

i-trust PKI SERVICES
IDRBT CERTIFYING AUTHORITY

Subscriber User Manual

Copyright 2002, IDRBT, All rights reserved



Institute for Development and Research in Banking Technology
Castle Hills, Road #1, Masab Tank,
Hyderabad (AP)- 500057, INDIA

<http://idrbtca.org.in/>, <http://infinet.org.in/>

<http://www.idrbt.com/>

Preface:

A Certifying Authority (CA) is a body that fulfills the need for trusted third party services in Electronic Commerce by issuing Digital Certificates that attests to some fact about the subject of the certificate. A certificate is a digitally signed statement by a CA that provides independent confirmation of an attribute claimed by a person offering a Digital Signature.

For securing the transactions through INFINET, IDRBT provides high end Public Key Infrastructure (PKI) based services and solutions to individuals, organizations as well as governments that enable trust and security. IDRBT has set up a high-end, global standards- based processing Center at its campus at Hyderabad, capable of issuing thousands of Digital Certificates, an important component of PKI. As a licensed Certifying Authority by the Controller of Certifying Authority (CCA), IDRBT CA will issue, administer and revoke the digital certificates over INFINET.

This manual will give you information about, the procedures for using Certification services of IDRBT Certifying Authority.

About This Manual

Typographic Conventions

Convention	Meaning
Select	Use the arrow key or mouse to select an item on the menu, a field in a window or an item in the interface.
Click	Press the primary mouse button once. The primary mouse button is typically the left button.
<i>Italic</i>	
Bold Lettering	Words in bold face type represent application's functionalities name, important notes, hints, paragraph headings.

What is in this Manual?

This manual introduces the i-trust PKI Services by IDRBT Certifying Authority and helps you by providing all the information to carry out the procedure for Certification Services.

Chapter	Description
Chapter 1	Introduction
Chapter 2	Getting Started

Getting Help:

If you have any questions that were not answered in this manual, please see the following source for additional help.

Contacting IDRBT CA Technical Support:

i-trust PKI Customer Services team is committed to supporting the users. If you have any questions, need additional assistance, or encounter a problem, please contact the following:

IDRBT CA	
i-trust PKI Services Support Team	
INFINET	http://idrbtca.org.in/ , http://infinet.org.in/
INTERNET	http://www.idrbt.com/
E-mail	caservice@idrbt.ac.in
Telephone	+91-40-3534981/82
Fax	+91-40-3535157



We Welcome Your Comments

Our support is committed. Please include the following information, when you contact us:

Your name, company/organization name, job title, phone number and e-mail address

Send us e-mail at:

caservice@idrbt.ac.in

Or, you can write us at:

The CA Administrator,
IDRBT
Castle Hills, Road #1, Masab Tank,
Hyderabad – 500057, INDIA

CONTENTS

1. Introduction	1
1.1. Introduction To Public Key Infrastructure	1
1.1.1. Internet Security Issues	1
1.2. PKI Model	3
1.3. Encryption and Decryption.....	4
1.3.1. Symmetric-Key Encryption	4
1.3.2. Public-Key Encryption	5
1.3.3. Key Length and Encryption Strength	7
1.4. Digital Signatures	7
1.5. Certificates and Authentication	10
1.5.1. A Certificate Identifies Someone or Something	10
1.5.2. Authentication Confirms an Identity.....	11
1.6. Password-Based Authentication.....	12
1.7. Certificate-Based Authentication	14
1.8. How Certificates Are Used.....	16
1.8.1. Types of Certificates	16
1.9. SSL Protocol	17
1.10. Signed and Encrypted Email	18
1.11. Object Signing	19
1.12. Contents of a Certificate	19
1.13. Distinguished Names	20
1.14. A Typical Certificate	20
1.15. How CA Certificates Are Used to Establish Trust.....	23
1.16. Managing Certificates	24
1.16.1. Issuing Certificates	24
1.17. Certificates and the LDAP Directory	25
1.18. Key Management	25
1.19. Renewing and Revoking Certificates	26
1.20. IDRBT Certifying Authority.....	27
1.21. Registration Authorities	28
2. Getting started.....	30
2.1. Procedures for requesting a Digital Certificate	35
2.2. Requesting an Encryption Certificate	50
2.3. Requesting an Server Certificate	53
2.4. Downloading the Digital Certificate	55
2.5. Suspending the Digital Certificate	67
2.6. Downloading the IDRBT CA Root Certificate	67
2.7. Downloading the IDRBT CA CRL	69

1. Introduction

1.1. Introduction To Public Key Infrastructure

1.1.1. Internet Security Issues

All communication over the Internet uses the Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP allows information to be sent from one computer to another through a variety of intermediate computers and separate networks before it reaches its destination.

The great flexibility of TCP/IP has led to its worldwide acceptance as the basic Internet and intranet communications protocol. At the same time, the fact that TCP/IP allows information to pass through intermediate computers makes it possible for a third party to interfere with communications in the following ways:

- **Eavesdropping.** Information remains intact, but its privacy is compromised. For example, someone could learn your credit card number, record a sensitive conversation, or intercept classified information.
- **Tampering.** Information in transit is changed or replaced and then sent on to the recipient. For example, someone could alter an order for goods or change a person's resume.
- **Impersonation.** Information passes to a person who poses as the intended recipient. Impersonation can take two forms:
 - **Spoofing.** A person can pretend to be someone else. For example, a person can pretend to have the email address `biju@idrbt.com`, or a computer can identify itself as a site called `www.idrbt.com` when it is not. This type of impersonation is known as spoofing.
 - **Misrepresentation.** A person or organization can misrepresent itself. For example, suppose the site `www.idrbt.com` pretends to be a furniture

store when it is really just a site that takes credit-card payments but never sends any goods.

Normally, users of the many cooperating computers that make up the Internet or other networks don't monitor or interfere with the network traffic that continuously passes through their machines. However, many sensitive personal and business communications over the Internet require precautions that address the threats listed above. Fortunately, a set of well-established techniques and standards known as **public-key cryptography** make it relatively easy to take such precautions.

Public-key cryptography facilitates the following tasks:

- **Encryption and decryption** allow two communicating parties to disguise information they send to each other. The sender encrypts, or scrambles, information before sending it. The receiver decrypts, or unscrambles, the information after receiving it. While in transit, the encrypted information is unintelligible to an intruder.
- **Tamper detection** allows the recipient of information to verify that it has not been modified in transit. Any attempt to modify data or substitute a false message for a legitimate one will be detected.
- **Authentication** allows the recipient of information to determine its origin — that is, to confirm the sender's identity.
- **Non-repudiation** prevents the sender of information from claiming at a later date that the information was never sent.

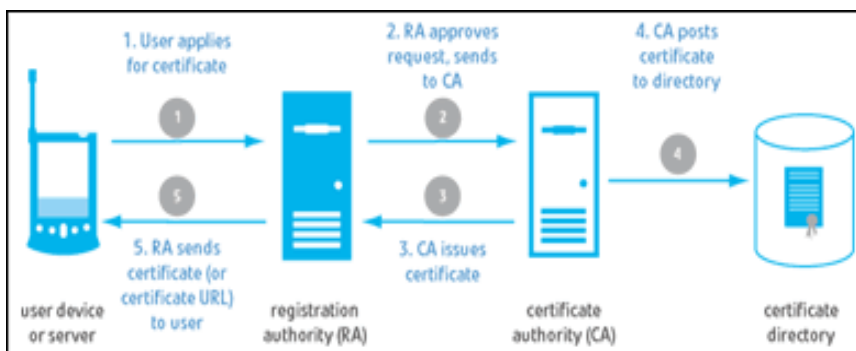
PKI is based on the use of digital certificates— the equivalent of a passport in the physical world. Digital certificates allow users to verify the identity of the person or institution that they're communicating with, and to digitally sign transactions.

A certificate-based system provides:

- **Authentication-** to verify the identity of the sender and the recipient of digital information

- Data integrity- to verify that information is received unaltered from the sender
- Data confidentiality- to ensure that sensitive information does not fall into the wrong hands
- Non-repudiation- to ensure that transactions are legally binding, protecting your business from fraud

1.2. PKI Model



The basic components of a PKI are the Registration Authority (RA) and the Certificate Authority (CA).

- The RA verifies the certificate request of the applicant and forwards to the CA
- The CA generates certificates on the RA's request and posts the certificate to a directory
- A PKI also includes policies, procedures, and contracts that govern how and when digital certificates are issued, renewed, or revoked, among other issues.

Applications that are PKI-enabled can manage user certificates and generate digital certificates on desktop PCs to secure communications and execute binding digital transactions.

1.3. Encryption and Decryption

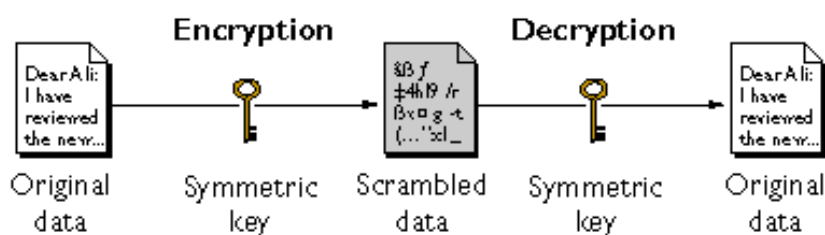
Encryption is the process of transforming information so it is unintelligible to anyone but the intended recipient. Decryption is the process of transforming encrypted information so that it is intelligible again. A **cryptographic algorithm**, also called a **cipher**, is a mathematical function used for encryption or decryption. In most cases, two related functions are employed, one for encryption and the other for decryption.

With most modern cryptography, the ability to keep encrypted information secret is based not on the cryptographic algorithm, which is widely known, but on a number called a **key** that must be used with the algorithm to produce an encrypted result or to decrypt previously encrypted information. Decryption with the correct key is simple. Decryption without the correct key is very difficult, and in some cases impossible for all practical purposes.

1.3.1. Symmetric-Key Encryption

With **symmetric-key encryption**, the encryption key can be calculated from the decryption key and vice versa. With most symmetric algorithms, the same key is used for both encryption and decryption, as shown in Figure 1.1.

Figure 1.1 Symmetric-key encryption



Implementations of symmetric-key encryption can be highly efficient, so that users do not experience any significant time delay as a result of the encryption and decryption. Symmetric-key encryption also provides a degree of authentication, since information encrypted with one symmetric key cannot be decrypted with any other symmetric key. Thus, as long as the symmetric key is kept secret by the two parties using it to encrypt communications, each party can be sure that it is

communicating with the other as long as the decrypted messages continue to make sense.

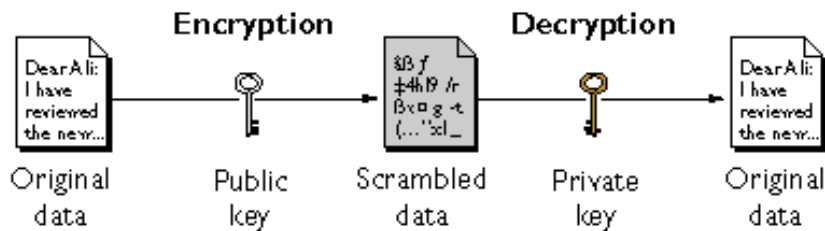
Symmetric-key encryption is effective only if the symmetric key is kept secret by the two parties involved. If anyone else discovers the key, it affects both confidentiality and authentication. A person with an unauthorized symmetric key not only can decrypt messages sent with that key, but can encrypt new messages and send them as if they came from one of the two parties who were originally using the key.

Symmetric-key encryption plays an important role in the SSL protocol, which is widely used for authentication, tamper detection, and encryption over TCP/IP networks. SSL also uses techniques of public-key encryption, which is described in the next section.

1.3.2. Public-Key Encryption

The most commonly used implementations of public-key encryption are based on algorithms patented by [RSA Data Security](http://www.rsa.com) (<http://www.rsa.com>). Therefore, this section describes the RSA approach to public-key encryption.

Public-key encryption (also called **asymmetric encryption**) involves a pair of keys — a **public key** and a **private key** — associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data. Each public key is published, and the corresponding private key is kept secret. Data encrypted with your public key can be decrypted only with your private key. Figure 1.2 shows a simplified view of the way public-key encryption works.

Figure 1.2 Public-key encryption

The scheme shown in Figure 1.2 lets you freely distribute a public key, and only you will be able to read data encrypted using this key. In general, to send encrypted data to someone, you encrypt the data with that person's public key, and the person receiving the encrypted data decrypts it with the corresponding private key.

Compared with symmetric-key encryption, public-key encryption requires more computation and is therefore not always appropriate for large amounts of data. However, it's possible to use public-key encryption to send a symmetric key, which can then be used to encrypt additional data. This is the approach used by the SSL protocol.

As it happens, the reverse of the scheme shown in Figure 1.2 also works: data encrypted with your private key can be decrypted only with your public key. This would not be a desirable way to encrypt sensitive data, however, because it means that anyone with your public key, which is by definition published, could decrypt the data. Nevertheless, private-key encryption is useful, because it means you can use your private key to sign data with your digital signature — an important requirement for electronic commerce and other commercial applications of cryptography. Client software such as Internet Explorer or Netscape Communicator can then use your public key to confirm that the message was signed with your private key and that it hasn't been tampered with since being signed. Digital Signatures and subsequent sections describe how this confirmation process works.

1.3.3. Key Length and Encryption Strength

In general, the strength of encryption is related to the difficulty of discovering the key, which in turn depends on both the cipher used and the length of the key. For example, the difficulty of discovering the key for the RSA cipher most commonly used for public-key encryption depends on the difficulty of factoring large numbers, a well-known mathematical problem.

Encryption strength is often described in terms of the size of the keys used to perform the encryption: in general, longer keys provide stronger encryption. Key length is measured in bits. For example, 128-bit keys for use with the RC4 symmetric-key cipher supported by SSL provide significantly better cryptographic protection than 40-bit keys for use with the same cipher. Roughly speaking, 128-bit RC4 encryption is 3×10^{26} times stronger than 40-bit RC4 encryption.

Different ciphers may require different key lengths to achieve the same level of encryption strength. The RSA cipher used for public-key encryption, for example, can use only a subset of all possible values for a key of a given length, due to the nature of the mathematical problem on which it is based. Other ciphers, such as those used for symmetric key encryption, can use all possible values for a key of a given length, rather than a subset of those values. Thus a 128-bit key for use with a symmetric-key encryption cipher would provide stronger encryption than a 128-bit key for use with the RSA public-key encryption cipher.

This difference explains why the RSA public-key encryption cipher must use a 512-bit key (or longer) to be considered cryptographically strong, whereas symmetric key ciphers can achieve approximately the same level of strength with a 64-bit key. Even this level of strength may be vulnerable to attacks in the near future.

1.4. Digital Signatures

Encryption and decryption address the problem of eavesdropping, one of the three Internet security issues mentioned at the beginning of this document. But encryption

and decryption, by themselves, do not address the other two problems mentioned in Internet Security Issues: tampering and impersonation.

This section describes how public-key cryptography addresses the problem of tampering. The sections that follow describe how it addresses the problem of impersonation.

Tamper detection and related authentication techniques rely on a mathematical function called a **one-way hash** (also called a **message digest**). A one-way hash is a number of fixed length with the following characteristics:

- The value of the hash is unique for the hashed data. Any change in the data, even deleting or altering a single character, results in a different value.
- The content of the hashed data cannot, for all practical purposes, be deduced from the hash — which is why it is called "one-way."

As mentioned in Public-Key Encryption, it's possible to use your private key for encryption and your public key for decryption. Although this is not desirable when you are encrypting sensitive information, it is a crucial part of digitally signing any data. Instead of encrypting the data itself, the signing software creates a one-way hash of the data, then uses your private key to encrypt the hash. The encrypted hash, along with other information, such as the hashing algorithm, is known as a **digital signature**. Figure 1.3 shows a simplified view of the way a digital signature can be used to validate the integrity of signed data.

Figure 1.3 Using a digital signature to validate data integrity

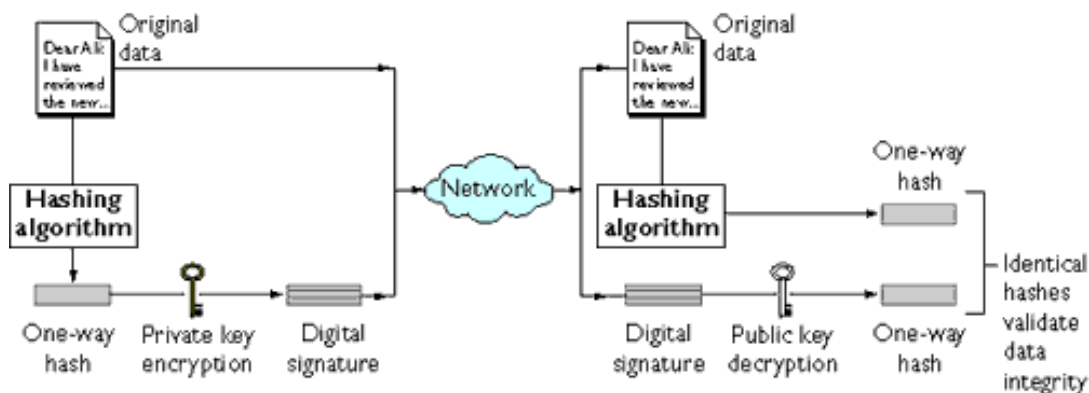


Figure 1.3 shows two items transferred to the recipient of some signed data: the original data and the digital signature, which is basically a one-way hash (of the original data) that has been encrypted with the signer's private key. To validate the integrity of the data, the receiving software first uses the signer's public key to decrypt the hash. It then uses the same hashing algorithm that generated the original hash to generate a new one-way hash of the same data. (Information about the hashing algorithm used is sent with the digital signature, although this isn't shown in the figure.) Finally, the receiving software compares the new hash against the original hash. If the two hashes match, the data has not changed since it was signed. If they don't match, the data may have been tampered with since it was signed, or the signature may have been created with a private key that doesn't correspond to the public key presented by the signer.

If the two hashes match, the recipient can be certain that the public key used to decrypt the digital signature corresponds to the private key used to create the digital signature. Confirming the identity of the signer, however, also requires some way of confirming that the public key really belongs to a particular person or other entity.

The significance of a digital signature is comparable to the significance of a handwritten signature. Once you have signed some data, it is difficult to deny doing so later — assuming that the private key has not been compromised or out of the

owner's control. This quality of digital signatures provides a high degree of non-repudiation — that is, digital signatures make it difficult for the signer to deny having signed the data. In some situations, a digital signature may be as legally binding as a handwritten signature.

1.5. Certificates and Authentication

1.5.1. A Certificate Identifies Someone or Something

A **certificate** is an electronic document used to identify an individual, a server, a company, or some other entity and to associate that identity with a public key. Like a driver's license, a passport, or other commonly used personal IDs, a certificate provides generally recognized proof of a person's identity. Public-key cryptography uses certificates to address the problem of impersonation.

To get a driver's license, you typically apply to a government agency, such as the Department of Motor Vehicles, which verifies your identity, your ability to drive, your address, and other information before issuing the license. To get a student ID, you apply to a school or college, which performs different checks (such as whether you have paid your tuition) before issuing the ID. To get a library card, you may need to provide only your name and a utility bill with your address on it.

Certificates work much the same way as any of these familiar forms of identification. **Certificate authorities (CAs)** are entities that validate identities and issue certificates. They can be either independent third parties or organizations running their own certificate-issuing server software. The methods used to validate an identity vary depending on the policies of a given CA — just as the methods to validate other forms of identification vary depending on who is issuing the ID and the purpose for which it will be used. In general, before issuing a certificate, the CA must use its published verification procedures for that type of certificate to ensure that an entity requesting a certificate is in fact who it claims to be.

The certificate issued by the CA binds a particular public key to the name of the entity the certificate identifies (such as the name of an employee or a server).

Certificates help prevent the use of fake public keys for impersonation. Only the public key certified by the certificate will work with the corresponding private key possessed by the entity identified by the certificate.

In addition to a public key, a certificate always includes the name of the entity it identifies, an expiration date, the name of the CA that issued the certificate, a serial number, and other information. Most importantly, a certificate always includes the digital signature of the issuing CA. The CA's digital signature allows the certificate to function as a "letter of introduction" for users who know and trust the CA but don't know the entity identified by the certificate.

1.5.2. Authentication Confirms an Identity

Authentication is the process of confirming an identity. In the context of network interactions, authentication involves the confident identification of one party by another party. Authentication over networks can take many forms. Certificates are one way of supporting authentication.

Network interactions typically take place between a client, such as browser software running on a personal computer, and a server, such as the software and hardware used to host a Web site. **Client authentication** refers to the confident identification of a client by a server (that is, identification of the person assumed to be using the client software). **Server authentication** refers to the confident identification of a server by a client (that is, identification of the organization assumed to be responsible for the server at a particular network address).

Client and server authentication are not the only forms of authentication that certificates support. For example, the digital signature on an email message, combined with the certificate that identifies the sender, provide strong evidence that the person identified by that certificate did indeed send that message. Similarly, a digital signature on an HTML form, combined with a certificate that identifies the signer, can provide evidence, after the fact, that the person identified by that certificate did agree to the contents of the form. In addition to authentication, the

digital signature in both cases ensures a degree of non-repudiation — that is, a digital signature makes it difficult for the signer to claim later not to have sent the email or the form.

Client authentication is an essential element of network security within most intranets or extranets. The sections that follow contrast two forms of client authentication:

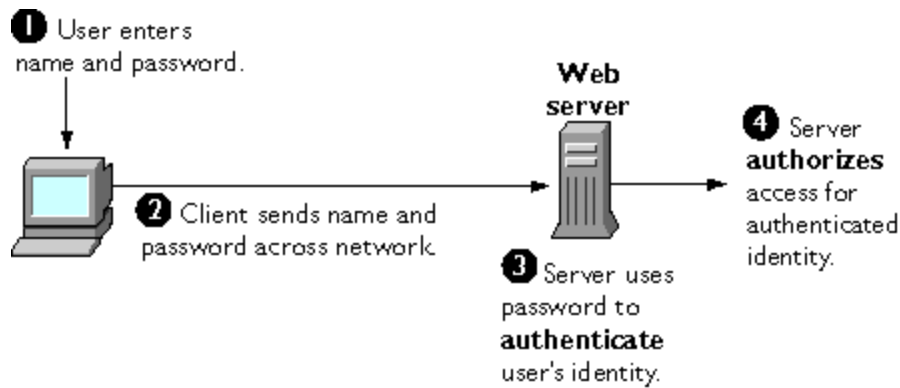
- **Password-Based Authentication.** Almost all server software permits client authentication by means of a name and password. For example, a server might require a user to type a name and password before granting access to the server. The server maintains a list of names and passwords; if a particular name is on the list, and if the user types the correct password, the server grants access.
- **Certificate-Based Authentication.** Client authentication based on certificates is part of the SSL protocol. The client digitally signs a randomly generated piece of data and sends both the certificate and the signed data across the network. The server uses techniques of public-key cryptography to validate the signature and confirm the validity of the certificate.

