Use Case Name	Remote Identity Proofing of an Applicant using Document Verification (in accordance with NIST 800-63-3, IAL2)
Scope	Remote resolution, validation and verification of PII, financial information and supporting documents
Context	Remote resolution, validation and verification of PII, financial information and supporting documents to establish the identity of a constituent, in order for that constituent to become a subscriber able to remotely interact and transact with a government agency Context is United States, Public Sector specific Flow based on NIST SP 800-63-3, IAL2
Primary Actor	Applicant, who through this process can become a Subscriber
Stakeholders & Interests	Applicant: seeking to remotely establish their identity and to become a subscriber able to remotely interact and transact with a government agency Government Agency: seeking to remotely establish the identity of a unique applicant within a general population, and to subsequently convert this Applicant to a Subscriber Identity Proofing Service Provider: seeking to provide the remote identity proofing service to the Government Agency
Minimal Guarantees	-
Success Guarantees	-
Preconditions	Applicant is willing and able to participate in remote identity proofing (versus a preference for in-person) Applicant is willing and able to provide correct PII and Financial Information through a remote system (web page of the Government Agency) to support the ‘Fair Evidence’ requirements of the NIST 800-63-3, IAL2 flow Applicant has a government issued Photo ID document Applicant has a smartphone with a working camera, and is willing and able to use this smartphone for the purpose of remote document verification to support the ‘Strong Evidence’ requirements of the NIST 800-63-3, IAL2 flow
Triggers	Applicant accesses the website of the Government Agency it seeks to interact and transact with (eg tax agency, SSA, DMV), with the goal of becoming a subscriber for the particular service of that government agency

Main Success Scenario	Applicant accesses the website of the Government Agency it seeks to interact and transact with, with the goal of becoming a subscriber for the particular service of that government agency Through the website of the Government Agency, Applicant provides PII and Financial Account information to support “Fair Evidence” requirement The Identity Proofing Service Provider confirms the authenticity, validity, and accuracy of the provided identity and financial information, and determines whether it relates to the real-life subject out of the general population The Identity Proofing Service Provider sends a SMS text to the Applicant, triggering the “Strong Evidence” part of the flow. The Applicant opens a link within that SMS text and follows instructions to capture and upload their government issued ID images and ‘selfie’ The Identity Proofing Service Provider confirms the validity of the ID document, verifies a match between the ‘selfie’ and document image, assesses the liveliness of the ‘selfie’ and extracts document PII info The PII that is extracted from the ID is matched against the PII of the Applicant, which was already provided in the “Fair Evidence” part of the flow Applicant becomes Subscriber **Alternative Paths** Applicant not able to meet the “Fair Evidence” requirements due to incorrect PII and/or financial information -> Identity Proofing Service Provider delivers a ‘refer’ outcome back to the Government Agency Applicant not able to meet the “Strong Evidence” requirements -> Identity Proofing Service Provider delivers a ‘refer’ outcome back to the Government Agency All other failures in the flow (no match between the ‘selfie’ and the document image, ‘selfie’ fails the liveliness test, etc) -> Identity Proofing Service Provider delivers a ‘refer’ outcome back to the Government Agency