

DIRECTORATE OF EDUCATION



Digital Signatures

The Paper System

Documents

- A paper document consists of four components
 - the carrier (the sheet of paper)
 - text and pictures (the physical representation of information)
 - information about the originator
 - measures to verify the authenticity (written signature)
- All the four components are physically connected
 - So, paper is the document
- There is only one original
 - can be reproduced in innumerable copies

The Paper System

Signature

- Supposed to be unique, difficult to be reproduced, not changeable and not reusable
- Its main functions
 - identification
 - declaration
 - proof
- The signature is used to identify a person and to associate the person with the content of that document
 - always related to a physical person

The Paper System

Signature (*contd*)

- In all legal systems
 - No exclusive method of signing e.g. Full name, initials, nickname, real or any symbol.
 - Token of will and responsibility
- From a legal point of view, nothing against the introduction of new types or technologies of signature
 - Digital Signature is a new technology

Electronic System

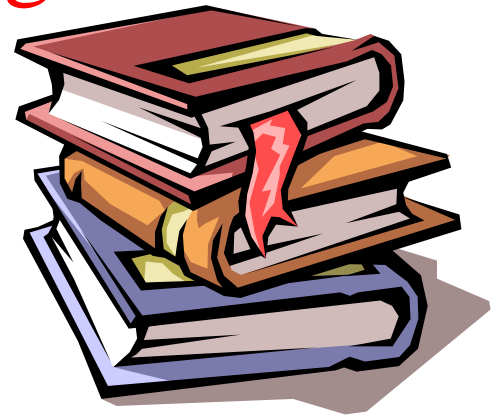
- Electronic document produced by a computer and stored in digital form.
 - It can be deleted, modified and rewritten without leaving a mark
 - Integrity of an electronic document is impossible to verify.

Electronic System

- Digital signatures created and verified using unbreakable coding
- A programme generates two different and related keys
 - Public key
 - Private Key
- Private key used to digitally sign.
- Public key used to verify.

Electronic Record

1. Very easy to make copies
2. Very fast distribution
3. Easy archiving and retrieval
4. Copies are as good as original
5. Easily modifiable
6. Environmental Friendly



Because of 4 & 5 together, these lack authenticity

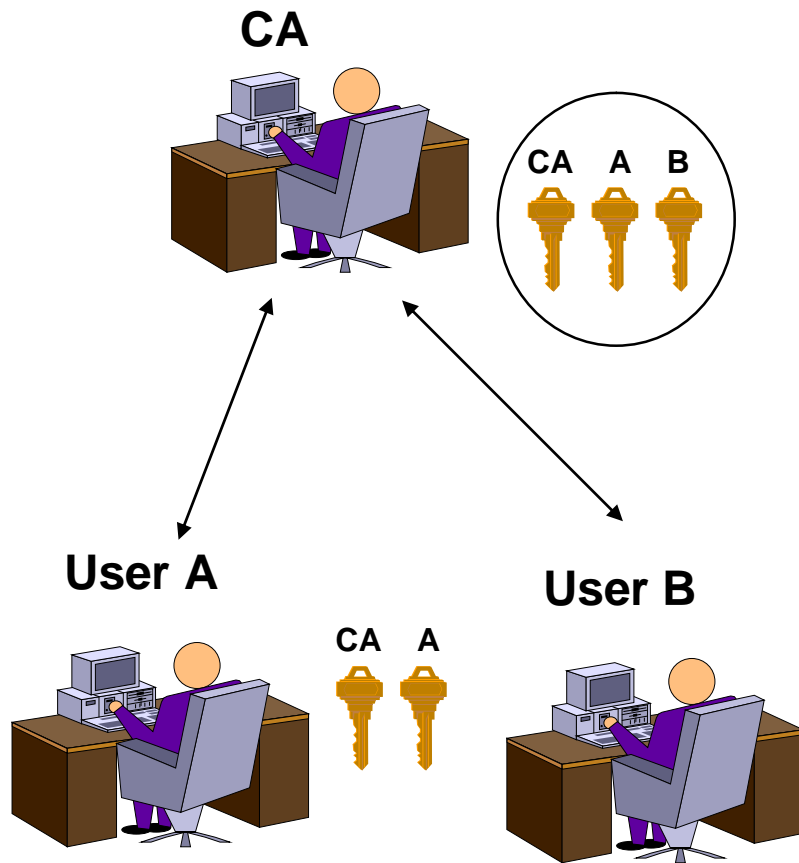
Public Key Infrastructure

- Allow parties to have free access to the signer's public key
- This assures that the public key corresponds to the signer's private key
 - Trust between parties even if they do not know one another
- Parties should have highest level of trust in one another. This creates the need of certifying authority.

Certifying Authorities

- A CA is an Authority which :
 - identifies persons applying for key certificates (signatures)
 - verifies their legal capacity
 - confirm the identity of a person to whom a public signature key belongs.
 - always maintain online access to the signature key certificates with the agreement of the signature key owner
 - take measures so that the confidentiality of a private signature key is guaranteed

Certificate based Key Management



- Operated by trusted-third party - CA
- Provides Trading Partners Certificates
- Notarises the relationship between a public key and its owner

IT ACT 2000 - Legal recognition of electronic records

4. Legal recognition of electronic records.

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is—

- (a) rendered or made available in an electronic form;
and
- (b) accessible so as to be usable for a subsequent reference.

IT ACT 2000 - Legal recognition of digital signatures

5. Legal recognition of digital signatures.

- Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person (then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

IT ACT 2000 - Use of electronic records and digital signatures in Government and its agencies

- **6. Use of electronic records and digital signatures in Government and its agencies.**

(1) Where any law provides for—

- (a) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;
- (b) the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner;
- (c) the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

IT ACT 2000 - Retention of electronic records

- **7. Retention of electronic records.**
- (1) Where any law provides that documents, records or information shall be retained
- for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if—
 - (a) the information contained therein remains accessible so as to be usable for a subsequent reference;
 - (b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;
 - (c) the details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record are available in the electronic record:

IT ACT 2000 - Publication of rule, regulation, etc., in Electronic Gazette

8. Publication of rule, regulation, etc., in Electronic Gazette.

- Where any law provides that any rule, regulation, order, bye-law, notification or
- any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

IT ACT 2000 - Creation of Digital Signature

Creation of Digital Signature.- To sign an electronic record or any other item of information,

- The resulting Digital Signature shall be unique to both electronic record and e-Token used to create it;
- Digital Signature shall be attached to its electronic record and stored or transmitted with its electronic record.

