U.S. Department of Homeland Security

SCIENCE AND TECHNOLOGY DIRECTORATE

Remote Identity Validation Rally
Presentation Attack Detection

Science and Technology

Yevgeniy Sirotin and **Richard Plesh**
Identity and Data Sciences Laboratory at
the Maryland Test Facility

Arun Vemury
Senior Engineering Advisor for Identity Technologies
DHS Science & Technology Directorate

July 31, 2025

[SCIENCE AND TECHNOLOGY DIRECTORATE]

Operationalizing science and technology.

The Science and Technology Directorate (S&T) researches, develops, tests, and evaluates solutions needed to meet the growing demands of our nation’s homeland security officials.

- We capture specific mission needs.
- We deliver impactful technology solutions.
- We conduct independent test and evaluation.

[INNOVATION: S&T IN ACTION]

Biometric & Identity Technology Center

S&T conducts foundational research to ensure advancements in science and technology are harnessed for cutting-edge solutions to new and emerging operational challenges.

- ☑ Drive biometric and identity innovation at DHS through research development, test and evaluation (RDT&E) capabilities
- ☑ Facilitate and accelerate understanding of biometrics and identity technologies for new DHS use cases
- ☑ Drive efficiencies by supporting cross cutting methods, best practices, and solutions across programs
- ☑ Deliver subject matter expertise across the DHS enterprise
- ☑ Engage industry and provide feedback
- ☑ Encourage innovation with industry and academia

Remote Identity Validation

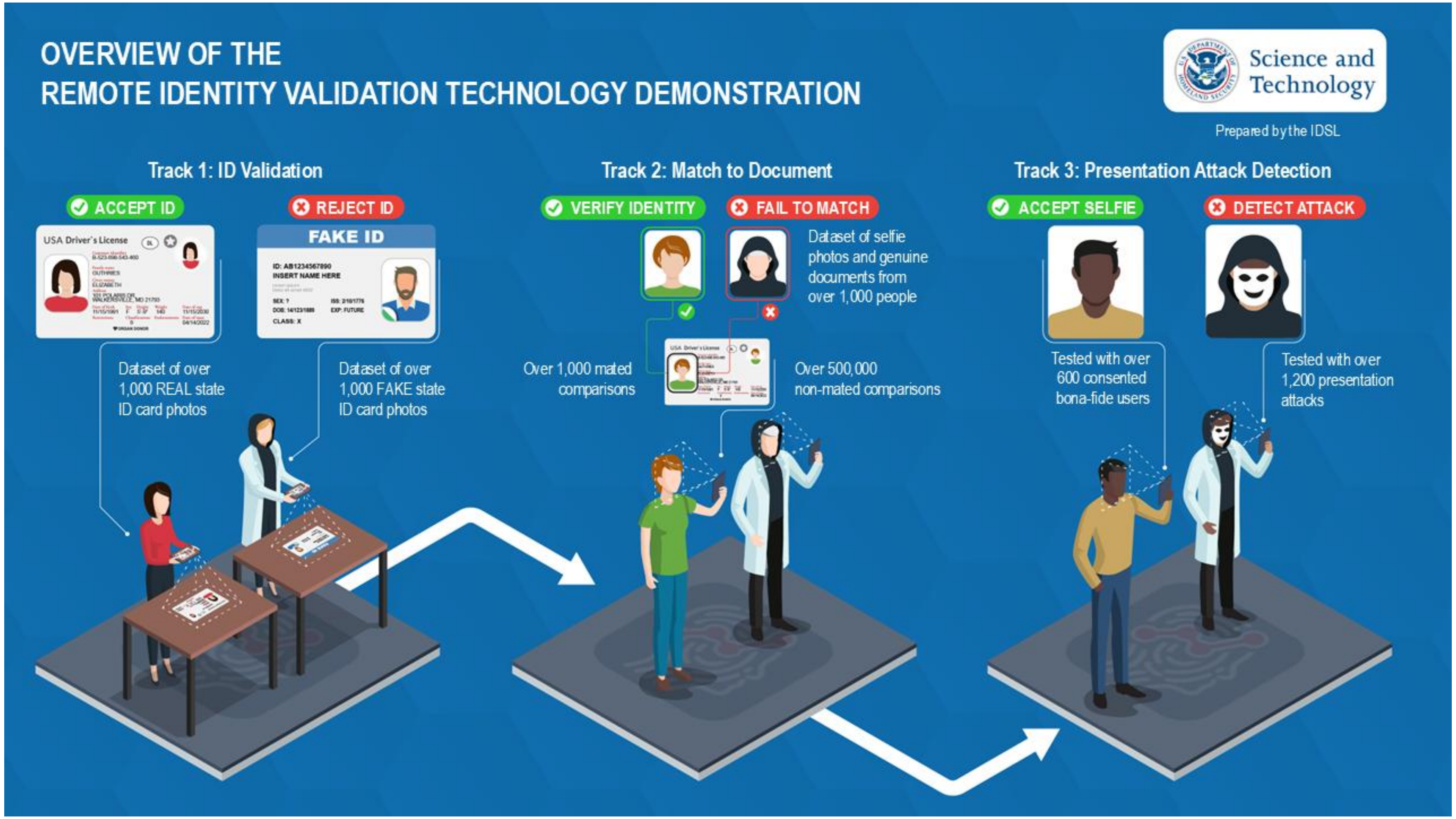
- Remote Identity Validation (RIV) technology is a tool to authenticate documents and verify the identity of users remotely

- These systems are complex, with multiple subsystems, and are increasing in popularity and adoption

- Industry performance benchmarks are not well defined making it difficult for organizations to test the effectiveness of these systems

- To address this need and spur industry innovation, DHS S&T carried out the Remote Identity Validation Technology Demonstration (RIVTD) from 2023 to 2024.
    - Comprehensively demonstrated performance of commercial RIV subsystems
    - Informed NIST digital identity guidelines
    - Identified metrics, performance gaps, and achievable performance benchmarks

Remote Identity Validation Technology Demonstration (RIVTD)



