INVENTION DISCLOSURE

1. **Invention Title.**

A way to anonymize transaction data in B2B2C scenarios.

2. **Invention Summary.**
Mechanisms to ensure anonymity of transaction data, while retaining the ability to authenticate/authorize/troubleshoot the transactions themselves – for use in partnership-based B2B2C offerings (e.g., heath care).

3. **Invention Description**.

a. Describe the invention in detail.

Business-to-Business-to-Consumer (B2B2C) offerings are instances where a Platform Provider (e.g., Cable Company) partners with another Service Provider (e.g., health care clinic, energy utility) who offers services (e.g., chronic health care monitoring) to end-consumers (residential or business). In this setting, the platform provider manages any consumer devices (e.g. health sensors, energy meters), the platform that connects to these devices, and – potentially - the network over which the devices connect to the platform.

In such examples, there are cases where the platform provider may choose (or be requested) to not have access to any communication between the partner service provider and the end-consumer devices - but still be able to manage and troubleshoot the devices and their features. While this seems easy enough, mechanisms such as tunnels don't really assist with real-time monitoring and troubleshooting of potential issues or effective routing by the platform provider (e.g., when you have multiple entities that receive different kinds of information from the same end-device).

Speaking of troubleshooting, for real anonymity, there is a need to ensure that platform provider's employees (e.g., customer service reps) cannot infer any information from the collected data, esp., over a period in time. There's also the concern that too much anonymity will impact management and troubleshooting.

Here's an example: a cable company partners with ABC Health Care to offer a monitoring service for post-operative care. The patient is provided with a few different sensors (blood pressure monitor, respiratory sensors) prior to being discharged. The patient is asked to use them a couple of times of day – and this data is transferred via the cable company's platform to ABC health care. If there are any issues with the devices then the cable company takes care of it. However, to be able to do so, the cable company may need to know when the data was collected, what kind of devices where in use, and whether the devices remained accurately calibrated etc. Customer service representatives, who should not have access to the actual data, may access this management data. However, if they are able to tie the information to a specific customer, they may be able to narrow down the patient's condition – and

INVENTION DISCLOSURE

cause privacy concerns. For instance, spirometer data collection on a regular basis may imply conditions such as COPD.

--- Idea

This invention disclosure proposes an architecture and interfaces to address such situations, by providing mechanisms that anonymize the consumers and the transactions from the platform provider – while retaining necessary security properties (authentication, authorization, integrity protection, non-repudiation etc.).

The crux of the disclosure is the following:

Consideration 1. *Mechanism to share temporary credentials (e.g., username, password) to the end-user system so that the transactions can be authenticated independently by the platform provider, but not over time (which would be easy if one used permanent credentials).*

Consideration 2. *Mechanism to obfuscate the end-user network connection (e.g., IP address) so that they cannot be implicitly recognized.*

Consideration 3. *Mechanism to retrieve associations for the service provider to recreate transaction to user association for full access to all the data.*

--- Architecture

This invention presents the following logical entities:

End-user System
Management System
Credential Store
Credential Coordinator;
User Database; and,
Network Translation Device.

INVENTION DISCLOSURE

Figure *depicts these entities, and interactions that are relevant to this disclosure.*

Figure : Components

The premise is that the End-User system (controls and/or sensors) has two secure interfaces: one with the service provider (e.g., health care system) and one with the platform provider (e.g., cable company). These interfaces are disambiguated by where the interfaces terminate, since they both pass through the provider's access network.

Here are the functional requirements for each of the systems.

