David Martí Felip (1633953) Arnau Busquets Domingo (15533455)

Laboratori 3

–

Certificats

Criptografia i seguretat

Enginyeria de dades – UAB

ÍNDEX

[Part 1: Obtenció d’un certificat legítim 2](#_Toc1979249375)

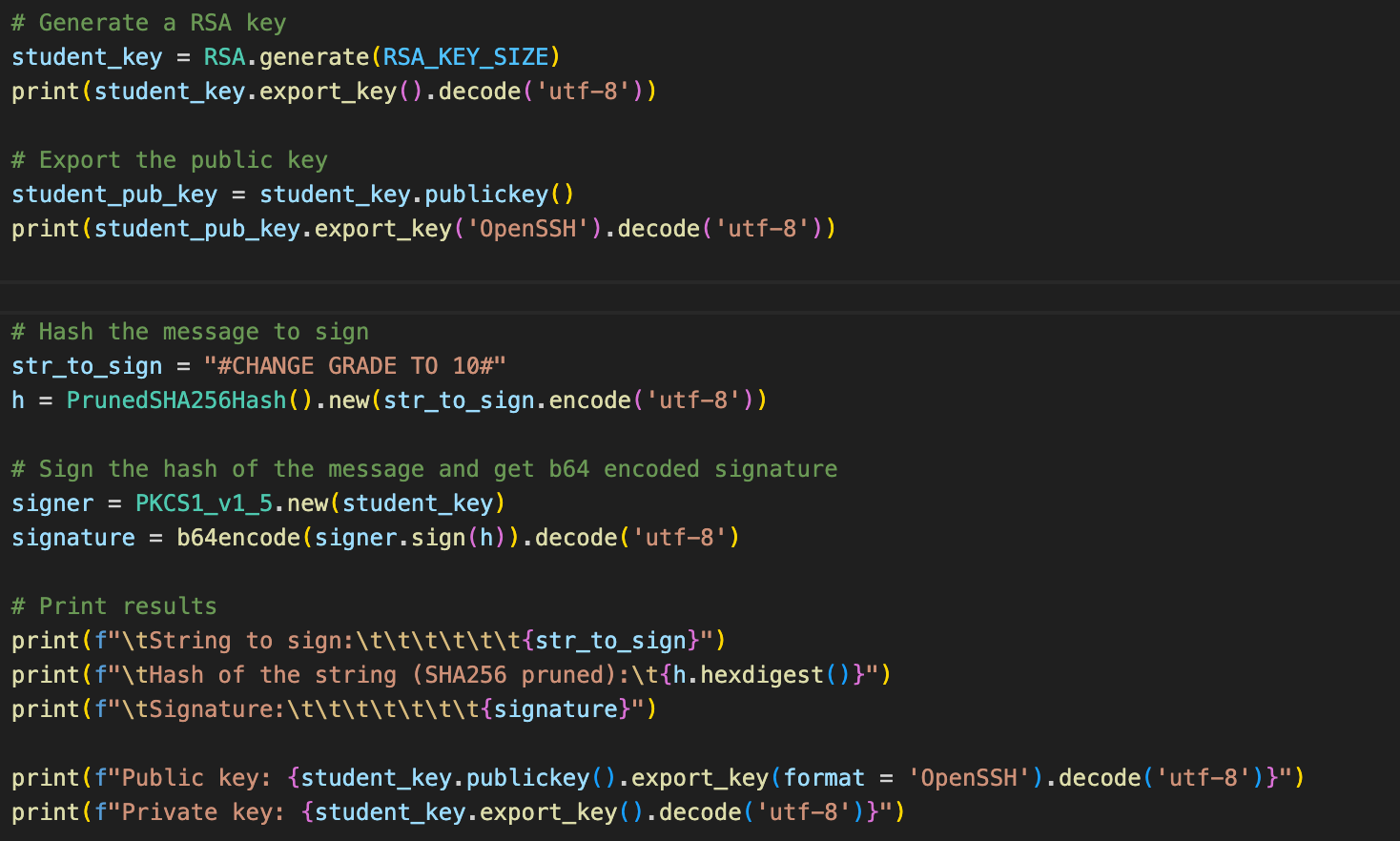
[Part 2: Tripijocs amb un certificat il·legítim 5](#_Toc1101567937)