OVERVIEW OF THE
REMOTE IDENTITY VALIDATION TECHNOLOGY DEMONSTRATION

Science and Technology

Prepared by the IDSL

Track 1: ID Validation

ACCEPT ID

REJECT ID

Dataset of over 1,000 REAL state ID card photos

Dataset of over 1,000 FAKE state ID card photos

Track 2: Match to Document

VERIFY IDENTITY

FAIL TO MATCH

Dataset of selfie photos and genuine documents from over 1,000 people

Over 1,000 mated comparisons

Over 500,000 non-mated comparisons

Track 3: Presentation Attack Detection

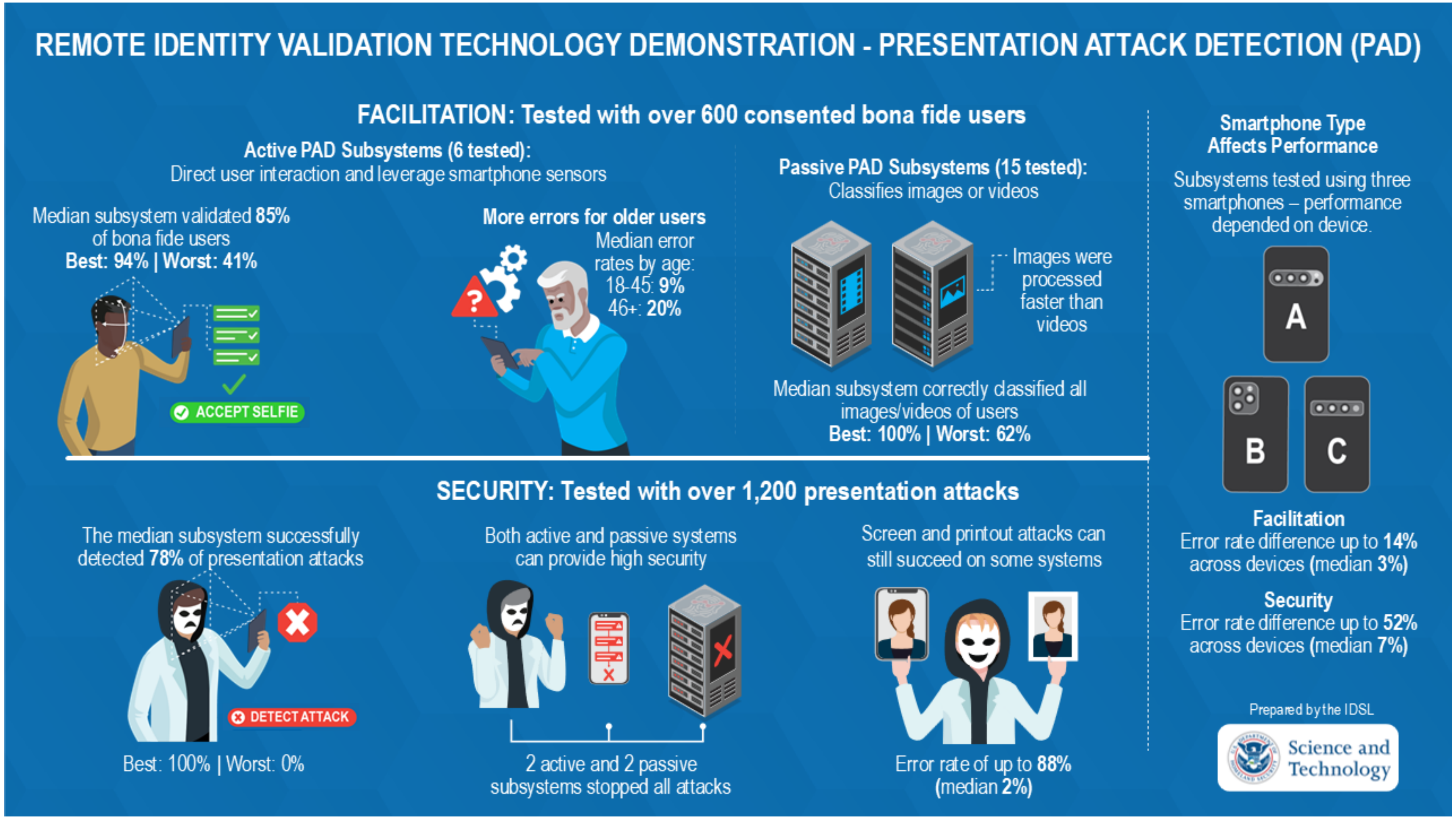
ACCEPT SELFIE

DETECT ATTACK

Tested with over 600 consented bona-fide users

Tested with over 1,200 presentation attacks

Remote Identity Validation Technology Demonstration (RIVTD)



REMOTE IDENTITY VALIDATION TECHNOLOGY DEMONSTRATION - PRESENTATION ATTACK DETECTION (PAD)

FACILITATION: Tested with over 600 consented bona fide users

Active PAD Subsystems (6 tested):
Direct user interaction and leverage smartphone sensors

Median subsystem validated **85%** of bona fide users
Best: 94% | Worst: 41%

More errors for older users
Median error rates by age:
18-45: **9%**
46+: **20%**

Passive PAD Subsystems (15 tested):
Classifies images or videos

Images were processed faster than videos

Median subsystem correctly classified all images/videos of users
Best: 100% | Worst: 62%

SECURITY: Tested with over 1,200 presentation attacks

The median subsystem successfully detected **78%** of presentation attacks

Best: 100% | Worst: 0%

Both active and passive systems can provide high security

2 active and 2 passive subsystems stopped all attacks

Screen and printout attacks can still succeed on some systems

Error rate of up to **88%** (median **2%**)

Smartphone Type Affects Performance

Subsystems tested using three smartphones – performance depended on device.

Facilitation
Error rate difference up to **14%** across devices (median **3%**)

Security
Error rate difference up to **52%** across devices (median **7%**)

Prepared by the IDSL

Science and Technology

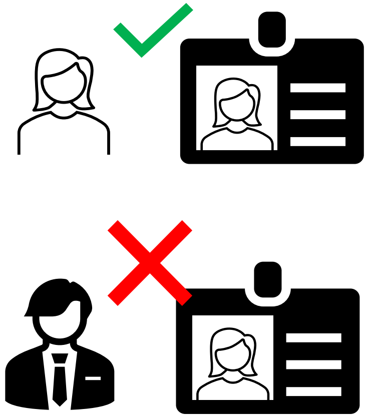
Remote Identity Validation Rally (RIVR)

- **Building on RIVTD Insights**: RIVTD identified key areas where RIV vendors should focus improvements, shaping the next phase of evaluation.
- **Establishing Achievable Benchmarks**: RIVR sets industry-informed performance benchmarks based on RIVTD results, providing clear targets for improvement.
- **Encouraging Innovation & Retesting**: Vendors have the opportunity to refine their technologies and participate in re-evaluation.
- **Confidential & Industry-Driven**: Vendor names are aliased, allowing companies to self-attest participation while fostering industry-wide progress.

