eDiplomas

Authenticity validation of diplomas issued by the Greek Higher Education Institutes (HEIs)
https://ediplomas.gr

**GUnet Technical Meeting,
Athens, June 2019**

eDIPLOMAS: goals

- **Re-establish the process of diplomas validation**, break free from document based methods, without invalidating the legacy flows

- **Motivate all stakeholders,** make it easy, quick, secure and GDPR compliant

- **Leverage the benefits of the digital transformation**, establish common semantics and data structures, introduce new privacy enhancing technologies

- **Go production now,** be realistic with the enabling technologies, make room for innovation

KEY CONCEPTS

THE ACTORS AND THEIR ROLES

THE CITIZEN

Diploma holder and resource owner

THE HEI

Awarding legal entity and primary authoritative source

THE ORGANIZATION

Legal entity entitled to act as validator, represented by registered authorized personnel

DESIGN PRINCIPLES

1. Authentication

Use a National AuthN provider (TAXISnet)

- For the diploma holder
- For the authorized personnel per organization

2. Authorization

Use the OAuth2 framework

- Diplomas are made up of several scopes
- Access is granted to specific scopes, for a given lifetime and organization

3. Security

Use Digital Certificates

- Responses are signed by the HEIs
- Encrypted for the intended organization by eDiplomas

4. Structured

Use well defined data structures

- Use Reference Data, where possible
- Promote linkage identifiers with Citizens' National Registries

1. AUTHENTICATION

Leverage TAXISnet, the OAuth2 based authentication service of the Greek Taxation Information System

1.

- Does not depend on alumni institutional accounts
- Requires a linkage identifier between the AuthN provider and the HEI

2.

- TAXISnet: Quick solution for State services
- TAXISnet: Not eIDAS ready yet, required for cross country services

3.

- HEIs staff authentication is provided by the institutional IdPs
- Institutional IdPs also provide entitlements for HEIs staff

2. AUTHORIZATION

OAUTH2 defines a delegation protocol for enabling citizens to authorize access to their diplomas, in a very flexible way

1.

Granular Access Control via OAuth2

- Per diploma section
- Access Lifetime
- Access Revocation

2.

- eDiplomas keeps no information about diplomas
- Stores only transient encrypted tokens and matching SSNs

3.

- Golden records of diplomas remain at HEIs
- Read access to HEI’s diplomas registry is required, by eDiplomas

3.

SECURITY (1/2)

When a diploma is requested:

