



Building a 'security chain' in an eDocument issuance program Introducing the eSAM (eSecurity Awareness Model) Free Web Tool

eSAM – V3 - June 2018



eDocument Issuance program

➤ **Governments need a secure, yet efficient way to manage the eDocument issuance process**

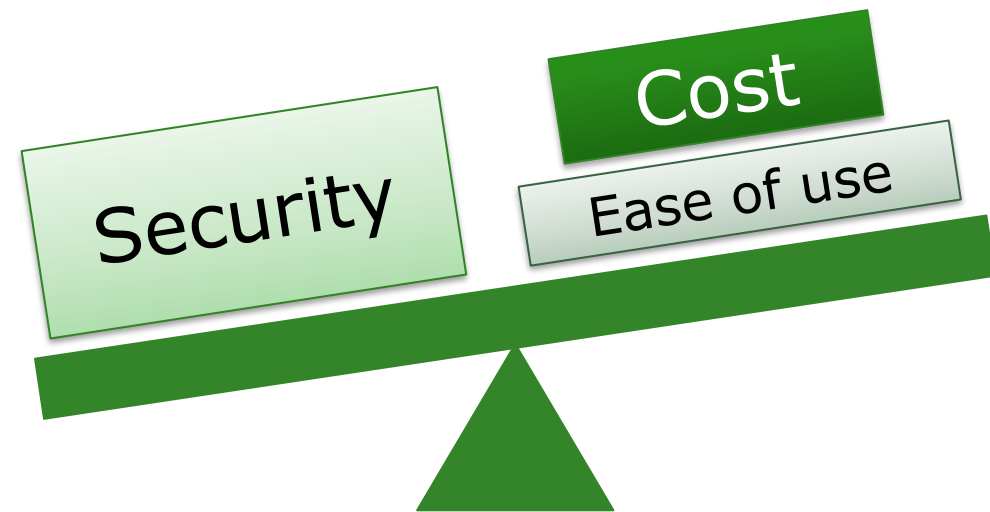
➤ **This starts with a careful evaluation of risks**

