Biometrics Capability Statement

Sales/Marketing Point of Contact
Evan Call

303.627.1110 ext 114
ECall@ibeta.com
www.ibeta.com

Technical Point of Contact
Dr. Wilson

303.627.1110 ext 177
KWilson@ibeta.com

We test – you succeed!

iBeta Company Background

iBeta is a privately held Limited Liability Company. Certified by the National Minority Supplier Development Council, iBeta is a Minority Business Enterprise (MBE –RM0152). iBeta has provided a full range of quality assurance testing services to clients in North America, Europe, Asia, and Australia since 1999.

iBeta built each client relationship by focusing on delivering solution based services that produce rigorously tested products on time and within budget. Quality and value are the key expectations of all of iBeta's clients. As a result of iBeta's focus on client satisfaction, iBeta maintains a 90% repeat business ratio after working with hundreds of clients.

iBeta, located in Aurora, Colorado, operates a fully staffed 40,000 square foot test facility supplied with the materials and equipment needed to fulfill the certification test services being proposed. As a privately held company, iBeta pledges that we have the necessary financial wherewithal to complete this project.

Accredited NVLAP Biometric Test Lab

iBeta is nationally accredited as a test lab by the NIST program National Voluntary Lab Accreditation Program (NVLAP) to the requirements of ISO/IEC:17025 (General requirements for the competence of testing and calibration laboratories).

- In 2007 iBeta was accredited by the Election Assistance Commission as a Voting System Test Lab (VSTL). The VSTL test efforts are parallel to the IV&V test efforts defined in IEEE 1012-2004 Software Verification and Validation.
- In 2011 iBeta was accredited by NIST under the National Voluntary Laboratory Accreditation Program (NVLAP) for Biometric Testing.

Accredited FIDO Alliance Biometric Test Lab

FIDO Alliance announced their Biometric Certification Program on September 6, 2018. Currently, iBeta is the only FIDO Alliance accredited biometric test lab. The test requirements include FMR of less than 0.01% and presentation attack detection limits. Please contact either the FIDO Alliance Biometric Secretariat or iBeta for more details.

iBeta Consulting and Certification Process

iBeta Quality Management System

The iBeta Quality Management System (QMS) has been audited and accredited to be in compliance with the ISO 17025 requirements by NIST/NVLAP. The QMS consists of the Quality Policy and Quality Procedures.

Biometric Certification

iBeta Quality Assurance is accredited to certify biometric systems and subsystems to the Standards provided in Table 1 below.

Table 1 – Status of NVLAP Accreditations

TEST	Standard	Title
Data Interchange Standards Conformance Testing (30/DISCT)		
30/DISC00A	ANSI/INCITS 423.1 (2008)	Information Technology – Conformance Testing Methodology Standard for Biometric Data Interchange Format Standards – Part 1: Generalized Conformance Testing Methodology
30/DISC00B	ISO/IEC 29109-1 (2009)	Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 1: Generalized conformance testing methodology
30/DISC01A	ANSI/INCITS 423.2 (2008)	Information Technology – Conformance Testing Methodology Standard for Biometric Data Interchange Format Standards – Part 2: Conformance Testing Methodology for INCITS 378-2004, Finger Minutiae Format for Data Interchange
30/DISC01B	ISO/IEC 29109-2 (2010)	Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 2: Finger minutiae data
30/DISC05A	ANSI/INCITS 423.4 (2009)	Information Technology – Conformance Testing Methodology Standard for Biometric Data Interchange Format Standards – Part 4: Conformance Testing Methodology for INCITS 381, Finger Image-Based Data Interchange Format
30/DISC05B	ISO/IEC 29109-4 (2010)	Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 4: Finger image data
30/DISC18	ANSI/NIST-ITL 1-2011	Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information
30/DISC20	ISO/IEC 30107-3 (2017)	Information technology – Biometric presentation attack detection – Part 3: Testing and reporting
System Level Testing (30/SLT): Graded Performance Testing (30/GPT)		
30/GPT01	INCITS 409.5 DRAFT 2 (2010-08-20)	Information technology – Biometric Performance Testing and Reporting – Part 5: Framework for

		Testing and Evaluation of Biometric System(s) for Access Control
30/GPT02	ISO/IEC 19795-5 (2011)	Information technology – Biometric presentation attack detection – Part 3: Testing and reporting
	ISO/IEC 30107-3 (2017)	Information technology – Biometric Performance Testing and Reporting – Part 5: Access Control Scenario and Grading Scheme
Technical Interface Standards Conformance Testing (30/TISCT)		
30/TISC01A	ANSI/INCITS 429 (2008)	Information Technology – Conformance Testing Methodology for ANSI INCITS 358-2002
30/TISC02A	ISO/IEC 24709-1(2007)	Information technology – Conformance testing for the biometric application programming interface (BioAPI) – Part 1: Methods and procedures
30/TISC02B	ISO/IEC 24709-2 (2007)	Information technology – Conformance testing for the biometric application programming interface (BioAPI) – Part 2: Test assertions for biometric service providers
United States Federal Standards		
EPCS	CFR 21 Part 1311.116 (March 31, 2010)	Department of Justice Drug Enformcement Administration Electronic Prescribing of Controlled Substances; Final Rule

NIST/NVLAP recently (April 2018) audited and added testing to the ISO/IEC 30107-3: 2017 Information technology – Biometric presentation attack detection – Part 3: Testing and Report Standards to the iBeta accredited testing scope.