1. eDiplomas requests specific fields for the diplomas mapped to a specific SSN

2. HEIs respond with the matching diplomas, their signatures and the signatures of the fields that were requested

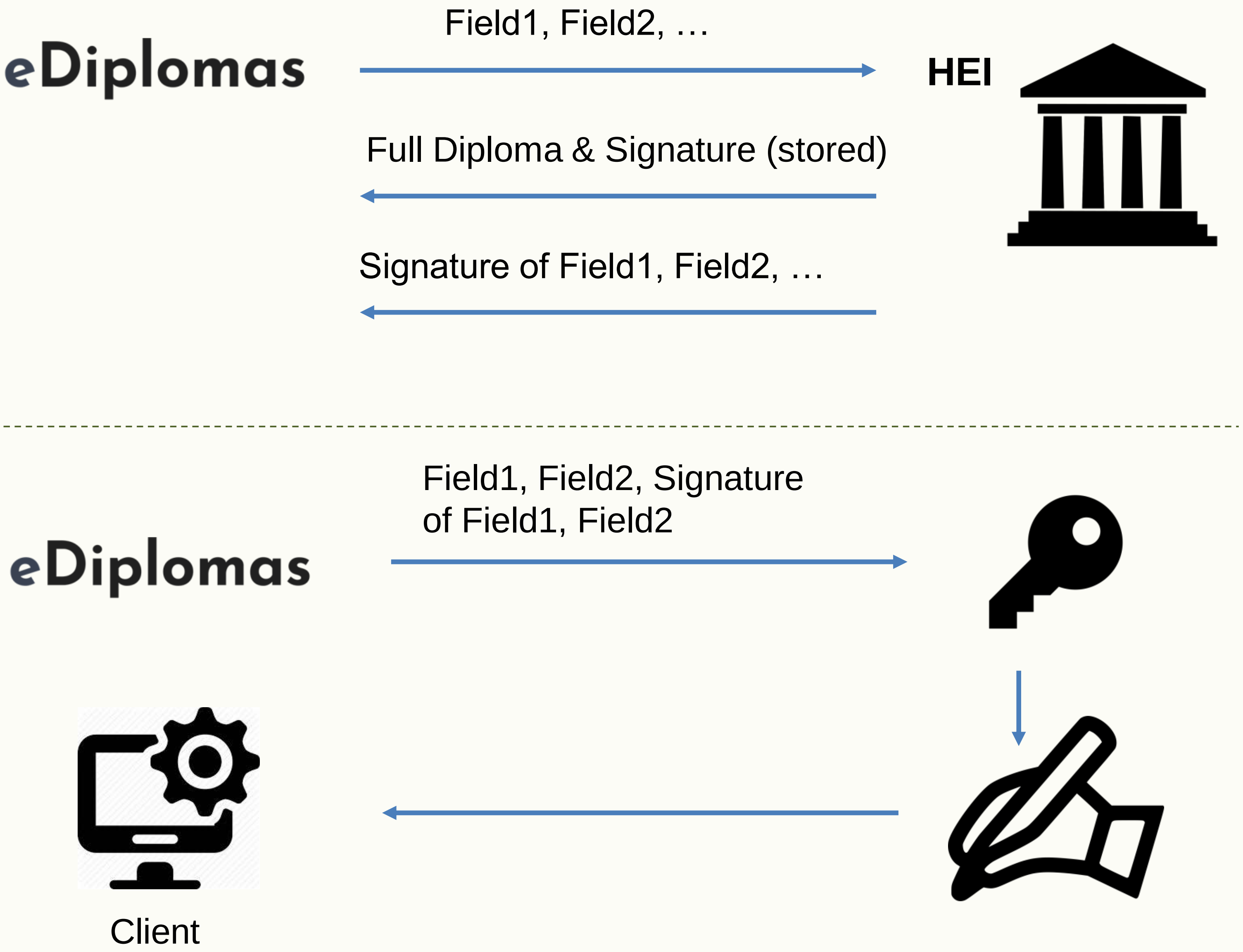
3. eDiplomas verifies the signature of each diploma

4. eDiplomas verifies the signature of the requested fields

5. eDiplomas encrypts the requested fields and their signature, signs them and sends them to the client

What's the security incident we need to protect from?

3. SECURITY (2/2)



eDiplomas

Field1, Field2, …

HEI

Full Diploma & Signature (stored)

Signature of Field1, Field2, …

eDiplomas

Field1, Field2, Signature of Field1, Field2

Client

4. STRUCTURED

Support HEIs to establish common semantics and vocabularies.
Foster interoperability and automation via well defined APIs

1.

- Use of Reference Data from national registries of Higher Education
- Extend the digital diploma with the ISCED codes for educational fields, and levels