- Type of fraud
- Cost/impact of fraud

➤ **Find balance between:**

1. **Cost**
2. **Security**
3. **End user convenience**

➤ **For their specific conditions**





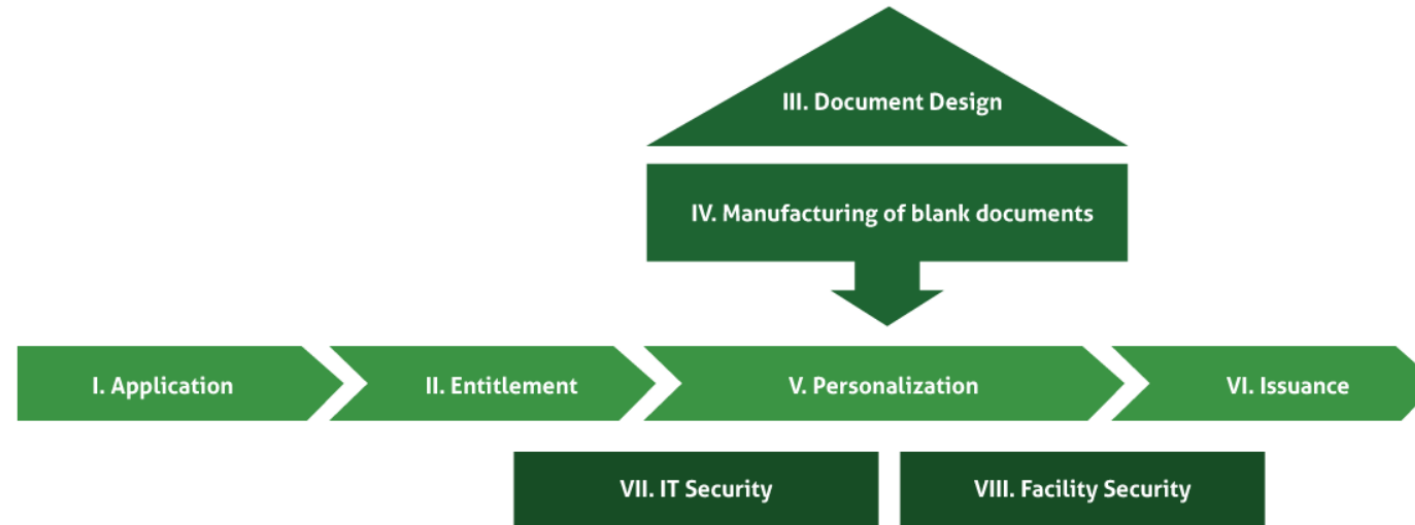
eDocument Issuance program

- **How to optimize the security, convenience and cost balance challenge ?**
- **Who to believe ?**
 - **Vendors will try to push their security features and their enrolment and personalization solutions**
- **Where to find 'Best Practices' ?**
 - **Security Awareness Model (eSAM) from**





eSecurity Awareness Model (eSAM)



➤ **The eDocument Security Awareness Model (eSAM) has been developed by SIA**

- To help governments with their secure document development program
- And to understand what is required to build a 'security chain'

➤ **Self-assessment tool:**

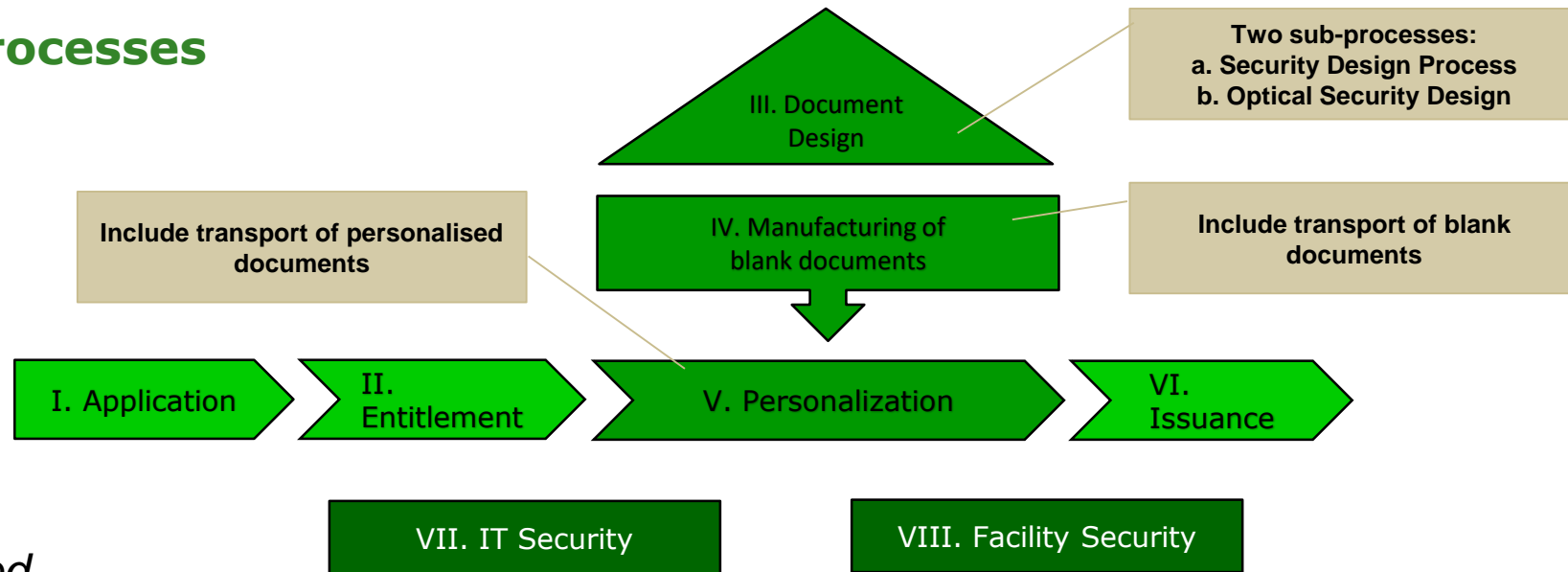
- For evaluation of an existing program or
- For trying different scenarios and see the effect on the security chain



