1.2 مقدمة:

أمن الأعمال التجارية عبر الإنترنت هي قضية تشهد تطوراً متسارعاً، ليس فقط من حيث التقدم التكنولوجي ، بل في طرق تنفيذ وتطبيق هذه التقنيات وتعدد استخداماتها وتنوعها، فعلى سبيل المثال تقنيات الجدران النارية وأنظمة كشف التسلل و'الشبكات الخاصة الافتراضية (VPN) جميعها كانت تخدم ولا زالت أهداف تعزيز أمن معلومات الشبكات وأنظمة المعلومات ومراكز المعلومات والتي من خلالها تم تدعيم مفاهيم مثل الشبكة الخاصة والشبكة العامة (Private network and Public Networks) ، أي تم التمييز بين ما هو خاص (Private) وما هوعام (Public) ، ولكن تم ربط هذه المفاهيم بالواقع الجغرافي الفيزيائي لمراكز المعلومات وشبكات المعلومات (حتى في الشبكات الخاصة الافتراضية (VPN) تقوم بربط جهتين ذات واقع فيزيائي وجغرافي) وذلك لخدمة توفير الحماية لكل ما هو داخل الشبكة الخاصة مثل الخوادم (Servers) ، والمستخدمين، وقواعد البيانات، والتطبيقات التجارية (Business Application) ، ولكن ماذا عن البيانات والمعلومات التي يتم إرسالها خارج الشبكة الخاصة عندما تسافر عبر الشبكة العامة (The Internet) ، كيف يتم التحقق من صحتها، كيف يتم حمايتها من السرقة وهي خارج حدود الشبكة الخاصة ، هنا يبرز دور البنية التحتية للمفتاح العام (مرفق المفاتيح العمومية) والشهادات المصدقة.

2.2 مفهوم الصرافة:

هي مؤسسة فردية أو شركة تضامن مرخص لها بمزاولة أعمال الصرافة وفقاً للأنظمة المعمول بها وأحكام هذه القوعد. ويصدر الترخيص لكل صرافة من الجهة المسؤولة عن منح التراخيص المالية. ويتم ذلك خلال فترة السنة المالية الميلادية التي تبدأ من 1 يناير وتنتهي في 31 ديسمبر من كل سنة، وذلك لأغراض الدراسات المالية المقارنة [1].

1.2.2 أعمال الصرافة:

- شراء وبيع العملات الأجنبية، والشيكات السياحية، وشراء الشيكات المصرفية.
- تحويل الأموال داخل الجمهورية وخارجها لمن سبق له الحصول على ترخيص من المؤسسة بذلك، ساري المفعول وقت صدور هذه القواعد [1].

2.2.2 الشروط التي يجب الإلتزام بها في كل صرافة:

1. الالتزام بمتطلبات السلامة الأمنية الصادرة عن المؤسسة.

2. تطبيق قواعد إعرف عميلك وقواعد مكافحة عمليات غسل الأموال وتمويل الإرهاب الصادرتين عن المؤسسة، وغيرها من التعليمات ذات العلاقة.

3. وضع الترخيص الممنوح له من المؤسسة والإعلان عن أسعار العملات التي يتعامل بها في مكان بارز في مقره.

4. أن يقرن إسمه برقم الترخيص في جميع مطبوعاته ومراسلاته وجميع ما يصدر عنه.

5. التعامل مع عملائه بموجب إيصالات رسمية لكافة عمليات الصرافة المسموح له بمزاولتها.

6. الإعلان للعملاء في مكان بارز عن ضرورة الحصول على إيصالات عن أي عملية يقوم بتنفيذها لعملائه.

7. تجهيز أماكن عمله بالأجهزة اللازمة لعد النقود وفرزه وكشف العملات المزيفة.

8. التأمين على الممتلكات ضد الحرائق والسرقة لدى أحد مقدمي التأمين المرخصين [1] .

3.2.2 شروط البدء بأعمال الصرافة:

يجب على كل صراف الحصول على موافقة كتابية مسبقة من المؤسسة وفقا للشروط التي تحددها قبل أن يقوم بأي عمل من الأعمال الآتية:

1. فتح فرع أو أكثر لمزاولة أعمال الصرافة، أو تغيير مقر المركز الرئيسي أو أحد الفروع.
2. ب. أي تغيير في هيكل رأس المال أو ملكيته.
3. ج. التوقف عن مزاولة أعمال الصرافة [1] .