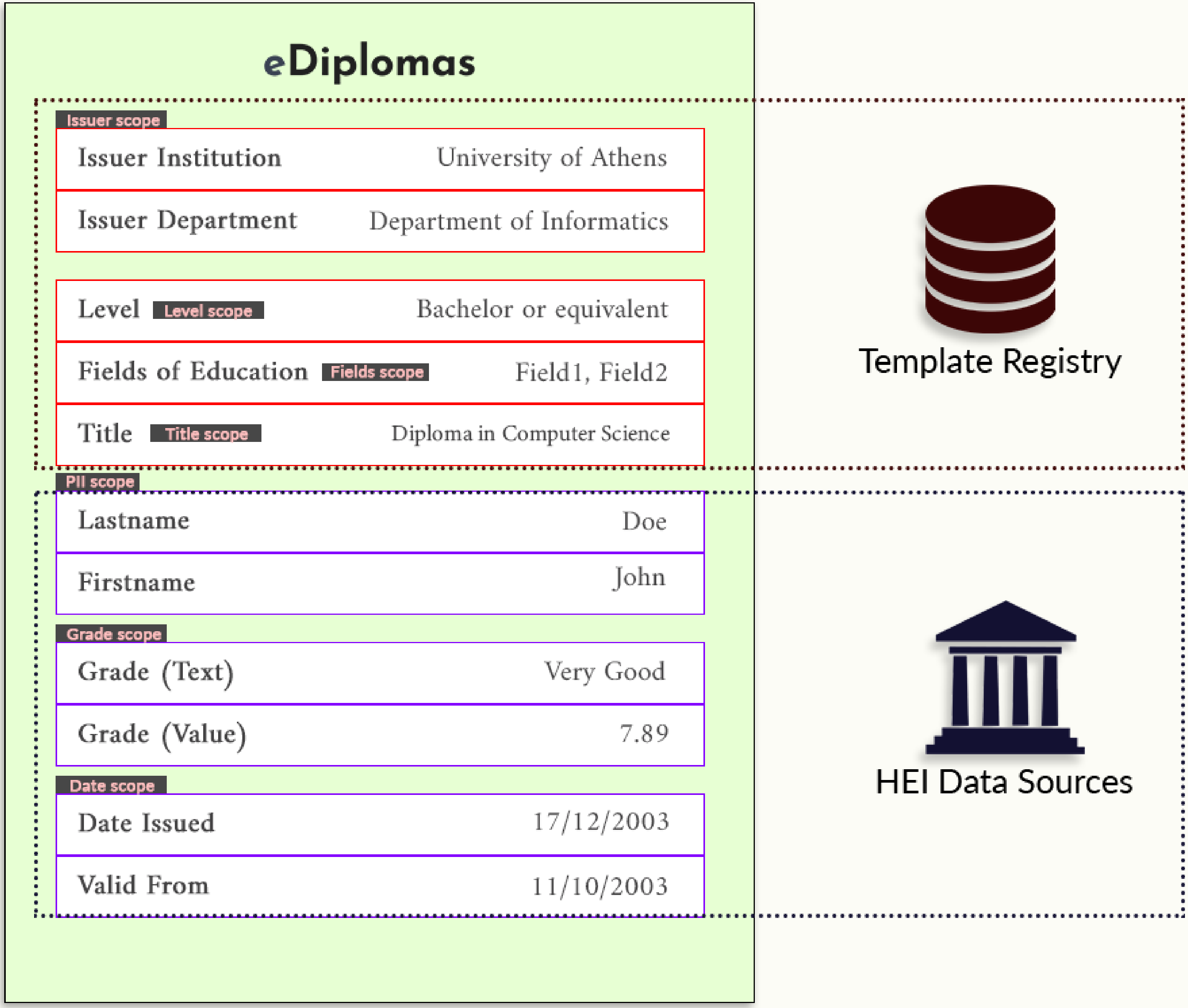
2.

- Each diploma references a diploma template via a persistent identifier
- Diploma templates should be available as Open Data on a public registry

3.

- Ignore the artistic appearance of the paper based diploma
- Not yet ready for Diploma Supplements, and curriculum details

4. STRUCTURED (1/2)



eDiplomas

Issuer scope

Issuer Institution	University of Athens
Issuer Department	Department of Informatics
Level (Level scope)	Bachelor or equivalent
Fields of Education (Fields scope)	Field1, Field2
Title (Title scope)	Diploma in Computer Science