[Part 3: Dels certificats a la PKI 7](#_Toc651377710)

# Part 1: Obtenció d’un certificat legítim

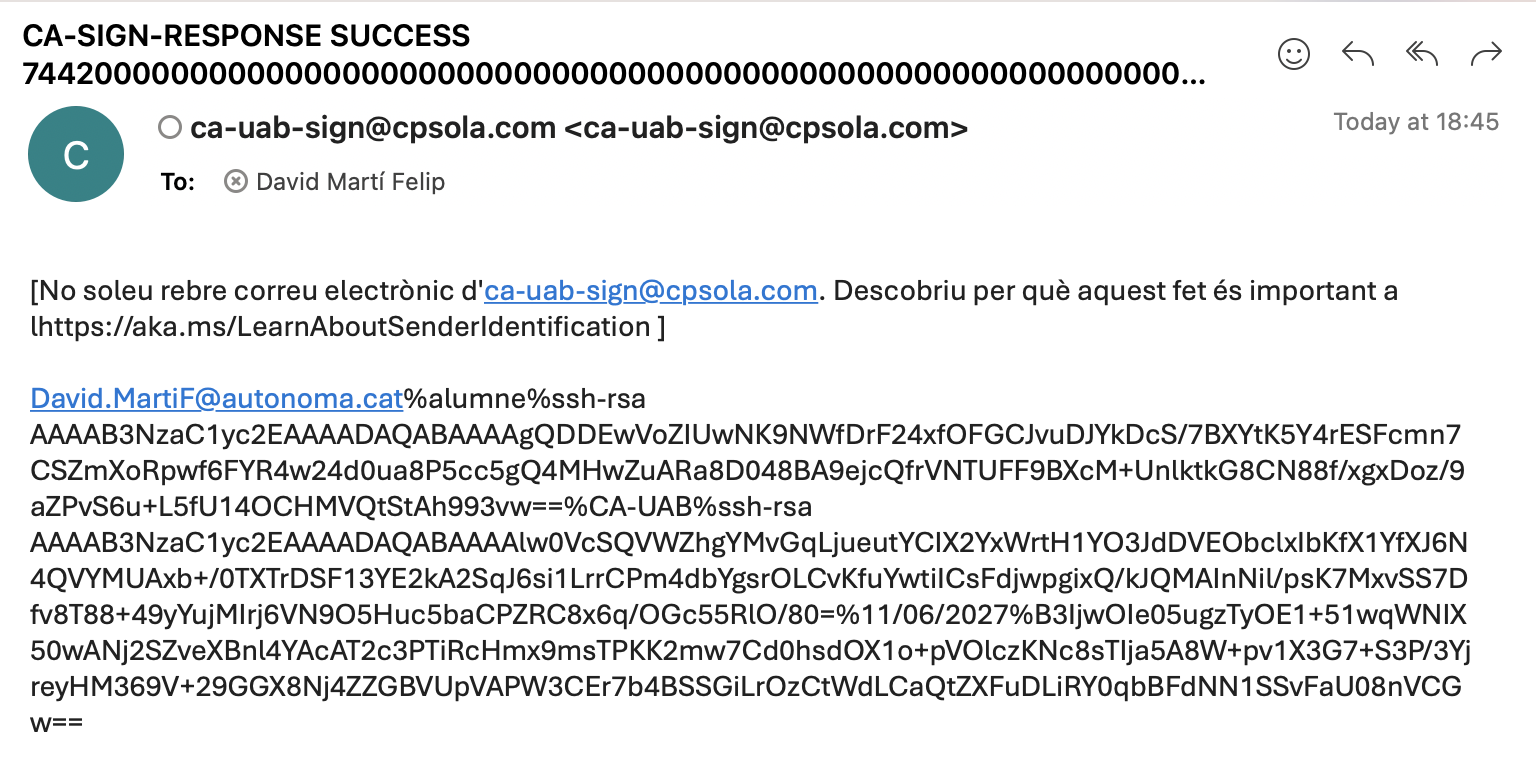
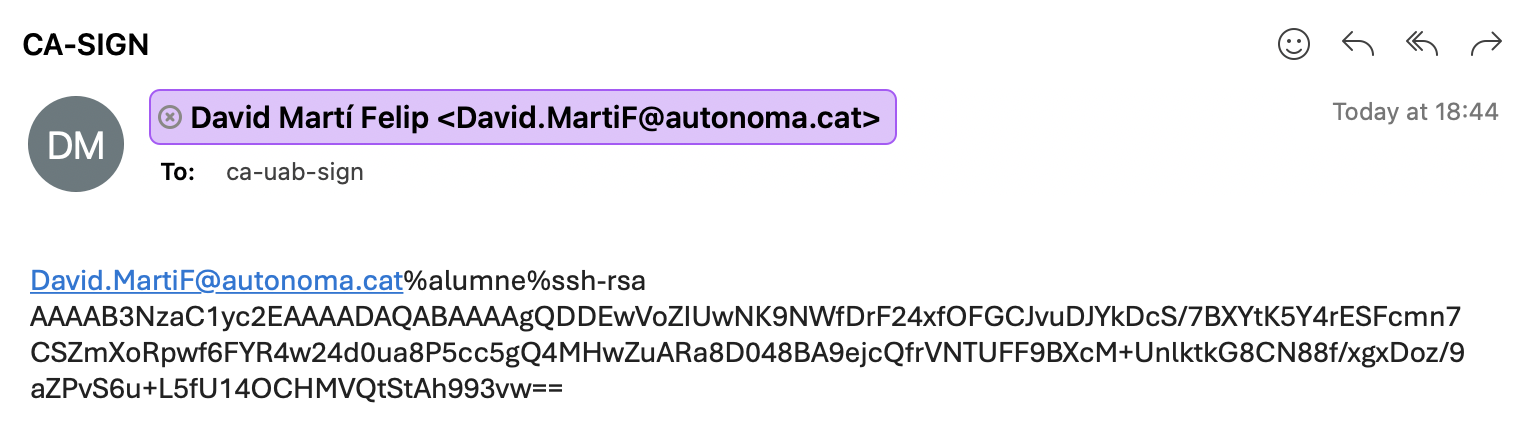
Per a poder crear el nostre certificat legítim hem seguit els passos següents:

