InCommon Certificate Service Review
Report - June 13, 2016

Executive Summary

The InCommon Certificate Service offers unlimited SSL certificates (server, user, and code-signing) for a single annual fixed fee, with pricing based on an institution's Carnegie Classification. The service has been very successful; to date, around 288,000 SSL certificates have been issued by 363 subscribing organizations. As the contract is up for renewal in 2016, InCommon leadership decided to engage the community in a review of the certificate service and chartered a working group to gauge satisfaction and prioritize new features and improvements.

The working group began by surveying the community about desired features and used those survey results to prepare a summary report with prioritized features. This document is that report. Here is a summary of the working group's findings and recommendations.

- Through the survey, the working group found that satisfaction with the InCommon Certificate Service is very high, with 89 percent of survey respondents indicating they are Very Satisfied or Satisfied with the features of the of service. None expressed any overall level of dissatisfaction.
- Based on the survey and group discussions, the working group developed a list of current gaps and desired features, and prioritized that list (which appears later in this report). The working group recommends that that InCommon work together with the vendor to close identified gaps, with attention to the priority list.
- The working group also recommends that InCommon continue to keep abreast of developments in the certificate services marketplace, so that the InCommon service can continue to offer a high quality product suite for a competitive price.

Background

In 2010, InCommon began offering a unique certificate service that represented a significant change in the acquisition model for certificates. Historically, participants paid enormous retail fees for each certificate they deployed. Besides the resulting strain on IT budgets, this reality also led to suboptimal use of certificates. Development environments many times did not have certificates, user certificates were not widely deployed, and code-signing was rarely done.

The InCommon Certificate Service completely changed that dynamic by offering an unlimited number of certificates (SSL, user, code-signing) for a single annual fixed fee. By using a pricing structure based on an institution's Carnegie Classification, this service was accessible to

institutions of all sizes. Further, the service would be controlled and governed by the research and higher education community.

The service has been very successful, now with 363 subscribers and approximately 288,000 SSL certificates issued via the InCommon Certificate Service. With the contract up for renewal in 2016, InCommon leadership decided to engage the community in a review of the certificate service, to ensure that the service remains a tremendous value in terms of the investment required and the features offered. As a result, a working group was formed to prepare a report detailing and prioritizing the features considered most important by the InCommon community.

Strategy

The working group sought feedback from the broader community, including both current subscribers to the service and potential future subscribers, in the form of a survey. Current subscribers were asked what was working well, what was not working well, and what new features would be of interest. From those who are eligible but not subscribing, the working group sought to learn what might make the service more attractive, and what obstacles might be preventing their joining. With this information, the working group would be able to prioritize the feature requests so as to best align the service with the needs of the community.

