John Mears

Identification as a Service

Biometric Technology Today

About the author:

John Mears is a Leidos Vice President and Tech Fellow, with current focus on cloud-based national scale biometric systems, biometric entry/exit, border security, and immigration reform. Previously, Mr. Mears was Director of Biometrics and Identity Management. Mr. Mears holds B.S.E.E. and M.S.E.E. degrees from the University of Florida. He is an Associate Member of the American Academy of Forensic Sciences, member of the Biometrics Institute, and a Director of the International Biometrics and Identity Association (IBIA).

About Leidos:

Leidos makes the world safer, healthier, and more efficient through information technology, engineering, and science. The company reported annual revenues of approximately $7.04 billion for the previous fiscal year, and employs 32,000 people world-wide. Leidos is the largest information technology services provider to the U._S. Federal government. The company is also one of the most prominent providers of biometric systems in the world, with deliveries of such significant technology as the FBI's Combined DNA Index System (CODIS), the original FBI Integrated Automated Fingerprint Identification System (IAFIS), the FBI Next Generation Identification System (NGI), and the U.S. DoD Automated Biometric Identification System (ABIS).

Introduction

The concept of Identification as a Service (IDaaS) is radically changing the way biometric matching and identity services are provided. So why is this transformation important? Mainly because it is a market disruption that will propel new growth in the industry, but it is also likely to change the way we interact with applications requiring strong authentication or identification services, moving from captive closely-held applications into efficient and indispensable widely available utilities.

What is "Identification as a Service" or IDaaS?

IDaaS is a derivative term, based on nomenclature closely associated with cloud computing. IDaaS inherits, and benefits from, many of the same characteristics that make cloud computing attractive in the provision of information processing applications of many kinds. According to NIST SP 800-145[1], "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of

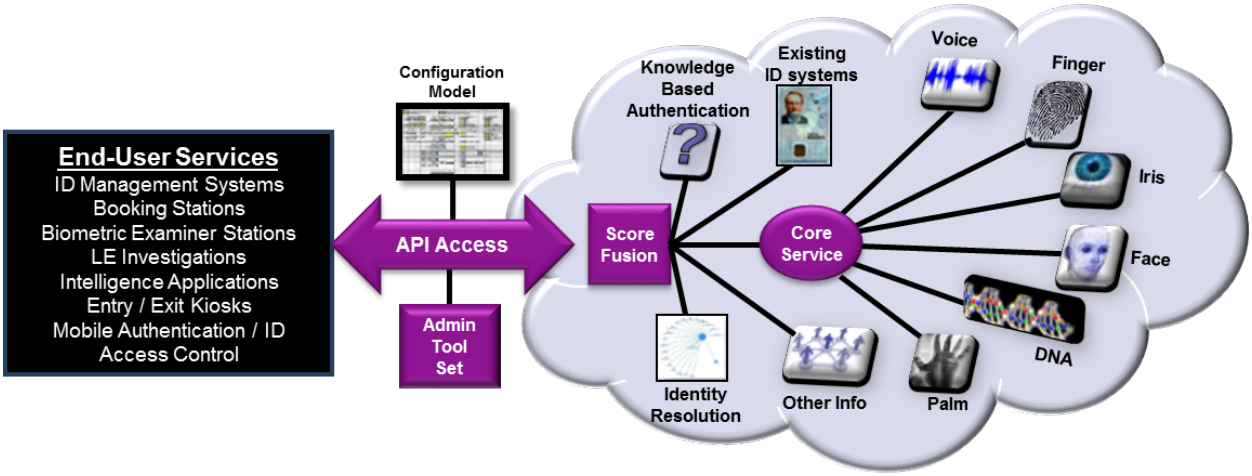
[1] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

The definition goes on to define three increasingly comprehensive service models including Infrastructure as a Service, Platform as a Service, and Software as a Service (SaaS). IDaaS falls under the final category, SaaS.

The "software" in this NIST model includes applications of various kinds. "The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings."

This model for SaaS has become so popular for many different applications that the term "X as a Service" was born, meaning a provider can deliver application "X" as a service. The term "IDaaS" was born from this concept by replacing "X" with "ID" for identity. The figure below is a graphical portrayal of one possible implementation concept based on this formal definition.



One Concept for an Identification as a Service Offering

While the cloud-based implementation fits this definition of IDaaS most closely, the term is interpreted by some to be any identification function implemented as a generally available service available to multiple constituents, whether cloud-based or not. I'll discuss examples of both non-cloud-based and cloud-based IDaaS applications later.

What Kinds of IDaaS Functions Are Provided?

