming and costly negotiation with IOUs and other stakeholders, whereas Solution 1 puts DRPs in the driver's seat to speed up the product development cycle at their own pace as technologies change over time. User experience improvements under Solution 3 require more working groups, time-consuming deliberation and possibly formal Commission action in order to implement minor changes, whereas Solution 1 gives DRPs end-to-end control over the user experience without having to consult the IOUs or the Commission with each product iteration.
- **Solution 1 is "future-proof" to accommodate mobile devices, increasingly used by consumers, whereas Solution 3 is designed primarily for web browsers on desktop computers.** Mobile internet usage is growing 58% year over year, with smart phones and tablets proliferating.[2] Mobile apps are rivaling the web as the primary mechanism for consumers to access different services. Solution 1 allows native apps on smart phones to develop and mature in the easiest possible manner with minimum IOU effort. In contrast, Solution 3 is geared toward interaction with a web browser. Mobile devices have web browsers, but Solution 3 penalizes native apps because of the clumsy and error-prone hand-off between a DRP's mobile app and the utility's webpage that is required in the Oauth process. An app experience in which the customer never leaves the app is supported by Solution 1 and not Solution 3.[3] Implementing only Solution 3 could

[2] http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/

[3] Not to mention the fact that consumers rarely remember their utility logins and passwords, making mobile web usage difficult for most consumers.

explicitly penalize native apps and limit customer enrollment in demand response with a *de facto* policy that does not address internet mega-trends toward mobile device support.

- **Solution 1 supports Southern California Edison's efforts to "not require its customers to use the SCE Green Button Connect approach to enroll" and to streamline and automate the enrollment process.** Given the challenges with manual forms -- asking customers for more information than they conveniently have on hand, the lack of instant feedback when a form is filled out incorrectly and associated processing delays -- Solution 1 is well-suited to processing the large number of forms on the horizon.

Several DRPs wish to use Solution 1 exclusively and strongly prefer it over Solution 3, but there are no parties who favor Solution 1 to the *exclusion* of Solution 3. This comes from the recognition that Solution 3 is useful for several use cases and Solution 3 is useful to several DRPs that want to support Oauth.

Both solutions include significant technical overlap as further described below. While we acknowledge that OAuth standards are more familiar to the IOUs, Solution 1 is commonly found today with online credit card processors. We recommend that the IOUs be supported and directed to collaborate with the DRPs and possibly seek outside consulting assistance to implement those areas of Solution 1 with which the IOUs may be unfamiliar.

The IOUs have argued that Solution 1 is insecure because login credentials could be intercepted by a DRP. Before the utility or the Commission jump to conclusions, Solution 1 needs to be scoped out in technical detail. Importantly, we note that Solution 1 does not have to require login credentials – it could use only the SAID/zip code combination, eliminating any real or perceived security concerns of DRPs intercepting credentials. More work is needed before any conclusion can be drawn on this security concern.

The IOUs have also argued that Oauth is an established standard, whereas Solution 1 is not. That assertion mischaracterizes Solution 1 because credit card processing on the internet today uses a very similar architecture as Solution 1. Solution 1 must be tailored to utilities' authentication parameters, but tailoring Solution 1 to utility operations does not disqualify it on the grounds of security concerns.

4. Price and Implementation of Solution 3

Utility Pros	Utility Cons
• Customer Experience: The customer provides their confidential information clearly on the utility website and is confident that they are authenticating and authorizing with the utility and no other entity, which builds trust. This solution supports mobile device use currently and the utilities are open to discussing enhancements. • Authentication and Authorization: Implementation is based on a single, consistent, reusable mechanism which is implemented, understood, and fully	• Customer Experience: The customer is directed between the DRP website and the utility website. This can cause confusion for the customer and/or customer drop off. • Testing: If the utility makes a change to the authentication and authorization forms and/or web service, it requires testing across all DRP platforms.

supported by the utilities. The utilities can enhance GBC to provide multiple mechanisms to authenticate for customers without a username and password (e.g., commercial). If authentication protocols change based on industry standards, the utilities could adopt those standards and test changes with DRPs. Customers understand the OAuth concept as a common way to share data (e.g. share your data by using your Facebook login). • Time and Cost: Utilities are leveraging existing functionality, at reduced cost and with shorter implementation time. Implementation would only require enhancements to existing processes to accommodate the needs of the DRPs. The solution is also scalable for Rule 24 and other implementations with low time-to-market. Since the existing functionality will be leveraged, training time and cost for operations in preparation for this solution will be relatively lower compared to Solution 1. • Security: Utilities can manage the cybersecurity and privacy concerns effectively because authorization and authentication occurs directly on its website and servers, which can evolve to manage emerging threats, vulnerabilities, and privacy concerns in a centrally managed and consistent manner. • Standards: OAuth utilizes industry standard solutions that align with the Green Button Alliance.	
DRP Pros	**DRP Cons**
• Reduces IT costs and workload for DRPs who already support OAUTH • Timing to implement the solution is important to be ready for the 2018 DRAM • Customers familiar with OAUTH from their use of Facebook/Twitter/etc. are unlikely to	• Customer experience can be disjointed when a utility website popout appears • DRPs have no control over the user experience • Improvements to the user experience over time involve significant resource

have problems • Redirecting C&I customers to a utility website will not likely result in significant loss of enrollment • IOUs are already familiar with OAUTH	commitments of time to work with utilities • Mobile devices – increasingly a large percentage of internet traffic – may have difficulties because of the native app to browser handoff

a. Utility Rationale:

Overall: The utilities strongly support this option as being superior and offers advantages in the most important areas: lower costs, standardization, less work and expense later on, and, most importantly, the ability to protect customers' privacy and security. This option leverages an industry standard and utilizes existing utility expertise and resources in a manner that is an efficient use of ratepayer funds, maintains a high level of security and privacy that aligns with Commission standards, reduces utility liabilities, and offers fewer uncertainties in the implementation process and operationally thereafter.

The utilities have also committed to enhancing the GBC process, by reducing the number of pages and clicks, performance assurances, and supporting two-party authorizations. In addition, the customer experience for GBC is continually being enhanced and there are existing stakeholder processes that support third party involvement. The DRPs also mentioned mobile support, which is currently available through GBC and the utilities are open to discussing enhancements.

Time and Cost: Solution 3 would comprise only of enhancements to existing functionality for authentication and authorization such as possibly providing for alternative authentication mechanisms (besides username/password) and ensuring customer authorization pages are consolidated to as few pages as possible. Internal IT project implementation and on-going support and maintenance needs are much better understood, particularly as it affects security concerns.

California ratepayers have invested millions in the IOUs building a standards-based customer data sharing platform in GBC. This standardized platform should be enhanced to support new use cases, arguably to the benefit of all third party data recipients, DRP and non-DRP alike, as opposed to utilities developing a new solution for each use case.

Authentication and Authorization: The utilities have committed to developing authentication methods for customers without a utility login to allow customers without a username and password, or are part of a large organization where it is difficult to track down the login, to use Solution 3. SDG&E has an existing Single Sign On (SSO) implementation which can be extended to enable authentication mechanisms as part of this option. So for SDG&E this would mean an additional "pro." SDG&E also has an existing OAuth implementation which can be extended to enable authorization mechanisms as part of this option. SCE and PG&E are considering implementing SSO, but may differ in specific implementation.

Security: Solution 3 leverages existing data delivery infrastructure built for GBC, of which DRPs today are already registered partners.[4] It is a design pattern proposed by the utilities to fulfill the

[4] Green Button Connect (GBC) standard was proposed and promoted as a national standard by the former White House Chief Technology Officer as well as NIST, NAESB, and other bodies.

use case understanding shared by the participants of this working group. It is a feature extension, and therefore a derivative work that leverages an existing and deployed system created to enable data release while protecting Personally Identifiable Information (PII) according to CPUC Decision 11-7-056. This proposal is a revision of GBC service already available from the utilities, but with features designed specifically to address the DRP's use cases.

It is important to emphasize that cybersecurity threat analysis of GBC has been performed by NIST (National Institute of Standards and Technologies) as part of Green Button Alliance work. As such, GBC and its implementation at the utilities conforms with NIST' Framework and Roadmap for Smart Grid Interoperability, Release 3.0 (NIST 1108r3, National Institute of Standards and Technology) and compatible with the listed smart grid specifications of NAESB (North American Energy Standards Board) REQ-21, as well as security requirements within IETF (Internet Engineering Task Force) RFC 6272, "Internet Protocols for the Smart Grid", where OAuth2.0 is referenced as an acceptable method for application layer authorization mechanism.

Therefore, the utilities deem the cybersecurity threats of Solution 3 to be similar in scope and content as GBC, and thus well known. Based on GBC details accumulated through its enterprise software architectural planning, design, build, test, review, and release, the utilities are confident that Solution 3 security aspects are manageable. Furthermore, ongoing monitoring of threats will be able to leverage the larger GBC community effort as it identifies, shares, and addresses any concerns.

b. Third Party Rationale:

<u>Overall:</u> Through this process, some DRPs have become satisfied that Solution 3 will be modified to result in an improved customer experience. Solution 3 will utilize an existing framework already employed by the IOUs to accomplish that end, has it the ability to be available in a timely manner for 2018 DRAM enrollment at a minimum of additional costs to ratepayers. For C&I customers, for whom redirection to utility webpages is unlikely to increase dissatisfaction with the enrollment process, Solution 3 will reduce additional IT build out relative to Solution 1.

There was near unanimous concern about SCE's GBC experience for the purpose of enrollment in the 2016 DRAM because of the complexity of the process, including the number of screens and clicks required in order to register one account, especially for the DRPs serving residential and small commercial customers. The GBC enrollment/ authorization process resulted in the providers of services to small customers losing a significant number of potential customers, as much as 50%. DRPs for all customers found this enrollment process unworkable as a long-term solution for DRAM. As such, the Commission found that SCE could not compel customers to use its platform as the sole venue for registering customers and for obtaining customer authorization to release data.

However, the IOUs have presented a much more streamlined option for Solution 3 to minimize the complexity, the number of pages and the number of clicks, such that Solution 1 and 3 are nearly the same with one important distinction. Solution 1 maintains the entire customer experience on the DRP website and Solution 3 redirects the customer to the IOU website to provide its authentication credentials and to provide the authorization.

If the solutions are largely similar with one main distinction, redirect or not, some DRPs do not feel that the redirection of its customers to the IOU website poses a difficulty for the customer to navigate nor will it create a negative customer experience. In addition, maintaining the customer experience solely to the DRP's website requires the DRP to create that portion of the customer experience which the IOU can already provide. It is duplicative for the DRP to create this effort and increases the costs for the DRP to do so. In other words, some DRPs do not believe that our customer experience or enrollment will be negatively affected by redirection to such an extent to offset the additional cost and buildout to accommodate Solution 1.

In addition, there is a concern about timing. DRPs would like to have Solution 3 available for DRAM 2018 enrollment. There is a concern that Solution 1 will require additional cost and programming time that could extend the availability of Solution 3 by the desired timeframe.

As such, certain DRPs would prefer to modify Solution 3 in the manner described herein to streamline and simplify the customer experience as opposed to creating an alternative Solution 1. However, in the interest of DRP unity, the supporters of Solution 3 will support a simultaneous advancement of both solutions in parallel, to the extent that such a process can be accomplished at a reasonable cost level and will not delay the availability of Solution 3 for 2018 DRAM enrollment.

In any event, the following elements of Solution 3 should be included for the DRPs to fully support it:

- Solution 3 must offer an alternative to utility account login credentials. According to the latest statistics published by the IOUs, over half of California ratepayers do not have an online utility account, or, if they do, it has not been accessed for at least 12 months. That means over 50% of potential demand response participants in California could be inconvenienced by the requirement to create an online utility account. The IOUs might require that customers create an online utility account prior to enrollment. No one has the statistics of the "drop-out rate" resulting from the requirement to create an online account, but if EnergyHub's recent statistics are any indication, there is an order-of-magnitude decrease in enrollment rates when the process is complex (40% with a simple process versus 3% with a complex one).[5]

Utility	*Percent of customers who have accessed their online account in the past year* [6]	*Percent of customers who have not*
PG&E	44.0%	56.0%
SCE	48.0%	52.0%
SDG&E	49.4%	50.6%

[5] "Optimizing the demand response program enrollment process." White paper by EnergyHub, Inc. dated April, 2016. Available at http://www.energyhub.com/blog/optimizing-demand-response-enrollment

[6] See the IOUs' smart grid annual reports, Metric #9, October, 2015.

It is possible that the IOUs will develop Solution 3 such that customers can enter a Service Agreement ID (SAID) and zip code to authenticate, as an alternative to login credentials. The DRPs, Mission:data and UtilityAPI supports this optionality because it may be easier for customers that do not have a preexisting utility account. At this time, the IOUs have stated they "would consider" using the SAID/zip code combination in lieu of login credentials, but the IOUs have not yet committed to do so. In any event, the SAID/zip code combination in Solution 3 would not diminish the value of Solution 1 in streamlining the enrollment process and enabling future innovation.

- **Solution 3's authentication process must not require anything of the customer above and beyond what is needed to authenticate at a utility's website directly.** For example, PG&E requires Service Agreement ID and zip code to authenticate customers for account creation. Those same authentication credentials, and nothing more, should be required of DRPs in Solution 3.
- **Solution 3 must incorporate ongoing feedback from the DRPs.** To address the fact that the customer experience in Solution 3 is controlled by the IOUs, the IOUs must be required to consult the DRPs prior to making any changes. DRPs shall have the ability to comment on and/or protest proposed user experience changes. Whenever a redesign or change is contemplated by the utility, the utility shall incorporate usability studies and customer feedback into any proposal. The DRPs should be involved early into any IOU redesign processes so that feedback can be meaningfully incorporated.
- **Solution 3 must incorporate the technical details described in Appendix E to fully achieve a streamlined authorization process.**

5. Price and Implementation of Both Solutions

Utility Pros	Utility Cons
• Customer experience can be tailored to the DRP's preferences.	• Time and Cost: Preparing estimates necessary for filing the advice letter and implementation would take significantly longer. Both options would have to be evaluated in sequence and implemented in sequence – with Solution 3 likely taking place first. • Redundancy: The two options offer very similar functionality and serve a basic purpose of what is likely to be a one-time interaction to authenticate and authorize a customer for a demand response program.

DRP Pros	**DRP Cons**
• Supports the broad array of DRPs whose customer experiences are different, particularly on mobile devices • Supports an authentication pathway that does not involve creating a utility account, removing an obstacle to enrollment • Leverages many parts of existing GBC infrastructure, on both the IOUs' and DRPs' systems • Allows creativity and innovation with regard to user experience over time	• More expensive to implement • May delay implementation for 2018 DRAM

a. Utility Rationale:

Overall: The utilities strongly object to implementing both options. Not only is implementing two similar solutions redundant, but it is an inefficient use of ratepayer funds. All three utilities caution that due to resource limitations, implementation of two solutions could not be undertaken concurrently, and could only be undertaken sequentially given resource constraints. While estimates of overlapping effort cannot be assessed due to the many open questions around requirements for Solution 1, the utilities do not believe there is much overlap in terms of its implementation of the two solutions. Furthermore, the utilities do not expect that these solutions could be implemented in time to support the 2018 DRAM.

b. Third Party Rationale:

Overall: The vast majority of DRPs -- including EnerNOC, Chai Energy, EnergyHub, and Olivine – as well as Mission:data and UtilityAPI believe both API Solution 1 and OAuth Solution 3 should be implemented together, provided that it is done in a cost-effective and timely manner *in time to support the 2018 DRAM*. The group would prefer to find a way to work with the utilities to ensure that both API Solution 1 and OAuth Solution 3 could be implemented in parallel on a cost-effective and timely manner in time to support the 2018 DRAM. If it is possible to proceed down a path where both solutions can be implemented in parallel, then that would be the preference of the group. If that is not possible, then parties will have individual preferences as between Solution 1 or Solution 3.

From a technical perspective, we believe the two solutions are in large part compatible with one another and there is significant technical overlap. We currently estimate that the overlapping effort of the two solutions is approximately 50 – 90% - and likely closer to 90%. Please see the attached Appendix G for more detail.

Solution Set Comparison

	Solution 1: API	Solution 3: Streamlined OAuth
Number of pages/screens	1-2	3-5
Third Party directs flow and	Yes	Somewhat; subject to IOU

authorization screen presentation		approval and implementation
Potential to streamline UX over time	Yes	Somewhat; subject to IOU approval and implementation
Can accommodate synchronous and asynchronous requests	Yes	Yes
Can facilitate out-of-band requests	Yes	Yes
Optimized for mobile devices	Yes	No

6. Additional Scope, Schedule, and Budget

The following topics are also being discussed in the working group sessions in San Francisco and in separate, weekly, sub-group conference call meetings:

- CISR-DRP form simplification and processing
- Data exchange and format: review of existing data elements provided under Rule 24/32

7. Conclusion

a. Utility Conclusion:

The utilities support the sharing of data through the click-through process that allows convenience and a positive customer experience, and a secure manner in which key privacy priorities are observed. The utilities strongly support Solution 3. It is secure, follows an industry standard based solution, it should be faster and less costly to deploy, and the IOUs are willing to work on the customer experience concerns presented by the DRPs in this solution.

The process should also provide the data necessary to register customers at the CAISO and provide accurate settlement for payment under Rule 24 (for PG&E and SCE) and Rule 32 (for SDG&E). The larger questions of sharing utility proprietary customer or utility data, beyond what is merely necessary for CAISO registration and DR settlement, are further discussion issues and deserve to be addressed fully in a larger discussion broader than the click-through process of Rule 24/32 implementation. Those issues deserve greater, deeper consideration of the implications for all involved, including to what degree further data should be provided, the costs of providing that data and what parties pay for it.

More time is needed to address some of the concerns that still linger with all the options, and in order to see if any or all of the “cons” for each option could be mitigated in some way.

b. Third Party Conclusion:

The DRPs would prefer to find a way to work with the utilities to ensure that both API Solution 1 and OAuth Solution 3 could be implemented in parallel on a cost-effective and timely manner in time to support the 2018 DRAM. Both solutions are useful in their own way, and both reach customers “where they are” – on mobile devices, or on desktop computers with or without having to have an online utility account.