PII scope

Lastname	Doe
Firstname	John

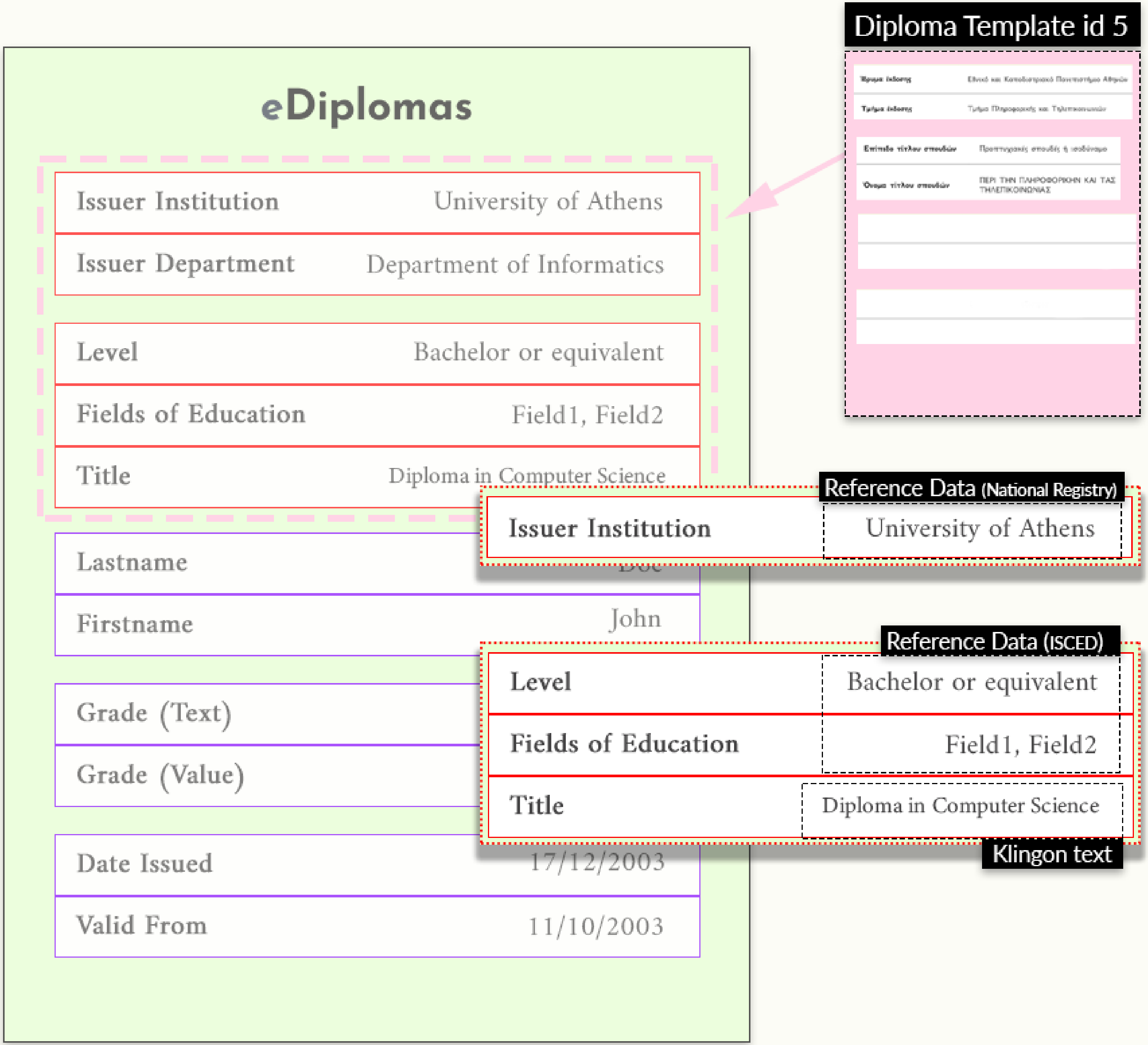
Grade scope

Grade (Text)	Very Good
Grade (Value)	7.89

Date scope

Date Issued	17/12/2003
Valid From	11/10/2003

4. STRUCTURED (2/2)



eDiplomas

Issuer Institution	University of Athens
Issuer Department	Department of Informatics
Level	Bachelor or equivalent
Fields of Education	Field1, Field2
Title	Diploma in Computer Science
Lastname	Doe
Firstname	John
Grade (Text)	
Grade (Value)	
Date Issued	17/12/2003
Valid From	11/10/2003

Diploma Template id 5

Ίδρυμα έκδοσης	Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών
Τμήμα έκδοσης	Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Επίπεδο τίτλου σπουδών	Προπτυχιακές σπουδές ή ισοδύναμο
Όνομα τίτλου σπουδών	ΠΕΡΙ ΤΗΝ ΠΛΗΡΟΦΟΡΙΚΗΝ ΚΑΙ ΤΑΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΣ

Reference Data (National Registry)

Issuer Institution	University of Athens

Reference Data (ISCED)

