



The University of Minnesota Enables Security at Scale with the InCommon Certificate Service

July 12, 2016



THE PROBLEM

With 51,000 students, two campuses and over 300 research, education, and outreach institutes, the University of Minnesota ranks eighth among public universities in research spending. That makes for a large demand for websites and servers and the associated certificates necessary for security. According to Chris Bongaarts of the Office of Information Technology, Minnesota had been spending \$53,000 on certificates, plus \$16,000 for internal administration and billing.

The university's previous vendor provided a volume discount, but still charged per certificate, tying up university resources to purchase tokens in advance and handle the internal chargebacks to requesting departments. "Billing was a huge pain previously, keeping a spreadsheet of requested certificates and making sure the orders were billed to the right departments," says Bongaarts.

Additionally, the university's IT administrators endured long waits for manual certificate issuance and were dependent on the vendor's often-jammed schedule for all changes. Bongaarts says the administrators enjoyed only haphazard community and collaboration in the process.

"BILLING WAS A HUGE PAIN PREVIOUSLY, KEEPING A SPREADSHEET OF REQUESTED CERTIFICATES AND MAKING SURE THE ORDERS WERE BILLED TO THE RIGHT DEPARTMENTS."

CHRIS BONGAARTS, OFFICE OF INFORMATION TECHNOLOGY, UNIVERSITY OF MINNESOTA

THE RESULT

As a very large university, Minnesota now invests only \$15,000 annually with InCommon for an unlimited number of certificates, compared to \$53,000 on 679 certificates previously. Smaller schools pay much less. A wide and increasing variety of certificates is also available, including wildcards, multi-domain, and code-signing. There is also the option—not yet exercised at Minnesota—for client, EV, IGTF and other types of certificates. These are all publicly rooted and publicly trusted, and available for every domain owned by the university (whether .edu, .org, .com, or any other).

THE SOLUTION

For the University of Minnesota, years of fragmented, inefficient certificate service administration was solved by the flat-rate, low-fee InCommon Certificate Service, which accommodates the volume, frequency, and variety of the university's required certs while significantly reducing administrative overhead.

COLLABORATORS

- **The University of Minnesota**
<http://twin-cities.umn.edu>
- **Certificate Service User Group**
<https://spaces.internet2.edu/display/InCCollaborate/InCommon+Certificate+Service>

PRODUCTS & SERVICES:

- **InCommon Certificate Service**
certificates.incommon.org

With InCommon, the annual flat-fee "all-you-can-eat" model simplified the financial process by enabling the university to provide certificates under a "common good" model with no chargebacks required. There is a single bill to pay once a year, instead of having to keep buying tokens every few months. And the flat fee is \$38,000 less than the total amount once paid for a year's worth of certificates.

MINNESOTA NOW INVESTS ONLY \$15,000 ANNUALLY WITH INCOMMON FOR AN UNLIMITED NUMBER OF CERTIFICATES COMPARED TO \$53,000 ON 679 CERTIFICATES PREVIOUSLY.

Requests now are usually fulfilled in minutes or less, and in extraordinary situations (such as a crisis like Heartbleed a couple of years ago), hundreds of certificates can be replaced in short order, which minimizes potential exposure. Even Extended Validation certificates (so-called "green bar" certificates), which by definition require much more vetting, are often handled within days.

Because of the ease, speed, and security with which certificates are issued, even development and test servers can enjoy real-world testing and ramp-up using “real” instead of placeholder certificates.

The university now uses the InCommon Certificate Service to serve dozens of academic departments, labs and research centers within the entire Minnesota system. Departmental registration authority officers can issue their own certificate requests, getting central IT out of the mix after initial setup and authorization. Such delegation lets a central administrator give control over specific parts of a domain to the appropriate departmental staff, who can request and approve certificates within their area.

Bongaarts estimates he has delegated authority to nearly 50 IT professionals across the university system. “For example,” he notes, “I can grant access to the St. Anthony Falls Lab IT staff to request and approve certificates for specific sites. As a central admin, I can still view their certificates and I still have to approve certificates they request outside of their delegation. We like to send that job off to the departments that actually own the domain names whenever possible.”



“One big win,” Bongaarts recalls, “was our College of Liberal Arts. Their IT group manages dozens of websites across 25 subdomains representing their constituent departments. We delegate the subdomains to the College of Liberal Arts ‘department’ in Certificate Manager, and set up their 5 administrators with access to the College of Liberal Arts ‘department.’ This pattern makes it easy to add or remove subdomains or administrators over time, without having to make the same change to each administrator.”

“Of course, one consequence of using delegation,” Bongaarts points out, “is I don’t often hear from the administrators once they are set up in the system unless they need additional domains configured. But I know that they appreciate being in control of cert issuance for those domains, especially in a decentralized IT environment which is typical for higher ed.”



The University of Minnesota was an early adopter, subscribing in September 2010, and continues to provide feedback on the certificate service to InCommon. In addition, as with most Internet2 services, community collaboration is key to providing support and sharing improvements.

Bongaarts recalled several instances where community members provided significant help to peers to solve integration and implementation snags. The most common place to find collaboration, he says, is on the cert users’ e-mail list, which serves as a type of user group and now includes more than 300 individuals who bring new ideas, problems, and solutions to the table.

What did the university expect to gain from the switch to the InCommon Certificate Service? “Cost alone was sufficient reason to subscribe,” Bongaarts notes, “but speed, the delegable workflow, and community support” were also compelling features. He confirms that the service has fully met those needs.

COST ALONE WAS SUFFICIENT REASON TO SUBSCRIBE, BUT SPEED, THE DELEGABLE WORKFLOW, AND COMMUNITY SUPPORT WERE ALSO COMPELLING FEATURES.

“Two features that we really like that didn’t directly factor into our initial decision were delegation and the effects of the buffet model.” As noted above, delegation helps save time by pushing control over cert issuance closer to those who actually make the requests. By “buffet model,” Bongaarts refers to the availability of unlimited certificates for all domains owned by the university. He says this encourages enhanced security, because test and development servers can be protected since there is no incremental cost.

“Overall, even where early on there may be the rare bump in availability or performance, those problems were promptly addressed,” says Bongaarts, and the University of Minnesota continues as a happy collaborator.