

U.S. Department of Homeland Security

SCIENCE AND TECHNOLOGY DIRECTORATE

Remote Identity Validation Rally
Identity Document Validation



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

July 1, 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.





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

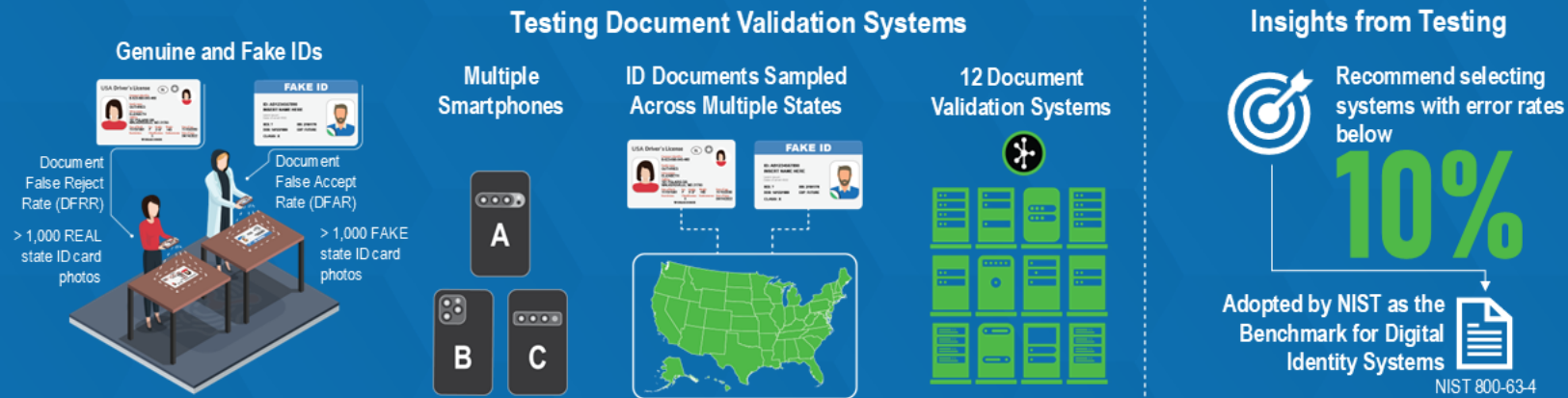
- Remote Identity Validation (RIV) technology is a tool to authenticate documents and verify the identity of users remotely
- These systems are complex, with multiple subsystems, and are increasing in popularity and adoption
- Industry performance benchmarks are not well defined, making it is difficult 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)



Remote Identity Validation Technology Demonstration (RIVTD)

REMOTE IDENTITY VALIDATION TECHNOLOGY DEMONSTRATION - DOCUMENT VALIDATION



What Impacts Document Validation System Performance?



!

System deployers should ensure compatibility with their users' documents and devices.

Prepared by the IDSL



Remote Identity Validation Rally (RIVR)

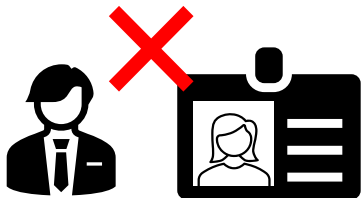
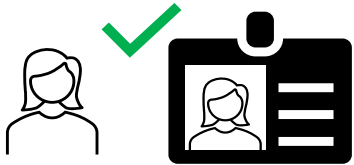
- **Building on RIVTD Insights:** RIVTD identified key areas where RIV vendors should focus improvements, shaping the next phase of evaluation.
- **Establishing Achievable Benchmarks:** RIVR sets industry-informed performance benchmarks based on RIVTD results, providing clear targets for improvement.
- **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

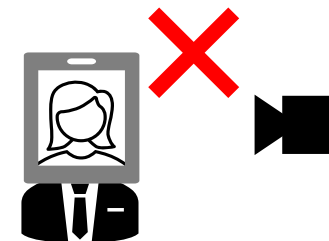
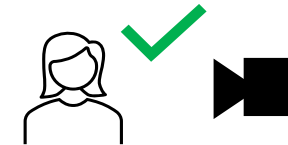
- Information Check
- Tamper Check
- Security Check



Today!

