

## ED FAQ (draft)

=====  
General ED:

Q: What is ED?

A: The Enterprise Directory (ED) is Virginia Tech's identity management system, providing information for authentication, authorization, application personalization, and business logic population. The ED consists of the Registry, ED-Lite, ED-Auth, ED-ID, and the business logic that ties all of these together.

Q: What is the Registry?

A: The Registry is Virginia Tech's central store of user data. In the context of ED-Lite, ED-Auth, and ED-ID, the Registry is their true backend, as data is pushed from the Registry to the ED-\*s.

Q: Why are there separate ED-\*s(Lite, Auth, ID)?

A: The ED project has several niches to fill: a quick, accessible whitepages directory (ED-Lite), a directory to do PID/pass authentication (ED-Auth), and a directory to provide more detailed user information for authorization (ED-ID). The ED-\*s were split up to facilitate development and management and to make each niche more perspicuous to end users.

=====  
General LDAP:

Q: What is LDAP?

A: LDAP stands for Lightweight Directory Access Protocol. A directory is a specialized database optimized for reading, browsing, and searching. See RFC2251 for details about LDAP (<http://www.rfc-editor.org/rfc/rfc2251.txt>).

Q: What does this have to do with ED-Lite, ED-Auth, and ED-ID?

A: ED-Lite, ED-Auth, and ED-ID are all LDAP directories (specifically OpenLDAP).

Q: What are binds?

A: Binding is the process that allows a client to authenticate to an LDAP server.

Q: What kinds of binds do the EDs support?

A: See section under each ED-\* type.

=====

=====  
ED-Lite:

Q: What is ED-Lite?

A: ED-Lite is a public, anonymously accessible LDAP directory used for whitepage related queries. It is the backend for People Search and finger.vt.edu.

Q: Why can't I see a person?

A: ED-Lite will only return data for people that are current employees (faculty, staff) or current students that have not chosen to be confidential. See ([http://www.computing.vt.edu/accounts\\_and\\_access/confidentiality.html](http://www.computing.vt.edu/accounts_and_access/confidentiality.html)) for more complete information on confidentiality settings.

Q: How do I suppress my information?

A: Log into Hokie PLUS and click on "Confidentialty Settings".

Q: I am a student. Why don't I show up in the summer?

A: Only those students who are taking classes during the summer will show up. Otherwise, they are not considered active members.

Q: Do the Confidentiality Settings in Hokie PLUS mean anything in ED-Lite?

A: For students, checking "Student Confidentiality" will cause you to be confidential in ED-Lite. Employees and students may suppress their mailing address and corresponding phone number. See ([http://www.computing.vt.edu/accounts\\_and\\_access/confidentiality.html](http://www.computing.vt.edu/accounts_and_access/confidentiality.html)) for more complete information on confidentiality settings.

Q: How long does it take for confidentiality settings to take place?

A: It typically takes about five minutes for the settings to take place in ED-Lite.

Q: How do I connect to ED-Lite?

A: Most access to ED-Lite is through the PeopleSearch interface (at <http://search.vt.edu/people.jsp>), though ED-Lite is accessible through any standard LDAP browser or program/application (at <ldap://directory.vt.edu>). Your application should use "ou=People,dc=vt,dc=edu" as the baseDN for searching.

Q: What kinds of binds does ED-Lite support?

A: You can only bind anonymously to ED-Lite. This means binding without a username or credentials.

Q: What data is in ED-Lite?

A: See the ED-Lite schema at ([http://www.middleware.vt.edu/pubs/ed\\_lite\\_schema.pdf](http://www.middleware.vt.edu/pubs/ed_lite_schema.pdf)). The intent of ED-Lite is to expose only public data to people.

=====

=====

ED-Auth:

Q: What is ED-Auth?

A: ED-Auth is an LDAP directory used for user authentication and role based authorization. ED-Auth is used for PID/pass authentication and authorization based on a person's affiliation with Virginia Tech ([http://www.middleware.vt.edu/pubs/person\\_affiliations.pdf](http://www.middleware.vt.edu/pubs/person_affiliations.pdf)). TLS/SSL is required for ED-Auth access.

Q: How can I do PID/pass authentication?

A: Please see the ED-Auth Usage Instructions at ([http://www.middleware.vt.edu/pubs/ed\\_auth\\_connection\\_instructions.pdf](http://www.middleware.vt.edu/pubs/ed_auth_connection_instructions.pdf)). The basic method is to search for the user by uupid and bind as the returned DN with the user's password.

