نبذة عن التوقيعات الالكترونية

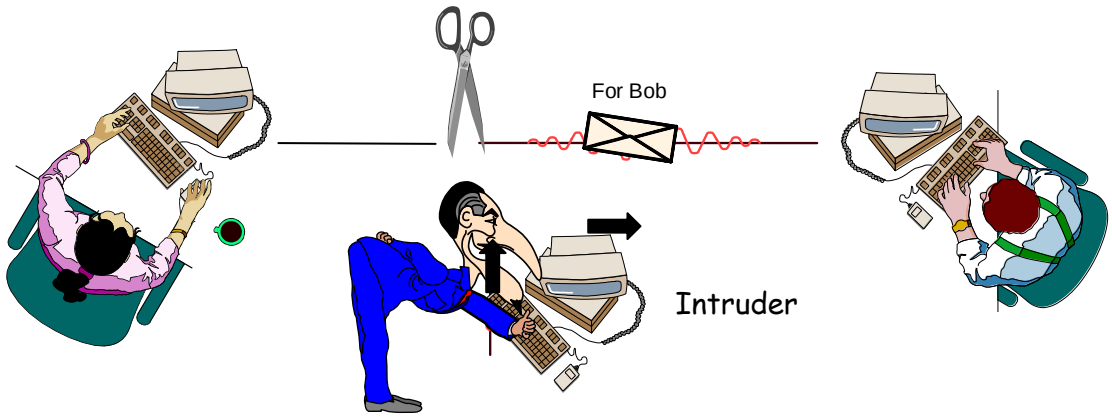
ما هو التوقيع الالكتروني ؟

لا يوجد تعريف بسيط للتوقيع الالكتروني **Digital Signature** ولكن في حال وجود مثل هذا التعريف فإنه يمكن أن يكون مشابها للتعريف التالي: طريقة إتصال مشفرة تعمل على توثيق المعاملات التي تتم عبر الإنترنت.

بشكل أساسي فإن الفكرة الكامنة وراء التوقيعات الالكترونية هي نفسها كما في التوقيع المكتوب بخط اليد . إنك تستخدمه للتصديق او لتوثيق الحقيقة بأنك وعدت بشيء ما ولا تستطيع التراجع عنه فيما بعد. إن التوقيع الالكتروني لا يتضمن القيام بتوقيع شيء ما باستخدام القلم والورقة وبعد ذلك إرساله عبر الإنترنت ولكنه مثل التوقيع على الورق يلتصق بهوية الموقع على معاملة ما.

يجب أن يكون للتوقيع بشكل عام الصفات المميزة التالية :

- توثيق الموقع : إن التوقيع يجب أن يبين أو يشير إلى الشخص الذي قام بتوقيع الوثيقة أو الرسالة أو السجل ويجب أن يكون من الصعب على شخص آخر القيام به بدون تفويض. الصورة التالية تظهر متسلل يزعم بكونه الطرف المرسل.



- توثيق الوثيقة : أي توقيع يجب أن يعرف عن الطرف الذي قام بتوقيعه بما يجعله غير ممكنا تزوير أو تغيير أي من المادة الموقعة أو التوقيع بدون انكشاف الحقيقة .

كيف تعمل تقنية التوقيع الالكتروني:

التشفير بواسطة المفتاح الشفرى العام**Public Key Cryptography** (شفرة تستخدم مفتاحين متناظرين أحدهما سري ويحفظه مستلم البيانات والآخر عمومي)

يتم انشاء التوقيعات وكذلك التثبت من صحتها من خلال التشفير وهو فرع من الرياضيات التطبيقية المختصة بتحويل الرسائل إلى أشكال تبدو وكأنها لا يمكن فهمها وإعادتها مرة أخرى كما كانت. تستخدم التوقيعات الالكترونية ما يعرف بنظام شفرة المفتاح الشفرى العام والذي يستخدم منهجا معينا مستعينا بمفتاحين مختلفين ولكنهما مرتبطين حسابيا ، واحد لانشاء التوقيع الالكتروني أو لتحويل البيانات إلى أشكال تبدو وكأنها لا يمكن فهمها والمفتاح الآخر للتثبت من صحة التوقيع الالكتروني أو لإعادة الرسالة إلى شكلها الأصلي . تدعى أجهزة وبرامج الحاسب الآلي التي تستخدم مثل هذين المفتاحين عادة " نظام التشفير اللا تماثلي **asymmetric**"

