AUTHORITI™

Inside the **Authoriti Permission Code®** Platform

Principles of the Disruptive Model for Authorizing Transactions

In the Authoriti model, the customer is able to control the use of his or her information instead of worrying about keeping it a secret. Institutions that process the information have confidence that the real owner authorized its use for the intended purpose. Significantly, the chance of fraud or misuse is dramatically reduced. Rather than merely shifting risk, our model seeks to eliminate risk.

The cornerstone of the model is the Authoriti Permission Code® PIN. Four key principles guided the system design:

1. **Clear separation.** Identification, Authentication and Authorization capabilities are completely separated from one another in the Authoriti Permission Code PIN.

2. **Customer control.** The Permission Code platform allows customers to restrict the authorized use of their data, and not persist over time.

3. **No new weaknesses.** The Permission Code service doesn't create any new, attackable stores of data.

4. **Easy adoption.** The Permission Code system can be implemented without major disruption to existing transaction systems.

With these principles in mind, we developed a completely new model from the ground up. The Authoriti Permission Code platform provides customer-controlled, permission-based use of sensitive information and Personally Identifiable Information (PII) such as user IDs, passwords, Social Security Numbers, account numbers, and credit card numbers.

As shown in Figure 1, the customer generates and submits a Permission Code PIN to the institution along with their authorized transaction detail. The institution makes simple automated web service call to Authoriti, who validates that the correct user generated the PIN, and that the PIN authorizes the transaction's specific details such that the institution can execute in confidence.

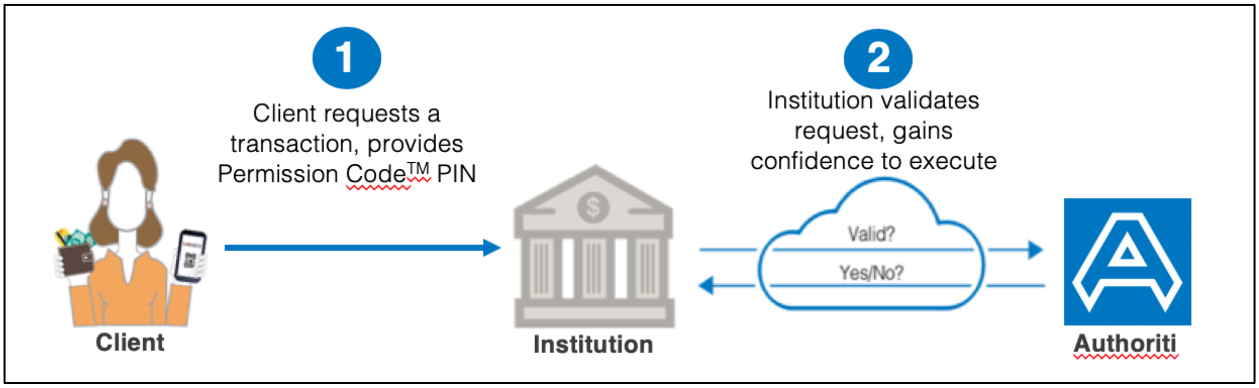
1
Client requests a transaction, provides Permission Code™ PIN
2
Institution validates request, gains confidence to execute
Valid?
Yes/No?
Client
Institution
Authoriti

Figure 1. Authoriti's Permission Code PIN answers one question: Is this transaction authorized?

The model goes beyond just authenticating identity – Authoriti also confirms that a specific transaction and/or the use of specific information was authorized by its owner.

Authoriti infrastructure ensures that the use of consumer identifiers, such as SSNs, is authorized, even if the identifier itself has become widely known. We use patent-pending techniques that allow companies and consumers to control how their information is used, rather trying to keep it secret.

The Permission Code smart PIN

Because the Permission Code smart PIN is originated by the user on their smartphone device, it can be embedded with user-defined details and restrictions (for example, who can use specific information and how). The Authoriti user authenticates him or herself to the device, sets the desired transaction terms or data restrictions, and creates the Permission Code smart PIN that authorizes use.

Unlike traditional passwords and both static and one-time PINs, Permission Code smart PINs are encrypted and digitally signed using PKI (Public Key Infrastructure) to eliminate the risk of tampering. Further, because they include transaction details (see Figure 2. for detail), the PINs cannot be repurposed or redirected for an unintended use. This smart, content-rich structure also eliminates the need for a centralized entity to generate, remember, and protect valid PINs.

