Two-Factor Authentication over Mobile: Simplifying Security and Authentication
Controlling Fraud and Validating End Users Easily and Cost-Effectively
About the Author

William Dudley is group director and mobile evangelist of global strategy and solutions at SAP. He has almost 30 years of experience building and managing telecommunications network infrastructures. He defines global strategy and solutions for the SAP Digital Interconnect group (formerly SAP Mobile Services), within the mobile ecosystem, focusing on solutions for messaging, next-generation networks (LTE, IPX), and mobile consumer engagement.

As mobile evangelist, Mr. Dudley communicates through both internal and external publications and is active in industry groups.
Two-factor authentication (2FA) is a means of controlling fraud and verifying end users. It can be implemented in a number of forms, by using software or hardware tokens or engaging through mobile devices. When implemented correctly – especially when using mobile devices – 2FA is a low-cost solution that is easy to implement, easy to use, and an effective deterrent to fraud – thereby protecting both the end user and the enterprise.
Two-Factor Authentication over Mobile: Simplifying Security and Authentication

Selecting the Key Factors for Two-Factor Authentication

2FA is a form of multifactor authentication. It requires at least two authentication factors, which may comprise:

- A knowledge factor – something only the user knows, such as a password or personal identification number (PIN)
- A possession factor – something only the user possesses, such as an ATM card, mobile device, or hardware token
- An inherence factor – something unique to the user, such as a fingerprint or retina pattern

2FA is often used in situations where the user must be accurately identified. A common illustration is the ATM usage scenario. The user swipes an ATM card (something the user possesses) and then enters a secret PIN (something the user knows). Without both authentication factors working, the user can’t withdraw cash from the ATM.

For many years, to secure access to corporate or government systems and more, organizations around the world have relied on hardware tokens (something that you have) along with user IDs and passwords (something that you know).

Recently, enterprises also have been able to make use of mobile devices as a common “something that you have.”

Using mobile devices for 2FA opens up a variety of use cases that make it difficult for many hardware-based “key fob” devices to adequately compete. For example, many smartphone apps can generate 2FA PIN codes of varying lengths that replace the dedicated hardware token. Such apps use industry standard algorithms to generate PIN codes that synchronize with server-side applications and Web sites to enable a second authentication for end users.

The goal of 2FA is to reduce instances of online fraud such as monetary theft or identity theft. While there are variations in the manner in which an individual can be authenticated (including the “something that you are” – the inherence factor), the strength of 2FA lies in the strength of its implementation – in particular, the strength of the two factors that are used to identify the individual.

2FA aims to reduce online fraud. Its strength lies in the strength of the two factors that are used to identify the individual.
When 2FA is deployed in a mobile ecosystem, safeguards must be in place to allow 2FA implementations to function securely and at all. Safeguards may include:
- Providing the second authentication factor through SMS messaging
- Using a dedicated application to generate the second authentication
- Employing biometric sensors on the mobile device
- Delivering tokens through some other channel such as push notifications

Each of these safeguards must be considered in light of the security offered, benefits obtained, ease of use, and ease of implementation.

**TWO-FACTOR AUTHENTICATION OVER SMS**

A popular way to deliver one-time passcodes or 2FA authentication tokens (PINs, alphanumeric codes, and so on) is to send the token to a registered mobile device in a text message. With growing digital transformation, social networks, digital commerce, and financial institutions often use 2FA for resetting passwords, authorizing users, and validating transactions. Delivery of 2FA tokens over SMS typically is reliable and quick and uses a medium that virtually every mobile device can support.

As a delivery channel for 2FA tokens, SMS is easy to implement and easy for the end user to employ. Today, most mobile users have received some sort of 2FA code over SMS. It’s a very popular means of providing a second authentication method. While software alternatives to 2FA over SMS are common, they usually rely on the user having a smartphone and downloading an app. In contrast, SMS is available to all mobile devices – smartphone or not – and in all regions.

Enterprises looking to implement 2FA with mobile devices should consider SMS as their first choice. Typically implemented using simple application programming interface calls, SMS can deliver a passcode that is already generated or, better yet, it both generates and delivers the message and then authenticates the code entered by the end user. Additionally, SMS can integrate easily into existing workflows.
While SMS is not inherently encrypted as the messages are transmitted over mobile networks, it’s still a high-security solution. 2FA tokens generally have a short expiration time – usually no more than a few minutes. Further, there are limits as to how many times a user may try to enter a received code before being locked out of an application for a specific period of time. While no scheme is 100% secure, 2FA over SMS works because, in virtually all situations, it provides enough security and confidence to protect both enterprises and end users from fraud. The figure depicts sample SMS-generated codes received on mobile devices.

