Digital Certificate Manager
A Sample Application using CSSM

December 1996

Subject to Change Without Notice

Specification Disclaimer and Limited Use License

This specification is for release version 1.0, updated December 1996.

THIS SPECIFICATION IS PROVIDED “AS IS” WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

Some aspects of this Specification may be covered under various United States or foreign patents. No license, express or implied, by estoppel or otherwise, to any other intellectual property rights is granted herein.

Intel disclaims all liability, including liability for infringement of any proprietary rights, relating to implementation of information in this specification. Intel doesn't warrant or represent that such implementation(s) will not infringe such rights.

If you are interested in receiving an appropriate license to Intel's intellectual property rights relating to the interface defined in this specification, contact us for details at cdsa@ibeam.intel.com.

Intel Corporation, 5200 N.E. Elam Young Parkway, Hillsboro, OR 97124-6497

Table of Contents

List of Figures

1. What is a Digital Certificate?

The Digital Certificate Manager (DCM) is a sample application that creates and displays digital certificates. Digital certificates are the electronic embodiment of trust between two or more parties. Certificates don't create any new trust models or relationships. They are the digital form of real-world trust. They are an unforgeable credential in cyberspace.

Consider an example application, elections by electronic ballot. To cast a ballot electronically, each voter must present their voter registration certificate. The certificate represents trust between the voter and the government. The government trusts that the certificate bearer is a qualified voter. The voter trusts the government to tally their vote and to maintain the privacy of their ballot.

Applications interpret and manipulate certificates based on policies representing application-specific trust models. Certificates can be used to:

- Establish the identity of the bearer.
- Authorize a set of actions the bearer may perform.

1.1 Certificate Authority

A certificate is issued by a Certificate Authority (CA), which is an institution, organization, or individual. The purpose, meaning, and value of the certificate is derived from the CA and the policies underwriting the trust model of that CA. The CA can also act as an agent for other institutions, representing their policies.

Individuals use separate certificates for different trust relationships and different applications. Voter registration certificates are issued by state and local governments. Similarly, credit card companies issue certificates to their subscribers. The credit company writes a policy statement representing the trust/agreement between the company and a given subscriber. Policies can be subscriber-specific. If the subscriber agrees with the policy statement, then a digital certificate is issued to the subscriber. The certificate allows the owner to carry out financial transactions electronically.

Mechanistically, a digital certificate contains a binding of the bearer's identification to a public key that can be used in cryptographic operations. The binding is made immutable when the issuing CA digitally signs the certificate. The digital signing process uses cryptographic algorithms for hashing and signaturing. The resulting signature is included in the certificate.

Users present one or more certificates to electronically initiate a transaction. Upon receiving a certificate, the recipient verifies that certificate. The verification process provides

- Tamper detection for the contents of the certificate.
- Accurate identification of the bearer.
- Establishes the level of trust between the communicating parties.

1.2 Certificate Chains

A certificate can be a compound credential consisting of a set of related certificates. The simplest relationship is an ordered, linear sequence of certificates corresponding to an authority hierarchy. This hierarchy defines the policy for issuing and managing subsequent certificates in the hierarchy. For example, an employee certificate can be a chain of three certificates: a terminal certificate unique to the employee, the certificate for the regional corporate office, and the certificate for the corporation. Each

certificate in the chain serves a purpose. The policy statement associated with the corporate certificate can define the corporate check writing level of the employee. The regional office certificate can define the employee's travel budget. The employee's certificate can define local site, computer room access for the employee.

Not all trust models are hierarchical. The Pretty Good Privacy* (PGP) model for secure electronic mail services is based on the introducer trust model. In PGP, trust is established by a certificate you know introducing you to a certificate you don't know. When first introduced to a new certificate, you can ascribe little if any trust to the certificate. Each time that certificate is introduced to you by another known certificate, you can increase the level of trust you assign to it.

