Evaluating physical security features in an eDocument

# Introducing the eSEC (eDocument Physical Security Evaluation Model) Free Web Tool

eSEC - V1 - June 2018

# Functionality

- **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

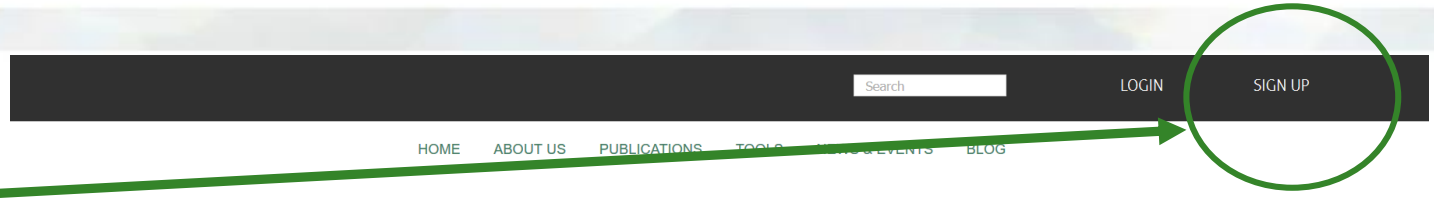
- **The scoring algorithm rewards more for "wide" protection than "tall"**
  - **Logarithmic score from features**
  - **negative score e.g. from threats that are not countered**

- **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**

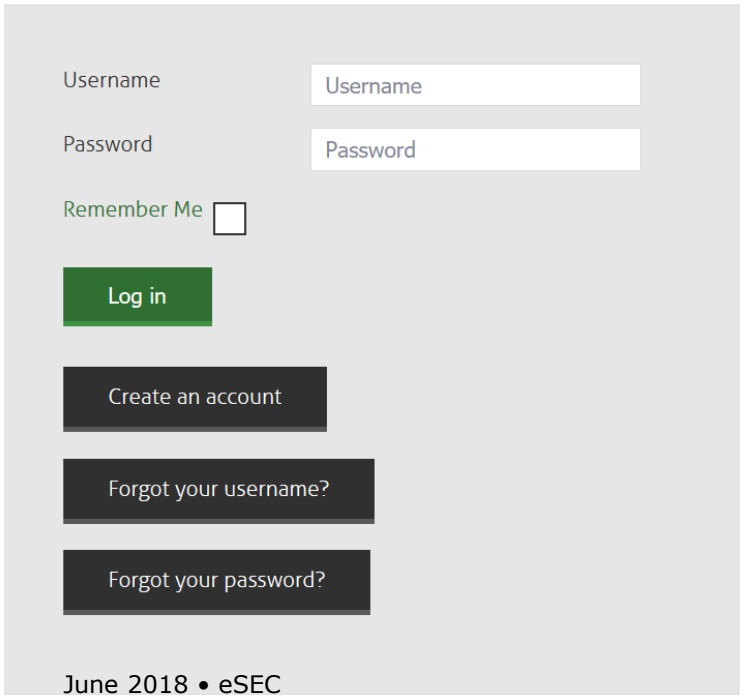
# eSEC : How does it work ?

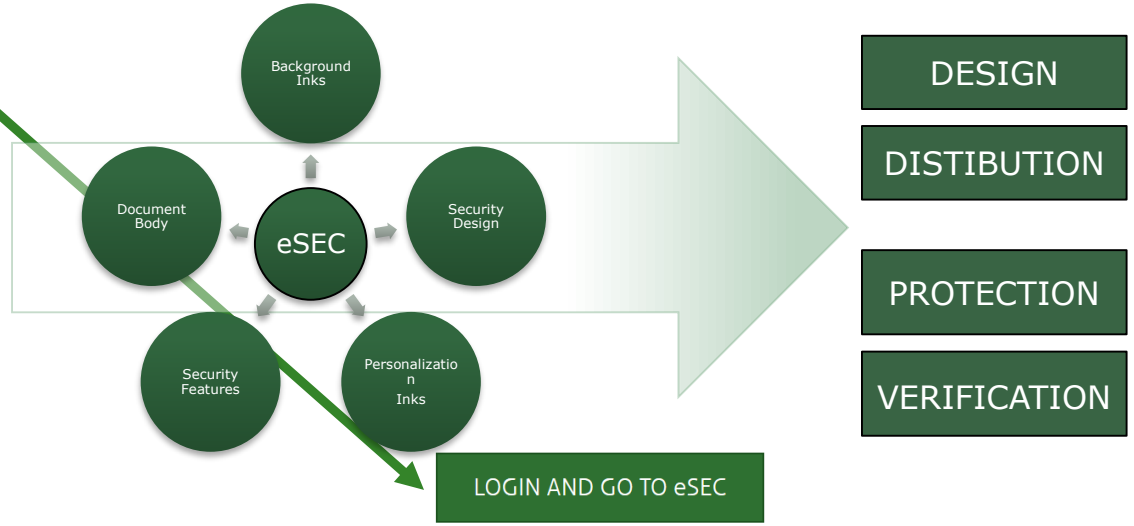
- **Go to SIA's Website**
- **Create a Web account**
- **Login to access eSEC**




