SEAL Project
StudEnt And citizen identities Linked

Enabling identity reconciliation and self-sovereign data management

EUNIS 21

June 10th 2021, Virtual Athens

GRANT AGREEMENT UNDER THE CONNECTING EUROPE FACILITY (CEF) - TELECOMMUNICATIONS SECTOR AGREEMENT INEA/CEF/ICT/A2018/1633170.
Action No: 2018-EU-IA-0024

Introduction

StudEnt And citizen identities Linked

- Project Duration: **27 months** (April 2019 – June 2021)
- Project partners:

UNIVERSITY OF THE AEGEAN

UNIVERSITAT JAUME I

UNIVERSIDAD DE MÁLAGA

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

Background

The Digital Education Agenda

European Parliament call *"to create a European Student eCard which would grant the status of EU student in a mobility context and offer access to services".*

Overall objectives:

- To enable students to identify themselves in a trusted manner
- Once-only principle
- Create a recognisable European Student identity
- Connect digitally the information systems of higher education institutions
- Allow the exchange of academic student data
- Digitalise administrative processes of managing student mobility

Background

European Student Card Initiative

- DG EAC & CNECT promote synergies between Erasmus+ & CEF projects for a common solution
- Create a unique student e-identifier
- Enable institutions to exchange student data & manage student mobility in streamlined processes
- Enable students to apply for and manage their mobility and access student e-services
- Securely share authenticated personal data and qualifications (ECTS)
- Smartphone access

Business Objectives

- Enable interoperability between eIDAS and Higher Education/Research (eduGAIN, ESC) e-identity schemes/ecosystems
- Provide an Identity Linking Service for HEI service providers, support for management of interlinking of different identities and attributes, and support for integration of these services.
- Empower students by giving them control over their data and promote mobile access to usable, self-managed linked identities, as well as the rights/control over their personal data
- Build the means to support trusted 3rd party matching of a user´s multiple e-identities, that could be reused in different scenarios

SEAL Service

SEAL project has two major technical goals:

- **Put the user in the centre of the data management**
  - Self-sovereign identity
  - Secure and trusted user-domain data storage
  - Verifiable Claims
  - Identity Derivation
  - Federated access to data
- **Normalise and optimise the reconciliation of identities**
  - Framework for IPV service interaction
  - Internal reconciliation mechanisms (automated and officer-aided)
  - Progressive framework for linking trust
  - Link data as a service

