الجمهورية العربية السورية

وزارة الاتصالات والتقانة

الهيئة الوطنية لخدمات الشبكة

الهيئة الوطنية لخدمات الشبكة
National Agency For Network Services

الرقم :

التاريخ:

معايير البطاقات الذكية السورية

النسخة الأولى

2018

هاتف: 3937078 11 963+، فاكس 3937079 11 963+، ص.ب: قدسيا-47، بريد إلكتروني
info@nans.gov.sy

ضبط الوثيقة

سجلات التغيير

التاريخ	الاسم	النسخة	الصفة
2018/6/21	علي علي	1	معاون المدير العام

المراجعات

التاريخ	الاسم	الصفة
2018/7/1	فاديا سليمان	المدير العام

1. نطاق الوثيقة:

كافة أنواع البطاقات الذكية.

وتخضع البطاقات المصرفية بالاضافة إلى ماسيرد في هذه الوثيقة إلى الضوابط والنواظم الموضوعة من قبل مصرف سورية المركزي.

2. خارج نطاق الوثيقة:

بطاقات الهوية الشخصية – جواز السفر.

3. لمحة تاريخية:

تعود تقنية البطاقات الذكية إلى سبعينيات القرن الماضي حيث كان المخترعون في الولايات المتحدة واليابان والنمسا يحاولون الحصول على براءات اختراع للبطاقات الذكية في الوقت الذي كان الفرنسيون فيه يدفعون مبالغ مالية ضخمة لدفع هذه التكنولوجيا إلى الأمام بالاستفادة من استثمارات وطنية كبيرة هدفت لتحديث البنية التحتية التكنولوجية الوطنية. ونتيجة أسباب مختلفة بقيت هذه التقنية رهينة مرحلة البحث والتطوير حتى منتصف الثمانينات حيث نمت صناعة البطاقات الذكية نمواً هائلاً ليصبح معدل الإنتاج منذ عام 1998 أكثر من مليار بطاقة.

4. مدخل إلى البطاقات الذكية:

تشبه البطاقات الذكية بطاقات الائتمان إلا أن مايميزها عنها ذكاؤها الذي تستمده من المعالج الصغري الموجود فيها مما يؤهلها لمعالجة المعلومات إضافة لقدرتها على تخزينها ويعطيها قابلية إعادة البرمجة بعد إصدارها. هذه الميزات تتيح استخدام البطاقة في التطبيقات الآنية وغير الآنية (on line and off line) كما يجعلها قابلة لاستضافة تطبيقات مختلفة لجهات مختلفة. حيث يمكن للبطاقات الذكية أن تستخدم في تطبيقات مثل الحقيبة الإلكترونية (e-purse)، وبطاقات الائتمان وبطاقات السحب، وبطاقات الهوية الشخصية والتحكم بالدخول، وفي الهواتف المحمولة، كما تستخدم لحفظ وثائق رسمية ولتخزين المعطيات ولتوقيع وثائق رقمياً لإثبات صحتها وسلامتها.

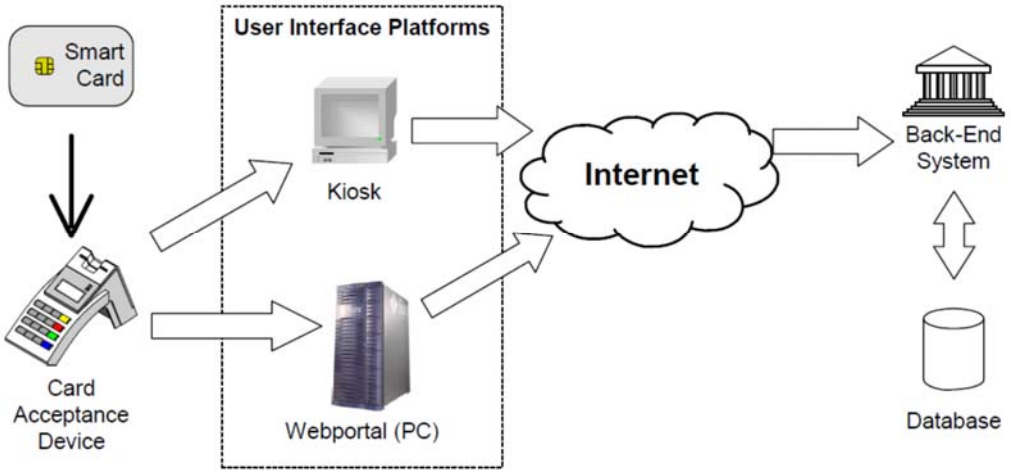
بالمقارنة مع بقية التقنيات يمكن للبطاقات الذكية أن تعيق محاولات العبث والقرصنة ويمكن أن تزود بتقنيات تشفير ووظائف تحقق من المستخدم.

لكي تكون البطاقة الذكية مفيدة يلزمنا تطبيق Application لتقديم بعض الخدمات للزبون ويلزمنا Card Acceptance Device(CAD) سواء كان مجرد قارئ بسيط يوفر تماسات فيزيائية أو طرفية مع برمجيات تسمح لها بالاتصال مع البطاقة الذكية.