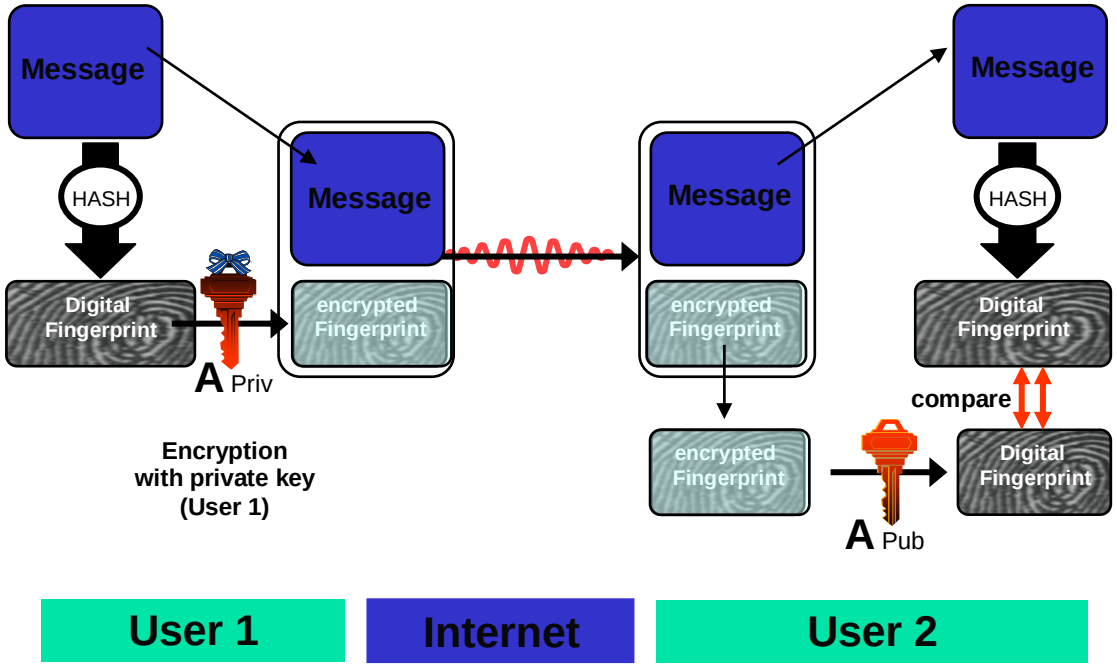
إن المفاتيح التكميلية في نظام الشفرة اللاتماثلية للتوقيعات الالكترونية تدعى عشوائيا المفتاح الخاص والذي يعرفه فقط الموقع ويستخدم لانشاء التوقيع الالكتروني والمفتاح الشفرى العام والمعروف عادة على نطاق أوسع ويستخدم من قبل شخص موثوق به للتثبت من صحة التوقيع الالكتروني. في حال استدعت الظروف أن أكثر من جهة بحاجة للتثبت من صحة التوقيع الالكتروني فإن المفتاح الشفرى العام يجب أن يكون متوفرا لتلك الجهات أو يوزع عليهم جميعا أو ربما يتم نشره في ملف للإتصال المباشر حيث من الممكن الوصول إليه بسهولة . بالرغم من كلا المفاتيح مرتبطين ببعضها رياضيا فإنه في حال تم تصميم نظام الشفرة اللا تماثلي وتم تطبيقه بشكل آمن فإنه حسابيا لا يمكن التوصل إلى معرفة المفتاح الخاص من خلال معرفة المفتاح الشفرى العام . وبهذا فإنه بالرغم من أن العديد من الأشخاص يمكن أن يكونوا على علم بالمفتاح الشفرى العام لموقع ما ويستخدمونه للتثبت من صحة توقيعات موقع معين إلا أنهم لا يستطيعون اكتشاف المفتاح الخاص لذلك الموقع واستخدامه في تزوير توقيعاته الالكترونية .

وظيفة الـ هاش **Hash Function**

عملية رئيسية وأساسية أخرى تدعى " وظيفة الـ هاش " وهي تستخدم في كلا عمليتي انشاء التوقيع الالكتروني والتثبت من صحته. إن وظيفة هاش هي عبارة عن منهج يعمل على انشاء تمثيل رقمي معين أو بصمة إصبع على شكل قيمة " هاش" أو " نتيجة هاش" بطول مقياسي يكون عادة أصغر من الرسالة ولكنه مقترنا بالرسالة ومحصورا بها. أي تغيير في الرسالة ينتج عنه نتيجة هاش مختلفة عند استخدام وظيفة الـ هاش نفسها. في حالة وظيفة الـ هاش الآمنة والتي تدعى أحيانا " وظيفة الـ هاش الأحادية الإتجاه" فإنه من الناحية الحسابية لا يمكن التوصل إلى الرسالة الأصلية من خلال معرفة قيمة الـ هاش الخاصة بها. لذلك فإن وظائف الـ هاش تتيح للبرمجيات انشاء توقيعات الكترونية للعمل على كمية أصغر يمكن التنبؤ بها من البيانات وفي نفس الوقت ما زالت توفر تلازم قوي وواضح مع محتويات الرسالة الأصلية وبهذا تعمل على توفير الضمان الفعال والتأكيد بأنه لم يتم إجراء أي تعديل على الرسالة منذ أن تم توقيعها الكترونيا.

تدفق أو سير العمل

الرسم التالي يوضح سير العمل الأساسي لتوقيع الكتروني تم استخدامه لإرسال رسالة :



كما يتضح من الرسم أعلاه فإن استخدام التوقيعات الالكترونية عادة يتضمن عمليتين ، واحدة يتم إنجازها من قبل الموقع والأخرى من قبل مستلم التوقيع الالكتروني :

- انشاء التوقيع الالكتروني يستخدم نتيجة هاش يتم اشتقاقها من وتكون مقتصرة على كل من الرسالة الموقعة ومفتاح خاص معين. بغرض أن تكون نتيجة الـ هاش آمنة ومحكمة يجب أن لا يكون هناك إمكانية أو احتمال ضئيل فقط بأن نفس التوقيع الالكتروني يمكن إنشائه من خلال تركيبة أي رسالة أخرى أو مفتاح خاص آخر.
- التثبت من صحة التوقيع الالكتروني: وهي عملية التأكد من التوقيع الالكتروني من خلال الرجوع إلى الرسالة الأصلية وإلى مفتاح عام معين وبهذا يتم تحديد ما إذا كان التوقيع الالكتروني قد تم إنشائه لتلك الرسالة باستخدام المفتاح الخاص المقابل للمفتاح العام المشار إليه.

لتوقيع وثيقة معينة أو أي معلومات معينة ، على الموقع أولا أن يعين بدقة الحدود لما يراد توقيعه . إن المعلومات التي تم تعيينها أو تحديدها كي يتم توقيعها تدعى " الرسالة " في هذه الإرشادات . بعد ذلك تقوم وظيفة هاش معينة في برنامج الموقع بإحتساب نتيجة الـ هاش المقتصرة (لكافة الأغراض العملية) على الرسالة . بعد ذلك يقوم برنامج الموقع بتحويل نتيجة الـ هاش إلى توقيع الكتروني باستخدام المفتاح الخاص للموقع . إن التوقيع الالكتروني الناجم عن ذلك هو مقتصر على كل من الرسالة والمفتاح الخاص المستخدم في إنشائه. أى ان لكل رسالة موقعة الكترونيا يكون التوقيع المنشأ هو توقيع فريد

نموذجيا يكون التوقيع الالكتروني (نتيجة هاش للرسالة موقعة الكترونيا) مرتبطا ومرفقا برسالته ويخزن أو يرسل مع رسالته. على أية حال يمكن أن يرسل أو يخزن أو يحفظ كعنصر بيانات منفصل طالما أنه يحافظ على ارتباط موثوق به مع رسالته. بما أن التوقيع الالكتروني مقتصر وينحصر في رسالته فإنه لن يكون له أي فائدة أو نفع عندما يتم فصله كليا عن رسالته.

