

RIVR-2 Identity Document Validation (RIVR-2-IDV)

Technical Information and Participation Requirements

Overview

Remote identity validation technologies verify the identity of users based on data, including document images, submitted over the internet using personal electronic devices such as smartphones. These technologies reduce friction for genuine users and guard against identity fraud. The Remote Identity Validation Rally 2 (RIVR-2) challenges industry to demonstrate secure, effective, and accurate remote identity validation solutions that help combat identity fraud when users apply for government services, open bank accounts, verify social media accounts, and more.

The RIVR-2 Identity Document Validation (RIVR-2-IDV) track is open to providers of commercial IDV technologies currently in deployment. It gives technology developers the opportunity to show their ability to create secure, accurate, and easy-to-use technologies that determine whether a U.S. territory or state-issued identification card, or international passport face page, is genuine or fraudulent.

Process and Schedule

The current schedule for RIVR-2-IDV is available at <https://mdtf.org/rivr2>.

Applications

Applications to participate in RIVR-2-IDV will be accepted through the “Applications Due” date. Please follow all application instructions provided on the website; deviations from instructions may lead to your subsystem not being selected to participate in RIVR-2-IDV.

DHS S&T will evaluate all received applications and notify those selected for participation. All participating vendors must have an active CRADA with DHS S&T. If there is a conflict between the statement of work in the CRADA and these instructions, act based on the CRADA. If the CRADA addresses something that these instructions do not address, you are expected to adhere to the CRADA. Please contact peoplescreening@hq.dhs.gov for details about the CRADA process.

Technology Submissions

All technology submissions for RIVR-2-IDV will be handled via MyConsole (<https://myconsole.mdtf.org>). MyConsole is a secure web-based platform that enables vendors to submit technology and data for automated validation and testing. The technical contact listed in your application to participate will receive access to the MdTF MyConsole and will be responsible for uploading your IDV subsystem. Once access is granted, the technical contact will receive login instructions by email. Questions about MyConsole access can be directed to rivr@mdtf.org.

Vendors will be expected to complete their submission to RIVR-2-IDV by the date posted at <https://mdtf.org/rivr2>. A “submission” is a software and data package uploaded using MyConsole.

The process is as follows:

- Login to MyConsole using your email address and OTP token.
- Navigate to the IDV upload tab.
- Upload test images and your containerized system.
 - Containerized system requirements are described in Technical Requirements (below).

- You will be asked to submit six test images:
 - State ID producing a genuine response – portrait side and non-portrait side.
 - State ID producing a fraudulent response – portrait side and non-portrait side.
 - Passport producing a genuine response – face page.
 - Passport producing a fraudulent response – face page.
- MyConsole will automatically validate the submission.
- Acceptance / rejection decision will be sent by email.

You must have at least one successful submission to be included in the RIVR-2-IDV evaluation. Up to three accepted submission attempts are allowed up until the submission deadline. Only the most recent accepted submission will be included in the RIVR-2-IDV evaluation.

Each submission will be checked against the requirements listed in System Requirements (below). If your submission is rejected, MyConsole will provide diagnostic information in the email with the rejection decision to help troubleshoot. If you require further assistance, limited troubleshooting support will be provided via rivr@mdtf.org. Please include the diagnostic information you received from MyConsole.

Evaluation

Test Dataset

Your IDV subsystem will be evaluated using a sequestered dataset of identity document images. Sample images will not be provided. The test data has the following properties:

- Document Validity:
 - Genuine documents and fraudulent documents.
- Document Types:
 - International passports (face page only)
 - U.S. state issued driver's licenses and ID cards.
 - Multiple issuing authorities.
- Image Quality Considerations:
 - Rotation from -180 to 180 degrees.
 - Optical blur and perspective distortions.
 - Variety of smartphone makes and models.
- Image Format:
 - JPEG or PNG format with the following extensions: *.jpg, *.png.

Data will be passed to your system as a request including DocumentFront and DocumentBack base64 encoded images (see <https://github.com/TheMdtF/mdtf-public/tree/master/apis/document-validation/api>).

For passports, DocumentFront will be an image of the face page and DocumentBack will be an empty string.

Metrics and Benchmarks

Your system will return results for each document in our dataset, and these results will be used to calculate the metrics listed. Metrics may be disaggregated by various factors, including but not limited to document state of issue and imaging smartphone. Each disaggregated metric will be compared to two

benchmarks: a threshold value, representing a high performing system, and a goal value, representing excellent performance.

Metric	Definition	Threshold	Goal
Document Processing Time	Time required for the system to return a response for a genuine document	10 (sec)	5 (sec)
System Error Rate (SER)	Proportion of document images for which the system fails to return an appropriate response	0.10	0.01
Document False Reject Rate (DFRR)	Proportion of genuine documents which the system determined to be invalid	0.10	0.01
Document False Accept Rate (DFAR)	Proportion of fraudulent documents which the system determines to be valid	0.10	0.01

RIVR-2-IDV uses a “**failure is suspicious**” policy: system errors on genuine documents are considered false rejections, and system errors on fraudulent documents are treated as fraudulent document detections.

RIVR-X Biometric Deepfake Participation

If you opted in to participating in the RIVR-2 biometric deepfake evaluation, your subsystem will be tested on digitally generated or manipulated images of documents. Details of this demonstration will be provided at a later date.

Technical Requirements

IDV systems shall process visible light images of identity documents and return a validity outcome. Your IDV system shall be uploaded as a Docker container to MdTF’s MyConsole. Docker images can be created using: `docker save ${COMPANY_NAME}-system:latest | gzip > ${COMPANY_NAME}-system.tgz`. For access information and expectations regarding MyConsole, see Process and Schedule (above).

The Docker container shall:

- Be a single container,
- Have either *.tgz or *.tar.gz file extension,
- Be started via a docker run command,
- Be Linux based,
- Host an HTTP server on port 8080,
- Implement the MdTF document-validation API: <https://github.com/TheMdTF/mdtf-public/tree/master/apis/document-validation/api>,
- Not exceed 5 GB in size,
- Have no CRITICAL or HIGH Common Vulnerabilities and Exploits (CVEs) at time of submission.
- Be able to process all test data (see Test Data),
- Have the Event field string in the Info schema set to: RIVR-2-IDV,
- Work without access to any external resource or network, and either:
 - Not require a license to operate, or

- Include a time-bound license to operate for a period of at least 3 months following submission for evaluation.