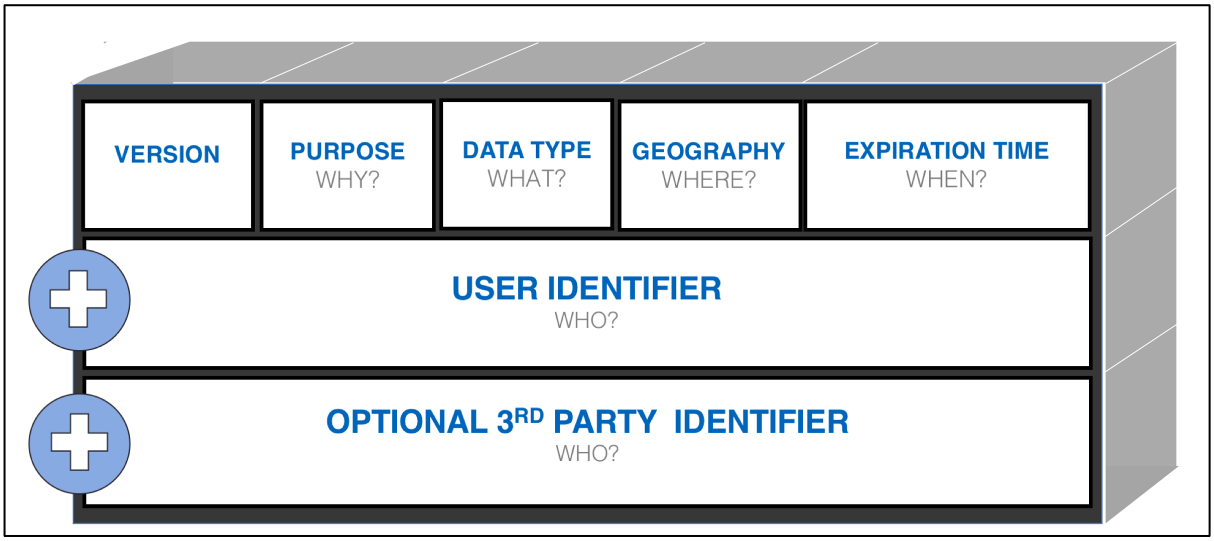

Figure 2. The transaction parameters are packed into the 10-digit Permission Code PIN

A user may choose to restrict a Permission Code PIN's validity to a specific period of time, to be available only for use within a certain geography, or only when presented by themselves or a specific third-party. For example, he or she may allow a SSN to be used for medical insurance billing but not for opening a new credit card.

Users can generate Permission Code PINs whenever and wherever they choose, no Internet access is required after the initial registration, and because the transaction details embedded in the PIN are digitally signed, Permission Code PINs can be distributed through any channel.

The business receiving the instruction from its customer simply captures and tests the Permission Code PIN through Authoriti. Capture can be input manually, scanned, or automated. Validating the code is generally done at the time of capture, which is simplest and most natural to the consumer, but can also be in subsequent batch processing. Authoriti customers are provided with a simple API that is easily callable from their existing applications. Authoriti unpacks the Permission Code PIN, checks for correctness (correctly signed, and not revoked, already used, or expired), and matches the transaction details against the embedded information. Dependent on the outcome of that testing, Authoriti returns an indication of Pass or Fail for the validation.

Permission Code PINs may be logged, but don't need to be stored by the receiving entity. This simplifies adoption by only requiring code capture and checking in the user interface – without requiring changes to the back end or to databases.

Who Benefits from the new Authoriti Model?

There are three beneficiaries of the new model:

- Customers (Consumers or Commercial) – By controlling the transaction, customers will value the comfort of knowing that their information can't be misused.
- Businesses (e.g. Financial Institutions) – Financial entities will gain very real reputational and economic benefits. The definitive Permission Code PIN prevents fraud more effectively, without rejecting valid transactions, than the behavioral models that are being developed.
- Data Holders and Aggregators – Entities that wish to collect and share information about consumers will know that the specific type of data is authorized for release in each and every instance, without the need to hold and secure the consumers' sensitive PII.

Inside the Permission Code Platform

Users download an app from the Apple App Store or Google Play, as appropriate for their device. The app can be Authoriti's primary build, a standalone build that is customized and branded for the business, or the partner company's mobile app with Authoriti's SDK.

The app contains a digital wallet which is held on the user's device in an encrypted store. This wallet includes a PKI private key for signing Permission Codes, with a corresponding public key stored in the Authoriti servers. The wallet and app also include one-way hashes of the user's account numbers. Unhashed account numbers are never know by any part of the Authoriti system, and the private key never leaves the user's device.

