CSE350: Programming Assignment 4

Ananya Lohani (2019018), Mihir Chaturvedi (2019061)

INDRAPRASTHA INSTITUTE *of*
INFORMATION TECHNOLOGY
DELHI

Background

Digital Signatures

Digital signatures are electronic signatures that prove the authenticity of digital documents like PDFs. To sign a PDF with a digital signature, a unique code is generated based on the document's content. This code is encrypted using the signer's private key, creating the digital signature, which is embedded within the PDF.

When the recipient receives the signed PDF, they verify the signature against already present, trusted certificates. If it does, then the signature is valid, and the document is considered authentic and unchanged since it was signed.

PKCS#7 Standard

The PKCS#7 standard is a technical specification for digitally signing and encrypting data. It provides a standard syntax for digital signatures and encryption messages using public-key cryptography, allowing multiple signers to sign the same data object. PKCS#7 is widely used in security protocols such as S/MIME, TLS, and secure PDF documents.

Steps to Digitally Sign a PDF

1. Generate a signature placeholder of the required signature length and properties (signer info) in the PDF.
2. Check if the pdf already contains an acroform field, and extract the acroform ID and field IDs if it exists.
3. Generate a signature annotation widget with the signature placeholder, and add it to the page.
4. Create or extend the existing acroform with the new widget, and link it to the root.
5. Create a signed PKCS#7 message (using libraries like node-forge) and replace the /ByteRange and /Contents sections (the placeholder) in the PDF with the signed message.
6. Save the PDF by writing it to the file system.

Important Questions

1. How and where do you get the correct GMT date and time? Is the source reliable and the GMT date and time obtained in a secure manner?

Use new Date() in Node.js to obtain the current date and time in the server's local timezone. This method is secure and reliable as it depends on the system clock and is built into JavaScript. It ensures high accuracy and precision without being affected by network latency or server response times.

2. How do you ensure that only the graduate is able to download it (by providing information beyond the roll no, such as date of birth, home pin code, etc.?

Implement secure JSON Web Token (JWT) authentication to verify a graduate's identity. Require the student to input their roll number (as username) and home pin code (as password). The server then checks the entered credentials against the stored data in the database to authenticate the student.

Important Questions

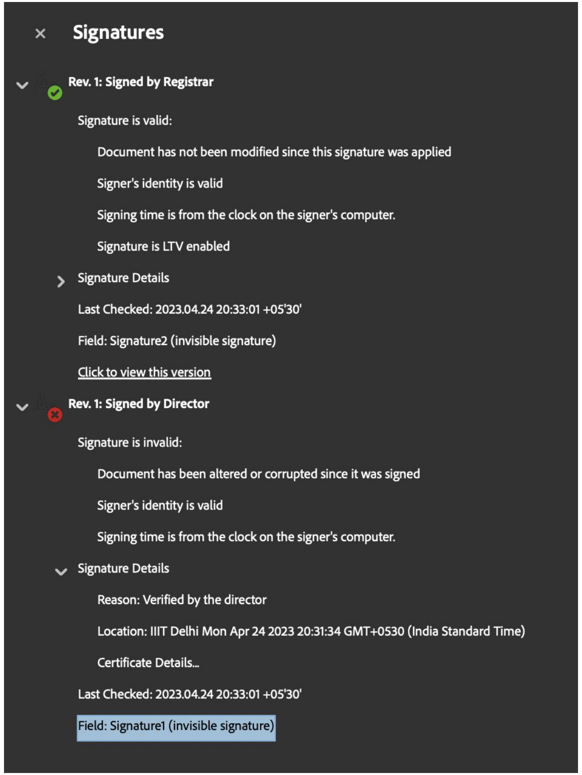
3. Should the graduate decide to share the document with others, how can one trace the origin of the document (could watermarks be useful?)?

Embed unique, identifiable digital watermarks in the documents during the signing process. These watermarks contain information about the signer and the signing date and time, making it possible to trace the origin and verify the authenticity of the shared document.

4. Do we need to have access to public-keys, and if so how?

Access the signer's PKCS#12 file (.p12 extension), which contains the public key, private key, and digital certificate necessary for document integrity. The .p12 file is passphrase-protected, with the server storing the passphrase in the .env file. The server uses the private key to sign the documents, along with the current date and time.