Q: How can I authorize on affiliation?

A: The most straightforward way to authorize based on affiliation is to do an LDAP compare operation for eduPersonAffiliation on a connection that has been bound as the user you are authorizing. Another way is to do an LDAP search operation on the bound user's entry for the desired affiliation. (need examples package)

Q: Why can't I see any user information?

A: In ED-Auth, if you bind anonymously (without username or credentials), you can only see a person's DN, uupid, and objectclass. This is to keep confidential information confidential. To see a person's affiliations, you must bind as that user. In other words, it is only possible for a bound user to see their own affiliations. Please note that the only real data available in ED-Auth is the uid, uupid, eduPersonAffiliation(s), and userPassword (not visible). ED-Auth does not contain names, major, department, etc. See the ED-Auth schema at ([http://www.middleware.vt.edu/pubs/ed\\_auth\\_schema.pdf](http://www.middleware.vt.edu/pubs/ed_auth_schema.pdf)).

Q: Whose affiliations can I see?

A: See previous answer. In short, a user is only allowed to see their own affiliations after they have been bound as themselves.

Q: How do I connect to ED-Auth?

A: See the ED-Auth Usage Instructions at

([http://www.middleware.vt.edu/pubs/ed\\_auth\\_connection\\_instructions.pdf](http://www.middleware.vt.edu/pubs/ed_auth_connection_instructions.pdf)). Please note that you must connect to ED-Auth over an encrypted connection, that is, over ldaps (ldap over SSL), or by upgrading your connection by using startTLS.

Q: Is PID/pass authentication really binding as PID/pass?

A: Not exactly, but we use this term generically. What is really taking place is a search on a person's UUPID that returns a DN, and then a bind with that DN and the user's password.

=====

=====

ED-ID:

Q: What is ED-ID?

A: ED-ID is an LDAP directory designed to allow applications easy programmatic access to data needed for authentication, authorization, application personalization and customization, and programmatic business decision evaluation.

Q: What data is contained in ED-ID?

A: See the ED-ID schema at ([http://www.middleware.vt.edu/pubs/ed\\_id\\_schema.pdf](http://www.middleware.vt.edu/pubs/ed_id_schema.pdf)). ED-ID contains all the attributes in ED-Lite and ED-Auth, plus additional authorization and personal data.

Q: What types of things should ED-ID be used for?

A: ED-ID exists primarily as an authorization directory used by applications to look up such things as a person's virginiaTechID, bannerPIDM, department, major, etc. ED-ID can also be used for PID/pass authentication in the same way as ED-Auth. Basically, if you need to get to user data, ED-ID is the one-stop shop for you. ED-ID services have the ability to look up information about a person, even if that person has been marked as confidential.

Q: How do I see data in ED-ID?

A: What you see in ED-ID is dependent on how you bind (anonymous, simple, SASL EXTERNAL) and the amount of privileges the bound user has. Connecting to ED-ID requires the use of TLS client certificate authentication, meaning you must have a signed certificate from the Virginia Tech Middleware CA (<http://vtmwra.eprov.iad.vt.edu>) in order to connect. Users bound anonymously can only search on uupid and can only see the DN (distinguished name) of any user. Users that have performed a simple bind as themselves (PID/pass) can only see their own objectclass, uupid, uid, and eduPersonAffiliation(s). Users that have performed a SASL EXTERNAL bind can only see

those attributes they have been approved to see (for all users), and only if the corresponding service is ACTIVE.

Q: What is a client certificate?

A: A client certificate is an X.509 certificate that is used for authentication during TLS negotiation. A client certificate signed by the VT Middleware CA is required to connect to ED-ID.

Q: What is SASL?

A: SASL stand for Simple Authentication and Security Layer, a framework for providing protocols (SMTP, IMAP, LDAP) a means to authenticate.

Q: What is SASL EXTERNAL?

A: SASL EXTERNAL, the SASL mechanism ED-ID uses, authenticates based on lower level network services, which in this case is TLS client certificate authentication. This means a client certificate is used to authenticate to ED-ID and is used to determine the username, or ED-ID service name.

Q: What is a SASL bind?

A: A SASL bind simply uses SASL to authenticate to an LDAP server. For ED-ID, a SASL EXTERNAL bind is performed.

Q: What is an ED-ID service?

A: An ED-ID service is a privileged user of ED-ID that has been approved to see certain user attributes. Typically, an application binds to ED-ID as its service to obtain authorization information about a particular user.

