ICS 35.100.01
L 79

中华人民共和国国家标准

GB/T 18794.2—2002
idt ISO/IEC 10181-2:1996

信息技术　开放系统互连
开放系统安全框架
第2部分:鉴别框架

Information technology—Open Systems Interconnection—Security frameworks for open systems—Part 2:Authentication framework

2002-07-18 发布　　2002-12-01 实施

中华人民共和国
国家质量监督检验检疫总局　发布

目　　次

前　言

本标准等同采用国际标准 ISO/IEC 10181-2:1996《信息技术　开放系统互连　开放系统安全框架:鉴别框架》。

GB/T 18794 在《信息技术　开放系统互连　开放系统安全框架》总标题下,目前包括以下几个部分:

第 1 部分(即 GB/T 18794.1):概述

第 2 部分(即 GB/T 18794.2):鉴别框架

在 ISO/IEC 10181-2 中缺 5.2.3 条,因此,将原标准的 5.2.4～5.2.8 条分别改为本标准的 5.2.3～5.2.7 条。

本标准的附录 A 至附录 G 都是提示的附录。

本标准由中华人民共和国信息产业部提出。

本标准由中国电子技术标准化研究所归口。

本标准起草单位:信息产业部电子第十五研究所。

本标准主要起草人:张莺、王雨晨、杜春燕、周珍妮。

ISO/IEC 前言

ISO(国际标准化组织)和 IEC(国际电工委员会)是世界性的标准化专门机构。国家成员体(他们都是 ISO 或 IEC 的成员国)通过国际组织建立的各个技术委员会参与制定针对特定技术范围的国际标准。ISO 和 IEC 的各技术委员会在共同感兴趣的领域内进行合作。与 ISO 和 IEC 有联系的其他官方和非官方国际组织也可参与国际标准的制定工作。

对于信息技术,ISO 和 IEC 建立了一个联合技术委员会,即 ISO/IEC JTC1。由联合技术委员会提出的国际标准草案需分发给国家成员体进行表决。发布一项国际标准,至少需要 75%的参与表决的国家成员体投票赞成。

国际标准 ISO/IEC 10181-2 是由 ISO/IEC JTC1"信息技术"联合技术委员会的 SC21"开放系统互连、数据管理和开放分布式处理"分技术委员会与 ITU-T 共同制定的。等同文本为 X.811。

ISO/IEC 10181 在《信息技术　开放系统互连　开放系统安全框架》总标题下,目前包括以下七个部分:

——第 1 部分:概述
——第 2 部分:鉴别框架
——第 3 部分:访问控制框架
——第 4 部分:抗抵赖框架
——第 5 部分:保密性框架
——第 6 部分:完整性框架
——第 7 部分:安全审计和告警框架

本标准的附录 A 至附录 G 仅提供参考信息。

引　言

很多应用具有安全需求以防范信息通信中遇到的威胁。一些共识的威胁及对付这些威胁可以使用的安全服务和机制在GB/T 9387.2中描述。

很多开放系统应用具有安全需求，具体需求依赖于正确识别应用所包含的主角。这些需求可能包括防止未经授权的访问以保护财产和资源，基于访问控制机制的身份鉴别可用于这种情况，和/或强制实施保持相关活动的审计日志，以用于记录和告诫目的。

确认身份的过程称为鉴别。本标准定义了鉴别服务规定的一般框架。

中华人民共和国国家标准

信息技术　开放系统互连 开放系统安全框架 第2部分：鉴别框架

GB/T 18794.2—2002
idt ISO/IEC 10181-2:1996

Information technology—Open Systems Interconnection—Security frameworks for open systems—Part 2:Authentication framework

1　范围

关于开放系统安全框架的本标准系列涉及在开放系统环境中的安全服务应用，术语“开放系统”系指包括诸如数据库、分布式应用、开放分布式处理和OSI一类的领域。安全框架主要用来提供在系统内和系统间交互时对系统和客体的保护方法。安全框架不考虑用于构造系统或者机制的方法学。