Process/Approach

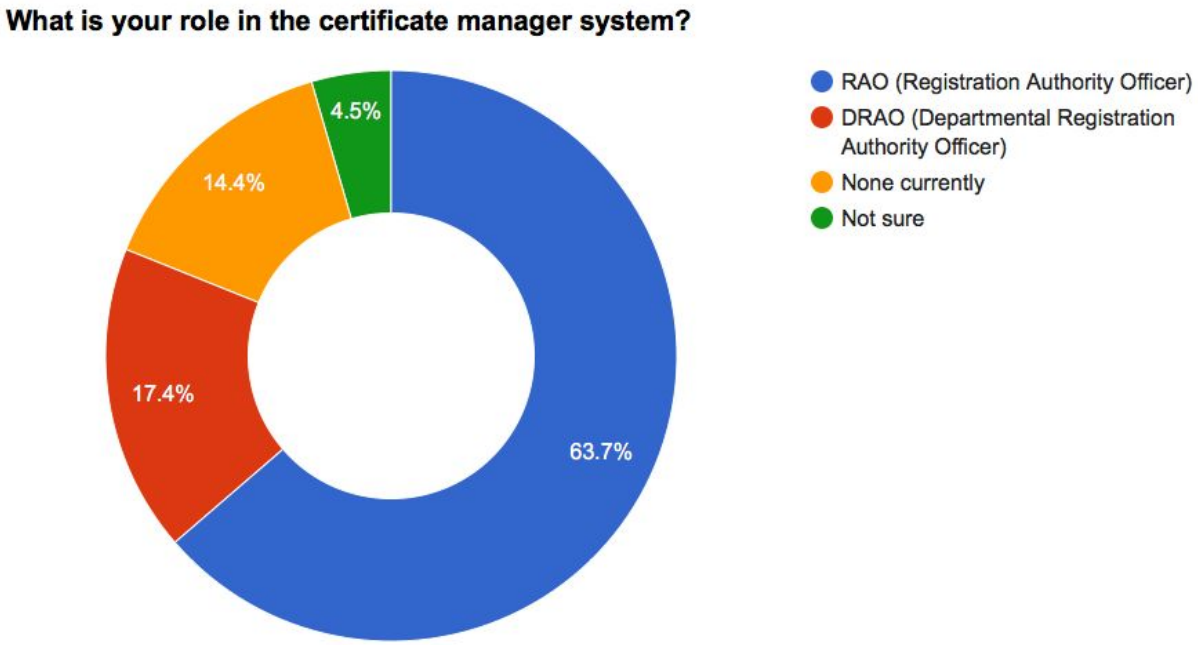
The working group distributed a survey via the InCommon Participants and Cert Users mailing lists on November 23, 2015. Many of the current subscribers have at least one representative on the Cert Users list. The InCommon Participants list was included in order to reach both current and prospective subscribers. A follow-up reminder was sent on December 2, since the survey notice was sent during the holiday season.The survey was briefly reopened in January to accommodate additional responses from members of the Common Solutions Group (an organization comprised of 31 research universities).

Survey Data

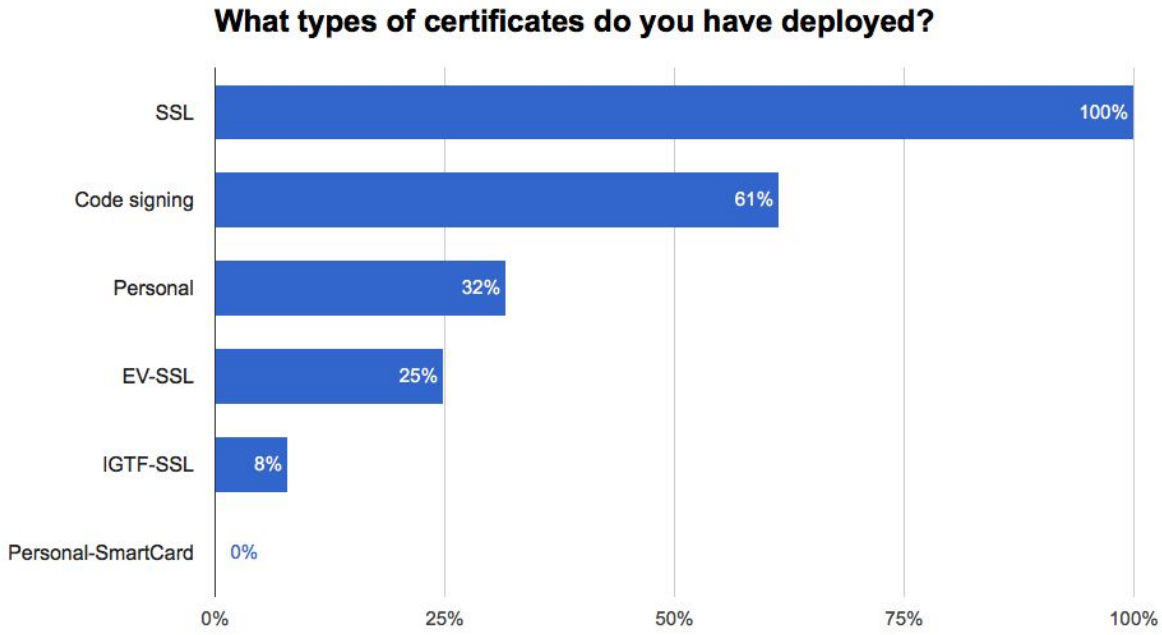
There were 166 completed surveys; 20 (about 12 percent) from non-subscribers. This summary of the survey results is presented primarily by using charts. When a question included an opportunity for open-ended responses, those answers are summarized.

