

be directly compared to these profiles. The closest match to one of the level profiles will determine the assurance level. In determining the required assurance level, an agency should initially identify risks inherent in the transactional process without considering the particular technologies used to implement authentication for that transaction. For example if during a medical procedure, the misuse of a user's electronic identity/credentials might result in risk to the user's personal safety, then, following this guidance, the agency would assign a level 4 assurance to this transaction, even if potential financial loss or other consequences are minimal. In making this determination, business process owners should seek to use the minimum assurance level that meets their risk requirements.

Step 3: Determine implementation technology based on the e-authentication technical guidance. After the assurance level has been determined, the agency should refer to the e-authentication technical guidance for the process requirements corresponding to that level. After the technical solution is chosen, a final validation should be conducted to confirm that the required assurance level of the end-to-end user to agency process has been operationally achieved. Note that authorization determines whether or not the authenticated has rights to complete the transaction.

Note that some technology solutions may create or compound particular risks. Thus, after selecting a specific solution, the agency should validate that the performance of the authentication process itself actually meets the identity assurance requirements for the transaction as part of required security procedures (e.g., certification and accreditation).

2.3. Assurance Levels: Descriptions and Examples

This section describes the four assurance levels. The levels represent ranges of confidence in an electronic identity presented to an agency by means of a credential. The levels are numbered from 1 to 4, with 1 being minimal assurance and 4 being the highest level of identity assurance.

For each level, there is a description and examples. The description and examples will assist the agency in identifying the appropriate level of assurance required to authorize a transaction. The key part of each description is a risk profile. This is a description of certain consequential risks that may ensue to participants in a transaction when there is an authentication error.

Level 1—Minimal Assurance

Description

At level 1, little or no assurance is placed in the asserted electronic identity of the transacting party. In particular, an authentication error of a user's identity at level 1 might result in at most—

- Minimal inconvenience to any party; and
- No financial loss to any party; and
- Minimal distress being caused to any party; and
- Minimal damage to any party's standing or reputation; and
- No risk of harm to agency programs or other public interests; and

- No risk of civil or criminal violations; and
- No release of personal, U.S. government sensitive, or commercially sensitive data to unauthorized parties; and
- No risk to any party's personal safety.

Examples

Examples of transactions that might merit level 1 authentication include—

- A user presents a self registered user ID or password to the United States Department of Education web page, which allows customization of a Web site to create a "My.ED.gov" page. There are some possible risks associated with this situation; for example, a third party who gained unauthorized access to such a user ID and password might be able to draw inferences about the user's business interests or plans or the user's personal situation based on the types of information in which the user has an interest. Unless the website is subject to a high degree of customization, however, these risks are probably very minimal.
- A user participates in an online discussion on the whitehouse.gov website. Assuming that the forum is not one that addresses sensitive or private information, there are no obvious risks associated with this situation.

Level 2—Low Assurance

Description

Level 2 is appropriate for transactions in which it is sufficient that, on the balance of probabilities, there is confidence in the asserted electronic identity of the transacting party. In particular, an authentication error of a user's identity at level 2 might result in—

- Minor inconvenience to any party; or
- Minor financial loss to any party; or
- Minor damage to any party's standing or reputation; or
- Minor distress being caused to any party; or
- Minor risk of harm to agency programs or other public interests; or

A risk of civil or criminal violations of a nature that would not ordinarily be subject to agency enforcement efforts; or

- A minor release of personal, or commercially sensitive data to unauthorized parties; and
- No release of U.S. government sensitive data to unauthorized parties; and
- No risk to any party's personal safety.

Examples

Examples of transactions that might merit level 2 assurance include—

- A user engages in online learning on the Gov Online Learning Center at golearn.gov. There is a need for authentication such that the user is recognized by the training service and be connected to the appropriate place in the course or given relevant assignment grades, when training affects compensation or promotion. The only risk associated with this transaction is that a third party will gain access to grading information, causing harm to the privacy interests or reputation of the student. If the agency determines, in the context of the particular program, that any such harm will be minor, the transaction is level 2.

- A user accesses their Social Security retirement account information online.

Level 3—Substantial Assurance

Description

Level 3 is appropriate for transactions that are official in nature, and for which there is a need for high confidence in the asserted electronic identity of the transacting party. In particular, an authentication error of a user's identity at level 3 might result in—

- Significant inconvenience to any party; or
- Significant financial loss to any party; or
- Significant damage to any party's standing or reputation; or
- Significant distress being caused to any party; or
- Significant harm to agency programs or other public interests; or
- A risk of civil or criminal violations that may be subject to agency enforcement efforts; or
- A significant release of personal, U.S. government sensitive, or commercially sensitive data to unauthorized parties; and
- No risk to any party's personal safety.

Examples

Examples of transactions that might merit level 3 assurance include:

- A patent attorney company reports and updates data on-line with the Patent and Trademark Office that would be of great value as competitive intelligence.
- A major contractor or supplier maintains an account with a General Services Administration Contracting Officer for a large government procurement involving significant government expenditures.
- A First Responder accesses a disaster management reporting website to report an incident and to share incident operational information, and to coordinate incident response activities.

Level 4—High Assurance

Description

Level 4 is appropriate for transactions that are official in nature for which there is a need for very high confidence in the asserted electronic identity of the transacting party. In particular, an authentication error of a user's identity at level 4 might result in—

- Considerable inconvenience to any party; or
- Considerable financial loss to any party; or
- Considerable damage to any party's standing or reputation; or
- Considerable distress being caused to any party; or
- Considerable harm to agency programs or other public interests; or
- A risk of civil or criminal violations that are of special importance to the agency enforcement program; or
- A damaging release of extensive personal, U.S. government sensitive, or commercially sensitive data to third parties; or
- A risk to any party's personal safety.

Examples

Examples of transactions that may require level 4 assurance include—