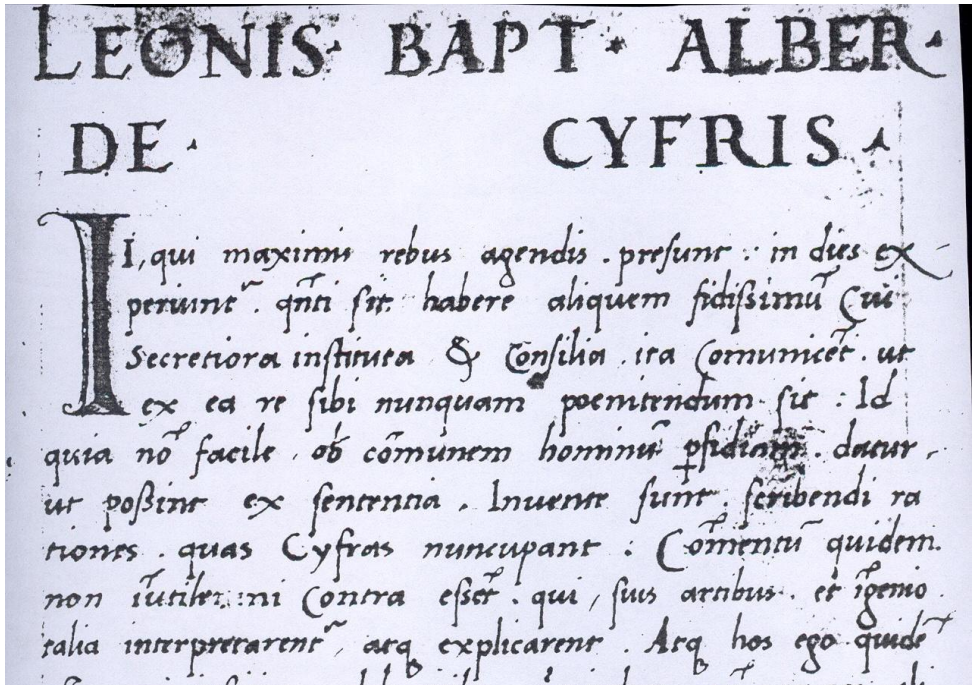


# De Cifris Schola Latina

DIPARTIMENTO DI INFORMATICA
SAPIENZA UNIVERSITÀ DI ROMA
disim
UNIVERSITA' degli STUDI di ROMA TOR VERGATA
ROMA TRE UNIVERSITÀ DEGLI STUDI

**Monday 18th January 2021 at 11.30**
**Virtual conference on Zoom**
**Meeting ID: 878 0977 8904**
**Passcode: 797955**

## Stefano Alberico

**Skudo**

## Skudo-HSM: integrazione tra una PKI ed un chip HSM (FPGA) per applicazioni spaziali ... e non solo

**Abstract:** Mettere in sicurezza le comunicazioni digitali anche per le applicazioni spaziali (tradizionalmente piú lente nell'adottare nuove metodologie) é da tempo un obiettivo strategico di grande importanza. La cyber-sicurezza deve essere parte integrante anche nella fase di progettazione di una missione spaziale ed offrire flessibilitá e protezione durante un lungo lasso temporale.

Skudo sta lavorando all'implementazione pratica di una PKI, combinando la criptazione asimmetrica e simmetrica applicate ai servizi di Telecontrollo e Telemetria basate sul protocollo spaziale CCSDS/SDLS. Un chip FPGA si occupa di eseguire le funzioni di generazione e salvataggio delle chiavi nonché di quelle per la criptazione. L'intera soluzione sará dimostrata all'ESA mediante il lancio di un pallone meteo a 25Km di altezza collegato ad un payload in grado di inviare a terra, mediante un link radio VHF, una serie di dati di telemetria in tempo reale per dimostrare l'avvenuta criptazione e la resilienza dell'informazione in condizioni HAPS (High Altitude Pseudo Satellite).

**Contact person:** Daniele Venturi

**CONTATTI**
**Iniziativa De Componendis Cifris**

seminari@decifris.it
segreteria@decifris.it