3.2 مفهوم أمن المعلومات:

مع تطور التكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة أو ما يسمى نقل_البيانات عبر الشبكة من موقع لآخر أصبح النظر إلى أمن تلك البيانات والمعلومات بشكل مهم للغاية. يمكن تعريف أمن المعلومات بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية. المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات.

وأمن المعلومات ليس بالاختراع الجديد ولكن دائماً ما كان يحرص الإنسان على الاستفادة مما لديه من معلومات وألا يبوح بها إلا لمن يثق به أو يمكن أن يستفيد من هذه المعلومات، ولكن مع تطور تكنولوجيا المعلومات والزيادة الهائلة والمضطردة في كميات المعلومات والبيانات المتاحة في العالم وظهور شبكات المعلومات وقواعد البيانات التي يتم تخزين المعلومات فيها، أصبح من الضروري تنظيم عمليات الوصول إلى هذه المعلومات بتحديد الأشخاص المخول لهم الوصول إلي هذه المعلومات وكيفية ومستوى الوصول إليها [2].

1.3.2 المبادئ الأساسية لأمن المعلومات:

وهي من أهم المفاهيم قبل أكثر من عشرين عاما، وأمن المعلومات قد عقدت السرية والنزاهة وتوافر (المعروفة باسم الثالوث (سي آي ايه (CIA)) والمبادئ الأساسية لأمن المعلومات. العديد من المتخصصين في مجال أمن المعلومات الذي نؤمن إيماناً راسخاً بأن المساءلة ينبغي أن تضاف كمبدأ أساسي لأمن المعلومات .

1.1.3.2 السرية:

السرية هو المصطلح المستخدم لمنع الكشف عن معلومات لأشخاص غير مصرح لهم بالإطلاع عليها أو الكشف عنها. على سبيل المثال، بطاقة الائتمان والمعاملات التجارية على شبكة يتطلب رقم بطاقة الائتمان على أن تنتقل من المشتري إلى التاجر ومن التاجر لإنجاز وتجهيز المعاملات على الشبكة. يحاول النظام فرض السرية عن طريق تشفير رقم البطاقة أثناء الإرسال، وذلك بالحد من ظهور تسلسل رقم البطاقة (في قواعد البيانات، وسجل الملفات، النسخ الاحتياطي، والإيصالات المطبوعة)، وذلك بتقييد الوصول إلى الأماكن التي يتم تخزين

الرقم والبيانات بها. أما إذا كان الطرف غير المصرح به قد حصل على رقم البطاقة بأي شكل من الأشكال، وبذلك فقد تم انتهاك مبدأ السرية في حفظ وتخزين البيانات.

2.1.3.2 السلامة:

في مجال أمن المعلومات، السلامة تعني الحفاظ على البيانات من التغيير والتعديل من الأشخاص الغير مخول لهم بذلك. عندما يقوم شخص بقصد أو بغير قصد بانتهاك سلامة أو الإضرار أو حذف ملفات البيانات الهامة وهو غير مخول بذلك فهذا انتهاك لسلامة البيانات، وعندما يصيب فيروس كمبيوتر ويقوم بتعديل بيانات أو اتلافها فهذا انتهاك سلامة بيانات، وعندما يكون الموظف قادراً على تعديل راتبه في قاعدة البيانات والمرتبات، وعندما يقوم مستخدم غير مصرح له بتخريب موقع على شبكة الإنترنت، وهلم جرا. و تعني سلامة البيانات كذلك، أن تكون التغيرات في البيانات مطردة، فعندما يقوم عميل البنك بسحب أو إيداع، ينبغي أن ينعكس ذلك على رصيده في البنك.

3.1.3.2 توفير قاعدة البيانات:

يهدف أي نظام للمعلومات لخدمة غرضه، يجب أن تكون المعلومات متوفرة عند الحاجة إليها. وهذا يعني أن الأنظمة الحاسوبية المستخدمة لتخزين ومعالجة المعلومات، والضوابط الأمنية المستخدمة لحمايته، وقنوات الاتصال المستخدمة للوصول إلى ذلك يجب أن يعمل بشكل صحيح. توافر نظم عالية السرية تهدف إلى استمرارية الحماية في جميع الأوقات، ومنع انقطاع الخدمة بسبب انقطاع التيار الكهربائي، أو تعطل الأجهزة، أو نظام الترقيات والتحديث.