1.6. Password-Based Authentication

Figure 1.4 shows the basic steps involved in authenticating a client by means of a name and password. Figure 1.4 assumes the following:

- The user has already decided to trust the server, either without authentication or on the basis of server authentication via SSL.
- The user has requested a resource controlled by the server.
- The server requires client authentication before permitting access to the requested resource.

Figure 1.4 Using a password to authenticate a client to a server



These are the steps shown in Figure 1.4:

1. In response to an authentication request from the server, the client displays a dialog box requesting the user's name and password for that server. The user must supply a name and password separately for each new server the user wishes to use during a work session.
2. The client sends the name and password across the network, either in the clear or over an encrypted SSL connection.
3. The server looks up the name and password in its local password database and, if they match, accepts them as evidence authenticating the user's identity.
4. The server determines whether the identified user is permitted to access the requested resource, and if so allows the client to access it.

With this arrangement, the user must supply a new password for each server, and the administrator must keep track of the name and password for each user, typically on separate servers.

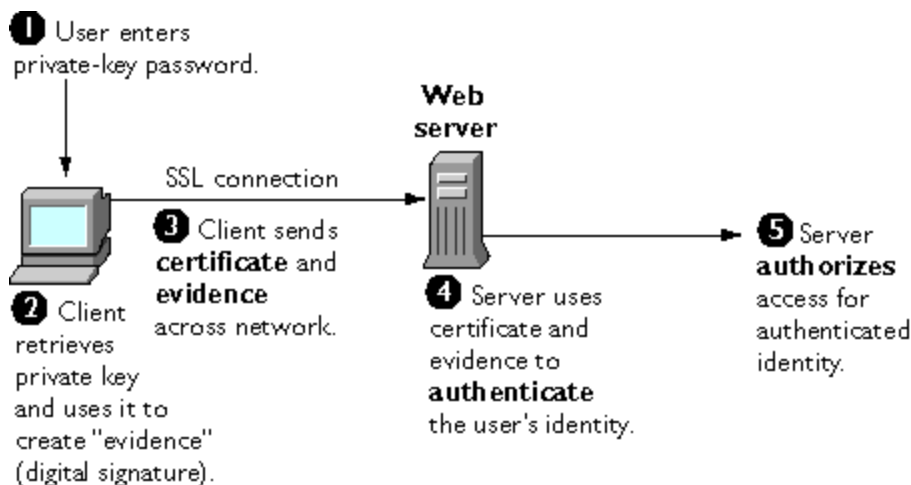
As shown in the next section, one of the advantages of certificate-based authentication is that it can be used to replace the first three steps in Figure 1.2 with a mechanism that allows the user to supply just one password (which is not sent across the network) and allows the administrator to control user authentication centrally.

1.7. Certificate-Based Authentication

Figure 1.5 shows how client authentication works using certificates and the SSL Protocol. To authenticate a user to a server, a client digitally signs a randomly generated piece of data and sends both the certificate and the signed data across the network. For the purposes of this discussion, the digital signature associated with some data can be thought of as evidence provided by the client to the server. The server authenticates the user's identity on the strength of this evidence.

Like Figure 1.4, Figure 1.5 assumes that the user has already decided to trust the server and has requested a resource, and that the server has requested client authentication in the process of evaluating whether to grant access to the requested resource.

Figure 1.5 Using a certificate to authenticate a client to a server



Unlike the process shown in Figure 1.4, the process shown in Figure 1.5 requires the use of SSL. Figure 1.5 also assumes that the client has a valid certificate that can be used to identify the client to the server. Certificate-based authentication is generally considered preferable to password-based authentication because it is based on what the user has (the private key) as well as what the user knows (the password that protects the private key). However, it's important to note that these two assumptions are true only if unauthorized personnel have not gained access to

the user's machine or password, the password for the client software's private key database has been set, and the software is set up to request the password at reasonably frequent intervals.

Important Neither password-based authentication nor certificate-based authentication address security issues related to physical access to individual machines or passwords. Public-key cryptography can only verify that a private key used to sign some data corresponds to the public key in a certificate. It is the user's responsibility to protect a machine's physical security and to keep the private-key password secret.

These are the steps shown in Figure 1.3:

1. The client software, such as Communicator, maintains a database of the private keys that correspond to the public keys published in any certificates issued for that client. The client asks for the password to this database the first time the client needs to access it during a given session — for example, the first time the user attempts to access an SSL-enabled server that requires certificate-based client authentication. After entering this password once, the user doesn't need to enter it again for the rest of the session, even when accessing other SSL-enabled servers.
2. The client unlocks the private-key database, retrieves the private key for the user's certificate, and uses that private key to digitally sign some data that has been randomly generated for this purpose on the basis of input from both the client and the server. This data and the digital signature constitute "evidence" of the private key's validity. The digital signature can be created only with that private key and can be validated with the corresponding public key against the signed data, which is unique to the SSL session.
3. The client sends both the user's certificate and the evidence (the randomly generated piece of data that has been digitally signed) across the network.
4. The server uses the certificate and the evidence to authenticate the user's identity.

5. At this point the server may optionally perform other authentication tasks, such as checking that the certificate presented by the client is stored in the user's entry in an LDAP directory. The server then continues to evaluate whether the identified user is permitted to access the requested resource. This evaluation process can employ a variety of standard authorization mechanisms, potentially using additional information in an LDAP directory, company databases, and so on. If the result of the evaluation is positive, the server allows the client to access the requested resource.

As you can see by comparing Figure 1.5 to Figure 1.4, certificates replace the authentication portion of the interaction between the client and the server. Instead of requiring a user to send passwords across the network throughout the day, single sign-on requires the user to enter the private-key database password just once, without sending it across the network. For the rest of the session, the client presents the user's certificate to authenticate the user to each new server it encounters. Existing authorization mechanisms based on the authenticated user identity are not affected.

1.8. How Certificates Are Used

1.8.1. Types of Certificates

- **Server SSL certificates.** Used to identify servers to clients via SSL (server authentication). Server authentication may be used with or without client authentication. Server authentication is a requirement for an encrypted SSL session.

Example: Internet sites that engage in electronic commerce (commonly known as **e-commerce**) usually support certificate-based server authentication, at a minimum, to establish an encrypted SSL session and to assure customers that they are dealing with a web site identified with a particular company. The encrypted SSL session ensures that personal information sent over the network, such as credit card numbers, cannot easily be intercepted.

- **S/MIME certificates.** Used for signed and encrypted email. As with client SSL certificates, the identity of the client is typically assumed to be the same as the identity of a human being, such as an employee in an enterprise.

Examples: A company deploys combined S/MIME and SSL certificates solely for the purpose of authenticating employee identities, thus permitting signed email and client SSL authentication but not encrypted email. Another company issues S/MIME certificates solely for the purpose of both signing and encrypting email that deals with sensitive financial or legal matters.

- **Object-signing certificates.** Used to identify signers of Java code, JavaScript scripts, or other signed files.

Example: A software company signs software distributed over the Internet to provide users with some assurance that the software is a legitimate product of that company. Using certificates and digital signatures in this manner can also make it possible for users to identify and control the kind of access downloaded software has to their computers.

1.9. SSL Protocol

The Secure Sockets Layer (SSL) protocol, which was originally developed by Netscape, is a set of rules governing server authentication, client authentication, and encrypted communication between servers and clients. SSL is widely used on the Internet, especially for interactions that involve exchanging confidential information such as credit card numbers.

SSL requires a server SSL certificate, at a minimum. As part of the initial "handshake" process, the server presents its certificate to the client to authenticate the server's identity. The authentication process uses Public-Key Encryption and Digital Signatures to confirm that the server is in fact the server it claims to be. Once the server has been authenticated, the client and server use techniques of Symmetric-Key Encryption, which is very fast, to encrypt all the information they

exchange for the remainder of the session and to detect any tampering that may have occurred.

Servers may optionally be configured to require client authentication as well as server authentication. In this case, after server authentication is successfully completed, the client must also present its certificate to the server to authenticate the client's identity before the encrypted SSL session can be established.

1.10. Signed and Encrypted Email

Some email programs support digitally signed and encrypted email using a widely accepted protocol known as Secure Multipurpose Internet Mail Extension (S/MIME). Using S/MIME to sign or encrypt email messages requires the sender of the message to have an S/MIME certificate.

An email message that includes a digital signature provides some assurance that it was in fact sent by the person whose name appears in the message header, thus providing authentication of the sender. If the digital signature cannot be validated by the email software on the receiving end, the user will be alerted.

The digital signature is unique to the message it accompanies. If the message received differs in any way from the message that was sent — even by the addition or deletion of a comma — the digital signature cannot be validated. Therefore, signed email also provides some assurance that the email has not been tampered with. As discussed at the beginning of this document, this kind of assurance is known as non-repudiation. In other words, signed email makes it very difficult for the sender to deny having sent the message. This is important for many forms of business communication.

S/MIME also makes it possible to encrypt email messages. This is also important for some business users. However, using encryption for email requires careful planning. If the recipient of encrypted email messages loses his or her private key and does

not have access to a backup copy of the key, for example, the encrypted messages can never be decrypted.

1.11. Object Signing

Object signing uses standard techniques of public-key cryptography to let users get reliable information about code they download in much the same way they can get reliable information about shrink-wrapped software.

Most importantly, object signing helps users and network administrators implement decisions about software distributed over intranets or the Internet — for example, whether to allow Java applets signed by a given entity to use specific computer capabilities on specific users' machines.

The "objects" signed with object signing technology can be applets or other Java code, JavaScript scripts, plug-ins, or any kind of file. The "signature" is a digital signature. Signed objects and their signatures are typically stored in a special file called a JAR file.

Software developers and others who wish to sign files using object-signing technology must first obtain an object-signing certificate.

1.12. Contents of a Certificate

The contents of certificates are organized according to the X.509 v3 certificate specification, which has been recommended by the International Telecommunications Union (ITU), an international standards body, since 1988.

Users don't usually need to be concerned about the exact contents of a certificate. However, system administrators working with certificates may need some familiarity with the information provided here.

1.13. Distinguished Names

An X.509 v3 certificate binds a **distinguished name (DN)** to a public key. A DN is a series of name-value pairs, such as `uid=biju`, that uniquely identify an entity — that is, the certificate **subject**.

For example, this might be a typical DN for an employee of IDRBT:

`uid=bij, e=biju@idrbt.ac.in, cn=Biju, o=IDRBT CA, c=IN`

The abbreviations before each equal sign in this example have these meanings:

- `uid`: user ID
- `e`: email address
- `cn`: the user's common name
- `o`: organization
- `c`: country

DNs may include a variety of other name-value pairs. They are used to identify both certificate subjects and entries in directories that support the Lightweight Directory Access Protocol (LDAP).

The rules governing the construction of DNs can be quite complex and are beyond the scope of this document.

1.14. A Typical Certificate

Every X.509 certificate consists of two sections:

- The data section includes the following information:
 - The version number of the X.509 standard supported by the certificate.
 - The certificate's serial number. Every certificate issued by a CA has a serial number that is unique among the certificates issued by that CA.
 - Information
 - Information about the user's public key, including the algorithm used and a representation of the key itself.

- The DN of the CA that issued the certificate.
- The period during which the certificate is valid (for example, between 1:00 p.m. on June 26, 2002 and 1:00 p.m. June 26,2003)
- The DN of the certificate subject (for example, in a client SSL certificate this would be the user's DN), also called the subject name.
- Optional **certificate extensions**, which may provide additional data used by the client or server. For example, the certificate type extension indicates the type of certificate — that is, whether it is a client SSL certificate, a server SSL certificate, a certificate for signing email, and so on. Certificate extensions can also be used for a variety of other purposes.
- The signature section includes the following information:
 - The cryptographic algorithm, or cipher, used by the issuing CA to create its own digital signature. For more information about ciphers.
 - The CA's digital signature, obtained by hashing all of the data in the certificate together and encrypting it with the CA's private key.

Here are the data and signature sections of a certificate in human-readable format:

Certificate:

Data:

Version: v3 (0x2)

Serial Number: 3 (0x3)

Signature Algorithm: PKCS #1 MD5 With RSA Encryption

Issuer: OU=IDRBT Certificate Authority, O=IDRBT, C=IN

Validity:

Not Before: Fri Oct 17 18:36:25 1997

Not After: Sun Oct 17 18:36:25 1999

Subject: C=US, O=IDRBT CA, OU=Class 1 Certificate, OU=Reserve Bank of India, CN=Biju Varghese

Subject Public Key Info:

Algorithm: PKCS #1 RSA Encryption

Public Key:

Modulus:

00:ca:fa:79:98:8f:19:f8:d7:de:e4:49:80:48:e6:2a:2a:86:
ed:27:40:4d:86:b3:05:c0:01:bb:50:15:c9:de:dc:85:19:22:
43:7d:45:6d:71:4e:17:3d:f0:36:4b:5b:7f:a8:51:a3:a1:00:
98:ce:7f:47:50:2c:93:36:7c:01:6e:cb:89:06:41:72:b5:e9:
73:49:38:76:ef:b6:8f:ac:49:bb:63:0f:9b:ff:16:2a:e3:0e:
9d:3b:af:ce:9a:3e:48:65:de:96:61:d5:0a:11:2a:a2:80:b0:
7d:d8:99:cb:0c:99:34:c9:ab:25:06:a8:31:ad:8c:4b:aa:54:
91:f4:15

Public Exponent: 65537 (0x10001)

Extensions:

Identifier: Certificate Type

Critical: no

Certified Usage:

SSL Client

Identifier: Authority Key Identifier

Critical: no

Key Identifier:

f2:f2:06:59:90:18:47:51:f5:89:33:5a:31:7a:e6:5c:fb:36:
26:c9

Signature:

Algorithm: PKCS #1 MD5 With RSA Encryption

Signature:

6d:23:af:f3:d3:b6:7a:df:90:df:cd:7e:18:6c:01:69:8e:54:65:fc:06:
30:43:34:d1:63:1f:06:7d:c3:40:a8:2a:82:c1:a4:83:2a:fb:2e:8f:fb:
f0:6d:ff:75:a3:78:f7:52:47:46:62:97:1d:d9:c6:11:0a:02:a2:e0:cc:
2a:75:6c:8b:b6:9b:87:00:7d:7c:84:76:79:ba:f8:b4:d2:62:58:c3:c5:
b6:c1:43:ac:63:44:42:fd:af:c8:0f:2f:38:85:6d:d6:59:e8:41:42:a5:

4a:e5:26:38:ff:32:78:a1:38:f1:ed:dc:0d:31:d1:b0:6d:67:e9:46:a8:
dd:c4

Here is the same certificate displayed in the 64-byte-encoded form interpreted by software:

-----BEGIN CERTIFICATE-----

```
MIICKzCCAZSgAwIBAgIBAzANBgkqhkiG9w0BAQQFADA3MQswCQYDVQQGEwJ  
VUzERMA8GA1UEChMITmV0c2NhGUxFTATBgNVBAsTDFN1cHJpeWEncyBDQ  
TAeFw05NzEwMTgwMTM2MjVaFw05OTEwMTgwMTM2MjVaMEgxGzAJBgNVBAY  
TAIVTMREwDwYDVQQKEwhOZXRzY2FwZTENMA8GA1UECxEUHViczEXMBU  
GA1UEAxMOU3VwcmI5YSBTaGV0dHkkgZ8wDQYJKoZIhvcNAQEFBQADgY0AMI  
GJAoGBAMr6eZiPGfjX3uRjGgEjmkIqG7SdATYazBcABu1AVyd7chRkiQ31FbXFOG  
D3wNktbf6hRo6EAmM5/R1AskzZ8AW7LiQZBcrXpc0k4du+2Q6xJu2MPm/8WKuM  
OnTuvzpo+SGXelmHVChEqooCwfdiZywyZNMmrJgaoMa2MS6pUkfQVAgMBAAGj  
NjA0MBEGCWCGSAGG+EIBAQQEAwIAgDAfBgNVHSMEGDAWgBTy8gZZkBhHU  
fWJM1oxeuZc+zYmyTANBgkqhkiG9w0BAQQFAAQBt6/z07Z635DfzX4XbAFpjl  
RI/AYwQzTSYx8GfcNAqCqCwaSDKvsuj/vwbf91o3j3UkdGYpcd2cYRCgKi4MwqdW  
yLtpuHAH18hHZ5uvi00mJYw8W2wUOsY0RC/a/IDy84hW3WWehBUqVK5SY4/zJ4  
oTjx7dwNMdGwbWfpRqjd1A==
```

-----END CERTIFICATE-----

1.15. How CA Certificates Are Used to Establish Trust

Certificate authorities (CAs) are entities that validate identities and issue certificates. They can be either independent third parties or organizations running their own certificate-issuing server software.

Any client or server software that supports certificates maintains a collection of **trusted CA certificates**. These CA certificates determine which other certificates the software can validate — in other words, which issuers of certificates the software can trust. In the simplest case, the software can validate only certificates issued by one of the CAs for which it has a certificate. It's also possible for a trusted CA

certificate to be part of a chain of CA certificates, each issued by the CA above it in a certificate hierarchy.

1.16. Managing Certificates

The set of standards and services that facilitate the use of public-key cryptography and X.509 v3 certificates in a networked environment is called the **public key infrastructure (PKI)**. PKI management is complex topic beyond the scope of this document.

1.16.1. Issuing Certificates

The process for issuing a certificate depends on the certificate authority that issues it and the purpose for which it will be used. The process for issuing nondigital forms of identification varies in similar ways. For example, if you want to get a generic ID card (not a driver's license) from the Department of Motor Vehicles in California, the requirements are straightforward: you need to present some evidence of your identity, such as a utility bill with your address on it and a student identity card. If you want to get a regular driving license, you also need to take a test — a driving test when you first get the license, and a written test when you renew it. If you want to get a commercial license for an eighteen-wheeler, the requirements are much more stringent. If you live in some other state or country, the requirements for various kinds of licenses will differ.

Similarly, different CAs have different procedures for issuing different kinds of certificates. In some cases the only requirement may be your email address. In other cases, your Unix or NT login and password may be sufficient. At the other end of the scale, for certificates that identify people who can authorize large expenditures or make other sensitive decisions, the issuing process may require notarized documents, a background check, and a personal interview.

Depending on an organization's policies, the process of issuing certificates can range from being completely transparent for the user to requiring significant user

participation and complex procedures. In general, processes for issuing certificates should be highly flexible, so organizations can tailor them to their changing needs.

Issuing certificates is one of several managements tasks that can be handled by separate Registration Authorities.

1.17. Certificates and the LDAP Directory

The Lightweight Directory Access Protocol (LDAP) for accessing directory services supports great flexibility in the management of certificates within an organization. System administrators can store much of the information required to manage certificates in an LDAP-compliant directory. For example, a CA can use information in a directory to pre-populate a certificate with a new employee's legal name and other information. The CA can leverage directory information in other ways to issue certificates one at a time or in bulk, using a range of different identification techniques depending on the security policies of a given organization. Other routine management tasks, such as Key Management and Renewing and Revoking Certificates, can be partially or fully automated with the aid of the directory.

Information stored in the directory can also be used with certificates to control access to various network resources by different users or groups. Issuing certificates and other certificate management tasks can thus be an integral part of user and group management.

In general, high-performance directory services are an essential ingredient of any certificate management strategy.

1.18. Key Management

Before a certificate can be issued, the public key it contains and the corresponding private key must be generated. Sometimes it may be useful to issue a single person one certificate and key pair for signing operations, and another certificate and key pair for encryption operations. Separate signing and encryption certificates make it possible to keep the private signing key on the local machine only, thus providing

maximum non-repudiation, and to back up the private encryption key in some central location where it can be retrieved in case the user loses the original key or leaves the company.

Keys can be generated by client software or generated centrally by the CA and distributed to users via an LDAP directory. There are trade-offs involved in choosing between local and centralized key generation. For example, local key generation provides maximum non-repudiation, but may involve more participation by the user in the issuing process. Flexible key management capabilities are essential for most organizations.

Key recovery, or the ability to retrieve backups of encryption keys under carefully defined conditions, can be a crucial part of certificate management (depending on how an organization uses certificates). Key recovery schemes usually involve an **m of n** mechanism: for example, m of n managers within an organization might have to agree, and each contribute a special code or key of their own, before a particular person's encryption key can be recovered. This kind of mechanism ensures that several authorized personnel must agree before an encryption key can be recovered.

1.19. Renewing and Revoking Certificates

Like a driver's license, a certificate specifies a period of time during which it is valid. Attempts to use a certificate for authentication before or after its validity period will fail. Therefore, mechanisms for managing certificate renewal are essential for any certificate management strategy. For example, an administrator may wish to be notified automatically when a certificate is about to expire, so that an appropriate renewal process can be completed in plenty of time without causing the certificate's subject any inconvenience. The renewal process may involve reusing the same public-private key pair or issuing a new one.

A driver's license can be suspended even if it has not expired — for example, as punishment for a serious driving offense. Similarly, it's sometimes necessary to

revoke a certificate before it has expired — for example, if an employee leaves a company or moves to a new job within the company.

Certificate revocation can be handled in several different ways. For some organizations, it may be sufficient to set up servers so that the authentication process includes checking the directory for the presence of the certificate being presented. When an administrator revokes a certificate, the certificate can be automatically removed from the directory, and subsequent authentication attempts with that certificate will fail even though the certificate remains valid in every other respect. Another approach involves publishing a **certificate revocation list (CRL)** — that is, a list of revoked certificates — to the directory at regular intervals and checking the list as part of the authentication process. For some organizations, it may be preferable to check directly with the issuing CA each time a certificate is presented for authentication. This procedure is sometimes called **real-time status checking**.

1.20. IDRBT Certifying Authority

IDRBT is an autonomous center for Development and Research in Banking Technology set up by Reserve Bank of India in 1996. IDRBT owns the INFINET, the communication backbone for the Indian Banking and Financial sector. Various inter-bank and intra-bank applications ranging from Simple Messaging, MIS, EFT, ECS, Electronic Debit, Online Processing and Trading in Government Securities, Centralized Funds querying for Banks and Financial Institutions, Anywhere/Anytime Banking and Inter-bank reconciliation are being implemented using the INFINET.

