



Evaluating physical security features in an eDocument
**Introducing the eSEC (eDocument
Physical Security Evaluation Model)
Free Web Tool**

eSEC - V1 - June 2018



- **The purpose of the eSEC is for the document issuers or manufacturers to do self-evaluation on their current or planned document.**

- **This self-evaluation is done by:**
 - **selecting the document type**
 - **listing security features**
 - **answering questions about the design process**

- **eSEC has a database of:**
 - **security features: strengths and threats countered**
 - **document types: special requirements**





Score

ePSEM

➤ The scoring algorithm rewards more for “wide” protection than “tall”

- Logarithmic score from features
- negative score e.g. from threats that are not countered

➤ The resulting score weights as follows:

- How widely security features are distributed to different parts of the document **15%**
- How strongly document is protected against different attacks **35%**
- How well different security feature levels are presented in the document **20%**
- The design process of the overall document **30%**

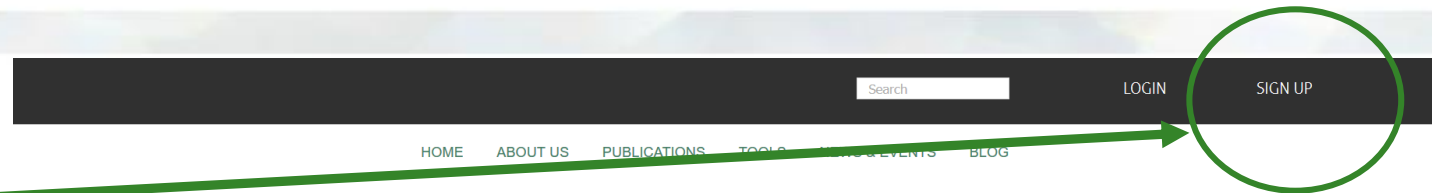
➤ The score is timeless and generic





eSEC : How does it work ?

- Go to SIA's Website
- Create a Web account
- Login to access eSEC



eDocument Physical Security Evaluation Model (eSEC)

The eDocument Scheme for Evaluating Physical Security (eSEC) is designed to help governments develop secure eDocuments. It can be used as a self-assessment tool to evaluate the physical security of current documents, the security impact of additional design changes, or simply to understand what is required to build a 'secure eDocument'.



Username

Password

Remember Me

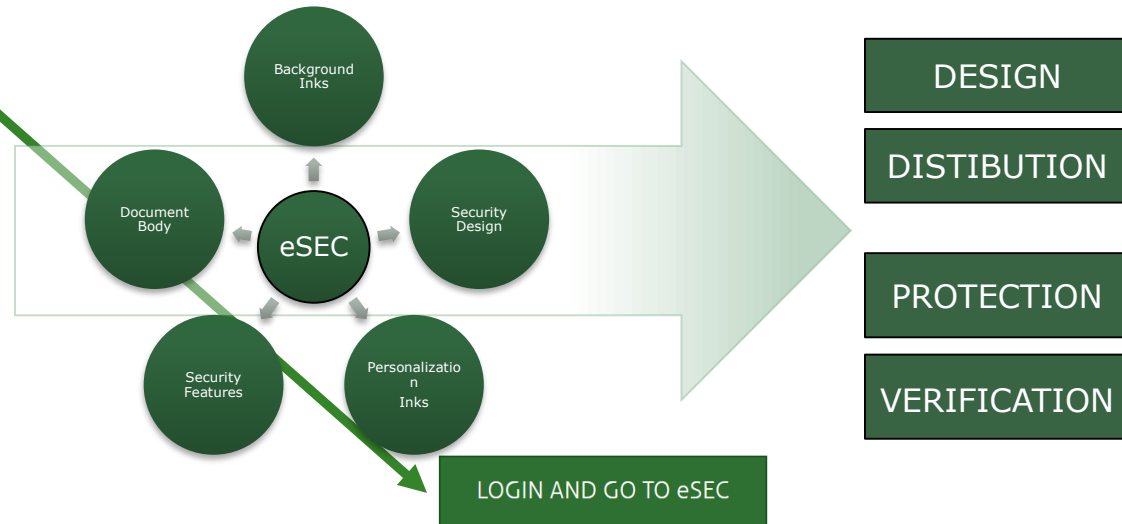
Log in

Create an account

Forgot your username?

Forgot your password?

