National Security Solutions

AN IDEMIA COMPANY

TABLE OF CONTENTS

ABOUT THE AUTHOR

MICHAEL RONAYNE
Senior Director, Identity Solutions
1 (703) 797-2600 mronayne@idemia-nss.com

Mr. Ronayne is an accomplished executive with more than eighteen years of repeated success guiding cross-functional research, product development, and support teams. He is a proven leader in the design, optimization, launch, and support of identity, credentials, and biometric solutions. Since 2014, Mr. Ronayne has served as a Senior Director for IDEMIA National Security Solutions and is a subject matter expert in multiple facets of the identity security industry to include secure credentials, security printing, and biometrics.

NSS

SYNOPSIS AND INTRODUCTION

Your identity comprises the unique, special, and complex components that make up who you are and who you present to the world.

It is for this reason that accurately capturing, securing, and ensuring ease of use of the identification documents which authenticate your persona to others are critical components of comprehensive individual identity management. Today, as a result of technological advancements and our increasing use of “smart” electronic devices and cloud-based platforms, your identity exists in the physical, mobile, and digital realms. This reality presents critical advancements as well as challenges. IDEMIA National Security Solutions amalgamates these aspects of your identity into one mobile identification (Mobile ID). The following discussion examines the significance of individual identification documents as well as propose security advancements that work to keep your identity safe in a rapidly changing world.

When an identification document is requested by an individual, it is the issuing authority's responsibility to analyze, verify, and approve the new identification for issuance based on the data and documents provided by the requester. Examples may include biometrics (e.g., face, finger, iris, voice), breeder documents (e.g., birth certificate, social security card, driver's license, passport), supporting documents (e.g., home utility bill, employment document, tax return) and personally identifiable information (PII) (e.g., name, date of birth, address) provided by that individual. These documents and data facilitate the adjudication process that ensures the information that will be personalized on the identification document is accurate and reflects the true identity of the individual, “A is A” (Aristotle's law of identity).

If there are no issues during the adjudication process, then the individual is issued a valid identification document that represents their true identity and will be an accepted form of identification by retailers, schools, and/or law enforcement. Physical identification documents are a rapid and simple way to prove an individual's identity is authentic and to allow an individual to gain access to products and areas where age and/or citizenship verification is required.

PHYSICAL IDENTIFICATION

The demand for individual physical identification documents increased exponentially in the 20th century.

This was due to a number of reasons including population growth, technological advancements, reduction in the cost of transportation, financial institutions issuance and retail adoption of credit cards, and the inception of company employee/visitor identification badges. This growth was further supported by industrial and governmental organizations which sought to establish regulations for identification documents, best practices for issuing authorities, and standards that would facilitate national and global interoperability. Organizations like the International Organization for Standardization (ISO), International Civil Aviation Organization (ICAO), National Institute of Standards and Technology (NIST), and American Association of Motor Vehicle Administrators (AAMVA) were established and made significant contributions to identification documents and identity management guidelines that continue to be updated and are used every day.

Physical identification documents are continuously evolving in order to meet the requirements, regulations, and demands of an ever-changing world, globalization, and to combat their susceptibility of being counterfeited. What started prior to the 20th century with a certified written description of an individual's identity has become the physical identification documents of today. Physical identification documents are designed with complex layers of security features that are added, embedded, and/or encoded in the document. Security features are essentially elements that are intended to ensure a document is unique, easy to identify as genuine, and difficult to counterfeit. These features are organized into three main categories: overt, covert, and forensic. Many features can be listed in several categories depending on their complexity.

DOCUMENT SECURITY CATEGORIES

OVERT
LEVEL ONE

Overt features can be authenticated visually and or tactilely. Your eyes, hands, and knowledge of the security feature are the only things that are needed to verify an overt security feature.

COVERT
LEVEL TWO

Covert features require some training and basic tools. The tools required may vary; however, most covert features can be verified with either a flashlight, ultraviolet (UV) light, and/or magnification lens. With these three simple tools and training, anyone can be taught to identify covert features and to quickly determine a genuine versus counterfeit document.

FORENSIC
LEVEL THREE

Forensic features are typically complex and require sophisticated and/or specialty tools used by experienced and well-trained document examiners at laboratories to complete detailed analysis and to determine their authenticity.

In the 21st century, major advancements in the physical size of electronics and memory storage capabilities enabled new technology-based features to be incorporated into an identification document without compromising on the standards of the documents. The growing and rapid implementations within both commercial and government physical identification documents have combined and integrated physical document security and technology-based features into the same document. Today, significantly more data can be digitally stored, including additional PII, biometrics, and public key infrastructure certificates (PKI) for enhanced digital and physical security of the identification document.

One of the latest advancements of a technology-based feature embeds a fingerprint biometric sensor in the document and enables authentication with no external hardware or system requirements. IDEMIA's F.Code, for example, enables all contact and/or contactless communication when a successful biometric match has occurred. This removes the need for a password or personal identification number (PIN) and enables the validation of the document to the registered individual's fingerprint biometric.

