TIP SHEET

Best Practices for One-time Password Authentication

Many organizations are looking for effective ways to strengthen their online defense with the use of one-time password technology. Traditional one-time password measures such as key fobs are not always a practical solution for customer transactions because of their high cost and the tendency for users to misplace them. One-time passwords provide an easy and cost-effective alternative way to implement an additional factor of authentication by leveraging a device that the user already has. The technology is flexible enough to be used in various authentication scenarios.

DETERMINE THE BUSINESS USE CASE

One-time password technology can be applied to a variety of use cases to provide a simple and intuitive user experience. It is important to apply it to appropriate use cases. One-time passwords are most commonly used for a variety of repeat access transactions. It can also be implemented to automate password reset processes. Many organizations also use one-time passwords when stronger or step-up authentication is required to complete a high risk transaction. In all of these use cases, one-time password is implemented as an additional authentication factor once a user has used some other authentication factor such as username/password.

KNOWN OR VERIFIED DELIVERY TARGET

One-time passwords are often sent either to a landline or a mobile phone. When the user produces the one-time password or code, they confirm that they are in possession of the device to which the one-time password was sent to. A best practice for implementing one-time passwords is to send the code only to a known or verified delivery target (email or phone number). Often organizations collect this information as part of a customer registration or enrollment process; however in some cases the provided information might not be verified. For a successful authentication using one-time passwords, it is important to verify that the delivery phone number is indeed associated and bound to the identity that is being authenticated. With the phone verification, you have the assurance that the one-time password is being sent to the intended user.

PROVIDE MULTIPLE DELIVERY CHANNELS

Users today are accustomed to accessing services across multiple channels and devices. Your one-time password solution must be able to support multiple delivery mechanisms. While some users are accustomed to getting one-time passwords sent as a text to their mobile phone number, others prefer to have it delivered as a phone

call either to a mobile phone or a landline and have the one-time password spoken out during the call. Email delivery is also a commonly used and desired delivery mechanism for some use cases.

SUPPORT INTERNATIONAL DELIVERY

Many organizations have a global presence and desire one-time password technology supported in multiple countries. Even when US based organizations do not have a global presence, they have customers or end users who might travel and attempt to access services from international locations. Thus, it is important to be able to support one-time password delivery to approved international targets.

SELECT THE RIGHT SOLUTIONS PARTNER

When choosing a one-time password solutions provider, look for a vendor providing a holistic solution approach capable of providing phone verification and identity proofing solutions and have the expertise and resources to support your mission critical business processes. The solutions partner should be able to provide full pre- and post-implementation support and have the flexibility to scale as your business grows.

CONCLUSION

With the right solutions partner and best practices implementation, organizations will be poised to reduce fraud and increase security for their business processes with the use of one-time passwords. LexisNexis® One Time Password with integrated phone verification can provide your end users with an easy but secure way to access their services or account information, resulting in a better user experience.

Call 866.277.8407 or visit
https://risk.lexisnexis.com/products/one-time-password

LexisNexis®
RISK SOLUTIONS

About LexisNexis Risk Solutions

At LexisNexis Risk Solutions, we believe in the power of data and advanced analytics for better risk management. With over 40 years of expertise, we are the trusted data analytics provider for organizations seeking actionable insights to manage risks and improve results while upholding the highest standards for security and privacy. Headquartered in metro Atlanta USA, LexisNexis Risk Solutions serves customers in more than 100 countries and is part of RELX Group, a global provider of information and analytics for professional and business customers across industries. For more information, please visit risk.lexisnexis.com.