
Report on Discussion Results Concerning Streamlined Approaches to Identity Proofing for Online Services (Overview)

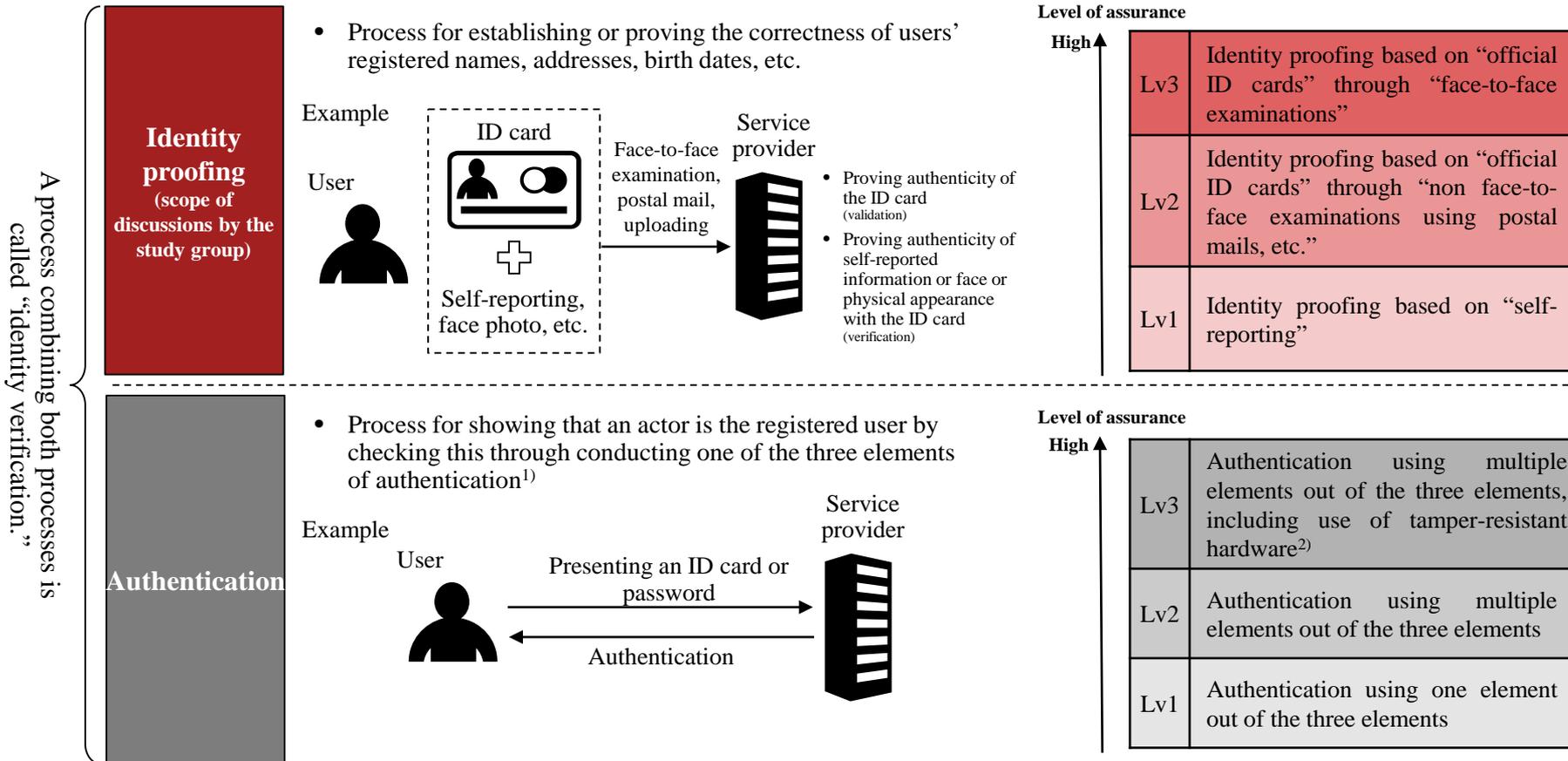


1. Difference between “Identity Proofing” and “Authentication”

The term “identity proofing” refers to a process for proving the physical existence of users, while the term “authentication” refers to a process for proving the acts by users. “Identity verification” is usually accomplished by combining these two processes.

Details of identity proofing and authentication

Reference: Category of levels³⁾



1) Elements subject to authentication are categorized into “biometrics” (faces, fingerprints, etc.), “possessions” (Social Security and Tax Number cards, etc.) and “knowledge” (passwords, etc.).

