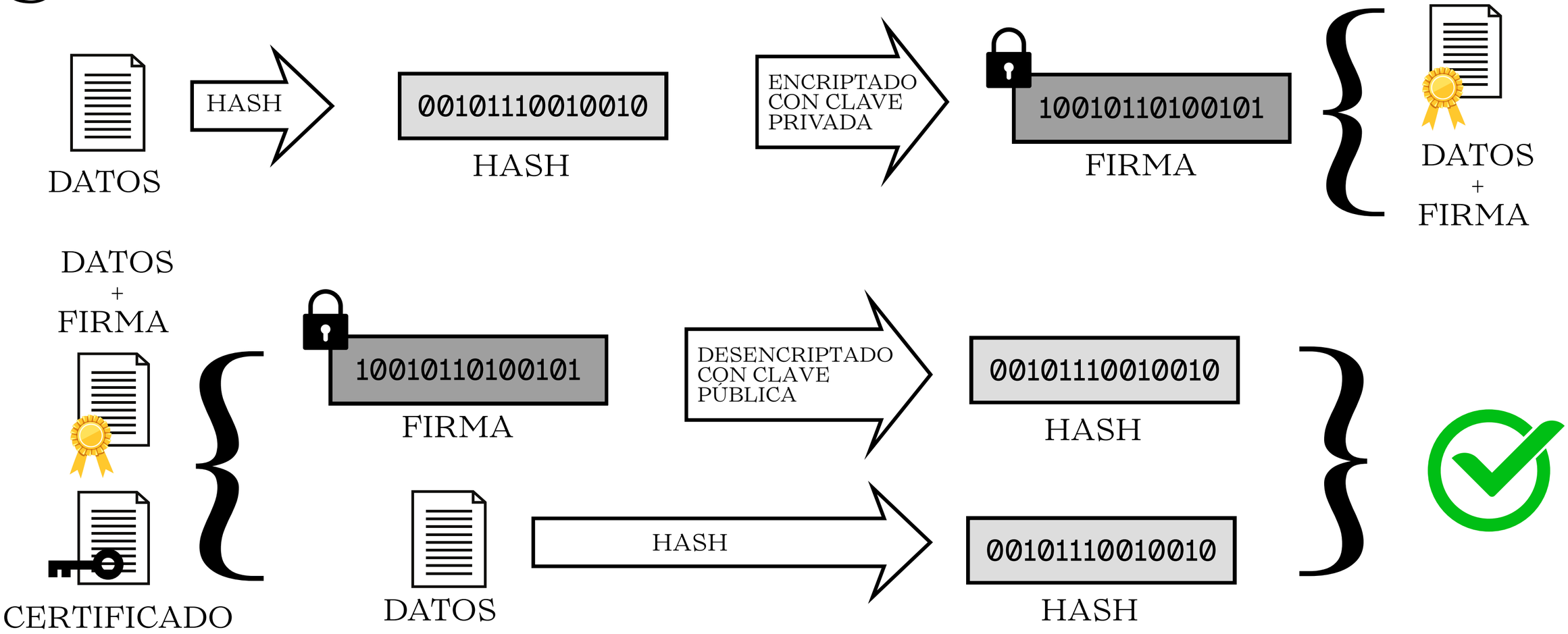
Firma Digital

Sistema de Firma digital

Presentado por Marcos Fraile y Arturo Francés

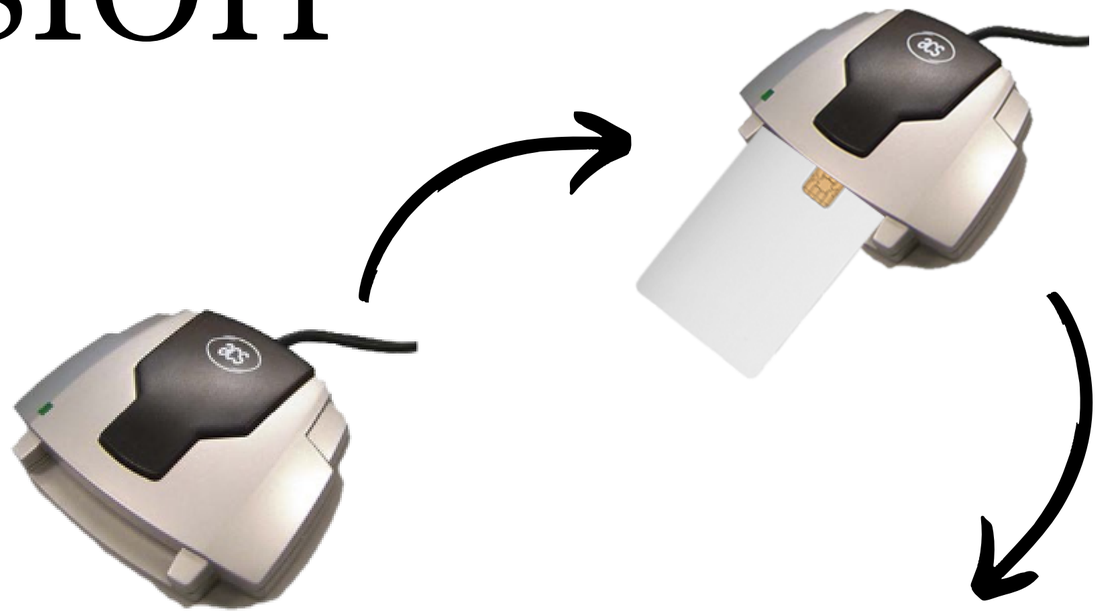
Funcionamiento general



Inicio de sesión

```python
# Esperamos un lector disponible.
lectores = False
leido = False
while not lectores:
    lectores = readers()
    lector = lectores[0] if lectores else None
    if not lectores and not leido:
        print("\nEsperando lector...")
        leido = True
    elif lectores:
        print("Lectura correcta por: ", lector)

# Esperamos a que se introduzca un DNI por el lector.
slots = False
leido = False
while not slots:
    slots = pkcs11.getSlotList(tokenPresent=True)
    slot = slots[0] if slots else None
    if not slots and not leido:
        print("\nEsperando tarjeta...")
        leido = True
    elif slots:
        print("Tarjeta detectada en la ranura: ", slot)
```



```python
# Introducimos el PIN e iniciamos sesión.
password = None
while not password:
    password = getpass.getpass("\nIntroduce el PIN del DNIe: ")

sesion = pkcs11.openSession(slot)
sesion.login(password)
print('\nInicio correcto')
return sesion
```

Exportación de certificados

```python
# Buscamos los certificados disponibles en el DNIe
certificados = sesion.findObjects([(PyKCS11.CKA_CLASS, PyKCS11.CKO_CERTIFICATE)])
if not certificados:
    raise Exception("No se encontró ningún certificado en el DNIe.")

# Buscamos el certificado de firma
for certificado in certificados:
    cert_der = bytes(sesion.getAttributeValue(certificado, [PyKCS11.CKA_VALUE], True)[0])
    cert = x509.load_der_x509_certificate(cert_der, default_backend())
    subject = cert.subject.rfc4514_string().upper()

    if "FIRMA" in subject:
        cert = certificado
        break
```