安全框架涉及用于获取具体安全服务所使用的数据元素和操作序列(但不是协议元素)。这些安全服务可适用于系统的通信实体，也可以用于系统间交换的数据和由系统管理的数据。

本标准：

——定义鉴别的基本概念；

——确定可能的鉴别机制类；

——定义用于这些鉴别机制类的服务；

——确定为支持这些鉴别机制类的协议的功能需求；

——确定鉴别的通用管理需求。

能够使用本框架的标准类型包括：

1) 符合鉴别概念的标准；

2) 提供鉴别服务的标准；

3) 使用鉴别服务的标准；

4) 规定在开放系统体系结构内提供鉴别手段的标准；

5) 规定鉴别机制的标准。

注：2)、3)和4)中的服务可以包括鉴别，但可以具有不同的初衷。

上述标准能以下列方式使用本框架：

——标准类型1)、2)、3)、4)和5)能够使用这个框架的术语；

——标准类型2)、3)、4)和5)能够使用本框架第7章定义的服务；

——标准类型5)能够基于本框架第8章定义的机制。

正如其他安全服务一样，鉴别只能够在为特定应用所定义的安全政策的上下文中被提供。安全政策的定义不属于本标准的范围。

本标准的范围不包括为取得鉴别所需执行的协议交换细节的规范。

本标准不规定用于支持这些鉴别服务的特定机制。其他标准(如GB/T 15843)更详细地制定了具体的鉴别方法。此外，这类方法的例子被收编在其他标准中(如GB/T 16264.8)以便涉及具体的鉴别需求。

中华人民共和国国家质量监督检验检疫总局2002-07-18批准　　2002-12-01实施

本框架中所描述的某些规程通过应用密码学技术来达到安全性。尽管某些鉴别机制类可以依赖于特定的算法特性，例如非对称特性，但本框架的使用不依赖于特定密码或者其他算法。

注：尽管 ISO 不对密码学算法进行标准化，但在 ISO/IEC 9979 中对用于注册算法的规程进行了标准化。

2 引用标准

下列标准所包含的条文，通过在本标准中引用而构成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 9387.2—1996 信息处理系统 开放系统互连 基本参考模型 第 2 部分：安全体系结构 (idt ISO/IEC 7498-2:1989)

GB/T 17964—2000 信息技术 安全技术 n 比特块密码算法的操作方式(idt ISO/IEC 10116:1997)

GB/T 18794.1—2002 信息技术 开放系统互连 开放系统安全框架 第 1 部分：概述(idt ISO/IEC 10181-1:1996)

ISO/IEC9979:1991 信息技术 加密技术 密码算法登记规程

3 术语和定义

本标准采用 GB/T 9387.2 中定义的下列术语：

——审计 audit；
——审计跟踪 audit trail；
——鉴别信息 authentication information
——保密性 confidentiality；
——密码学 cryptography；
——密码校验值 cryptographic checkvalue；
——数据源鉴别 data origin authentication；
——数据完整性 data integrity
——解密 decipherment
——数字签名 digital signature；
——加密 encipherment；
——密钥 key；
——密钥管理 key management；
——冒充 masquerade；
——口令 password；
——对等实体鉴别 peer-entity authentication；
——安全政策 security policy；

本标准采用在 GB/T 17964 中定义的下列术语：

——块链接 block chaining

本标准采用 GB/T 18794.1 中定义的下列术语：

——数字指纹 digital fingerprint；
——散列函数 hash function；
——单向函数 one-way function；
——私有密钥 private key；
——公开密钥 public key；
——封印 seal

——**秘密密钥** secret key；

——**安全机构** security authority；

——**安全证书** security certificate；

——**安全域** security domain；

——**安全权标** security token；

——**信任** trust；

——**可信第三方** trusted third party。

本标准定义下列术语：

3.1 **非对称鉴别方法** asymmetric authentication method

并非所有鉴别信息都由双方实体共享的一种鉴别方法。

3.2 **已鉴别的身份** authenticated identity

通过鉴别保证的主角的可区分标识符。

3.3 **鉴别** authentication

提供对于某个实体自称身份的保证。

3.4 **鉴别证书** authentication certificate

由鉴别机构担保的并且可以被用于保证某个实体身份的安全证书。

3.5 **鉴别交换** authentication exchange

一个或者多个用于执行鉴别目的的交换鉴别信息(AI)的传送序列。

3.6 **鉴别信息** authentication information

用于鉴别目的的信息。

3.7 **鉴别发起方** authentication initiator

发起鉴别交换的实体。

3.8 **盘问** challenge

由验证者生成的时间变量参数。

3.9 **申请鉴别信息(申请 AI)** claim authentication information(claim AI)

由申请者用于生成为鉴别某个主角所需要的交换 AI 的信息。

3.10 **申请者** claimant

本身就是或代表用于鉴别目的的主角的实体。申请者包括为代表主角从事鉴别交换所必须的函数。

3.11 **可区分标识符** distinguishing identifier

在鉴别过程中无歧义地区分实体的数据。本标准要求这类标识符至少在安全域内是无歧义的。

3.12 **交换鉴别信息(交换 AI)** exchange authentication information(exchange AI)