Service Use and Potential Enhancements

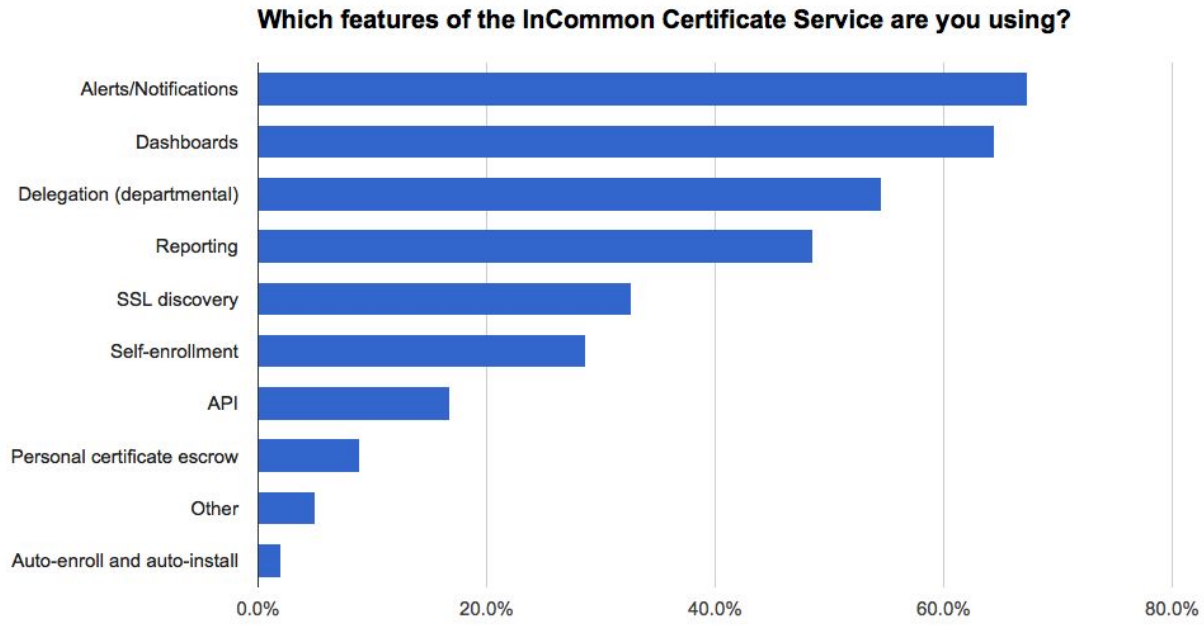
Role in the Certificate Management System



