 企业是如何使用Oracle技术来管理用户身份的"这个平台针对的是我们实验室计算机安全性计划部门为8000多名员工提供的非常分散的用户账户数据、身份标识和密码，"Oracle应用服务器10g基础架构项目经理兼加州劳伦斯利弗莫尔国家实验室的计算机科学家Macedo说道，"主要是想使各位董事摆脱管理用户账户这样一些琐事，并为那些与该平台集成的各应用程序提供单一登录功能。我们希望获得一个通用的集中化的账户管理方案，这样我们就能够轻松地说创建那个账户，保留那个账户或撤销那个账户，因而实验室的所有的业务或科学研究系统都会立即采用。"身份管理的重要意义 Macedo的解决方案不愧是一场及时雨，因为"身份混乱"如今是企业的常见问题。在很多机构中，员工身份分散在几十个应用程序中，相互独立，彼此之间无法识别。这种情况常常在雇佣的当天当人力资源部门将员工的资料输入到HR系统中的时候就出现了。此后，当此位员工被允许访问其他应用程序和服务的时候，与此类似的过程将不断重复--由于针对每个账户所分配的角色和权限是形形色色的，于是这种情况将变得越发复杂化。这种角色划分所造成的结果常常犹如一场恶梦--不仅对于那些必须记住使用每个应用程序所需的ID号和密码的员工来说是这样的，而且对于跟踪和管理这些ID号和密码的管理员来说，也是如此。"在企业和政府机构中，这一问题处处皆是，" Forrester研究公司负责安全问题的首席分析家Jonathan Penn说道，"身份管理的问题无

所不在，且形式多样。对于IT机构来说，不仅存在着很多使其增加开支的大量冗余和效率低下的问题，而且很难确保企业遵循安全性政策与要求。此外，更难开发和推广能够帮助企业更加敏捷、更具快速响应能力的应用程序与服务。" 信息技术研究、顾问服务与战略咨询的一流提供商--Meta集团负责安全与风险战略的副总裁Earl Perkins先生对此深表赞同，同时他强调说"企业和政府承担着很大的压力，它们需要遵循州和联邦政府关于管理身份信息的各种法令。"他所说的美国法令包括用于确保财务披露和会计的准确性的萨班斯-奥克斯利法案、医疗保险可移植性和责任法案（HIPAA）以及家庭教育权和隐私保护法案（FERPA），后两个法案分别用于保护医疗保健和教育方面个人信息的私密性。 这些法令的遵循取决于身份管理的定义。"身份管理通常是从旁观者的角度来看待的，" Oracle 公司首席安全官Mary Ann Davidson说道。" 有些人会想到智能卡或生物测定学。而另外一些人会想到单一登录或目录。然而，更广义地说，它是用于管理企业中针对人员和网络实体的全面安全性与身份管理生命周期的所有处理方法和技术。" 身份管理生命周期中的管理步骤包括创建账户，修改权限，以及停止和取消无效的账户。虽然应用程序用户的身份管理是很多身份管理解决方案的重中之重，但是身份管理还可能包括设备、流程与应用程序--以及在网络环境中进行交互的一切事物。 "当谈到身份管理技术的时候，有两个重要领域值得考虑，"Perkins补充说，"第一个就是身份管理基础架构，它提供基本认证、授权、目录和集成服务。第二个就是身份管理本身，它提供用户供给、工作流（用于流程自动化）、委托管理（包括自助式服务和密码管理），