Verified Signatures on Adobe Acrobat



Rev. 1: Signed by Registrar

Signature is valid:

Document has not been modified since this signature was applied

Signer's identity is valid

Signing time is from the clock on the signer's computer.

Signature is LTV enabled

Signature Details

Last Checked: 2023.04.24 20:33:01 +05'30'

Field: Signature2 (invisible signature)

Click to view this version

Rev. 1: Signed by Director

Signature is invalid:

Document has been altered or corrupted since it was signed

Signer's identity is valid

Signing time is from the clock on the signer's computer.

Signature Details

Reason: Verified by the director

Location: IIIT Delhi Mon Apr 24 2023 20:31:34 GMT+0530 (India Standard Time)

Certificate Details...

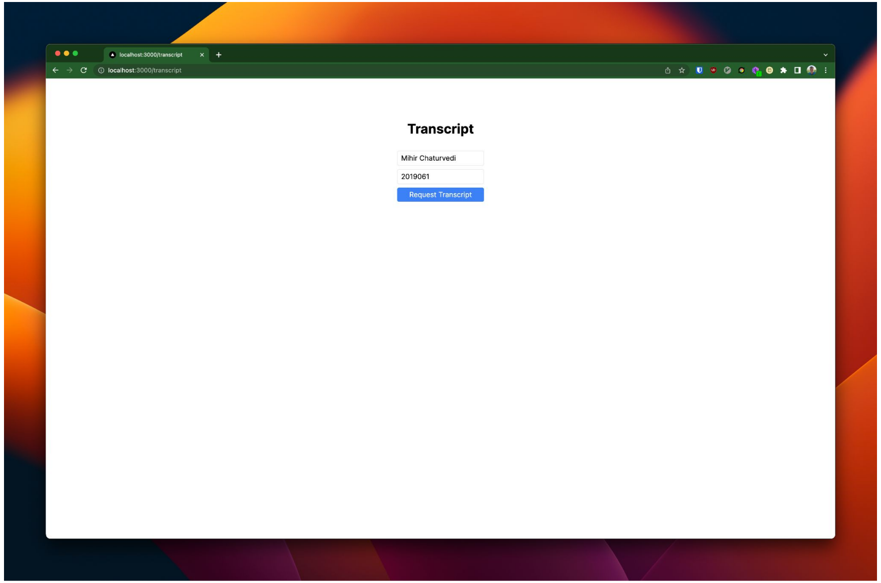
Last Checked: 2023.04.24 20:33:01 +05'30'

Field: Signature1 (invisible signature)

When a PDF document is signed, it is possible to make changes to the document without invalidating the original signature. This is because PDFs support incremental updates, which means that when changes are made to the document, they are appended to the end of the file without overwriting the previous content.

As a result, each revision of the PDF is valid and can be verified independently of the other revisions. If a PDF document has multiple signatures, each signature applies only to the revision of the document that existed when it was signed. Any changes made to the document after that point will not be reflected in the signature.

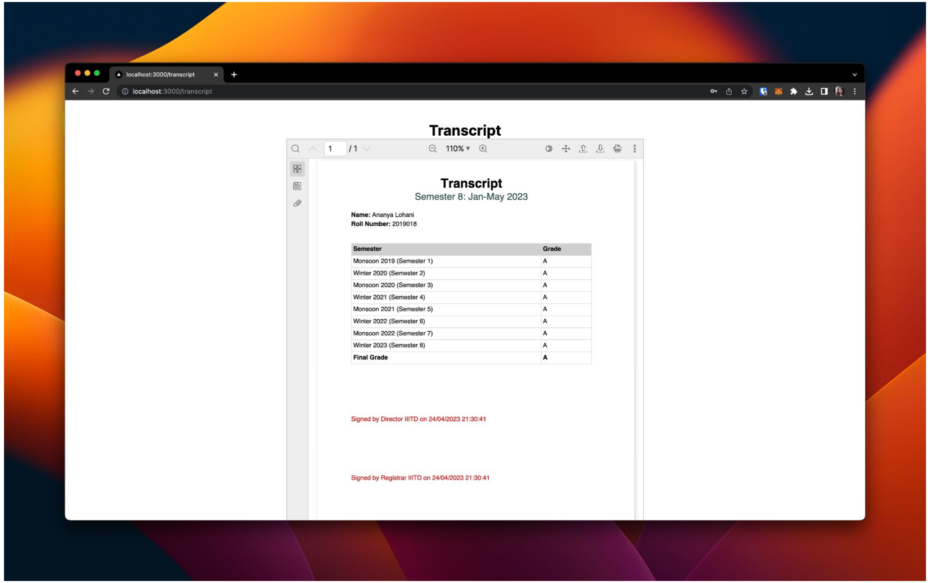
Screenshots (Webapp)