RIVR Tracks

Selfie Match to Document

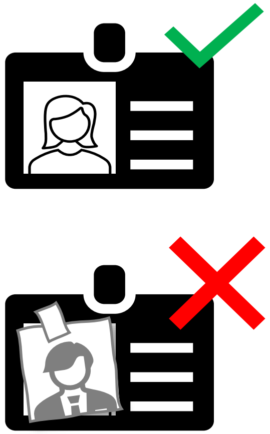
- 1:1 Verification



In Progress

ID Validation

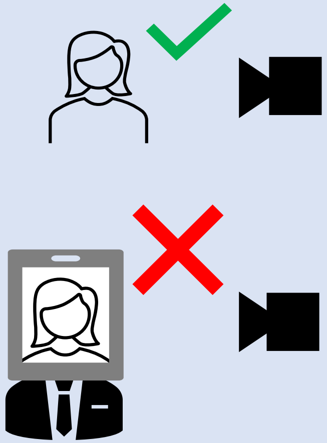
- Information Check
- Tamper Check
- Security Check



In Progress

Presentation Attack Detection (PAD)

- Reject screens and printouts
- Reject masks and other PAs

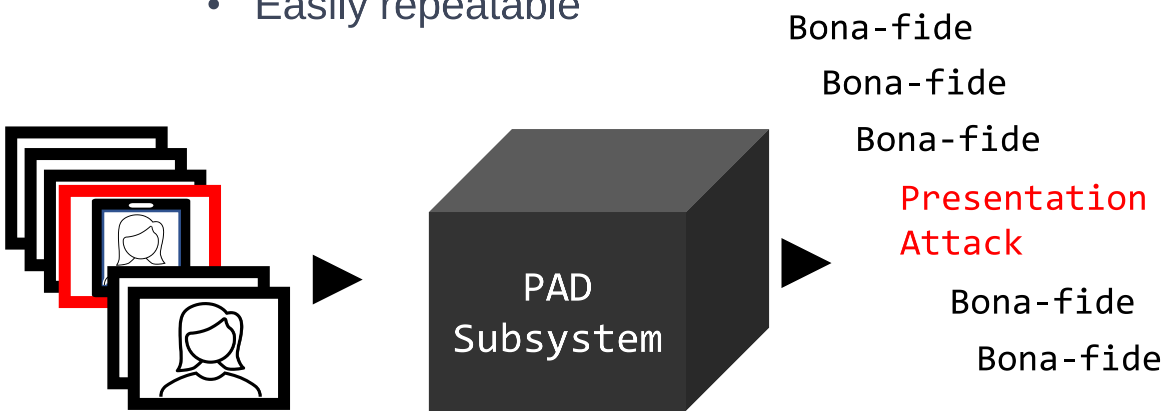


Today!

Presentation Attack Detection Track

Technology Tests vs. Scenario Tests

- Technology Testing:
  - Focus on performance of a multiple presentation attack detection subsystems (e.g., bona fide biometric samples, masks, replay videos)
  - Passive PAD Subsystems
  - Easily repeatable



PAD Subsystem

Bona-fide

Bona-fide

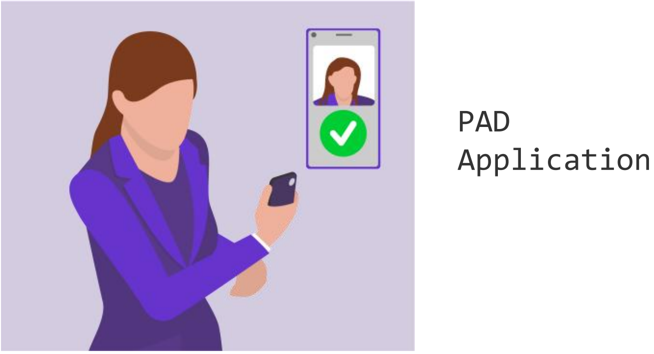
Bona-fide

Presentation Attack

Bona-fide

Bona-fide

- Scenario Testing:
  - Assess performance of PAD application in the context of use
  - Real people interact with the system
  - Active PAD subsystems
  - Costly to repeat



PAD Application

PAD track will include both technology and scenario testing of PAD subsystems.

Presentation Attack Detection Track

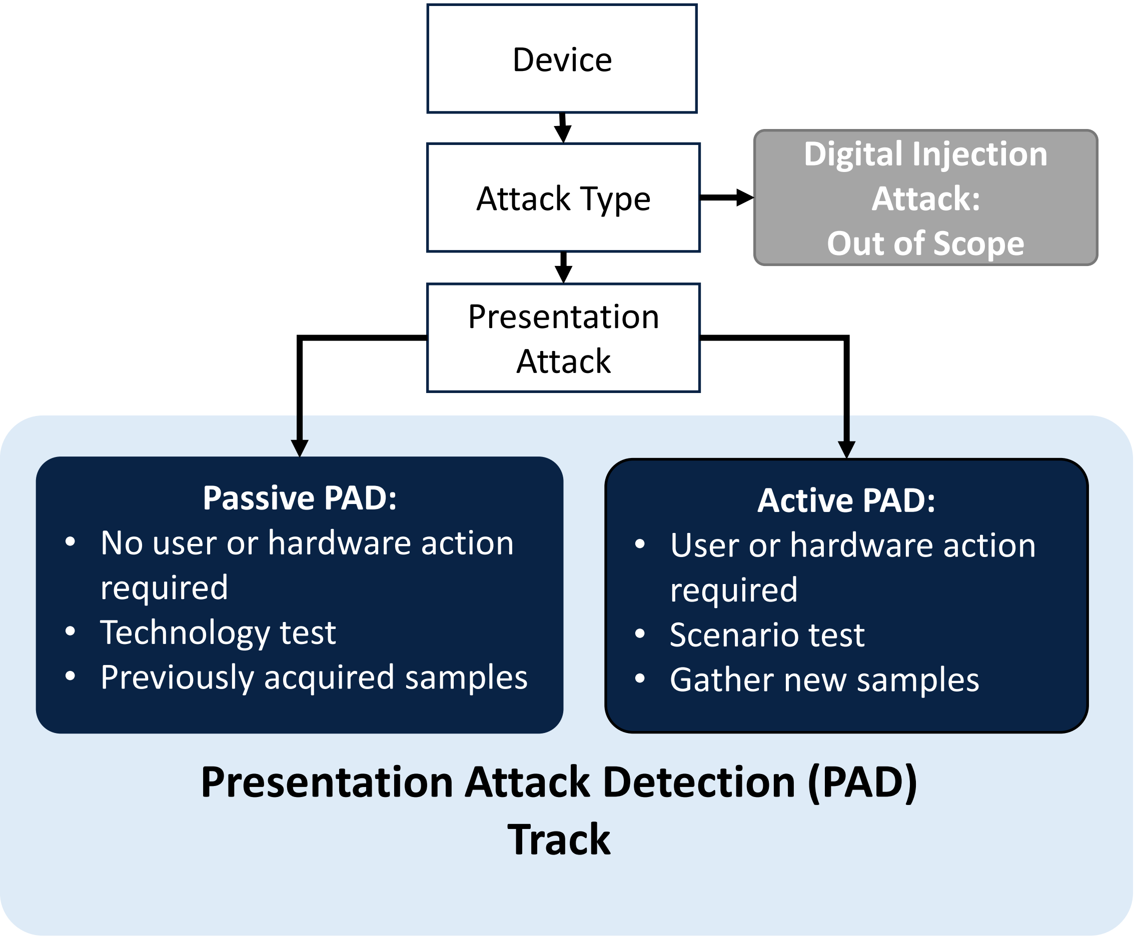
- PAD subsystems will demonstrate their ability to differentiate between presentation attacks and bona-fide users

- Presentation attacks will be performed through use of various attack instruments

- Two PAD subsystem types are in scope:
  - Passive PAD
  - Active PAD

Active PAD user action:
- Turn / Rotate head, blink, etc.

