

U.S. Department of Homeland Security

---

# SCIENCE AND TECHNOLOGY DIRECTORATE

Remote Identity Validation Tech Demo Challenge



Science and  
Technology

**Yevgeniy Sirotin**

Identity and Data Sciences Laboratory at  
the Maryland Test Facility

**Arun Vemury**

Senior Engineering Advisor for Identity Technologies  
DHS Science & Technology Directorate

January 2024

[ SCIENCE AND TECHNOLOGY DIRECTORATE ]

# We are the Department's Science Advisor and research and development arm.

---

Since 2003, the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) has provided sound, evidence-based scientific and technical perspectives to address a broad spectrum of current and emerging threats.

---





# 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 Tech Demo (RIVTD)

- Industry has developed new tools to authenticate documents and verify the identity of users remotely:
  - Remote Identity Validation (RIV)
- Difficult for industry to test the effectiveness and fairness of these systems:
  - Hard to obtain fraudulent documents
  - Testing for demographic differentials is costly
- DHS S&T is interested in understanding the current performance of RIV and helping industry to develop more secure, accurate, and equitable technologies

# 2023 Remote Identity Validation Technology Demonstration (RIVTD)

- DHS S&T is looking for full RIV systems and/or component technologies that are capable of:
  1. Assessing the validity of an identity document (US driver's license)
  2. Matching a “selfie” photo to the photo on the identity document
  3. Assessing the “liveness” of the “selfie” photograph
- DHS S&T encourages providers of technologies that can perform any portion of the RIV process to apply to participate in this demonstration
- The demonstration will follow a phased approach such that each step in the RIV process will be demonstrated separately



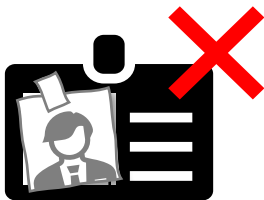
# Technology Demonstrations

- Demonstrations are a distinct evaluation performed by DHS S&T
  - Allows DHS S&T to survey the current state of technology
  - Provides technology providers an opportunity to:
    - Demonstrate their capabilities to government and private sector stakeholders
    - Collaboratively evaluate technologies with DHS S&T
- Quantitative results of the Remote Identity Validation Technology Demonstration will be shared within the government and with participating companies
- Select insights may be shared publicly in a manner that preserves the anonymity of the companies that participated

