

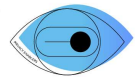
*#EADPPCertification  
WebinarSeries*

# **BOKS Domain C** Information Security

- EADPP  
Certification
- BOKS Domain C
- Q&A

**EADPP**

European association  
of data protection  
professionals

*PRIVACY*   
DATA PROTECTION  
X CERTIFICATION *ENABLERS*

# **EADPP Certification for Data Protection Professionals**

# Aim, Content & Exam

- ▶ Providing a certification that focuses on **how data protection principles can be implemented**, beyond the legal aspects
  - ▶ Structured by a Body of Skills and Knowledge (BOKS) reflecting a holistic approach on data protection and privacy
- ▶ Becoming certified requires **passing the exam**
  - ▶ 40 single-option questions
  - ▶ **Exam package** includes (o.a.)
    - ▶ One online exam
    - ▶ Study book “A Holistic Approach to Data Protection”
  - ▶ **Detailed information** can be found in the Syllabus and Candidate Handbook





# **BOKS Domain C:** Information Security

# Overview

1. Confidentiality – Integrity – Availability (CIA) Triad
2. Open Systems Interconnected (OSI) model
  - ▶ Example
  - ▶ Use case (digital / non-digital)
3. OSI model & Information security
  - ▶ Example
4. Conclusion

## CIA Triad

### *Confidentiality*

Ensures that sensitive information is **accessible only to authorized individuals**. It is achieved through authentication methods like passwords and biometrics.