1.3 Digital Certificate Manager

The Digital Certificate Manager is a sample application that displays existing certificates, displays relationships among certificates, and issues new certificates. The certificates managed by DCM are stored in one or more certificate databases. DCM accesses security services through the Common Security Services Manager (CSSM) API. Services for manipulating certificates in memory and in data stores are provided by Intel's add-in security service modules. DCM allows any user who owns a public-private key pair to issue sample certificates on their system.

2. Using the Software

To run the software, double-click IDCM.EXE from the Windows Explorer*. The application window should appear similar to the display below.

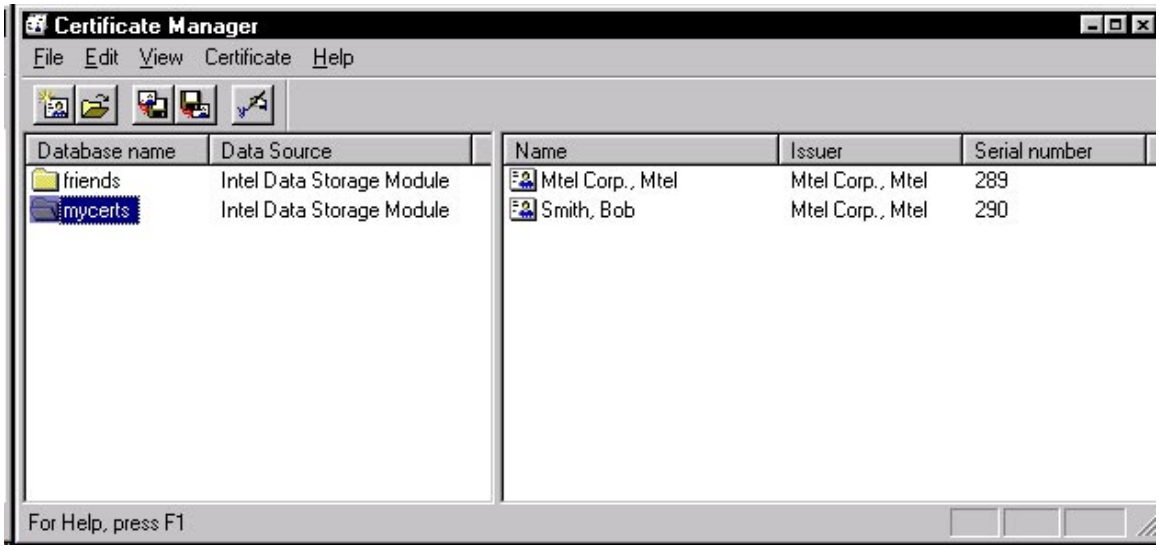

Figure 1. Digital Certificate Manager application window.

2.1 The Window Panes

The main window is divided into two panes displaying:

- Certificate database names
- Certificates names from a selected database

The left pane lists the names of all of the certificate databases stored on your local system. A demonstration database named MYCERTS was downloaded and installed with this software. The database was created at the Intel Architecture Lab, using the DCM application.

When a certificate database is selected in the left pane, the right pane lists the certificate name from each certificate in the selected database. A certificate name has two parts: a subject name and an issuer name. The subject name is the name of the certificate owner. The issuer name is the name of the person, organization, or institution that created/issued the certificate to the subject. Each certificate name is prefaced with an icon indicating whether or not the private key associated with the certificate resides on the local system. A small key-shaped emblem indicates that the private is locally held.

2.2 Viewing Digital Certificates

To view a certificate, double-click its name in the right pane, or select the certificate name and choose **Open** from the **Certificate** menu. A viewing window similar to the one shown below is displayed.