تصنف CAD في ثلاثة أصناف:

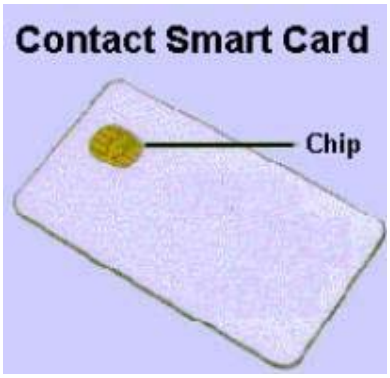
- الصنف الأول: قوارئ بسيطة،
- الصنف الثاني: لديه لوحة مفاتيح،
- الصنف الثالث: لديه شاشة إظهار ولوحة مفاتيح وهنا يكون مصطلح طرفية مرادفاً لـ CAD .

يمكن أن تتصل الـ CAD مباشرة بنظام يقدم تطبيقات خدمية أو يمكن أن تتكامل أو تتصل بمنصات واجهات تخاطبية مع المستخدم User Interface Platform مثل الأكشاك Kiosk terminal أو الحواسب الشخصية PC حيث تتصل الأكشاك عادة مع الأنظمة الخلفية Back End Systems بينما يمكن للحواسب إما أن توفر خدمات بذاتها أو يمكنها أن تكون فقط طرفية لقوارئ موصولة بها لتتصل مع الأنظمة الخلفية. ويتم الاتصال عادة بالأنظمة عبر شبكات غير آمنة مثل الإنترنت والأنظمة الهاتفية حيث تتصل هذه الأنظمة بقواعد المعطيات لإدارة المعطيات.

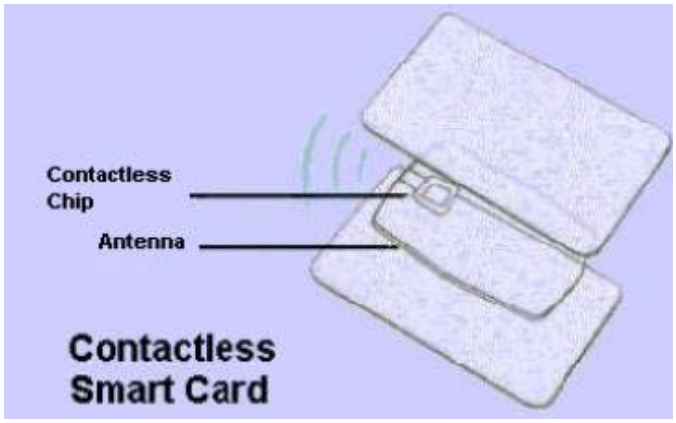


يمكن أن نصادف البطاقات الذكية بشكلين:

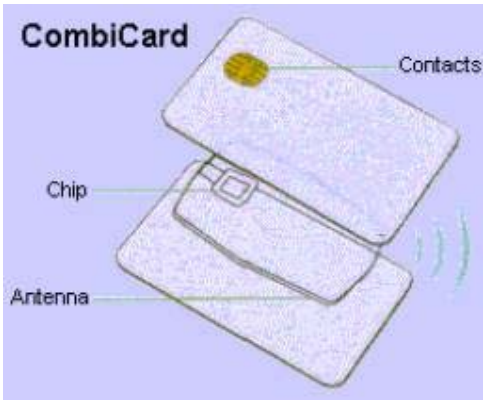
1- بطاقات تلامسية: حيث تكون البطاقة وقارئ البطاقة على تلامس فيزيائي مباشر (كما في البطاقة المصرفية).



2- بطاقات غير تلامسية: حيث يتم التفاعل بين البطاقة والقارئ عن بعد بواسطة موجات راديوية ووفقاً لنوعها يمكن أن تختلف المسافة بين القارئ والبطاقة من بضع ميليمترات إلى عدة أمتار.



3- بطاقات هجينة يمكن أن تعمل بطريقة تلامسية أو غير تلامسية.

