Assignment Guidance and Front Sheet

This front sheet for assignments is designed to contain the brief, the submission instructions, and the actual student submission for any WMG assignment. As a result the sheet is completed by several people over time, and is therefore split up into sections explaining who completes what information and when. Yellow highlighted text indicates examples or further explanation of what is requested, and the highlight and instructions should be removed as you populate 'your' section.

This sheet is only to be used for components of assessment worth more than 3 CATS (e.g. for a 15 credit module, weighted more than 20%; or for a 10 credit module, weighted more than 30%).

To be completed by the student(s) prior to final submission:

Your actual submission should be written at the end of this cover sheet file, or attached with the cover sheet at the front if drafted in a separate file, program or application.

Student ID or IDs for group work	**e.g. 1234567**

To be completed (highlighted parts only) by the programme administration after approval and prior to issuing of the assessment; to be consulted by the student(s) so that you know how and when to submit:

Date set	Assignment 2 – 07th November 2023
Submission date (excluding extensions)	Assignment 2 – 14th February 2024 (design & implementation/simulation)
Submission guidance	Submit Electronically to Tabula
Late submission policy	If work is submitted late, penalties will be applied at the rate of **5 marks per University working day** after the due date, up to a **maximum of 10 working days** late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). "Late" means **after the submission deadline time as well as the date** – work submitted after the given time even on the same day is counted as 1 day late. For **Postgraduate** students only, who started their **current course before 1 August 2019**, the daily penalty is **3 marks** rather than 5.
Resubmission policy	If you fail this assignment or module, please be aware that the University allows students to remedy such failure (within certain limits). Decisions to authorise such resubmissions are made by Exam Boards. Normally these will be issued at specific times of the year, depending on your programme of study. More information can be found from your programme office if you are concerned.

To be completed by the module owner/tutor prior to approval and issuing of the assessment; to be consulted by the student(s) so that you understand the assignment brief, its context within the module, and any specific criteria and advice from the tutor:

Module title & code	Implementing Secure Systems (WM242-24)
Module owner	Sandy Taramonli
Module tutor	Sandy Taramonli
Assessment type	A2: design and implementation/ simulation
Weighting of mark	A2: design and implementation/simulation – 35%

Module learning outcomes (numbered)	1. Reason about the relationship between human trust and the technological tokens that represent trust in cyber systems. 2. Design a security architecture that satisfies the security needs of a given scenario. 3. Configure systems, applying cryptographic techniques as needed, to achieve desired security objectives.
Learning outcomes assessed in this assessment (numbered)	1, 2, 3
Marking guidelines	Generally indicated within specification
Academic guidance resources	1. The Teams Channel. 2. A special Moodle forum. 3. Through emails directed to the module tutor. 4. Specialist assessment support session. 5. One to one sessions (please arrange meetings with me). **Notes to students:** If support is provided on a Teams Channel or a Moodle forum, please ensure you check previous questions posted on the channel. The Teams/Moodle channel will typically be closed one week before the submission date and no new questions will be addressed, please organise your time accordingly. Please be patient with module tutors. Please turn on your Teams Channel/Moodle notifications. If a tutor has not responded to a query within 5 working days, please email the module tutor.
Special instructions	Your submission will comprise the following files: **A2 - Sequence diagram and implementation:** 1. A sequence diagram in PDF format 2. A working configuration simulation Files must not be zipped or placed in any type of file

	container. You will only have one opportunity to submit the above. If you miss any files out, they will not be assessed, and you will not be given a second opportunity to submit.

Implementing Secure Systems (WM242-24, First Sit)

Context

You are a recently qualified cybersecurity graduate working for MediTech Solutions, a leading healthcare technology company. As part of a new project, you have been assigned to enhance the security practices of St. John's Clinic, a healthcare provider. St. John's utilizes various systems to manage patient data and clinic operations, including:

- MedRecords: A system for maintaining electronic health records (EHR) of patients.
- FinCare: A finance system used for managing financial transactions, accessible only by authorized staff members.
- CareConnect: A platform accessible to patients for accessing medical records, appointment scheduling, and other healthcare-related information.
- Electronic Prescribing System: A system for electronically prescribing medications and managing prescriptions within the clinic.
- MediCloud: An open-source cloud storage and file sharing system for St. John's.