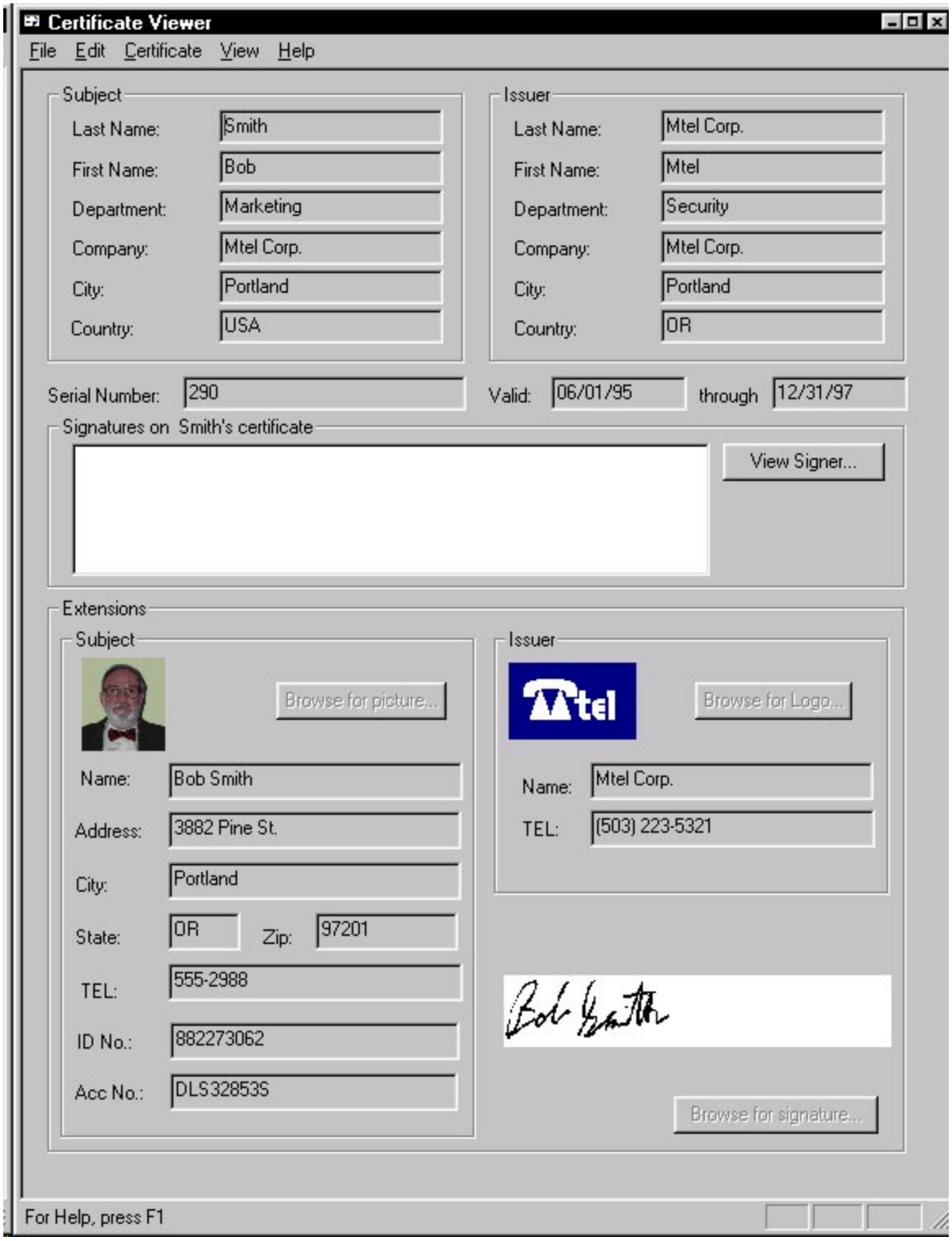

Figure 2. A certificate opened for viewing.

The standard certificate fields are displayed in the **Subject** pane, the **Issuer** pane, and the **Valid** pane. The **Extensions** pane displays optional certificate information such as a photo of the certificate owner and a logo of the certificate issuer.

The **Signatures** pane lists the name of each certificate that was used to digitally sign the certificate currently being viewed. Once a digital signature has been computed on a certificate, the contents of that certificate can not be modified. To view a signer's certificate, select a signature in the **Signatures** pane and click the **View signer. . .** button.

When you finish viewing a certificate, close the viewing window by choosing **Exit** in the **File** menu or click the X box in the upper right corner of the window.