以及审计日志和生成报告的功能等。""目录服务的部分功能通常是以层次结构的方式来创建和管理安全性及访问政策，该功能具有政策的继承性，"Penn说道，"从创建全局性政策开始，然后在此基础上创建继承全局属性的地区或业务部门的政策，这些政策比企业政策更加严格。此外，应用程序政策和用户访问规则还可能更加严格。"通过Oracle软件进行身份管理 Oracle在Oracle 10g身份管理基础架构中提供了多种身份管理功能，从而体现出现有版本较以往一些版本有了显著改进。"Oracle 10g的发布使Oracle在身份管理的关键领域中迈出了重要的一步，"Oracle公司负责身份管理与安全产品的资深总监 Uppili Srinivasan说道，"作为知名的安全性产品的一流厂商，我们充分利用自己25年来积累的经验和优势力量，致力将自己发展成为一家以安全解决方案而闻名于世的一流厂商--而Oracle身份管理是这种努力成果的核心。"[NextPage]
Oracle身份管理作为Oracle应用服务器10g和Oracle平台安全性体系结构的一部分来提供，它为构建身份管理解决方案提供了一个坚实的基础（请参阅《Oracle应用服务器10g身份管理基础架构》一文）。其组件包括： Oracle互联网目录（OID）--一种可伸缩的、安全的目录服务，符合轻量级目录访问协议（LDAP）标准，可用于存储和管理用户信息。 Oracle目录同步服务--一个目录集成平台，使企业能够将身份管理目录与原有的或者特定的应用程序目录连接起来。 Oracle供给集成服务--一个可以与企业供给系统（如人力资源应用程序）连接在一起或者以单独的模式进行操作的供给框架。
Oracle委托管理服务--一个委托管理模型和应用程序，使身份管理器的管理员能够有选择地代理某个应用程序管理员的管

理访问权限，或者直接代理某个用户管理访问权限。 Oracle应用服务器单一登录（SSO）--用户认证的运行时模型 Oracle应用服务器证书授权--用于创建和管理公共密钥基础架构（PKI）证书的系统"虽然Oracle应用服务器10g是发布这套功能的主要承载工具，但是Oracle身份管理也是所有Oracle产品和技术（包括Oracle数据库、Oracle协作套件和Oracle电子商务套件）的共享安全性基础架构，"Oracle身份管理产品的管理总监Michael Mesaros说道，"它还可以作为一种通用的身份管理解决方案来支持那些集成在全企业身份管理部署过程中用户编写的和第三方企业的应用程序。""Oracle合作伙伴也提供了一些具有多种功能的身份管理应用程序，用于身份认证、访问控制和用户管理等，"Oracle公司安全性与身份管理业务开发总监Milan Thanawala解释道，"合作伙伴通过Oracle身份管理基础架构进行确认，以保证其产品与该基础架构能很好地协同工作。" 安全的身份管理与可用性 Oracle身份管理基础架构吸引了很多公司的注意，因为它能满足他们的实际需要。例如总部在芝加哥的Archipelago Holdings LLC公司是群岛交易所（ArcaEx）--美国首个开放式的全电子化股票交易所--的创建者。在这个交易所里，客户可以公开买卖所有在纳斯达克、美国证券交易所、太平洋股票交易所及中央交易所上市的股票。为客户提供最佳信息是Archipelago 努力的目标之一，为此它开发了一个称作ArcaVision 的Web应用系统，用来为参加交易的客户提供及时的市场信息--证券发行商和交易商的市场交易行情。在该应用程序的开发过程中，Archipelago Holdings公司的IT小组确定公司需要为这些用户提供一个单一登录的解决方案，以及一种能够集中管理针对

其用户的所有认证和访问控制功能的方式。 由于重点考虑的是投放市场的时间问题，该公司决定购买一套完全由Oracle软件构成的解决方案。通过使用Oracle9i数据库、Oracle9i应用服务器、Oracle单一登录和Oracle互联网目录及Oracle 应用服务器中的J2EE软件，Archipelago Holdings公司的IT小组能够为该公司内部和外部ArcaVision用户提供一种基于由Archipelago客户账户小组授权的角色和访问权限的Web单一登录访问方式。"我们之所以决定部署一个完全由Oracle软件构成的系统是因为我们希望让一个厂家对所有组件负责。这种方式提供了一个紧密集成的解决方案，有助于缩短开发周期，避免了厂商之间互相推委的现象，"Archipelago公司数据库操作执行董事Steve Hirsch说，"由于我们知道Oracle数据库、Oracle应用服务器、Oracle互联网目录及Oracle单一登录能够轻松地协同工作，与其他方案相比，采用这种方案使我们缩短了产品投放市场的时间，实施起来更轻松。" ArcaVision的用户群中包括那些能够通过互联网访问该计划所有特性的人们、员工和交易商。系统中构建的访问控制功能不仅能够控制用户的权限，而且能够改进最终数据的质量，因此用户可以根据业务关系和用户简档，获得定制的报告，这些报告为他们提供所需要的准确信息。"借助OID中的认证信息，我们能够知道谁登录到该网站，这确实让我们收益良多，"Hirsch解释说。ArcaVision已正常运行一年多了，Archipelago IT小组还在不断增添新的功能。"这个应用程序最初是部署给内部用户使用的，但是目前已经扩展到其外部用户使用，"Hirsch说道， "一旦账户管理器提供给了用户，这些用户就可以只登录一次即可访问网站上所有允许访问的内容，而无需再次登录

