



SecuTech Solution Inc.

UniOTP Solution Brief

SecuTech



With critical intellectual property and company assets guarded by out-dated protective measures increasing along with the sophistication of cyber-attacks on infrastructures that exploit the very nature of weak authentication systems, companies and institutions are risking unauthorised modification, deletion or theft of irreplaceable data. Protection against malicious threats requires effective and resilient authentication processes at the forefront of security measures.

The Ineffectiveness of Static Passwords

Vulnerabilities in authentication systems that rely on static passwords lie in using an unchanging username and password combination to verify a user. Due to the fixed nature of static passwords, a possible intruder that has a user's password can openly reuse the user's credentials to access the system, a vulnerability otherwise known as a replay attack. Consequently, performing a replay attack simply requires the possession of the username-password combination to access the system, through which can be obtained through countless means.

Multiple methods are available to obtain a user's password. Potential attackers can leverage the invariability, or, with more advanced attacks, the predictability of passwords to attempt either every possible password combination, probable passwords from information gathered about the user, or even former passwords obtained elsewhere. Static passwords stress proper password hygiene, where more than often users chose easily-guessable or similar passwords that are easy to remember but undermine the security of their credentials. Passwords can be intercepted, either in transit through unprotected or poorly implemented processes, or locally through malware extracting credentials from recorded keystrokes. Moreover, more sophisticated attacks utilise social engineering to either directly obtain passwords or otherwise bolster the acquisition process, augmenting the difficulty in training and awareness of users to maintain the safekeeping of their credentials.

As such, the use of static passwords alone provide an ineffectual means of authenticating users and a more robust and secure process for authentication is crucial for the protection of key information and assets by today's standards.

Dynamism Offered by One-time Passwords

Dynamic passwords used together with existing password systems provide both an effective and secure method of addressing the limitations of static passwords. The key characteristic of one-time passwords (OTP) is the generation of a random single-use password, adding an additional layer to the authentication process. To be able to successfully authenticate therefore requires the correct username and password in combination with a one-time password specific to that instance. Two-factor authentication in this fashion, otherwise known, drastically hinders the ability of potential intruders replicating credentials as both the correct username-password combination and a valid OTP must be used.

UniOTP, SecuTech's one-time password solutions, encases numerous advantages of dynamic passwords which contribute to its effectiveness. As a result of the cryptographically secure randomness of one-time passwords, each password generated will always be different from one another, rendering statistical prediction of future generated OTPs infeasible. Together with one-time passwords being valid for one use only, OTPs thwart attempts of replay and brute-force attacks, even if the potential attacker is in possession of a previously used OTP. One-time passwords automatically prohibit unauthorised access from credential theft by malware or data breaches. UniOTP authenticators are specifically designed to be communication-independent, avoiding risks associated with interception or malware acquisition of OTPs altogether. Use of UniOTP authenticators is uncomplicated and intuitive, simply requiring users to enter the password directly from the token at the time to authenticate. Since getting a hold of a one-time password requires physical access to the authenticator, stolen or lost authenticators can be reported and deactivated immediately, minimising risks resulting from the loss. Moreover, the convenient design of UniOTP authenticators is small and robust enough to be carried around with users anywhere, where a single token can be used for more than 3 years, delivering a secure yet highly cost-effective two-factor authentication solution.

Deployment of UniOTP Solutions

SecuTech has undergone comprehensive research and analysis to assist in delivering advanced solutions for numerous conditions. UniOTP solutions are designed specifically by SecuTech to address multiple security challenges present in a diverse number of environments, as outlined below:

UniOTP E-Commerce Solutions

E-commerce has become a tightly woven and indispensable part of businesses and commercial activities, and with e-commerce in European countries such as Germany and France accounting for one quarter of aggregate business revenue, and with USA as high as one third, e-commerce has been quick to become one of the most fundamental business models today. However, with the convenience e-commerce has provided, e-commerce has also brought an array of hidden security risks, with sophisticated and unprecedented attacks on systems resulting in substantial data and financial losses not uncommon. Strong and effective authentication in one of the most lucrative markets is crucial for the functioning of and confidence entrusted in e-commerce.

UniOTP Enterprise Solutions

Different categories of information management systems, such as Enterprise Resource Planning (ERP) systems and Customer Relationship Management (CRM) systems, greatly improve the efficiency in enterprise management and manufacturing processes. Typically, however, information handled by ERP systems include confidential data, and without the correct measures in place to ensure core enterprise interests are accessible to persons with the appropriate authentication levels, the security of confidential enterprise data may be needlessly put at risk.

UniOTP Financial Institution Solutions

Financial institutions deal with arguably one of the most sensitive information and processes, encompassing banks, financiers, and insurance and fund companies at the least. Networking technology has allowed for new-founded opportunities for institutions and convenient accessibility for customers, but the ease of access offered has also posed difficult security challenges. Authentication systems in place that do not provide the security measures needed to protect institutions and their customers risk not only severe economic losses, but irreversible damage to an institution's reputation.

UniOTP VPN and Intranet Network Solutions

Virtual Private Networks and Intranet Networks all handle and extensively use assets such as internal software, documents, printers and a whole host of resources. Given that company-sensitive data and assets are accessible either locally, or even more precariously, remotely through virtual private networks, constant threats of company assets either being stolen, modified or lost through malicious activities rely on stringent authentication processes. Proper access to and permissions on networks require highly robust authentication processes to ensure the protection of highly-valuable and irreplaceable data.