鉴别主角过程中在申请者和验证者之间交换的信息。

3.13 **离线鉴别证书** off-line authentication certificate

关联了可区分标识符到验证 AI 的鉴别证书，可能对所有实体都可用。

3.14 **在线鉴别证书** on-line authentication certificate

由申请者直接从担保它的机构获得的用于鉴别交换的鉴别证书。

3.15 **主角** principal

其身份能够被鉴别的实体。

3.16 **对称鉴别方法** symmetric authentication method

双方实体共享公共鉴别信息的一种鉴别方法。

3.17 **时间变量参数** time variant parameter

由实体用于验证某个报文不是一个重发报文的数据项。

3.18 **唯一编号** unique number

由申请者生成的时间变量参数。

3.19 验证鉴别信息(验证 AI) verification authentication information(verification AI)

由验证者用于验证通过交换 AI 所声称的身份的信息。

3.20 验证者 verifier

本身就是或者代表要求鉴别身份的实体。验证者包括从事鉴别交换所必须的函数。

4 缩略语

本标准定义下列缩略语:

AI 鉴别信息(Authentication Information)

OSI 开放系统互连(Open Systems Interconnection)

5 鉴别的概述性讨论

5.1 鉴别的基本概念

鉴别提供了对某个实体自称身份的保证。鉴别仅在主角和验证者关系的上下文中才有意义。两个重要的案例是:

——主角由某个与验证者具有某种具体通信关系的申请者所代表(实体鉴别);

——主角是验证者可用的数据项的源(数据源鉴别)。

本标准区分这两种形式的鉴别。

实体鉴别在通信关系的上下文中提供主角身份的证明。主角的可鉴别身份仅当这种服务被引用时才被保证。鉴别连续性的保证可以按 5.2.7 中所描述的方式获取。例如 GB/T 9387.2 中定义的 OSI 对等实体鉴别。

数据源鉴别提供负责具体数据单元的主角身份的证明。

注

1 当使用数据源鉴别时,还必须具有关于数据未曾被修改过的适当保证。这可以通过使用完整性服务实现。例如:

a) 使用数据不能被篡改的环境;

b) 验证所接收的数据匹配所发送数据的数字指纹;

c) 使用数字签名机制;

d) 使用对称密码学算法。

2 定义实体鉴别中使用的术语通信关系可以被广义地解释和能够被引用,例如:OSI 连接、进程间通信或用户和终端间的交互。

5.1.1 身份和鉴别

主角是其身份能够被鉴别的实体。主角具有一个或多个与其相关联的可区分标识符。鉴别服务可以被实体用于验证主角身份。已被验证的主角身份称为已鉴别的身份。

能够被识别并因此能够被鉴别的主角的例子包括:

——人类用户;

——进程;

——实开放系统;

——OSI 层实体;

——企业。

可区分标识符必须在给定的安全域内无歧义性。可区分标识符以下列两种方式之一,区分在一个相同的域中的不同主角与在相同域中的其他主角:

——在粗粒度级别上,依靠在鉴别方面被认为是等价的一组实体的成员关系(在此情况下整个组被认为是一个主角并且具有可区分标识符);

——在最细粒度等级上，只标识一个实体。

当鉴别发生在不同的安全域实体之间时，可区分标识符可能不足以无歧义地标识一个实体，因为不同的安全域机构可能使用相同的可区分标识符。在此情况下，可区分标识符必须与安全域的标识符联合使用以便为实体提供一个无歧义性的标识符。

可区分标识符的典型例子有：

——目录名(GB/T 16264.8)；

——网络地址(GB/T 15126)；

——AP 标题和 AE 标题(GB/T 17176)；

——客体标识符(GB/T 16262)；

——人名(在域的上下文内无歧义)；

——护照或社会安全号。

5.1.2 鉴别实体

术语“申请者”被用于描述其本身就是或者代表用于鉴别目的的主角的实体。申请者包括代表主角为从事鉴别交换所必须的函数。

术语“验证者”被用于描述其本身就是或者代表要求鉴别身份的实体。验证者包括从事鉴别交换所必须的函数。

参与双向鉴别(见 5.2.3)的实体将被认为既担当申请者又担当验证者角色。

术语“可信第三方”被用于描述安全机构或者其代理，这些安全机构或者其代理是由参与安全相关活动的其他实体所信任的。在本标准的上下文中，可信第三方是由用于鉴别目的的申请者和/或验证者所信任的。

