

ActivIdentity Solutions Overview

Empowering employers, businesses, and governments to confidently establish a person's identity when interacting digitally





Market Drivers

The following factors are driving the adoption rate of strong authentication and credential management solutions:

- Rise of identity fraud, theft, and compromise
- Tightening of government regulations
- Increased insider threats during economic downturns
- Demand for versatile authentication infrastructure across different user communities

Introduction

Facing advanced persistent threats of cyber attacks and an increased risk of insider attacks that can result in the loss of national intelligence, corporate data, intellectual property, and personal identity information, organizations must find ways to effectively protect their information infrastructures and data. In this context, the ability to securely and confidently establish the identity of individuals accessing networks, applications, facilities, intellectual property, and other information assets is critical to national security programs, commercial businesses, and individual citizens all over the world.

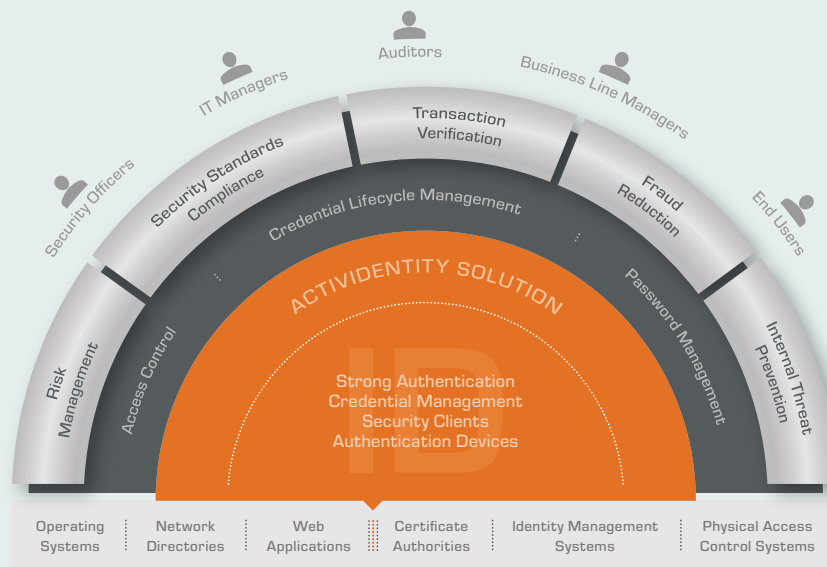
ActivIdentity™ provides solutions that maximize an organization's investment in identity and access management by providing Strong Authentication and Credential Management solutions that encompass a 360-degree view of an organization's operations, user communities, and service channels. This ID360™ vision drives ActivIdentity product development, customer solutions, and expert services.

ActivIdentity delivers ID360 solutions in three key markets: Employer-to-Employee, Business-to-Customer, and Government-to-Citizen. Organizations in these market segments leverage ActivIdentity Strong Authentication and Credential Management solutions to apply a systematic approach to registration, enrollment, authentication, authorization, auditing, credential issuance, credential management, and credential use. Regardless of the market segment, ActivIdentity Strong Authentication and Credential Management is the key technology to help secure information infrastructures and to facilitate compliance with strict mandates such as the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry (PCI) Data Security Standards.

ActivIdentity ID360 Solutions

ActivIdentity Employer-to-Employee Solutions

Although simple passwords have served for years as the primary authentication mechanism for employees who need access to corporate applications and data, a password alone is insufficient to secure access to high-value information and IT resources. To prevent unauthorized access in today's complex environment, organizations are moving to provide greater access control and audit methods internally. In addition, they need strong authentication solutions to combat identity fraud and system corruption threats that originate externally and take advantage of increasingly amorphous IT perimeters. When these drivers are combined with



business requirements to meet government regulations and industry guidelines, the demand for easy-to-integrate, advanced authentication and credential management technologies becomes even greater.

ActivIdentity Employer-to-Employee (E2E) solutions offer a multi-layered security approach across networks, systems, facilities, data, intellectual property, and information assets. The foundation of E2E solutions is a versatile authentication platform to control access to data and / or network assets. The platform supports a variety of authentication methods (e.g., user name and password, knowledge-based authentication, and one-time password) and authentication devices (e.g., soft tokens, hardware tokens, mobile devices, and smart cards). The authentication platform's versatility enables employers not only to provide access control for their employees, but also to extend the schema to contractors and employees of partner organizations. In these scenarios, organizations can tailor the authentication method based on the risk associated with specific types of transactions.

