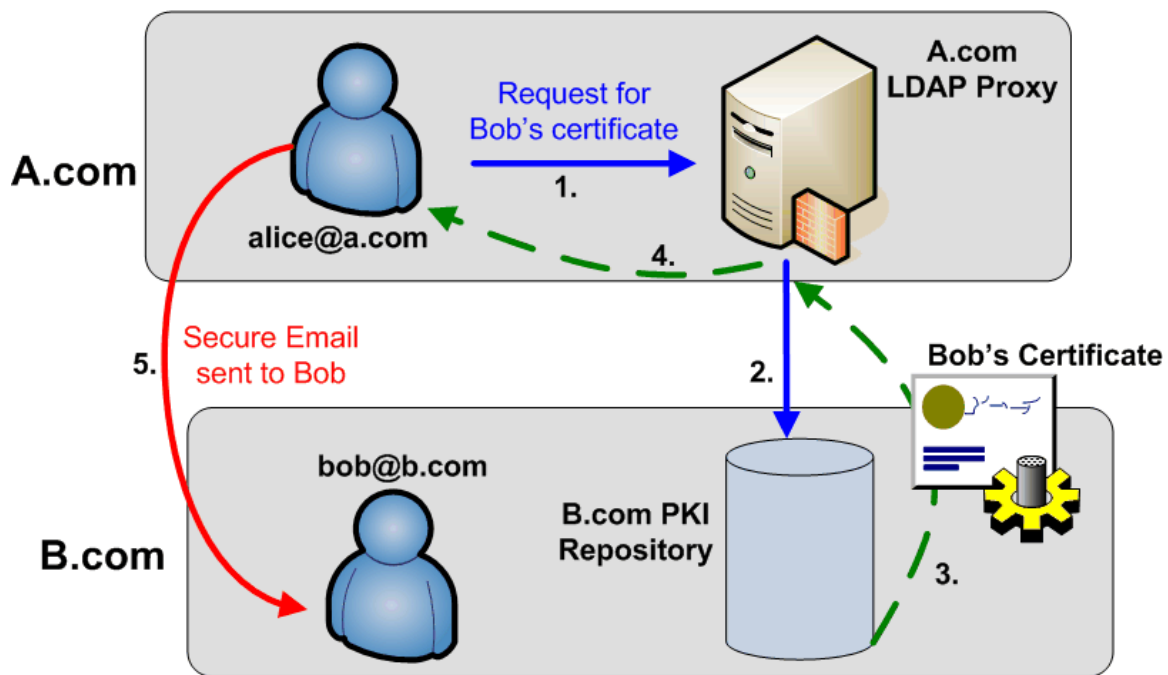


# Carillon LDAP Proxy

Enabling secure email in a multi-enterprise collaborative environment

An LDAP Proxy is a key ingredient in a collaborative secure email architecture. It solves the problem of certificate distribution: the sender of an email locates the encryption certificate of the recipient by querying an LDAP Proxy configured with information about all the company's collaboration partners.



Carillon's LDAP Proxy is the most secure, flexible, and comprehensive LDAP Proxy available. It ensures certificate validity and provides simple centralized configuration management, all while meeting the most stringent security requirements.

## Carillon LDAP Proxy

The LDAP Proxy accepts queries for remote user certificates and revocation lists, and forwards (proxies) them to another LDAP repository known to contain the requested information. The result is relayed back. (It is not a proxy in the firewall sense.) For secure email applications, this is used by a sender to retrieve recipient encryption certificates.

Carillon's LDAP Proxy is built on top of version 2.3.43 of the OpenLDAP open-source LDAP server and a heavily modified version of the open-source "getcert" back-end module originally written by The Boeing Company.

Our updates provide numerous important security and interoperability enhancements. Secure proxying and certificate verification provide end-to-end trust in the entire certificate lookup process. Centralized configuration management ensures that all collaboration partners are using the same set of proxy information.

## Secure proxying

Carillon's LDAP Proxy can open an LDAP/SSL session when forwarding a request to a remote server. In contrast, traditional LDAP Proxies only use unsecured connections. Combined with certificate verification, this allows for complete end-to-end trust in the lookup process, from the user's request, through the proxy, to the certificate returned from the remote server.