Design Goals

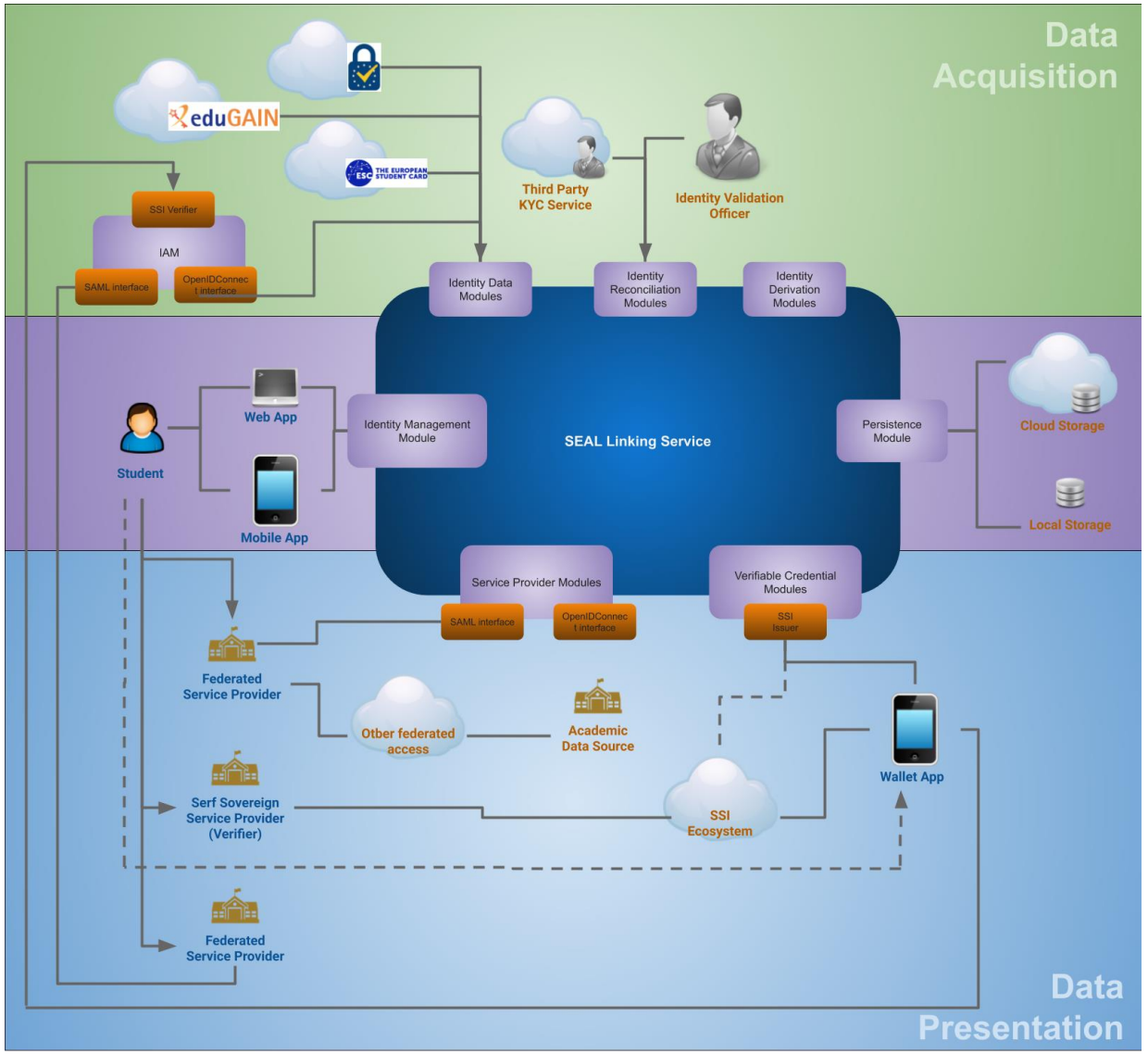
Functional:

- Offer a reference infrastructure for the management of identities and IPV
- Allow connecting new identities, service modules, IPV methods, etc.
- Minimise risk on data by avoiding central storage
- User always has control of his own data
- Enforce establishing progressively stronger links between identities
- Form a virtually single identity

Technical:

- Support both federated and self-sovereign approach to data gathering and delivery
- Develop a modular, extensible, scalable application

Architecture Diagram



SEAL Solution

- **Identity Management Module**: main business logic of the service, interacts with user interface.

- **Identity Data modules**: to obtain delegated authentication or retrieve trusted user data sets (Users can add available digital identities to their identity store: eIDAS, eduGAIN, European Student Identifier, orcID, ePassport, etc.).

- **Identity Reconciliation Modules**: Receive requests and implement a trusted mechanism to establish to which assurance level two datasets belong to the same individual, through comparisons or additional validation data request. Validation methods may be local or remote, automated, semi-automated or manual.

SEAL Solution

- **Identity Derivation Modules**: allow generating new identifiers strongly linked to the authenticated identity. They can be used to mitigate credential theft in specific use cases, and to prevent traceability or provide anonymity to a user while still having the trust of a strong identity being behind.

- **Service Modules**: e-Services consume the delegated authentication and/or the identity linking information, to grant access to the user and establish a relationship between data sets received from different sources.

- **Verifiable Claim Generation Modules**: Self-Sovereign Identity reduces dependency on the infrastructure, so these modules allow to generate standard self-validating objects containing the data sets and the linking information. This way, Consumers can receive this objects offline, without relaying directly on the SEAL service.