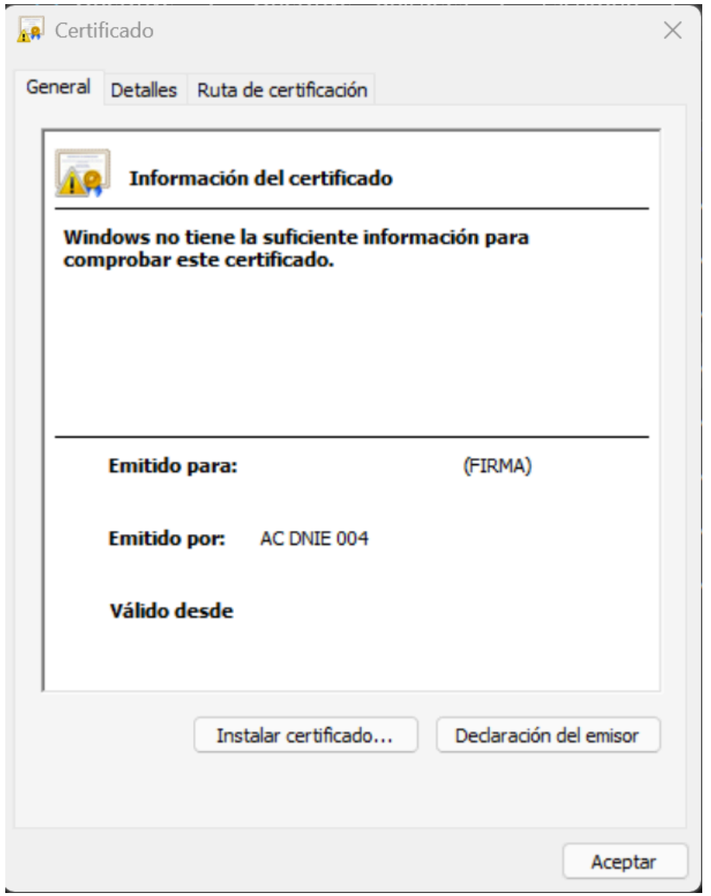
```
Certificados encontrados:

CertAutenticacion
CertCAIntermediaDGP
CertFirmaDigital
```

Exportación de certificados

```python
# Exportamos el cetificado en formato DER
with open("certificado.der", "wb") as f:
        f.write(cert_der)

# Exportamos el cetificado en formato PEM
b64 = base64.b64encode(cert_der).decode('ascii')
pem = "-----BEGIN CERTIFICATE-----\n" + "\n".join(textwrap.wrap(b64, 64))
+ "\n-----END CERTIFICATE-----\n"
with open("certificado.pem", "w") as f:
    f.write(pem)
```



.pem

```
-----BEGIN CERTIFICATE-----
LnBvbGljaWEuZXMvZG5pZS9wdWJsaWNhY2lvbmVzL2RwYzBABggrBgEFBQcCAjA0
DDJESVJFQ0NJw5NOIEdFTkVSQUwgREUgTEEgUE9MSUPDjUEsIFZBVEVTLVMyODE2
MDE1SDCB8AYIKwYBBQUHAQIEgeMwgeAwMgIBATALBglghkgBZQMEAgEEINVD7RQn
zkxap/q0r1E7OpvVseQ6kCDtu3SXQDH1+wBEMDICAQAwCwYJYIZIAWUDBAIBBCC9
YqYWr7/Fbr0kkRhQ7mLfI+vsmnpn5u8DNt45SkAI2jA6BglghVQBAgIEAgEwCwYJ
jKJcyuk+6P1IJgu1qQbm+vsFL1tRvppt1D8xOG6BTDi0HHlqUsQarCpp10vtw5qs
-----END CERTIFICATE-----
```

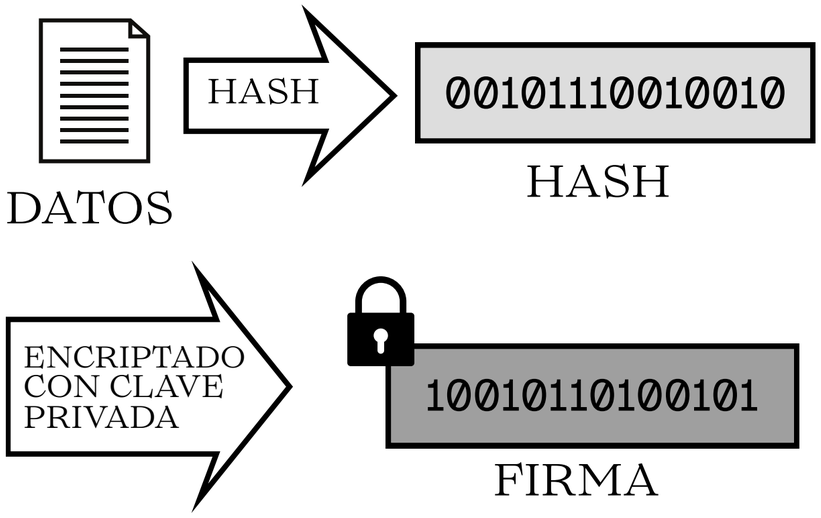
.der

Firma de archivos

```python
# Buscamos la clave privada de FIRMA en el DNIe.
claves_privadas = sesion.findObjects([(PyKCS11.CKA_CLASS, PyKCS11.CKO_PRIVATE_KEY)])
for clave in claves_privadas:
    label = sesion.getAttributeValue(clave, [PyKCS11.CKA_LABEL])[0]
    if label == "KprivFirmaDigital":
        clave_privada = clave
        break
```

```
Claves privadas encontradas:

KprivAutenticacion
KprivFirmaDigital
```