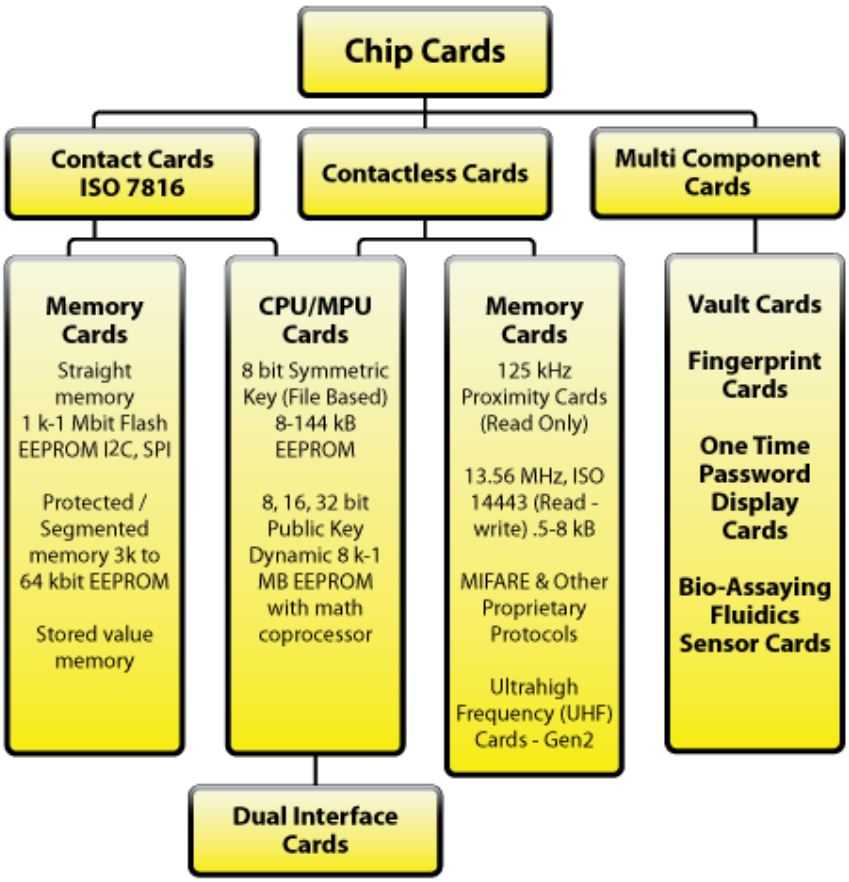


عادة نجد البطاقات التلامسية بحجم مماثل لحجم بطاقات الائتمان (باستثناء بعض البطاقات المستخدمة في الهواتف المحمولة وبعض التطبيقات الخاصة) وهذا يعرف تقنياً بالبطاقة رقم 1 (ID 1 card) .

يمكن للبطاقات غير التلامسية أن تكون بنفس حجم البطاقة الائتمانية ولكن يمكن أيضاً أن توجد بأشكال أخرى مثل سلاسل المفتاح (key fobs).

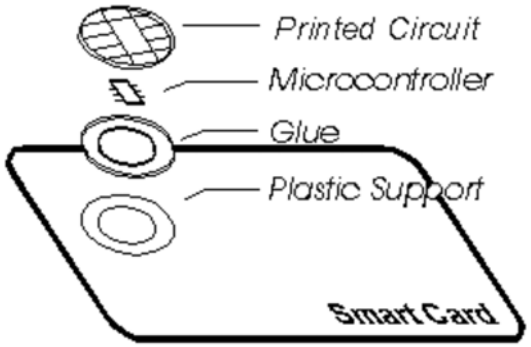
يمكن أن نجد البطاقات الذكية بأبعاد أصغر مثل البطاقات المخصصة ذات التطبيق الواحد والتي تحتوي فقط دارة متكاملة وحيدة التطبيق والوظيفة (Application Specific Integrated Circuit ASIC).

يوضح الشكل أنواع البطاقات الذكية:



5. بطاقات الذواكر Memory Cards وبطاقات المعالج Microprocessor Cards:

لا نستطيع القول عن بطاقات الذواكر أنها ذكية لأنها لاتحتوي على معالج فهي قادرة على تخزين كمية محدودة من المعلومات مثل اسم ورقم حامل البطاقة وتقوم البرمجيات الموجودة في الحاسب المضيف باسترجاع هذه المعلومات.
أما البطاقات الذكية فهي تلك التي تمتلك معالجاً وهي بدورها تقسم إلى قسمين بطاقات وحيدة التطبيق وبطاقات متعددة التطبيقات



الحاسب الموجود على البطاقة الذكية:
يتكون من الأجزاء الآتية:

- **وحدة معالجة مركزية CPU:**

أغلب البطاقات تستخدم معالجات 8-bit زهيدة الثمن، لكن هناك بطاقات بمعالجات تصل حتى 32-bit .

- **معالج التشفير Cryptographic Processor:**

وهو خياري يحسن من أداء عمليات التشفير. إن إنجاز عمليات التوقيع الرقمي على البطاقة بحد ذاتها يزيد الأمن وعندما يترافق مع توليد زوج المفاتيح على البطاقة، المفتاح الخاص سيتواجد فقط على البطاقة الذكية.

- **ذاكرة قابلة للقراءة فقط ROM:**

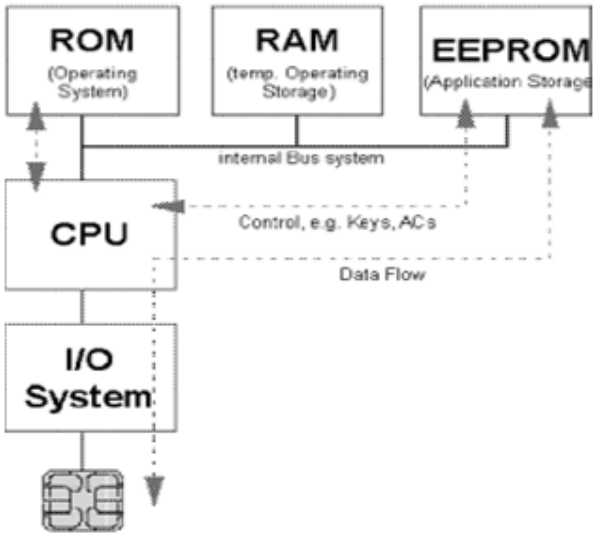
المعلومات المخزنة على الـ ROM تكتب أثناء التصنيع أو الإنتاج. وهي متشابهة في جميع الشرائح الخاصة بسلسلة ما وهي تحتوي على نظام تشغيل البطاقة.

- **ذاكرة قابلة للقراءة والبرمجة والمحي(Electrical Erasable Programmable Read Only Memory EEPROM):**

تستخدم للتخزين الدائم للمعطيات وهي تحتفظ بالمعطيات حتى في حالة انقطاع التغذية الكهربائية.

- **ذاكرة عشوائية الوصول RAM**:

وتستخدم لتشغيل البرمجيات Applets وهي لا تحتفظ بالمعطيات عند انقطاع التيار الكهربائي.



إن وجود المعالج الصغري في البطاقة الذكية يعني أنها:

- قادرة على معالجة المعلومات فضلاً عن تخزينها.
- قابلة للبرمجة وتحديث التطبيقات الموجودة عليها وإضافة تطبيقات جديدة بعد إصدارها.
- قادرة على تخزين أحجام كبيرة نسبياً من المعلومات (مقارنة مثلاً مع البطاقات ذات الشريط المغناطيسي)، وقادرة على التحكم بالوصول إلى هذه المعلومات.