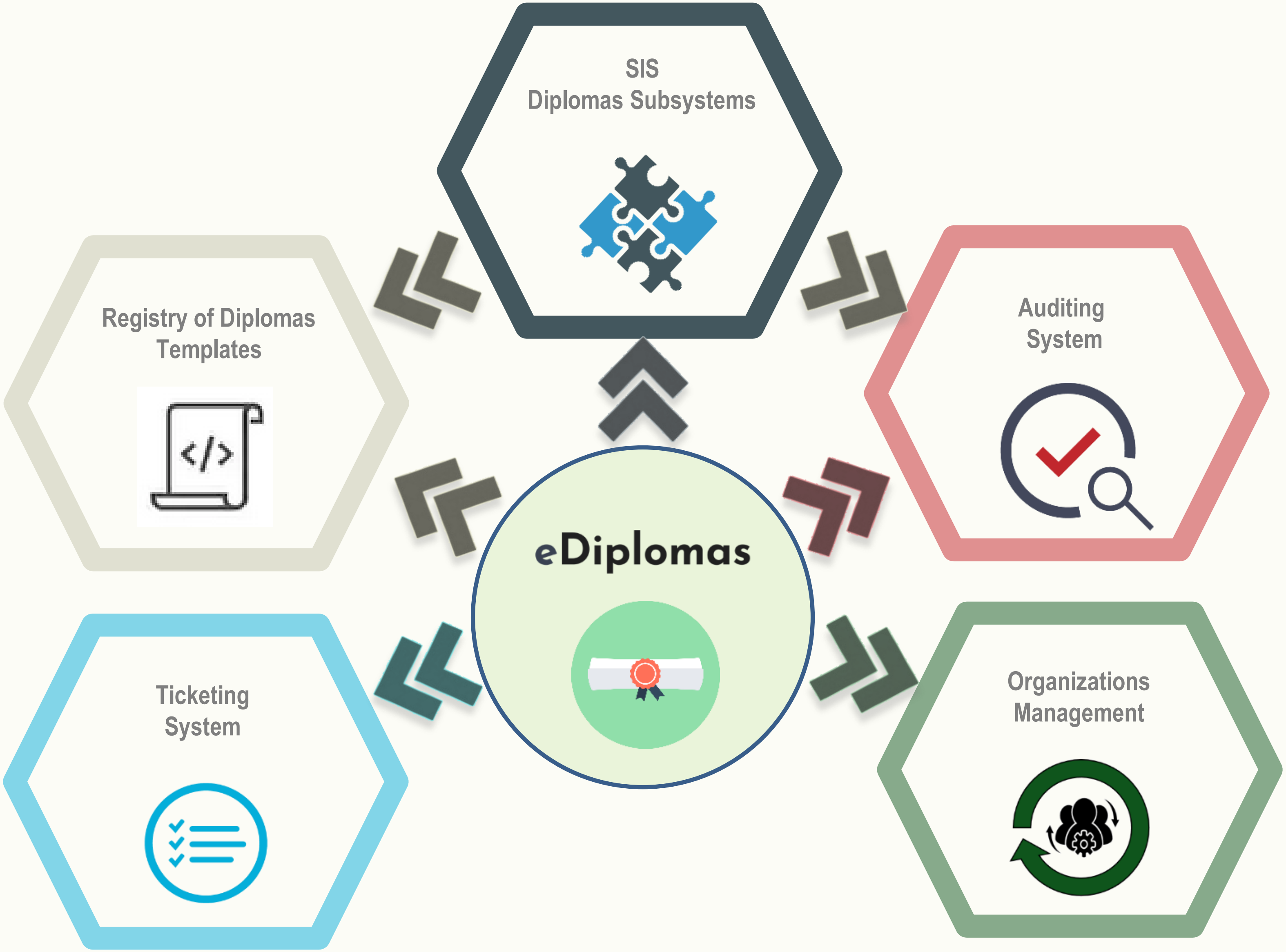
Level	Bachelor or equivalent
Fields of Education	Field1, Field2
Title	Diploma in Computer Science

