Telos®

IDTrust360®

Digital Identity Services for Securing IT Infrastructures

Is your identity trust verification infrastructure placing your business or your customer data at risk? Do you manage identity trust with monolithic legacy applications or spreadsheet workflows that block your progress towards IT modernization?

The process of assessing customer, employee, and vendor identities efficiently relies on the collection and analysis of biometric, biographic, and other external vetting information pertinent to your organization's threat environment. Once you gain the ability to leverage identity trust, you can mitigate risks to your critical infrastructure, operations, and sensitive information.

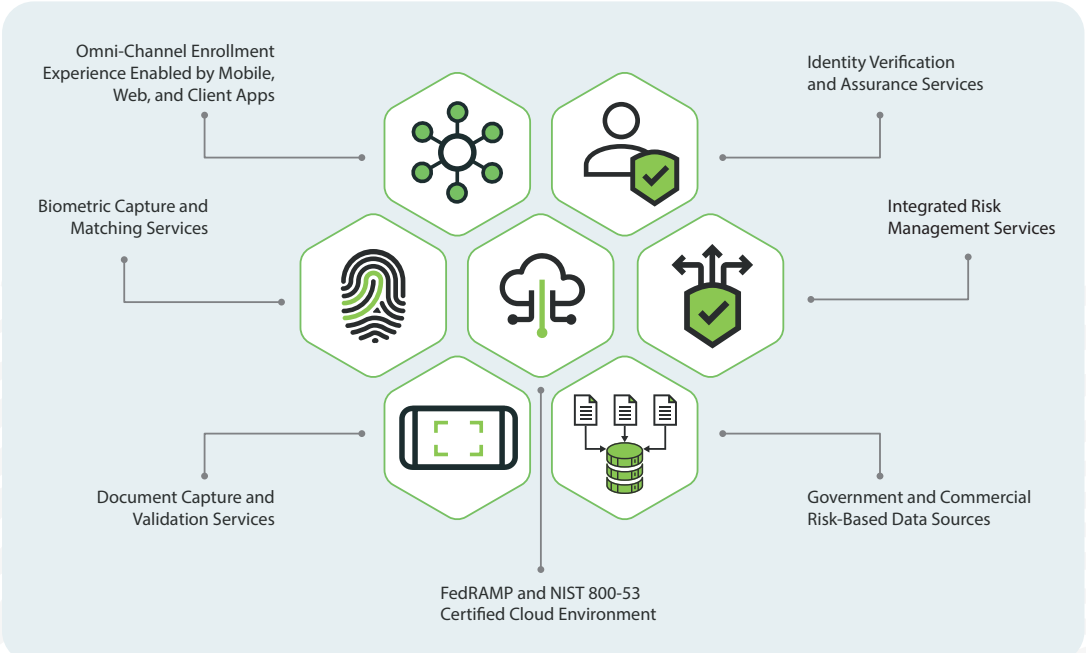
Telos® IDTrust360® provides you with the tools to tackle these challenges—whether you need to address requirements pertaining to Know Your Customer (KYC), insider threats, access and authorization, or regulatory compliance. The solution **secures enterprises against threats** by rapidly enabling digital identity services within complex operational ecosystems that span millions of identity transactions across all user devices — computer workstations, kiosks, laptops, smartphones, and access control systems.

Secure and flexible to give you confidence in digital transformation.

Built on an enterprise hybrid-cloud platform that is certified and operational in several U.S. federal agencies, IDTrust360 gives you the flexibility to rapidly and securely deploy modular services to **transform your business-to-business (B2B) identity environment.** The solution also supports business-to-consumer (B2C) applications to extend secure identity services to your customers.

IDTrust360 meets stringent federal requirements for cybersecurity and identity standards, including NIST SP 800-53 security controls and 800-63 identity assurance requirements. The platform also **delivers identity services in support of the largest digital identity programs in the U.S.** These include military, transportation, health, law enforcement, financial, and civil service organizations that manage millions of identity transactions across thousands of locations around the world.