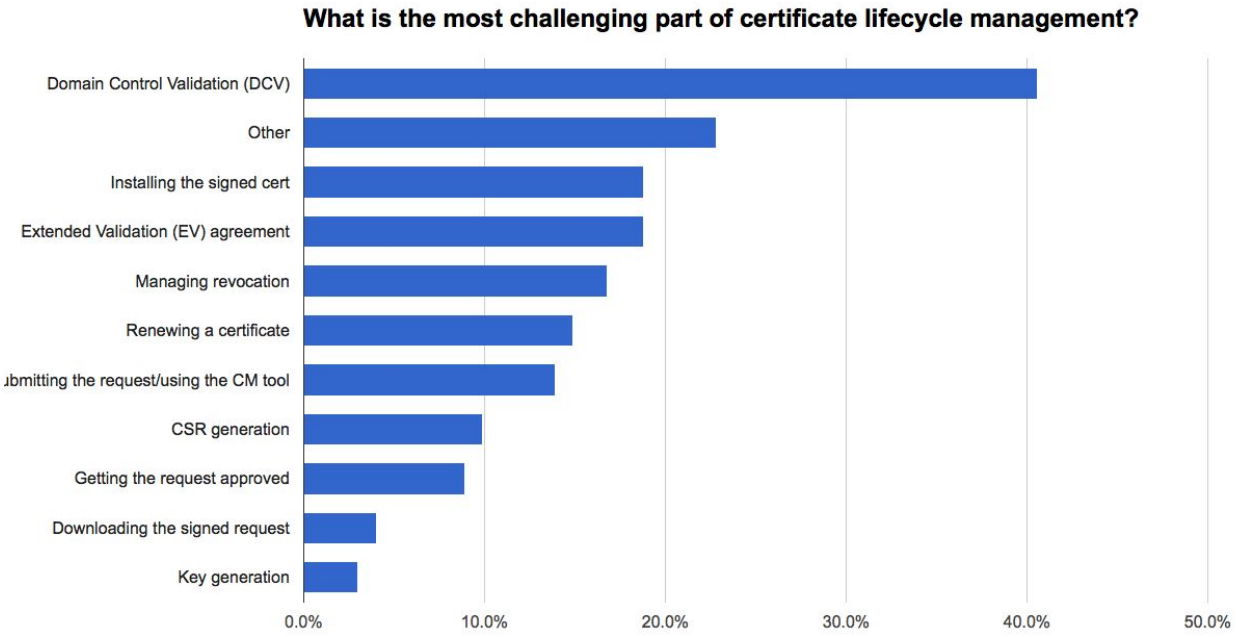
Types of Certificates Deployed



Certificate Service Features Used