يتم التثبت من صحة التوقيع الالكتروني من خلال احتساب نتيجة هاش جديدة للرسالة الأصلية بواسطة نفس وظيفة الـ هاش المستخدمة في انشاء التوقيع الالكتروني. بعد ذلك وباستخدام المفتاح الشفرى العام ونتيجة هاش الجديدة يقوم الطرف الذي يعمل على التثبت من الصحة بالتأكد من ١) ما إذا كان قد تم انشاء التوقيع الالكتروني باستخدام المفتاح الخاص المقابل و ٢) ما إذا كانت نتيجة الـ هاش التي تم احتسابها مؤخرا مطابقة لنتيجة الـ هاش الأصلية والتي تم تحويلها إلى توقيع الكتروني خلال عملية التوقيع. إن برامج التثبت من الصحة سوف تؤكد " صحة " التوقيع الالكتروني في حال : ١) كان قد تم استخدام مفتاح الموقع الخاص لتوقيع الرسالة الكترونيا وهذا ما سيكون الحال عليه لو أنه تم استخدام مفتاح الموقع العام للتثبت من صحة التوقيع لأن المفتاح الشفرى العام الخاص بالموقع سوف يثبت فقط صحة توقيع الكتروني تم إنشائه بواسطة مفتاح الموقع الخاص. و ٢) بأن الرسالة لم يتم تغييرها وهذا يكون في حال كانت نتيجة الـ هاش التي تم احتسابها من قبل المتثبت من الصحة مشابهة ومطابقة لنتيجة الـ هاش المستخرجة من التوقيع الالكتروني خلال عملية التثبت من الصحة .

<u>الأهداف العامة والأغراض من استخدام التوقيع الالكتروني:</u>

إن عمليات انشاء التوقيع الالكتروني والتثبت من صحته تحقق التأثيرات الجوهرية المرجوة من التوقيع لعدة أغراض قانونية :

- توثيق الموقع : في حال كان هناك زوج من المفاتيح واحد عام والآخر خاص وكانا مرتبطين بموقع معين ومحدد فإن التوقيع الالكتروني ينسب ويعزو الرسالة إلى الموقع . لا يمكن تزوير

التوقيع الالكتروني ما لم يفقد الموقع السيطرة على المفتاح الخاص (تعرض المفتاح الخاص للخطر) كأن يقوم بإفشائه او يفقد الوسط أو الوسيلة المحتفظ به فيها مثل البطاقة الذكية .

- توثيق الرسالة : كذلك فإن التوقيع الالكتروني يعمل على تحديد هوية الرسالة الموقعة بثقة ودقة ويقين أكثر من التوقيعات على الورق. إن عملية التثبت من الصحة تكشف أي تلاعب حيث أن مقارنة نتائج الـ هاش (واحدة يتم إعدادها عند التوقيع والأخرى عند التثبت من الصحة) تبين ما إذا كانت الرسالة هو نفسها عندما تم توقيعها.

- عمل إيجابي : إن انشاء توقيع الكتروني يتطلب من الموقع أن يستخدم مفتاح الموقع الخاص وهذا العمل بإمكانه أن ينجز الوظيفة الرئيسية في تنبيه الموقع إلى حقيقة أن الموقع يقوم باستكمال معاملة لها عواقب ونتائج قانونية .

- الفعالية : إن عمليات انشاء التوقيع الالكتروني والتثبت من صحته تتطلب مستوى عال من الضمان بأن التوقيع الالكتروني هو للموقع بدون تكلف أو رياء . مقارنة مع الأساليب الورقية مثل بطاقات نموذج اعتماد التوقيع والتي هي أساليب مملة و تستغرق الكثير من الجهد بحيث أنه نادرا ما يتم استخدامها بالواقع – فإن التوقيعات الالكترونية تعطي وتولد درجة ضمان أعلى بدون أن تضيف كثيرا على الموارد المطلوبة للمعالجة .

شهادات التصديق الالكتروني **Public Key Certificates**

للتثبت من صحة توقيع الكتروني معين ، على الطرف الذي يقوم بالتثبت من الصحة أن يكون قادرا على الوصول إلى مفتاح الموقع العام وأن يكون واثقا بأنه متطابق مع مفتاح الموقع الخاص. على أية حال فإن أي زوج من المفاتيح العامة والخاصة ليس له أي ارتباط جوهري أو فعلي بأي شخص . إنه ببساطة زوج من الأرقام . من الضروري وجود استراتيجية مقنعة لكي يتم ربط شخص أو هيئة معينة بزوج المفاتيح.

إن الحل لهذا هو استخدام طرف ثالث واحد أو أكثر يكون موثوق به لكي يربط موقع معين مع مفتاح عام محدد . تلك الحهة الثالثة الموثوق بها يشار إليها بعبارة " جهة التصديق الالكتروني "

<u>كيف يتم إنشاء ثقة رقمية ؟</u>

كي يتم ربط زوج من المفاتيح بموقع محتمل تقوم " جهة التصديق الالكتروني " بإصدار شهادة ، سجل إلكتروني يذكر فيه المفتاح الشفرى العام على أنه " موضوع" الشهادة ويؤكد بأن الموقع المحتمل المعرف عنه في الشهادة يحمل المفتاح الخاص المقابل. يشار إلى الموقع المحتمل بعبارة " المشترك" . إن وظيفة الشهادة الرئيسية هي ربط زوج من المفاتيح مع مشترك معين. أي " مستلم " للشهادة يرغب في الإعتماد على والوثوق بتوقيع الكتروني ينشئه المشترك المذكور في الشهادة (عندئذ يصبح المستلم هو الطرف المعتمد) بإمكانه استخدام المفتاح الشفرى العام المذكور في الشهادة للتثبت من صحة التوقيع الالكتروني أي بأنه تم إنشائه بواسطة المفتاح الخاص المقابل. في حال نجحت عملية التثبت من الصحة فإن هذه السلسلة من الوقائع والمقدمات توفر الثقة والضمان بأن المفتاح الخاص المقابل محتفظ به من قبل المشترك المذكور إسمه في الشهادة وبأن التوقيع الالكتروني قد تم إنشائه من قبل ذلك المشترك.