Service Characteristics

SEAL service design:

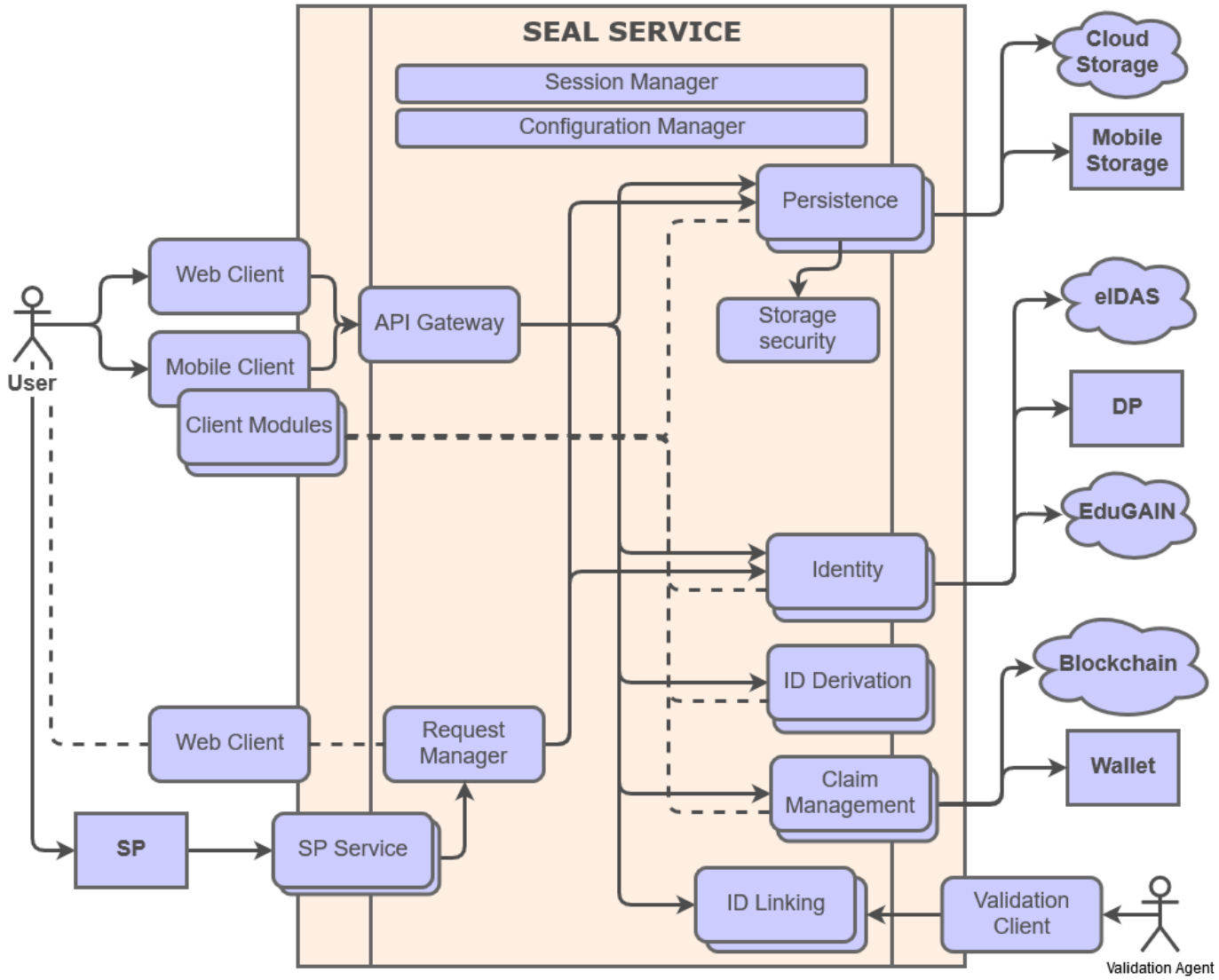
- Microservice-based architecture
- Two main clients: web and mobile, connect to the service through API
  - Most of the functionality will be server-side. Clients have minimal logic
  - Mobile client has some more functionalities than web client
- User data is stored on user-space storage
  - Data is stored only when (and if) user commands to (usage can be volatile and anonymous)
  - **No storage of personal data, not even on reconciliation modules**
    - **Ciphered sessions**
- A user can access different instances of SEAL carrying his own data with him
  - Different instances can have different functional modules connected (identities, identity linking procedures, etc.)