الاستخدام غير الآني: Off line use

وهنا تعمل البطاقة الذكية كمخزن معطيات وهذا يقلل تكاليف البنية التحتية ويخفف العبء عن شبكة الاتصالات ويجعل الاستخدام المتنقل عملياً. وبالرغم هذا فمن الضروي اتباع استراتيجية نسخ احتياطية لضمان أن المعلومات المخزنة على البطاقة تنسجم مع المعطيات المخزنة في قواعد المعطيات المركزية.

الاستخدام الآني: On line use

وهنا تتيح البطاقة الوصول الآمن لعدد من التطبيقات الآنية وهذا يجعل إدارة المعطيات أسهل منها في تطبيقات الاستخدام غير الآني.

الاستخدام المتعدد:

وهنا تستخدم بطاقة واحدة لأغراض متعددة وهنا يمكن أن نصادف الأنواع التالية:

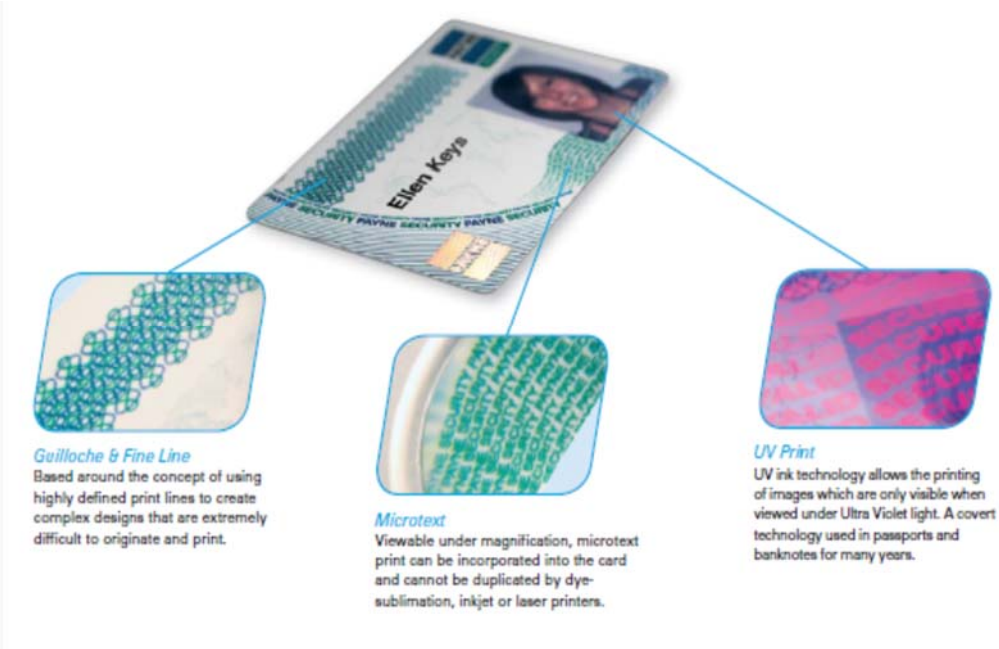
- **وظيفة واحدة واستخدام متعدد:** مثل بطاقات الدفع في مواقع مختلفة.
- **وظائف متعددة واستخدام متعدد:** وهنا يمكن للبطاقة أن تحوي عدة مجموعات معطيات كل منها يخدم غرضاً مختلفاً.
- **تطبيقات متعددة:** وهنا يمكن للبطاقة أن تحوي عدداً من التطبيقات الذكية ينجز كل منها وظيفة مختلفة. ويمكن إضافة وإزالة التطبيقات خلال دورة حياة البطاقة.

لو قامت عدة أطراف بالاتفاق على تشارك البطاقة والبنية التحتية لأدى ذلك إلى إنقاص التكلفة وزيادة المواقع التي تستخدم البطاقات الذكية. ولكن من الضروري أن تؤخذ تفاصيل التقنيات والإدارة والتشريعات والأمن بالاعتبار.

6. المتطلبات الأمنية للبطاقة الذكية:

أ. الأمن الفيزيائي للبطاقة:

يتداخل مجال تقنيات البطاقات البلاستيكية مع البطاقات الذكية ويتضمن طيفاً واسعاً من التدابير الأمنية الأخرى مثل الهولوغرام Holograms، التراكبات الأمنية Security Overlays، طباعة غيوش Guilloche Printing، طباعة مجهرية Micro-printing، طباعة متغيرة ضوئياً Optically Variable Printing الخ... وهذا مجال غني ومعقد وليس خاصاً بالبطاقات الذكية ومع ذلك فهو وثيق الصلة بالبطاقات الذكية ولاسيما عندما يكون مطلوباً ميزات أمنية قابلة للقراءة مباشرة (من قبل الإنسان).



- الهولوغرام Hologram: وهو هولوغرام ثلاثي الأبعاد يختم على بطاقات فارغة من الحجم القياسي في واحد من ثماني مواقع اختيارية ولديه تأثير مرئي حيث يتغير اللون والمظهر عند النظر إليه من زوايا مختلفة.
- الصفيحة المختومة Foil Stamped: وهنا يمكن لأي شكل أن يختم على صفيحة ذهبية أو فضية بشكل مميز وصعب النسخ والتكرار.
- أحبار فوق بنفسجية UV Inking: وهذه طريقة لإضفاء فرادة Uniqueness على البطاقة بحيث لاترى هذه الأحبار بالعين المجردة.
- الكتابة المجهرية Microtexting: وهنا تتم طباعة أحرف متناهية الصغر في موقع محدد على سطح البطاقة ولا يمكن تنفيذ هذه الطباعة بالطابعات الحرارية بسبب وجود محددات على حجم الخط.