IT ACT 2000 - Verification of Digital Signature

- The verification software will confirm the Digital Signature as verified if:-
 - (a) the signer's e-Token was used to digitally sign the electronic record,
 - (b) the electronic record was unaltered.

Why Digital Signatures?

- To provide Authenticity, Integrity and Non-repudiation to electronic documents
- To use the Internet as the safe and secure medium for e-Commerce and e-Governance



Digital Signatures

I agree

efcc61c1c03db8d8ea8569545c073c814a0ed755

My place of birth is at Gwalior.

fe1188eecd44ee23e13c4b6655edc8cd5cdb6f25

I am 62 years old.

0e6d7d56c4520756f59235b6ae981cdb5f9820a0

I am an Engineer.

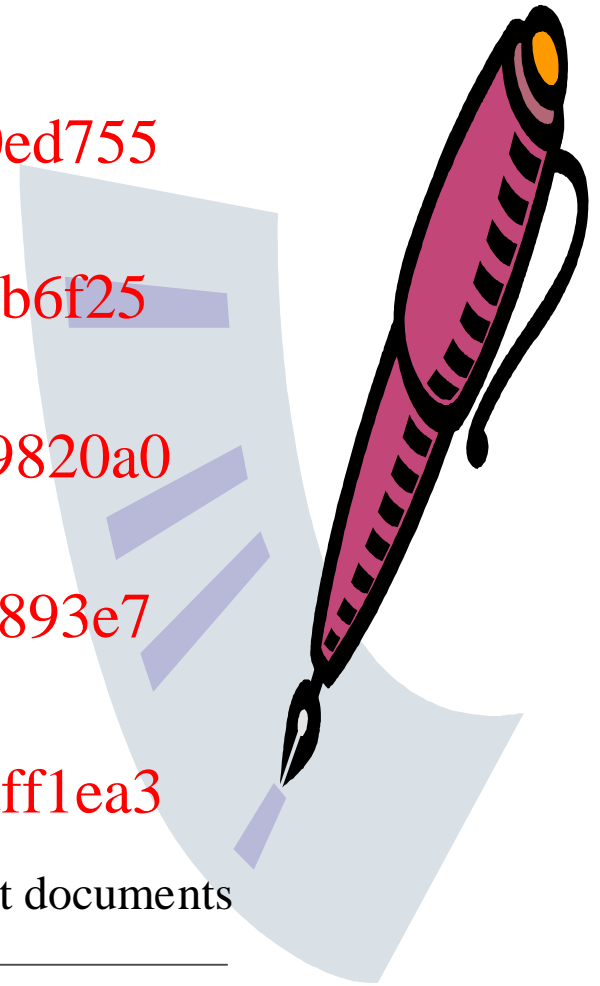
ea0ae29b3b2c20fc018aaca45c3746a057b893e7

I am a Engineer.

01f1d8abd9c2e6130870842055d97d315dff1ea3

- These are digital signatures of same person on different documents

-
- Digital Signatures are numbers
 - Same Length – 40 digits
 - They are document content dependent



Concepts

- **Two numbers of a pair are called keys, the Public Key & the Private Key. User himself generates his own key pair on his computer**
- **Any message irrespective of its length can be compressed or abridged uniquely into a smaller length message called the Digest or the Hash.**
- **Smallest change in the message will change the Hash value**



What is Digital Signature?

- Hash value of a message when encrypted with the private key of a person is his digital signature on that e-Document
 - Digital Signature of a person therefore varies from document to document thus ensuring authenticity of each word of that document.
 - As the public key of the signer is known, anybody can verify the message and the digital signature



Digital Signatures

Each individual generates his own key pair
[Public key known to everyone & Private key only to the owner]



Private Key – Used for making
digital signature

Public Key – Used to verify the
digital signature

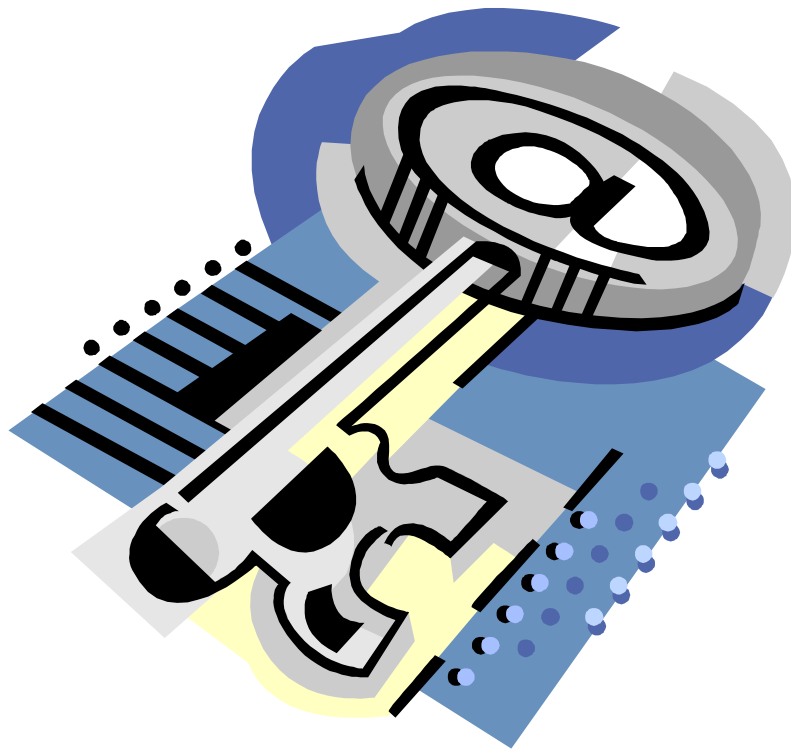
Paper signatures v/s Digital Signatures



V/s



Parameter	Paper	Electronic
Authenticity	May be forged	Can not be copied
Integrity	Signature independent of the document	Signature depends on the contents of the document
Non-repudiation	a. Handwriting expert needed b. Error prone	a. Any computer user b. Error free



- Key Generation
 - Random Numbers
 - RSA Key Pair [Private/Public Key]
- Digital Signature
 - Generate Message Digest [SHA1]
 - Encrypting Digest using Private Key [Signatures]
 - Attaching the Signatures to the message.
- **Verification of Signatures**
 - Run the test for Authentication, Integrity and Non repudiation.
- Digital Signature Certificate
 - ITU X.509 v3

