# IBM 客户端安全软件版本 5.30 部署指南

第三版（**2004** 年 **7** 月）

# 前言

部署 IBM® 客户端安全软件时，IT 管理员必须了解并且规划诸多因素。本指南并非意在说明如何使用嵌入式安全子系统芯片或客户端安全软件；实际上，它是有关在企业内如何将软件部署到装配有嵌入式安全芯片的计算机中的指南。

## 读者

本指南意在供 IT 管理员或负责在组织内的计算机上部署 IBM 客户端安全软件 V5.3（CSS）的那些人员使用的。本指南意在提供在一台或多台计算机上安装 IBM 客户端安全软件所需的信息。IBM 为客户端安全软件提供《用户指南》、《客户端安全软件管理员指南》以及应用程序帮助，您可以通过参考这些内容获取有关使用该应用程序本身的信息。

## 产品出版物

以下文档可在客户端安全软件 V5.3 库中获得:

- *客户端安全软件 V5.3 管理员指南*,

  提供有关设置和使用客户端安全软件随附的安全功能的信息。
- *客户端安全软件 V5.3 用户指南*,

  包含关于执行客户端安全软件任务（例如，使用 UVM 登录保护、设置客户端安全屏幕保护程序、创建数字证书以及使用用户配置实用程序）的信息。
- *客户端安全软件 V5.3 安装指南*,

  包含有关在包含 IBM 嵌入式安全芯片的 IBM 网络计算机上安装客户端安全软件的信息。
- *结合 Tivoli® Access Manager 使用客户端安全软件 V5.3*,

  包含有关设置客户端安全软件以结合 Tivoli Access Manager 使用的有用信息。

## 其它信息

您可以从 http://www-132.ibm.com/content/search/security.html IBM Web 站点获取其它信息和安全产品更新（可用时）。

# 目录

# 第 1 章 部署 IBM 客户端安全软件前的注意事项

有多种方法部署 IBM 客户端安全软件（CSS），该软件使用集成到 IBM 个人计算机的 IBM 嵌入式安全子系统（ESS）硬件。本文档将帮助您确定如何在您的环境中部署 ESS。考虑您公司将如何部署计算机的过程（从映像创建到向最终用户提供 PC 的方式）十分重要。该过程将极大地影响您公司如何部署 ESS。IBM ESS 实质上由两部分组成（如图 1 中所示）：

1. 客户端安全软件
2. 嵌入式安全芯片

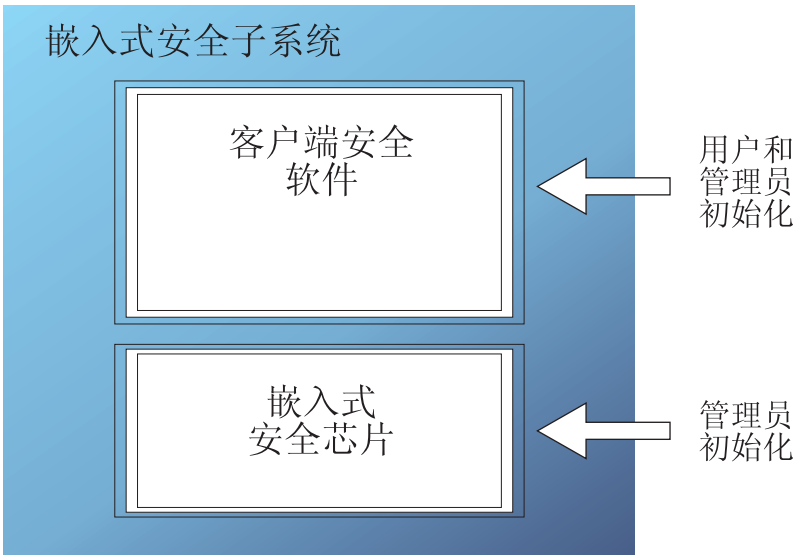


*图 1. IBM 客户端安全系统组件*

## 部署的要求和规范

如果您计划将 IBM 客户端安全软件安装在装配有嵌入式安全芯片的计算机上，则请计划好以下服务器存储空间以及下载需求和安装次数:

1. 带有嵌入式安全芯片的 IBM PC
2. 用于可安装代码的服务器存储空间需求: 大约 12 MB
3. 每个用户用于密钥存档数据的平均服务器存储空间需求: 每个用户 200 KB 用于存档存储

# 第 2 章 嵌入式安全芯片如何运行

IBM 嵌入式安全芯片在图 2 中以图形表示。有三个主要组件:

1. 管理员密码
2. 硬件公钥
3. 硬件私钥

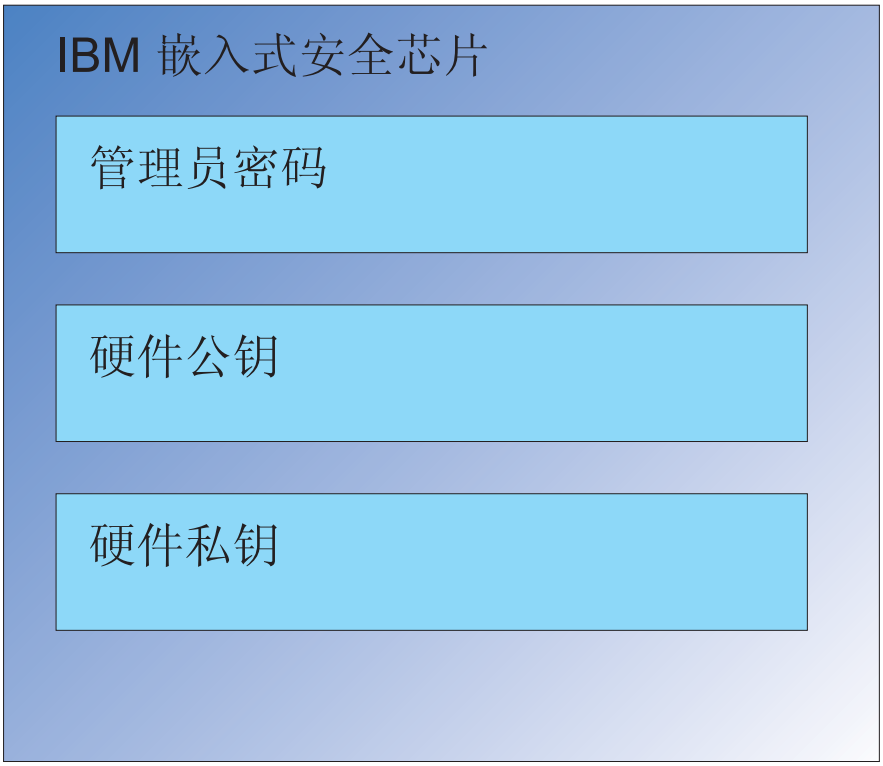


*图 2. 保留在 IBM 嵌入式安全芯片中的数据。*

硬件公钥和私钥在每台计算机上都是唯一的。不可从芯片抽取硬件私钥。可以下列方式生成新的密钥对:

- 通过客户端安全软件向导
- 通过管理员实用程序
- 使用脚本

请注意，不能从芯片中抽取硬件密钥。

管理员使用管理员密码访问以下功能，包括:

- 添加用户
- 设置安全策略
- 设置口令策略
- 登记智能卡

- 登记生物统计法验证设备

例如，管理员可能需要使其他用户能够利用嵌入式安全芯片的特点和功能。管理员密码是在安装客户端安全软件时设置的。本文档稍后将详细说明如何以及何时设置管理员密码。

**要点:** 请开发维护管理员密码（该密码必须在首次配置 ESS 时建立）的策略。有可能每台带有嵌入式安全新片的计算会拥有相同的管理员密码（如果 IT 管理员或安全管理员有意如此确定的话）。或者，也可以选择给每个部门或大楼指定不同的管理员密码。

IBM 嵌入式安全芯片的其它组件是硬件公钥和硬件私钥。该 RSA 密钥对在配置客户端安全软件时生成。

每台计算机将拥有唯一的硬件公钥和唯一的硬件私钥。IBM 嵌入式安全芯片上的随机数功能确保了每个硬件密钥对在统计上都是唯一的。

第 5 页的图 3 描述了 IBM 嵌入式安全芯片的其它两个组件。理解这两个组件是有效管理您的 IBM 嵌入式安全子系统基础结构的关键。第 5 页的图 3 显示管理员公钥和私钥以及用户公钥和私钥。以下是公钥和私钥的简单说明。

- 公钥和私钥被认为是 “密钥对”。
- 私钥和公钥在数学上与以下内容相关:
  - 用公钥加密的任何内容只能用私钥解密。
  - 用私钥加密的任何内容只能用公钥解密。
  - 知道私钥并不使您能够派生公钥。
  - 知道公钥并不使您能够派生私钥。
  - 公钥通常对任何人都可用。
- 私钥必须被很好地保护起来。
- 公钥和私钥是公钥基础结构（PKI）的基础。

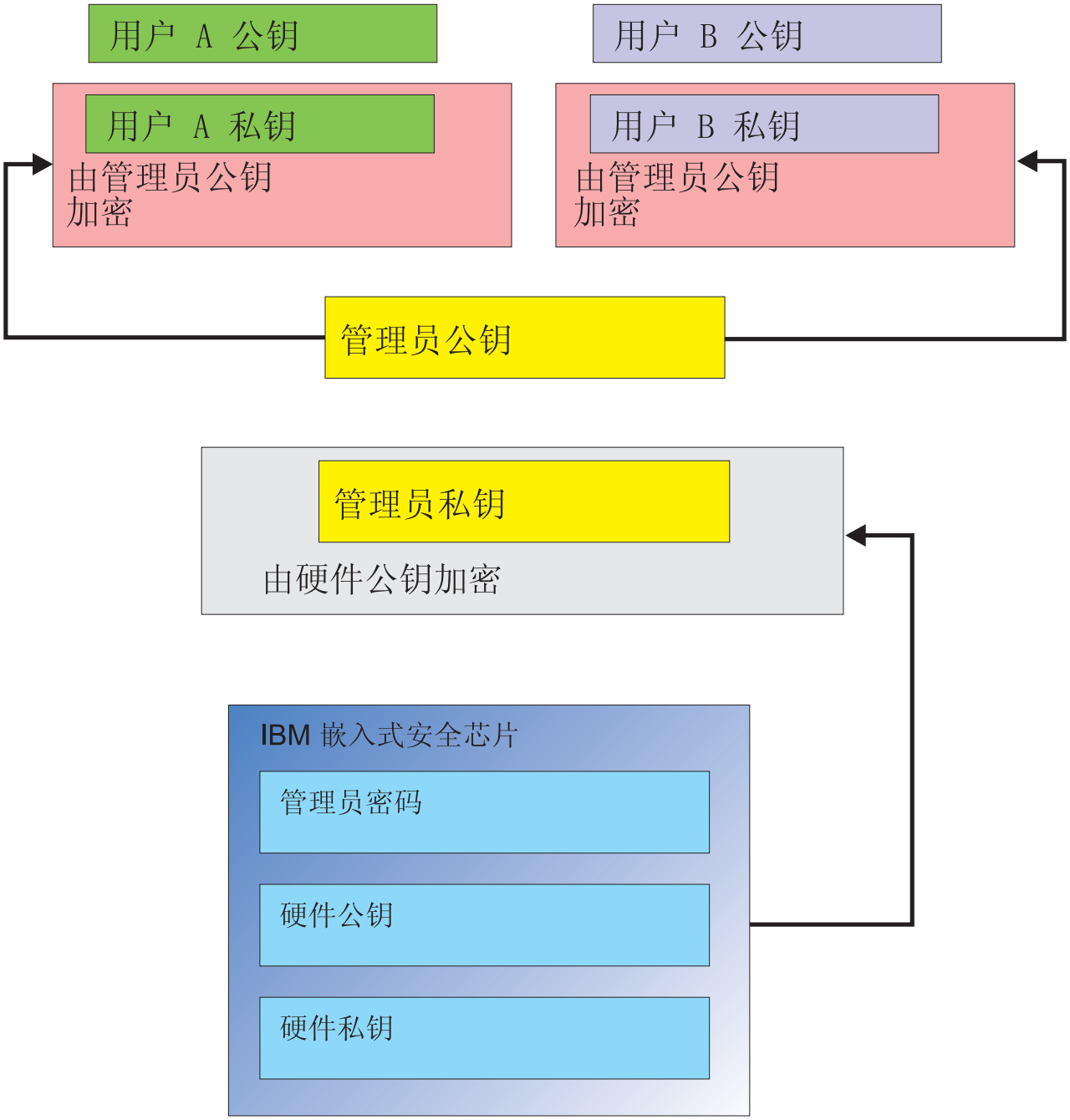


*图 3. 多层加密提供强大安全性*

## 密钥交换层次结构

IBM ESS 体系结构的一部分是“密钥交换”层次结构。*《管理员指南》*中包含精确描述该结构如何运行的详细信息；然而，在此处介绍该概念是因为其适用于大规模配置、部署和管理。在图 3 中，您可以看到硬件公钥和硬件私钥。如上文所提及，这些密钥由客户端安全软件创建并且从统计的角度来讲在每台客户机上都是唯一的。您可以在 IBM 嵌入式安全芯片上面看到管理员公钥和私钥对。管理员公钥和私钥对既可以在所有计

算机上都是唯一的，也可以在所有客户机或客户机子集上相同。这样做的优缺点将在本文档的稍后部分讨论。管理员公钥和私钥执行以下操作:

- 保护用户的公钥和私钥
- 启用用户凭证的存档和复原
- 启用*《管理员指南》* 中所述的用户凭证漫游

## 为什么要交换密钥?

在以下部分中，您将阅读有关在 IBM ESS 环境中的用户的信息。在这些部分中会涉及如何设置 IBM 客户端安全软件和 ESS 以容纳这些用户的详细信息。在这种情况下，我们只需阐明每个用户有一个公钥和私钥。用户的私钥用管理员公钥加密。从第 5 页的图 3，您可以看到管理员私钥用硬件公钥加密。为什么我们不厌其烦地加密这些不同的私钥呢？

原因必须追溯到先前提及的层次结构。由于 IBM 嵌入式安全芯片中的存储空间有限，因此在任何给定时间内芯片中仅能存在有限数量的密钥。硬件公钥和私钥是该方案中仅有的持久（从引导到引导）密钥。为了支持多个密钥和多个用户，IBM ESS 实现一种密钥交换层次结构。任何时候需要密钥，都将它“交换”到 IBM 嵌入式安全芯片中。通过将加密的私钥交换到芯片中，私钥只能在该芯片的受保护环境中解密并且使用。

管理员私钥通过硬件公钥加密。仅在芯片中可用的硬件私钥用于将管理员私钥解密。管理员私钥在芯片中解密后，可以将用户私钥（已通过管理员公钥加密）从硬盘传递到芯片中并且通过管理员私钥将其解密。从第 5 页的图 3，您可以看到可以通过管理员公钥加密多个用户私钥。它提供了使用 IBM ESS 在计算机上根据需要设置任意多个用户的能力。

# 第 3 章 密钥存档注意事项

密码和密钥以及其它可选的验证设备协同工作以验证系统用户的身份。

图 4 显示 IBM 嵌入式安全子系统和客户端安全软件如何共同工作。Windows® 登录提示用户 A 登录，用户 A 进行登录。IBM 客户端安全系统通过操作系统提供的信息确定当前用户是谁。使用硬件公钥加密的管理员私钥已装入嵌入式安全芯片中。

