# Healthcare
# Utilizing Trusted Identity Credentials


**NextgenID® - Headquarters**
10226 San Pedro Ave, Suite 100
San Antonio, TX 78216
(210) 530-9991

**NextgenID® - Washington DC**
13454 Sunrise Valley Drive, Suite 430
Herndon, VA 20171
(703) 429-8532

# Utilizing Trusted Identity Credentials within Healthcare

Healthcare providers and networks on a national level are investing resources to protect their employees, patients and community by improving their physical and logical security. As such, a fine balance must be found between inconveniences, time consumption and complexity that comes with added security and day to day operational needs and efficiencies that must be in place to be successful. Additionally, terrorism has now grown to be a major threat not just to national security, but also to the healthcare industry effecting business interests, quality of care, and patient privacy.

- Medical-related identity theft accounted for 43 percent of all identity thefts in the U.S. in 2013.
- Clinical staff's in most every organization battle user name and password issues and commonly share them amongst co-workers or leave networks and applications logged in and "shared" by others that require access.
- Network and system passwords must be replaced and strengthened frequently, at substantial cost in both time and money. Our user community then finds ways to "survive" this and aside from sharing user names and passwords, they store them on post-it notes found under keyboards or placed in plain sight on desks and counters.
- Physical (building) access systems typically use dedicated and sole use proprietary card systems that have no means to add more value or usability. It is commonplace to see multiple cards within organizations for general building access, department access, parking lot access and staff only areas.
- Imposters posing as nurses, doctors, and hospital staff are common.
- Hackers frequently exploit username/password security to steal valuable, sensitive data. Remote access (VPN) is a common pathway for hackers due to reliance on single factor user name/password access through tightly secured communications. The weakest link principle…
- Current hospital solutions are proprietary, inconsistent, and not broadly trusted across disparate entities — impacting everything from operational efficiencies to quality of service and life.
- Hospital IT operations lack common, open-standards-based identity and authentication solutions for interoperability and a future enterprise growth.
- Emergency responders with trusted ID cards can be put to work faster upon arriving at the scene.



13454 Sunrise Valley Drive, Suite 430 - Herndon, VA 20171 - (703) 429-8532 www.nextgenid.com

## The "One-Card" - ONE IDENTITY CARD FOR MULTIPLE USES

NextgenID provides the healthcare community with a secure way to confirm the identity of physicians and staff with a high degree of assurance. NextgenID products and services a founded on the "gold standard" that has been established and implemented IDs within the federal government, military, and defense-aerospace industries to enable trust amongst all healthcare personnel with an interoperable and trusted credential. This approach enables organizations to know with certainty the identity of each person.

As an example, for a Physician, the NextgenID credential can be used daily for physical access to the building, the emergency room, the physician's parking lot, and the physician's lounge. The card carries an embedded smart chip that contains digital certificates allowing secure authentication not only for physical access but for a host of value added integrations and application use. Applications such as "tap-and-go" application and network sign-on, single sign-on (SSO) use, digital signing of documents, forms and orders, document and file encryption, and VPN authentication and access all become enabled to support higher security while providing increased efficiency and user simplicity. More than 4,500 doctors within the San Antonio area use smart card ID's today.

## FLEXIBILITY IN REAL TIME

Though a cardholder's identity never changes, hospitals frequently change the cardholder's access rights to places and systems. Because the NextgenID provides certainty of who the cardholder is, a hospital can immediately remove or add access rights when the need arises. For example, NextgenID can develop a service for its hospitals that enables near-real-time removal of an identity from all participating physical access systems. And, if a card should be compromised (for example, if a hospital learns there was fraud in its issuance), it can be electronically revoked immediately so that any entity will know not to trust the cardholder's asserted identity—in proper usage the credentials validity is electronically checked each time it is used by the card holder. The NextgenID KIOSK, used for fraud elimination and speedy issuance, supports self-service operations supporting employee diverse availabilities.

## TRUST

At the heart of the value of the NextgenID is trust—trust that the credential follows specific technical interoperability requirements, and a trust that the credential being provided and used follows a specific and know rigorous process in proofing the identity of credential holders that is therefore trusted by organizations for their use.. This trust is maintained through independently audited compliance against national standards and compliance requirements. NextgenID is a certified credential issuer compliant to "Personal Identification Verification – Interoperable" (PIV-I) issuance and operations. This provides a means for automatic acceptance and trust from all federal, state and DOD agencies.