## 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'.



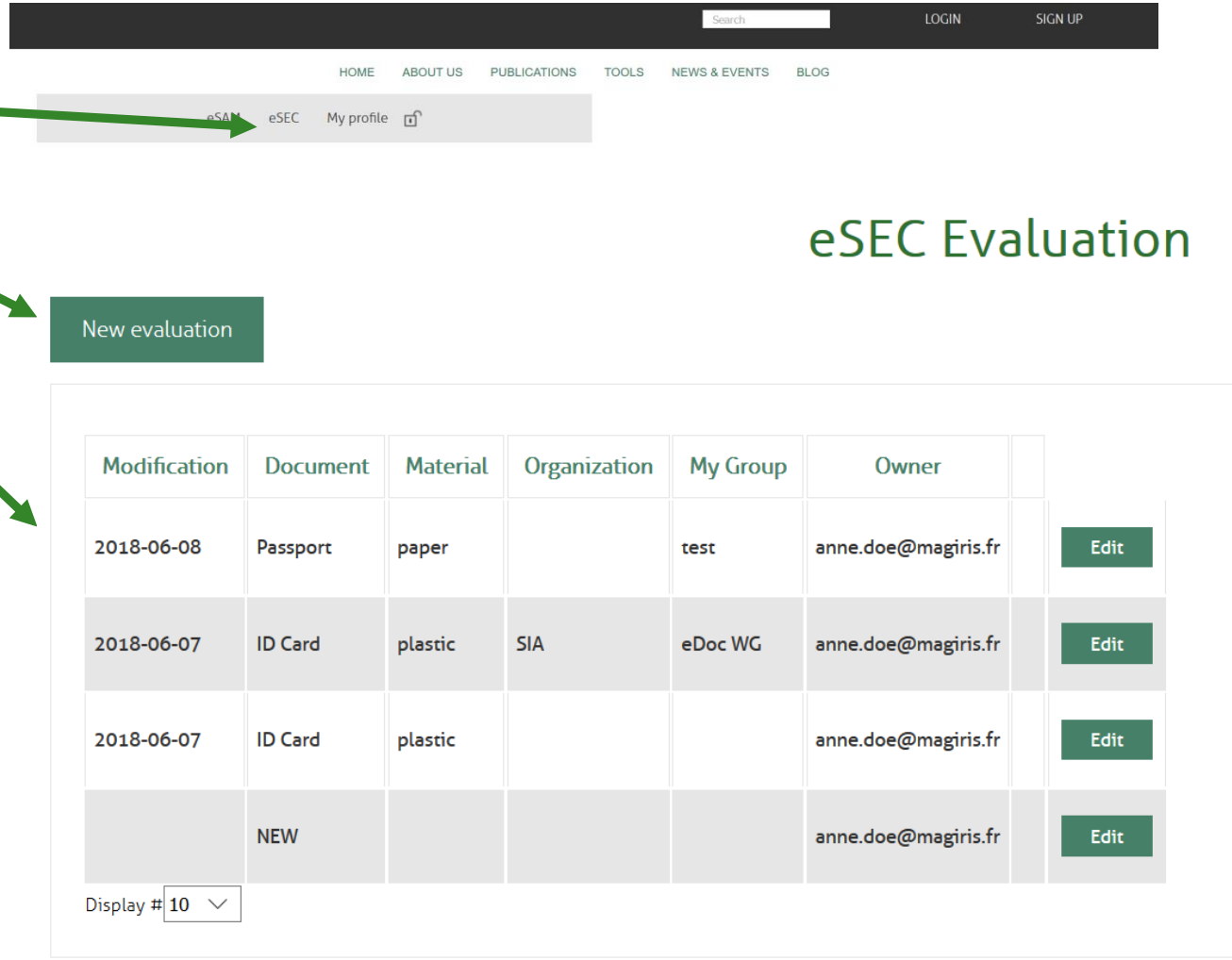




***www.secureidentityalliance.org***

# eSEC : Evaluation