Transcript

Mihir Chaturvedi

2019061



Transcript

Transcript

Semester 8: Jan-May 2023

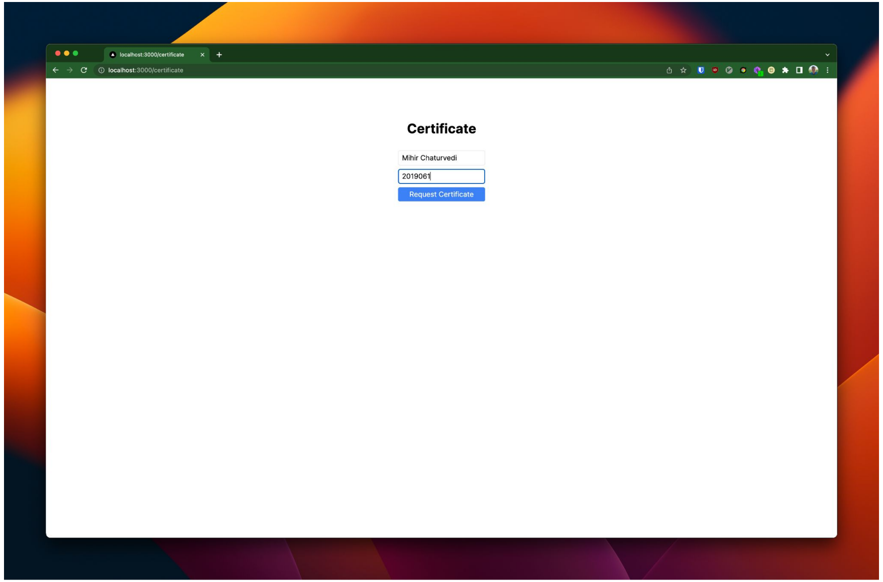
Name: Ananya Lohani
Roll Number: 2019018

Semester	Grade
Monsoon 2019 (Semester 1)	A
Winter 2020 (Semester 2)	A
Monsoon 2020 (Semester 3)	A
Winter 2021 (Semester 4)	A
Monsoon 2021 (Semester 5)	A
Winter 2022 (Semester 6)	A
Monsoon 2022 (Semester 7)	A
Winter 2023 (Semester 8)	A
Final Grade	**A**

Signed by Director IIITD on 24/04/2023 21:30:41

Signed by Registrar IIITD on 24/04/2023 21:30:41

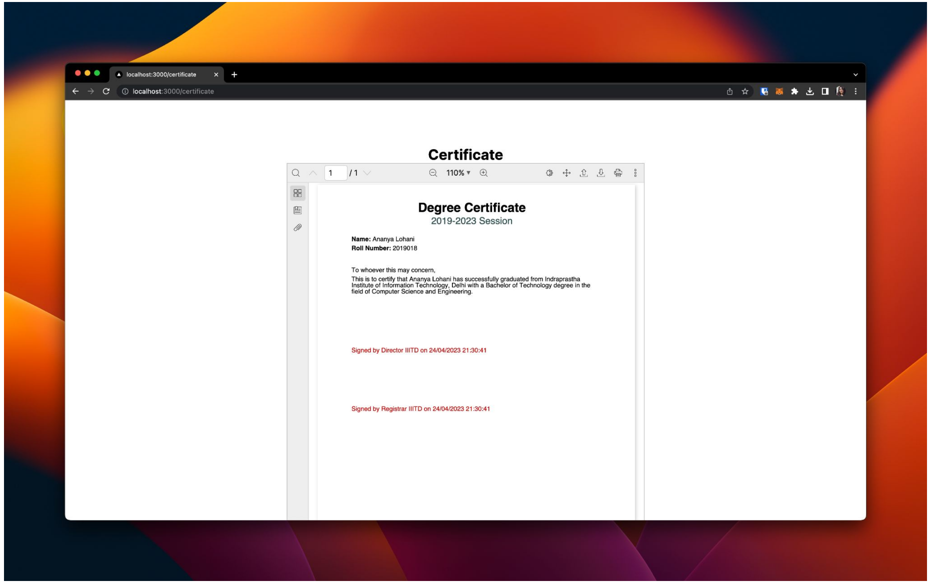
Screenshots (Webapp)