ب. الأمن المنطقي للبطاقة:

على نقيض البطاقات ذات الشريط الممغنط، توفر اليوم البطاقات الذكية متعددة التطبيقات المتطورة خيارات واسعة من الوظائف الأمنية الممكنة حيث يمكن لكل وظيفة منها أن تمتلك قواعد تحكم بالوصول يمكن أن تكون سرية بدرجات متفاوتة مثل: PIN ، المفتاح المتناظر Symmetric Key ، القياسات الحيوية Biometrics، ...الخ.

- حماية الوصول عبر PIN (Personal Identification Number): حيث يمكن لمناطق محددة من الذاكرة بواسطة التحكم بالوصول إلى المعطيات أن تخضع لقواعد أمنية مختلفة. وبالمثل يمكن للوظائف Functions الموجودة في البطاقة بما فيها تلك الوظائف التي تتحقق باستخدام تطبيقات البطاقة التي تم تحميلها ضمن بطاقة متعددة البرمجيات أن تكون محمية بالـ PIN للمساعدة في الحفاظ على البطاقات الضائعة أو المسروقة من أية إساءة محتملة.
- التحقق من حامل البطاقة Cardholder Verification: يمكن أن تستخدم البطاقة PIN مدمج أو نموذج حيوي Biometric Template لتمنع أي استخدام خاطئ في حالة ضياع البطاقة أو سرقتها.
- التحقق من البطاقة والطرفية Card and Terminal Verification: يجب أن تتبادل البطاقة مع القارئ المصادقة لضمان أن كلاً منهما حقيقي.
- التشفير Cryptography: بما في ذلك تخزين المفتاح الخصوصي Private Key ، وتوليد المفتاح على الشريحة On-chip key generation، والتشفير المتناظر Symmetric encryption، ووظيفة أمن المفتاح العمومي Public key security functionality، وتخزين الشهادة Certificate storage، والإدارة. فالبطاقة الذكية يمكن أن تملك قوة معالجة كافية وخصوصاً إن كانت مصنعة مع معالج صغري مشارك في التشفير Cryptographic co-processor لتنفيذ مجموعة من وظائف التشفير بشكل مستقل عن المعدات الخارجية لضمان تنفيذ عدد من المهام الأمنية. هذا يتضمن وظائف متناظرة ووظائف غير متناظرة (المفتاح العمومي). على وجه الخصوص يمكن توليد التواقيع الرقمية Digital Signatures على البطاقة دون تحرير المفتاح الموقع الخصوصي private signing key للعالم الخارجي. يتحقق أمن البطاقة ومنع التزوير أو الاستنساخ أو القراءة بواسطة عدد من ميزات السلامة العالية المقاومة لمحاولات الوصول غير المصرح به. مثلاً الرموز منخفضة المستوى low-level codes أو الأرقام التسلسلية يمكن أن تكون hard-wired أو محروقة في المصنع عند صنع البطاقة الذكية وهكذا لا يمكن أن تتكرر البطاقات الذكية دون اختراق مسبك البطاقة الذكية نفسه Smartcard foundry أو عن طريق الحصول على تفاصيل تصميم شريحة أنصاف النواقل تلك المعلومات التي لا يمكن أن تفيد المخترقين إلا في حال قدرتهم على صناعة شرائح. فحتى لو تم اختراق الـ PIN الخاص بحامل البطاقة فلن يستطيعوا تكرار البطاقة أو استنساخها.

- مقاومة العبث Tamper-resistance:إن محاولات الوصول للشريحة بشكل مباشر وتجاوز الموصلات أو التماسات يمكن كشفها وتوضيحها عبر تصميم الأمن البلاستيكي و/أو الاستجابة للنشاط عبر إغلاق وظائف الشريحة Shutting down chip functions أو تصفير المعطيات Zero-ising data.
- القياسات الحيوية Biometrics : وهي طرق آلية للمصادقة على هوية شخص حي اعتماداً على خصائص حيوية فيزيولوجية أومسلكية فممكن للقياسات الحيوية أن تعتمد بصمة الاصبع، معالم الوجه، قزحية العين،الصوت، راحة اليد، شبكية العين، التوقيع. يمكن تخزين نماذج التحقق واحد لواحد الآمنة على البطاقة. ويمكن الحصول على أمن إضافي عبر إنجاز match-on-card والتي تستدرك الحاجة للتخزين المركزي لنماذج القياسات الحيوية. تملك match-on-card عدة مزايا منها المقاومة الكبيرة لمحاولة إعادة الهجوم والتقليل من الاعتماد على أداء الشبكة أو توافرها والحد من المعلومات الحساسة التي يتم تخزينها مركزياً بحيث يمكن الهجوم عليها. من ناحية أخرى وبما أن ملكية خوارزميات ونماذج القياسات الحيوية تعود لبائعين مختلفين فإن التوافق بين الحساسات والبرمجيات والبطاقات التي تعود لبائعين مختلفين يجعل اختيار بائع حلول قياسات حيوية محدد صعباً. الحل الشائع اليوم هو فقط تخزين المعطيات الحيوية الخام فقط على البطاقة الذكية مثل صور JPEG لبصمات الأصابع أو الوجوه على أساس أن عدداً كبيراً من الخوارزميات سيتم استخدامها للمعالجة المتوافقة وهذا سيزيد من متطلبات الذاكرة.
- إدارة الهوية Identity Management: يمكن تهيئة البطاقات الذكية لتكون حاوية لوثائق التعريف Identifiers ووثائق التفويض Digital Credentials بشكل معطيات خام أو بشكل شهادات المفتاح العمومي لتحقيق مزايا أمنية أكبر. يمكن أن توجد بعض المعرفات في الذاكرة حرة القراءة Free-read memory أو يمكن حفظها في ذاكرة متحكم بالوصول إليها عن طريق الحماية عبر الـ PIN الذي يضيف خصوصية وأمن.
- المفتاح العمومي PKI : تمتاز بعض البطاقات الذكية بكونها جزء لايتجزأ من البنية التحتية للمفتاح العمومي Public Key Infrastructure(PKI) والتي تدعم الآليات الأمنية مثل التشفير ورسائل المصادقة والتواقيع الرقمية. في بعض البطاقات الذكية ينجز PKI التشفير والتواقيع الرقمية عن طريق استخدامه لتقنيات المفتاح العمومي. بعض التقنيات تستخدم زوج من المفاتيح يتكون من مفتاح خاص يبقى سرياً، ومفتاح عمومي يشاع على نطاق واسع بين الجمهور. يتم توليد المفتاحين بحيث

