A SAFER WORLD

Security by Design

Passports and identity documents are critical to national security, personal identity protection, and the facilitation of global travel. Adopting Security by Design principles embeds protection across the entire material and production process building resistance to forgery, tampering, and substitution from the ground up by making the physical document itself inherently secure.

Why Security by Design Matters

Defends Against Evolving Threats

Counterfeiters and forgers continually adapt their methods, targeting both physical and digital elements of documents. Integrated security design ensures that multiple, interdependent features work together, making unauthorised replication or alteration significantly more difficult.

Protects National and Personal Security

Fraudulent documents enable a range of criminal activities, from identity theft and financial crime to terrorism and human trafficking. Robust security design protects citizens and upholds the integrity of national borders.

Supports International Standards and Interoperability

Security features must be compatible with global standards (e.g., ICAO Doc 9303), ensuring documents are interoperable, universally recognised, verifiable, and accepted at border controls worldwide.

Balances Usability and Security

Effective design integrates security features without compromising document durability, readability, or convenience for legitimate users and authorities.

AG2
A SAFER WORLD

Key Elements of Integrated Security Design

Security Element	Purpose & Benefit	Example Features
Substrate Security	Makes forgery and tampering visible and difficult	Watermarks, security threads, embedded fibres
Optical Features	Enables quick, intuitive verification by humans and machines	Holograms, optically variable inks, tactile embossing
Chemical Protection	Reveals attempts at alteration using solvents or erasure	Chemical sensitisers, anti-tamper coatings
Personalisation Security	Protects holder data and photo against modification	Laser engraving, multiple image portraits, digital seals
Electronic Security	Secures digital data and biometrics, prevents chip cloning or manipulation	Encrypted chips, digital signatures, BAC/EAC/PACE protocols
Multi-Level Security	Provides overt, covert, and forensic features for layered defence and varying inspection environments	Visible fibres, UV features, forensic taggants

Best Practices for Integrated Security Design

- **SECURITY BY DESIGN:** For physical identity documents such as passports and ID cards, adding the concept of Security by Design means embedding protection principles into the material and production process—not simply layering features. The aim is to build resistance to forgery, tampering, and substitution from the ground up by making the physical document itself inherently secure.
- **LAYER MULTIPLE FEATURES:** No single feature can prevent all types of fraud. A combination of physical, optical, chemical, and electronic measures provides robust protection.
- **EMBED SECURITY AT EVERY STAGE:** Security must be designed into the very fabric of the document—from unique substrate formulation and fibre embedding to secure lamination, printing, and personalisation—ensuring tamper visibility, material integrity, and traceability throughout the lifecycle.
- **RANDOMISATION AND UNIQUENESS:** Features such as randomly distributed security fibres and threads ensure no two documents are identical, making counterfeiting extremely challenging.
- **FACILITATE FAST, RELIABLE VERIFICATION:** Features should be easy for border and inspection staff to check quickly, even in suboptimal conditions, without specialised tools.
- **ENABLE FORENSIC INVESTIGATION:** Advanced covert and forensic features allow for in-depth analysis by experts in cases of suspected fraud.

Consequences of Weak Security Design

- **INCREASED FRAUD RISK:** Documents lacking integrated security are easier to counterfeit or alter, increasing the risk of illegal border crossings and identity theft.
- **REPUTATIONAL DAMAGE:** Compromised documents can harm the credibility of issuing authorities and nations.
- **OPERATIONAL INEFFICIENCIES:** Poorly secured documents require more time and resources for verification and increase the likelihood of errors or delays at checkpoints.

Conclusion

Security by Design is not optional—it is fundamental to the credibility, safety, and effectiveness of passports and identity documents. By embedding multiple, complementary security features throughout the production process, issuing authorities can deter fraud, protect individuals and borders, and ensure trust in identity systems worldwide.

Unit 5, Ballywaltrim Business Park, Bray, Co. Wicklow, Ireland. A98 EH97
info@ag2.ie +353 (1) 533 2888 www.ag2.ie

CSSI CERTIFIED SECURITY SUPPLIER INTERGRAF
DSA ENHANCING DOCUMENT AND IDENTITY SECURITY
BIOMETRICS INSTITUTE
ARTIVO ISO 9001 Certified