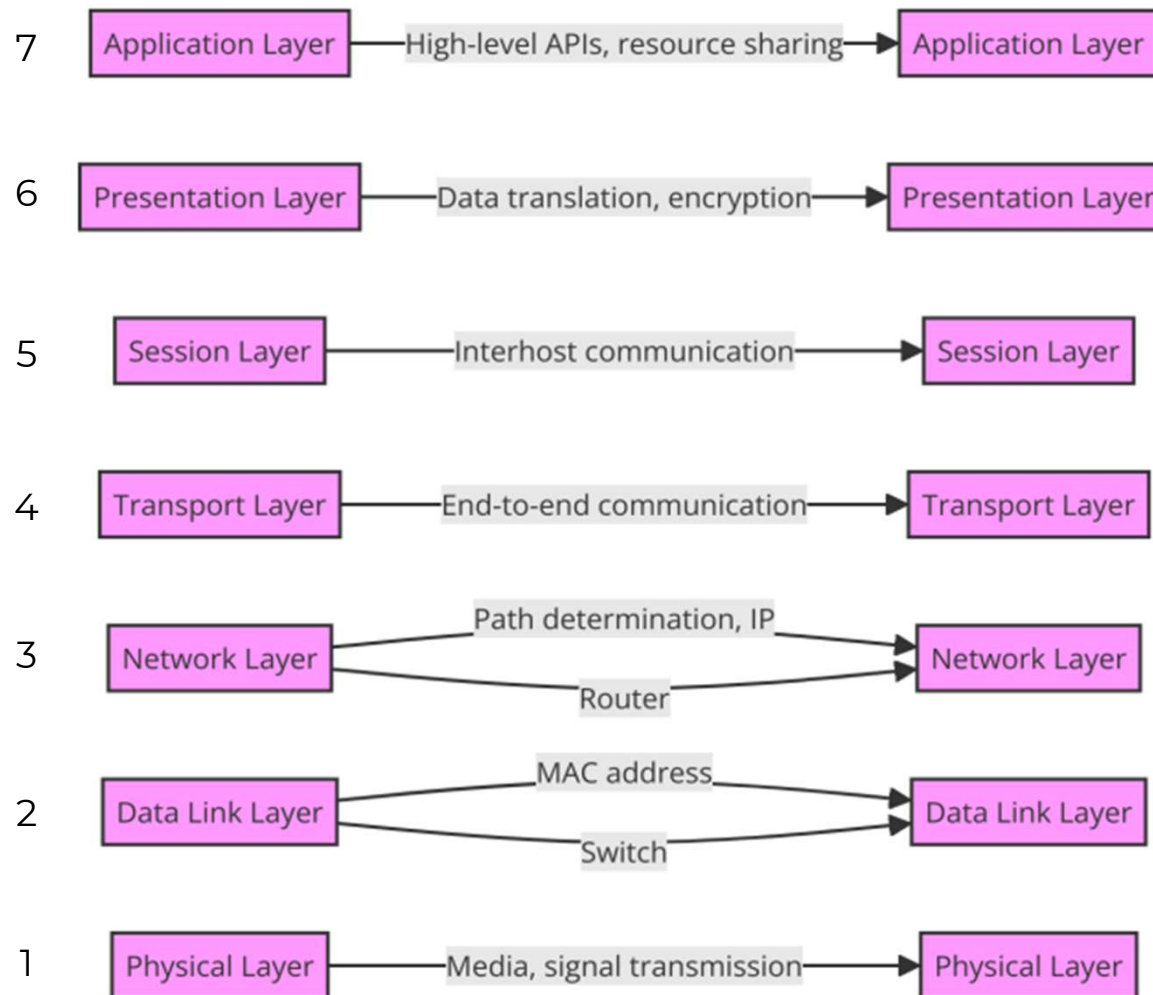
### *Integrity*

Guarantees the **accuracy and reliability of data**, preventing unauthorized modifications. Techniques like hashing and checksums are employed to maintain data integrity.

