بسم الله الرحمن الرحيم

مارس ٢٠١١

المصادقة الالكترونية
النموذج السوداني المقترح

د/ عادل عبد العزيز الفكي
adilalfaki@hotmail.com

١. مقدمة:

إن التطور الهائل في التقنيات الإلكترونية خلال العقود الماضية أدى لتطور وتنوع حياة البشر بصورة غير مسبوقة من قبل في التاريخ البشري. وحصر هذه الوسائل والمعدات التي دخلت في الحياه اليومية للانسان يصعب حصرها .

وفي هذا الحيز سنتناول جزئية صارت هامة في هذه التقنيات المتسارعة الخطى .

إن قيام وتطور الشبكة العنكبوتية العالمية أدى لتطورات وتطبيقات سهلت كثيرًا من سبل الحياة، وسهولة تداولها، وكفاءة الإنسان في تناول الموارد صياغة ونقلاً وتغييراً. وبالتالي صارت صناعة المعلوماتية والاتصالات من الممكنات، وليست ترفاً تقنياً بل ان اقتصاديات البشرية اليوم تعتمد تماماً على هياكل تقنية المعلومات والاتصالات وبذلك صارت ما يسمى Enabling Technology صناعة لها هيمنة وبأس. عبرها يتم تداول المعلومات التجارية، المالية، الأمنية، المعرفة الإنسانية، الأقمار الصناعية، الموارد الطبيعية والتواصل الإنساني بكل تبعاته. وتطول القائمة .

وفي عالم اليوم نجد أن الشبكة العنكبوتية قد غطت كل أطراف الكون عبر شبكة الاتصالات السلكية واللاسلكية ، وصارت وسيطاً هاماً للتبادل التجاري والاقتصادي والمالي . ونظاماً كفءً ورخيصاً بسيطاً ، خاصة عبر البرمجيات التي سهلت الربط وسهولة التناول والمخاطبة .

ولكن حساسية المعلومات المتداولة في النشاطات المالية والبنكية، التجارية، والعقود القانونية المتنوعة جعلت من الضروري العمل على حماية هذه المعلومات اثناء سيرها وحملها في الشبكات الإلكترونية. خاصة حمايتها من الأعمال الإجرامية المتمثلة مثلاً في :

١- التصنت الغير مأذون Confidentially
٢- تغيير المعلومات وتزويرها Integrity
٣- انتحال الشخصية الاعتبارية Authenticity

فرغم ان الشبكة العنكبوتية بكل معداتها من أجهزة الكمبيوتر، محولات المسارات Routers، المانعات Firewalls والبرمجيات قد سهلت الكثير إلا أن نفس هذه التقنيات أتاحت ثغرات يمكن عبرها إفساد كل هذه الميزات، وإضاعة الحقوق .

لذلك اهتم العلماء والمختصون بايجاد وسائل من خلالها يمكن ان يتم التداول الآمن للنشاط الإقتصادي ، التجاري ، المالي والقانوني وبذلك يستفاد من ثمرة التقنيات الالكترونية وما قدمته من سهولة الاتصال والتواصل.

وكان من أهم هذه الإجراءات هو قيام كيان متكامل من:

- المعدات
- الأفراد
- البرمجيات
- الإجراءات

يؤمن ويمكن من التداول الآمن للتجارة والخدمات عبر الشبكة الإلكترونية.

وهو ما يصطلح بتسمية " البنيات الأساسية للمصادقة الإلكترونية" Public Key Infrastructure.

٢. هيكل المصادقة الإلكترونية:

قامت الدولة بإصدار التشريعات القانونية الضرورية والكافية، لحد ما، لقيام هذه المؤسسات فأصدرت قانون المعاملات الالكترونية للعام ٢٠٠٧ الذي نص على قيام اللجنة الوطنية للمصادقة الالكترونية. كما أصدرت قانون جرائم المعلوماتية وهو قانون عقابي استقي من قانون الاونسترال النموذجي مع بعض التعديلات التي تلائم طبيعة المجتمع السوداني. غير أننا في هذه المذكرة سنتناول طرح مقترح إنشاء جزئية "الهيكل التصديقي" Trust Model.