UniOTP Web Authentication Solution

Web applications have grown exponentially in popularity in recent years due to their ease of access and multiplatform nature, requiring only an internet browser to access services and resources over the Internet. As for the complex nature of web services, considering all data is processed and stored online, the strength of authentication measures directly affect the safety measures of both organisational and personal information. Effectual and secure authentication for online applications is necessary for the security of one of the most frequently used and breached platforms.

UniOTP's Dynamic Password Authentication Solution

Developed by SecuTech, the UniOTP dynamic password authentication system offers powerful and uncomplicated protection of company and personal data, and can be easily integrated and configured with support for a diverse range of systems without the need of transforming existing processes. UniOTP's dynamic password authentication system provides two integration methods: Agent or Server SDK integration.

Agent SDK integration combines the UniOTP Agent with the Web Server to handle communication with the UniOTP Authentication Server. Use of the UniOTP Agent allows for high stability and seamless integration with UniOTP authentication.

UniOTP integration with Agent SDK



Server SDK integration incorporates the UniOTP authentication module alongside the Web Server, without requiring the UniOTP Authentication Server. Although using the server SDK to perform dynamic password authentication directly requires in-depth configuration, this method allows for powerful customisation and control.

UniOTP integration with Server SDK



SecuTech's OTP solutions are purposely developed to deliver a selection of solutions suitable the needs of the client, providing secure and robust protection to the highest of standards whilst remaining highly cost-effective to alternatives. The UniOTP product family consists of: UniOTP 300; UniOTP 500; and Mobile UniOTP solutions.

UniOTP 300



UniOTP 300 is an event-based two-factor authentication device capable of generating HOTPs (event-based one-time passwords), which displays a one-time password onto the LED display after the button on the device is pressed. Usage of the UniOTP authenticator does not require the modification of existing systems; simply integrate the UniOTP authentication layer into existing authentication processes to begin usage. Passwords generated are random and invalid after first use, and it is infeasible to reproduce duplicate one-time passwords from the given allotment of possible passwords generated. Moreover, the UniOTP device is completely independent, bypassing the risk of interception or malware infection to bypass the OTP factor. Reliability is placed at the core of design principles, with UniOTP constructed to be water-resistant, shock-resistant and electrostatic-discharge-resistant, with the device customisable upon clients' requests. Altogether, where lost or stolen devices can be reported and deactivated immediately allowing risk control, UniOTP enables highly sophisticated yet cost-effective protection suitable for all needs.

UniOTP 500



UniOTP 500 is a time-based two-factor authentication device capable of generating TOTPs (time-based one-time passwords), which displays a one-time password onto the LED display every 60 seconds. Time-based authentication renders it impractical to brute-force all possible password combinations within the time-frame of 60 seconds, with each randomly generated password invalid either outside the set time period or after one used. Usage of the UniOTP authenticator does not require the modification of existing systems; simply integrate the UniOTP authentication layer into existing authentication processes to begin usage. Moreover, the UniOTP device is completely independent, evading the risk of interception or malware infection to bypass the OTP factor. Reliability is placed at the core of design principles, with UniOTP constructed to be water-resistant, shock-resistant and electrostatic-discharge-resistant, with the device customisable upon clients' requests. In addition where lost or stolen devices can be reported and deactivated immediately allowing risk control, UniOTP enables highly sophisticated yet cost-effective protection suitable for all needs.

Mobile UniOTP



Unlike UniOTP 300 and UniOTP 500, Mobile UniOTP is deployable as an app onto existing mobile devices, and functions as both an event- and time-based authenticator. Mobile UniOTP contains all of the benefits of the UniOTP family, with the addition of a challenge and response token system. After receiving a randomly-generated token from the server, the challenge, the user enters the code into their application and responds to the server with the code generated from the server's challenge, the response. The correct response from a server-side randomly generated token entered into the application is required to complete the authenticate process. As such, Mobile UniOTP allows for easy and secure authentication without the need of deploying hardware in the presence of existing mobile devices.

About SecuTech

SecuTech Solutions Inc. is a company specializing in data protection and strong authentication, providing total customer satisfaction in security systems & services for banks, financial institutions & other industries. Having extensive and in-depth experience within the information security market, SecuTech has drawn upon this experience to utilize today's cutting-edge technologies, enables enterprises, financial institutions, and government to safely adopt the economic benefits of mobile and cloud computing that are effective against increasingly sophisticated cyber attacks.

SecuTech

www.eSecuTech.com
SecuTech Solution Inc.

North America

1250 Boulevard René-Lévesque Ouest
#2200, Montreal, QC, H3B 4W8, Canada
T: +1-888-259-5825
F: +1-888-259-5825 ext.0
E: INFO@eSecuTech.com

APAC

Suite 5.14, 32 Delhi Rd, North Ryde,
NSW, 2113, Australia
T: 00612-9888 6185
F: 00612-9888 6185
E: AUS@eSecuTech.com

China

Level 12, #67 Bei Si Huan Xi Lu,
Beijing, China, 100080
T: +8610-8288 8834
F: +8610-8288 8834
E: CN@eSecuTech.com

EMEA

4 Cours Bayard 69002 Lyon,
France
T/F: +33-042-600-2810
M: +33-060-939 6463
E: Europe@eSecuTech.com