ADUCID

Minimum Requirements for Seamless and Efficient eID Ecosystem.

In an eID ecosystem, eID infrastructure enables Users in accessing and utilizing all online services with a single eID token. Services that trust and support eID tokens may sign up new Users without lengthy verification processes that are costly for Service Providers and frustrating for Users. With a single eID token, Users may sign up, access and authorize service use for all online services in the ecosystem. The seamless and efficient eID ecosystem must operate on a technically robust eID infrastructure that satisfies a series of minimum requirements, which all must be met for its successful deployment.

Security

Security of an eID ecosystem is determined by the technical ability of its eID infrastructure to protect target assets. An eID infrastructure must therefore support:

Strong Authentication:

- Cryptographically strong, dynamic and mutual authentication.
- Using minimum 2 non-chained authentication factors (possession, knowledge, or inherence).
- Security parameters adjustable by target service system administrator.

Authentication and Protection of Data Channel:

- Data channel authentication between user and service(s).
- Data channel protection for secure target asset access.

Usability

Usability of eID is defined by the ease of access and the ability of Users to complete identity verification tasks for all services in the eID ecosystem. The eID must respect User's cognitive ability and experience without assuming special skills or knowledge. An eID infrastructure must therefore support:

- **Usable Interface** for a variety of Users regardless of their age, financial and physical status. It must be effortless to become familiar, recall and achieve a variety of objectives in across many industry sectors.
- **System Architecture Design** that supports key functionality and simultaneously does not systematically limit needs of Users and services in a wide range of user scenarios.

Privacy Protection

Privacy protection of an eID is determined by the ability of the complete eID infrastructure to, directly and indirectly, protect personal and sensitive data of an individual. With dynamic protection employed to maximize data protection, it holds that all ciphers will be broken eventually. **Privacy by design is, therefore, a must.** An eID infrastructure must ensure protection of implicit data. The following privacy measures must be enforced to ensure privacy protection:

- No personal data used in authentication for any task.
- No personal data used before authenticating and ensuring the protection of data channel in identity authentication and identity federation.
- Embedded personal data protection.
- Scope of personal data used after authentication appropriate to target use. Only personal data that target system needs should be used.
- Protection of identifier anonymity in the ecosystem. Users should not be identifiable between two independent Service Providers in the ecosystem.

Economical Affordability

- **No Additional Hardware** – Users expect an eID that is accessible directly on devices they already own (smartphone, PC, Mac, etc.)
- **Free for Users** – Users expect to be able to authenticate without having to pay for the authentication method directly.
- **Affordable for Service Providers** – Technology purchase price must respect the authentication market. Integration must be simple and accessible through standard interfaces to minimize integration and operational costs.
- **Affordable for Identity Providers** – Low issuance, activation, and distribution costs enabled by automated generation of eID and using standard distribution channels.

Service Availability

- Minimization or complete elimination of a target service/application failure due to a failure of authentication devices (redundancy and backup of authentication devices).
- Built-in easy-to-use recovery support from emergency situations (malfunction, loss, or theft of authentication tools).

Long-Term Sustainability

- Ability to adapt to future technology development and future security threats.
- Possibility of changing cryptographic parameters live without outages or scheduled maintenance windows.
- Possibility to upgrade the infrastructure at runtime.