Active PAD hardware action:
- On-board cameras, sensors, etc.



Device

Attack Type

Digital Injection Attack: Out of Scope

Presentation Attack

Passive PAD:
- No user or hardware action required
- Technology test
- Previously acquired samples

Active PAD:
- User or hardware action required
- Scenario test
- Gather new samples

Presentation Attack Detection (PAD) Track

Track 3: Presentation Attack Instruments

Level A	Level B	Level C
• Printout on Paper • Display on Screen	• Paper Masks • Video Replay on Screen	• Attacks requiring special hardware and significant effort/cost to perform

- The number and specific species of PAIs will not be disclosed
- PAD performance will be assessed per PAI species

Active PAD Subsystem Requirements

About the Maryland Test Facility (MdTF)

- Active PAD subsystems will be evaluated at the MdTF in a scenario test
  - Conveniently located in Maryland near Washington DC

- You will need to physically install systems and any supporting hardware or equipment at a dedicated station

- Staff must be available to address break/fix issues encountered during testing

- **No access to the internet is allowed during the evaluation**

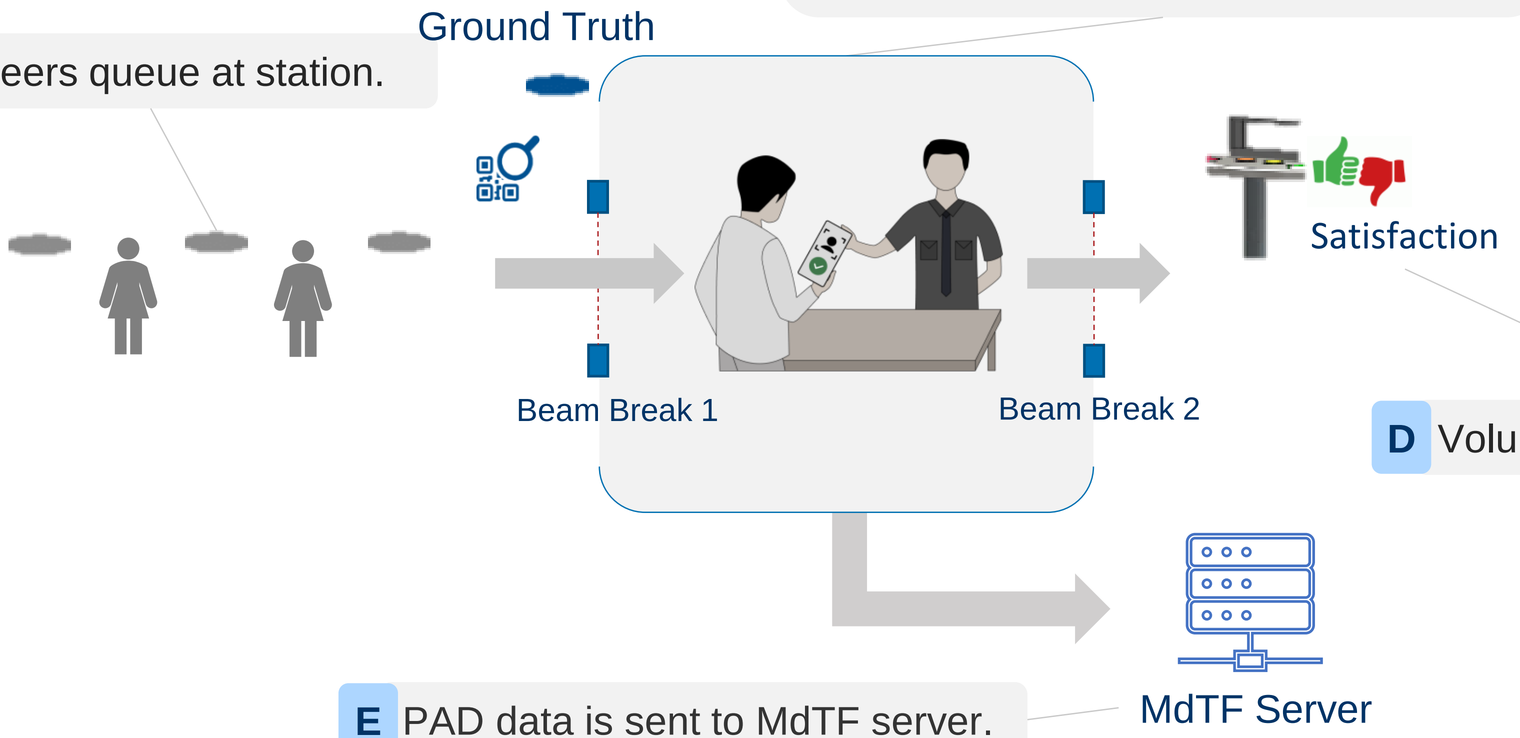
Active PAD Subsystem Scenario Test

B MdTF staff member starts transaction and volunteer enters station.

C MdTF staff member provides volunteer a device with installed PAD application. Volunteer initiates and performs one **PAD transaction** using device.

The PAD transaction may be either bona fide or a presentation attack.

A Volunteers queue at station.

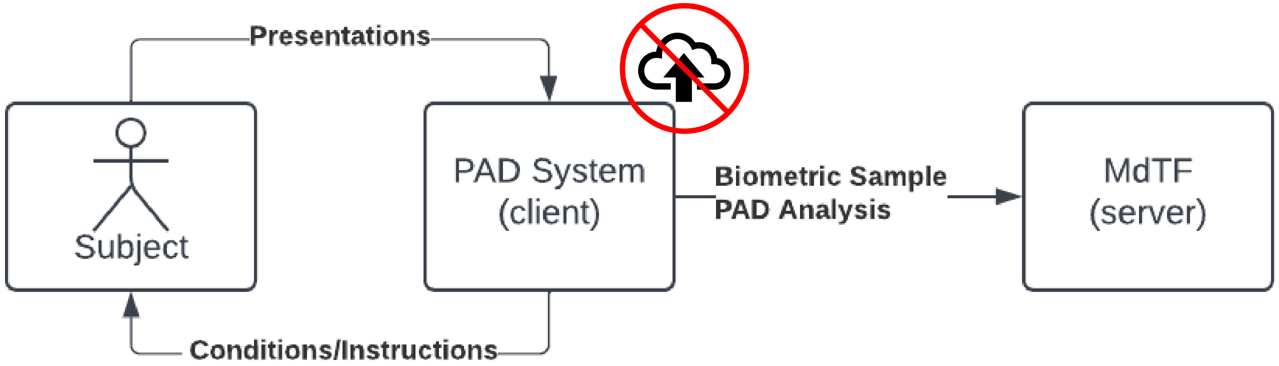


D Volunteer rates experience.

