2023 Remote Identity Validation Technology Demonstration

Document Validation Application Instructions

Identity Validation technology providers may apply to participate in the 2023 Remote Identity Validation Technology Demonstration (RIVTD). Additional information about the 2023 RIVTD is available at https://mdtf.org/rivtd, including but not limited to slides from informational webinars.

These application instructions are specifically for the Document Validation track. The Document Validation Track portion of the demonstration is intended as an initial step to survey the current state of remote identity technology. It is an opportunity for you to describe and demonstrate the capabilities and performance of your document validation technology.

All application materials are due by February 15, 2023 at 11:59PM Eastern Standard Time. All application materials should be sent to peoplescreening@hq.dhs.gov and rivtd@mdtf.org.

Applications MUST include a white paper in pdf format, up to five (5) pages in length.
Any proprietary materials included in the application SHOULD be clearly marked.
Whitepapers MUST include the following information:

1. **Company overview:**
   - Company name, location (including country of headquarters), and year formed.
   - Contact information (name, email, telephone number, citizenship) of a business representative and, separately, a technology representative.
   - Provide a brief description of company history, experience in the identity validation community, and the primary markets served.
   - Describe any remote identity validation technologies offered: Document Validation, Face Matching, Face Liveness / Presentation Attack Detection, Other.
2. **Document validation system overview:**
   - Describe the complexity and maturity of your document validation system, including a high-level overview of the underlying document validation technology.
   - When was the system first conceived and developed? Is it still under development?
   - Where was the source code developed and what security controls are implemented?
   - Are there examples where the product is in use now?
3. **Document validation system technical capabilities:**
   - State the recommended CPU, RAM, disk, operating system, and list any runtime dependencies.
   - What are the acceptable document types: Passports, US Drivers Licenses, Other?
   - What sorts of fraud/attacks is the product able to detect?
   - Are there known document validation issues?
4. **Document validation system inputs and data processing steps:**
   - What are the required system inputs (supported image formats, Exif data, etc.)?
   - What document image restrictions / limitations / requirements does your system have?
   - What detections and classifications are made to establish document validity?
   - Are any document validity properties explained?
   - How will your system process the document images provided through the MdTF API?

5. **Document validation system outputs:**
    - How will the required MdTF API document *ValidityOutcome* be determined?
    - Will a *ValidityScore* be provided (strongly encouraged)? How is the score determined?
    - Will *ValidityProperties* be provided (suggested)? What properties are returned?
    - What other outputs should be considered for your system?
6. **Document validation system performance estimates:**
    - Describe any measurements of the performance characteristics of the document validation system and how they were tested, including references to any whitepapers, performance benchmarks, and/or benchmark datasets used.
    - Provide estimates of performance for the following metrics:
        - Expected Document False Reject Rate (DFRR).
        - Expected Document False Accept Rate (DFAR).
        - Expected System Error Rate (SEC) - (e.g., when you are unable to validate).
        - Expected Document Processing Time (DPT).
    - Provide estimates of system stability to race, and gender.