لتأكيد صحة كل من الرسالة والهوية في الشهادة تقوم جهة التصديق الالكتروني بتوقيعها الكترونيا. إن التوقيع الالكتروني لجهة التصديق الالكتروني على الشهادة يمكن التثبت من صحته باستخدام المفتاح الشفرى العام الخاص بجهة التصديق الالكتروني والمذكور في شهادة أخرى من قبل جهة تصديق الكتروني أخرى (والتي يمكن أن تكون على مستوى أعلى فيما يتعلق بالرتبة ولكن ذلك ليس بالضرورة) وتلك الشهادة الأخرى يمكن توثيقها بدورها بواسطة المفتاح الشفرى العام المذكور كذلك في شهادة أخرى

وهكذا .. حتى يتثبت الشخص المعتمد على التوقيع الالكتروني من صحته . في كل حالة فإن جهة التصديق الالكتروني المصدرة للشهادة يجب أن توقع الكترونيا على شهادتها الخاصة بها خلال الفترة التشغيلية للشهادة الأخرى المستخدمة للتثبت من صحة التوقيع الالكتروني لجهة التصديق الالكتروني. الرسم التالي يوضح شكل شهادة التصديق الالكتروني

إن أي توقيع الكتروني سواء تم إنشائه من قبل مشترك معين لتوثيق رسالة ما أو تم إنشائه من قبل جهة تصديق الكتروني لتوثيق شهادتها (بالفعل رسالة متخصصة) يجب أن تكون مختومة زمنيا بشكل موثوق به وذلك كي يستطيع المتثبت من الصحة تحديد ما إذا كان التوقيع الالكتروني قد تم إنشائه خلال الفترة التشغيلية (مدة الصلاحية) المذكورة في الرسالة .

كي يكون مفتاح عام وتعريفه مع مشترك معين متوفرين بسرعة وسهولة للإستخدام في التثبت من الصحة ، يمكن نشر شهادة في حافظة أو يتم توفيرهم من خلال أي طريقة أخرى . إن الحافظات هي عبارة عن قاعدة بيانات الكترونية من الشهادات والمعلومات الأخرى المتوفرة للإسترجاع والإستخدام في التثبت من صحة التوقيعات الالكترونية . يمكن القيام بالإسترجاع أوتوماتيكيا من خلال أمر برنامج التثبت من الصحة بأن يستفسر مباشرة من الحافظة للحصول على الشهادات المطلوبة .

<u>لشهادة التصديق الالكتروني المميزات التالية :</u>

- تعتمد صحة التوقيعات الالكترونية على صحة زوج المفاتيح الشفرية (العام والخاص)
- تستخدم الشهادات لضمان حصة زوج مفاتيح معين
- إن الشهادة تربط مفتاح شفرى عام معين بهوية معينة (مثلا إسم شخص معين ، إسم المضيف في الحاسب الآلي الخ)
- يمكن أن تتضمن الشهادة معلومات أخرى مثل تاريخ الإنتهاء
- يتم توقيع الشهادة من قبل جهة التصديق الالكتروني .

بنية المفتاح المعلن **PKI Infrastructure**

إن بنية المفتاح المعلن هى كامل كرة الشمع التي تتضمن مفاتيح شفرية ونظام إدارة شهادات . إن بنية المفتاح المعلن تتيح إجراء المعاملات بطريقة آمنة بالإضافة إلى أنها تتيح تبادل المعلومات الخاصة بين الأطراف الذين يمكن أن يكونوا على معرفة ببعضهم البعض أو يمكن أن يكونوا غرباء عن بعضهم البعض. إن بنية المفتاح المعلن توفر الخصوصية واستقامة وتوثيق وعدم الرفض عند التقدم بطلب ومعاملات التجارة الإلكترونية .

تركيبات المفتاح الشفرى العام

- تعمل على توليد وتوزيع أزواج المفاتيح الخاصة / العامة
- تنشر المفاتيح العامة مع هوية المستخدم على شكل شهادة في دليل مفتوح
- توفر الثقة بأن تبقى المفاتيح الخاصة آمنة ومصانة ومأمونة
- مفاتيح عامة معينة مرتبطة فعليا بمفاتيح خاصة معينة
- حامل زوج المفاتيح الشفرية العامة/ الخاصة هو من يدعي أن يكون.

إن تركيبة المفتاح الشفرى العام تتكون من واحد أو أكثر من الأنظمة الموثوق بها والمعروفة بـ جهات التصديق الالكترونى وهذه السلطات منظمة في هيكل هرمي شبيه بالشجرة حيث يتم وضع المفتاح الشفرى العام والتعريف فيما يتعلق بكل عميل في شهادة رقمية وتقوم جهة التصديق الالكتروني بالتوقيع الكترونيا على كل شهادة وتجعل الشهادات متوفرة مجانا وبحرية من خلال نشرها في فهارس أو دليل يمكن الوصول إليه من قبل العامة . أي عميل في بنية المفتاح المعلن يمكنه الوصول إلى المفتاح الشفرى العام لأي مستخدم آخر والتثبت من صحته باستخدام المفتاح الشفرى العام الخاص بجهة التصديق الالكتروني للتثبت من صحة توقيع جهة التصديق الالكتروني على الشهادة . إن جهة التصديق الالكتروني التي هي على رأس التسلسل الهرمي توقع شهادات جهات التصديق الالكترونى التابعة لها أو التي تأتي في مرتبة أدنى منها وجهات التصديق الالكترونى تلك توقع شهادات جهات التصديق الالكترونى التي يكون ترتيبها أدنى منها وهكذا . هذه النظام يشكل سلسلة من الثقة في أي نظام جهة تصديق الكتروني موزع.