While there are many different end-user needs driving demand for IDaaS, there are only two major functions provided by them – authentication services and identification services.

Authentication services provide the end-user with the ability to verify that a person asserting an identity is indeed the person they claim to be, based on their prior enrollment in the IDaaS system. This is often used for access control, both logical and physical. Logical access control refers to verifying identity for controlling access to applications, computers, or networks. Physical access control can refer to controlling building access or entry and exit at country border crossings. Authentication can be accomplished by biographic matching, biometric matching, behavioral matching, or combinations of these functions, all potentially provided by the IDaaS system. This is sometimes called one-to-one, or 1:1, matching to indicate that you are simply trying to match data provided by a user or other person (e.g. biometric or biographic) to a prior trusted enrollment of similar data.

Identification services refer to the comparison of an unknown person or user to a potentially large gallery of known subjects, often called one-to-N or 1:N identification. This service is useful in forensics or law enforcement (LE), border control, and de-duplication of enrollments in such sensitive applications as benefits or aid programs, healthcare, and voting.

Why Is This Likely to be a Growth Market?

According to Gartner[2], the SaaS market will grow about 20 percent in 2017 to a market segment size of about $46 billion. While IDaaS is for the moment a nascent portion, there are both general and segment-specific trends that indicate growth. There are many organizations that have adopted a cloud-first or cloud-only strategy to ensure they can reap the benefits described in the NIST definition.

Specifically, it is the desire of government and commercial procuring organizations to reduce traditional data center costs, increase security, and minimize time to deploy systems to an operational environment. Users may ask “why should I should I spend the time and money to build something that I can readily buy? Why should I spend capital money up front to build when I can buy cloud-based services in only the amounts I need, with expandability and elasticity as growth and demand respectively dictate?”

While there are a number of financial and competitive incentives, there are also regulatory motivations. In the financial industry, Know Your Customer (KYC) is not only required by law (especially for financial transactions), but is also of increasing importance to businesses. Continuous reports of fraudulent activity emphasize the need for businesses to know with whom they are dealing. Older security methods that rely

[2] https://www.gartner.com/newsroom/id/3616417

upon passwords alone are often insufficient to protect a business' data. These pressures and others, in conjunction with competition and increasing numbers of IDaaS offerings in the market space, will drive adoption.

Another trend to watch is consumer adoption of devices, such as smart phones, that increasingly have biometric and behavioral authentication techniques built-in. Societal acceptance of such advanced authentication and identification techniques is increasing as a result, and there is a building expectation that such technology advancements will speed and secure many other applications we use, not just our smart phones. This can reduce "friction" in our daily transactions, while at the same time providing extra assurance for our increasingly connected and populous planet. However, it is difficult for individual companies to provide such services to their customers, leading to pressures to aggregate into IDaaS utility offerings, again driving growth in the segment.

What Types of Organizations and Industry Sectors are Attracted to IDaaS?

Government agencies that deploy systems that can have widely varying daily or month-to-month transaction volumes have an interest in the elasticity capability of IDaaS Cloud systems. With elasticity capabilities of Cloud, procuring agencies only pay for the compute processing power that is needed in a given period. If transaction volumes surge or drop below normal volumes, compute power is automatically added or subtracted to dynamically meet the needs of the customer. In addition, growing populations and travel trends make the scalability features of IDaaS as attractive as the elasticity characteristics.

The financial industry is also attracted to IDaaS, but for different reasons. Other than the know-your-customer regulation mentioned previously, financial institutions are motivated by increased transaction flow and reduction of process friction while simultaneously providing greater security to customers. Their business is not biometrics or identity management, so they are inclined to outsource such functions in service to their primary missions – processing financial transactions and enhancing access for an increasingly mobile customer base.

The healthcare industry is attracted to IDaaS capabilities for patient identification, facilitating rapid admission to facilities, and elimination of patient misidentification. This can reduce errors in administration of medical procedures and medications. In addition, stronger identification and verification capabilities in our healthcare ecosystem can reduce fraud, waste, and abuse, leading to more controlled costs.

What Biometric Modalities are Most Popular for IDaaS Applications?

The most popular biometric modalities are undoubtedly fingerprints, faces, and irises, though facial recognition is gaining in popularity for applications other than forensics. Voice is next with increasing numbers of applications in Government services (for

citizen authentication 1:1 over the phone), and phone banking. There are also voice forensic and legal intercept applications in law enforcement.

There is also a growing desire for the use of DNA with obvious forensic applications, and an increasing number of personal heritage or personalized medicine applications. DNA analysis as a service is becoming widely available, and I can cite two that I've used myself, including 23 and Me[3] and the Illumina Understand Your Genome project[4]. This illustrates another factor driving IDaaS adoption. Not many of us can afford a genome sequencer, nor do we have the genomics skill to interpret the results. However, we can access a related "identification as a service" offering for DNA.