Hardware Tokens



- **They are similar to smart cards in functionality as**
 - **Key is generated inside the token.**
 - **Key is highly secured as it doesn't leave the token.**
 - **Highly portable.**
 - **Machine Independent.**
- **iKEY is one of the most commonly used token as it doesn't need a special reader and can be connected to the system using USB port.**

Hardware Tokens



Cryptography and Confidentiality



- When A uses his own private key, it demonstrates that
 - he wants to sign the document
 - he wants to reveal his identity
 - he shows his will to conclude that agreement
- The encoded message travels on the Net, but nobody can read it : confidentiality

Cryptography and Authentication

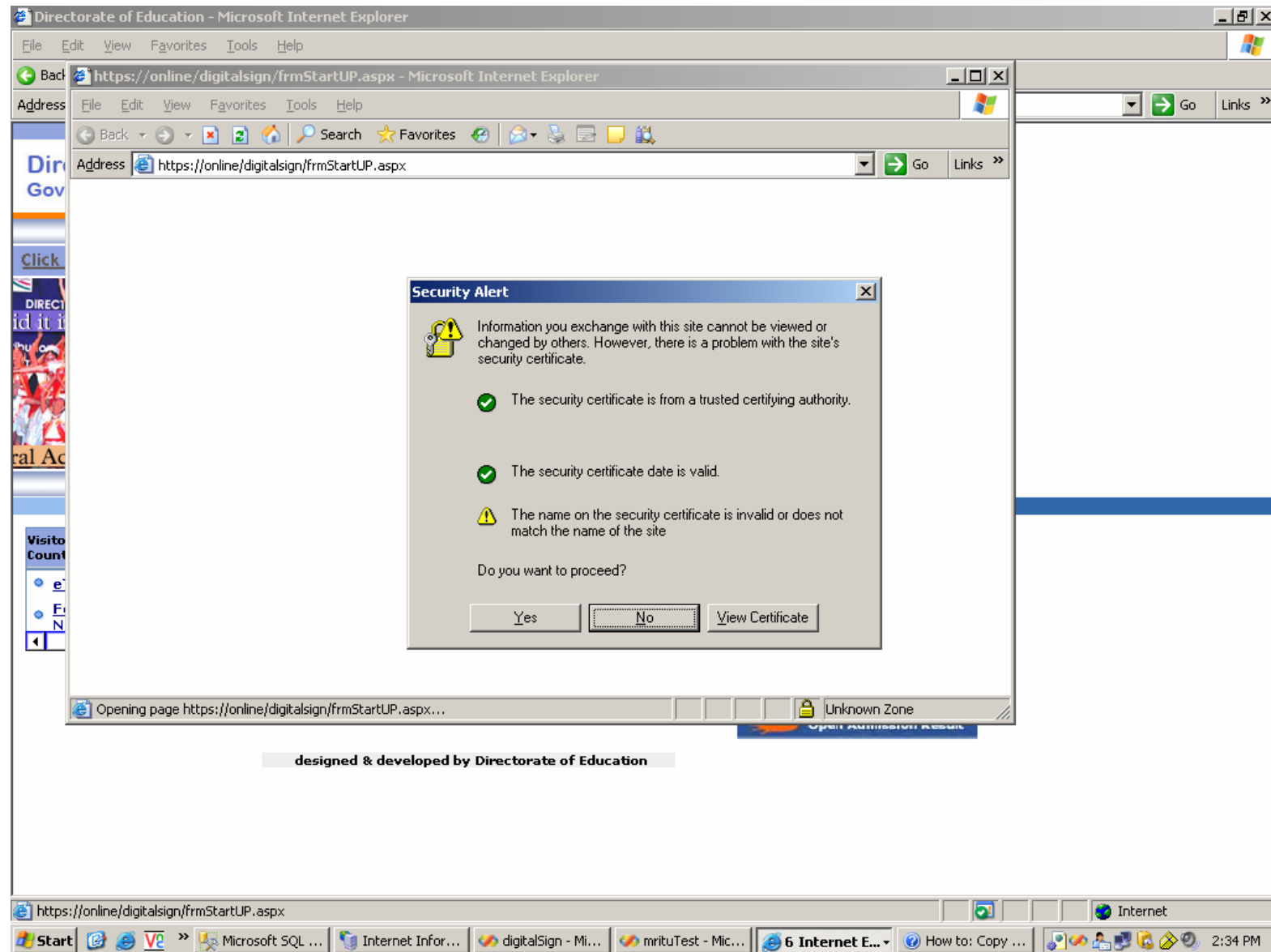


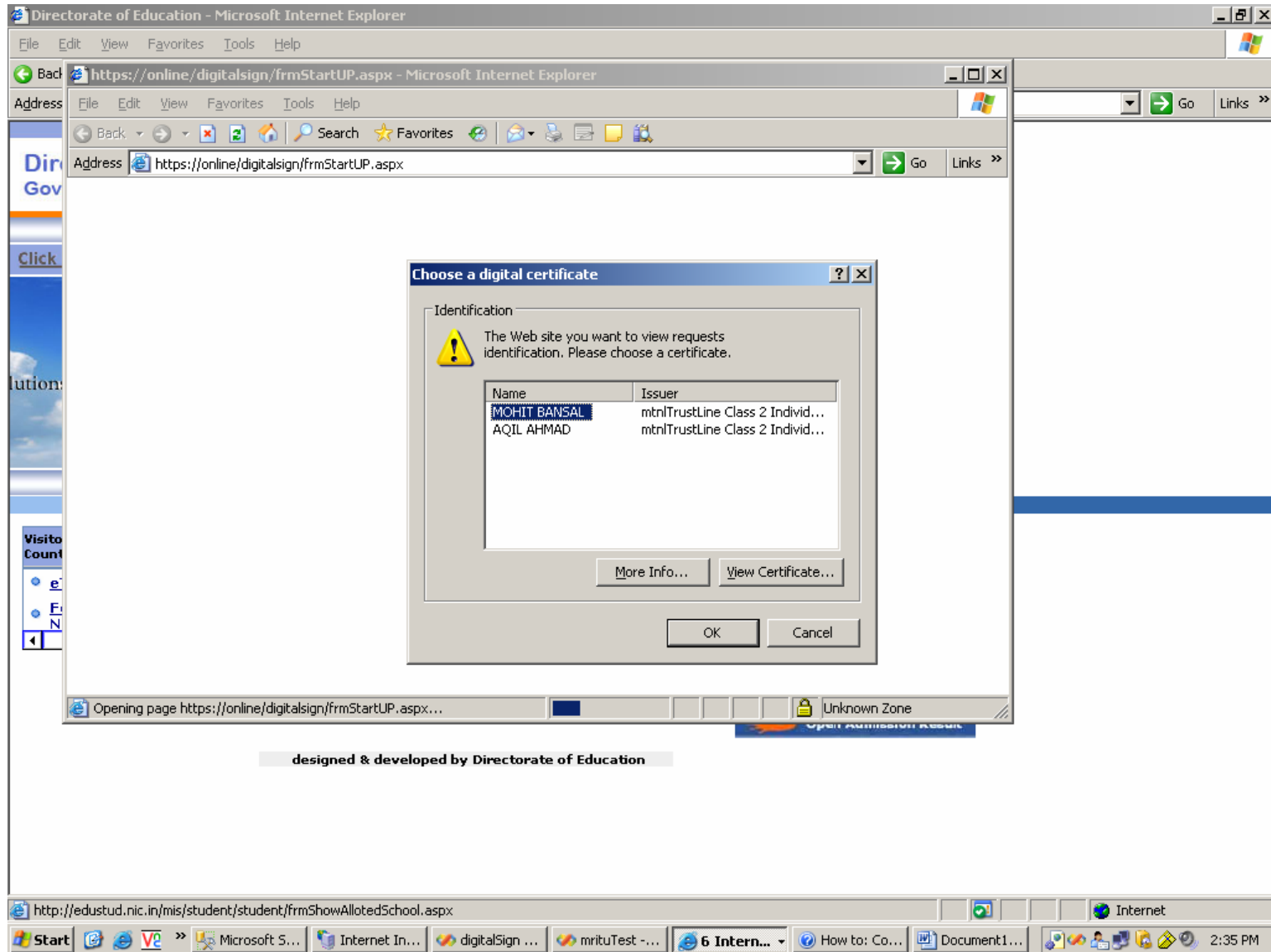
- B needs to know that A and only A sends the message
 - B uses A's public key on the signature
 - Only A's public key can decode the mail
 - A cannot repudiate his signature
- Digital signature cannot be reproduced from the message
- No one can alter a ciphered message without changing the result of the decoding operation

