ما ه ي PKI

البنية الأساسية للمفتاح العام (PKI) هي مجموعة من البرمجيات، وتقنيات التشفير، والخدمات التي تمكن مؤسسة ما من حماية أمن الانترنت والاتصالات والعمليات. وتستخدم الـ PKI الهويات الرقمية (أو *الشهادات الرقمية*) عمليات تشفير المفتاح العام، وسلطات الشهادات (Certificate Authorities) لخلق معمارية أمان للشبكة على كامل مستوى المؤسسة لتوفير حماية ضد الاختراقات الأمنية التي قد تتسبب في سرقة كلمات المرور السرية أو الاضطلاع على محتويات رسائل البريد الالكتروني والعمليات المالية أثناء إرسالها.

تعتبر الهويات الرقمية مستندات تعريفية للموظفين، والمخدمات (Servers)، وحتى الأفراد غير الموظفين ممن لديهم تعاملات مع الشركة أو المؤسسة . وكما هو الحال في رخصة القيادة أو جواز السفر تفيد الهوية الرقمية بإثبات هوية حاملها. كما يتم استخدام ما يسمى *بالتوقيع الرقمي* عن طريق إرفاقه با لرسالة عند إرسالها للتأكيد على هوية مرسلها و على عدم حدوث تغيير في محتواها . وعادة ما يتم حفظ الهوية الرقمية في بطاقة ذكية حيث يتم استخدامها عند إر سال البريد الالكتروني والدخول للمعلومات المتاحة على الانترنت والشبكة الداخلية للمؤسسة

من يستخدم الـ PKI

يتسع نطاق استخدام الـ PKI في العالم وتحديدا في القطاعين الحكومي والتجاري . وكل دولة في العالم غالبا ما تمتلك مصدر للشهادات بما فيها دولة الكويت والتي وفرت التواقيع الإلكترونية للمواطنين في عام 2009. ويمكن استخدام هذه التواقيع المواطنين من التصويت في الانتخابات، وتوقيع العقود ورسائل البريد الإلكتروني . وبتوظيف الـ PKI يمكن لمستخدمي الانترنت من إجراء مختلف العمليات دون القلق من اعتراض معلوماتهم الخاصة أو السرية من المخترقين.

كيف تعمل؟

تعتبر ال PKI توظيفا لتقنيات المفتاح العام. بإمكانك أنت وأي شخص آخر متصل على شبكة الانترنت من امتلاك زوج من المفاتيح أحدهما عام والآخر خاص.

ولكن عموما لن ترى هذه الحالة في حياة العمل اليومية . وبدلا من ذلك ستقوم بالا شتراك في الهيئة العامة للمعلومات المدنية للحصول على هوية إلكترونية من خلال مركز خدمة العملاء حيث س يقوم فريقهم بمساعدتك في اجراءات استخراج الهوية الرقمية.

وفيما يلي طريقة العمل :

استخدام شهادتك الرقمية

توقيع رسالة بريد إلكتروني

توقيع رسالة بريد إلكتروني رقميا، تجهز الرسالة بالطريقة المعتادة (شاملة المرفقات إن وجدت) ومن ثم يتم استخدام أداة "توقيع" الموجودة في برنامج البريد الاكتروني. وهكذا يتم توقيع الرسالة إلكترونيا ثم إرسالها.

كيف تعمل هذه الميزة؟

يقوم برنامج البريد الالكتروني باستخدام المفتاح الخاص Private Key لتوقيع محتويات الرسالة. وبإمكانك ضبط برنامج البريد الالكتروني ليقوم تلقائيا بتوقيع جميع الرسائل المرسلة . كما يمكن ضبط البرنامج بحيث يرسل نسخة من الرسالة الأصلية دون توقيع ليتمكن مستلم الرسالة من قراءتها حتى عند عدم تمكنه من التحقق من صحة التوقيع (مثلا في حال إرسالها لأشخاص خارج المؤسسة).

قراءة رسالة بريد إلكتروني موقعة رقميا

لقراءة رسالة بريد الكتروني يلزم فقط الضغط على الرسالة ضغطا مزدوجا، حيث يقوم البرنامج بعملية التحقق باستخدام هوية المستخدم الالكترونية. ففي حال كان التوقيع صحيحا تتم قراءة الرسالة بالطريقة المعتادة، أما أذا كانت هناك مشكلة في التحقق يتم تنبيه المستخدم.