عرض تبسيطي لفكرة التوقيع الالكتروني

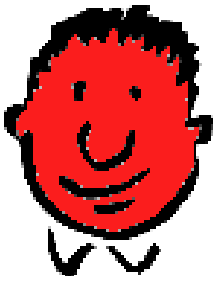
- **بافتراض أن أحمد يمتلك مفتاحين**

المفتاح الخاص: وهذا المفتاح يحتفظ به ويستخدمه فى التوقيع الالكتروني

المفتاح العام: ويستخدمه الآخرون ليستعرضوا الرسائل المرسلة من أحمد

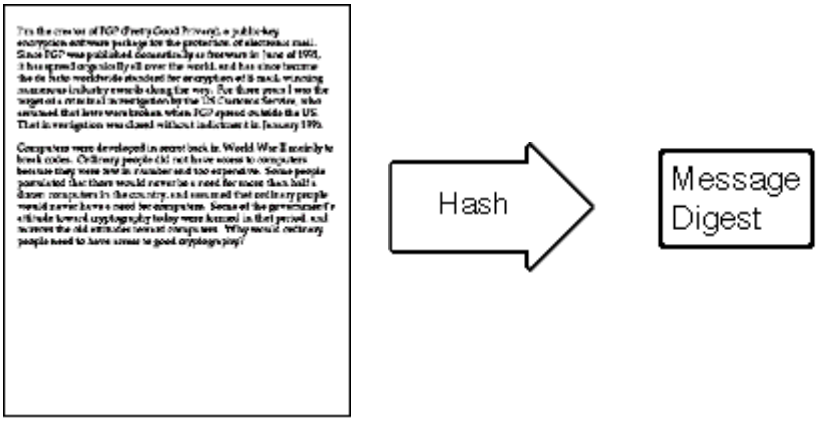
أحمد

- **نفترض أن أحمد له ثلاث زملاء**



الأستاذة سامى الحرامى مصطفى سوزان

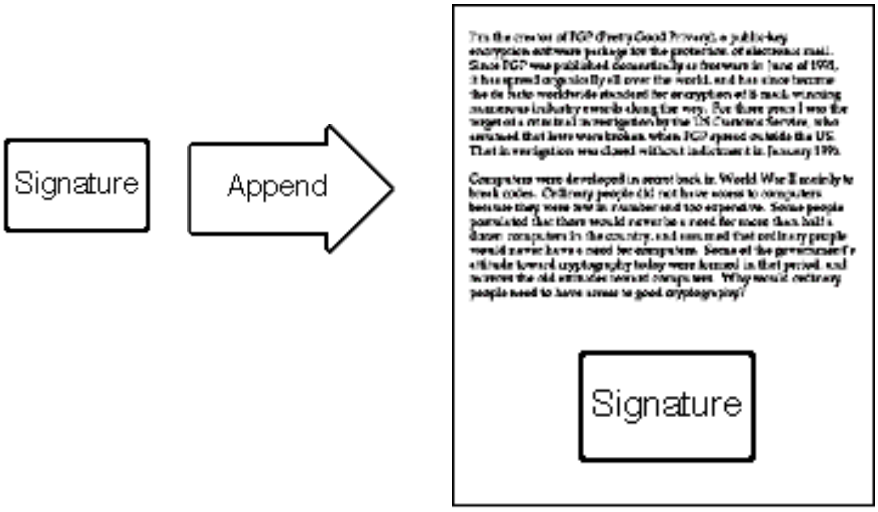
- **احمد يريد ان يرسل رسالة موقعة الكترونيا إلى مصطفى**
  - احمد سيقوم باستخدام برنامج يحول الرسالة المرسلة منه الى صورة أخرى بعمل **Hashing** لها فتتكون ما يسمى **Message Digest** تبقى صورة مصغرة من الرسالة صغيرة الحجم وتحوى بيانات كافية عن الرسالة ذاتها (مثل بصمة الرسالة)



  - البرنامج الخاص بأحمد سيقوم بتشفير ال **Message Digest** بواسط المفتاح الخاص فيكون هذا هو التوقيع الالكترونى (عبارة عن **Message digest** مشفرة بإستخدام المفتاح الخاص بأحمد

Message Digest + Encryption by Private Key = ELECTRONIC SIGNATURE

  - أخيرا البرنامج الخاص بأحمد سوف يضع هذا التوقيع الالكتروني على الرسالة المرسلة ويتم إرسال الرسالة إلى مصطفى



- **الموقف عند مصطفى عندما يستقبل الرسالة**
  - أولاً: البرنامج الموجود عند مصطفى سيقوم بعملية عكسية

بأن يقوم بعمل فك شفرة التوقيع الالكتروني الخاص بأحمد باستخدام المفتاح العام الخاص بأحمد (المعلن للجميع  ويعيد التوقيع الى صورة **Message Digest** مرة ثانية.

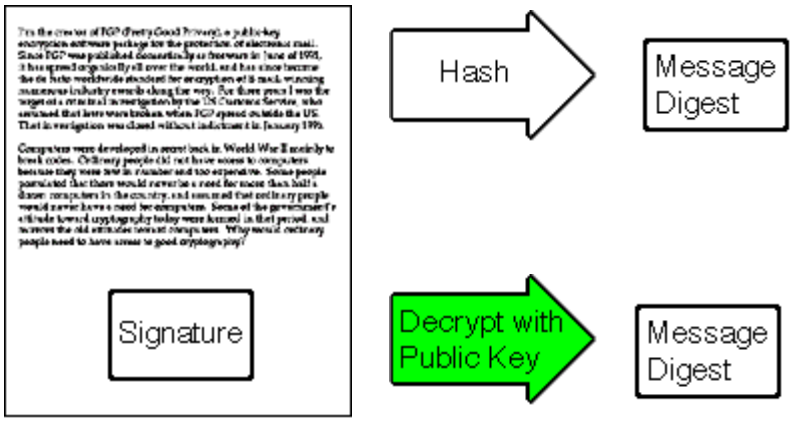
فى حالة نجاح الخطوة السابقة إذن هذا التوقيع توقيع أحمد فعلا لأنه باستخدام المفتاح العام الخاص بأحمد تم التمكن من فك شفرة توقيعه الالكتروني.

