x.1255协议白皮书

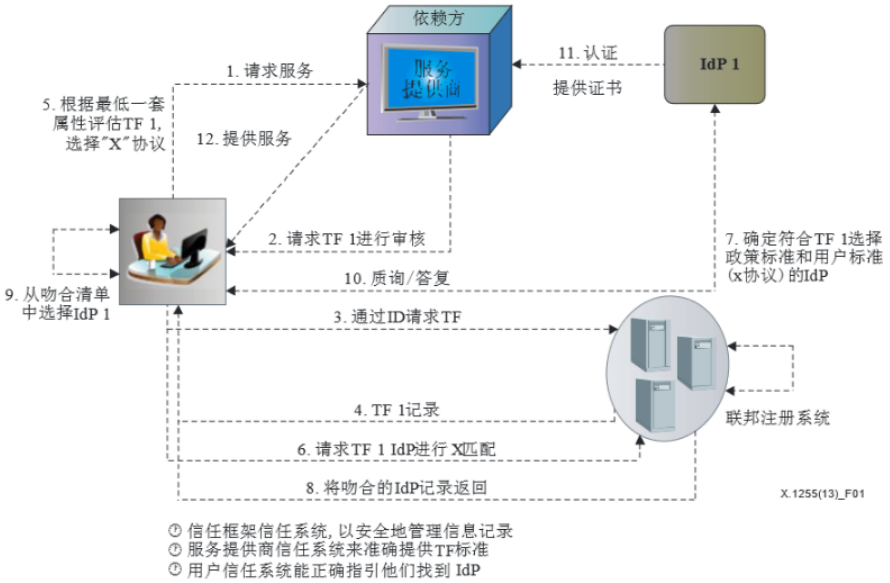
前言

DOA IdM尝试实现

方案概述

- 定义
  - IdM 身份管理
  - IdP 身份提供商
- 实现模式
  - 步骤1：在该示例中，最终用户要求使用依赖方服务。
  - 步骤2：依赖方以RP信任的一个或多个信任框架身份做出答复，在此情况下为一个框架（TF1）。
  - 步骤3：终用户利用TF1识别符到系统中去。
  - 步骤4：系统以TF1的相关记录做出答复。有关TF1的信息包括在框架中得到信任的低限度 属性。
  - 步骤5：终用户对这些低要求做出评估，以确定是否能够获得RP的信任。在此我们假设 终用户通过评估做出正面回应，并表明终用户可满足低属性，如，驾照。
  - 步骤6：此时终用户可回到系统中，请求使用属于TF1且满足终用户支持的协议（如 HTTP和电子邮件）要求的IdP，在此我们仅简单地将其表示为X协议。
  - 步骤7：系统找出TF1与X协议相匹配的身份提供商（IdP）。
  - 步骤8：系统以一系列符合依赖方和终用户要求的IdP向终用户做出答复。
  - 步骤9：终用户对由系统返回的这一系列IdP做出评估，并做出选择（IdP1）。
  - 步骤10：拥有IdP所需属性且使用IdP1理解的协议的终用户参与与IdP1进行的质询/答复互动。
  - 步骤11：成功的质询/答复互动会使IdP1提供对RP证书的认证。

- 步骤12：信任终用户的依赖方现在可以提供所请求的服务。



图I.1 – 涉及信任框架的认证

- 实现思想
  - 服务通信
    - 在TCP协议上层确立新协议，此协议对应实现模式中第12步。即在提供服务中，数据报在TCP首部下确定新协议首部，假设新协议为X，服务通信中通过使用x协议首部进行通信，首部信息包含用户ID以确认用户身份。
  - 身份验证
    - 用户与服务商确定唯一的注册系统TF，此TF与用户、服务商共同确立得出身份提供商IdP，IdP对用户质询若满足条件则向服务提供商发送用户ID，使服务商注册表添加用户信息。