أدركت الدولة أهمية تقنية الاتصالات في إدارة النشاط المالي والتجاري وكان لا بد من إصدار التشريعات القانونية اللازمة لترتيب هذه الممارسة الجديدة وتكييفها قانونياً وتأكيد تبعاتها اللازمة، حسب مقتضيات القوانين السارية في البلاد. وكذلك القوانين العالمية، التي تنظم البنوك ، والتجارة، والمنازعات المدنية عامة، وحقوق التملك، ونقل الملكية. بصدور قانون ٢٠٠٧ للمعاملات الإلكترونية صرح بقيام سلطة جديدة، أتاح لها الإشراف والإنشاء والتصديق الكامل بإنشاء اللوائح المنظمة والإجراءات الكفيلة بممارسة التداول الإلكتروني للتجارة والخدمات.

ولكي تمارس هذه الهيئة الجديدة سلطاتها كان لا بد لها من إنشاء جهاز تنفيذي يناط به العمل اليومي والتفضيلي لهذه السلطة الجديدة.

ومهام هذه السلطة موضحة بالعموم في نص القانون المذكور في المواد من ١٤-٢٦ وأهم ما يستهدفه التنظيم القانوني للجنة في المواد المذكورة:-

- بناء الثقة في نظام الشهادات الرقمية.
- بناء الثقة في سرية تداول المعلومات.
- بناء الثقة في إثبات الهوية وإجراءاتها.
- الثقة في حفظ المفاتيح الإلكترونية السرية.

وعليه فإن اللجنة تمارس عملاً سيادياً قانونياً له تبعاته الخطيرة على الدولة ككل وأجهزتها العاملة. ان أي تسريب في هذا الجهاز التنفيذي أو خلل في إجراءاته سيؤدي لإنهيار الثقة في أجهزة البلاد عامة، دع عنك

الأضرار المالية التي ستصيب البنوك والشركات التي ستعتمد إجراءاتها على هذه الشهادات الصادرة من سلطة المصادقة الإلكترونية.

٢,١ كيف ستؤثر هذه المهام على هيكلية السلطة؟

ولكي نتناول هذا السؤال المحوري الهام سنتطرق أولاً لأجهزة شبيهة المهام داخل البلاد. ونرى كيف بنيت سلطاتها وأجهزتها التنفيذية.

إن إثبات الهوية والشخصية الإعتبارية في الدولة تنتجها أجهزة سيادية بحتة:

١- إثبات الهوية "الجنسية"

هذه الخدمة تقوم بها الشرطة القومية من إجراءات التحقق والإصدار والحفظ والمتابعة والتوثيق لكل مراحل الإجراءات. وقد كلفت الشرطة بهذا الإجراء بموجب القانون الصادر . وتم تكليف الشرطة كجهاز حكومي سيادي بحت للقيام بهذه المهمة لخطورتها المعلومة. بل كل المراحل تقوم بها أجهزة الشرطة:

١. إصدار أُرنيك الطلب
٢. فحص الأُرنيك
٣. إجراء التحري
٤. المصادقة
٥. إصدار الأوراق
٦. ختم بطاقة الهوية وإصدار رقم سري لها.
٧. حفظ كل المستندات المرافقة للطلب.
٨. حفظ الإجراءات التي تمت.

الملاحظ أن معظم الدول في العالم يلتزم فيها الإجراء أعلاه هيئات حكومية وليس بالضرورة الشرطة.

وفي قليل جداً من الدول المتقدمة صناعياً يتم جزء من هذه الإجراءات بواسطة القطاع الخاص. فجزء تقوم به هيئة حكومية وجزء آخر مثل توفير الطباعة، وأجهزة حفظ المستندات; تقوم به شركات.

٢- البطاقة الشخصية (ID)

وهذه أيضاً وثيقة هامة يتم اعتمادها في كل الإجراءات المالية، وإجراءات التعاقدات، وتحويل الملكيات المختلفة. وأي خللٍ في إصدار هذه البطاقة يؤدي لعواقب مضرة بالمجتمع والأجهزة المعنية.

أيضاً يقوم جهاز الشرطة القومية بعمل إجراءات البطاقة من:

- طلب أُرنيك
- فحص أُرنيك
- مراجعة الوثائق المرفقة
- سلطة التصديق
- إصدار البطاقة (وأرقامها السرية)
- حفظ كل مستندات الإجراءات

ولم يفكر أحد في معظم الدول إسناد هذا الإجراء لجهة تجارية تقدم كل الضمانات الطلوبة من سرية وحفظ وخلافه.