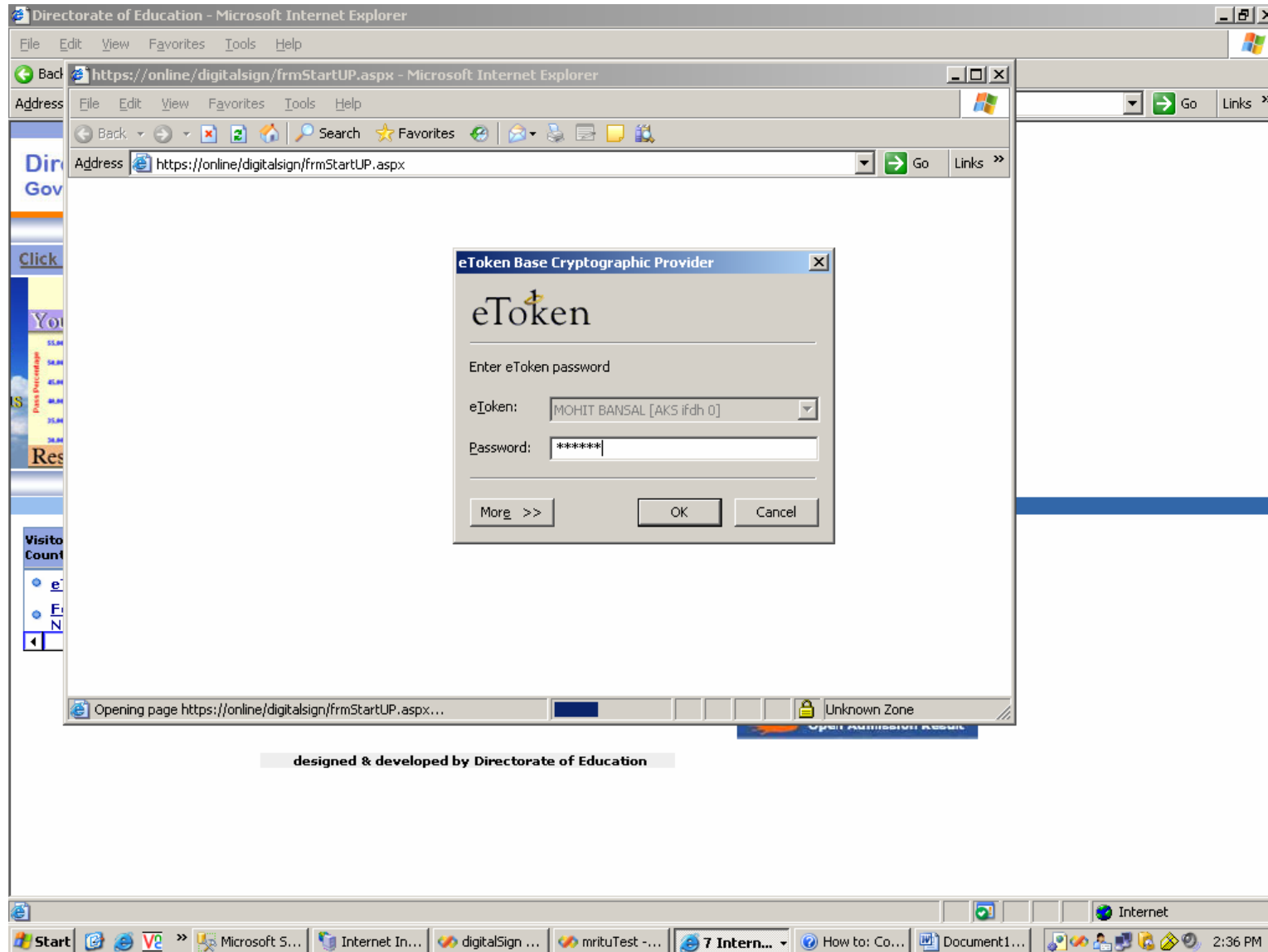
Government Online

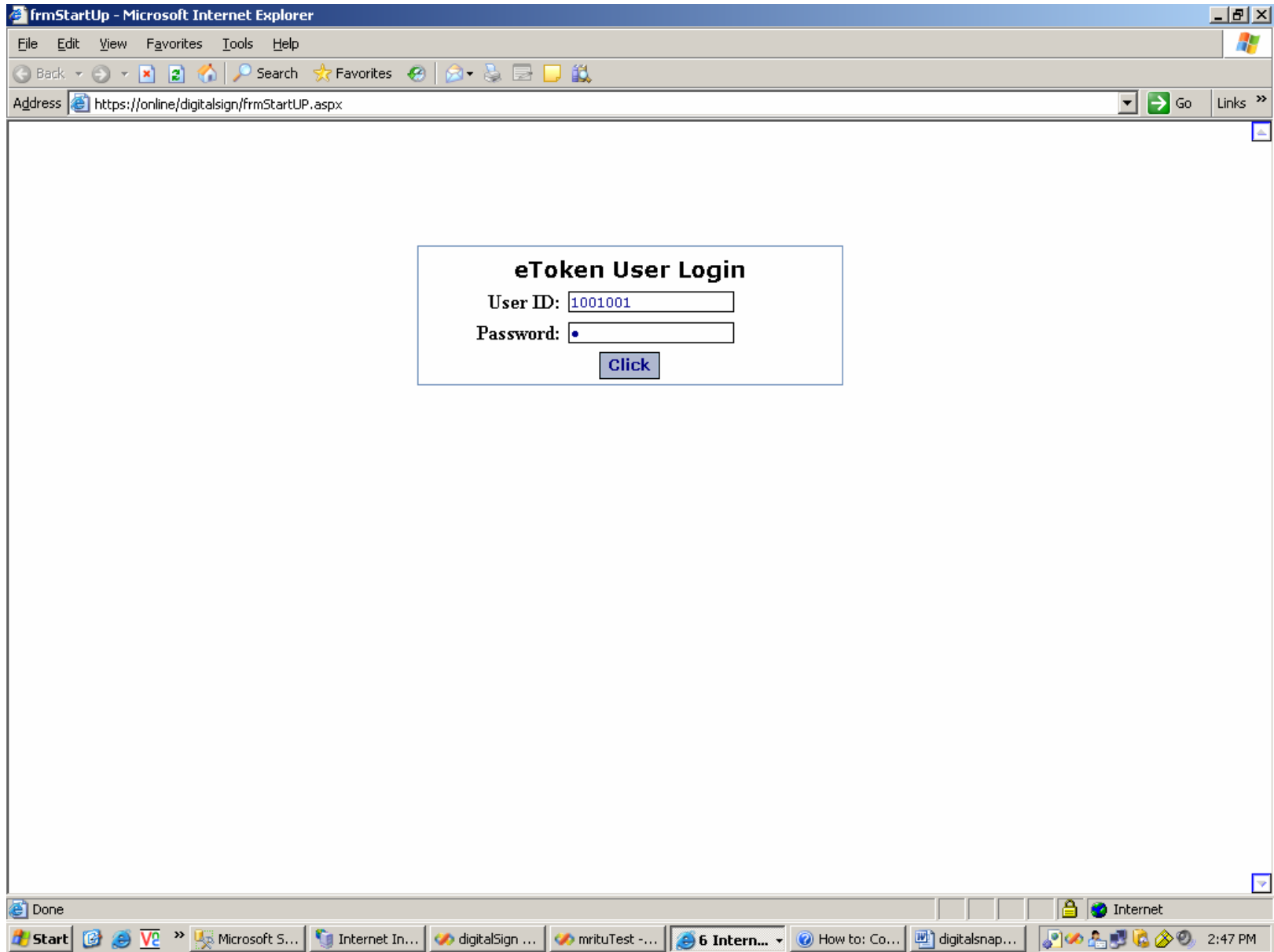
1. Issuing forms and licences
2. Filing tax returns online
3. Online Government orders/treasury orders
4. Registration
5. Online file movement system
6. Public information records
7. E-voting
8. Railway reservations & ticketing
9. E-education
10. Online money orders