End-user System

- *The system is capable of mutually authenticating itself to the Platform Provider AND the Service Provider.*

INVENTION DISCLOSURE

  - *This is done via pre-configured credentials (one or more) or via the use of a mechanisms, such as X.509 certificates using Public Key Infrastructure (PKI)*
- *The end-user system is capable of receiving, securely storing and using temporary identities and credentials that may be specific to one or more operational transactions (but not every transaction).*

Credential Store and Coordinator

- *The store is responsible for creating a bunch of 'temporary identities and credentials' (e.g., temporary username and pre-shared key) that are associated with each end-consumer. This is stored in a database.*
- *The coordinator can reverse-map temporary identities and credentials to point to real user end-consumers.*

The behavior defined by this disclosure is as follows:

STEP 1:

- *The end-user system, when first configured, establishes a secure (mutually authenticated, integrity and privacy protected) connection with the platform provider's credential store*
- *The credential store then gives it a set of temporary identities and credentials, and stores this mapping in a database*

STEP 2:

- *Whenever the end-user system needs to communicate with the platform provider (e.g., to send notifications) it creates messages with the components illustratively indicated in* Figure .

INVENTION DISCLOSURE

Figure : Message Components (Logical)

- The Platform provider is able to access components #1 and #2, and can route #2 and #3 to the service provider.

- *Component #2 is used to tie the data elements together in case the transaction needs to be revisited, and also for the Service Provider to recognize the sender (and to decrypt the sensitive data using the credentials associated with the user name).*

- *At the same time, this message is received by an 'intermediary' that does not have access to any of the two credentials and its job is to modify the network address of the end-device (e.g., IP, Mac) with a different one (e.g., it's own). This may be accomplished via a Network Address Translation (NAT) box.*
  - *The intermediary "may" remember the mapping by tagging the message in* Figure *with a "pseudo-random" (non-repeatable, or periodic) identifier (and time stamp if it is periodic) that maps to the originator of the message to the end-device.*

STEP 3:

- *The Service Provider who receives #2 and #3 can then use the database to figure out the associated credentials (for decryption) and to identify the end-user system (and the end-user).*

--- *What do these steps do?*

When the Platform provider (e.g., cable provider) obtains the notifications from the end-devices, it neither has access to sensitive information nor does it know which specific end-device sent this information (exceptions are when there is only one deployed device).

Note: This also requires that Component #1 in Figure *does not include any information that identifies the end-device or the consumer.*

However, it does get access to the device management information and can be immediately alerted to take any necessary steps. It can also filter data in cases where the messages need to be filtered based on parameters, such as: destination (e.g., care giver, doctor) or classification (without the actual data).

--- *Security Credentials and associated considerations*

Examples of the kinds of temporary identities are:

- *Username (e.g., login, name, identifier) of the end-user*
- *Device identifier (e.g., mac address) of the ES*

Examples of credentials associated with these identities include:

- *passwords*
- *pre-shared keys*
- *certificates*

The following table describes a few options for these temporary credentials.

#	Mechanism	Notes
1	Temporary identities and credentials that are not time bound	All identities are unique and there is a 1-to-1 correlation.
2	Temporary identities and credentials that are time bound	Identities can overlap across end devices, and hence there is a need for identities AND their validity periods to be shared and stored in the database.

Temporary identities and credentials are repeated periodically, and each transaction can provide a bunch of temporary identities, any of which can be used in a pseudo-random or cyclical manner

--- *Components from* Figure

The components and their boundaries are meant to be illustrative. For instance, the Platform provider may be the one who provides the credential store and coordinator, but not have access to its data or interfaces. The intermediary could be part of the service provider if there are sufficient policies to prevent the same people from having access to both the management and network translation device. It could also be in the service provider network.

INVENTION DISCLOSURE

b. Why was the invention developed? What problem(s) does the invention solve? How is it better?
The above invention can help cable operators who wish to provide services, such as energy management or health care.

c. Briefly outline the potential commercial value and customers of the invention.
Allowing for such a mechanism can allow MSOs to safely support B2B2C services, without fear of Customer Support or Backoffice Management personnel from gaining unauthorized access to end-user data. This may be a consideration for those worried about regulatory requirements (e.g., HIPAA).

4. **HOW is this invention different from existing products, processes, systems?**
The alternatives to this are simple:
- *Don't worry about access issues (e.g., platform providers may assume responsibility for the sensitive data)*
- *Use policies instead of technology to obfuscate the data*
- *Use technical alternatives, such as tunnels; which may be hard to troubleshoot and manage*

This disclosure allows for the platform provider to technically separate sensitive data, yet have troubleshooting and management capabilities.