أنه عندما يستخدم أحد المفتاحين لتحويل المعلومات إلى صيغة غير مفهومة (مشفرة) فإن الطريقة الوحيدة لإعادة المعلومات (فك التشفير) هي استخدام المفتاح الآخر. لنأخذ المثال التالي: لنفرض أن الجميع يعلم المفتاح العمومي لشخص افتراضي يدعى علي، عندها يمكن لأي شخص استخدام المفتاح العمومي العائد لعلي لتشفير بعض المعلومات وإرسالها ثانية إليه وبما أن علي وحده يعلم المفتاح الخاص به فهو الوحيد االقادر على فك التشفير لذلك فالتشفير باستخدام المفتاح العمومي للمستقبل أو المتلقي يضمن السرية. ومن جهة أخرى لو استخدم علي مفتاحه الخاص في تشفير بعض المعلومات وأرسلها إلى محمد الذي استطاع بنجاح فك التشفير باستخدام المفتاح العمومي لعلي عندها سيعرف محمد أن علي قد شفر المعلومات أو قام بالتوقيع عليها وبما أن علي الوحيد الذي يعلم المفتاح الخاص فهو الذي يستطيع تشفير معلوماته . هذا المفهوم يطلق عليه التوقيع الرقمي وهو يضمن أن المعلومات موثوقة وأنها قادمة من الجهة التي يفترض أنها قادمة منها. عادة يتم التحكم بالـ PKI عن طريق برمجيات خاصة مثل (iVEST) التي تخلق بيئة افتراضية لمناقلات آمنة. عند تلقي شخص ما بطاقته الذكية يجب عليه أن يقوم بالآتي:

- وضع قارئ البطاقة في الحاسوب.
- تنصيب برمجية التحكم الخاصة على الحاسوب.
- وضع البطاقة في القارئ.
- الدخول إلى موقع معين على الإنترنت والحصول على زوج المفاتيح الخاصة بك.

وبعد هذا ستكون البطاقة جاهزة حيث أن المفتاح الخاص والشهادة الرقمية التي تحتوي المعلومات الشخصية والمفتاح العام باتوا مخزنين على البطاقة.

تستخدم بعض البرمجيات مثل iVEST لإنجاز التشفير المعايير التقنية مثل RSA أو ESA (Advanced Encryption Standard).

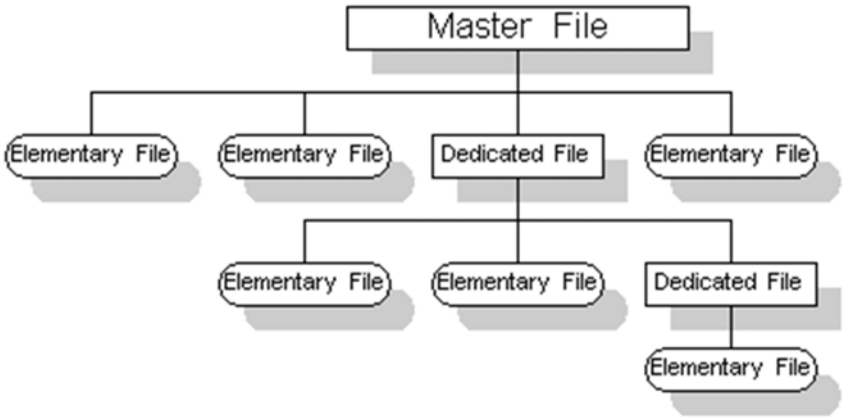
إن تقنية التوقيع الرقمي تعتمد على المعيار رقم 7 لتشفير المفتاح العام Public Key Cryptography Standard (PKCS) وبما يتوافق مع المعيار المعتمد لمنظومة التوقيع الإلكتروني في سورية X509.V3 حيث أن المناقلات الآنية ستكون محمية بواسطة Transport Layer Security (TLS) و Secure sockets layer (SSL) .

