Les défis techniques de la carte biométrique avec puce électronique:

Étude de cas en Tunisie:

Des éléments de notre vie quotidienne peuvent endommager la puce électronique:

La chose la plus simple pourrait causer la détérioration de cette puce en effet, si elle est exposée à une chaleur intense (oubliez-la dans la voiture pendant un temps chaud), ou même si elle se mouille, la puce serait endommagée et ne sera plus efficace et le problème ici n'est pas dans la partie dommageable elle-même, mais le fait que le propriétaire de la carte ne sache pas que sa carte est endommagée car il n'aura pas l'accès à sa carte. En outre, seulement Quand il va l'utiliser quand on lui dira que son identifiant n'est plus disponible et qu'il aura besoin d'un nouveau qui lui coûtera un autre 20DT.

Une entreprise étrangère pour surveiller vos données personnelles?

En Tunisie, les équipements techniques liés au suivi des ID biométriques ne sont pas disponibles. Par conséquent, une entreprise étrangère est censée prendre ce projet en charge. Forcément, elle aura accès aux données personnelles des Tunisiens et toute réglementation ou mise à jour faite dans les données sera prise en charge par l'entreprise. Concrètement, la vie privée des citoyens tunisiens sera exposée à un pays étranger et cela peut représenter un risque énorme.

Patrimoine national aux mains d'étrangers

Comme toute technologie, celle qui sera adoptée pour gérer la nouvelle carte d'identité biométrique devra être constamment mise à jour pour pallier à toute vulnérabilité qui pourrait l'affaiblir (en matière de sécurité). Ce qui rendra le pays tributaire de la société qui a vendu cette technologie. Ainsi, une dépendance sera mise en place avec une entitée non-tunisienne. Comment pouvons nous être dépendant d'organisme / entité étrangère pour gérer et sauvegarder notre patrimoine national (les données personnelles de tous les Tunisiens, vu l'obligation (instituée par ce projet de loi) de l'établissement de la carte d'identité biométrique).

Nos forces de l'ordre: sont-elles également en danger?

La mise en place d'identifiants biométriques en Tunisie pourrait poser un problème non seulement aux citoyens tunisiens mais aussi aux forces militaires. En effet, tous les militaires en Tunisie portent leurs cartes d'identité avec eux et si un individu a eu l'accès à la plate-forme des identifiants biométriques, il pourrait finalement retrouver n'importe qui et dans ce cas, des forces militaires pour des raisons criminelles, tout en sachant

que selon des événements récents, les forces militaires tunisiennes sont ciblées par des terroristes.

Non séparation des tâches: La gestion des droits d'accès

L'administrateur du projet et de la base de données dépendera du ministère de l'intérieur qui sera en même temps l'organisme de collecte, de stockage et d'accès à ces données.
Si nous prenons des cas réels et concrets, des personnes travaillant pour ce même ministère (ayant droit d'accès aux bases de données) pourraient consulter des données privées sur simple demande d'une connaissance. Des cas pareils ont déjà existé avec le leaks des informations des opérateurs téléphoniques en Tunisie (cas de Ooredoo et Tunisie telecom).
Ce qui nous mène à se demander, comment un organisme sous tutelle du Ministère de l'intérieur pourrait protéger des données personnelles contre toute intrusion?
Est-ce que l'accès à ces données serait régi par un circulaire (note interne) Sachant que cette note restera interne à l'organisme et ne sera publié ni disponible au public.

Vulnérabilité et désuétude de la technologie

Toute technologie sera un jour désuète et présentera des vulnérabilités quant à sa sécurité. La technologie change aussi avec les nouvelles études et recherches en développement.
La Tunisie restera tributaire de ce fournisseur pour les mises à jour et les interventions techniques. Pour le moment, le gouvernement n'a pas formé des centres en recherche et développement pour pallier à ces risques et développer un service d'assistance technique.

Algorithme et technique de chiffrement

Tout chiffrements stipulent l'utilisation d'un algorithme suffisamment complexe pour déjouer les risques de piratages et intrusions criminelles.
Seulement, avec le développement technologiques et les nouvelles méthodes, tout algorithme sera un jour vulnérable.
Si l'etat consent à dépenser 35 milliards de dinars en 2017 pour une technologie répondant aux normes actuelles de sécurité, combien de temps sera-t-elle valable?
Faudrait-il changer de technologie pour pallier à cette défaillance?

Étude de cas au Maroc:

Les données à caractère personnel sont exposées aux pirates informatiques:

Dans le cas où quelqu'un aurait besoin d'une copie de son certificat de naissance, il peut le demander en ligne, mais les systèmes électroniques par lesquels vous obtenez votre certificat de naissance sont insécurisés et vulnérables aux pirates qui pourraient facilement entrer dans le système et utiliser vos informations personnelles contre Vous (fraude, chantage ...).

De plus, si une simple erreur a été faite dans l'entrée des données personnelles de quelqu'un dans le système, par exemple une erreur sur le type de sang (au lieu de B négatif, ils ont un A négatif), les conséquences seraient fatales car la personne risque de perdre sa vie.

Étude des cas en Algérie:

Des failles techniques pourraient provoquer des fuites de données:

En 2016 l'Algérie s'est dotée d'une carte d'identité biométrique et d'un passeport biométrique afin de (officiellement) lutter contre l'usurpation d'identité et la falsification des documents officiels. Le problème ici se trouve dans la centralisation de la base de données, qui pourrait éventuellement être sujet à des abus par les autorités ou être attaquée par des tierces personnes comme des hackers. De plus, d'éventuelles faiblesses dans la technologie développée et dans la sécurité des infrastructures pourrait provoquer des fuites de ces données. Ces données sont d'ailleurs stockées non pas en Algérie comme le voudrait la loi, mais dans d'autres pays comme la France, les Pays-bas ou l'Allemagne. Il est important de noter que la carte nationale d'identité algérienne n'est pas seulement développée par Gemalto, mais aussi par Giesecke et Devrient (GND), ce qui veut dire qu'il existe plusieurs ramifications de sécurité entre les compagnies. Cette situation accroît alors les risques d'être sujet à des attaques de cyber-criminelles.

Étude de cas: Nigeria

Manque de centres d'inscriptions:

Afin d'adopter la carte d'identité biométrique au Nigeria, les candidats doivent se rendre dans un centre d'inscription afin qu'ils puissent avoir leurs données biométriques stockées et vérifiées. Mais les centres dans les régions rurales ne disposent une connexion internet limitée et ne possèdent pas les équipements nécessaires pour terminer les procedures necessaires.

Ls risques d'emprisonnement :

Les données recueillies sur les individus pourraient en fait impliquer des orientations sexuelles / maladies sexuellement transmissibles, ce qui est une question sensible surtout pour les pays musulmans. Dans le cas où le pays qui adopte l'identité biométrique manque de protection des données, les individus pourraient même avoir un risque d'être emprisonnés en raison d'informations sensibles qui devraient être purement privées en premier lieu.

Pour avoir plus d'informations contactez
Emna Sayadi |Communication Trainee | emna@accessnow.org +216 56 125 568
Islam Khoufi | Regional Operations Manager | islam@accessnow.org +216 98 403 327

Vous pouvez visiter notre site web
www.accessnow.org