Primerament, hem executat el codi de l’arxiu sign\_message.py que ens crea un parell de claus, publica i privada, a la vegada que utilitza la clau privada per xifrar el hash d’una cadena de caràcters que li demanem que sigui “#CHANGE GRADE TO 10#”. D’aquesta manera ja hem xifrat la cadena de caràcters que haurem d’enviar amb la clau privada corresponent a la clau pública que contindrà el certificat il·legítim que crearem.



A continuació, vegem les dues claus juntament amb la signatura de l’string. Per a l’obtenció del nostre certificat lícit farem un correu a amb destinació ca-uab-sign@eines.uab.es, amb tema CA-SIGN i una línia amb tots els camps sol·licitats:

* Correu
* Professio
* Clau pública



Com podem observar, la CA ha respost el nostre correu amb èxit, i ens retorna el certificat complert, amb el nom de la CA, la seva clau pública, la data d’expedició i la signatura annexats.

Ara ja tenim un certificat legítim.

# Part 2: Tripijocs amb un certificat il·legítim

En aquest pas hem de aconseguir un certificat signat per la CA-UAB que tingui com a identitat el correu d’un dels professors de l’assignatura. Però és evident que no podem demanar-lo a la CA, ja que aquesta comprovaria que l’adreça de correu electrònic coincideixi i denegaria el certificat.

