|  |  |
| --- | --- |
| **Heading** | **Description** |
| Scope / Use Case Class | **Identity Proofing (Online)** |
| Use Case Name | **Device ID and Reputation**  |
| Context | A Device ID and Reputation service provider (DIR-SP) provides services to a wide range of RPs. The DIR-SP uses information obtained from the Individual’s network interaction to attempt to uniquely identify the device, such as the following:* IP
* MAC
* browser language settings
* screen resolution
* domain cookies
* OS version
* browser version
* time zone

The DIR-SP encourages its RPs to supply obfuscated markers related to the Individual, such as SHA 256 hashes of: name, address, email. RPs can leverage the DIR-SP insights to make risk-based identity proofing determinations. This scenario has some parallels to Self-Sovereign Identity:* The Individual must actively consent to involvement of the DIR-SP
* DIR-SP record represents a (non-distributed) ledger or Individual relationships with other RPs
* The DIR-SP is leveraging interactions between the Individual and other RPs to make determinations
 |
| Stakeholders & Interests | * Individual – completing a transaction or gaining access to a system
* Relying Party (RP) – prevent identity fraud and transact with the Individual
* DIR-SP – provide quality service for a fee
 |
| Triggers | * Individual needs access to an Online service and the RP requires confidence in the identity of the Individual
 |
| Success Guarantees | * A risk score indicating the confidence in the device and the makers (e.g., hashed name) based on historical, ongoing interaction across a network of RPs as well as fraud analytics.
 |
| Minimum Guarantees | * There is a device profile matching this profile that has a history of interactions with other RPs
* The claimed markers (e.g., hashed name) have or have not been previously used with the device profile
 |
| Primary Actor | Individual / DIR-SP |
| Preconditions | The individual has a browser and consents to involvement of the DIR-SP |
| Main Success Scenario | 1. The Individual connects to the RP, is presented with privacy statements and a clear description of the DIR-SP
2. The Individual consents to involvement of the DIR-SP
3. The Individual’s device connects to the DIR-SP (typically through browser Javascript)
4. The DIR-SP collects network and device information from the connection
5. The RP collects identifying information from the Individual such as name, email
6. The RP hashes the identity information and provides the markers to the DIR-SP
7. The DIR-SP examines the device information and markers, comparing it to matching historical interactions (proprietary analytics)
8. The DIR-SP provides a risk score and indicates whether each marker matched
9. The RP decides whether to enroll the Individual or put them through additional proofing (e.g., photo ID scan, in-person)
 |
| Resolution (SP 800-63) | Name, address, and other identifying information (e.g., email) is collected and used to uniquely identify the Individual. |
| Evidence (SP 800-63A) | The Individual’s device has a unique profile that matches interactions (both positive and negative) across multiple RPs |
| Validation (SP 800-63A) | The DIR-SP validates the evidence (Device Profile) and identity information (markers) using its ledger, which indicates interaction over time with multiple RPs. |
| Verification(SP 800-63A) | The DIR-SP connection between the device and the Individual’s device is used to directly present the device characteristics to the DIR-SP. |
| Address Confirmation(SP 800-63A) | A notice can be sent to the email or address if upon marker match. |