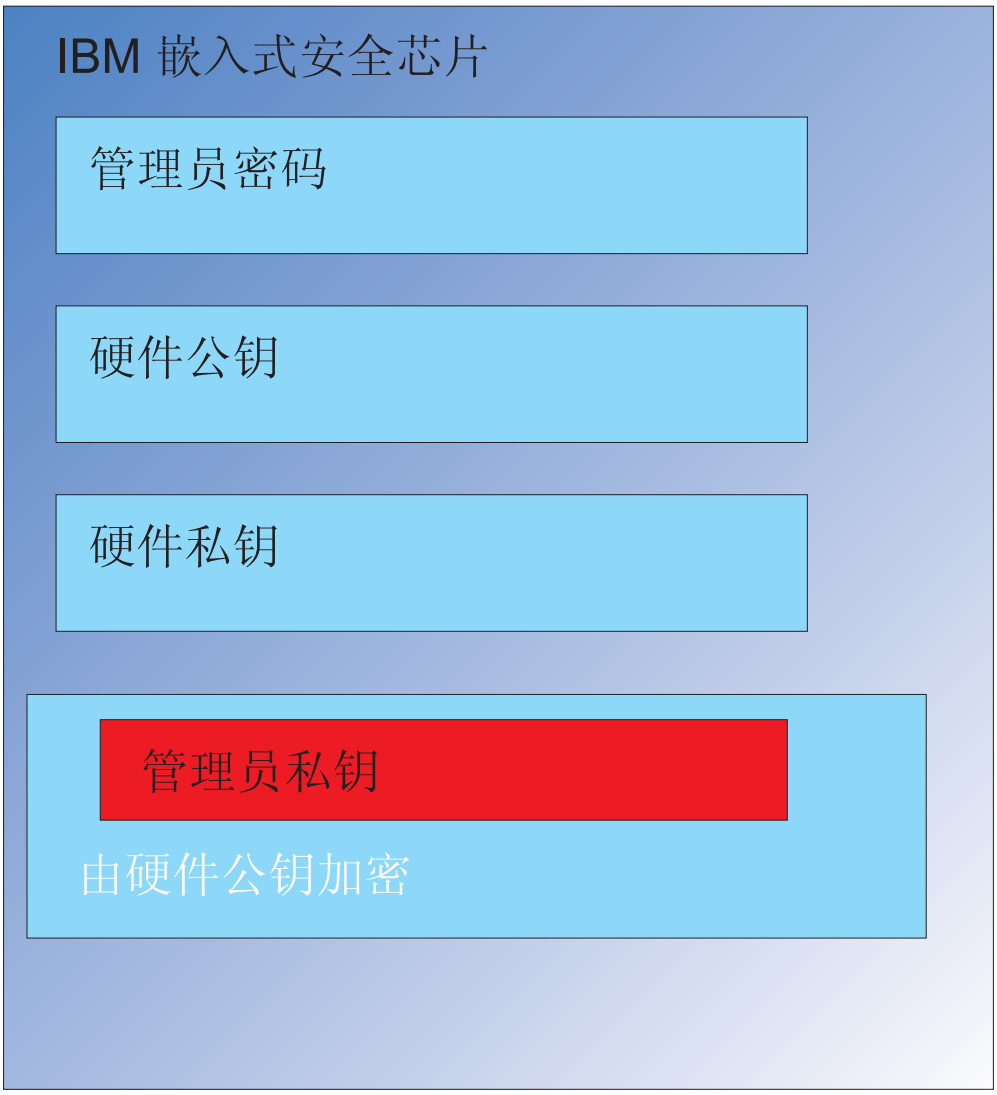


*图 4. 通过硬件公钥加密的管理员私钥已装入嵌入式安全芯片中。*

第 8 页的图 5 显示硬件私钥（仅在芯片中可用）解密管理员私钥。现在管理员私钥可在芯片中使用。

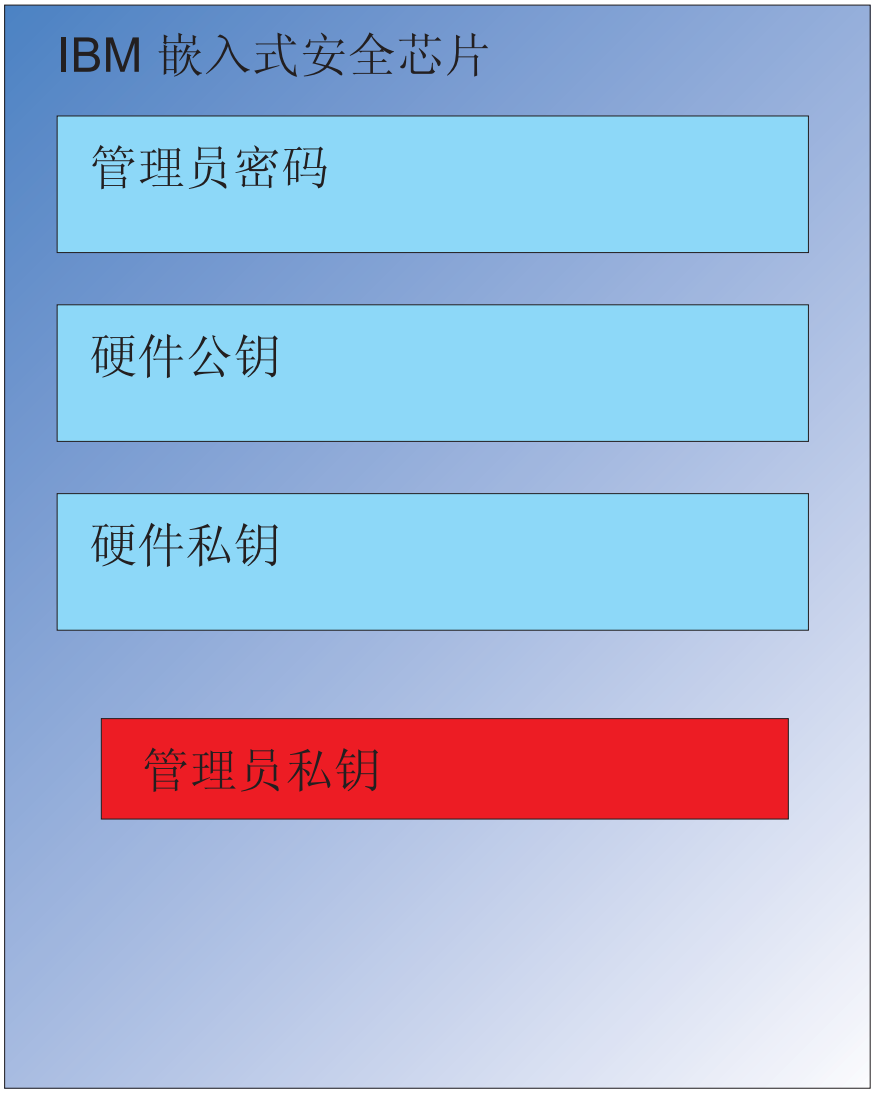


*图 5. 管理员私钥在安全芯片中可用。*

显示因为用户 A 已登录计算机，所以用户 A 的私钥（已用管理员公钥加密）被传递到如第 9 页的图 6 中所示的芯片中。

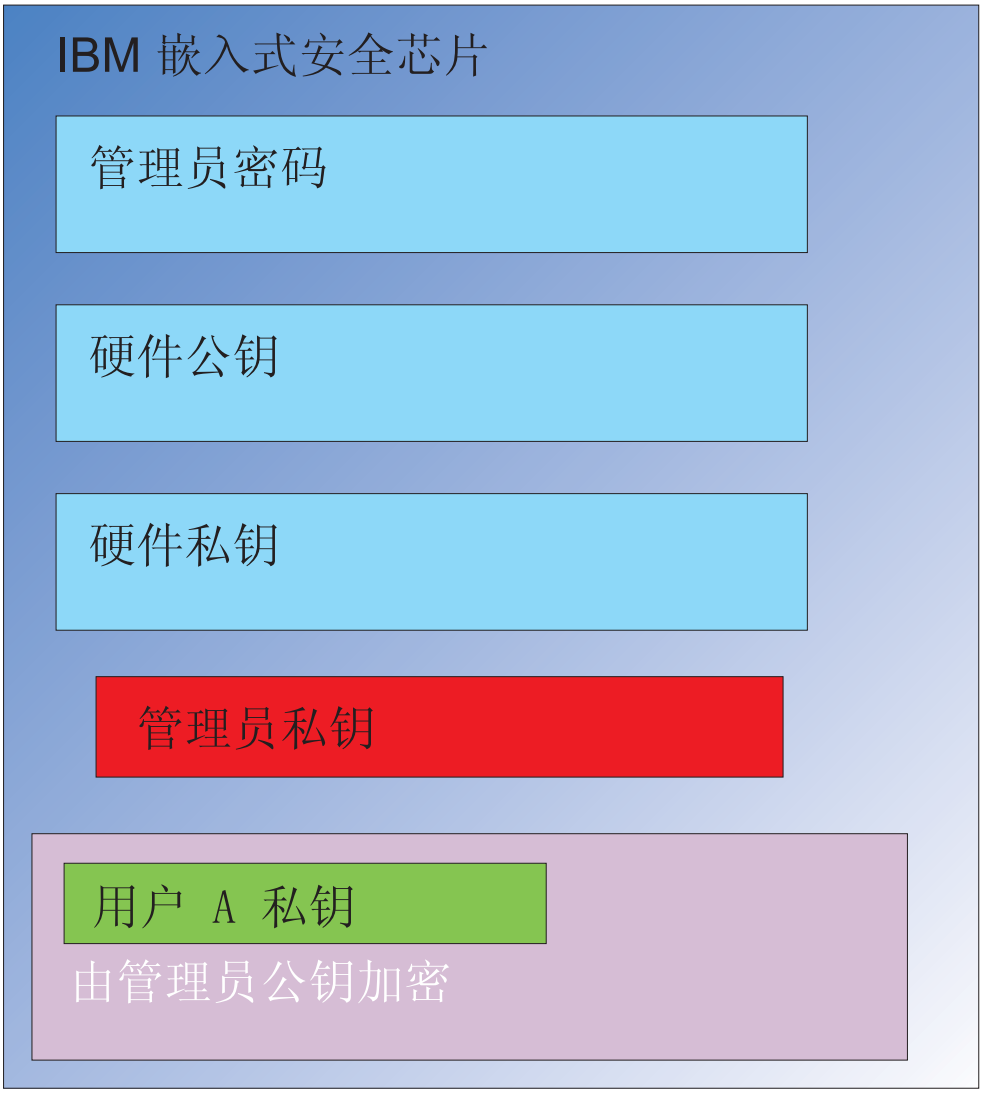


*图 6. 通过管理员公钥加密的用户 A 私钥被传递到安全芯片中。*

管理员私钥用于将用户 A 的私钥解密。现在用户 A 的私钥已准备就绪可供使用（如第 10 页的图 7 中所示）。

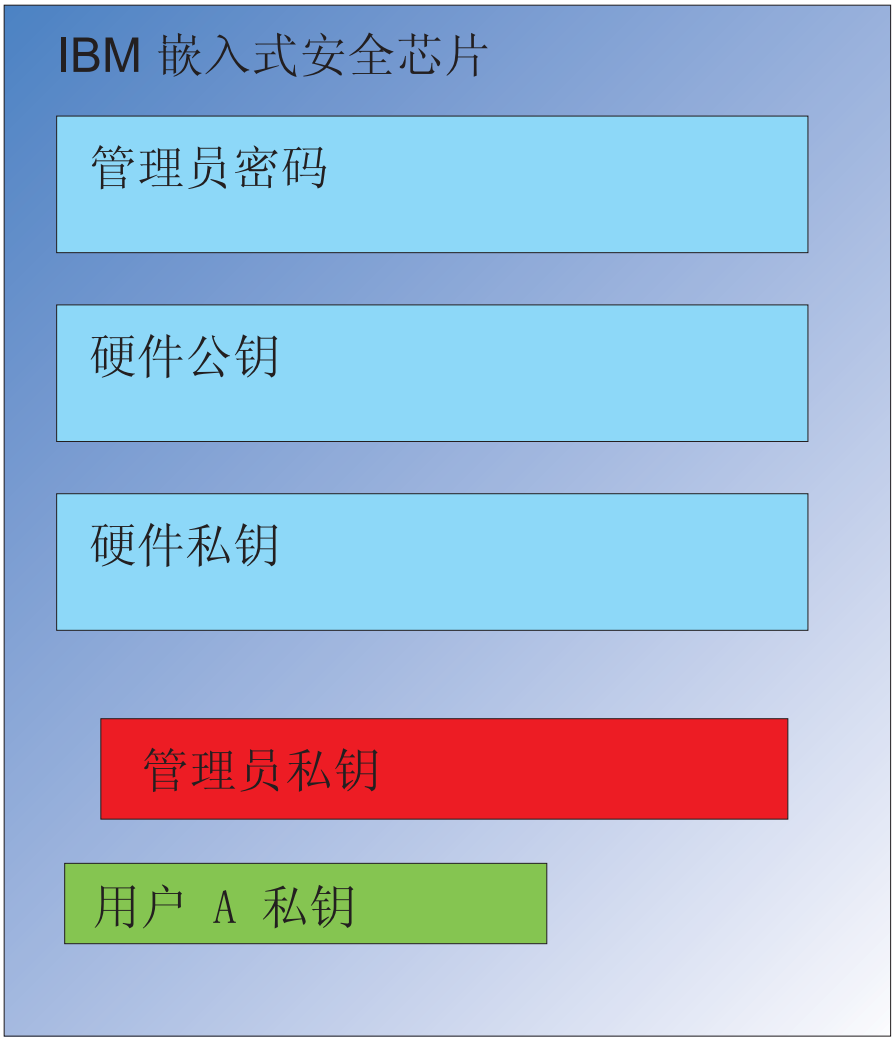


*图 7. 用户 A 的私钥已准备好可供使用。*

使用用户 A 的公钥可以加密其它几种密钥。用于签名电子邮件的私钥就是这样一个示例。当用户 A 发送已签名的电子邮件时，用于签名的私钥（已通过用户 A 的公钥加密）将被传递到芯片中。用户 A 的私钥（已位于芯片中）将解密用户 A 的签名私钥。现在，用户 A 的签名私钥在芯片中可用于执行期望的操作，在本示例中该操作是创建数字签名（加密散列）。请注意，当用户 B 登录到计算机上时，将采用相同的密钥移入和移出芯片的过程。

## 为什么使用管理员密钥对?

使用管理员密钥对的主要原因是为了实现存档和复原能力。管理员密钥对作为芯片和用户凭证之间的抽象层。如第 11 页的图 8 中所示，特定于用户的私钥信息使用管理员公钥加密。

**要点**：开发用于保持管理员密钥对的策略。有可能每台带有嵌入式安全新片的计算会拥有相同的管理员密码（如果 IT 管理员或安全管理员有意如此确定的话）。或者，也可以给每个部门或大楼指定不同的管理员密钥对。

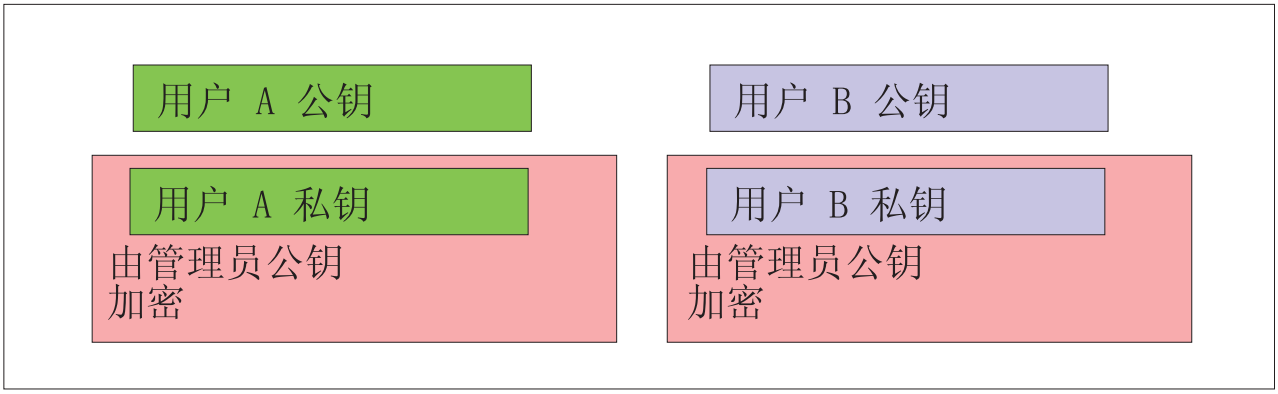


*图 8. 特定于用户的私钥信息通过管理员公钥加密。*

使用管理员密钥对的另外一个原因是签名客户端安全策略文件，从而防止除管理员以外的任何人更改安全策略。为了获得客户端安全策略文件的高等级安全性，您可以在多达五个人之间分割管理员私钥。在这种情况下，拥有私钥一部分的五个人都必须出来签名并且加密文件（例如客户端安全策略文件）。这样就能防止个人单方面执行管理员功能。有关分割管理员私钥的信息，请参阅第 34 页的表 4 中的 Keysplit=1 设置。

在 IBM 客户端安全软件初始化过程中，管理员密钥对可以通过软件创建或者可以从外部文件导入。如果您希望使用公共管理员密钥对，则您需要在客户机安装过程中指定所需文件的位置。

如图 8 中所示，将特定于该用户的信息备份到（写入）管理员定义的存档位置。该存档位置可以是物理上或逻辑上连接到客户机的任何类型的介质。IBM 客户端安全系统安装部分将讨论该存档位置的最佳做法。

管理员公钥和私钥未存档。存档位置中的用户数据通过管理员公钥加密。如果您没有解锁数据的管理员私钥，则用户存档数据本身对您没有什么用处。管理员公钥和私钥通常在 IBM 客户端安全软件文档中涉及，称为 “密钥对存档”。请注意，存档私钥未加密。在存储和保护密钥对存档时必须多加注意。

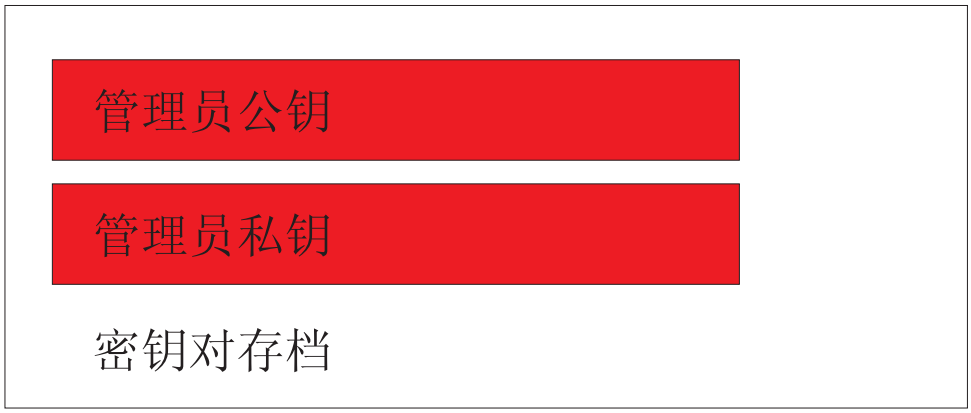


*图 9. 管理员公钥和私钥组成密钥对存档。*

如上文所提及，管理员公钥和私钥的最重要功能之一就是备份和复原磁盘内容。该功能已在10 到15 中显示。步骤如下:

1. 如图 10 中所示，客户机 A 由于某些原因对于用户 A 不可用。在该示例中，我们假定计算机（客户机 A）受到雷击。

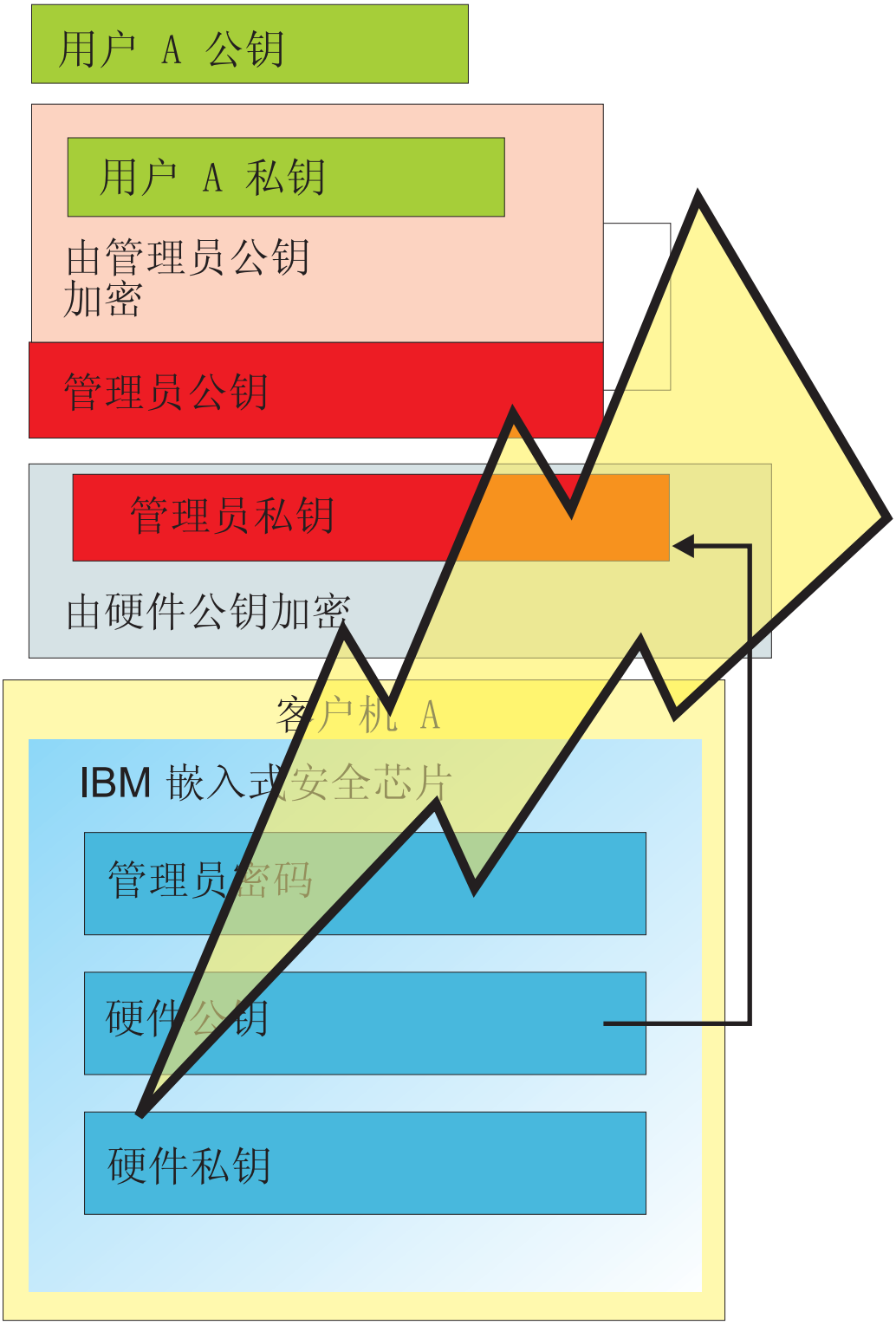


*图 10. 用户 A 的计算机受雷击，从而无法使用。*

2. 用户 A 获得新的改进的 IBM 计算机，称为客户机 B（如第 13 页的图 11 所示）。客户机 B 与客户机 A 的不同之处在于其硬件公钥和私钥与客户机 A 的不同。视

觉上这种区别在客户机 B 中用灰色密钥表示，而在客户机 A 中用绿色密钥来表示。然而，请注意，在客户机 B 和客户机 A 中管理员密码是相同的。

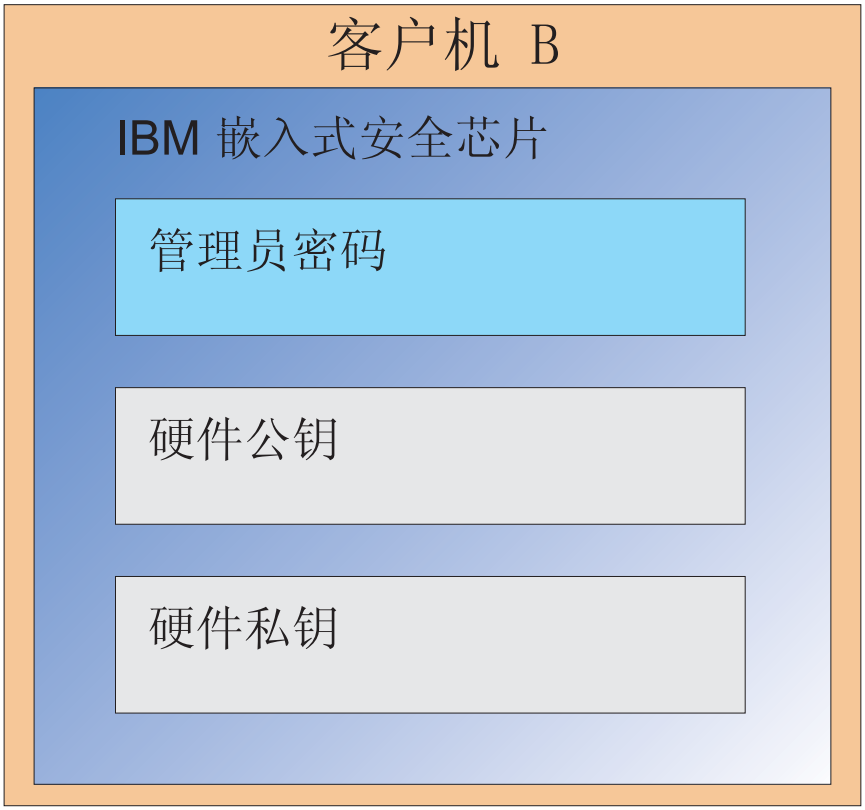


*图 11. 用户 A 接收新的计算机，就是带有新的嵌入式安全芯片的客户机 B。*

3. 客户机 B 现在需要与客户机 A 上相同的用户凭证。该信息已从客户机 A 存档。如果回顾第 11 页的图 8，则您将回想起用户密钥已通过管理员公钥加密并且被存储在存档位置中。为了使该用户凭证在客户机 B 上可用，必须将管理员公钥和私钥传送到该机器上。图 12 显示客户机 B 从存档位置检索管理员公钥和私钥以恢复用户数据。

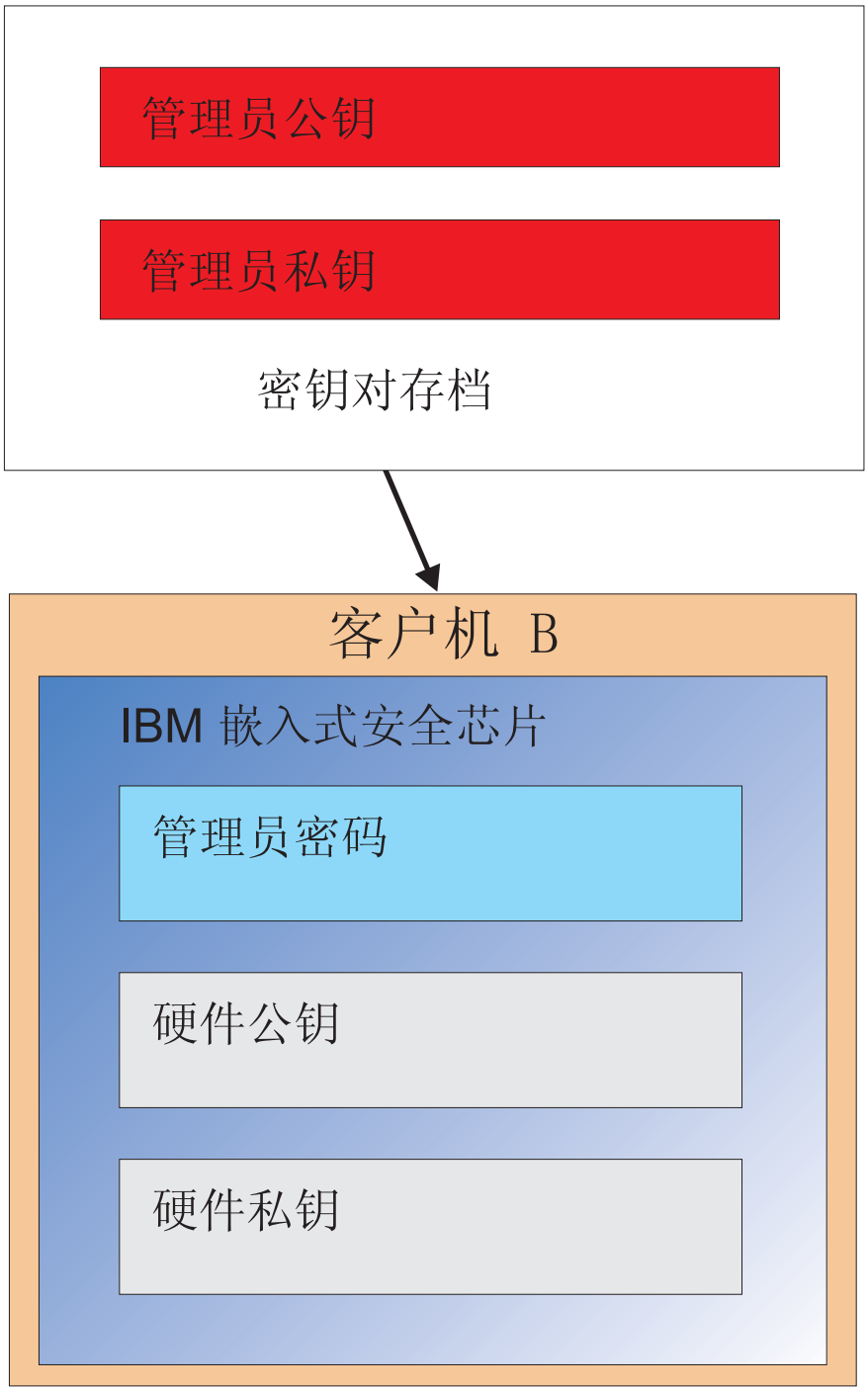


*图 12. 客户机 B 从存档位置检索管理员公钥和私钥。*

4. 第 15 页的图 13 显示正使用客户机 B 的硬件公钥加密管理员私钥。

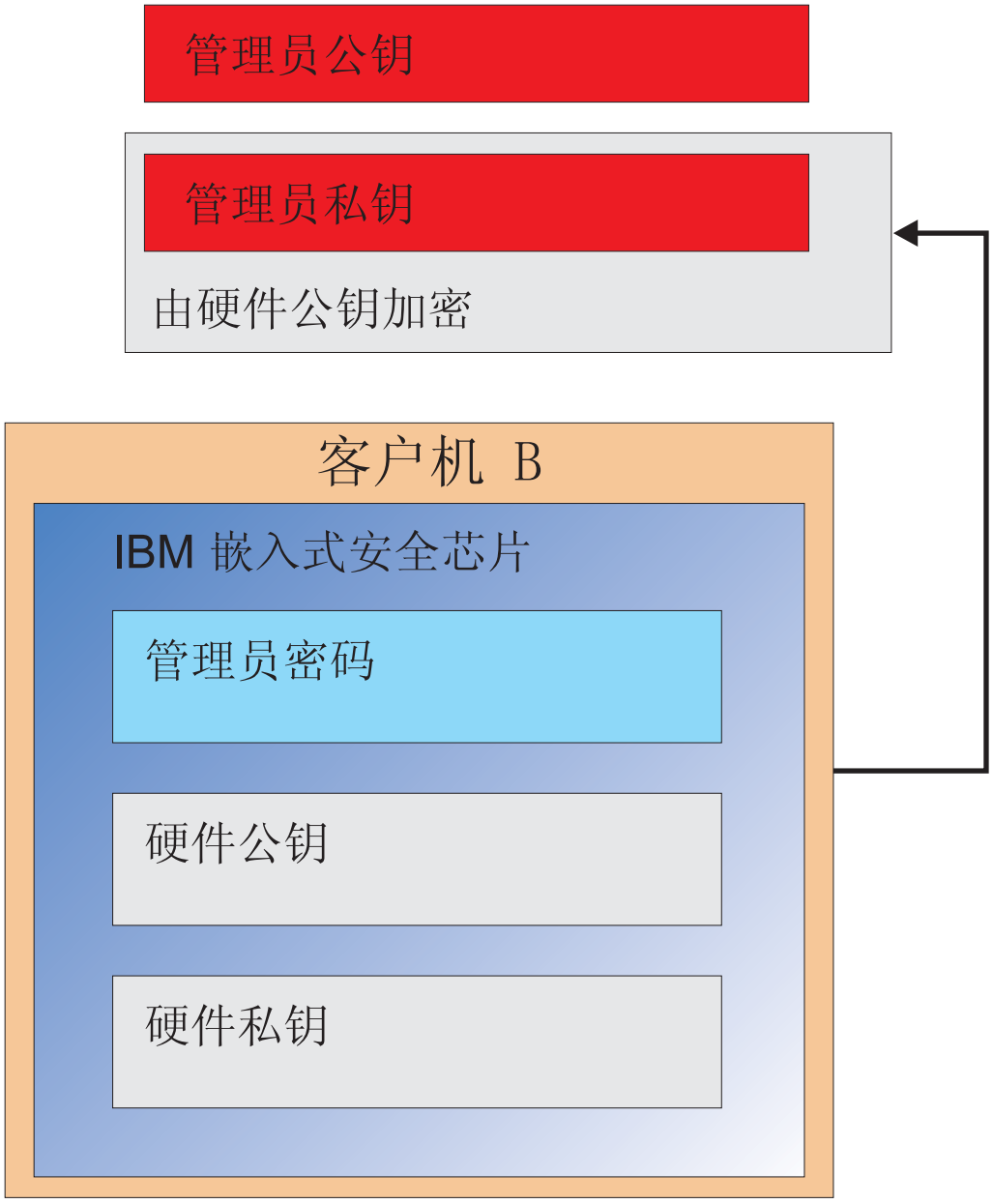


*图 13. 管理员私钥通过客户机 B 硬件密钥加密。*

现在，管理员私钥已使用硬件公钥加密，可以为客户机 B 上用户 A 导入用户凭证（如第 16 页的图 14 中所示）。

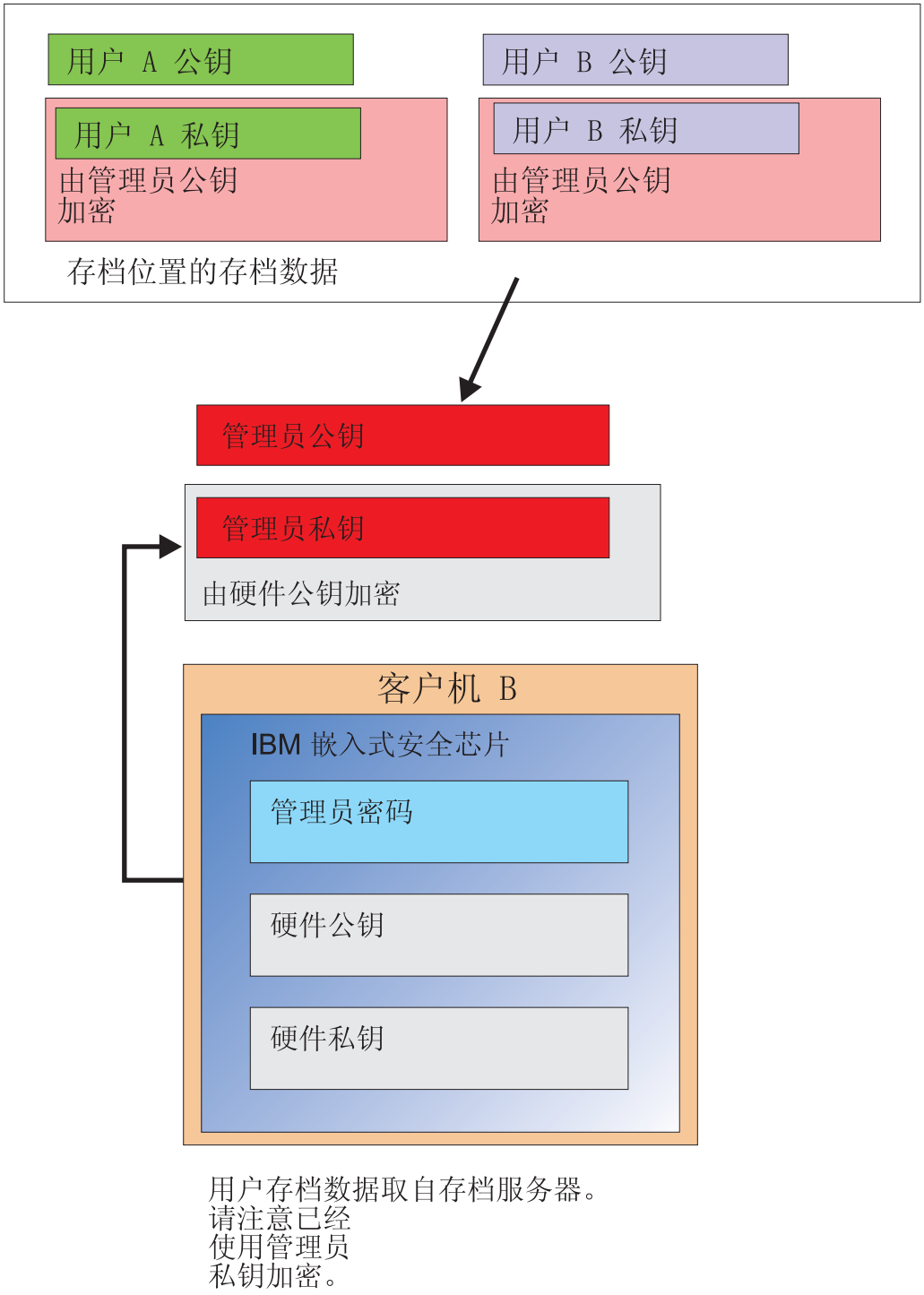


*图 14. 用户 A 的凭证可以在加密管理员私钥后装入客户机 B。*

第 17 页的图 15 显示用户 A 在客户机 B 上完全复原。请注意，当位于存档服务器上时，用户 A 的私钥已用管理员公钥加密。管理员公钥是 2048 位 RSA 密钥，且几乎不可能破解。这意味着存档位置不必受保护或者拥有强大的访问控制。只要安全地保护存档密钥对（管理员公钥和私钥，更确切的讲是管理员私钥），则用户凭证的存档位置基本上可以在任何地方。

