# Encadrement des prestataires de sécurité : retour d'expérience

Olivier Dembour <Olivier.Dembour@arjel.fr>
Responsable du suivi des certifications techniques

# Plan

- Rôle de l'ARJEL ;
- prestations imposées ;
  prestataires de conseil ;
- les certificateurs ;
  - critères de choix,
  - nos besoins vis à vis des rapports,
  - profil des certificateurs ;
- bilan des certifications ;
- assurance qualité ?
- premiers résultats ;
- conclusion.

# Rôle de l'ARJEL (1)

- Objectif : régulation du marché des jeux en ligne
  - Loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne
- d'un point de vue technique :
  - délivrance, par l'ARJEL :
    - d'agréments (PS, PH et JC), en fonction d'un cahier des charges s'appuyant sur un dossier d'exigences techniques (DET) et ses annexes (ANNEXE au DET) ;
    - d'homologations logicielles, portant sur les logiciels de jeu et leurs évolutions ;
  - encadrement, par l'ARJEL, de prestations de certification, effectuées par des organismes certificateurs agréés ;
  - réalisation, par l'ARJEL, d'audits collaboratifs, consistant en une analyse en profondeur des plates-formes techniques et des logiciels de jeu.

# Rôle de l'ARJEL (2)

- Les opérateurs sont donc aidés / contrôlés :
  - par les sociétés de conseil :
    - audits initiaux, permettant de constituer la demande d'agrément,
    - homologations des logiciels de jeu et de leurs évolutions,
    - besoins propres de l'opérateur, *i.e.* non liés au contexte règlementaire ;
  - par les organismes certificateurs :
    - certification unique à 6 mois du composant frontal,
    - certification annuelle initiale,
    - certifications annuelles ;
  - par l'ARJEL :
    - entretiens collaboratifs, effectués chaque année,
    - audits collaboratifs (l'objectif n'est pas de sanctionner), effectués ponctuellement ;
  - remarque : le règlement d'inscription à la liste des certificateurs impose, afin de prévenir les conflits d'intérêts, une séparation entre les missions de conseil et de certification : une durée minimale de 18 mois doit donc séparer une certification d'une prestation de conseil (audits initiaux inclus).

# Les prestations imposées (1)

- Audit initial de la plate-forme :
  - élément constitutif du dossier de demande d'agrément ;
  - périmètre :
    - audit de configuration de la plate-forme de jeu,
    - test d'intrusion externe de la plate-forme de jeu ;
- homologation du logiciel de jeu :
  - initiale : élément constitutif du dossier de demande d'agrément ;
  - prestation exigée pour le logiciel de jeu et ses évolutions, préalable à sa mise en production :
    - nouveau logiciel (ex : changement de réseau, pour le poker en ligne),
    - nouveau support (iPad, Android, etc.),
    - → plus généralement : toute évolution ayant un impact sur la sécurité du logiciel ;
  - périmètre :
    - vérification du respect des règles de jeu,
    - audit du générateur de nombres aléatoires (JC),
    - audit intrusif du logiciel de jeu (client / serveur) ;
- l'obtention d'un agrément et l'homologation d'un logiciel de jeu relèvent de décisions du collège de l'ARJEL :
  - l'audit initial et les homologations logicielles peuvent être réalisés par toute société spécialisée en sécurité : l'instruction des dossiers est effectuée par les services techniques ARJEL,
  - ces prestations sont susceptibles de présenter des niveaux d'analyse et de qualité variables, car sont réalisées par des prestataires a priori méconnaissants du niveau d'exigences attendu par l'ARJEL.

# Les prestations imposées (2)

- Certifications :
  - effectuées par les organismes certificateurs, dont la liste est établie par l'ARJEL :
    - http://www.arjel.fr/-Organismes-certificateurs-.html
  - certification unique à 6 mois du composant frontal :
    - périmètre: frontal (capteur + coffre), ainsi que sa plateforme d'hébergement :
      - audit de conformité, consistant en la vérification du respect des exigences du DET et de son annexe,
      - audit applicatif intrusif du capteur, selon l'état de l'art,
      - audit de configuration de l'infrastructure d'hébergement (logique & physique), selon l'état de l'art ;
  - certifications annuelles :
    - périmètre: intégralité de la plate-forme de jeu,
      - excepté le logiciel de jeu (jusqu'à adoption du DET 1.2)
      - audit de conformité, consistant en la vérification du respect des exigences du DET et de son annexe,
      - audit intrusif, selon l'état de l'art,
      - audit de configuration de l'infrastructure d'hébergement (logique & physique), selon l'état de l'art ;
    - le composant frontal est exclu, lors de la certification annuelle initiale, du périmètre des analyses.

