٣ التحقق من الهُويّة (Authentication) تعني الخدمة التي يمكن من خلالها التحقق من هوية الشخص (أو الجهة) وأنه الشخص المعني لا غيره . فعند اتصالالشخصين (أو جهتين) بعضهما ببعض ، فلا بد من أن يتعرف كل منهما إلى الآخر ، لضمان أن يتخاطب كل منهما مع الشخص أو الجهة المعنية وليس مع غيرها . بعبارةأخرى : فإنّ التحقق من الهُويّة هو التحقق من أن المستخدم النظام ما هو بالفعل من ادعى أنه ذلك المستخدم ، فإنه يجب التحقق من هوية المرسللضمان أن المعلومة قادمة من مصدرها الحقيقي ، وكذلك يجب التحقق من هوية المستلم لضمان أن المعلومة ذاهبة إلى وجهتها الصحيحة . تبدأ عملية التحقق من الهويةتحديد الهوية (Identification) . ويمكن تحقيق ذلك من خلال اسم المستخدم أو رقم الحساب مثلا . إن تحديد هوية الشخص أو التعريف به رقميًا (إلكترونيًا) أمر مهم، إذ إن الشخص الواحد نفسه قد يكون لديه أكثر من هوية رقمية . فمثلا قد يكون الموظف واحد اسم مستخدم للدخول إلى الشبكةالمحلية العاملة على نظام النوافذ Windows) ، واسم مستخدم آخر على نظام اليونكس (Unix) ، وثالث على النظام المركزي (Mainframe) ، ورابع على نظامالمحادثة الآنية . وهذا ما يصعب كثيرًا من مهام التدقيق والمتابعة وتسجيل الأحداث مستخدم ؛ لذا يجب أن تتوافر في طريقة تحديد الهوية المعايير الآتية : . أنتكون الهُويّة فريدة : ومعنى ذلك أن تكون غير قابلة للتكرار . ومثال ذلك أن يكون للشخص رقم هوية فريد خاص به لا يشترك معه غيره فيه . ومثال آخر هو استخدامالخصائص الحيويّة للإنسان ، . أن تكون غير مفصحة عن معلومات المستخدم ووظيفته والغرض من وصوله إلى . ومثال ذلك أن لا ينم اسم المستخدم لمدير النظام عن أنه المدير ، مثل استخدام " أو عبارة " Backup Operator " . . أن لا تكون مشتركة بين المستخدمين ، كإعطاء قسم كامل به عدد من الموظفين اسم المستخدم نفسه . ● اتباع معايير التسمية المعتمدة عند المنشأة عند إنشاء حسابات المستخدمين ، كاستخدام أول حرف مناسم المستخدم الحقيقي متبوعا برقم الهوية ، أو غير ذلك من التسميات التي قد يستفاد منها في تحديد الشخص بسهولة عند إجراء عمليات التدقيق والمتابعة . يطلق على عنصر التحقق من الهوية والمصادقة ، وتعني المصادقة أن تكون جميع الاتصالات موثوقة . ففي حالة إرسال رسالة باتجاه واحد (من طرف واحد ولاتحتاج إلى رد) كرسائل التحذير أو الأوامر والتعليمات ، فإنه يجب أن يكون لدى المستقبل الضمان بأن الرسالة التي وصلته صادرة فعلا من المصدر الذي يدعي أنهأرسلها ، وفي حالة الرسائل التفاعلية بين طرفين ، فإن المصادقة تضمن أن الطرفين محددان ، وأنهما فعلا الشخصان المعنيان (أنهما فعلا من يدّعيان أنهما كذلك) . ا تحدد توصيات X . 800 شقين رئيسين للتحقق من الهوية ، هما : ● التحقق من هوية الشخص أو الجهة (Peer Entity Authentication) : ويوفر التحقق من هوية طريق الاتصال في جميع مراحله ، وضمان عدم قدرة المعتدي علىانتحال شخصية أحد طرفي الاتصال . وتجدر الإشارة إلى ضرورة إعادة التحقق من هوية طرفي الاتصال في كل عمليّة اتصال منفردة . ويجب ألا يكشف نظام التحققمن الهوية انتحال شخصية أحد طرفي الاتصال من قبل الغرباء فقط ، ولكن أيضا يكشف الإعادة غير المشروعة لاتصال سابق . ● التحقق من أصل منشأ المعلومة (Data Origin Authentication) : أي التحقق من أصل المعلومة بأنها صادرة من جهتها الأصلية ، أو بعبارة أخرى : تأكيد مصدر المعلومات . مع العلم أن التحقق من أصلمنشأ المعلومة لا يوفر الحماية ضد عمليات النسخ أو التعديل (يتم كشف ذلك عن طريق عنصر سلامة المعلومة وتكاملها) ، وإنّما يصادق على أن الرسالة أرسلت بالفعلمن الجهة التي تدعي أنها أرسلتها . تظهر الحاجة إلى هذا النوع من التحقق من الهوية في التطبيقات التي لا يكون فيها اتصال مسبق ، كإرسال رسالة بريد إلكترونيلأول مرة . يمكن استخدام معيار أو أكثر للتحقق من الهوية حسب درجة قوة التحقق المطلوبة . فيمكن التحقق باستخدام معيار واحد أو معيارين أو ثلاثة معايير معا ، كما يلي : ● التحقق باستخدام معيار واحد : هذا المعيار هو « ماذا تعرف ؟ » كاستخدام كلمات المرور أو أرقام التعريف الشخصية (Personal Identification Number – PIN) . ويعتمد هذا المعيار في التحقق من الهُويّة على طلب إدخال معلومة لا يعرفها إلا الشخص المعني فقط ، ويُعدّ من أدنى درجات التحقق من الهُويّة . ● التحقق باستخداممعيارين : ويتم ذلك باستخدام معيار « ماذا تعرف ؟ » ، بالإضافة إلى معيار آخر هو « ماذا تملك ؟ » وتعتمد هذه الطريقة في التحقق من الهُويّة على طلب إدخال معلومةلا يعرفها إلا الشخص المعني فقط ، ومعلومة أخرى لا يملكها إلا الشخص نفسه أيضا ، ويوفر التحقق باستخدام معيارين درجة جيدة من درجات التحقق من الهوية أعلىمن التحقق باستخدام ميار واحد . ومن الأمثلة على ذلله استخدام بطاقات الصرف الإلكتروني (Automatic Teller Machine – ATM) حيث يتم التحقق من هويةالشخص من خلال رقم بطاقة الصراف التي لا يملكها إلا هو ، ثم إدخال الرقم السري الذي لا يعرفه إلا هو كذلك ، ولا يمكن أن يفني أحدهما عن الآخر . ومثال آخر هوماتتخذه بعض المصارف من إجراءات عند الدخول إلى الخدمات البنكية من خلال موقع المصرف على شبكة الإنترنت ، حيث بعد أن يدخل المستخدم كلمة المرور التي لايعرفها إلا

هويرسل له البنك رسالة نصية بها رقم سري عشوائي يُستخدم لمرة واحدة على هاتف المستخدم المحمول الذي يفترض أنه لا يملكه إلا هو ، ومعيار ماذا تملك ، بالإضافة إلى معيار ثالث هود من أنت ؟ » . وتعتمد هذه الطريقة في التحقق من الهوية على طلب إدخال معلومة لا يعرفها إلا الشخص المعني فقط ، ومعلومة أخرى لا يملكها الا الشخص نفسه ، ومعلومة ثالثة منواحدة أو أكثر من خصائص الشخص الحيوية التي تميزه من غيره ، كبصمات الأصابع والعين ، وأبعاد راحة اليد والوجه ، وغير ذلك . وتوفر هذاالطريقة أعلى درجات التحقق من الهوية ، لكنها تحتاج إلى أجهزة وبرامج إضافية ، وتُعدّ أكثر تعقيدًا من سابقاتها . وفي بعض الحالات ومن أجل إزالة التعقيد في هذهالطريقة قد يكتفي بمعيار « من أنت ؟ فقط ، والاستغناء عن المعيارين الآخرين . فبمجرد تمرير الإصبع على قارئ البصمات يسمح للمستخدم بالدخول دون طلب إدخالاسم المستخدم وكلمة المرور . من الأمثلة على الخروقات الممكنة لأمن المعلومات التي يمكن أن تتم في حال عدم توفر عنصر التحقق من الهوية هي إمكانية دخول أشخاصغير مصرح لهم إلى شبكة المنشأة أو أنظمتها الداخلية ، ومن ثم حصول اطلاع غير مشروع على معلومات المنشأة . ومثال آخر هو إمكانية استخدام بعض منسوبيالمنشأة أسماء مستخدمين وكلمات مرور الموظفين آخرين ، والاطلاع على معلومات غير مصرح لهم بالاطلاع عليها ، أو القيام بأعمال وإجراءات ليست من اختصاصهم ، أوقيامهم بأعمال تخريبية .