Use Cases

SEAL Service allows the user to:

- Set-up or load a persistence storage
- Retrieve identity data from a source
- Store the retrieved data on a persistence store
- Request establishing a trusted link between two retrieved data sets
- Move data between persistence storages
- Generate derived identifiers
- Generate a Verifiable Claim from the data in storage and store it on a wallet
- Allow a requesting SP to consume data from the sources or the storage
- One of the sources is a SSI VC validator

Modular Design



Modules

Authentication/Data sources:

- eIDAS, EduGAIN, Machine-readable travel documents, SSI Wallet

Link modules:

- Automated linking, Remote officer validation

Service modules:

- SAML2, OIDC, UPort VC issuer

Storage modules:

- Cloud Storage, mobile storage, local file storage, browser storage

Derivation modules:

- Random UUID module, combined datasets

eID Linking

- Move the effort of binding two datasets away from the data consumer
- We define the Linking level of assurance (LLoA)
- The data consumer will receive a security assertion issued by SEAL with the LLoA
- The assertion states that:
  - *For dataset A belonging to subject A and issued by data provider A*
  - *For dataset B belonging to subject B and issued by data provider B*
  - *Subject A and subject B are the same individual*
  - *With a certainty level of L*

Link Trust

- Links follow transitive property:
  - *If we have an AB link and a BC link then we have an AC link*
  - *Resulting AC LLoA is the minimum value in the chain*
- Datasets have a LoA that depends on their source, and their bind has a LLoA
  - Consumers must infer the trust from both the LoA of the sets and the LLoA of the link

Linking Level of Assurance

- Proposal of 5 Levels
- Level 3-5 paired with the requirements for the eIDAS EC Implementing Act 2015/1502, Annex 2.1
- Level 1-2 for usage below government-agency grade assurance

Linking Level of Assurance

Level	Name	Description
0	*self*	User self-stated link (default)
1	*basic*	Basic verifications on the link. Mostly automated or non-accountable.
2	*enhanced*	Improved verifications on the link, involving human agents and records.
3	*low*	eIDAS LoA level low enrolment requirements
4	*substantial*	eIDAS LoA level substantial enrolment requirements
5	*high*	eIDAS LoA level high enrolment requirements