E PAD data is sent to MdTF server.

Active PAD Subsystem Requirements

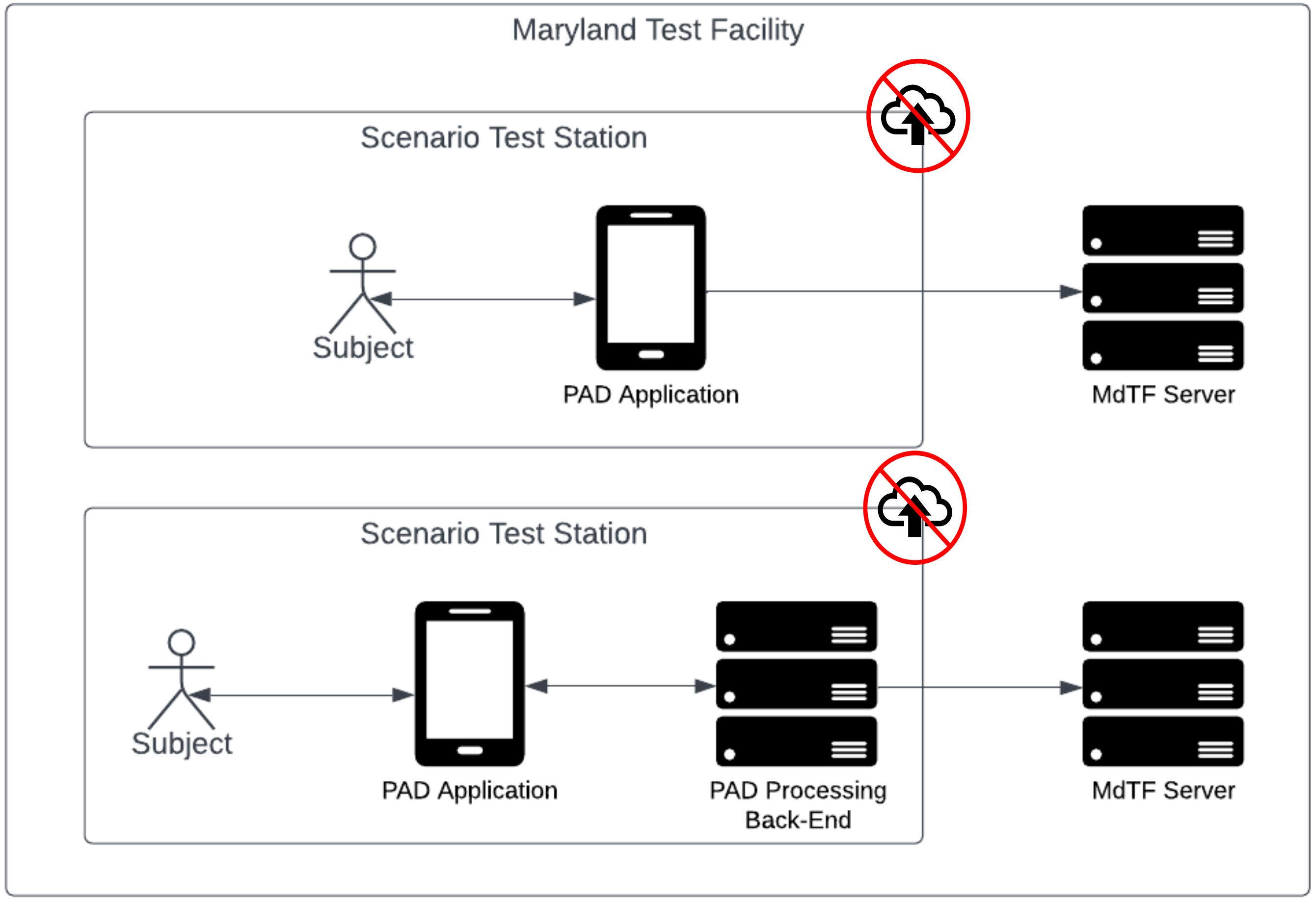
- Shall be installed in a physical test station at the MdTF
- Shall operate without access to the internet / cloud
- May leverage any additional compute resources installed within the test station
- Shall include an “app” on a smartphone to facilitate a subject completing a PAD transaction
  - i.e., Subject will use the “app” and complete any required actions
- May instruct the subject and use standard hardware / sensors on the smartphone