Q: What is the VT Middleware CA?

A: The VT Middleware CA is a subordinate CA of the VT Root CA that signs ED-ID service certificates. To connect to ED-ID you need a client certificate signed by this Certification Authority.

Q: What attributes can a service see?

A: A service can see only those attributes they have been approved to view, which correspond to the "viewablePersonAttribute" in a service's ED-ID entry. A service can view its viewablePersonAttribute (s) by searching on the ED-ID branch "ou=services,dc=vt,dc=edu". Attributes a service can see are chosen during the ED-ID registration process. Narrowing down the viewable attributes allows us to give snapshots of entries, and assures that we do not expose any more data than is needed by any given application.

Q: What is the difference between authentication and authorization?

A: Authentication is confirming the identity of a user, while authorization is determining if a user has the proper rights or permissions to access a resource.

Q: How fast is ED-ID?

A: A typical ED-ID query can be broken down as follows:

connect, TLS client certificate auth, SASL BIND: 0.072 seconds

search on exact uupid, return entry: 0.002 seconds

The most time consuming part of interfacing with ED-ID is the TLS client certificate authentication, but after this connection overhead, search times are blazingly fast. Indexing of attributes has also been used extensively in ED-ID to ensure fast searching.

Q: Why should I use persistent connections to ED-ID?

A: Due to the connection overhead of using TLS client certificate authentication, persistent connections are recommended when interfacing with ED-ID. Applications that use persistent connections do not have to renegotiate TLS, so access to data in ED-ID is that much faster.

Q: If I lose or expose my service's key (client key), could someone get access to ED-ID?

A: Your client key is meant to be kept ABSOLUTELY PRIVATE. Safeguards should be put in place such that no one other than you can have access to your client key. If your client key were to get in the hands of another person, they would be able to connect to ED-ID as your service. If we know of the exposure, we can turn off the ED-ID service account that corresponds to the certificate. This will effectively shut off access for this certificate. If your client key is lost or compromised, it is your responsibility to notify us as soon as possible to prevent possible exposure of data.

Q: Where do I get my certificate for ED-ID?

A: Signed certificates are available for download from (<http://vtmwra.eprov.iad.vt.edu>).

Q: How long is my certificate valid?

A: Your certificate is valid for one year. It is your responsibility to renew your certificate after this time. Failure to renew your certificate will result in the inability to connect to ED-ID.

Q: Can I view confidential data with ED-ID?

A: Yes. If your service has been approved to see confidential data, ED-ID will allow you to view those attributes.

Q: Is ED-ID's data up-to-date?

A: Replication from the Registry takes place in near real time. The data in ED-ID is current.

Q: Can my service update data in ED-ID?

A: Currently, no. Middleware may provide the ability to update certain data in ED-ID in the future, but this access will most likely be extremely limited.

Q: Data that I want is not contained in ED-ID. What should I do?

A: If the data makes sense in an ED-ID world and is useful, there is the chance the ED-ID schema can be extended. Contact Middleware and IRM to begin discussion. Future enhancements may include better degree/major information and current class information for students. ED-ID has been designed to be extensible for these sorts of enhancements.

Q: Can I request a service that can only see people in a certain department?

A: Currently, no. Middleware is developing a feature in ED-ID that will allow you to specify which affiliation, campus, major, and department you wish to view, and the overall relationship between these attributes (intersection or union). When that is in production, this sort of thing will be possible.

Q: What about users with tenuous affiliation with VT?

A: These issues are currently being worked out by our busy policy makers. New affiliations are on the horizon to accommodate these sorts of things.

Q: I only need to use PID/pass authentication. Should I use ED-ID?

A: No, ED-Auth is better suited for PID/pass authentication. If you only need this, ED-Auth is recommended. ED-ID supports PID/pass authentication, but you still must get a client certificate to connect.

Q: What programming languages can you use to connect to ED-ID?

A: Any language that has the capability to do LDAPv3 things, namely TLS client certificate authentication and SASL binding, can connect to ED-ID. Middleware provides examples for Java, C/C++ (including WinLDAP), and Perl.

Q: Can I do PID/pass authentication with ED-ID?

A: Absolutely, but if this is all you need ED-ID for, we highly recommend using ED-Auth.

Q: What should my ED-ID service name be?

A: Your ED-ID service name should be something descriptive,

preferably in the form "department-application". For instance, suppose the Library would like to use ED-ID for their proxy needs. A suitable ED-ID service name would be: "library-proxy".

=====