|  |  |
| --- | --- |
| *Trust Elevation Method:* | End Point Identity: End Point Identity is an umbrella term that describes any of a number of sub-methods used to identify the device by which the user is accessing the service provider. Transactions are considered less risky when a known device is used. If an unknown device or a compromised device is used, then additional methods may be required to mitigate risk. Gathering information about an end point device is sometimes called device fingerprinting. End point identity attributes may include landline number, mobile phone number and/or SIM and/or OS, IP address, router, provider, cookie, OS, browser, chip. The end point identity chain of trust can also include software tokens/digital certificates that provide information about other layers of the data stack. |
| Questions: |  |
| Which party is performing the method? | Relying Party |
| How does the method improve trust? | This method looks past the inputs of the human customer to the device that is being used on his/her end. The method determines the kind of device being used and one or more components (hardware and software) to determine if the application service provider has ever seen that unique device in the past associated with successful login by that customer and the device is classified as banded platforms approved for the service requested. If a previous correlation is found, the method raises the confidence that the customer is who his/her credential asserts he/she is combined with the device identity as the second factor. If there is no previous correlation with that customer and device, and there is correlation with many failed login attempts, then the confidence is significantly reduced. If the device is not recognized, then confidence is reduced and additional methods may be required to raise confidence back to acceptable levels (including the device provisioning for the targe. |
| How does the method address the threat of eavesdropping? | N/A |
| How does the method address the threat of online guessing? | This method does not contain information that can be guessed. |
| How does the method address the threat of replay attack? | Last login is tracked in cloud and the device identity is augmented with the credential associated with the last login. A session keys and the antireplay protocol are employed. There are sequential counters stored in the secured storage and the cloud server that guarantee that packets are received and processed in order. Whenever out of order the two sides know that something has gone wrong. May also help with replay attacks if the device identity includes the time on the device clock. |
| How does the method address the threat of man in the middle? | N/A |
| How does the method address the threat of spoofing and masquerading? | Cryptographic authentication (shared secret + session key) along with other multi factor authentication methods such as OTP and biometric will be employed for higher level of assurance reducing the risk of spoofing. |
| Are there implementation requirements for improving trust? If so, what are they and why are they necessary? | This method assumes that there is a persistent one-to-one relationship between the login data and the device used at the customer end. Moreover, there is the possibility of aliased device ID for each user addressing shared devices challenges. Besides per user device ID, a per service/app device identity can be provisioned to segregate the device identity provisioned for a financial institution as an example from a social network or content provider identity. Prior registration of that relationship could improve trust, since that information could serve also as a shared secret. Agreement by the user not to share the device could improve trust, perhaps, by providing some confidence that no other user's login credentials were affiliated with that device. Because users do sometimes change devices and devices are not always exclusive, or services are terminated or replaced this method can result in too many false negatives, unless as we have noted above, there is a unique binding of the user to a distinct device identity and service is applied. In many cases, such as use of a family computer by many members of a household or as a public kiosk, this would be impractical unless we have ample storage to provision device, user and service binding. |
| Are there privacy and/or confidentiality issues engaged when using the method, such as user consent for attribute release/exchange? Are there reasonable solutions for potential privacy impacts? | Since the method does not engage the customer in the exchange of information, he or she may not be aware that the device attributes are even being sent. Mobile devices particularly can expose PII. Explicit consent for release of device data should be a prerequisite of application device query. If the device identity of each service is aliased and is unique, privacy risk is significantly reduced |
| What are the usability issues when using the method? Are there reasonable solutions for potential usability impacts? | This method is particularly well-suited to customer usability as it requires little or no user interaction for the typical session. This method is typically used in conjunction with an additional method such as relationship-based KBA. |

|  |  |  |
| --- | --- | --- |
| Initial NIST LOA | Resulting NIST LOA | Comments |
| 0 |  |  |
| 1 |  |  |
| 2 | 3 | When performed with a previously registered phone that is subscribed to by the user, can constitute a second factor hard token. |
| 3 | 3 | Can confirm confidence in LOA |
| 4 | 4 | Can confirm confidence in LOA |

Just for grins, I’ve added the M 04-04 risk/assurance table. It continues to make perfect sense.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Table 1 – Maximum Potential Impacts for Each Assurance Level  **Assurance Level Impact Profiles** | | | | |
| **Potential Impact Categories for Authentication Errors** | **1** | **2** | **3** | **4** |
| Inconvenience, distress or damage to standing or reputation | Low | Mod | Mod | High |
| Financial loss or agency liability | Low | Mod | Mod | High |
| Harm to agency programs or public interests | N/A | Low | Mod | High |
| Unauthorized release of sensitive information | N/A | Low | Mod | High |
| Personal Safety | N/A | N/A | Low | Mod  High |
| Civil or criminal violations | N/A | Low | Mod | High |