13454 Sunrise Valley Drive, Suite 430 - Herndon, VA 20171 - (703) 429-8532 www.nextgenid.com

## USE CASES

- Physical access and security for hospital facilities including rooms, building and campus level access.
- Data Security to control access to patient records, healthcare information and other sensitive data.
- Data Protection through encryption of sensitive documents, correspondence, and data.
- Business process automation through digital signatures and direct integration into core Microsoft and Adobe products
- Cashless Payments (contactless smart card technology - multiple campus services including meals, store, laundry, printing, etc.).
- Parking and transportation operations including parking and transportation access and sharing systems.
- Time and Attendance monitoring - monitoring and recording attendance through integration and leveraging of facility physical access systems. Supported academic pilot activities to integrate into authentication of remote student population and presence.
- Valuable Asset Protection & Management - accurate and fast management of capital assets. Supports wired and wireless locks installed on secure storage receptacles like cabinets and lockers which can be connected to the building's online access control system for near- online and near-real-time control. Supports protection and monitoring of high-value resources like fleet vehicles, and industrial, laboratory or other equipment.
- Mobil Access Control and Interoperability - solutions can be implemented supporting contactless smart cards that are also portable to NFC-enabled mobile devices. Mobile access control solutions will co-exist with ID cards on a typical hospital campus, enabling institutions to implement a choice of smart cards, mobile devices or both.
- Support identity management and credential sharing on and off hospital campus, including partnerships with third-party/partner service providers (for example - services range from banking, food service, transit, facility access, equipment usage, safety certification compliance and cashless payment, to multi-factor authentication with biometrics, secure logical authentication, and attendance authentication at testing centers for accreditation vetting).



13454 Sunrise Valley Drive, Suite 430 - Herndon, VA 20171 - (703) 429-8532 www.nextgenid.com

## SMART CARD BENEFITS FOR:
## HEALTHCARE PROVIDERS

Machine-readable health identification credentials:

- Increase clinical and administrative staff efficiency,
- Eliminates shared and unknown access to networks and systems,
- Provides a platform for standardized authentication services across the enterprise and systems, and
- Provide a means for paper elimination through electronic document and form data integrity and signatory requirements.

If credentials are extended to patients, identification credentials:

- Eliminate patient and insurance benefit identification errors,
- Reduce costs and aggravation of rejected claims,
- Reduce lengthy admission processes, and
- Contribute to smoother office procedures and patient satisfaction.

Significant reduction in claim errors will enhance provider relations with plans. The costs of traditional photocopying the front and back of cards, manual lookup and key entry of card information, and filing paper copies can be eliminated over time. When integrated with enhanced provider systems, machine-readable identification cards will facilitate immediate automatic transactions such as eligibility inquiries. Even in phone conversations, the simplicity of needing only two identifiers aids both patient and provider to convey insurance benefit information or medical record identification quickly with complete accuracy.

***According to the WEDI Health Information Card Workgroup, the industry can realize an estimated $2.2B savings annually - if a machine readable card is used within Healthcare.***

## HEALTH PLANS & ADMINISTRATORS

Patient and insurance benefit identification errors significantly increase processing and service costs for plans; they aggravate providers; and they contribute to member dissatisfaction. Elimination of patient identification errors will benefit health plans to:

- Improve subscriber or member satisfaction
- Improve employer and plan sponsor satisfaction
- Reduce cost to return and subsequently reconcile claims with errors
- Reduce significantly the cost of both provider and member help desks and administrative record searches, and
- Improve plan-provider relations.



13454 Sunrise Valley Drive, Suite 430 - Herndon, VA 20171 - (703) 429-8532 www.nextgenid.com

In addition, the universal health plan identifier conveyed by the card is one ingredient for improved coordination of benefits. With multiple-benefit cards, administrators and medium sized payers are able more easily to provide a convenient range of benefit plans to meet the needs of employers.

## PATIENTS AND CONSUMERS

Elimination of patient and insurance identification errors significantly reduces the hassle factor and increases patient and subscriber satisfaction. Consumers' desire simplicity, and they want a single card for multiple benefits and functions. This implementation guide, using only two identifiers, enables multiple benefits on a single card. Patients can more easily and accurately read the essential identifiers from a card to a provider over a telephone. It also permits an option to combine an insurance card with a bank card on the same card.

## FOR EMPLOYERS

Employers desire to improve employer-employee satisfaction and reduce costs. Elimination of patient and insurance identification errors increases employee satisfaction with the company's benefit plans and reduces cost of helping employees resolve insurance benefit problems. With a multiple-benefit card, employers are able more competitively to purchase multiple benefits using different administrators while presenting to an employee only a single, simple card.

## FOR CLEARINGHOUSES

The standard health plan identifier conveyed by the card assists all-plan routing without requiring translation of trading-partner specific identifiers. Reduction of errors will reduce expense and increase client satisfaction. Multi-benefit cards enable clearinghouses to support increased value to providers.

## PROCESS NEUTRALITY

The card should meet stakeholders' needs. It should be neutral to the conduct of business. For example, it should permit but not require multi-functional cards. It should permit host and home plan structures, geographical or regional plan structures, provider networks, and any other such arrangement. It should support different types of benefit plans such as medical, dental, drug, vision, supplemental; and it should permit but not require combinations of benefit plans. It should have flexibility to permit new business structures and processes in the future, including potential financial transactions. Its processes should be open, and supporting directories should be publicly accessible to responsible participants in healthcare electronic commerce.