ثانيا: يقوم البرنامج الذى عند مصطفى أيضا بعمل **Hashing** للرسالة المستقبلة من احمد وتحويلها الى **message digest** وتتم مقارنة الاثنين :-

١- الـ **message digest** الذى تم الحصول عليه بعد فك شفرة التوقيع الالكتروني

٢- الـ **message digest** الذى تم الحصول عليه بعد عمل **hashing** للرسالة الاصلية

لو كانوا متشابهين إذن هذا دليل على أن محتويات الرسالة لم تتغير إثناء الإرسال. إذن الرسالة تم توقيعها بواسطة أحمد فعلا ولم يتم اى تغيير فيها بعد توقيعها.



- **نفترض أن سامى يريد أن يخدع مصطفى ويرسل له رسالة كأنها ارسلت من احمد**

سامى يريد أن يجعل مصطفى يستقبل الرسالة الموقعة والمفتاح العام كأنهم مرسلين من احمد !

سامى انشأ مفتاح عام كأنه من احمد كما انشأ مفتاح خاص به هو .

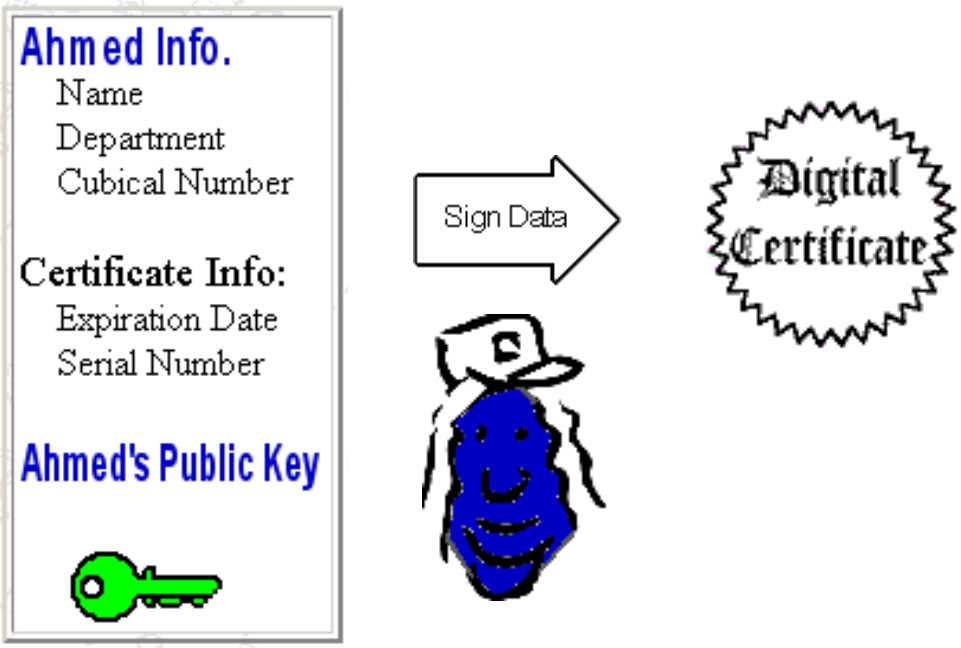
سامى أرسل المفتاح العام المزور الى مصطفى

سامى أرسل رسالة منه ووقعها الكترونيا باستخدام مفتاحه الخاص كأنها مرسلة من احمد

السؤال: كيف يتأكد مصطفى (المستقبل) ان المفتاح العام المرسل له هو من احمد شخصيا وليس مزورا؟؟؟

- **هنا يظهر دور الأستاذة سوزان و التى تعمل في الجهة المختصة بإصدار شهادات التوقيع الالكترونى.**

حيث تقوم سوزان بالتصديق على أن هذا المفتاح العام خاص بأحمد وتصدر شهادة لأحمد بها المفتاح العام خاصته كما تذكر بيانات أخرى خاصة بأحمد فى الشهادة.



الآن كل زملاء احمد يمكن أن يتأكدوا من الشهادة التي أعطتها لـه سوزان انـه فعلا المفتـاح المعلن المرسل هو خاص بـه. ومن الطبيعي انـه لا احد من زملاء احمد سوف يعتد بتوقيعه إلا بالشهادة المرسلة من سوزان (والتى يمكن التأكد منها **online**).
هذا بالتالي يعطـى الصلاحية لسوزان أن تقوم بإلغاء التعامل بالتوقيع في حالات ضياع المفتاح الخاص بأحمد وغيرها من الظروف التي تضطرها إلى ذلك .

دلوقتى سوف نقول أن احمد سوف يرسل رسالة موقعة مرة ثانية إلى مصطفى . فإن البرنامج الذى عند مصطفى يقوم بالتأكد من أن المفتاح المرسل هو من احمد وذلك بواسطة الرجوع الى الشهادة التى أصدرتها سوزان .
أولا برنامج مصطفى يستخدم المفتاح المعلن الخاص بسوزان لكى يفك شفرة شهادة احمد ولو نجح فى الفك اذا الشهادة مصدرة فعلا من سوزان. اذا وجد ان فعلا سوزان هي مصدرة الشهادة فينتقل الى مرحلة التأكد من الشهادة الخاصة باحمد فى حالة سليمة وانه فعلا يحق له التوقيع الكترونيا ولم يتم مثلا انتهاء صلاحية التوقيع الالكتروني الخاص به.
اذا كان كل شيء تمام فإن برنامج مصطفى يأخذ المفتاح العام الخاص باحمد من شهادته لمتابعة باقى خطوات التأكد من صحة توقيع احمد الالكترونى

بالرغم من ان هذه الخطوات السابقة تبدو عديدة ومعقدة إلا أن الأمر يتم من خلال برنامج سهل لاستقبال الرسائل يتيح لمصطفى فقط أن يضغط بالماوس ضغطة واحدة للتأكد من صحة توقيع احمد وبالمثل ضغطة واحدة بالماوس من احمد لكى يمكن ان يوقع رسالة ما توقيعا الكترونيا