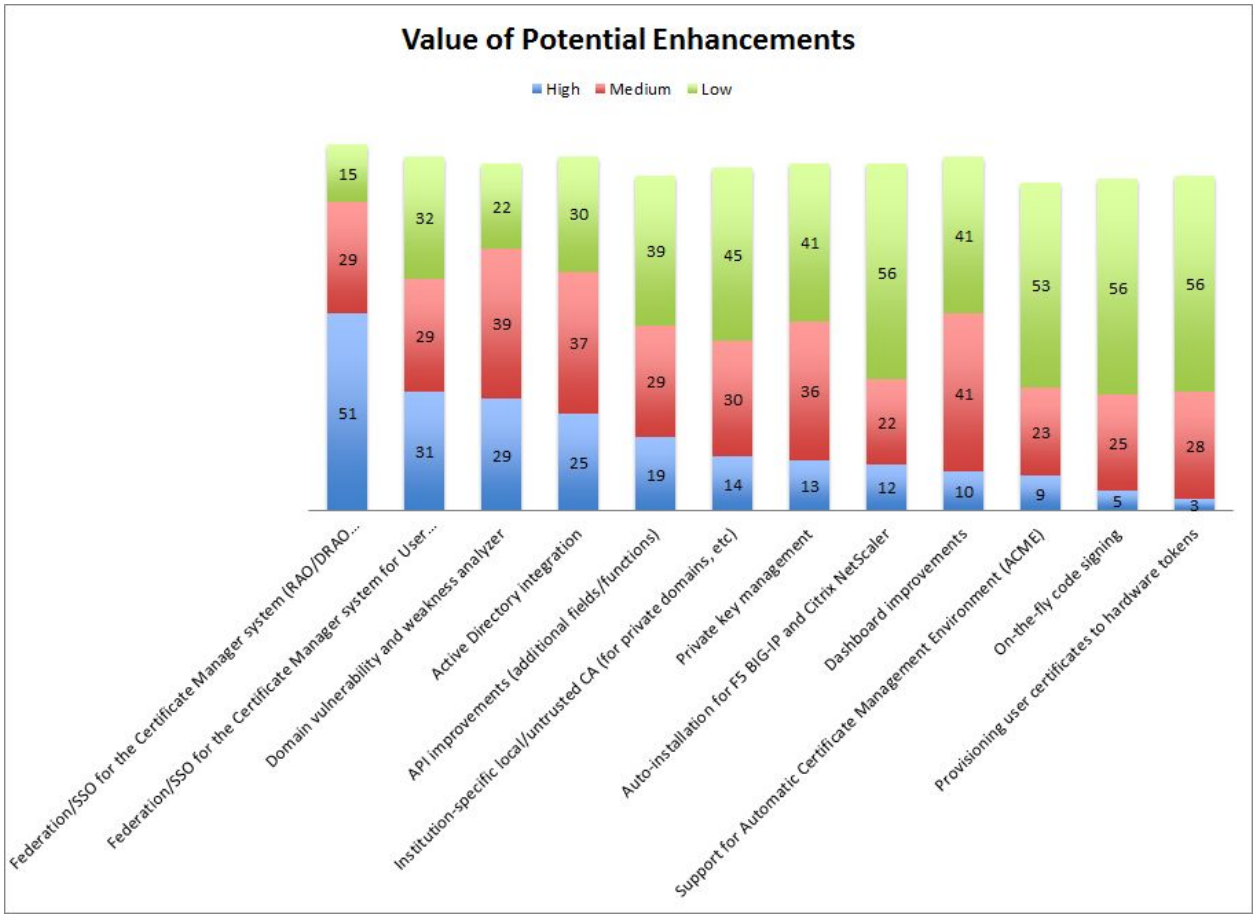
Challenges in Certificate Lifecycle Management in the InCommon Service



