CU t-t CREDIT UNION tech-talk
LEADER'S FORUM
SPECIAL ROUNDTABLE SECTION
TECHNOLOGY NEWS FOR CREDIT UNIONS SINCE 1988
WWW.CUNEWS.COM

Addressing the Big 3: Compliance, Fraud & Cyber Security

Without a doubt, staying compliant with FFIEC regulations is a difficult task for any credit union. The real challenge is finding practical ways to meet all of the regulators' complex and varied guidelines in an affordable manner. Multi-factor authentication is one of the most important requirements that the FFIEC has ever issued. Hardware tokens can be used to mitigate the risk of password theft by introducing additional factors of authentication, they are secure but they are expensive to deploy and are easily forgotten since they are an additional device that the user needs to carry. Software based tokens are another option, but they require the user to download an app and install it on their smart device. The software approach requires a few steps which need to be accomplished before the user can start using their two-factor authentication.

Direct Risk Management (DRM) has developed and introduced the World's First, "Invisible Token." This token-less solution delivers 2-Factor Authentication security via the LAN, Web and Cloud while transforming the users' browser to act as a virtual token. The Direct Authenticator Invisible Token is based on HTML5 and transforms your browser into an OTP-token that is independent of the platform. Your browser is enrolled when used for the first time with a patented technology that seamlessly configures your browser and integrates an OTP-token into it. End users can continue to use password-based authentication and existing passwords in directories such as Active Directory. With our single sign on support, the user can have access via a resource portal to many applications without having to login to each of them. The Direct Authenticator Invisible Token is easily integrated with any web-based application and service through an API.

When it comes to fraud, credit unions are increasingly seen as targets by fraudsters. While the large institutions represent the "mother lode" of millions of accounts, smaller institutions oftentimes do not have the same risk analysis and fraud prevention software installed that the larger institutions can afford to deploy. Fraud is moving to the online channel, especially in the United States. Case in point: while America represents 23% of worldwide card dollar volume 47% of card fraud worldwide occurs in the US! The credit unions are migrating to the much more secure EMV cards and these "chip and PIN" cards boost security for card present transactions and unfortunately offer limited fraud fighting capabilities in card not present situations, hence the need for multi-factor authentication.

As mobile banking skyrockets in popularity, security concerns for this channel are increasing. We have addressed this issue with the DA-Mobile e-Token solution; this is software based and complies with FFIEC multi-factor authentication requirements. It provides the same level of security as other authentication solutions, without the hassle of distributing and maintaining multiple hardware tokens. For members, it provides utmost security and the ease of use with respect to accessing your online banking platform; while for employees it secures access to cloud applications, Microsoft Outlook, Web-based portals, Citrix, and VPNs used to access your local area network. The great news is that DA-Mobile e-Token client is FREE. As a user, you can install the DA-Mobile e-Token on as many smart devices you own. This provides flexibility and ease to connect back to your systems, applications and networks from any device, anytime and anywhere. Whether it is mobile or via a Personal Computer, we have affordable and robust authentication solutions that meet the needs of credit unions of all sizes.

Donald E. Malloy, Jr.
Director of Product Marketing

DirectRM
Software Defined Security

Don is the Director of Business Development and Product Marketing at DirectRM. He has 25 years' experience in sales, product marketing, security and authentication. Prior to DirectRM he was the Director of Business Development at NagraID Security, he also was Marketing Manager at Philips Semiconductors and Infineon Technologies responsible for product marketing of their smart card semiconductors and RFID products. Mr. Malloy has a Master's level in Organic Chemistry and an M.B.A in Marketing. He began his career as a research scientist at Brookhaven National Laboratory. He has spoken at conferences around the world on a variety of technical topics including security, RFID, authentication and EMV migration.

Contact Info

www.directrm.com