THE BUSINESS CASE FOR BIOMETRIC AUTHENTICATION
## CONTENTS

<table>
<thead>
<tr>
<th>The Business Opportunity of Deploying Biometric Authentication</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Why Authentication is Required</td>
<td>3</td>
</tr>
<tr>
<td>Risk and Regulatory Concerns</td>
<td>4</td>
</tr>
<tr>
<td>Inconvenient &amp; Insecure Legacy Authentication</td>
<td>4</td>
</tr>
<tr>
<td>Biometric Authentication – A Secure and Convenient Method</td>
<td>5</td>
</tr>
<tr>
<td>The Business Case for Biometric Authentication</td>
<td>7</td>
</tr>
<tr>
<td>Business Case Study</td>
<td>7</td>
</tr>
<tr>
<td>Survey</td>
<td>7</td>
</tr>
<tr>
<td>Cost Benefits – A Worked Example</td>
<td>8</td>
</tr>
<tr>
<td>The Business Case – Results</td>
<td>9</td>
</tr>
<tr>
<td>Lower Customer Acquisition Costs</td>
<td>10</td>
</tr>
<tr>
<td>Better Customer Engagement</td>
<td>12</td>
</tr>
<tr>
<td>Operational Cost Efficiencies</td>
<td>13</td>
</tr>
<tr>
<td>Security and Compliance Benefits</td>
<td>15</td>
</tr>
<tr>
<td>Consistent Authentication Across Channels</td>
<td>17</td>
</tr>
<tr>
<td>Daon’s IdentityX®</td>
<td>19</td>
</tr>
<tr>
<td>Key Features</td>
<td>20</td>
</tr>
<tr>
<td>About Goode Intelligence</td>
<td>24</td>
</tr>
<tr>
<td>About Daon</td>
<td>24</td>
</tr>
</tbody>
</table>
THE BUSINESS CASE FOR BIOMETRIC AUTHENTICATION

The Business Case for Biometric Authentication is a white paper from research and consulting company Goode Intelligence (GI). The study sets out the qualitative and quantitative basis for the return on investment from the use of biometric authentication in new customer registration and ongoing customer authentication across a number of business channels, commercial units and usage scenarios.

This study is intended for those in banking, broader financial services organisations and other regulated industries who have an interest in how methods of identifying and authenticating customers can be improved.

The study concluded the following benefits can be derived from biometric authentication:

- Better customer engagement, contributing to Net Promoter Score (NPS)
- Lower Customer Acquisition Costs
- Operational Cost Efficiencies
- Security and Compliance Benefits, including PSD2
- Consistent Customer Experience Across Channels

The study is based on Goode Intelligence's expertise in research and analysis of authentication and identity technology and uses primary information gathered from a survey of organisations that are using biometric authentication services for consumer facing implementations. It has been commissioned by Daon and includes input from Daon customers, including global financial services organisations.

NPS: Net Promoter Score is a management tool that can be used to gauge the loyalty of a firm’s customer relationships. It serves as an alternative to traditional customer satisfaction research.

OTP: A one-time password or pin is a password that is valid for only one login session or transaction, on a computer system or other digital device.

PSD2: Payment Services Directive 2 is EU legislation that plans to increase pan-European competition and participation in the payments industry from non-banks, and to provide for a level playing field by harmonising consumer protection and the rights and obligations for payment providers and users.
The primary business opportunity of deploying biometric authentication is to ensure that customers can interact with a business in a way that is convenient and consistent, while ensuring the organisation can address their security, risk and compliance obligations.

The benefit of biometric authentication is that it can balance both security and convenience without requiring a compromise of either. A multi-factor platform using biometrics can identify or authenticate across all business units, customers and channels in a consistent way, supporting an omni-channel strategy. There are significant benefits compared to legacy approaches.

Dealing with these issues within large financial service providers is now a C-Suite problem. Evidence shows that the business case, cost saving and ROI of deploying biometric authentication exists across multiple business units. This is a methodological research and data driven study that presents some of those business benefits, including the ROI.

