IdPSkills

Operation of a Shibboleth IdP in production benefits from a broad set of skills. Many of the below are general software questions that would be applicable for operation of any high-availability Java servlet, and some of them are specifically oriented towards the security functionality that is leveraged by Shibboleth.

This is not a mandatory nor critical list; instead, it's meant to serve as a good reference guide for anyone who wants to learn what it takes to really run an IdP smoothly.

Specific software skills:

- A thorough understanding of Java
    - How classloading works
    - What endorsement is, how it works, and why it's important
    - The Java memory model and what type of JVM parameters are associated with it
    - How Java threads map to system threads and what type of JVM parameters are associated with this
    - The difference between the Java key management and trust management mechanisms
- A thorough understanding of `<insert your web app container name here>` (e.g. Tomcat)
    - How classloading is performed by the container
    - How the container handles/routes requests
    - The threading model used by the container and its configuration
- Some LDAP and relational database knowledge; extensive knowledge is not needed, since the IdP operator generally relies upon rather than operates these systems

General technical skills:

- How network and low-level internet services work (things like DNS, NTP)
- How SSL/TLS works
    - The way that TLS uses both asymmetric and symmetric keys
    - The difference between validating a certificate and trusting it
    - How TLS client authentication differs from server authentication
- How HTTP works
    - An understanding of what HTTP redirects really are
    - An understanding of what an HTTP POST request looks like on the wire
    - A familiarity with the rest of HTTP, and not just its most common methods
- How web applications create, persist, and use sessions
    - Can you explain why cookies are the least bad mechanism for session reference?
    - Can you explain ways to decrease the chances that your session gets hijacked?
- How digital signature and encryption work; XML digital signature and encryption aren't dramatically different from signature and encryption of other data types for deployers
- Experience with other SSO solutions is a helpful foundation, but not necessary
- Since Shibboleth is open-source, an ability to trace and read code can help with debugging, understanding, and operation

Personal skills:

It's important for anyone operating an IdP to understand the importance and nature of the job. Enterprise identity information comes from a lot of sources, goes to a lot of applications, and is often highly sensitive and personal. Many stakeholders need to be participants in the process to make sure that everyone is comfortable and policies are adhered to. Users' data needs to be treated with great respect and caution and released only when necessary.

As operator of an identity management system, your purpose is to serve and help applications that rely on you for critical information. Without your service available, it's impossible for the application to function. Shibboleth is just plumbing.