**Once logged in**

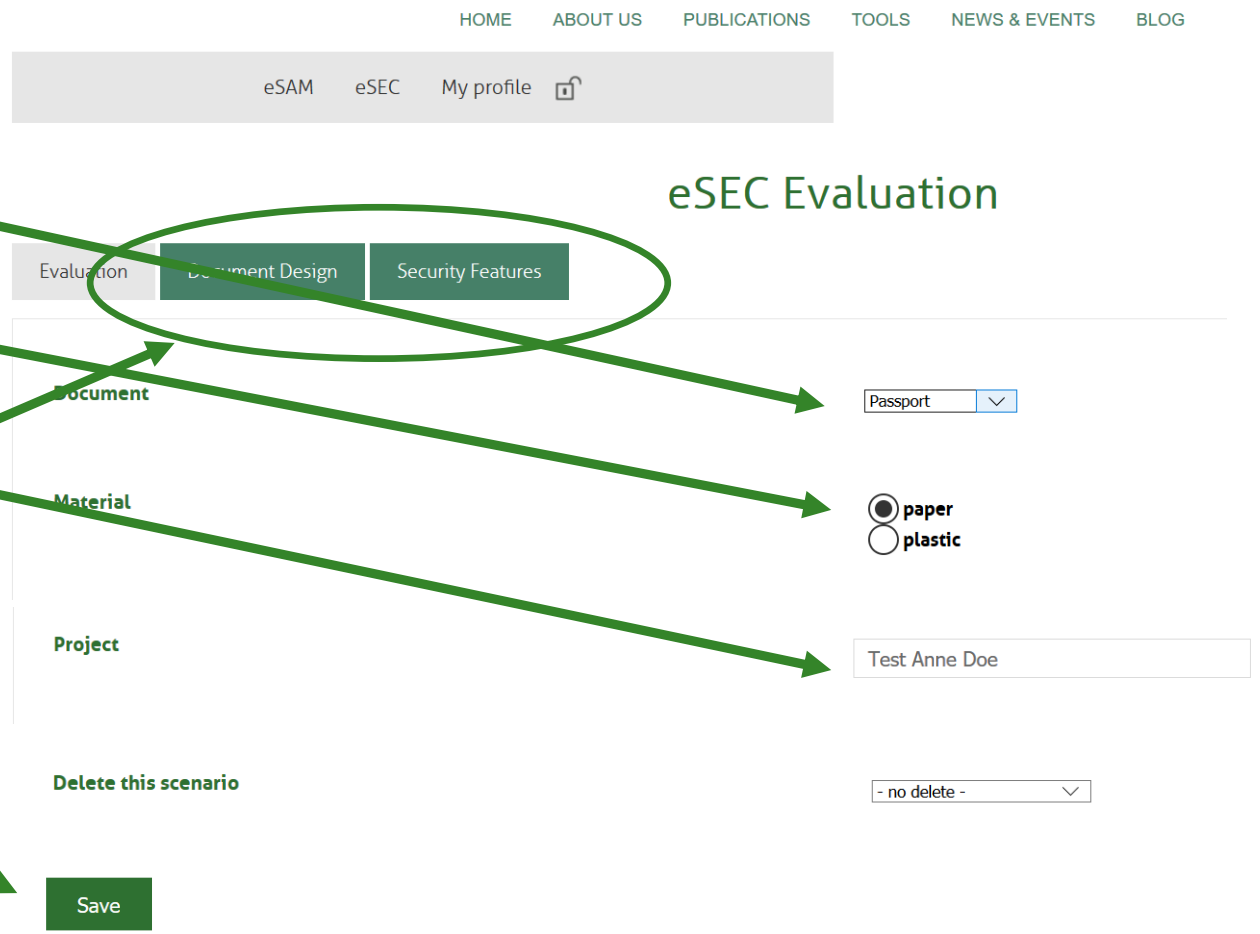
- **Access eSEC**
- **Create a new evaluation**
- **Access an evaluation you have created previously**