2.3 Creating Digital Certificates

As a Certificate Authority, you can use the DCM application to issue certificates. To create a new certificate and add it to the certificate database, choose **New Certificate** in the **Certificate** menu. A certificate viewing window is displayed containing empty form fields. The window looks similar to the one shown below. Each form field is editable. To initialize field values for the certificate, select a form field and enter the value for that field.

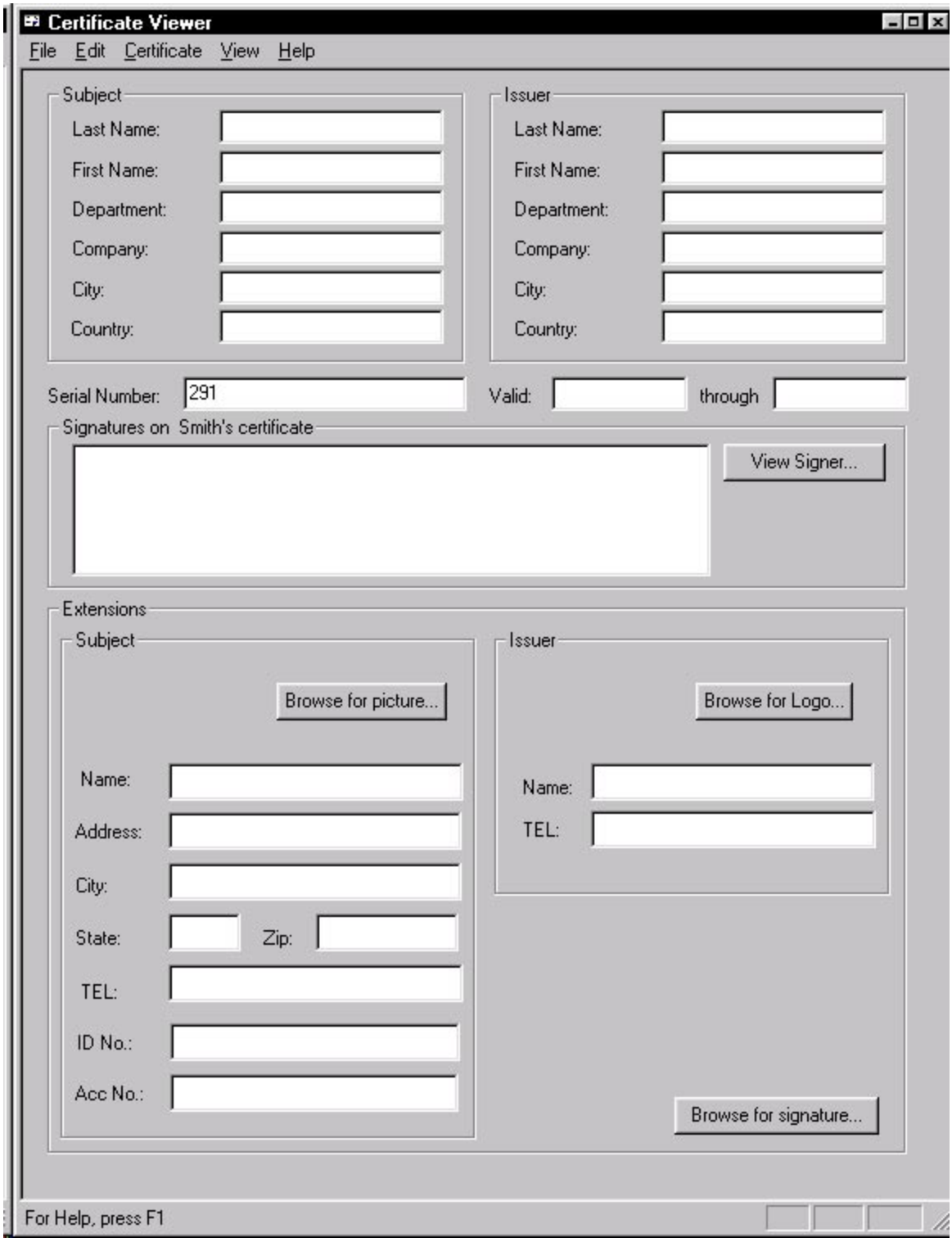

Figure 3. Editable form for creating a new certificate.

