Trusted Credential and Digital ID Leveraging

ID4 Africa, May 24-25, 2016

KIGALI, RWANDA
Agenda

• Credential security relies on 4 pillars
• Security features of physical credentials
• Portrait vulnerability
• Benchmark of portrait printing processes for polycarbonate
• Physical credential derivation?
• See Lasink demo on our booth
Agenda

- Credential security relies on 4 pillars
  - Security features of physical credentials
  - Portrait vulnerability
  - Benchmark of portrait printing processes for polycarbonate
  - Physical credential derivation?
  - See Lasink demo on our booth
Credential security relies on 4 pillars

1. **Document materials**
   Maintain the document integrity over a period of time from delamination, cracks, tampering

2. **Security features**
   Protect graphical information from manipulation (tampering, counterfeiting, stolen blank document)

3. **Personalization technology**
   Tamperproof and durable integration of card holder data

4. **Electronics**
   Integrate biometric data for automated control of document and holder
Agenda

- Credential security relies on 4 pillars
  - Security features of physical credentials
  - Portrait vulnerability
  - Benchmark of portrait printing processes for polycarbonate
  - Physical credential derivation?
  - See Lasink demo on our booth
Definition
“A physical security feature is a physical element which is added to a document to make it impossible to copy and to modify.”

The security features governing the security of an identity document can be divided into three levels of security, i.e.

- **Level 1** Security (Overt) => visible with naked eyes at point of usage
- **Level 2** Security (Covert) => for examination by trained personnel with simple equipment
- **Level 3** Security (Forensic) => visible in laboratory by forensic specialists, requiring special equipment

The three levels of security, in combination, provide comprehensive security coverage to ensure their validity and authenticity.
<table>
<thead>
<tr>
<th>Card security features</th>
<th>Personalization security features</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level 1</strong></td>
<td><strong>Level 1</strong></td>
</tr>
<tr>
<td>- Complex fiduciary printing</td>
<td>- Variable Laser image - CLI / MLI</td>
</tr>
<tr>
<td>- Inks mixing (rainbow)</td>
<td>- Tactile or clear laser marking</td>
</tr>
<tr>
<td>- Optical variable inks – OVI</td>
<td>- Ghost image</td>
</tr>
<tr>
<td>- Iridescent inks</td>
<td>- Image laser perforation</td>
</tr>
<tr>
<td>- Optical variable device - OVD</td>
<td>- Tilted Laser perforation</td>
</tr>
<tr>
<td>- Diffractive device - DOVID</td>
<td>- Greyscale image</td>
</tr>
<tr>
<td>- Tactile surface elements</td>
<td>- Laser colour image – LASINK™</td>
</tr>
<tr>
<td>- Moiré elements</td>
<td>...</td>
</tr>
<tr>
<td>- Clear window</td>
<td><strong>Level 2</strong></td>
</tr>
<tr>
<td></td>
<td>- Digital watermarking ( Hidden or encrypted information in portrait)</td>
</tr>
<tr>
<td></td>
<td>- Laser micro text</td>
</tr>
<tr>
<td></td>
<td>- Personalized thermal printed UV</td>
</tr>
<tr>
<td></td>
<td>- Proprietary fonts</td>
</tr>
<tr>
<td></td>
<td>- Personalized photopolymer holograms</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
<tr>
<td><strong>Level 2</strong></td>
<td><strong>Level 3</strong></td>
</tr>
<tr>
<td>- Invisible inks (UV or IR), including rainbow printing</td>
<td>- Printed deliberated errors</td>
</tr>
<tr>
<td>- Microtext printing</td>
<td>- Special fonts</td>
</tr>
<tr>
<td></td>
<td>- Tagged or metameric inks</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
</tbody>
</table>
Agenda

- Credential security relies on 4 pillars
- Security features of physical credentials
  - Portrait vulnerability
- Benchmark of portrait printing processes for polycarbonate
- Physical credential derivation?
- See Lasink demo on our booth
• 300 hologram manufacturers only in China
• Retransfer printers deployed everywhere
• Inkjet printers deployed everywhere
• Black and white laser printers deployed outside of governments