# eSEC: New Evaluation

## New Evaluation

- **Select Type of eDocument**
- **Select Material Type**
- **Name Evaluation**
- **Access Sections separately**
- **Don't forget to save!**

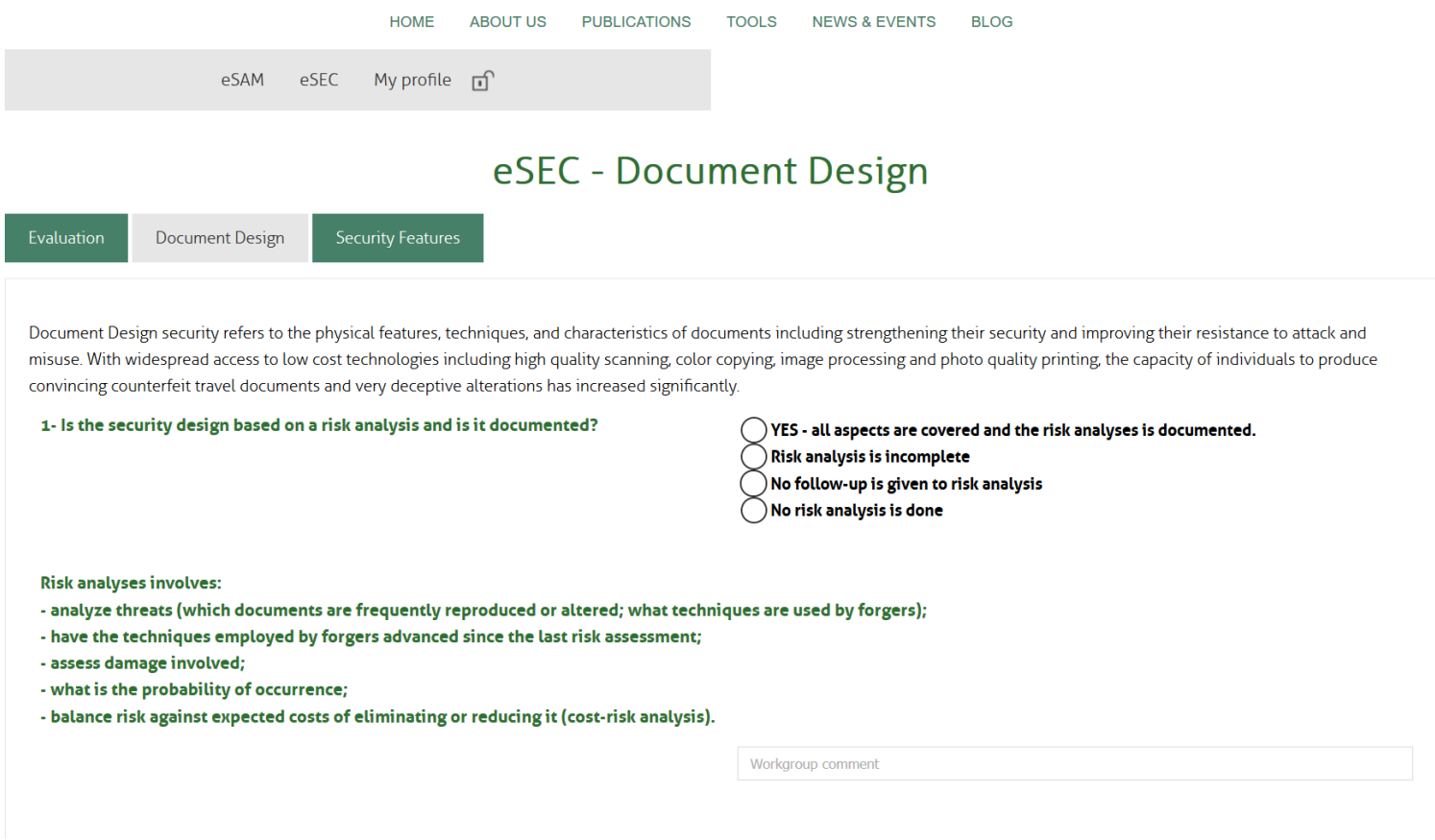



***www.secureidentityalliance.org***

# eSEC : Document