eDocument Security Awareness Model

➤ The eSAM consists of three basic process flows and covers the complete security chain:

- 1. Application to Issuance (dataflow)
- 2. Document design to Personalization (material flow)
- 3. Support processes



*Any data inputted
is fully confidential*



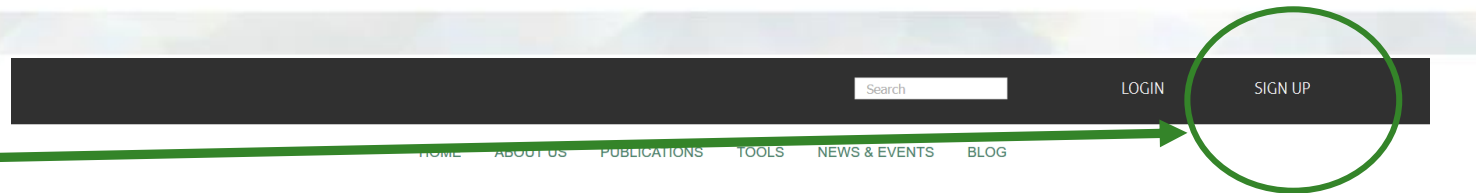
eSAM Sub-Processes

- **Application/entitlement (first time/renewals; in person/on-line; lost or stolen document; limited breeder documents; biometrics)**
- **Design (design process; international standards; substrate material; durability; security features; how to inspect?)**
- **Personalization (central/de-central/overseas; safeguard transport and storage of blank documents and consumables)**
- **Issuance (in person/mail; how to mitigate risk of issuance to wrong person?)**
- **IT- and Facility security (how to protect data and prevent unauthorized access; security certification)**



eSAM : How does it work ?

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



eSecurity Awareness Model (eSAM)

The eDocument Security Awareness Model (eSAM) is designed to support governments in the development of their eDocument programs – helping them understand what is required to build an effective 'security chain'. It can be used as a self-assessment tool to evaluate existing programs, the security impact of additional changes, or to test multiple new scenarios.



