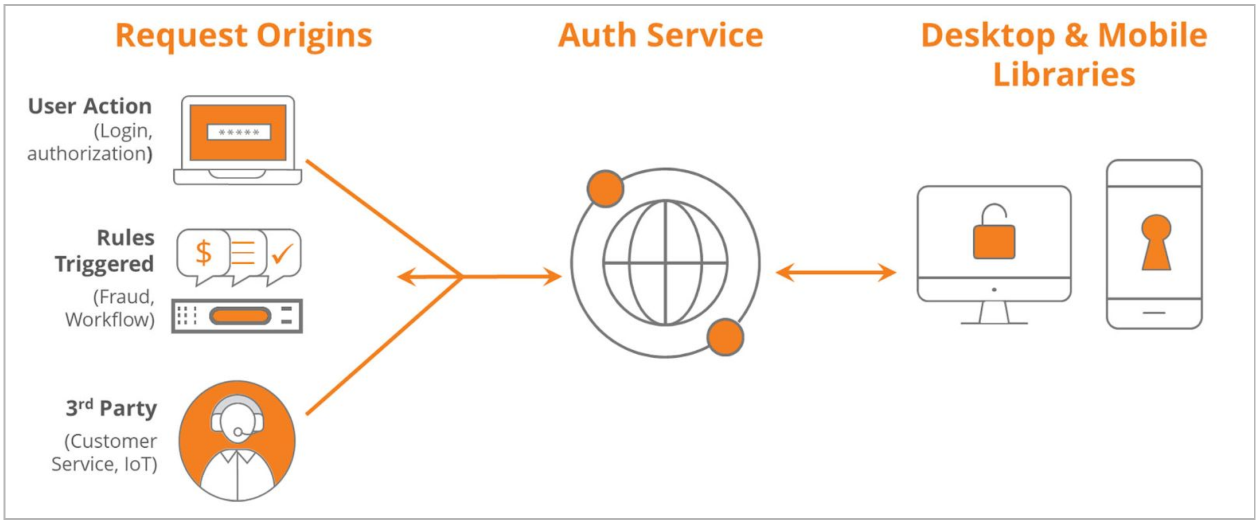
Privakey CX Technical Overview

Privakey CX is a licensable product that allows services to deploy Privakey's core technology in their existing mobile and desktop application. By employing simple platform libraries and a centralized Auth Service, existing end-user application are transformed into consistent, user-friendly, omni-channel authenticators and process authorizers.

Component Architecture



Privakey's architecture is comprised of a Mobile Library and an Auth Service that interacts with services' pre-existing processes (Request Origins).

The Mobile Library is leveraged to develop apps or, more likely, extend the capabilities of existing apps to enable Privakey Authentication and Authorization. Once employed, the libraries handle device registration, cryptographic key generation and secure storage, request/challenge receipt and handling, revocation, and suspension.

The Auth Service is a RESTful service that can be called by any Request Origin (authorized and authenticated service) to invoke user-specific Authentication and Authorization Challenges. It also federates those challenges to registered user devices and brokers the interaction between the Privakey enabled devices and the services that initiated requests/challenges.

Component Descriptions

Request Origins (Existing Services)

The request origins are the current processes and workflows of an application or service that would benefit from strong and definitive user authorization.

Any authorized, internet-connected service that can interact with the Auth Service can behave as a Request Origin. They can be an application authentication flow, fraud triggers, or workflow processes.

Request Origins interact with the Privakey CX Auth Service by calling a secure, RESTful interface.

Privakey CX Auth Service

The Privakey CX Auth Service is a simple, headless web application that exposes an API. It is the central hub in a licensed CX deployment.

The Privakey CX Auth Service registers and maintains users and their devices (interacting with Privakey App Library components) and interacts with Request Origins, receiving and responding to requests. It does this via RESTful interface and brokers the response from the users' registered devices by federating requests and validating the returned responses.

The Privakey CX Auth Service maintains limited information in its own data structure. This includes user information (Privakey GUID, Service GUID), device information (device IDs, public keys, and encryption information) and request information (requests' content, digitally signed requests' results).

Privakey CX App Library

The Privakey CX App Library allows app developers to rapidly incorporate Privakey Authentication and Authorization in their existing or planned applications. The App Library performs a number of functions, including:

- Binding a device to the Auth Service
- Securing connections to the Auth Service
- Managing PINs and Biometric factors
- Generating and rotating RSA-2048 asymmetric key-pairs
- Securely storing private keys (in hardware key stores or in memory)
- Receiving and processing request challenges from the CX Auth Service.
- Receiving and processing key encryption material delivered out-of-band in notification streams
- Processing challenge responses (Approve and Reject)

Implementing Privakey CX

Privakey CX is designed to provide implementation and roll-out flexibility. In its most complete manifestation, Privakey CX could be used to do away with passwords altogether - creating a secure, easy and password-free way for users to authenticate and authorize events, across all of a service's consumer channels.

But, recognizing such a shift may seem too disruptive for services and their users, the core elements of Privakey can be leveraged for several, more limited use cases including: step-up authentication; strong event verification; and user-opt-in enhanced security and convenience. Once users switch to using Privakey in this more limited fashion, the service can expand the scenarios in which it is employed.

Whichever path a service takes, implementing the core of Privakey is straightforward and simple.

Integration Overview

Regardless of how a service chooses to implement Privakey, the basics remain the same:

1. Deploy Privakey CX Auth Service
    a. Optionally Implement Notifications
2. Integrate Privakey CX App Library
3. Connect Request Origins

We provide different, more in-depth documentation for each of these steps, because it’s possible a different developer will be implementing each one. A quick description of each step and a link to its more thorough documentation follows.

Deploy Privakey CX Auth Service

This document describes the process of deploying the Privakey CX Auth Service into your environment:
https://s3.amazonaws.com/cx.docs.privakey.com/server-deployment.pdf

If you do not want to use the PrivakeyCX Comm Server, and instead want to use your own method of sending notifications, this document explains how the data will be sent to you:
https://s3.amazonaws.com/cx.docs.privakey.com/notification-interface.pdf

Integrate Privakey CX App Library

This document describes the process of implementing the Privakey CX App Library into your own Android app: https://s3.amazonaws.com/cx.docs.privakey.com/android-library.pdf

Connect Request Origins

This document describes the process of hooking up your new or existing Request Origin(s) with the deployed Privakey CX Auth Service. It also provides documentation on each API call you may need to make: https://documenter.getpostman.com/view/384357/RWEfNeky