أسئلة عامة

ماذا يعنى الشكل القانوني لمقدم العرض؟
- شركة مصرية (مساهمة ، تضامن) أو أجنبية أو تحالف
ما المقصود بالرخص والبيانات الفنية للأجهزة والأنظمة والتطبيقات ؟
- الرخص : اى التراخيص الخاصة بالبرامج المستخدمة
ماذا يقصد بتقديم الضمانات والتأمينات المالية والإجرائية اللازمة لتغطية أي أضرار أو أخطار تتعلق بذوي الشأن ؟
هى الضمانات المادية والإجرائية التي يقدمها طالب الترخيص لقيامه بإصدار شهادات تصديق الكتروني وهى تشمل خطابات الضمان واو ما يماثلها وذلك لتغطية اية اضرار تتعلق بتوقف الخدمة للمستخدمين وكذلك لتغطية التكاليف المطلوبة للتشغيل

بالنسبة للشركات حديثة الانشاء المتقدمة بعروض الترخيص والتى لا تستطيع استيفاء بعض المتطلبات نظرا لحداثتها مثل التقرير المالى السنوي
تقدم الشركات ما يفيد انها حديثة الانشاء . على ان يتم إبداء جدية العروض من خلال الخطة المستقبلية وما يفيد الجدية فى التنفيذ. مدعما ذلك بالمستندات.

- التكنولوجيا المستخدمة :

ما هي حالات قبول او رفض الترخيص؟

- المتقدم للحصول على التراخيص الالتزام بالشروط الفنية والتقنية المذكورة فى اللائحة التنفيذية والملحق الفنى والتقنى
- رفض العرض للحصول على الترخيص اذا تم الإخلال باى شرط من شروط من الشروط والمواصفات الفنية المنصوص عليها في اللائحة التنفيذية
- إلغاء الترخيص اذا ثبت إخلاله بالمتطلبات المذكورة فى القانون واللائحة التنفيذية

ما هي بيانات إنشاء التوقيع الالكتروني ؟

- هى البيانات الخاصة بشهادة التصديق الالكتروني
- البيانات المسجلة فى قواعد البيانات الخاصة بمستخدمي الشهادات
- البيانات الخاصة بقوائم الشهادات الموقوفة والملغاة.

ما هو الـ **PKI** :

هى تكنولوجيا بنية المفتاح المعلن (تقنية شفرة المفتاحين العام الخاص) والتي تستخدم المفتاح العام (المفتاح الشفري العام) والمفتاح الخاص (المفتاح الشفري الخاص) والبيانات المذكورة فى شهادة التصديق الالكتروني المصدرة من جهة تصديق مرخص لها من الهيئة

ماذا تعنى كلا من المصطلحات الآتية؟

- **X 509**
- **PKIX**
- **RSA**
- **A symmetric algorithm**
- **RFC**
- **RFC 3647**
- **Hash algorithm (SHA -1)**
- **RFC 3739**

	Meaning	Comments
X 509	**Cryptographic standards for securing various Internet services like WWW, Mail, etc. and is most widely used standards .**	**In addition to x509 there are many used standard**
PKIX	**The PKIX Working Group X.509-based (PKI technology based on**	

	x 509 group of standards) was established in the Fall of 1995 with the intent of developing Internet standards needed to support an X.509-based PKI.	
RSA	**RSA cryptography is a popular asymmetric key cryptosystem**	**There are other types of a symmetric algorithm like:(DSA, ElGamal, RC[n] etc.)**
Asymmetric algorithm	**When the two keys (private & public) that used in cryptography are different and not deducing one from each other**	**DSA , RSA, EGamal, RC [n]**
RFC	**Request for comment, is based on ideas came from experts around the world and be formulated in standards like.**	
RFC 3647	**Public Key Infrastructure Certificate Policy and Certification Practices Framework This document presents a framework to assist the writers of certificate policies or certification practice statements for participants within public key infrastructures, such as certification authorities, policy authorities, and communities of interest that wish to rely on certificates. In particular, the framework provides a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in a certificate policy or a certification practice**	

	statement. This document supersedes RFC 2527.	
Hash algorithm (SH A-1)	**(Secure Hash Algorithm) A digital signature is formed by encrypting a message digest or hash of the content to be signed.**	
RFC 3739	**This document forms a certificate profile, based on RFC 3280, for identity certificates issued to natural persons. The profile defines specific conventions for certificates that are qualified within a defined legal framework, named Qualified Certificates. However, the profile does not define any legal requirements for such Qualified Certificates. The goal of this document is to define a certificate profile that supports the issuance of Qualified Certificates independent of local legal requirements. The profile is however not limited to Certificates and further Qualified profiling may facilitate specific local needs.**	

لماذا تم اختيار تكنولوجيا شفرة المفتاحين العام والخاص **PKI** دون غيرها؟

- اجمع الخبراء العالميون المتخصصون في مجال تأمين تكنولوجيا المعلومات ان هذه التكنولوجيا هى الاقوى من الناحية التأمينية والتطبيقية.

ما الفرق بين **Symmetric algorithm ، Asymmetric algorithm** ؟

HSM	FIPS 140 -1 Level 3 or higher	Common Criteria
Hardware security module	Federal Information Processing Systems, USA Standards	Common criteria (ISO 15408)

Asymmetric algorithm	Symmetric algorithm
The two different asymmetric keys are mathematically related. If a message is encrypted by one key, the other key is required in order to decrypt the message. In a public key system, the pair of keys is made up of one public key and one private key. The public key can be known to everyone, and the private key must only be known and used by the owner	cryptography, both parties will be using the same key for encryption and decryption. This approach provides dual functionality. Symmetric keys are also called secret keys, because this type of encryption relies on each user to keep the key a secret and properly protected.

ما هو طول المفاتيح الشفرية الجذرية **root key** الخاصة بجهات التصديق الالكتروني ؟

التقنية المستخدمة في إنشاء مفاتيح الشفرة الجذرية لجهات التصديق الإلكتروني من التي تستعمل مفاتيح تشفير بأطوال لا تقل عن ٢٠٤٨ حرف إلكتروني (**bit**).