Sample Hardware Setup at MdTF

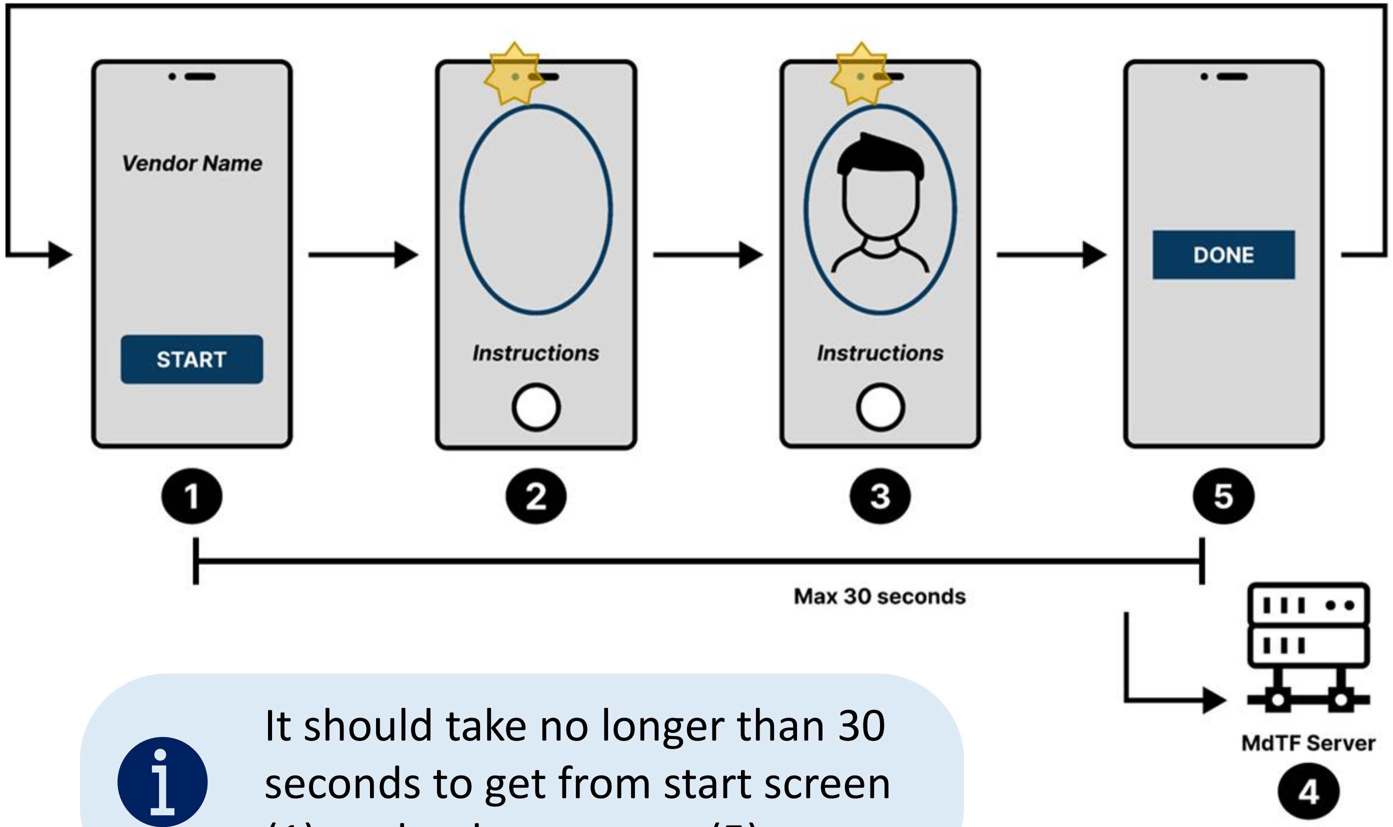
- Option 1:
  - All processing performed on mobile device
  - Mobile device sends results to MdTF Server

- Option 2:
  - Some processing performed on collaborator-furnished back-end server in the test station
  - Collaborator back-end server sends results to MdTF Server



Sample PAD Application

1. **Home Screen**
   - Contains a button to start capture
   - Proceed to Capture (2) on tap
2. **Biometric Capture Screen**
   - Provides instructions
   - Captures a face sample using front camera
3. **Volunteer Interaction**
   - Volunteer follows instructions
4. **API Response**
   - Sample acquired and analyzed → Send result to MdTF Server (4)
5. **Done**
   - Volunteer Interaction complete or 30 second limit reached → Present "Done" screen (5)
   - "Done" button push → Reset to Home Screen (1)



It should take no longer than 30 seconds to get from start screen (1) to the done screen (5).

Additional Active PAD Subsystem Requirements

- Technology provider shall deliver their active PAD subsystem installed on the following platforms:
  - iOS smartphone (e.g., iPhone 14)
  - Android smartphone (e.g., Samsung Galaxy S22)

- Shall implement the RIVR Active PAD subsystem API
  - Review API requirements at http://github.mdtf.org
  - Demonstrate API conformance before arriving at MdTF

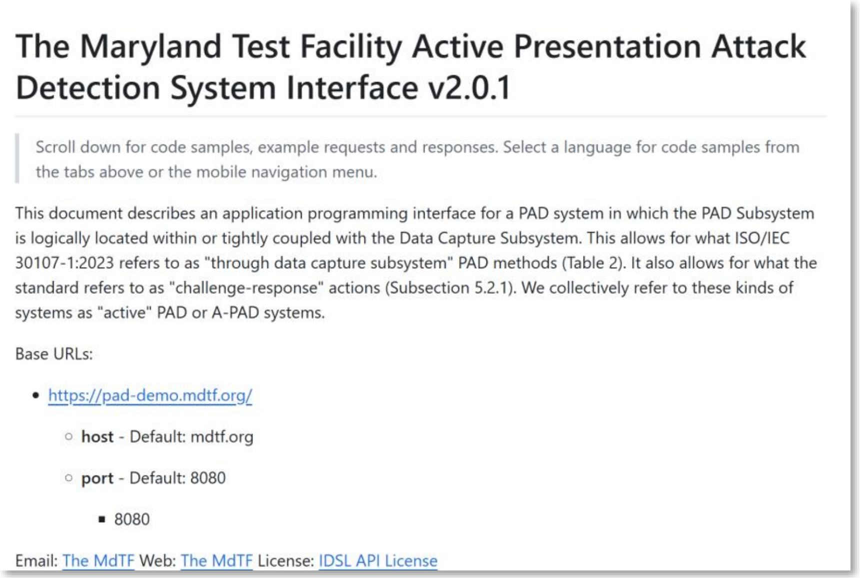
- Conform with MdTF physical/network requirements

- No biometric comparison is required

- Shall cost share with DHS S&T non-recurring engineering costs (e.g., scenario test planning, engineering, volunteer compensation)

iPhone 14

Samsung Galaxy S22



The Maryland Test Facility Active Presentation Attack Detection System Interface v2.0.1

> Scroll down for code samples, example requests and responses. Select a language for code samples from the tabs above or the mobile navigation menu.

This document describes an application programming interface for a PAD system in which the PAD Subsystem is logically located within or tightly coupled with the Data Capture Subsystem. This allows for what ISO/IEC 30107-1:2023 refers to as "through data capture subsystem" PAD methods (Table 2). It also allows for what the standard refers to as "challenge-response" actions (Subsection 5.2.1). We collectively refer to these kinds of systems as "active" PAD or A-PAD systems.