For securing the transactions through INFINET, IDRBT provides high end Public Key Infrastructure (PKI) based services and solutions to individuals, organizations as well as governments, which enable trust and security. IDRBT has set up a high-end, global standards- based processing Center at its campus at Hyderabad, capable of issuing thousands of Digital Certificates, an important component of PKI. As a licensed Certifying Authority by the Controller of Certifying Authority (CCA), IDRBT CA will issue, administer and revoke the digital certificates over INFINET.

1.21. Registration Authorities

Interactions between entities identified by certificates (sometimes called **end entities**) and CAs are an essential part of certificate management. These interactions include operations such as registration for certification, certificate retrieval, certificate renewal, certificate revocation, and key backup and recovery. In general, a CA must be able to authenticate the identities of end entities before responding to the requests. In addition, some requests need to be approved by authorized administrators or managers before being services.

As previously discussed, the means used by different CAs to verify an identity before issuing a certificate can vary widely, depending on the organization and the purpose for which the certificate will be used. To provide maximum operational flexibility, interactions with end entities can be separated from the other functions of a CA and handled by a separate service called a **Registration Authority (RA)**.

Registration Authority receives the applications for the Digital Certificate from the Applicant/Subscriber and verifies the details contained in the Application. An RA will also verify the documents accompanying the application form for different Classes of Certificate as mentioned in the IDRBT CA CPS. In case of Class 3 Certificates, the Applicant/Subscriber must present before the RA for personal verification. If the verification is successful, then the request is forwarded to the IDRBT CA recommending generation of a Digital Certificate for the verified Applicant/Subscriber. If he finds anything wrong in the certificate application, the RA has the right to reject it.

An RA shall be responsible for the following:

- Receiving the Certificate requests and Subscriber Agreement for the Digital Certificates from the Applicants.
- Verifying the applications as per the terms and conditions of the IDRBT CA CPS, and upon successful verification, requesting the IDRBT CA to

generate a Digital Certificate for the respective applicant as per the terms and conditions in the IDRBT CA CPS.

- Receiving and verifying the requests for Certificate suspension, activation and revocation from the Subscribers and upon successful verification, forwarding the request to the IDRBT CA.
- May notify the Subscribers when their Digital Certificate shall expire in advance.
- Creating and maintaining an accurate audit trail of all RA operations.
- Rejection of Digital Certificate applications in the event the Applicant/Subscriber does not indicate acceptance of obligations as per IDRBT CA CPS or inaccurate information furnished by the Applicant/Subscriber.
- Additional obligations as set forth in the RA agreement.

Others:

- The RA or IDRBT CA shall not be responsible if the Subscriber's Private Key is compromised and a request for Suspension, Revocation or Activation is placed on Subscriber's behalf.
- The RA or IDRBT CA shall not be responsible to inform users of revocation of their Certificates in case of the request being initiated by the Subscribers themselves. In case of request being initiated by RA or IDRBT CA, the Subscriber shall be informed of the action being taken.

The procedure for becoming a Registration Authority are mentioned in the document entitled "Rules and Guidelines for Registration Authorities"

2. Getting started

A Certifying Authority (CA) is a body that fulfills the need for trusted third party services in Electronic Commerce by issuing Digital Certificates that attests to some fact about the subject of the certificate. A certificate is a digitally signed statement by a CA that provides independent confirmation of an attribute claimed by a person offering a Digital Signature.

For securing the transactions through INFINET, IDRBT provides high end Public Key Infrastructure (PKI) based services and solutions to individuals, organizations as well as governments that enable trust and security. IDRBT has set up a high-end, global standards- based processing Center at its campus at Hyderabad, capable of issuing thousands of Digital Certificates, an important component of PKI. As a licensed Certifying Authority by the Controller of Certifying Authority (CCA), IDRBT CA will issue, administer and revoke the digital certificates over INFINET.

IDRBT CA's i-trust PKI Services are currently available only on INFINET.

Visit IDRBT CA's official website on INFINET at <http://idrbtca.org.in/>. This website contains the information about the IDRBT CA Certification Practice Statement, the classes of digital certificates offered by IDRBT CA, general information about PKI, Registration Authorities, Information Technology Act, Subscriber Agreement, Privacy Statement, Frequently Asked Questions, IDRBT CA Help Desk, etc.

Fig 1 shows the home page of <http://idrbtca.org.in/> .

Note: This website will only be accessed on INFINET. You are advised to become a member of INFINET to utilize the certification services offered by IDRBT CA.



Fig 1 IDRBT CA home page

It is assumed that the applicant of the digital certificate of IDRBT CA must have knowledge of Public Key Infrastructure, the general usage of certificates, the rights and obligations as prescribed in IDRBT CA CPS. We suggest the applicants must read and understand the rights, obligations, liabilities, warranties, documents required at time of certificate request, certificate practices, etc. mentioned in the IDRBT CA CPS. The information related to PKI and the IDRBT CA Certification Services are available at <http://idrbtca.org.in/>.

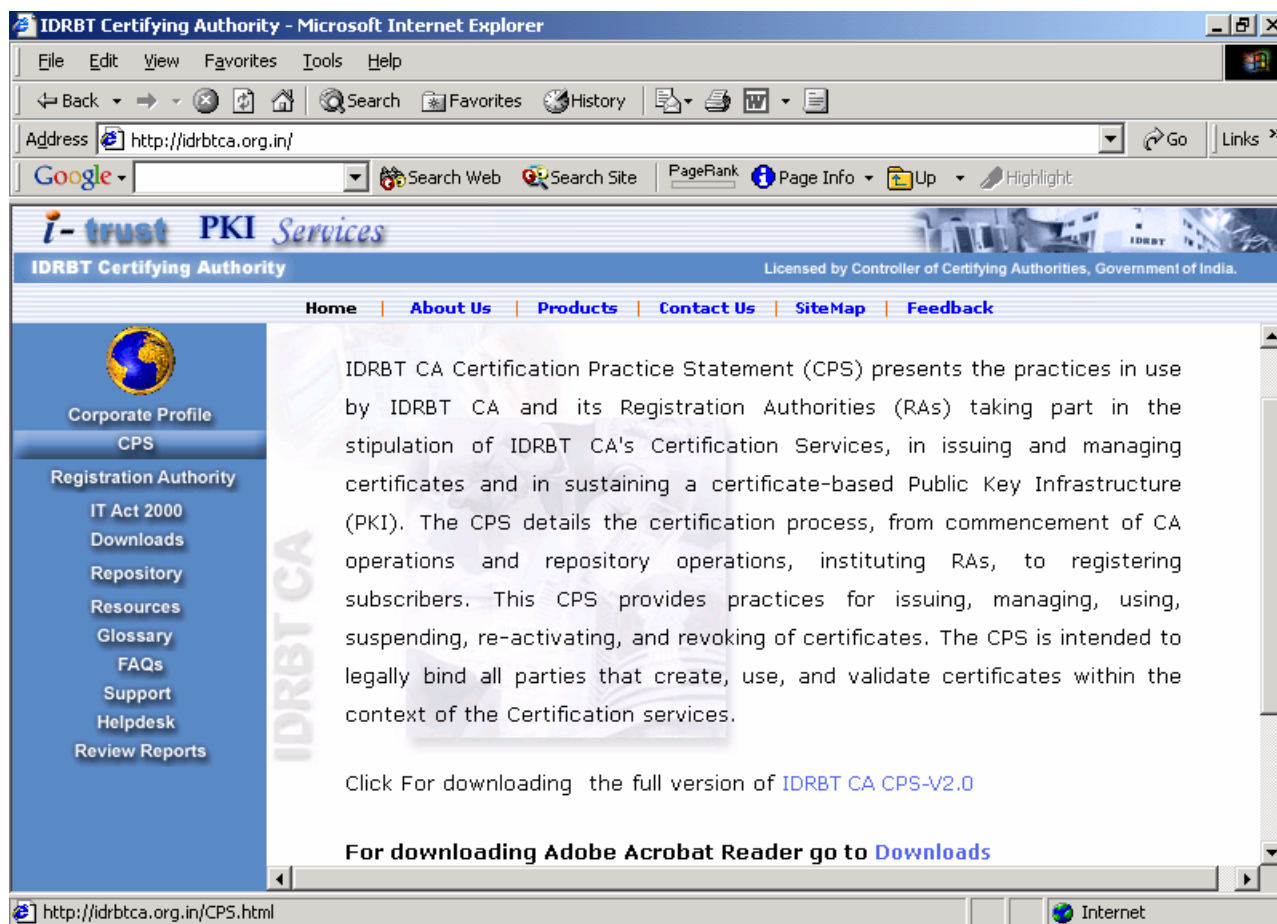


Fig 2. CPS page.

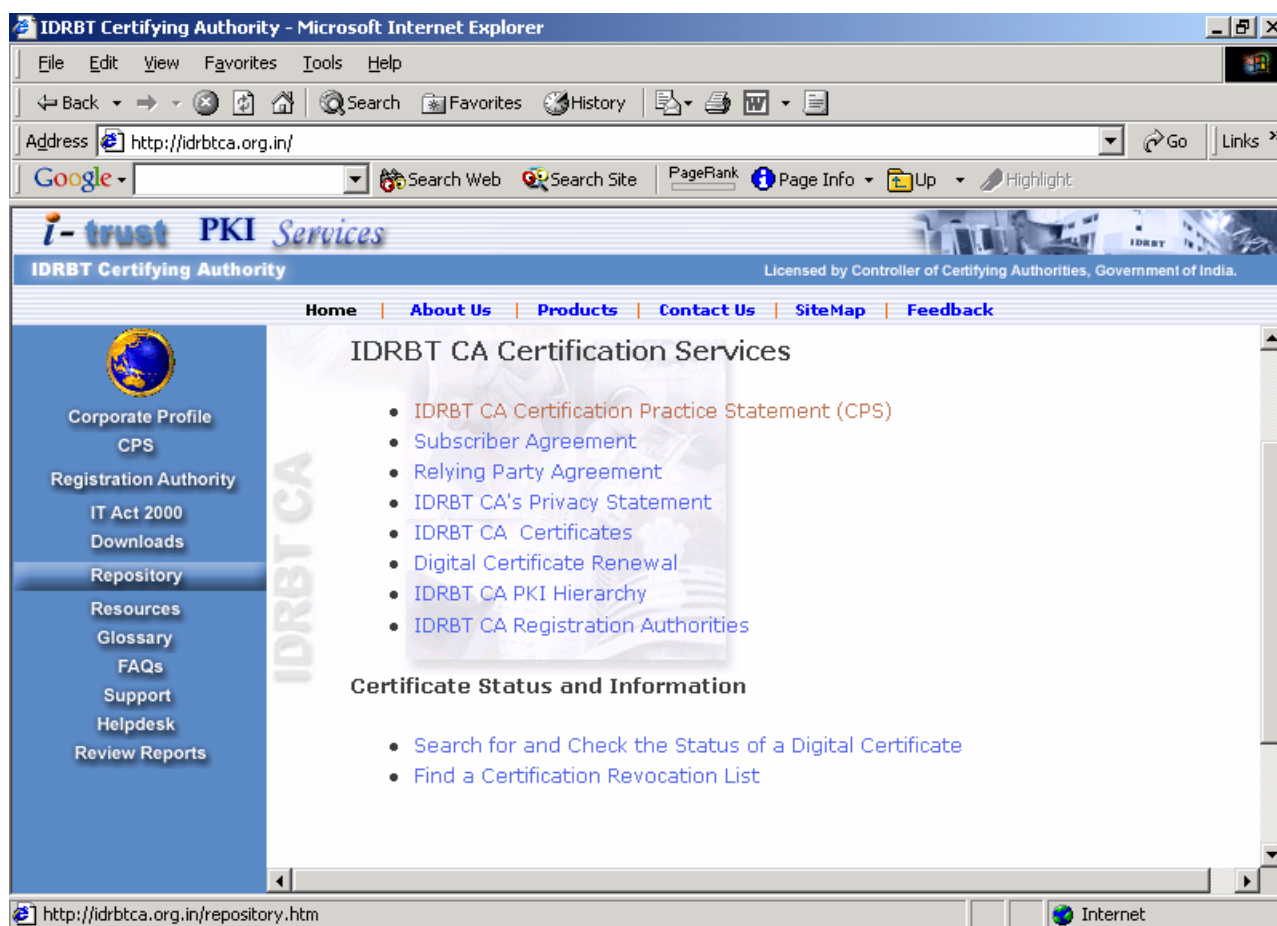


Fig 3. Repository Page.

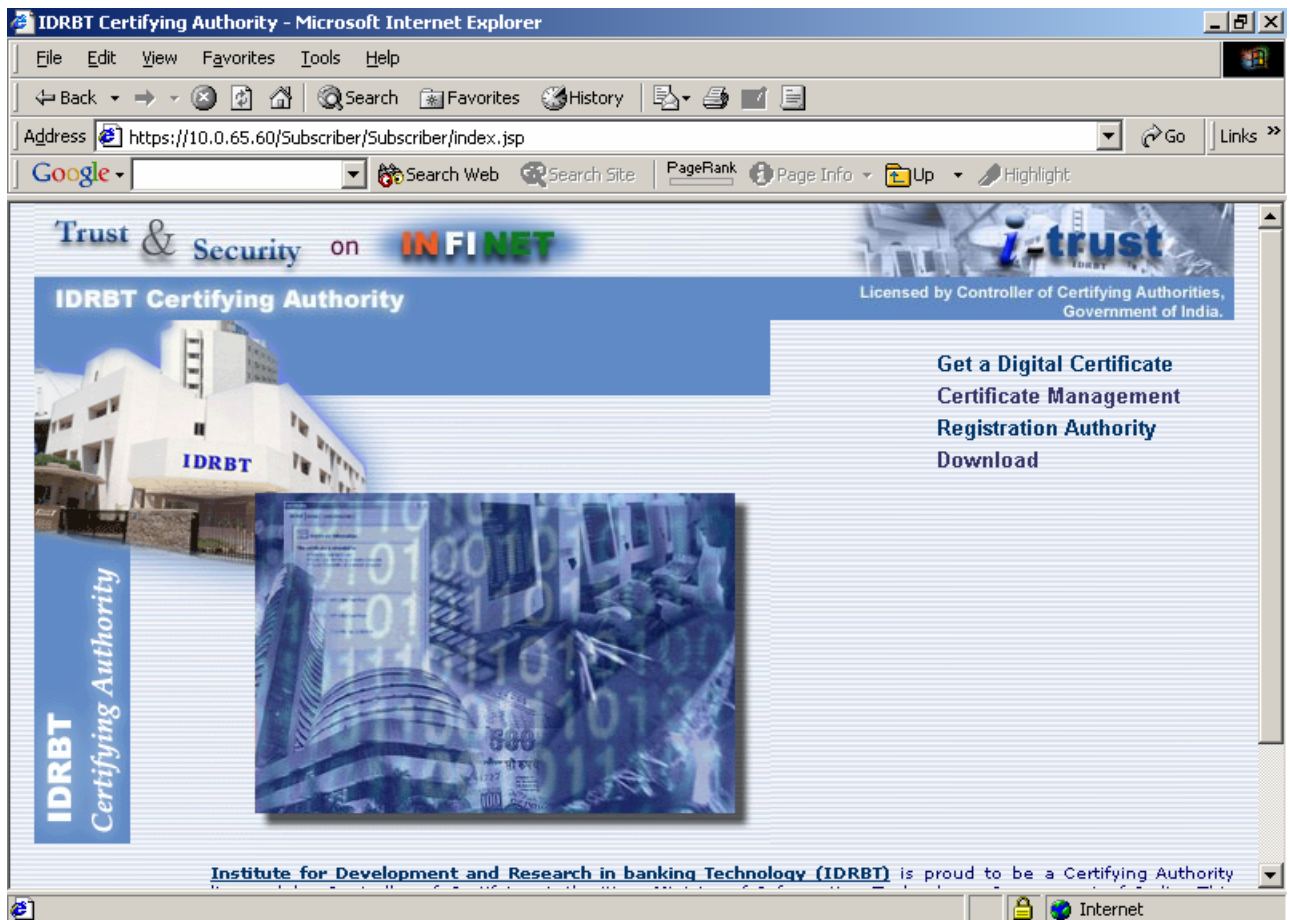
You can proceed with the IDRBT CA Certification Services (i-trust PKI Services) by clicking the link provided in the homepage as shown in Fig 4.



Fig 4

You can select the type of certificate you need, and can view the description and select the Class of certificate you require.

After selecting the Class of certificate you need, Click the appropriate link to obtain the certificate. This will guide you to IDRBT CA's secured site <https://10.0.65.60/Subscriber/Subscriber/index.jsp>



Click the 'lock' icon in the Internet Explorer status bar to view the Secure Server Certificate of IDRBT CA Website (Fig 3).

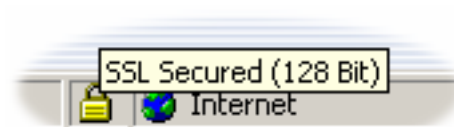


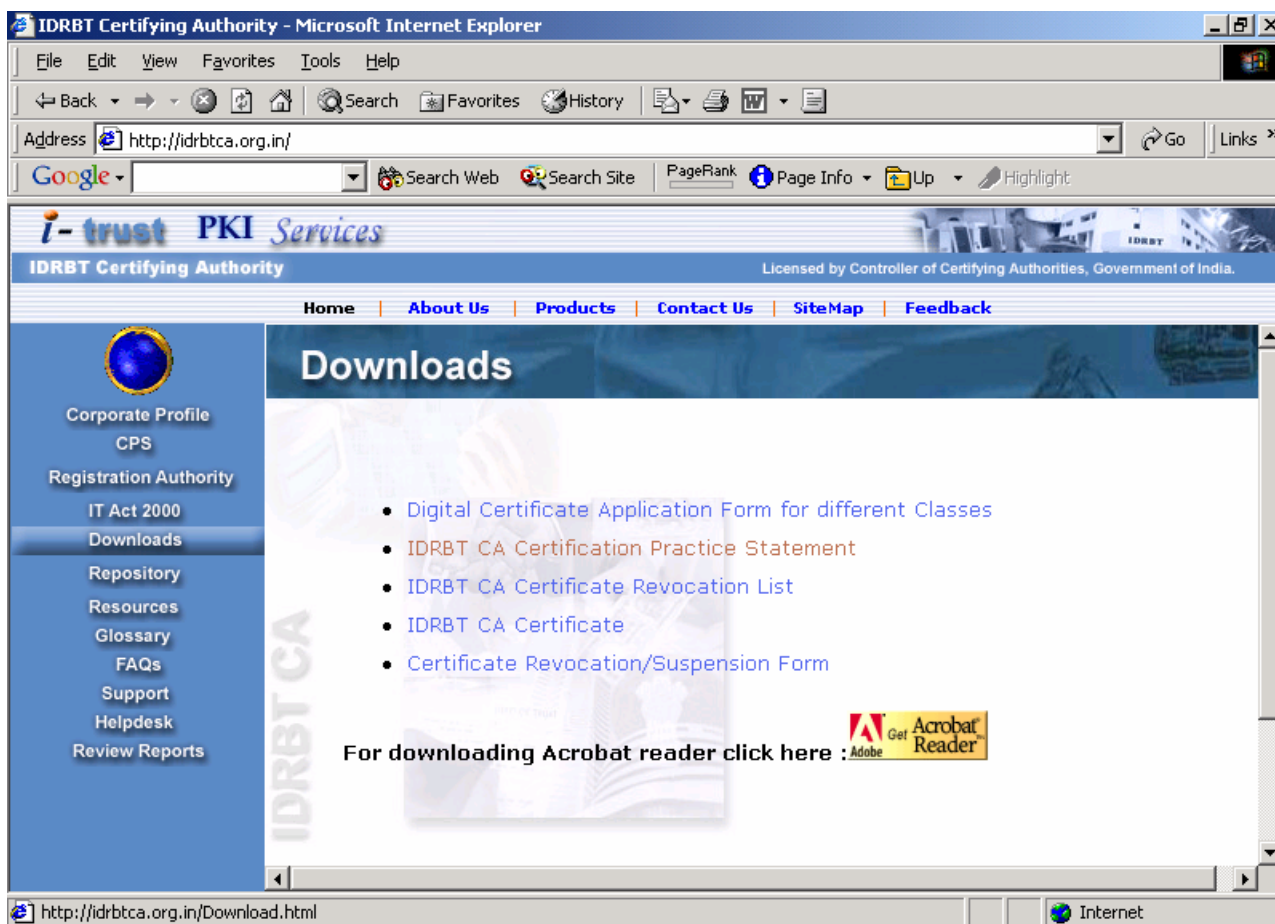
Fig 3

IDRBT CA Certification Services supports the following functionalities:

- Getting a Digital Certificate
- Viewing Status of the Digital Certificate
- Querying the Certificate details
- Revoking a Digital Certificate
- Suspending the Digital Certificate
- Activating the Digital Certificate
- Changing the Password
- Changing the personal details
- Getting others Digital Certificate
- Downloading the IDRBT CA Root Certificate
- Downloading the latest Certificate Revocation List

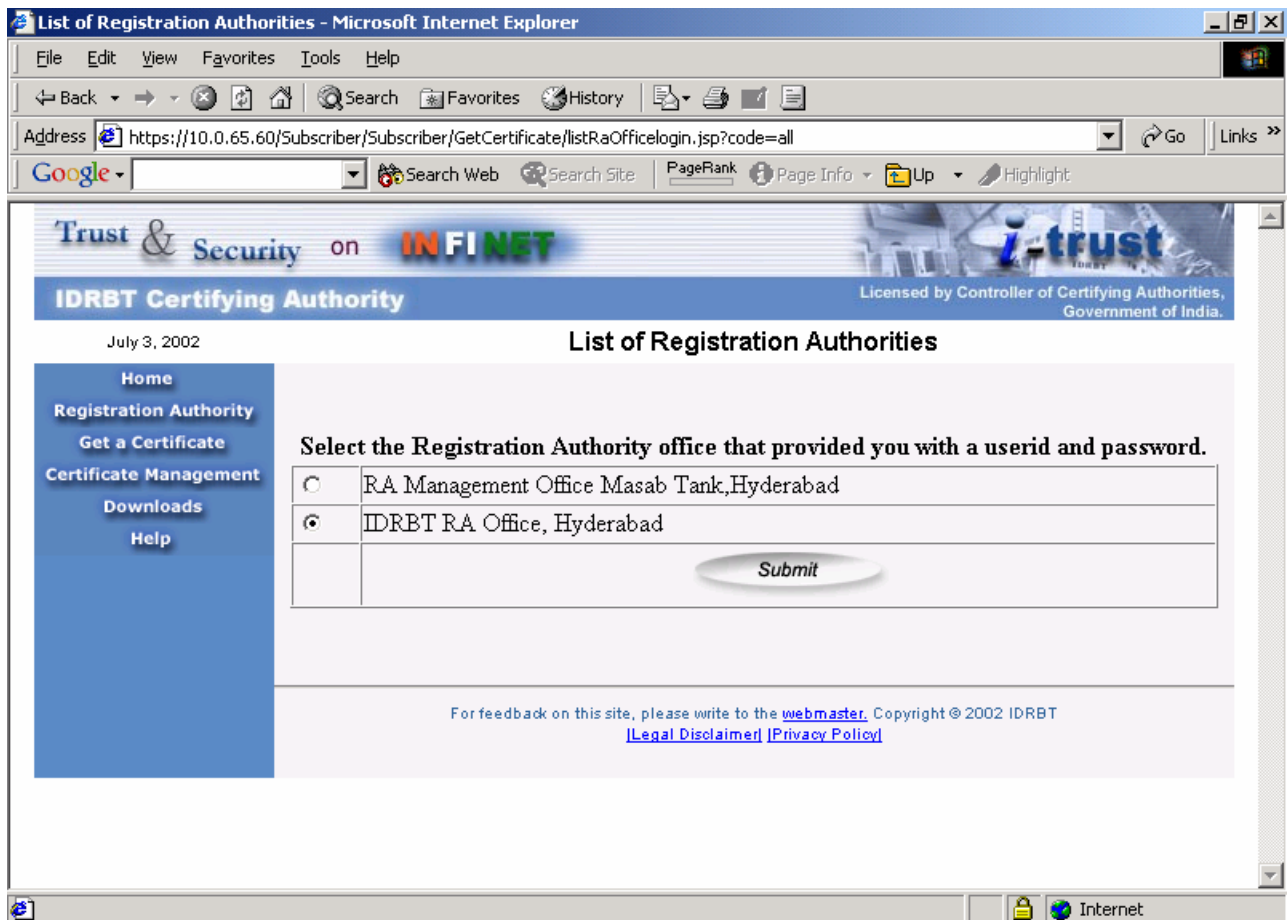
2.1. Procedures for requesting a Digital Certificate

1. Browse <http://idrbtca.org.in/> and go to the Downloads link. Download the application form for Digital Certificate for different Classes.