- ماذا تعنى كلا من المصطلحات الآتية؟

- **HSM**
- **FIPS 140 -1 Level 3 or higher**
- **Common Criteria**

هل استخدام **FIPS 140-1 level 3** و **Common criteria** مطلوب ؟

يجب الالتزام باستخدام احدهما او ما يعادلهما كمعيار لتأمين الاجهزة المستخدمة فى تقديم خدمات التوقيع الالكتروني

ما الغرض من استخدام البطاقات الذكية؟ و ما هى خصائص البطاقات الذكية المستخدمة فى التوقيع الالكتروني؟

تم اختيار البطاقات الذكية كوسيط الكتروني عالى التأمين يضمن عدم النسخ للمفتاح الشفرى الخاص بالمستخدم و يستخدم في عملية إنشاء وتثبيت التوقيع الالكتروني على المحرر الالكتروني

الخصائص:

- المفتاح الشفري الخاص لا يغادر البطاقة أبدا.
- البطاقة محمية بكود سرى
- التشفير وانشاء التوقيع الالكتروني يتم داخل البطاقة الذكية.

- ما المقصود ولماذا تم اختيار الاتى :

Security evaluation ITSEC E4 .
X.509 v 3 certificates .
ISO 7816 .
Microsoft PC/SC .
CAPI – Microsoft cryptographic .
PKCS # 11 .
PKCS # 15 .

APP.	Meaning	Comments
Security evaluation ITSEC E4	**High Security evaluation**	**There are a many levels like E1,E2,E3 …..,etc**
X.509 v 3 certificates	**The used Certificates are formatted in X 509 v 3 . Based on RFC 3739**	**If you have a x.509 v3 cert. you shouldn't you be able to add extensions**
ISO 7816	**The ISO/IEC 7816 series of standards define:** • **The physical shape of the smart card** • **The positions and shapes of its electrical connectors** • **The communications protocols and power voltages to be applied to those connectors** • **The functionality** **the format of the commands sent to the card and the response returned by the card**	**ISO 7816:5 defines numbering for ISO 7816 smart cards. An application identifier (AID) consists of an Registered Application Provider Identifier (RID), identifying the vendor, then a Proprietary Application Identifier Extension (PIX), identifying the application offered by the vendor.**
CAPI	**CAPI, or Cryptographic**	

(Cryptographic Application Programming Interface.) – Microsoft cryptographic	**Application Programming Interface, is an interface to a library of functions software developers can call upon for security and cryptography services. The goal of a CAPI is to make it easy for developers to integrate cryptography into applications. Separating the cryptographic routines from the software may also allow the export of software without any security services implemented. The software can later be linked by the user to the local security services. CAPIs can be targeted at different levels of abstraction, ranging from cryptographic module interfaces to authentication service interfaces.**	
PKCS # 11(Cryptographic Token Interface Standard)	**This standard specifies an API, called Cryptoki, to devices which hold cryptographic information and perform cryptographic functions. Cryptoki, pronounced crypto-key and short for cryptographic token interface, follows a simple object-based**	

	approach, addressing the goals of technology independence (any kind of device) and resource sharing (multiple applications accessing multiple devices), presenting to applications a common, logical view of the device called a cryptographic token	
PKCS # 15(Cryptographic Token Information Format Standard)	**PKCS #15 establishes a standard that enables users in to use cryptographic tokens to identify themselves to multiple, standards-aware applications, regardless of the application's cryptoki (or other token interface) provider.**	**PKCS #15 covers two groups of devices, conventional hardware tokens/IC cards and soft-tokens implemented entirely in software.**

- ما الفرق بين (**Reader / Readerless / Contactless**) ؟

Reader	Readerless	Contactless
استخدام بطاقات ذكية تعمل على قارئ البطاقات التى يتم تزويد الاجهزة به.	يتم استخدام بطاقات ذكية تدعم تكنولوجيا **USB** وذلك لسهولة الاستخدام مع أجهزة الحاسب المدعمة بهذه التكنولوجيا	يتم استخدام تكنولوجيا عدم الاتصال (لاسلكى) للربط بين البطاقة الذكية وجهاز الحاسب

ملحوظة :

البطاقات الذكية يتم استخدام **FIPS PUB 140 – 1 Level 2 or higher**، بينما **HSM** يتم استخدام **FIPS 140- 1 level 3 or higher**

اذكر المعايير الفنية المستخدمة في عمل اللائحة العملية للتنفيذ؟

ETSI 456	RFC 3647
Recommended Standards: ETSI (The European Telecommunications Standards Institute) TS 101 456 V1.2.1 (2002-04) Policy requirements for certification authorities issuing qualified certificates, specifically Chapter 7	**A baseline Certificate Policy for service providers issuing qualified certificates should be written according to the IETF (Internet Engineering Task Force) PKIX framework RFC 3647.**

ما هي النقاط التي يتناولها ٤٥٦ **ETSI** ؟

- اللائحة العملية للتنفيذ.
- إدارة المفاتيح.
- إدارة الشهادات.
- إدارة العمليات.
- النواحي التنظيمية

- ما الفرق بين **BS7799-2** ، **ISO/IEC 17799** ؟

ISO/IEC 17799	BS7799-2
This guidance is used to guide applicants for BS 7799 showing how to implement these standards. But the certificate is issued against the BS 7799	**(British Standards, Information security management systems specification The certificate is issued against the BS 7799. And this standard is the audit criteria**

ما الفرق بين النموذج ١ والنموذج ٢ المذكورين فى فى كراسة الشروط والمتطلبات؟

نموذج ١ :

نموذج التقدم بعرض للحصول على الترخيص (مرحلة أولى)

نموذج ٢:

نموذج طلب الترخيص (مرحلة تالية بعد تخطى المرحلة الأولى) ويشمل هذا النموذج القواعد الحاكمة لاجراءات الحصول على الخدمة، والتى يلتزم طالب الترخيص بها قبل وبعد الترخيص له بمزاولة النشاط