Whether your organization is a government agency or a large, medium, or small business, you can leverage IDTrust360 to quickly validate individual identities. You can also use **flexible workflow options** for capturing identity data, integrating with back-end and third-party data sources, and extending biometric matching, mobile wallet, case management, and other advanced identity services. With these capabilities, your organization gains the ability to meet complex technical, operational, and regulatory identity requirements.



Telos IDTrust360 Capabilities

Identity Verification & Assurance

- Supports touchless, live scan, and wet fingerprint card scanning using either Telos proprietary or third-party software
- Applies multi-modal biometric matching
- Scans and validates government-issued identity documents
- Schedules user identity verification sessions via email, text, and phone notifications
- Captures payments via web, mobile devices, and point-of-sale systems
- Scales across retail, e-commerce, gig, mobile, and on-premises channels
- Provides self-service identity services across web, mobile, desktop, and kiosk devices

Integrated Risk Management

- Identifies, prioritizes, and mitigates threats to protect enterprise resources
- Automates security processing and compliance
- Manages insider threats in real time by analyzing government and commercial data streams
- Triggers AI-driven alerts within the context of managed risk elements
- Simplifies case tracking through AI-driven workflows
- Reduces risk exposure through mitigation, baseline scoring, and security plan documentation
- Screens staff that access sensitive facilities, information, and infrastructure services

Government and Commercial Risk-Based Data Sources

- Integrates with third-party and government systems to track criminal history, terrorist watchlists, vetting, case management, and payment processing
- Uses APIs approved by federal, state, and local government organizations
- Connects to FBI systems for processing non-criminal fingerprint checks and continuous insider threat monitoring
- Uses web and point-of-sale payment capture and extends payments to federal agencies in real-time

Document Capture and Validation

- Aligns with NIST and federal agency guidelines for digital identity, enrollment, and identity proofing
- Validates identity documents to assure people actually are who they claim to be
- Verifies documents using artificial intelligence, biometric matching, and optical recognition
- Authenticates documents leveraging identity template library containing thousands of document types and defined security attributes

Biometric Capture and Matching

- Provides facial recognition, live scan, and no-touch fingerprint scanning and matching
- Uses neural network to detect fingertips via mobile device cameras
- Captures and segments each fingertip into separate fingerprint image file
- Normalizes captured fingerprints with patented image processing to generate high-resolution images
- Applies artificial intelligence to detect liveness and prevent anti-spoofing
- Performs 1:1 and 1:N up to 50,000 biometric records on mobile devices via device-matching algorithm
- Generates facial images that comply with ICAO 9303 passport quality standards

Omnichannel Enrollment

- Provides access and appointment scheduling via mobile (iOS, Android), web, kiosk, and client apps
- Leverages flexible workflows to enable customization and configuration of data fields-based and role-based features
- Encompasses biometric, biographic, identity document, and payment capture services with back-end verification services
- Ingests, creates, and manages identities within either multi-tenant or single-tenant environments that securely manage all data

Streamline Onboarding and Identity Verification

As you enroll customers, employees, contractors, and vendors in systems that grant access to your IT infrastructures and digital assets, validating their identity is mission-critical—particularly if your systems transact sensitive data. Assuring each end-user identity and trusting your validation process are a must for mitigating risks to the critical infrastructure of your identity management system and reducing the threat of sensitive information exposure.

Telos IDTrust360 enables you to take on these challenges. Built on a FedRAMP-certified, high-performance, hybrid-cloud computing environment, the platform can be rapidly deployed to support multi-cloud and hybrid infrastructures that process sensitive data. By leveraging IDTrust360, you can streamline your processes for onboarding, verifying, managing, and monitoring identities to not only protect your digital assets, but also those belonging to your customers, employees, and vendors.

Telos® Solutions that **empower** and **protect** the enterprise.™

To learn more about IDTrust360, contact us today.
info@telos.com

Telos Corporation | 19886 Ashburn Road, Ashburn, VA 20147-2358 | 1.800.70.TELOS | 1.800.708.3567 | Fax 703.724.3865 | www.telos.com