。"[NextPage] Oracle身份管理基础架构 分布式身份管理 Oracle身份管理解决的另一个实际问题涉及机构的发展与演变的方式。一般来说，随着机构的发展和合并，或者购并新的公司，其系统和应用程序会变得更加分散和多样。劳伦斯利弗莫尔国家实验室便是如此。LLNL与其他大型机构很相似，用户的身份遍布多个应用程序和部门，需要用户多次登录并保持多种用户姓名和密码来进行日常业务工作。为了解决这一问题，LLNL的管理信息服务部门(AIS)部署了一个集中化的Oracle 10g 身份管理实例，为那些与连接到该系统的所有应用程序及整个12个董事会成员使用的分布式身份管理体系结构提供单一登录功能。 LLNL的Macedo解释说，"开始实施这个项目的时候，我们询问了一些重要问题：在你的IT机构高度分散的情况下，如何实施集中式的单一登录方案？如何在支持集中化的SSO方案的同时提供基础架构的自治功能？我们的答案是以Oracle单一登录、Oracle应用服务器10g及Oracle互联网目录为中心来构建自己的系统，并将系统设计成一个高度可用的平台，提供给各个董事会。该系统从中央计算机安全计划（CSP）机构获得用户账户和密码信息，然后通过身份管理平台，将这些信息分发到所有参与该系统的应用程序。这就意味着将我们的董事会纳入到一个全企业范围的身份管理基础架构中--这是我们向终极目标迈进的第一步，我们的最终目标是为LLNL的所有机构和员工提供一个统一的身份管理解决方案。"公司简介 Archipelago Holdings LLCArchipelago Holdings LLC的总部位于芝加哥，它是群岛交易所--美国首家开放式全电子化股票交易所--的大本营。群岛交易所创立于 1999年，客户可以在此公开买卖所有在纳斯达

克、美国证券交易所、太平洋股票交易所及中央交易所上市的股票。ArcaVision交易与市场信息应用系统利用 Oracle身份管理基础架构提供单一登录机制和用户账户管理。所使用的Oracle产品：Oracle9i数据库、Oracle9i应用服务器、Oracle单一登录、Oracle 互联网目录、Oracle应用服务器中的J2EE软件，以及 Oracle真正应用集群 劳伦斯利弗莫尔国家实验室劳伦斯利弗莫尔国家实验室（LLNL）位于加州利弗莫尔市，它是美国能源部的一个重点实验室，由加利福尼亚大学进行管理。 该实验室的使命就是利用科学与技术为国家造福，其重点领域是全球安全性、全球生态系统及生物科学。为了解决身份分散问题，LLNL设计了一个Oracle 10g身份管理服务器，来为连接到该系统以及部署给12个董事会成员的分布式身份管理体系结构的所有应用程序提供单一登录功能。所使用的Oracle产品：Oracle应用服务器10g、 Oracle单一登录、Oracle应用服务器门户和Oracle互联网目录金门大学金门大学（GGU）成立于1901年，位于旧金山。它是加州第五大私立大学，设有本科及研究生课程，专业涉及商务和管理、信息技术、税务及法律。GGU正在开发全校范围内的身份管理基础架构，将包括支持托管的Oracle电子商务套件应用系统和本校开发的应用系统的Oracle身份管理基础架构。所使用的Oracle产品：Oracle应用服务器10g、 Oracle单一登录、Oracle互联网目录、Microsoft活动目录代理、Oracle电子商务套件和Oracle在线系统 这种模式具有一系列优点：所有Oracle应用服务器服务的自主管理、自动同步OID和用来解决与区域分散相关的问题的完善SSO性能。然而，其缺点是LLNL没有获得真正的全球化SSO。而SSO能够使一个用户在跨越访问