Design Section

## Section

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



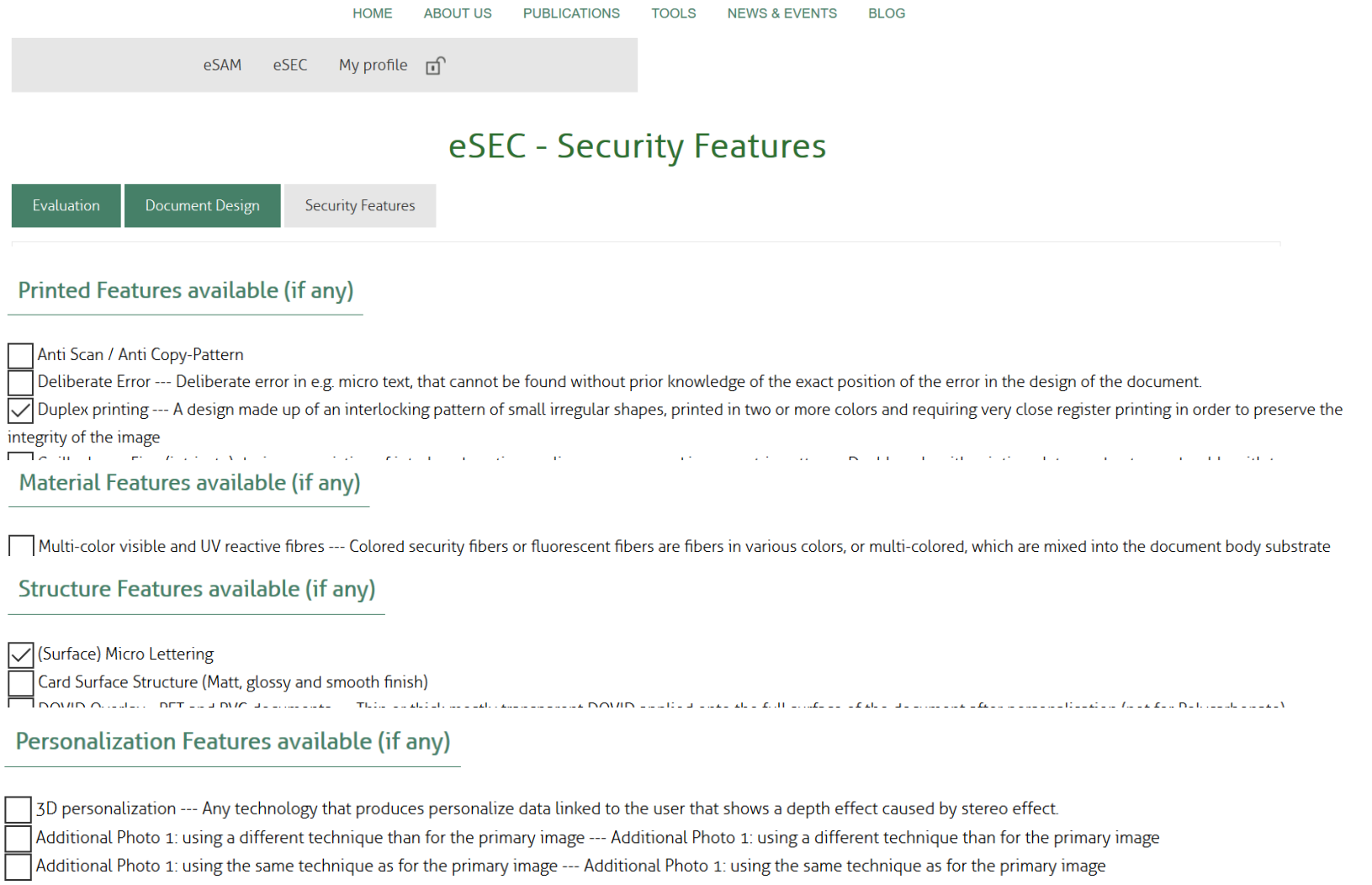

***www.secureidentityalliance.org***

# eSEC – Security Features Section

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

- **Printed**
- **Material**