**WHY AUTHENTICATION IS REQUIRED**

Financial services businesses need to authenticate customers in a variety of scenarios, such as:

- Confirming the customer’s identity (identification), during account opening, onboarding and for other KYC/AML checks
- When a customer accesses their account
- Authorising payments
- Approving or signing a transaction
- In higher-risk scenarios, re-authenticating the customer to a higher degree
- When a customer has requested a transaction through an external device or service (e.g., IoT and Open Banking API scenarios)
- When a customer interacts with the contact centres
- When a customer has lost a credential and needs to regain access to their account (account recovery)
- Registering the customer for a new device or credential (e.g., when registering a customer’s new smartphone for quick account access)

These types of authentication activities may occur across a variety of different channels and interaction points.
There are significant data protection, security and regulatory risks to be managed in relation to customer identities. According to a report from identity threat intelligence specialist 4iQ, there were 8.7 billion stolen identity records available on the web in 2017 when taken across the surface, deep, and dark web.

Corporate responsibility for the cyber safety of an organisation is now one of the top priorities for businesses. The European Union’s General Data Protection Regulation (GDPR) makes it even more of a priority. Any country that does business in the EU and has EU citizens as customers has to adhere to the GDPR, which imposes significant responsibilities and potential penalties on organisations.

INCONVENIENT & INSECURE LEGACY AUTHENTICATION

Usability issues with traditional authentication systems are creating real headaches for both consumers and organisations alike. Many organisations are still reliant on legacy identity and authentication platforms that are insecure and inconvenient to use. The use of two-factor authentication (2FA) is slowly on the rise but too often organisations rely on SMS one-time password (OTP), hard tokens and/or Knowledge-based Authentication (KBA) mechanisms without understanding their security or usability problems.

SMS OTP, the most widely-deployed consumer 2FA solution has usability shortcomings and security issues. In July 2016, NIST in SP 800-63-3, deprecated the use of SMS as a strong second factor due to weaknesses in the mobile operator network that delivers the SMS OTPs and it being prone to man-in-the-middle (MitM) attacks.

Hard tokens, cards and card readers are expensive to issue, require a physical exchange with the customers, frequently need replacement, and are often disliked by the end users. They also do not lend themselves well to the user experience expected by customers within digital services.

Knowledge-based authentication is susceptible to social engineering and inherently insecure where similar knowledge artefacts are used across multiple services providers.

1 Identities in the Wild: The Tsunami of Breached Identities Continues. 2018 Identity Breach Report from 4iQ.
2 https://threatpost.com/nist-recommends-sms-two-factor-authentication-deprecation/119507/
Biometric authentication offers solutions for the three major problems of consumer authentication:

- **Usability**: Convenient biometric authentication meeting the needs of digital transformation programmes
- **Security**: When matched with secure architecture and protocols that counteract the most common authentication security weaknesses
- **Compliance**: Addressing GDPR and Payment Services Directive 2 (PSD2) Strong Customer Authentication requirements

Usability improvements, in particular improving the user experience for digital commerce, are high up on the list for organisations wanting to improve their relationship with customers.

Biometric authentication is a proven mechanism for improving the user experience and removing much of the friction which often accompanies the digital experience. When a customer has one or more biometric options registered with the organisation and used in conjunction with their smartphone, they have a consistent means of authenticating across the range of scenarios mentioned previously.

One of the critical interactions during customer acquisition and account opening is identity verification, especially for those businesses that are subject to Anti-Money Laundering (AML) and Know-Your-Customer (KYC) regulations. Get it right and new customers will be easily acquired and retained; get it wrong and customers will be lost to competitors.

During AML/KYC checks, organisations have often had a fall-back position of face-to-face checking of identity documents, however, signing up for a digital service using physical identity verification methods is inconvenient and costly. Biometrics helps solve this problem by allowing businesses to verify the customer’s identity and conveniently onboard them through the digital channel.