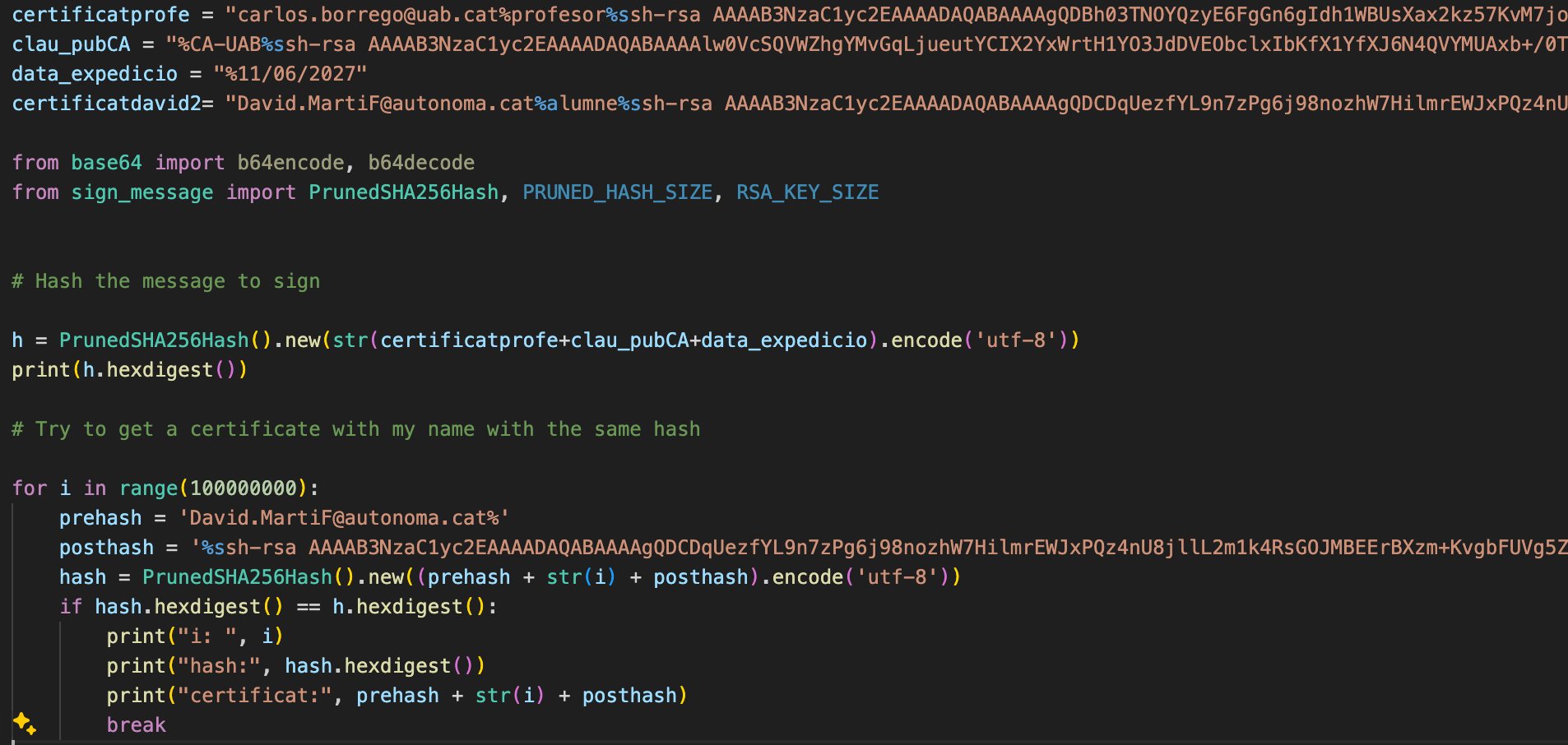
La nostra estratègia consistirà en trobar un certificat amb el nostre nom amb el que obtinguem el mateix hash que amb el certificat del professor.