Noting that, DRPs prioritize the solutions differently and therefore have taken slightly different positions:

- Olivine[7], Chai Energy, EnerNOC, CPower, and Stem support the development of Solution 1 and 3 with an emphasis on there being a streamlined solution in time to support the 2018 DRAM in fall 2017. Our support of both solutions is conditional on the following:
    - Support for Solution 1 is on the basis that it allows alternative authentication credentials only and does not allow username and password.
    - If the development of the two solutions in parallel significantly impacts the implementation timeline for Solution 3, then Solution 3 is given priority and developed first.
    - Solution 3 must abide by commitments to be made by the IOUs to streamline number of pages and clicks, to establish look and feel and performance metrics as requirements for its implementation – see examples in Appendix E -- as well as an ongoing joint design group and process that survives the initial implementation.
    - In addition it must support alternative credentials beyond username and password.
    - The development of each solution should be in a cost-effective and timely manner.
    - Note that these parties agree that Solution 1 can be "added on" to Solution 3 and need not be an independent effort.

EnergyHub and WeatherBug support Solution 1 alone, unless Solution 1 and 3 are developed in parallel and in a timely manner to support the 2018 DRAM, in order to meet the needs of mass-market implementation, especially among residential customers. The chosen Solution has a significant impact on enrollments, and thus performance, in any third party demand response program (as shown by EnergyHub's white paper, "Optimizing the demand response program enrollment process'). As such, the DRP should be enabled, but not required, to design its own solution end to end if it so desires.

OhmConnect supports Solution 3 alone, unless Solution 1 can include a login mechanism that will securely pass customer credentials. If these security concerns are resolved, then OhmConnect supports Solution 1 and 3 in parallel so long as the Solutions can be developed in a cost-effective and timely manner in time to both support the 2018 DRAM. OhmConnect stresses that the click-through process must include at least one solution that allows customer authentication using existing utility log-in credentials (i.e. user name and password), to meet the needs of mass-market implementation, especially among residential customers.

Finally, supporting either or both solutions requires implementation of a full dataset. The DRPs request that a full dataset be made available synchronously to meet market needs. We recognize

[7] Olivine is a DRP and represents 8 of the 9 2016 DRAM winners both in the wholesale market and in the Distributed Energy Resource (DER) Coalition. It was Olivine's hope to get a single consensus from DER Coalition members for inclusion in this report and in support of the overall workshop goals; however, there is not a consensus position at this time. As such, Olivine's position stated does not represent the position of the DER Coalition.

that achieving synchronous data may require a transition over some period of time; we believe the IOUs should work with DRPs and others to provide necessary data points through an interim solution until such time as the full dataset is made available synchronously through a new platform.

We note that the DRPs, Mission:data and UtilityAPI all support the Appendices attached hereto.

8. Appendices

a. Utility Appendices:

Appendix A: Description of Click-Through Solutions[8]

Appendix B: Proposed Solutions for Click-through Implementation

Appendix C: Solution 1 Customer Journey PGE

Appendix D: Solution 3 Customer Journey PGE

b. DRP Appendices:[9]

Appendix E: DRP Requirements for Solution 3

Appendix F: Example of user experience using Solution 1 (one screen)

Appendix G: Interaction Diagram Showing Relationships Between Solutions 1 and 3

Appendix H: Wireframe example of customer experience with and without security “badge”

[8] Please note that the DRPs have not been provided the opportunity to review and discuss the Utility’s appendix A, and first saw it when they were sent after close of business on October 7, 2016, and have not been able to address them in the status report.

[9] Please note that the utilities have not been provided the opportunity to review and discuss the DRP appendices E, F, G and H, and first saw them when they were sent after close of business on October 11, 2016, and have not been able to address them in the status report.

APPENDIX A

Streamlining and Simplification of Direct Participation Enrollment Process Informal Status Report [Description of Solution 1 and 3]

Appendix A: Description of Solution 1 and 3

High Level Overview:

Solutions 1 and 3 are alternative approaches to addressing a common need for online customer authentication and authorization for 3rd party Demand Response Providers (DRPs) to access customer data. In sequential flow, both Solutions 1 and 3 require the following functionality in order to work properly:

1. 3rd Party Registration (with the utility)
2. Utility issues a 3rd party registration key and secret
3. Customer Authentication
4. Customer Authorization (and subsequent authorization updates or revocation)
5. 3RD Party API Data Requests
6. On-going Operation and Maintenance (as needed)

Similarities in implementation of Solutions 1 and 3:

1. DRP Registration:

   3rd parties establish their identity and relationship with the utility whereby the DRP provides basic company, contact, and DRP specific info for the utility to review and verify.

2. Utility Issues a DRP registration key and secret:

   The utility issues to each registered DRP a private “key” and “secret” which uniquely identifies them, differentiating them from each other as well as from non-registered DRP. The key and secret are used by DRPs in subsequent steps for authentication and data request.

5. DRP API Data Request:

   Registered DRPs make secure requests for data to an API endpoint that IOUs open to the outside world using aforementioned DRP unique key/secret and customer authorized access tokens (see functionality # 4) as proof for the utility to validate, respectively, who the DRP is, and that they have been authorized to receive a customer’s specific data. The customer authorized data comprises data elements necessary for Rule 24 processing by DRPs as specified in an initial proposed list provided by DRPs.

   It should be noted that DRPs have requested both Solutions 1 and 3 require the utilities respond to the API request with customer data within 90 seconds, however this requirement is not feasible for the utilities, especially in regards to providing the full list of DRP proposed data elements due to various reasons (e.g. data availability, system limitations, etc.).

6. On-going Operation and Maintenance:

   On-going operational support and maintenance of Solution both from a business process (documentation, training, etc.) and technical support standpoint including managing DRP and customer inquiries, complaints, issues as well as deploying future changes.

Differences in implementation:

Solution 1

3. Customer Authentication:

   The DRP web site serves up a login form (hosted on the DRP systems) which allows the customer to authenticate with the utility. Once the customer’s credentials are entered in the form and the customer clicks a button to submit the authentication form, the DRP invokes a utility web service (hosted on utility systems) and passes those credentials to the utility via that web service. If the customer is authentic (according to utility records), the web service returns a confirmation for the DRP web site to proceed to the next step in the process (authorization).

4. Customer Authorization:

   The DRP web site serves up an authorization form (hosted on the DRP systems) which allows the customer to authorize the utility to release that customer's data to the DRP. Once the customer clicks a button to submit the authorization form, the DRP invokes a utility web service (hosted on the utility systems) and passes the authorization data to the utility via that web service. The utility then stores a record of that transaction in its systems. The web service then returns a token (e.g., authorized) to the DRP, which can be used by the DRP to call other utility web services and retrieve customer data.

Solution 3

3. Customer Authentication:

   The DRP web site redirects the customer's browser to a utility web site (hosted on utility systems) for the customer to authenticate with the utility. Once the customer's credentials are entered in the form and the customer clicks a button to submit the authentication form, those credentials are passed from the utility web site to an authentication web service (also hosted by the utility).

4. Customer Authorization:

   After authentication, the DRP web site takes the customer to a (utility hosted) page to authorize release of their data to the DRP. Once the customer clicks a button to submit the authorization form, the authorization details are stored in the utility's system, and the authorization page responds with a success confirmation, instructing the customer's browser to redirect the customer back to the DRP site from which the DRP can subsequently make a web service request for an authorization code and finally a token. The final resulting token can be used by the DRP going forward to call other utility web services to retrieve customer data.

Detailed Descriptions of Solutions 1 and 3

Solutions 1 and 3 have key differences in the ways that they implement the following functionality for customer authentication and authorization. In addition to the details described below, please find attached appendix documentation for both an accompanying illustration of the customer journeys for Solution 1 and 3 as well as technical sequence diagrams capturing the interactions between customer, DRP and IOU (depicting both visible and non-visible interactions to the customer).

3. Customer Authentication

   Solution 1

   From a user experience standpoint, assuming there is only a single Service Account[1] that a customer intends to authorize to a DRP (e.g. residential use case), 3rd party DRPs can potentially implement customer authentication and authorization as a single page with a single step/transaction for the customer to initiate (e.g. 'Authorize button') on their websites. In regards to a customer intending to authorize multiple Service Accounts, additional steps and/or pages and supporting backend API calls to the IOU must be made to complete authorization (detailed further in 'Customer Authorization' functionality section 4).

   Solution 1 depends on the development of a common set of code (i.e. a 'Library' most likely developed in JavaScript programming language) to be provided by the IOUs to registered 3rd party DRPs. The provided Library is designed to ensure the customer provided authenticating information (e.g. username and password, or Service Account ID, Zip Code, Name etc.) that is entered by customers <u>on 3rd Party DRP websites</u>, is immediately and securely transferred to the IOUs for the IOUs systems to authenticate the customers' identities, while in theory, simultaneously avoiding such sensitive customer information to be stored by DRPs in their systems unbeknownst to customers. From a customer experience and security standpoint (to be elaborated on in other sections), this design does not necessarily address customers' trust and comfort in providing such sensitive authentication information on 3rd party DRP websites, for which customers must agree to do at their own risk and discretion.

   3rd party DRPs integrate the aforementioned IOU provided library into their websites to facilitate the collection and backend transmittal of customer authenticating information directly to the IOUs, however the front end form/page with which customers interact and enter their authenticating information and authorization of data sharing is wholly designed and owned by the 3rd Party DRPs. This is accomplished in part by the library executing such transactions directly within the client (web) browser as opposed to such functionality executing on a backend server serving the website.

   Complimentary to the code Library that is deployed on DRP websites/applications, IOUs also open an API endpoint to the outside world (e.g. public internet) for secure API requests by 3rd Party DRPs whereby the DRP implemented library supporting the front end page automatically combines the customer provided authentication information with the DRP specific key and secret (provided earlier as part of completing DRP registration with IOUs) and transmits it directly over encrypted transport layer to the IOU end point for authentication of the customer's identity by IOU systems in real time.

[1] This is a more universal term. For PG&E, the service agreement is the level at which the CISR is processed, and refers to a specific identifier for tracking and measuring energy service deliveries for retail billing purposes of a specific load associated to a specific physical location, within the context of Rule 24. Multiple service agreements may fall under a service account, which is commonly tied to the financial account. For SCE, there are service accounts and customer accounts, respectively. For SDG&E, there are service accounts and bill account, respectively.

Upon real time authentication of the provided customer authenticating information by IOU systems, a response is returned by the IOUs with a 'token' that is to be provided in subsequent API requests by DRPs as proof that the 3rd party DRP has authorized access to retrieve customer data.

To the customer, these backend API calls (and encapsulated transmission of customer authenticating info) between 3rd Party DRPs and IOUs are seamless and behind the scenes save for the short processing time it takes to send/receive authentication, authorization and associated token.

As an analogy, the design pattern for Solution 1 follows online credit card payment processing model employed by companies like Stripe and Paypal whom provide such code libraries for 3rd party online merchants (analogous to 3rd party DRPs) in order to collect customer credit card info (i.e. credit card #, CVS code, Expiration date, Name – analogous to the utility customer authenticating info of Service ID, Zip etc.) that is then transmitted to the credit card companies/banks (analogous to IOUs) for authentication by their systems. Detailed information of Stripe's implementation is exampled here as reference: https://stripe.com/docs/custom-form#step-1-collecting-credit-card-information

Solution 3

Solution 3 facilitates customer authentication by temporarily redirecting customers from the DRP website to an IOU customer log in page. From a customer experience standpoint, the customers will observe an additional page for identity verification on the IOU side, but at the same time they can verify that they are indeed entering in their authenticating info directly onto the IOU website. To address use cases where customers do not have IOU log-in username and password credentials or do not wish to create log in credentials, the IOU customer authentication page may need to be enhanced to support alternative authentication credentials besides username/password such as the providing of Service ID, Zip, name, etc., similar to what is proposed for Solution 1. Regardless of authentication credentials, the IOU website will provide for real time customer authentication.

Once the customer has logged in, they are directed to a second page on the IOU's side for the customer to review and submit their authorization to share data with the pre-selected 3rd party DRP (i.e. DRP from who's website they came from) and upon authorization confirmation are then redirected back to the 3rd party website for any further interactions with the 3rd party DRP. Similar to Solution 1, at the end of the authentication and authorization sequence, the 3rd party is provided a token to be used in subsequent API requests by DRPs as proof that the DRP has authorized access to retrieve customer data. In industry standard terms, this overall framework employed by Solution 3 is known as 'OAuth'.

4. Customer Authorization (and subsequent authorization updates or revocation)

Solution 1

Assuming there is only a single Service Account that the customer intends to authorize to a DRP (e.g. residential use case), Solution 1 allows for customer authentication and authorization to potentially operate as a single transaction and page for the customer and there are no additional details as far as initial customer authorization. In the event there are multiple Service Accounts a customer intends to authorize (e.g. commercial customer use case), however, the customer journey involves more back-end interactions and potential front end steps and pages to be presented on the DRP site to the customer. To elaborate, DRP must either request the customer provide all service account identifiers they wish to authorize upfront for authentication, or otherwise assuming the different service accounts are all linked and owned by the same customer and account, the customer could provide their account ID, and the DRP must make additional API calls to retrieve a list of underlying Service Accounts for authorization after the initial authentication, for which the DRP then presents a list of those service accounts to the customer to select which ones they want to authorize.

In regards to subsequent updates (e.g., changing scope of data elements, service accounts, and duration of authorization) and/or revocation by customers, DRPs again own the customer interface for customers to initiate such requests on the DRP website, however IOUs must open another API for 3rd parties to make corresponding API requests for updates/revocation to the authorization while providing similar credentials (e.g., token, etc.) as when making other API request such as for customer data.

Solution 3

From a customer experience standpoint, Solution 3's employment of the OAuth standard adds 2-3 pages to the customer authentication and authorization flow (i.e. IOU log in page, authorization submission and optional confirmation page), but can uniformly handle authorizations for both a single utility service account or multiple utility service accounts without additional steps or pages given that the IOU provided pages for authorization are able to present all customer managed service accounts for the customer to select from when authorizing.

Given Solution 3 entails customers being temporarily redirected to the IOU website for authentication and authorization, there is an additional behind the scenes exchange of an initial 'authorization code' acknowledging both receipt and acceptance of customer authorization is provided by the DRP, prior to the DRP requesting an access token (however the resulting end token for Solution 3 functions in essentially the same manner as that provided in Solution 1).

In regards to subsequent updates (e.g., changing scope of data elements, service accounts, and duration of authorization) and/or revocation by customers, ownership of customer initiated changes can happen either on the DRP side or IOU side. Authorization changes and revocations initiated on the DRP website would function in the same way as Solution 1, whereas authorization changes and revocations directly on the IOU side would provide for a notification posting to affected 3rd parties.

Appendix B, C, and D provide additional documentation on the Solutions 1 and 3.

APPENDIX B

Proposed Solutions for Click-through Implementation

Proposed Solutions for Click-through Implementation

With HUGE thanks to DRPs, Coalition Letter Signatories, Mission Data, Chai Energy, OhmConnect, EnergyHub, Enernoc and Olivine for their input and content additions

Guiding principles

1. ***Full Data Set***: Standardize availability of a requisite set of data for historical and ongoing data access. Please see Appendix A for suggested data set.

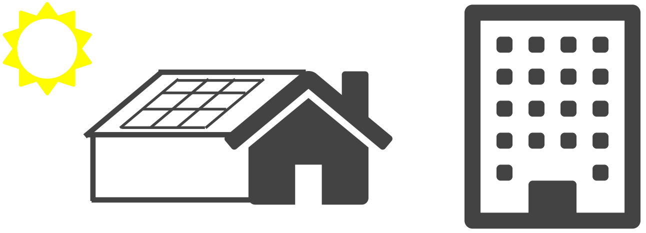
2. ***Synchronous Data:*** Once a data request is authorized and authenticated, data is delivered on-demand, upon authorization, (e.g. data begins streaming w/in 90 seconds of request).

3. ***Instant, Digital Authorization***: A digital signature (incl. click-through) is valid for authorizing data sharing.

4. ***Instant, Consumer-Centric Authentication:*** A third-party will not be held to a higher authentication standard than the Utility holds itself. Accordingly, the Utility will authenticate using consumer-centric login credentials, for example, zip code and account # or Online Account username and password.

5. ***Seamless Click-through***: A utility account holder will be allowed to begin and end the click-through process on the Third-Party website. This may happen without any requirement to log in to any other site/ process during this flow (e.g. checkbox) or may allow the user to remain in the third party website flow, even in various authentication scenarios (login, signup, forgotten password, etc.), as in the case of OAuth or open authorization protocols. The click-through process shall be designed to be one-click and the third party may lead the customer request for the types of data and the time frame of data sharing. The customer may approve or reject such a request in its sole discretion.

6. ***Strong Security Protocols***: Adopt strong security protocols. Data security may accommodate cloud-based systems. In addition, we recommend consideration of the security elements listed in Appendix B.