Presentation Attack Detection (PAD)

- Reject screens and printouts
- Reject masks and other PAs



Fall 2025 (Planned)

Identity Document Validation Track

Identity Document (ID) Validation

- RIVR will evaluate the ability of document validation subsystems to establish the authenticity of US state and territory-issued ID cards based on images (front and back) gathered using smartphones
 - ID cards will include driver's licenses and non-license state ID cards issued by US states or territories
 - Future evaluations may include images of passports
- Evidence Validation Processes:
 - Test identity evidence for authenticity against document type libraries for **information completeness**, **format**, and **correctness**;
 - Test identity evidence for authenticity through **tamper and counterfeit detection** (this includes document liveness); and
 - Test identity evidence for authenticity by **validating and confirming presence of security features** for the type of evidence presented.

DHS S&T's RIVTD helped inform NIST SP 800-63A evidence validation standards

- Defined performance measures
- Informed acceptable performance levels

[NIST SP 800-63A-4 second public draft, Digital Identity Guidelines: Identity Proofing and Enrollment](#)

3.1.12. Requirements for Evidence Validation Processes (Authenticity Checks)

Evidence validation can be conducted by remote optical capture and inspection (often called document authentication or doc auth) or conducted by visual inspection of a trained proofing agent or trusted referee. CSPs may employ either or both processes for evaluating the authenticity of identity evidence.

The following requirements apply to CSPs that employ optical capture and inspection for the purposes of determining document authenticity:

1. Automated evidence validation technology **SHALL** meet the following performance measures:

- Document false acceptance rate (DFAR) of .10 or less. ⁶
- Document false rejection rate (DFRR) of .10 or less. ⁷

Identity Document – Image Properties

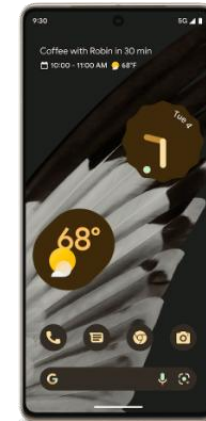
- Genuine and fraudulent document images (front and back) from different U.S. States and territories
- Images captured with a selection of modern smartphones (i.e., optical captures)
- JPEG or PNG encoding
- Reasonable efforts to ensure quality
- Optical perspective distortions may be present
- Images provided as base64 encoded strings



Note: Document images may be rotated -180 to 180 degrees.

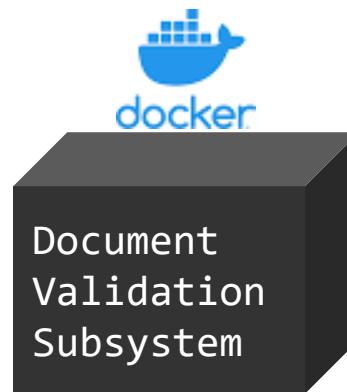


Apple iPhone 14



Google Pixel 7

Identity Document Validation API



- Validity Outcome (**required**):
 - boolean (true, false)
- Validity Score:
 - numeric (0.0 – 1.0)
- Validity Properties:
 - key-value pairs



Technical details are provided at
<http://github.mdtf.org>

Images: What do the new Maryland driver's licenses look like? (wbaltv.com)

Identity Document Validation API, Overview

- The API for this evaluation is available at <http://github.mdtf.org>
- The API for this evaluation has two endpoints
- Technically very similar to RIVTD Identity Document Validation API



API details may change – Refer to <http://github.mdtf.org> for current API information.

