

Amaranth Networks Inc.

Amaranth Networks Inc.
324 Still River Road
Bolton, MA 01740
<http://www.amaranth.com/>

Phone 978 779 6813
FAX 978 779 6652
Email dts@amaranth.com

CATooltm Product Description

Simplifying Certificate Management for
Enterprises and Network Providers

CATool™ Product Description

Overview

Digital certificates are a mechanism to convey digital identity, and are used to authenticate identity. Certificate Authorities issue certificates in a Public Key Infrastructure or PKI, using public/private key pairs for authenticating identity and for encryption.

Certificate Authorities (CAs) provide a self-signed certificate referred to as a root certificate. Users deal mostly with identity certificates, which are used to identify systems, hosts, or other names. The certificate authority is considered a trusted resource. Identity certificates signed by the CA will be trusted if the user trusts the CA itself. By indicating trust in the root certificate, all subordinate certificates are trusted.

For most applications, creation of these certificates generally takes one of three forms:

- 1) Certificates purchased from one of the public certificate authorities, such as Verisign or GeoTrust.
- 2) Certificates created using a private Certificate Authority.
- 3) Certificates created using simple tools, permitting “self signed” certificates.

Where CATool Fits

CATool is a private Certificate Authority tool. It permits enterprises or network providers to create and manage a Certificate Authority for their business. It provides user authentication, manages the workflow of the request and signing process, and provides for certificate delivery.

By automating the process via a web-based interface, CATool simplifies the job of managing certificates for Intranet or Extranet web servers, Virtual Private Networks, Wireless LAN access and other tasks.

catool Main Menu

Amaranth Networks Inc.
Certificate Authority

You are signed in as *dts*.

- View Directory of Certificates
- Install CA Cert into Browser
- View Pending Requests
- Submit a New Request
- Submit a CSR
- User Administration
- Change My Password
- Logout

\$Id: mainmenu.html,v 1.14 2002/12/22 21:22:18 chip Exp \$

How It Works: User Levels

CATool is intended to be used by several classes of users. Below is a description of the user experience for each of the user levels, ranging from the administrator of the product, to the user of the certificates.

Administrator

The administrative user is responsible for administering the username and password registry maintained by the tool. Each user is permitted a number of possible privileges, which dictate what the user may do and what menu choices are presented. The levels are:

- 1) Admin: has authority to create, alter and delete user accounts.
- 2) Signer: has the ability to sign certificates using the Root Certificate.
- 3) Ordinary User: without the admin or signer privileges, users can submit requests, but then must wait for someone with signing authority to sign the certificates.

Providing these role capabilities provides the flexibility to manage certificates for a large or small organization.

Signer

A user with signing privilege is permitted to submit requests and to sign them. Certificates signed by such a user are signed with the Root Certificate created (or imported) during installation.

User

Users without signing or administrative privileges are permitted to submit requests for certificates. The tool accepts a web form that collects relevant information, but also will accept Certificate Signing Requests (CSRs) for situations where the use of a CSR is preferred.

Non User

Without logging in to CATool, the Root Certificate is available for import into a browser. This provides a way for staff of an organization to easily and simply import the root certificate, for example to provide trusted access to intranet or extranet web sites. For greater security, a user of CATool is able to download the certificate file, which facilitates installation or distribution by IT personnel.

Amaranth Networks Inc. Certificate Authority

catool: Directory of Certificates

	Serial	Subject	Status	Requester	Date Requested	Signer	Date Signed
View Download	1	catool.amaranth.net	valid	dts	2003-01-17 18:02:44	dts	2003-01-17 18:02:56
View Download	2	store.caribbeanwebcams.com	valid	dts	2003-01-17 18:37:55	dts	2003-01-17 18:38:13
View Download	3	vpn1.amaranth.net	valid	dts	2003-01-18 13:26:14	dts	2003-01-18 13:26:25
View Download	4	vpn1.amaranth.net	valid	dts	2003-01-18 22:58:03	dts	2003-01-18 22:58:11
View Download	5	mysql.rye.amaranth.net	valid	dts	2003-01-29 12:49:57	dts	2003-01-29 12:50:06
View Download	6	netsaint.amaranth.net	valid	dts	2003-01-29 12:57:52	dts	2003-01-29 12:57:57

[View](#) [Download](#) *Amaranth Networks Inc. Certificate Authority*

select download format: auto PEM DER

[Return to Main Menu](#)

Amaranth Networks Inc. Certificate Authority

catool: New Certificate Request

Required Information

Organization	<input type="text" value="Amaranth Networks Inc."/>	(required)
Department	<input type="text"/>	(optional)
City	<input type="text" value="Bolton"/>	(required)
State (full name)	<input type="text" value="Massachusetts"/>	(required)
Country (2 letter code)	<input type="text" value="US"/>	(required)
Name of Cert Holder (hostname, person name, etc.)	<input type="text"/>	(required)
Email Address of Cert Holder	<input type="text"/>	(required)
Certificate Type	<input checked="" type="radio"/> Standard <input type="radio"/> EAP-TLS Client <input type="radio"/> EAP-TLS Server	
Optional Comments to Signer	<input type="text"/>	

Advanced Settings

(Do not touch unless you know what you are doing!)