2. Download the Subscriber Agreement from the Repository link.
3. Fill the Application form for Digital Certificate. Make sure that you have filled all the mandatory fields.
4. The price for each Classes of Digital Certificate is listed in the website. Take a Demand Draft for the corresponding amount in favour of "IDRBT" payable at Hyderabad.
5. The list of Registration Authority (RA) Offices is mentioned in the website. The addresses of the RA Offices are also listed. You can select your corresponding RA Office and send the duly filled Application form for Digital Certificate, duly signed Subscriber Agreement and the Demand Draft for the concerned amount.
6. The Registration Authority will assign a User name and Password and will send to the Applicant in a sealed envelope.

7. Acknowledge the receipt of the Username and Password to the concerned RA. The username and password will be inactivated till the user acknowledges the receipt of the sealed envelope.
8. If the seal is broken/ envelope is torn, intimate the concerned RA immediately for taking necessary action.
9. Proceed with the IDRBT CA Certification Services from the homepage of <http://idrbtca.org.in/>. Click the “Get a Digital Certificate” from the homepage of the IDRBT CA Certification Services (<https://10.0.65.60/Subscriber/Subscriber/>).
10. Read the description of the certificates and click the Login button.
11. Select the Registration Authority from which you have obtained the User ID and Password and click Submit button.



The screenshot shows a Microsoft Internet Explorer browser window displaying the IDRBT Certifying Authority website. The address bar shows the URL: <https://10.0.65.60/Subscriber/Subscriber/GetCertificate/listRaOfficellogin.jsp?code=all>. The website header includes the IDRBT logo and the text "IDRBT Certifying Authority". Below the header, there is a navigation menu with links: Home, Registration Authority, Get a Certificate, Certificate Management, Downloads, and Help. The main content area is titled "List of Registration Authorities" and contains a form for selecting a Registration Authority office. The form has two radio buttons: "RA Management Office Masab Tank, Hyderabad" and "IDRBT RA Office, Hyderabad". The second option is selected. Below the radio buttons is a "Submit" button. At the bottom of the page, there is a footer with the text: "For feedback on this site, please write to the [webmaster](#). Copyright © 2002 IDRBT. [Legal Disclaimer](#) | [Privacy Policy](#)".

12. Enter the User ID and Password given to you by the Registration Authority and click Login button.

caservice@idrbt.ac.in'." data-bbox="143 166 934 602"/>

13. You are advised to change your login password at the first login time. Click the Certificate Management link and Click the Change Password from the top menu.

Certificate Management - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print

Address <https://10.0.65.60/Subscriber/Subscriber/CertManagement/certMgmtHome.jsp> Go Links

Google Search Web Search Site PageRank Page Info Up Highlight

Trust & Security on INFINET

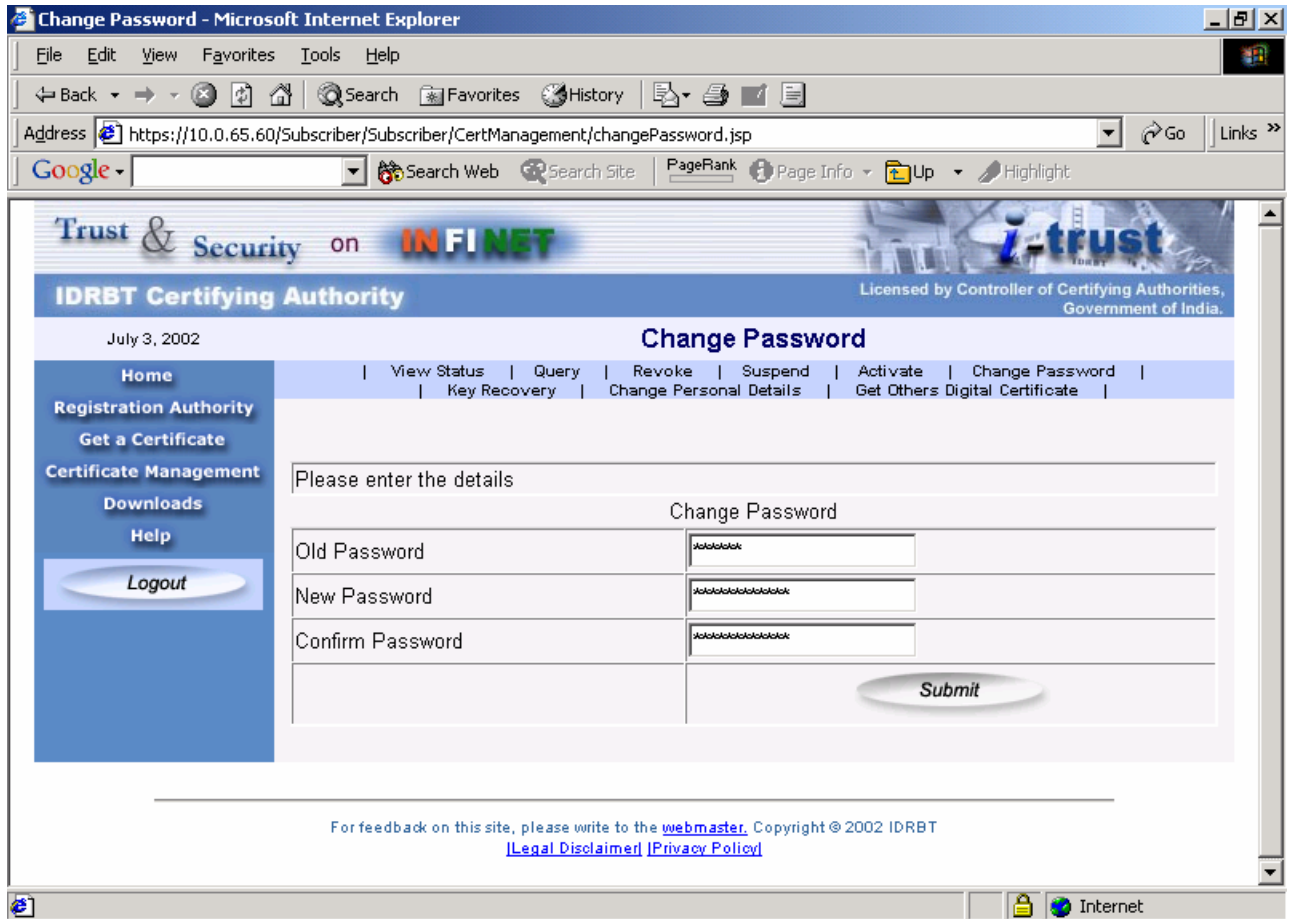
IDRBT Certifying Authority Licensed by Controller of Certifying Authorities, Government of India.

July 3, 2002 **Certificate Management**

Home Registration Authority Get a Certificate Certificate Management Downloads Help Logout	View Status Query Revoke Suspend Activate Change Password Key Recovery Change Personal Details Get Others Digital Certificate
	<p>You have last logged on 2002-06-28 12:25:44.0 from 10.0.67.101</p> <p>You may need to query your request status or perform Certificate Maintenance operations, to ensure the security and privacy of your web based transactions.</p> <p>You can</p> <ul style="list-style-type: none"> • View the Status of your request if you remember your request number. • View the Status of your request based on certain specified criteria. • Put a Revoke request • Change the password

<https://10.0.65.60/Subscriber/Subscriber/CertManagement/changePassword.jsp> Internet

14. Give the old Password, new Password and confirm the new Password. Click the Submit button. Confirmation message showing that “Your password has been changed” will be displayed.



Change Password - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Search Favorites History Print

Address <https://10.0.65.60/Subscriber/Subscriber/CertManagement/changePassword.jsp> Go Links

Google Search Web Search Site PageRank Page Info Up Highlight

Trust & Security on INFINET

IDRBT Certifying Authority

July 3, 2002

Change Password

Licensed by Controller of Certifying Authorities, Government of India.

Home | View Status | Query | Revoke | Suspend | Activate | Change Password |
Registration Authority | Key Recovery | Change Personal Details | Get Others Digital Certificate |

Get a Certificate

Certificate Management

Downloads

Help

Logout

Please enter the details

Change Password

Old Password

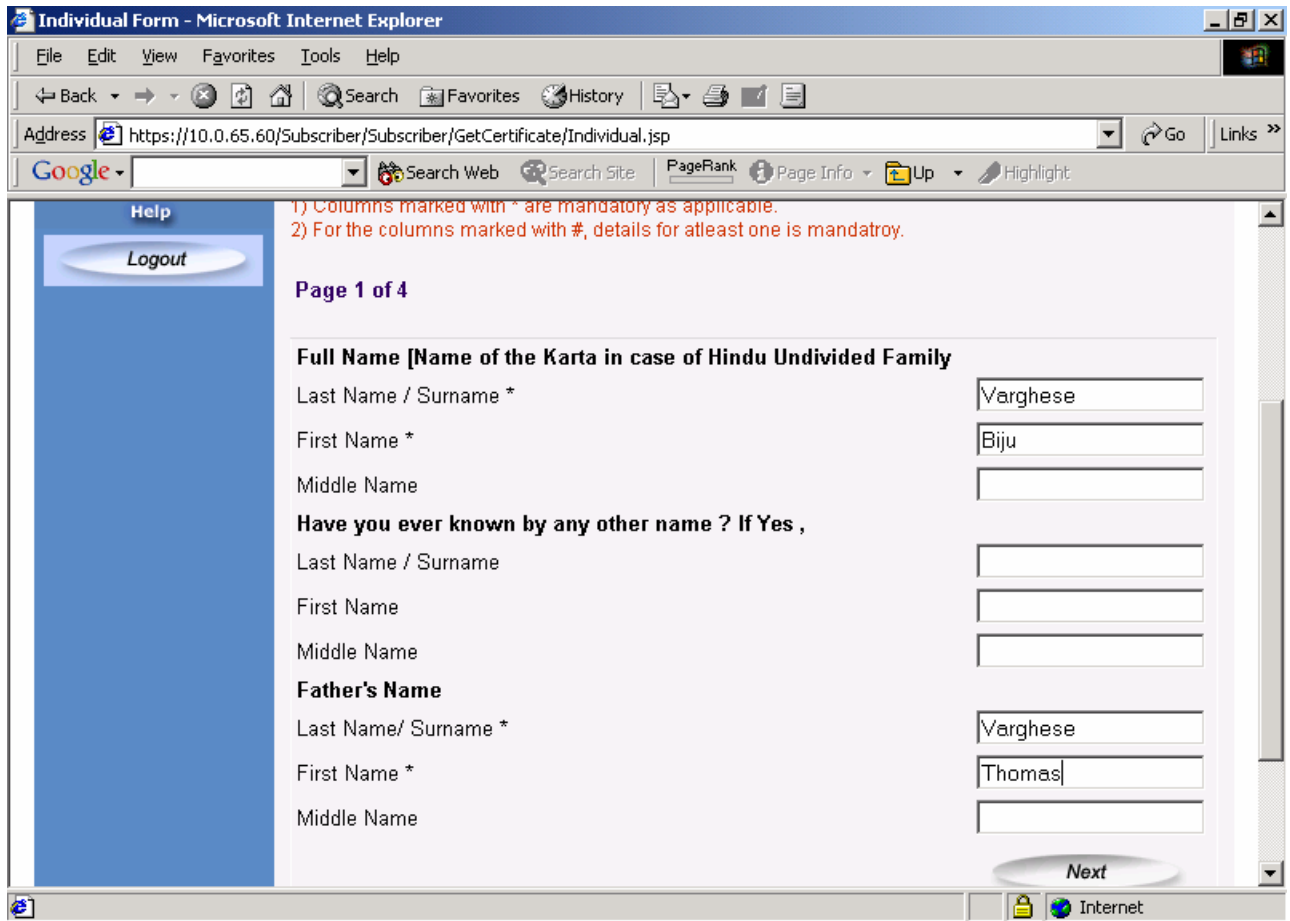
New Password

Confirm Password

Submit

For feedback on this site, please write to the [webmaster](#). Copyright © 2002 IDRBT
[Legal Disclaimer](#) [Privacy Policy](#)

15. Click on the Get a Certificate link on the left pane to proceed with getting a Digital Certificate. Fill up the Page 1 of the four page application form. This online application form is required even if you have filled up the paper based application form which has send to the Registration Authority. Click the Next button to proceed to the next page.



Individual Form - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print Mail

Address <https://10.0.65.60/Subscriber/Subscriber/GetCertificate/Individual.jsp> Go Links >>

Google Search Web Search Site PageRank Page Info Up Highlight

Help
Logout

1) Columns marked with * are mandatory as applicable.
2) For the columns marked with #, details for atleast one is mandatroy.

Page 1 of 4

Full Name [Name of the Karta in case of Hindu Undivided Family]

Last Name / Surname *

First Name *

Middle Name

Have you ever known by any other name ? If Yes ,

Last Name / Surname

First Name

Middle Name

Father's Name

Last Name/ Surname *

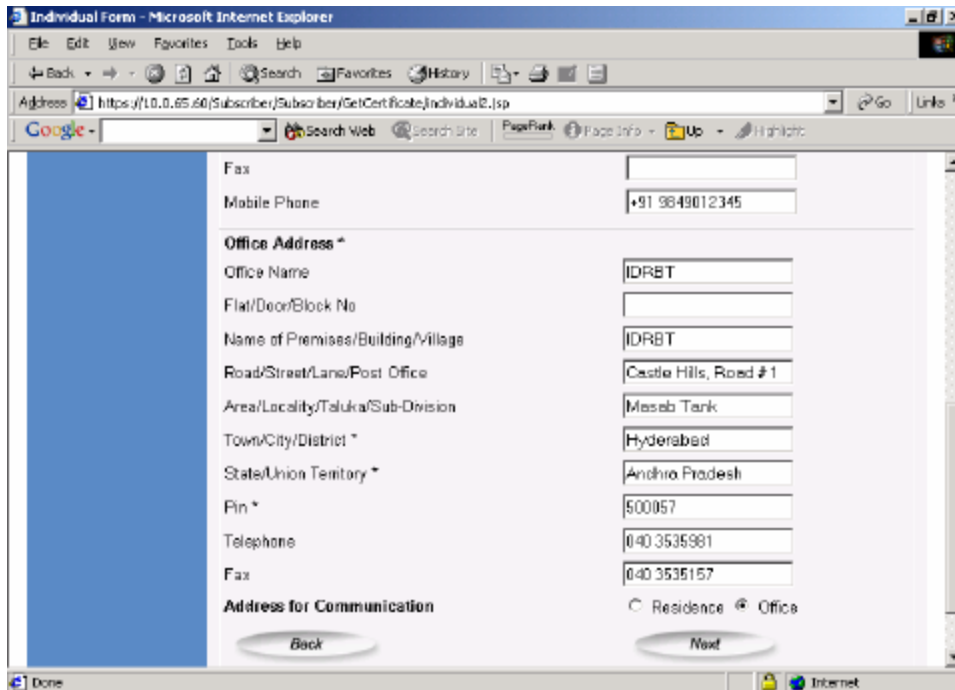
First Name *

Middle Name

Next

Internet

16. Fill the four pages of the online application form.



Individual Form - Microsoft Internet Explorer

Address: https://10.0.65.60/Subscriber/Subscriber/GetCertificate/individual2.jsp

Fax:

Mobile Phone:

Office Address *

Office Name:

Flat/Door/Block No:

Name of Premises/Building/Village:

Road/Street/Lane/Post Office:

Area/Locality/Taluka/Sub-Division:

Town/City/District *:

State/Union Territory *:

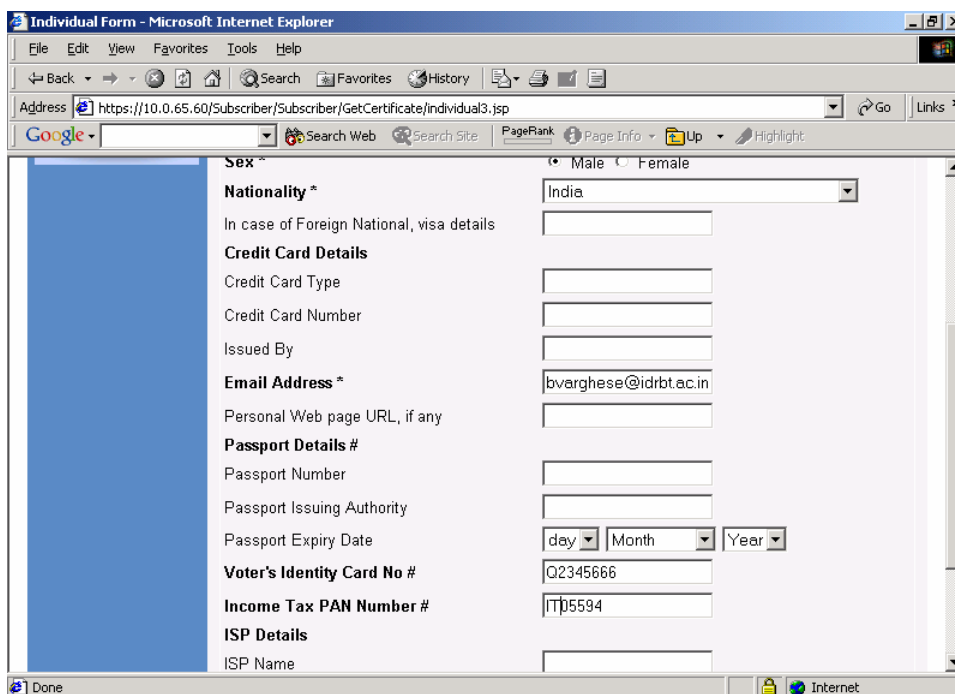
Pin *:

Telephone:

Fax:

Address for Communication

☐ Residence ☒ Office



Individual Form - Microsoft Internet Explorer

Address: https://10.0.65.60/Subscriber/Subscriber/GetCertificate/individual3.jsp

Sex * ☒ Male ☐ Female

Nationality *

In case of Foreign National, visa details:

Credit Card Details

Credit Card Type:

Credit Card Number:

Issued By:

Email Address *

Personal Web page URL, if any:

Passport Details #

Passport Number:

Passport Issuing Authority:

Passport Expiry Date:

Voter's Identity Card No #

Income Tax PAN Number #

ISP Details

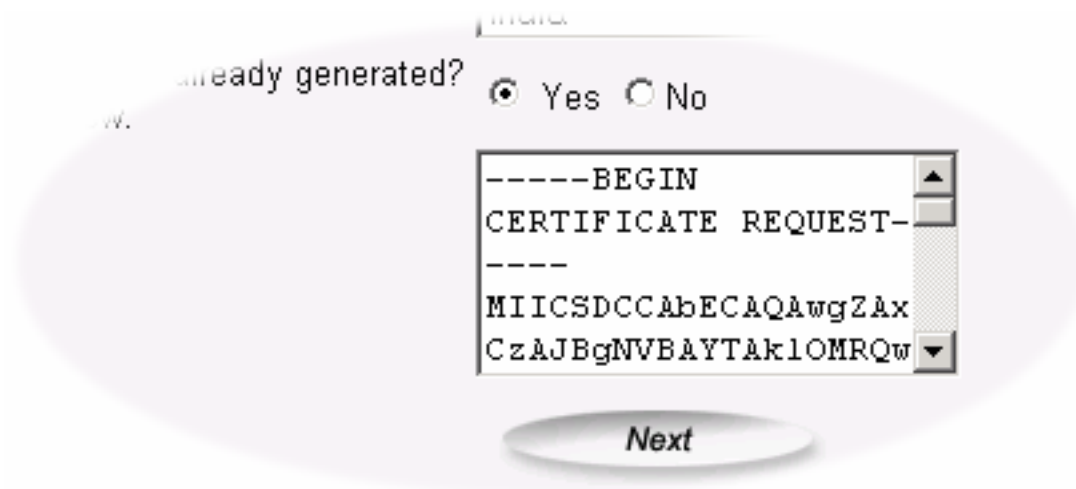
ISP Name:

Select the type of Certificate i.e., Signing Certificate, Encryption certificate, Server Certificate, Object Signing Certificate.

