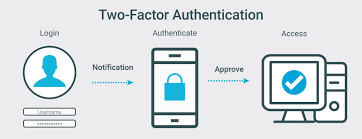
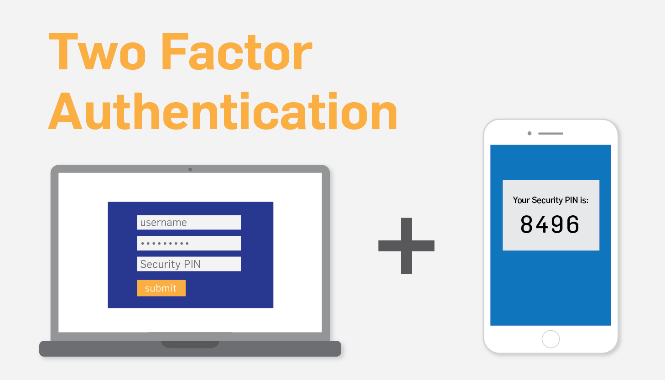
Mobile Multi Factor Authentication Solution

# 1 Background

Before addressing the question ‘what is two-factor authentication’ or ‘what is 2FA,’ let’s consider why it’s important to do everything you can to improve your online account security. With so much of our lives happening on mobile devices and laptops, it’s no wonder our digital accounts have become a magnet for criminals. Malicious attacks against governments, companies, and individuals are more and more common. And there are no signs that the hacks, data breaches, and other forms of cybercrime are slowing down!

Luckily, it’s easy for businesses to add an extra level of protection to user accounts in the form of two-factor authentication, also commonly referred to as 2FA.



Two-factor authentication replaces traditional user name and password with strong identity-based authentication.

2FA is an extra layer of security used to make sure that people trying to gain access to an online account are who they say they are. First, a user will enter their username and a password. Then, instead of immediately gaining access, they will be required to provide another piece of information. This second factor could come from one of the following categories:

Something you know, such as a personal identification number (PIN), password or a pattern

Something you have, such as an ATM card, phone, or fob

Something you are, such as a biometric like a fingerprint or voice print

With 2FA, a potential compromise of just one of these factors won’t unlock the account. So, even if your password is stolen or your phone is lost, the chances of a someone else having your second-factor information is highly unlikely. Looking at it from another angle, if a consumer uses 2FA correctly, websites and apps can be more confident of the user’s identity, and unlock the account.

Let’s look at the most common forms of 2FA.

Hardware Tokens, SMS Text-Message and Voice-based, Software Tokens, Push Notification, Other Forms of Two-Factor Authentication

The main SMS 2FA weakness is the dependency on the service provider. ... If your OTP is delivered via SMS, all the hackers need to do is get the ownership of your phone number. A criminal impersonates their target and convinces the provider the user's phone is lost so the number needs to be transferred.

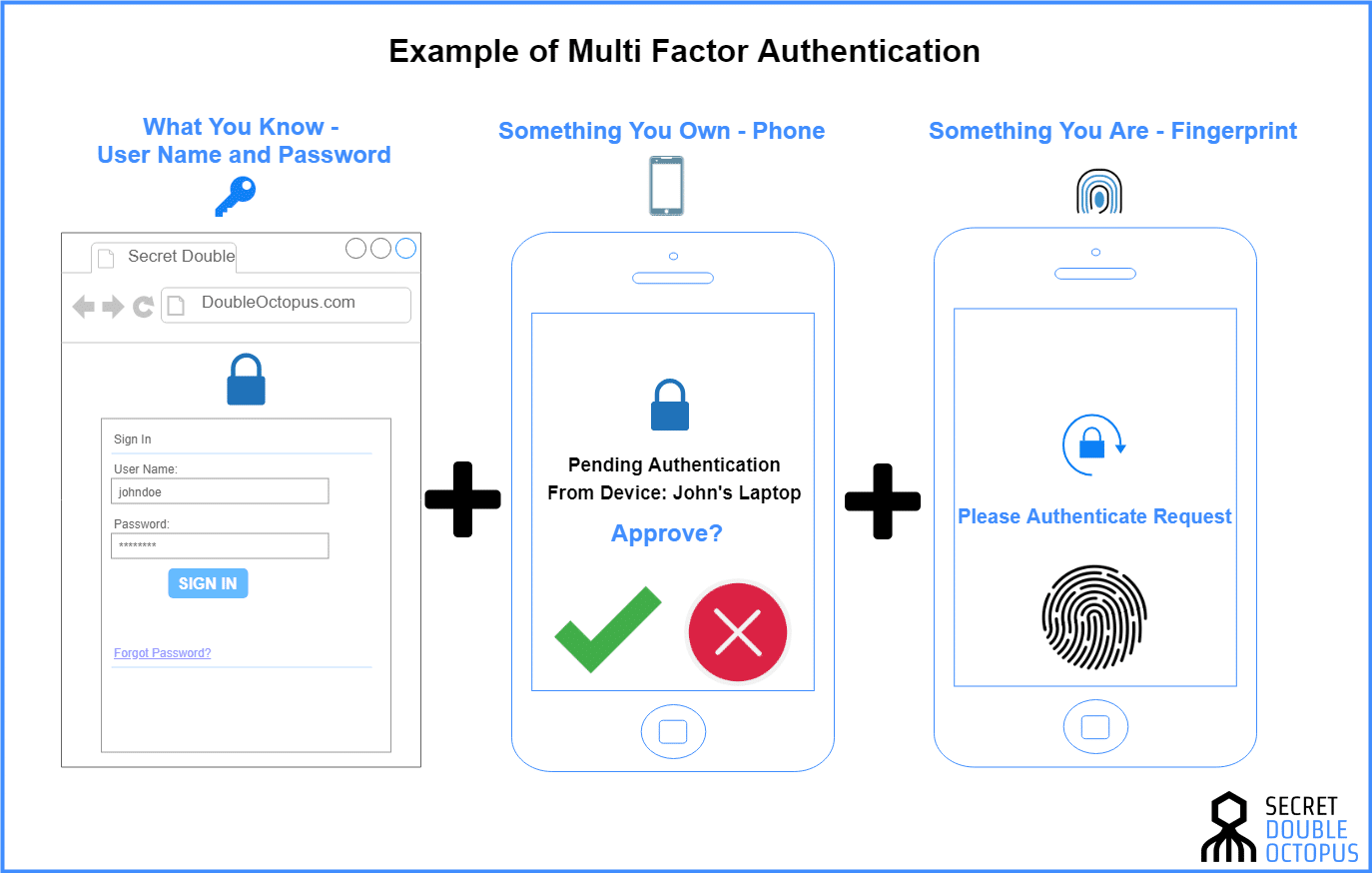
Although any form of multi-factor authentication is a considerable improvement on simple password models, SMS-based verification tokens can be stolen with a variety of well-known techniques, including social engineering, mobile malware, or by directly intercepting and decrypting signals from cell towers.

