IDaaS: Managed Credentials for Local & State Emergency Responders

NextgenID – ID*TRUST Platform™

NextgenID® - Headquarters USA
10226 San Pedro, Suite 100
San Antonio, TX 78216
+1 (210) 530-9991

www.nextgenid.com

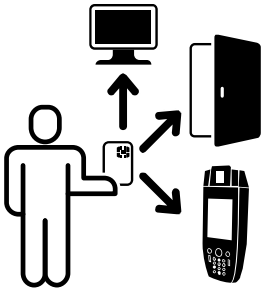
NextgenID® - Washington DC
13454 Sunrise Valley Drive, Suite 430
Herndon, VA 20171
+1 (210) 530-9991

IDaaS: Managed Credentials for Local & State Emergency Responders

NextgenID – ID*TRUST Platform™

The ID*TRUST Platform delivers automated enterprise enrollment and card issuance capabilities for physical and logical operational use by Emergency Management Personnel. This capability includes two factor authentication for secure network authorization without passwords, time and attendance reporting, physical access to buildings and parking facilities with full reporting and alerting capabilities, people tracking, mustering, asset assignment management and mutual aid manifest organization.

Protecting and securing assets such as facilities, computers and data information systems are a primary responsibility for EM personnel. To ensure consistent implementation across the City, County and State, a standardized identity credential should be designed to enhance security, reduce identity fraud for all citizens, protect the personal privacy of those issued government identification and allow for interoperability and instant identification between Law Enforcement officers, Homeland Security personnel, Emergency Management staff and First Responders across the State.

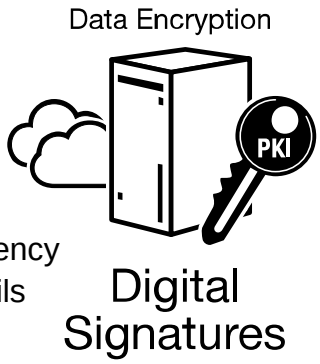


NextgenID solutions provide State Agencies, including associated Municipal and County operations, with interoperable identity management and credentialing solutions that provide end-to-end services to effortlessly enroll applicants, issue secure credentials, and manage the complete lifecycle of these credentials, including integration of Agency specific programs into the smart card. NextgenID delivers a managed, shared service solution that simplifies the process of procuring and maintaining credentials, while at the same time, meeting compliance for issuing credentials at a commercial, state and/or Federal level of assurance and interoperability.

NextgenID has developed a comprehensive end-to-end managed ID service to issue fully compliant PIV-I and PIV-C (CIV) identity credentials for Administrative Employees, Contractors, Elected Officials, Emergency Management personnel, First Responders and Citizen Volunteers. State Agencies benefit from a centralized, streamlined and efficient operational program infrastructure, technical expertise, and economies of scale for credential management. The NextgenID ID*TRUST Platform delivers a key structural component to assist State agencies in unifying their logical (computer) and physical (building) access control systems as per implementation plans.

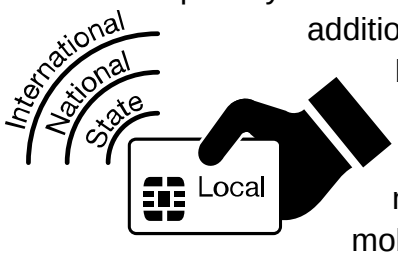
NextgenID® solutions address the challenges associated with reliably assuring personal identity for:

- Two factor authentication for network authorization, eliminating the need for passwords on State networks,
- eGovernment and eHealthcare Initiatives including digital signature and encryption capabilities
- A State-wide (city, county, school) “ONE CARD” ID solution providing custom time and attendance tracking and reporting tools based on customer specific requirements,
- ID Badge access and reporting for buildings & parking areas,
- Federal HSPD-12 Identity Compliance, Healthcare workers and suppliers ID and medical information on card
- National, State and Local Emergency Response, Safety & Security Interoperability,
- Biometric Identification on the card,
- Multiple Citizens State Benefit Programs – contained within the smart card as an attribute container with configurable accessibility (wide-open (none), card holder only, authorized container owner only, or cardholder plus authorized container organization owner),
- State-wide & Agency-wide Streamlined Program Enrollment,
- Financial Systems Stability,
- Agency Interoperability with customized privacy measures, and
- Customizable to support any State initiatives achievable via unique ID credential.



