# Host Identity Protocol (HIP) Socket Report

## 

## Team members

## Farida Ahmed Salem 2206160

## Hadir Amr 22010450

## Martin Maher 22010445

## Youssef Ahmed Ragaee 2202126

## Youssef Tamer Mohamed Ahmed 2206172

## Rewan Salah Mahmoud Shiha 20221447143

## Introduction

This report describes a simulated implementation of the Host Identity Protocol (HIP) using Python. The implementation demonstrates the key features of HIP, including host identity generation, mutual authentication, key exchange, encryption, authorization, and replay attack protection. The simulation uses a socket-based communication model to replicate realistic network behavior.

## 2. Features Implemented

* 1. HIT Generation: SHA-256 based unique identity tags derived from RSA public keys.

A screen shot of a computer code

AI-generated content may be incorrect.

* 2. Mutual Authentication: Performed using RSA digital signatures with PSS padding.

A close-up of a computer code

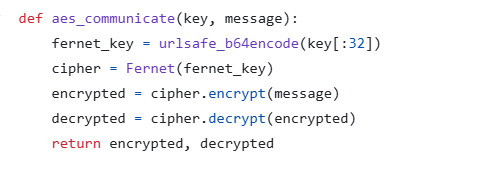
AI-generated content may be incorrect.

* 3. Key Exchange: Implemented using 2048-bit Diffie-Hellman and HKDF key derivation.

A computer screen shot of text

AI-generated content may be incorrect.

* 4. Encryption: AES encryption (via Fernet) using the derived session key.

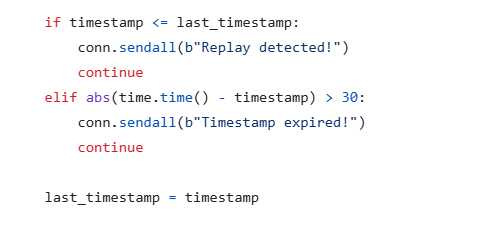


* 5. Authorization: Role-based access control using ACL (admin, analyst, guest).

A computer code with blue text

AI-generated content may be incorrect.

* 6. Replay Attack Protection: Timestamps are validated to detect message replays.



* 7. Real-Time Communication: Implemented using Python socket communication.

Implementing Python socket and two classes, server and client

## 3. System Architecture

The system comprises two main components:  
- Server: Listens for client connections, validates identity, handles authorization,  
 and decrypts messages.



A screenshot of a computer code

AI-generated content may be incorrect.

- Client: Connects to server, signs a timestamp, sends encrypted message with action request.

A screenshot of a computer program

AI-generated content may be incorrect.

## 4. Scenario Results

|  |  |  |
| --- | --- | --- |
| Scenario | Description | Result |
| 1 | Analyst reads (first request) | Auth Success |
| 2 | Replay of same request | Replay Detected |
| 3 | Admin writes | Auth Success |

## A white background with black text AI-generated content may be incorrect.