Username

Password

Remember Me

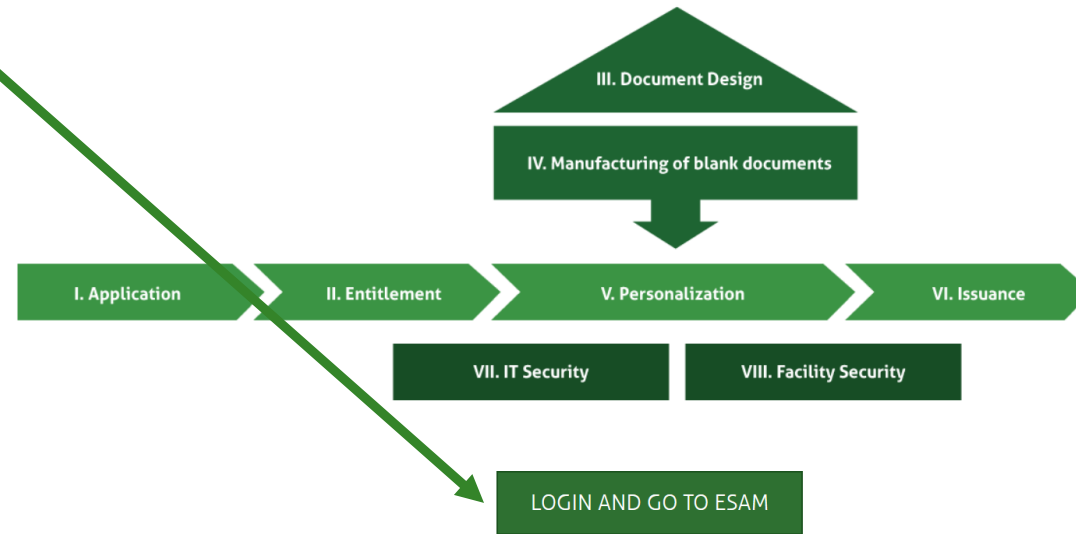
Log in

Create an account

Forgot your username?

Forgot your password?

June 2018 • eSAM



www.secureidentityalliance.org



eSAM : Scenario

Once logged in

- Access eSAM
- Create a new scenario
- Access a scenario you have created previously

The screenshot shows the eSAM user interface. At the top, there is a navigation bar with a search box and links for LOGIN and SIGN UP. Below this is a secondary navigation bar with links for HOME, ABOUT US, PUBLICATIONS, TOOLS, NEWS & EVENTS, and BLOG. A user menu is visible with options for eSAM, eSEC, and My profile. A 'New scenario' button is highlighted. Below this is a table of scenarios with columns for Modification, eDocument, Organization, Project, and Owner. Each row has an 'Edit' button. At the bottom, there is a 'Display #' dropdown menu set to 10.

Modification	eDocument	Organization	Project	Owner	
2018-06-08	Driving License		Test Anne Doe	anne.doe@magiris.fr	Edit
2018-06-08	ID Card			anne.doe@magiris.fr	Edit
2018-06-08	COPY			stephdelab@hotmail.com	Edit
	NEW			anne.doe@magiris.fr	Edit

Display # 10

www.secureidentityalliance.org



eSAM : Sub-processes

New Scenario

➤ Select Type of eDocument

➤ Name Scenario

➤ Access sub-processes separately

➤ You may delete your scenario here

➤ Sections you have submitted appear here

HOME ABOUT US PUBLICATIONS TOOLS NEWS & EVENTS BLOG

eSAM eSEC My profile

Scenario eSAM

Scenario Application Entitlement Document Optical Manufacturing Personalization Issuance IT Facility

eDocument

Organization

Project

Delete this scenario

Sections submitted so far

www.secureidentityalliance.org



eSAM : Multi-choice Questionnaire

Section

- **The questionnaire consists of a list of questions with multiple choice answers.**

HOME ABOUT US PUBLICATIONS TOOLS NEWS & EVENTS BLOG

eSAM eSEC My profile

Scenario - Section I. Application

Scenario Application Entitlement Document Optical Manufacturing Personalization Issuance IT Facility

To obtain a document, applicants typically must follow a specified application process, including the completion of forms, documentary evidence, submission of photographs, and in some cases secondary biometrics. The information and documentation they provide will enable Issuance Authority (IA) employees to establish the entitlement of the applicant to a document. The information the applicant submits must be protected during the whole issuance process and also after the document is issued. Privacy and protection of data are essential elements to ensure the security of the document issuance process.

1- Are all applications processed in a uniform and consistent manner throughout the issuing Authorities?

YES - at all locations.
 At most locations, exceptions well documented.
 NO

Workgroup comment

2- Are the same standardized forms, software and hardware configurations and procedures always used?

YES - at all locations.
 At most locations, exceptions well documented.
 NO

Workgroup comment



eSAM - Support Processes

Two support processes are distinguished:

- IT security
- Facility security

These only contain some basic questions if not covered by a certificate in the first place.

HOME ABOUT US PUBLICATIONS TOOLS NEWS & EVENTS BLOG

eSAM eSEC My profile

Scenario - Section VII. Information Technology Security

Scenario Application Entitlement Document Optical Manufacturing Personalization Issuance IT Facility

Information Technology (IT) security is defined as safeguards to preserve the confidentiality, integrity, and availability, intended use and value of electronically stored, processed or transmitted information.