Other challenges (not listed on the chart) include the code signing certificate process, determining which certificate to download, expiration situations and having customers renew in a timely manner, managing departments, and automating via the API.

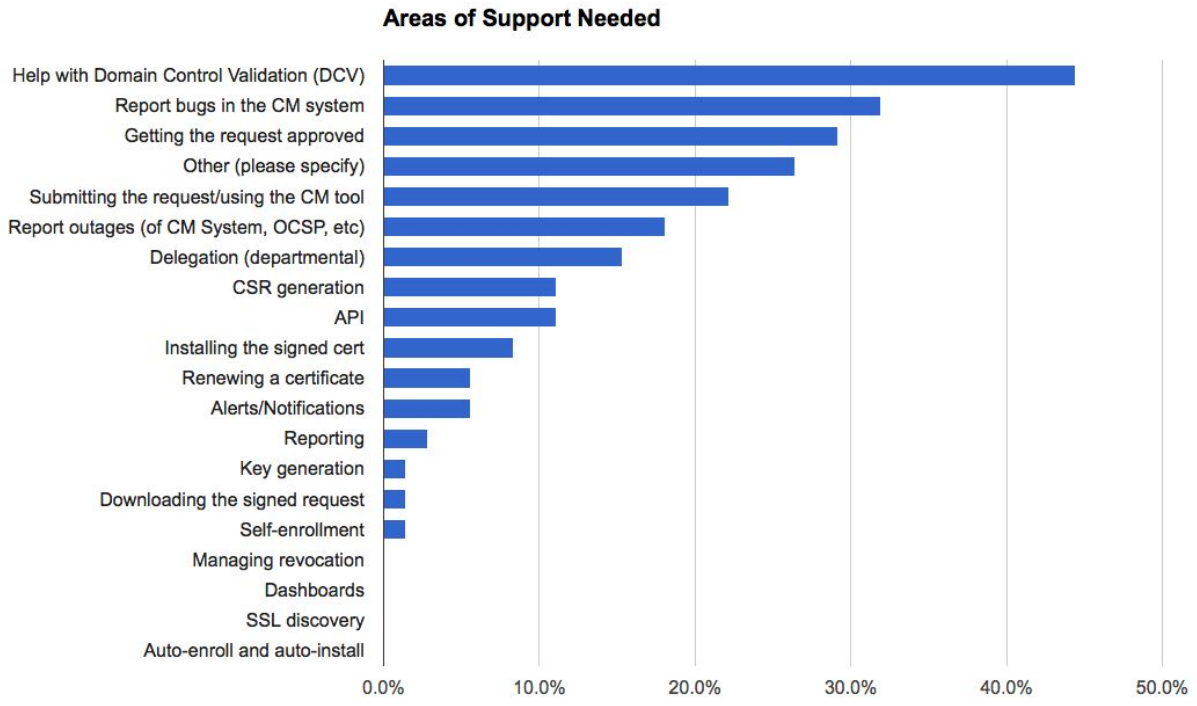
Desired Enhancements to the Service

Federation/SSO for RAO/DRAO access to the system was the only highly valued potential enhancement at 54%. No value was dominant for Federation/SSO or User Certificate self-enrollment. Medium value potential enhancements include Active Directory Integration (40%) and domain vulnerability/weakness analyzer (43%). Dashboard improvements are of medium to low value. Private key management, auto-installation, on-the-fly code signing, Additional API fields and functions, Provisioning user certificates to hardware tokens, Automatic certificate management environment, and Institution-specific local/untrusted CA are all low value potential enhancements. See the chart below for details.



Certificate Service Support

Most respondents (73%) needed and contacted support as they used the InCommon Certificate Service. Help with DCV topped the list. Other top reasons for contacting support were reporting bugs with the Certificate Manager (CM), issues with getting a request approved, or problems submitting the request using CM.



Improvements suggested in the open-ended portion of the question include:

- maintain an updated FAQ based on questions and problems posed to cert-users list and support requests
- streamline the EV request/approval process
- Enhance the search capability for the knowledge base and other online docs

Respondents also noted requests for new features, mostly around expansion of single sign-on convenience, multifactor authentication support, and additional APIs.

Almost 92 percent of respondents said they knew where to look for support. When asked if their issues were satisfactorily resolved after contacting support, 96 percent responded “always” or “usually.”

Service Reliability and Improvements

When asked if they are satisfied with the reliability and availability of the InCommon Certificate Service, 97% of respondents answered “very satisfied” (58%) or “satisfied” (39%).

When asked if they are satisfied with the Certificate Service web interface, 79% responded “very satisfied” (25%) or “satisfied” (54%). Suggestions for improvement include:

- Implementing single sign-on (e.g. federating the interface)
- Simplifying the interface. Comments include:
    - dealing with departments and organizations is confusing
    - heavy handed when it comes to performing a general task
    - need support for bulk approval of requests
    - better reporting functions

When asked if they are satisfied with the features of the InCommon Certificate Service, 90% answered “very satisfied” (36%) or “satisfied” (54%). Ideas for improving the service and community engagement include more communication about upcoming feature changes, documentation of problems encountered with the service and the resolution thereof, as well as a general status page. In general, smaller institutions said they would be interested in the service at a lowercost.

Key Features Desired by Subscribers

High priority (“must-have”)

- IGTF certificates
- Single sign-on to CM interface
- Multi-factor authentication to CM interface
- API for automated certificate requests
    - Secure/flexible authentication
    - Reflects all relevant functions/fields of CM interface
- Delegation of request and/or approval process for subdomains/departments
- FAQ doc on support site
- Roadmap for support communications
- Automated service status page for CM interface, CA issuance (NOT hosted on CM servers)
- Forum/email list for certificate service discussions
- Knowledge base tailored to InCommon service
- Email, web and phone support routes
- Customizable notifications from CM interface

- Adequate performance for CM interface and API (SLA)

Medium priority (“really nice to have”)

