# Tirocinio Formativo Universitario

Breve elaborato sull’attività svolta durante il tirocinio curricolare interno.

## Obiettivi

Progettazione e realizzazione di un sistema di erogazione di bevande, automatizzato tramite l'utilizzo di tecnologie RFID e componenti comunemente impiegate nel campo dell'IoT.

Tale sistema, consentirà all'utente di effettuare in maniera autonoma una consumazione, una volta riconosciuto, usando la tecnologia dei moduli RFID; inoltre l'utente potrà consultare le proprie consumazioni registrate e saldare l'importo dovuto tramite un applicativo per smartphone.

Il sistema garantirà un livello di sicurezza tramite la cifratura dei dati utente sui moduli RFID e delle trasmissioni tra l'applicativo ed il server che ospita il database del progetto.

Sarà implementata una gestione dei canali di trasmissione tra i vari componenti del sistema adibiti al riconoscimento utente ed erogazione della bevanda, applicando le necessarie misure di QoS.

Verrà implementata la possibilità di avere una visione generale del sistema tramite software di monitoraggio.

## Sicurezza

Per garantire un maggiore livello di sicurezza durante l’uso dei tag/card NFC, bisogna impedire l’accesso a terzi alla memoria delle schede, in quanto è possibile modificare i byte di memoria che corrispondono al proprio ID che viene utilizzato per il riconoscimento e addebito del costo delle bevande.

Attualmente, tengo in considerazione 3 metodi diversi per prevenire ciò:

* Impedire l’accesso alla memoria con uno step auth
* Crittografare l’ID dentro al tag
* Riempire la memoria di byte randomici con lo scopo di rendere più difficile quale parte della memoria viene effettivamente utilizzata per salvare il vero ID utente

Consultando la documentazione su xnp.com, è possibile trovare le specifiche sull’implementazione di uno step di autenticazione. Ci sono alcuni campi chiave circa la protezione con psw:

* La pagina CFG0 (0x29): L’ultimo byte (AUTH0) rappresenta lo stato della protezione con password. In particolare, il valore indica il numero della pagina da cui è richiesta l’autenticazione. Un valore 0xFF rappresenta che il tag non è protetto da psw, mentre un valore 0x00 sì, indicando che tutte le pagine sono soggette alla protezione. [pag 19 su 60 del pdf]
* Immagine che contiene testo, schermata, Carattere, numero

  Descrizione generata automaticamentePROT bit in ACCESS byte (primo byte nella pagina 0x2A)



Immagine che contiene testo, schermata, Carattere, linea

Descrizione generata automaticamente



Il valore default per il byte ACCESS è 0x00 🡪 00000000b.

Il valore default per il bit PROT è 0b, che indica il tipo di protezione WRITE PROTEXTED by PSW, invece 1b indica READ AND WRITE PROTECTED by PSW

Gli altri byte sulla pagina 0x2A sono per ‘Reserved for future use – implemented’ (RFUI). Gli altri bit in ACCESS sono 0b per default.