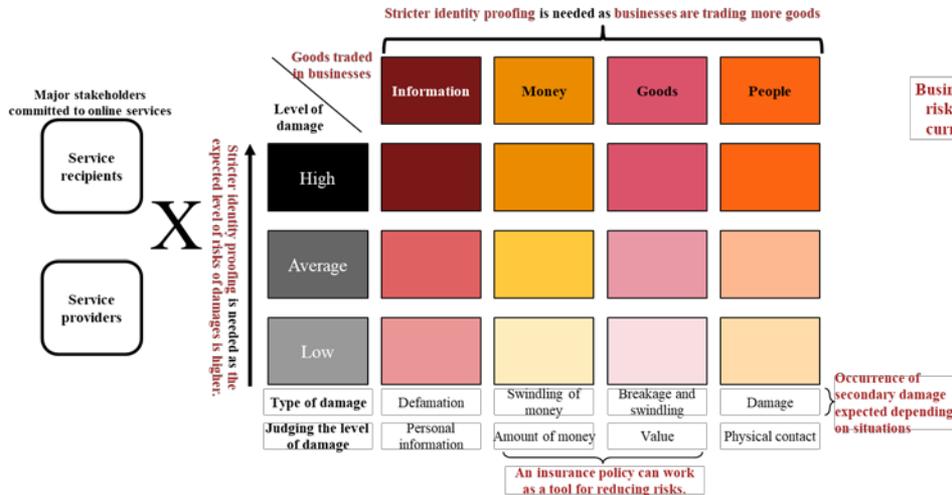
2) The term “tamper-resist hardware” refers to physical units from which it is difficult for unauthorized parties to be able to read inside information, e.g., data contained in Social Security and Tax Number cards.

3) These categories are in accordance with those stipulated in the “Guidelines on Approaches to Online Identity Assurance for Administrative Procedures” (decided by the CIO Liaison Council in February 2019)

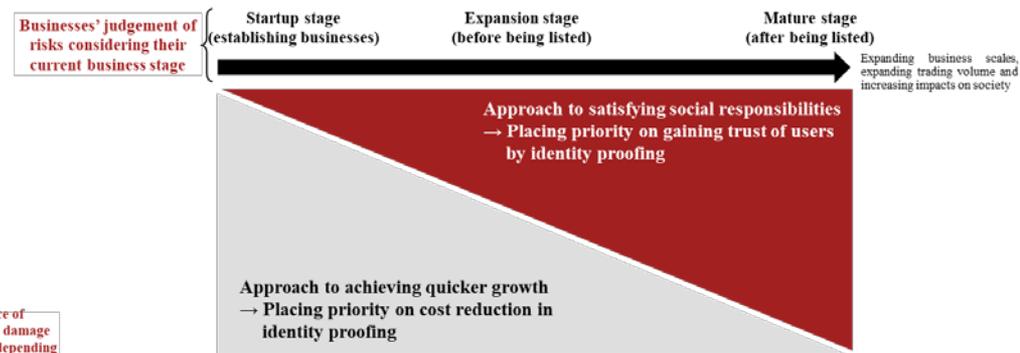
2. Indices to Judge Risks in Businesses

The study group held discussions on indices using which businesses, by themselves, are able to check and assess the need for identity proofing based on data on potential risks of damages that service recipients and providers may incur according to the goods to be traded. It also streamlined tendencies of prioritized value, which change in accordance with business stages.

Indices to assess risks in businesses involving identity proofing



Tendencies of risk judgement according to business stages



- Presenting assessment criteria for judging risks involving identity proofing that may occur soon or in the future before conducting such proofing is considered useful for the existing businesses, businesses in the startup stage and future business founders.
- In advancing such risk assessment, businesses should examine the level of damages, mainly taking into consideration [i] goods to be traded, details thereof and stakeholders and [ii] phases and scale of businesses, while secondarily bearing in mind [iii] presence of insurance policies or compensation, [iv] possibility of secondary damages, and other elements.
- From the startup stage to the expansion stage: As businesses have a limited number of users and many early adapters, they tend to prioritize approaches to achieving quicker growth and place higher incentives on reducing costs for identity proofing or on conducting no identity proofing.
- From the expansion stage to the mature stage: As businesses are likely to bear more social responsibilities, they tend to: prioritize approaches to securing trust in them to prevent any troubles with users involving their businesses so as to avoid loss of social trust caused by such troubles and severe damages to their businesses caused by such loss; and, as a result, place higher incentives on introducing identity proofing.