رغم وجاهة المقترح من أن يترك الأمر للمنافسة التجارية الحرة، وأن تقوم شركات مختلفة بالولايات وخلافه لإصدار هذه الأوراق الثبوتية.

ولا نريد أن نذكر تفاصيل الكثير من الإصدارات الثبوتية تقوم بها أجهزة حكومية محضة، وذلك لحساسية المهمة والتصاقها بسيادة الدولة.

وكسبيل المثال نذكر:

- شهادات الشركات : مسجل الشركات – وزارة العدل
- سجل المركبات : شرطة المرور
- سجل الأراضي : الهيئة القضائية
- سجل الأندية : وزارة الشباب
- سجل الجمعيات : مسجل المنظمات
- سجل الطائرات والبواخر : سلطات الطيران المدني والنقل البحري
- اعتماد الشهادات التعليمية : وزارة التربية والتعليم
- اعتماد شهادات الخبرة : وزارة الخارجية

فمن الملاحظ أن معظم أعمال السيادة تقوم بها جهات حكومية، وتمارس فيها سلطاتها ونشاطاتها بموجب القانون. وهي في جلها خدمات ولا مانع من رسوم تفي بأغراض المصروفات وتسيير العمل.

ولكن أيضاً بنظرة موضوعية للشأن السوداني فيما يتعلق بأمر تطور المرافق العامة والخاصة، نرى فيه نهجاً معيناً، هو السائد وهوالأكثر نجاحاً لظروف وخصوصية البلد، وطباعها وتركيبها الاجتماعي والثقافي وهياكل الحكم وأدواته والموروثات من الأداء الإداري.

وخلاف ذلك; فالمثال الأوحد الذي يذكر دائماً في المناسبات الإدارية والإقتصادية لنهج تحويل إدارة حكومية لتجارية هو هيئة الاتصالات التي تحولت لشركة "سوداتل".

وبنظرة دقيقة لهذه الحالة الفريدة، نرى ما يلي:

- عرضت الحكومة سعر متدني جداً للأصول من أراضي ومباني وحصر المكالمات العالمية لمدة خمسة عشر سنة . وذلك لغرض إغراء المستثمرين وتشجيعهم للشراء والمشاركة، وهذا أمر مطلوب.

- رغم ذلك لم يتم دفع رأس مال معتبر يمكن من تحديث المعدات والكبانيات والكوابل.

- كان القرار الصائب من مدير الهيئة آنذاك أن وقع عقداً مع شركة Siemens الألمانية و Alcatel بمقتضاها تقوم الشركتان بتركيب كبانيات رقمية متقدمة وكوابل وألياف ضوئية ... الخ. على أن تقوم الشركة بتحصيل المكالمات العالمية كضمان لعملها.

وعليه نرى حتى في هذا المثال الوحيد أن الدور الحكومي هو الذي كان حاسماً في تحويل وإنجاح المؤسسة.

ونعود مرة أخرى لسلطة المصادقة الإلكترونية ودورها السيادي والتشغيل للمفاتيح السرية ومقارنتها بالهيئات والسلطات الشبيهة. والتي جلها مؤسسات حكومية سيادية تشرف على الإجراءات وإصدارها. وعليه فإن ما ستقوم به هيئة المصادقة الإلكترونية هو دور سيادي متعلق ببناء الثقة والمحافظة عليها وسرية المفاتيح وتأمين المتعاملين فيها وبها.

وبقرائتنا للحال السوداني وتاريخه، وكذلك آخذين في الاعتبار الدول الشبيهة بنا نرى أن مثل هذه الأعمال يجب أن تقوم بها الدولة، وتوفر لها كل المقومات اللازمة واليد القانونية النافذة.

فيمكننا أن نصنف عمل سلطة المصادقة الإلكترونية بانه عمل سيادي يتوقف على حسن أداءه إعتماد التعامل القانوني للتبادل المالي والتجاري والتعاقدي، وكذلك سرية تداول أي وثائق ومنها الجواز الإلكتروني. وليس بأي حال هو عمل تجاري محض يحقق أرباحاً لمتعاطيه والمستثمرين فيه.