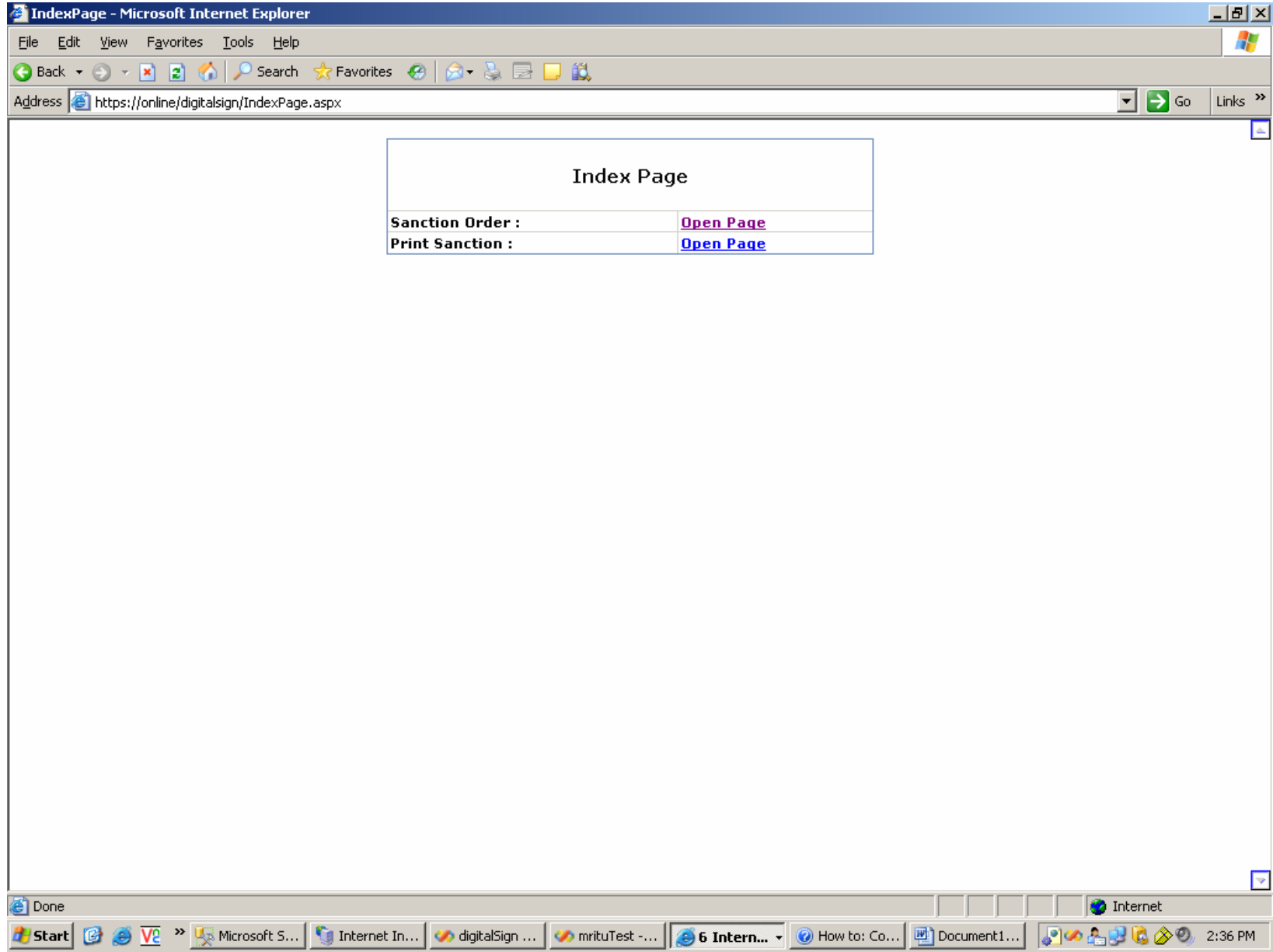
How to use e-Token

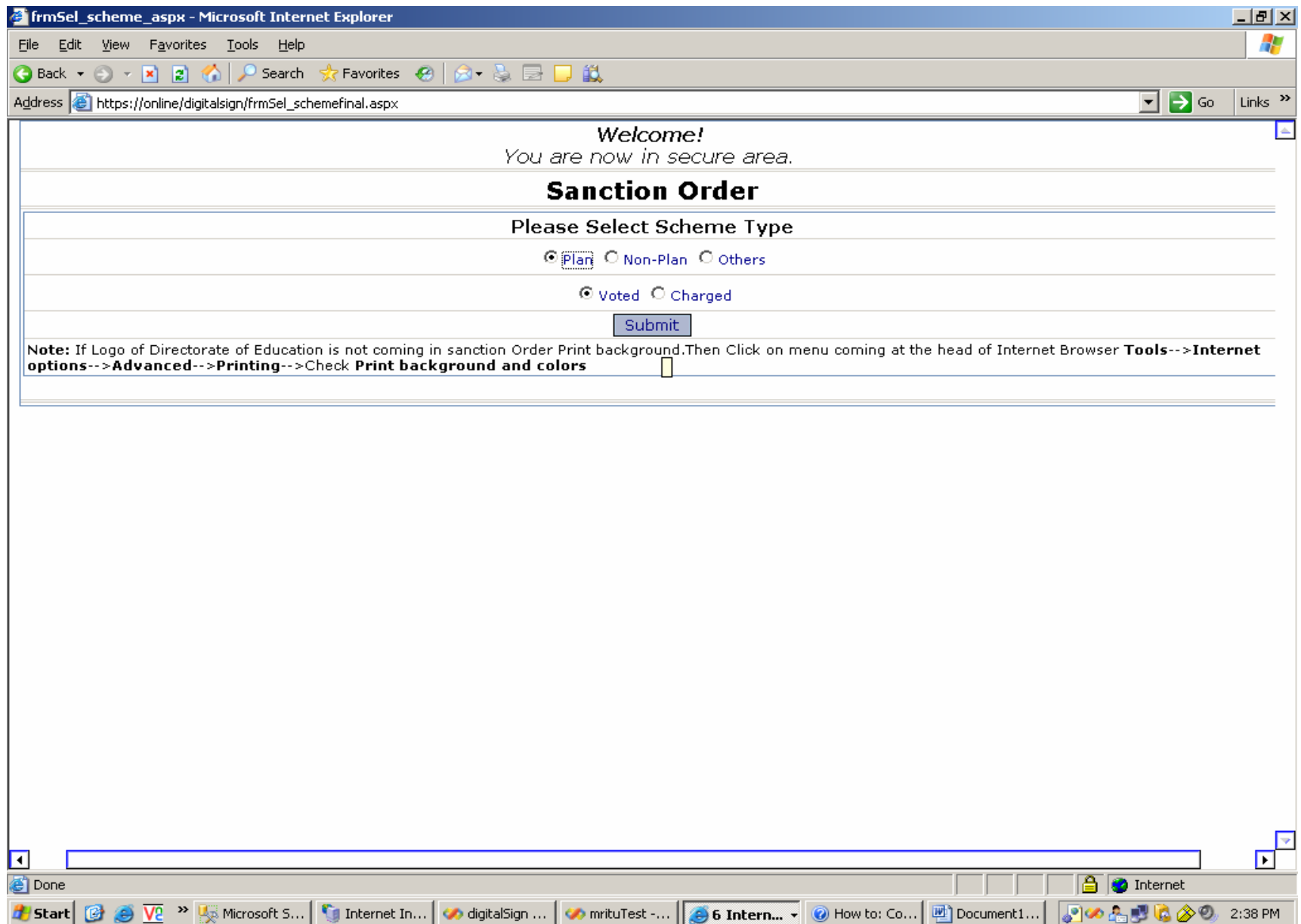












frmSel_scheme.aspx - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address https://online/digitalsign/frmSel_schemefinal.aspx Go Links

Welcome!
You are now in secure area.

Sanction Order

Select Scheme	A.1(2)(8)(6)*Subsidy for School Uniforms to the		
Alloted Amount	349500		
Already Utilized Amount	753		
Balance Amount	348747		
Sanction Date	26/09/2007		
Select Year	2007		
Bill No.	MMD123		
Bill Date	26	Sep	2007
Bill Amount(Gross)	5000		
Remarks	sanction only five thousand		
<div>Preview Reset</div>			

Done

Start Internet Explorer digitalSign mrituTest 6 Intern... How to: Co... Document1... 2:42 PM

frmSel_scheme.aspx - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address https://online/digitalsign/frmSel_schemefinal.aspx Go Links

Welcome!
You are now in secure area.

