



BIOMETRIC-ENABLED CHECK-IN FOR MICROSOFT CERTIFIED MASTER (MCM) EXAMS CANDIDATE FAQs

Biometric-enabled check-in is designed to protect candidate privacy and improve the integrity and security of the testing process. Use of the enhanced biometric-enabled check-in procedures for candidate authentication and identification are performed by Prometric*.

How does biometric-enabled check-in work?

As the test taker, you must first present a valid form of government-issued photo identification at the testing center. The Test Center Administrator (TCA) will compare your roster name and signature with that on your identification. You will then be required to provide a fingertip pattern template. You will place your fingertip on the scanner, providing three swipes from one finger on each hand (finger closest to thumb) to create a digitized representation template (this version of creating a template is for enrolling first time testers only). When you test as a return tester, one finger from either hand may be used to capture the fingertip pattern and identify you as a previously enrolled tester.

The template is an algorithm which represents the pattern from the fingertip. The system stores a secured and encrypted fingertip pattern template. An image of the fingertip pattern is also encrypted and stored. This image is not accessed and exists only to rebuild the fingertip pattern template in the event of a corruption event in the database. The template will be stored at Lexis Nexis with other personal information that you may have already provided to Prometric.

How will biometric-enabled check-in enhance my experience at the test center?

Biometric-enabled check-in generally takes less than two minutes for first time testers to complete the biometric-enabled check-in enrollment process. If you are a returning candidate, the process is even faster with the use of biometric-enabled check-in; your fingertip pattern template is easily found in the system each time you return to test for a Biometric enabled exam.

Is biometric-enabled check-in conducted at all Prometric test centers that offer the MCM Exams?

The implementation of biometric-enabled check-in is based on a country's specific biometrics laws. We have provided information for you to read in advance of your exam, which will explain the biometrics consent status for the countries which offer the MCM Exams. Please read the consent form for the country in which you will be taking the exam. Where indicated, you will sign the same form at the point of check in for your exam.

United States, India, Malaysia: There are no laws in these countries regarding biometrics; please read the General Consent Form.



Germany: This country requires that an informed consent form be signed at the testing center. Please read the Explicit Informed Consent Form, and be prepared to sign the form at the testing center when you check in. This form will be stored at Prometric Headquarters.

Japan, United Kingdom, Western Australia: These countries require that an informed consent form be signed at the testing center. Please read the Implied Informed Consent Form, and be prepared to sign the form at the testing center when you check in. This form will be stored at Prometric Headquarters.

Canada and South Africa: These two countries do not permit the collection of fingerprints for biometric enabled check-in. If candidates take their MCM exam(s) at test centers in these countries, fingerprints will not be collected. Please read the Not Permitted Form for details.

What if I am a resident of Canada or South Africa, but take an MCM exam in a country which permits the collection of fingerprints for biometric-enabled check-in?

The law follows the country, not the exam candidate. If you take an MCM in a country which permits the collection of fingerprints for biometric-enabled check-in, your fingerprint will be collected.

How is the information, captured during biometric-enabled check-in, used?

Personal information captured during biometric-enabled check-in is used by Prometric to: (1) administer tests, (2) create a smoother check-in process for an already biometrically-enabled candidate, by positively identifying them as a returning Prometric candidate, (3) identify and prevent testing fraud and maintain the integrity of the testing process by detecting and preventing test taking by unauthorized candidates, (4) improve security of test centers by detecting and preventing unauthorized access of candidates to secure areas, and (5) if needed, for legal compliance.

When is the information, captured during biometric-enabled check-in, disclosed to third parties?

Please keep in mind that the fingertip pattern template provided is secured and encrypted throughout all data transmission points. Prometric will not disclose the demographic information to any third party except (1) as required by law, (2) to your Test Sponsor in accordance with the notices provided to you as the candidate, and/or (3) as necessary to complete a fraud investigation directly related to a testing incident. Lexis Nexis is the only 3rd party vendor that will store your fingertip pattern. This information will not be disclosed with any 3rd parties.

How is the biometric information, captured during biometric-enabled check-in, secured?

Prometric has implemented appropriate technical, physical and administrative safeguards to help protect your personal information against unauthorized access or loss. Prometric's workers who access the information are trained on these procedures and bound by appropriate confidentiality obligations. All personal data captured at any point during the check-in process is encrypted and transmitted to a secure site.

Am I required to provide my biometric data at the time of biometric-enabled check-in?



All candidates are required to provide valid identification documents on the day of their examination and individuals who fail to provide valid identification will be refused admission to test. You are encouraged to provide a fingertip pattern at check-in as that provides a higher level of security during the testing experience. If you do not wish to provide a fingertip pattern, you may continue to schedule and test, however, your Test Sponsor will be informed

How long is my personal biometric information retained?

The fingertip pattern templates are stored in a centralized and secured database at Lexis Nexis for an allotted period of time specified by local law. The fingertip template is retained for fraud investigation or other legal purposes for a reasonable period of time required for potential legal or fraud investigations. That period will not exceed five (5) years after inactivity.

Is my identity at risk once I've provided my biometric information?

The quality of the fingertip pattern template collected at the site is NOT associated with the FBI (14-point prints) or matched against any other government database of prints. The fingertip templates taken at the test sites create a 2-point template image and increase the level of security at the test site to prevent one candidate from attempting to test on behalf of another candidate.

Contact Information:

If you have questions or concerns about privacy and the biometric-enabled check-in procedures you can contact Prometric at:

Prometric Inc.
1501 S. Clinton Street
Baltimore, MD 21224 USA

Anthony R. Scicchitano
Data Protection Officer
Telephone: 1-443-455-8493
E-Mail: anthony.scicchitano@prometric.com

If you have general questions regarding the decision to use biometrics for the MCM exams, please contact your local [Regional Service Center](#).