# Callsign Comments on National Institute of Standards and Technology (NIST) Call for Comments: Digital Identity Guidelines

To: dig-comments-RFC@nist.gov

Callsign Company Overview

Founded in 2012, Callsign's mission is to seamlessly power the identification of every web, mobile and physical interaction.

Callsign products use deep learning techniques to combine event, threat, and behavioral analytics with multi-factor authentication, securing access to services whilst uniquely ensuring the most frictionless and transparent user experience.

We provide risk intelligence in real time, enabling organizations to intelligently adjust authentication journeys, also in real time. By pinpointing suspicious access attempts, we can step up and step down the authentication requirement, catching fraudulent activity more effectively while simultaneously removing friction for legitimate users.

Apart from looking to keep people safe from fraud, we are also looking to make their digital lives better with ubiquitous technology that works for all, regardless of circumstance.

Relevant Topics

Callsign's comments relate to the following topics of interest to NIST:

- Privacy enhancements and considerations for identity proofing, authentication, and federation, including new developments in techniques to limit linkability and observability for federation.
- Continued use of short message service (SMS) and public switched telephone networks (PSTN) as restricted authentication channels for out-of-band authenticators.
- Security and privacy considerations and performance metrics for the use of behavioral characteristics as an authentication factor.
- Additional controls and mitigation to address the ongoing evolution of threats such as phishing and automated attacks.

Callsign Comments

## Digital identity solutions should be privacy-first and event-driven

Privacy laws and regulations such as the General Data Protection Regulation (GDPR) in Europe aim to put ownership and control of data back in the hands of the user. One of the seven key principles of GDPR is Data Minimization. This requires the collection of a user's personal data to be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"[1].

This is an important consideration when collecting user information for verification or authentication purposes. There should be controls over when and what data gets added to a user's profile, with only the necessary information being collected and processed rather than extraneous material (for example websites the user has visited). Privacy should be about following the spirit as well as the letter of the regulation.

Continuous authentication, the monitoring of user activity before and after an authentication event, is often proposed as a method of enhancing fraud prevention. Based on regulations such as GDPR, we believe that continuous authentication does not represent user privacy and arguably does not apply the best practice principles of Data Minimization. The monitoring of every aspect of a user's journey is not necessary for the purposes of authentication.

Event-driven authentication solutions that only capture the necessary data at specific points during a user's journey can deliver best in class security while building trust with users.

**User privacy should be a key requirement for identity solutions**

Privacy enhancements and considerations should be a key objective in the design of identity verification and authentication solutions. The following privacy hierarchy framework provides a means by which we believe systems can be designed to deliver best practice user privacy:

1. **Design systems with privacy in mind** as a fundamental requirement.
2. **Minimize data collection**. Validate the business value or need for the data items being collected. This is especially important when designing Artificial Intelligence (AI) or automated processing systems.
3. **Consider client-side controls** to constrain the accuracy of data, particularly any Personal Identifiable Information (PII), at source. This could be through the use of obfuscation techniques which, in the example of location data, will prevent a system building up an exact picture of location history and linking it to an individual.
4. **If data is consumed and processed, consider platform side controls** to inhibit revealing the underlying data. For example, pseudonymization techniques can be used alongside encryption, both at rest and in transit, to convert data into less human readable forms.
5. **If data is consumed and accessed, consider the above plus restrictive controls**. For example, anonymization techniques or role-based access patterns based upon data usage requirements.

Beyond privacy regulations, there are important ethical considerations associated with the use of AI models in identification solutions. When models are trained or evaluated on population groups, it is essential that they avoid any predictive biases towards specific genders, cultural or ethnic backgrounds.

Organizations should implement a framework to monitor the accuracy of predictions and pre-empt degradation in the form of prediction performance, enrolment performance or bias.

## Behavioral biometrics should be promoted as a secure method of authentication

Behavioral biometrics provide a simple and secure method of authentication. It reduces the risks of fraud, isn't reliant on users remembering PINs or passwords and is a more accessible option than biometrics. Behavior can be collected passively while users input data or interact with their device, through the analysis of keystrokes and mouse movements, without adding friction to the journey. And completely new methods such as Swipe (gesturing to provide a non-repudiable digital signature) provide innovate ways for users to easily authenticate themselves.

