CRYPTOGRAPHY AND STEGANOGRAPHY

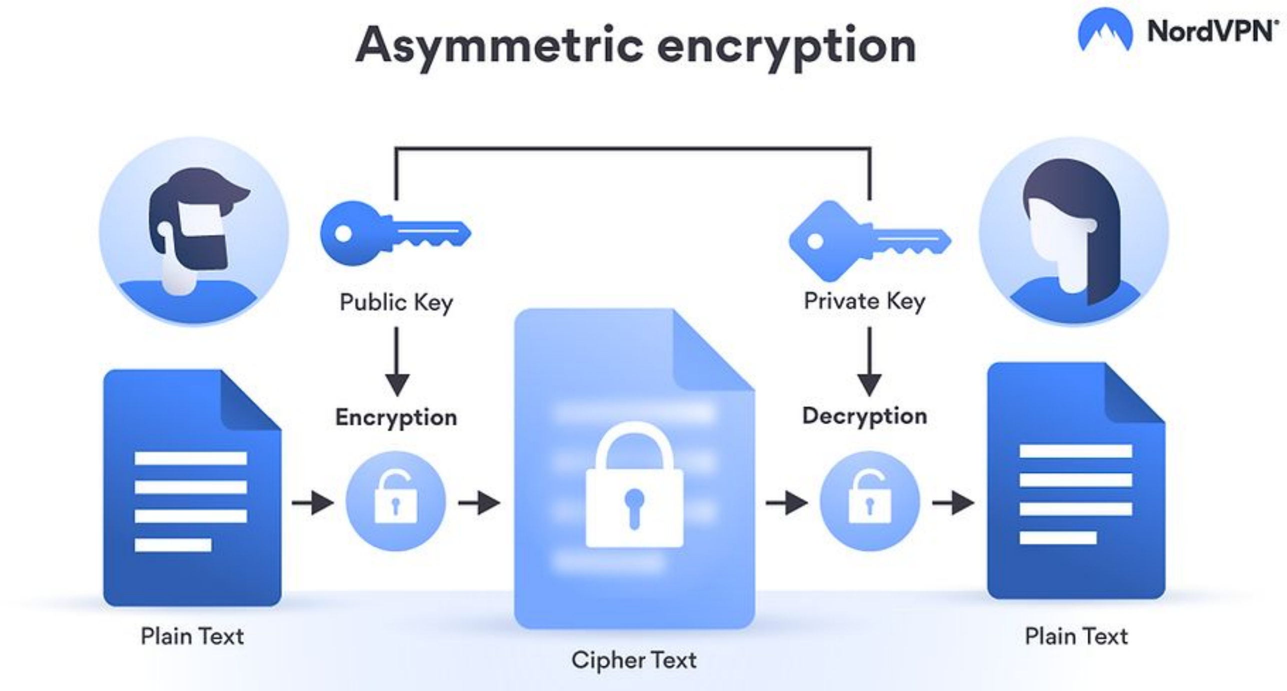
Department of Informatics

Sesi 6 – Cryptography Implementation for Personal Data Protection

Abdul Azzam Ajhari, S.Kom., M.Kom.

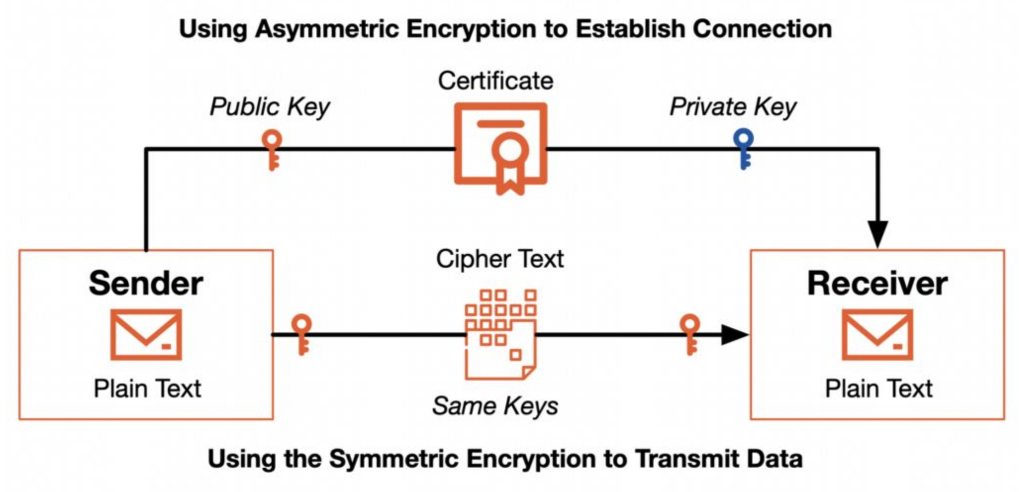
Refreshment Sesi 5

Asymmetric cryptography is also known as public key cryptography. It is the most popular cryptographic method to encrypt and decrypt messages to provide data security in most communication networks. A pair of different keys are used: public and private keys.