إنه عمل يكاد يطابق إجراءات البطاقة الشخصية من التحقق والإثبات.

أن النموذج الأمريكي لشركة VeriSign وأخواتها نموذج فريد تتفرد به الولايات المتحدة لما تتميز به من تاريخ وتركيب حكم وفلسفة إقتصاد وممارسة. حتى أن السجون هناك تديرها شركات خاصة ولا يوجد مثيل لذلك حتى في الدول الأوروبية الصناعية المتقدمة.

بل إن كل الصناعات الحربية المتقدمة والحساسة يقوم بصناعتها القطاع الخاص وهذا ليس في خيال دول في عالمنا، بل ان مفاعلات الطاقة الذرية في دول الغرب تقوم بها الشركات الخاصة . فلا مجال للمقارنة حيث أن التطور التاريخي والإجتماعي لهذه الدول يختلف تماماً عما هو حادث في بلادنا.

ولكي نكون أكثر دقة في نموذج الولايات المتحدة أن المنسق العام للمفاتيح تديره الهيئة الفدرالية Federal Bridge CA وفي ذلك تمثل السلطة وخاصة فيما يتعلق بأجهزة الحكومة الإلكترونية. خاصة ان هناك الكثير من المشاكل والعوائق التي يجب أن تنسق حتى يمكن أن يحقق هدف بناء الثقة (Trust) وبالتالي توفير الخصوصية للتبادل الإلكتروني من:

- التوثيق Authentication
- السرية والخصوصية Confidentiality
- إنتحال وتزوير المحتوى Integrity

هذه كلها أمور خطيرة ودقيقة ولا يمكن بأي حال في الظروف الحالية أن يقوم بها القطاع الخاص منفرداً. ولكن ربما في المستقبل أن يعطي القطاع الخاص دوراً في سلسلة الإجراءات التي تتم في التوثيق الإلكتروني.

وحتى نكون أكثر وضوحاً ودقة في هذه النقاط لا بد أن نستعرض المشاكل والمعوقات التي تحتاج لدرجة عالية من التنسيق والتعاون الحكومي ومن الجهات المختلفة حتى تتمكن اللجنة من القيام بدورها حسب مقتضيات القانون والمهام والواجبات المناط بها. والمحافظة التامة لأهداف المشروع وهو سيادة وموثقية الشهادات الإلكترونية وسريتها حتى تؤمن التبادل المالي والتجاري والعقودات ومعلومات خاصة الأفراد.

ولكي ندرك التشابك والتداخل في مسألة بناء الثقة بين الجهات المختلفة سنستعرض النماذج الممكنة لبناء هيكل المصادقة.

٣. هياكل المصادقة ومواصفاتها: Trust Models

إن من المهام الأساسية والرئيسية في بنيات المفاتيح الإلكترونية هو إنشاء وصيانة الثقة بين الجهات المتعاملة، بل المساعدة في انتشار هذه الثقة.