Certificate

Mihir Chaturvedi

2019061



Certificate

Degree Certificate

2019-2023 Session

Name: Ananya Lohani
Roll Number: 2019018

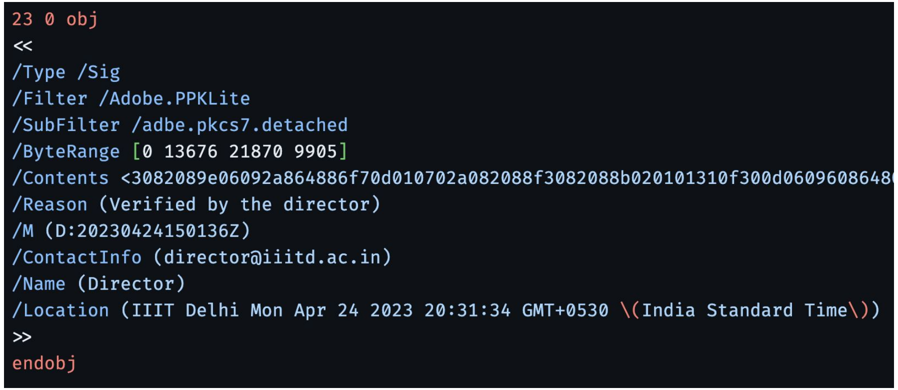
To whoever this may concern,

This is to certify that Ananya Lohani has successfully graduated from Indraprastha Institute of Information Technology, Delhi with a Bachelor of Technology degree in the field of Computer Science and Engineering.

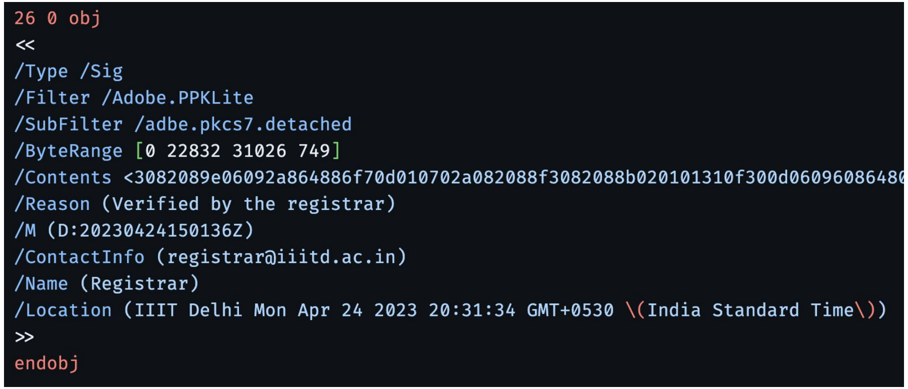
Signed by Director IIITD on 24/04/2023 21:30:41

Signed by Registrar IIITD on 24/04/2023 21:30:41

Screenshots (RAW PDF File after signing)



```
23 0 obj
<<
/Type /Sig
/Filter /Adobe.PPKLite
/SubFilter /adbe.pkcs7.detached
/ByteRange [0 13676 21870 9905]
/Contents <3082089e06092a864886f70d010702a082088f3082088b020101310f300d060960864800
/Reason (Verified by the director)
/M (D:20230424150136Z)
/ContactInfo (director@iiitd.ac.in)
/Name (Director)
/Location (IIIT Delhi Mon Apr 24 2023 20:31:34 GMT+0530 \(India Standard Time\))
>>
endobj
```



```
26 0 obj
<<
/Type /Sig
/Filter /Adobe.PPKLite
/SubFilter /adbe.pkcs7.detached
/ByteRange [0 22832 31026 749]
/Contents <3082089e06092a864886f70d010702a082088f3082088b020101310f300d060960864800
/Reason (Verified by the registrar)
/M (D:20230424150136Z)
/ContactInfo (registrar@iiitd.ac.in)
/Name (Registrar)
/Location (IIIT Delhi Mon Apr 24 2023 20:31:34 GMT+0530 \(India Standard Time\))
>>
endobj
```