Sanction Order

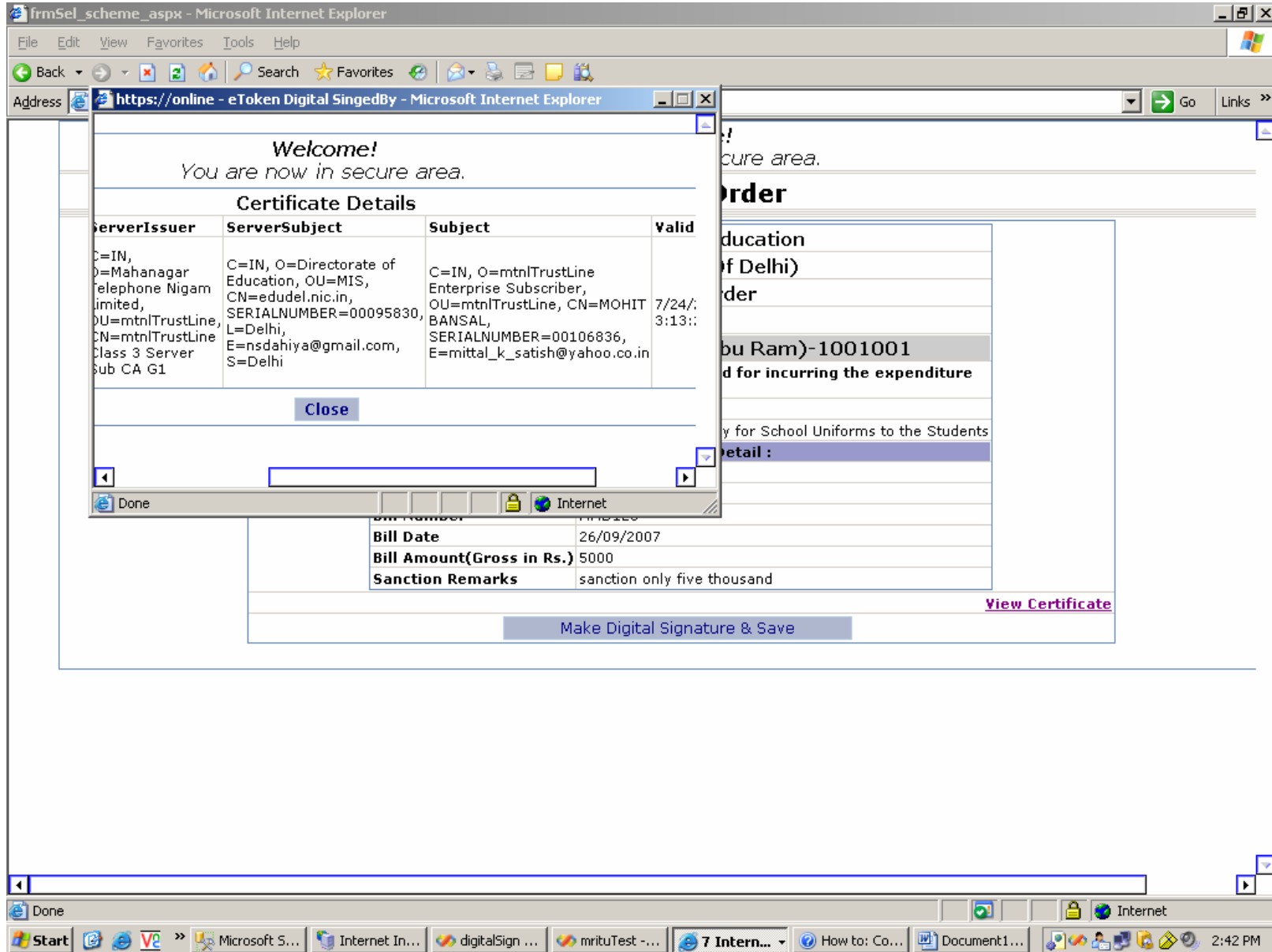
Directorate Of Education (Govt. Of NCT Of Delhi)	
Sanction Order Plan	
Bhola Nath Nagar-SBV (Babu Ram)-1001001	
Sanction of Head of Office is hereby granted for incurring the expenditure as detailed below.	
Sanction Order No.	
Scheme Name	A.1(2)(8)(6)*Subsidy for School Uniforms to the Students
Sanction Order Detail :	
Sanction Order NO.	
Sanction Date	26/09/2007
Bill Number	MMD123
Bill Date	26/09/2007
Bill Amount(Gross in Rs.)	5000
Sanction Remarks	sanction only five thousand

[View Certificate](#)

[Make Digital Signature & Save](#)

Done

Start Internet Explorer digitalSign mrituTest 6 Intern... How to: Co... Document1... 2:42 PM




frmSel_scheme.aspx - Microsoft Internet Explorer

https://online//DigitalSign/pdf/2007029406.pdf - Microsoft Internet Explorer

1 / 1 92.2% Find

Go Links

Directorate of Education (Govt. Of NCT of Delhi) Sanction Order Plan



2007029406

Bhola Nath Nagar-SBV (Babu Ram)-1001001
Sanction of Head of Office is hereby granted for incurring the expenditure as detailed below.
Sanction order Detail :-

