IDM-17: Obtain a high-assurance X.509 certificate for accessing a service that requires one

A **community member** needs to obtain a high-assurance X.509 identity certificate in order to access a service that uses high-assurance X.509 certificates for authentication. These certificates are required by some services (e.g., remote login, data, compute) in the European Grid Infrastructure (EGI).

In most cases, the researcher expects it to work as follows.

1. First, the community member opens a web browser and visits the community's certificate-issuing service.
2. Then, the community member authenticates using his/her community identity. (The community member may need to select the community from a list of options.)
3. Then, the community member downloads the resulting certificate, which is now available for use with services that require it.

We'll accept any solution as long as the following are true.

1. The community member can complete this use case using any device with a standard (up-to-date) web browser.
2. In Step 2, it must be possible for the community member to use an identity issued by the community (e.g., username and password) to authenticate.
3. In Step 3, the certificate satisfies the IGTF MICS/BIRCH level of assurance.

SPI-13: Configure a service to allow or require a high-assurance X.509 certificate for user access

A service provider needs to configure a service to allow or require a high-assurance X.509 certificate for user access so that the user authentication process is assured to satisfy the IGTF "MICS/BIRCH" level of assurance. Some service providers are required to have this assurance for their systems. We assume the service already supports X.509 authentication.

In most cases, the service provider expects it to work as follows.

1. The service provider visits the community's documentation for service providers and locates the documentation on high-assurance X.509 certificates.
2. The service provider follows the documentation's instructions for configuring a service's X.509 authentication to either allow or require a high-assurance certificate issued by the community's certificate-issuing service.

We'll accept any solution as long as the following are true.

1. In Step 2, the instructions should be consistent with widely-used X.509 authentication configuration practices (e.g., signing policy files, root certificate distribution mechanisms).