FOR IMMEDIATE RELEASE

April 8, 2026 — Washington, D.C., Brussels, Paris

Raising the Bar: New Framework Sets Higher Standard for Government Identity Document Security
Best Practice Guidelines and Minimum Security Standards for Identity Documents: Recommendations for Advanced Document Design and Integration of Security Features

At a time when the sophistication of counterfeit credentials poses an escalating threat to public safety and national security, the Document Security Alliance (DSA), INTERGRAF, and the Secure Identity Alliance (SIA) are pleased to announce the publication of our best-practice guidelines for Identity Documents. Intended for issuing authorities and policymakers, this unique and collaborative international endeavor between industry, forensic and secure document experts provides a practical roadmap to creating robust and secure identity documents.

Passports, national identity cards, driver's licenses, and other government-issued credentials are woven throughout the structure of modern civic and economic life; enabling citizens to cross borders, open bank accounts, board aircraft, access healthcare and receive numerous other essential government services. For government officials that bear responsibility for the integrity of the credentials they issue, the Best Practice Guidelines and Minimum Security Standards for Identity Documents is an actionable tutorial for going well beyond today's existing minimum standards to create a truly secure document.

"The holders of identity documents place considerable trust in the authorities that issue them. That trust deserves to be honored with the highest standards of security that each authority can responsibly achieve."
— TONY POOLE, PRESIDENT, DSA

The publication comes against a backdrop of serious and growing concern. Counterfeit identity documents are now pervasive across Europe, North America, and beyond — facilitating identity theft, financial crime including money laundering, worksite enforcement violations, and immigration-related offences such as human smuggling and trafficking. Fraudulent credentials are also actively exploited by individuals connected to organized criminal networks, including international terrorist groups, to reduce scrutiny at travel screening and border control. The paper's authors are unequivocal: the threat is not abstract. It is active, adaptive, and escalating.

A PRACTICAL GUIDE, NOT AN ENCYCLOPEDIA

The paper is explicitly designed as a guide to concepts, principles, and decision-making — focused on the "why" and "how" rather than exhaustive technical specifications. It acknowledges directly that not all technologies are equal: laser engraving, for example, offers a level of durability and tamper resistance that thermal personalization cannot match, and authorities with the means to adopt superior technologies should do so. But it also recognizes the realities of long procurement cycles, constrained budgets, and the time required for transition — and offers guidance on extracting the maximum security benefit from current tools while planning for future uplift.

THREE CRITICAL THEMES

- **Advancing the Physical.** The strongest modern credentials integrate physical security features with embedded digital elements — cryptographic chips and codes, Machine-Readable Zones, and biometric data — in ways that reinforce one another. The paper explores how issuing authorities can approach that integration thoughtfully, regardless of their current technical baseline.
- **Quality Control and Image Management.** A document is only as secure as its weakest process. Portrait photographs — the primary biometric identifier in most identity documents — are a frequent point of vulnerability. Poor image acquisition, inadequate quality checks, and inconsistent enrollment standards can undermine even the most sophisticated personalization technologies. Effective quality control is foundational, not peripheral.
- **Continuous Education as a Security Imperative.** Technologies evolve. Threat actors adapt. Standards develop. No document produced today can be considered permanently secure against tomorrow's threats — and no practitioner trained five years ago can be assumed current without ongoing development. The paper treats continuing education through conferences, structured training, webinars, and peer exchange as an integral component of any credible security framework.

"Security printing sits at the intersection of technology, process, and trust. Raising the bar on identity document security is not a one-time achievement — it demands continuous investment in standards, skills, and supply chain integrity across the entire industry."
— BEATRICE KLOSE, SECRETARY GENERAL, INTERGRAF

AN INVITATION TO RAISE THE STANDARD

The framework is grounded in both established best practice and the practical realities facing issuing authorities worldwide. It is offered, in the authors' own words, not as criticism of current practice, but as an invitation: to examine existing standards honestly, identify where improvements are achievable, and commit to a trajectory of continuous improvement.

Governments are continually under pressure to define security, technical, and design requirements that are financially sustainable and genuinely effective — keeping their documents ahead of counterfeiters who are rapidly closing the gap. This paper aims to show what a higher standard looks like in practice, and how every issuing authority can aspire to it.

"Not every issuing authority will adopt the same solutions, and not every context will support the same technologies. But every authority should regularly review its documents against threat scenarios and aspire to a higher standard of security."
— BERND KUMMERLE, CHAIRMAN, SIA

AVAILABILITY

The full paper is available for download from the DSA, INTERGRAF and SIA websites.
https://documentsecurityalliance.org
https://www.intergraf.eu
https://secureidentityalliance.org

ABOUT THE PUBLISHERS

Document Security Alliance (DSA)
The Document Security Alliance is a nonprofit association created by government agencies, private industry, and academia with the goal of identifying methods to improve security documents and related procedures to help combat fraud, terrorism, illegal immigration, identity theft, and other criminal acts. The organization brings together collaborative expertise from over 125 government, industry, and academic organizations, representing more than 400 individual members dedicated to improving the security and authentication of critical value documents.

DSA operates around three core pillars — Secure, Enforce, and Educate — to address the full lifecycle of document security challenges. Its public safety Identity Security Campaign, known as *#NoFakeIDs*, supports outreach and education through materials deployed in airports, universities, law enforcement training, and local communities. DSA also serves as a resource for governments seeking to build their understanding of existing solutions on issues ranging from counterfeiting to the security of travel and identity documents.

INTERGRAF
Intergraf is a trade association promoting and protecting the interests of the graphic industry at the European level, representing 22 member federations from 21 countries. Founded in 1930, the organization today advocates for Europe's printing industry toward the European Union, supporting the sector's competitiveness through advocacy, information sharing, networking, social dialogue, and EU projects. The industry Intergraf represents employs more than 550,000 people across more than 100,000 European printing companies, spanning books, newspapers, packaging, voting ballots, and identity documents.

A particularly notable area of Intergraf's work is its role in security printing standards and certification, centered on two complementary schemes: ISO 14298 for security printers and hologram manufacturers, and Intergraf 15374 for suppliers to the security printing industry. Intergraf is also a founding member of the World Print & Communication Forum (WPCF) and administers its Secretariat in Brussels.

Secure Identity Alliance (SIA)
The Secure Identity Alliance is an expert, globally recognized not-for-profit organization that brings together public, private, and non-government organizations to foster international collaboration, help shape policy, provide technical guidance, and share best practice in the implementation of identity programs. SIA's mission is to unify the ecosystem of identity so that people, the economy, and society thrive — with work spanning four pillars: Identity for Good, Outreach, Open Standards Development, and Industry Services and Solutions. The Alliance's members' technologies cover over 85% of the world's population through multiple applications.

A central pillar of SIA's technical work is its Open Standard Identity APIs initiative, known as OSIA — a set of interfaces enabling seamless connectivity between all building blocks of the identity management ecosystem, independent of technology, architecture, or vendor, and recognized as an official International Telecommunications Union (ITU) standard. SIA aligns its work with major international frameworks including the UN's 2030 Agenda for Sustainable Development and the OECD Recommendation on the Governance of Digital Identity.

— END —