Select the Class of Certificate, i.e. Class 1 Certificate, Class 2 Certificate, Class 3 Certificate. If you are selecting the Server Certificate or Object Signing Certificate, make sure that you select Class 3 Certificate.

17. Click Next to proceed.

Note: If you have generated PKCS#10 request of your own, you can paste it in the appropriate text box provided after clicking the 'Yes' radio button.

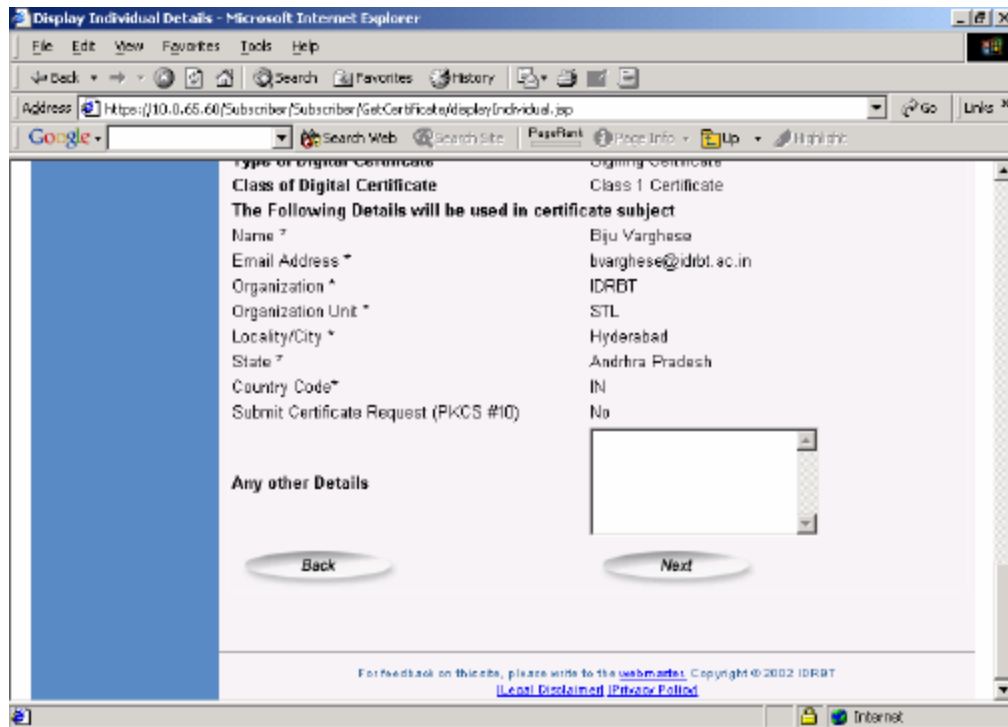


Certificate already generated? ☒ Yes ☐ No

-----BEGIN
CERTIFICATE REQUEST-----
MIICSDCCAbECAQAwgZAx
CzAJBgNVBAYTAklOMRQw

Next

18. The details you have given are listed in the page. You can click Back button to go back to change any of your details. If everything is perfect, click Next button.



Display Individual Details - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print PageRank Page Info Up Highlight

Address <https://10.0.65.60/Subscriber/Subscriber/GetCertificate/displayIndividual.jsp> Go Units

Google Search Web Search Site

Type of Original Certificate: Signing Certificate
Class of Digital Certificate: Class 1 Certificate

The Following Details will be used in certificate subject

Name *: Biju Varghese
Email Address *: bvarghese@idrbl.ac.in
Organization *: IDRBT
Organization Unit *: STL
Locality/City *: Hyderabad
State *: Andhra Pradesh
Country Code*: IN
Submit Certificate Request (PKCS #10): No

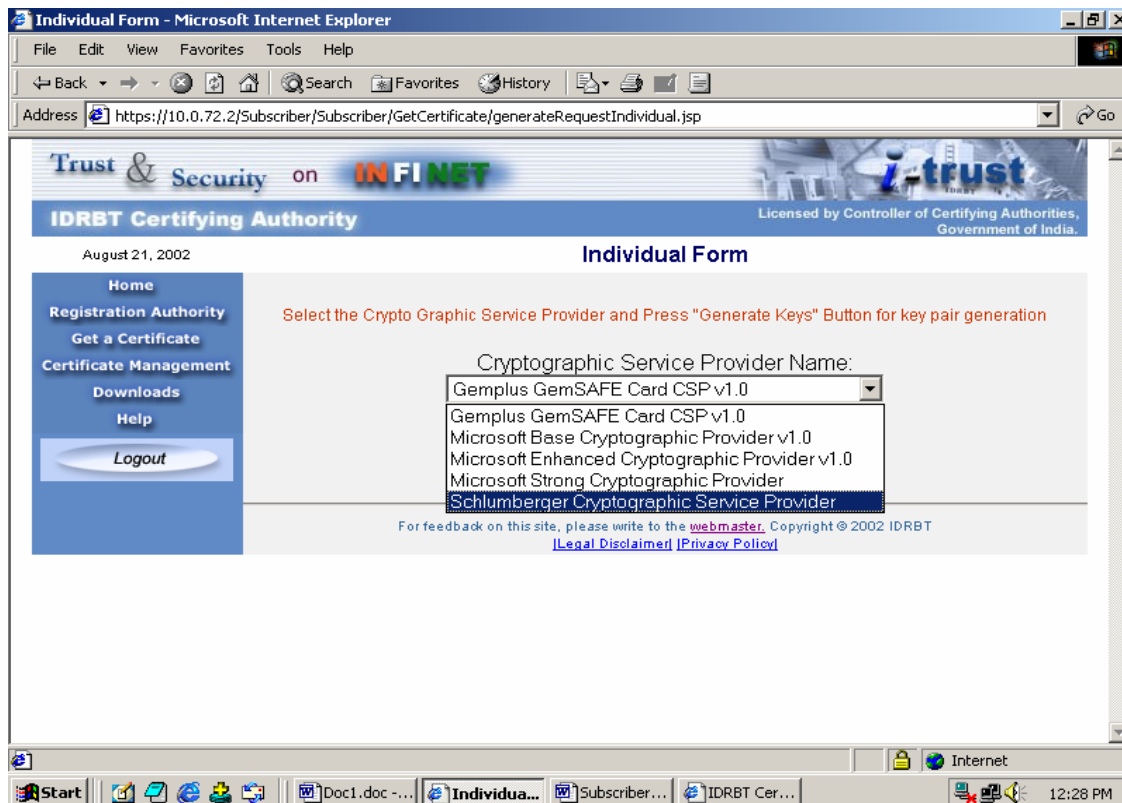
Any other Details

Back Next

For feedback on this site, please write to the [webmaster](#). Copyright © 2002 IDRBT
[Legal Disclaimer](#) [Privacy Policy](#)

Internet

19. Select the Cryptographic Service provider from the list provided. If you have installed a smart card reader or hardware token in your machine, the corresponding name will be listed there. If you don't have a smart card reader or hardware token installed in you machine, choose the **Microsoft Base Cryptographic Provider v1.0** from the list. In the below it shown for the Schlumberger Smart Card Reader.

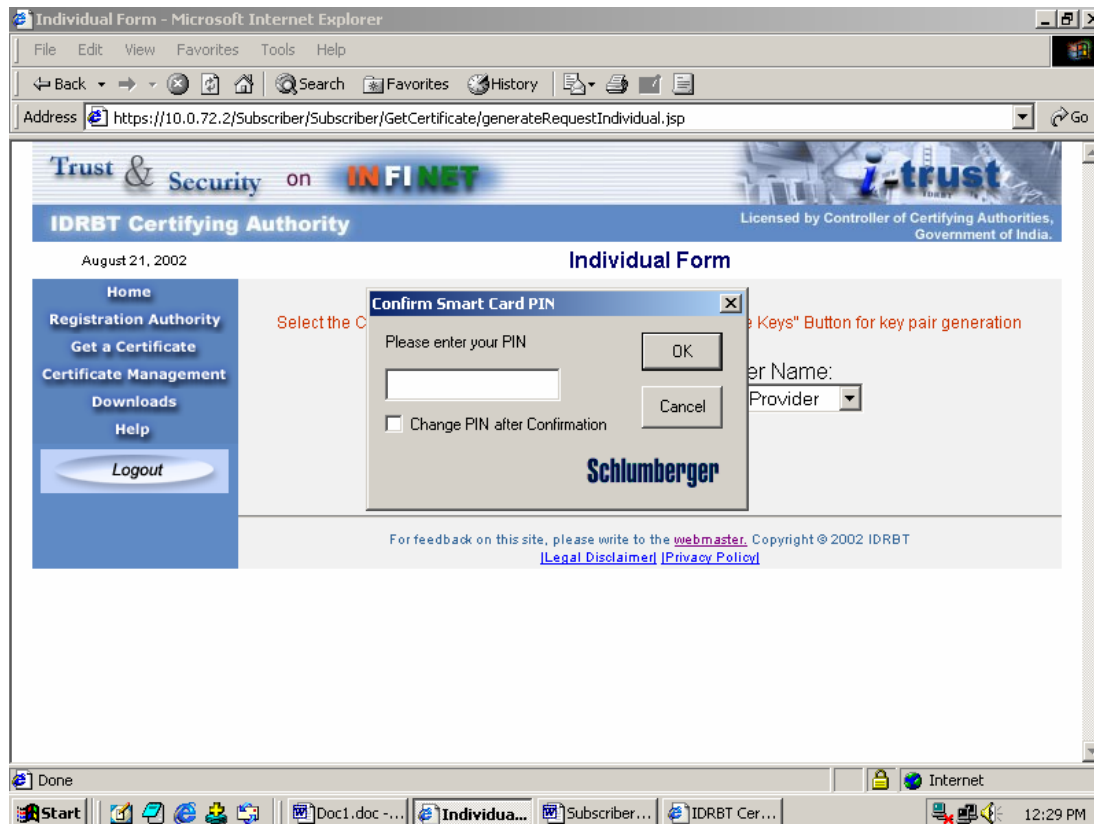


20. Click the Generate Keys Button to generate the key pair.

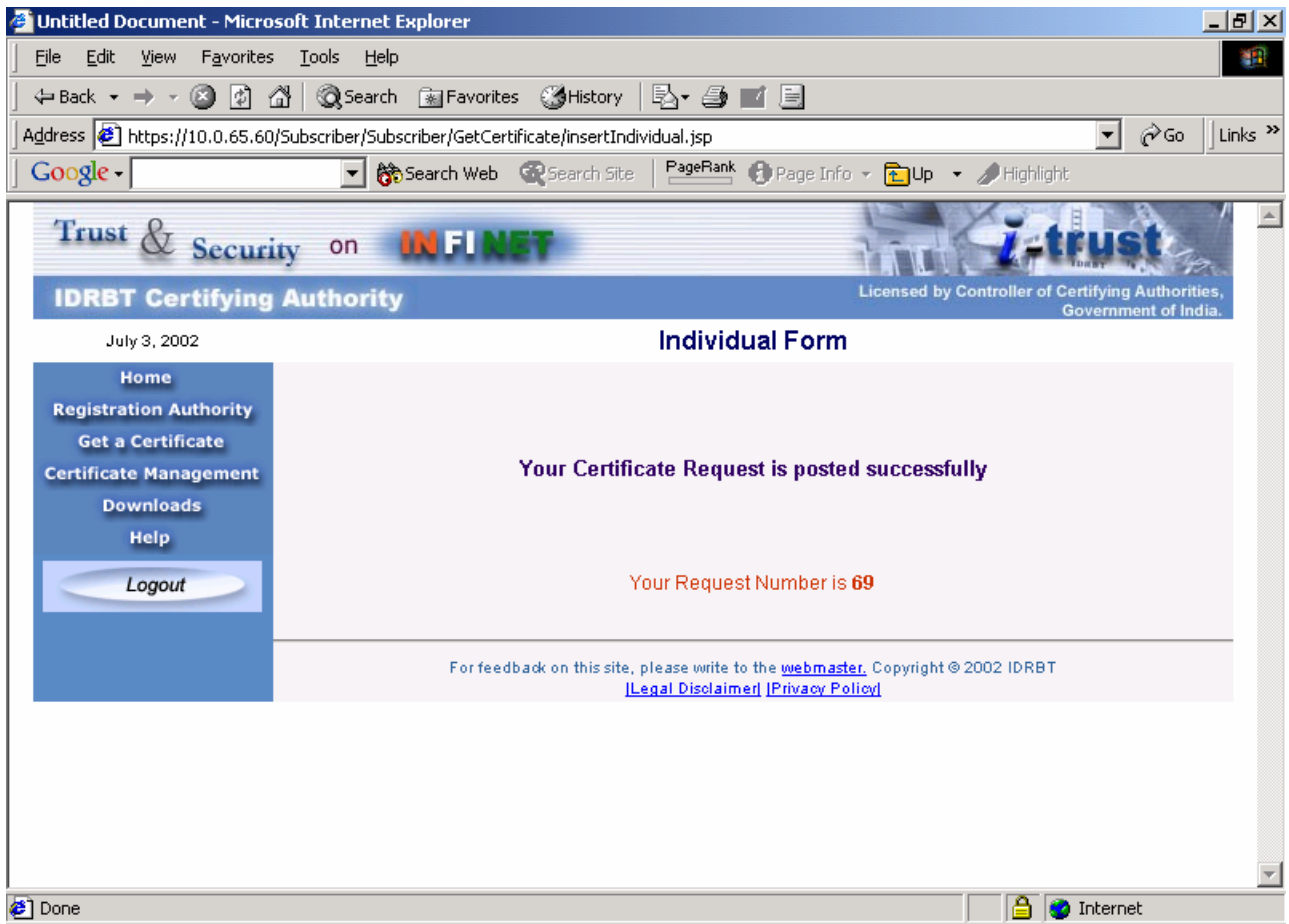
Generate Keys

21. For example if you are using Schlumberger, then choose the Schlumberger provider. When you click generate, it will ask you Smart Card PIN for authentication. Give your PIN and press ok.

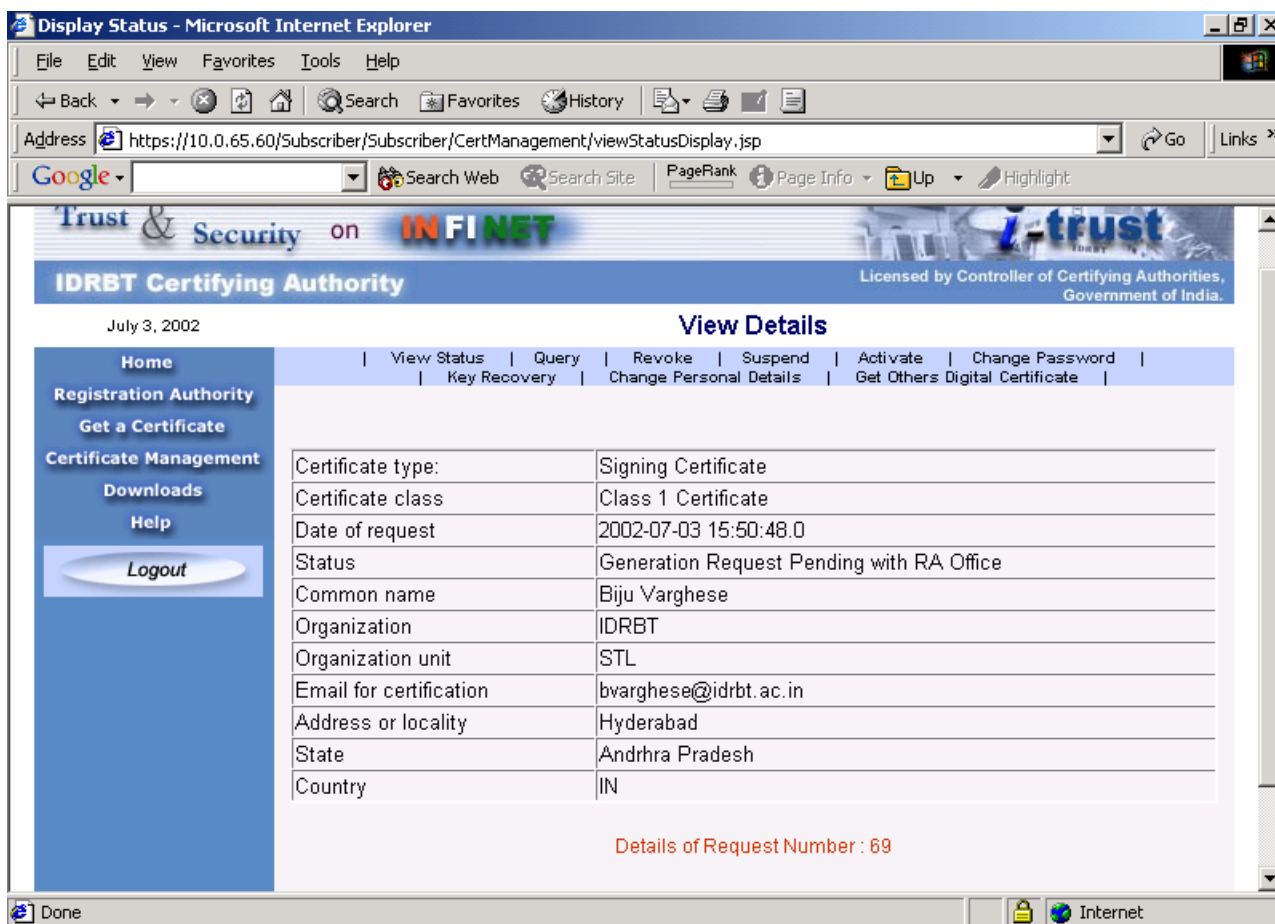
Note: Be sure that, before using the Smart Card for the request generation first time, you have personalized the card.



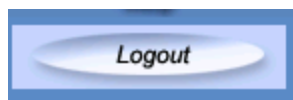
22. If you have selected the correct Card provider and your PIN is correct then, it will take few second to generate the key pair. After the successful creation of the keys it will give the following Fig. Your Certificate request will be posted to the Registration Authority for verification. You will get a confirmation message and the corresponding request number. Note this certificate request number for further enquiry.



23. You can query your Certificate request status by clicking the **Certificate Management** link in the left page and then clicking the View Status on the top menu.



24. Click Logout button on the left pane for logging out from the system.



25. Next time when you login to the system using your User ID and Password, the details you have filled earlier will be listed.

Check Detail - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print

Address <https://10.0.65.60/Subscriber/Subscriber/GetCertificate/individualUpdate.jsp> Go Links

Google Search Web Search Site PageRank Page Info Up Highlight

Trust & Security on **INFINET** **i-trust**

IDRBT Certifying Authority Licensed by Controller of Certifying Authorities, Government of India.

July 3, 2002 **Check Details**

Home
Registration Authority
Get a Certificate
Certificate Management
Downloads
Help
Logout

Instructions
Check whether the details are correct. If it is wrong, change the details

Full Name [Name of the Karta in case of Hindu Undivided Family]

Last Name / Surname *	Varghese
First Name *	Biju
Middle Name	null

Have you ever known by any other name ? If Yes ,

Last Name / Surname	null
First Name	null
Middle Name	null

Father's Name

Last Name/ Surname *	Varghese
First Name *	Thomas
Middle Name	null

Residential Address *

Done Internet

26. You can change your personal details if you are requesting for another certificate. This can be done by clicking the Certificate Management link from the left pane and selecting the Change Personal Details from the top menu. Change the details if required and click the Submit button.


Change Details - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print

Address <https://10.0.65.60/Subscriber/Subscriber/CertManagement/changeDetailsIndividual.jsp> Go Links >>

Google Search Web Search Site PageRank Page Info Up Highlight

Trust & Security on **INFINET** 

IDRBT Certifying Authority Licensed by Controller of Certifying Authorities, Government of India.

July 3, 2002 **Change Details**

Home Registration Authority Get a Certificate Certificate Management Downloads Help Logout	View Status Query Revoke Suspend Activate Change Password Key Recovery Change Personal Details Get Others Digital Certificate
	Instructions Check whether the details are correct. If it is wrong, change the details
	Full Name [Name of the Karta in case of Hindu Undivided Family] Last Name / Surname * Varghese First Name * Biju Middle Name null
	Have you ever known by any other name ? If Yes , Last Name / Surname null First Name null Middle Name null
	Father's Name Last Name/ Surname * Varghese First Name * Thomas Middle Name null

Done Internet

2.2. Requesting an Encryption Certificate

1. Login to the website as per the procedure mentioned above. For obtaining an Encryption certificate, you must obtain a signing certificate prior to the application.
2. Select 'Encryption Certificate' from the certificate type in the Page 4 of the Certificate Request form. It will prompt for obtaining a signing certificate prior to you application for Encryption Certificate.

Individual Form - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print Mail

Address <https://10.0.65.60/Subscriber/Subscriber/GetCertificate/individual5.jsp> Go Links

Google Search Web Search Site PageRank Page Info Up Highlight

July 3, 2002 **Individual Form** Government of India.

Home
Registration Authority
Get a Certificate
Certificate Management
Downloads
Help
Logout

Instructions
1) Columns marked with * are mandatory as applicable.
2) For the columns marked with #, details for atleast one is mandatroy.

