TATA COMMUNICATIONS DIGO

NEW MESSAGE

BANK

9451 is your verification code.

SECURE PAYMENT

3579 Maria

Enter your OTP below

9 4 5 1

OTP VERIFIED

AUTHENTICATE

Protect Customer Transactions with Authenticate

Multi-Factor Authentication for enterprise grade, secure transactions

If you offer web-based services to your customers, it's imperative for you to ensure strong security and validate transactions. A widely implemented approach for strong authentication is to use a one-time password (OTP), also referred to as 2-Factor Authentication. With Tata Communications DIGO Authenticate, we extend this approach, using multiple customer engagement channels (Messaging, Email, Voicemail). This enables you to provide more options and convenience to your customers while protecting their transactions using their preferred communications medium.

Integral Component of our Customer Engagement Platform

Authenticate is an integral component of our broader Tata Communications DIGO cloud communications portfolio, supporting transaction management, customer engagement and collaboration services.

Turnkey Solution

No need to build an MFA application from scratch. Tata Communications DIGO Authenticate is a pre-built solution for you, that just requires configuration for your specific requirements.

Multi-Factor Authentication Advantage

Deliver a reliable and scalable MFA solution to your customers and developers. With Tata Communications DIGO Authenticate you are ready to launch quickly, to start protecting your customers transaction with minimal IT resource or support needed.

Advantage

- Carrier grade platform, for delivery assurance
- Integration with our carrier networks already serving 100s of international destinations
- No Coding needed. Power up communications workflows quickly
- Assured regulatory compliance in every region
- End-to-end lifecycle and service management

Benefits

- Automate customer sign up, device registration and password management
- Ease of integration, using REST APIs
- Adding a recovery phone number to an account can block up to 100% of automated bots
- Block 99% of bulk phishing attacks
- Secure, carrier grade message delivery

How Does Authenticate Work?

1. **User Accesses Your App**
   User visits your website or mobile app and attempts to log in, authorize a transaction, or perform another action that requires a second authentication.

2. **Send User Identity to DIGO platform**
   Your application sends Tata Communications DIGO Authenticate the phone number or email address of the user and requests Tata Communications DIGO Authenticate to validate the user with a one-time password: Example '568219'.

3. **Tata Communications DIGO Validates the OTP**
   Tata Communications DIGO Authenticate shares this OTP with the user through their preferred communication channel. The user receives and enters the OTP into your application. The Tata Communications DIGO platform validates the OTP and allows the user to access your App/website.

Typical Use Cases

Healthcare: Protect patient information with OTPs for health portal logins, sent securely over SMS or voice call.

Financial Transactions: Secure customers financial information with OTPs sent over SMS or voice call to verify account logins.

E-Commerce: Add key capabilities and provide shoppers with more ways to browse and buy safely and securely.

Marketing: Manage loyalty and marketing campaigns with special coupons (OTP) validated by your retail partners.

Tata Communications DIGO Authenticate Key Features

Automated failover – If OTP fails over default channel, it automatically sends across a back-up channel.

Channel: SMS (default), Voice, Email, with failover process in the case of primary channel not verified

Language: Text-to-Speech (TTS) language for announcing OTP message over voice. Supports 45 languages across OTP Voice

Repeat: Number of times the TTS OTP message will be played. It's only required in voice; default value is 1

Length: Number of digits for OTP is variable. Default is a 6 digit number generated for OTP code

Time-Out: Time in seconds for which OTP is valid. Post timeout period, OTP is automatically cancelled if still not successfully verified. Default is 300 seconds

Guard Time: OTP is valid for a defined time and then cancelled. If the underlying communications channel is slow, multiple OTP can be sent but only one verified within the guard time

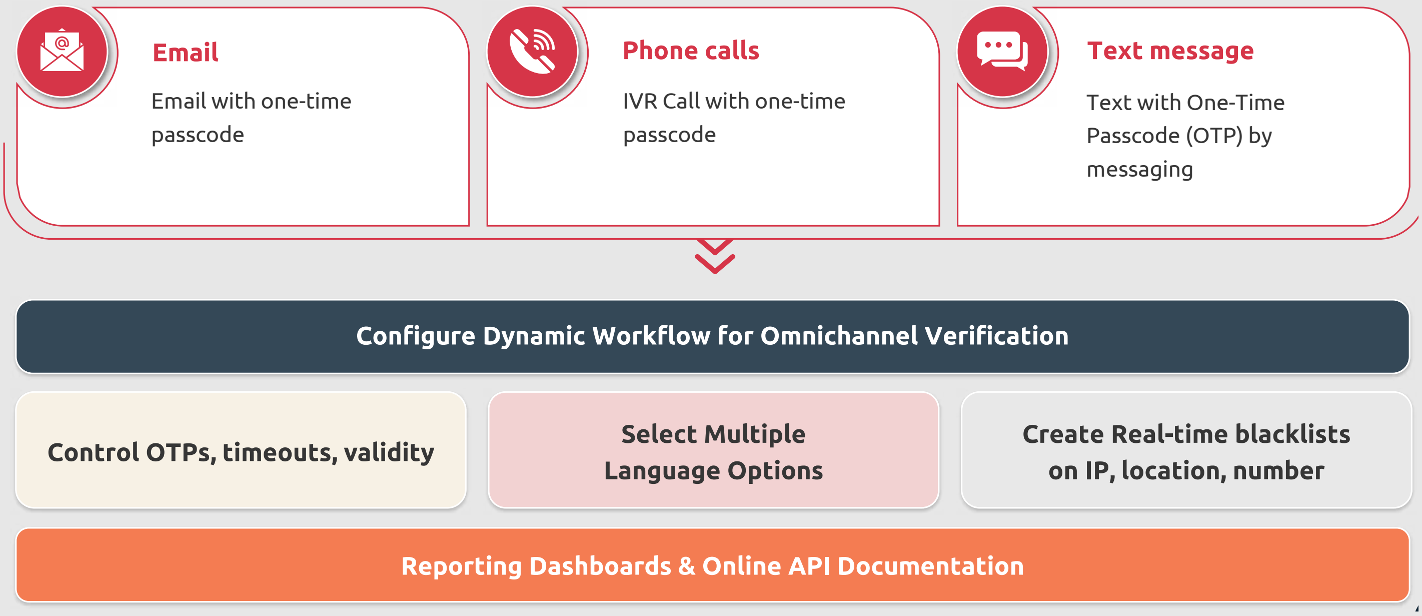
Process Templates: Define one or more channels into a failover process in the case of primary channel not verified

Limit: Enforce limitations on the number of OTPs sent based on various keys defined. Keys can be defined to put limits based on many parameters, such as phone number, Customer IP address and Geo-location, Application specific Session ID

TATA COMMUNICATIONS DIGO

‘Authenticate’ – Multi Factor Authentication

Enterprise authentication using any phone



Email

Email with one-time passcode

Phone calls

IVR Call with one-time passcode

Text message

Text with One-Time Passcode (OTP) by messaging

Configure Dynamic Workflow for Omnichannel Verification

Control OTPs, timeouts, validity

Select Multiple Language Options

Create Real-time blacklists on IP, location, number

Reporting Dashboards & Online API Documentation

Tata Communications DIGO branded service is available only in select countries.

For more information, visit us at https://tatacommunicationsdigo.io/

Contact us | Share