# RIVTD Tracks

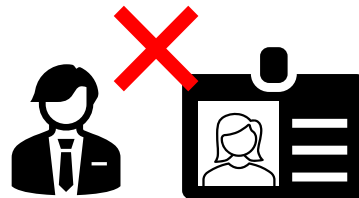
## Track 1: ID Validation

- Information Check
- Tamper Check
- Security Check



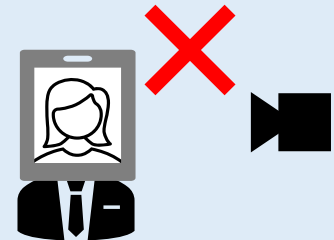
## Track 2: Match to ID

- 1:1 Verification



## Track 3: Liveness and Presentation Attack Detection (PAD)

- Reject screens and printouts
- Reject masks and other PAs

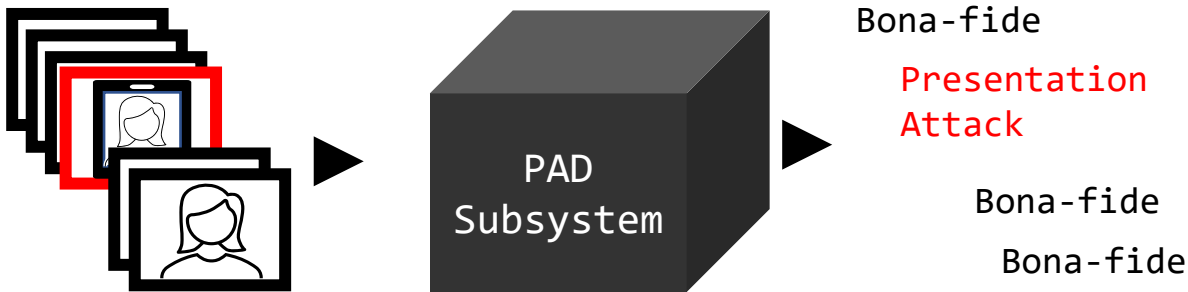


Current focus is Track 3: Liveness and Presentation Attack Detection

# Technology Tests vs. Scenario Tests

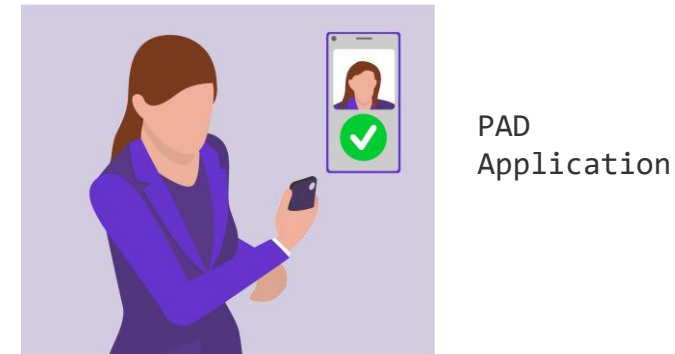
- Technology Testing:

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



- Scenario Testing:

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



Track 3 will include both technology and scenario testing of PAD subsystems.