إن أبسط أنواع الحماية هي استخدام نظام التعريف بشخص المستخدم و موثوقية الاستخدام ومشروعيته وهذه الوسائل تهدف إلى ضمان استخدام النظام أو الشبكة من الشخص المخول بالاستخدام وتضم هذه الطائفة كلمات السر بأنواعها، والبطاقات الذكية المستخدمة للتعريف، ووسائل التعريف البيولوجية والتي تعتمد على سمات معينة في الشخص المستخدم متصلة ببنائه البيولوجي المفاتيح المشفرة ويمكن أن نضم إلى هذه الطائفة ما يعرف بالأقفال الإلكترونية التي تحدد مناطق النفاذ[3] .

4.2 البنية الأساسية للمفتاح العام ومكوناتها:

إن التجارة الإلكترونية و المعاملات المصرفية تتطلب التدابير الأمنية الصارمة و المشددة، ومن المعروف بأن استخدام الشركات للإنترنت كمنصة لممارسة أنشطتها التجارية سيرفع معدل نجاحهم لكن هناك المخاطر التي ستواجهها الشركة و أهمها انتحال الشخصيات وتغيير المعلومات الحساسة المتناقلة عبر الإنترنت أو التجسس عليها و هنا تظهر أهمية وجود بروتوكولات أمنية مشددة لحماية مصالحهم ، والخصوصية ،وتوفر الاتصالات الآمنة ، وقيمة التبادل ، وأصول المعلومات.

البنية التحتية للمفتاح العمومي (PKI) هي عبارة عن منظومة أمنية متكاملة لتوفير بيئة مناسبة للتعامل الآمن عبر شبكات الحاسب الآلي وتعتبر نظاما لإدارة مفاتيح التشفير بواسطة الشهادة الرقمية.

هيكل المفتاح العمومي هو نظام كامل لإنشاء وإدارة المفاتيح العمومية يستخدم لتشفير البيانات وتبادلها بين مستخدمي تلك المفاتيح، إما أن تكون مثبتة على شبكة مؤسسة، أو أنها قد تكون متوفرة في البيئة العامة، فظهرت الحاجة لهذا النظام بسبب المخاطر التي تواجهها التجارة الإلكترونية في الإنترنت والتي من أهمها انتحال الشخصيات وتغيير المعلومات المتناقلة عبر الإنترنت أو التجسس و الإطلاع عليها [4].

حاليا تعتبر الشهادة الرقمية المبنية على تقنية المفتاح العمومي أفضل وسيلة لتحقيق المتطلبات الأمنية لمستخدمي التطبيقات الإلكترونية. إن استخداماتها في مجال التعاملات الإلكترونية عديدة فهي تستخدم في التحقق من هويات المستخدمين عند الدخول إلى أنظمة الحاسب و الإنترنت من خلال الشهادة الرقمية و تستخدم أيضا للحد من الخطابات الورقية في التعاملات الإلكترونية وذلك بتفعيل التوقيع الرقمي، وكذلك لمنع المتجسسين والعابثين من الإطلاع على وثائق وتعاملات الآخرين من خلال آلية التشفير المتوفرة من خلال بنية المفاتيح العامة و المفاتيح السرية، بشكل عام يمكن الاستفادة منها في جميع الأنظمة الإلكترونية كالحكومة الإلكترونية والتعليم عن بعد والتجارة الإلكترونية وغيرها من الأنظمة التي تتطلب اتصالات آمنة و موثقة. من خلال هذا المقال سنتعرف على البنية التحتية للمفتاح العمومي و كيف أن الترميز بالمفتاح العمومي يدعم متطلبات الإدارة التجارية الإلكترونية و أنه حل مناسب للمشاكل الأمنية في بيئات الشبكات غير المتجانسة (heterogeneous network environments) [7] .

1.4.2 أهداف البنية التحتية للمفتاح العام:

تتلخص أهداف البنية التحتية للمفتاح العمومي (PKI) كالتالي:

1.1.4.2 التحقق من الهوية (Authentication):

هي تمكين المستخدمين من معرفة هوية بعضهم البعض و التحقق منها بشكل قاطع.

2.1.4.2 سرية البيانات (Confidentiality):

هي التمكن من تبادل المعلومات بحيث لا يمكن للآخرين معرفة طبيعة تلك البيانات.

3.1.4.2 سلامة البيانات (Integrity):

هي التمكن من كشف أي محاولة لتغيير أو تعديل محتوى المعلومة بعد الإرسال.