The most common technique is most likely use of smartphone malware, which automates the process of stealing passwords and obtaining verification codes while obfuscating the activity from the end-user, but this seems less likely in such a targeted campaign.

These are all possibilities, but it may be as simple as calling up the victim’s cellular provider and convincing them to transfer the phone number to a new SIM.

So we need to use MFA.

# 2 Methods



Multi-factor authentication is an electronic authentication method in which a device user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge, possession, and inherence.

The difference between MFA and 2FA is simple. Two-factor authentication (2FA) always utilizes two of these factors to verify the user's identity. Multi-factor authentication (MFA) could involve two of the factors or it could involve all three. “Multi-factor” just means any number of factors greater than one.

Here we will add HOTP Password, Hardware backed attestation validation (Android)Mobile session, Device Profiling, Account activity Notification, Native login functions into current controls including Single session, Device Binding, App & Device Integrity, App Obfuscation, Certificate pinning, Replay Protection, Time Based One Time Password

The HOTP algorithm specifies an event-based OTP algorithm, where the moving factor is an event counter. The present work bases the moving factor on a time value. A time-based variant of the OTP algorithm provides short-lived OTP values, which are desirable for enhanced security

Device profiling allows you to gather device type and operating system information by inspecting packets that are sent by these devices in the network. For example, you can identify that a device is a smart device, a laptop, a printer, or IP phone.

When we use Hardware backed attestation validation and Native login, it is more secure because user signs up or enters their credentials directly into the app and allows the device to provide proof of its hardware security information.

Customers who use mobile banking account activity alerts are slightly more likely to detect and contact their bank regarding fraud or unauthorized account.

By minding the type of authentication factors used, we can find that right balance of security and convenience needed to make the authentication process secure enough without interfering with the user experience.

# 3 Conclusion

Multi-factor authentication is clearly the more secure authentication method, as it considers two or more authentication factors, making it harder for attackers to bypass the additional layers of security.

If you're going to step up security by going beyond passwords and even past traditional two-factor authentication, you don't want it to slow down or frustrate your users.

One way to keep things simple for them is to use a risk-based approach that that transparently verifies who they are, and automatically asks for additional authentication only when the risk they present warrants it. For example, if a user is signing in on the same device, to the same applications and from the same location every day, the risk that they're not who they say they are is low-so the system shouldn't require them to jump through hoops to login. However, if they suddenly travel to another country and attempt to log in from a strange location, you'll want to reconfirm their identity with convenient step-up authentication options. For that, you need a variety of authentication choices including Hardware backed attestation validation, HOTP Password, Device Profiling, Account activity Notification and more.

Avoid making MFA onerous; choose when the extra authentication is needed to protect sensitive data and critical systems rather than applying it to every single interaction. Consider using conditional access policies and Azure AD Identity Protection, which allows for triggering two-step verification based on risk detections, as well as pass-through authentication and single-sign-on (SSO).

Offer a choice of alternative factors so people can pick the one that best suits them. Biometrics are extremely convenient, but for example some employees may be uncomfortable using their fingerprint or face for corporate sign-ins and may prefer receiving an automated voice call.

