Shibboleth IDP : choisir un CAS en fonction du SP

- Si vous utilisez l'IDP Shibboleth et shib-cas-authn pour déléguer l'auth à un CAS
- Et si vous avez un CAS "mot de passe" et un CAS MFA (notamment esup-otp-cas-server)

Il peut-être utile de choisir le CAS en fonction de l'application.

Pour cela :

Modifier shib-cas-authn

Une petite modif sur shib-cas-authn : "allow multiple ShibcasAuthServlet with different conf", cf https://github.com/UnivParis1/shib-cas-authn

Modifier idp.properties

```
# since we decide which CAS to use dynamically, we can not cache the result
# (otherwise the first succesful CAS login will be kept)
# (alternative is to use "idp.session.enabled = false" but you loose SLO)
# (require https://github.com/Unicon/shib-cas-authn/pull/8)
shibcas.doNotCache = true

shibcasotp.casServerUrlPrefix = https://cas-test.univ-paris1.fr/otp
shibcasotp.casServerLoginUrl = ${shibcasotp.casServerUrlPrefix}/login
shibcasotp.serverName = ${shibcas.serverName}
shibcasotp.ticketValidatorName = ${shibcas.ticketValidatorName}
shibcasotp.doNotCache = ${shibcas.doNotCache}
# to allow cas/otp to decide to force OTP or not:
# (require a fix in shib-cas-authn to work with esup-otp-cas-server)
shibcasotp.entityIdLocation=embed
```

Modifier conf/authn/external-authn-config.xml

```
    <bean id="shibboleth.authn.External.externalAuthnPathStrategy"
parent="shibboleth.ContextFunctions.Scripted"
factory-method="resourceScript"
        c:_0="%{idp.home}/conf/choose-cas.js" />
```

Modifier webapp/WEB-INF/web.xml

```
    <servlet>
        <servlet-name>ShibCasOtp Auth Servlet</servlet-name>
        <servlet-class>net.unicon.idp.externalauth.ShibcasAuthServlet</servlet-class>
        <init-param>
            <param-name>idp_properties_prefix</param-name>
            <param-value>shibcasotp</param-value>
        </init-param>
        <load-on-startup>2</load-on-startup>
    </servlet>
    <servlet-mapping>
        <servlet-name>ShibCasOtp Auth Servlet</servlet-name>
        <url-pattern>/Authn/ExternalOtp/*</url-pattern>
    </servlet-mapping>
```

Créer conf/choose-cas.js

```
var url = "contextRelative:Authn/External";
var rpCtx = input.getSubcontext("net.shibboleth.idp.profile.context.RelyingPartyContext");
if (rpCtx != null) {
    var rpid = rpCtx.getRelyingPartyId();
    if (rpid === "https://pass.renater.fr" || rpid === "https://registry.federation.renater.fr" || rpid ===
"https://cert-manager.com/shibboleth") {
       var logger = Java.type("org.slf4j.LoggerFactory").getLogger("net.shibboleth.idp.PRI");
       logger.warn("forcing ExternalOtp for {}", rpid);
       url = "contextRelative:Authn/ExternalOtp"
    }
}
url;
```

NB : il faut redémarrer shibboleth IDP pour prendre en compte les modifs de conf/choose-cas.js