|  |  |
| --- | --- |
| **Heading** | **Description** |
| Use Case Class / Scope | **Identity Verification** |
| Use Case Name | **Identity Verification Scoring based on Factors of Authentication** |
| Context / Scope | The classic authentication factors – something they know, something they have, something they are (biometrics) – have been useful establishing standard levels of assurance for login events. This use case uses the same factors as “identity evidence classes” to provide an robust approach to measuring the level of confidence in identity verification.  As the list of evidence classes expands (e.g., someplace they are, some time they interacting, some way they behave) the scoring method can expand as well. |
| Stakeholders & Interests | * Individual – completing a transaction or gaining access to a system * Identity Verification Service (IVS) – to provide a service that optimizes security, customer experience, and cost based on the risk of the Relying Party * Relying Party (RP) – An organization that is consuming IVS services in order to transact with the Individual |
| Triggers | * Relying Partly needs a certain level of confidence in the identity of the Individual, which is conveyed the IVS |
| Success Guarantees | * An agreed-up, risk-based approach has been used to score the confidence that the user is who they claim to be |
| Primary Actor | IVS |
| Preconditions | A standard rubric / scoring matrix has been developed, evaluated, and agreed upon between the RP and the IVS |
| Main Success Scenario | 1. The RP directs the Individual to the IVS while indicating its risk level 2. The IVS examines the options available for achieving a level of confidence >= the corresponding RP risk level 3. The IVS asks the user to choose from the various evidence types (i.e., KNOW, HAVE, ARE, etc.) to prepare the user and predetermine the workflow 4. The Individual selects a permutation of evidence that meets the risk/confidence requirements 5. The IVS collects the evidence from the Individual, evaluates it, and makes a decision |
| Identity Evidence Classes and Risk | Different levels of confidence can require different numbers of *identity evidence classes* with different security scores from the following:   * KNOW – information that can be reasonably expected to be known only by the Individual Security Scoring Info Examples:   + How widely exchanged is the information (every time they apply for credit)?   + Is the information managed by a regulated industry (government, financial, utility)?   + Does the Individual know a phone number corresponding to them according to the carrier?   + Does the individual know an email corresponding to the user in consumer records?   + Can the individual identify recent transactions? * HAVE – An object that is reasonably expected to be in the possession of the Individual Security Scoring Info Examples:   + Does the individual have a cryptographic key that unlocks access to ledger items associated with the individual?   + Out-of-band confirmation of possession of a phone that has been validated in combination with a KNOW factor   + Out-of-band Email confirmation of access to an email account (possession of a digital object) that has been validated in combination with a KNOW factor   + ID Document with/without security features from a State (high), University (low), etc. * ARE – A physiological characteristic of the Individual that can reasonably expected to be demonstrated by only that Individual   + Fingerprint matched against records   + Live portrait comparison with either something they HAVE or in authoritative records   + Behavioral biometrics, such as gait, click speed, cross-site transaction velocity, etc. |