不同的SSO 领域时不必多次登录。"虽然如此，与目前现有的情况相比，也有很大的进步：现在面对的是用户登录多种应用系统的混乱状态，" Macedo说，"我们的目标是拥有一套用于基础架构服务的高度可用的解决方案，我们打算不仅将其用作CSP来推动ID，而且将其作为所有生产用的应用程序服务器实例的元数据存储库来使用。" 本年度后期，当全面部署这个平台的时候，AIS将把Oracle的 SSO作为其 Live Link 文档管理系统的前端。它还将把Oracle应用服务器门户连接到实验室的中央Web内容管理方案中，在此用户可以访问标准的Web内容、文档、PDF文件、图表等等。 "其他用于快速迁移的可供选择的应用系统还包括我们使用得最频繁的考勤卡输入系统，以及一个集成的工作表系统，该系统纳入了实验室高度机密性工作的所有流程和过程，"Macedo说， "我们对这套解决方案很满意，但是我们仍然在努力实现一种神圣的统一的单一登录模式。我们知道Oracle正在研发这种模式。它会使我们的各董事会成员们运行自己的身份管理基础架构，但是他们将利用我们的CSP的SSO，而且不需要增加现有成本。" 一个ID环境 有些企业不仅需要应付各种异构型系统集和应用程序的问题，而且很多诸如加州第五大私立大学--金门大学(GGU)这样的机构，还要应付不同的和不断变化的用户群的问题。GGU的用户群涵盖了将近20多个不同的用户群体。作为简化大学身份管理，同时也为学生、教职员工和其他用户提供更好的用户体验的一部分，该大学的中央IT部门正在提供一种全院范围内的身份管理战略，其中包括实施Oracle身份管理基础架构。在与6种Oracle托管的Oracle电子商务套件应用程序相连的条件下，该套解决方案将提供一个目录集

成和单一登录层，作为中介器来处理全部学术和商务应用程序及连接美国西部三个数据中心的各种基础架构组件所需的身份信息。"我们的身份管理目标之一就是通过一个网站门户，为我们的企业应用程序和数据创建一个集成式输入点，所以单一登录对我们很重要，除了我们的员工以外我们还需要将其推广到其他用户，"GGU 首席技术官Anthony Hill说，"我们还将基于角色的个性化特性构建到网站中，这样便能够基于员工的角色为他们创建个性化的工作区。身份信息源仍然是该应用系统，但是身份数据将需要整合，并将整合后的数据提供Oracle互联网、Novell公司的eDirectory及微软的活动目录使用，从而创建一个中心-辐射型模式，来简化整个GGU的身份管理。我们希望减少为了重新设置密码而打入服务中心的电话数量--这种电话会消耗服务中心70%的时间，我们也希望重新安排这些资源去支持新的技术，并提供更加有效的技术支持。" Hill强调了全企业进行自动资源供给的需要，不仅针对核心应用系统，而且针对网站和很多基础架构应用系统，包括网络访问、消息传递、学术系统和学生项目环境等。尽管多数系统和应用程序将被设置成自动供给，但是有些账户还将使用自助与人工供给相结合的方式。 [NextPage] GGU所面临的一大挑战将是内部与外部环境相结合的问题--利用奥斯汀和得克萨斯数据中心（ERP基础架构就设置在那里）的各种Oracle技术以及GGU大学自己开发的应用程序，同时利用该身份管理基础架构。"在GGU，我们的身份管理系统面临着一些独特的挑战，这是你在美国其他企业中很少会遇到的，因为我们需要维护的系统较多，且学生用户群的变动性很大。此外，随着时间的推移，每个身份所担当的各个角