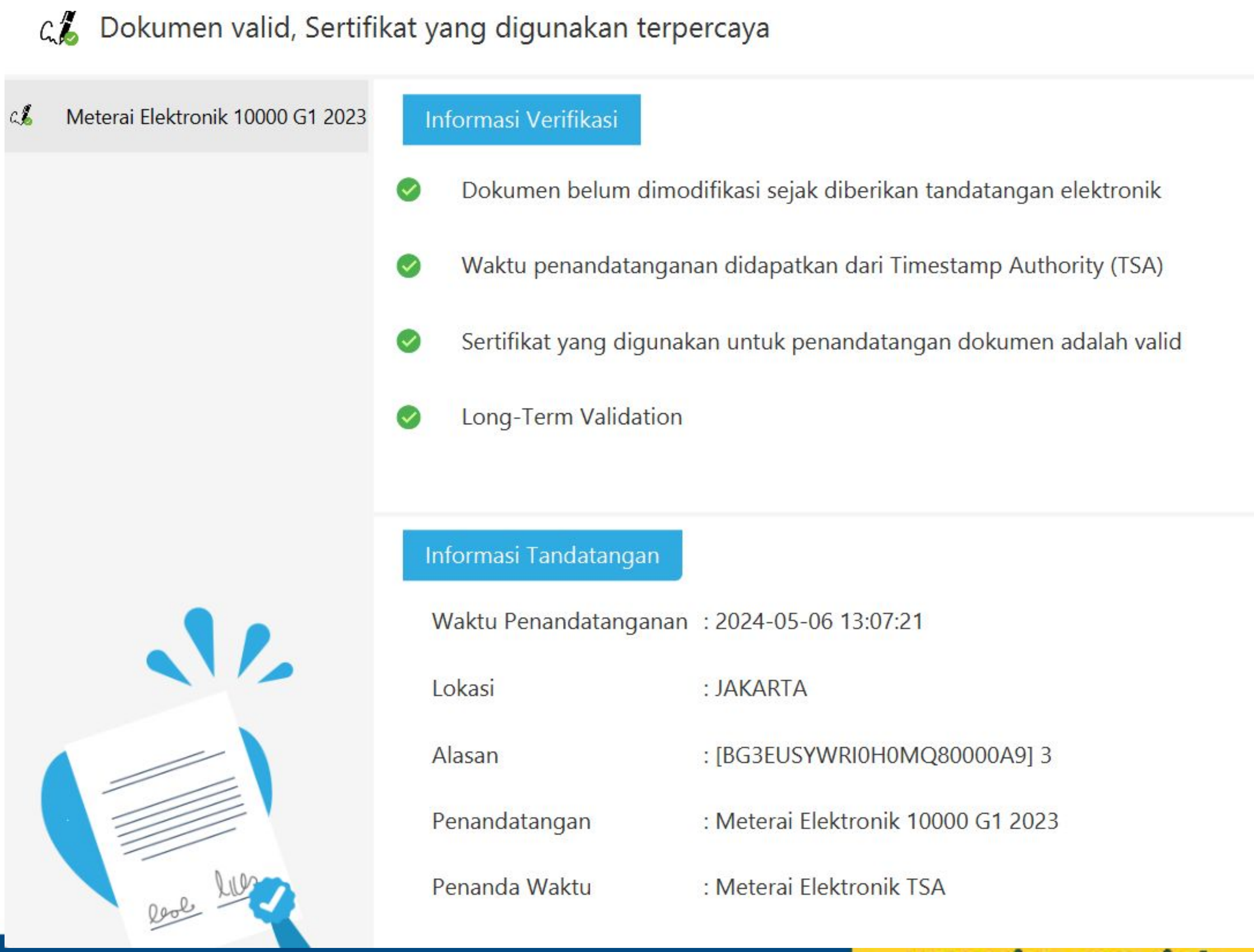


https://www.sciencedirect.com/topics/computer-science/asymmetric-cryptography

Kriptografi Asymmetric in Daily Life


Using Asymmetric Encryption to Establish Connection
Certificate
Public Key
Private Key
Sender
Plain Text
Cipher Text
Receiver
Plain Text
Same Keys
Using the Symmetric Encryption to Transmit Data

