SecuriKey

CU*ANSWERS
A Credit Union Service Organization

MACO

Multi-Authentication Convenience Option

VERSION
June 2021

MACO
Multiple Authentication Convenience Options

LEGAL DISCLAIMER

The information contained in this document does not constitute legal advice. You should retain and rely on your own legal counsel, and nothing herein should be considered a substitute for the advice of competent legal counsel. These materials are intended, but not promised or guaranteed to be current, complete, or up-to-date and should in no way be taken as an indication of future results. All information is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose. In no event will CU*Answers, its related partnerships or corporations, or the partners, agents or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information provided or for any consequential, special or similar damages, even if advised of the possibility of such damages.

Quick Reference Summary of Controls

MACO SOFTWARE CONTROLS

Online Banking Authentication
Members cannot use MACO unless initially authenticated through Online Banking.

Authentication Process
Biometric authentication is a process, requiring the member to ensure identity recognition prior to authentication with the Mobile Banking system.

DATA TRANSMISSION

Encryption
Information entered by the member is encrypted through 256-bit encryption.

Data Storage
No biometric data is stored on the MACO servers. Any biometric information is stored on the member's device using the device's native encryption (not in the MACO app itself).

AUTHENTICATION CONTROLS

Temporary/Permanent Lockout
MACO temporary locks out the member if member authentication fails. If the member fails to authenticate four times, the lockout is permanent.

Probabilistic Authentication
If the member chooses biometric authentication options, authentication is provided through a probabilistic authentication algorithm.

SecuriKey

Credit unions may be asked by examiners or auditors to provide a MACO risk assessment, documenting MACO's safeguarding of authentication information. Members may have concerns about biometric information used for authentication. This document is meant for public use, with information to assist credit unions in creating their own risk assessments.

CU*Answers' Multi-Authentication Convenience Option ("MACO") allows our network credit unions to provide your members more options for authentication in **It's Me 247 Mobile Banking**. MACO includes four convenience options: fingerprint, face recognition, voice recognition, and PIN.

CU*Answers does not recommend advertising MACO as being "more secure." MACO meets requirements for reasonable security, but the tool is primarily a convenience option for members.

Overview of MACO Security Features

MACO is a secure method for Mobile Banking authentication. When the member selects to enroll in a MACO method, authentication must be established by entering standard login credentials (username, password, and security question answer). After enrollment in MACO, the standard authentication is not required; however, standard authentication can always be selected in place of MACO.

FINGERPRINT

Fingerprint authentication will only show on devices that support fingerprint technology. To use fingerprint authentication, the member must first save a fingerprint sample in the operating system of the device. During MACO fingerprint enrollment, the member touches the sensor of their device (for example the Home button) to verify the member has a match with the fingerprint saved in the operating system of the device. During MACO fingerprint authentication, the member places their finger on the device's sensor. If the fingerprint matches the fingerprint saved in the device's operating system, the member is logged on to Mobile App Banking.

FACE RECOGNITION

During face recognition enrollment, the device camera takes several pictures of the member. Helpful messaging assists the member to align their face in the proper manner. The best photo is analyzed according to a series of measurements which may include eye socket depth, distance between the eyes, and the width of the nose. An encrypted metric assigned to the photo is sent to the DAON server. During face recognition authentication, the member gives a live-test sample by blinking (shaking or nodding) which causes the camera of the device to take a photo of the member. The photo metrics are sent to the MACO server. If the photo metric matches what is saved on the MACO server, the member is logged on to Mobile App Banking. If the member is using a device with Apple Face ID, MACO will adjust to use this authentication method.

VOICE RECOGNITION

During enrollment, the member says a passphrase that is presented on the screen. Three acceptable recordings are captured, and the best is converted to encrypted voice data that is sent to the DAON server. During voice recognition authentication, the member is asked to say the phase again. The voiceprint is compared with the audio data on the DAON server. If a match is found, the member is logged on to Mobile App Banking.

PIN

During enrollment, the member is presented a number pad on the screen of their device. Members tap a four-digit PIN and then tap it again to confirm the number. An encrypted PIN is sent to the DAON server. During PIN authentication, the member taps their PIN twice in the number pad that is presented. If this PIN matches the number saved on the DAON server, the member is logged on to Mobile App Banking.

Authentication Information

Authentication information entered by the member is encrypted. Transmission security is provided using 256-bit encryption. For fingerprint, voice, and face recognition, the credential information is compared against the MACO probabilistic algorithm on the server. If there is a match, the member is authenticated. No biometric data is stored on the MACO servers. The biometric information is stored encrypted on the member device through the native encryption of the device OS, not the MACO application. Credit unions and members who wish to know more about device native encryption can review options provided by the manufacturer of the device.

Members should not use MACO on a device that is shared. If a member loses the device, MACO can be removed on all devices by creating a new profile on a device. If this is not an option, the credit union can request CU*Answers to disable the profile.

Failed authentications will lock out MACO authentication for a temporary time. Standard login is still available if the account is locked out. The lockout time increases with each lockout. Members will be unable to use MACO for fifteen minutes, then twenty and then twenty-five minutes. At the fourth lockout, the MACO profile will be disabled.

Unenrollment

Members can unenroll MACO from all devices using the Reset Authentication Options on All Devices menu option. More information can be found in the How can I ensure MACO is unenrolled from all devices for a member's account? AnswerBook item.

About Daon

MACO is provided through Daon, Inc., and their IdentityX product. Daon is based out of Ireland, and has a worldwide customer base, including government agencies. Many of their clients include international banking institutions that use their products for mobile authentication, in the same way used in the CU*Answers Mobile Banking solution.

Product Feature Matrix

To help you assess MACO security controls, CU*Answers has developed a Product Feature Matrix that lists the security features of MACO.

AUTHENTICATION PROCESS	ENCRYPTION IN TRANSIT	DATA STORAGE
Members must be authenticated through a standard login to Mobile Banking before using MACO	Authentication information is transmitted using 256-bit encryption	Biometric information is not stored on the MACO servers; encryption on the device using the device’s native encryption (in the OS, not the app)
Members go through a process with biometric identifiers to ensure high degree of accuracy in authentication		
Members can de-enroll if the device is lost or stolen; MACO is not recommended if the member shares the device		

Version Control

VERSION	DATE	CHANGE	TEAM
1.0	June 14, 2018	First published	Internal Audit
2.0	June 1, 2020	Revised for clarity Added “Unenrollment”	Internal Audit

Learn More

INTERNET RETAILER SUPPORT CENTER

You can download the MACO brochure here.

Learn more about MACO here.