- Streamlined EV process
- Well-documented DCV process
- ACME protocol support (supported out of box in newer server software)
- Smart card capable client certificates (OID for cert use)
- Bulk cert requests/approvals (API, possibly CM interface)
- Standardized API
- Webinars (support)
- Training
- Single point of contact for support (one neck to wring them all)
- Wildcards with subjectAltNames (needed for some systems)
- Bulk certificate renewals via CM interface
- Synchronize or adjust DCV expirations to allow mass DCV renewals

Low priority (“kinda nice to have”)

- Alternative subscription models (e.g. metered use with smaller fees for smaller institutions)
- Local CA options: hosted/on-site (for a fee)
- Private User cert CA (for fee)
- Cross-certification with FBCA (for fee)
- Easy filtering in CM interface and reports (e.g. to filter out old certs - expired, revoked, superceded)
- Domain vulnerability/weakness analyzer
- Active Directory integration (client certs e.g. computer certs without needed to explicitly trust Microsoft CA, or hooks into Microsoft cert request API)
- Certificate discovery
- Dashboard display
- CM display of all relevant request fields needed for approval (e.g. requester, CSR fields like CNs, subjectAltNames, OUs that will be copied to issued cert)
- CA certificate in Adobe trust list
- CA certificate trusted by Blackboard Transact

Gap Analysis with Current Service

Category	Gap	Priority	Description	Responsible Group
Service	DCV - documentation	M	make the process easier/smoother	InCommon

Offering				
Service Offering	Alternative subscription models	L	For small schools where the 'unlimited' option is too expensive, it would be desirable to offer less expensive plans with more limited services.	InCommon/ Comodo
Service Offering	ACME support	M	New web server software is starting to come with support for the ACME request protocol baked in. Supporting it would make it easier for server administrators to request certificates.	Comodo
Service Offering	OID for smart card clients certs	M	In order to allow client certificates to be used with smart cards, the certificates need to specify a particular certificate usage OID.	Comodo
Service Offering	Better docs for EV processes	M	make the process easier/smoother and/or document it better	InCommon
Service Offering	More vendor support familiarity with InCommon EV	M	At times, subscribers have been frustrated or confused when they engage with Comodo support, but their requests are misrouted or misunderstood because the support person doesn't understand InCommon's unique circumstances, process, and needs.	Comodo
Service Offering	Performance (strengthen SLA)	H	The current Service Level Agreement does not specify any meaningful consequences for failure to meet service level goals. It would be useful to have a broader range of tools, such as financial penalties, rather than having to rely on contract termination for enforcement (the "nuclear option").	InCommon/ Comodo
Service Offering	Wildcards with SAN	M	Certain systems require certificates with a wildcard in the Common	Comodo

			Name field, and additional hostnames in the subjectAltNames extension. Currently, only the opposite is supported (wildcard must be in the SANs).	
Service Offering	Local CA options	L	(should already be in next contract)	Comodo
Service Offering	CA trusted by Adobe/Blackboard Transact	L	Getting certificates trusted by additional products would make deployment easier for schools that use them. Two key applications would be Adobe (which has a common trust list for their apps) and Blackboard Transact (which has only two valid CAs at this time and is likely to be difficult to change).	InCommon/ Comodo
Service Offering	FBCA cross-cert	L	Cross-certification with the Federal Bridge CA would be useful in some research contexts.	Comodo
CM Interface	Single sign-on	H	Ideally SAML federated SSO through InCommon	InCommon/ Comodo
CM Interface	Multi-factor authentication	H	Aligned with MFA Interoperability profile, possibly leveraging an InCommon proxy.	InCommon/ Comodo
CM Interface	Bulk cert requests/approvals/renewals	M	Key use case: mass reissuance (e.g. Heartbleed, SHA2) currently requires administrators to manually submit requests for hundreds of certificates, and then have them manually reviewed and approved. It would be nice to have a way to request a number of certs at one time, perhaps by uploading a CSV file with the necessary data. A similar function is desired in the API.	Comodo
CM	Sync DCV expirations	M	To allow for mass DCV renewals on a	Comodo