Sumber gambar: Tetrate


Dokumen valid, Sertifikat yang digunakan terpercaya

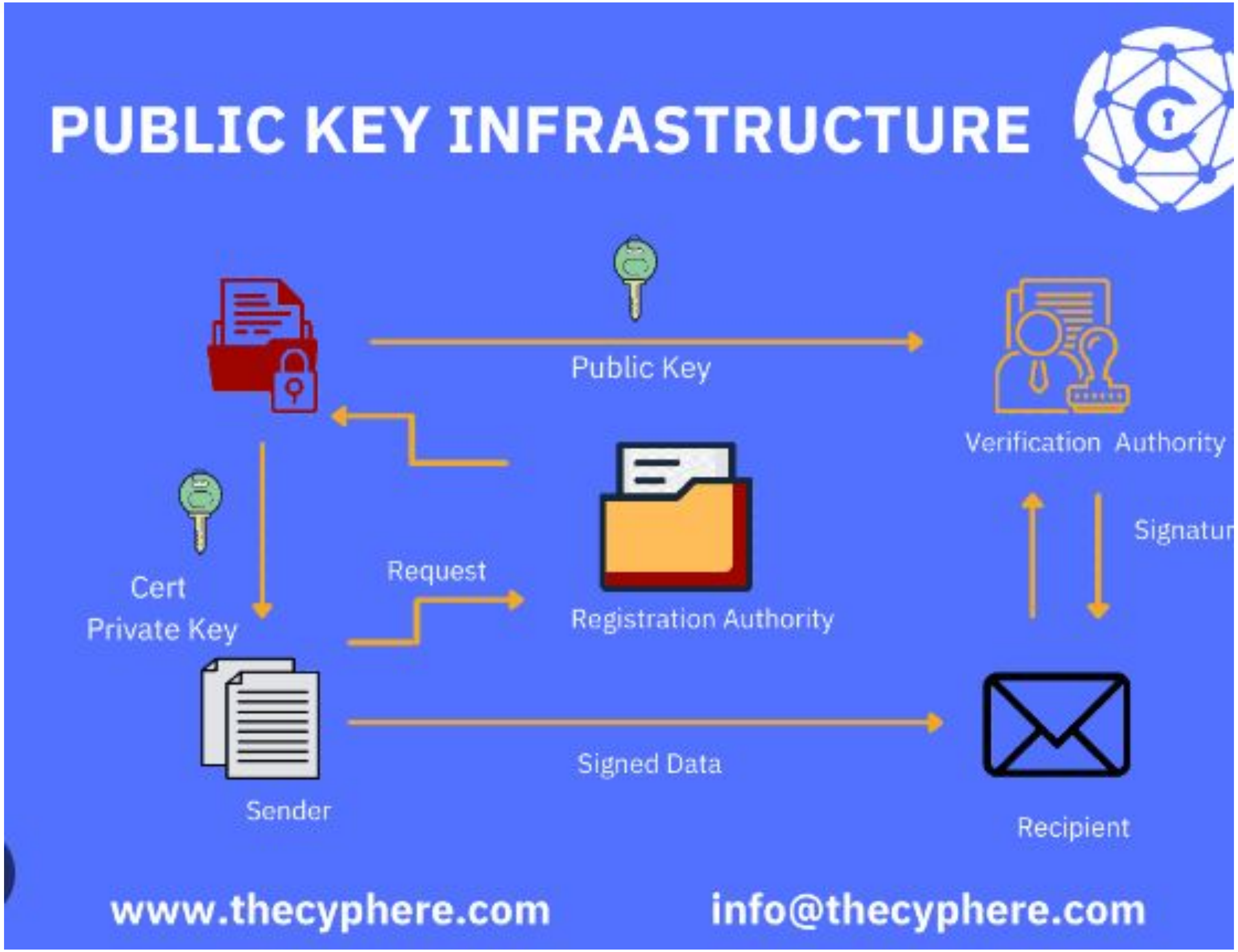
Meterai Elektronik 10000 G1 2023

Informasi Verifikasi

- ✓ Dokumen belum dimodifikasi sejak diberikan tandatangan elektronik
- ✓ Waktu penandatanganan didapatkan dari Timestamp Authority (TSA)
- ✓ Sertifikat yang digunakan untuk penandatangan dokumen adalah valid
- ✓ Long-Term Validation

Informasi Tandatangan

Waktu Penandatanganan	: 2024-05-06 13:07:21
Lokasi	: JAKARTA
Alasan	: [BG3EUSYWRI0H0MQ80000A9] 3
Penandatangan	: Meterai Elektronik 10000 G1 2023
Penanda Waktu	: Meterai Elektronik TSA



PUBLIC KEY INFRASTRUCTURE
Public Key
Verification Authority
Signatur
Cert
Private Key
Request
Registration Authority
Sender
Signed Data
Recipient
www.thecyphere.com
info@thecyphere.com