Vein pattern (finger, palm) and periocular and scleral vein pattern biometrics are next, with applications as diverse as automated school lunch purchases, financial applications, and subject verification for standardized tests. Schools, financial institutions, and test services don't normally have the skills to implement such authentication functions themselves, so it is attractive and efficient to buy a service.

Increasingly, we are seeing behaviors being used for authentication in a continuous fashion. How a person types, swipes, moves, holds their device, uses shortcuts, and a number of other observable behaviors, situations (e.g. time, place) and biometrics can be used together to continuously authenticate a person and provide extra assurance that the person using a device or computing resource really is who they say they are. Projects like Google's ATAP or offerings like those of BehavioSec[5] provide more device-centric examples of advancements in this approach. Solutions like those of Biocatch[6] use a neural network approach and monitor as many as 2000 parameters and behavioral attributes, which does require a hosted component.

What are the Most Prominent IDaaS Applications?

The Federal Bureau of Investigation (FBI) has been in the IDaaS business with fingerprints for state and local authorities consuming the service for years[7]. The same is true for the Department of Homeland Security (DHS) Office of Identity Management (OBIM) IDENT system, which OBIM regards as a "utility" to provide identification services to DHS components like Customs and Border Protection (CBP) and U.S.

---

[3] www.23andme.com

[4] https://www.illumina.com/company/events/understand-your-genome.html

[5] https://www.behaviosec.com/google-unveil-their-behavioral-biometrics-efforts-at-io/

[6] https://www.biocatch.com/

[7] https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics

Citizenship and Immigration Service (USCIS), among others[8]. These two examples represent the most prominent traditional applications – for law enforcement and border security/immigration, respectively. However, these systems were purpose-built for their Government applications. The emerging new IDaaS concept is to make such sophisticated identification services available to individuals and organizations of all sizes, for many different applications, without requiring the large capital outlay that systems like NGI and IDENT represent.

An interesting emerging trend is the leveraging of previously established national identification and biometrics systems for the benefit of commercial companies, individuals, or even other countries. I can cite several salient examples, and others are emerging.

I mentioned USCIS as a consumer of the OBIM IDENT service earlier. USCIS in turn offers their own IDaaS capability to other countries. Many countries now require biometric data from individuals filing applications for immigration-related benefits. Several countries, including the United Kingdom and Canada, have partnered with USCIS to collect the requisite biometrics and limited biographical information on behalf of their own immigration services. On behalf of the country, USCIS collects biometric and biographic information at its 138 Application Support Centers (ASCs) and deletes the records immediately after it receives confirmation that the partner country has received the information it transmits[9].

Among other countries in the world, India's Aadhaar program is the largest multi-modal biometrically-based IDaaS project, with 1.21 billion enrollees. Aadhaar enables citizens to receive food coupons, receive cooking gas deliveries, open checking accounts, apply for loans, get insurance, receive pensions, and acquire property deeds, among other services. For India, the system levels the playing field, embraces the diversity of the population, and provides documentation to many segments of the population that lacked it. The country expects that this identification service will not only propel its economy to the next level, but also reduce embezzlement of Government subsidies by about $1 billion dollars per annum[10]. It is a strategic tool of individual and economic well-being and development for India.

---

[8] https://www.dhs.gov/obim-biometric-identification-services

[9] https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-ibps-may2016.pdf

[10] "Aadhaar ID saving Indian govt about USD 1 bln per annum: World Bank." http://indianexpress.com/article/india/india-news-india/aadhaar-id-saving-indian-govt-about-usd-1-bln-per-annum-kaushik-basu/
.

China has announced its intention to build a giant facial recognition database to identify any citizen within seconds with an accuracy rate in excess of 90%[11]. Reportedly being developed for security, tracking wanted suspects, and public administration, some think that commercial uses may be allowed in the future based on development of the economy and increasing demand for such services from Chinese society.

While I've focused on national identification services to this point, there are trans-national services as well. Interpol has been in the trans-national identification service for law enforcement since its inception. The United Nations High Commission for Refugees (UNHCR) provides global identification services for refugees and displaced people[12]. The UNHCR has developed a portable system capable of the capture, enrolment, and verification of biometric data across a large refugee population distributed across disparate locations across the globe. The system ensures equitable distribution of food and medicine to a needy population where identity documents can be lost, if they existed previously at all. This kind of biometrically verified record-keeping service can be especially important where vaccination records are needed to assure disease control. It can also be important for this to be a service that is completely independent of the governments from which the refugees are fleeing.