Residential and commercial

Additional content credit to Broad Coalition

Overview of all solutions

All solutions:

- Can be completed on a mobile device or on a computer
- Can facilitate an out-of-band request (e.g. a paper CISR with the same computerized data output)
- Are synchronous for the authorization/authentication section
- Can provide synchronous and/or asynchronous data feeds
- Meet the six principles
- Provide audit-able records and user receipts
- Are compatible with one another and can be implemented side-by-side

Three solutions

API Solution 1

The same process that credit card payment processors use, like Stripe, Paypal

API Solution 2

Simple and fast-to-implement solution

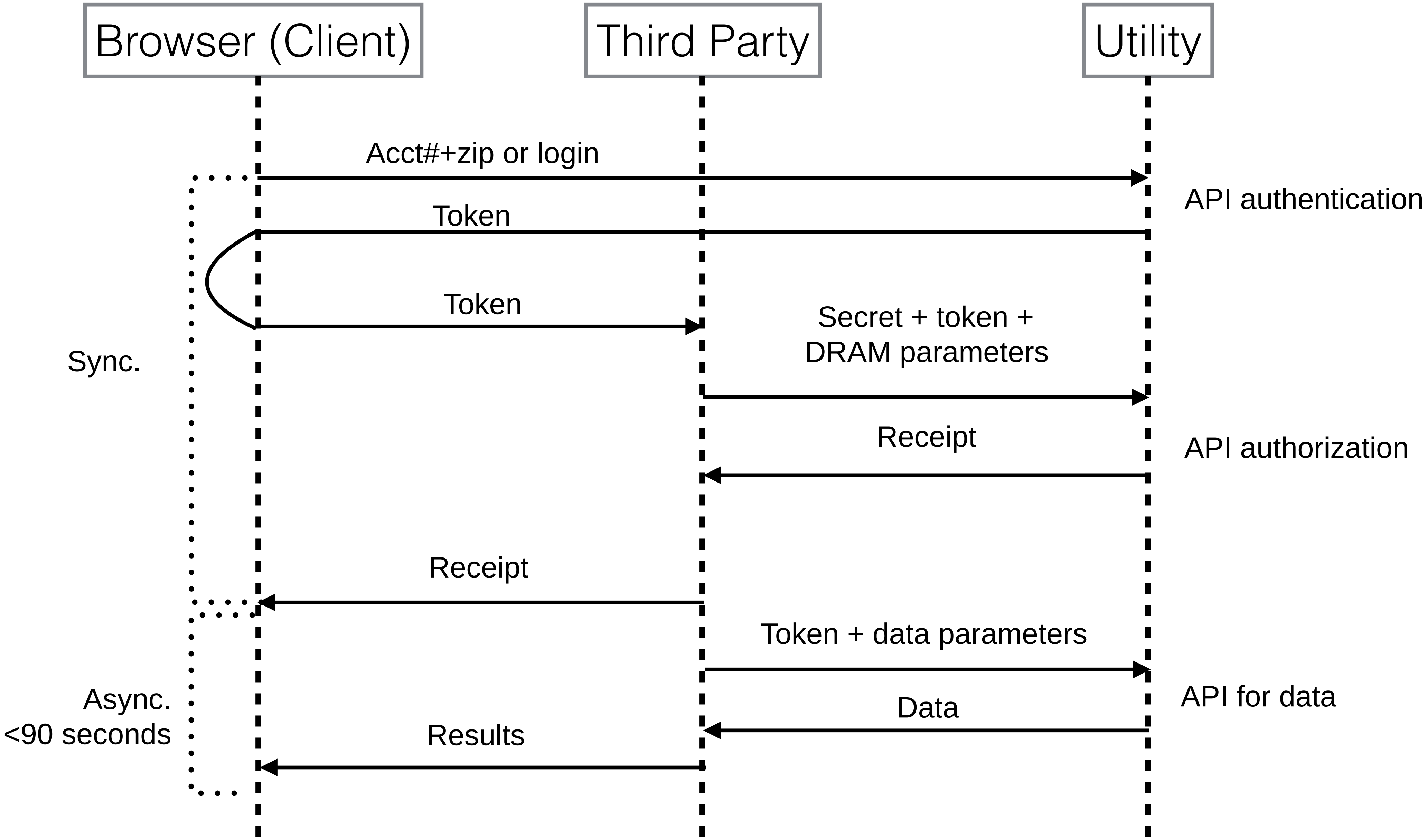
OAuth Solution 3

Streamlined and simplified process similar to social networks like Facebook and Twitter"

Disclaimer: At this time, the third parties are not advocating for one (or a limit of one) solution

API - Solution 1

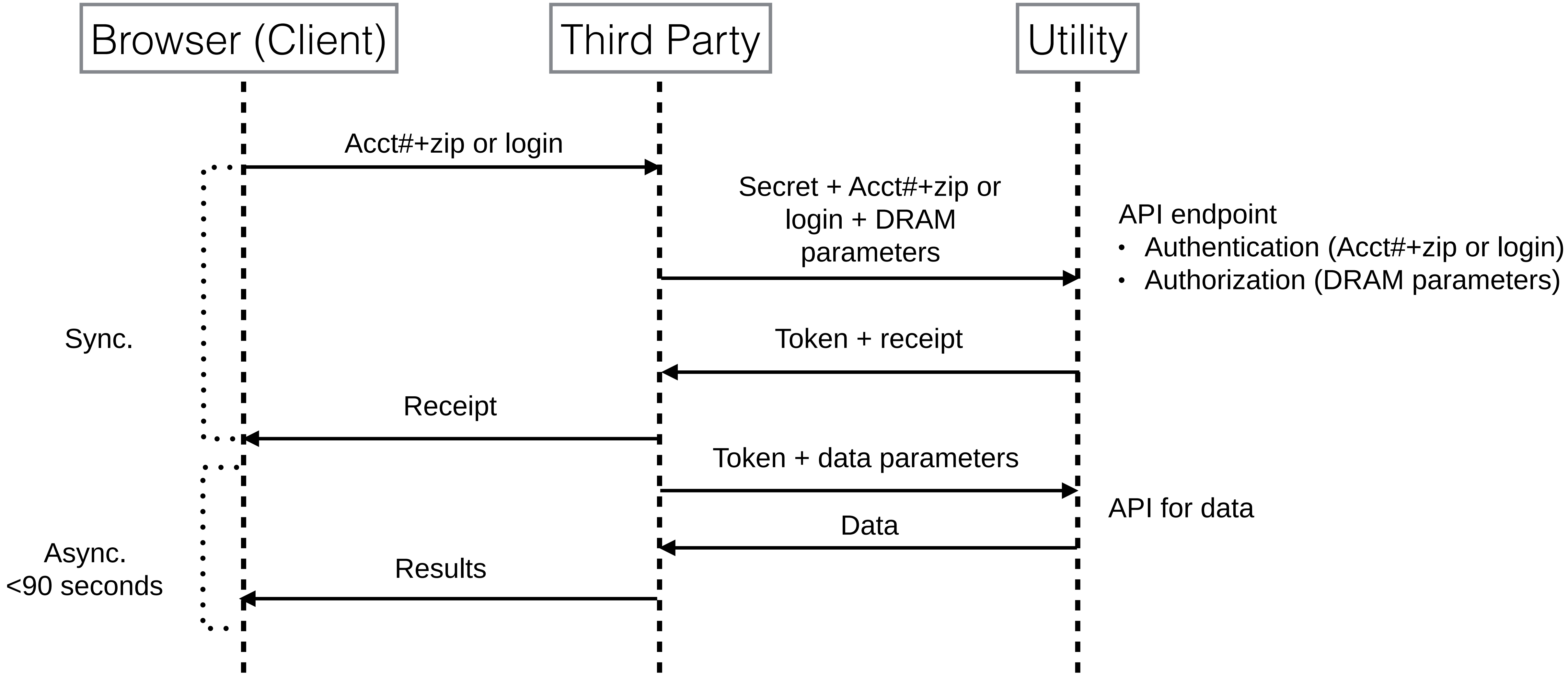
Utility authenticates - either via login or account #



Pro - pretty easy to implement; authentication parameters go straight from browser client to utility (*does not pass through 3rd party servers*); does not require integration to IOU user experience; eliminates the most “clicks” for the user; third parties can capture all information on just one page

Con - Two API endpoints that the utility has to implement and the second endpoint has to be browser friendly, not just server friendly. Could create additional time/cost requirements due to the need for two endpoints. This option cannot accommodate a password reset, but it could be implemented alongside a password-reset wizard.

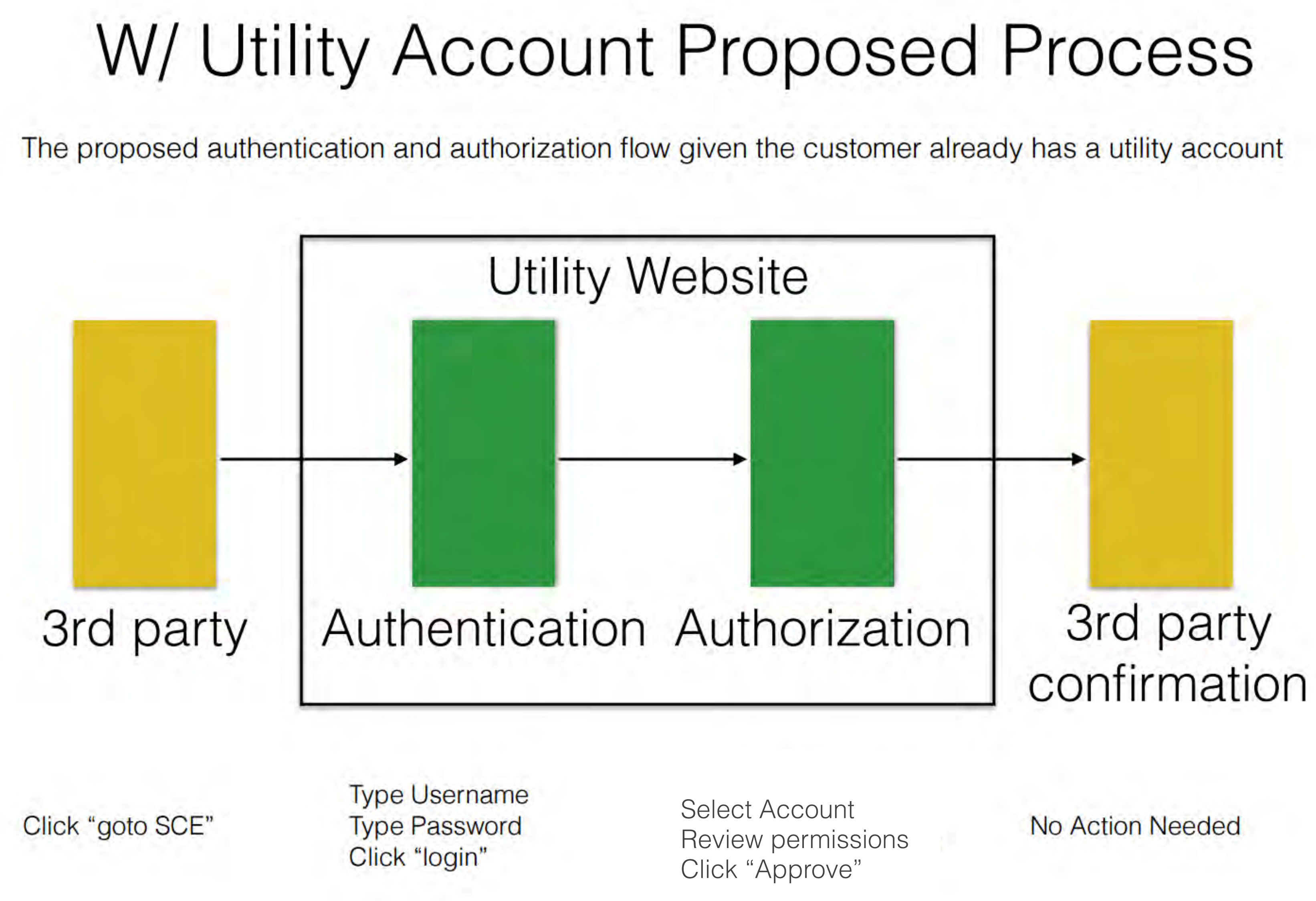
API - Solution 2



Pro - fastest and cheapest to build; does not require integration to IOU user experience; eliminates the most "clicks" for the user; third parties can capture all information on just one page

Con - Authentication credentials pass directly through the 3rd party servers. This option cannot accommodate a password reset.

OAuth: Solution 3



W/ Utility Account Proposed Process

The proposed authentication and authorization flow given the customer already has a utility account

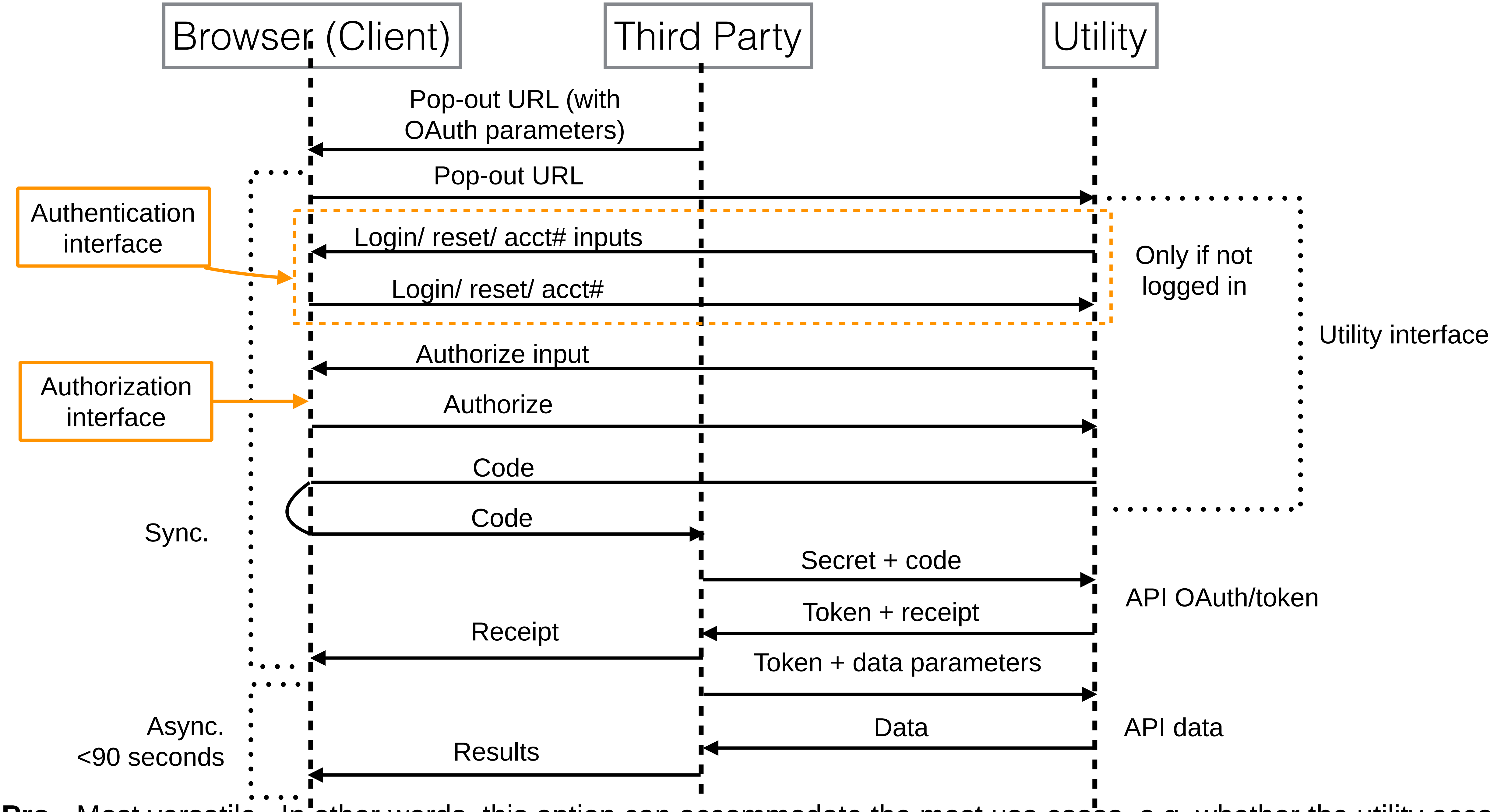
Streamlined & improved:

- Don’t ask customer for datatypes, scope, etc.
- 3P can mandate options on utility’s auth page (“take it or leave it”)

Additional content credit to Chai Energy and to Mission Data

OAuth Solution 3

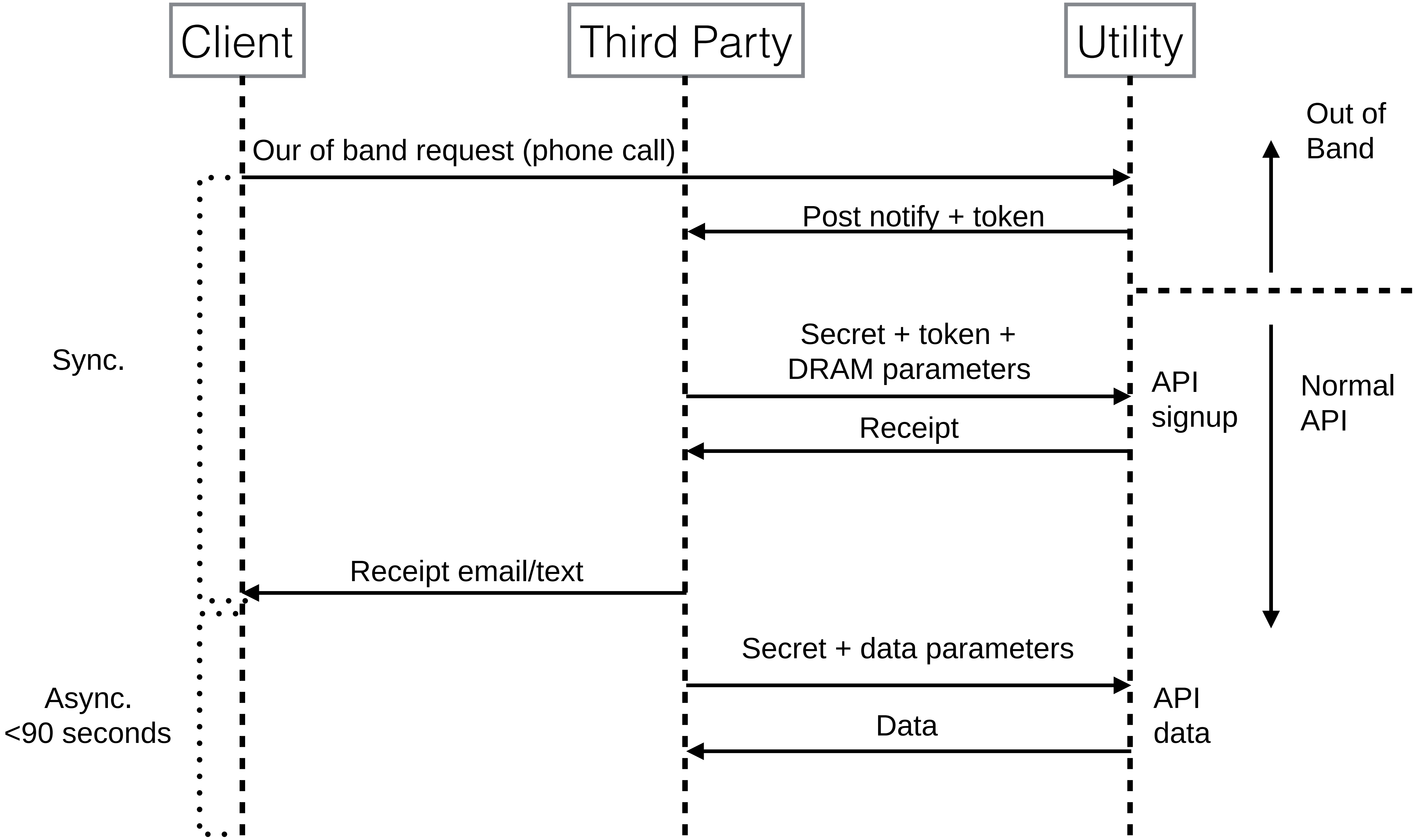
Pop Out or iFrame (OAuth) - Pop-out to Utility website, Utility authenticates - either via login, account # or cookie



Pro - Most versatile. In other words, this option can accommodate the most use cases, e.g. whether the utility account holder has an online account or not, remembers password or not, wishes to bypass online account, etc.

