Remote Identity Validation Rally:

Passive PAD Application

Identity validation technology providers may apply to participate in the Presentation Attack Detection (PAD) Track of the Remote Identity Validation Rally (RIVR). Additional information about RIVR is available at <https://mdtf.org/rivr>, including but not limited to slides from informational webinars.

Please complete and submit the following form, in both .docx and .pdf, to apply for participation in the PAD track of RIVR as a **Passive PAD system**. Passive PAD systems do not require user or hardware action and will be evaluated in a technology test using previously acquired samples. Only edit the form boxes, the form is used to expedite application review.

**All application materials are due by August 8, 2025 at 11:59PM Eastern Standard Time. All application materials should be sent to** **peoplescreening@hq.dhs.gov** **and** **RIVR@mdtf.org****.**

# Company Information

Company Name: Click or tap here to enter text.

Company Country (use company headquarters country if multinational): Click or tap here to enter text.

Company Year Formed: Click or tap here to enter text.

Provide a brief description of company. Limit to 300 words.

Click or tap here to enter text.

|  |  |
| --- | --- |
| **Business Contact:** |  |
| Name:Click or tap here to enter text. | Email:Click or tap here to enter text. | Phone:Click or tap here to enter text. |

|  |
| --- |
| **Technical Contact:**This individual will be given access to MdTF MyConsole to submit your IDV system for evaluation. |
| Name:Click or tap here to enter text. | Email:Click or tap here to enter text. | Phone:Click or tap here to enter text. |

# Presentation Attack Detection System Commercial Deployments

Is your system commercially deployed? [ ] Yes [ ] No

If yes, please describe. Limit to 100 words:

Click or tap here to enter text.

When was the system first deployed (year): Click or tap here to enter text.

# Passive PAD System Technical Description

Provide a high-level overview of the underlying technology (e.g., DCNN) and the types of presentation attacks it is designed to detect. Limit to 300 words:

Click or tap here to enter text.

Can the system be provided as a single Linux Docker image (.tgz) under 5.0GB in size? [ ] Yes [ ] No

Can your system implement the MdTF Passive PAD API (<https://github.com/TheMdTF/mdtf-public/tree/master/apis/pad-systems/passive-pad-system/api>) including all required system inputs and outputs? [ ] Yes [ ] No

Can your system operate in a local environment without access to the internet? [ ] Yes [ ] No

Can your system detect attacks in both image and video media (JPEG, PNG, MOV, MP4)? [ ] Yes [ ] No

Can your system maintain media processing times below 10 seconds? [ ] Yes [ ] No

Can your system work without a GPU? [ ] Yes [ ] No

Required CPU: Click or tap here to enter text.

Required RAM: Click or tap here to enter text.

Required Disk: Click or tap here to enter text.

List any runtime dependencies that may affect operation in scalable microservice environments. Limit to 100 words:

Click or tap here to enter text.

# Performance Characteristics

Please describe any measurements of performance of your system and how they were tested. Include references to whitepapers, test events, and/or datasets. Limit to 300 words:

Click or tap here to enter text.

Please fill in the table below based on results of previous testing described above. Please provide metrics for your configured operating point/threshold value.

|  |  |
| --- | --- |
| Metric | Error Rate |
| System Error Rate (System Non-Response Rate) | Click or tap here to enter text. |
| Bona Fide Presentation Classification Error Rate (BPCER) | Click or tap here to enter text. |
| Attack Presentation Classification Error Rate (APCER) | Click or tap here to enter text. |

Metrics as defined in ISO/IEC 30107-3.

Please provide any additional information to consider about your system. Limit to 300 words:

Click or tap here to enter text.