Page 4 of 4

Certificate Type Signing Certificate

Certificate Class Encryption Certificate

The Following Details will be used in certificate subject

Name *

Email Address *

Organization *

Organization Unit *

Locality/City *

State *

Done Internet



3. Fill the details and click the Submit button.

Individual Form - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print Mail

Address <https://10.0.65.60/Subscriber/Subscriber/GetCertificate/individual5.jsp> Go Links >>

Google Search Web Search Site PageRank Page Info Up Highlight

Logout

Certificate Type Encryption Certificate

Certificate Class Class 1 Certificate

The Following Details will be used in certificate subject

Name * Biju Varghese

Email Address * bvarghese@idrbt.ac.in

Organization * IDRBT

Organization Unit * STL

Locality/City * Hyderabad

State * AP

Country Code* India

Do you have a certificate request already generated?
Choose 'No' to generate it now. ☐ Yes ☐ No

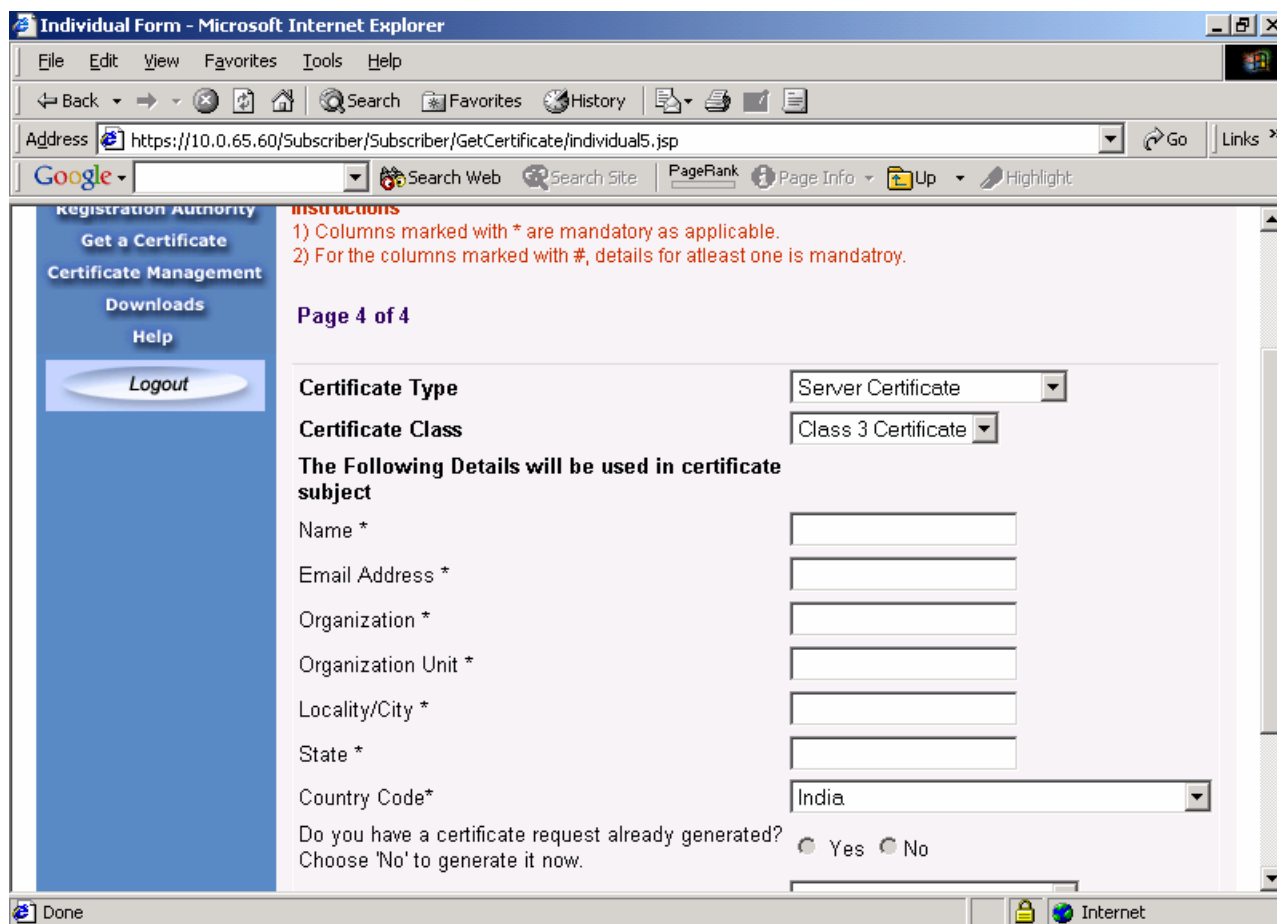
Any other Details

Done Internet

4. You will be informed with the Certificate Request number.
5. Query the Certificate request number for viewing the status of Certificate request.
6. Logout from the system.

2.3. Requesting an Server Certificate

1. Select 'Server Certificate' from the certificate type in the Page 4 of the Certificate Request form. Make sure that you select the Class 3 Certificate from the Certificate Class.



Individual Form - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print Mail News

Address <https://10.0.65.60/Subscriber/Subscriber/GetCertificate/individual5.jsp> Go Links >>

Google Search Web Search Site PageRank Page Info Up Highlight

Registration Authority
[Get a Certificate](#)
[Certificate Management](#)
[Downloads](#)
[Help](#)
[Logout](#)

Instructions
 1) Columns marked with * are mandatory as applicable.
 2) For the columns marked with #, details for atleast one is mandatroy.

Page 4 of 4

Certificate Type Server Certificate

Certificate Class Class 3 Certificate

The Following Details will be used in certificate subject

Name *

Email Address *

Organization *

Organization Unit *

Locality/City *

State *

Country Code* India

Do you have a certificate request already generated? ☐ Yes ☐ No
 Choose 'No' to generate it now.

Done Internet

2. Fill the necessary details and click the Next button.
3. It will prompt for pasting the PKCS#10 request generated by the Server. Paste it on the space provided. Click the Submit PKCS 10 Request Button.

Individual Form - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print

Address <https://10.0.65.60/Subscriber/Subscriber/GetCertificate/generateRequestIndividual.jsp> Go Links

Google Search Web Search Site PageRank Page Info Up Highlight

Trust & Security on INFINET

IDRBT Certifying Authority Licensed by Controller of Certifying Authorities, Government of India.

July 3, 2002 **Individual Form**

Home

Registration Authority

Get a Certificate

Certificate Management

Downloads

Help

Logout

Please Copy and Paste the Certificate Request (PKCS#10) in BASE64 format with -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST----- delimiters

```

MJV1TF1YVr48ngGULD//1Y1dWAXY&zmj1Xbxbus68czkyF8ZJ1
5n3SprPLdgzpBy
3a0jPe8HLnes0QM1h42fcDQ7omzMD2TODZ5vq1oUg9euPyz0Ww
et7FXfq5DDi+PK
5IK4m39i9DGFja6E
-----END CERTIFICATE REQUEST-----

```

Submit PKCS10 Request

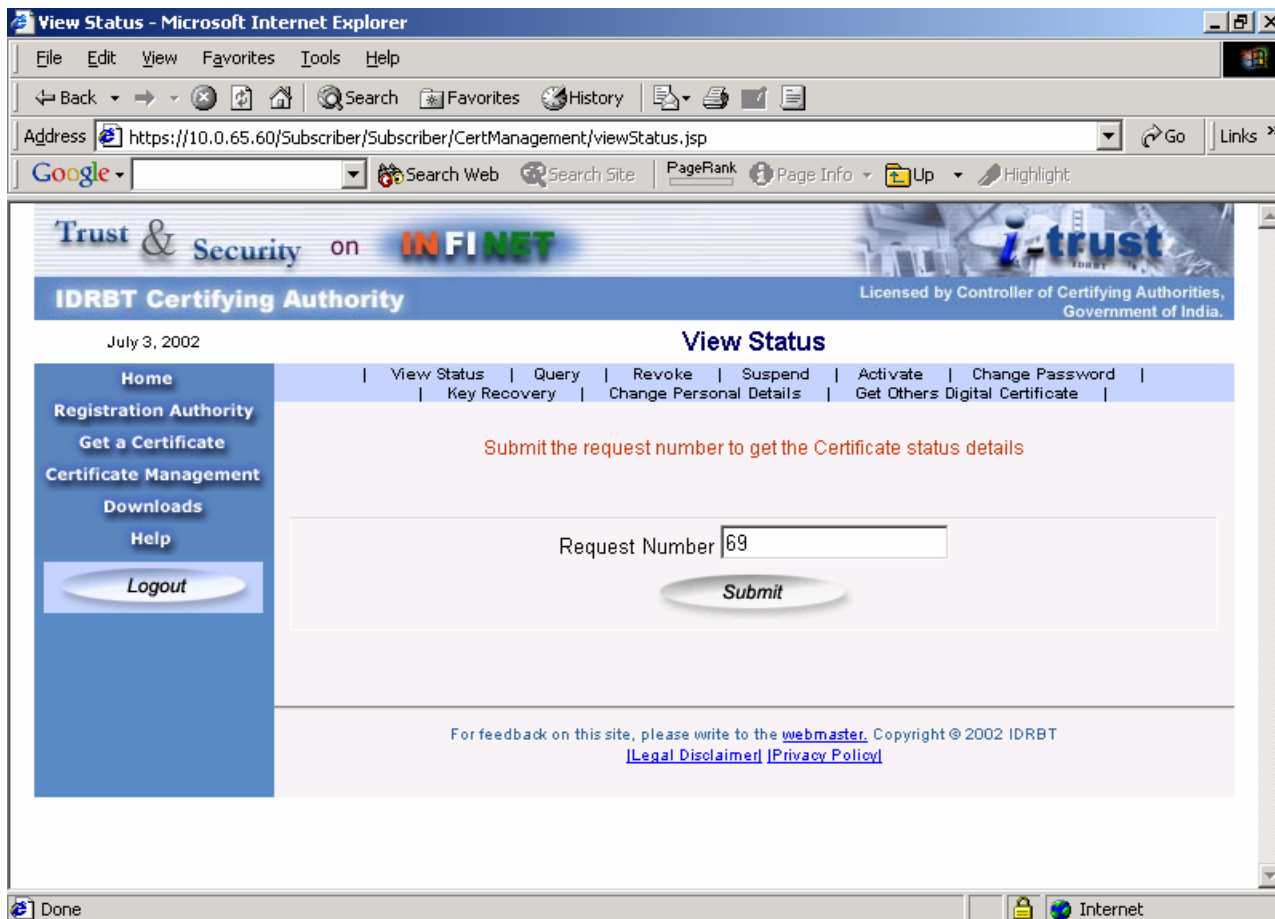
For feedback on this site, please write to the [webmaster](#). Copyright © 2002 IDRBT
[\[Legal Disclaimer\]](#) [\[Privacy Policy\]](#)

Done Internet

4. You will be informed with the Certificate Request number.
5. Query the Certificate request number for viewing the status of Certificate request.
6. Logout from the system.

2.4. Downloading the Digital Certificate

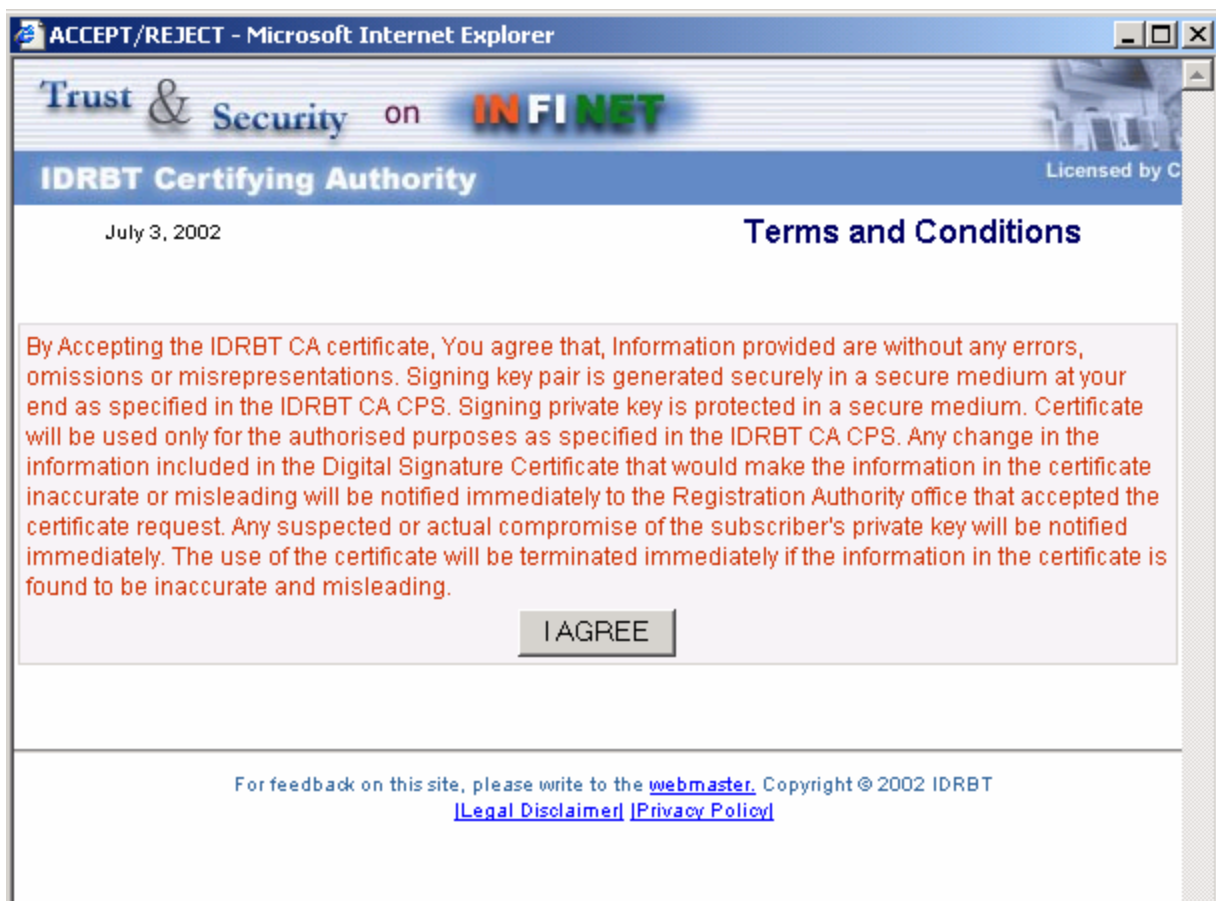
1. Click the “Certificate Management” link on the homepage.
2. Select the Registration Authority and login using User ID and Password.
3. Click the View Status on the top bar. Give the request number and Click Submit Button.



4. If the certificate is issued by IDRBT CA, the Certificate will be available for Downloading. The status of the certificate will be shown as given below:

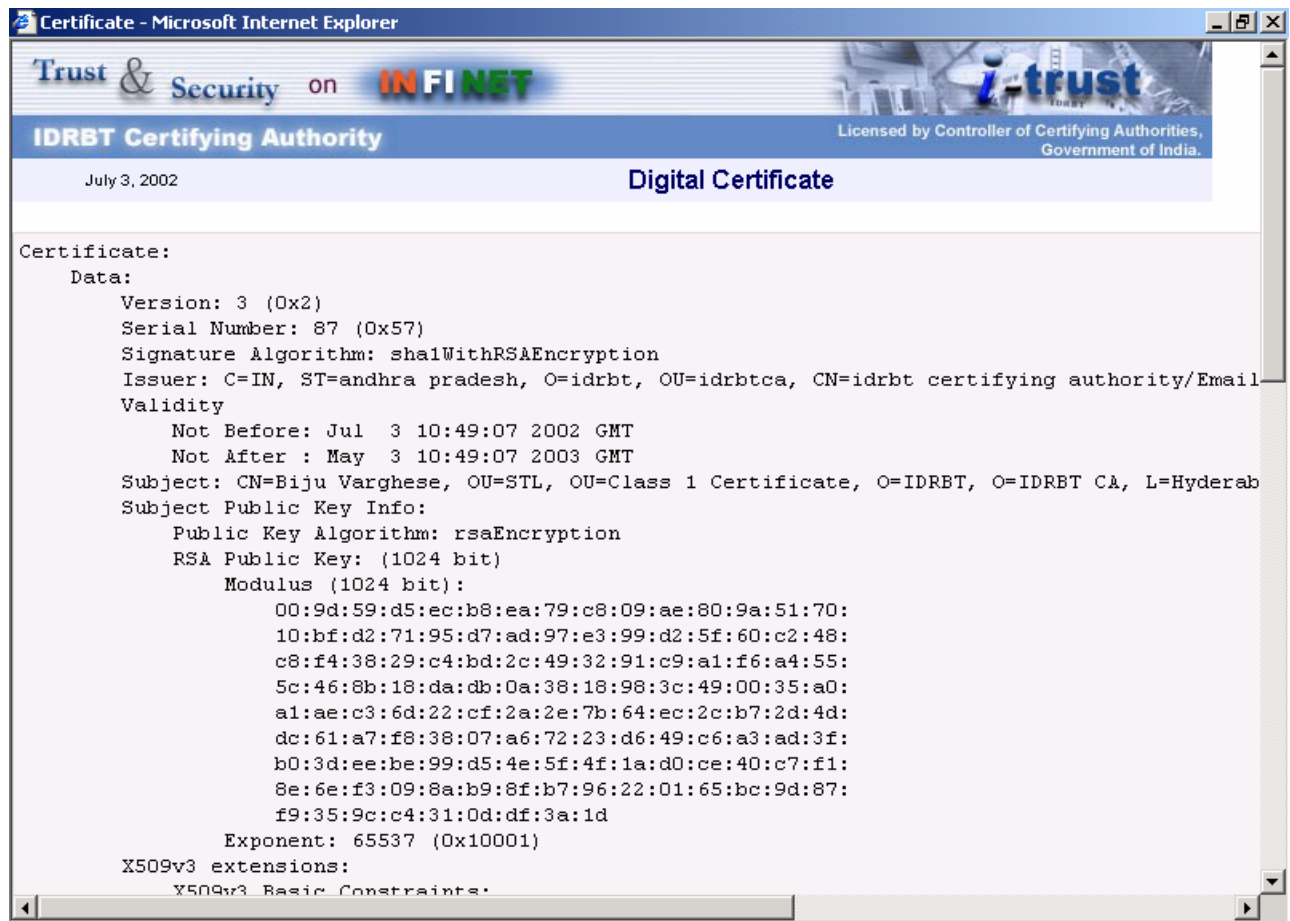
Click Here to view the generated certificate and download [69](#)

5. Click the request number to download the Digital Certificate.
6. You will be prompted for accepting or rejecting the Certificate issued.

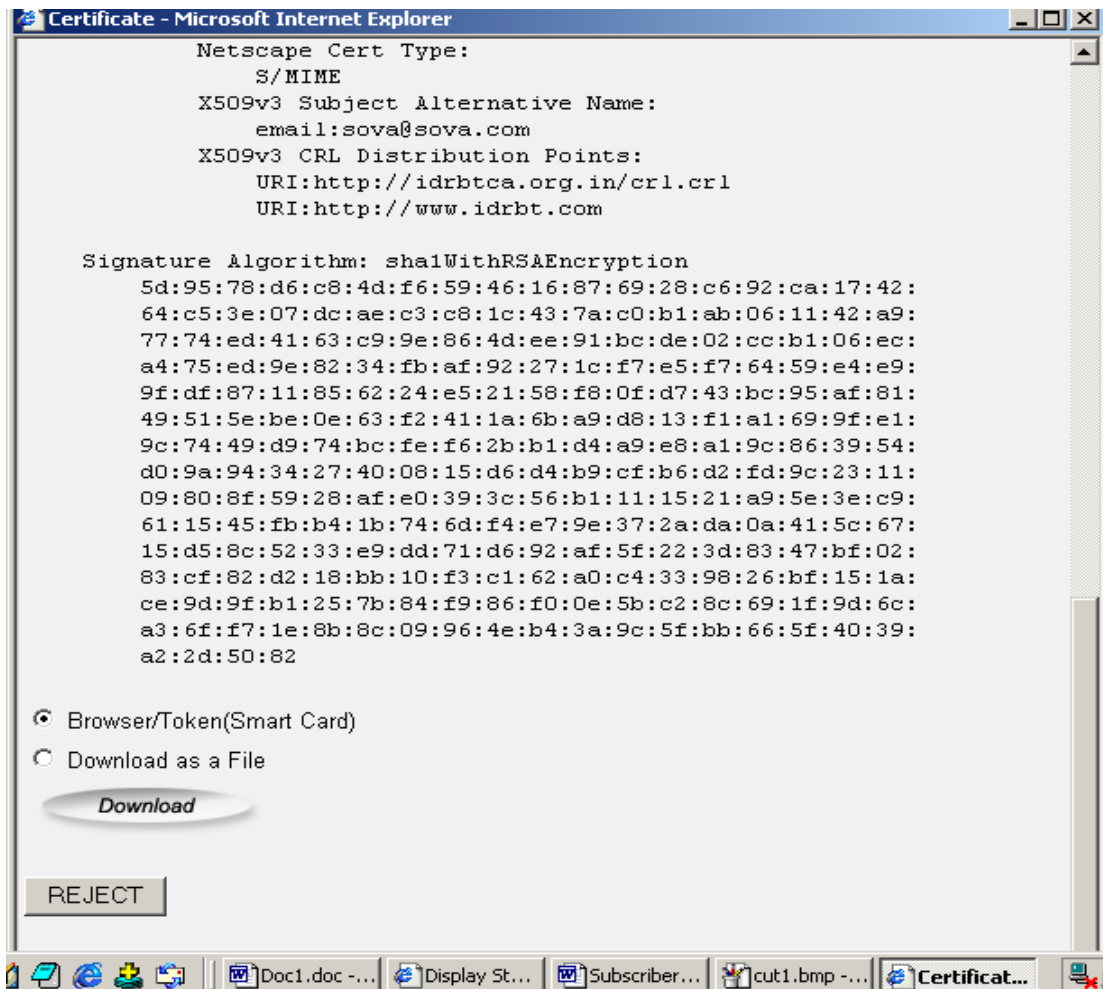


7. Click the I AGREE button.

8. The Certificate details will be shown to you.



9. You can download the Certificate into the browser or to a file depending on whether that request is browser generated or a PKCS#10 request.



10. You can also reject the certificate in case if the details are incorrect. In that case, intimate your Registration Authority as per Subscriber obligation. You must give the reason for rejection and Click the Submit button.