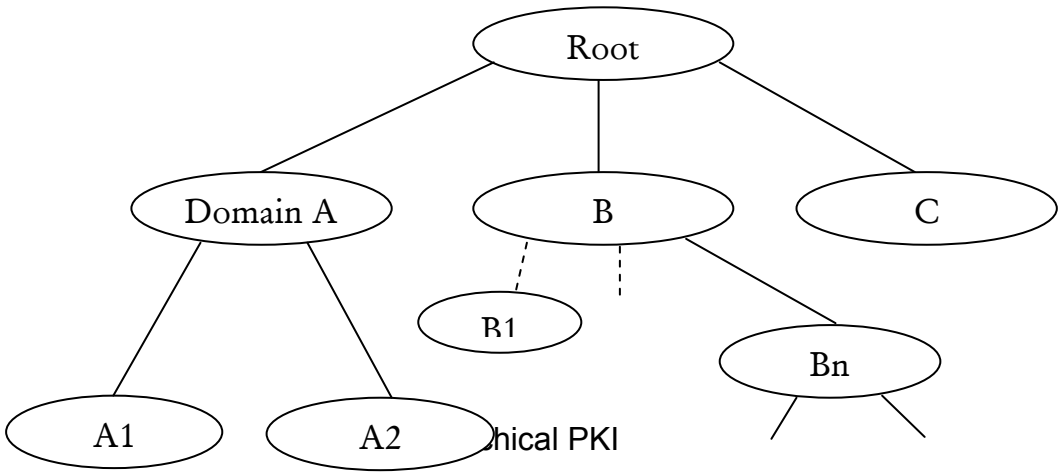
٣,١ جهاز تنفيذي وحيد: Single CA

وهذا نموذج سهل لأنه جهاز واحد لكل البلد، وبالتالي المرجعية للجذر سهلة ومحدودة . ولكن بالطبع يعاني مشكلة تعامل قطاعات غير متشابهة في نطاق واحد. أي بمعنى أن مؤسسات الدولة المختلفة السيادية، الخدمية ، الاجتماعية والقطاع الخاص بمشاربه المختلفة تتعامل بمواصفات واحدة دون الخصوصية التي ربما توجد أحياناً في قطاع معين، مثل القوات المسلحة.

ولتفادي مشكلة الخصوصية هذه، تنشأ تحت الجهاز التنفيذي الوحيد عدة نطاقات متفرعة من الجسم الرئيسي ولكن مربوطة به مباشرة، هذا يسمى النظام الهرمي (Hierarchy) .

٣,٢ بنيات المصادقة الهرمية: Hierarchy PKI

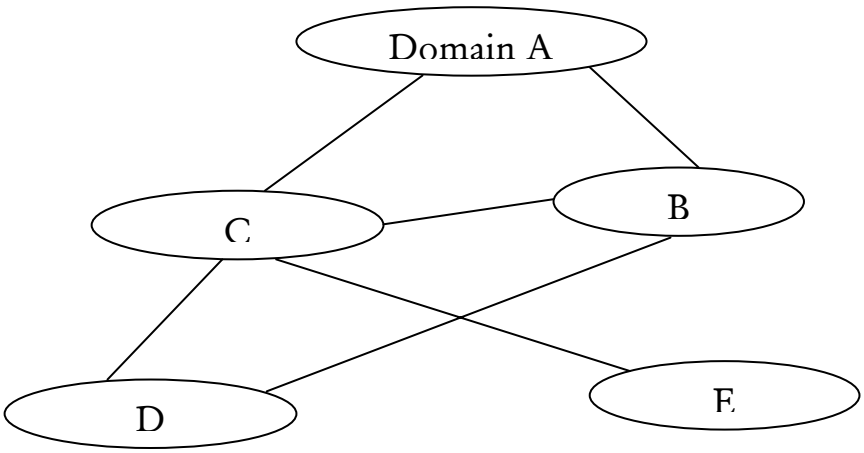
وفي هذا النظام يكون الجهاز التنفيذي واحداً تتدلى منه في شكل شجرة مفاتيح فرعية مربوطة كلها بالمفتاح الجذر (Root CA) . وهنا تبنى الثقة من أعلى إلى أدنى، ويكون المفتاح الجذر هو النقطة المحورية للثقة في كل الشهادات والمفاتيح الفرعية.



hical PKI

في هذا النظام يكون التحقق من الشهادات الفرعية الصادرة سهلاً لأن مسار التحقق واحداً من تحت إلى أعلى، أي متسلقاً من الفرع إلي فرع أكبر منه إلى أن يصل إلى الجذر مكان الثقة النهائية التامة. والأمر سهل التحقق منه لأن الشجرة واحدة وجذرها واحد.

وهذا النظام يوفر خصوصية للنطاقات المختلفة وسهولة التداول في النطاق (Domain) الواحد ولكن أيضاً يضمن سهولة المرور بين هذه النطاقات عندما تتداول المرور بين نطاقين مختلفين. ولكن عندما ينعدم جذر واحد في أعلى تصير هذه النطاقات شبكة تفقد فيها دور سيادة الاعلى، وبالتالي صعوبة التحقق من الثقة . كما سنرى.