Users go through a one-time registration process, with two methods available: 1) Pre-Registration, or 2) Self-Registration with identity proofing.

The Pre-Registration process is used by existing clients of a partner company. The user opens the app, is prompted to enter a User ID and User Password provided by the company, and then asked whether to allow biometric access to the app. This completes the bulk registration process. The user may immediately use the app to generate Permission Code PINs authorizing transactions as their relevant accounts and information have simultaneously been downloaded into the device's digital wallet.

Pre-registration relies on the company's prior onboarding of the user. Hashes of the user's ID, password, and account numbers are submitted to Authoriti (through an API or web portal) in advance of the user registration. For added upfront security, the user could also be required to go through the self-registration process at the time of pre-registration.

Self-Registration is generally used by new clients of a company. The user opens the app, creates a password, and is then directed through the identification process (which includes taking pictures of their government issued ID like a state driver license and a "proof of liveness" selfie). Upon completion of identification, the user may choose to allow biometric access to the app. This completes the self-registration. The user may begin to populate their digital wallet with accounts and data to be used for future transaction authorizations. Adding information to the wallet can be completed through either direct entry or cloud downloads of hashed account information from a partner company.

After registration, whether through self- or pre-registration, additional accounts and information may be added to the user's wallet through either the direct entry or cloud download process. Of note, the wallet can hold multiple accounts from the same company as well as accounts from multiple different partner companies.

Public Key Infrastructure (PKI)

PKI is a well-respected security technique. Rather than sharing a password between someone who needs to be authenticated and someone who needs to verify authentication, PKI creates a pair of keys: one called Private and one called Public.

The Authoriti app creates a unique PKI key pair within the user's device at the time of registration. The private key, which is used to encrypt and digitally sign the Permission Code PINs, is stored locally and never leaves the device's wallet. Authoriti never has or stores private keys. The user's device holding the private key acts as a decentralized factor in our multi-factor authorization system.

The public key is transferred to Authoriti's servers where is can be used to check the signature and decrypt the PIN – validating that the signature was indeed from the ID who owns the private key and the request transaction's details are correct. The public key cannot create a valid signature.

Security and Resiliency

Validation of the Permission Code PIN is conducted via a RESTful API service call from the institution to Authoriti. The company provides Authoriti with the encrypted Permission Code PIN, a hashed account number, and other hashed parameters to be checked (e.g. wiring instructions). In addition to the data being hashed, the API service is authenticated and the request transmitted over https.

Authoriti does not hold centralized data sets of currently valid Permission Code PINs, nor maintain central servers with unhashed PII and other sensitive account information. All sensitive account data held by Authoriti is hashed and salted. Unhashed account numbers are never known by Authoriti. Should anyone ever steal information from Authoriti's servers, they would have an extremely hard time using it. That's the problem that we solve.

The Authoriti service is built on Amazon's AWS infrastructure. We are creating multiple instances that leverage AWS East and West, and can failover as needed. The Amazon Lambda compute service is being utilized to ensure scalability and robust performance with low processing latency. The Authoriti APIs are network scanned by a 3rd party service for vulnerabilities, and the Lambdas and related software continuously monitored for unauthorized changes. Synthetic transactions against the service are performed on an ongoing basis to ensure availability.

Summary

As shown in Figure 3, the Authoriti Permission Code PIN has several advantages over other PINs. By putting control in the hands of the customer, Authoriti provides confidence that every transaction is authorized.

Authorization confidence ↑

	VALIDATES SECRET ACCESS CODE	EXPIRES	CHANGES	LIMITS BY TIME, PLACE, BUSINESS TYPE, ETC.	CONSUMER AUTHORIZED TRANSACTIONS	NO MASSIVE DATA STORE
Authoriti Permission Code	✓	✓	✓	✓	✓	✓
One Time PINS	✓	✓	✓			
Fixed PIN (Debit)	✓					
No PIN						

Figure 3. Advantages of the Authoriti Permission Code platform versus other models.

About the Authoriti Network

The Authoriti Network was founded in 2017 to identify new approaches to prevent misuse of Identifiers and Personally Identifiable Information. Our founders have significant leadership experience dealing with InfoSec at-scale at the world's leading financial institutions. Authoriti develops the Authoriti Permission Code®, which puts control of transactions in the hands of the consumer and gives institutions the confidence that the transactions are authorized. Please visit us at Authoriti.Net.