The data captured as part of an onboarding process can then be leveraged for use in account access, payments and transaction authorisation to create a continuous and coherent customer experience. Biometrics also facilitates an improved customer experience for account recovery and setting up new device credentials, making it considerably more painless than previous procedures.

Our research found that the IT Security departments of large global banks are approving the use of biometric authentication for both account access and transaction approval.
This section details the business case for large-scale customer biometric authentication deployments.

BUSINESS CASE STUDY

This business case has been created using both quantitative and qualitative methods including:

• Market research survey of biometric authentication users
• Interviews with key stakeholders
• Senior analyst research
• Analysis and market research data obtained from Goode Intelligence’s primary research in the biometric authentication market
• Material obtained from Daon customers, including early and recent adopters of biometric authentication

SURVEY

Goode Intelligence ran a targeted survey and conducted focused interviews with organisations who are ahead of the industry using biometrics for identification and authentication. 40+ participants in senior roles from organisations across Europe, North America and Asia took part in this study.
COST BENEFITS | A WORKED EXAMPLE

This study covers biometric authentication for a financial services provider, a bank (although many of the findings are applicable regardless of the bank size or even industry vertical).

The study is based on a typical bank with the following characteristics:

1. Based in a capital city (e.g., of an EU country) with an international customer base
2. Involved in:
   - Retail banking services (primary business line)
   - Wealth management
   - Private banking
   - Commercial banking
3. The bank is a card issuer
4. Undergoing a digital transformation programme that involves review of branches
5. Seeing an increase in customers using digital banking channels including web and mobile
6. Five million customers
7. Average cost of inbound support call (Cost per call or CPC) $5.00³
8. Average SMS OTP termination costs a bank sending 60,000 messages per month: average price per message is $0.03992⁴ or $2,395 per month

---

⁴ Based on publicly available costs from the SMS aggregator, Clickatell
This study found that banks who use biometric technology to manage customer onboarding and authentication typically have:

- Lower acquisition costs and ongoing management costs
- Better customer engagement including improvements in the Net Promoter Score (NPS) – a critical measure of customer support for your brand or offering
- Operational Cost Efficiencies
- Security Benefits
- Better, more consistent experiences across multiple channels and customer contact points

Beyond materially reducing security process failures or exception handling, biometric identification creates a simple yet intimate connection between Atom and our customers. Instead of Atom being ‘a bank’ or just ‘Atom Bank,’ biometric identification makes it possible for us to become ‘my bank’ or better still, ‘Mark’s Bank.’

Mark Mullen | Chief Executive, Atom Bank
Acquiring a customer, especially in the heavily regulated banking sector is expensive. According to a Thompson Reuters survey of 2016, the average financial organisation is spending $60m annually on basic KYC needs and some larger financial firms are spending up to $500m a year on KYC and customer due diligence (CDD).\(^5\)

The banking industry traditionally has a high customer acquisition cost (CAC) with estimates of $303\(^6\) per customer so there are compelling reasons for wanting to reduce current banking CAC. Traditionally, and to meet AML/KYC regulations, bank account opening and onboarding might involve a visit to a physical bank branch for identity and document verification or multiple staff interactions with the customer while correct documents are sought and checked. These are high-cost activities for banks and new customers alike.

Our research estimates that a bank onboarding process can cost up to $4,000 per new customer.\(^7\)

Lower CAC can be achieved by including biometrics into a digital onboarding solution where identity and document verification can occur through an interactive mobile app that uses facial recognition and leverages multiple security techniques to detect and prevent false actors.

Banks are aware of these savings and are embracing biometric technology to support customer acquisition processes. Our survey found that over two-thirds (67%) of respondents are using biometrics to support customer acquisition by verifying their customer’s identity and to assist with digital customer onboarding. Additionally, 25% of these respondents said that the main reason for deploying biometric technology was to “improve customer onboarding.”

---

**CDD**: information that comprises the facts about a customer that should enable an organisation to assess the extent to which the customer exposes it to a range of risks. These risks include money laundering and terrorist financing.