# Track 3: Presentation Attack Detection

- 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

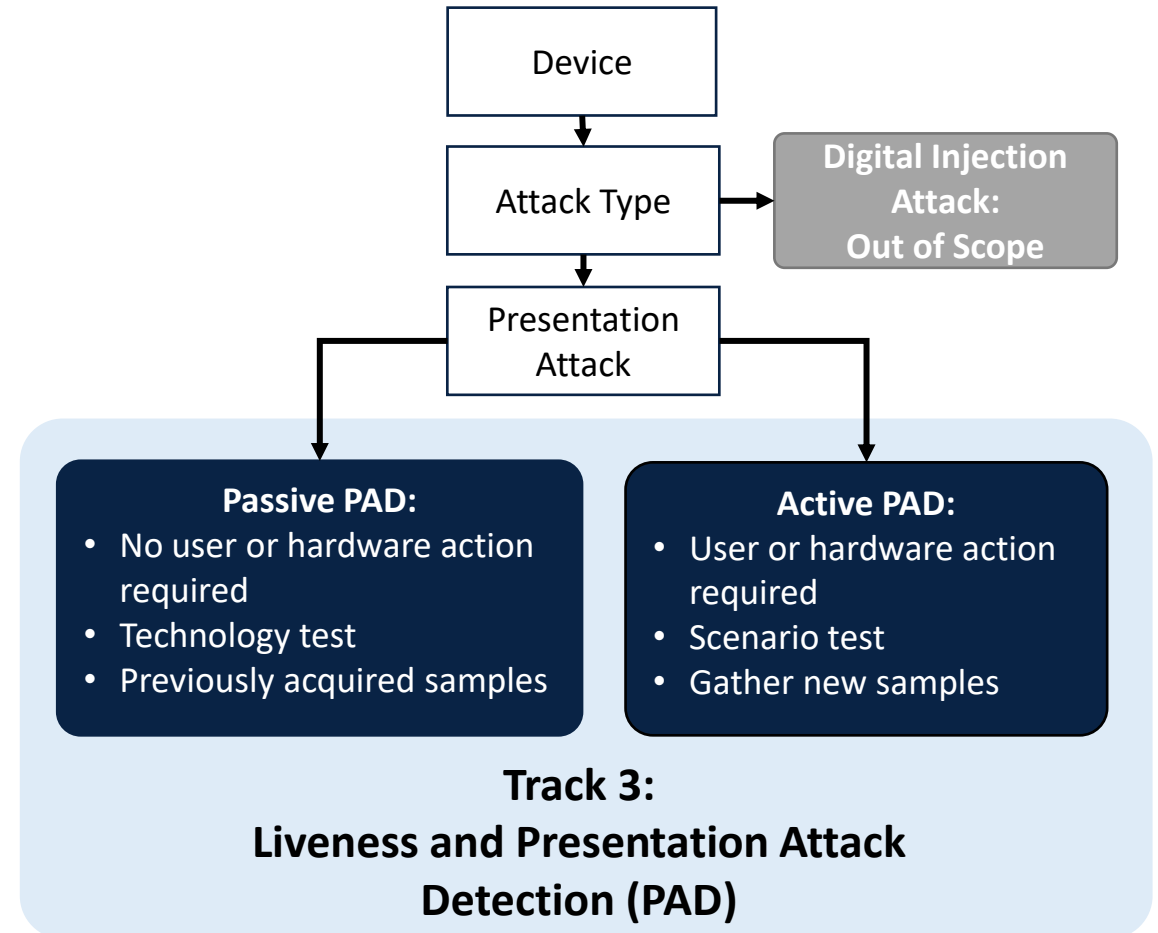


Active PAD user action:

- Turn / Rotate head, blink, etc.

Active PAD hardware action:

- On-board cameras, sensors, etc.



# Track 3: Presentation Attack Instruments

Level A	Level B	Level C
<ul style="list-style-type: none"><li>• Printout on Paper</li><li>• Display on Screen</li></ul>	<ul style="list-style-type: none"><li>• Paper Masks</li><li>• Video Replay on Screen</li></ul>	<ul style="list-style-type: none"><li>• Attacks requiring special hardware and significant effort/cost to perform</li></ul>