- **Structure**
- **Personalization**

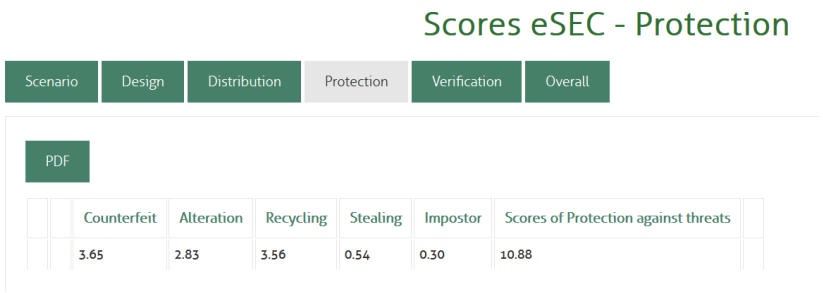
**Just tick the features you decide to include**



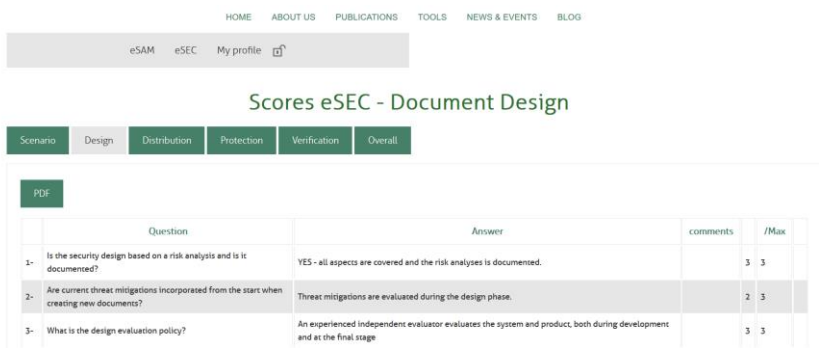
# eSEC Scores

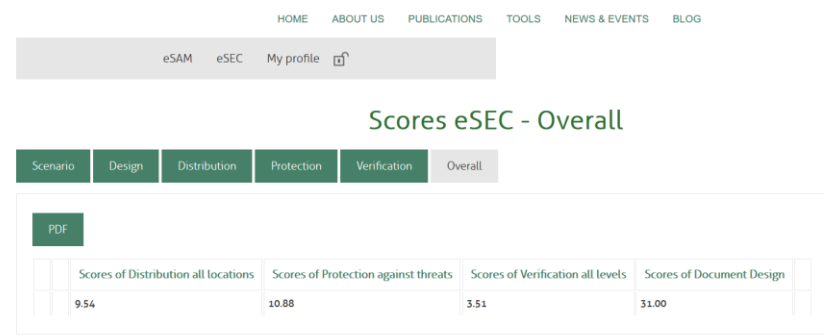
**Scores achieved are given for each parameter and overall:**