ت. أمن بروتوكول الاتصال:

البروتوكول هو مجموعة من القواعد التي تعرف كيفية القيام بعمل ما عند الاتصال بين طرفين، وبما أن البطاقة الذكية سوف تتصل مع القوارئ والحواسب والمخدمات ومواقع الويب وغيرها فإن كل اتصال يجب أن يتبع بروتوكول معين. فمثلاً عند اتصال البطاقة الذكية مع موقع ويب فإن بروتوكولات المصادقة والبروتوكولات الأخرى المتعلقة بالأمن ستكون هدفاً للهجمات، وأكثر هذه الهجمات شيوعاً: هجمات الإعادة، وهجمات التمثيل، وهجمات التداخل، وهجمات الانعكاس، وهجمات الانحراف، والهجمات المتعددة. ويتوجب على البروتوكولات المستخدمة في البطاقات الذكية أن تقاوم هذه الهجمات.

ث. أمن نظام التشغيل:

تخزن المعطيات الموجودة على البطاقة الذكية على شكل هرمية شجرية Tree hierarchy حيث يوجد ملف رئيسي Master File (MF) يعرف بالجذر Root والذي يحتوي عدة ملفات ابتدائية (EF) Elementary Files وعدة ملفات مخصصة (DF) Dedicated Files. وبشكل مشابه لأنظمة تشغيل الحواسب الشخصية تعتبر الملفات المخصصة DF والملف الرئيسي MF أدلة بينما تعتبر الملفات الابتدائية EF ملفات. يحتوي رأس الملفات MF,DF,EF على صفات attributes أمنية تشبه حقوق الوصول User Rights التي تعطى لملفات وأدلة نظام تشغيل الحواسب الشخصية. يمكن لأي تطبيق تجاوز شجرة الملف ولكنه لا يستطيع الانتقال إلى عقدة دون امتلاك الحقوق المناسبة.



توجد خمسة مستويات أساسية لحقوق الوصول لملف ما سواء كان ملف مخصص أو ملف ابتدائي يمكن ترتيبها وفق تزايد الأمن كما يلي:

1- وصول دائم للملف
2- تحقق أولي من حامل البطاقة
3- تحقق إضافي من حامل البطاقة
4- وصول بعد موافقة إدارية
5- ممنوع الوصول

تخزن معرفات الـ PIN (Personal Identification Number) في ملفات ابتدائية منفصلة حيث يتم تعطيل Block البطاقة بعد إدخال معرف الـ PIN عدة مرات متتالية ويختلف عدد مرات الإدخال الخاطئ المسموح بها من نظام تشغيل لآخر وفي حال تعطيل البطاقة يستخدم معرف PIN ليلغي التعطيل والذي يمكن أن يعطل أيضاً في حال تكرار إدخاله بشكل خاطئ.

عند تعطيل الـ PIN تتغير صفة جميع الملفات الأمنية لتتطلب تحقق أولي من حامل البطاقة وعند إلغاء التعطيل تعود الصفة الأمنية إلى الوضع العادي.

ج. أمن التطبيقات:

يسهم منتجو التطبيقات البرمجية في أمن البطاقات الذكية ومن مهامهم ضمان تشفير المعطيات بمساعدة مكتبات برمجية تستند إلى خوارزميات تشفير متقدمة.

7. المعايير العالمية لأمن البطاقات الذكية:

أ. FIPS 140 (Federal Information Processing Standards):

إن FIPS 140 هو معيار وضع من قبل المعهد الوطني للمعايير والتكنولوجيا (NIST) وهيئة أمن الاتصالات (CSE) في الحكومة الكندية ويهدف إلى:

- تنفيذ الوظائف الأمنية المعتمدة لحماية المعلومات الحساسة.
- حماية النماذج المشفرة (Cryptographic Module) من الاستخدام غير المصرح به.
- منع إفشاء محتويات النموذج المشفر.
- منع تعديلات النموذج المشفر وخوارزميات التشفير غير القابلة للكشف.
- توفير مؤشرات عن الحالة التشغيلية (Operational State) للنموذج المشفر.
- ضمان عمل النموذج المشفر بشكل صحيح عند التشغيل في إطار نمط تشغيل معتمد.

– كشف الأخطاء التالجة عند تشغيل النموذج المشفر ومنع ما قد تنتجه هذه الأخطاء من تعرض للمعطيات الحساسة والمحددات الأمنية الحرجة.

متطلبات المعيار FIPS الوظيفية:

المتطلبات الأمنية للمعيار FIPS 140 والتي تغطي التصميم الآمن والتنفيذ للنموذج المشفر هي كالآتي:

– مواصفات النموذج المشفر.
– الواجهات التخاطبية (Interfaces) والبوابات (Ports) للنموذج المشفر.
– الأدوار والمسؤوليات (مثل: المستخدم، المدير، من يقوم بالصيانة ....).
– الخدمات والمصادقة.
– نموذج الحالة المحدودة (Finite State Model).
– الأمن الفيزيائي.
– البيئة التشغيلية (Operational Environment).
– إدارة مفتاح التشفير.
– التداخل الكهرطيسي / التوافق الكهرطيسي.
– الاختبارات الذاتية.
– ضمان التصميم Design Assurance.
– التخفيف من الهجمات ذات الصلة.

وللمعيار FIPS 140 أربع مستويات أمنية للمحتويات المشفرة تتدرج من المستوى الأول الأقل أمناً إلى المستوى الرابع الأكثر أمناً.