注：申请者或验证者可以被细化为多重功能部件，可能驻留于不同的开放系统中。

5.1.3 鉴别信息

鉴别信息的类型有：

——交换鉴别信息(交换 AI)；

——申请鉴别信息(申请 AI)；

——验证鉴别信息(验证 AI)；

术语鉴别交换被用于描述一个或者多个用于执行鉴别目的的交换鉴别信息(AI)的传送序列。

图 1 说明了申请者、验证者和可信第三方之间的关系以及鉴别信息的三种类型。

在某些情况下，为生成交换 AI，申请者可能需要与可信第三方交互。类似地，为验证交换 AI，验证者可能需要与可信第三方交互。在这些情况下，可信第三方可以保存与主角相关的验证 AI。

可信第三方还可能被用于交换 AI 的传送。

实体也可能需要保存将被用于鉴别可信第三方的鉴别信息。

三种类型鉴别信息的例子在 6.1 中给出。

注：因为术语凭证在其他标准中并非总是以一致的方式使用，因此本安全框架不使用这个术语。GB/T 9387.2 所定义的术语凭证可能被当作交换 AI 的例子。

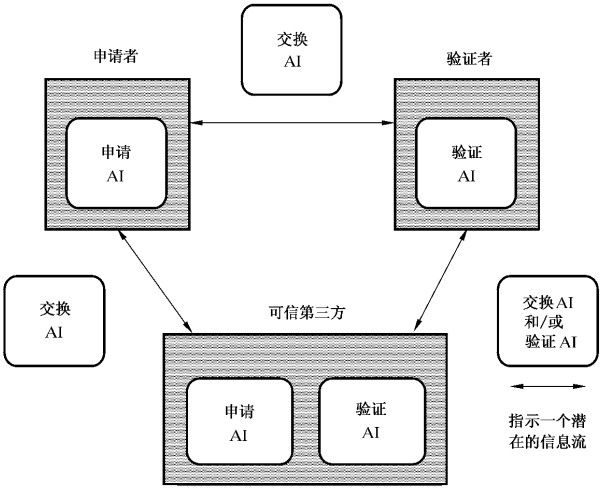
5.2 鉴别服务的有关方面

5.2.1 对鉴别的威胁

鉴别的目标在于提供主角身份的保证。提供鉴别的机制通常必须消除冒充和重发威胁。

冒充系指一个实体作为另一个不同的实体出现。也就是说，实体以特定的方式(例如：通过数据源或通过通信关系)装作与验证者相关的另一个实体。这些类型包括重发、中继和申请 AI 泄露。

冒充威胁发生在由申请者或验证者发起的活动(例如：通过数据源或通过通信关系)的上下文中。防止对于某个活动的冒充威胁要求使用关联这些数据项与鉴别交换的完整性服务。为对抗与冒充相关的威胁，鉴别必须与某种形式的完整性服务一起使用，这样就把被鉴别的身份与这个活动关联起来。



注

1 在某些情况中不包括可信第三方；

2 验证 AI 可能是主角的 AI 或者可信第三方的 AI(详见 5.5)

图 1 申请者、验证者和可信第三方之间关系以及鉴别信息类型的说明

重发系指交换 AI 的重复，以产生非授权的效果。重发通常与其他攻击组合使用，诸如数据修改。并非所有鉴别机制都同等地能抗御重发。重发能够威胁其他安全服务。鉴别能够用于对抗重发，因为它提供了确定被交换信息的来源的手段。

5.2.2 鉴别转发

在某些情形下，主角可以具有在某个系统之内间接行事的要求。在此情况下，主角在该系统内的表示将必须被创建。此外，主角在该系统内的表示被创建之前，主角必须被鉴别。

当代表该主角行事时，代替主角身份的表示将被鉴别。由于主角的表示好似其作为主角本身一样行事，因而主角的行为能够在该系统内被执行而无需主角直接参与。其例子见附录 A。

当主角是人类用户时，可以使用这样的机制，即把该表示的生命期限制在该用户在特定位置实际出现的时间段内。

在代表主角行事中，申请者可以访问另一个在鉴别之后创建了其自己的主角表示的系统。这个表示的创建被称之为鉴别转发。

以这种方式转发鉴别的能力可能为安全政策所影响。

5.2.3 单向和双向鉴别

鉴别可以是单向或双向的。单向鉴别仅提供一个主角身份的保证。双向鉴别提供双方主角身份的保证。

实体鉴别可以是单向或双向的。就其本质而言，数据源鉴别总是单向的。

5.2.4 鉴别交换的发起

鉴别交换可以由申请者或验证者发起。开始交换的实体被称之为鉴别发起者。

5.2.5 鉴别信息的撤消

鉴别信息的撤消系指验证 AI 的永久性失效。

政策可以要求在特定情形下的鉴别信息撤消。撤消鉴别信息的决定可以基于检测到安全违规事件，政策的更改或其他原因。鉴别信息的撤消可以或不可以隐含现有访问的撤消，或具有其他引出效果。