June 2018 • eSEC



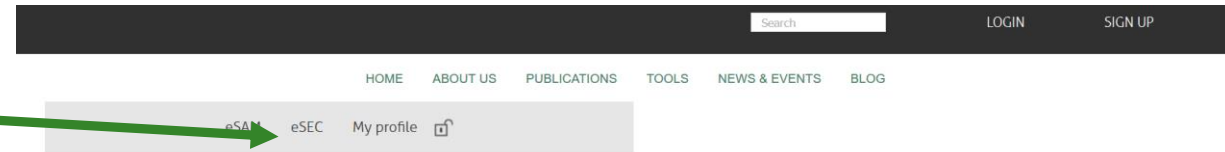
www.secureidentityalliance.org



eSEC : Evaluation

Once logged in

- Access eSEC
- Create a new evaluation
- Access an evaluation you have created previously



eSEC Evaluation

New evaluation

Modification	Document	Material	Organization	My Group	Owner	
2018-06-08	Passport	paper		test	anne.doe@magiris.fr	Edit
2018-06-07	ID Card	plastic	SIA	eDoc WG	anne.doe@magiris.fr	Edit
2018-06-07	ID Card	plastic			anne.doe@magiris.fr	Edit
	NEW				anne.doe@magiris.fr	Edit

Display # 10



eSEC: New Evaluation

eSEC Evaluation

New Evaluation

➤ Select Type of eDocument

➤ Select Material Type

➤ Name Evaluation

➤ Access Sections separately

➤ Don't forget to save!

The screenshot shows the 'eSEC Evaluation' form with several sections and a 'Save' button. Green arrows from the instructions on the left point to the following elements in the form:

- 'Select Type of eDocument' points to the 'Document Design' and 'Security Features' tabs.
- 'Select Material Type' points to the 'Material' section with radio buttons for 'paper' and 'plastic'.
- 'Name Evaluation' points to the 'Project' text input field.
- 'Access Sections separately' points to the 'Document' section.
- 'Don't forget to save!' points to the 'Save' button.

Form fields include: Document (Passport), Material (radio buttons for paper and plastic), Project (Test Anne Doe), and a 'Delete this scenario' dropdown menu (no delete).



eSEC : Document Design Section

Section

- **The Document Design Section consists of a list of questions with multiple choice answers.**

HOME ABOUT US PUBLICATIONS TOOLS NEWS & EVENTS BLOG

eSAM eSEC My profile

eSEC - Document Design

Evaluation Document Design Security Features

Document Design security refers to the physical features, techniques, and characteristics of documents including strengthening their security and improving their resistance to attack and misuse. With widespread access to low cost technologies including high quality scanning, color copying, image processing and photo quality printing, the capacity of individuals to produce convincing counterfeit travel documents and very deceptive alterations has increased significantly.

1- Is the security design based on a risk analysis and is it documented?

- YES - all aspects are covered and the risk analyses is documented.
- Risk analysis is incomplete
- No follow-up is given to risk analysis
- No risk analysis is done

Risk analyses involves:

- analyze threats (which documents are frequently reproduced or altered; what techniques are used by forgers);
- have the techniques employed by forgers advanced since the last risk assessment;
- assess damage involved;
- what is the probability of occurrence;
- balance risk against expected costs of eliminating or reducing it (cost-risk analysis).

Workgroup comment



eSEC – Security Features Section

The Security Features Section consists of a list of four types of security features:

- Printed
- Material
- Structure
- Personalization

Just tick the features you decide to include

eSEC - Security Features

Printed Features available (if any)

- Anti Scan / Anti Copy-Pattern
- Deliberate Error --- Deliberate error in e.g. micro text, that cannot be found without prior knowledge of the exact position of the error in the design of the document.
- Duplex printing --- A design made up of an interlocking pattern of small irregular shapes, printed in two or more colors and requiring very close register printing in order to preserve the integrity of the image
- ...

Material Features available (if any)

- Multi-color visible and UV reactive fibres --- Colored security fibers or fluorescent fibers are fibers in various colors, or multi-colored, which are mixed into the document body substrate

Structure Features available (if any)

- (Surface) Micro Lettering
- Card Surface Structure (Matt, glossy and smooth finish)
- ...

