通常在登录web2服务时，我们需要使用用户名或电子邮件地址和密码。然后，该服务可以在他们的内部数据库中查找我们的用户名或电子邮件地址，看看相应的密码是否与我们提供的密码匹配。生成用于进一步身份验证的随机密钥，通常存储在cookie中。

然而，一个新的规范EIP-4361：用以太坊登录，希望通过使用web3服务(如钱包和dapps)常用的方法来改变我们登录web2服务的方式。

这份规范描述了使用签名消息的现有web2服务的身份验证方法。用户可以使用自己的私钥(带有相应的地址)进行身份验证，而不是使用用户名和密码的组合。这样，就不需要再把敏感信息储存在web2服务的数据库中，提高了用户数据的安全性。

具体来说，EIP-4361使用增强的Backus-Naur表单(ABNF)为这些身份验证消息定义了一种标准化格式，想要登录的服务可以对这些消息进行验证。该格式遵循EIP-191规范，该规范已经得到许多钱包的广泛支持。登录不需要密码，只需用私钥对消息进行签名，就完成了。服务器可以验证消息并生成密钥存储在cookie中。

除此之外，EIP-4361还与以太坊名称服务(ENS)集成，可用于控制自己的数据。如果一个地址有一个主ENS名称(也称为反向记录)集，服务可以查找这个主ENS名称并基于它解析数据。例如，可以将自己的首选用户名、头像、电子邮件地址或其他任意信息存储在ENS名称中。ENS还允许用户指定其他网络的地址，如比特币和莱特币。这样就可以控制自己的数据，并且不需要web2服务来存储关于用户的这些信息。

这个模型本质上是一个去中心化的、100%正常运行的、用户数据所有的Gravatar。数据不是由一个私有实体持有，而是发布到以太坊区块链供应用程序使用。用户将在多个应用程序中拥有一个身份，所有应用程序都通过用户的签名钱包进行身份验证。未来，这种经过身份验证、签名的EIP-191消息登录到身份验证的应用程序可能会成为标准，使电子邮件/密码组合的登录方式逐渐淘汰。