**CAC**: Customer acquisition cost is the cost associated with convincing a consumer to buy a product or service, including research, marketing, and advertising costs. CAC includes marketing, sales and onboarding costs.

---

5 https://blog.atrivity.com/the-cost-of-onboarding-in-the-banking-industry  
6 https://www.propellercrm.com/blog/customer-acquisition-cost  
7 https://blog.atrivity.com/the-cost-of-onboarding-in-the-banking-industry
“Digital onboarding is becoming a prerequisite to strong identification and authentication especially in processes with high security needs (i.e., banking)”

Goode Intelligence Biometric Benefits Survey 2018

Identity verification with ID documents and biometrics can be incorporated into digital channels providing a quick and easy account opening experience – an example below using Daon’s IdentityX Digital Onboarding.

Biometrics is the future and it can be used in many unique ways apart from the traditional use case of customer identification and authentication. Biometrics can be used for transaction authorisation, digital onboarding of customers, enhancing customer experience and protecting customers and organisation both.

Rajnish Khare | Head - Digital Transformation, Social Business & New Media and Mobility Banking | HDFC Bank
Biometric technology is having a positive effect on customer engagement and satisfaction ratings due to its convenience and positive impact on the user experience. A more engaged customer is more likely to be a more valuable customer to financial services organisations with a higher likelihood of retaining their account and additional sales opportunities.

In the survey, 62% of respondents had already experienced “increased customer satisfaction benefits as a result of deploying biometrics.”

“We removed our customers’ need to remember passwords, thanks to Login with Selfie. The frequency of customer login increased notably with this feature and the users also found they could access banking transactions much more easily and faster than before.

We successfully incorporated the “selfie experience” which is a very important part of our customers’ daily life into our banking application.

Tolga Ulutaş
Executive Vice President in charge of Direct Banking, Akbank

An important metric for customer engagement and satisfaction, especially for digital commerce, is the Net Promoter Score (NPS). At least half of the participants in the study said their organisation had already seen an increased NPS as a result of deploying biometrics.

In the survey, 62% of respondents had already experienced “increased customer satisfaction benefits as a result of deploying biometrics” and many said “their organisation had already seen an increased NPS as a result of deploying biometrics.”
A major headache of organisations that have to manage outdated identity and authentication methods is sustaining high operational costs. Passwords and other inconvenient two-factor authentication technologies (particularly hard tokens, smartcard and card readers) put a high cost burden on financial institutions.

For authentication, two of the biggest operational costs are contact (call) centres, including account recovery (password resets), and SMS termination costs for OTP message services.

Biometrics can lead to significant operational cost savings for these items including:
- Reduced call centre interaction for credentialing issues including resets
- Elimination of expensive SMS costs
- Removal of hard token related costs

**REDUCING CONTACT CENTRE COSTS FOR ACCOUNT RECOVERY**

More than half of the participants (56%) in the study achieved reduced call centre call volume benefits as a result of deploying biometrics.

For our typical bank with five million customers, the average cost of an inbound support call (cost per call or CPC) is $5.00. Assuming that 25% of these customers (1.25 million) will make a call to the contact centre for an account recovery request (password reset) in a given year, the cost to the bank will be $6.25m annually. Some banks report that up to half of their customer care costs relate to difficulties encountered by their customers with registration or verification.

As a result of using biometric authentication, a bank can reduce this burden with the possibility of removing some contact centre calls completely.

During our research, Frederic Matterne, Head of Sales Development International Europe at BNP Paribas Wealth Management, said that “For the contact centre, we have seen some customers sometimes need hand-holding or a little bit of help at the start but once they get used to the biometric system, there is little subsequent interaction with the contact centre.” Furthermore “some clients of the bank are adamant they would never go back to using the previous authentication solution.”

**GI DEFINITIONS**

**CPC:** Cost per call is a contact centre metric calculated by dividing the total operational costs by the total number of calls for a given period of time.
SMS OTP has become a popular two-factor authentication method used by millions of bank customers around the world. It is probably the most popular 2FA method currently being used but it has serious issues.

