App-less authentication offers big business, security benefits

Issued by Entersekt

28 Sep 2021

As more industries move to secure their data and protect customers, deploying outdated technology that cannot withstand modern security threats is simply bad business practice. For the many companies looking to replace legacy solutions like SMS OTP with stronger authentication mechanisms, or supplement OTP-based solutions with more robust alternatives, GSM authentication offers a compelling solution - both for the business and their customers.

Lincoln Naicker

“SMS OTPs were a good go-to solution, but they are long past their sell-by date. Companies must look for better step-up authentication methods if they hope to fulfil their duties of protecting customers and their data,” says Lincoln Naicker, product owner at Entersekt. “GSM authentication offers an app-less, truly out-of-band, secondary factor that is both low friction and simple to implement. For companies looking to protect all customers against fraud, GSM authentication is a great solution.”

For decades, SMS OTPs were the favoured second-factor authentication mechanism. This was largely for reasons of convenience. Almost everyone has a mobile phone, which is always with them, and everyone is familiar with SMS.

However, it’s been years since we reached the tipping point where security risks posed by (SMS) OTP technology outweigh user familiarity.

“The SMS channel is not considered the most secure for many reasons. Our phones are susceptible to any number of trojans which leverage open access to SMS on mobile phones specifically to intercept OTPs. What’s more, mobile SIM swaps or SIM clones can also significantly devalue this mechanism as an authentication option,” Naicker explains.

GSM authentication is familiar, but far safer

“Reducing SIM-swap fraud is at the heart of the GSM authentication solution. We transform the device itself into a unique identifier, communicating directly with that device through a real-time push notification over the mobile network. This true out-of-band communication means it’s a much more secure solution,” Naicker says.

Using a separate authentication channel makes it more difficult for an attacker to intercept and subvert the authentication process – such as in the case of a man-in-the-middle attack - because it would require the attacker to compromise two communications channels.

In addition to the security aspect, Naicker explains that this slicker user experience remains very familiar, which makes it easy for companies whose customers are used to OTP to deploy GSM authentication with minimal fuss or re-education required. Customers don’t need to register, enroll or sign up – an authentication message is automatically pushed to their mobile phone when they attempt an interaction with their institution that has to be authenticated.

Benefits extend to the organisations deploying GSM authentication

Naicker says that Entersekt has further developed its offering to include patented technologies as well as direct integration with local mobile network operators (MNOs).

“While the customer simply sees a decline or accept message when they are about to log in or make a sensitive transaction, in the background we are applying complex algorithms which check the device identity, but can also see if a SIM has been swapped recently. This information will be flagged to the institution, alerting them to a potentially risky transaction. This fits into the security end-game for today’s businesses that need to do whatever it takes to prevent fraud and protect their customers,” he says.

Businesses that don’t want to force their users to download yet another app, or would like to have a secure fallback authentication method, should their app go down, can also rely on GSM authentication as a step-up option.

Naicker points out that GSM authentication also offers compelling inclusivity benefits.

“This authentication method is perfect for South African companies. USSD functionality means customers don’t have to have a smartphone. This is great for companies where inclusivity is a big priority, especially healthcare, financial services and even government services. This service works beautifully as a simple way to onboard new users and the use cases for this alone are endless,” he says.

An additional benefit for companies looking to transition from SMS is the meaningful cost saving. SMS remains an expensive delivery method and for companies that need to authenticate hundreds of thousands of transactions every day, this can quickly add up.

Finally, Naicker says that while Entersekt’s GSM authentication solution has always had a strong showing with South Africa’s banks and MNOs, they are seeing strong interest from other sectors.

“All local companies now have to show that they are protecting their customers’ and partners’ data. Adding layers of complexity and cost by deploying technology that is no longer safe is just not sensible. For companies looking for a safe, simple solution that won’t introduce additional friction or confuse customers, GSM authentication is a great option.”

About Entersekt

Entersekt is a leading provider of strong device identity and customer authentication software. Financial institutions and other large enterprises in countries across the globe rely on its multi-patented technology to communicate with their clients securely, protect them from fraud, and serve them convenient new experiences irrespective of the channel or device in use. They have repeatedly credited the Entersekt Secure Platform with helping to drive adoption, deepen engagement, and open opportunities for growth, all while meeting their compliance obligations with confidence.