Base URLs:

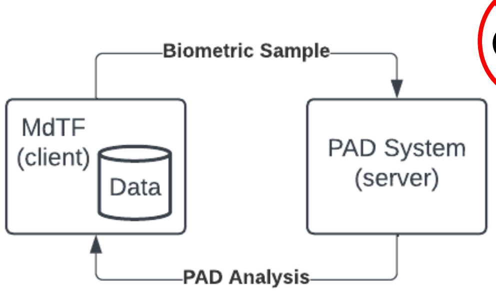
- https://pad-demo.mdtf.org/
  - **host** - Default: mdtf.org
  - **port** - Default: 8080
    - 8080

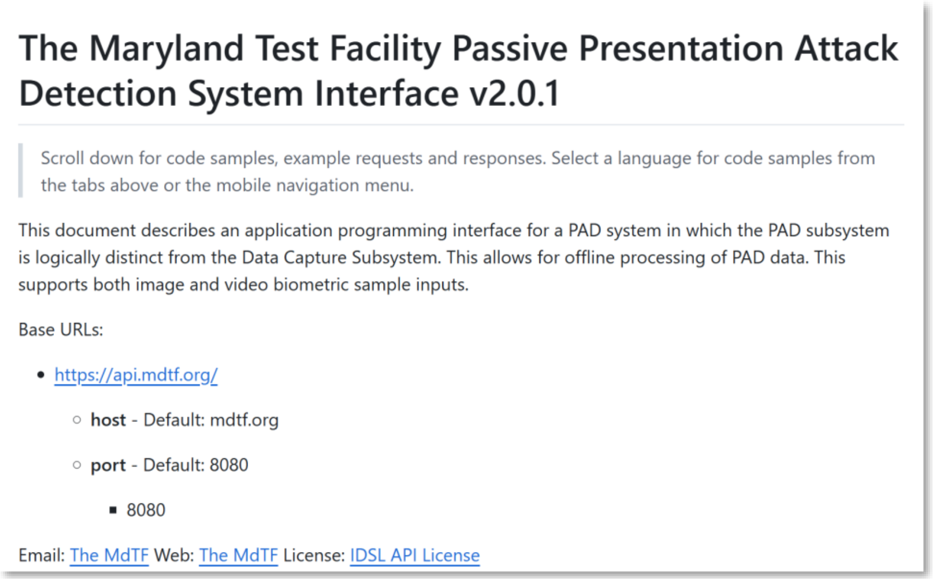
Email: The MdTF Web: The MdTF License: IDSL API License

Passive PAD Subsystem Requirements

Passive PAD Subsystem Requirements (1)

- Passive PAD subsystems will be evaluated at the MdTF in a technology test
- Shall be packaged in a single **Docker** image
- Shall require **no outside functionality** and will be run on internal machines without access to the internet
- Shall operate on **previously** acquired biometric samples from a selection of mobile phones
- Shall implement the RIVR Passive PAD System API
  - Review API requirements at http://github.mdtf.org





The Maryland Test Facility Passive Presentation Attack Detection System Interface v2.0.1

> Scroll down for code samples, example requests and responses. Select a language for code samples from the tabs above or the mobile navigation menu.

This document describes an application programming interface for a PAD system in which the PAD subsystem is logically distinct from the Data Capture Subsystem. This allows for offline processing of PAD data. This supports both image and video biometric sample inputs.

Base URLs:

- https://api.mdtf.org/
  - **host** - Default: mdtf.org
  - **port** - Default: 8080
    - 8080

Email: The MdTF Web: The MdTF License: IDSL API License

Bona-fide “Selfie” Images and Videos

- Bona-fide samples will be drawn from a dataset of “selfie” images and videos

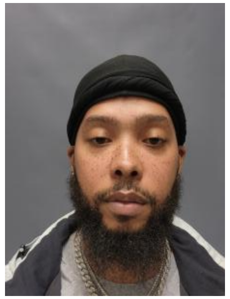
- Imagery will be captured in a standard environment at MdTF
  - Selfie images and videos may include variation in pose and expression
  - Selfie video will be 10 seconds long

- Images and video will be acquired using a selection of mobile phones
  - Images will be JPEG or PNG
  - Videos will be MOV or MP4

- Images and videos will be provided as base64 encoded strings

Samsung Galaxy S22

iPhone 14



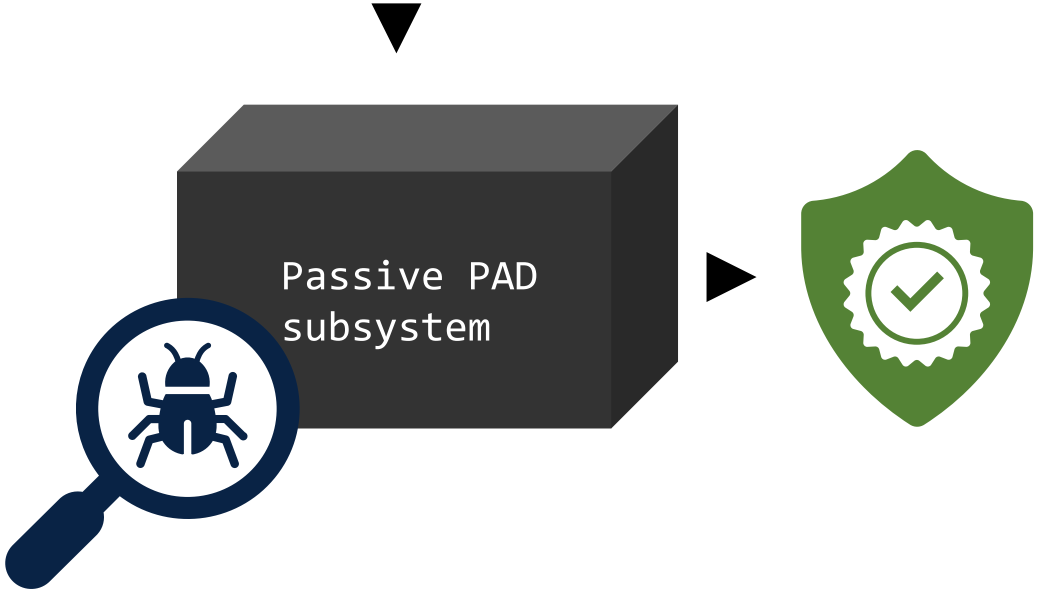
All volunteers shown here consented to have their images used in government presentations.

ℹ Passive PAD subsystems must accept both images and video samples.

Passive PAD Subsystem Requirements (2)

- Deployed inside a single Linux-based **docker** container, started via a docker run command
- Delivered via a **.tgz** uploaded to the **MdTF MyConsole** (limit 5GB)
- Provide **two test samples (jpg, png, mov, mp4)** to produce True and False PADOutcome
- Docker containers will be automatically assessed for API compliance and security
- Issues will be automatically flagged and sent to console users
- If subsystems require a **license to operate**, that license shall be time bounded to operate, without restrictions (usage, machine portability, etc.) for at least 1 year from the RIVR Presentation Attack Detection submission deadline

```
docker save ${COMPANY_NAME}-rivr-pad-system:latest |
gzip > ${COMPANY_NAME}-rivr-pad-system.tgz
```



PAD
Subsystem Metrics

System Error Rate

- Active and Passive PAD subsystems

- System Error Rate (SER):
  - Active PAD - Proportion of presentations for which no PAD data capture is sent
  - Passive PAD - Proportion of biometric samples for which no PAD analysis result is returned
  - **Threshold: 0.10, Goal: 0.01**

- Systems should return a result for each presentation
- **Failure is suspicious policy:** failure to respond will be interpreted as an attack detected response

ℹ All non-responses from the PAD subsystem will be treated as errors.