Con - Utility needs to build and maintain a section of the interface that must facilitate most minimal user fatigue and DRP input; may add 2-3 more “clicks” and “pages”; less customizable for the DRPs

Add-Alternate: Out of Band



Pro - Entirely over paper CISR or by telephone call (presumably to utility), but provides same data output

Con - Longer utility implementation time and documentation

Three Potential Solutions

Solutions 1 and 2: All user experience on 3rd party site (using an IOU API for interaction during the user experience)

Step 1: The user enters identifying information in the 3rd party web site for authentication.

Step 2: The 3rd party requests data through an API call to the IOU

Step 3: The 3rd party collects user authorization (i.e., with signature, checkbox, etc.) [important distinction - in Solution 1 authentication parameters go straight from browser client to utility (do not pass through 3rd party servers)]

Step 4: Authorization is transmitted to IOU (in some format).

Solution 3: All Auth on utility site (using streamlined OAuth solution)

Step 1: 3rd Party Site

Steps 2 and 3: Authentication and Authorization by Utility (on their site or through other mechanism - *e.g. a single pop-out*)

Step 4: 3rd Party Site

An important component is streamlining the OAuth workflow and specifying text/presentation in detail within the scope of the workshop. This is to resolve the critical concern that user experience is handed over to the IOUs without input from the DRPs. We need to be specific about look and feel, text, # of screens, clicks, etc. in order to agree upon a vision for the use of OAuth technology. This vision does not imply that the utility account holder has an existing utility web-site account nor do they have to create one, so it supports the other optionality for customer authentication.

Additional content credit to Olivine

Rule 24 Data Set

* **Account Elements**
  * Account name (ACME INC. or JOE SMITH)
  * Account address (123 OFFICE ST...)
  * Account ID (2-xxx...)
* **Outage block (A000)**
* **Service Elements**
  * Service ID (3-xxx...)
  * Service address (123 MAIN ST #100...)
  * Service tariff (D-TOU) (incl. any applicable demand response tariffs)
  * Service tariff options (CARE, FERA, etc.)
  * Service voltage (if relevant)
  * Service meter number (if any)
  * # of Service meters – a service account many have multiple meters, is that captured?
* **Historical bills (since beginning of service)**
* **Billing Elements**
  * Bill start date
  * Bill end date
  * Bill total charges ($)
  * Bill total kWh
* **Bill tier breakdown (if any)**
  * Name (Over Baseline 1%-30%)
  * Volume (1234.2)
  * Cost ($100.23)
* **Bill TOU kWh breakdown (if any)**
  * Name (Summer Off Peak)
  * Volume (1234.2)
  * Cost ($100.23)
* **Bill demand breakdown (if any, incl. options)**
  * Name (Summer Max Demand)
  * Volume (1234.2)
  * Cost ($100.23)
* **Bill line items/options (sum should equal bill total charges above)**
  * Charge name (DWR Bond Charge)
  * Volume (1234.2)
  * Unit (kWh)
  * Rate ($0.032/kWh)
  * Cost ($100.23)
* **Tracked line items**
  * Charge name (e.g. Net In/Net Out)
  * Volume (1234.2 in kWh)
  * Unit (kWh)
  * Rate ($0.032/kWh, if any)
  * Cost ($100.23, if any)
* **Payment Information**
* **Historical Intervals (since beginning of service)**
  * Start (unix timestamp)
  * Duration (seconds)
  * Volume (1234.2)
  * Unit (kWh)
* **Also:** Capacity Reservation Level (CRL) for CPP/PDP customers, Demand Response program name and nomination, if fixed, Standby reservation if a customer has on-site generation, and sublap for wholesale nomination.
* Sub-Load Aggregation Point (sub-Lap)
* Pricing node (Pnode)
* Local Capacity Area
* Direct Access, CCA or Service Customer
* Identity and contact information of customer’s LSE, MDMA and MSP.
* Utility’s demand response program(s) and tariff schedule(s) in which the service account(s) are currently enrolled (if any)
* Estimated date of when the customer may be eligible to participate in DR Service w/o financial or tariff implications
* Customer 1 Digit meter read cycle letter

Solution Set Comparison

	Solution 1: API	**Solution 2: API**	**Solution 3: Streamlined OAuth**
Number of pages/ screens	1-2	1-2	3-5
Third Party directs flow and authorization screen presentation	Yes	Yes	Yes
Potential to streamline UX over time	Yes	Yes	Somewhat
Login credentials passed to third party	No	Possibly	No
Can accommodate synchronous and asynchronous requests	Yes	Yes	Yes
Can facilitate out-of-band requests	Yes	Yes	Yes

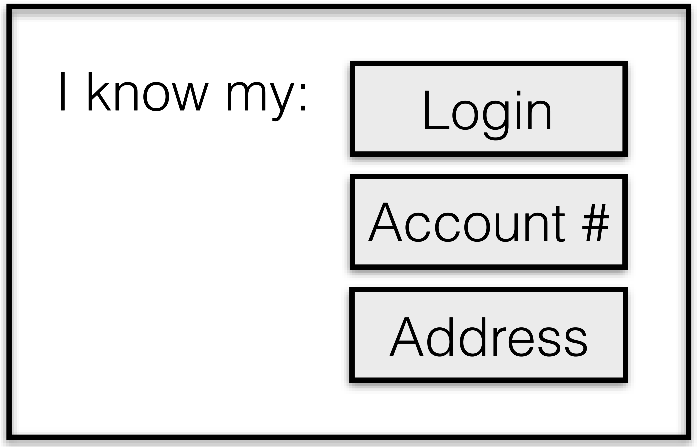
Conclusion

- All three solutions meet 6 guiding principles
- All three solutions can be implemented side-by-side
- Out-of-band also possible add-on in both API and OAuth
- Can have multiple third parties being authorized simultaneously [e.g. Olivine & DRP]

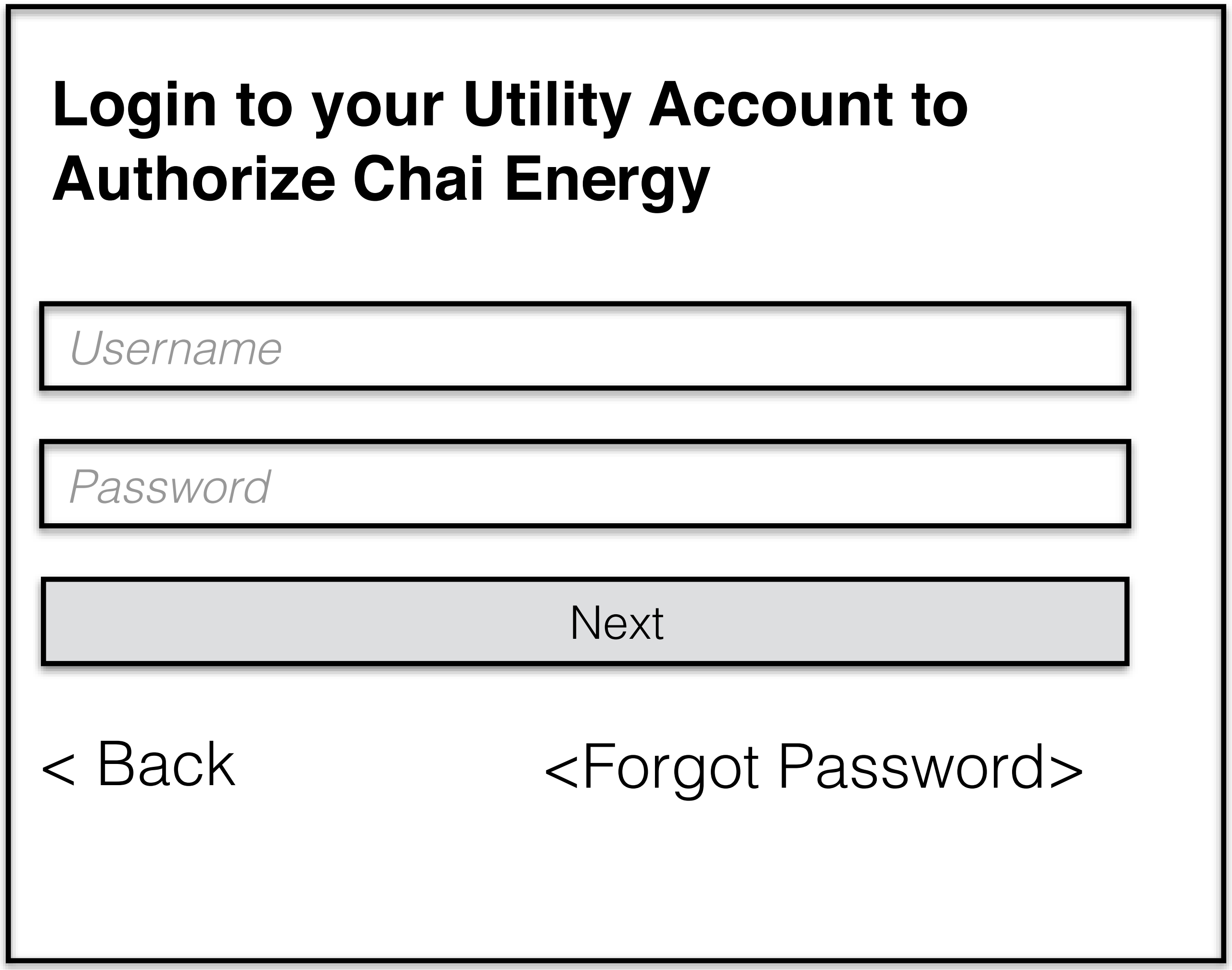
Thank you!

Appendices for Discussion

OAuth Authentication Interface
Sample Draft for Discussion Only

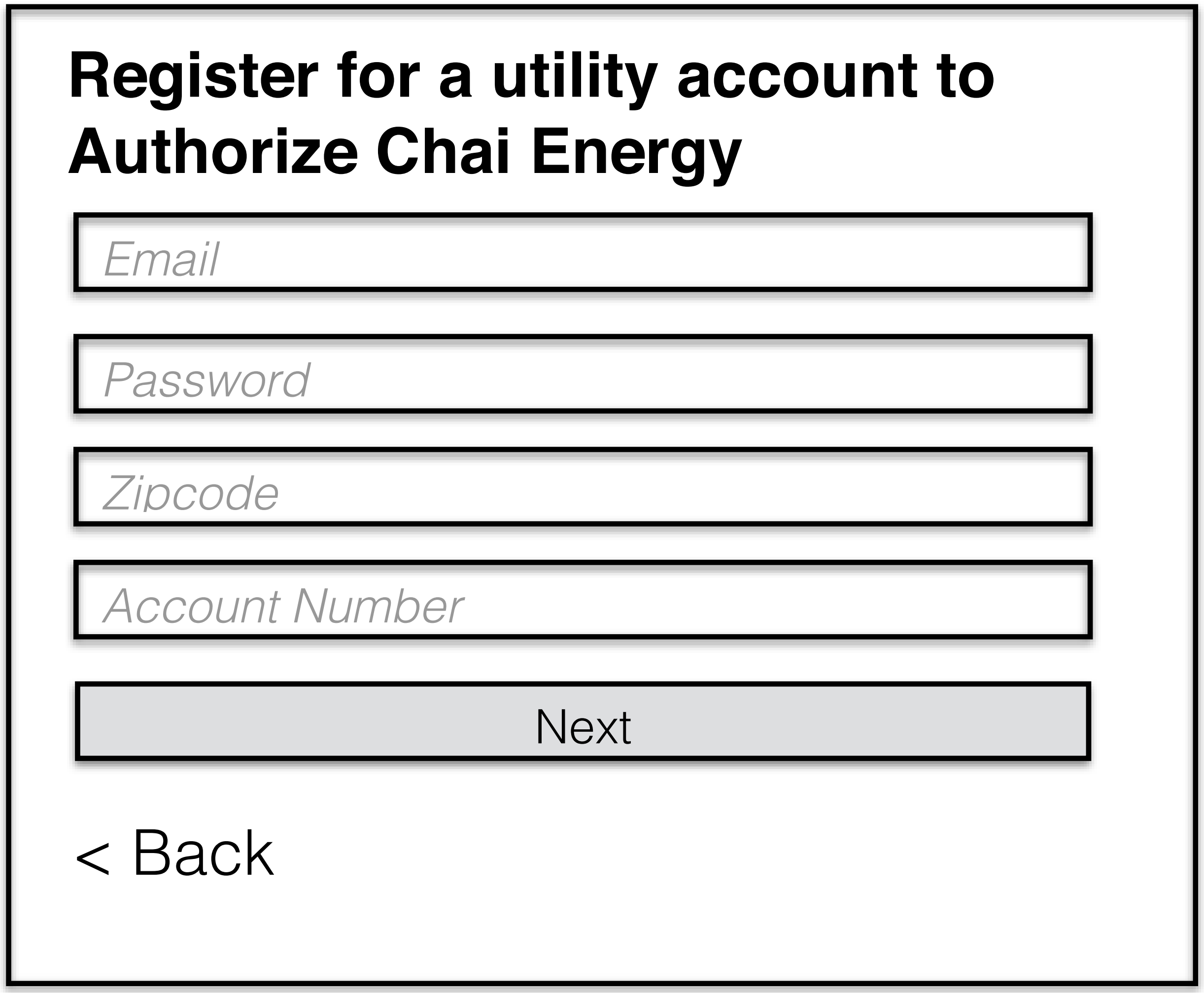


Authentication page when a user already has an online account



Login to your Utility Account to Authorize Chai Energy

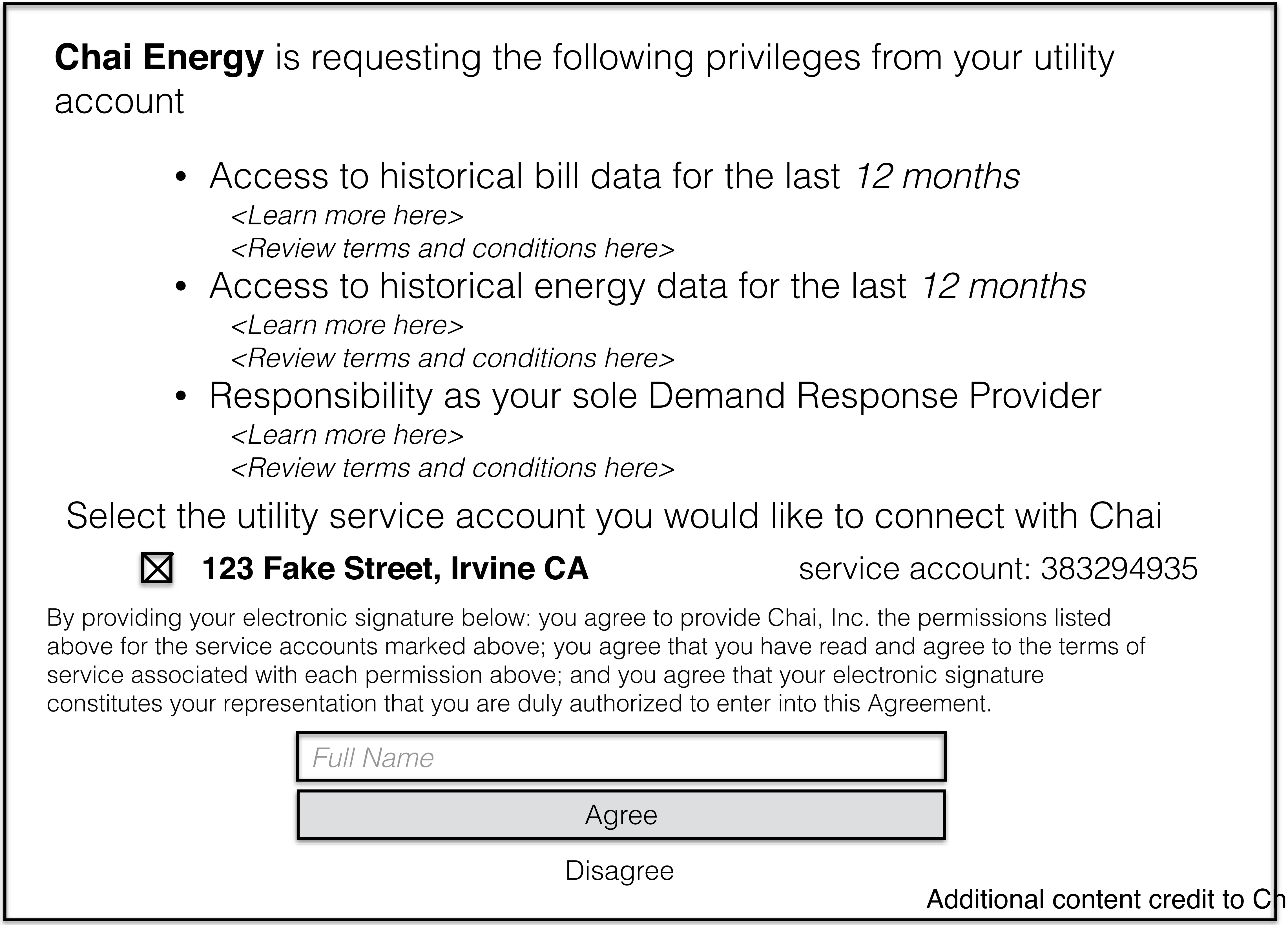
Authentication page when a user does not already have an online account



Register for a utility account to Authorize Chai Energy

Additional content credit to Chai Energy

OAuth Authorization Interface Sample Draft for Discussion Only



Chai Energy is requesting the following privileges from your utility account

- Access to historical bill data for the last *12 months*
  <Learn more here>
  <Review terms and conditions here>
- Access to historical energy data for the last *12 months*
  <Learn more here>
  <Review terms and conditions here>
- Responsibility as your sole Demand Response Provider
  <Learn more here>
  <Review terms and conditions here>

Select the utility service account you would like to connect with Chai

☒ **123 Fake Street, Irvine CA** service account: 383294935

By providing your electronic signature below: you agree to provide Chai, Inc. the permissions listed above for the service accounts marked above; you agree that you have read and agree to the terms of service associated with each permission above; and you agree that your electronic signature constitutes your representation that you are duly authorized to enter into this Agreement.