كيف تعمل هذه الميزة؟

لقراءة الرسالة المستلمة يجب أن يتوفر المفتاح العام الخاص بالمرسل. ولا تعتبر هذه مشكلة لأن المفتاح العام مخزن في هويتهم الرقمية ومعظم المستخدمين يقومون بإرسال هوي اتهم الرقمية مع كل رسالة موقعة أو مشفرة . بالإضافة لذلك، معظم أنظمة البريد الالكتروني تضم دليلا يحوي جميع الهويات الرقمية للأفراد كما يمكن تحميل الهوية الرقمية من مركز الهويات الرقمية التابع للهيئة.

تشفير (بعثرة) مستند أو رسالة بريد الكتروني

لتشفير مستند أو رسالة بريد الكتروني، تجهز الرسالة بالطريقة المعتادة ومن ثم يتم استخدام أداة "توقيع" الموجودة في برنامج البريد الاكتروني. يتم توقيع الرسالة إلكترونيا ثم إرسالها.

كيف تعمل هذه الميزة؟

يقوم برنامج البريد الالكتروني باستخدام المفتاح العام للمستلم (مخزن في الهوية الالكترونية – نظام البريد الالكتروني الخاص بك يضم الهوية الالكترونية في الدليل الخاص به) للقيام بالتشفير.

فقط يلزمك تفعيل التشفير والبرنامج سيقوم بكل التفاصيل الأخرى التي تشمل البحث عن الهوية الرقمية، وتشفير الرسالة وإرسالها. ويمكنك ضبط البرنامج ليقوم بالتشفير تلقائيا لجميع الرسائل المرسلة.

في حال لم تحصل على الهوية الرقمية الخاصة بك يمكنك تحميلها من مركز الهويات الرقمية التابع للهيئة

فك تشفير مستند أو رسالة بريد مشفرة

لفك تشفير المستند أو رسالة البريد الالكتروني عليك أن تضغط على المستند أو الرسالة وسيقوم البرنامج بفك التشفير وعرض الرسالة. حيث تقوم بقراءة الرسالة دون أن تميز أنها كانت مشفرة.

ويجب ملاحظة أنه لا يمكن إرسال رسالة مشفرة لشخص لا يملك هوية رقمية . وفي هذه الحالة يملك المرسل خيار إلغاء تفعيل التشفير والذي يتم بسهولة عن طريق إلغاء اختيار زر التشفير في البرنامج.

الدخول إلى عنصر محظور بالشبكة

بما أن الهوية الرقمية مفيدة للتعريف بهوية حاملها، تعتبر وسيلة مثالية للتحكم بالدخول للمعلومات الحساسة الموجودة في شبكة المؤسسة. وعلى سبيل المثال، قد تمتلك المؤسسة شبكة محلية خاصة بالموظفين فقط أو ربما حصر الدخول للبيانات المالية على موظفي القسم المالي.

وعندما يطلب النظام منك تحديد هويتك عند الدخول إلى عنصر محظور يمكنك اختيار الهوية الرقمية الخاصة بك من قائمة الشهادات التي يعرضها لك النظام.

إدارة الهويات الرقمية الخاصة بك

تجديد الهوية الرقمية

جميع الشهادات الرقمية لها فترة صلاحية محددة وتهدف هذه الميزة لزيادة مستوى الأمان. عندما تنتهي صلاحية شهادة لا تستطيع استخدام هويتك الرقمية. ويجب في تلك الحالة تجديد الشهادة لتتمكن من استخدامها.

تعتبر عملية التجديد سهلة وبسيطة . فباستخدام المتصفح يمكنك فتح صفحة موقع مركز الهويات الرقمية التابع للهيئة والضغط على تجديد واتباع التعليمات. عندها تستلم رسالة بريد الكتروني تشرح كيفية استلام الشهادة الجديدة.

سحب الهوية الرقمية

في حال سرقة هويتك الرقمية والتي تحتوي على المفتاح الخاص، قد يتمكن السارق من استخدام مفتاحك الخاص لانتحا ل شخصيتك. ولذلك إن وجدت نفسك في هذا الموقف يجب سحب\إيقاف هويتك الرقمية (بشكل دائم). وهذا سيجعل أي توقيع أو استخدام معتمد على هويتك الرقيمة غير صحيح \ناجح بعد إتمام عملية السحب . يجب ملاحظة أن عملية سحب الشهادة هي عملية دائمة الأثر أي بمعنى أنه لا يمكن التراجع عنها بمجرد إتمامها.