UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

MODULE:	**IT08X47/IT8X298**
	INFORMATION SECURITY
CAMPUS:	**APK**
ASSESSMENT:	**EXAM JUNE 2021.**

DATE	JUNE 2021	**SESSION**	Morning
INTERNAL EXAMINER		Dr J du Toit	
EXTERNAL EXAMINER		Dr R Serfontein	
DURATION 2 Hours		**MARKS** 100	

Please read the following instructions carefully:

1. Write clearly and legibly.
2. Answer all questions.
3. This paper consists of 4 pages
4. This is an open book assessment. You may consult your notes and textbook during the assessment.
5. You are **NOT** allowed to copy from any notes or other sources.
6. You are **NOT** allowed to assist or gain assistance from anyone else.

QUESTION 1 (The need for security) **[20]**

You have been employed as the Information Security (IS) Engineer at the Utopian National Medical Aid Scheme (UMAS). The Utopian government is in the process of providing national medical aid for all its citizens. (20)

One of your first tasks as the IS Engineer is to produce a document that clearly highlights five of the most common IS threats a typical general practitioner (GP) will have. The identification of the five threats can only use the information provided in this question. At least one control must be described for each threat that the GP can implement that will address the threat. The control MUST be realistic to the size of and capability of a typical GP.

The typical GP in Utopia has the following IT infrastructure:

- One or two reception computers that stores and manage patient information.
- One or two tablet devices used by GPs in their consultation rooms to look up symptoms.
- The computers are typically connecting to the Internet through an ADSL router with built-in firewall.
- Receptionists use the computers for email and basic Internet browsing.
- In most cases, computers and tablet computers use wireless connections, using a shared password for the WiFi network.
- Backups of patient information are normally done on removable USB devices taken home by the GP at the end of each day.

Your document must contain the following:

- **Describe** five typical threats applicable to the average GP in Utopia.
- For each threat, highlight **why** the threat was identified.
- For each threat, **describe** one control the GP (*or IT service provider of the GP*) can implement that will address the threat. The control must be applicable for such a small enterprise.

Marks are awarded as follow:

- Describing five threats. One mark per threat. (5)
- Describing why each one is a threat. (5)
- Control of threat. Two marks per control (10).

QUESTION 2 (Information Security Planning) **[16]**

2.1 The UMAS are gearing up for a major IT project that will automate the processing of medical aid claims from GPs. You have been asked to ensure that information security management in UMAS follow best practice. You are thinking of using either Cobit or ISO 27002 as a guideline. (10)

Compare Cobit against ISO 27002 and state which one you would select as best practice and **why** you have made that decision.

2.2 A comprehensive IS awareness and training program is one of the requirements for the new IT project. Write a brief memo that describes how you will implement both IS *training* and *awareness* for UMAS. The memo must address the following aspects for the awareness portion as well as the training portion: (6)

- Which employees will be targeted.
- What format it will take.
- How employees will be tested to determine if they understood the training and awareness.

QUESTION 3 (The five information security services) **[15]**

One of the General Practitioners (GPs) contacted you after you visit them. They are considering using a cloud-based booking system to handle their daily patient appointments. Reception staff must be able to manage the appointments, while the doctors only need to see bookings for them. They are concerned about the risks that such a system may have. (15)

By specifically referring to the 5 Information Security services covered in ISO 7498/2, what controls will you recommend they implement?

Marks are awarded as follow:

- Describing the 5 IS services of ISO 7498/2. (5)
- Describing one or more controls per IS service relevant to the scenario. (10)

QUESTION 4 (Digital Signatures, Confidentiality and Non-Repudiation) **[34]**

UMAS is ready to start developing and designing its automated medical aid processing system. General Practitioners (GPs) will use the new system to submit claims on behalf of patients

The first version of the messaging system makes use of a centralised system that stores public keys.

4.1 **Describe** how the system can use *Forward Public Key Encryption* (only) to ensure a claim is kept confidential when a GP submits it. (4)

4.2 **Describe** how the system can use *Inverse Public Key Encryption* (only) to ensure the non-repudiation of messages sent from the GP to UMAS. (4)

4.3 The Managing Director of UMAS heard about Inverse Public Key Encryption and would like to ensure confidentiality. (2)

What would you say to the MD regarding his request?

4.4 **Discuss** the problem that Envelope Public Key Encryption has with regards to perfect forward secrecy. (4)

4.5 **Describe** how the process in 4.2 (Inverse Public Key Encryption) can be changed to be more processing efficient. (8)

4.6 UMAS would like to enhance the message system to use Diffie-Hellman to establish ephemeral keys. **Describe** how the Diffie-Hellman process generates two ephemeral keys on two devices. The description should describe each variable or component and the process that eventually creates an ephemeral key on the one unit and the other unit. (12)

QUESTION 5 (Digital Identities) **[15]**

The implementation of the claims system was a success, but the UMAS would like to plan and upgrade the claims system to use digital identities managed by a Certificate Authority.

5.1 **Discuss** two IS reasons why UMAS may have decided to consider using digital identities from a Certificate Authority, instead of continuing to use the centralised storage of digital identities? (4)

5.2 **Describe** the process that would allow UMAS to get a digital identity from a Certificate Authority. (6)

5.3 One of the general practitioners (GPs) signed an email using their private key. The GP attached an X.509v3 certificate in the email. (5)

Statement: You are assured that the message was sent by the GP.

Discuss the validity of the above statement.

TOTAL PAPER **[100]**