色不断变化，"Hill说，"一个个体可以是一名学生、员工、教员，并且还可能是一名毕业生。因此，为了满足这种复杂情况的需要，我们的解决方案最终将把最佳品牌的身份管理工具集与Oracle身份管理平台结合起来。"下一步 阅读更多有关Oracle身份管理的资料 通过范例来了解Oracle身份管理 下载Oracle应用服务器10g 即将到来的改进和功能增强 Oracle身份管理是一种不断发展的基础架构，它的每个组件都是为了不久以后的发展而按计划进行了改进和提高。本年度后期将对三个领域进行改进，并增添一些新的功能。该平台将提供：应用服务器座席使Oracle单一登录机制更加适合于不同企业应用程序的环境。 用户供给工具集，包括一个Web用户供给控制台、一个工作流组件、一套服务供给标志语言与供给连接器，以及一套目录连接器，该连接器将把OID连接扩展到Novell Nsure（电子目录）和OpenLDAP目录。 一套基于标准的用于统一的SSO、供给和分散及单一注销的技术集。 "随着我们不断提供这些增强的功能，我们的总体目标更加清晰了，"Oracle公司的Mesaros总结道，"我们正在逐步扩展我们的基础架构，以便更有效地处理分布式企业和企业间的身份管理设施。同时，Oracle 10g身份管理提供了一种更加强劲的基础，来满足当今复杂的身份管理需要。" [NextPage]身份管理方面的Oracle合作伙伴 虽然Oracle身份管理作为一种综合性的身份管理基础架构而设计的，但是Oracle认为第三方应用程序和工具集也是需要的。为此，Oracle鼓励身份管理领域的独立软件厂商开发兼容的产品。"我们与合作伙伴们合作，利用Oracle产品帮助他们验证自己的产品，并提供技术支持和资源，从而帮助他们以最有效的方式将其产品与Oracle产品集成

，"Oracle公司安全与身份管理业务发展总监Milan Thanawala说道，"一般的安全性与特殊的身份管理是我们关注的重要领域。" 以下是一些Oracle身份管理合作伙伴的例子 虚拟专用网络/负载平衡器/防火墙认证F5 Networks公司BIG-IP FireGuard 520提供了防火墙负载平衡功能、高可用性和最高的安全性。 NetScaler公司NetScaler 9000 Series保护并优化基于Web的或客户机/服务器应用系统传输的数据。 Radware公司提供多层企业安全解决方案。 生物测定 Bio-key国际公司通过指纹识别来提供用于Oracle应用系统的安全单一登录功能。 A4Vision公司利用对象识别与验证技术，来对进入一些公共场所的人们进行控制。 Iridian Technologies公司生产虹膜识别软件。 标记/智能卡ActivCard公司提供了一个处理卡和证书的智能卡以及卡管理系统。 RSA安全公司生产处理发布前和发布后的小应用程序的基于Java的智能芯片和数字化证书。 Secure Computing公司生产功能强大的认证系统，用于定制网络认证。具有高保障的CA服务 RSA安全公司开发用于管理数字证书和提供一种经过认证的、私有的、符合法律规定的电子通信与交易环境的软件。 Entrust公司开发能够帮助你集中管理用于多种Web服务器的SSL认证部署的软件。 访问控制Web授权RSA安全公司RSA的产品使企业能够集中管理用户身份、认证政策和用户权限。Netegrity公司提供与 Oracle单一登录协同工作的软件，使客户能够提供企业范围内的单一登录环境。 Oblix公司Oblix CoreID 与Oracle单一登录一起扩展了所有基于Web的应用程序的身份管理功能。 企业应用系统单一登录 Evidian公司Evidian SSO Xpress将单一登录扩展到了Windows环境中的所有应用系统。 Passlogix公司v-GO SSO为Windows

、Web、Java、Unix和专有应用程序提供了通用的单一登录功能。 用户管理用户供给Thor Technologies公司提供了一个用于管理访问企业应用程序和受控制的系统的供给系统。Courion公司提供了一个自动化的账户供给和用户IS管理解决方案。Waveset公司 (Sun)提供了自动、安全地访问Oracle资源的软件。 Computer Associates公司提供了与Oracle 10g协同工作的管理、安全性与实施的解决方案。 密码的同步Courion公司提供了自助式的密码重设与同步解决方案。Blockade系统公司提供了为网络用户实时传送密码和身份管理属性的软件。 M-Tec公司提供了具有透明的同步功能并可在一些精选类型的系统上扩展本地密码管理的软件。 