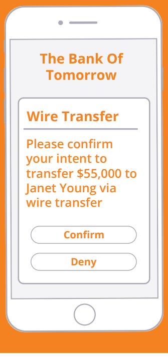
Privakey CX for Linux on IBM Z

Multi-Factor Authentication and Intent Verification Solution

Contextual - Single Step - Interactive



The Bank Of Tomorrow

Wire Transfer

Please confirm your intent to transfer $55,000 to Janet Young via wire transfer

Privakey CX offers a next generation utility for multi-factor authentication and transaction intent verification on IBM Z. Combining authentication and authorization into a single action, Privakey enhances the user experience of high value/high risk interactions while ensuring strong identity confirmation.

An Elegant User Experience

- Eliminates inconvenient and expensive hard tokens
- Simple and contextual messages
- Utilizes friendly mobile biometrics

Optimized for IBM Z

- Operates in an IBM Secure Service Container
- Combines authentication and authorization into one user action

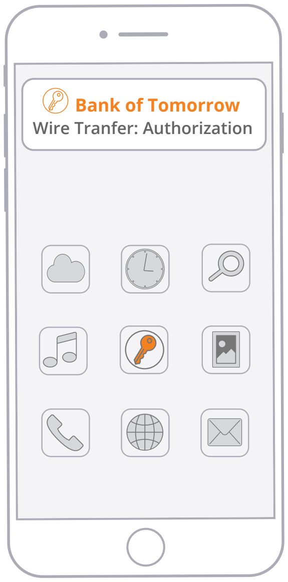
How It Works

Secure Notifications: Any authorized service can connect to Privakey's API to deliver users secure, push notifications. Privakey only sends notifications to users' devices that are cryptographically bound to their accounts.

Contextually Rich Messages: Upon receiving a challenge, users will be presented with a context rich message that clearly communicates a required response. Content can include HTML, documents and interactive forms.

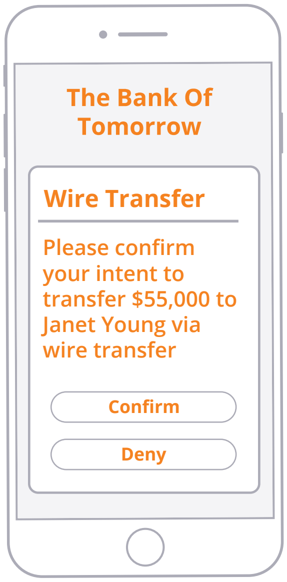
Biometric Identity Confirmation: Users assert a biometric gesture or pin to confirm their response to a challenge. Privakey's mobile libraries access bound private keys and sign the users' response, ensuring its integrity and non-repudiation. Encrypted and digitally signed response returned to the initiating service.

The Privakey User Experience



Bank of Tomorrow
Wire Tranfer: Authorization

User receives push notification

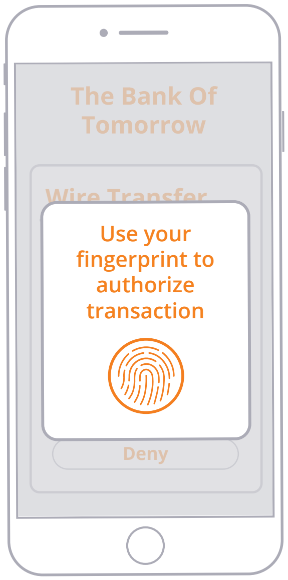


The Bank Of Tomorrow

Wire Transfer

Please confirm your intent to transfer $55,000 to Janet Young via wire transfer

Reviews & responds to Privakey challenge



The Bank Of Tomorrow

Wire Transfer

Use your fingerprint to authorize transaction

User confirms identity with biometric or PIN

www.privakey.com

Privakey CX for Linux on IBM Z

Security & Convenience in One Solution

At Privakey, we believe that mobile devices hold the promise to improve the security and convenience of interactions across the user experience. Our approach utilizing asymmetric cryptography and device biometrics can be used to streamline how users, regardless of channel, authenticate their identities, assert their consent and approve transactions of any type.

Example Uses of Privakey

- Eliminate the need for hard security tokens in multi-factor authentication workflows
- Approve financial and other high value transactions
- Review and confirmation of policy exceptions
- Amazon Alexa identity assurance
- Acceptance of terms and conditions
- Workflow approvals
- Permission changes

Challenge Flow Diagram

A challenge is sent from an existing application to the Privakey Auth Service which federates notifications to the user's device. User's secure response is returned through the Auth Service to the originating source.

Technical Overview

Privakey CX is comprised of two primary components, a central Auth Service and mobile libraries for iOS and Android.

Privakey CX Service

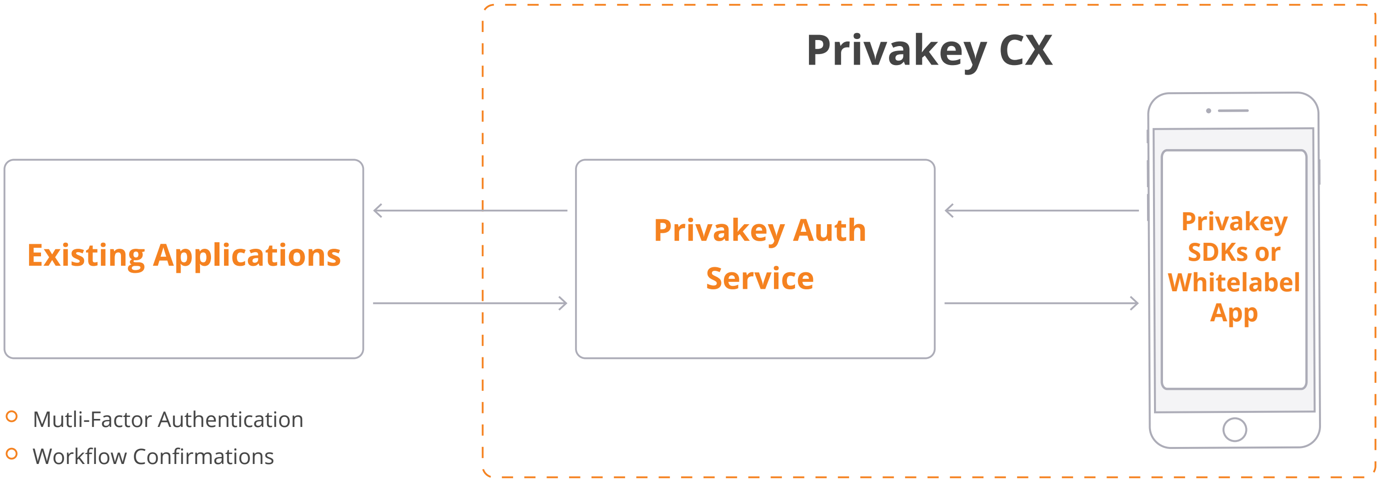
- Federates challenges to registered user's devices
- Brokers interactions between users and challenge origins
- Utilizes RSA 2048 encryption
- Multi-tenant support

Mobile Libraries

- SDK's (iOS and Android) for integration into existing mobile apps
- Optional white-label standalone mobile app
- Handles device registration and cryptographic key generation
- Supports native biometric gestures and PINs
- Challenge content is completely customizable (HTML, forms, videos, documents, etc...)

Integrations

- OpenID Connect
- Simple ID bind
- Firebase
- Extensible to other notification frameworks
- Simple API



- Mutli-Factor Authentication
- Workflow Confirmations
- Exception Processing
- Transaction Approvals
- Voice Platform ID Assurance