The Issuing Authority (IA) has become more and more automated and is using information technology to improve efficiency, security and service delivery. At the same time, the number and potential severity of threats, vulnerabilities and incidents are similarly increasing. Because IA demands the collection of detailed personal information; sometimes including biometrics, the protection and security of IT systems and databases is crucial.

1- Does the site have a security certification?

- YES - multiple certifications covering all the aspects of IT Security in the full operation.
- YES - Some areas of operations are certified.
- No certifications.

Workgroup comment

IT Security Policy

2- Is there a comprehensive and converged IT security policy in place?

- YES - one truly converged IT security policy with a fully interoperable and multi-layered security strategy is in place.
- IT security team and facility management team separately provision and enrol IT and PACS identities. Each team has its own security policy in place. Audit logs are not monitored by one converged detect system.
- NO

www.secureidentityalliance.org



Different choices in program

In the Issuance process the Issuing Authority (IA) can make different choices :

- **Applicant picks up document in person**
- **Third party is permitted to pick up document**
- **Document is mailed to home address**

The IA's choices have a clear impact on the security, convenience and cost of the program.

HOME ABOUT US PUBLICATIONS TOOLS NEWS & EVENTS BLOG

eSAM eSEC My profile

Scenario - Section VI. Issuance

Scenario Application Entitlement Document Optical Manufacturing Personalization **Issuance** IT Facility

Once personalized, the document is handed over to the applicant. Here, a few options exist regarding process implementation:
in-person pickup (or release to a third party);
secure mail, delivery or courier services.

Depending on the method(s) chosen, some techniques can be used to mitigate the risk of the document being released to a person impersonating the true applicant or using a false identity.

1- How is the document collected by the recipient?

- Applicant picks up document in person.
- Third party is permitted to pick up document.
- Document is mailed to home address.

Workgroup comment

Save



eSAM Scores and Recommendations

Scores for Security Awareness (SA), Cost Effectiveness (CE) and Convenience (C)

Recommendations (if applicable) to improve security

Your scores for Security Awareness, Cost Effectiveness and Convenience against the maximum score

HOME ABOUT US PUBLICATIONS TOOLS NEWS & EVENTS BLOG

eSAM eSEC My profile

Score - Section I. Application

Scores Application Enrollment Document Optical Manufacturing Personalization Issuance IT Facility Chart