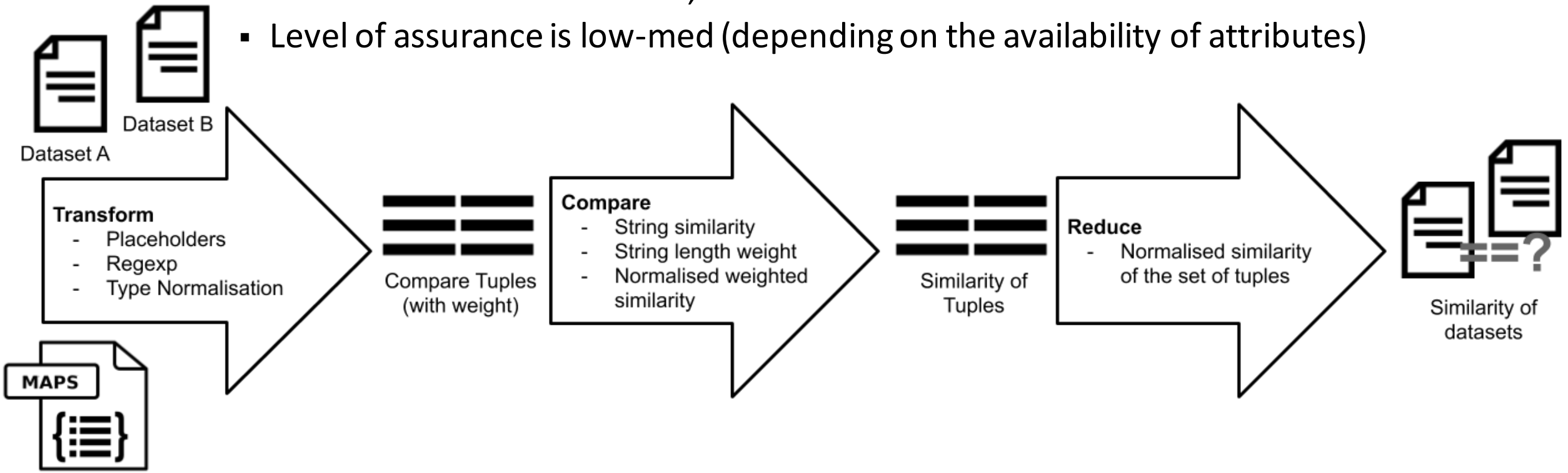
eID Link Representation

- URI format proposed to fit in an attribute
- Included fields to ensure completeness:
  - Issuer ID of the entity that asserts the link
  - Link level of assurance
  - For each of the two datasets:
    - A unique identifier of the subject
    - A unique identifier of the issuer of the dataset
- To ensure the commutative property, the sorting of both datasets fields follow a canonicalization algorithm (alphabetic order of subjects, issuers)

urn:mace:project-seal.eu:link:{LinkIssuerId} :{LLoA} :{SubjectA} :{IssuerA} :{SubjectB} :{IssuerB}

Automated Linking

- An algorithm does the pairing. No human interaction. Configurable
  - Establish a similarity index between two datasets by comparing its attributes
  - Attributes are paired and transformed according to a specific rule set
  - If index is above a threshold, link is issued
  - Level of assurance is low-med (depending on the availability of attributes)



Benefits

For the identity sources:

- Reduced workload, thanks to the trusted self sovereign identity
- Improved interoperability between identity realms
- Procedures designed to assure the trust on the imported data
- Avoid Data Honeypots thanks to data being kept by the user herself
  - Different solutions available: cloud, mobile wallet, local storage, to provide a better experience and resiliency.

Benefits

For the end-user:

- Enabled to get, pair and operate all unrelated e-identities owned
- **User-centred**: decides at all times which information is gathered and released and for how long, and is the keeper the information
  - Web and mobile client; cloud, mobile and file storage
- Thanks to the trusted self sovereign identity:
  - Less dependency on third parties
  - Get federated data to VCs in wallets and VCs to federated SPs
  - Uport and Jolocom are supported
- Identity and **credential exposure reduced** by derived identities
  - Identities and credentials bootstrapped at the user's demand
    - Temporary or persistent
    - Anonymous while still trusted

Benefits

For the Service Provider:

- Reduced dependency on the IdP, less central failure points
- Procedures designed to assure the trust on the imported/generated data, so only trusted data is provided from SEAL
- All data issued or proxied comes with a level of assurance, to support multiple trust-level operations.
- Access to **trusted identity linking** information from users
- Thanks to the trusted self sovereign identity
  - Issued verifiable claims come with a level of assurance
  - Distributed verification info on the distributed ledger
  - Link with eIDAS identity can be proved on demand

THANKS YOU
for your attention

farago@uji.es

To contact or keep up with the latest news, refer to our project web page
www.project-seal.eu

GRANT AGREEMENT UNDER THE CONNECTING EUROPE FACILITY (CEF) - TELECOMMUNICATIONS SECTOR AGREEMENT INEA/CEF/ICT/A2018/1633170.
Action No: 2018-EU-IA-0024

Atos

UNIVERSITAT JAUME I

UNIVERSITY OF THE AEGEAN

UNIVERSIDAD DE MÁLAGA

U.PORTO

grnet

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Ψηφιακής Πολιτικής Τηλεπικοινωνιών και Ενημέρωσης