Personalization Features available (if any)

- 3D personalization --- Any technology that produces personalize data linked to the user that shows a depth effect caused by stereo effect.
- Additional Photo 1: using a different technique than for the primary image --- Additional Photo 1: using a different technique than for the primary image
- Additional Photo 1: using the same technique as for the primary image --- Additional Photo 1: using the same technique as for the primary image



eSEC Scores

Scores achieved are given for each parameter and overall:

- Design
- Distribution
- Protection
- Verification
- Overall

Scores eSEC - Protection

Scenario	Design	Distribution	Protection	Verification	Overall	
PDF						
	Counterfeit	Alteration	Recycling	Stealing	Impostor	Scores of Protection against threats
	3.65	2.85	3.56	0.54	0.30	10.88

HOME ABOUT US PUBLICATIONS TOOLS NEWS & EVENTS BLOG

eSAM eSEC My profile

Scores eSEC - Document Design

Scenario	Design	Distribution	Protection	Verification	Overall
PDF					
	Question	Answer	comments	/Max	
1-	Is the security design based on a risk analysis and is it documented?	YES - all aspects are covered and the risk analyses is documented.		3	3
2-	Are current threat mitigations incorporated from the start when creating new documents?	Threat mitigations are evaluated during the design phase.		2	3
3-	What is the design evaluation policy?	An experienced independent evaluator evaluates the system and product, both during development and at the final stage		3	3

Scores eSEC - Verification

Scenario	Design	Distribution	Protection	Verification	Overall
PDF					
	Level 1 (weight 50%)	Level 2 (weight 30%)	Level 3 (weight 10%)	ABC (weight 10%)	Scores of Verification all levels
	1.86	1.24	0.28	0.13	3.51

HOME ABOUT US PUBLICATIONS TOOLS NEWS & EVENTS BLOG

eSAM eSEC My profile

Scores eSEC - Overall

Scenario	Design	Distribution	Protection	Verification	Overall
PDF					
	Scores of Distribution all locations	Scores of Protection against threats	Scores of Verification all levels	Scores of Document Design	
	9.54	10.88	3.51	31.00	

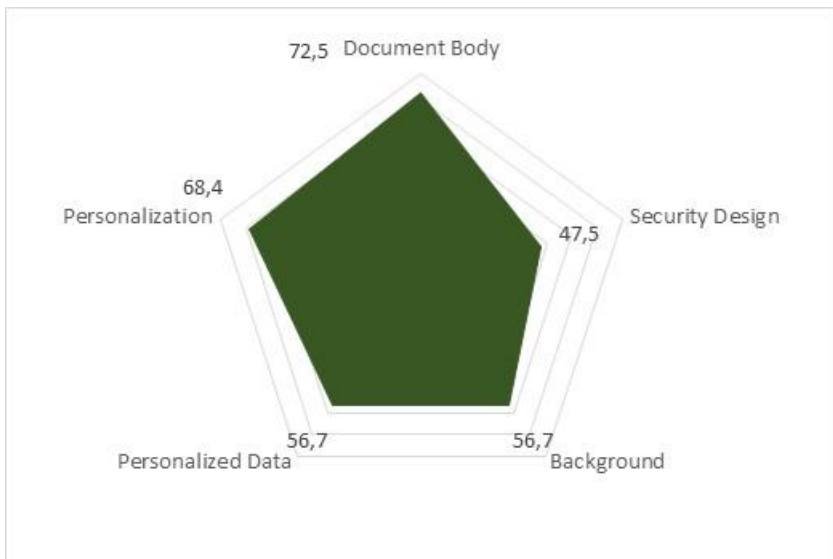
www.secureidentityalliance.org



eSEC Charts

Charts eSEC - Distribution of features

- Scenario
- Normalized
- Distribution
- Protection
- Verification
- Overall



Charts show scores achieved for each parameter and overall:

- **Design**
- **Distribution**
- **Protection**
- **Verification**
- **Overall**

A Management Report is available

Charts eSEC - Overall Security

- Scenario
- Normalized
- Distribution
- Protection
- Verification
- Overall





Part of a wider plan...

The 'common criteria' like approach to Physical Security Features Evaluation – The Proposed Scheme



The Why?