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

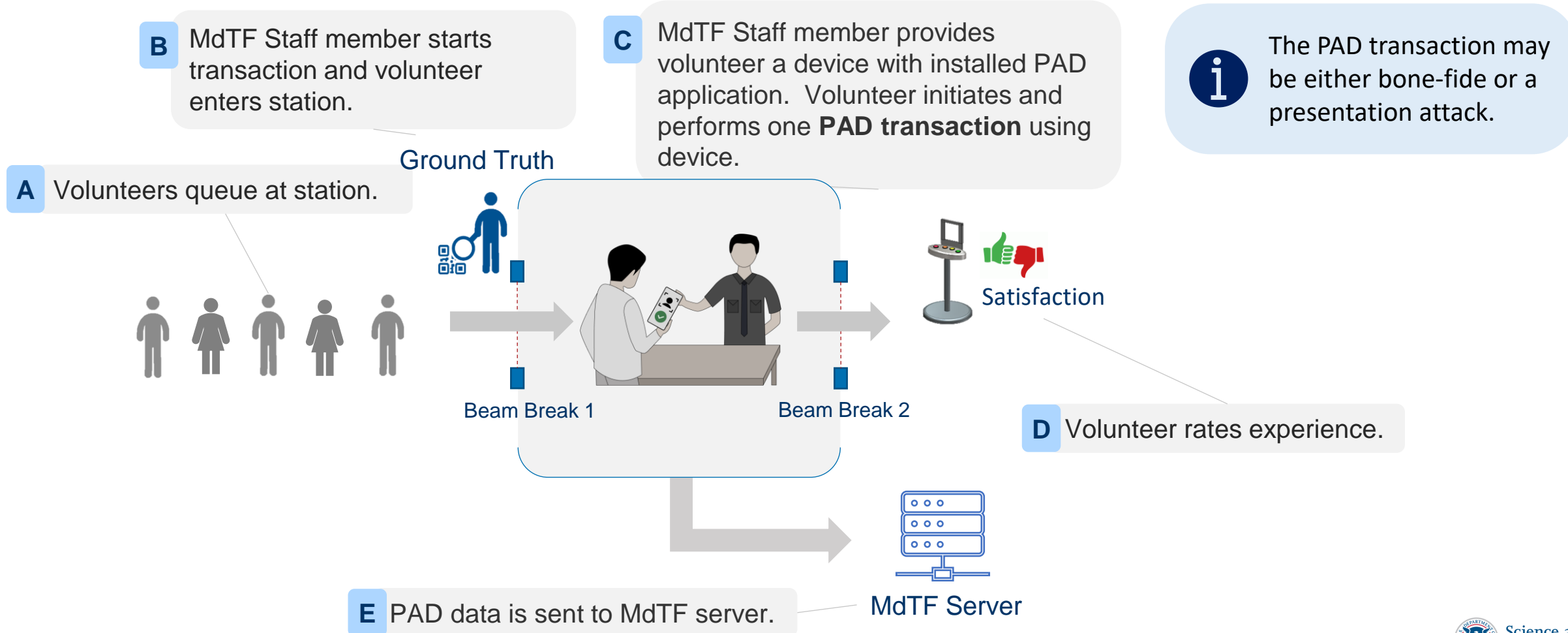
# Active PAD Subsystem Requirements

# About the Maryland Test Facility (MdTF)

- Active PAD subsystems will be demonstrated at the MdTF
  - 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 demonstration**

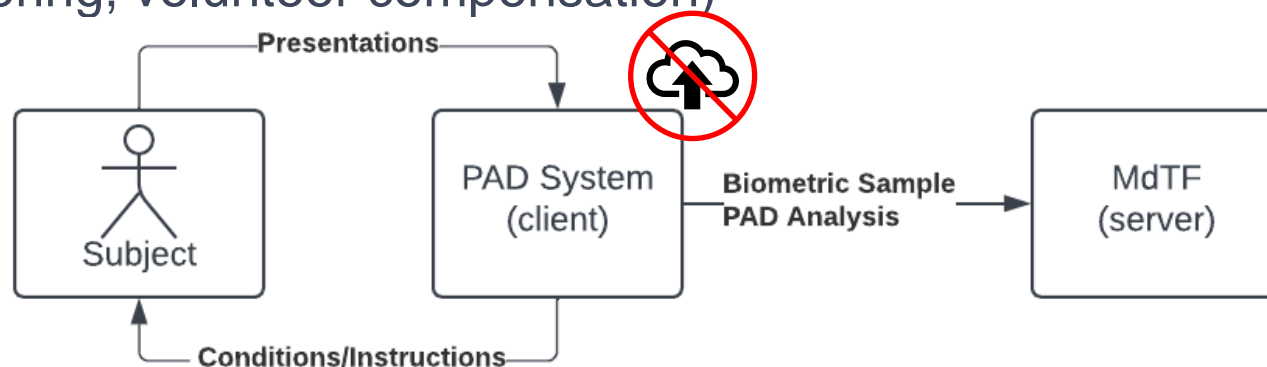


# Active PAD Subsystem Scenario Test



# Active PAD Subsystem Requirements (1)

- 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
- Shall implement the RIVTD Active PAD subsystem API
- May instruct the subject and use standard hardware / sensors on the smartphone
- Shall cost share with DHS S&T non-recurring engineering costs (e.g., scenario test planning, engineering, volunteer compensation)



# Active PAD Subsystem Requirements (2)

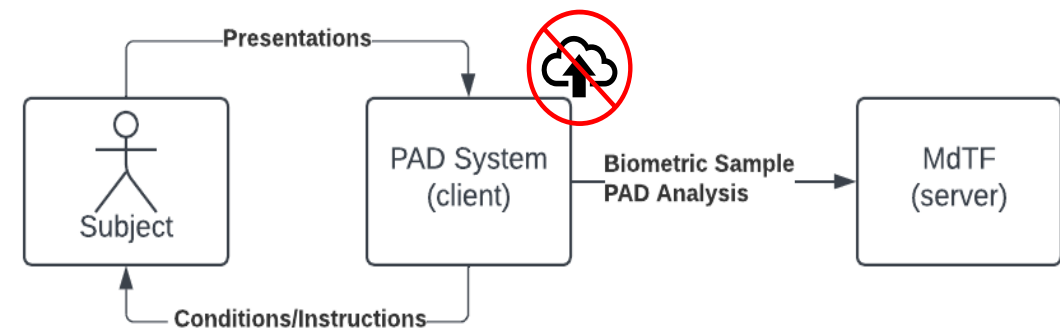
- Technology provider shall deliver their active PAD subsystem installed on the following platforms:
  - iOS Mobile Phone (e.g., iPhone 14)
  - Android Mobile Phone (e.g., Samsung Galaxy S22)
- No biometric comparison is required
- Shall provide the following to the MdTF server for each transaction:
  - Biometric Sample
  - PAD Outcome: (true or false)
  - PAD Score: (0 – 1)
  - PAD Properties (key value pairs)