Additional content credit to Chai Energy

APPENDIX C

API Solution 1 Mock Up

API Solution 1 Mock Up

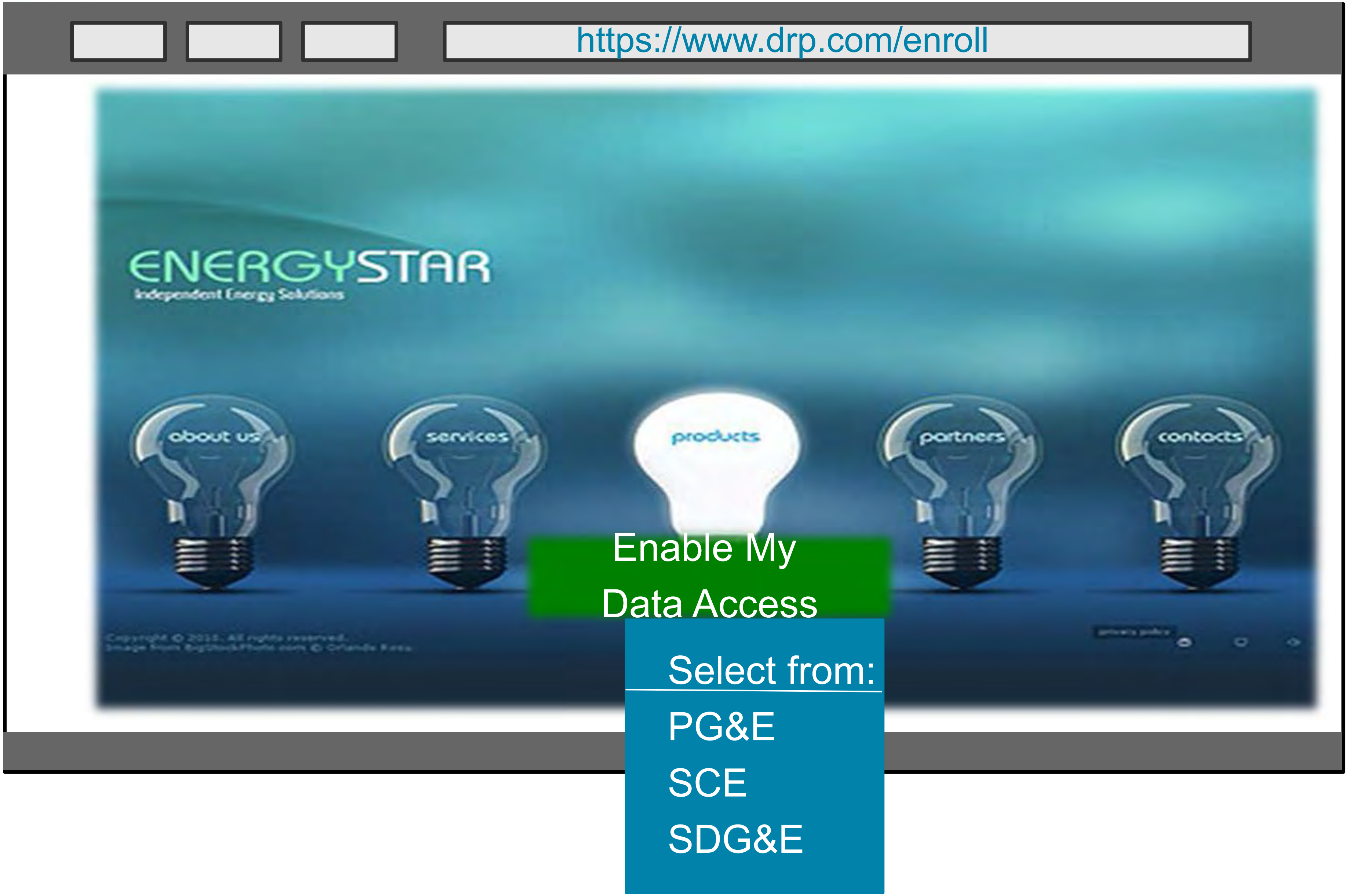
October 3, 2016

API Solution 1 Process

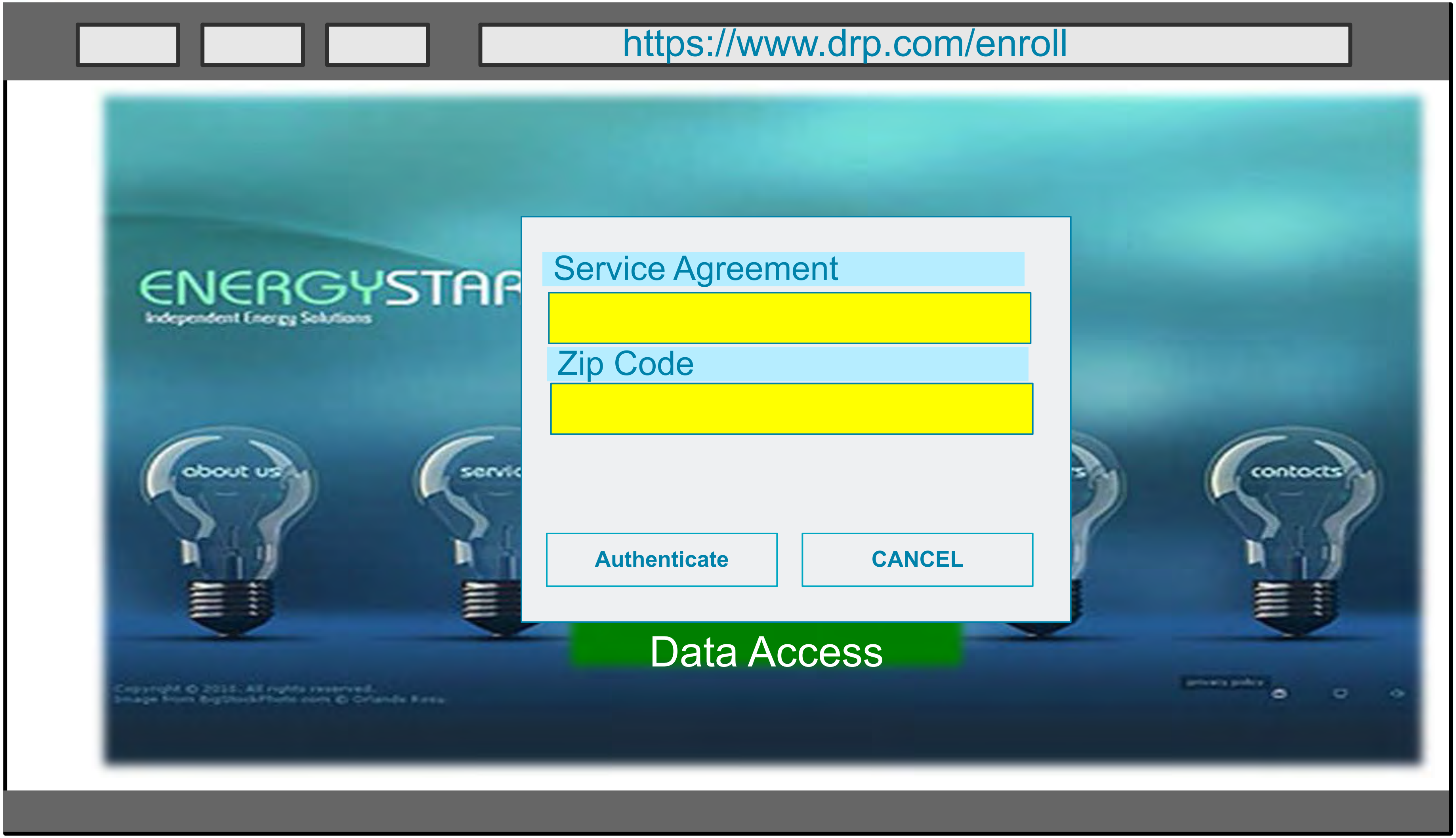
Flow:

1. Start at DRP site
2. Customer selects Utility at DRP site
3. Customer authenticates in to Utility at DRP site
4. Customer authorizes data transfer at DRP site

At the DRP Site



At the DRP Site (one example)



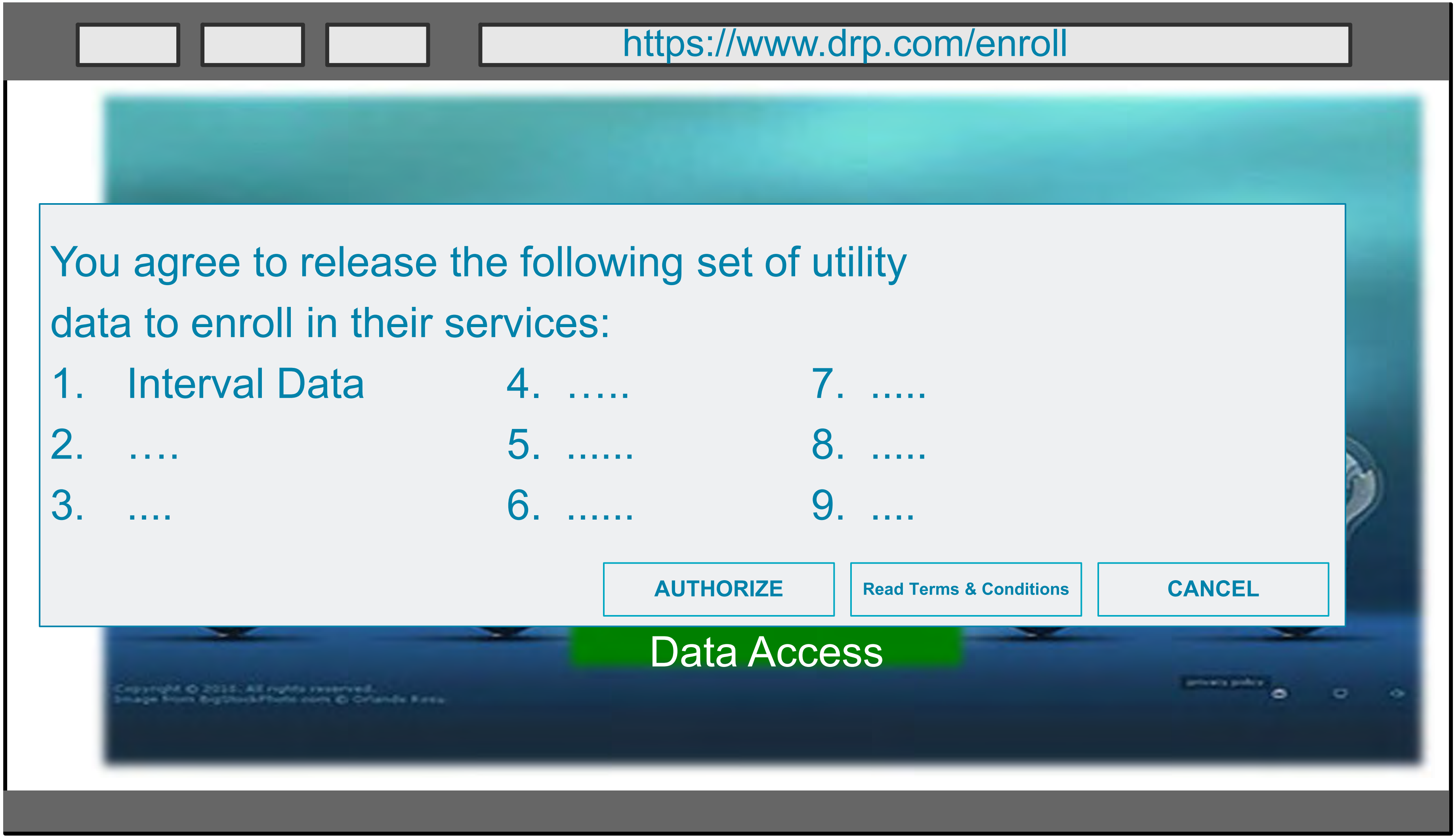
https://www.drp.com/enroll

Service Agreement

Zip Code

ENERGYSTAR
Independent Energy Solutions
about us
servic
s
contacts
Authenticate
CANCEL
Data Access
Copyright © 2015. All rights reserved.
Image from BigStockPhoto.com © Orlando Rosu
privacy policy

At the DRP Site (one example)



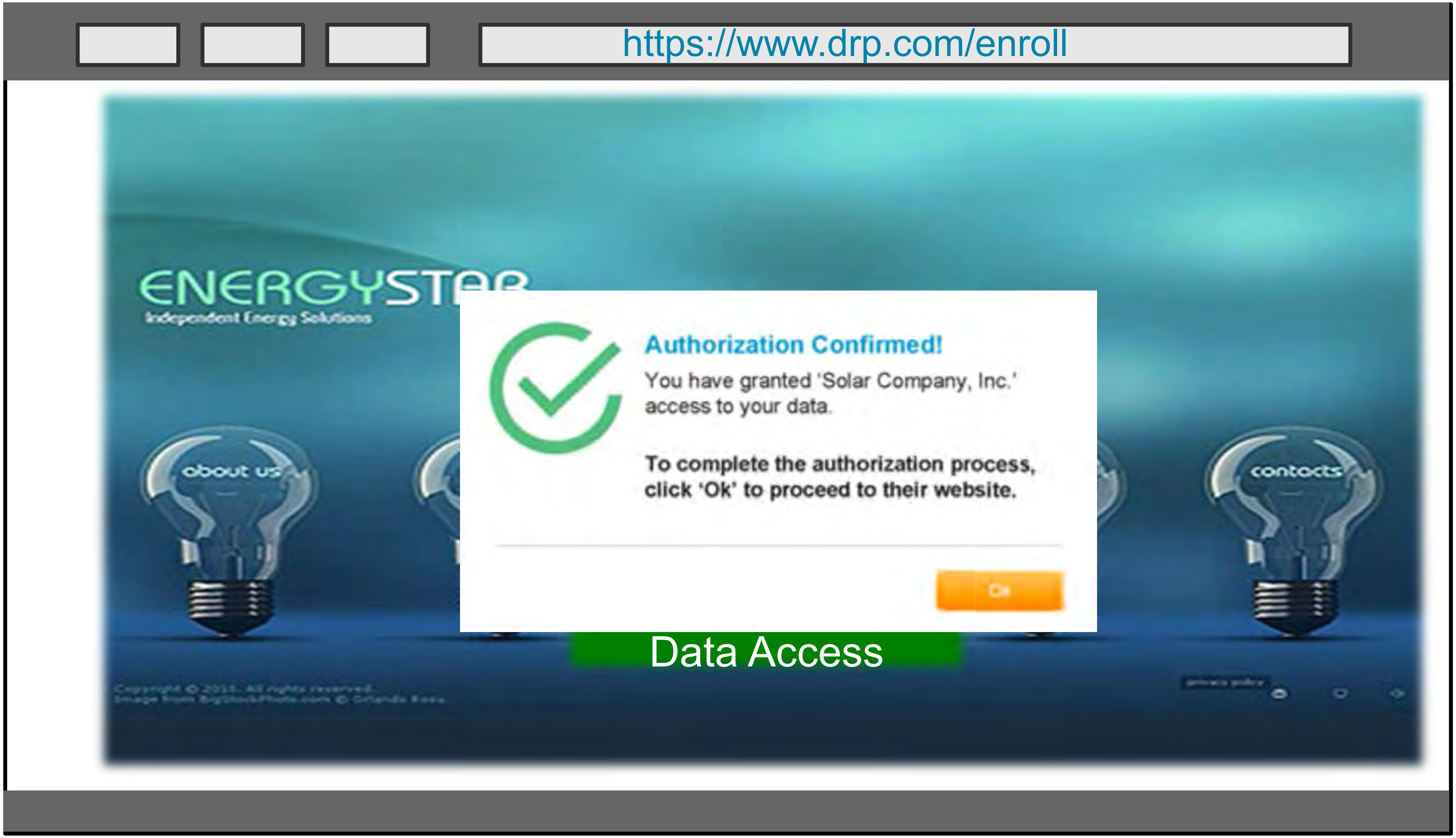
https://www.drp.com/enroll

You agree to release the following set of utility data to enroll in their services:

1. Interval Data
2. ….
3. ….
4. …..
5. ……
6. ……
7. …..
8. …..
9. ….

- *Need revocation processing
- *Page must indicate end date (or no end date) of authorization (e.g. in T&Cs etc.)

At the DRP Site (one example)


https://www.drp.com/enroll
ENERGYSTAR
Independent Energy Solutions
about us
contacts
Ok
Data Access
Copyright © 2015. All rights reserved.
Image from BigStockPhoto.com © Orlando Rosu
privacy policy

Authorization Confirmed!

You have granted 'Solar Company, Inc.' access to your data.

To complete the authorization process, click 'Ok' to proceed to their website.

- * Illustration only. Confirmation does not need to be a modal window.

APPENDIX D

API Solution 3 Mock Up

API Solution 3 Mock Up

October 3, 2016

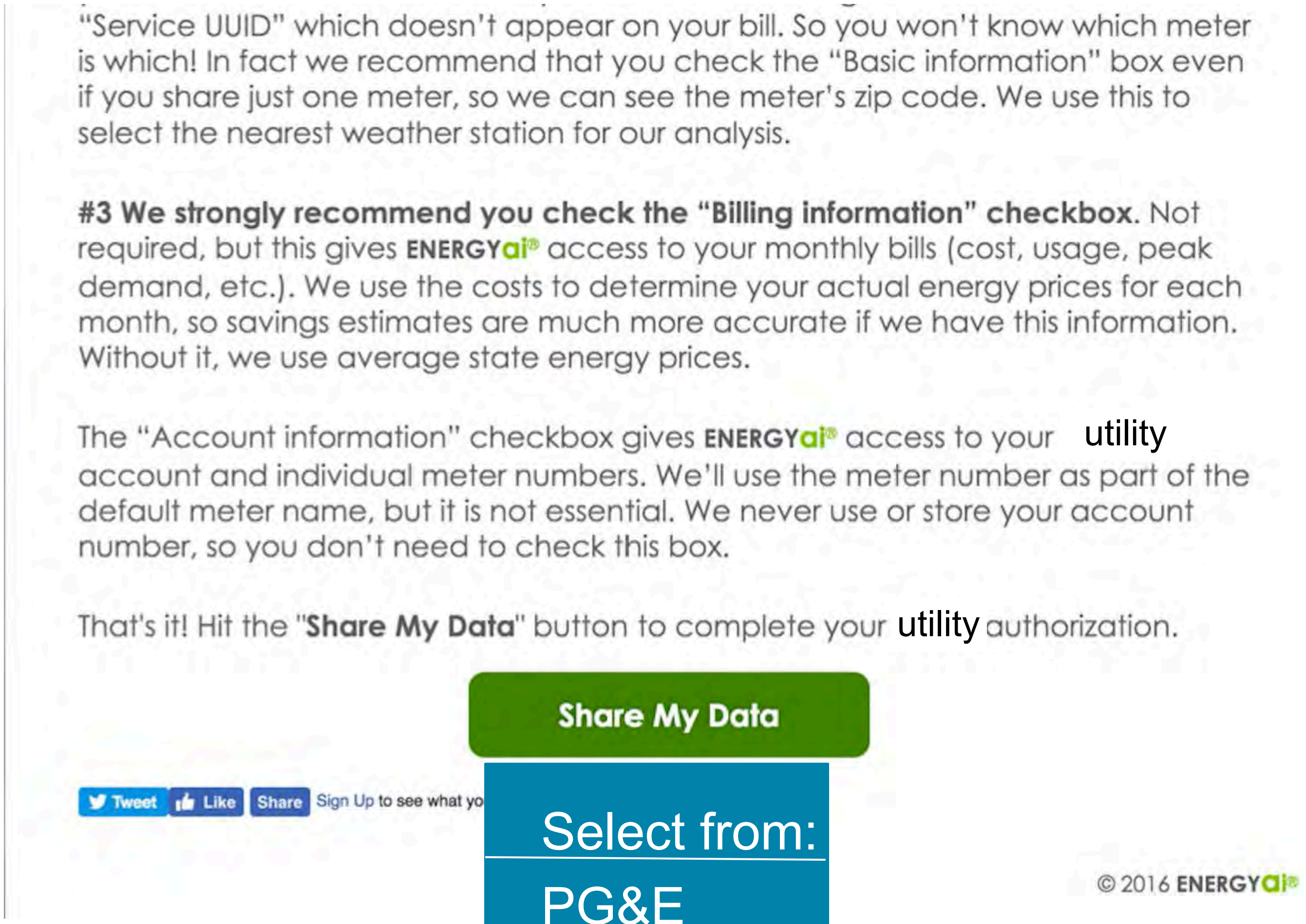
API Solution 3 Process*

Flow:

1. Start at DRP site
2. Customer selects Utility
3. Customer logs in to Utility
4. Customer authorizes
5. Customer returns to DRP site

* Note that API Solution 3 is the preferred method for the IOU

At the DRP Site



"Service UUID" which doesn't appear on your bill. So you won't know which meter is which! In fact we recommend that you check the "Basic information" box even if you share just one meter, so we can see the meter's zip code. We use this to select the nearest weather station for our analysis.