此外，可以采取下列与管理相关的动作：

a）在审计跟踪中记录事件；

b）事件的本地报告；

c）事件的远地报告；

d）拆除通信关系的连接。

对于每个事件所采取的具体动作依赖于所执行的安全政策和与通信关系状态相关的其他因素，例如：当主角被登录和活动时是否发生了更新。

5.2.6 鉴别连续性的保证

实体鉴别仅提供一瞬间的身份保证。获取鉴别连续性的保证的一种方式是通过链接鉴别服务和数据完整性服务。

当主角最初使用鉴别服务来被鉴别并且使用完整性服务使更多的代表主角被发送的数据与交换AI被关联在一起时，鉴别服务和完整性服务则称之为被链接。这确保了后来的信息不被任何其他实体篡改，因此必须来自于最初被鉴别的主角。重要的是完整性服务是在信息从该主角到验证者经过的整个路径上提供。例如：如果其中某些信息能够由未被鉴别的主角产生，则可能是冒充。

获取后来出现的仍然是相同的远地实体保证的另一种方式是不断执行进一步的鉴别交换。然而，这样不能防止间歇期间的入侵，因此无法获取连续性的保证。例如：下列攻击是可能的：某个入侵者，当被调用进行进一步鉴别时，允许有效的一方进行鉴别动作；在这些动作完成之后，该入侵者再次接管。

如果完整性机制要求密钥，该密钥可以从在鉴别交换期间所规定的参数中派生出来。由于确立了密钥是与已鉴别主角相关联的，其在完整性机制中的使用将用于链接如上述提供的两个服务。

为完整性派生密钥的方式能够作为指定哪种方法和算法应该被用于整个鉴别交换的参数的一部分被规定。

注：当使用其他安全服务时，还可能从鉴别交换期间指定的参数派生出服务信息，例如：保密性密钥。

5.2.7 跨多重域鉴别组件的分布

有可能使安全域进入一种这样的关系，使得一个域的申请者能够被另一个域的验证者所鉴别。多重安全域可以是交错的，包括：

——发起者驻留的安全域；

——验证者驻留的安全域；

——可信第三方驻留的安全域。

这些域不需要各不相同。

在鉴别能够在不同的安全域进行之前，有必要建立安全交互政策。

5.3 用于鉴别的原则

一般而言，特定的鉴别方法将依赖于与一个或多个原则相关的一系列假设或期望。

使用原则包括：

a）某些已知的东西，例如：口令；

b）某些已拥有的东西，例如：磁卡或智能卡；

c）某些永远不变的东西，例如：生物标识符；

d）接受第三方（可信第三方）已经确立的鉴别；

e）上下文，例如：主角的地址。

应该注意到所有原则都有固有的弱点。例如：已拥有某些东西的鉴别通常是拥有客体而非其持有者的鉴别。在某些情况下，这些弱点可以由多个原则的组合所克服。例如，当使用智能卡（已拥有的东西）时，通过增加PN来实现用户到卡的鉴别（某些已知的东西）这样就可以克服弱点。此外，原则e）特别弱并且实际上总是与其他原则一起使用。

注意 在d）中存在两种类型的递归：

——为被标识第三方实体可能要求其自身被鉴别；

——第三方建立的鉴别可以使用第四个实体。

结合这些原则的实际鉴别方法的分析将指出被包含的实体、被使用的原则和被鉴别的主角。

5.4 鉴别的阶段

鉴别可以包括下列阶段：

——安装阶段；

——更改鉴别信息阶段；

——分发阶段；

——获取阶段；

——传送阶段；

——验证阶段；

——关闭阶段；

——重开启阶段

——卸载阶段。

这里所描述的阶段并非必须在时间上不同，即它们可以重叠。

并非所有这些阶段都为鉴别方法所要求。同样，在某些情况下，阶段的排序可能不同于由下列规则所隐含的顺序。

5.4.1 安装

在安装阶段，申请 AI 和验证 AI 被定义。

5.4.2 更改鉴别信息

在更改鉴别信息阶段，主角或管理员使申请 AI 和验证 AI 发生改变（例如：口令被改变）。

5.4.3 分发

在分发阶段，验证 AI 被分发给验证交换 AI 中使用的实体（例如：申请者或验证者）。例如：在离线方式中，实体可以获取鉴别证书、证书撤消列表和机构撤消列表。分发阶段可以在传送阶段之前、期间或之后。