Interface			per-org/department basis, rather than having a trickle of them come through during the year.	
CM Interface	Improved custom notifications	H	Add more fields/events, documentation of existing ones	Comodo
CM Interface	Improved filtering for certs, domains, etc.	L	E.g. automatically filter expired/revoked certs	Comodo
CM Interface	Improved reporting	L	Filter out old/irrelevant certs	Comodo
CM Interface	Better integration of vulnerability scanner	L	Scanning for firewalled or RFC1918-addressed servers, perhaps via a local agent/proxy	Comodo
CM Interface	Microsoft Active Directory (ADDS) integration	L	Focus is on client cert issuance, particularly computer certs for e.g. SCCM, and not needing to manually configure trust for local Microsoft CA: have client certs effectively signed by already-trusted CA. A couple ideas: signing the local MS CA with a trusted CA, or maybe by hooking in to MS CA's request provisioning, so requested certs are signed by external trusted CA; latter option was available from Verisign(?) at one point.	Comodo
CM Interface	Show DN for issued cert prior to approval	L	Enables approver to verify resulting DN will be acceptable - currently need to cut/paste CSR from Edit panel into openssl to see OU field that will be copied into final cert. Applicable to certs with Department set to "ANY".	Comodo
API	Improved auth options	H	Want passwordless option, such as private key. Ideally not tied to person, since the person is seldom actually handling the requests.	Comodo

API	Additional API fields/functions	H	Currently missing the ability to set some fields in requests, such as external requester. Would be nice to be able to perform DRAO user management and delegation, and organization management (creating/delegating departments and domains, requesting DCV).	Comodo
API	Bulk cert requests/approvals/renewals	M	Key use case: mass reissuance (e.g. Heartbleed, SHA2) currently requires administrators to manually submit requests for hundreds of certificates, and then have them manually reviewed and approved. It would be nice to have a way to request a number of certs at one time via the API, perhaps via a list of order IDs to renew. A similar function is desired in the CM interface.	Comodo
API	Standardized API	M	for report Recommendations - standardized API could improve vendor independence/agility (compare TERENA experience) InCert tool as part? InCommon-run gateway not desirable (liability, security) but InCommon-curated adapter code might be a reasonable workaround if vendor cannot directly implement.	InCommon
Support	Service status page(s) for CM interface, issuing CA	H	Automated service status page giving current assessment of operational status; Duo's status page is a good example of what this could look like. Ideally this would include both the CM interface (frontend) as well as the actual issuing CA status (backend).	Comodo
Support	Roadmap for support communications	H		Comodo

Support	Single point of contact	M	Have one place to go for support, rather than having to be sent to the Other One for problems. Potentially integrate with vendor ticketing (single initial POC).	InCommon/ Comodo
Support	Training for CM interface	M	Vendor-led training for the CM interface, for onboarding new subscribers and/or DRAOs.	InCommon/ Comodo
Support	FAQ doc on support	H		InCommon
Support	Tailored KB	H	Vendor knowledge base covers many products, some of which are not relevant to the InCommon service. For example, it can be confusing to find the correct root certificate. A knowledge base tailored to the InCommon service could minimize these problems.	InCommon/ Comodo
Support	Support webinars	M	Describing/demonstrating new features or best practices for using current features of the CM interface and API. Previewing upcoming releases. Roadmaps for future service development. Ideally would include content provided by vendor, InCommon staff, and participants.	InCommon/ Comodo

Recommendations

The working group recommends that InCommon work together with the vendor to close the gaps identified in the Gap Analysis, with attention to the priorities identified by the community. Also, InCommon should continue to keep abreast of developments in the certificate services marketplace, so that the InCommon service can continue to offer a high quality product suite at a competitive price.

The community seems to feel pretty positive about the certificate service in general; of 95 responses, 85 indicated they were Very Satisfied or Satisfied with the features of the service, and none expressed any level of dissatisfaction. But there are plenty of features and

improvements that the community would like to see in order to keep the service current and responsive to their input.