#3 We strongly recommend you check the "Billing information" checkbox. Not required, but this gives **ENERGYai®** access to your monthly bills (cost, usage, peak demand, etc.). We use the costs to determine your actual energy prices for each month, so savings estimates are much more accurate if we have this information. Without it, we use average state energy prices.

The "Account information" checkbox gives **ENERGYai®** access to your utility account and individual meter numbers. We'll use the meter number as part of the default meter name, but it is not essential. We never use or store your account number, so you don't need to check this box.

That's it! Hit the "**Share My Data**" button to complete your utility authorization.

© 2016 ENERGYai®

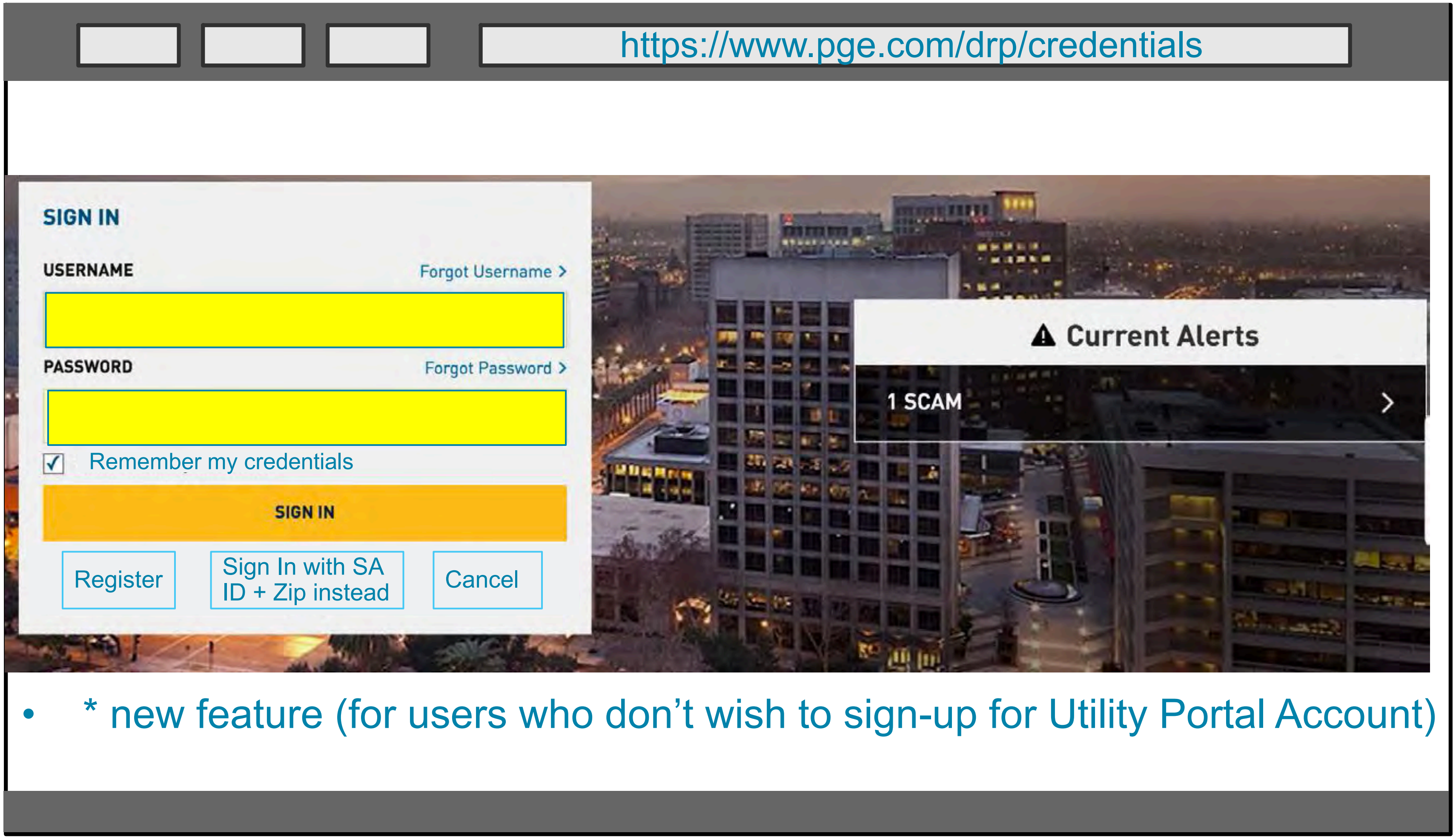
Select from:

PG&E

SCE

SDG&E

At the Utility Site



https://www.pge.com/drp/credentials

SIGN IN

USERNAME Forgot Username ›

PASSWORD Forgot Password ›

☑ Remember my credentials

SIGN IN

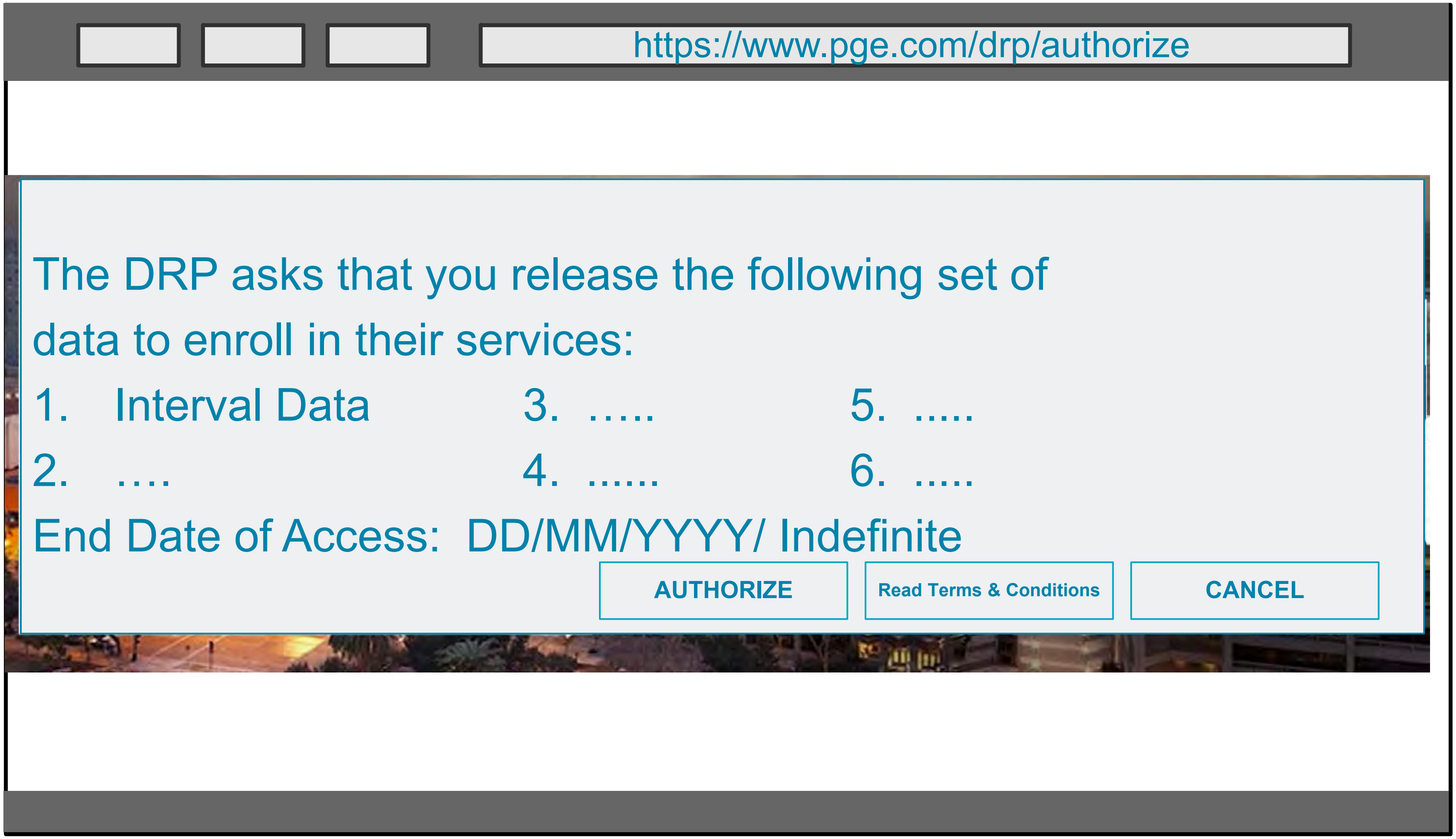
Register | Sign In with SA ID + Zip instead | Cancel

Current Alerts

1 SCAM ›

- * new feature (for users who don't wish to sign-up for Utility Portal Account)

At the Utility Site



https://www.pge.com/drp/authorize

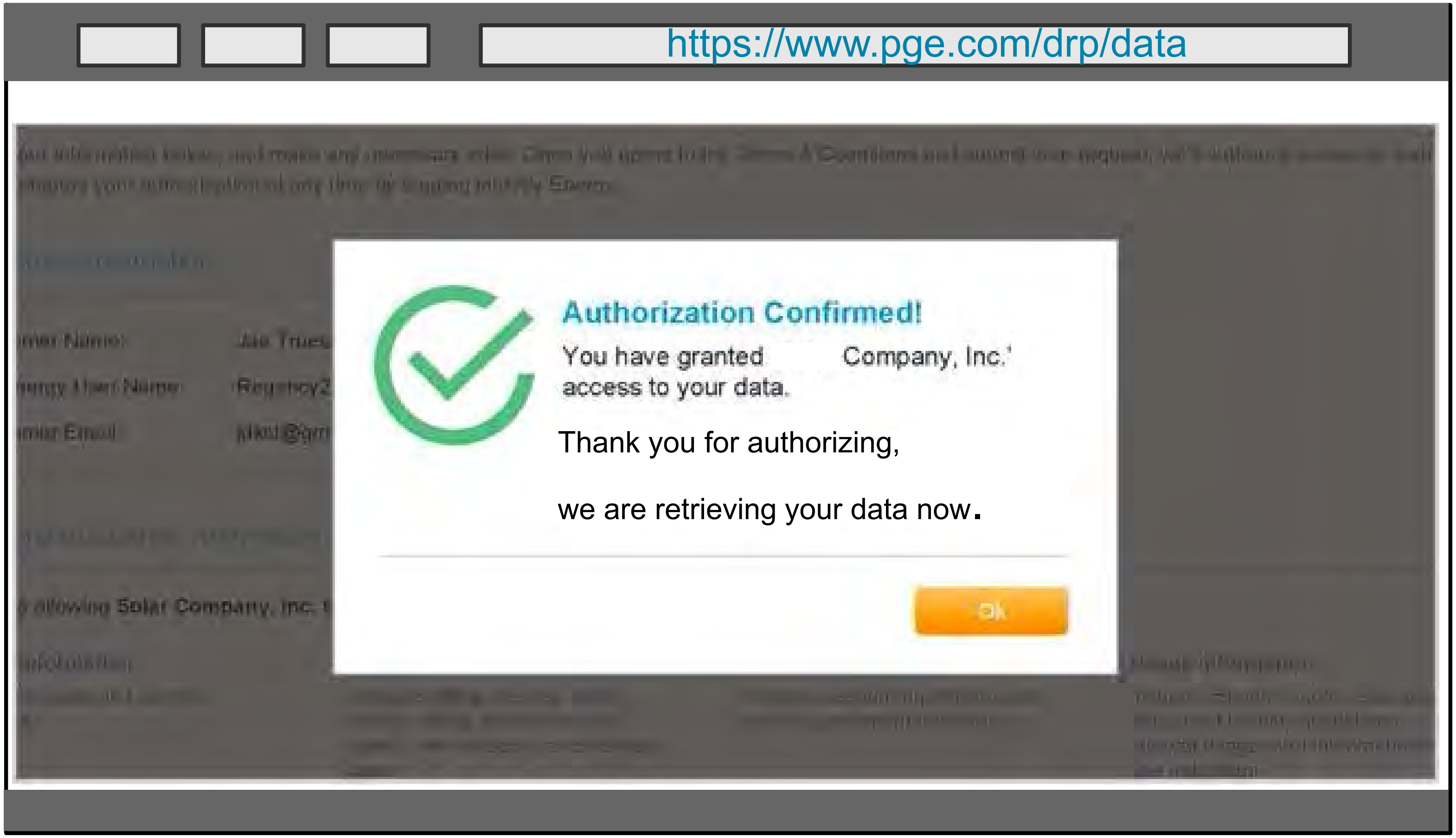
The DRP asks that you release the following set of data to enroll in their services:

1. Interval Data 3. ….. 5. .....
2. …. 4. ...... 6. .....

End Date of Access: DD/MM/YYYY/ Indefinite

* Need revocation processing

At the Utility Site



https://www.pge.com/drp/data

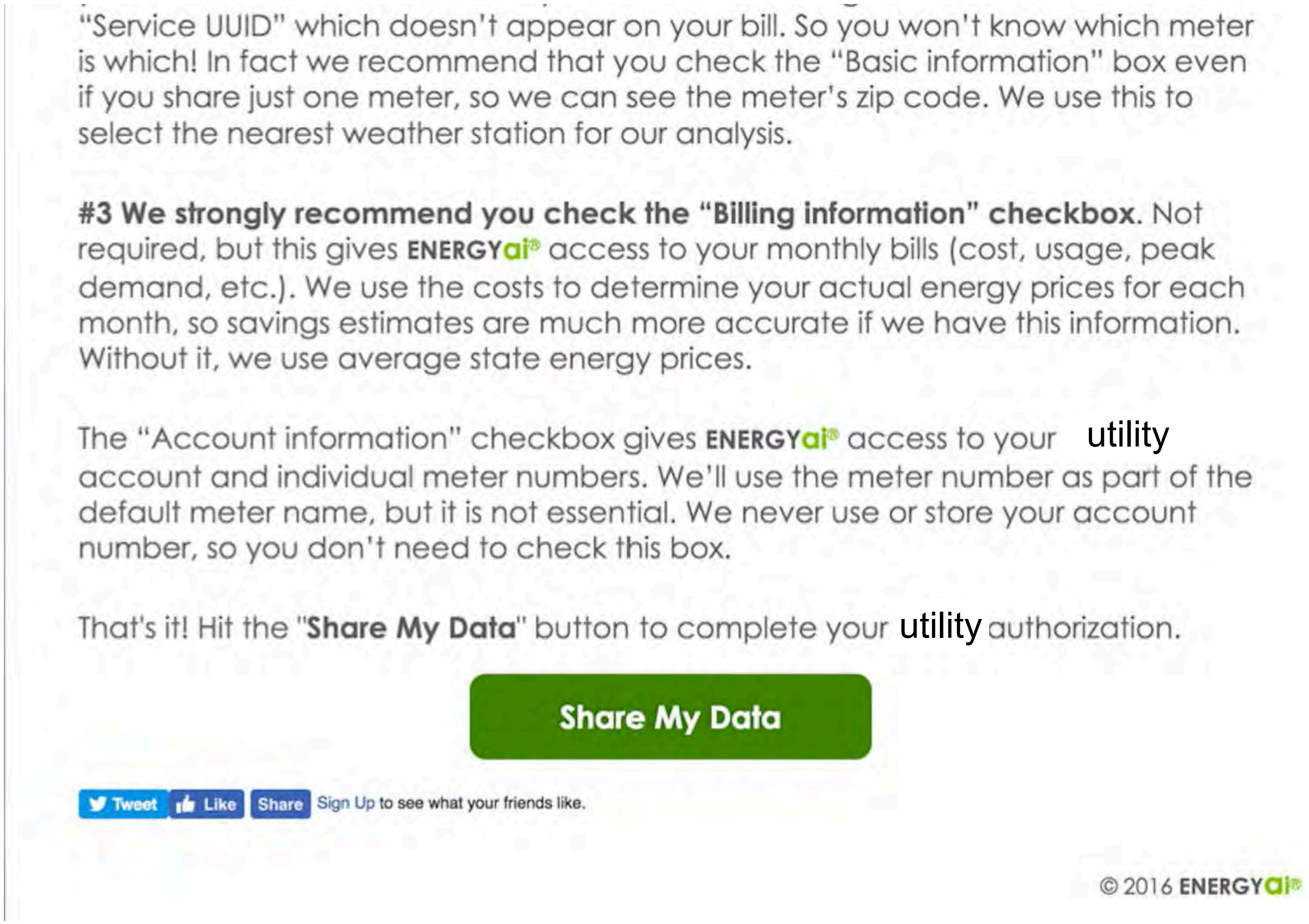
Authorization Confirmed!

You have granted Company, Inc.' access to your data.

Thank you for authorizing,

we are retrieving your data now.

Back to DRP Site



"Service UUID" which doesn't appear on your bill. So you won't know which meter is which! In fact we recommend that you check the "Basic information" box even if you share just one meter, so we can see the meter's zip code. We use this to select the nearest weather station for our analysis.

