

Challenge 3

Background

The Mina spy master is unhappy with the current message processing systems and wants to try out Protokit.

He wants you to build a Protokit project that will receive messages as transactions, there will be one message per transaction.

Each message has

- Message number
- Message details
 - AgentID
 - 12 characters
 - Security code

The security code is a 2 character code that should match a value held in the contract for a particular agent.

The details about the agent needs to be checked against state in the contract.

This state should hold the following information

- AgentID

- Last message number received
- Security code

You can assume that this has been populated with valid data for all the existing agents

When processing a message, ensure that. :

- The AgentID exists in the system
- The security code matches that held for that AgentID
- The message is of the correct length.
- The message number is greater than the highest so far for that agent.
- You should update the agent state to store the last message number received.

The spymaster is worried that this design is not private.

Is he correct ?

How could you change the system to ensure that messages are private ?

Deliverables

- An app chain implementing the above functionality.

- Tests for the chain to demonstrate the required functionality
- An answer to the question regarding privacy (you don't need to implement that yet)

I recommend you start with the Protokit [starter kit](#) and customise it to your solution. You should also check the notes from Session 5.

Submitting your solution

You should send us a link to the github repo containing the solution.

Deadline

Your solution needs to be submitted by midnight (UTC) on 14th April 2024.

If you have any questions, please ask on Discord.