



DUBLIN INSTITUTE OF TECHNOLOGY

**DT211C BSc. (Honours) Degree in Computer Science
(infrastructure)**

Year 4

DT228 BSc. (Honours) Degree in Computer Science

Year 4

SUMMER EXAMINATIONS 2016/2017

ENTERPRISE APPLICATION DEVELOPMENT [CMPU4023]

MR. BRIAN GILLESPIE
DR. DEIRDRE LILLIS
MR. THOMAS NOLAN - T211C
MR. KEVIN FOLEY - DT228

THURSDAY 11TH MAY 9.30 A.M. – 11.30 A.M.

TWO HOURS

Question 1 is **compulsory**.

Answer question 1 **and** any two of the other three questions.

Question 1 is worth 40 marks, all other questions are worth 30 marks

Illustrate your answers with appropriate examples and diagrams

- 1 (a) In the context of enterprise application architecture, distinguish between a monolithic design and a service-oriented design (SOA). Mention two advantages of the SOA approach to enterprise application construction.

(8 Marks)

- (b) Explain what an object-relational mapper (ORM) does. Give your opinion as to when you would and would not recommend using an ORM for an enterprise service implementation.

(7 Marks)

- (c) Remote APIs can be implemented using several different paradigms. Briefly explain each of the following three approaches:

- Message Passing
- Remote Procedural Calls
- Distributed Shared Memory

(9 Marks)

- (d) What is a SQL-injection attack? What vulnerability is an attacker able to exploit in such an attack? Mention two ways that this vulnerability can be prevented.

(8 Marks)

- (e) In the context of API security, explain the difference between authentication and authorisation. Explain how these concepts are related to enterprise identity management.

(8 Marks)

- 2 (a) Representational State Transfer (REST) has been described as a stateless client-server API design pattern. Describe the principles behind REST and how it works.

(10 Marks)

- (b) Consider a hypothetical service API for an ecommerce shopping cart having the following exposed resources:

Products	Items that can be bought including name, price and description
Cart	Zero or more order items in the basket pending checkout
Orders	Cart items checked out for purchase
Customers	Service users

Provide the RESTful API interfaces that can perform the following actions. Illustrate each answer by providing an example REST query and response bodies, including the HTTP verbs, URIs, query parameters and response status codes

- List all electrical products for sale at €250
- Add a product to the cart, specifying a quantity
- Create a new customer order from the cart contents
- Cancel a specific order
- List all orders for a given customer for the past 12 months

(20 Marks)

- 3 (a) Discuss the role of an RDBMS system in the implementation of an *Authentication Authority Service*. In your opinion, when does it make sense to carry out the associated cryptographic operations within the service database rather than within the service middleware? Illustrate your answer with examples.

(10 Marks)

- (b) Describe, in detail, the following API authentication schemes. In your answer, state any security-related assumptions you are making about the environment in which each scheme will operate.

- JSON Web Tokens
- Hash-based Message Authentication

(20 Marks)

- 4 (a) One of the desirable characteristics of an API is that it should be learnable by its consumer which is typically an application developer charged with implementing an API client in code. What, in your opinion, should good documentation describe about an API?

(10 Marks)

- (b) Describe, in detail, the following approaches to API specification and documentation. Mention one advantage of each approach:

- Open API Specification (Swagger)
- GraphQL (Facebook)

(20 Marks)