

DG – DeepfakesIDV Discussion Group

**Proposed Work Product**

Maxine Most, October 22, 2024

## Deepfake Detection, Protection and Countermeasures for Remote Identity Verification (PowerPoint Document)

### Executive Summary

### Introduction

## **Context**

* Introduce concepts of Remote IDV and Deepfakes
* Motivation for this Kantara Workgroup
* Define Key terms– link to Appendix: Glossary
* Introduce Deepfakes
  + Benefits and Threats (spectrum chart) with descriptions
  + Current state of the market
    - Critical Trends
    - Key Challenges and Dangers
    - Primary deepfake technologies
    - Role of GenAI
    - Regulatory Environment – link to Appendix: Regulations
    - Standards - link to Appendix: Relevant Standards
* Audience – Identify key constituencies:
* Enterprise: IT, Security, Cybersecurity
* Vendors: Biometric, IAM, CIAM, Fraud, Cyber3eecurity,
* Policy Makers: Government and NGO’s in Privacy, Cybersecurity,
* Standards/testing/certifications bodies

## **Scope**

* OBJECTIVE: Identify key deepfake threats and vulnerabilities and present prevention , detection, and countermeasure capabilities.
* USE: Educate and provide best practice recommendations to address the threats posed by deepfakes.
* FOCUS: Types of deepfakes in and out of scope
* CONTENT
  + RIDV Process
  + Deepfake Attack Vectors
  + Deepfake Prevention, Detection, and Countermeasures

### Content

## **RIDV Process**

RIDV Process Diagram

* Define and explain of each step
* Relevant technologies and solutions (Generic)

**Deepfake Attack Vectors**

RIDV Process Diagram with Attack Vectors Overlay

* Define and explain Attack Vectors at each step

[Current threats and attack vectors](https://kantara.atlassian.net/wiki/spaces/DGDF/pages/279969793/B.1+Current+threats+and+attack+vectors)

# 

# **Prevention, Detection and Countermeasures**

RIDV Process Diagram with Attack Vectors Overlay + Preventions, Detection, Countermeasures Overlay

* Define and explain Prevention, Detection, and Countermeasures to applied at each step
* Detail relevant/related processes, technologies, and solutions (Generic)

[Prevention and Countermeasures](https://kantara.atlassian.net/wiki/x/IQCjE)

### **TABLE: RIDV Process, Prevention, Detection and Countermeasures**

Create Table that captures the information from the Conant sections above

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Step Name | Process | Key Technologies | Attack Vectors | Prevention Process/Tech | Detection Process/Tech | Countermeasures Process/Tech | Relevant Regulations | Relevant Standards |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

### Key Findings & Recommendations

* Overall
* For each type of audience
* Enterprises
* Vendors
* Policy Makers
* Standards/testing/certifications bodies

### Appendices

* Glossary
* Regulations
* Technical References
* Standards