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/

**European and UK regulators support the use of behavioral biometrics for authentication**

The European Banking Authority (EBA) has recognized that of the different authentication elements (inherence, knowledge and possession), inherence is the most innovative and fastest moving. Identifying a user by the way they type and swipe, and the angle at which they hold a device, was highlighted by the EBA in June 2019 as a compliant way to achieve inherence for Strong Customer Authentication (SCA) as part of the EU's Second Payment Services Directive (PSD2)[2].

The financial services industry and online retailers across Europe are required to implement SCA for e-commerce payments. In the UK, the recommended industry approach, as set in early 2020, is for behavioral biometrics as the second authentication factor alongside possession. This position was established by the financial services trade body, UK Finance, and has been welcomed by the UK's Financial Conduct Authority (FCA)[3].

**Behavioral biometric solutions must positively identify the user**

An important requirement for behavioral biometric solutions is the ability to positively identify the user. Fraud prevention solutions exist that aim to detect behavioral anomalies during an authentication journey such as those arising from BOTs or bad actors. However, these solutions alone do not positively identify the user and therefore do not achieve an inherence element for authentication.

**Model score performance can be enhanced through ensembling**

Best in class solutions can combine behavioural biometric modelling with user device and location information to strengthen authentication capabilities. Combining these modalities to create a single score, in a process known as ensembling, gives a robust method by which we can positively assert an individuals' digital identity. Our research shows that by running device and location analytics alongside behavioural biometrics, we further enhance model score performance.

## Vulnerabilities in SMS OTPs have decreased their effectiveness as an authentication channel

SMS One-Time Passcodes (OTPs) have become the principal authentication factor for many user journeys, be that logging in to online services, verifying a password change or making a payment. This has in part been driven by the new PSD2 SCA requirements in Europe. Although the move to multi-factor authentication is a welcome enhancement to user security, we believe that current approaches represent only the first stage in the evolution of digital authentication.

**Security risks associated with SMS OTPs are becoming increasingly apparent**

Whilst a seemingly simple and easy to implement solution, it is becoming increasingly apparent that the use of SMS OTPs for authentication has significant security weaknesses. Fraudulent attacks on SMS OTP, whether using sim swaps, call forward or SS7 network attacks, are evolving and becoming more difficult to detect and prevent. In addition, users are being phished to share SMS OTPs with fraudsters presenting themselves as representatives of a reputable bank or merchant.

In their 2019 Annual Review[4], the UK Government's National Cyber Security Centre (NCSC) recognized a recent rise in the sophistication of SMS interception attacks, with multiple financial institutions and Communications Service Providers being affected. In November 2019, the NCSC issued guidance[5] to organizations highlighting that SMS technology was never intended to be used to transmit high risk content and that there are a number of inherent weaknesses in the ecosystem that supports SMS.

Compensating controls and security methods exist that aim to reduce the risk of compromise. Cross-referencing user information with live Mobile Network Operator (MNO) intelligence data during an interaction or transaction provides a means of flagging potentially fraudulent or high-risk activity. This can include looking for whether SIM swap has recently taken place, whether a call forward exists on the number, fraud checks on the phone and whether the phone number is associated with the account.

The NCSC has recognized, however, that while mobile telecoms companies are actively working to address vulnerabilities, the issues associated with SMS are complex and it may be impossible to fully compensate for the inherent weaknesses of the system. As a result, we believe that the industry should be actively moving towards the use of alternative and more secure authentication methods.

[2] https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf?retry=1
[3] https://www.ukfinance.org.uk/system/files/Strong%20Customer%20Authentication%20-%20Considerations%20for%20what%20can%20be%20used%20as%20a%20second%20factor%20alongside%20One%20Time%20Passcode%20%28OTP%29_0.pdf
[4] https://www.ncsc.gov.uk/annual-review/2019/ncsc/docs/ncsc_2019-annual-review.pdf
[5] https://www.ncsc.gov.uk/guidance/protecting-sms-messages-used-in-critical-business-processes

**SMS OTP should not be a long-term industry solution**

While we welcome NIST's categorization of SMS OTPs as a Restricted Authenticator, we believe the guidance should go further and should set a deadline to no longer support the use of SMS OTP as an out of band authentication channel. The threats associated with SMS OTPs have evolved, degrading the ability of this channel to resist attacks to such an extent that we believe this update to guidance is warranted.

Given NIST's strong international influence, this messaging would be a positive and important step in pushing the authentication industry towards implementing more secure and future-proof solutions.