4.1.4.2 التوقيع الإلكتروني (Electronic Signature):

التوقيع على وثيقة مع مقدرة المستلم التحقق من صحة التوقيع، و بذلك يتم التحقق من الهويات عبر الوثائق الإلكترونية و الشهادات الرقمية [4] .

2.4.2 مكونات البنية الأساسية للمفتاح العام:

البنية التحتية للمفتاح العام هي عبارة عن إطار عمل- أي مجموعة من الخدمات المشتركة سواء كانت برمجيات ، أجهزة ، سياسات وإجراءات أو أشخاص- لإنشاء وسيلة آمنة لتبادل المعلومات بالاعتماد على تشفير المفتاح العام. أساس ال (PKI) هو شهادة السلطة ((certificate authority (CA)) والتي تصدر الشهادات الرقمية التي توثق هوية المنظمات و الأفراد عبر نظام عام مثل شبكة الانترنت. وتشتخدم الشهادات أيضا في توقيع الرسائل ، مما يضمن صحة و مصداقية الرسائل وعدم العبث بها [8].

تتألف البنية التحتية للمفتاح العام (PKI) من:

1.2.4.2 سلطة المصادقة على الشهادات الرقمية ((CA) Certificates Authority)) :

سلطة للتحقق من هوية الأفراد وهي تصدر شهادات رقمية وتدير أعمال الشهادات الرقمية .

2.2.4.2 سلطة التسجيل ((Registration Authorities(RAs)) :

سلطة للتدقيق في طلبات المتقدمين لطلب شهادة رقمية .

3.2.4.2 المشتركون (End Entities or Subscribers) :

أشخاص أو جهات بحاجة إلى الشهادة الرقمية لتمييزهم عن بعضهم البعض .

4.2.4.2 إعتماد الأطراف (Relying Parties) :

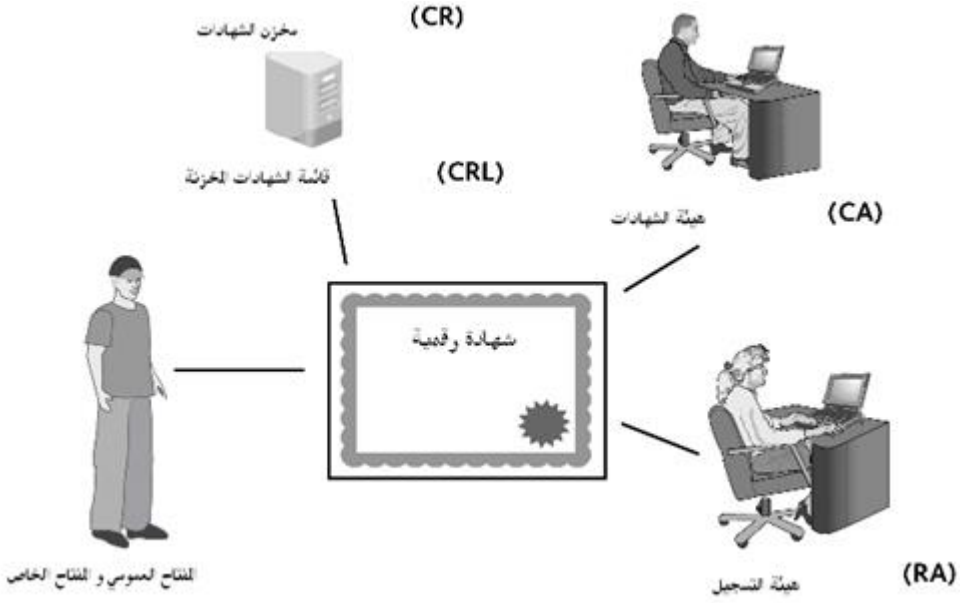
يتم إعتماد الأطراف بواسطة رقم هوية (جواز سفر ،رخصة قيادة ،بطاقة شخصية ،...) أو غيرها، ويجب أن تكون سارية المفعول حين يتم إستخدامها .

5.2.4.2 الدلائل (Directories) :

يخزن بها الـ (Public key) والشهادات الرقمية وقوائم إلغاء الشهادات الرقمية .

6.2.4.2 السياسات والإجراءات (Policy and Procedure) :

لابد من وجود سياسات معتمدة من قبل جهة موثوقة من أجل تطبيق البنية الأساسية للمفتاح الأساسي [4] .