Cryptography Implementation for Personal Data Protection

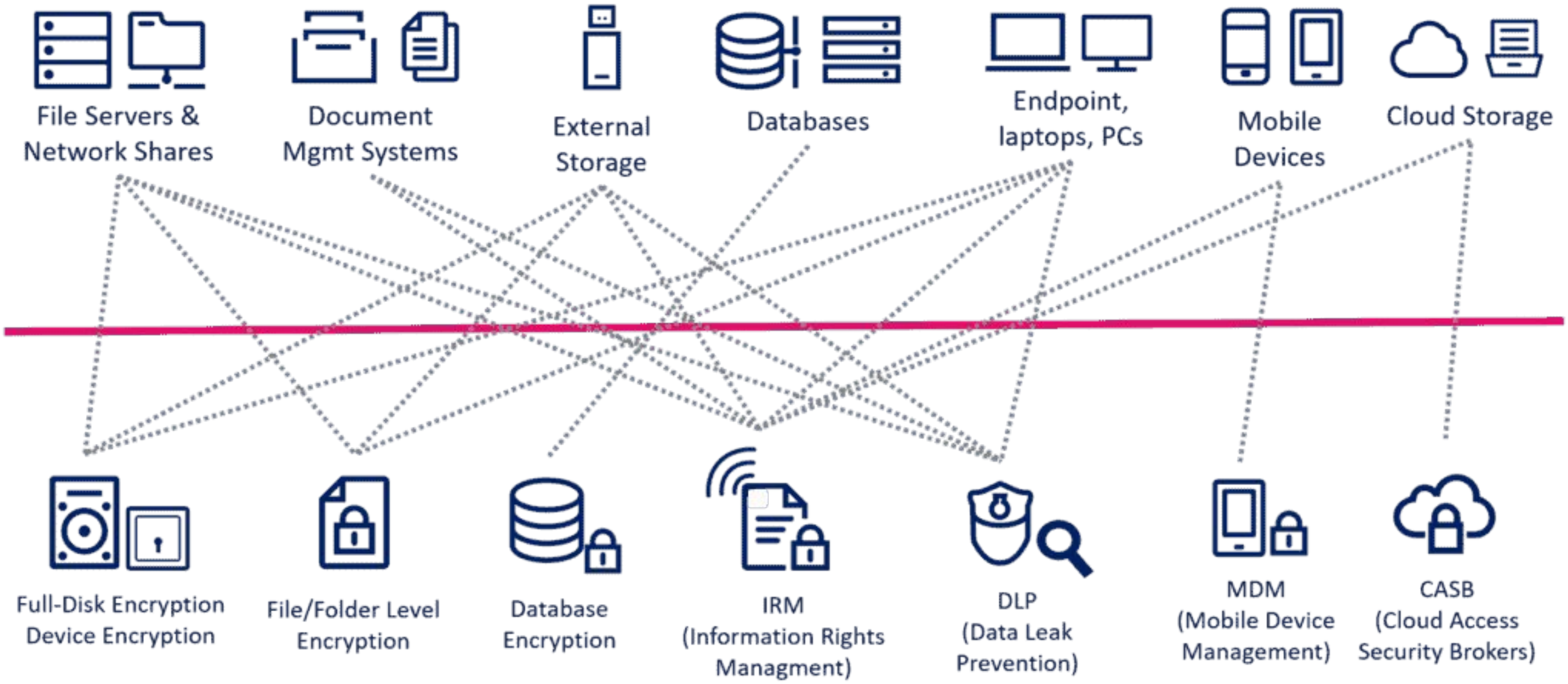
THE THREE STATES OF DATA

AT REST

IN TRANSIT

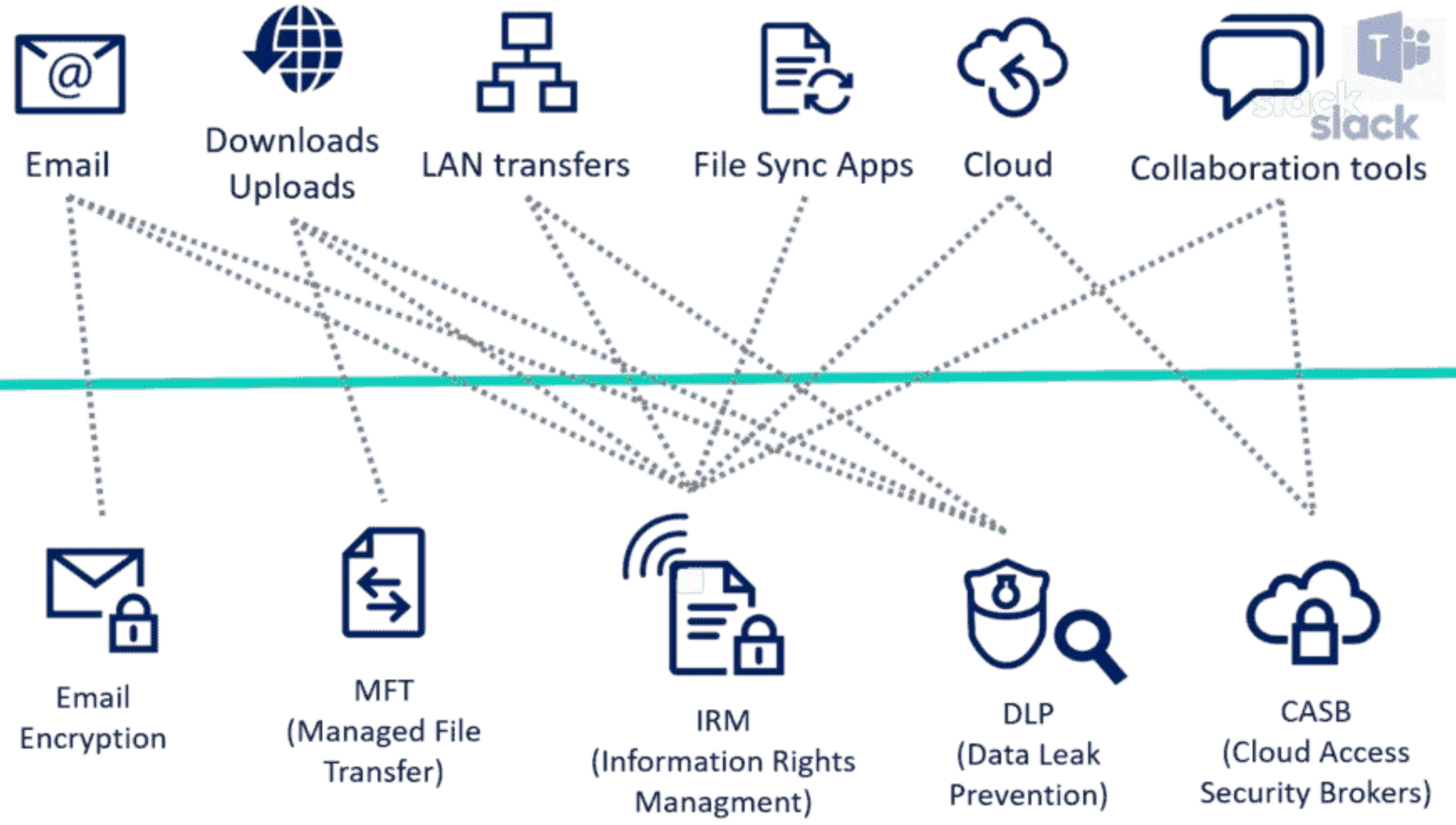
IN USE

PROTECTING DATA AT REST


File Servers & Network Shares
Document Mgmt Systems
External Storage
Databases
Endpoint, laptops, PCs
Mobile Devices
Cloud Storage
Full-Disk Encryption Device Encryption
File/Folder Level Encryption
Database Encryption
IRM (Information Rights Managment)
DLP (Data Leak Prevention)
MDM (Mobile Device Management)
CASB (Cloud Access Security Brokers)