A: Identity documents have more options and unknowns than before

Specifications
Requirements
Implementation
Technology
Supplier

Traditional approach
Stable
Strict set of features
One option
Relying on well established features
One and known

Modern approach
Frequent updates
Functionality, threats, recommendations
Multiple options up-to the supplier
New security features/technology used
Multiple possible

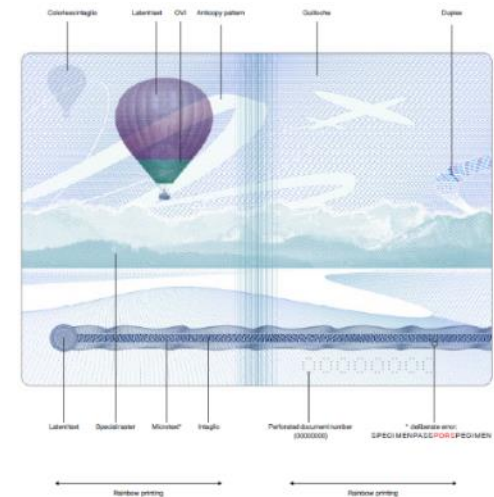
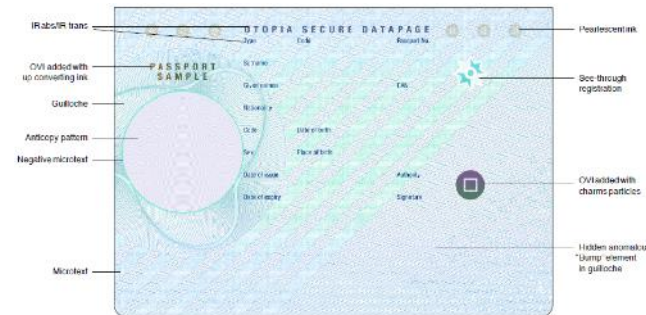
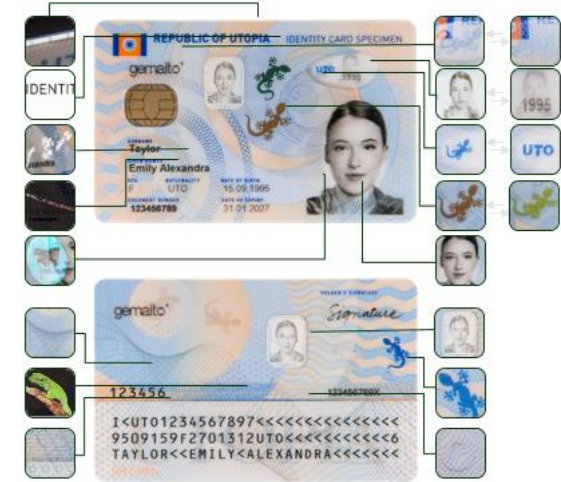
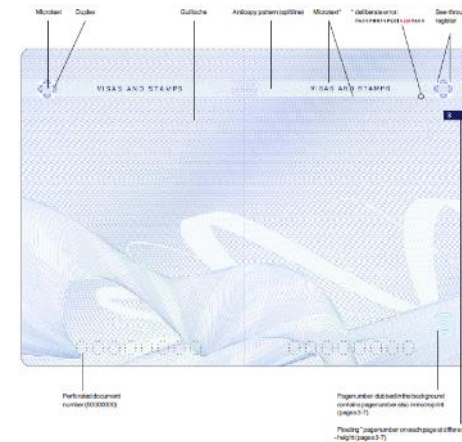
REQUIREMENTS FOR MRP DATA PAGE OPPOSITE THE MIRROR PAGE
The background print shall also contain: <ul style="list-style-type: none"> • A multicoloured guilloche (green, blue and yellow as in the specimen) • Iris (rainbow print) that shall fluoresce, where one of the colours is fluorescent • Micro lettering as in the enclosed specimen • A motive that is difficult to forge and reproduce (screen trap in the three hexagonal areas), as in enclosed specimen
The Changeable Laser Image (CLI) or Multiple Laser Image (MLI) or similar shall have a icon of the face image of the owner and the owner's birth date, which consists of six digits with no space between them (day month year, ddmmyy).
The DOVID shall be as shown in appendix A4.
The DOVID shall be metallic and placed as in the enclosed specimen.





The Challenge

- Physical security is being evaluated, but there is no formal method
- Experts share know-how with a limited group
- Comparing different documents security levels or setting public and measurable target is not possible
- Often no choice when evaluating the document





The Inspiration

- **No formal method for physical document, but**
 - ...guidelines in standards**
 - ...existing method for software**



ISO/IEC 18013





The Basis

› Security risk based evaluation (with possible durability aspect)

- Identify threats → create protection profile → evaluate products against the protection profile

› Open scheme → Different Protection Profiles can be defined

- for different types of documents with different threats

› The evaluation results in a score



Opposite to CC
(pass/fail)

› Multiple processes for evaluation (levels of assurance)



Similar to CC (EAL)
details differ

- Assurance Level 1 = generic self evaluation (no PP)
- Assurance Level 2 = 3rd party review of security features
- Assurance Level 3 = 3rd party test of security features
- Assurance Level 4 = 3rd party test of security features and features durability



The Actors

Similar to CC, but simplified with less actors

Scheme Owner
SIA / ICAO / ...