5.4.4 获取

在获取阶段，申请者或验证者可以获取为生成用于鉴别实例的具体交换 AI 所需的信息。不同的规程可以通过与可信第三方的交互或通过鉴别实体间的报文交换获取不同的交换 AI。

例如：当使用在线密钥分发中心时，申请者或验证者可以从密钥分发中心获取某些信息，诸如鉴别证书（见 6.1.3），以便能够进行与其他实体的鉴别。

5.4.5 传送

在传送阶段，交换 AI 在申请者和验证者间被传送。

5.4.6 验证

在验证阶段，交换 AI 与验证 AI 进行对比检查。在这个阶段，不能验证交换 AI 本身的实体可以与将执行交换 AI 验证的可信第三方联系。在此情形下，可信第三方将送回一个肯定或否定响应。

5.4.7 关闭

在关闭阶段，先前已经能够被鉴别的主角临时不能被鉴别的状态被建立。

5.4.8 重开启

在重开启阶段，关闭阶段所建立的状态被终止。

5.4.9 卸载

在卸载阶段，一个主角从众多主角中消除。

5.5 可信第三方参与

鉴别机制能够由一系列参与其中的可信第三方的特征所表示。

5.5.1 无可信第三方参与的鉴别

在最简单的情形，申请者和验证者在生成和验证交换 AI 过程中都得不到其他任何实体的支持。在此情况下，用于主角的验证 AI 必须已经安装在验证者中。

除非大多数实体被限于少数几个可能的通信伙伴，否则这类方法在大规模通信环境中的使用是有限的。在最坏情形，验证者被要求具有用于安全域中所有主角的验证 AI，其全部信息需求随参与实体个数的平方而快速增长(见图 2)。

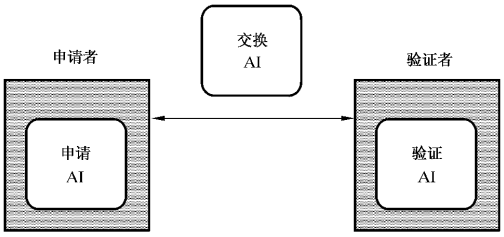


图 2 无可信第三方参与的鉴别

5.5.2 可信第三方参与的鉴别

验证 AI 能够通过与可信第三方的交互而获得。这个信息的完整性必须得到保证。假如申请 AI 可以从其中推导出的话，它也是维护可信第三方的申请 AI 的保密性和验证 AI 的保密性所必需的。

正如 5.3 的原则 d)所述及的，鉴别可以包含一个可信第三方或者一个可信第三方链。额外可信第三方的引入使得在众多实体间的鉴别中每一个实体只维护了有限个实体(非所有实体)的信息。因此，全部信息可以随参与的实体个数呈线性增长。

