

Preventing identity document fraud: some of the best practices for an easier detection

Windhoek, 27th April 2017

A few words about the Imprimerie Nationale Group



Integrator of security solutions for governments

Long time document fraud cooperation



National ID cards



Passports & travel documents



Driving licence cards



Residence permit cards



Agents ID cards

**Multi-credentials
platforms**

Main issues of document & ID fraud, in France, 2015

ID documents



44 %

Vehicule documents



24 %

Other documents



30%

Source: © January 2017 - INHESI/ONDRP (France) – 2016 annual report

Huge consequences

→ Fake identities are used by **criminal organisations**



→ Fake identification documents cause **massive financial burden**




A holistic approach for security design

Documents for each country shall be specific to meet with their **particular needs and constraints**

Recommendation:
homogenize ALL
issued documents



Counterfeiting

	Counterfeiting 
How often	Rare attacks but very efficient because highly professional
What it is	Imitation of an authentic document
Why it happens	production technics used are old or too common
Solution	Use of non commercial security features, cleverly mixed, regularly changed

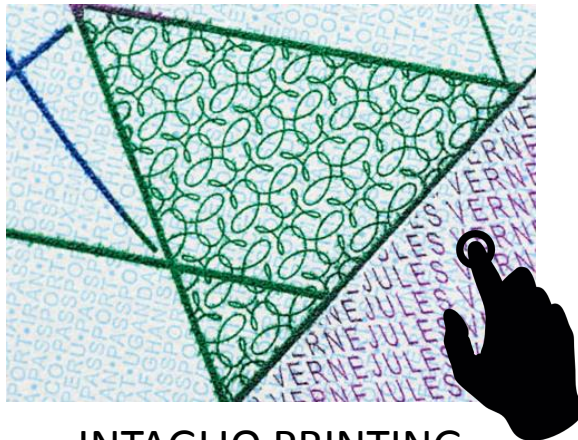


Security features to fight counterfeiting

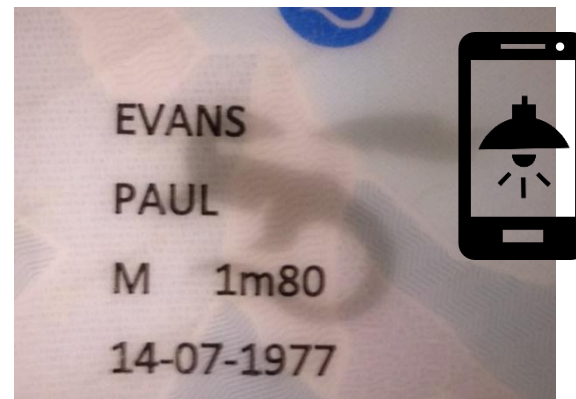
RECOMMENDATION: MIXING A FEW COMPLEX CUSTOMIZED FEATURES



WATERMARK



INTAGLIO PRINTING



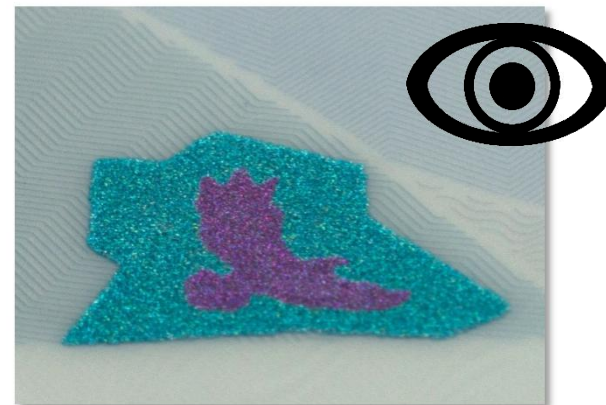
METALIZED WATERMARK
(CAI™)



COMPLEX UV PRINTING




COMPLEX OFFSET
BACKGROUND



HIGH SECURITY INKS

Falsification

	Falsification 
How often	Growing trend; focused on the photo
What it is	Fraudulent transformation of personal data
Why it happens	Variable data are not enough protected
Solution	Protection of the data with chemical reactivities, security design, tactile features...



Security features to fight falsification

PURPOSE: MAKING ANY ATTACK/CHANGE OF DATA TAMPER EVIDENT



PAPER & INKS WITH
CHEMICAL REACTIVES



SECURITY DESIGN MIXED
WITH PRINTED DATA



COMPLEX UV PRINTING
OVER THE DATA



DATA TACTILE ENGRAVING




TACTILE LAMINATION
OVER THE DATA





MLI/CLI

Exotic documents

	Exotic 
How often	Rare attacks
What it is	Creation of a fake document totally different from the real one
Why it happens	The design of the document is too ordinary and/or unknown
Solution	Very specific design, highly memorable. Communication.



Other types of document & ID frauds

	Blank stolen 	Look alike 
How often	Highly variable	Growing trend
What it is	Document stolen before personalisation	Fraudulent use of a document belonging to a third party
Why it happens	Non secure storage	No/few easily controlable physical characteristics
Solution	Close spaces, restricted areas. Centralized personalization. Secure transport & numbering for better flows traceability.	Biometric enrolment



Awareness, knowledge and tooling for efficient detection

Awareness (alerts about frauds types & new docs)

→ Communication
toward on-field agents



Knowledge (about detection methods)

→ Basic training is critical



Tooling (for effective on-field controls)

→ Simple and affordable tools make a difference



How to avoid fraudulent obtaining of document

1. Audit existing processes to obtain ID documents



2. List the important required documents: SECURE THEM

- ✓ Secure design & raw materials
- ✓ Personalization
- ✓ Encrypting data



3. Digitalize the workflow, create secure databases with encryption



12EV3456789

Interoperability & standardization



We will be pleased to welcome you on booth D7



Integrator of security solutions for governments

The digital support of this presentation (with additional contents) is available on request