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








***www.secureidentityalliance.org***

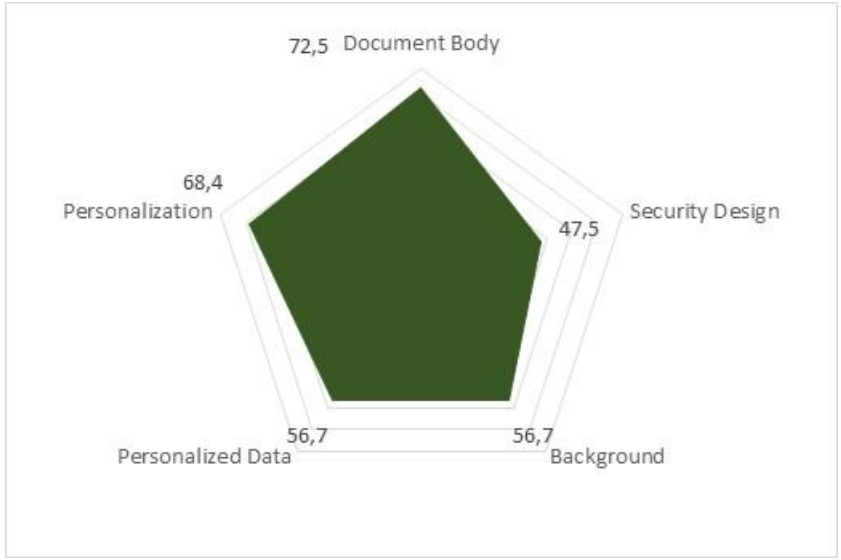
# eSEC Charts

HOME ABOUT US PUBLICATIONS TOOLS NEWS & EVENTS BLOG

eSAM eSEC My profile

## 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**

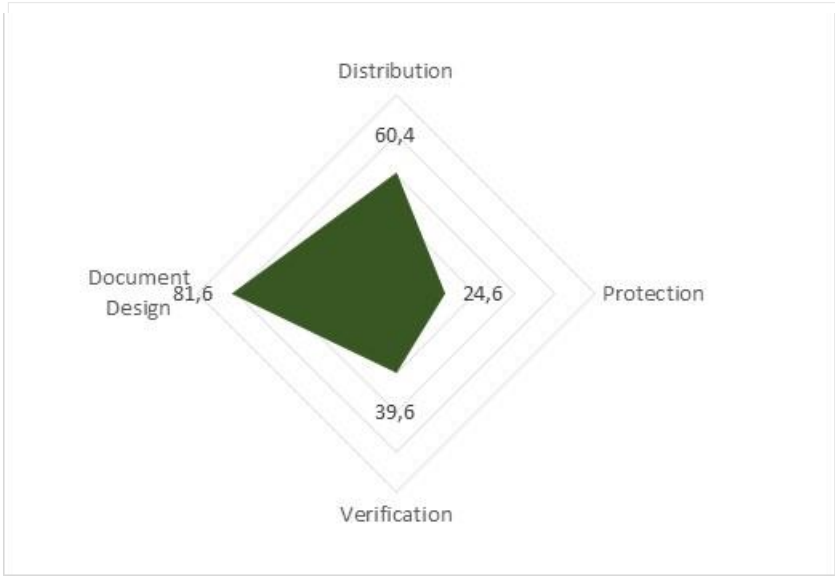
**A Management Report is available**

HOME ABOUT US PUBLICATIONS TOOLS NEWS & E

eSAM eSEC My profile

## 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

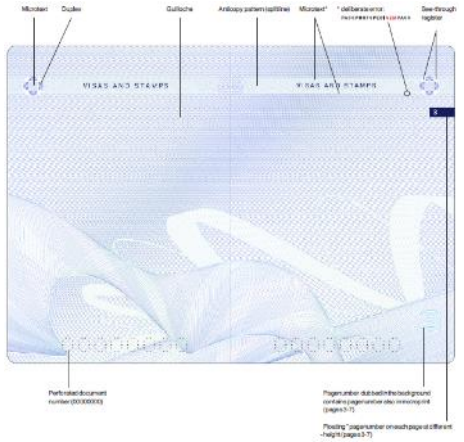
| | Traditional approach | Modern approach |
|---|---|---|
| **Specifications** | Stable | Frequent updates |
| **Requirements** | Strict set of features | Functionality, threats, recommendations |
| **Implementation** | One option | Multiple options up-to the supplier |
| **Technology** | Relying on well established features | New security features/technology used |
| **Supplier** | One and known | Multiple possible |

| REQUIREMENTS FOR MRP DATA PAGE OPPOSITE THE MIRROR PAGE |
|---|
| The background print shall also contain:<br>• A multicoloured guilloche (green, blue and yellow as in the specimen)<br>• Iris (rainbow print) that shall fluoresce, where one of the colours is fluorescent<br>• Micro lettering as in the enclosed specimen<br>• 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. |

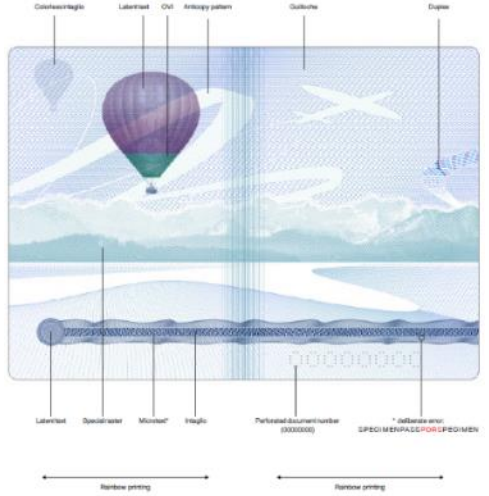
*SIA - Physical Security Evaluation Scheme*