Mesh PKI

٣,٣ بنيات المصادقة الشبكية Mesh PKI

وهنا يكون كل نطاق أو عدة نطاقات في جسم واحد، وبالتالي يوجد داخل الدولة عدة أجسام تصدر شهاداتها دون رابط بينها. أي كلهم على مستوى واحد. ولكن يتفقون على الاعتراف بشهادات بعضهم البعض ويمكنوا المتعاملين من المرور من نطاق لآخر بتأمين متساوي. وهنا مربط الفرس! التأمين المتساوي! حيث من المتوقع أن يعترف النطاق (A) بالنطاق (B) ولكن النطاق (B) ربما يتحفظ على أجزاء من نطاق (A) أو لا يثق في بعض النطاقات المربوطة بالنقاط (A). وهنا يصعب تماماً إدارة المفاتيح.

وحيث أن أثناء المرور التثبتي من نطاق لآخر يتم مراجعة السياسات التأمينية (Policy Mapping). وعلى ضوءها تتم الموافقة بالمرور أو عدمه.

وحيث هذه السياسات التأمينية تكون مختلفة أحياناً فهذا سيؤدي لفشل المصادقة بين النطاقات المختلفة وبالتالي إنقطاع نظام الثقة.

وإن كان IETF أوجدت ما يسمى بنظام المصادقة العابرة (Cross Certification) إلا أن النظم البرمجية التطبيقية العامة العاملة في البريد الإلكتروني (Email) وأدوات التصفح (Browsers) لم تعتمده. فما زال في مجال البحث النظري.

٤,٣ قوائم الثقة: Trust List

وهي عبارة عن قائمة من الشهادات موضوعة في المتصفح "Browsers " . هذه الشهادات عادة تكون معتمدة من جهة ما توزع هذا المتصفح الذي به القائمة المعتمدة من الشهادات.

Certificate Trust List (CTL) وأيضاً يمكن للمستعمل أن يمسح أو يضيف من جانبه أي عدد من الشهادات.

فشركة مايكروسوفت Microsoft من أكبر الجهات التي تعتمد هذه الطريقة في توزيع الثقة. بالمتصفح إكسبلورر "Explorer" به المئات من الشهادات ولكي تعتمد شهادتك بهذد "المتصفح" تدفع رسوم لشركة مايكروسوفت (Microsoft). ولكن كما نرى أن هذه الوسيلة لا تترك مجالاً للمستعمل للتحقق من مصدري هذه الشهادات وبالتالي بناء الثقة بالشهادة الصادرة.

من عيوب القائمة المعتمدة بواسطة المتصفح الإلكتروني (Trust List):

- من هو الذي يعتمد ويناقش احتياجات الأطراف المختلفة.
- مشكلة توسعة النظام حيث يزيد باستمرار عدد العلاقات الثنائية كلما زاد عدد المشتركين.
- هذا النظام "القائمة" لا يتيح لجسم مركزي ليفرض السياسات والإجراءات وينسق بين النطاقات المتعددة، وبالتالي التضارب وبالتالي انهيار الفكرة الاساسية للجسر بين النطاقات.
- نظام القوائم المعتمدة في المتصفح تتطلب إجراء فني ليمنع المتصفح تغيير القائمة بواسطة مستعمل جهاز الكمبيوتر.
- نظام القوائم يزيد من تكلفة الصيانة الدورية للقوائم حيث يتطلب الأمر مراجعة كل جهاز كمبيوتر على حدة.!
- مسألة صيانة القوائم عملية مستمرة حيث تدخل جهات جديدة وتحرج أخرى. وبالتالي يتطلب الأمر التدخل المستمر على كل جهاز لتعديل هذه القوائم بالمتصفح.

ولكل هذه الأسباب وأخرى نرى صعوبة هذه الطريقة لإنتشار وتبادل الثقة بين الجهات الإعتبارية.

٥,٣ الجسر Bridge CA

هذا النموذج دفعت به حكومة الولايات المتحدة الفدرالية لتحقيق هيكل المصادقة العابرة (Cross Certification) بين الهيئات الفدرالية. وفي هذه الحالة تعتمد كل هيئة سلطة المصادقة لديها ويقوم الجسر بالتمرير بين سلطات المصادقات الأخرى. وكما نرى أن الجسر ليس شهادة جذرية (Root Certificate) بل إنما هو جسر بين الشهادات المختلفة، أي هو معبر بين هذه الجزور. وعليه المطلوب من " الجسر" هو التحقق من اشتراطات وأحكام الشهادات المختلفة وضمان تكافوء المفاتيح بصورة معتمدة. فبالتالي يكون الجسر هو مصدر الثقة للمستعمل.