iPhone 14



Samsung Galaxy S22



# RIVTD Track 3 – Active PAD API

## The Maryland Test Facility Active Presentation Attack Detection System Interface

2.0.0 OAS 3.0

### Data Submission

**POST** /v1/capture-data-with-pad Create a biometric data capture with associated PAD information.

- Active PAD subsystems shall send:
  - Biometric Sample
  - PAD Outcome (true or false)
  - PAD Score (0-1)
  - PAD Properties (key value pairs)
- API Documentation is available at:
  - <http://github.mdtf.org/>



# Biometric Sample

- PAD subsystems shall provide **Biometric Sample** data
- The biometric sample should best represent the PAD decision:
  - If bona-fide, it's the sample that best represents the bona-fide face
  - If presentation attack, it's the sample that best represents the attack



The biometric sample can be a still image or a short video clip (<10 seconds).

```
PADDataCapture {
  description: Data transfer object for biometric data capture and presentation attack information.
  BiometricSample* string
  example: iVBORw0KGgoAAAANSUhEUgAAAAEAAAABCAIAAACQd1PeAAAAEELQVR4nGJiYGAABAAA//8ADAADcZGLFWAAAABJRUSErkJggg==
  x-nullable: false
  The captured biometric sample, encoded as a base64 string. This can be an image, encoded as a PNG or JPEG or a short (<15s) video, encoded as a MOV.
  PADAnalysis*
  PADAnalysis {
    description: Data transfer object for presentation attack information.
    PADOutcome* boolean
    example: true
    Whether a presentation attack was determined to be detected (True) or not detected (False).
    PADScore* number($double)
    example: 0.8
    A score corresponding to the level of confidence that a presentation attack was detected ranging between 0 and 1.
    PADProperties
    [
      example: List [ OrderedMap { "Property": "EyesMoving", "Value": true }, OrderedMap {
        "Property": "MouthMoving", "Value": true }, OrderedMap { "Property": "PupilsResponsive",
        "Value": true }, OrderedMap { "Property": "NonconformantILLuminationDetected", "Value":
        true }, OrderedMap { "Property": "MoirePatternDetected", "Value": true }, OrderedMap {
        "Property": "ObsscurationDetected", "Value": true } ]
      Key value pairs describing presentation attack properties and their relationship to the
      presentation attack outcome/score. There are no strictly defined properties. The inclusion
      of descriptive properties is encouraged to provide more context. (optional)
    PADProperty > {...}
  }
}
```

