InCommon Certificate Service Survey

*Responses to open-ended questions/options*

**Question 14:** “What ideas do you have for improving support for the InCommon Certificate Service?”

* Having our customers being able to email support@comodo directly instead of going through central administrators (us)
* Better search engine for KB
* I really would like to have ONE support line. Either InC or Comodo. Not two.
* The cert-users list has been invaluable. We've been able to answer most questions or resolve most issues based on the experience of others on the list. Please continue to make it available.
* use SSO for authentication or automate/streamline password recovery
* None so far.
* I would like to see, and maybe there is already a way, to 1) not have expired certs in default views in the CSM and 2) to not send expiry warnings for certs that were already renewed.
* Need a faster process for EV certificates to be approved.
* Nothing.
* Updated web docs, which are more (google) searchable would be nice. PDF form is good, but is less usable from a web-only perspective.
* Create a FAQ of resolved requests (deidentified) internal to InCommon institutions.
* InCommon should provide tier-1 support for the InCommon Cert Service, not Comodo, since our subscriber agreement is with InCommon, and InCommon best understands our needs.
* provide access to roadmap/timeline and feature/bug tracking information to cert-users list
* I've always had an excellent support experience. No needed changes spring to mind.
* Comodo always ends up solving the issue but there tends to be more follow-up required on our end then is desired to get a solution.
* A true FAQ, based on the repeat (frequently asked) questions on the cert-users list.
* Comodo support is fantastic. I am so, SO impressed. They are always extremely helpful and insightful. I appreciate everything they do.
* Nothing
* Excellent service overall - this program has been quite successful for us, and has been well-received. Streamline the EV request process - make it consistent. Comodo often contacts our contract signer instead of the RAO who requested the certificate, and that causes unnecessary delays in EV issuance.
* I hate to say this, but the certificate authorization people have been uniformly grumpy when I've talked with them on the phone. Very curt in their speech. I've also been told that automatic cert installation isn't supported for .edu customers, which is odd.

**Question 18:** “Are there other new features you would like to see added to the InCommon Certificate Service?”

* See Question 8's high priority items
* Would like to see an easier way to handle EV requests, issuing personal certs, and better account protections.
* Ability for RAO to select/deselect certificates that a DRAO can manage.
* We're not expert users at it yet.
* Multi-factor authentication on the console is of extremely high importance to us.
* The ones we would like to see were captured in a previous question.
* Shibboleth/SAML SSO
* I believe the feature request question lists all that I would like.
* easy integration with F5, other management software, puppet, etc
* For "Subject Alternative Names" allow one name per line rather than requiring comma separated on a single line
* The ability for an end user to reset their own password somehow.
* I'd love to have the ability to sort the certs list by recent activity. To make it easier to find actionable items.
* AD integration would be amazing. As would SSO federation.
* API improvements: need ability to approve requests, exclude Street and PostalCode, and specify external requester.
* Ability to silence expiration e-mail notifications
* Federated authentication for DRAOs/RAOs and clients. Keep expanding the API capabilities. Better documentation about API capabilities, as opposed to primarily what the calls are.
* Being able to change the requestor on a certificate after it has been issued so expiration notifications can be sent to an appropriate contact after employee turnover.
* Ability to hide/delete/cleanup old/unused/test SSL certs from Interface (without having to filter to find what I am looking for)
* We have a hard time with revoking certs that are no longer needed when a new cert is issued. Be nice to have a separate screen list a specific cert being approved in order to go back to the person and ask if any past approved cert needs revoked.
* Again, that question already answered on feature enhancement.
* Ability to have a wildcard cert with SANs. Currently can have a SAN cert with a wildcard as a SAN, but some applications require the wildcard to be the primary name.
* It would be nice not to have to change passwords so frequently. Maybe we could optionally use client-side certs for authentication? Also, certificate manager site does not work in Chrome for me. I have to use Firefox.
* API, so certs can be requested and retrieved using Powershell.
* We would like to issue individuals separate client certs. One for encryption and one for signing rather than having to use a dual use cert.
* Ability to see info about our draos through the Api. It's currently very hard to audit.
* You have already identified them. :)
* More fields available in API. Better responsiveness with API - sometimes it takes several \*minutes\* for the API call for an enrollment to respond, which causes issues with timeouts.
* Better automation for certificate installation. REST API.