## Certificate verification

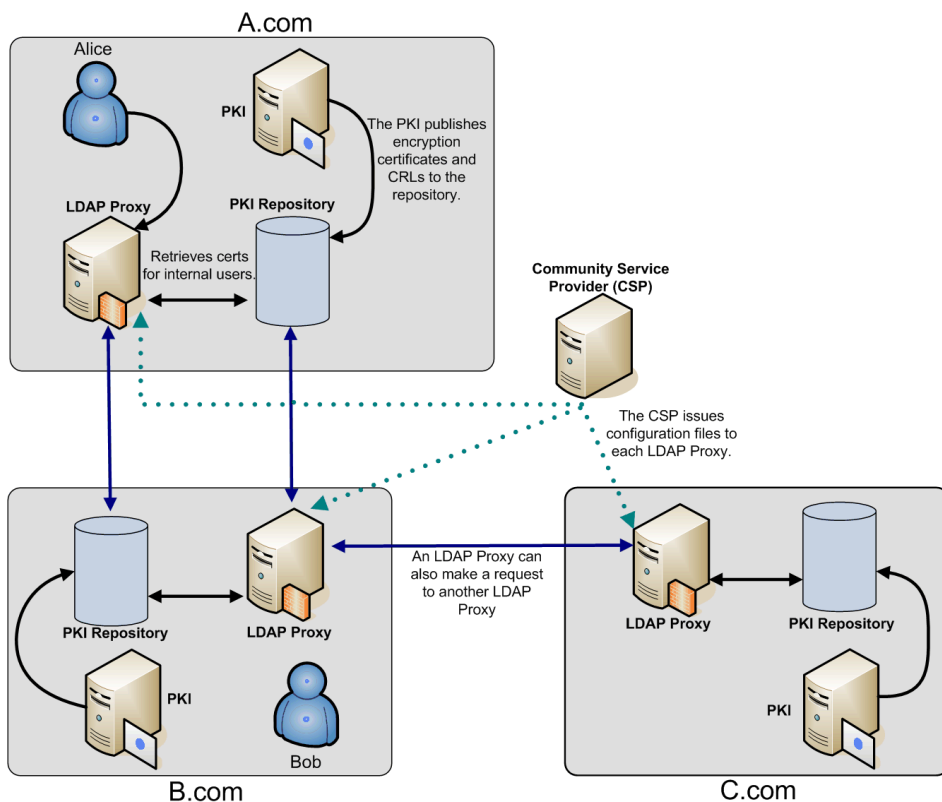
Carillon's LDAP Proxy verifies every certificate it encounters, by performing complete Path Discovery and Validation (PDVal) in compliance with RFC 5280, using Carillon's Pathfinder software. Policy mapping, policy constraints, and name constraints are all handled transparently, satisfying the stringent requirements of a bridged trust model. Policy matching can be configured to require specific policy OIDs if desired.

Client and server LDAP/SSL certificates are verified in this manner. Subscriber encryption certificates returned from the remote LDAP server are also verified in this manner before being passed back to the requester.

## Centralized configuration management

Traditionally, each collaboration partner needed to set up its own LDAP Proxy and maintain the proxy information for all its partners.

Carillon's ProxyConfig software simplifies this. Proxy information for collaboration partners can be automatically retrieved from a central location, usually known as a Community Service Provider (CSP). All collaboration partners retrieve the same proxy information regularly. Maintenance overhead is thereby greatly reduced, and each participant has an up-to-date list of partner LDAP Proxy servers, with no changes or server restarts required.



## Supported platforms

Carillon's LDAP Proxy is supported on:

- Debian GNU/Linux
- Ubuntu Linux
- Red Hat Enterprise Linux / CentOS
- Solaris



<http://www.carillon.ca/>

334 Joseph Carrier, Suite 101  
Vaudreuil-Dorion, QC J7V 5V5  
Canada

Phone: +1 514 485 0789  
Fax: +1 450 424 9559  
E-mail: [info@carillon.ca](mailto:info@carillon.ca)