CERTIFICATE REJECTED - Microsoft Internet Explorer

Trust & Security on INFINET

IDRBT Certifying Authority

July 3, 2002

Certificate Rejection

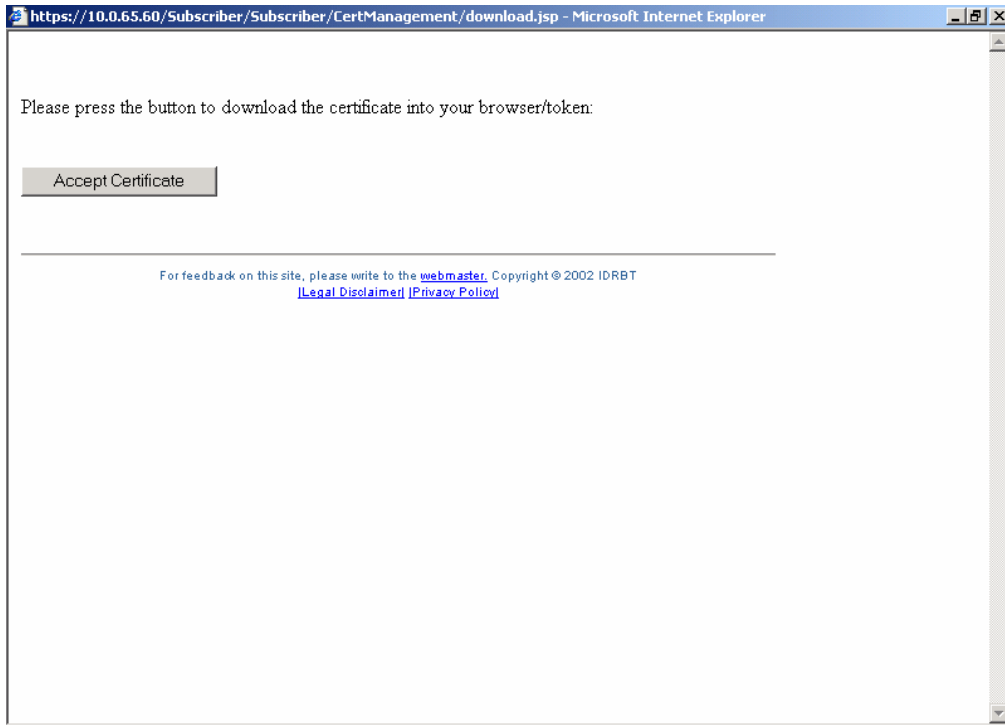
REASON FOR REJECTING CERTIFICATE

The details in the certificate are wrong.

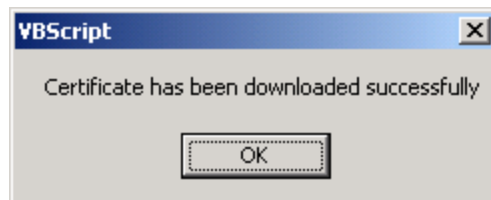
SUBMIT

For feedback on this site, please write to the [webmaster](#). Copyright © 2002 IDRBT
[Legal Disclaimer](#) [Privacy Policy](#)

11. If you have accepted the certificate, Click the Download button. It will prompt for Accepting the Certificate.



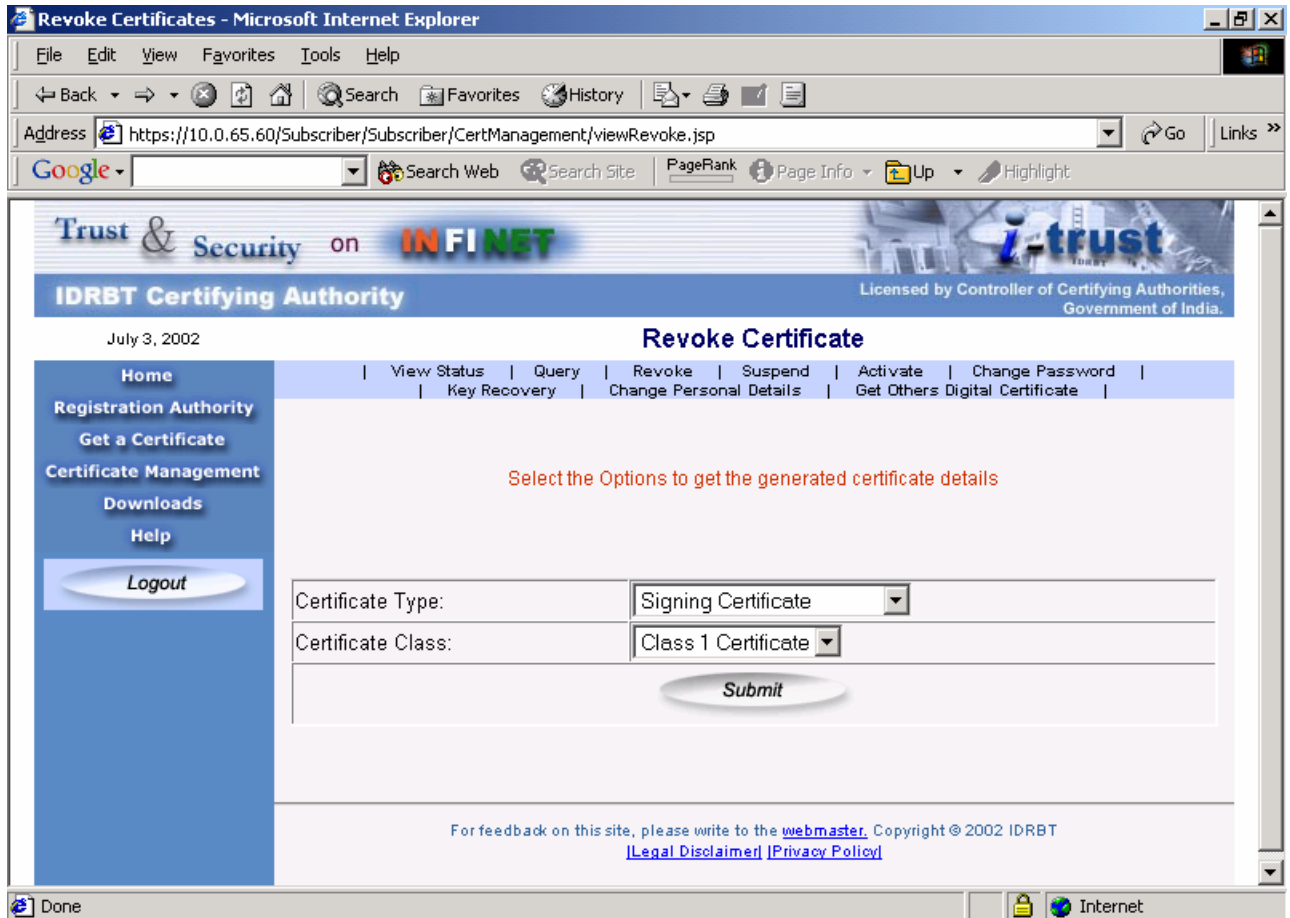
12. The message stating the successful download of the certificate will popup.



13. Close the dialog box.

Revoking the Digital Certificate

1. Click the "Certificate Management" link on the homepage. Select the Registration Authority and login using your User ID and Password.
2. Click the Revoke item in the top menu.
3. Select the type of Certificate and Class of certificate and click submit.



Revoke Certificates - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print

Address <https://10.0.65.60/Subscriber/Subscriber/CertManagement/viewRevoke.jsp> Go Links >>

Google Search Web Search Site PageRank Page Info Up Highlight

Trust & Security on **INFINET** **i-trust**

IDRBT Certifying Authority Licensed by Controller of Certifying Authorities, Government of India.

July 3, 2002 **Revoke Certificate**

Home | View Status | Query | Revoke | Suspend | Activate | Change Password |
Key Recovery | Change Personal Details | Get Others Digital Certificate |

Registration Authority
Get a Certificate
Certificate Management
Downloads
Help
Logout

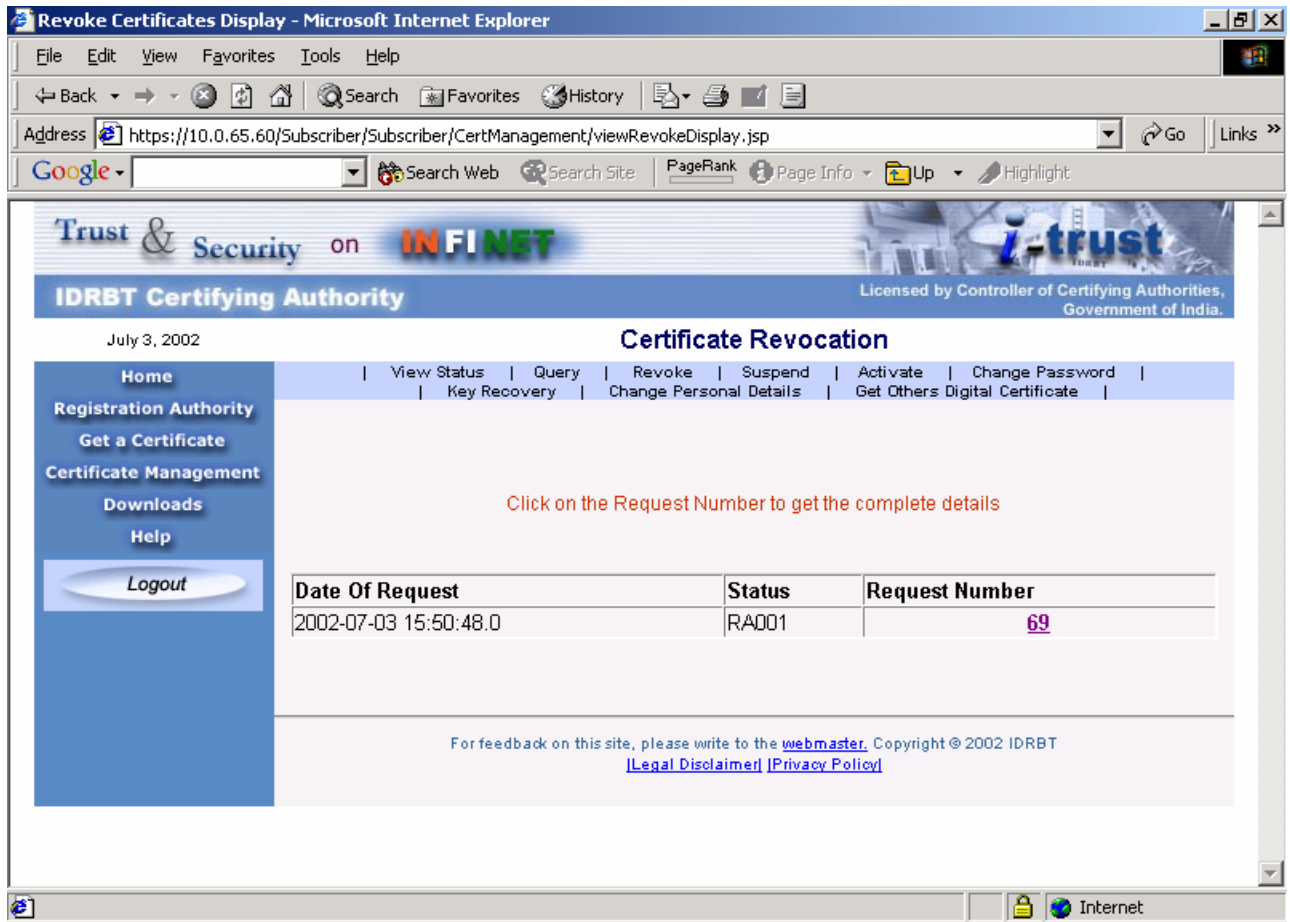
Select the Options to get the generated certificate details

Certificate Type: Signing Certificate
Certificate Class: Class 1 Certificate
Submit

For feedback on this site, please write to the [webmaster](#). Copyright © 2002 IDRBT
[Legal Disclaimer](#) | [Privacy Policy](#)

Done Internet

4. Click the certificate number for which you want to revoke.



Trust & Security on **INFINET**

IDRBT Certifying Authority Licensed by Controller of Certifying Authorities, Government of India.

July 3, 2002

Certificate Revocation

Home | View Status | Query | Revoke | Suspend | Activate | Change Password |
Registration Authority | Key Recovery | Change Personal Details | Get Others Digital Certificate |

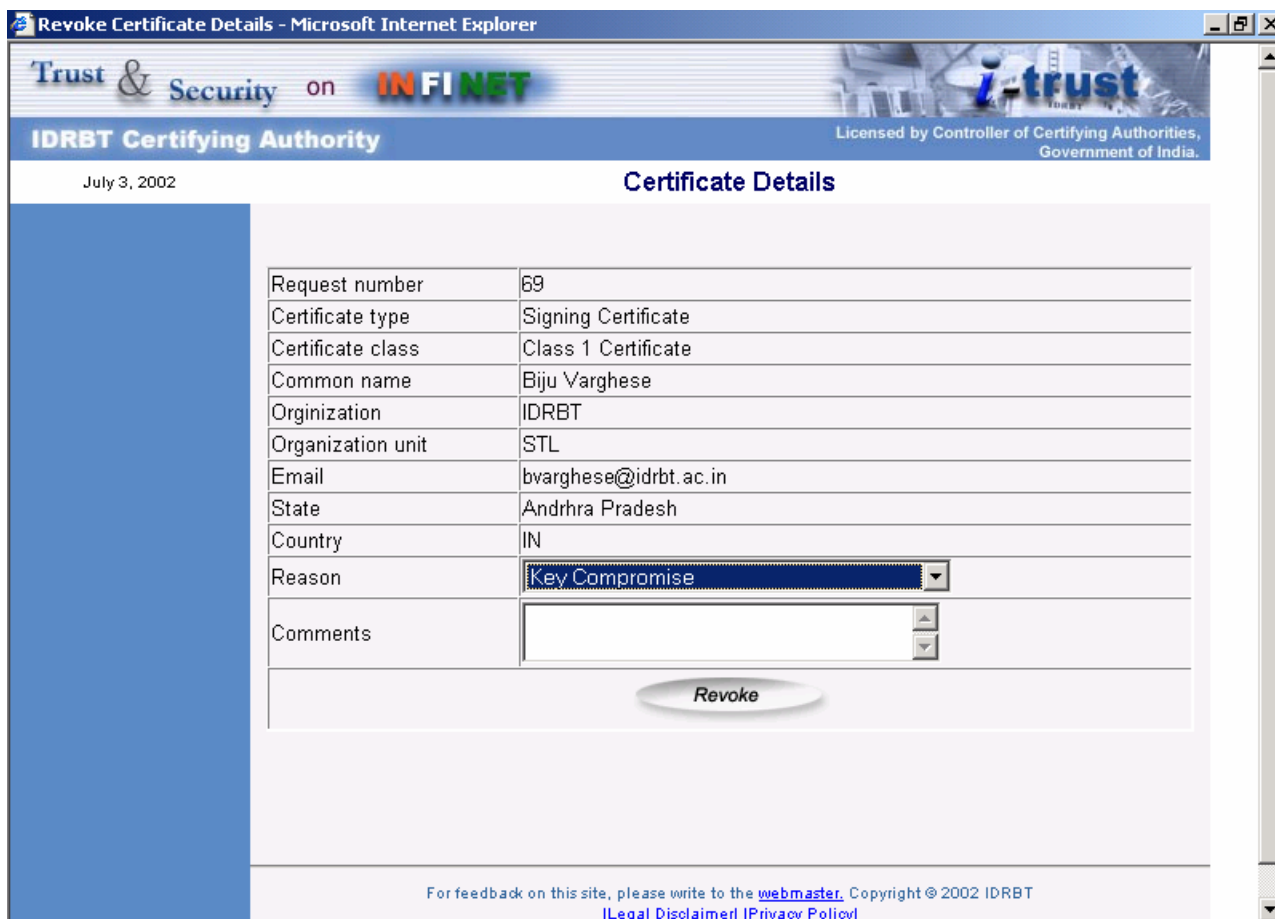
Get a Certificate
Certificate Management
Downloads
Help
Logout

Click on the Request Number to get the complete details

Date Of Request	Status	Request Number
2002-07-03 15:50:48.0	RA001	69

For feedback on this site, please write to the [webmaster](#). Copyright © 2002 IDRBT
[Legal Disclaimer](#) [Privacy Policy](#)

5. Select the revocation reason and click revoke button.



Trust & Security on **INFINET**

IDRBT Certifying Authority Licensed by Controller of Certifying Authorities, Government of India.

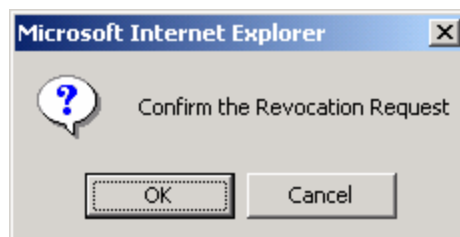
July 3, 2002 **Certificate Details**

Request number	69
Certificate type	Signing Certificate
Certificate class	Class 1 Certificate
Common name	Biju Varghese
Organization	IDRBT
Organization unit	STL
Email	bvarghese@idrbt.ac.in
State	Andhra Pradesh
Country	IN
Reason	Key Compromise
Comments	<input type="text"/>

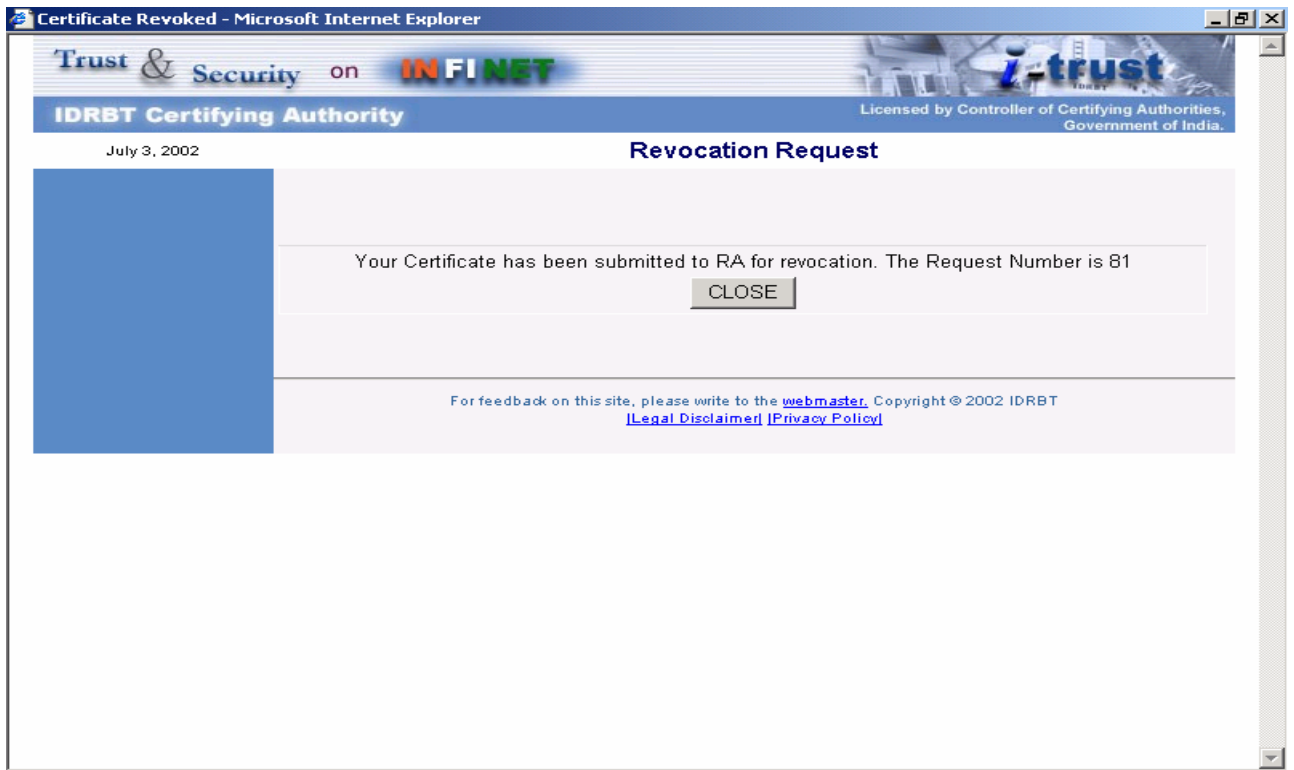
Revoke

For feedback on this site, please write to the [webmaster](#), Copyright © 2002 IDRBT
[\[Legal Disclaimer\]](#) [\[Privacy Policy\]](#)

6. Confirm the revocation request.



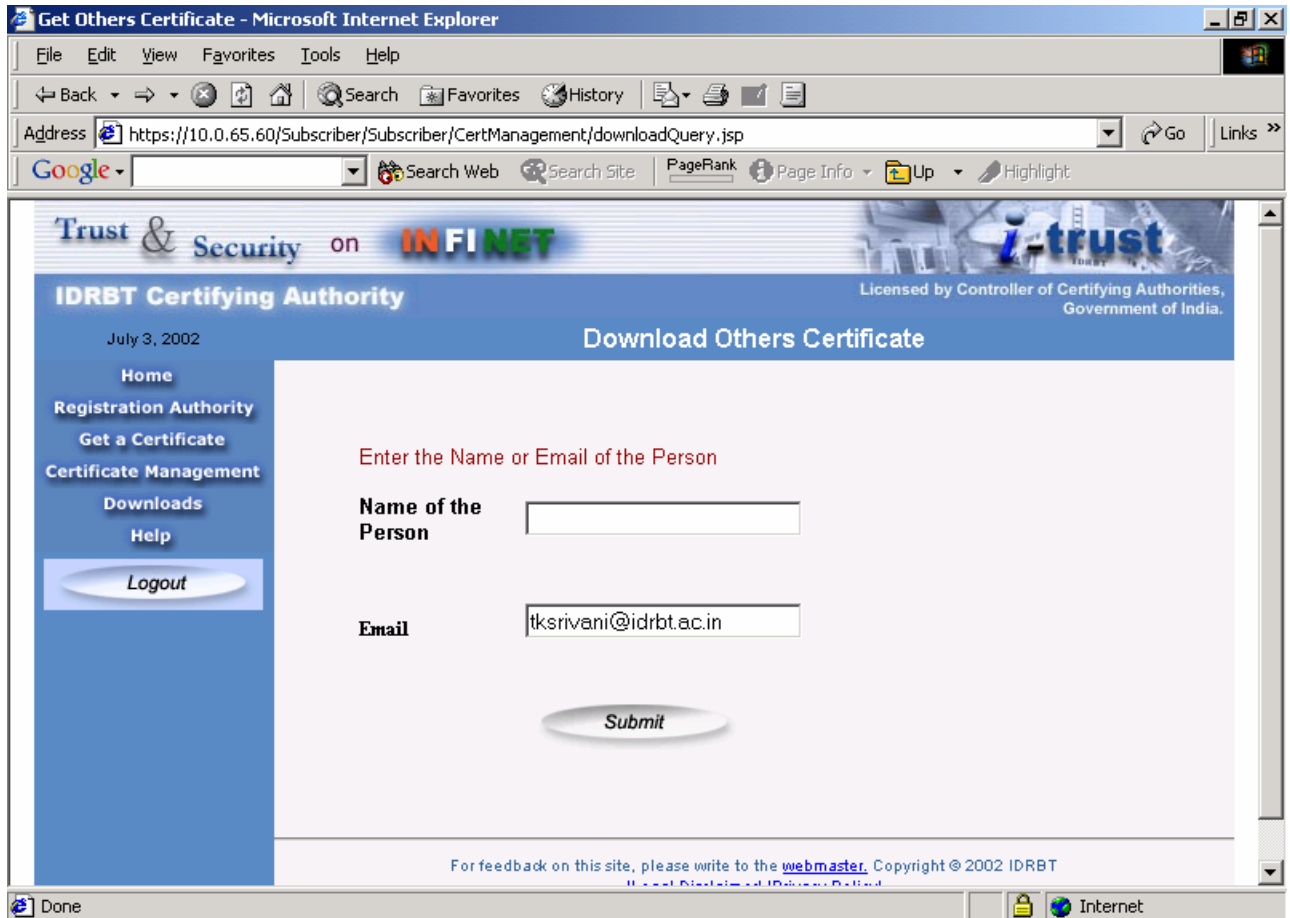
7. You will be informed about the status.