Key Size	<input type="text" value="1024"/>	bits
Key Encryption Passphrase	<input type="text"/>	
Repeat Passphrase	<input type="text"/>	
Requested Certificate Lifetime	<input type="text" value="365"/>	days
Trusted Uses	<input checked="" type="radio"/> Not Specified <input type="radio"/> SSL Server <input type="radio"/> SSL Client <input type="radio"/> S/MIME Email	

\$Id: new-request.html,v 1.12 2002/12/20 19:18:43 chip Exp \$

How It Works: Workflow

Installation

During installation the user specifies whether the tool is to generate its own root certificate or if one already exists. It is expected that most users will instruct CATool to construct its own root certificate.

Make a Request

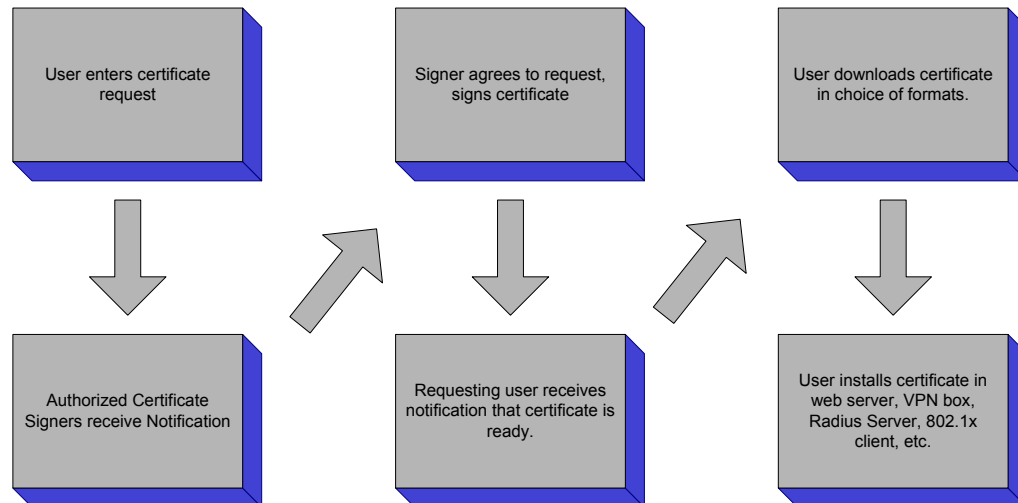
User logs in, generates a certificate request (or imports a CSR). User may download the private key at this point, if desired. An email message is generated to those with signing authority, alerting them to the presence of a new request in the queue.

Signing

A user with signing authority, upon reviewing outstanding requests, signs the request. The requesting user is sent an email indicating the certificate is available. The certificate can be downloaded in a variety of formats.

Use

Any user with the CA Root Certificate installed will be able to use the resultant certificate, once installed properly. For example, an Intranet web site set up with the private key and certificate generated may be accessed by anyone with the Root CA Cert installed, without any error messages or complaints from the browser.



Additional Features

Certificate Revocation Lists

Digital certificates are subject to revocation. When a certificate is revoked, information indicating that event is posted to a Certificate Revocation List (CRL). A periodic housekeeping process runs in the background and ensures the CRL is properly updated on a periodic basis.

802.1x Certificates

IEEE 802.1x specifies a port based access control mechanism. While 802.1x is not specific to media types it has gained popularity in the world of 802.11a/b networking.

Microsoft shipped Windows XP with an 802.1x client, and several vendors of access points provide complementary support.

CATool provides support for generating client and server certificates compatible with 802.1x.

Examples of Usage

Intranet and Extranet Web Servers, password authentication

Users of company internal or external, restricted web sites use web certificates generated by CATool to prove the validity of the web server to the client. User is prompted for username and password, which are conducted to the server via SSL/TLS, encryption based on the certificate.

Intranet and Extranet Web Servers, client authentication

Building on the previous case, the users could be authenticated by use of client certificates, installed on each user's computer. The web server could allow all users with certificates signed by the Root Certificate, or may maintain its own list of user certificates authorized to access that server.

Wireless Network Authentication

As noted above, 802.1x has been promoted as a method for securely identifying and separately encrypting network traffic for each user of a wireless LAN. CATool generates the certificates required for both client and server, permitting Microsoft XP-based workstations (and any other machines with 802.1x client support) to access corporate networks via a wireless access point.

Wired Network Authentication

While 802.1x is gaining popularity in wireless environments, support for the protocol has been incorporated into Ethernet switches from companies such as 3Com and Extreme Networks. Just as with the wireless case, this support can be used to authenticate users of a wired network.

Virtual Private Network

VPN systems work with pre-shared keys or certificates. The VPN administrator generates certificates with CATool for each user, and is able to keep track of them in the CATool database.

System Requirements

CATool requires a Linux server on which Perl, Apache, MySQL and OpenSSL are all installed. The product is written in Perl and as such can be ported to other operating systems and SQL database servers. Versions for other platforms will become available based on customer request.

For 802.1x support, a Radius server software package, such as Radiator™ from Open System Consultants is required.

Availability

CATool is available now and is licensed to companies based on the number of servers and the number of certificate authorities they plan to run. Contact Amaranth Networks for pricing details and licensing terms. Amaranth is open to OEM licensing opportunities where they make sense. Customization services are also available.

Amaranth Networks may be contacted via telephone, mail, email or web at the following addresses:

Amaranth Networks Inc.

324 Still River Road
Bolton, MA 01740
978 779 6813
978 779 6652 FAX
sales@amaranth.com
<http://www.amaranth.com/>