The Maryland Test Facility Document Validation Interface 0.0.1 OAS 3.0

This documents the API requirements for MdTF testing of document validation algorithms. Document validation testing at the MdTF is supported by the Department of Homeland Security Science and Technology Directorate (DHS S&T). For more information please visit <https://mdtf.org> and <https://www.dhs.gov/science-and-technology/BI-TC>.

[The MdTF - Website](#)

[Send email to The MdTF](#)

[IDSL API License](#)

Algorithm Information Return information about the document validation algorithm ^

GET **/v1/info** Return information about the document validation algorithm. v

Validate Return validation decision based on images of an identity document ^

POST **/v1/validate** Validate an identity document based on images. v

Identity Document Validation API, Validate ID

- `/v1/validate` (POST)
 - Accepts: Two Individual base64 encoded PNG or JPG image bytes
 - Returns: ValidationResponse for each pair of document images (front and back)
 - Note:
 - ValidityOutcome (required): true = valid ID.
 - Higher ValidityScores indicate greater document validity confidence.
 - Expected request duration: <30 sec.
 - Do not return PII in ValidityProperties.
 - Image orientation is **not guaranteed**. Subsystem must distinguish and process accordingly.



API details may change – Refer to <http://github.mdtf.org> for current API information.

```
{
  "DocumentFront": "iVBORw0KGgoAAAANSUhEUgAAAAESUVORK5CYII=",
  "DocumentBack": "iVBORw0KGgoAAAANSUhEUgAAAAESUVORK5CYII="
}
```



POST

`/v1/validate`

Validate an identity document based on images.



```
{
  "ValidityOutcome": true,
  "ValidityScore": 0.8,
  "ValidityProperties":
  [
    { "Property": "InformationFormatCorrect", "Value": true },
    { "Property": "InformationCorrect", "Value": true },
    { "Property": "InformationComplete", "Value": true },
    { "Property": "CheckSumsCorrect", "Value": true },
    { "Property": "MRZCorrect", "Value": true },
    { "Property": "PhotoTampered", "Value": true },
    { "Property": "LivenessCheck", "Value": "Passed" },
    { "Property": "InformationCompleteness", "Value": 0.9 },
    { "Property": "SecurityFeaturesTampered", "Value": "None" },
    { "Property": "DataFieldsTampered", "Value": "Age changed" }
  ]
}
```

Identity Document Validation API, Algorithm Info

- `/v1/info` (GET)
 - Algorithm name and version will be used in validating your system
 - Please version appropriately
- Event is RIVR_IDV



API details may change – Refer to <http://github.mdtf.org> for current API information.

GET `/v1/info` Return information about the document validation algorithm.



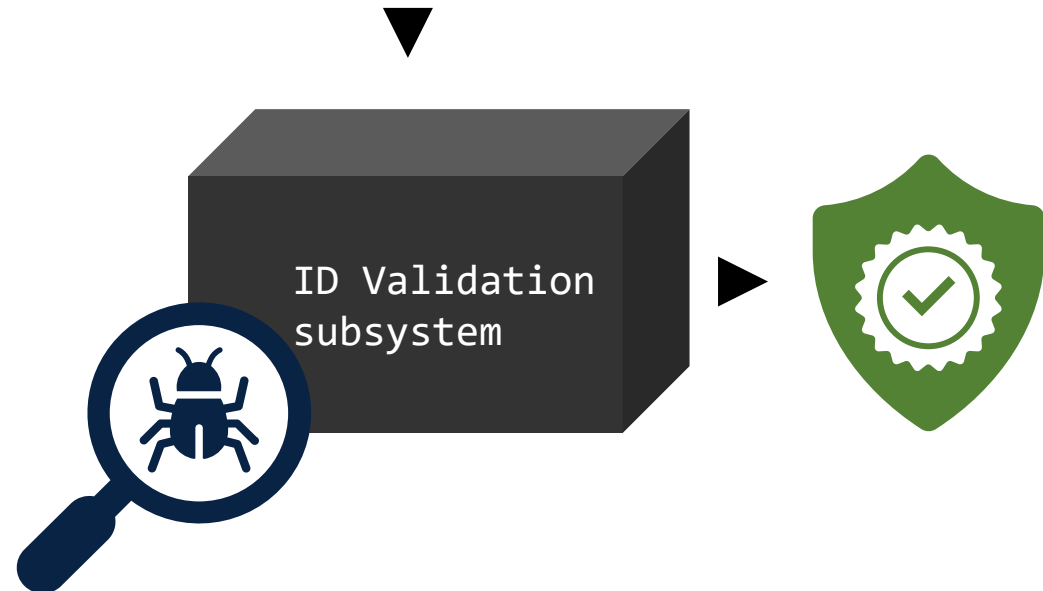
```
{
  "AlgorithmName": "Docvalidate",
  "AlgorithmVersion": "1.0.0",
  "CompanyName": "IDSL",
  "Event": "RIVR_IDV",
  "RecommendedCPUs": 4,
  "RecommendedMem": 256,
  "TechnicalContactEmail": "info@mdtf.org"
}
```