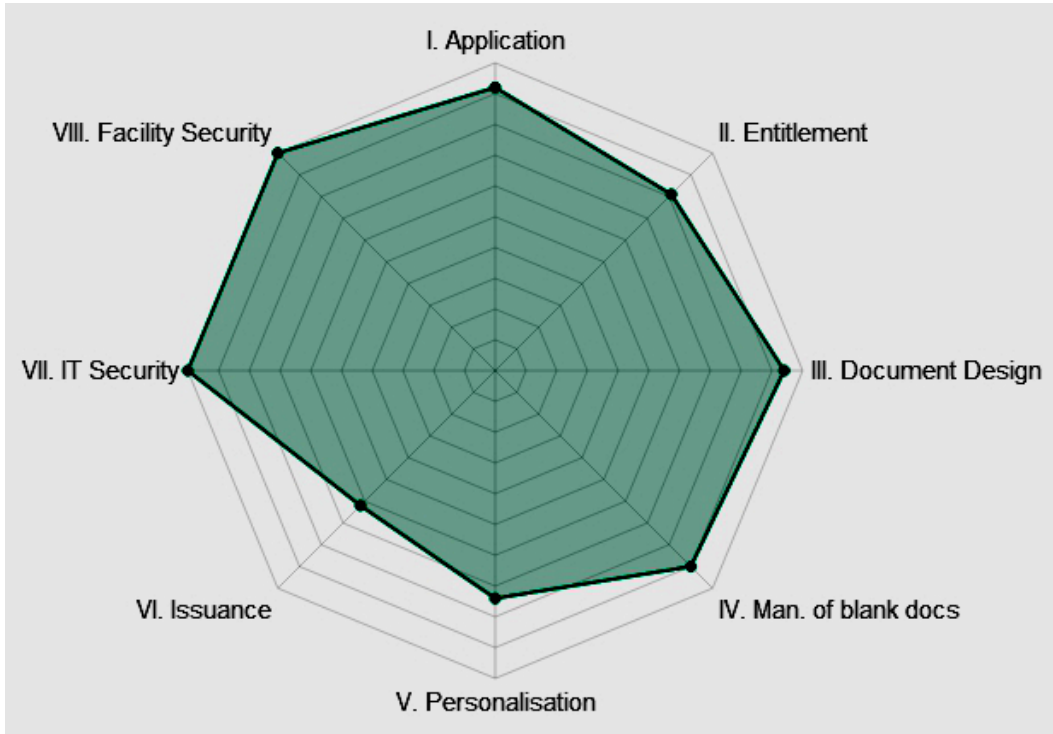
PDF

Question	Answer	Recommendation	Workgroup Comments	/SA	/CE	/C
1- Are all applications processed in a uniform and consistent manner throughout the Issuing Authorities?	YES - at all locations.			3 3	0 0	0 0
2- Are the same standardized forms, software and hardware configurations and procedures always used?	NO			1 3	1 2	0 0
3- Is it required that applicants appear in person for application?	Personal appearance is only required applying					
5- How is the photograph submitted?	It is required to include a photograph with the application. Submitted photographs can be taken by an official authorized photographer, trusted partner considering to meet the specifications.	Live-capturing shortens the portrait acquisition chain, makes direct feedback on the quality of the digital image possible (re-do enrolment if quality is unsatisfactory) and ensures the photograph is recent and portrait and person are linked.			3 4	1 2 1 3
6- Is a secondary biometric feature collected as part of the application process?					0 3	0 2 0 2
7- How is the photograph submitted?	Are Anti-fraud specialist (AFS) installed in every application authority location to provide assistance in dealing with any suspicious application? In some small locations AFS assistance is offered from a nearby location.	AFS assistance from nearby location is easy to get and used when required.			2 3	1 2 0 0
8- Is regular training conducted for those authority staff whose task it is to process applications?	YES				1 3	0 0
				17 / 25 5 / 13 5 / 11		