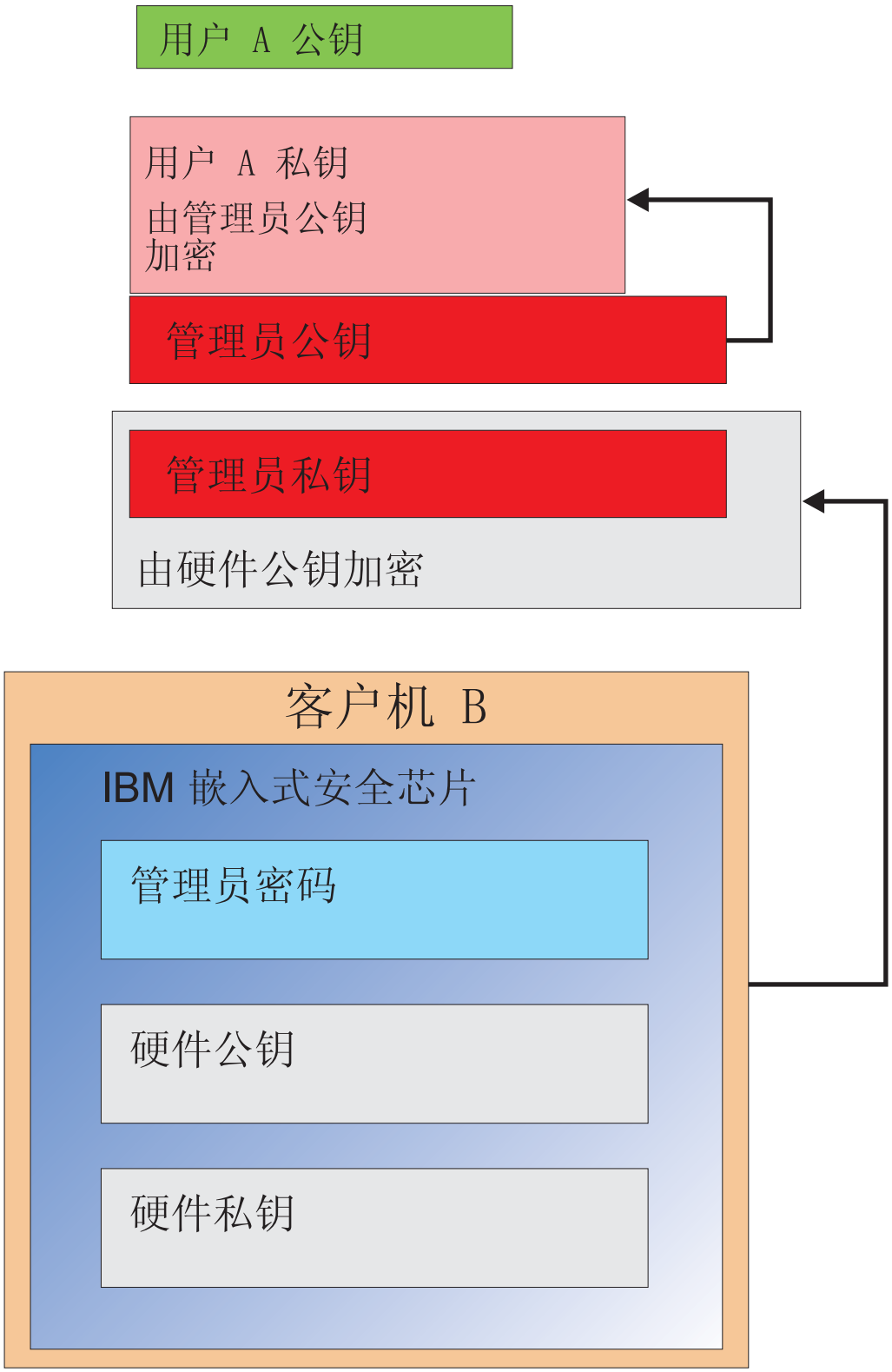


*图 15. 用户 A 在客户机 B 上完全复原。*

在软件安装部分将更加详细地讨论如何设置管理员密码、存档位置应该在哪里等详细信息。图 16 显示 ESS 环境中的组件的概述。要点是从硬件公钥和私钥的角度来看每

台客户机都是唯一的，但是都具有公共的管理员公钥和私钥。客户机拥有公共的存档位置，但是该存档位置可以用于用户段或用户组。

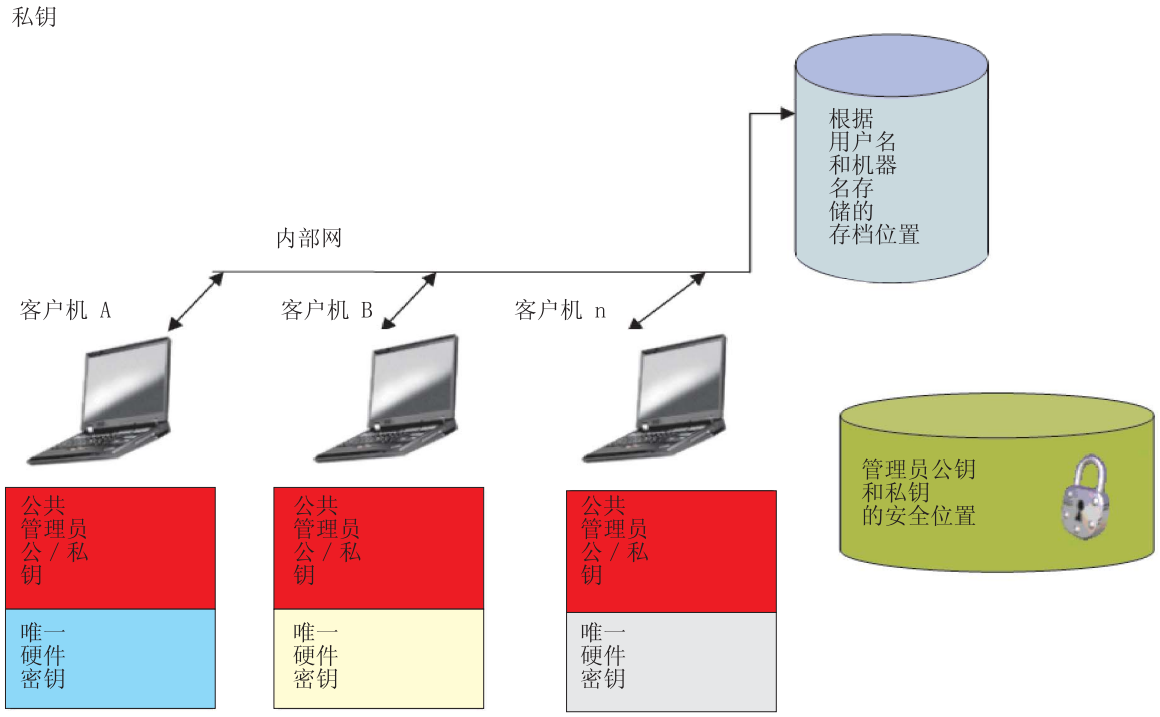


*图 16. IBM 客户端安全系统的主要组件。*

让我们来看以下示例。人力资源部可以拥有与工程部不同的存档位置。存档在用户名和计算机名的基础上完成。如先前在用户 A 和用户 B 中所示，IBM 客户端安全软件将根据用户名和计算机名将系统用户存档到定义的存档位置。还请注意管理员公钥和私钥的安全位置。

**注:** 将存档到相同位置的每个计算机名和用户名都必须是唯一的。重复的计算机名或用户名将覆盖相同名称的先前存档。

# 第 4 章 IBM 客户端安全软件

IBM 客户端安全软件是应用程序和 IBM 嵌入式安全芯片之间的连接，也是登记用户、设置策略和执行基本管理功能的界面。IBM 客户端安全系统实质上由以下组件构成:

- 管理员实用程序
- 用户配置实用程序
- 管理员控制台
- 安装向导
- 用户验证管理器（UVM）
- 加密服务提供程序
- PKCS#11 模块

IBM 客户端安全系统使您能够执行多个关键功能:

- 登记用户
- 设置策略
- 设置口令策略
- 重新设置遗忘的口令
- 复原用户凭证

例如，如果用户 A 登录到操作系统，则 IBM 客户端安全系统的所有决策都基于用户 A 已登录而假定。（**注**: 安全策略基于机器而不是用户；该策略应用到单个计算机的所有用户上。）如果用户 A 尝试利用 IBM 嵌入式安全子系统，则 IBM 客户端安全系统将在该计算机上强制执行为用户 A 设置的安全策略，例如口令或指纹验证。如果有人作为用户 A 登录而无法提供正确的口令或正确的指纹以进行验证，则 IBM ESS 将禁止该用户执行请求的操作。

## 登记用户和管理登记

IBM ESS 用户只是在 IBM ESS 环境中登记的 Windows 用户。用户可以使用几种方法登记，稍后在本文档中会涉及有关详细信息。在本部分中，我们将涉及用户登记时发生的情况。了解在该过程中发生的情况将使您能够更好地了解 IBM ESS 如何工作，并且最终如何在您的环境中成功管理 ESS。

客户端安全软件使用用户验证管理工具（UVM）管理口令和其它元素来验证系统用户。UVM 软件支持以下功能:

- UVM 客户端策略保护
- UVM 系统登录保护
- UVM 客户端安全屏幕保护程序保护

IBM ESS 环境中的每个用户至少有一个与他或她关联的个性化对象，该对象用于进行验证。口令是最低要求。ESS 环境的 UVM 组件中的每个用户（从用户的角度来说，UVM 管理验证并且强制执行安全策略）必须有一个口令并且该口令必须至少为每次计算机启动给出一次。以下部分将解释为什么使用口令、如何设置口令以及如何使用口令。

## 要求口令

简单地说，要求口令是出于安全的目的。具有硬件元素（例如 IBM 嵌入式安全子系统）有极大好处，因为它为在其上进行操作的用户凭证提供安全、自治的位置。然而，如果访问芯片所要求的验证较弱时，硬件芯片提供的保护几乎不起作用。例如，设想您具有执行安全功能的硬件芯片。然而，调用芯片执行操作所要求的验证是单位数。这样使得潜在的黑客可能猜出单位数（0 到 9）来调用您的安全证书执行操作。单位数验证削弱了芯片的安全性以致于它在基于软件的解决方案上提供极少或不提供更多的好处。如果您没有结合硬件保护的强验证，则您将得不到任何安全性。IBM ESS 要求的口令用于在使用硬件中的用户凭证进行任何操作之前验证用户。UVM 口令仅可用管理员密钥对恢复，因此它无法从窃用系统检索。

## 设置口令

每个用户选择口令以保护其凭证。在第 3 页的第 2 章，『嵌入式安全芯片如何运行』中，您看到用户的私钥通过管理员公钥加密。用户私钥还具有关联的口令。该口令用于使用用户的安全证书来验证用户。图 17 显示通过管理员公钥加密的口令与私钥组件。

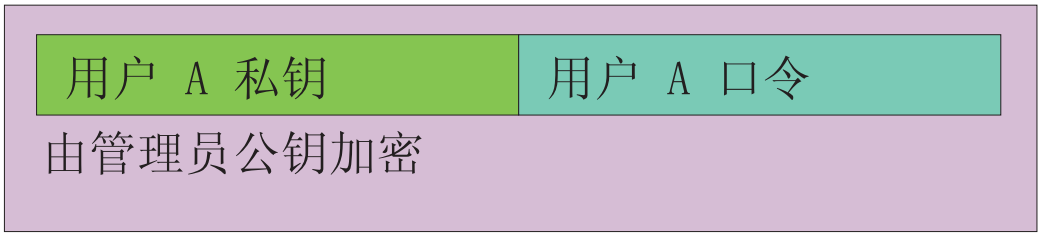


*图 17. 用户 A 必须提供口令以执行要求用户 A 私钥的任何功能。*

在图 17中描述的口令由用户根据现有的策略选定，即，位于控制密码创建中的规则（例如，字符个数和密码有效的天数）。当用户登记到 UVM 中时，将创建口令。需要再次指出的是，大量部署 IBM 客户端安全软件时，该情况实际如何发生将稍后在本文档中讨论。

由于将该私钥解密要求管理员私钥，所以用户 A 的私钥通过管理员公钥加密。因此，如果忘记用户 A 的口令，则管理员可以重新设置新的口令。

## 使用口令

第 21 页的图 18 到第 23 页的图 20，显示了如何在芯片上处理用户口令。每个会话必须始终首先使用口令且至少要使用一次。始终要求口令。可以选择添加其它验证设备，但是这些验证设备中没有一个设备可以替换初始的用户口令要求。简而言之，生物验证或其它验证数据通过用户公钥加密。要将该附加安全数据解密，必须访问私钥。


*图 18. 管理员私钥在芯片中解密。*

因此，要将其它数据解密，要求每个会话至少提供一次口令。将组成用管理员公钥加密的用户 A 私钥和用户 A 口令的凭证传递到 IBM 嵌入式安全芯片中。如上文所述，管理员私钥已在芯片中解密。凭证如第 22 页的图 19 中所述传递。

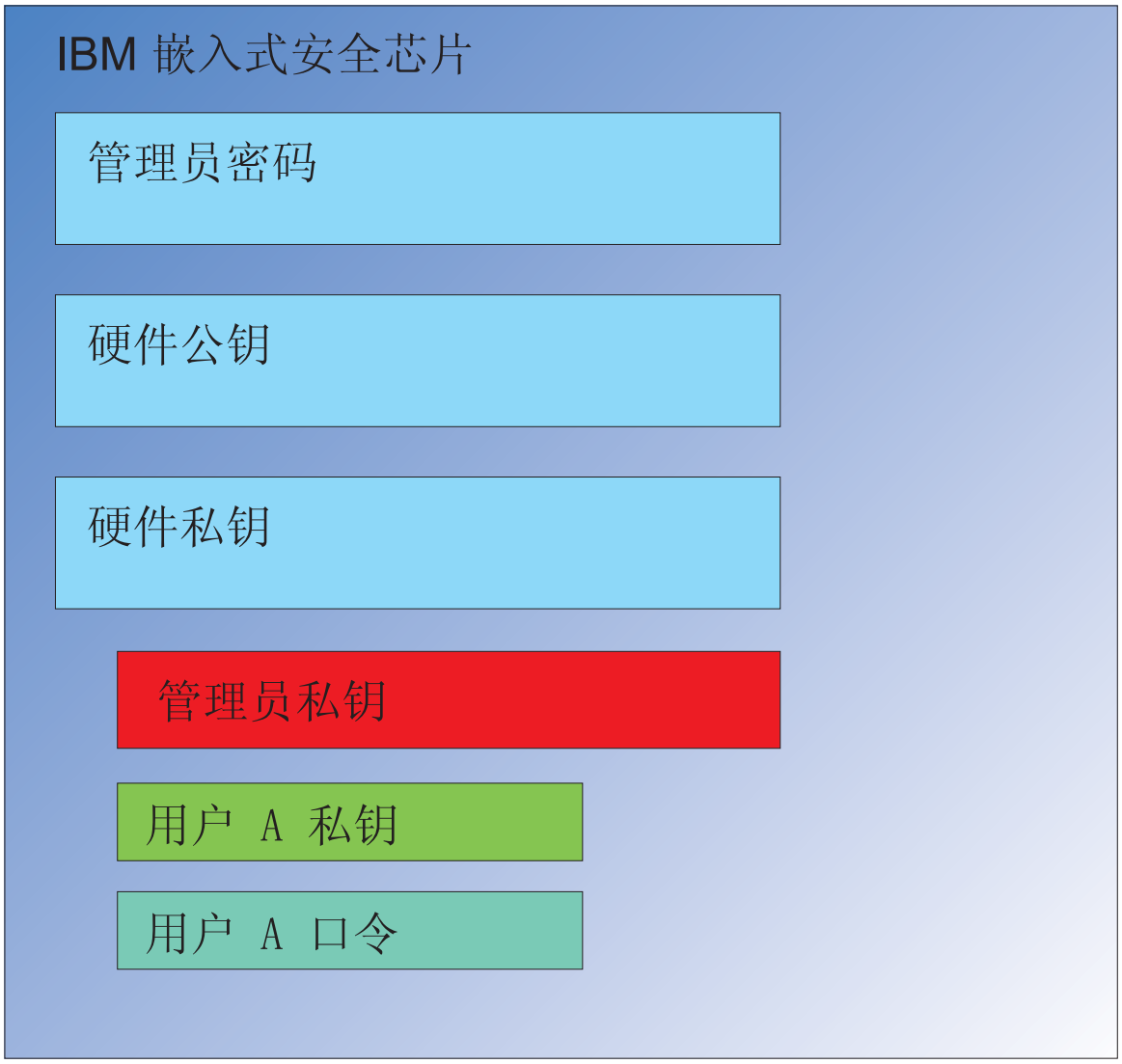


*图 19. 用户 A 的私钥和用户 A 的口令在芯片中可用。*

将凭证解密，使用户 A 的私钥和用户 A 的口令在芯片中可用。当由 IBM 客户端安全系统标识为用户 A 的当前登录的用户尝试使用用户 A 的凭证时，口令对话框将打开，如第 23 页的图 20中所示。