St. John's Clinic is planning to expand its cloud infrastructure, particularly its secure storage solution, to support various systems used within the organization, including MedRecords, FinCare, CareConnect, and the Electronic Prescribing System. Some of the data handled by these systems is highly sensitive and includes financial records, patient personal information (including medical data), and confidential documents such as medical test results and reports. The clinic recognizes the need to enhance its security and cryptographic practices. Additionally, St. John's Clinic aims to establish a Single Sign-On (SSO) system to streamline user authentication and provide a unified login experience across all clinic services. This system will enable users to access multiple online services run by the clinic using a single set of credentials.

To ensure appropriate access control and data protection, the clinic has implemented role-based access control (RBAC) across all its services. This means that access to sensitive data is restricted to certain users, based on their roles and responsibilities. For example, the finance team can access financial data, the medical staff can access patient health records, and the administrative team has access to administrative documents. The clinic wishes to strengthen data protection measures by implementing encryption at rest for sensitive data stored within the cloud infrastructure. While the cloud platform supports file- and disk-level encryption, the choice of cryptographic algorithms and key management strategies will be determined based on industry best practices and compliance requirements. A justification of these selections is required.

In addition to internal operations, St. John's Clinic collaborates with pharmaceutical companies, research institutions, and academic partners to conduct medical research and clinical trials. As part of these collaborations, the clinic may store partners' intellectual property and research data within its cloud infrastructure. To ensure the confidentiality and integrity of this sensitive information, it should be encrypted at rest and accessible only by authorized individuals, such as the collaborating researchers and relevant personnel. Access to these files will be granted based on invitation or authorization from the data owners.

Given the clinic’s commitment to data security, compliance with relevant regulations is of utmost importance. The proposed cryptographic practices and security measures should align with these regulations and provide a robust framework for protecting patient data, intellectual property, and confidential information.

Key Data to Protect:

- Patient health records, including personal and medical information, currently stored in MedRecords.
- Sensitive financial data, accessible only to the finance department, stored in FinCare.
- Electronic prescriptions and medication-related data in the Electronic Prescribing System.
- Collaborative research data and industry partner intellectual property, stored in MediCloud.

The chosen authentication method, whether it be username and password, two-factor authentication (2FA), or other approaches, should prioritize both usability and security considerations. Furthermore, the proposed system must seamlessly integrate with the existing infrastructure.

Your task is to design a cryptographic simulation that meets these requirements. There are no constraints on the proposed solution as long as it effectively meets the specified criteria. Where relevant, your solution should be compliant with GDPR, CCPA, and PSD2. Your solution should address the following aspects:

Data Storage: Identify the storage location for each service's data within the clinic's system.

- Data Transfer: Define the mechanisms and protocols for secure data transmission between different clinic services.
- Cryptographic Protocols and Algorithms: Specify the cryptographic protocols and algorithms used to protect sensitive data within the clinic's system.
- Key Management: Describe the process for generating and storing cryptographic keys within the clinic's infrastructure.
- Authentication: Propose an authentication framework that meets the usability and security requirements.

Your task is to propose a cryptographic solution that addresses the security requirements outlined by St. John's Clinic. More detailed assignment requirements are outlined below:

Assignment task

Assignment 2: Cryptosystem design and simulation (35%)

Use Cryptool to simulate the proposed cryptosystem. Test and validate the simulation to ensure the functionality and effectiveness of the implemented security measures. All elements of your simulation must be provably functional. Your configuration must be easy to follow and be prepared in a single configuration project. The recipient should be able to run your configuration file with no intervention. Provide a sequence diagram that shows the communication between entities such as the authentication authority, the different services, and the user.

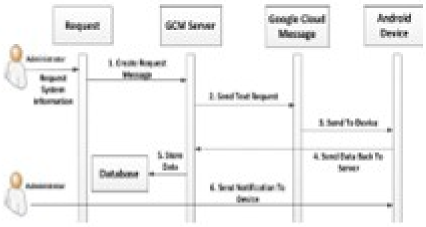

Figure 1 An example of a sequence diagram