Perhaps the newest instantiation of IDaaS is through blockchain services holding birth certificates, passports, wedding certificates, social security numbers, and other foundation documents for establishment of identity. The idea is to put digital records of these foundation documents in the immutable ledger of the blockchain, for secure and selective release of such information when the need arises, under the control of the owner. A number of companies have started to provide blockchain-based identity management and authentication[13], thus extending applications of blockchain beyond crypto-currency and smart contracts into the IDaaS business.

What are the Pros and Cons of the IDaaS Approach?

Generally, the pros closely align with those you'd expect for other SaaS applications. No capital expenditure is required by service subscribers, and you don't have to host your own data center on premise. The underlying infrastructure is maintained for you, including all patches and required cyber hygiene. Resiliency and redundancy can be built in, along with the scalability and elasticity to respond to long-term as well as

---

[11] http://www.scmp.com/news/china/society/article/2115094/china-build-giant-facial-recognition-database-identify-any . South China Morning Post, 13 October 2017.

[12] "Use of biometrics in migration: UN High Commission on Refugees." Bachenheimer, Dan. NIST International Biometric Performance Conference. Gaithersburg, MD, USA. May 5, 2016.

[13] https://medium.com/@LetsTalkPayments/21-companies-leveraging-blockchain-for-identity-management-and-authentication-d09d88e3a4bf

transient demands on the service. Application expansions can be made as warranted or needed. If the IDaaS is sufficiently general and popular, the costs of standing up the service can be spread across multiple customers, thus enhancing the business case for the offeror. For authentication end-users served by the subscribers, successful applications will reduce the "friction" associated with IDaaS-enabled transactions, and provide enhanced security resulting from augmentation or replacement of traditional IDs and passwords.

Cons can include a perception of the loss of immediate control, particularly of the data, by IT staff. Users and subjects alike may worry about the security of their data in the cloud. From the perspective of the offeror, significant investment is required before revenue can begin. Depending on customer acceptance, there can therefore be a significant negative cash flow until enough subscribers sign up.

What are the Tech Suppliers Doing in this Market?

In conjunction with the International Biometrics and Identity Association[14], I contacted four prominent member suppliers to provide a sampling of the emerging IDaaS offerings of each[15]. I'll cover them in alphabetical order, and give footnote citations where further information can be found. All of the companies have had significant development activities in IDaaS offerings, along with marketing efforts to support sales.

Gemalto recently acquired Cogent, and the combination has produced a new version of the Cogent Automated Biometric Identification System (CABIS) which supports multi-modal identity searches using fingerprints, palm prints, faces and iris recognition. A cloud-based version called CABIS Core Cloud has been added to the company's offerings[16]. The company says that the new CABIS Core Cloud will accelerate deployment of biometrics services by law enforcement and other government agencies.

Idemia, formed from Oberthur's Morpho acquisition, offers a Microsoft Azure-based multi-modal cloud offering called MorphoCloud. MorphoCloud is marketed as a secure and flexible cloud platform that supports Morpho products and solutions, starting with MorphoBIS, the company's flagship biometric solution for criminal justice and public security[17].

---

[14] www.ibia.org

[15] Thanks to Ramsey Billups of Gemalto, John Bredehoft of Idemia, Mike Lamke of Leidos, and Benji Hutchinson of NEC.

[16] https://www.gemalto.com/press/Pages/Gemalto-investment-speeds-development-of-new-Cogent-biometric-identification-solutions.aspx

[17] https://usa.morpho.com/file/download/morphocloud-brochure-20160515.pdf

Leidos offers an IDaaS solution called IDHaystack[18], hosted on Amazon Web Services (AWS). The system is multi-modal, with fingerprint, face, and iris identification and verification services offered at present. The system is marketed as “algorithm agnostic”, and can incorporate different algorithms from different vendors for each modality as desired or specified by customers.

NEC’s offering is marketed as NEC Identification-as-a-Service[19]. The offering is an extensible unimodal or multimodal platform comprised of NEC’s Automated Fingerprint Identification System (AFIS), Multimodal Biometric Identification System (MBIS) and Facial Recognition System (FRS) solution offerings.

This list isn’t exhaustive, and I’ve mentioned a few other companies working in this space earlier in the article. However, I think there is adequate evidence that the trend toward IDaaS offerings is real, with customer and societal pressure to create the offerings, and companies willing to make the investments necessary to meet the increasing demand.

---

[18] https://www.leidos.com/transportation-security/biometrics/identity-service-id-haystack

[19] https://www.necam.com/AdvancedRecognitionSystems/Products/IDaaS/