-> The portrait is at risk
• Credential security relies on 4 pillars
• Security features of physical credentials
• Portrait vulnerability
• Benchmark of portrait printing processes for polycarbonate
• Physical credential derivation?
• See Lasink demo on our booth
• Invented 20 years ago
• Black and White
• Then Grey Scaled
- Portrait is printed in sheet format using digital printing (inkjet or toner)
- After printing, layers are laminated
- Cards or datapages are punched
- Laser engraving most of the time to increase security
• Portrait is printed using D2T2 direct or retransfer, or inkjet
• Holographic overlay is laminated (we don’t consider UV cured varnish or clear patch as relevant for MRTD)
Color in PC – Laser bleaching

- Process

![Image of barcode reader and colored labels: Camera, Green, Red, Blue, YAG, YAG]

- X, Y, Registration
- Bleach Magenta pigments
- Bleach Cyan pigments
- Bleach Yellow pigments
- Black layer + text data
- Reverse side
Color in PC – Laser masking

• Principle
Counterfeiting attempt on Lasink™

No digital printer available to copy a LASINK™ picture

Genuine Lasink™ image

Genuine Lasink™ digital image printed on a high resolution digital color printer
In a Lasink image, no overlap of the 4 colors, only grey scaling on pure colors.
Authentication of the exact frequency
Every technology has strengths and weaknesses

Security: a color picture should offer maximum protection against forgery and fraud. It should be well protected and difficult to change or imitate.

Durability: the color picture should remain unaltered under all circumstances for a 10-year lifetime application.

Flexibility: personalization should be possible at a stage later than manufacturing.

Picture classicism: the color photo classicism can be appreciated through its pattern, resolution, contrast and color saturation.

Picture authentication: it is important for authorities or document checkers at level 1, 2 and 3 to have criteria to authenticate a genuine portrait versus a counterfeit one.

Cost per document: lower is the total cost of ownership of a solution higher is the score.

- Security: maximum protection
- Durability: unaltered for 10 years
- Flexibility: personalization possible later
- Picture classicism: pattern, resolution, contrast, color saturation
- Picture authentication: criteria for authorities
- Cost per document: lower cost higher score

Marks:
- 5 points when the best for a particular criteria
- 3 points when good
- 1 point when average
Every technology has strengths and weaknesses

**Security**: a color picture should offer maximum protection against forgery and fraud. It should be well protected and difficult to change or imitate.

**Durability**: the color picture should remain unaltered under all circumstances for a 10-year life time application.

**Flexibility**: personalization should be possible at a stage later than manufacturing.

**Picture classicism**: the color photo classicism can be appreciated through its pattern, resolution, contrast and color saturation.

**Picture authentication**: it is important for authorities or document checkers at level 1, 2 and 3 to have criteria to authenticate a genuine portrait versus a counterfeited one.

**Cost per document**: Lower is the total cost of ownership of a solution higher is the score.

---

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>5</td>
</tr>
<tr>
<td>Durability</td>
<td>3</td>
</tr>
<tr>
<td>Flexibility</td>
<td>1</td>
</tr>
<tr>
<td>Picture classicism</td>
<td>5</td>
</tr>
<tr>
<td>Picture authentication</td>
<td>3</td>
</tr>
<tr>
<td>Cost per document</td>
<td>1</td>
</tr>
</tbody>
</table>

---

Marks:
- 5 points when the best for a particular criteria
- 3 points when good
- 1 point when average
Every technology has strengths and weaknesses

**Security**: a color picture should offer maximum protection against forgery and fraud. It should be well protected and difficult to change or imitate.

**Durability**: the color picture should remain unaltered under all circumstances for a 10-year life time application.

**Flexibility**: personalization should be possible at a stage later than manufacturing.

**Picture classicism**: the color photo classicism can be appreciated through its pattern, resolution, contrast and color saturation.

**Picture authentication**: it is important for authorities or document checkers at level 1, 2 and 3 to have criteria to authenticate a genuine portrait versus a counterfeited one.

