IS YOUR VALUABLE DATA SECURE?

AUTHENTICATION MEASURES CAN PREVENT DATA THEFT AND FRAUD

E-business helps organizations work more efficiently, providing access to information assets in ways that were never dreamed possible. However, as companies open their networks to distributed computing and a variety of remote users, valuable and sensitive information is potentially exposed. Security breaches result in data theft and financial fraud, which can result in significant financial losses and brand damage. For this reason, organizations are enhancing security systems by adding an authentication layer to verify network users.

Tata Communications' Authentication Service uses both a user-created Personal Identification Number (PIN) and randomly generated token code to protect network-connected assets against unauthorized access.

Companies can choose from token-generating mechanism options that include a physical device (hard token) carried by users or a software application (soft token).

Take advantage of a solution that is flexible yet comprehensive, ensuring you maintain control over your service. Reporting is both scheduled and available on-demand for IT audits and internal charge-back, and a self-service portal can be accessed to track token usage, report generation, PIN generation, PIN resets and emergency token requests.

Key Benefits

- Cloud based model offers low cost of operation, low CAPEX, built-in scalability, reliability and out-of-the-box integration with existing infrastructure
- With in-the-cloud 2FA validation, Tata Communications handles the complexity of securing, managing, and maintaining the infrastructure for strong authentication
- Helps reduce complexity of deployment, staffing requirements, administrative and logistics overhead, user management and infrastructure costs for lower TCO
- Performance-based Service Level Agreements (SLAs)—covering change management, proactive system monitoring, responsiveness, availability and token replacement
- Money-back guarantees on the performance and responsiveness of our Managed Authentication Service

Key Features

- Fully managed and secure authentication servers hosted at the Tata Communications' Security Services Operations Center
- Choice of multiple form factors—hard/ soft tokens, mobile soft tokens and one-time password (SMS based)
- 24/7 service desk for PIN resets, lost/damaged token replacements, application issues, account lockouts, modification of users and token resynchronization
- Comprehensive reporting-on- demand and scheduled for IT audits/internal charge-back
- Self-service portal which enables end-users and administrators to track token usage, report generation, PIN generation, PIN resets and emergency token requests
- SAML support for Cloud based applications
- Support for single sign-on in corporate environment

Soft Token Managed Authentication

Soft Token Authentication helps companies authenticate users without additional security hardware. Users no longer are required to carry around multiple hardware tokens. Instead, they can install token software on their existing cell phones, PDAs or desktops.

- Mobile token software can be easily installed on the user's mobile device and run on BlackBerry, iPhone, or any Java-enabled mobile device
- No replacement costs incurred—soft tokens never expire
- Cellular network connectivity or SMS client are not required to generate token codes
- Multiple integration points for existing application and services (HTTPS Servlet, Radius, Secure Web Services)
- Supports multiple tokens on a single device

Hard Token Managed Authentication

Tata Communications' hardware token is provided by SafeNet, and is a physical device that generates a One-Time Password (OTP). Tata Communications supports complete end-to-end deployment and management of these tokens by administering the procurement, provisioning, application integration and end-user support.

- Unique time-synchronous approach automatically changes the user's password every 60 seconds
- SafeNet authentication is built upon the Advanced Encryption Standard (AES) algorithm, a recognized standard that is continuously scrutinized and challenged by cryptologists around the world to ensure its strength and dependability
- SafeNet Tokens support interoperability with over 350 partner applications, including VPN, wireless, network communications, web applications and more
- Token replacement and emergency token code provided to ensure continuity of service