https://www.sealpath.com/blog/protecting-the-three-states-of-data/

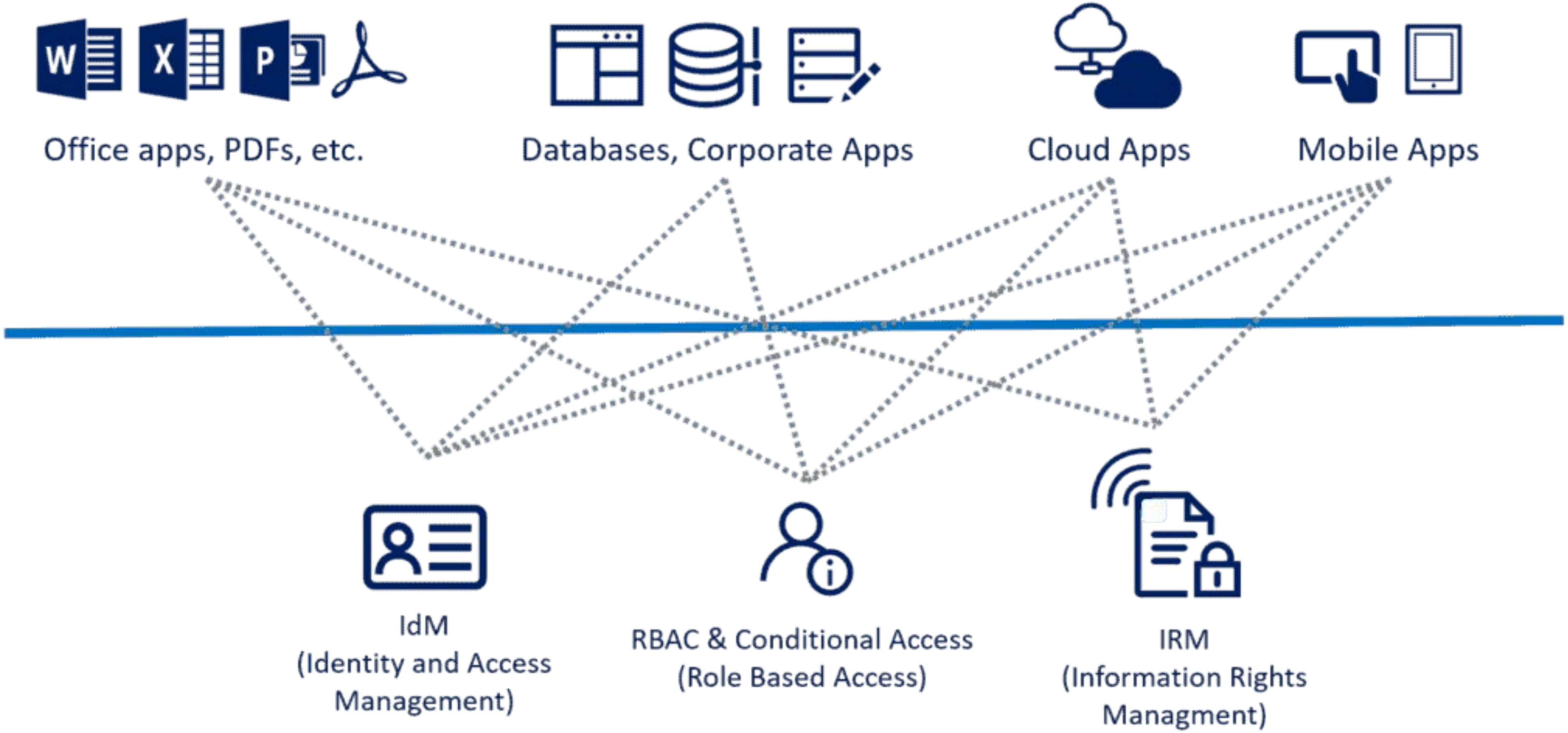
PROTECTING DATA IN TRANSIT



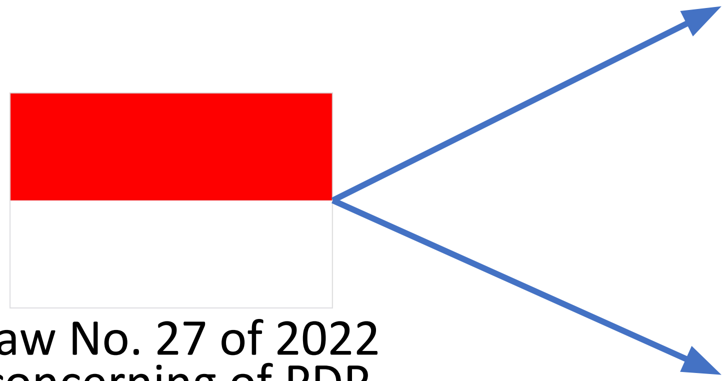
Email
Downloads Uploads
LAN transfers
File Sync Apps
Cloud
slack
Collaboration tools
Email Encryption
MFT (Managed File Transfer)
IRM (Information Rights Managment)
DLP (Data Leak Prevention)
CASB (Cloud Access Security Brokers)

