

# Analisi del protocollo Written Authenticated Through Anonymous (WATA)

---

Uno scenario reale in cui gli attori in gioco vogliano ottenere sia l'autenticazione che l'anonimato è dato dagli esami scritti universitari. Il docente ha un certo interesse nell'autenticare lo studente e lo studente, al fine di tutelarsi dalla possibile non imparzialità del docente, ha abbastanza interesse a rimanere anonimo.

Queste due proprietà abbiamo visto essere in netto contrasto e, da una prima analisi, esclusive.

Analizziamo il protocollo [qui descritto](#) per spiegare come queste proprietà possano coesistere all'interno dei sistemi reali.

**Written Authenticated Through Anonymous (WATA)** è un protocollo progettato e implementato in **nas.inf**.

- Autenticazione del compito per prevenire imbrogli dello studente (tutela del docente)
- Anonimato del compito per prevenire votazione iniqua (tutela dello studente)

Seguire le regole di un protocollo di sicurezza è fondamentale se si vuole godere delle proprietà offerte da quest'ultimo, ma non solo: fare in modo che anche gli altri attori in gioco rispettino la **cerimonia di sicurezza** garantisce le proprietà. Se gli altri non rispettano il protocollo anche noi veniamo compromessi. Le procedure d'esame non fanno eccezione. Per questo motivo è importante conoscere e verificare che gli altri siano diligenti nel seguire le direttive date.

Nel caso in cui il protocollo sia pienamente distribuito verificare che la controparte segua il protocollo è molto più difficile.


Come molti dei concetti visti, autenticazione ed anonimato non sono concetti assoluti ma vanno sempre visti in relazione al "di che cosa" o "da chi". Ad esempio, nello scenario dell'esame scritto vanno identificati sia lo studente che il compito (e la loro relazione deve essere chiara), ovvero l'autenticazione in questo contesto richiede che il compito sia legato (**autenticato**) rispetto alla persona.

C'è anche bisogno del controllo sulle procedure (sorveglianza), per fare in modo che tutto venga rispettato.

Ritroviamo qui il **principio di accatastamento delle difese**: utilizzare più misure di sicurezza per ottenere il risultato voluto. Il fallimento di una delle difese lascia spazio alla violazione della proprietà di sicurezza, anche se non necessariamente il fallimento di un obiettivo del protocollo porta inevitabilmente al fallimento degli altri, dipende infatti da quanto gli obiettivi sono legati.

Il problema dell'**invigilation** è complesso sia dal punto di vista del docente che dello studente. Il riconoscimento dello studente da parte del docente avviene inevitabilmente durante un esame, di fatto può esserci l'anonimato dei dati personali ma non del volto.

La semplice azione di rimescolare la pila dei compiti può essere vista come una misura di sicurezza, lì dove l'obiettivo sia l'anonimato. Una pila di compiti non ordinati non permetterebbe al docente di risalire allo studente.

 **Domanda d'esame:** perchè il compito di WATA ha un ID?

Risposta: perchè altrimenti non sarebbe de-anonimizzabile nella fase di autenticazione.

In **WATA v2** il token e il compito sono abbinabili per mezzo di un ID.

## Osservazioni sull'impiego di un oggetto fisico per l'autenticazione

- Lo studente porta a casa il token, se lo studente perde il token, perde il compito.  
Solo lui risolvere tra compito e anagrafica.
- Il token deve essere robusto all'attacco fisico.

## Alcune soluzioni per (provare ad) ottenere le due proprietà durante un esame

- il ruolo del docente e del vigilator non colludono
- nel momento dell'autenticazione lo studente copre dal codice a barre a scendere, così il docente può memorizzare solo nome, cognome e matricola
- consegna dei compiti randomizzata all'inizio dell'esame
- il docente appone la firma sul token: a cavallo tra bar code e token, così da avere più tutela
- il token deve essere pre-firmato così che il docente possa controllare che l'anagrafica dello studente corrisponda
- l'anonimato è abbinato al compito quando il compito è in fase di marking (valutazione).  
**Il compito non è anonimo sempre ma solo in questa finestra temporale.**

Alcune delle soluzioni qui descritte sono presenti nel protocollo **WATA**.

 **Domanda d'esame:** descrivere il protocollo WATA.

## Fasi del protocollo

L'esame viene definito da **4 fasi**:

- **setup**
- **testing**
- **marking**
- **notifica di voto**

Nel caso di WATA2 le misure sono così stringenti che la figura di docente e vigilator possono coincidere (prima delle soluzioni proposte al punto precedente).

 **Domanda d'esame:** quanti sono i controlli del protocollo WATA che fa l'esaminatore?

**Esempio di risposta:** 4. I tre visti nelle slide ed in aggiunta la verifica del volto.



**Domanda d'esame:** dov'è l'autenticazione del candidato nel protocollo **WATA2**? Dov'è invece l'anonimato del compito?

**Esempio di risposta:** l'autenticazione avviene in fase 2, durante al fase di testing. L'anonimato lo si ottiene in fase di marking