In July 2016, NIST deprecated the use of SMS as a strong second factor due to weaknesses in the mobile operator network that delivers the SMS OTPs and risks of it being prone to man-in-the-middle (MitM) and SIM-Swap attacks."

It is also an expensive option for banks to manage as the bank has to pay for each OTP SMS message that is delivered to its customers. If each of our five million bank customers logs into their account just twice a week using OTP SMS, then a bank’s cost would be over $20.75m annually for OTP SMS message costs. Replace SMS OTP with biometric authentication and your typical bank would save $20.75 million per year.

The survey found that banks are already seeing cost-savings as a result of replacing OTP SMS authentication with biometric authentication. Nearly 30% of respondents have seen reduced OTP SMS termination costs.

Many banks use multiple authentication schemes across personal, business, corporate and wealth businesses. For those that also deploy hard tokens or card and card reader, using biometrics as a replacement of these devices removes the purchase, issuance and management costs. There is a very strong ROI just to replace these expensive legacy methods with mobile biometric authentication.

Additionally, existing account recovery processes using SMS OTP, KBA or tokens can be very expensive and cumbersome for both the bank and the end user. Many banks in the study describe account recovery as the equivalent of treating an existing customer as a new customer registration as account recovery is seen as a high risk process. Multi-Modal biometric authentication offers significant opportunities to streamline the account recovery process and crucially not to treat genuine customers in a customer care scenario as if they were potential fraudsters. It also offers the ability to take a tiered approach based on risk: in low risk scenarios, optimise for convenience and in high risk scenarios, apply more security.
In addition to increased convenience and the positive impacts found on reducing operational costs, biometrics also bring additional security benefits particularly in fraud deterrence and also in fraud detection.

Biometric authentication assists with compliance with the latest European data protection (GDPR and national) and payment security (e.g., PSD2) legislation. PSD2’s Strong Customer Authentication (SCA) technology standards support biometrics as one of the authentication factors – inherence.

Biometric methods that meet inherence requirements under PSD2 authentication also enable the avoidance of additional high friction confirmation steps for users, such as entering passwords, one-time codes in connection with token devices or card, or using physical card readers.

The use of biometrics in two-factor and multi-factor authentication systems is an extremely important consideration for banks and payment providers.

AS BNP PARIBAS TOLD GOODE INTELLIGENCE

“We have paid a lot of attention to the two-factor authentication aspects of our use of biometrics so we are not reliant on a single factor and we are fully compliant with the PSD2 SCA regulations.”

Frederic Matterne | Head of Sales Development International Europe

GI DEFINITIONS

SCA: Strong Customer Authentication is the technology standard for PSD2 consumer authentication and is defined as “an authentication based on the use of two or more elements categorised as knowledge, possession and inherence (something the user is, i.e., biometrics).”

8 Daon white paper on biometrics and PSD2: https://www.daon.com/solutions/psd2-strong-customer-authentication
Being compliant with the latest regulations without putting unnecessary obstacles in the customer’s way is essential for banks and payment providers; almost 80% of the study participants realised increased compliance benefits as a result of deploying biometrics.

In addition to being compliant with state and financial regulation, biometrics can have a positive effect on fraud management. Financial fraud in the UK alone costs the industry over £768m (2016). Biometrics has the ability to deter and combat financial fraud and even a modest 1-2 percent reduction could lead to a $20M saving for the UK financial services industry. Individual organisations can easily assess what a 1-2 percent reduction in their fraud would be annually.

A respondent in the biometrics business benefits survey was keen to point out that it is “easier to track a fraudster” when using biometric technology. A combination of passive and active biometrics that leverage a combination of biometric modalities that include face, voice and behavioural biometrics and also includes strong anti-spoofing techniques are an essential tool in combating financial fraud.

The fraud reduction is remarkable figure bearing in mind that we are at the beginning of the curve for deploying biometric technology in financial institutions.