Sanction Order No. :	2007029406
Scheme Name :	A.1(2)(8)(6)*Subsidy for School

Done Unknown Zone

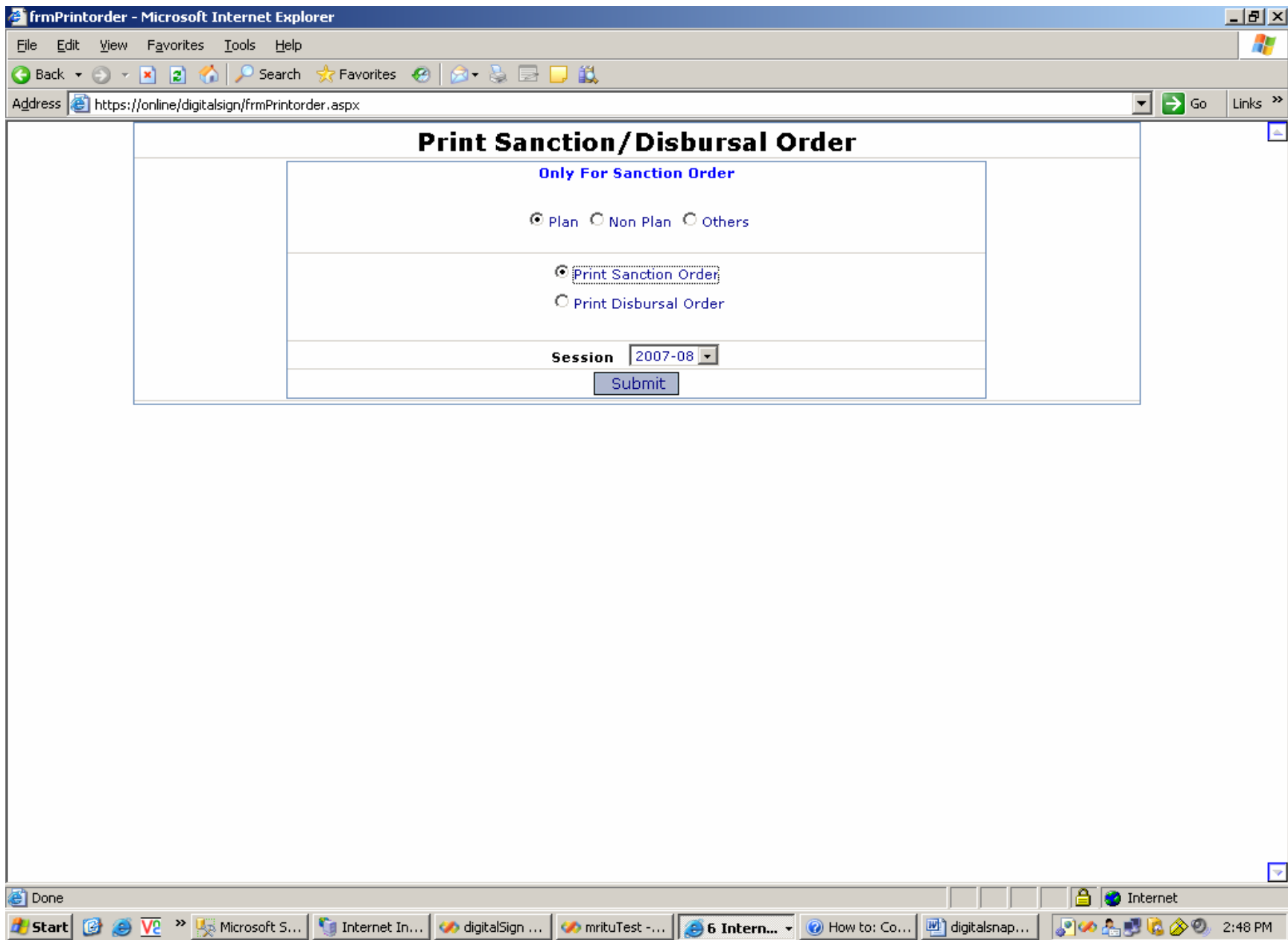
Sanction Remarks	sanction only five thousand
-------------------------	-----------------------------

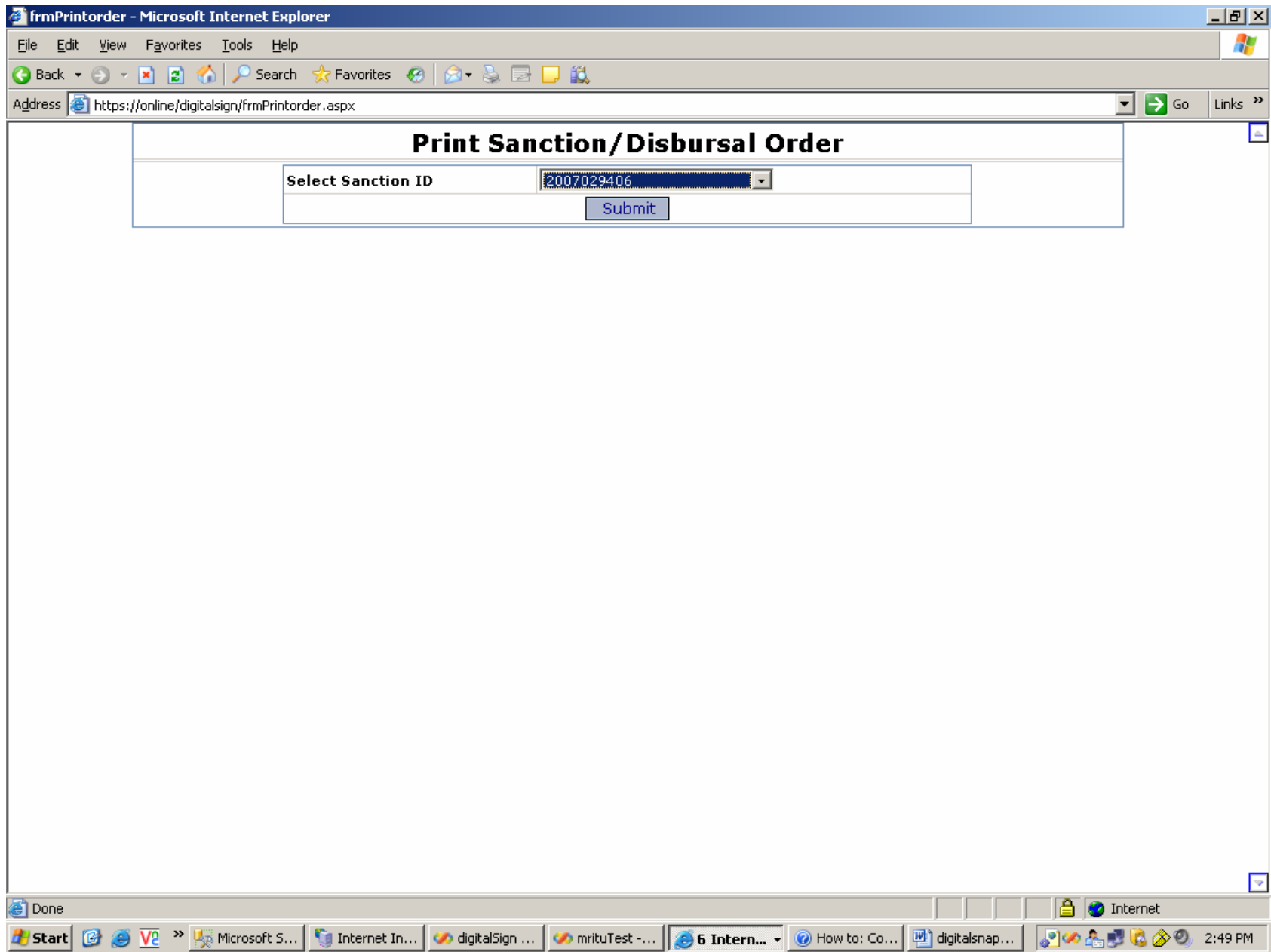
[View Certificate](#)

[Make Digital Signature & Save](#)

Done Internet

Start Microsoft S... Internet In... digitalSign ... mrituTest -... 7 Intern... How to: Co... Document1... 2:44 PM





Thank You