#3 We strongly recommend you check the "Billing information" checkbox. Not required, but this gives **ENERGYai®** access to your monthly bills (cost, usage, peak demand, etc.). We use the costs to determine your actual energy prices for each month, so savings estimates are much more accurate if we have this information. Without it, we use average state energy prices.

The "Account information" checkbox gives **ENERGYai®** access to your utility account and individual meter numbers. We'll use the meter number as part of the default meter name, but it is not essential. We never use or store your account number, so you don't need to check this box.

That's it! Hit the "**Share My Data**" button to complete your utility authorization.

© 2016 ENERGYai®

APPENDIX E
DRP Requirements for Solution 3

Appendix E: DRP Requirements for Solution 3

The DRPs, Mission:data, Olivine and UtilityAPI believe the following technical improvements must be incorporated into Solution 3.

The IOUs must provide a full data set and billing, interval and location data must be available synchronously.

OAUTH improvements:

1. Support authorizations to 2 or more DRPs for the same customer at the same time
2. The url that DRP redirects the user to should be the OAuth authorize url (as defined in OAuth 2.0 specification).
3. The IOU only redirects to authentication interface if needed, then redirects back to the original OAuth authorization url.
4. Authentication interface must be skipped if user already has valid authentication session cookie
5. Authentication interface must be able to allow password resets/reminders and still remain in authorization flow.
6. Authentication interface must be able to allow login credentials as authentication fields.
7. Authentication interface must have alternative instant authentication for users without logins (account#+zip, etc.).
8. Best case authorization interface must be 1-click "Authorize" button.
9. Default is all services are pre-selected and customer has to un-select the ones they want to exclude.
10. Redirected back to DRP with code after clicking "Authorize", no confirmation page on IOU.
11. Valid implementation of OAuth 2.0 Code Grant Flow per https://tools.ietf.org/html/rfc6749#section-4.1
12. Authorize url meets OAuth 2.0 spec per https://tools.ietf.org/html/rfc6749#section-4.1.1
13. Be able to handle state parameters, even through authentication interface.
14. Be able register multiple redirect_uris with IOUs so that DRPs can have testing/staging/production redirect_uris.
15. Be able to handle re-authorization for new code grant if DRP has lost previous code or access_token.
16. Be able to handle a user declining to authorize a DRP in both authentication and authorization interfaces.
17. Be able to redirect errors back to the DRP per https://tools.ietf.org/html/rfc6749#section-4.1.2.1

User experience:

1. The best-case number of clicks to complete the combined Authorization and Authentication step shall be at most **four**
    a. This assumes that the user can select the next field by pressing tab
    b. This assumes that the user will click in order to check any boxes
    c. This assumes that the user will click in order to select the first field on the authorization page
2. The best-case number of fields the user must complete for combined authorization and authentication step shall be at most **two**
3. The best-case number of unique pages or sections of a page that must load is at most **two**
4. The minimum number of form fields filled out by the customer shall be **two** fields used for Authentication.
5. No form fields shall be required to be filled out during the Authorization Step.
6. The Authentication step shall require one of the following sets of information to be typed into a form fields Username & Password or Service Account ID & Zipcode

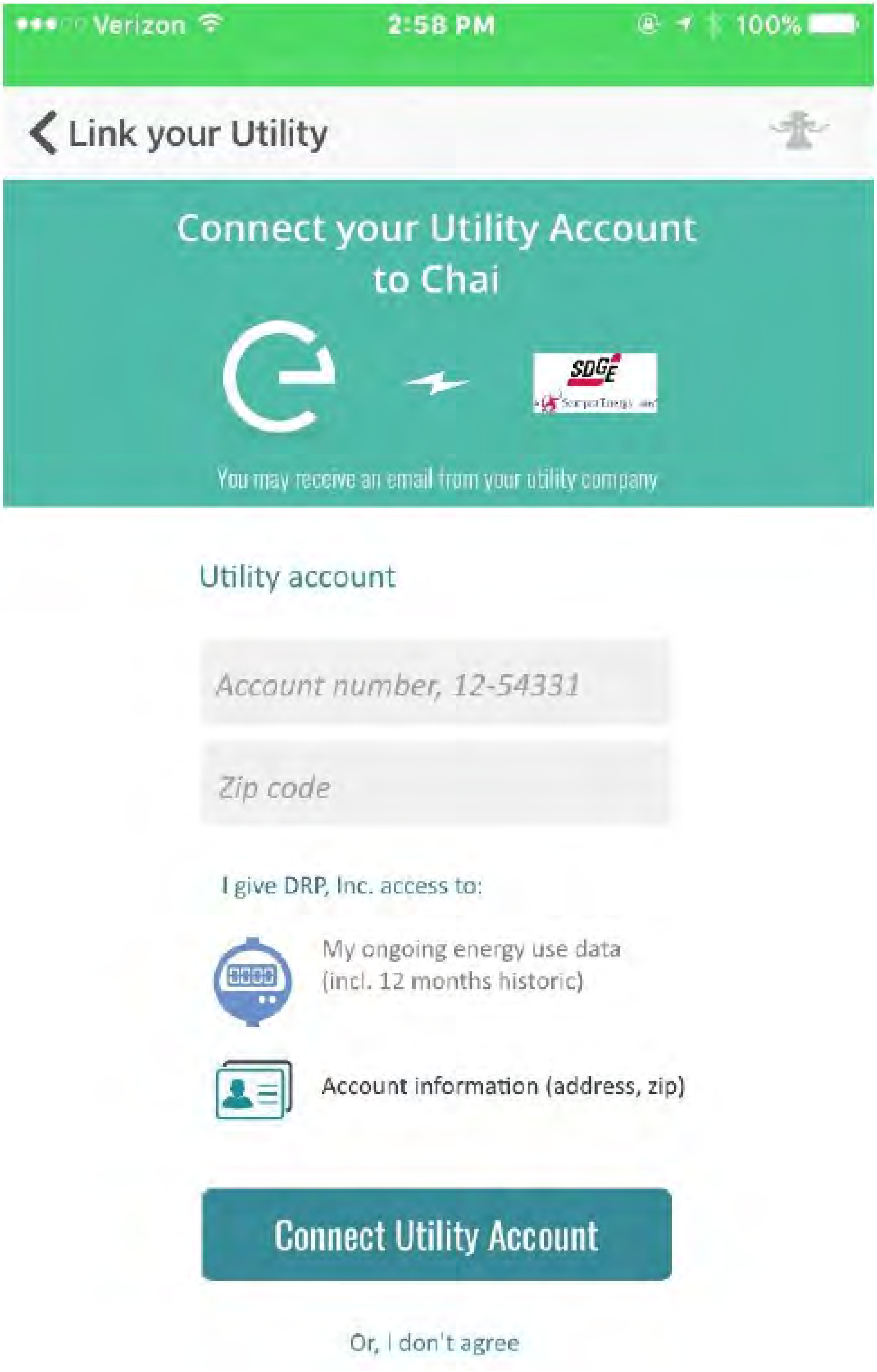
7. Ensure all form fields are properly HTML attributed such that browser-based username and password autofillers work (such as OnePassword or Apple's Keychain)
8. Reduce all legalese language while maintaining the availability of all legalese
9. Improve clarity of language that helps the majority of customers understand what they are agreeing to by using clear and concise plain English
10. Eliminate all "screen clutter" including any links, images, or space that does not directly related to helping the customer with rule 24 registration
11. When the page is displayed on mobile devices, all elements and fields required to complete the process shall be visible and interactable above 600 pixels below the top of the screen (or similar as dimensions may change and screen height/width ratios change)
12. When the page is displayed on desktop devices, all elements and fields required to complete the process shall be visible and interactable above 1000 pixels below the top of the screen (or similar as dimensions may change and screen height/width ratios change)
13. Do not allow the user to complete the Authorization process if they change configurations such that the DRP's service will no longer be viable given the modified configurations

Utility webpages' performance:
Part of streamlining customer enrollment in Solution 3 is the IOUs reporting on metrics and maintaining a high-performance, error-free customer experience. The longer web pages take to load, or the more errors that are seen, the fewer customers will enroll. Ongoing metrics should be tracked as described below. We encourage consideration of an independent group that can monitor these values objectively for all utilities and report them consistently across the state of California.

1. The IOUs shall track the following metrics on a per-user basis:
    a. Start Page
    b. Order of pages viewed
    c. Time on each page
    d. Last Page viewed
    e. Authorizations completed
2. These metrics shall be compiled, anonymized, and reported on a daily basis (the IOU could aggregate over
3. 10 users for the purpose of anonymizing the reported metrics).
4. The following aggregated values shall be reported:
    a. Load time per page
    b. Mean and max load time
    c. Standard deviation
    d. 90th percentile load time
5. Time spent between the first step and the last step
    a. Mean and max load time
    b. Standard deviation
    c. 90th percentile load time
6. Number of views per page (tracked daily)
7. Number of unique user views per page (tracked daily)

APPENDIX F
Example of user experience using Solution 1 (one screen)

Appendix F: Example of user experience using Solution 1 (one screen)



Link your Utility

Connect your Utility Account to Chai

You may receive an email from your utility company

Utility account

Account number, 12-54331

Zip code

I give DRP, Inc. access to:

My ongoing energy use data (incl. 12 months historic)

Account information (address, zip)

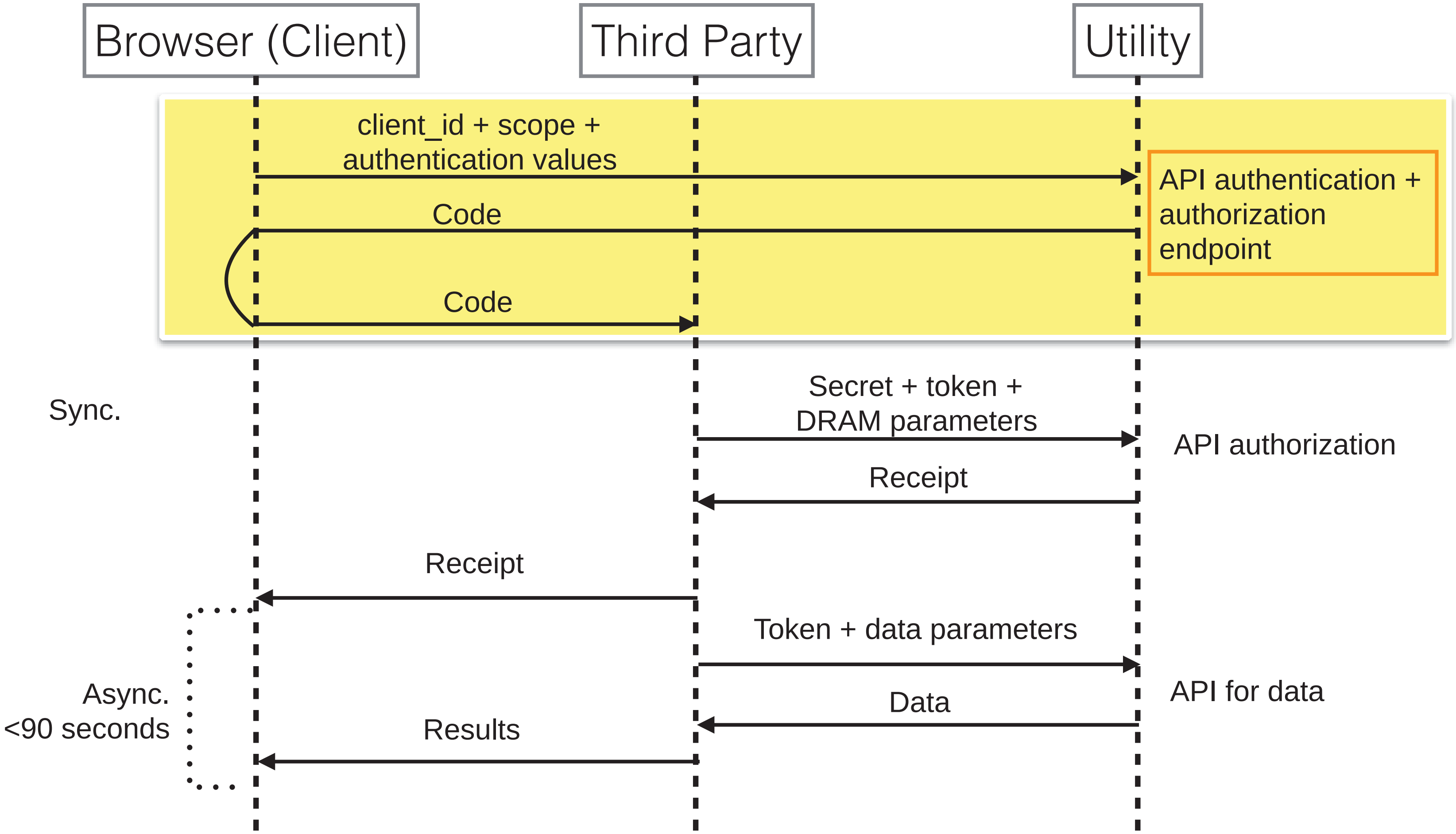
Or, I don't agree

APPENDIX G
Proposed Combined Solution for Click-through Implementation

Proposed Combined Solution for Click-through Implementation

API - Solution 1

Utility authenticates - either via login or account #



Browser (Client)

Third Party

Utility

client_id + scope + authentication values

API authentication + authorization endpoint

Code

Code

Sync.

Secret + token + DRAM parameters

API authorization

Receipt

Receipt

Token + data parameters

Async. <90 seconds

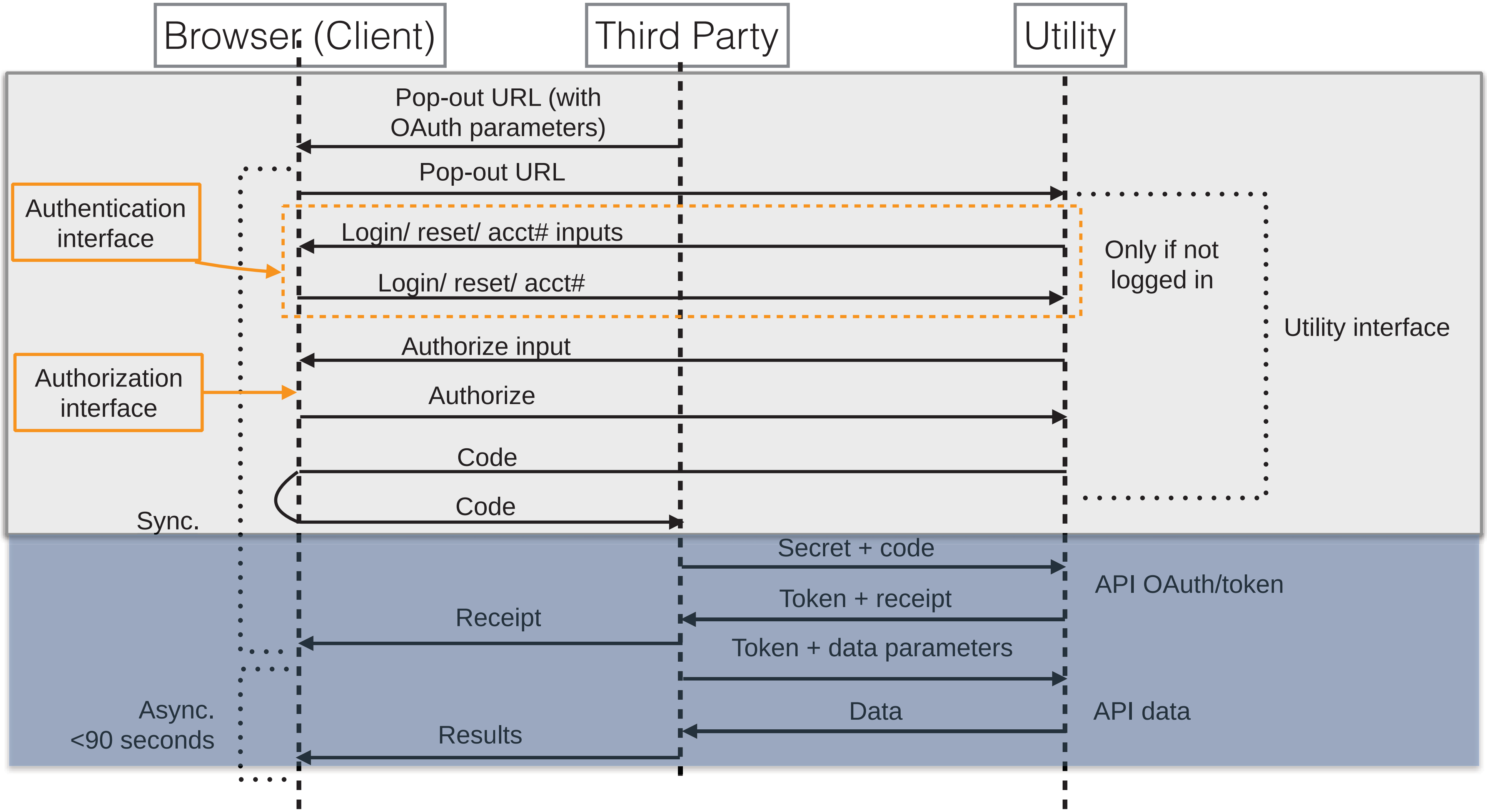
API for data

Data

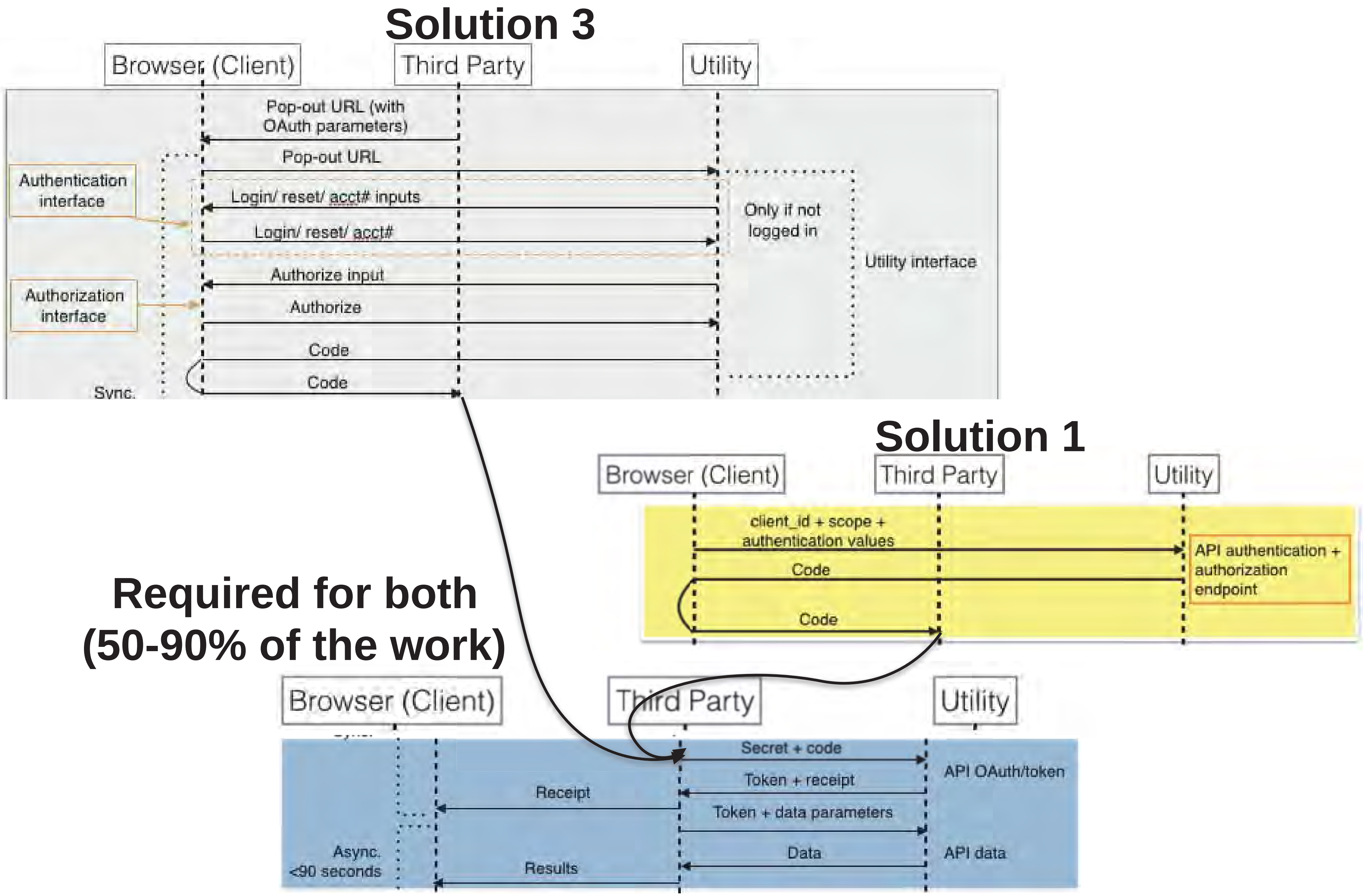
Results

OAuth Solution 3

Pop Out or iFrame (OAuth) - Pop-out to Utility website, Utility authenticates - either via login, account # or cookie