Identity Document Validation Subsystem

- Identity Document Validation API will be implemented via an **HTTP server**
- Deployed inside a **docker** container
- Delivered via a **.tgz** uploaded to the **MdTF MyConsole** (*new* limit 5GB)
- Provide **four test images** (two documents - front and back) to produce True and False ValidityOutcome
- Docker containers will be automatically assessed for API compliance and security
- Issues will be automatically flagged and sent to console users
- **All systems will require CVE scan results with no CRITICAL or HIGH vulnerabilities**



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

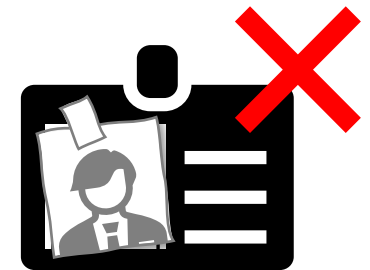


Identity Document Validation Subsystem

- Additional requirements:
 - Subsystems shall consist of a **single** docker container, started via a docker run command
 - Subsystems shall be **Linux** based docker containers
 - HTTP servers shall be hosted on **port 8080**
 - Subsystems shall be less than **5 GB** in size
 - Subsystems shall require **no outside functionality** and will be run on internal machines without access to the internet
 - 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 Identity Document Validation submission deadline

ID Validation Metrics

- **System Error Rate (SER)** – proportion of document images for which the system fails to return an appropriate response
 - Threshold: 0.10, Goal: 0.01
- **Document False Reject Rate (DFRR)** – proportion of genuine documents which the system determined to be invalid
 - Threshold: 0.10, Goal: 0.01
 - Failure is suspicious policy: system errors treated as genuine document false rejections
- **Document False Accept Rate (DFAR)** - proportion of fraudulent documents which the system determines to be valid
 - Threshold: 0.10, Goal: 0.01
 - Failure is suspicious policy: system errors treated as fraudulent document detections
- **Disaggregated by factors of interest:**
 - State of issue
 - Smartphone type



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

- Provide an application package (limit 5 pages), in the form of a white paper addressing each of the following:
 1. Description of the company
 2. Description of identity document validation 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



Future evaluations may include validation of passports. The application will ask if the document validation system submitted for RIVR is capable of validating passports

- Submit application package to RIVR@mdtf.org by **11:59pm (ET) July 18, 2025**



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

What's next?

- Application package is due **July 18, 2025**
- Notification of participation is **July 25, 2025**
- MdTF MyConsole for Docker submission of IDV systems opens **July 29, 2025**
- Initial Docker submission is due **August 15, 2025**
- Docker submission deadline is **August 22, 2025**

- Docker submission requires executed CRADA with DHS S&T
 - CRADA execution requires signature of authorized company representative

- Stay tuned for:
 - RIVR Presentation Attack Detection Track Announcement

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>