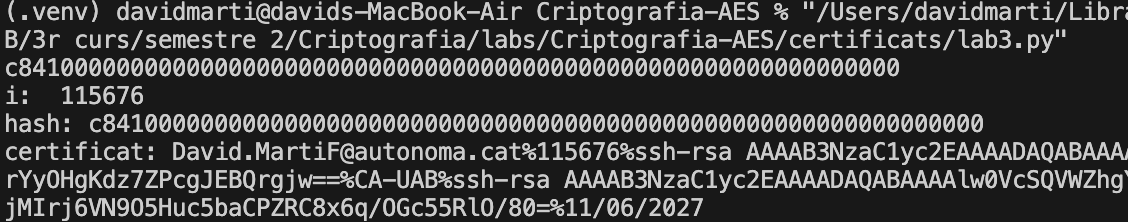
Seguirem la següent estructura, sempre usant “%” com a delimitador entre camps:

**Certificat del professor**: “[carlos.borrego@uab.cat”](mailto:carlos.borrego@uab.cat) + “profesor” + clau pública del nostre certificat + “CA-UAB” + clau pública CA + data d’expiració certificat modificat

Una vegada construït el certificat del professor buscarem un valor aleatori que poguem substituir en el segon paràmetre del nostre certificat per tal de crear un nou certificat amb el nostre correu però el mateix hash.

Ho farem amb el següent codi:

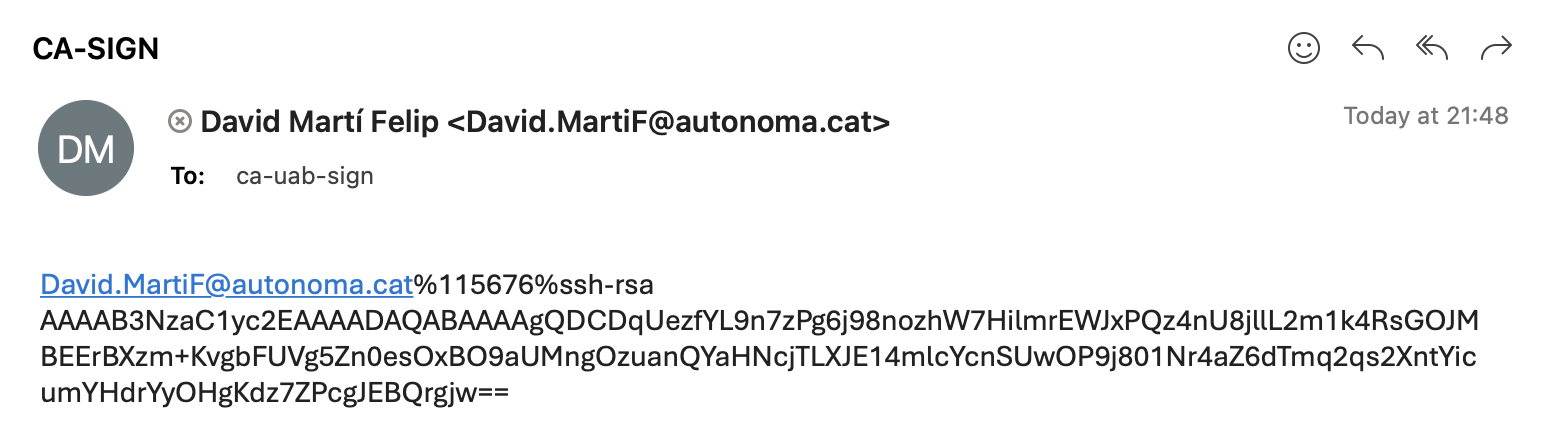
I obtenim :

Per tant canviarem el camp de professió per el valor “115676”.

Així ens quedarà el certificat modificat:

**Certificat modificat** : [David.MartiF@autonoma.cat](mailto:David.MartiF@autonoma.cat) + valor trobat(“115676”) + clau pública del nostre certificat + “CA-UAB” + clau publica CA + data d’expiració

Ara si, enviarem aquest certificat de nou a la CA per a que ens el firmi, ja que aquest si que conté el nostre correu. Rebrem un certificat firmat del que només en volem la firma:

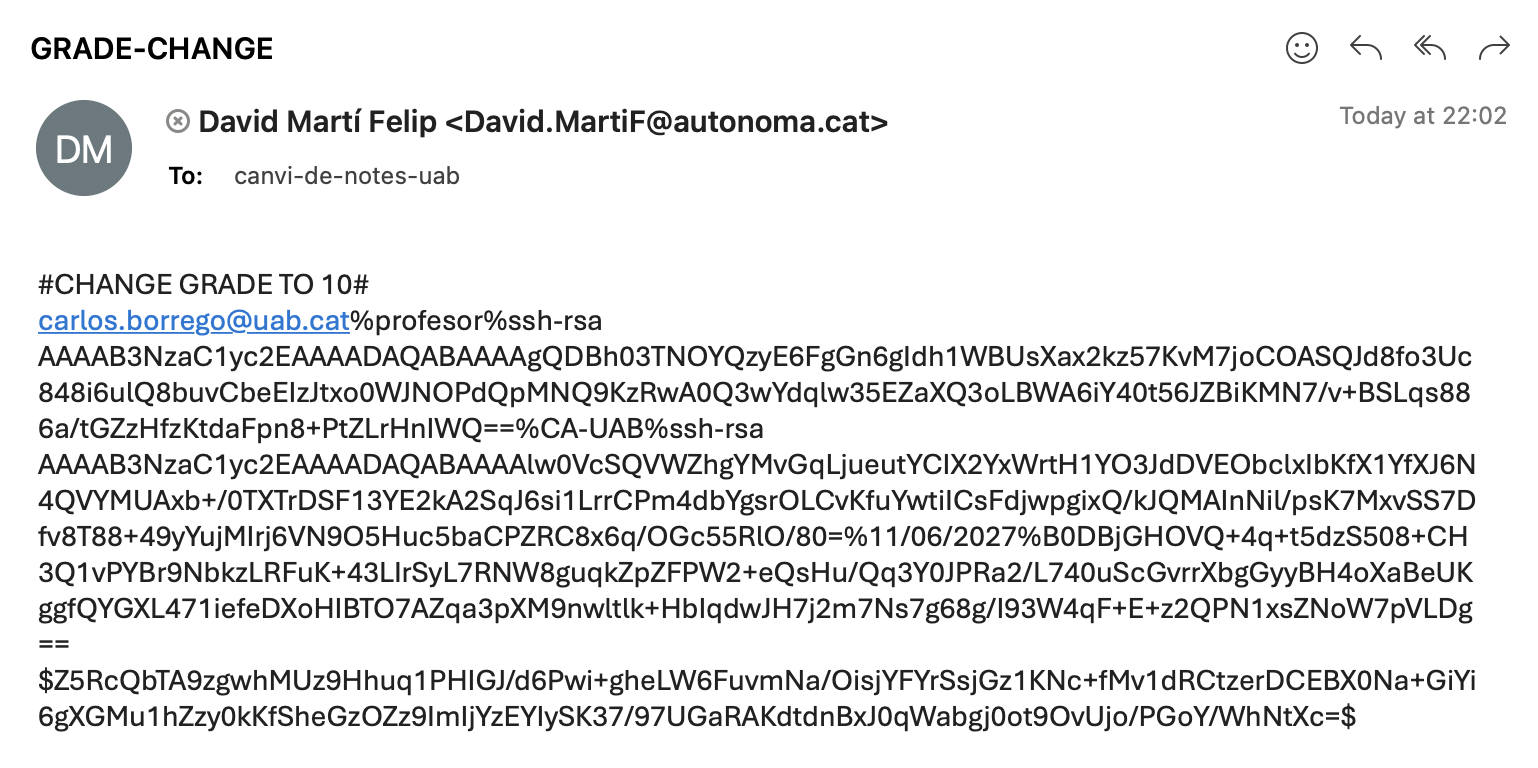


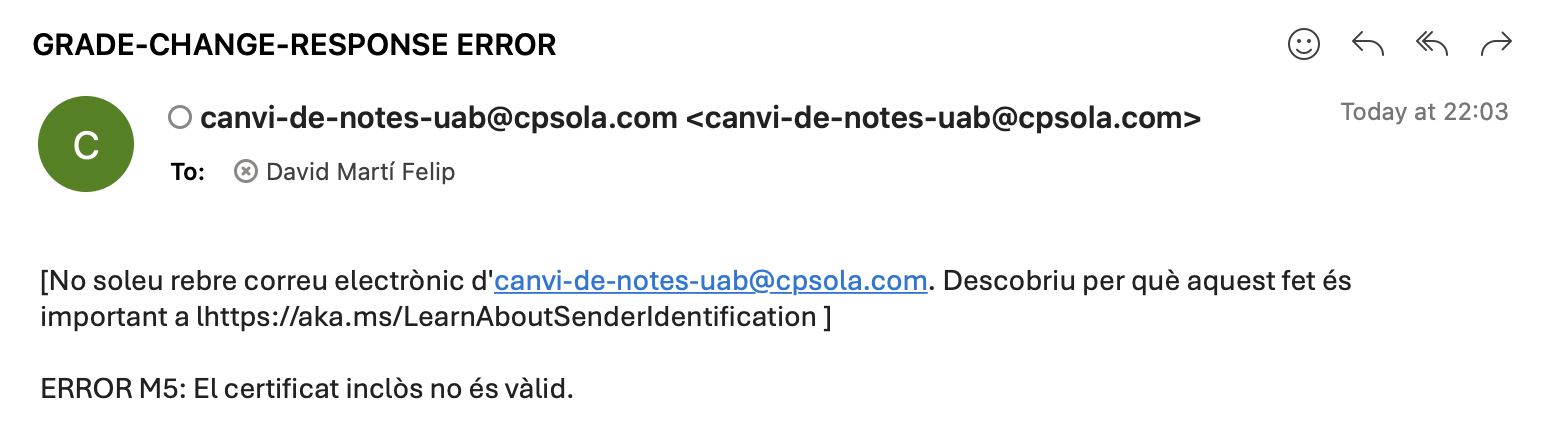


Ara usem la firma rebuda per afegir-la al certificat creat del professor

**Certificat del professor**: “[carlos.borrego@uab.cat”](mailto:carlos.borrego@uab.cat) + “professor” + clau pública del nostre certificat + “CA-UAB” + clau pública CA + data d’expiració + Signatura del certificat modificat

Aquest certificat l’enviem a l’adreça [canvi-de-notes-uab@eines.uab.es](mailto:canvi-de-notes-uab@eines.uab.es) amb l’string “#CHANGE TO GRADE 10#” a la primera línia, el certificat a la segona i la cadena del principi xifrada amb la nostra clau privada al final. D’assumpte del correu posem “GRADE-CHANGE”.

Després de repetir diverses vegades el procés complert i provar canvis en el codi, escrivint a mà part dels correus i canviant els encoders al script python, sempre acabem rebent la resposta següent:



Així doncs, hem decidit deixar el nostre procediment durant la pràctica detallat en aquest document per a que quedi reflectit el nostre coneixement dels passos a seguir i quin ha estat el nostre camí.