ورغم سهولة وبساطة الشكل والإجراء هذا من جانب المستعمل إلا أن الصعوبات التقنية لايجاد الممرات بين الشهادات المختلفة بواسطة الجسر بصعوبة بمكان ما. فالأمر يتطلب الكثير المعقد من الإجراءات من " الجسر" حتى يتمكن من التوصيل والتمرير بين سلسلة الشهادات.

وحاولت الدول الأوروبية تطبيق نظرية الجسر إلا أنهم توصلوا في آخر الأمر لصعوبة تطبيقه وكذلك صعوبة " المصادقة العابرة" "Cross Certification" واعتمدوا نظام القوائم المعتمدة Trust List.

كان هذا عرضا لما هو متاح عالمياً من نماذج للهيكلة التصديقية "Trust Models"، وكيف يحقق كل هيكل صفات معينة للبنية الاساسية للمفاتيح. وكان لا بد لنا في السودان من هذا الاستعراض حتى نتمكن من تصميم الهيكل الأمثل والذي يتماشى ويتسق مع الهياكل الشبيهة الموجودة في الدول، وكذلك الهيكل الذي يتناسب مع التركيب الثقافي والاجتماعي والنفسي في السودان .

على ضوء هذا توصلنا للملاحظات وللتوصيات التالية:-

١. موثوقية الشخصية الاعتبارية جوهرية لكل نظام التامين .

٢. حتى تتمكن نظم البنيات الاساسية للمفاتيح في مجتمع تعددي كبير يجب أن يكون المرور عبر نظم تأمين ومراجعة الثقة أتوماتيكي، يمكن الحصول على النظام، ويسهل إدارته وكذللك يمكن أن يحجم.

٣. تلاحظ من التطبيقات الشبيهة أن مراجعة التأكد من البيانات في وقت وجيز في كل مرحلة أمراً عصيباً.

٤. كل الدول تحكم سيطرتها على إدارة وتوزيع الشهادات الرقمية مباشرة عدا الولايات المتحدة التي أعطت دورا للشركات الخاصة لإدارة المفاتيح تحت هيئة الجسر الفدرالي، والتي تقوم بدور الربط بين هذه الشركات المتعددة، وبالتالي تعتبر جهة مركزية مخولة بعملية المصادقة البينية.

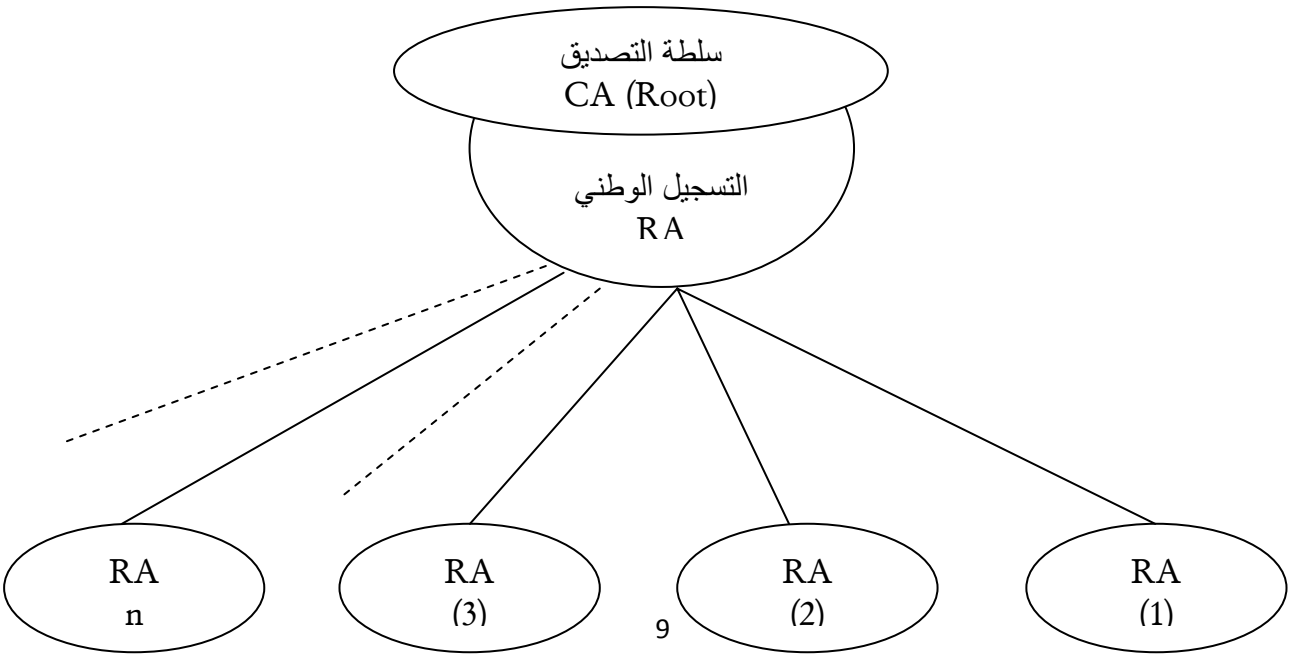
٥. أن المعضلة الأساسية في هذه الصناعة (PKI) هو صعوبة ربط أكثر من جهة في تسلسل متصل (Interoperability). وهذا الاشكال مازال يأخذ وقتاً طويلاً من البحث والدراسة لايجاد صيغة يمكن عبرها أن تتناغم وتتخاطب عدة PKI موثقة ببعضها البعض .