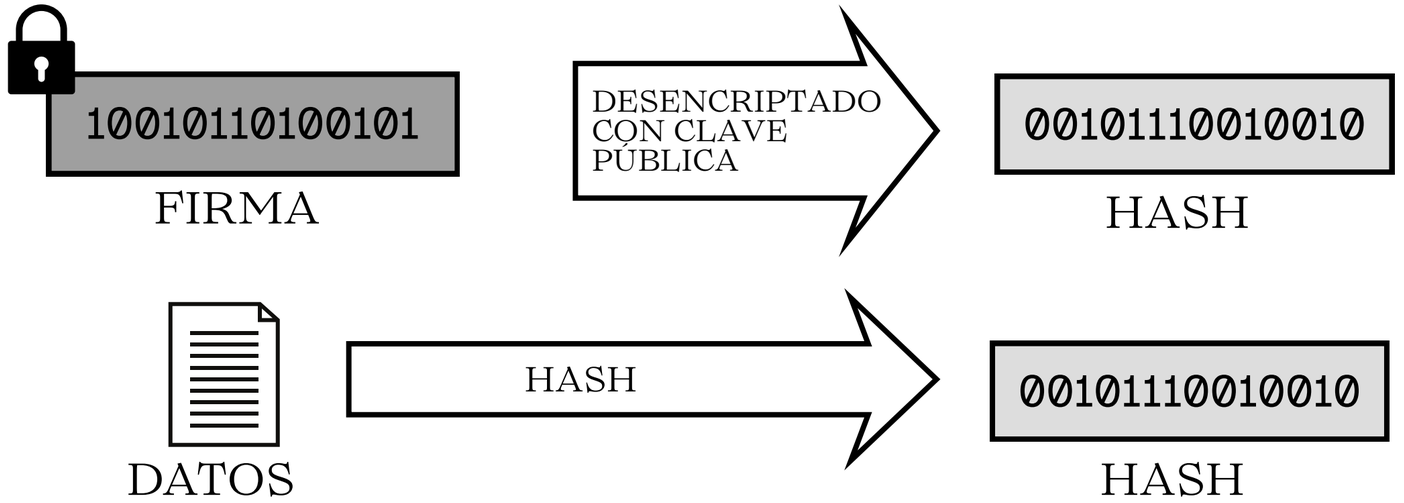

```python
for archivo in archivos:
    with open(archivo, "rb") as f:
        data = f.read()

    # Firmamos el documento.
    mechanism = PyKCS11.Mechanism(PyKCS11.CKM_SHA256_RSA_PKCS, None)
    firma_raw = bytes(sesion.sign(clave_privada, data, mechanism))
    firma = archivo + ".sig"
    with open(firma, "wb") as f:
        f.write(firma_raw)
```

Verificación de firma

```python
# Cargamos el certificado, el documento y la firma.
with open("certificado.der", "rb") as f:
    der = f.read()
    certificado = x509.load_der_x509_certificate(der, default_backend())
with open(archivo, "rb") as f:
    data = f.read()
with open(sig_file, "rb") as f:
    signature = f.read()
```

```python
# Verificamos la firma
try:
    clave_publica = certificado.public_key()
    clave_publica.verify(
        signature,
        data,
        padding.PKCS1v15(),
        hashes.SHA256()
        )
```



Interfaz


Profesor Oak


Heracross ♂ Nv35
PS
Sia ♀ Nv42
PS
179/ 179
Elige una opción:
Firmar
Verificar
Exportar
Salir


ARCHIVO
CARPETA
Elige que quieres firmar:

Qué pasa si bloqueas el pin