# 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**

ICAO

Doc 9303
Machine Readable Travel Documents
Seventh Edition, 2015

ISO/IEC 18013

Common Criteria

# 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

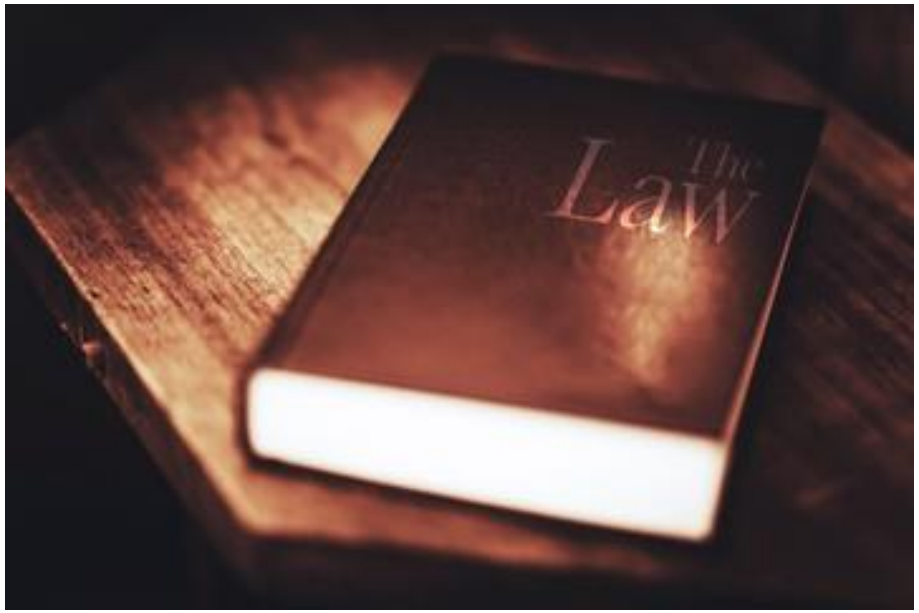
- Self evaluation according to the scheme and guidelines
- Issue products to evaluation labs for assessment

*SIA - Physical Security Evaluation Scheme*

# The Scheme

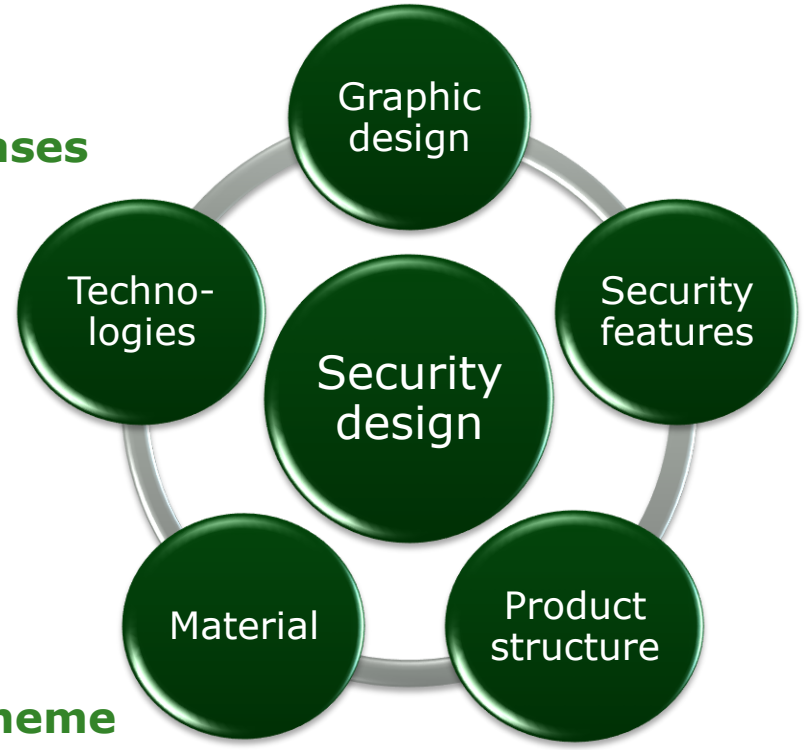
- **Rules/requirements for…**
  - **…creating protection profiles**
  - **…performing self evaluation**
  - **…becoming an evaluation lab**
    - Capabilities, security, confidentiality etc…
  - **…performing evaluation in a 3rd party labs**

- **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