**Cost per document**: Lower is the total cost of ownership of a solution higher is the score.

---

**Marks**

- 5 points when the best for a particular criteria
- 3 points when good
- 1 point when average
Every technology has strengths and weaknesses

Security: a color picture should offer maximum protection against forgery and fraud. It should be well protected and difficult to change or imitate.

Durability: the color picture should remain unaltered under all circumstances for a 10-year life time application.

Flexibility: personalization should be possible at a stage later than manufacturing.

Picture classicism: the color photo classicism can be appreciated through its pattern, resolution, contrast and color saturation.

Picture authentication: it is important for authorities or document checkers at level 1, 2 and 3 to have criteria to authenticate a genuine portrait versus a counterfeited one.

Cost per document: Lower is the total cost of ownership of a solution higher is the score.

Marks
5 points when the best for a particular criteria
3 points when good
1 point when average
Every technology has strengths and weaknesses

- **Security**: a color picture should offer maximum protection against forgery and fraud. It should be well protected and difficult to change or imitate.

- **Durability**: the color picture should remain unaltered under all circumstances for a 10-year life time application.

- **Flexibility**: personalization should be possible at a stage later than manufacturing.

- **Picture classicism**: the color photo classicism can be appreciated through its pattern, resolution, contrast and color saturation.

- **Picture authentication**: it is important for authorities or document checkers at level 1, 2 and 3 to have criteria to authenticate a genuine portrait versus a counterfeited one.

- **Cost per document**: Lower is the total cost of ownership of a solution higher is the score

Marks:
- 5 points when the best for a particular criteria
- 3 points when good
- 1 point when average
Every technology has strengths and weaknesses

**Security**: A color picture should offer maximum protection against forgery and fraud. It should be well protected and difficult to change or imitate.

**Durability**: The color picture should remain unaltered under all circumstances for a 10-year life time application.

**Flexibility**: Personalization should be possible at a stage later than manufacturing.

**Picture classicism**: The color photo classicism can be appreciated through its pattern, resolution, contrast and color saturation.

**Picture authentication**: It is important for authorities or document checkers at level 1, 2 and 3 to have criteria to authenticate a genuine portrait versus a counterfeited one.

**Cost per document**: Lower is the total cost of ownership of a solution higher is the score.

---

- **Marks**
  - 5 points when the best for a particular criteria
  - 3 points when good
  - 1 point when average
Every technology has strengths and weaknesses

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Black &amp; White in PC</th>
<th>Color in PC at manufacturing</th>
<th>Color on PC</th>
<th>Lasink Color in PC</th>
<th>Sealys Color in PC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Durability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flexibility</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Picture classicism</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Picture authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost per document</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>16</td>
<td>20</td>
<td>18</td>
<td>22</td>
<td>20</td>
</tr>
</tbody>
</table>

Marks

5 points when the best for a particular criteria
3 points when good
1 point when average
Agenda

• Credential security relies on 4 pillars
• Security features of physical credentials
• Portrait vulnerability
• Benchmark of portrait printing processes for polycarbonate
  • Physical credential derivation?
• See Lasink demo on our booth
Do you trust your ID documents?

- Governments spend more and more money to secure always more your identity credential.

Plain ID document with a specific Lasink™ photo

Passport with chip

Let's use your ID document to create your digital ID
How?

Creation of your account

Plain ID

Picture of your Lasink™ photo on your ID:
The application verifies that it is a genuine photo

Photo of you

Passport

Picture of your photo on your passport chip:
The application verifies that it is a genuine document

Photo of you

The application verify that you are the real holder of your genuine document
Once you have created your account, you can connect to your website with a selfie

- Your digital identity created from your identity document is stored in a embedded secure element inside your phone.

- You can connect to your secured website thanks to a selfie

Forgot your dozens of password and trust your digital ID!
Agenda

• Credential security relies on 4 pillars
• Security features of physical credentials
• Portrait vulnerability
• Benchmark of portrait printing processes for polycarbonate
• Physical credential derivation?
  • See Lasink demo on our booth
Questions?