8. Click Close button and Logout from the system.

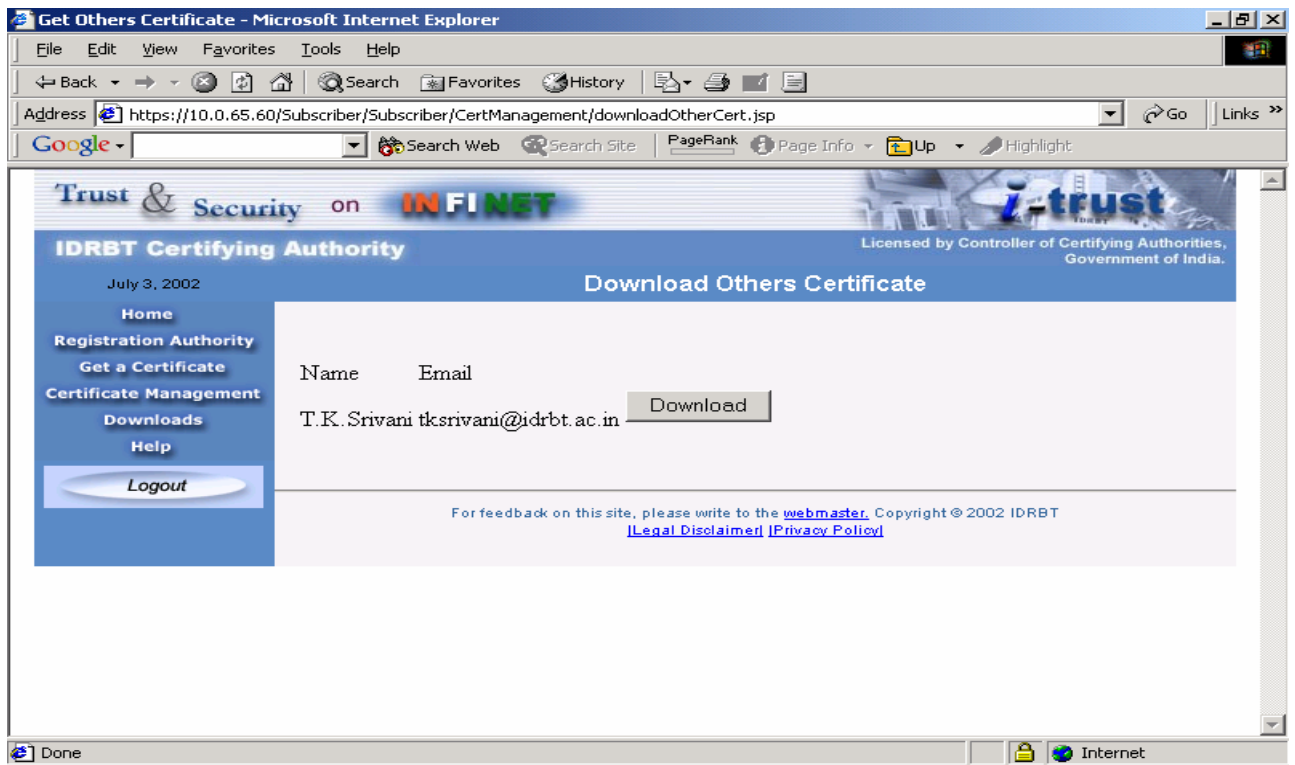
Getting other's Digital Certificate

1. Click the "Certificate Management" link on the homepage. Select the Registration Authority and login using your User ID and Password.
2. Click the Get other's Certificate item in the top menu.
3. You can give the name of the Person or the email address and click submit.



The screenshot shows a Microsoft Internet Explorer window titled "Get Others Certificate - Microsoft Internet Explorer". The address bar displays the URL: <https://10.0.65.60/Subscriber/Subscriber/CertManagement/downloadQuery.jsp>. The page content includes a header with "Trust & Security on INFINET" and "i-trust". Below this, it says "IDRBT Certifying Authority" and "Licensed by Controller of Certifying Authorities, Government of India." The main heading is "Download Others Certificate". On the left, there is a navigation menu with links: Home, Registration Authority, Get a Certificate, Certificate Management, Downloads, Help, and a Logout button. The main content area has a red prompt "Enter the Name or Email of the Person". Below this, there are two input fields: "Name of the Person" and "Email". The "Email" field contains the text "tksrivani@idrbt.ac.in". A "Submit" button is located below the input fields. At the bottom of the page, there is a footer that reads: "For feedback on this site, please write to the [webmaster](#). Copyright © 2002 IDRBT".

4. You can download the Certificate by clicking the Download Button.



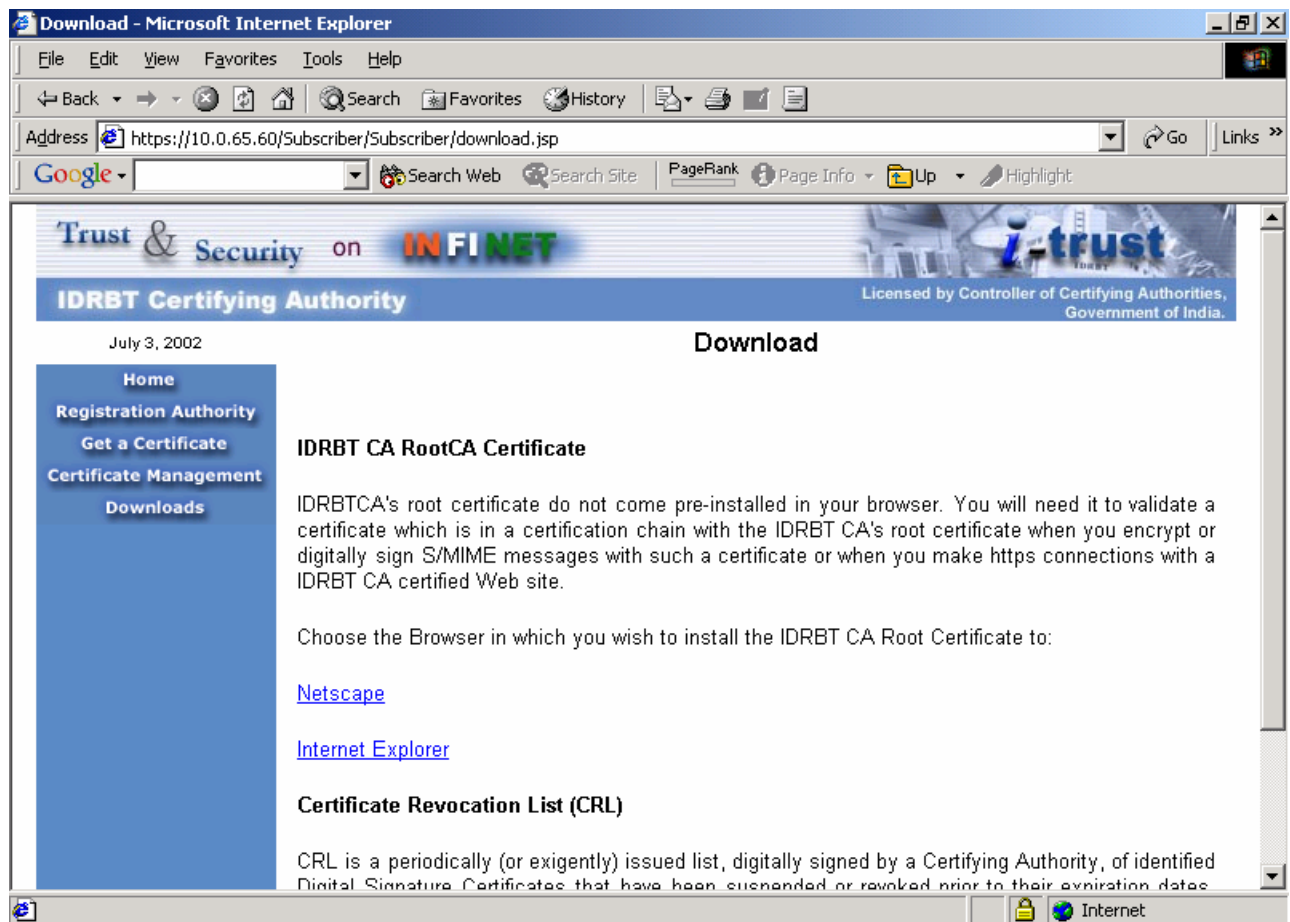
5. Logout of the system.

2.5. Suspending the Digital Certificate

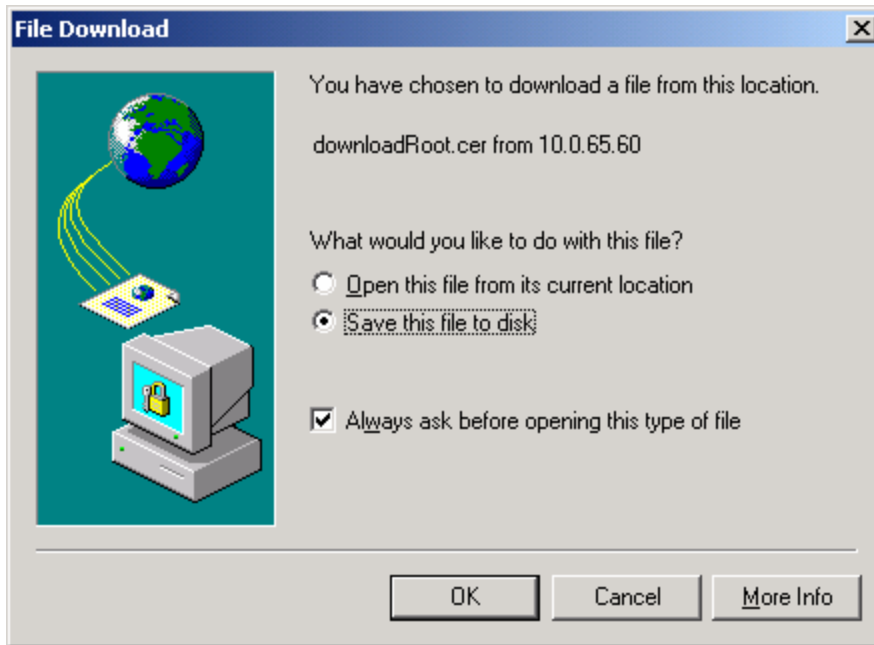
1. Click the “Certificate Management” link on the homepage. Select the Registration Authority and login using your User ID and Password.
2. Click the Suspend item in the top menu.
3. Proceed the same way as mentioned in the Revocation process.

2.6. Downloading the IDRBT CA Root Certificate

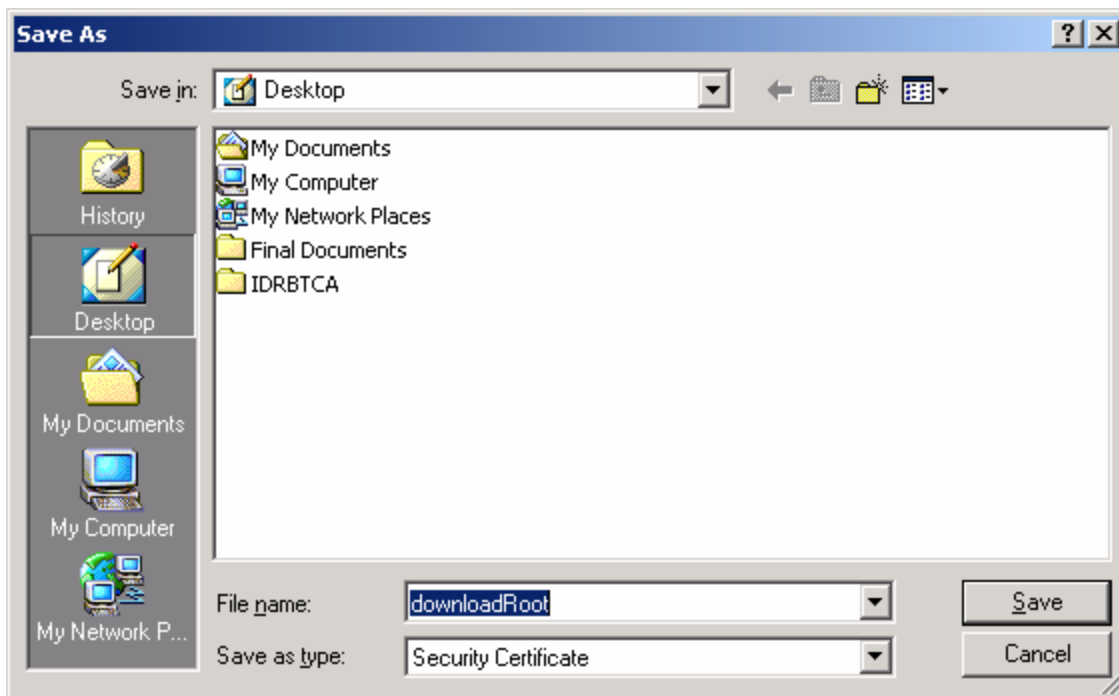
1. Click the “Download” link on the homepage.
2. Click the link suitable for your browser.



3. In case of Internet Explorer, it will prompt the following message.



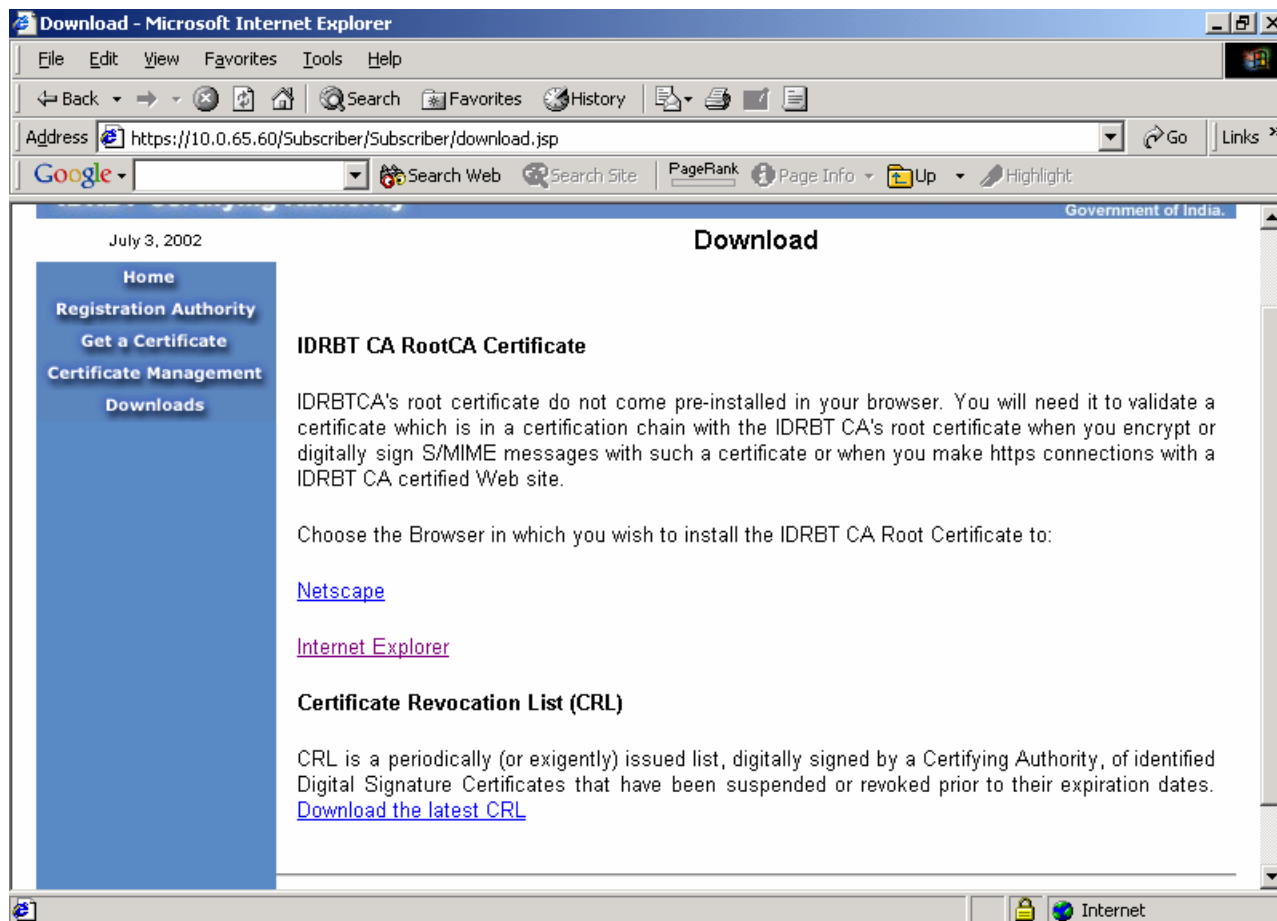
4. Click OK to save the Certificate file.
5. Select the path to which the certificate is stored.



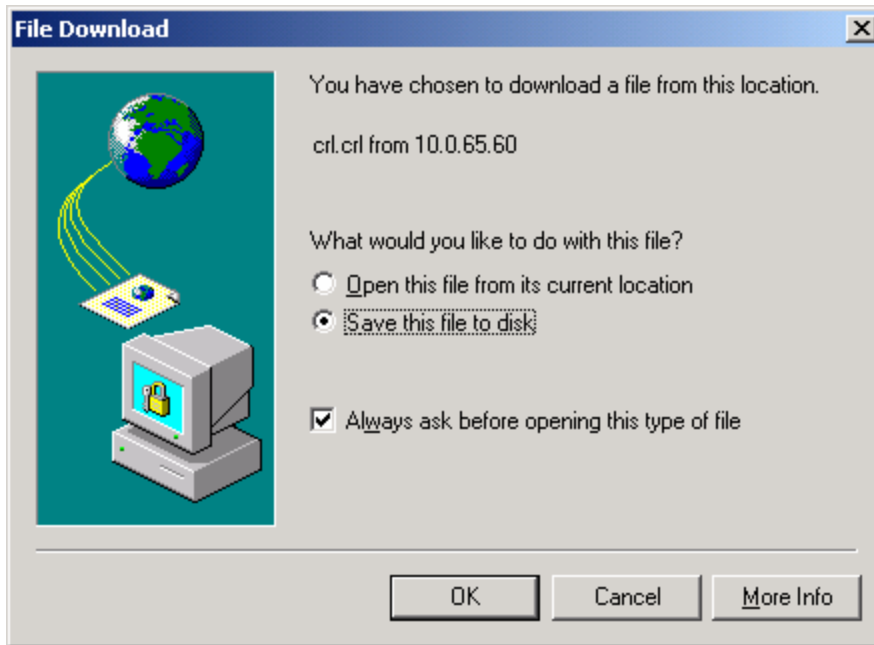
6. Click Save to save the certificate.

2.7. Downloading the IDRBT CA CRL

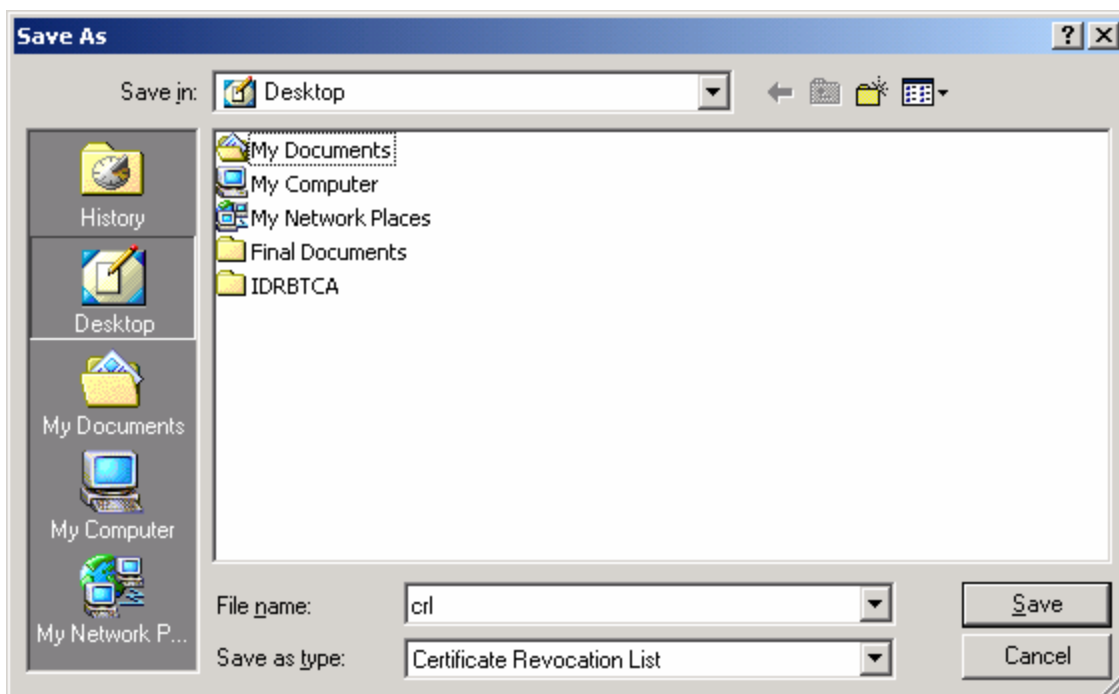
1. Click the “Download” link on the homepage.
2. Click the Download latest CRL link.



3. In case of Internet Explorer, it will prompt the following message.



4. Click OK to save the Certificate file.
5. Select the path to which the certificate is stored.



6. Click OK to save the CRL file.

For more details contact:

caservice@idrbt.ac.in

Visit us on: <http://www.idrbt.com/> on Internet

<http://idrbtca.org.in/> or <http://infinet.org.in/> on INFINET