# PAD Outcome and PAD Properties

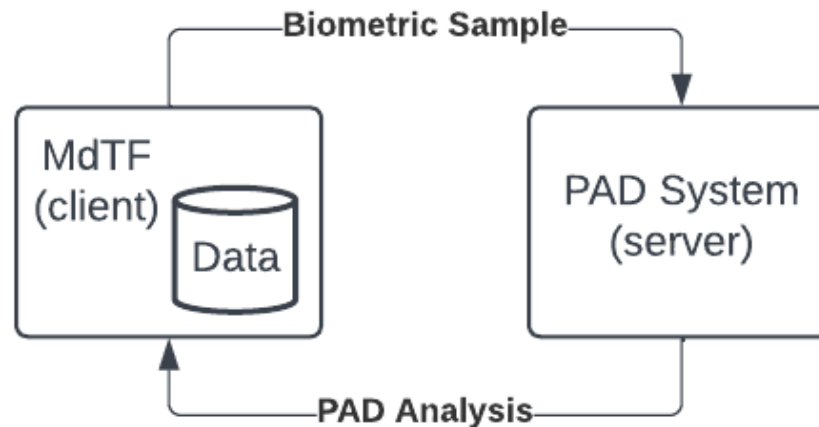
- Each PAD DataCapture shall provide PAD Analysis results
- **PADOutcome** must specify whether the biometric sample is bona-fide (False) or a presentation attack (True)
- **PADScore** indicates level of confidence on whether the biometric sample is a PA:
  - 1 means 100% certain it's a PA
  - 0 means 0% certain it's a PA (i.e., its bona-fide)
- **PADProperties** are key value pairs indicating any properties used by the PAD subsystem to determine PAD outcome and the values of those properties

```
PADDataCapture {
  description: Data transfer object for biometric data capture and presentation attack information.
  BiometricSample* string
  example: iVBORw0KGgoAAAANSUhEUGAAAAEAAAABCAIAAACQd1PeAAAAEELQVR4nGJiYGAABAAA//8ADAADcZGLFwAAAAABJRUS5ErkJggg==
  x-nullable: false
  The captured biometric sample, encoded as a base64 string. This can be an image, encoded as a PNG or JPEG or a short (<15s) video, encoded as a MOV.
  PADAnalysis* PADAnalysis {
    description: Data transfer object for presentation attack information.
    PADOutcome* boolean
    example: true
    Whether a presentation attack was determined to be detected (True) or not detected (False).
    PADScore* number($double)
    example: 0.8
    A score corresponding to the level of confidence that a presentation attack was detected ranging between 0 and 1.
    PADProperties
      [
        example: List [ OrderedMap { "Property": "EyesMoving", "Value": true }, OrderedMap {
          "Property": "MouthMoving", "Value": true }, OrderedMap { "Property": "PupilsResponsive",
            "Value": true }, OrderedMap { "Property": "NonconformantIlluminationDetected", "Value":
              true }, OrderedMap { "Property": "MoirePatternDetected", "Value": true }, OrderedMap {
                "Property": "ObsscurationDetected", "Value": true } ]
        Key value pairs describing presentation attack properties and their relationship to the
        presentation attack outcome/score. There are no strictly defined properties. The inclusion
        of descriptive properties is encouraged to provide more context. (optional)
      PADProperty > {...}
    ]
  }
}
```

# Passive PAD Subsystem Requirements

# Passive PAD Subsystem Requirements (1)

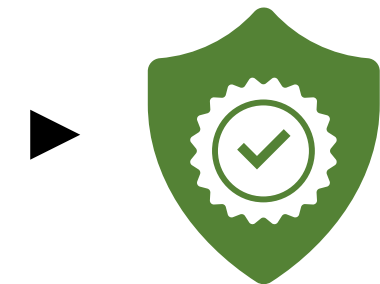
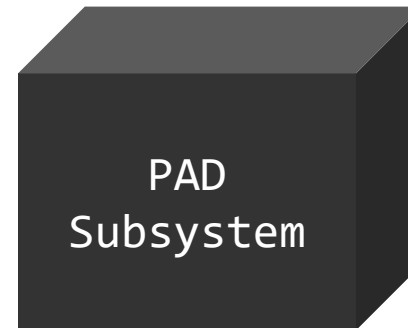
- Shall be packaged in a single Docker image (limited size)
- Shall operate without access to the internet / cloud
- Shall operate on previously acquired biometric samples
- Shall implement the RIVTD Passive PAD System API



# Passive PAD Subsystem Requirements (2)

- MdTF PAD API shall be implemented via a **HTTP server**
- Shall be deployed inside a single **docker** container
- Shall be delivered via a **.tgz** file
- Docker containers may be required to run on government systems and may be assessed for **security**

```
docker save ${COMPANY_NAME}-rivtd-track3-  
system:latest |  
gzip > ${COMPANY_NAME}-rivtd-system.tgz
```




We will work with technology providers to address security requirements

# RIVTD Track 3 – Passive PAD API


## The Maryland Test Facility Passive Presentation Attack Detection System Interface

2.0.0 OAS 3.0

### Data Analysis

**POST** /v1/analyze-data-for-pad Analyze biometric capture data for a presentation attack. 

### Algorithm Information

**GET** /v1/info Returns basic information for the algorithm. 

- MdTF systems will send:
  - Biometric Sample
- Passive PAD subsystems reply with:
  - PAD Outcome (true or false)
  - PAD Score (0-1)
  - PAD Properties (key value pairs)



The biometric sample can be a still image or a short video clip (<10 seconds).