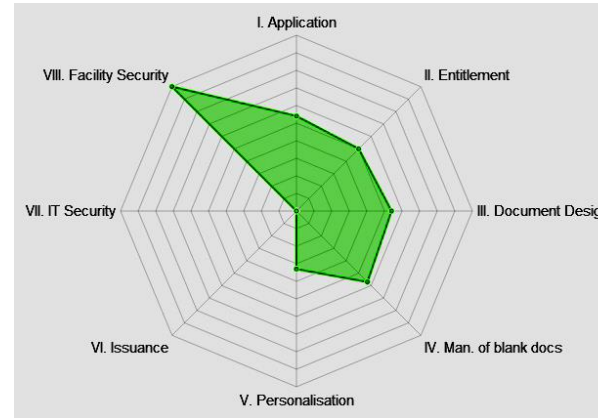


eSAM Management report with scores

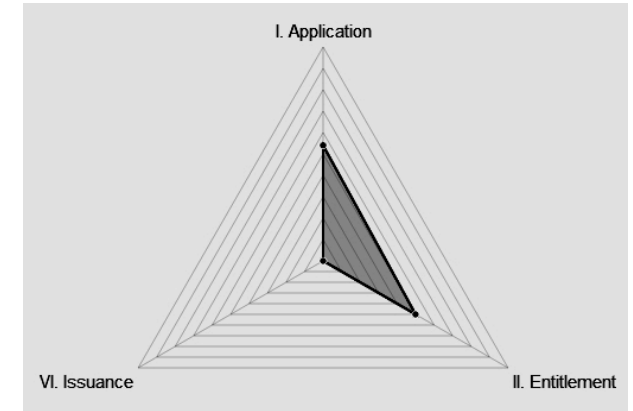
SECURITY AWARENESS



COST EFFECTIVENESS



CONVENIENCE



- **Security is not the only aspect you have to balance in your program**
- **Convenience (ease of use) score only for processes that interfere with citizens (end users)**



3.

Examples

Low-end and high-end security scenarios



Two scenario's

Process	High security	Cost optimized
Type of Document	<ul style="list-style-type: none">• Passport with PC e-data page	<ul style="list-style-type: none">• PVC DL, no chip
Application	<ul style="list-style-type: none">• Capturing biometrics• Background check	<ul style="list-style-type: none">• Application by mail or web• Legitimation through previous documents or copy thereof
Issuance	<ul style="list-style-type: none">• Pick-up in person	<ul style="list-style-type: none">• Mailed to home address
Document design	<ul style="list-style-type: none">• Design with security printing• Portrait and data laser engraved• Inspection conditions considered	<ul style="list-style-type: none">• Basic design with CMYK printing• Portrait and data applied with D2T2 and protected with clear patch



Summary scenario's

Process	High security	Cost optimized
Security elements	<ul style="list-style-type: none"> • High security print (offset, PMS, OVI) • Secondary portrait in MLI • Security design based on integral security concept 	<ul style="list-style-type: none"> • Basic security (digital, CMYK) • Security design for minimum cost
Manufacturing process	<ul style="list-style-type: none"> • Production in high security zones • Serial numbering for blank documents • Secure transport 	<ul style="list-style-type: none"> • Production in standard industrial environment • Blank documents shipped by courier
Personalization	<ul style="list-style-type: none"> • Central personalization in high security zones with high quality laser equipment 	<ul style="list-style-type: none"> • D2T2 desktop personalization with no special security measures
Security	<ul style="list-style-type: none"> • Production and personalization sites are certified 	<ul style="list-style-type: none"> • No physical access system • No systematic checks on staff • Alarm system in place