Klingon text

THE ARCHITECTURE

THE ECOSYSTEM

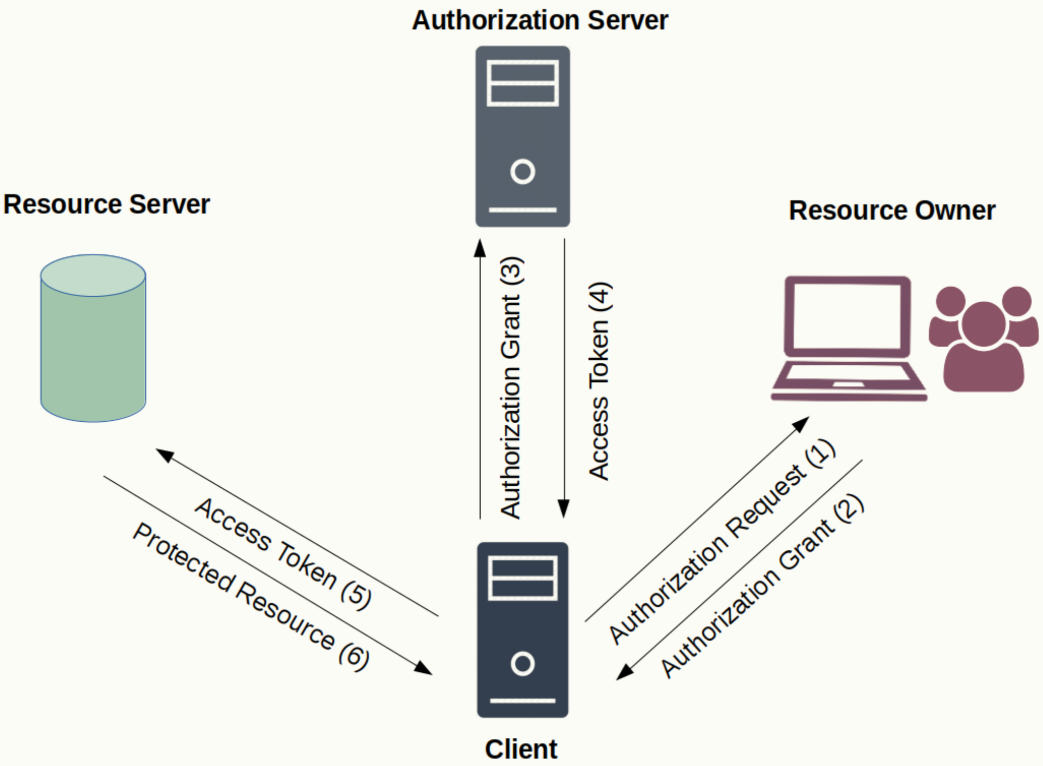
It’s not just eDiplomas



ARCHITECTURE OF OAUTH2

The OAuth2 Client:

- Interacts with the authorization server when a user wants to authorize an entity.
- Interacts with the resource server when an entity is authorized.
- Accomplishes the authorization process using the Authorization Code Grant method.
- eDiplomas is a client itself. A custom client can also be implemented.



USE CASE SCENARIOS

THE SCENARIOS:
ORGANIZATION W/O eDiplomas CLIENT (1 OUT OF 3)

Use Case: The **citizen** authorizes a registered organization to gain access to her diplomas. Organization has not implemented any eDiplomas client.

1. Citizen selects the organization to provide access
2. Gets authenticated, via her eID on TAXISnet
3. National identifiers are used to lookup her diplomas on all HEIs
4. Authorizes access to diplomas and receives a token
5. Sends the token to the organization

THE SCENARIOS:
ORGANIZATION W/O EDIPLOMAS CLIENT (2 OUT OF 3)

Use Case: **Authorized Personnel** of the **Organization** has been designated to access diploma information

1. Receives token from citizen
2. Gets authenticated, via her eID on TAXISnet
3. Enters token
4. Gets access to diploma information along with its signature

THE SCENARIOS:
ORGANIZATION W/O EDIPLOMAS CLIENT (3 OUT OF 3)

Use Case: Authorized Personnel of the **Organization** wants to validate the provided diplomas info on the eDiplomas platform.