# PAD Outcome and Properties

- The system shall return PAD Analysis results for each Biometric Sample
- **PADOutcome** must specify whether the biometric sample is bone-fide (False) or a presentation attack (True)
- **PADScore** indicates level of confidence on whether the biometric sample is a PA:
  - 1 means 100% certain it's a PA
  - 0 means 0% certain it's a PA (i.e., its bona-fide)
- **PADProperties** are key value pairs indicating any properties used by the PAD subsystem to determine PAD outcome and the values of those properties

```
PADAnalysis {
  description: Data transfer object for presentation attack information.
  PADOutcome* boolean
  example: true
  Whether a presentation attack was determined to be detected (True) or not detected (False).
  PADScore* number($double)
  example: 0.8
  A score corresponding to the level of confidence that a presentation attack was detected ranging between 0 and 1.
  PADProperties
    [
  example: List [ OrderedMap { "Property": "EyesMoving", "Value": true }, OrderedMap {
"Property": "MouthMoving", "Value": true }, OrderedMap { "Property": "PupilsResponsive",
"Value": true }, OrderedMap { "Property": "NonconformantIlluminationDetected", "Value":
true }, OrderedMap { "Property": "MoirePatternDetected", "Value": true }, OrderedMap {
"Property": "ObscurationDetected", "Value": true } ]
  Key value pairs describing presentation attack properties and their relationship to the
presentation attack outcome/score. There are no strictly defined properties. The inclusion
of descriptive properties is encouraged to provide more context. (optional)
  PADProperty > {...}
}
```

# PAD

# Subsystem Metrics



# System Error Rate

- Active and Passive PAD subsystems
- System Error Rate (SER):
  - For Active PAD - Proportion of presentations for which no PAD data capture is sent
  - For Passive PAD - Proportion of biometric samples for which no PAD analysis result is returned
- Each transaction must result in a response from PAD subsystem including all required API fields



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



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

# PAD Efficiency and Satisfaction Metrics

- Active PAD subsystems only
- Average Transaction Time
  - Amount of time needed to complete a transaction with the PAD subsystem
- Positive Satisfaction Rate
  - Percent of volunteers who give positive satisfaction ratings after using the PAD subsystem

# PAD Effectiveness and Equitability

- Active and Passive PAD Subsystems
- Bona Fide Presentation Classification Error Rate (BPCER)
  - Proportion of bona fide presentations that results in presentation attack classification
- Attack Presentation Classification Error Rate (APCER)
  - Proportion of attack presentations that results in bona fide classification
- Equitability:
  - Depending on overall system performance, metrics may be calculated separately for different demographic groups: Age, Gender, Race, and Skin Tone

# Benefits of Participation

- Attend VIP Day, a networking opportunity with government and industry representatives
- Inform government regarding your system's performance in an operationally relevant demonstration
- Form an ongoing Cooperative Research and Development Agreement (CRADA) with DHS S&T
  - Measure performance of system with diverse volunteers
  - Measure performance with specific demographic groups
  - Active PAD subsystems: View videos of volunteers using system to identify use errors and improve your system

# Application Package Requirements

- Provide an application package (limit five pages), in the form of a white paper addressing each of the following:
  1. Description of the company
  2. Presentation attack detection system technical capabilities
    1. Passive PAD system, or
    2. Active PAD system
  3. Mobile Device and OS support
  4. System inputs and data processing steps
  5. System outputs
  6. Description of the complexity and maturity of the remote identity validation system, including any active deployments
  7. Any measurements of the performance characteristics of the system and how they were tested
- Optional demonstration video of system functionality
- Submit application package to [RIVTD@mdtf.org](mailto:RIVTD@mdtf.org) by **11:59pm (EST) February 29, 2024**



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



# Questions & Answers

- Contact information
  - [peoplescreening@hq.dhs.gov](mailto:peoplescreening@hq.dhs.gov)
- DHS S&T is exploring industry interest in video injection attack detection testing
  - Please indicate interest by sending a description of your digital injection attack detection system and / or a demonstration video to [peoplescreening@hq.dhs.gov](mailto:peoplescreening@hq.dhs.gov)
- Visit our websites for additional information
  - To see additional work DHS S&T supports, visit [www.dhs.gov/science-and-technology](http://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/rivtd>