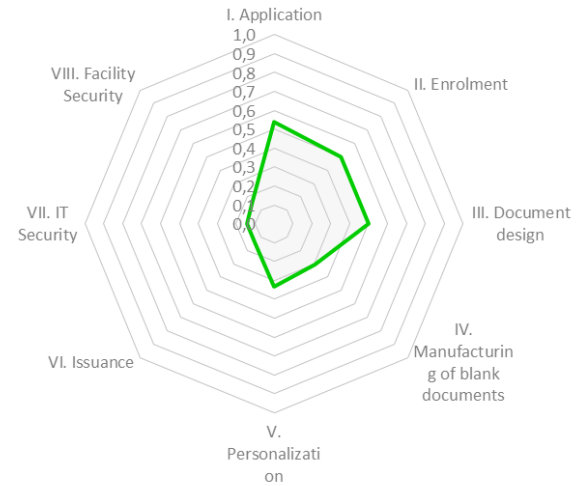


Results High Security Scenario

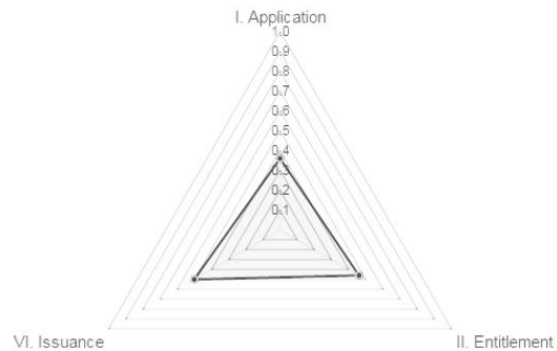
Security Awareness



Cost Effectiveness



Convenience

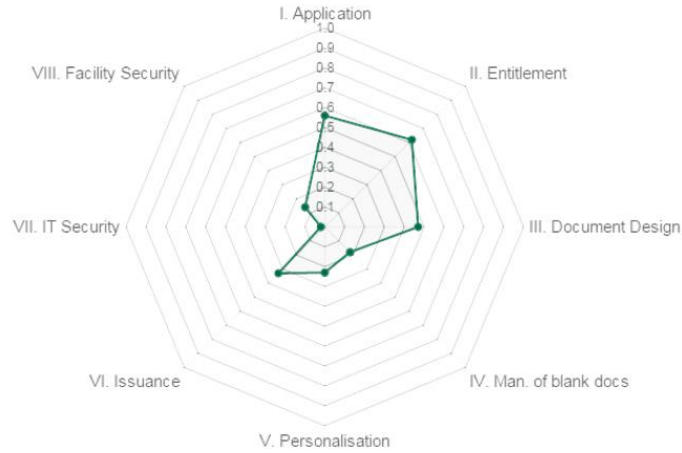


- HIGH ON SECURITY
- LESS COST EFFECTIVE
- LESS CONVENIENT

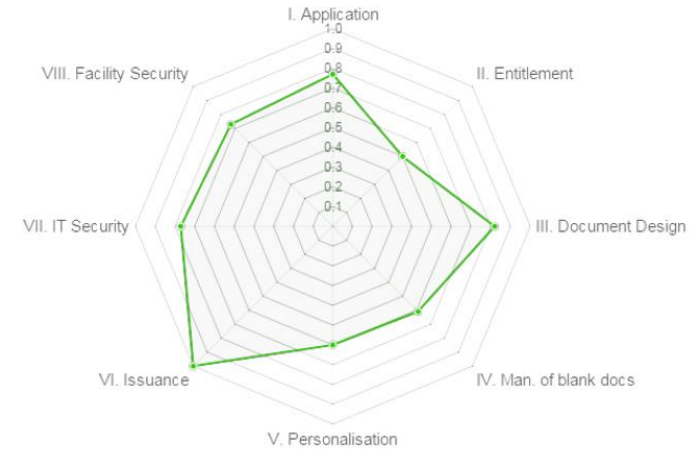


Results Cost Optimized Scenario

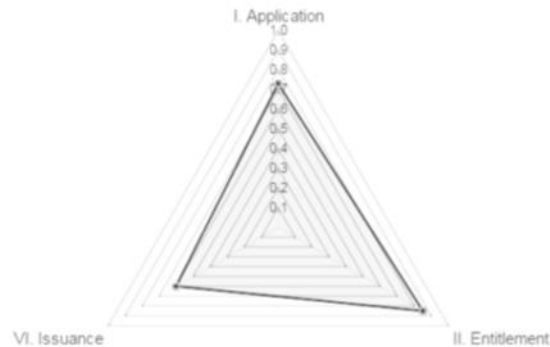
Security Awareness



Cost Effectiveness



Convenience



➤ **LOW ON SECURITY**

➤ **HIGH ON COST EFFECTIVENESS**

➤ **MORE CONVENIENT**



Sources of information

Main Sources

- **ICAO Doc 9303 Part 1, Vol1**
- **ICAO Guide for Assessing Security of Handling and Issuance of Travel Documents**
- **Optical Document Security by Rudolf L. van Renesse**
- **Documents: the Developer's Toolkit by Diana Ombelli and Fons Knopjes**

Many more sources have been used and combined with the experience from multiple document programs by the SIA members.



Contacts:

Jean-Claude Perrin at

jean-claude.perrin@secureidentityalliance.org

Stéphanie de Labriolle at

stephanie.delabriolle@secureidentityalliance.org

www.secureidentityalliance.org