---

9 https://www.financialfraudaction.org.uk/fraudfacts17/assets/fraud_the_facts.pdf
With the development and increasing rise of digital bank channels, traditional banks now have many distinct channels to support including the physical (branch and automated), telephone, web, mobile and new emerging channels such as those enabled by IoT devices. Supporting these channels and managing identity and authentication in all of them can be a complex and costly business – especially if you have to rely on legacy technology.

It is quite common for a bank to have to support multiple authentication methods – an authentication scheme targeted for each channel approach. This could include knowledge-based authentication (KBA) for a visit to a bank branch, an EMV card with PIN authentication at the ATM, an OTP hardware token for web-based banking, SMS OTP for mobile banking and a mixture of KBA and passive voice authentication for telephone banking channel. That equates to five separate authentication systems to support all of these channels. This also means potentially five different authentication vendors with five different licensing models for five different account teams to manage.

A modern platform should support authentication requirements for all bank channels – a single platform for a modern omni-channel banking strategy. This offers significant cost savings for banks and also benefits bank customers in that they no longer have multiple different authentication mechanisms to use and manage. By adopting a single scalable biometric authentication platform, it has the effect of enhancing customer experience, reducing friction, eliminating passwords and reducing operational costs for banks.

For a typical bank, if the average cost of a single authentication system is $500,000 annually then a bank may be spending a total of $2.5m annually to support five bank channels where these systems and costs are spread across the bank. By replacing five different authentication systems with a single authentication platform that supports all channels, then your typical bank would save in the region of $1m-$2m annually.

**EMVCo 3D Secure 2.0:** EMV® Three-Domain Secure (3DS) is a messaging protocol developed by EMVCo to enable consumers to authenticate themselves with their card issuer when making card-not-present (CNP) e-commerce purchases.

**Polarify:** is an identity service available to consumers in Japan allowing them to register and use a single biometric-enabled mobile app to log in to a range of different services. See https://polarify.co.jp/
SMFG/SMBC IT Innovation Dept. foresaw the rising demand for innovative authentication techniques in the Japanese market place. Due to consumers’ willingness to adopt biometrics and our desire not to build biometric authentication capability in silos for each SMFG/SMBC business unit that might require it, we decided to offer this as a platform and established Polarify on May 1st 2017.

Already 20 customers have selected Polarify in less than 12 months of operation and user feedback is positive. The business benefits for our customers are very strong as biometric authentication facilitates existing expensive business processes to be moved to much more cost effective digital channels.

Tomohiro Wada | President and CEO, Polarify, Inc.  
General Manager of IT Innovation Dept.  
Sumitomo Mitsui Financial Group | Sumitomo Mitsui Banking Corporation
This study from Goode Intelligence explores the tangible business benefits including ROI from deploying a biometric authentication platform. It is based on Goode Intelligence’s expertise in research and analysis of authentication and identity technology and uses primary information gathered from a survey of organisations that are using biometric authentication services for consumer facing implementations.

A combination of identity insecurity and usability issues is causing organisations to research new ways of correctly identifying and securely authenticating their customers. In choosing an authentication strategy as part of digital transformation efforts or replacing legacy systems, organisations need to consider an authentication platform that supports a range of use cases over a range of channels integrating device intelligence, multi-factor authentication and all type of biometrics, including native (device) biometrics.

This business benefits study has been created using both quantitative and qualitative methods including:

- Market research survey of biometric authentication users
- Interviews with key biometric authentication users
- Senior analyst research
- Analysis and market research data obtained from Goode Intelligence’s primary research in the biometric authentication market
- Material obtained from Daon customers
THE RESULTS OF THE RESEARCH GIVE A DEFINITIVE ROI FOR DEPLOYING BIOMETRIC AUTHENTICATION SUMMARIZED IN THE GRAPHIC BELOW.

**Better Customer Engagement**
- 62% of respondents rated 'high' and 'very high' to a question whether they had seen "increased customer satisfaction benefits as a result of deploying biometrics."