For each biometric certification, iBeta provides testing and reporting in accordance with the standard. Typical performance testing consists of the following:

- Plan/prepare for corpus acquisition – iBeta maintains an IRB approval for most modality PII collection
- Acquire the corpus of biometric records
- Execute matching and cross-matching of acquired dataset (match scores are required for most analysis not simply a pass/fail)
- Collect, correlate, and produce Certification Test Report

Deliverables from the certification services may include discrepancy reports. Consistent with the NVLAP accreditation, iBeta produces an Excel spreadsheet containing line item summaries of findings of discrepancies between the tested application and the requirements. The discrepancy report is used in our procedures to track the findings to closure. Once all discrepancies are closed and the software is fully functional, then it is capable of passing an audit and being certified.

Other deliverable may also include daily or weekly status reports, a requirements to test matrix, test cases, and a final report with opinions and recommendations.

iBeta will produce a certificate of compliance. The full report of compliance typically contains the following sections:

1. Executive Summary – including identification of the application audited
2. Introduction – Test methods, documentation and introduction to the test report
3. Background – Nomenclature and summary of procedures and any deviations from documented test methods.
4. System Identification – Detailed identification of system including all dependencies and detailed description of the test environment and test systems
5. Review and Test Results – Summary of results, exceptions and exclusions from testing (if any)
6. Opinions and Recommendations – generally contains the affirmation that all requirements of the regulations are met. Table of high level requirements that were tested and passed.
7. Appendix A – Security Assessment Results – detailed line item regulations tested and result

Biometric Scenario Testing

iBeta Quality Assurance conducts scenario testing per vendor requirements and also creates and administers certification programs for entities (such as banks) to vet and incorporate various vendor biometric solutions and/or modilities.

As an example, iBeta has conducted 'bake-offs' where a client submits numerous biometric susbsystems (and modalities). iBeta Quality Assurance's assessment and testing of five biometric identity verification applications resulted in a test report. The testing and calculation of the False Accept Rate (FAR) and False Reject Rate (FRR) of the applications on a single test platform is reported. The methodology for obtaining these metrics was to collect 100 subjects' data with an enrollment and then 6 authentication or verification samples. Additional scenario testing was conducted to attempt to spoof the biometric modality to gain access emulating a malicious imposter.

The target accuracy for the application was established within the Statement of Work (SOW) calculate a FAR at or above the 0.1% at 95% confidence and an FRR calculated in the 1.2% range.

iBeta also conducted testing to provide a repeatable vendor agnostic evaluation process for face biometrics. This process includes testing face biometric based authentication application for False-Match Rate (FMR) and False-Nonmatch Rate (FNMR). The test described is primarily a technology type of test, but the biometric samples are obtained under scenario types of conditions and are obtained specific to the device under test. Under most situations, device vendor software is used and or modified to acquire the samples. The test is operational in the sense that if the sensor accepts a sample then that sample is automatically included (barring any downstream

storage errors) as the appropriate sample (either registration or authentication) for later technology testing.

In addition to conducting a spoofing analysis on each of the applications, the test also produced failure-to-enroll (FTE) and failure-to-acquire (FTA) or failure-to-capture (FTC) statistics in addition to the above.

Scenario testing may also incorporate environmental factors such as varying sound levels, varying the light environment to simulate night and daylight conditions, and introducing differing backgrounds. The purpose of these tests is to verify that the application can be used in the various environments where the application may realistically be used.

iBeta Presentation Attack Detection (PAD) Testing

iBeta is accredited to test to ISO 30107-3 and is also informed by the Draft ISO 30107-4 for mobile device based application testing. iBeta follows the Levels of Testing as defined in the table below.

Level	Time	Expertise	Artefact source
1	8 hours per subject	None	Cooperative subject and equipment is readily available in a normal home or office environment
2	2-4 days per subject	Moderate – participated in at least 1 other PAD test with the target modality	Cooperative subject and equipment is more expensive (such as a 3D printer)
3	3 weeks per subject	Significant – has dedicated at least 16 hours to research of presentation attacks of the target modality and has participated in at least 2 other PAD tests with the target modality	Cooperative Subject and latent sources for subject data. Equipment is extensive e.g., special order contact lenses, facial masks, and 3D printed spoofs

Prior to the release of the ISO standard, iBeta conducted numerous spoof and liveness detection testing for the voice, face, schlera and fingerprint modalities.