– **المستوى الأول**: وهنا يجب استخدام خوارزمية معتمدة واحدة على الأقل أو وظيفة أمنية معتمدة واحدة على الأقل. ويتطلب أيضاً استخدام مكونات عالية الجودة. يسمح للبرمجيات والمكونات المادية أن تنفذ على نظم تشغيل غير مقيمة (Unevaluated Operating System).

– **المستوى الثاني**: يقوي المستوى الأول عن طريق إثبات العبث Tamper-Evidence . يتطلب المستوى الثاني مصادقة مستندة إلى الدور (Role Based Authentication) يتم فيها مصادقة النموذج المشفر على إذن لمشغل ذي دور محدد لإنجاز مجموعة من الخدمات.

– **المستوى الثالث**: بالإضافة إلى المستوى الثاني يتطلب هذا المستوى تدابير لمنع مهاجم ما من الوصول إلى المحددات الأمنية الحرجة للنموذج المشفر.

- **المستوى الرابع:** وهنا توفر الآليات الأمنية حماية كاملة للنموذج المشفر حيث تكشف وتصد كل المحاولات غير المرخصة للوصول المادي .الحماية مطلوبة أيضاً ضد أية تنازلات أمنية تفرضها شروط بيئية أو تقلبات خارجية في الجهد ودرجة الحرارة.

ب.المعيار CC/ISO 15408 (Common Criteria /International Standards Organization):

إن المعيار CC هو أداة لتحديد الوظائف الأمنية ومتطلبات الضمان وهو يسمح بصياغة محددات تقييم جدارة الثقة بالمنتجات والنظم المعلوماتية وقد أتى نتاج عمل مشترك بين مجموعة دول وبشكل رئيسي كندا وفرنسا وألمانيا والمملكة المتحدة والولايات المتحدة.

ت.المعيار EMVCo (Europay, MASTERCARD, Visa):

هذا المعيار مستخدم في القطاعات المصرفية وقد أنشأ عام 1999 من قبل Europay, MASTERCARD, Visa لتحسين مواصفات الدارة المتكاملة المستخدمة في بطاقات الدفع الإلكتروني.

ث.المعيار ITSO :

ويحدد مواصفات التخاطب مع البطاقات الذكية غير التلامسية Contact Less هادفاً لتأمين نقل آمن وقليل الضياع للمعلومات المتبادلة بين البطاقة والطرفية والمكاتب الخلفية Back office وقد تم تطوير هذا المعيار من قبل السلطة المشرفة على وسائل النقل ويتطلب هذا المعيار وجود جميع المفاتيح الأمنية ضمن نموذج وصول أمني Secure Access Module (SAM) يفترض وجوده في كل طرفية.

ج. مجموعة معايير ETSI European Telecommunications Standards Institute :

وهي مجموعة معايير خاصة بتطبيقات البطاقات الذكية في مجال الاتصالات ونذكر منها: ETSI TS 101 181 ، ETSI TS 102 221 ، ETSI TS 102 222، ETSI TS 102 223 ، ETSI TS 101 476 V8.3.0 (2001-12).

8. أمن منظومة البطاقات الذكية السورية:

استناداً إلى ما تقدم شرحه فإن البطاقات الذكية السورية:

- يجب أن تتمتع بما لا يقل عن ميزتين من الميزات الأمنية الفيزيائية المذكورة سابقاً، على أن يتم اختيار هذه الميزات وفقاً للتطبيقات الموجودة على البطاقة، ففي حال وجود تطبيق الهوية الشخصية أو تطبيق دفع إلكتروني لا بد من الارتقاء بعدد الميزات الأمنية الفيزيائية المتاحة على البطاقة.
- أما بالنسبة للميزات الأمنية المنطقية فلا بد من توافر PIN، ومقياس حيوي للتعرف على حامل البطاقة، وكذلك يجب اعتماد نموذج مصادقة بين البطاقة والطرفيات المتعاملة مع البطاقة.
- كما يجب استخدام تقنيات تشفير متطورة تراعي المعيار FIPS 140 وفي حال كون البطاقات غير تلامسية يجب مراعاة المعيار ITSO، وفي حال وجود تطبيقات تخص الدفع الإلكتروني يتوجب مراعاة المعيار EMV.
- تتوافق البطاقات مع السياسة الوطنية لأمن المعلومات الصادرة عن الهيئة.
- تدعم استخدام الشهادات الرقمية الصادرة عن الهيئة.

9. الاختبارات

- يجب أن تخضع البطاقات الذكية على مجموعة من الاختبارات ،هناك ثلاثة أنواع من الفحوص المطبقة بكثرة على البطاقات الذكية ضمن المعيار الفيزيائي:
  - A1 خاصيات الثني.
  - A2 خاصيات Torsion.
  - A3 الكهرباء الساكنة.
- يقدم للهيئة خطة الاختبار المطبقة على البطاقات الذكية.
- تقوم الهيئة باختبار عينة من كل نوع من أنواع البطاقات الذكية المصنعة قبل طرحها للاستثمار التجاري، على أن يتم تقديم كافة الأدوات والبرمجيات اللازمة للهيئة لفحص البطاقات المصنعة.
- يتم تكليف لجنة فنية من الهيئة لزيارة المصنع والاطلاع عن كثب على خطوط الانتاج وأدوات الاختبار للوقوف على جودة البطاقات المصنعة.

Digitally signed by علي عبد الرحمن علي
DN: c=SY, ou=معاون مدير, o=National Agency for Network Services (NANS), 0.9.2342.19200300.100.1.1=10270001790, cn=علي عبد الرحمن علي
Date: 2019.03.10 13:26:30 +02'00'

علي عبد الرحمن علي