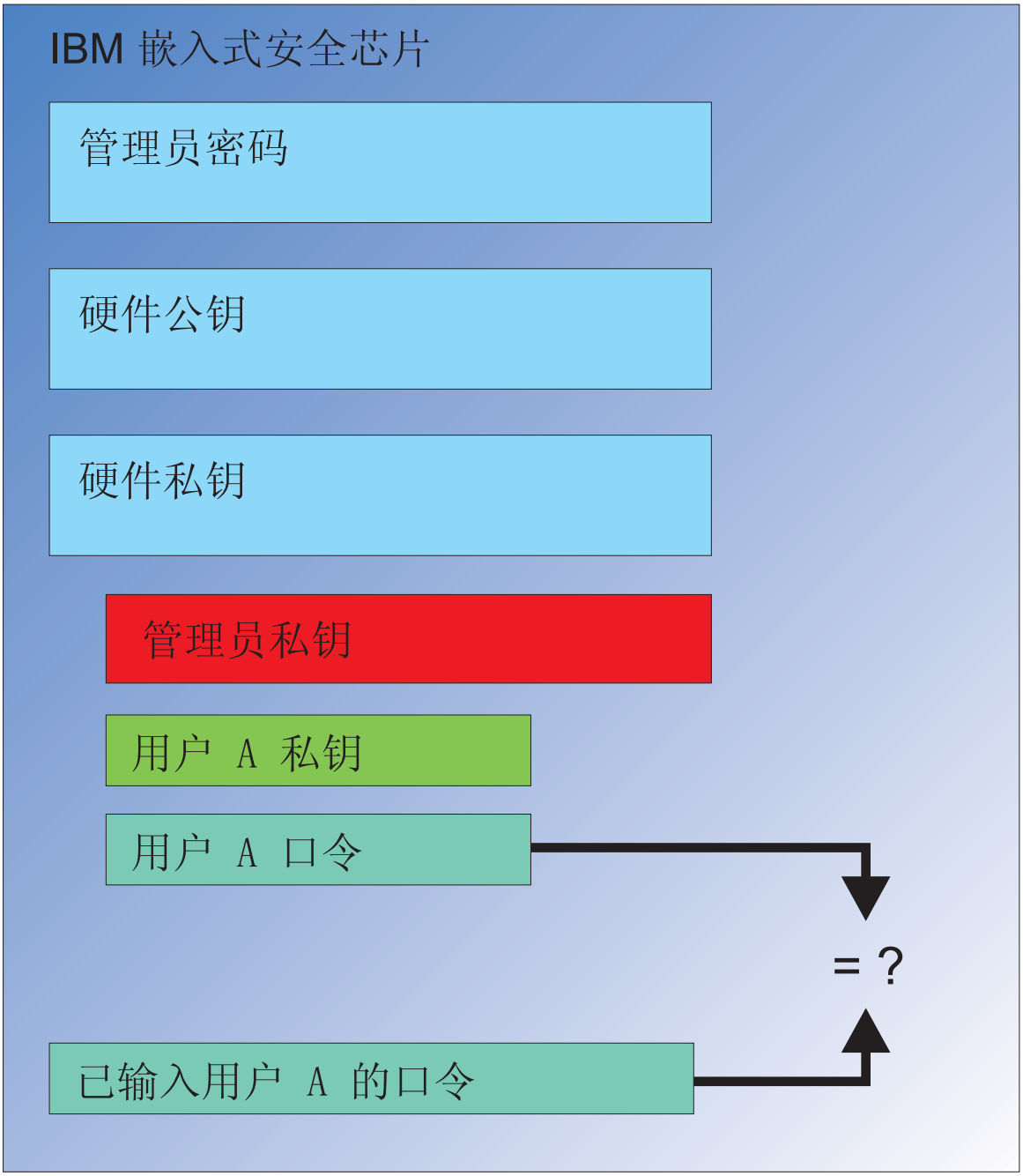


*图 20. 如果用户 A 尝试使用用户 A 的凭证，则口令对话框将打开。*

输入的口令被传递到芯片并且与解密的口令值进行比较。如果它们匹配，则用户 A 的凭证可以用于各种功能，例如数字签名或将电子邮件解密。请注意，该口令比较在芯片的安全环境中完成。芯片具有防攻击能力以检测重复失败的访问尝试。还请注意用户 A 注册的口令从不暴露在芯片外。用户登记作为 IBM 客户端安全软件安装的一部分。该登记过程的一部分是创建用户的口令。我们将讨论如何设置该口令以及可以如何强制执行口令规则的详细信息。

第 1 页的图 1 显示 IBM 嵌入式安全芯片和 IBM 客户端安全系统。第 1 页的图 1 还描述了公司初始化和用户初始化。公司初始化与嵌入式安全子系统关联且用户初始化与

IBM 客户端安全软件关联。前面部分描述了进行的初始化以提供对一般概念的理解。以下部分将提供有关初始化过程的更多详细信息。

## TPM 初始化

TPM 初始化实质上是添加硬件公钥和私钥以及管理员密码的过程。该过程采用从 IBM 装运的通用机器并且使其对您的企业来说是唯一的。以下图表将显示初始化公钥和私钥以及管理员密码的方法。

*表 1. 硬件初始化方法*

| 操作 | 可以在 BIOS 中创建 | 可以在 CSS 软件中由管理员手动创建 | 可以在脚本中创建 |
|---|---|---|---|
| 硬件公钥 / 私钥创建 | 否 | 是 | 是 |
| 管理员密码创建 | 是（在某些兼容 TCPA 的客户机上）。请检查 BIOS 条目。 | 是 | 是 |

表 1 证明硬件公钥和私钥并非在安装软件时自动创建。必须在软件中或者通过脚本手动启动硬件公钥和私钥的创建。管理员密码可以在 BIOS、IBM 客户端安全软件应用程序中创建或者通过脚本创建。芯片控制为硬件公钥和私钥设置的值；您无法设置这些值。芯片中的随机数功能用于产生在统计上随机的公钥和私钥对。然而，您确实设置了管理员密码。

不过，由于管理员必须设置该值，所以管理员密码会有所不同。必须解决与管理员密码相关的几个问题:

- 您将设置什么密码来作为管理员的一个或多个密码？
- 是否具有多个密码以用于不同的组？如果需要多个密码，则您逻辑上将如何确定哪些计算机拥有哪个密码？
- 哪个管理员将具有密码访问权？如果您有多个密码用于不同的用户组，则谁将对哪个密码具有访问权？
- 自我管理的最终用户是否将对管理员密码具有访问权？

要根据以上各项得出有效决策，了解管理员密码使您能够执行的操作很重要:

- 获取对管理员实用程序的访问权
- 添加 / 删除用户
- 定义可以使用哪些 IBM 客户端安全软件应用程序 / 功能

后继部分将解释策略文件和管理员私钥之间的关系。现在请注意管理员私钥是更改策略所必需的。表 2 总结了拥有管理员密码和 / 或管理员私钥的能力。

*表 2. 基于密码和私钥的管理员操作*

| 操作 | 管理员密码 | 管理员私钥 |
|---|---|---|
| 获取对管理员实用程序的访问权 | 是 | 否 |
| 添加 / 删除 / 复原用户 | 是 | 否 |
| 定义可以使用哪一个 CSS 应用程序 / 功能 | 是 | 否 |

*表 2. 基于密码和私钥的管理员操作 (续)*

| 操作 | 管理员密码 | 管理员私钥 |
| --- | --- | --- |
| 定义 / 更改策略 | 是 | 是 |
| 创建文件以重新设置用户的口令 | 是 | 是 |

TPM 初始化也涉及管理员公钥和私钥。从以上图表您可以查看与该密钥关联的能力。提供某些想法以设置管理员公钥和私钥。该密钥对对于每台计算机可以是唯一的或者它对于所有机器可以是相同的。当初始化 IBM 客户端安全软件时，管理员将可以选择对于客户机使用现有密钥对或创建新的密钥对。使用型号将再一次确定对您企业的最佳做法。

# 最佳做法

大型企业可以针对每台机器或者每个部门使用唯一密钥。例如，为所有用于人力资源部的计算机设置一个管理员密码和 / 或管理员私钥，为工程部设置另一个管理员密码和 / 或管理员私钥等等。可以从物理上区分，例如根据大楼或站点位置。根据谁请求复位，在创建口令复位文件时能够确定使用哪一个管理员私钥应该是一个方便的过程。如第 24 页的表 1 和第 27 页的表 3 所表明，用户和公司或者硬件必须进行初始化。

## 部署 CSS 前设置安全策略

安全和验证需求将来自组织中有趣的各方。虽然具有管理员访问权的个人可以进行策略更改并可以将它们“推入”客户机（请参阅第 49 页的第 7 章，『远程部署新的或已修正的安全策略文件』），但是部署前配置策略设置将可以获取最佳效果。有关设置策略的其它信息，请参阅*《客户端安全软件管理员指南》*中的“处理 UVM 策略”。

## 为忘记了口令或验证设备出现故障作准备

用户不可避免会忘记口令并且验证设备（如指纹生物统计法验证设备或智能卡）也可能无法正常工作。

***忘记了口令:*** 用户口令不是以人类可读的格式存储在客户机硬盘或嵌入式安全芯片中的某处。它安全地记在用户的脑海中并存储在另一个地方: 由管理员密钥对保护的存档文档中。管理员将需要使用管理员私钥对存档文档中的用户信息进行解密。然后管理员才可以向用户提供解密后的口令。

当用户更改口令后，新的信息将被存档到指定的存档位置。

如果验证设备出现故障，您可以配置 IBM 客户端安全软件以显示**单击此处忽略**按钮。只要单击忽略按钮就会请求用户成功输入口令。然后用户可以执行安全任务。

要配置 CSS 显示忽略按钮，请执行以下操作:

1. 在 CSEC.INI 文件（位于根目录下）中找到 `AllowBypass= 0` 项。缺省值 `0` 设置了 CSS 隐藏忽略按钮。
2. 将 `AllowBypass` 值设置为 1。CSS 窗口请求用户时显示忽略按钮以提供除口令以外的验证。
3. 保存 CSEC.INI 文件。

**注:**

1. 要存档该信息，主要是必须在 CSEC.INI 文件的 `kal=c:\jgk\archive` 中指定存档位置。并且，如果 c:\jgk\archive 是网络驱动器，则要存档口令，必须在客户机中映射了该驱动器。
2. 如果未指定存档位置并且未在客户机中映射该位置，则无法恢复口令。

## 用户初始化

IBM ESS 提供几个用户在单台计算机上执行独立和安全事务的能力。这些用户必须具有与其关联的口令并且可以另外具有其它验证元素，例如指纹和 / 或智能卡。这称为*多因素授权*。用户初始化是配置客户机以使用 IBM ESS 的一个关键步骤。请注意，用户初始化是一个两步骤的过程:

1. 注册
2. 个性化

### 注册

注册只是将用户添加到 IBM 客户端安全系统或者向 IBM 客户端安全系统注册用户。在图 21 中，您可以查看 IBM 客户端安全软件的用户验证管理器（UVM）组件。UVM 控制每个用户的凭证并且强制执行策略。

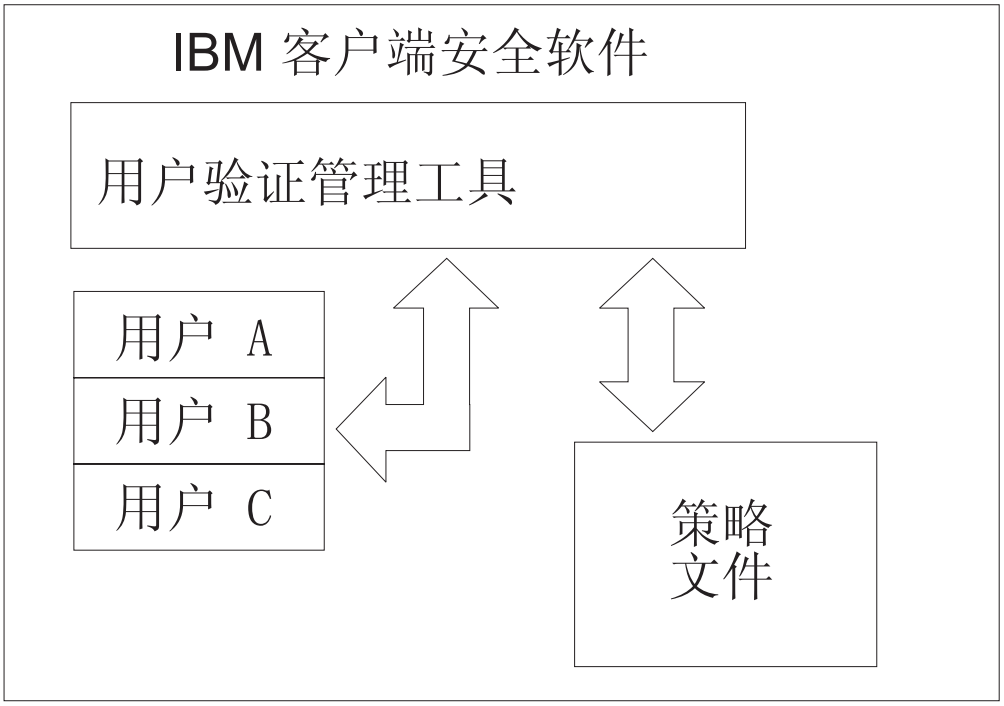


*图 21. 用户验证管理器控制每个用户的凭证并且强制实施安全策略。*

策略文件（如图 21 中所描述）包含 UVM 管理的每个用户的验证要求。请注意，UVM 用户只是 Windows 用户（本地或域）。UVM 基于当前登录到计算机和操作系统的用户来管理凭证。例如，如果用户 A 登录到 Windows 并且用户 A 也是 UVM 的一部分，则 UVM 将在用户 A 尝试执行需要凭证的操作时强制实施策略。另举例，用户 A 登录到计算机上。然后，用户 A 转到 Microsoft® Outlook 中并且发送数字签名的电子邮件。用于发送该数字签名的电子邮件的私钥在 IBM 嵌入式安全子系统中受保护。在

UVM 允许执行该操作之前，它将如策略文件中定义的那样强制实施策略。在该示例中，只要求在执行操作之前验证口令。UVM 将提示用户要求口令并且如果它验证正确，则将在芯片中应该执行私钥操作。

## 个人初始化

个人初始化只是设置单独的个人 UVM 口令。不同的人可以执行过程的不同部分。个人的 UVM 口令仅对个人已知。然而，如果每个人都不执行初始化过程，则该用户可能需要执行其它步骤。UVM 也可以配置为强制用户在其首次登录时更改口令。

例如，用户 A 由 IT 管理员来初始化。该 IT 管理员从 Windows 用户列表（例如从域）选择用户 A。UVM 要求 UVM 口令与用户 A 关联。IT 管理员输入 “IT 管理员口令” 的 “缺省值”。要确保系统的安全性，用户 A 在接收系统后必须定制口令以防止任何人使用缺省口令执行安全事务。

*表 3. 用户初始化的方法*

| 方法 | 命令过程 | 过程要求 |
| --- | --- | --- |
| 手工 | 管理员可以通过管理员实用程序手动个性化用户的 CSS。 | 为了设置计算机，管理员必须呆在每台计算机旁边。 |
| 管理员配置文件 | 管理员可以创建包含管理员密码的已加密版本的配置文件。该文件已发送给用户，该用户随后可以单独登记而无需管理员干预或在场。 | 用户完成设置过程。 |
| *.ini | 管理员创建执行 .ini 文件并且设置缺省或个性化密码的脚本。 | 管理员或用户是否在场是可选的。 |

## 部署方案

您要将 1,000 台客户机部署给 1,000 个最终用户。以下方法之一可以描述您的部署方法:

- 您确切知道哪一台机器正部署到哪一个最终用户。例如，您知道机器 1 是要给 Bob 的，您就可以在机器 1 上注册 Bob。Bob 在接收到计算机后必须进行个性化（设置其个人口令）。Bob 接收到计算机、启动 IBM 客户端安全软件，然后设置其口令。
- 您不知道哪一台机器要部署到哪一个最终用户。您拿出客户机 1 并且将它交给最终用户 X。

这两个可变因素使部署 IBM ESS 不同于部署典型的应用程序。然而，因为存在几个部署选项，所以给部署 IBM ESS 提供了灵活性。

您公司中 PC 交付的典型流程图可能与下图类似:

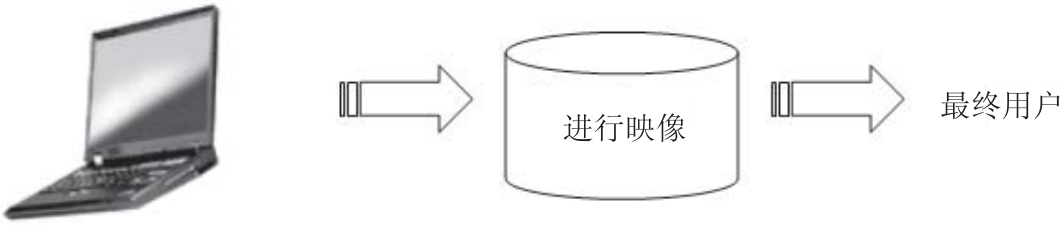


*图 22. 典型的 PC 部署流程图*

## 六个部署方案

有六种部署方法用于 IBM 客户端安全软件:

1. **添加的组件** – IBM 客户端安全软件代码不是磁盘映像的一部分。它在部署计算机后安装、初始化和个性化。
2. **映像组件** – IBM 客户端安全软件代码是映像的一部分，但未安装。公司个性化和用户个性化都未启动。（请参阅第 29 页的图 23。）
3. **简单安装** – 已安装 IBM 客户端安全软件并且已为公司或最终用户个性化。（请参阅第 30 页的图 24。）
4. **部分个性化** – 已安装 IBM 客户端安全软件并且已出现公司个性化，但最终用户个性化未出现。（请参阅第 30 页的图 24。）
5. **临时个性化** – 已安装 IBM 客户端安全软件并且已设置公司和用户个性化。该用户将需要复位用户口令并且（如果需要）提供其它验证信息，例如指纹识别或智能卡关联。（请参阅第 31 页的图 25。）
6. **完全个性化** – 已安装 IBM 客户端安全软件并且已设置公司和用户个性化。管理员设置用户口令。如果要求指纹识别或其它验证，则用户必须提供该个性化设置。（请参阅第 31 页的图 25。）

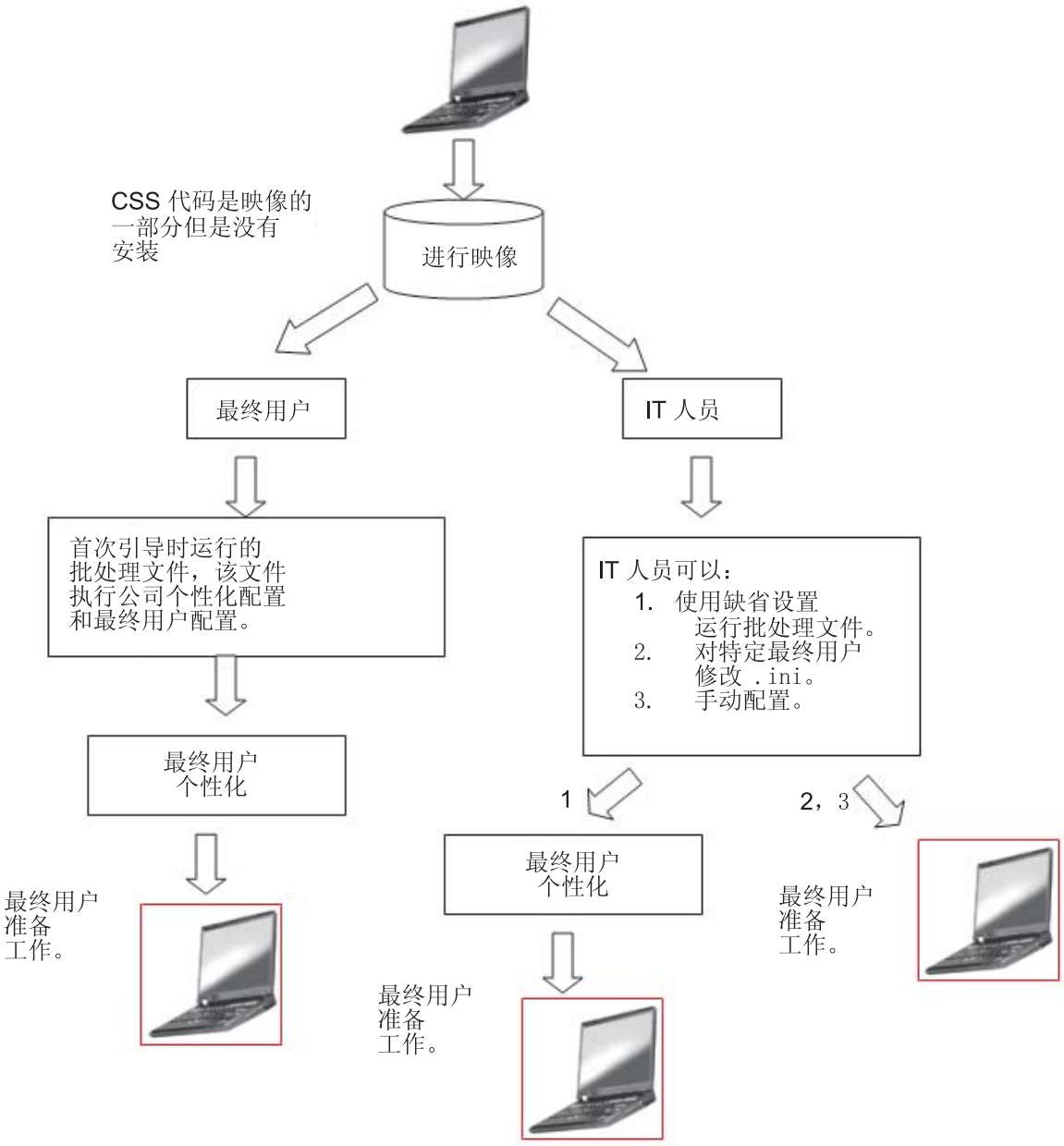


*图 23. IBM 客户端安全软件代码是映像的一部分，但未安装。*

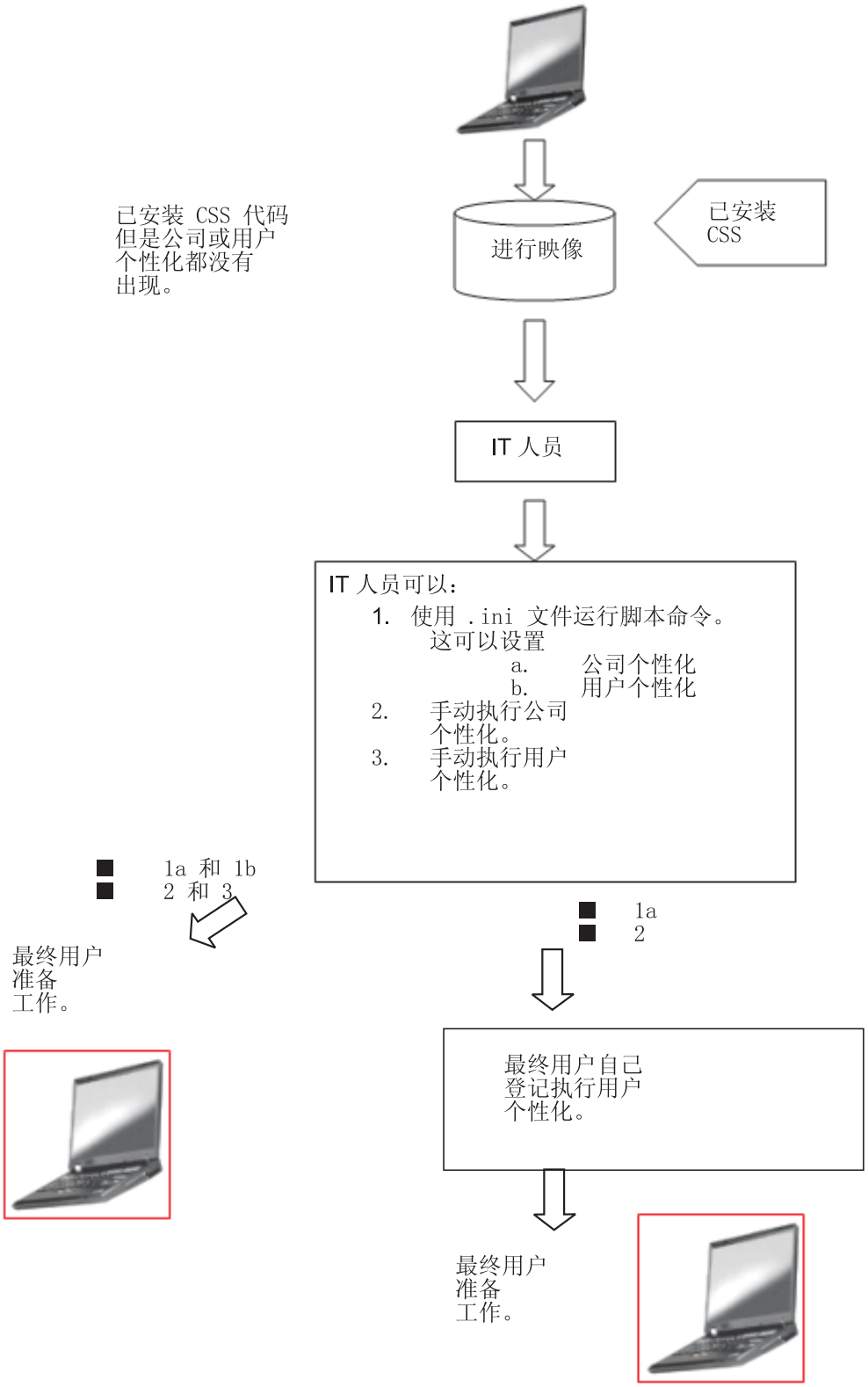


*图 24. 已安装 IBM 客户端安全软件代码，但公司和用户个性化都未出现。*

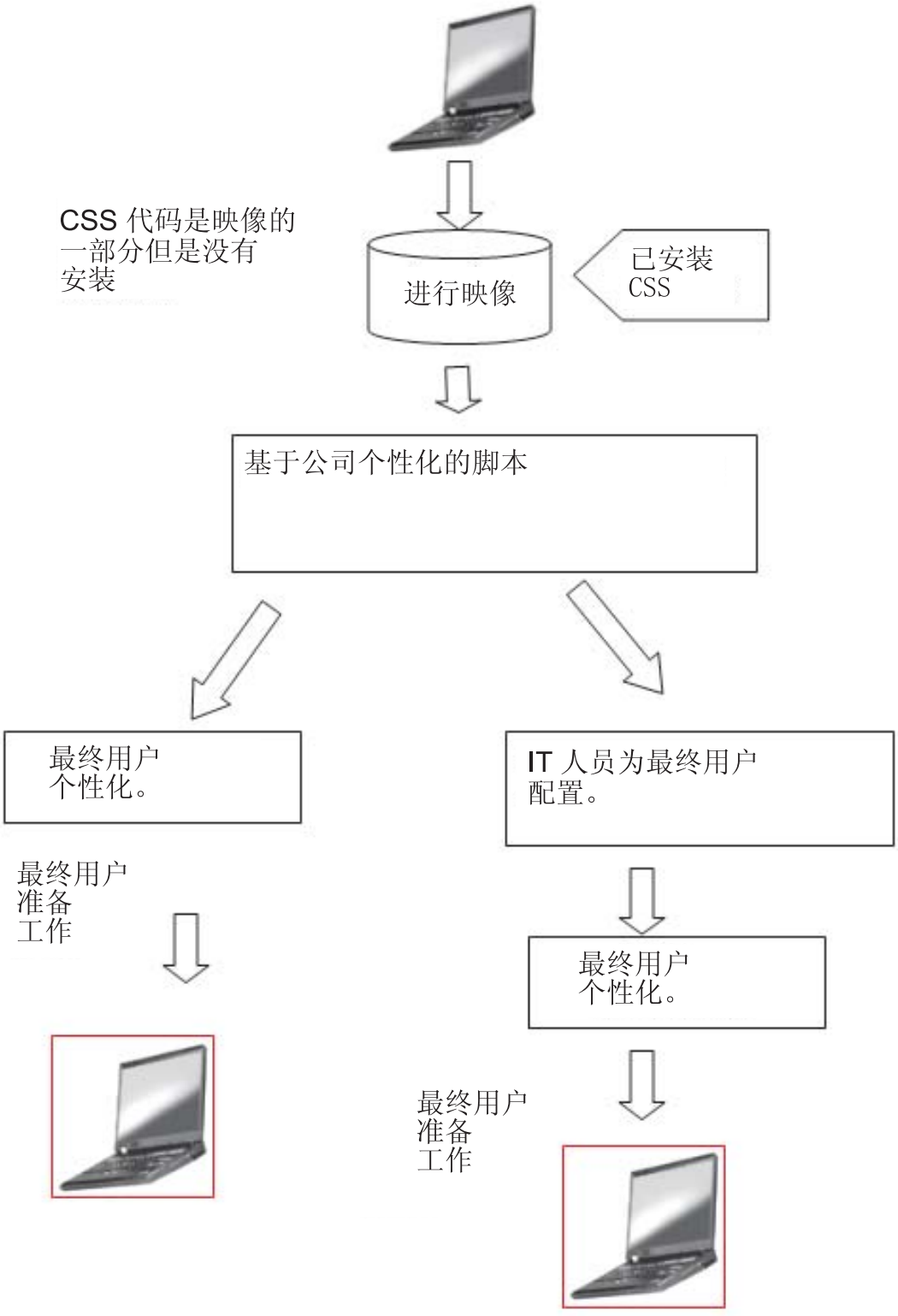


*图 25. 已安装 IBM 客户端安全软件并且公司和用户个性化都已设置。*

在方案 1 中，将磁盘映像放置到计算机后部署 IBM 客户端安全安全软件。在安装磁盘映像后，安装和配置 IBM 客户端安全软件以及配置嵌入式安全芯片。

方案 2-6 表示软件部署和配置以及芯片配置的多种选项。根据您的需要和环境，可以选择最能满足您需求的方案和安装方法。请参阅『安装和初始化』以获取有关安装方法的进一步信息。

## 安装和初始化

IBM 客户端安全软件安装可以分成两个过程: 安装和初始化。安装过程与安装典型软件的过程相似。可以通过两种方法完成安装:

1. 客户端安全软件被添加到已部署的计算机中。（请参阅第 28 页的 1 方案。）
2. 客户端安全软件是基本映像的一部分。（请参阅方案第 28 页的 2 到方案第 28 页的 6。）

### 安装

在方法 1 中，将 IBM 客户端安全软件添加到映像，该映像由程序（例如 IBM 的 ImageUltra™ Builder）添加到每台计算机上。

在方法 2 中，部署带有基本映像的计算机后，将 IBM 客户端安全软件添加到最终用户的 PC。可以两种方法完成方法 2:

1. **用户引导** – 单击对话框并且提供所有必需的用户输入，用户开始并完成安装。
2. **静默安装** – 安装过程可以在无用户参与的情况下远程启动并且以无人照管方式完成。

### 初始化

有两种初始化方式:

1. 大规模初始化
2. 个别初始化

在大规模初始化选项中，必须使用 CSS.ini 文件。该文件为选项（例如在系统上登记所有用户并且给所有那些用户提供已设置的口令）提供参数。在个别初始化中，可以向最终用户提供启用自我登记和用户定义密码的文件。

### 将 IBM 客户端安全软件添加到带有安全芯片的已部署计算机

管理员可以仅（在基本映像上）部署 IBM 客户端安全软件（而不进行个性化或配置），然后在客户机上配置。或者管理员可以大规模部署 IBM 客户端安全软件，然后自动进行大规模配置。无论在哪一种情况下，都请首先安装软件，然后配置。

***安装 IBM 客户端安全软件:*** 要将 IBM 客户端安全软件添加到基本映像，必须包括以下组件:

1. 驱动程序: LPC（针对 TCPA 系统）和 SMBus

   **注®:**

   a. 虽然 SMBus 具有自动安装的代码，但是该驱动程序未通过 Microsoft 签名，因此安装该驱动程序过程中必须有人在场。该限制是在删除过程中。

   b. 如果正在为部署创建 Sysprep 提供者映像，则提供者映像创建过程中将需要照看该驱动程序安装。

   c. 如果您使用的是 IBM ImageUltra Builder，则必须准备可移植 Sysprep 映像。SMBus 必须成为基本映像的一部分。如果不希望每台计算机都将 SMBus 作为基本映像的一部分，则您将需要创建两个基本映像。

2. IBM 客户端安全软件代码
3. 已定义的管理员密码和私钥。
4. 安装 IBM 客户端安全软件 applet（如果在策略文件中要求必须安装，则安装文件和文件夹加密以及密码管理器。有关以静默方式安装这些 applet 的信息，请参阅《*IBM 客户端安全管理员指南*》）

在将以上列出的三个组件添加到提供者系统后，嵌入式安全子系统硬件 –（安全芯片）– 必须被初始化。要启动大规模安装，请完成以下过程:

1. 创建 CSEC.INI 文件。（您可以使用客户端安全向导: 安全目录中的 CSECWIZ.EXE 来创建 CSEC.INI 文件。完成向导后，选中**保存设置，但请勿配置子系统。（设置将保存在 C:\CSEC.INI 中）**旁边的复选框。
2. 通过 Winzip 使用文件夹名称将 IBM 客户端安全软件安装软件包（csecxxxxx_00xx.exe）的内容进行解压缩。
3. 编辑 SETUP.ISS 文件中大规模配置所必需的 szIniPath 和 szDir 条目。szIniPath 参数对于大规模配置是必需的。（请参阅以下完整的 SETUP.ISS 文件。）
4. 将文件复制到目标系统。
5. 创建 \setup -s 命令行语句。从具有管理员权限的用户的桌面上运行命令行语句。“启动”程序组或“运行”关键字很适合执行该操作。
6. 在下一次引导时除去命令行语句。

setup.iss 文件的完整内容（带有几处描述）列出如下:

```
[InstallShield Silent] Version=v6.00.000 File=Response File szIniPath=d:\csec.ini
```