الشكل (1.2) : يوضح عناصر توليد الشهادة

5.2 وظائف البنية التحتية للمفتاح العام:

1.5.2 إصدار شهادات التوثيق (Issuing Certificates) :

تقوم (CA) بالتوقيع على الشهادة لتوثيق شخص ما ، شهادات التوثيق يضاف إليها تاريخ انتهاء ومعلومات أخرى، نستطيع تلخيص دورة حياة الشهادة إلى أربع نقاط هي:

1. إنشاء
2. إلغاء
3. إنتهاء
4. تعليق

2.5.2 إبطال الشهادات (Revoking Certificates) :

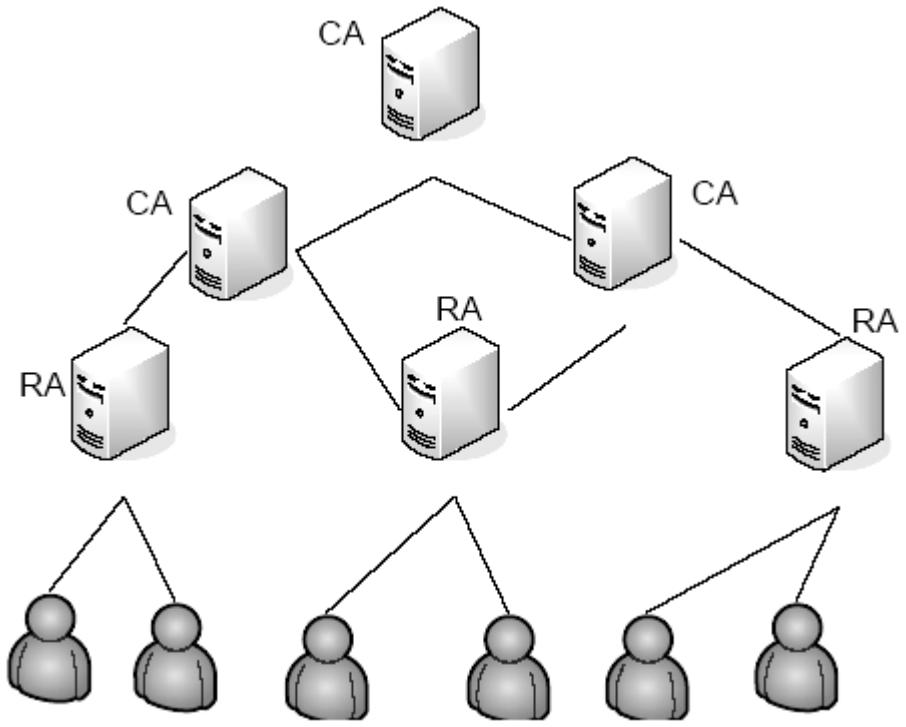
قد تقوم (CA) بإبطال الشهادة قبل انتهاءها لعدة أسباب منها تغير اسم المستخدم، اكتشاف مفتاح المستخدم الخاص، تحت هذه الظروف تقوم CA بإبطالها بتضمين رقم تسلسلي على قائمة الشهادات المرفوضة ((Corticated Revocation Lists(CRL)).

3.5.2 تخزين واسترجاع الشهادات (Storing and Retrieving Certificates and (CRLs)):

أغلب طرق تخزين و استرجاع الشهادات تكون عن طريق خدمات الأدلة، من خلال نظام الدخول في أدلة المعلومات (LDAP) ، الانترنت (HTTP) و البريد الالكتروني .

4.5.2 إعطاء الثقة (Providing trust) :

كل مستخدم عنده مفتاح عام يجب أن يكون مسجل عند (CA) يوثق به ، المنظمات تستطيع أن تأسس وتعدل لتمنح هذه الثقة من خلال ما يسمى بـ: مجال إدارة الأمن (single security management domain) مع بقاء الإشراف عن طريق (CA).



الشكل (2.2) : يوضح هرمية إعطاء الثقة.

5.5.2 التوقيع الإلكتروني:

عندما يقوم المستخدم بتشفيرالرسالة مستخدما المفتاح الخاص به فإنه يكون قد أضاف إليها ما يسمى بالتوقيع الإلكتروني، حيث أن هذا التشفيرلايفك إلا بواسطة المفتاح العمومي للمستخدم نفسه – مالك المفتاح الخاص – وبذلك يضمن بأن الرسالة قد أرسلت من ذلك الشخص [4].