**Question 19:** “Do you have any other ideas for how InCommon can improve the Certificate Service, engagement with the community, communications, etc.”

* Perhaps capture the experiences of current users of the service to make others aware of its benefits. The service has been well received at our institution. We have been fortunate to be able to fund it centrally and make it available at no charge to our community and have a much wider adoption rate for SSL.
* None at this time although whenever something comes to mind InCommon will be notified of the suggestion.
* When there are issues that are brought up, that impact the issuing of certificates, the email list should not be the place I have to look to see if the service is operating. An email should go out to all users of the interface that there is currently an issue and another when it is resolved. I do not believe this is occurring currently.
* have some webinars
* E-mail notification is adequate for outages and related issues. However, a general status page that always has the current information rather than having to wind through my e-mails to try to find any relevant messages would be very helpful.
* Communication relating to the retirement of private/internal names could have been more frequent.
* provide access to roadmap/timeline and feature/bug tracking information to cert-users list. this survey was good idea also!
* Communication about changes to the CM interface, even small changes.
* I have learned everything I've needed to know to administer the system at our institution from the Admin Guide and the mailing list. These are great resources. One thing that might help the admin guide is a common tasks section - i.e. when I first started using the system knowing the difference between a "Replace", a "add", and a "Renew" when requesting an SSL certificate was a bit confusing. Make perfect sense once you have done it a time or two but just something to get new folks onboard quicker. Thanks for the great service!
* I think you guys are doing a fantastic job. I'm currently not a RAO but I work closely with all of ours.
* Thanks for all the work InCommon does to provide this service!
* Decrease cost
* It seems like we often learn that there are issues with the Certificate Service's availability from our peers (via the mailing list), rather than directly from InCommon. It would be nice if you could be more proactive about notifying your subscribers when there are known issues with the site (availability, performance, etc.). And then be better about notifying us when things are back to normal, as well as what caused the problem and how it was resolved. And what's being done to prevent it from happening again. Sometimes it seems like your clients have to nudge you to get this information when there are problems.

**Question 24:** “Do you have any questions about, comments on, or features desired in the InCommon Certificate Service offering that could influence your decision to subscribe in the future?”

* No. We made the above choice shortly before the InCommon offering became available.
* Does the InCommon service offer certificates that are "branded" for the institution?
* Our annual spending on certificates is slightly less then subscription costs for the certificate service through InCommon.
* Using InCommon's cert service would be beneficial to us. Unfortunately it means lots of work converting our certs from many other vendors to Comodo -- work that we don't have time to do at this point.
* We are in the process of subscribing and are looking forward to it!
* Currently it costs too much for us to consider. Our current yearly expense is under $3000 and InCommon would cost us $5000
* I believe you have a clause that disqualifies government institutions.
* How well accepted are the InCommon certificates by main stream browsers and modern day Operating Systems. I have heard some have had trouble in that the root certificates are not being distributed to all browsers / OS's
* Our security team has concerns about Comodo. If there was a different organization in that role we would definitely be more interested in certificates.

**Open-Ended Response Options**

**Question 6** (Features in Use), Answer choice “**Other**”:

* Certificates
* Unsure since there is a process created for LIGO administrators by Caltech.
* Settings->Domains and Certificates
* I don't interact w/InCommon directly. We have a go-between system that end users/system administrators like me use to request certs, and to get upcoming expiration notifications from.
* We have just signed for the service, but I don't think we have deployed anything yet.