*（以上参数是大规模配置所必需的 .ini 文件的名称和位置。如果 .ini 文件的位置处于网络驱动器上，则必须映射该驱动器。如果您正执行静默安装（并不是大规模配置的一部分），则除去该条目。如果您想仅安装 IBM 客户端安全软件，则从以上代码行删除 szIniPath=d:\csec.ini。如果您希望安装并且配置，则将该命令留在适当的位置上并且验证该路径。）*

```
[FileTransfer] OverwrittenReadOnly=NoToAll [{7BD2CFF6-B037-47D6-A76BD941EE13AD96}-
DlgOrder] Dlg0={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-
SdLicense-0 Count=4 Dlg1={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-
SdAskDestPath-0 Dlg2={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-
SdSelectFolder-0 Dlg3={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-
SdFinishReboot-0 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdLicense-0]
Result=1 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdAskDestPath-0]
szDir=C:\Program Files\IBM\Security
```

*（以上参数是用于安装客户端安全的目录。它必须位于计算机本地。）*

```
Result=1
[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdSelectFolder-0] szFolder=IBM Client Security Software
```

*（以上参数是客户端安全的程序组。）*

```
Result=1 [Application] Name=Client Security Version=5.00.002f
Company=IBM Lang=0009 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-
SdFinishReboot-0] Result=6 BootOption=3
```

***配置:*** 在初始化大规模配置时，以下文件也是必须的。文件可以用任何名称命名，只要它有 .ini 扩展名。以下列表详细说明了您必须创建的 .ini 文件的设置和设置解释。在打开并修正 CSEC.INI 文件之前，必须首先使用 Security 文件夹中的 CONSOLE.EXE 将其解密。

当大规模配置没有和大规模安装一起执行时，以下命令从命令行运行 .ini 文件:

```
<CSS installation folder>\acamucli /ccf:c:\csec.ini
```

*表 4. 客户端安全系统配置设置*

| | |
|---|---|
| [CSSSetup] | CSS 设置的节头。 |
| suppw=bootup | BIOS 管理员 / 超级用户密码。<br>如果不要求，则保留为空。 |
| hwpw=11111111 | CSS 硬件密码。必须是八个字符。始终需要。如果已经设置硬件密码，则它必须正确。 |
| newkp=1 | 1 表示生成新的管理员密钥对<br>0 表示使用现有的管理员密钥对。 |
| keysplit=1 | 当 newkp 为 1 时，它确定私钥组件的数量。<br>**注:** 如果现有密钥对使用多个私钥部件，则所有私钥部件必须保存在相同的目录中。 |
| kpl=c:\jgk | newkp 为 1 时管理员密钥对的位置，如果是网络驱动器，则必须进行映射。 |
| kal=c:\jgk\archive | 用户密钥存档的位置，<br>如果是网络驱动器，则必须进行映射。 |
| pub=c:\jk\admin.key | 使用现有的管理员密钥对时管理员公钥的位置，<br>如果是网络驱动器，则必须进行映射。 |
| pri=c:\jk\private1.key | 使用现有的管理员密钥对时管理员私钥的位置，<br>如果是网络驱动器，则必须进行映射。 |
| wiz=0 | 确定该文件是否由 CSS 安装向导生成。该条目不是必需的。如果您将它包含在文件中，则该值应该是 0。 |
| clean=0 | 1 表示在初始化后删除 .ini 文件，<br>0 表示在初始化后保留 .ini 文件。 |
| enableroaming=1 | 1 表示为客户机启用漫游，<br>0 表示为客户机禁用漫游。 |
| username=<br>[promptcurrent] | [promptcurrent] 表示提示当前用户需要系统注册密码。<br>[current] 表示 sysregpwd 条目何时向当前用户提供系统注册密码以及何时授权该当前用户向漫游服务器注册系统。<br>[<specific user account>] 表示指定的用户是否得到授权向漫游服务器注册系统以及该用户的系统注册密码是否由 sysregpwd 条目提供。<br>如果 enableroaming 值为 0 或者 enableroaming 条目不出现，请勿使用该条目。 |
| sysregpwd=12345678 | 系统注册密码。将该值设置为正确的密码以使系统能够向漫游服务器注册。如果 username 值设置为 [promptcurrent] 或者 username 条目不出现，请勿包含该条目。 |
| [UVMEnrollment] | 用户登记的节头。 |
| enrollall=0 | 1 表示在 UVM 中登记所有的本地用户帐户，<br>0 表示在 UVM 中登记特定的用户帐户。 |
| defaultuvmpw=top | 当 enrollall 为 1 时，这将是所有用户的 UVM 口令。 |
| defaultwinpw=down | 当 enrollall 为 1 时，这将是所有用户向 UVM 注册的 Windows 密码。 |

*表 4. 客户端安全系统配置设置 (续)*

| | |
|---|---|
| defaultppchange=0 | 当 enrollall 为 1 时，这将为所有用户确定 UVM 口令更改策略。<br>1 表示要求用户在下一次登录时更改 UVM 口令，<br>0 表示不要求用户在下一次登录时更改 UVM 口令。 |
| defaultppexppolicy=1 | 当 enrollall 为 1 时，这将为所有用户确定 UVM 口令到期策略。<br>0 表示 UVM 口令会到期<br>1 用于表明 UVM 口令没有失效 |
| defaultppexpdays=0 | 当 enrollall 为 1 时，这将为所有用户确定 UVM 口令到期前的天数。<br>当 ppexppolicy 设置为 0 时，设置该值以确定 UVM 口令到期前的天数。 |
| enrollusers=*x*，其中 x 是您将在计算机上登记的用户总数。 | 该语句中的值指定您将登记的用户总数。<br>当 enrollall 为 0 时，它是将要在 UVM 中登记的用户数量。 |
| user1=jknox | 为每个用户提供信息以从用户 1 开始登记。（没有用户 0。）用户名必须是帐户名。为了获取 XP 上的实际帐户名，请执行以下操作<br>1. 启动计算机管理（设备管理器）。<br>2. 展开“本地用户和组”节点。<br>3. 打开“用户”文件夹。<br>在“名称”列中列出的项是帐户名。 |
| user1uvmpw=chrome | 为用户 1 UVM 指定 UVM 口令。 |
| user1winpw=spinning | 为将要向 UVM 注册的用户 1 指定 Windows 口令。 |
| user1domain=0 | 指定用户 1 的帐户在本地还是在域上。<br>0 表示该帐户是本地的，<br>1 表示该帐户在域上。 |
| user1ppchange=0 | 指定是否要求用户 1 在下一次登录时更改 UVM 口令。<br>1 表示要求用户在下一次登录时更改 UVM 口令，<br>0 表示不要求用户在下一次登录时更改 UVM 口令。 |
| user1ppexppolicy=1 | 指定用户 1 的 UVM 口令是否会到期。<br>0 表明 UVM 口令会到期。<br>1 表明 UVM 口令不会到期。 |
| user1ppexpdays=0 | 如果 user1ppexppolicy=0，则设置该值以表示 UVM 口令到期前的天数。 |
| 以表的阴影部分中指定的次序为每个用户提供一组完整的配置设置。先为一个用户提供所有参数，然后为下一个用户提供参数。例如，如果 enrollusers 设置为 2，则您将添加以下配置设置组。 | |
| user2=chrome | |
| user2uvmpw=left | |
| user2winpw=right | |
| user2domain=0 | |
| user2ppchange=1 | |
| user2ppexppolicy=0 | |
| user2ppexpdays=90 | |
| [UVMAppConfig] | UVM 感知的应用程序设置和 UVM 感知的模块设置的节头。 |

*表 4. 客户端安全系统配置设置 (续)*

| | |
|---|---|
| uvmlogon=0 | 1 表示使用 UVM 登录保护,<br>0 表示使用 Windows 登录。 |
| entrust=0 | 1 表示将 UVM 用于 entrust 验证,<br>0 表示使用 entrust 验证。 |
| notes=1 | 1 表示将 UVM 保护用于 Lotus Notes,<br>0 表示使用 Notes 密码保护。 |
| netscape=0 | 1 表示使用 IBM PKCS#11 模块签名并加密电子邮件。<br>0 表示不使用 IBM PKCS#11 模块签名和加密电子邮件。 |
| passman=0 | 1 表示使用密码管理器,<br>0 表示不使用密码管理器 |
| folderprotect=0 | 1 表示使用文件和文件夹加密,<br>0 表示不使用文件和文件夹加密。 |

**注:**

1. 如果任何文件或路径处于网络驱动器上，则该驱动器必须映射到盘符。
2. INI 文件支持在系统已配置之后添加新用户的功能，这对于执行用户登记将非常有用。如前所述运行 INI 文件，当不包括 “pub=” 和 “pri=” 的值。该代码将仅假定用户登记而不重新初始化子系统。
3. CSEC.ini 文件必须对于软件加密以装入内容。它必须在安全目录中通过 CONSOLE.EXE 加密。以下命令也可以通过脚本用于加密 INI 文件。（对于长路径名将需要加引号）：`CSS installation folder>\console.exe /q /ini:` *`full path to an unencrypted ini file`*
4. 由于增强且更新了 IBM 客户端安全软件，所以 *.ini 参数可能有所更改。

IBM 客户端安全软件允许您再次运行 CSEC.INI 文件，而不影响当前客户端安全软件的安装。例如，您可以再次运行该文件以登记其它用户。

*表 5. 再次运行时的客户端安全系统配置设置。*

| | |
|---|---|
| [CSSSetup] | CSS 设置的节头。 |
| suppw= | BIOS 管理员 / 超级用户密码。<br>如果不要求，则保留为空。 |
| hwpw=11111111 | CSS 硬件密码。必须是八个字符。始终需要。如果已经设置硬件密码，则它必须正确。 |
| newkp=0 | 输入 0 以使用现有的管理员密钥对。 |
| keysplit=1 | 当 newkp 为 1 时，它确定私钥组件的数量。<br>**注:** 如果现有密钥对使用多个私钥部件，则所有私钥部件必须保存在相同的目录中。 |
| pub= | 保留空格 |
| pri= | 保留空格 |
| kal=c:\archive | 用户密钥存档的位置,<br>如果是网络驱动器，则必须进行映射。 |
| wiz=0 | 确定该文件是否由 CSS 安装向导生成。该条目不是必需的。如果您将它包含在文件中，则该值应该是 0。 |
| clean=0 | 输入 0 以在初始化之后保留 .ini 文件。 |
| enableroaming=0 | 输入 0 以禁用客户机漫游。 |

*表 5. 再次运行时的客户端安全系统配置设置。 (续)*

| | |
|---|---|
| [UVMEnrollment] | 用户登记的节头。 |
| enrollall=0 | 1 表示在 UVM 中登记所有的本地用户帐户,<br>0 表示在 UVM 中登记特定的用户帐户。 |
| enrollusers=1 | 该语句中的值指定您将登记的用户总数。 |
| user1=*eddy* | 这是已登记的新用户的名。 |
| user1uvmpw=pass1word | 为用户 1 UVM 指定 UVM 口令。 |
| user1winpw= | 为将要向 UVM 注册的用户 1 指定 Windows 口令。 |
| user1domain=0 | 指定用户 1 的帐户在本地还是在域上。<br>0 表示该帐户是本地的,<br>1 表示该帐户在域上。 |
| user1ppchange=0 | 指定是否要求用户 1 在下一次登录时更改 UVM 口令。<br>1 表示要求用户在下一次登录时更改 UVM 口令,<br>0 表示不要求用户在下一次登录时更改 UVM 口令。 |
| user1ppexppolicy=1 | 指定用户 1 的 UVM 口令是否会到期。<br>0 表明 UVM 口令会到期。<br>1 表明 UVM 口令不会到期。 |
| user1ppexpdays=0 | 如果 user1ppexppolicy=0, 则设置该值以表示 UVM 口令到期前的天数。 |

# 第 5 章 在 Tivoli Access Manager 服务器上安装客户端安全组件

在客户机级别上验证最终用户是一个重要的安全考虑因素。客户端安全软件提供了管理 IBM 客户机的安全策略必需的界面。此界面是验证软件用户验证管理工具（UVM）的一部分，该软件是客户端安全软件的主要组件。

可以用两种方法管理 IBM 客户机的 UVM 安全策略:

- 在本地使用驻留在 IBM 客户机上的策略编辑器
- 在整个企业中使用 Tivoli Access Manager

在客户端安全可以与 Tivoli Access Manager 一起使用之前，必须已安装了 Tivoli Access Manager 的客户端安全组件。该组件可从 http://www.pc.ibm.com/us/security/index.html IBM Web 站点下载。

## 先决条件

在 IBM 客户机和 Tivoli Access Manager 服务器之间建立安全连接之前，必须在 IBM 客户机上安装以下组件:

- IBM Global Security Toolkit
- IBM SecureWay Directory Client
- Tivoli Access Manager Runtime Environment

要获得关于安装和使用 Tivoli Access Manager 的详细信息，请参阅 http://www.tivoli.com/products/index/secureway_policy_dir/index.htm Web 站点上提供的文档。

## 下载和安装客户端安全组件

客户端安全组件可以作为一个免费的组件从 IBM Web 站点下载。

要下载并在 Tivoli Access Manager 服务器和 IBM 客户机上安装客户端安全组件，请完成以下过程:

1. 使用 Web 站点上的信息，通过将型号与系统要求表中提供的型号相匹配来确保 IBM 集成的安全芯片在系统上；然后单击 **Continue**。
2. 选择与机器类型相匹配的单选按钮并单击 **Continue**。
3. 创建用户标识，通过填充在线表单向 IBM 注册，并复查许可证协议；然后单击 **Accept Licence**。

   您将被自动重定向到客户端安全下载页面。
4. 遵循下载页面上的步骤来安装所有必需的设备驱动程序、自述文件、软件、引用文档和其它实用程序。
5. 通过完成以下过程安装客户端安全软件:

   a. 从 Windows 桌面，单击**开始 > 运行**。

b. 在“运行”字段中，输入 d:\directory\csec53.exe，其中 d:\directory\ 是文件所处的盘符和目录。

c. 单击**确定**。

打开“欢迎使用 IBM 客户端安全软件 InstallShield 向导”窗口。

d. 单击**下一步**。

该向导将解压缩文件并安装该软件。安装完成后，将给您现在重新启动计算机或等到稍后重新启动的选项。

e. 选择相应的单选按钮并单击**确定**。

6. 当计算机重新启动后，从 Windows 桌面，单击**开始 > 运行**。
7. 在“运行”字段中，输入 d:\directory\TAMCSS.exe，其中 d:\directory\ 是盘符和文件所在的目录，或者单击**浏览**找到该文件。
8. 单击**确定**。
9. 指定目的地文件夹，然后单击**解压缩**。

向导将把文件解压缩到指定的文件夹。有一条消息表明文件已成功解压缩。

10. 单击**确定**。

## 在 Tivoli Access Manager 服务器上添加客户端安全组件

pdadmin 实用程序是一个命令行工具，管理员可以用它来执行大多数 Tivoli Access Manager 管理任务。多个命令执行使管理员能够使用包含多个 pdadmin 命令的文件来执行一个完整的任务或一组任务。pdadmin 实用程序和管理服务器（pdmgrd）之间的通信是通过 SSL 保护的。pdadmin 实用程序作为 Tivoli Access Manager Runtime Environment（PDRTE）软件包的一部分来安装。

pdadmin 实用程序接受标识文件位置的文件名自变量，例如:

```
MSDOS>pdadmin [-a <admin-user >][-p <password >]<file-pathname >
```

以下命令是如何在 Tivoli Access Manager 服务器上创建 IBM 解决方案对象空间、客户端安全操作和单个 ACL 条目的示例:

```
MSDOS>pdadmin -a sec_master -p password C:\TAM_Add_ClientSecurity.txt
```

请参考 *Tivoli Access Manager Base Administrator Guide* 以获得关于 pdadmin 实用程序及其命令语法的更多信息。

## 在 IBM 客户机和 Tivoli Access Manager 服务器之间建立安全连接

IBM 客户机必须在 Tivoli Access Manager 安全域中建立它自己的验证标识，以便从 Tivoli Access Manager 授权服务请求授权决定。

必须在 Tivoli Access Manager 安全域中为应用程序创建一个唯一标识。为了使验证标识执行验证检查，应用程序必须是远程 acl 用户组的成员。应用程序要联系其中一个安全域服务时，它必须首先登录到该安全域中。

svrsslcfg 实用程序使 IBM 客户端安全应用程序能够与 Tivoli Access Manager 管理服务器和授权服务器进行通信。

svrsslcfg 实用程序使 IBM 客户端安全应用程序能够与 Tivoli Access Manager 管理服务器和授权服务器进行通信。

svrsslcfg 实用程序执行以下任务:

- 创建应用程序的用户标识。例如，DemoUser/HOSTNAME
- 创建该用户的 SSL 密钥文件。例如，DemoUser.kdb 和 DemoUser.sth
- 把该用户添加到远程 acl 用户组

需要以下参数:

- **-f cfg_file** 配置文件路径和名称，使用 TAMCSS.conf
- **-d kdb_dir** 包含服务器的密钥环数据库文件的目录。
- **-n server_name** 预期的 IBM 客户机用户的实际 Windows 用户名／UVM 用户名。
- **-P admin_pwd** Tivoli Access Manager 管理员密码。
- **-s server_type** 必须指定为远程。
- **-S server_pwd** 新创建的用户密码。该参数是必需的。
- **-r port_num** 设置 IBM 客户机的侦听端口号。这是 PD 在 Tivoli Access Manager Runtime 变量 SSL 服务器端口中为管理服务器指定的参数。
- **-e pwd_life** 设置密码到期时间（以天数为单位）。

要在 IBM 客户机和 Tivoli Access Manager 服务器之间建立安全连接，请完成以下过程:

1. 创建一个目录并把 TAMCSS.conf 文件移动到该新目录。

   例如，`MSDOS> mkdir C:\TAMCSS MSDOS> move C:\TAMCSS.conf C:\TAMCSS\`

2. 运行 svrsslcfg 以创建用户。

   MSDOS> svrsslcfg -config -f C:\TAMCSS\TAMCSS.conf -d C:\TAMCSS\ -n <server_name> - s remote -S <server_pwd> -P <admin_pwd> -e 365 -r 199

   **注**: 用 IBM 客户机的预期 UVM 用户名和主机名替换 <server_name>。例如: –n DemoUser/MyHostName。在 MSDOS 提示符下输入 “hostname” 可以找到 IBM 客户机主机名。svrsslcfg 实用程序将在 Tivoli Access Manager 服务器中创建一个有效条目，并为加密通信提供唯一的 SSL 密钥文件。

3. 运行 svrsslcfg 把 ivacld 的位置添加到 TAMCSS.conf 文件。

   缺省情况下，PD 授权服务器在端口 7136 上侦听。通过查看 Tivoli Access Manager 服务器上的 ivacld.conf 文件的 ivacld 节中的 tcp_req_port 参数可以验证它。获取正确的 ivacld 主机名很重要。使用 pdadmin server list 命令获得该信息。服务器名为: <server_name>-<host_name>。以下是运行 pdadmin server list 的示例:

```
MSDOS> pdadmin server list   ivacld-MyHost.ibm.com
```

随后，以下命令用于为上述显示的 ivacld 服务器添加复制条目。假设 ivacld 在缺省端口 7136 上侦听。

```
svrsslcfg -add_replica  -f <config file path> -h <host_name> MSDOS>svrsslcfg
-add_replica  -f C:\TAMCSS\TAMCSS.conf -h MyHost.ibm.com
```

# 配置 IBM 客户机

可以使用 Tivoli Access Manager 控制 IBM 客户机的验证对象之前，必须通过使用管理员实用程序（一个与客户端安全软件一起提供的组件）来配置每个客户机。本部分包含配置 IBM 客户机的先决条件和说明。

## 先决条件

确保以下软件以下列顺序安装在 IBM 客户机上:

1. **Microsoft Windows 支持的操作系统。** 您能够使用 Tivoli Access Manager 控制对于运行 Windows XP, Windows 2000 或 Windows NT Workstation 4.0 的 IBM 客户机的验证要求。
2. **客户端安全软件 v3.0 或更高版本。** 安装该软件并启用 IBM 嵌入式安全芯片后，您可以使用客户端安全管理员实用程序设置用户验证并编辑 UVM 安全策略。要获得关于安装和使用客户端安全软件的详尽说明，请参阅*《客户端安全软件安装指南》*和*《客户端安全软件管理员指南》*。

## 配置 Tivoli Access Manager 安装信息

Tivoli Access Manager 安装在本地客户机之后，您可以通过使用管理员实用程序（一个客户端安全软件所提供的软件组件），配置 Access Manager 安装信息。Access Manager 安装信息包括以下设置:

- 选择配置文件的全路径
- 选择本地高速缓存刷新间隔

要在 IBM 客户机上配置 Tivoli Access Manager 安装信息，请完成以下过程:

1. 单击**开始 > 设置 > 控制面板 > IBM 嵌入式安全子系统**。
2. 输入管理员密码，然后单击**确定**。

   您输入密码后，管理员实用程序主窗口打开。
3. 单击**配置应用程序支持和策略**按钮。

   显示 “UVM 应用程序和策略配置” 屏幕。
4. 选中**使用 UVM 的安全登录替换标准 Windows 登录**复选框。
5. 单击**应用程序策略**按钮。
6. 在 Tivoli Access Manager 安装信息区域，选择 TAMCSS.conf 配置文件的完整路径。例如，`C:\TAMCSS\TAMCSS.conf`

   Tivoli Access Manager 必须安装在客户机上以使该区域可用。
7. 单击**编辑策略**按钮。

   显示 “输入管理员密码” 屏幕。
8. 在提供的字段中输入管理员密码，然后单击**确定** 。

   显示 “IBM UVM 策略” 屏幕。

9. 从“操作”下拉菜单中选择您要 Tivoli Access Manager 控制的操作。
10. 选中“Access Manager 控制所选对象”复选框，以便在该框中出现选中标记。
11. 单击**应用**按钮。

    在下一次高速缓存刷新时发生更改。如果您需要立即发生更改，请单击**刷新本地高速缓存**按钮。

## 设置并使用本地高速缓存功能

选择 Tivoli Access Manager 配置文件后，可以设置本地高速缓存刷新间隔。由 Tivoli Access Manager 管理的安全策略信息的本地副本是在 IBM 客户机上维护的。您可以每隔（0-12）月或（0-30）天来调度本地高速缓存的自动刷新。

要设置或刷新本地高速缓存，请完成以下过程:

1. 单击**开始 > 设置 > 控制面板 > IBM 嵌入式安全子系统**。
2. 输入管理员密码，然后单击**确定**。

   打开管理员实用程序窗口。要获得关于使用管理员实用程序的完整信息，请参阅*《客户端安全软件管理员指南》*。
3. 在管理员实用程序中，单击**配置应用程序支持和策略**按钮，然后单击**应用程序策略**按钮。

   显示“修改客户端安全策略配置”屏幕。
4. 请执行以下操作之一:
   - 要立即刷新本地高速缓存，单击**刷新本地高速缓存**。
   - 要设置自动刷新速率，在提供的字段中输入月号（0-12）和天数（0-30），然后单击**刷新本地高速缓存**。将刷新本地高速缓存，并且将更新文件到期日期以表明何时会发生下一个自动刷新。

## 启用 Tivoli Access Manager 以控制 IBM 客户机对象

UVM 策略是通过全局策略文件控制的。称为 UVM 策略文件的全局策略文件包含 IBM 客户机系统上执行的操作（如登录到系统、清除屏幕保护程序或签名电子邮件消息）的验证需求。

在您能够启用 Tivoli Access Manager 控制 IBM 客户机的验证对象前，使用 UVM 策略编辑器编辑 UVM 策略文件。UVM 策略编辑器是管理员实用程序的一部分。

**要点**: 启用 Tivoli Access Manager 来控制对象，则将控制授予 Tivoli Access Manager 对象空间。如果您这样做，则必须重新安装客户端安全软件以重新建立对该对象的本地控制。

### 编辑本地 UVM 策略

尝试编辑本地客户机的 UVM 策略之前，确保至少有一个用户在 UVM 中登记。否则，在策略编辑器试图打开本地策略文件时将显示错误消息。

编辑本地 UVM 策略并只在编辑它的客户机上使用它。如果您在其缺省位置安装客户端安全，则本地 UVM 策略存储为 \Program Files\IBM\Security\UVM_Policy\globalpolicy.gvm。仅添加到 UVM 的用户可以使用 UVM 策略编辑器。

**注:** 如果您设置 UVM 策略以要求用于验证对象（如操作系统登录）的指纹，则添加到 UVM 的用户必须注册其指纹以使用该对象。

要启动 UVM 策略编辑器，请完成以下管理员实用程序过程:

1. 单击**配置应用程序支持和策略**按钮，然后单击**应用程序策略**按钮。

   显示“修改客户端安全策略配置”屏幕。
2. 单击**编辑策略**按钮。

   显示“输入管理员密码”屏幕。
3. 在提供的字段中输入管理员密码，然后单击**确定** 。

   显示“IBM UVM 策略”屏幕。
4. 在“对象选择”选项卡上，单击**操作**或**对象类型**，然后选择您要为其指定验证要求的对象。

   有效操作的示例包括系统登录、系统解锁和电子邮件解密；对象类型的示例是获取数字证书。
5. 对于您选择的每个对象，选择 **Tivoli Access Manager 控制所选对象**，为该对象启用 Tivoli Access Manager。

   **要点:** 如果启用 Tivoli Access Manager 来控制对象，则将控制授予 Tivoli Access Manager 对象空间。如果您以后要重新建立对该对象的本地控制，则必须重新安装客户端安全软件。

   **注:** 编辑 UVM 策略时，通过单击**策略摘要**可以查看策略摘要信息。
6. 单击**应用**保存您的更改。
7. 单击**确定**退出。

### 编辑和使用远程客户机的 UVM 策略

要跨越多个 IBM 客户机使用 UVM 策略，请编辑和保存一个远程客户机的 UVM 策略，然后将 UVM 策略文件复制到其它 IBM 客户机。如果您在客户端安全的缺省位置安装它，UVM 策略文件将存储为 \Program Files\IBM\Security\UVM_Policy\remote\globalpolicy.gvm。

将以下文件复制到要使用该 UVM 策略的其它远程 IBM 客户机:

- \IBM\Security\UVM_Policy\remote\globalpolicy.gvm
- \IBM\Security\UVM_Policy\remote\globalpolicy.gvm.sig

如果您在缺省位置安装了客户端安全软件，则上述路径的根目录是 \Program Files。将这两个文件复制到远程客户机的 \IBM\Security\UVM_Policy\ 目录路径。

## 故障诊断图表

以下部分提供的故障诊断图表可在您使用客户端安全软件遇到问题时提供帮助。

### 数字证书故障诊断信息

如果在获取数字证书时遇到问题，则以下故障诊断信息可能会有帮助。

| 问题症状 | 可能的解决方案 |
| --- | --- |
| **在数字证书请求期间 UVM 口令窗口或指纹验证窗口显示多次** | **操作** |
| UVM 安全策略规定用户在获取数字证书之前提供 UVM 口令或指纹验证。如果用户尝试获取证书，将多次显示要求 UVM 口令或指纹识别的验证窗口。 | 每次打开验证窗口时输入您的 UVM 口令或识别您的指纹。 |
| **显示 VBScript 或 JavaScript 错误消息** | **操作** |
| 当您请求数字证书时，可能显示与 VBScript 或 JavaScript 相关的错误消息。 | 重新启动计算机，并再次获取证书。 |

## Tivoli Access Manager 故障诊断信息

以下故障诊断信息可以在您结合客户端安全软件使用 Tivoli Access Manager 过程中遇到问题时向您提供帮助。

| 问题症状 | 可能的解决方案 |
| --- | --- |
| **本地策略设置不符合服务器上的那些设置** | **操作** |
| Tivoli Access Manager 允许 UVM 不支持的某些位配置。因此，本地策略要求可以覆盖管理员在配置 PD 服务器时所做的设置。 | 这是一个已知限制。 |
| **Tivoli Access Manager 设置项不可访问** | **操作** |
| 在管理员实用程序的“策略设置”页面上无法访问 Tivoli Access Manager 设置和本地高速缓存设置项。 | 安装 Tivoli Access Manager runtime Environment。如果未在 IBM 客户机上安装 Runtime Environment，则“策略设置”页面上的 Tivoli Access Manager 设置将不可用。 |
| **用户的控制对于用户和组都有效** | **操作** |
| 配置 Tivoli Access Manager 服务器时，如果您将用户定义到组，并且打开了**遍历位**，则用户的控制对于用户和组都有效。 | 不需要任何操作。 |

## Lotus Notes 故障诊断信息

如果在结合客户端安全软件使用 Lotus Notes 时遇到问题，以下故障诊断信息可能会有帮助。

| 问题症状 | 可能的解决方案 |
| --- | --- |
| **为 Lotus Notes 启用了 UVM 保护后，Notes 无法完成它的设置** | **操作** |
| 使用管理员实用程序启用 UVM 保护之后，Lotus Notes 无法完成设置。 | 这是一个已知限制。<br><br>必须在使用管理员实用程序启用 Lotus Notes 支持之前配置和运行 Lotus Notes。 |
| **当您尝试更改 Notes 密码时显示错误消息** | **操作** |
| 在使用客户端安全软件时更改 Notes 密码可能显示错误消息。 | 重试密码更改。如果这不起作用，则重新启动客户机。 |
| **随机生成密码后显示错误消息** | **操作** |

| 问题症状 | 可能的解决方案 |
| --- | --- |
| 当您执行以下操作时可能显示错误消息:<br>• 使用 Lotus Notes 配置工具为 Notes 标识设置 UVM 保护<br>• 打开 Notes 并使用 Notes 提供的功能来更改 Notes 标识文件的密码<br>• 在您更改密码后立即关闭 Notes | 单击**确定**关闭错误消息。不需要任何其它操作。<br><br>与错误消息相反，密码已更改。新的密码是由客户端安全软件创建的随机生成的密码。Notes 标识文件现在用随机生成的密码加密，并且用户不需要新的用户标识文件。如果最终用户再次更改密码，UVM 将为 Notes 标识生成新的随机密码。 |

## 加密故障诊断信息

如果在使用客户端安全软件 3.0 或更高版本加密文件时遇到问题，以下故障诊断信息可能会有帮助。

| 问题症状 | 可能的解决方案 |
| --- | --- |
| **将不解密先前加密的文件** | **操作** |
| 使用客户端安全软件的先前版本加密的文件在升级到客户端安全软件 3.0 或更高版本之后不解密。 | 这是一个已知限制。<br><br>安装客户端安全软件 3.0 或更高版本之*前*，您必须解密使用客户端安全软件的先前版本加密的所有文件。由于客户端安全软件 3.0 的文件加密实现中的更改，客户端安全软件 3.0 无法解密使用客户端安全软件先前版本加密的文件。 |

# 第 6 章 安装第三方硬件设备驱动程序以辅助 IBM 客户端安全软件

通过客户端安全和第三方解决方案，可以通过集成附加产品、允许您定义适合计算环境的保护级别来保护整个基础结构。

IBM 嵌入式安全子系统必须已经测试符合以下这些组织提供的选择安全验证硬件:

- 用于指纹阅读器的 Targus
- 用于智能卡解决方案的 Gemplus
- 用于感应胸卡的确保技术

访问该包含这些组织的 Web 站点以了解 http://www.pc.ibm.com/us/security/index.html 中提供的每个组织的更多信息

因为带有许多作为磁盘映像的组件，所以安装顺序非常重要。如果您计划部署以上列出的验证设备及其关联的设备和其它软件，则必须首先安装 IBM 客户端安全软件。如果放置设备驱动程序文件之前未将 CSS 放置在硬盘中，则不能正确安装这些设备的驱动程序和软件。

有关安装启用验证硬件的软件和驱动程序的每天更新的具体信息，请参考设备随附的文档。

# 第 7 章 远程部署新的或已修正的安全策略文件

对于不同的计算机，无论您更新安全策略还是创建不同的策略，具有签名权限的 IT 管理员都可以修正并且部署策略文件。请使用 ACAMUCLI.EXE 编辑策略文件。（也可以通过在“控制面板”中双击“IBM 安全子系统”图标来编辑策略。）

单击“应用”后，根据屏幕指示信息签名策略文件。（**注**: 如果已分割管理员私钥，则为了签名策略文件，必须输入所有的组件。）您已编辑的文件是 GLOBALPOLICY.GVM 和 GLOBPOLICY.GVM.SIG。将这些文件分发到相应的用户文件，确保它们被保存到 Security\UVM_Policy 文件夹中。

可以在部署后远程更新口令策略。更新口令策略文件使您能够在（或如果）用户接下来更改其口令时更改口令要求。管理员可以定义强制用户更改口令后的时间段。该时间段在用户登记或注册过程中定义。示例如下: 管理员登记用户 Jane 并且初始策略表明用户 Jane 必须具有每 30 天失效的八字符密码。管理员可以更新策略文件并且要求 Jane 下一次更改她的口令，新的口令现在必须是 12 个字符。管理员也可以更改到期期限。例如，管理员可以要求 Jane 每 15 天更改一次口令而不是每 30 天一次。在以下情况中发生了什么呢？您处在 30 天口令“期限”的第 10 天。新的口令策略文件被发送到客户机，该文件表明必须每 15 天更改一次口令。口令在 5 天或 20 天后到期。如先前策略中所述，口令在 20 天后到期。口令到期策略在设置口令后生效。15 天更改的策略在 Jane 20 天后更改她的口令时开始。

如果您希望更改口令的必需特性，请按照以上指示信息操作。然后，将以下文件从 SECURITY\UVM_POLICY 文件夹中分发: UVM_PP_POLICY.DAT 和 UVM_PP_POLICY.DAT.SIG。

# 附录. 声明

IBM 可能并非在所有国家或地区都提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务，则由用户自行负责。

IBM 公司可能已拥有或正在申请与本文档中所描述内容有关的各项专利。提供本文档并未授予用户使用这些专利的任何许可。您可以用书面方式将许可查询寄往:

*IBM Director of Licensing*
*IBM Corporation*
*North Castle Drive*
*Armonk, NY 10504-1785*
*U.S.A.*

International Business Machines Corporation “按现状” 提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的非侵权、适销和适用于某特定用途的保证。某些辖区在某些交易中不允许免除明示或暗含的保证。因此本条款可能不适用于您。

本信息中可能包含技术方面不够准确的地方或印刷错误。此处的信息将定期更改；这些更改将编入本出版物的新版本中。IBM 可以随时对本出版物中描述的产品和／或程序进行改进和／或更改，而不另行通知。

本文档中描述的产品并非旨在用于移植或其他生命支持的应用，在这些应用中的故障可能导致人身伤害或死亡。本文档中包含的信息不影响或更改 IBM 产品规格或保证。本文档中的任何内容都不能作为对 IBM 或第三方知识产权的明示或默示的许可或保证。本文档中包含的所有信息都在特定环境中获得并且作为一种说明提供。在其他操作环境中获得的结果可能会有所不同。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

## 非 IBM Web 站点

本信息中对非 IBM Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

## 商标

下列术语是 International Business Machines Corporation 在美国和／或其他国家或地区的商标:

IBM
ThinkPad®
ThinkCentre™

Tivoli

Microsoft、Windows 和 Windows NT® 是 Microsoft Corporation 在美国和／或其他国家或地区的商标。

其他公司、产品或服务名称可能是其他公司的商标或服务标记。