https://www.sealpath.com/blog/protecting-the-three-states-of-data/

PROTECTING DATA IN USE



https://www.sealpath.com/blog/protecting-the-three-states-of-data/



Law No. 27 of 2022 concerning of PDP

General

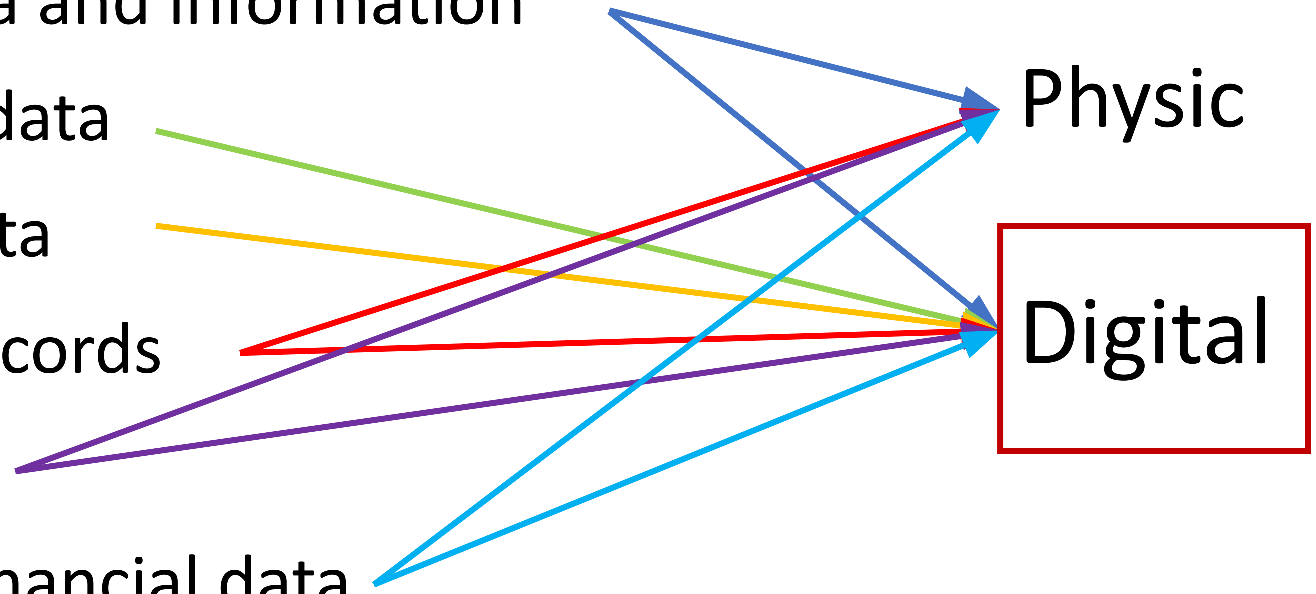
Full name, gender, nationality, religion, marital status

Spesific

Health data and information, biometric data, genetic data, criminal records, child data, personal financial data

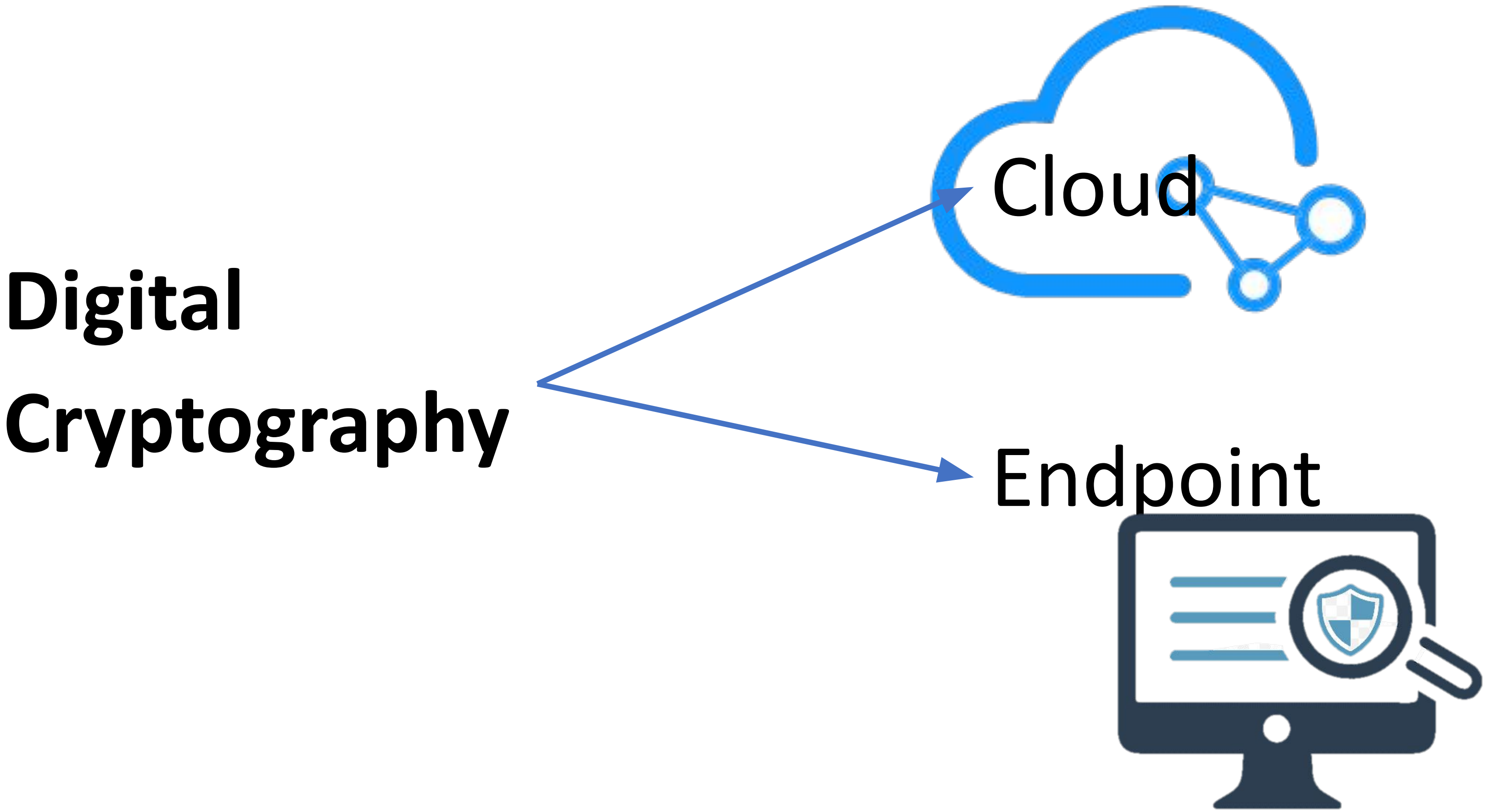
Spesific

1. Health data and information
2. Biometric data
3. Genetic data
4. Criminal records
5. Child data
6. Personal financial data