**Alternative authentication methods including the use of Behavioral Biometrics should be promoted**

For the purposes of proving possession for authentication, alternative and more secure methods exist. In Europe, the EBA has recognized that approaches relying on mobile apps, web browsers or the exchange of public and private keys can be used as evidence of possession, provided that they include a device-binding process that ensures a unique connection between the user's app, browser or key and the device[6].

New technologies offer secure and reliable methods of device identification that are privacy-preserving. There are different ways of achieving device binding including through dynamic device fingerprinting and continuous learning of evolving fingerprints to ensure a unique and persistent connection between the user and device. Alternatively, binding can be achieved through public or private key generation and exchange between the device and communicating platform. Keys securely stored on a device can be used to re-identify it to the communicating service provider.

More than one method can be used concurrently to further strengthen the binding of a device. Controls and conditions on when to bind a device can be driven through confidence score thresholds, absence of detected threats and strong authentication.

It is our view that the use of behavioral biometrics on a securely bound device represents a significantly stronger method of authentication than reliance on SMS OTPs. We believe that this should be recommended as an alternative industry approach to SMS OTP.

**In the short term, implementing behavioral biometrics alongside SMS OTP can provide an extra layer of security**

While our recommendation is for the industry to move to more secure authentication methods in the future, we recognize that SMS OTP is a widely utilized channel at present. Where the use of SMS OTP is unavoidable in the short term, or while organizations look to make the transition across to more secure methods, there are ways in which additional security can be built in.

By capturing behavioral biometrics alongside the entry of the OTP, it is possible to verify that the genuine user is initiating the transaction or interaction. This can be achieved by asking the user to enter their email address, phone number, a short memorized PIN, or other familiar data item as part of the user journey. As well as providing an additional layer of authentication, increasing confidence in the secure delivery of the OTP (that is has been delivered to the genuine user), this also put organizations in a strong position to increase their reliance on behavioral biometrics and make the future transition away from SMS OTP.

## By predicting the next evolution of automated attacks, the industry can stay one step ahead

One of most adaptable and fastest growing threats in the world of cybercrime comes in the form of automated attacks. Malicious bots are a significant threat to critical infrastructure and security systems. The latest advance in this threat has seen the rise of more technologically sophisticated 'parasitic' bots or Botnets, which are capable of mimicking human behavior on web pages.

Looking ahead to the next evolution of threat, criminals are beginning to make use of data from distributed malware which is capable of keylogging and recording mouse movements. Cutting edge methods in Deep Learning and AI have shown the capability of learning and then simulating advanced human actions such as paintings, writing and even speech.

These methods rely on Generative Adversarial Networks (GANs), which consist of two separate AI's working against one another to better learn and understand any given data distribution such as human behavior. This method could be used by criminals to feed a GAN data on how a particular individual behaves, on a particular webpage. This algorithm could then generate new behavior points that appear as if they have originated from the same user.

[6] https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf?retry=1

While this threat does not currently exist, the following will still hold true. Any malicious bot that is designed to simulate human behavior or interact with a webpage has ultimately been programmed to execute a set of instructions or code. It is not able to dynamically alter its interaction with a web page the same way humans do and ultimately will still leave a trail of breadcrumbs in the data points that highlight its programmatic nature. These signals will be harder to detect but will always be present when bots are used.

**Fraud prevention solutions must be able to adapt to any threat**

Modern cyberattacks have advanced to the point where a blanket approach to security is not enough. Fraud prevention solutions need to be able to react to every variant of every threat on an individual basis, to provide a full spectrum of coverage and defend against attacks.

Combining this with authentication solutions that understand an individual user's device, behavior and location, can provide a full suite of security without reducing usability.

**Intelligent authentication solutions should help protect against social engineering**

Social engineering fraud has become an increasingly important topic over the past few years, with fraudsters going to increasing lengths to defraud individuals. Tactics include users being tricked into sharing sensitive information that compromises security or making payments to the incorrect recipient. In the UK, Authorized Push Payment (APP) scams alone cost the financial services industry over £450million in 2019[7].

Authentication solutions should employ intelligent mechanisms and dynamic intervention to protect users from social engineering. Solutions should be able to detect in a passive and seamless way whether or not the consumer, who may themselves be genuine, is being manipulated as part of a social engineering attack.

**We would welcome the opportunity to discuss any of these topics with NIST and to contribute to further development of the Digital Identity Guidelines.**

To discuss content of this response, please contact:

Rachel Bentley.

[7] https://www.ukfinance.org.uk/system/files/Fraud-The-Facts-2020-FINAL-ONLINE-11-June.pdf