When you have initialized all the fields, you must generate a public and private key pair for the new certificate. Choose **Generate key pair** in the **Certificate** menu. Key-pair generation requires two input values from you to complete the process:

- A secret passphrase to be associated with the new key pair. Enter the passphrase in the dialogue box when requested.
- A random sequence of keyboard inputs to be used as a random value in the computation of a key pair. Enter an arbitrary length sequence of random keystrokes in the dialogue box when requested.

The public key portion of the public-private key pair is added as a certificate field value, but it is not displayed in the viewer window.

To complete the certificate creation process, you must digitally sign the new certificate. Once the certificate has been signed the field values stored in the certificate can not be modified. Before signing the certificate, review the values you have entered and make all necessary corrections.

To sign the certificate, choose **Sign** in the **Certificate** menu. A dialogue box is displayed similar to the one shown below.

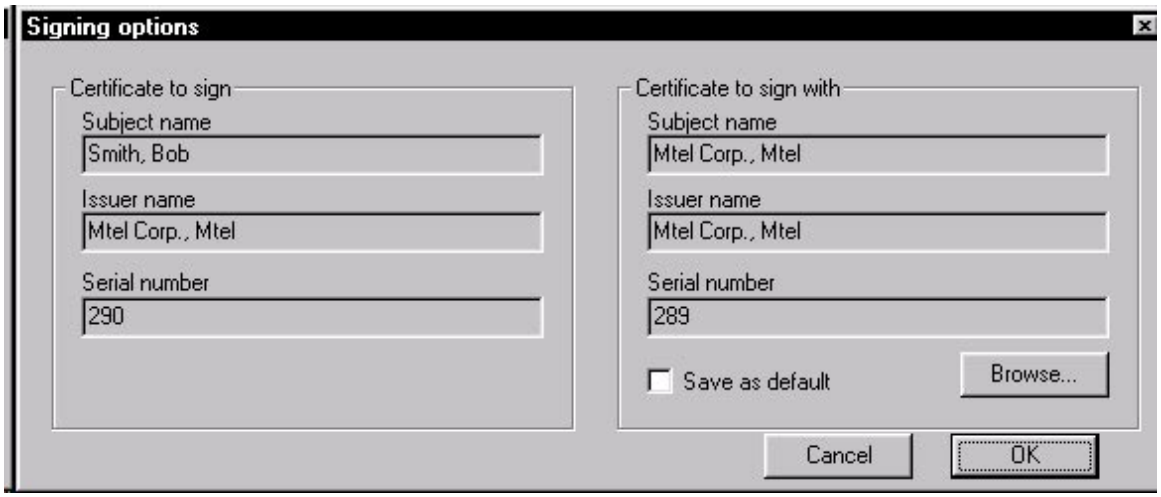

Figure 4. Dialogue box for signing a new certificate.

The dialogue box contains two panes:

- **Subject** pane – gives the subject name contained in the new certificate being created. This value is already initialized with the value you entered for the subject name in the main certificate forms display.
- **Signer** pane – a display to hold the subject name contained in another certificate. The other certificate will be used to sign the new certificate. You can't edit the signer fields directly. To select an existing certificate for signing the new certificate, click the **Browse** button. A dialogue box is displayed. In the left pane, select a certificate database. In response, the system displays the subject name and issuer name from each certificate stored in that database. Select the

certificate representing the entity that should sign the new certificate. The private key associated with the selected certificate must reside on the local machine to complete the digital signing process. Click **OK** to use the selected certificate for signing the new certificate. The signer pane should now be initialized.

Click **OK** to complete the signing process. Now that the certificate has been signed, the DCM application rejects all user efforts to modify any field value in the new certificate. The DCM application automatically adds the new certificate to the certificate database you selected at the beginning of this process.

2.4 Using Digital Certificates

Once a certificate has been signed, the certificate can be presented to an application as identification and authorization for performing some action. When the certificate is presented, the application evaluates trust in the certificate by verifying the signature contained in the certificate.