EXECUTIVE BRIEF | APRIL 2017

CA Strong Authentication for Payments

Introducing push notification for in-app authentication

Push Notification— A PSD2 Compliant Solution

The European Commission's second Payment Services Directive (PSD2) was designed to create a single and efficient market for payments. The directive sets out the legal, regulatory, procedural and technological framework for electronic payments within the European Union.

One of the directive's key components is the requirement to implement Strong Consumer Authentication (SCA) within specific aspects of the electronic payment process. In this case, strong is defined as authentication that includes two or more factors:

- **Knowledge:** Something the consumer **knows** (for example, a password or shared secret)
- **Possession:** Something the user **has** (for example, a token, EMV Card, mobile device, etc.)
- **Inherence:** Something the user **is** (for example, a biometric such as a fingerprint)

Push notification is a method of linking a card with a mobile device and protecting that association with a credential—complying with the something you have, something you know or something you are criteria of PSD2. During an online transaction, for example, an authentication request would be pushed to an application—generally an issuer's mobile banking app—on the cardholder's registered mobile device. The cardholder would receive a notification on the device asking them to confirm that they are the person that initiated the transaction. The cardholder would authenticate into their device with a passcode or biometric to access their mobile banking platform, before being presented with the transaction details to authenticate.

How is push notification initiated for the cardholder's device? During a simple, one-time provisioning process, the handset's specific address (or identifier) on the push network—operated by Apple and Google—is registered with CA. This enables a specific application on a specific handset to be targeted by the notification, and provides a high standard of proof that it is indeed the provisioned instance of the app on a specific mobile device, phone or tablet—making the push notification an incredibly robust system that is tough to forge.

Additional server-side security prevents malicious injection of messages into the push network. In other words, to send messages on the push network, you must first be authenticated to the network and you must go through the registration process as a push notification provider—usually by obtaining a credential (such as a certificate in the case of Apple, or an API key in the case of Google).

Push Notification Offers Robust Security

Compared with SMS, a push notification provides robust proof of ownership of the device and installation of a legitimate app. Push notifications are also not subject to the challenges inherent in delivering one-time passwords (OTPs) via SMS. Why? Because push notifications are sent to the registered device via the available data connection—3G, 4G, LTE or Wi-Fi—and not susceptible to SIM Swap attacks, it's more difficult for multiple accounts to be registered to a single, physical device.

This is important because fraudsters have been able to rent SMS-receiving numbers and configure them to point to the same physical device, which allows a single handset to support multiple fake accounts—for example, fraudulent PayPal accounts.

Transparent Data for the Account Holder

PSD2 also states that when a consumer is making a purchase (or undertaking a transaction), the transaction details should be clearly visible to the person who is initiating the transaction. CA Technologies' push notification displays data including merchant name, transaction date/time and amount to the account holder to provide full information of the transaction they're approving. The mobile app receives the push notification and the transaction details are displayed to the user, who approves (or denies, if required) the transaction via the mobile app. The server continuously learns the approval or non-approval behavior in real time, and users can do all the authentication work in the context of their mobile devices.

How Does the Registration Process Work?

There is a simple, one-time setup process that must be performed to associate the cardholder's device with the cardholder's cards. A single app can support multiple cards, so if a customer has both a debit and a credit card from the same issuer, for example, both can be supported in the same app.

Generally, this would happen when the app is first launched. There are two options for registration. If this is occurring in an unprotected area of the application, then the cardholder can be prompted to enter an activation code that would be sent to them by email or SMS in much the same way a card is added to Apple Pay, Android Pay, etc. However, because this provisioning activity generally starts from a protected area of the application where the user has already been authenticated, it is possible to remove the need to manually enter an activation code, and the device can be registered with no manual intervention from the cardholder.

Behind the scenes, CA has registered that device's unique address with the handset provider's notification system (Apple Push Notification System or Google Cloud Messaging) so that any authentication request can be targeted at that specific device.

Getting the Solution Up and Running Is Simple

CA provides a software development kit (SDK) that the issuer can embed into their existing mobile banking application. Alternatively, if the issuer doesn't have an existing mobile banking app, the SDK contains a pre-made sample application which could be taken by the issuer, branded appropriately, then published to Apple's App Store or Google's Play Store.

Push notification is a generic app development technology that's not specific to CA. However, where CA's solution differs lies in our patented cryptographic camouflage, which secures the key material on the cardholder's device and gives issuers the confidence that when an approved response is received, it has actually come from the legitimate cardholder's device.

How Else Is Push Notification Useful?

In principle, anywhere an authentication or authorization is required. For instance, authorizing an online transaction, balance transfer or even making a faster payment, assuming we can link an identifier that can authenticate to a card number/account with the app—which could be a user ID or a mobile number. We strongly encourage banks using this approach to adopt a push strategy in parallel to a risk-based approach, which minimizes cardholder effort and maintains a high level of device-trust analysis. Additionally, push notification provides a significant cost advantage to alternative options such as PIN-generating cards, SMS or physical tokens.

Next Steps

Final draft adopted by the EBA and submitted to the European Commission

The European Banking Authority (EBA) issued a final draft of the Regulatory Technical Standards (EBA-RTS-2017-02) on February 23, 2017. Based on this final draft, a risk-based exemption is allowed, provided that the bank stays with the fraud allowances set out by the EBA.

At this stage, therefore, CA Technologies would make the following recommendations:

- **Start planning for multifactor/strong authentication.** PSD2 will require strong authentication for payment transactions, and CA Technologies offers a range of options that comply with PSD2.
- **Leverage predictive models for transaction risk assessment.** PSD2 does not make fraud risk scoring/ screening redundant in any way, and issuing banks should continue to gain the fraud prevention benefits of denying risky or suspicious transactions.

To learn more about CA Technologies payment security products, visit ca.com/payment-security or talk with your account representative. CA Technologies customers can contact their account representative for a detailed assessment on how to proceed.

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.