**Question 7** (Most challenging aspects), Answer choice “**Other**”:

* no issues
* none
* Configuration of Organizatonal Key Escrow
* none
* No longer capable with issuing private certificates for internal use
* would like the ability to delete old cv's or ssl certs
* Customers not renewing certs in a timely manner
* none, it's all easy with InCommon
* Determining the right signed cert to download
* The code signing certificate process
* Approval is the only part we have to do by hand.
* managing automated emails to requesters, especially expiration warnings
* Inablilty to simply hide/delete/manage older certificates cluttering up the interface
* Being 100% sure no certs expire while still in use.
* None of these are challenging, that is what is so useful.
* Nothing really
* None of these challenging. Everything works well.
* scheduling, not letting certs expire
* None really, as we have an intermediary system
* key management
* Managing departments
* Automating certificates with agent/API
* see q 6

**Question 12** (Didn’t know where to find support, how I did it), Answer choice “**No-describe**”:

* I just asked on the cert-users forum
* Confusion between whether it was an InCommon or s Comodo issue
* used the cert-users mailing list initially, and was given good advice there
* I think I somehow ended up at the generic Comodo support. They directed me to the right place.
* I felt like I knew where to look; however, I was often redirected to a different point of contact than the support instructions on InCommon's website indicated.
* I called the support number on the InCommon website; got redirected to two or three different Comodo numbers.

**Question 13** (Method used to initiate support), Answer choice “**Other**”:

* Email my DRAOs
* Phone Incommon
* Phone call to incommon
* Emailed API support: cmapi@comodo.com

**Question 16** (Are you satisfied with the web interface), Answer choice “**Please elaborate**”:

* Very click intensive. Dealing with departments and organizations is confusing. Delegation is confusing. Interface is not SSO'd!
* The interface is a bit heavy handed when it comes to performing a general task. At my Institution, 90% of this is just requesting a cert. The forms are a bit dated and don't feel like they streamline the process very much.
* I'd love to have the ability to sort the certs list by recent activity. To make it easier to find actionable items.
* Need support for bulk approval of requests. Approving requests one-at-a-time is very time-consuming.
* It would be nice to be able to delete expired or invalid certificates from the management interface rather than just filter them
* CSRs uploaded are sometimes rewritten without notifying me, in the case of wildcard / multidomain certs.
* The web interface is functional at a basic level. It is also somewhat simplistic. Some examples: Re-submitted domain requests are listed under the original submission date so the new request can be buried; no consolidated reporting on domains; limited API capability; no support for Chrome for code-signing cert enrollment; login is not federated; no obvious way to un-check the Street address and Zip code boxes in the cert request form by default so this info isn’t included in the certs unless manually checked.
* better reporting functions - not a fan of having to go through Excel to parse information I need - too time consuming and easily miss information
* This has not caused any issues here (because the services is of low usage and low priority for us), but the service is down for maintenance extremely frequently (if we had a service that was down as frequently, there would be an inquiry).
* search functionality would be useful. - common name, requester, etc.
* I don't see that interface.
* Some of the bugs I have ran into in the CM interface have been really annoying.
* Too many errors and glitches. Needs stability desperately.
* Compared to previous provider, this is heaven even when there are problems.
* I would like the ability to optionally hide certs we no longer care about, expired, not approved, etc.
* I don't use it so I have no opinion

**Question 17** (Are you satisfied with the service overall), Answer choice “**Please elaborate**”:

* didn't explore them until this survey brought them to my attention
* Would be nice to be able to issue code-signing certs at the departmental level and still use a top level email address. E.g., issue a code-signing cert to me for the biology.ucsc.edu department, but have my email address be julieg@ucsc.edu, not julieg@biology.ucsc.edu.
* certain parts can be improved upon - reporting function for sure - more reporting options to better capture information I need
* Nice to have a one-stop-service for certificates.
* Fast and cheap and reliable.
* See that question about feature enhancement, would love to see those!!
* Missing ability to have a wildcard cert with SANs. Can have a SAN cert with a wildcard as a SAN, but some applications require the wildcard to be the primary name.
* We are moving to hardware tokens, need user certs, need local CA for firewall SSL MitM, and would love to have all this integrated in your service. We are having to look outside for other options and we are limited on staff for managing multiple cert sources.