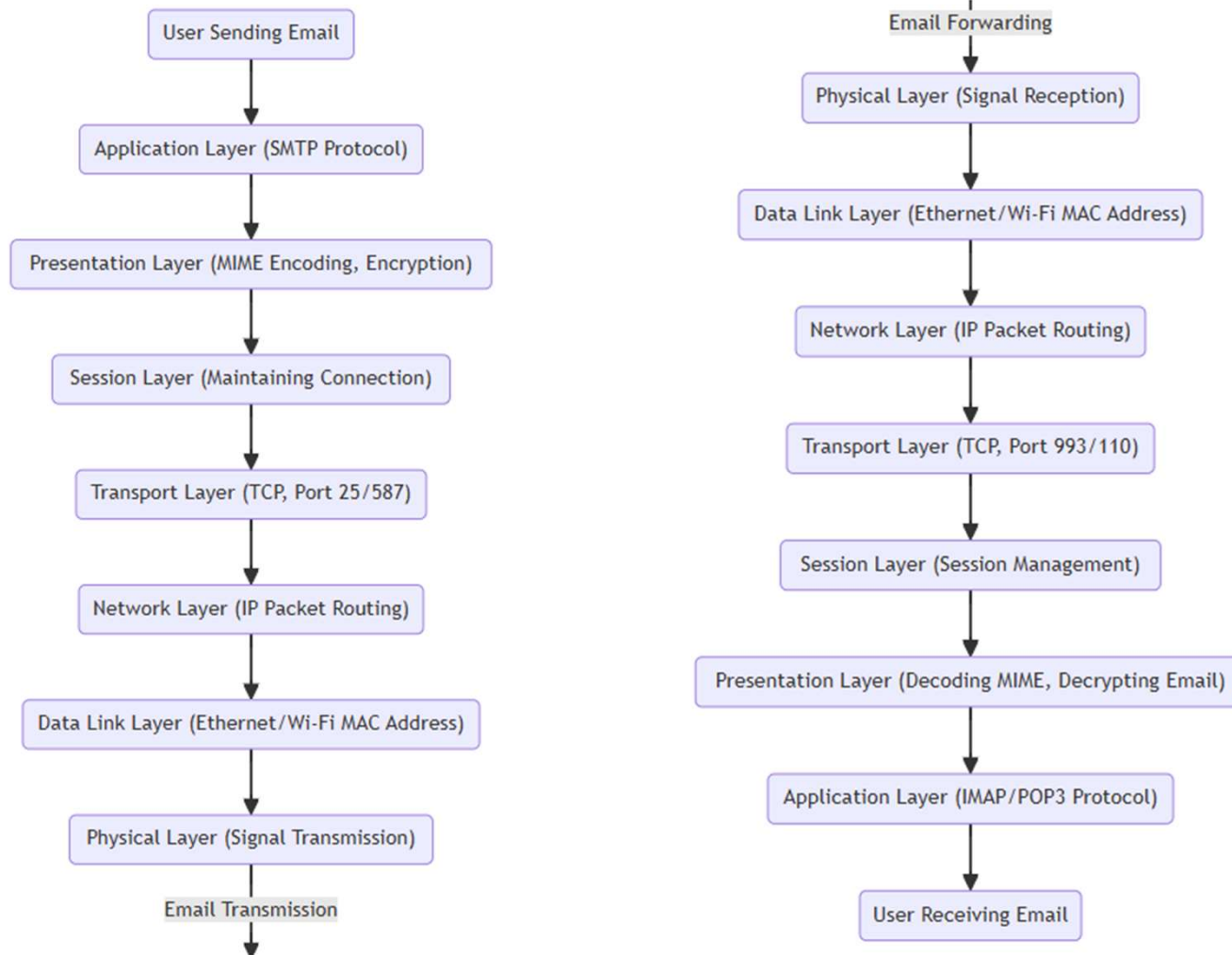
### *Availability*

Ensures that information **systems are operational and accessible** when needed. This is supported by redundancy, backups, and robust disaster recovery plans.

# Open Systems Interconnected (OSI) model



# Example: Sending an email



## Use case

- ▶ The CEO has a document containing private information stored in a physical safe at the company. Only the CEO and CFO are allowed to read this document.
- ▶ The CEO wants to transfer the document to the CFO, who works in a different location.
- ▶ To facilitate this, the CEO scanned the document and stored it on the company's storage (SAN) device.
  - ▶ The physical document can be considered as a backup for the digital version.

Non-digital



Digital



## Non-digital use case (1/3)

<i>OSI layer</i>	<i>Reference model</i>	<i>People</i>	<i>Processes</i>	<i>Risk</i>	<i>Prevention</i>
<b>Layer 1 (Physical)</b>	Paper document in a safe located in a house	Document accessed by one person alone or with two persons	Putting the document in safe or taking it out	Person who puts document in safe can change its content, document gets lost, key gets lost, theft, fire, flooding	Minimum of two people to put document in the safe, dedicated safe location for key storage, humidity control, ensuring safe is secure in the house, making a copy of the document and store in another location, "geese police" to protect the area around the house, digitize the document as backup for non-digital version

## Non-digital use case (2/3)

<i>OSI layer</i>	<i>Reference model</i>	<i>People</i>	<i>Processes</i>	<i>Risk</i>	<i>Prevention</i>
<b>Layer 2 (Data link)</b>	–	–	–	–	–
<b>Layer 3 (Network)</b>	Roads	Driving	Walking into room with safe, driving to CFO	Key theft, accident	Perimeter protection around room with safe, driving safely
<b>Layer 4 (Transport)</b>	By post or car	Postman or driver	Walking	Document gets lost	Registered post mail
<b>Layer 5 (Session)</b>	–	–	–	–	–

## Non-digital use case (3/3)

<i>OSI layer</i>	<i>Reference model</i>	<i>People</i>	<i>Processes</i>	<i>Risk</i>	<i>Prevention</i>
<b>Layer 6 (Presentation)</b>	Are they aware that storing in a humid area degrades paper quality? (data integrity)	Handwriting with ink	Signing the document	Document gets less easy to read over time	Guarantee data integrity by storing the document in a dry room away from UV light
<b>Layer 7 (Application)</b>	Key to open the safe, read the document	Only the CEO alone or with two admins of the CEO	Open safe, take the document	Admins can take or read the document, or make copies	Lock room, minimum of two persons required when opening the safe

## Digital use case (1/3)

<i>OSI layer</i>	<i>Reference model</i>	<i>People</i>	<i>Processes</i>	<i>Risk</i>	<i>Prevention</i>
<b>Layer 1 (Physical)</b>	SAN device and scanner device, Wi-Fi, notebook	–	Scan, verify integrity and store document on SAN device	Storage device can be stolen or hacked, storage device with same name (cybercrime), virus or malware	Install SAN device in physically protected area with a digital certificate, install scanner in a locked room, install sensors for flooding, fire, etc., install cameras
<b>Layer 2 (Data link)</b>	MAC	–	Switching	Cyber risks	VLAN segmentation