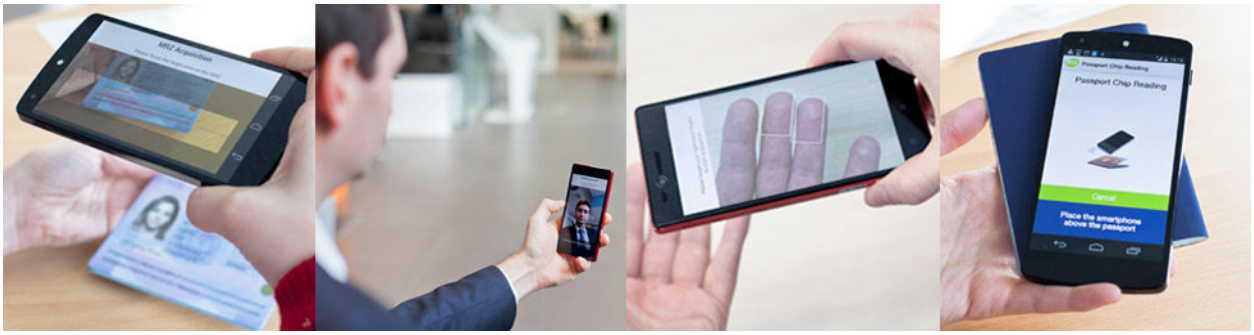
Today's physical identification documents provide numerous advantages, including security, integrity, and readability. As our world continues to evolve and we become more reliant on the mobile and digital realms, so does our need for quick and effective identity verification.

MOBILE IDENTIFICATION

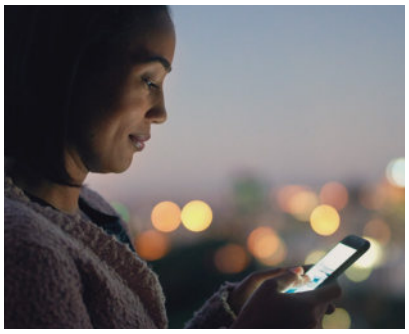
In 1964, Star Trek Season One had the first appearance of a Communicator

– a handheld device that allowed for instant voice communication between a person on a planet's surface and the Enterprise orbiting above. This was one of the first manifestations in television or film of what today is known as a “mobile phone”. Mobile phones have evolved into much more than a tool for voice communication. They are now an alarm clock, calculator, camera, compass, daily planner, email, flashlight, global positioning system (GPS), library, messenger, music player, and phone book all in a single device. In today's world, the mobile phone is capable of storing and tracking so much of our personal information that it essentially has become an integral representation of an individual's identity that can navigate both the physical and digital realms. Despite these advantages, the primary missing element from the mobile phone continues to be a means to validate the authenticity of an individual's identity in the same way that a physical identification document (e.g., driver's license and passport) is capable of today.

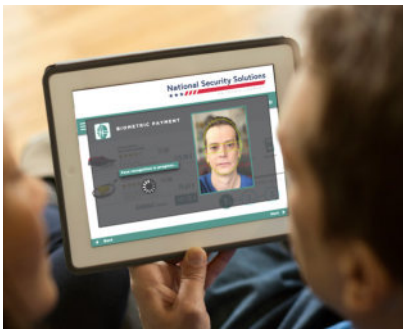
Secure identification on a mobile phone is undoubtedly advantageous; however, the challenge to the issuing authorities is ensuring compliance with both NIST 800-63 and ISO/IEC 18013-5 draft. Furthermore, additional challenges exist for providing ease of use to the individual identity holder and ensuring that if a mobile phone is stolen or lost, then an individual's identification and/or PII will not be compromised.



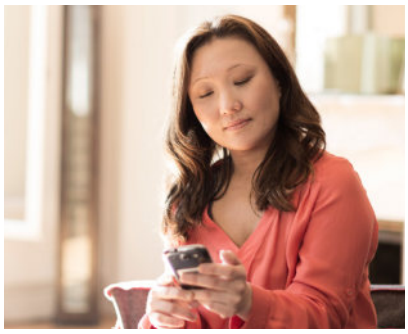
Iowa, Oklahoma, and other states are currently implementing programs for issuing mobile driver's licenses, and Alabama became the first state to issue Electronic ID (eID) for state income tax returns on a mobile phone. The issuing authority remains the adjudicator for validating the identity of the individual, as we discussed in the prior Synopsis & Introduction section. A Mobile ID has numerous advantages, including multi-factor authentication and direct communication with the issuing authority to the registered mobile phone over a secure connection. In order for the identity holder to access their Mobile ID there are 3 keys required for multi factor authentication:



WHAT YOU KNOW
Issuing Authority
Mobile Application



WHAT YOU ARE
Multi Angle Selfie
Facial Biometrics



WHAT YOU HAVE
Registered
Mobile Phone

Mobile ID allows for the biometric and mobile phone verifications, communication, and a display of a visual digital identification on an identity holder's mobile phone. The mobile application offers multi-layered, end-to-end security protection for data transferred between the identity holder and the issuing authority's system of record and is in compliance with both NIST 800-63 and ISO/IEC 18013-5 draft. The issuing authority can quickly and effectively review privileges, add security/system enhancements and global updates to all users at an extremely low cost to the issuing authority and no cost or time to the individual identification holder.