# Part 3: Dels certificats a la PKI

**Els certifcats X.509 són un estàndard que es fa servir en la majoria de protocols que requereixen certicats digitals. Investigueu quins són els camps bàsics que conté un certifcat X.509 i indiqueu quins canvis caldria fer als certifcats d'aquesta pràctica per tal d'adaptar-los a l'estàndard.**

Un certificat X.509 conté els següents camps:

* Version: *Indica la verió de standard*
* Serial number: *és un nombre únic (com un ID) assignat al certificat per la CA*
* Signature Algorithm: *és l’algoritme que s’utilitza per a firmar el certificat*
* Issuer: *entitat de la CA (“CA-UAB” en el nostre cas)*
* Validity: *No només tenim data de caducitat sinó que també una data d’inici de validesa.*
  + Not before
  + Not After
* Subject: *Identitat del propietari (en el nostre cas el correu)*
* Subject Public Key Info
  + Public Key Algorithm: *Algoritme de clau pública (p.e. RSA)*
  + Subject Public Key: *Clau pública del propietari*
* Extensions (optional)
* Signature

Per a adaptar el nostre certificat als standards X.509 caldria afegir-hi els camps de **Version, Serial Number, Signature Algorithm,** la data **Not before, Public key algorithm** i un espai per **extensions.** A més d’odenar-lo tal i com ho fa l'Standard.