## Digital use case (2/3)

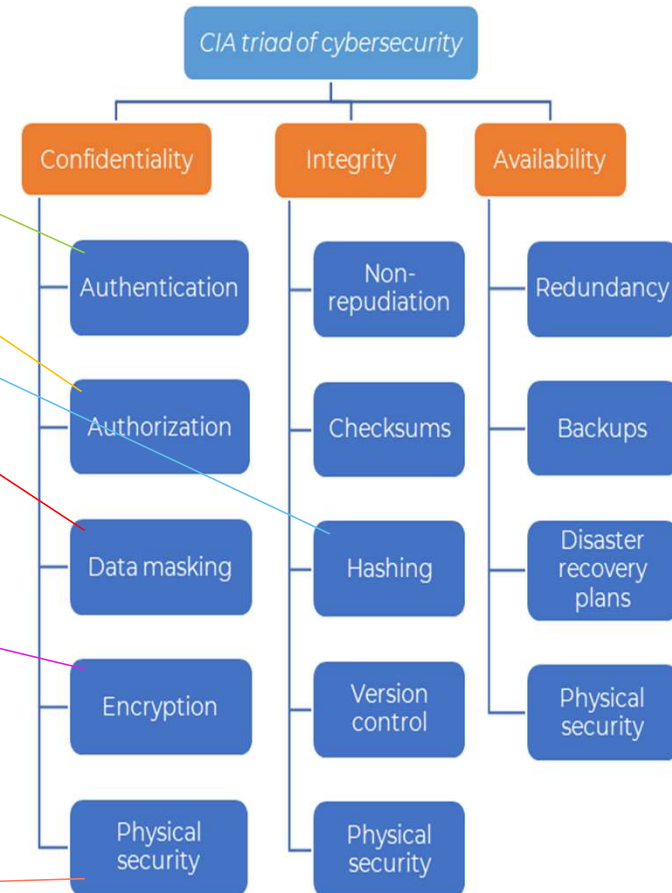
<i>OSI layer</i>	<i>Reference model</i>	<i>People</i>	<i>Processes</i>	<i>Risk</i>	<i>Prevention</i>
<b>Layer 3 (Network)</b>	IP	–	Routing	Cyber risks	Next-generation firewall (NGFW), network segmentation
<b>Layer 4 (Transport)</b>	TCP, SSL (for encryption)	–	Monitor uptime of storage device	Network outage, no encryption	Use encryption for transport and storage of data
<b>Layer 5 (Session)</b>	–	–	Session control	Outage	Redundancy

## Digital use case (3/3)

<i>OSI layer</i>	<i>Reference model</i>	<i>People</i>	<i>Processes</i>	<i>Risk</i>	<i>Prevention</i>
<b>Layer 6 (Presentation)</b>	PDF format	–	Digitally sign the document	PDF file can get corrupted or become unreadable, data Integrity issues due to SAN software bug	Hash PDF file, backup PDF file, update SAN software
<b>Layer 7 (Application)</b>	PDF viewer	Username	Read the file using PDF viewer	Other people can read the document, people can email or scan the document, virus on notebook, user access control	Screen or privacy protector for notebook, hash PDF document, install virus scanner, authentication and authorization of users

# OSI model & Information security

- [Layer 7 - Application] 🌐 (User Interaction & Security)
  - IAM (Identity & Access Management) ✓
  - Web apps, email, APIs
  - Security: WAF, input validation
  - GDPR: Data Subject Rights, Consent
- ↓
- [Layer 6 - Presentation] 🗝️ (Data Encryption & Privacy)
  - PETs (Privacy-Enhancing Technologies) ✓
  - SSL/TLS, encoding, compression
  - Security: Encryption, Data masking
  - GDPR: Data Confidentiality, Encryption (Art. 32)
- ↓
- [Layer 5 - Session] 🔑 (Authentication & Secure Sessions)
  - IAM (Multi-Factor Authentication, SSO) ✓
  - Secure user sessions, login management
  - Security: MFA, token-based auth
  - GDPR: Secure access controls (Art. 25 - Privacy by Design)
- ↓
- [Layer 4 - Transport] 📦 (Data Integrity & Delivery)
  - Secure data in transit, TCP, UDP
  - Security: TLS, transport encryption
  - GDPR: Secure communication (Art. 32)
- ↓
- [Layer 3 - Network] 📶 (Routing, Cloud Networking, and Access Control)
  - Cloud Computing (Networking & Connectivity) ✓
  - Firewalls, VPNs, IPsec
  - Security: DDoS mitigation, packet filtering
  - GDPR: Cloud network security & risk mitigation
- ↓
- [Layer 2 - Data Link] 🌐 (Network Infrastructure)
  - VLANs, MAC filtering
  - Security: Segmentation, Switch security
  - GDPR: Data flow control for privacy compliance
- ↓
- [Layer 1 - Physical] 🏢 (Cloud Data Centers & Infrastructure)
  - Cloud Computing (Infrastructure as a Service - IaaS) ✓
  - Cables, routers, servers
  - Security: Server locks, biometric access
  - GDPR: Physical security controls for cloud providers