1. Staff member of the organization gets authenticated, via her eID on TAXISnet
2. Inserts the signature with copy/paste or by scanning the QR code of the printed diploma

THE SCENARIOS:
ORGANIZATION WITH EDIPLOMAS CLIENT

Use Case: The **citizen** authorizes a registered organization to gain access to her diplomas. Organization has its own app for Diplomas submission and validation.

Same as before, but:

1. The organization implements the eDiplomas API (OAUTH protocol)
2. User experience and handling of data depend on the organization’s custom client implementation

THE SCENARIOS:
REVOKE AUTHORIZATION TOKENS

Use Case: Review the list of access tokens and provide the option to revoke access token.

The **citizen**:

1. Gets authenticated, via her eID on TAXISnet.
2. Gets informed about the state of the access tokens (used/expired)
3. Selects the access tokens that he wants to revoke

THE SCENARIOS:

EX OFFICIO AUTHORITY TO PERFORM DIPLOMAS AUTHENTICITY CHECKS

Use Case: Authoritative state bodies, need to check whether a submitted diploma is authentic.

The authorized personnel of the **state body**:

1. Gets authenticated, via her eID on TAXISnet
2. Selects an institution
3. Enters basic Degree/Graduate data
4. Gets informed about whether the data matches a registered degree

GREEK UNIVERSITIES NETWORK

THE OFFERING

THE SERVICES

Diplomas Validation, for organizations via API

Diplomas Validation, for organizations via Web Client

Diplomas Lookup & Validation, for Authorized Bodies

My Diplomas online lookup across HEIs, for citizens

Authorization & Revoke Authorization, for citizens

Submit request for missing diplomas, for citizens

INSTITUTIONS

How to participate?

INSTITUTIONS

HOW TO PARTICIPATE?

Requirements for joining eDiplomas:

- Social Security Number – Diploma mapping
- Submit the templates of the diplomas it can issue
- Make the diplomas issued available through an API

INSTITUTIONS

HOW TO PARTICIPATE?

Useful Terminology

- **Issuer** : The Institution/Department that originally issued the diploma. Issuer might not exist anymore.
- **Maintainer:** The Institution/Department that maintains the diploma at the current time. Maintainer has to be active.

MOVING FORWARD

FUTURE PLANS
THE ROADMAP TO PRODUCTION

A fully functional, large scale deployment requires all components of the eDiplomas ecosystem to be completed.

- **SIS at HEI:** Updates are required to fully support the eDiplomas protocol (signing, auditing)
- **Diplomas Templates Registry**: Data Model is finalized, but the application for their management is missing
- **Registered Organizations**: Data Model is finalized, but the application for their management is missing
- **Ticketing System**: Task has already begun. Additional mechanism to fuel eDiplomas via citizens' requests
- **Auditing**: Is to provide additional legal proofs. Functional and technical requirements are to be defined

FUTURE PLANS

ALIGNMENT WITH EU INITIATIVES

The **eIDAS Regulation**. To achieve cross border authentication. Get ready to intergrade with the National eIDAS Node.

The **EMREX Network**. To facilitate the exchange of digital transcripts with other participant HEIs. Get ready to join EMREX.

The **PRIViLEDGE H2020 Research Project**. The role of GUnet in the project is to develop the SIS gateway and validate the Privacy-Enhancing Technologies, and the Distributed Ledger Technologies (a.k.a blockchain), in the Diplomas use case.

FUTURE PLANS
JOIN EMREX

EMREX provides the enabling technologies to streamline **student mobility** via a set of well-defined protocols.

- Work with the Aegean University to launch the EMREX **National Contact Point** in Greece
- Implement an **ELMO gateway** in eDiplomas, build the path for cross-border transfers of certifications
- Implement the exchange of **Diploma Supplements**
- Coordinate the **dissemination and promotion** of EMREX standards to Greek HEIs.

GIVE CONTOL BACK TO CITIZENS

By integrating different type of ‘stores’, the same solution can provide the basis for other use cases **when access to centrally stored citizens’ data requires their consent**.

- Are you an eligible student?
- Employment data?
- Social security data?
- Taxation data?
- Demographics?

Verifiable Claims is another emerging technology that aims to provide assertions about an entity’s profile, achievement or qualification in a privacy preserving way. Verifiable Claims could enable future versions of eDiplomas

THANK YOU!

https://ediplomas.gr