ActivIdentity E2E solutions are highly scalable. In larger deployments, they can be complemented by ActivIdentity Credential Management products and ActivIdentity Security Client software to streamline device management.

ActivIdentity Business-to-Customer Solutions

Consumers and institutional customers increasingly rely on the Internet for banking and retail transactions, as well as communication with financial services, health care, and insurance providers. In response to this growing trend, organizations are using websites, mobile applications, call centers, and interactive voice response (IVR) systems to enhance customer loyalty, build brand equity, and deliver cost-savings that can be leveraged for greater customer value. Although these systems have existed in separate silos in the past, their coordinated use for strategic advantage is a recent trend that promises greater customer reach and increased transaction flow. To take advantage of these opportunities, however, organizations must be able to ensure that digital interactions are secure across any channel. Banks, for example, can use electronic channels to enhance the consumer experience, but only if they can provide security at login time and when users trigger thresholds for transactions with high risk for fraud (e.g., changing personal profile information, adding a new payee, and transferring money).

ActivIdentity Business-to-Customer (B2C) solutions address the diverse needs of organizations with electronic channels that serve consumers, businesses, suppliers, and partners. The comprehensive ActivIdentity portfolio of Strong Authentication and

ID360 Market Segments and Industries

- Employer-to-Employee
 - Government
 - Government contractors
 - Law enforcement
 - Banking, financial services, and insurance
 - High-tech
 - High-value IP manufacturing
 - Health care
 - Many others
- Business-to-Customer
 - Banking, financial services, and insurance
 - e-commerce and m-commerce
 - Entertainment
 - Health care (provider-to-patient)
 - Transportation
- Government-to-Citizen
 - e-government
 - Driver's licenses
 - e-health cards
 - e-identity cards

Credential Management solutions help organizations secure electronic interactions across multiple channels. ActivIdentity solutions can be tailored to meet each organization's unique needs for device authentication versatility, a range of transaction risk-levels, and user and credential life cycle management.

Government-to-Citizen Solutions

Government institutions worldwide increasingly depend on digital technologies to securely authenticate citizens for travel, access to government-provided benefits, and transactions related to public services such as professional licensing and document filing. In this context, citizens must be able to surrender their personal identification data to the government with absolute trust in the administration, protection, and soundness of these technologies. At the same time, the government must be able to protect and manage this ever-changing body of data and identities.

Smart cards have emerged as the preferred method of Government-to-Citizen (G2C) identity programs in most areas of the world. Like ATM cards, smart cards can be configured to release private information only upon the correct entry of a personal identification number (PIN), which is known only to the citizen / owner of the card. For the public, they offer convenience and peace of mind regarding the security of their personal information. For government institutions, smart cards and other secure identity management technologies have the added benefit of increasing efficiency and accuracy by eliminating traditionally time-consuming and error-prone paper forms that are frequently prevalent in G2C environments.

ActivIdentity Government-to-Citizen solutions help systems integrators (SIs) address the challenges of G2C deployments by offering a Credential Management solution, as well as complementary components that SI clients can leverage to securely upload data onto chip-based authentication cards. In addition, ActivIdentity solutions provide post-issuance update capabilities that are essential for managing applications that require continual data revisions.

General Benefits

ActivIdentity solutions deliver multiple benefits, including greater digital and physical security, protection against online fraud, business process efficiencies, secure access to digital assets, and a pathway to regulatory compliance.

Americas +1 510.574.0100
US Federal +1 571.522.1000
Europe +33 (0) 1.42.04.84.00
Asia Pacific +61 (0) 2.6208.4888
Email info@actividentity.com
Web www.actividentity.com

About ActivIdentity

ActivIdentity Corporation (NASDAQ: ACTI) is a global leader in strong authentication and credential management, providing solutions to confidently establish a person's identity when interacting digitally. For more than two decades the company's experience has been leveraged by security-minded organizations in large-scale deployments such as the U.S. Department of Defense, Nissan, and Saudi Aramco. The company's customers have issued more than 100 million credentials, securing the holder's digital identity.