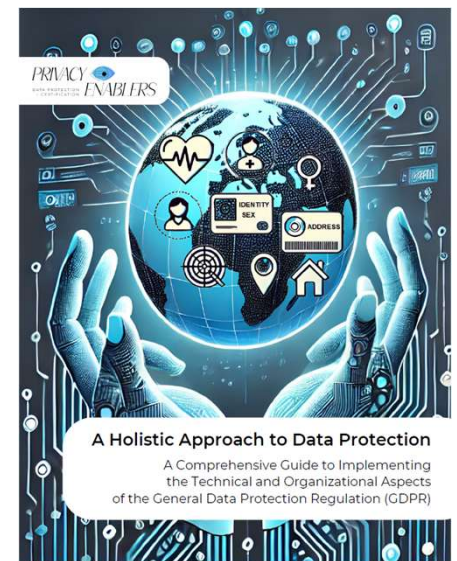


# Example: Assessing the Attack surface in Layer 7 (Application Layer)

<i>OSI layer</i>	<i>Process</i>	<i>Risk</i>	<i>Mitigation</i>
<b>Layer 7 (Application)</b>	<ul style="list-style-type: none"> <li>- User interaction</li> <li>- Protocols (e.g., HTTPS, SMTP, FTP, SSH, DNS, Telnet, POP3, IMAP)</li> <li>- API</li> <li>- Rest/Soap</li> </ul>	<ul style="list-style-type: none"> <li>- Email spoofing</li> <li>- False domain identity</li> <li>- Brute force attacks</li> <li>- Phishing</li> <li>- False identity</li> <li>- MitM attacks</li> <li>- DDoS</li> <li>- Configuration mistakes</li> <li>- Zero-Day Exploits</li> <li>- XSS</li> <li>- SQL injection</li> <li>- CSRF/XSRF</li> </ul>	<ul style="list-style-type: none"> <li>- SPF, DKIM, DMARC.</li> <li>- Certificate (digital signatures)</li> <li>- DNSSEC</li> <li>- Use strong encryption</li> <li>- Awareness</li> <li>- WAF</li> <li>- Application-aware segmentation</li> <li>- Container network segmentation</li> <li>- Virtual Private Network (VPN)</li> <li>- Micro-segmentation</li> <li>- Content Security Policy (CSP)</li> <li>- Parameterized queries</li> <li>- CSRF token</li> <li>- Samesite cookie</li> </ul>

# Conclusion

- ▶ The OSI model can **help structure data protection needs** by breaking down security measures layer by layer
  - ▶ This ensures a comprehensive, multi-layered security approach that addresses threats at every level of data transmission
- ▶ Our **Study Book** provides an overview of security threats at each layer and explains how to mitigate them



## Q&A

- ▶ Questions?
- ▶ Comments?



# Planning upcoming webinars

- ▶ **BOKS Domain D:** Action Plan – How

- ▶ Tuesday, 18 March 2025 at 11am CET

- ▶ Registration link: <https://events.teams.microsoft.com/event/4747f13b-a74c-4ee5-a439-f1d9fa19ac15@8b75739f-c4ad-49d3-baaa-74bbf671c99a>

- ▶ **BOKS Domain E:** Privacy Culture – Human Perspective

- ▶ Tuesday, 15 April 2025 at 11am CET