When SMS is used, the delivery provider should make use of as many direct mobile operator connections as possible, using all high-quality routes, since many of these 2FA tokens have short expiration times. It is imperative that these SMS messages comply with all regulations and best practices for the country for which they are intended. Service providers that offer lower-cost or least-cost routing for 2FA traffic run the risk of their messages being delayed or blocked entirely (for example, leveraging the so-called grey routes for SMS).

### TYPICAL USE CASES FOR TWO-FACTOR AUTHENTICATION OVER SMS

Employing two-factor authentication (2FA) over SMS enables a number of use cases that support greater security and confidence for your enterprise. For example, 2FA over SMS allows you to:
- Automate mobile devices while managing unrecognized IP addresses
- Enable secure logins by requiring users to input an additional code sent to their mobile devices
- Confirm user registration while using verification codes to validate mobile devices
- Enable more secure e-commerce transactions by validating a transaction with a code sent to the mobile device
- Reset an end-user password by sending a one-time passcode to the user’s mobile device
- Validate money transfers using one-time passcodes to confirm secure transactions
- Support marketing or couponing engagement by sending codes to mobile devices, so users can enter codes to obtain on-site savings
Using Push Notifications as a Channel – “Smartphone Simple” and More

2FA over SMS isn’t the only route that 2FA tokens generated in the cloud (or server side) can use to reach smartphones. They may also be “pushed” to devices over direct IP links using various mechanisms called “push notifications,” which are typically specific to the mobile operating system.

When push notifications are used, the enterprise or app builder incorporates specific functionality within the mobile app through integration of software development kits (SDKs). Using SDKs, messages sent through the IP connections of a device can be displayed within the app as well as within the notification panels of mobile devices. Both displays are commonly used in Android and Apple iOS devices.

2FA push notifications act very similarly to 2FA over SMS in the sense that the 2FA token is generated on the server side and then transferred to the mobile device. But with 2FA push notifications, instead of using SMS, the data is delivered directly to the mobile app.

There are some limitations that should be noted with 2FA push notifications – especially Android or native iOS push notifications. Some native push messages can time out or be blocked by Wi-Fi firewalls, and some servers stagger deliveries, which can affect delivery time – which is paramount for 2FA tokens. That noted, there are now implementations of push notifications – such as the SAP® Intelligent Notification 365 mobile service – that overcome these limitations, making push a strong channel for 2FA token delivery.

Push notifications work when there is already an enterprise or commerce app that can be leveraged for the purpose of displaying the 2FA tokens. Additionally, this channel is good for markets where most subscribers using the service are also using the mobile app – even if they are engaging through the mobile app. These types of situations are perfect gateways to use a different second factor of authentication – the “something you are.”

Delivery of 2FA tokens over SMS typically is reliable and quick and uses a medium that virtually every mobile device can support.
INCORPORATING THE INHERENCE FACTOR

For in-app authentication, sometimes pushing or generating 2FA codes does not meet the criteria for true two-factor authentication. Instead, we must leverage characteristics about the users themselves – the inherence factor, or the “something they are.” This authentication factor includes fingerprint sensors, retina scans, and other biometrics.

For example, some mobile apps with high-value content such as financial information ask for a user ID and password (something you know or have) and then require a fingerprint scan (something you are). This type of authentication is still only limited to smartphones; however, with today’s penetration of smartphones in most markets, it may eventually supersede other forms of second-factor authentications.

SUMMARY

The usage of a second authentication factor should always be considered as a means of protecting the interests of end users when engaging in the digital world over mobile devices. One of the first considerations should always be that the second authentication factor includes a mobile device – something virtually everyone today has. For simplicity’s sake, nothing really comes close to delivery of 2FA tokens over SMS. Unless you have specific requirements, 2FA over SMS can support many, many use cases.

As authentication requirements become more sophisticated, the inclusion of push notifications and even biometrics through mobile devices should also be considered as strong alternatives to stand-alone hardware tokens and, in many cases, dedicated software-token generators.

LEARN MORE

The SAP Digital Interconnect group, formerly SAP Mobile Services, enables enterprises to aggregate messages globally and reliably.

The SAP®® Authentication 365 mobile service is an end-to-end, portable, and configurable two-factor authentication (2FA) solution for multiple channels that include SMS, push notifications (such as the SAP Intelligent Notification 365 mobile service), and more. The SAP Authentication 365 mobile service is an authentication service add-on for SAP SMS 365, enterprise service. The mobile service provides:

- Integrated connectivity to SAP SMS 365, enterprise service, reaching almost 980 mobile networks through a single, standard interface
- Accurate and fast message routing, utilizing our advanced number resolution system to correctly identify the destination mobile network operator
- High-priority messaging delivery solutions that help ensure fast delivery of 2FA and one-time passcode (OTP) messages
- High-quality, approved routes for reliable delivery of all messaging, including 2FA and OTP messages
- Multiple configurability options for 2FA tokens, as well as a comprehensive administrative and analytics user interface
- Simple application programming interfaces for easy integration of 2FA capabilities into existing workflows