Make sure that you include mobile devices in your MFA solution, managing them through Mobile Device Management (MDM), so you can use conditional and contextual factors for additional security.

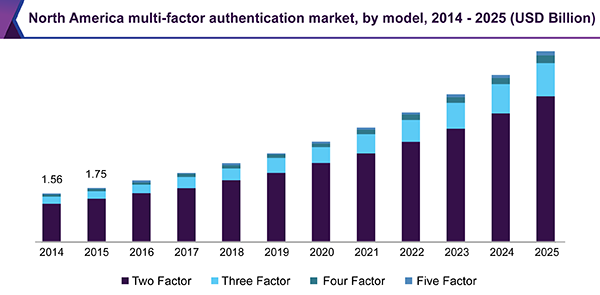
One to highlight is that using risk-based approach we can complete this since we provide the same or better level of comfort and enhancing security.

In the end, we can use Multi Factor Authentication (MFA) option that reduces friction in client experience but provide the same level of comfort (or better) that digital certs currently provide for financial transactions clients

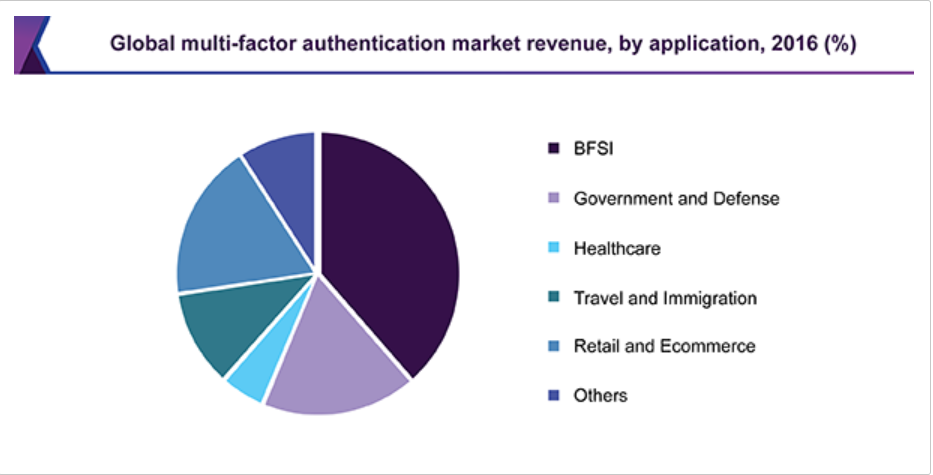
# 4. Appendix

## Marketing Analyze

Rising investments in cloud technologies, enterprise mobility, and increasing adoption of BYOD across enterprises are anticipated to further boost the adoption of multi-factor authentication solutions. Advent of authentication-as-a-service solutions, which offer advanced security and authentication to organizations, is also projected to bolster the growth of the market.



Companies such as CA Technologies; Vasco Data Security International, Inc.; RSA Security LLC; and Symantec Corporation are making significant investments in R&D to develop new authentication products, solutions, and services.



Cost and implementation complexities will act as a restraint for the market; however, their impact will decrease with time. With the rise in data and security breaches, most of the industries have launched data security standards. To address security breaches and cyber-attacks, enterprises have adopted MFA solutions. These solution implementations are complex in nature and at the same time require more capital investment for procurement, implementation, maintenance, and management. Heterogeneous IT environments across industries further increase the complexity.



The overall investment for implementing MFA is estimated to be high owing to an increase in support services, training, SMS gateway, and hardware and software tokens. Requirement of additional drivers for physical authenticators and interoperability with varying IT environments increase the complexity of deployment. Hence, issues pertaining to cost of procurement and complexity of implementation are poised to limit the widespread adoption of multi-factor authentication solutions.

## 8 reasons to support use of multi-factor authentication

These data points support the need for MFA.

1. Identity theft is an easy, low-risk, high-reward type of crime and a threat to all businesses. It is the fastest-growing type of crime and is now more profitable than drug-related crimes.
2. Weak or stolen user credentials are hackers' weapon of choice, used in [95 percent](http://www.verizonenterprise.com/DBIR/2015/) of all Web application attacks.
3. From 2013 to 2014, the number of successful breaches went up by 27.5 percent. The malicious actors are winning the war.
4. Headlines tend to belong to the household-name companies, but they are not the only companies being targeted. Of all targeted attacks, [31 percent](http://www.symantec.com/security_response/publications/threatreport.jsp) are aimed at businesses with fewer than 250 employees.
5. Anti-virus systems and advanced firewalls are necessary security elements, as are vulnerability tests. Without user authentication, though, the front door is wide open to intruders.
6. Password theft is constantly evolving as hackers employ methods like keylogging, phishing, and pharming.
7. Cyber criminals do more than merely steal data. Often they destroy data, change programs or services, or use servers to transmit propaganda, spam, or malicious code.
8. Employees are already accustomed to authenticating themselves in their personal lives, as providers of online services like home banking, gaming, social media, and email have all adopted mobile-based tools to effectively authenticate their users when accessing their systems.