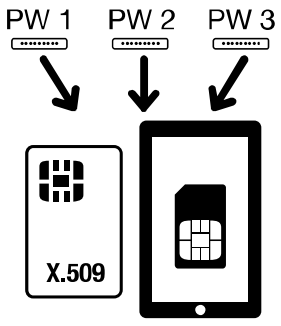
NextgenID's proven ID*TRUST Platform delivers a cost effective approach that is designed to support multiple stakeholders on a single system. It avoids each Government agency from having to create separate backend infrastructure and capabilities to issue agency and program specific ID cards and eliminates identity fraud, curtails misrepresentation, and prevents identity theft.

For customers desiring biometric solutions, it provides biometrics and independent attribute modules making each issued card unique; adding a technical solution to the privacy challenge. With the implementation of the ID*TRUST Platform, additional initiatives such as eCommerce, eHealth, and eGov become viable to meet all current and known future Government security and identity mandates. The ID*TRUST platform provides the ability to support outreach, notification, sponsorship and scheduling activities online and mobile. This aids elimination not only in expediting the enrollment process and reduced enrollment times, it aids in sponsorship validation and fraud reduction.



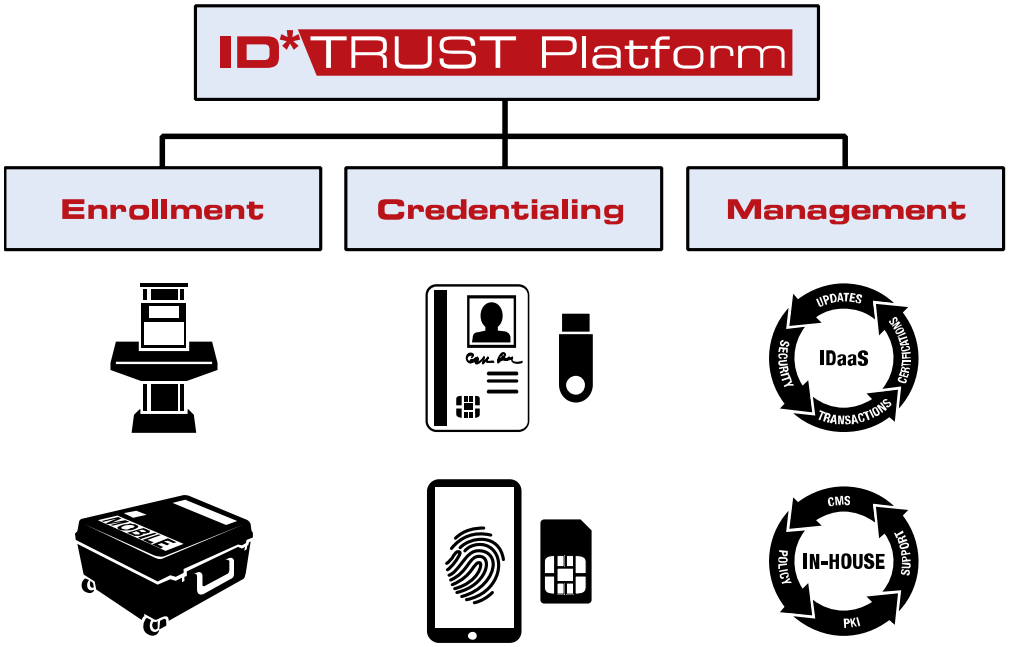
Global
Interoperability

When a State begins issuing Smart Card credentials, focus must be placed on how to achieve the myriad of benefits that accompany the use of State-wide Smart Card credentials beyond simply using the credential as a visual ID or card-key badge replacement. Learning to take full advantage of the power of the vast amounts of partitioned data stores on the card, the State and its associated agencies can use the smart card credential in a broad variety of capacities. It can be used to eliminate or reduce the need for passwords by using the card as a single interoperable ID token for one, two or three factor login to computers, computer systems and local area networks.



Eliminate
Passwords

As a "one card" solution, the smart card credential will immediately limit the number of building entry key-cards required to be held by employees, visitors and contractors. For higher security locations, the card can be used for two-factor contact and contactless authentication into building access and alarm systems. This will increase security by validating identity of those requesting access at a higher level, using information such as digital certificates stored on the credential, to compare the photo on the card to the face of the cardholder, verify the PIN stored on the card and/or fingerprint verification as well.



**"As a turn-key managed credentialing service,
there are no network servers or computers to buy"**

Another benefit will be the reduced transaction time on internal business processes while reducing paper waste and eliminating ink signatures for official approvals by using the credential for a legal digital signature.