Combined solution



Solution 3

Browser (Client)
Third Party
Utility
Pop-out URL (with OAuth parameters)
Pop-out URL
Authentication interface
Login/ reset/ acct# inputs
Login/ reset/ acct#
Only if not logged in
Utility interface
Authorization interface
Authorize input
Authorize
Code
Code
Sync.

Solution 1

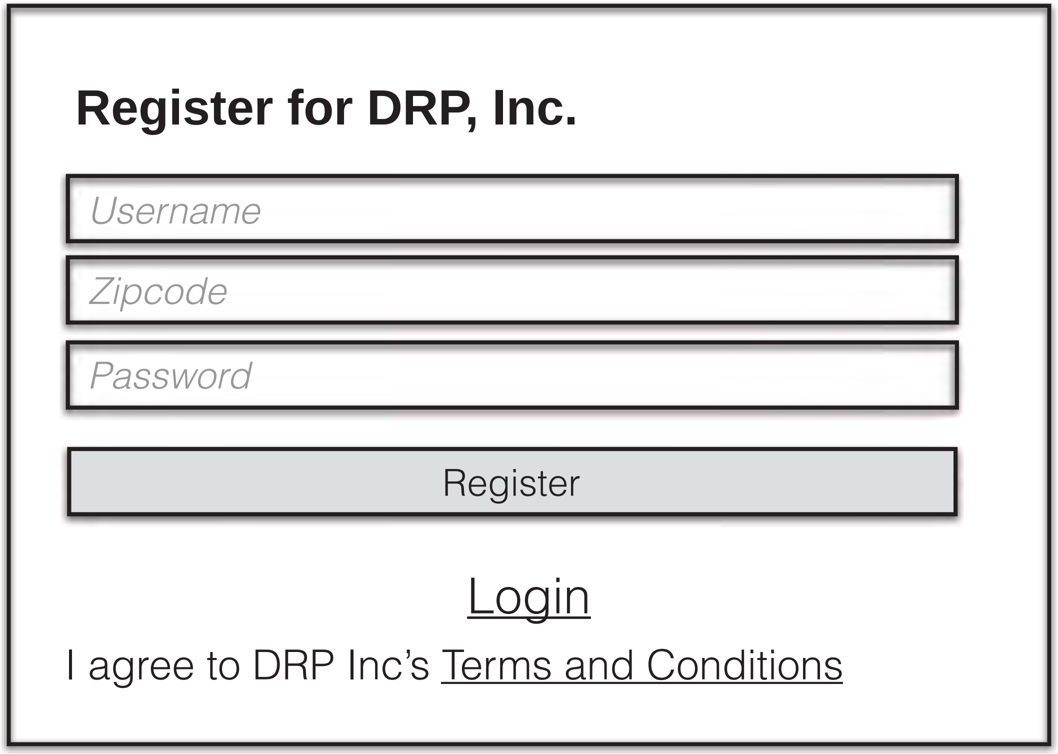
Browser (Client)
Third Party
Utility
client_id + scope + authentication values
API authentication + authorization endpoint
Code
Code

Required for both (50-90% of the work)

Browser (Client)
Third Party
Utility
Secret + code
API OAuth/token
Token + receipt
Receipt
Token + data parameters
Data
API data
Async. <90 seconds
Results

APPENDIX H
Third Party Enrollment

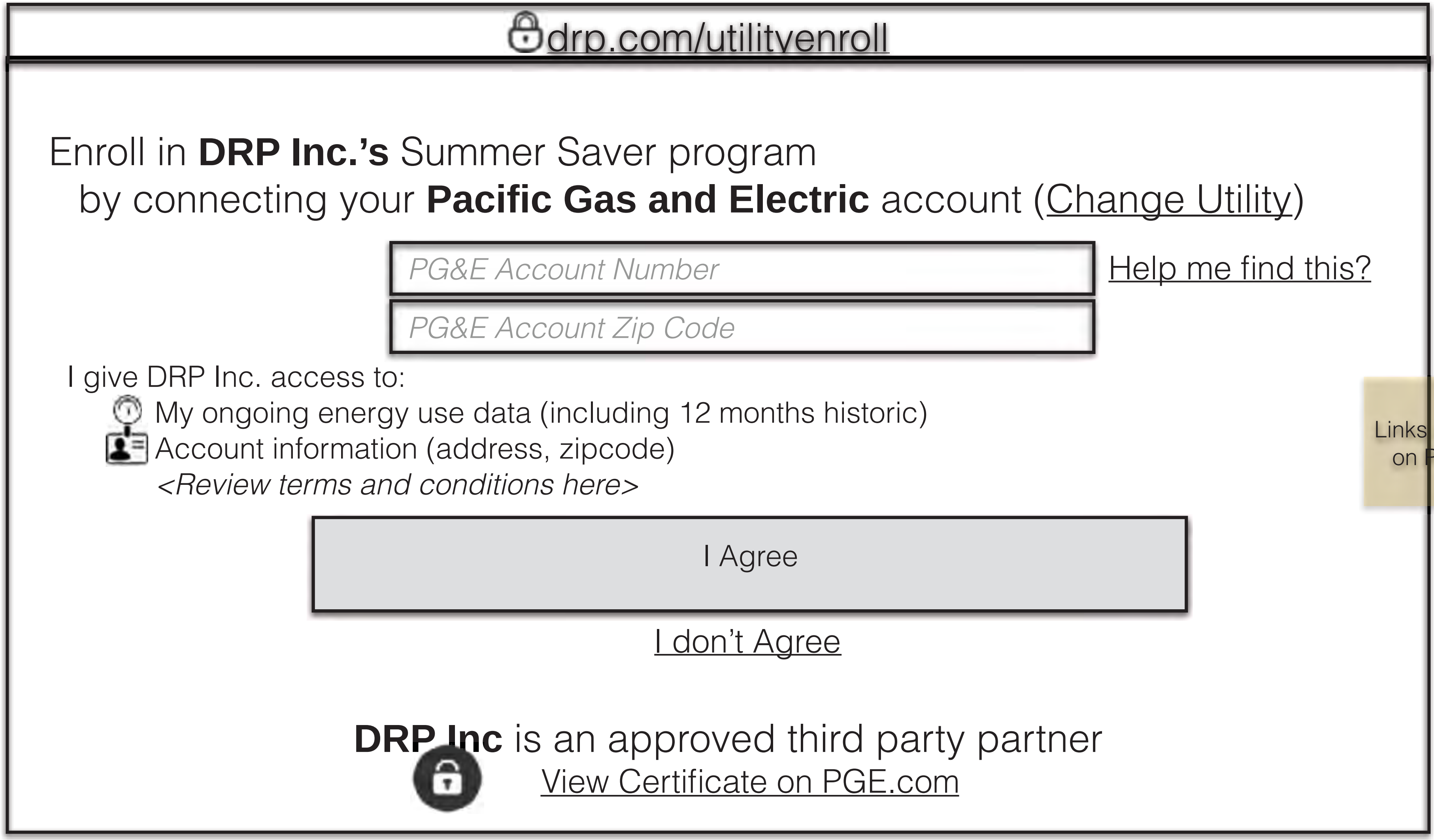
Third Party Enrollment



Register for DRP, Inc.

I agree to DRP Inc’s Terms and Conditions

Authentication and Authorization v1



drp.com/utilityenroll

Enroll in **DRP Inc.'s** Summer Saver program
by connecting your **Pacific Gas and Electric** account (Change Utility)

PG&E Account Number

Help me find this?

PG&E Account Zip Code

I give DRP Inc. access to:

- My ongoing energy use data (including 12 months historic)
- Account information (address, zipcode)

<Review terms and conditions here>

I Agree

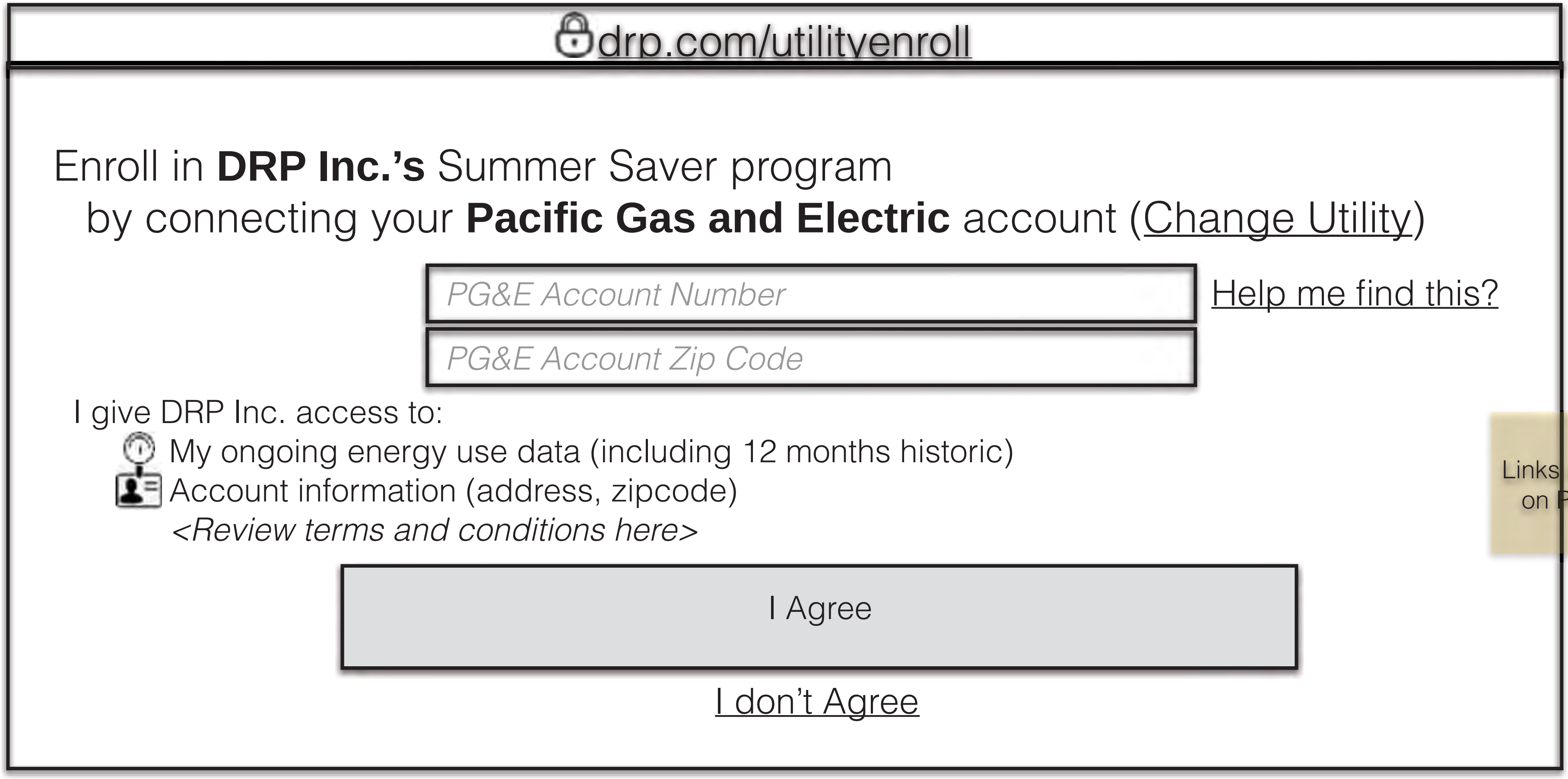
I don't Agree

DRP Inc is an approved third party partner
View Certificate on PGE.com

Links out to T&Cs on PG&E.com

Links out to third party partner page

Authentication and Authorization v2



drp.com/utilityenroll

Enroll in **DRP Inc.'s** Summer Saver program
by connecting your **Pacific Gas and Electric** account (Change Utility)

PG&E Account Number — Help me find this?

PG&E Account Zip Code

I give DRP Inc. access to:

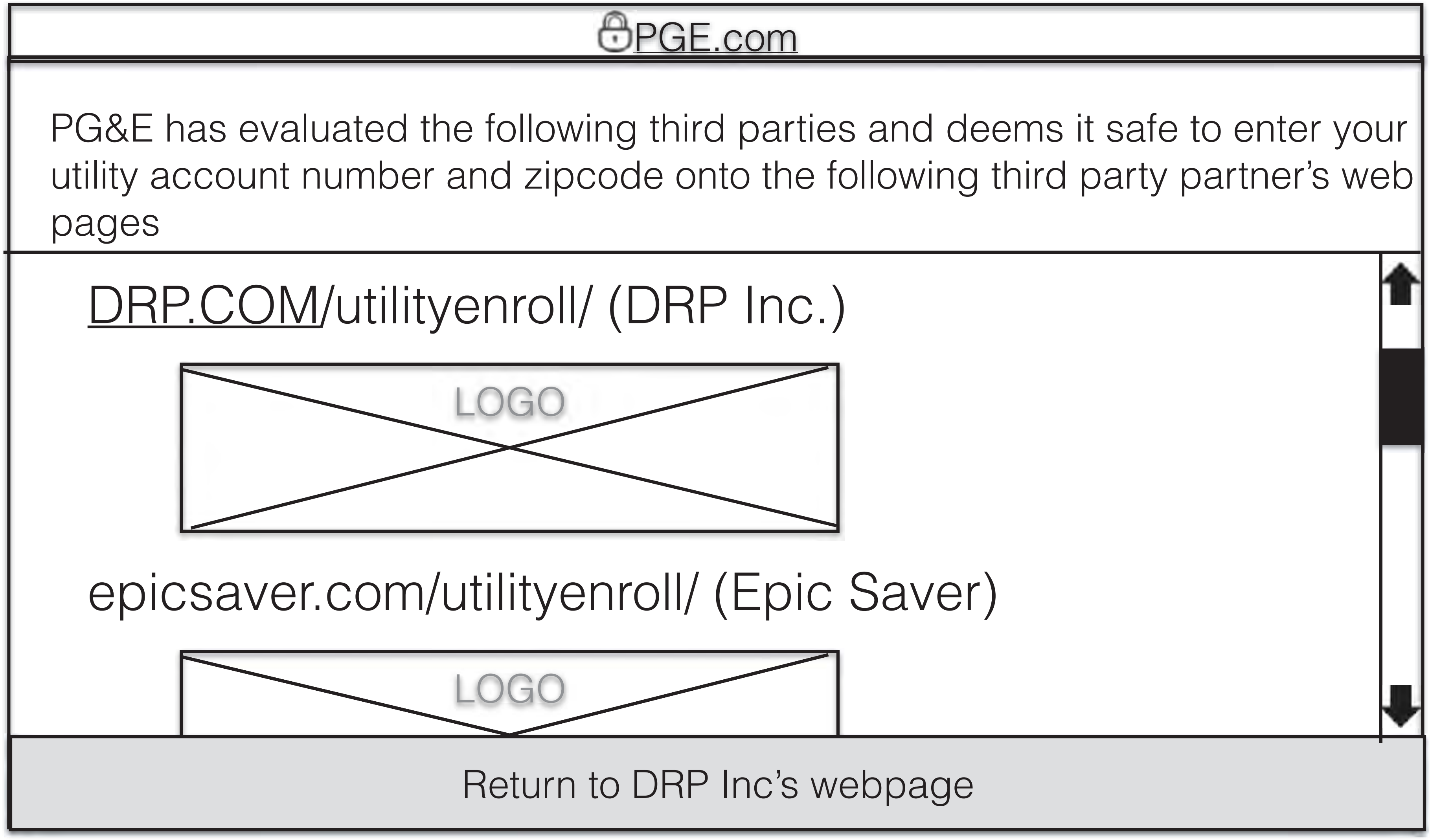
My ongoing energy use data (including 12 months historic)
Account information (address, zipcode)
<Review terms and conditions here>

I Agree

I don't Agree

Links out to T&Cs on PG&E.com

PG&E Third Party Partner Page



PGE.com

PG&E has evaluated the following third parties and deems it safe to enter your utility account number and zipcode onto the following third party partner’s web pages

DRP.COM/utilityenroll/ (DRP Inc.)

epicsaver.com/utilityenroll/ (Epic Saver)