**Reduced Contact Centre Costs**
- 56% of respondents were seeing reduced call centre call volume benefits as a result of deploying biometrics. *Cost savings to a five million customer bank of $6.25m annually.*

**Compliance With Strong Customer Authentication**
- 78% of the survey respondents are seeing increased compliance benefits as a result of deploying biometrics particularly addressing Open Banking/PSD2 Strong Customer Authentication.

**Increase to Net Promoter Score**
- 45% of respondents rated ‘very high’ to the question "my organisation has seen an increased NPS as a result of deploying biometrics."

**Eliminate Expensive OTP SMS Costs**
- An estimated $20.75 million saving for eliminating SMS OTP costs annually.

**Security Benefits**
- 56% of survey respondents are already seeing the benefits of reduced fraud from deploying biometric technology.

**Benefits of Single Authentication Platform for Omni-Channel Banking**
- By replacing five different authentication systems with a single authentication platform that supports all channels, then your typical bank could save in the region of $1-2m annually.

10 The savings have been calculated for a typical bank that has five million customers.

www.goodeintelligence.com | Goode Intelligence © 2018
This study concentrates on the business benefits of biometric authentication but it is also an opportunity to briefly discuss some of the customer benefits that truly personal authentication provides.

Goode Intelligence recognises Daon’s IdentityX authentication platform as a solution that blends convenience and security making it an ideal solution achieving the benefits described in this paper. Customers of IdentityX include Mastercard, Visa, USAA, Atom Bank UK, Akbank Turkey, Dah Sing Bank Hong Kong, Gulf Bank Kuwait, BNP Paribas Wealth Management and the New Zealand Department of Internal Affairs among others.
**Multiple biometrics:** Supports face, voice, finger, behavioural and emerging biometrics.

**Best of the biometric industry:** Supports algorithms from multiple vendors, providing customers with the "best of breed" for a particular application and future-proofing the solution to take advantage of tomorrow’s developments.

**Biometric capture security:** Supports multiple layered biometric security functions to ensure the presence of a live person for face and voice biometrics.

**Extensive policy control:** Overall aspects of authentication – biometric type(s), confidence, attempts, device capabilities. This provides customers maximum flexibility in balancing convenience for users with the security required for high-value transactions.

**Multi-tenant:** Allows different business units to be managed independently of each other.

**Scalability:** The core technology has scaled to populations of hundreds of millions of users. Some customers exceed 1,000 authentication transactions per second.

**High-Availability:** Deployed in highly-available and disaster recovery configurations.

**FIDO Certified Server:** Can be configured as a FIDO UAF Server and has been certified in this configuration and includes FIDO 2.0 (W3C Web Authentication) with support for U2F.

**FIDO Certified Clients:** FIDO iOS and Android clients.

**Flexibility:** Provides flexible integration options (SOAP/ RESTful APIs), match-on-server or match-on-device, supports in-band and out-of-band use cases.

**Multiple channels:** Can be integrated to give a consistent authentication experience across different channels/use cases including mobile, website, ATMs, call-centres and in-person. Also includes QR codes, notifications and other methods.

**Deployment options:** As a ‘Service’ or ‘On Premise.’
ABOUT GOODE INTELLIGENCE

Since being founded by Alan Goode in 2007, Goode Intelligence has built up a strong reputation for providing quality research and consulting services for the biometric and authentication sectors.

We publish analyst and market intelligence reports, provide custom technology-driven market research and act as trusted advisors to our clients. For more information on this or any other research please visit www.goodeintelligence.com.

ABOUT DAON

Daon is an innovator in developing and deploying biometric authentication and identity assurance solutions worldwide. Daon has pioneered methods for securely and conveniently combining biometric and identity capabilities across multiple channels with large-scale deployments that span payments verification, digital banking, wealth, insurance, telcos, and securing borders and critical infrastructure. Daon's IdentityX® platform provides an inclusive, trusted digital security experience, enabling the creation, authentication and recovery of a user’s identity and allowing businesses to conduct transactions with any consumer through any medium with total confidence.

For more information on Daon, please visit www.daon.com.