多重实体关系可以依据通信需求(包含的活跃链接的数目)和其所具有的管理控制程度(例如：取消鉴别信息过程中的固有的延迟)来表示。

5.5.2.1 内线

在内线鉴别情况下，可信第三方(中间者)直接介入申请者和验证者间的鉴别交换。主角由在后续内线鉴别交换中担保其身份的中间者鉴别。

内线鉴别要求验证者信任中间者能够正确鉴别主角，并且要求通过鉴别向验证者保证中间者的身份。

鉴别能力的撤消可以被控制到下一次鉴别尝试的粒度上。假如申请者已经撤消其鉴别信息，中间者能够立即更新申请者的状态并且拒绝任何进一步的鉴别尝试。

个别情况下，该方式能够被扩展以便包含可信中间者链的保证可以被接收。基于生效的安全政策，链上的验证者或者最后的 TTP 负责决定中间者链是否有效。

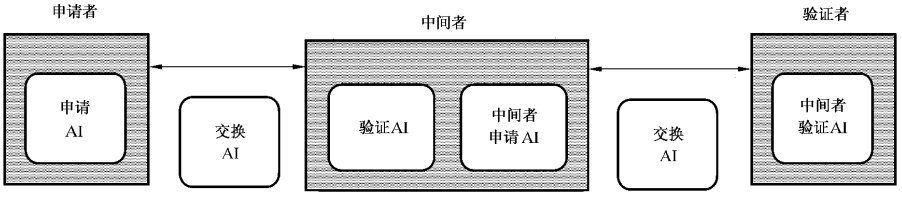


图 3 内线鉴别

5.5.2.2 在线

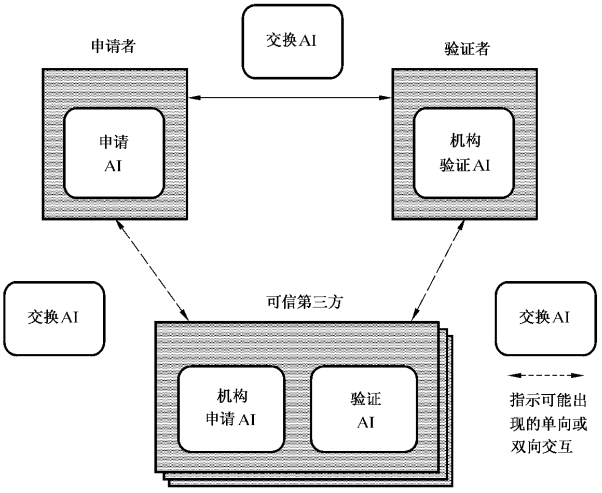
在在线鉴别情况下，一个或多个可信第三方被包含在某个鉴别交换的每一个实例中。但是，与内线鉴别不同，在线可信第三方不直接位于申请者和验证者鉴别交换的路径上。在线可信第三方能被申请者

要求生成交换 AI 以便能帮助交换 AI 进行交换验证。在线可信第三方能够生成在线鉴别证书(见 6.1.3)。

在线鉴别要求在验证者和能够证明主角申请 AI 有效性的可信第三方之间,存在一个在生成交换 AI 过程中所包含的可信第三方链。在最简单的情形下,只需要一个可信第三方直接与申请者或验证者交互。然而,这能够被扩展到直接或者间接与申请者或验证者通信的可信第三方链。

鉴别能力的撤消可以被控制到下一次鉴别尝试的粒度上。

在线可信第三方的例子有在线可信服务器或密钥分发中心。



注:本图示出的发生在三个不同实体间的实际交换 AI 是不同的

图 4 在线鉴别

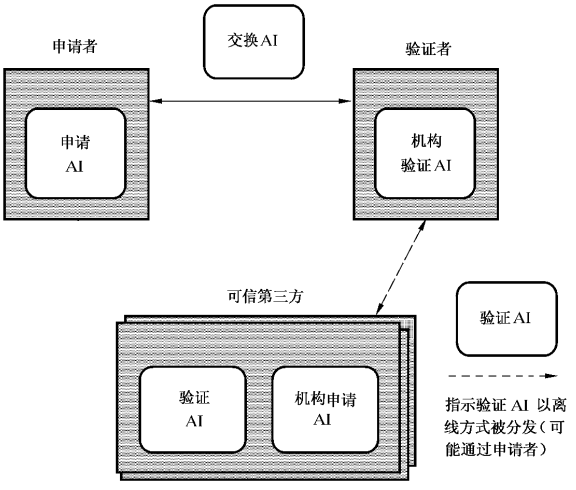


图 5 离线鉴别

5.5.2.3 离线

离线鉴别是由需要使用撤消证书的签发列表、撤消证书的证书列表、证书超时、或用于验证 AI 撤

消的其他非直接方法所表示的。

在离线鉴别情况下，一个或多个可信第三方支持鉴别而无需参与其中的每一个鉴别实例。离线可信第三方提前生成和分发被验证者以后用于验证鉴别交换有效性的离线鉴别证书。鉴别交换因此自治地进行，而无需机构的介入。

由于可信第三方不能在鉴别发生时直接与申请者或验证者交互，这种途径就所需的交互次数而言可以更加有效。

撤消必须依赖于诸如证书的期满和更新等一类的额外条文，以及撤消证书的签发列表。

离线可信第三方的例子有颁发离线鉴别证书的机构(见 6.1.3)。

5.5.3 申请者信任验证者

在其中必须信任某个验证者的机制是不适当的，除非所有可能的验证者都能被信任。这是因为，假如验证者的身份还未被鉴别，其可信度是未知的。例如：使用简单的口令鉴别，必须信任验证者未保存和重用某个口令。