A Mobile ID will eventually be used in any context in which a physical identification document would be used, but with enhanced privacy features. The individual identity holder of the Mobile ID directly controls what and with whom any PII is shared, and how it is shared via near-field communication (NFC), display, and/or other communication protocols.

A Mobile ID is issued in support of, and as an enhancement to, the primary physical identification document. The physical identification document will remain the primary tool for identity verification for some time to come. However, a Mobile ID is an essential component of properly managing and protecting an individual's identity in the mobile realm.

DIGITAL IDENTIFICATION

The creation of the World Wide Web, has arguably been one of the most transformative influences on modern society and on our individual identification needs.

We are now able to access endless amounts of data, connect to people all over the world with a single click, and keep track of our sleep, heart rate, and the number of steps we take in a day using any number of wearable connected devices and cloud-based applications. Near constant use of the internet is now the norm and many of us have multiple devices that we carry daily and have installed in our homes that are connected at any given time. The websites we go to, the blogs we follow, the posts we like, comment on, and/or share on countless social media platforms, the bank accounts we maintain, the items we purchase, and the weather apps we check before a motorcycle ride all capture elements of our individual identity in the digital realm. Although there are numerous advantages to this, the challenge is how to keep your identity safe and protected while enabling organizations to verify that you are who you say you are. As our online imprint grows and we become dependent on the digital realm, the need for a fast and accurate verification of our digital identity with our physical and mobile identification is critical.

Exploring this intersection and providing advanced solutions is one of the core missions of IDEMIA National Security Solutions and the foundation for our Mobile ID. This is an individual's means to securely and confidently protect and confirm their identity in the digital realm. The Mobile ID captures and certifies your existing Physical IDs, then incorporates additional security in order provide for accurate authentication and generates an identity blockchain when multiple Mobile IDs are linked.

This empowers the individual to have control of their own identity in the digital realm and allows individuals to interact with confidence that people are who they claim to be, “A is A”, for the first time in the digital realm.

A Mobile ID can be used to securely verify the identity for any mobile or digital transactions that could compromise an individual's identity. For example, accessing bank accounts, applying for benefits or employment, social media account verification, tax return submissions, and/or any documents that currently require a digital signature for all legal and binding transactions or agreements.

The issuing authority of the Mobile ID will determine the multi-factor authentication requirements and chooses what biometric(s) (e.g., face, finger, iris, voice) and/or password/PIN are required from an individual to access their Mobile ID with a registered organization.

AREAS OF CONSIDERATION

Federal, state, and international regulations and organization standards are constantly evolving, and it is imperative that solutions are available to individuals to protect their identity in the physical, mobile, and digital realms.

- Physical identification documents remain and will remain the primary tool for individual identity verification domestically and internationally.
- Innovation of new overt, covert, and forensic security features for physical identification documents is critical to ensure the validity of the documents from each issuing authority.
- Multi-factor authentication secures the Mobile ID returning direct control of the PII that is shared to the individual.
- Mobile ID is a vital enhancement to driver's licenses, passports, visas, birth certificates, and any other breeder and secure identification documents.
- Corporations, banks, and federal/state governments should consider a Mobile ID as a solution to protect both the physical and digital identity of anyone whose identity has been compromised in any of the frequent and widescale physical and digital data breaches.
- Social media platform adoption of a Mobile ID will enable verification of accounts and assist in eliminating spoofed and nefarious actors.
- Mobile capabilities enable visibility and a level of trust in identity in the digital realm that simply has not been possible until today.

WHO WE ARE

IDEMIA National Security Solutions LLC, is headquartered in Alexandria, Virginia.

The United States government has mitigated our Foreign Ownership, Control, or Influence (FOCI) through a Department of Defense approved Special Security Agreement (SSA) directly with IDEMIA National Security Solutions. This SSA calls for an outside board of directors who, in conjunction with the IDEMIA National Security Solutions executives, comprise of the Government Security Committee (GSC). The GSC has responsibility for overseeing the company's compliance with the U.S. Government and SSA regulations. IDEMIA National Security Solutions history of successful delivery and compliance with the SSA as well as a Top-Secret facility clearance enables IDEMIA National Security Solutions to provide the products and services to the Department of Defense, Homeland Security, Justice, State and the Intelligence Community on some of the United States' most sensitive programs.

National Security Solutions

AN IDEMIA COMPANY

NSS

National Security Solutions

FOCI-mitigated SSA subsidiary of IDEMIA

675 N. Washington Street Ste 350, Alexandria, VA 22314 USA

www.idemia-nss.com