

BIOMETRIC IDENTITY MANAGEMENT SERVICE

Frequently Asked Questions

Beginning January 2008, the CPA Exam Program will begin using enhanced security systems. Biometrics will be used to capture candidates' fingerprints and match the fingerprints with other personal identity information to increase security and identity validation. The Biometric Identity Management Service (BIMS) is designed to protect test candidate privacy and improve the security and integrity of the testing process.

1. Why has the CPA Program decided to start using the BIMS?

The CPA Credential is designed to protect the public interest. It is imperative that all due diligence be used to assure the highest degree of confidence in the integrity of the entire process. As new technology becomes available that can be used to enhance public trust in the credential, it is appropriate to leverage such technology for the CPA Exam Program. BIMS technology is being employed to enhance the identification of individuals taking the CPA Exam. Specifically, once a candidate has provided fingerprints the first time he or she enters a Prometric test center, BIMS will be used to (1) verify that candidate's identity each time he or she returns to a Prometric test center from a rest break, to take another Exam section, etc. (2) protect candidates' privacy by enabling movement around the test center without the requirement that identification documents be carried and presented regularly, (3) identify and guard against testing fraud by detecting and preventing test-taking by unauthorized candidates, and (4) improve security of test centers by preventing unauthorized individuals from accessing restricted areas.

2. What information is collected from an individual candidate?

The BIMS uses the minimum information necessary from commonly used identification documents to accurately identify and authenticate an individual. The System also scans one or more fingers from each hand.

3. What information is obtained from my identification documents?

The information obtained from the identification documents includes name, address, birthdate/age, and the document number. For example, when a driver's license is used as identification, it includes the name, address, birthdate/age, and the license number. The driver's license is also scanned to retain a digital image of the document for the BIMS.

4. How is a candidate's fingerprint obtained?

During the check-in process, a candidate places his or her finger (generally the finger closest to the thumb) on a small electronic device. The device electronically obtains an image. Typically, three images are captured and a template is built from those images.

The process is repeated for the other hand. The templates are then stored and used to recreate the image when required and used to compare to subsequent return captures. For candidates returning from breaks or for candidates returning to re-take a test or a different test section, the stored fingerprint template is used to confirm that the returning candidate is the same person.

5. What information is collected in the BIMS?

The BIMS contains a digitized representation of the fingerprint, along with the candidate's name, address, birthdate/age, the document number, and a digitized, scanned copy of the provided identification document (such as the candidate's driver's license or passport).

BIMS combines the common government identification document with the digital scan of the fingerprint to better authenticate an individual's identity. It is not used to compare data of any other governmental agency.

Once this information is captured on the first visit to the test center, it will be retrieved upon each subsequent visit using the fingerprint scan regardless of which test center a candidate chooses.

6. How is the information stored? Is the information stored at the test center where I took my test?

The information is not stored at the test center. No BIMS information resides on the local computers. All information is electronically transmitted through a secure connection to a state of the art database. This database is safeguarded with the latest computer security protections. These safeguards include anti-virus, intrusion detection, firewall, web server and application scanning. All data are encrypted at rest within the database and during secure communications with the test center.

The vendor undergoes SAS70 Type II reviews on an annual basis and averages 30 successful security audits by major governmental agencies, insurance companies, and financial institutions a year.

7. For what purposes are the candidate information and fingerprint template used?

The information is used to authenticate the identity of the candidate. If this is the first time that a candidate has taken a test at a Prometric test center, the information is used to build a record for use in future authentication. The fingerprint is used to prove that the same candidate returns from breaks during the time a candidate is at the test center. For subsequent examinations, it is used to demonstrate that the same individual has returned to test. Each time a candidate leaves or enters the testing center a fingerprint comparison is made to the stored record to confirm it is the same person.

Additionally, in some circumstances, the information is provided to NASBA and Prometric for other uses which are related to the administration and integrity of the examination. Specifically, the information may be used by Prometric only to:

- investigate a security violation of the examination taken by the candidate.
- defend itself in a legal proceeding or to assist the client in a legal proceeding.

8. What safeguards are in place to ensure that the data is used ONLY for the purposes for which its collection is intended?

Prometric shall only use the data collected, electronic image, and biometric information captured as part of the identify verification process and in compliance with applicable law.

BIMS combines common government identification documents with the digital scan of the fingerprint to better authenticate an individual's identity. It is not used to compare data of any other governmental agency.

9. When is the information in the BIMS disclosed to third parties?

Only NASBA, Prometric, and the vendor storing the identification information have access to the information. Prometric and the vendor will only have access to store and maintain the information and to use the information to identify and authenticate the candidate for an examination and to ensure the integrity of the examination process. No other use of the identification information may be made by Prometric or its vendor. Prometric will not disclose the demographic information to any third party except as required by law or as necessary to complete a fraud investigation directly related to the candidate. Encrypted BIMS information will be disclosed to NASBA upon request for investigation purposes only.

12. Will BIMS replace Image Capture?

The CPA Exam Program will continue to collect a current digital image of the candidate at the time of the test event. This image is in addition to the capture of BIMS and is stored separately from the BIMS information.

13. What if I refuse to provide a fingerprint or have my identification scanned?

As with current CPA Exam Program procedures, all candidates are required to provide valid identification documents, image capture, etc. Candidates who fail to provide the required information or fingerprint will be refused admission to the test.

14. What if I have a medical condition that renders my fingerprint unreadable (such as amputated fingers or skin conditions)?

If you have a physical/medical condition that prevents you from providing a clear accurate fingerprint, you **MUST** contact your State Board of Accountancy or its designee to make arrangements for Special Accommodations.

15. What happens if the Biometric Identity Management System (BIMS) is not functioning on the day of a test?

In the event that the BIMS is not functioning at the test center on the day of your exam, the system can be overridden and existing check-in and identification procedures will be used to enable testing to proceed.