5.6 主角类型

主角可以多种不同方式分类，如：

a) 具有被动特征的主角，例如指纹、视网膜特征；

b) 具有信息交换和处理能力的主角；

c) 具有信息存储能力的主角；

d)具有唯一固定位置的主角。

主角可能适于一个以上的类别，例如：人类实体适于 a)、b)和 c)。鉴别的不同方法适用于每一种情况：

a) 被动特征的量度；

b) 复杂盘问和响应评估；

c) 秘密的存储(诸如口令)；

d) 位置的确定。

5.7 人类用户鉴别

在鉴别实例中，可能有必要鉴别最终的人类用户，而不是代表人类用户动作的进程。

用于鉴别人类用户的方法必须为人类用户所能接受并且经济和安全。不可接受的方法可能鼓励人类用户去寻找避免某种规程的方式，因此潜在的入侵增加。

用于鉴别人类用户的方法基于 5.3 中所描述的原则。用于鉴别人类用户的规程基于 5.4 中所描述的阶段。

附录 A 提供了关于人类用户和代表人类用户动作的进程鉴别的进一步信息。

5.8 鉴别攻击类型

所考虑的三种攻击形式是：

——重发攻击，交换 AI 被读并随后被重发；

——中继攻击，由入侵者发起；

——中继攻击，由入侵者响应。

中继攻击是一种交换 AI 被中断然后再被立即转发的攻击。

5.8.1 重发攻击

存在两种将要考虑的重发攻击情况。这些都是某些交换 AI 的重发：

——在相同的验证者上的重发；

——在另一个验证者上的重发。

当主角的(相同的)验证 AI 为若干验证者所知时可能出现后一种情况。当一个成功的重发可以被完成时，这是一种冒充的特例。

使用盘问则能够对抗两种重发情况。盘问是由验证者生成。相同的盘问决不能由相同的验证者颁发两次。这能够以若干方式实现(见附录C)。

5.8.1.1 相同的验证者上的重发

相同的验证者上的重发可以使用唯一编号或盘问对抗。

唯一编号是由申请者生成的。相同的唯一编号决不可被相同的验证者接收两次。这能够以若干方式实现(见附录C)。

5.8.1.2 不同的验证者上的重发

不同的验证者上的重发可以使用盘问对抗。在交换AI计算中可采用的对抗不同的验证者上的重发的其他方法是使用对验证者具有唯一性的特征。这类特征可以是验证者名字,其网络地址或任何就共享验证鉴别信息的验证者而言是唯一的属性。

5.8.2 中继攻击

5.8.2.1 入侵者发起的中继攻击

这类攻击包含了作为鉴别发起者的入侵者。这个攻击仅当申请者和验证者双方都能发起这个鉴别时才可能。这个攻击使得申请者和验证者在未意识到的情况下通过入侵者交换鉴别信息,即入侵者相对于申请者假装验证者并且相对于验证者假装这个申请者。

例如:假定C想向验证者B冒充其是申请者A。C开始与A和B双方的交互。C告诉A其是B,要求A去鉴别B,并且还告诉B其是A和其想鉴别自身(见图6)。

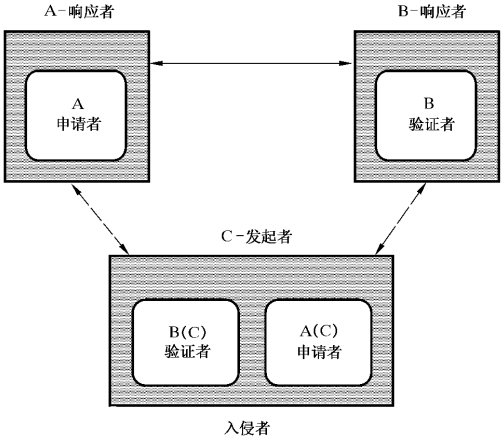


图6 入侵者发起的中继攻击

在鉴别期间,A作为相对于B的申请者(实际上C假扮B),并且,因此向B提供C能够用于鉴别的信息。B作为验证者并且还提供C需要起验证者作用的信息。按照这个鉴别,对B而言,入侵者C看似已鉴别的A。

这种攻击类型可以被对抗,假如:

a) 发起交互的实体或者总是申请者或者总是验证者(注意这在使用双向鉴别时也许是不可能的);

b) 由申请者提供的交换AI根据其作为鉴别请求发起者或对鉴别邀请的响应者作用的不同而不同。这些差别允许验证者发现所描述的截获。进一步的细节见附录D。

5.8.2.2 入侵者响应的中继攻击

在这类攻击中,入侵者位于鉴别交换中间,截获并且转发鉴别信息,接管发起者的位置。这类攻击可能发生于巧合,在此情况下入侵者等待以被误认作响应者;或通常,在此情况下入侵者宣称自己作为响应者(例如在集中式资源位置表中)。