- ✘ Defines the evaluation scheme
- ✘ Approves protection profiles
- ✘ Approves evaluation laboratories
- ✘ Publication

Contributor
Recognized experts

- ✘ Define Protection Profiles

Evaluator
Laboratory / expert

- ✘ Perform evaluations
- ✘ Issue evaluation reports

Customer
Issuing state / vendor

- ✘ Self evaluation according to the scheme and guidelines
- ✘ Issue products to evaluation labs for assessment



The Scheme

➤ Rules/requirements for...

- ...creating protection profiles
- ...performing self evaluation
- ...becoming an evaluation lab
 - Capabilities, security, confidentiality etc...
- ...performing evaluation in a 3rd party labs

➤ Guidelines / Repository of...

- ...security threats in following categories
 - Counterfeit a complete document
 - Alteration of real document
 - Recycling document or it's components
 - Theft of blank document
 - Impostor pretending to be the document owner
- ...how to verify documents combined security strength
- ...methods for aging and wear for security features



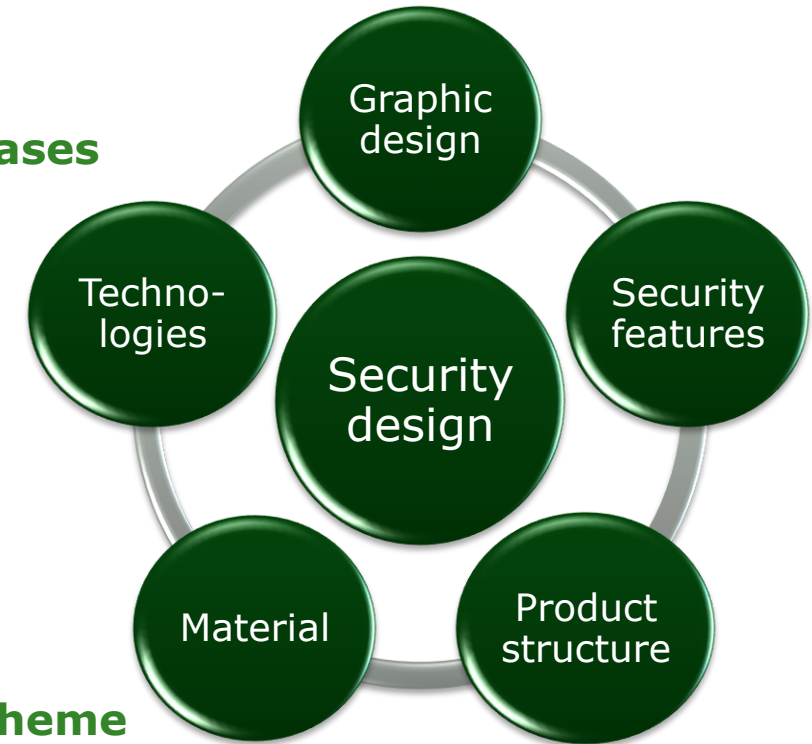


The Protection Profile

› Defines...

- ...the security product under evaluation and it's normal use cases
- ...the threats to the document
- ...what assurance levels (2-4) are covered by this profile
- ...how to review against the threats (L2)
- ...how to test against the threats (L3)
 - i.e. try to forge the document
- ...how to age security features and test them (L4)
- ...how to score / rank the security level of the document

› Guidelines for threats and evaluation will be available in the scheme





The Plan

› Development steps

- **1st step - develop the assurance level 1 - self evaluation**

- Define the generic self evaluation concept in detail
- Create an online self evaluation tool (ePSEM)

- **2nd step - expand into assurance level 2**

- ...and create first protection profiles for specific documents

- **3rd step - more protection profiles**

- **4th step - expand in to assurance level 3**

› Co-operation

- **ICAO, universities, labs**

- **More co-operation and contributions welcome**





Contacts:

- › **Jean-Claude Perrin (Secretary General)**
jean-claude.perrin@secureidentityalliance.org
- Stéphanie de Labriolle (Marketing Director)**
stephanie.delabriolle@secureidentityalliance.org

www.secureidentityalliance.org

follow us