**Question 23** (Other institutional certificate service), Answer choice “**Please tell us about it**”:

* DigiCert
* Established around 2002, using EJBCA. We issue web application and SSL certificates trusted by GlobalSign. Personal certificates are trusted locally, and issued on SafeNet eTokens.
* Purchased certificates through Thawte, and an internal openssl based ca for non-user facing certificates.
* We currently use multiple vendors depending on the project
* Comodo
* I assume you are asking about SSL certificates? We use two commercial sources and one specialty source for certificates that chain back to the federal bridge. Some groups also acquire certificates from other independent suppliers.
* Symantec Verisign

**Question 2:** Name of your institution, if you wish to provide it (all responses listed, but sorted alphabetically):

|  |
| --- |
| * Arizona State University
 |
| * Baylor College of Medicine
 |
| * Brandeis University
 |
| * Brown University
 |
| * Buckell University
 |
| * Bucknell University
 |
| * Cal Poly San Luis Obispo - California State University
 |
| * California Institute of Technology
 |
| * California State Polytechnic University, Pomona
 |
| * California State University, Monterey Bay
 |
| * Colorado State University
 |
| * Colorado State University
 |
| * Columbia University
 |
| * Comodo
 |
| * Coppin State University
 |
| * Denison University
 |
| * Duke University
 |
| * Duke University
 |
| * duke.edu
 |
| * Fort Lewis College
 |
| * George Mason University
 |
| * Georgia Institute of Technology
 |
| * hartnell
 |
| * Harvey Mudd College
 |
| * Indiana University
 |
| * Indiana University
 |
| * Kansas State University
 |
| * Lafayette College
 |
| * LIGO via Caltech
 |
| * Loyola University Maryland
 |
| * Macalester College
 |
| * Macalester College
 |
| * Madison Area Technical College
 |
| * Marshall University
 |
| * Michigan State University
 |
| * Michigan State University
 |
| * NC State University
 |
| * North Carolina State University
 |
| * Ohio Northern University
 |
| * Ohio University
 |
| * Ohio University
 |
| * Ohio University
 |
| * Oregon State University
 |
| * Oregon State University
 |
| * Oregon State University
 |
| * Oregon State University
 |
| * Oregon State University
 |
| * Otis College of Art and Design
 |
| * Owens Community College
 |
| * Pacific Lutheran University
 |
| * Purdue University
 |
| * Rensselaer Polytechnic Institute
 |
| * Rice University
 |
| * RIT
 |
| * Rowan University
 |
| * Sacred Heart University
 |
| * Southern Illinois University
 |
| * Southern Methodist University
 |
| * Stanford University
 |
| * The University of Arizona
 |
| * The University of Tennessee
 |
| * The University of Texas Medical Branch
 |
| * UC Berkeley
 |
| * UC Berkeley
 |
| * UC Berkeley
 |
| * UC Santa Cruz
 |
| * ucar
 |
| * UCI
 |
| * UCSB
 |
| * UCSD
 |
| * UCSD
 |
| * UIUC
 |
| * Univ of Michigan
 |
| * University at Albany
 |
| * University of Alaska
 |
| * University of California, Office of the President
 |
| * University of Chicago
 |
| * University of Cincinnati
 |
| * University of Hawaii
 |
| * University of Idaho
 |
| * University of Illinois at Urbana-Champaign
 |
| * University of Illinois at Urbana-Champaign
 |
| * University of Iowa
 |
| * University of Maryland College Park
 |
| * University of Missouri
 |
| * University of Nebaska at Kearney
 |
| * University of Nebraska
 |
| * University of Notre Dame
 |
| * University of Notre Dame
 |
| * University of Notre Dame du Lac
 |
| * University of Rochester
 |
| * University of the Pacific
 |
| * university of wisconsin-madison
 |
| * University of Wisconsin-Milwaukee
 |
| * USC
 |
| * UT Arlington
 |
| * VCU
 |
| * Virginia Commonwealth University
 |
| * Washington and Lee University
 |
| * Weber State University
 |

**Other Institutions** (those who don’t subscribe):

|  |
| --- |
| * Argonne National Laboratory
 |
| * Bates College
 |
| * Bryn Mawr College
 |
| * California University of PA
 |
| * Comodo
 |
| * Ohio Technology Consortium
 |
| * Portland State University
 |
| * St. Olaf College
 |
| * U.C. Riverside
 |
| * University f Nevada, Las Vegas
 |
| * University of Houston
 |
| * University of Maryland, College Park
 |
| * Virginia Tech
 |