

eIDAS Assurance Levels

EU Electronic Identification Trust Framework

Requirements	Use Cases
HIGH <ul style="list-style-type: none">* In-person or remote with NFC + liveness* Government-issued eID* Biometric verification* Photo match to authoritative source	<i>Banking, healthcare, legal documents, government services</i>
SUBSTANTIAL <ul style="list-style-type: none">* Remote identity proofing* Document + selfie verification* Database checks* Liveness detection	<i>Account opening, age verification, KYC</i>
LOW <ul style="list-style-type: none">* Self-asserted identity* Email/phone verification* Basic attribute validation* Social login acceptable	<i>Newsletter signup, basic access, non-sensitive services</i>

Higher assurance = More rigorous proofing = Greater trust in identity claim

Increasing Assurance