ℹ Video recordings of volunteers interacting with an Active PAD subsystem may show why a system error occurred.

PAD Efficiency and Satisfaction Metrics

- Passive PAD - Average Run Time
  - Amount of time needed to process a bona fide presentation sample with the PAD subsystem
  - Average Run Time Max is the maximum time needed across devices
    - **Expected: < 10 seconds**

- Active PAD - Average Transaction Time
  - Amount of time needed to complete a bona fide transaction with the PAD subsystem
  - Average Transaction Time Max is the maximum time needed across devices
    - **Threshold: 30 seconds, Goal: 20 seconds**

- Active PAD - Positive Satisfaction Rate
  - Percent of volunteers who give positive satisfaction ratings after using the PAD subsystem
  - Positive Satisfaction Rate Min is the minimum rate across devices
    - **Threshold: 90%, Goal: 95%**

PAD Effectiveness

- Active and Passive PAD Subsystems

- Bona fide Presentation Classification Error Rate (BPCER)
  - BPCER is the proportion of bona fide presentations that result in presentation attack classification
  - $\text{BPCER}_{\text{Max}}$ is the maximum BPCER across devices
    - **Threshold: 0.05, Goal: 0.01**
  - **Failure is suspicious policy: system errors treated as bona fide classification errors**

- Attack Presentation Classification Error Rate (APCER)
  - APCER is the proportion of attack presentations that result in bona fide classification
  - $\text{APCER}_{\text{Max}}$ is the maximum APCER across tested attack species and devices
    - **Threshold: 0.10, Goal: 0.01**
  - **Failure is suspicious policy: system errors treated as presentation attack detections**

- Demographic Effects:
  - Metrics may be calculated separately for different demographic groups: Age, Sex, Race, and Skin Tone

PAD
Track Participation

Benefits of Participation

- Demonstrate the technical maturity of your product
- Inform government and other stakeholders regarding your system’s performance in an operationally relevant evaluation
- Understand performance of your system relative to industry averages
- Returning systems can gauge performance improvement over time
- Form an ongoing Cooperative Research and Development Agreement (CRADA) with DHS S&T
  - Protects your intellectual property
  - Provides mechanism for ongoing dialog and collaboration with DHS S&T
  - Provides opportunity for data sharing

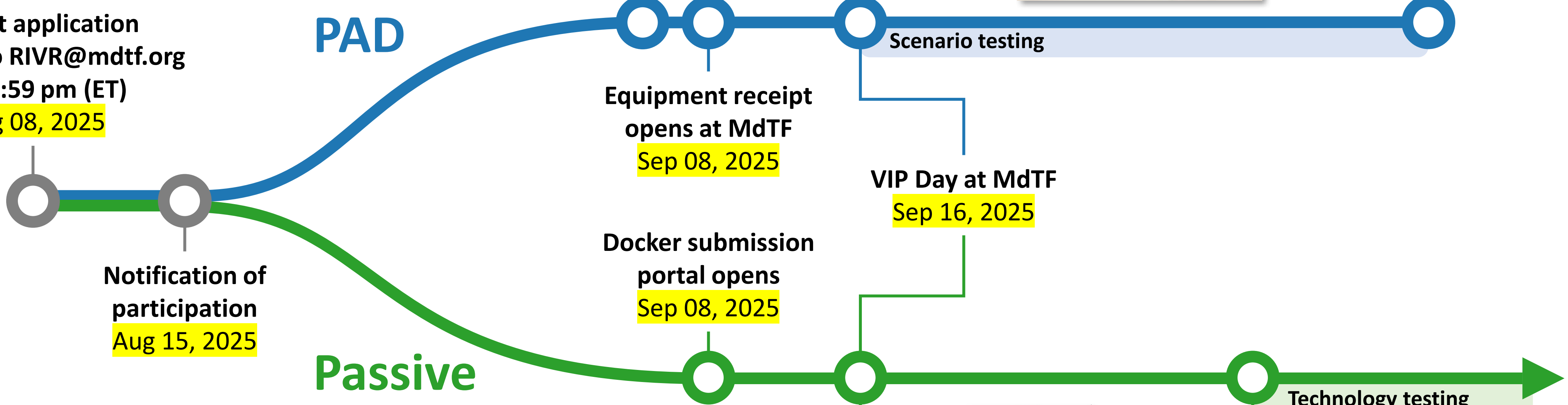
Application Package Requirements

- Complete application form for the RIVR PAD Track:
  1. Description of the company
  2. Description of Presentation Attack Detection subsystem commercial deployments
  3. Describe subsystem technology and attest it will align with the MdTF API
  4. Provide measurements of the performance characteristics of the system

- Application form will be made available at https://mdtf.org
- Submit application form to RIVR@mdtf.org by **11:59pm (ET) August 8, 2025**

These webinar slides and detailed application package instructions will be made available at https://mdtf.org/rivr

What’s next? – PAD Track Deadlines



Submit application package to RIVR@mdtf.org by 11:59 pm (ET) Aug 08, 2025

Notification of participation Aug 15, 2025

Active PAD

Demonstrate API conformance Sep 05, 2025

Equipment receipt opens at MdTF Sep 08, 2025

Equipment install at MdTF Sep 15, 2025

VIP Day at MdTF Sep 16, 2025

Scenario testing

Equipment return after Dec 19, 2025

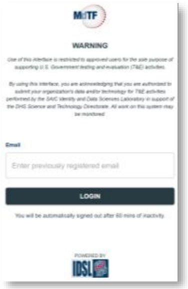
Passive PAD

Docker submission portal opens Sep 08, 2025

Initial Docker submission Sep 15, 2025

Final Docker submission Oct 03, 2025

Technology testing



WARNING

Use of this interface is restricted to approved users for the sole purpose of supporting U.S. Government testing and evaluation (T&E) activities.

By using this interface, you are acknowledging that you are authorized to submit your organization's data and/or technology for T&E activities performed by the SAIC Identity and Data Sciences Laboratory in support of the DHS Science and Technology Directorate. All work on this system may be monitored.

Email

Enter previously registered email

LOGIN

You will be automatically signed out after 60 mins of inactivity.

POWERED BY

Participation will require executed CRADA with DHS S&T.
CRADA execution requires signature of authorized company representative.

Science and Technology

Questions & Answers

- Contact information
  - Programmatic: peoplescreening@hq.dhs.gov
  - Technical: RIVR@mdtf.org
- Visit our websites for additional information
  - To see additional work DHS S&T supports, visit www.dhs.gov/science-and-technology
  - For information about this and other DHS S&T technology evaluations, visit https://mdtf.org

These webinar slides and detailed application package instructions will be made available at https://mdtf.org/rivr