٦. ما زال نموذج المفتاح الجذر (Root Key) أو الهرمي المنتهي في قمته مفتاح جذري هو الأسهل تطبيقاً رغم بعض القصور المصاحب له.

٧. سياسة الشهادة الرقمية Certificate Policy: تحدد هذه السياسة مدى الثقة الممكن افتراضها من الشهادة الصادرة من السلطة. والأوجه المشروعة لاستخدامها، إلى جانب تبيانها لالتزامات سلطة التصديق تجاه الأطراف المستفيدة وحقوق المستخدمين.

٨. تصدر اللائحة التنفيذية لسياسة الشهادة الرقمية (Certification Practice Statement) والتي يستطيع المستخدم معرفة الطرق الفنية والمهنية والإجرائية المتبعة لإصدار، أو تجميد أو إلغاء الشهادة الرقمية من قبل السلطة. وأيضاً عن طريق هذه اللائحة التنفيذية يمكن للجهات الأجنبية والعالمية وسلطات المراجعة الدولية تقدير عمل ومصداقية السلطة.

٩. يمكن عمل الهيكل المقترح على النحو الآتي:-



أ- حيث يمكن أن تكون كل سلطة تسجيل Registration Authority تابعة لنطاق معين مثل الشرطة، القوات المسلحة، البنوك، الغرف التجارية، التعليم العالي، التعليم العام، ..... الخ.
ب- تصدر المفاتيح الخاصة والشهادات في سلطة المصادقة القومية وإلى حين تتمكن السلطات الفرعية من التمكن من هذه التقنية .

١٠. يبدأ في تنفيذ الهيكل أعلاه على مراحل تمتد لمدة ثلاثة أعوام.

١١. خلال تلك الفترة الانتقالية أعلاه من المتوقع أن يكون هناك كادر بشري بدأ يجيد العمل في تقنية PKI. حينها يمكن التفكير في قيام هيئات جزئية بأن تتطور إدارات التسجيل إلى إدارات فرعية لسلطة إصدار الشهادات، بدلاً من السلطة الجذر. أي بمعنى أن نبدأ في تطوير نظام الثقة من أحادي مربوط مباشرة بالجذر إلى نظام هرمي (Hierarchical).

١٢. ايضاً يكون قيام هذا النظام الهرمي على مراحل، وكلما كان هناك كادر بشري مقتدر وملم بتقنيات PKI، وأيضاً إيجاد التجانس والتناغم بين العاملين في هذه الأجهزة، وموثوقية أداءهم.

١٣. ختاماً أن مخدم إصدار الشهادات سيكون منفصلاً تماماً عضوياً ومنطقياً من الشبكة، وسيتم نقل بيانات الشهادات الصادرة بوسائط متحركة لمخدم RA الذي بدوره محمي بالطابيات القوية والقلاع الحامية.