Physic

Digital

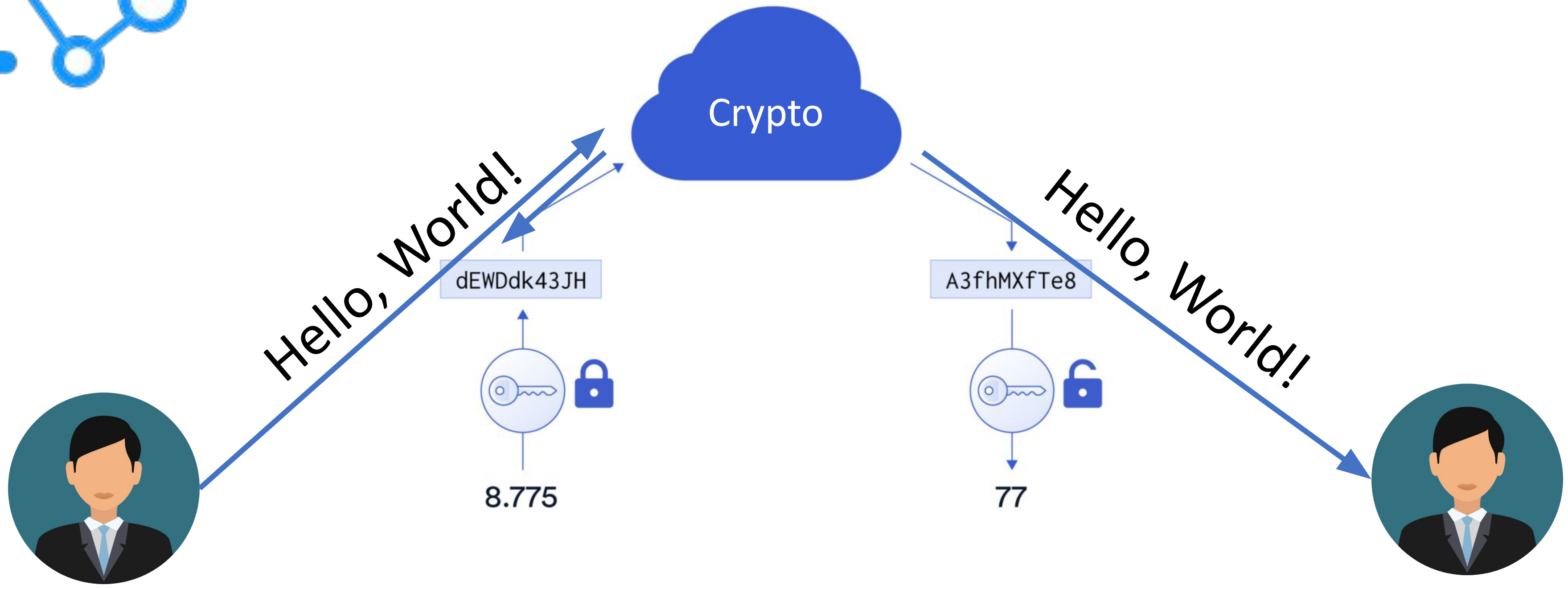


Digital Cryptography

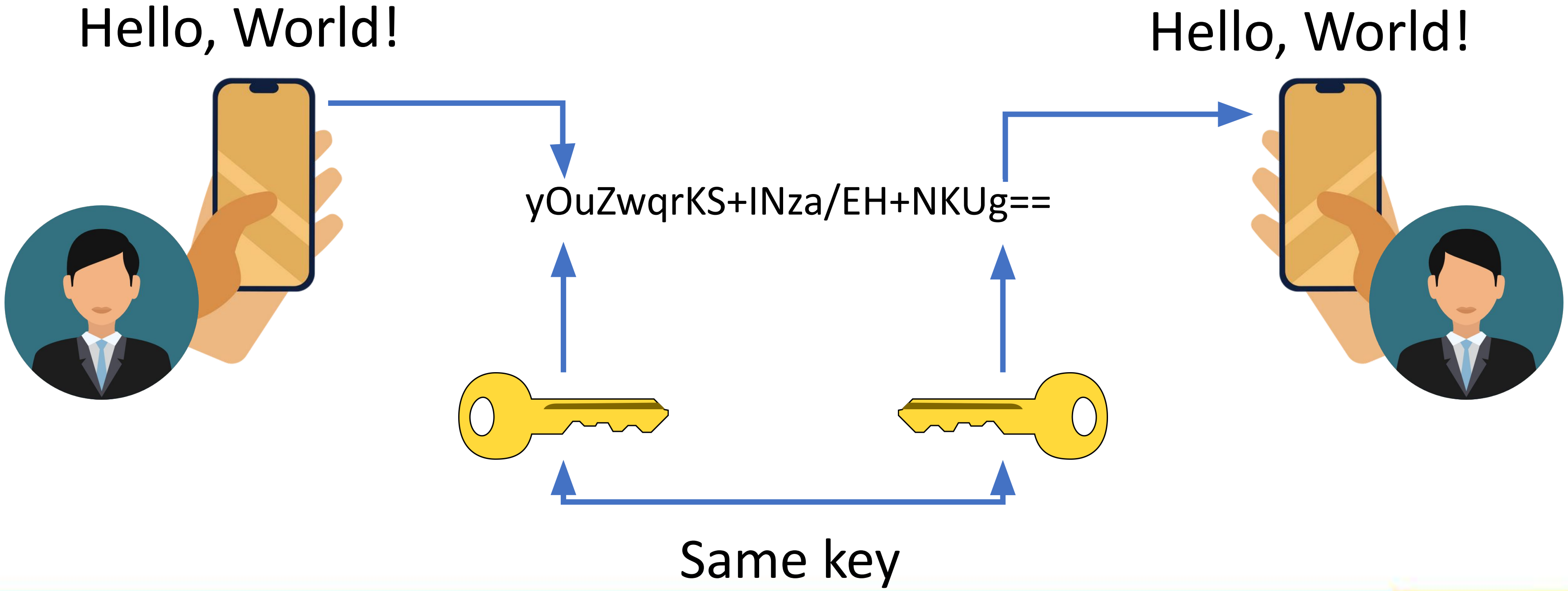
Cloud

Endpoint

Cloud


Hello, World!
dEWDdk43JH
8.775
Crypto
A3fhMXfTe8
77
Hello, World!

Endpoint



Hello, World!

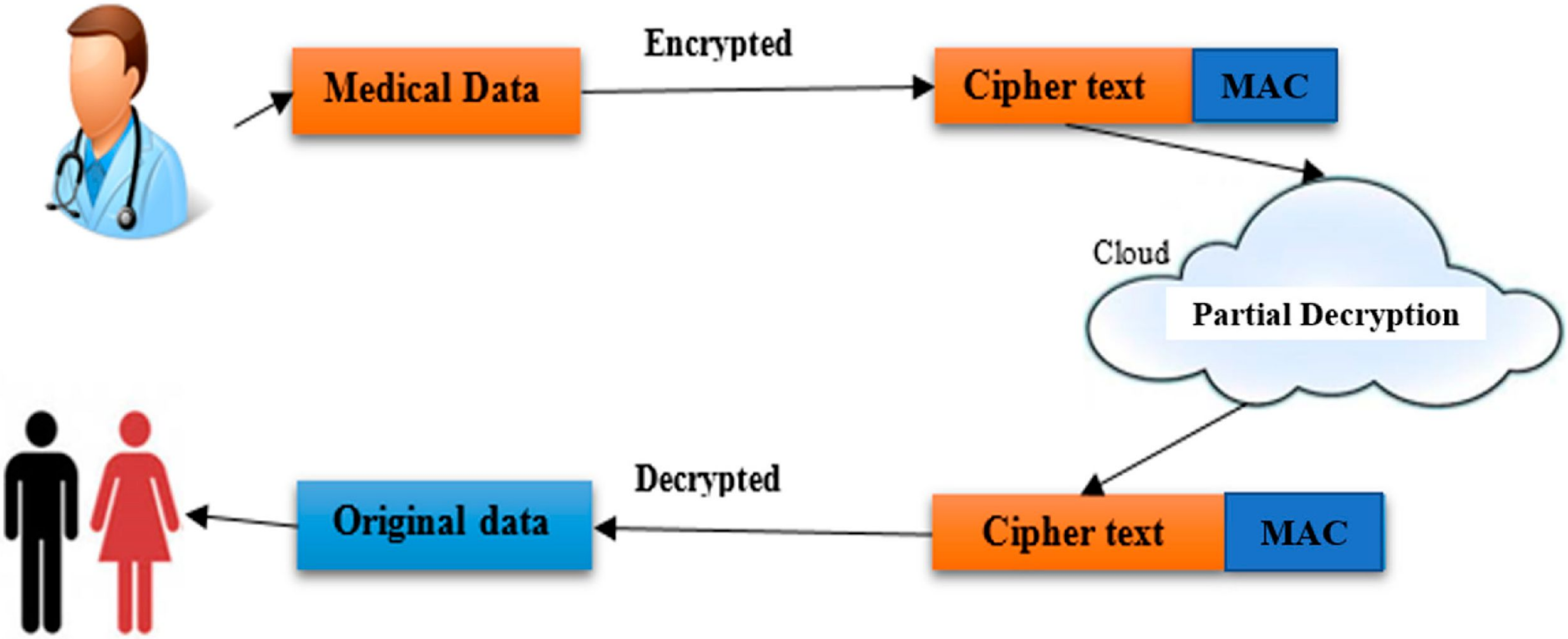
yOuZwqrKS+INza/EH+NKUg==

Hello, World!

Same key

No	Cloud	Endpoint
1.	Protects data while it's stored on cloud servers	Protects data on the user's device before it is uploaded to the cloud.
2.	Allows for secure data sharing across different locations.	Provides an additional layer of security by encrypting sensitive information locally.
3.	Managed by the cloud provider, who handles key generation and management.	Can be more user-managed, depending on the device and application.

Dual Authentication-Based Encryption with a Delegation System to Protect Medical Data in Cloud Computing



https://www.mdpi.com/2079-9292/8/2/171

- Computer Security Principles and Practice Third Edition, William Stallings and Lawrie Brown, Pearson, 2012
- Introduction to computer security, Matt Bishop, Addison Wesley, 2005
- Computer Networking: A Top Down Approach 6th edition Jim Kurose, Keith Ross, and Addison-Wesley
- https://www.ericsson.com/en/blog/2021/7/cryptography-and-privacy-protecting-private-data
- https://selembardigital.com/pelajari-semua-tentang-cryptocurrency-kriptografi-bagaimana-cara-kerjanya/
- https://learning.quantum.ibm.com/course/practical-introduction-to-quantum-safe-cryptography/cryptographic-hash-functions
- Katz, J., & Lindell, Y. (2007). Introduction to Modern Cryptography: Principles and Protocols. CRC Press.
- Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
- Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th Edition). Pearson.
- National Institute of Standards and Technology (NIST) - Publications on Secure Hash Standards (SHS)