# Les prestations imposées (2)

- Au final, le panel de compétences demandées est relativement large, mais classique :
  - audit de conformité ARJEL ;
  - audit intrusif :
    - test intrusif couplé à (suivant le composant) :
      - un audit de code,
      - un audit de configuration et/ou applicatif ;
  - tests intrusifs externes / internes ;
  - analyse d'architecture ;
  - audit de serveurs (système et applicatif) ;
  - audit des équipements de routage / filtrage.

# Prestations de conseil (1)

- Certaines prestations ne sont donc pas encadrées directement par l'ARJEL... :
  - homologations, initiales ou non,
  - prestations d'audit constituant la demande d'agrément ;
- … et ne répondent, parfois, absolument pas au niveau d'analyse et de qualité attendu :
  - ex : rapport d'audit de code, en vue d'une homologation, se résumant à une simple note de synthèse et affirmant, sans aucune démonstration d'analyse technique, qu'un logiciel de jeu est exempt de vulnérabilités et est donc conforme* *[sic]* aux exigences de l'ARJEL ;
    - demande de complément d'information par l'ARJEL dont résulte la fourniture, au format papier, de 3 exemplaires de 700 pages comportant un listing complet des noms des fichiers source et de leurs empreintes MD5 ...
  - ex : rapport présentant des vulnérabilités qui n'existent pas :
    - absence de désallocation mémoire considérée comme une vulnérabilité permettant l'exécution de code à distance,
    - nécessité de masquer l'entête « Date: » des serveurs Web,
    - copier/coller d'anciens rapports, avec des analyses de composants inexistants (d'un autre client !) sur la plate-forme auditée...

* l'homologation est une décision du collège de l'ARJEL, et non du prestataire de services

# Prestations de conseil (2)

- Face à des rapports inadaptés, nécessité de réagir de façon pragmatique :
  - souvent, forte contrainte de temps :
    - lors de la demande d'agrément, la durée d'instruction est contrainte par des délais réglementaires, avant qu'un refus ne soit prononcé,
    - urgence potentielle de la mise en production de la version logicielle visant une homologation (correction de bugs),
    - urgence liée à l'actualité de l'opérateur (lancement d'une application spécifique à un tournoi sportif) ;
  - volonté de ne pas pénaliser l'opérateur, face à un défaut du prestataire (et pour une prestation dont il assume la charge financièrement), tout en ne transigeant par sur le niveau de sécurité ;
    - demande de compléments d'informations (traces, analyses complémentaires, etc.), afin d'obtenir un niveau d'analyse acceptable,
    - demande d'une nouvelle prestation :
      - changement de profils éventuel, voire un changement complet de prestataire, en dernier recours ;
  - remarque : des doutes sur le niveau d'analyse d'une prestation peuvent motiver la réalisation d'un audit technique par les services de l'ARJEL.

# Certifications : choix des certificateurs (1)

- Le dossier de candidature à l'inscription à la liste des certificateurs est :
  - instruit par les services techniques de l'ARJEL,
  - soumis au Collège de l'ARJEL ;
- règlement voté par la décision n°2010-065 du Collège de l'ARJEL :
  - http://www.arjel.fr/IMG/pdf/2010-065.pdf
  - publié en octobre 2010, en vue des premières certifications uniques à 6 mois du composant frontal, prévues en décembre 2010,
  - remarque : le « référentiel d'exigences pour la labellisation des prestataires d'audit SSI » de l'ANSSI, dans le cadre du RGS, n'était pas encore publié à cette période ;
- le demandeur est évalué sur ses compétences en termes d'analyses :
  - technique,
  - juridique,
  - financière.

# Certifications : choix des certificateurs (2)

- pour le volet technique, dossier technique composé des éléments suivants :
  - CV du personnel ;
  - des rapports d'analyse « type », décorrélés du périmètre technique des jeux en ligne et du référentiel d'exigences de l'ARJEL : audits de code, tests intrusifs et audit de configuration ;
  - premier filtre, permettant de ne retenir que les sociétés qui présentent une réelle expertise et expérience dans ces domaines d'analyse ;
    - difficulté d'évaluer de manière plus approfondie les compétences et connaissances des candidats :
      - une prestation « test » ne serait pas envisageable dans le processus d'inscription à la liste des organismes certificateurs ;
- disposant de compétences techniques internes à l'ARJEL, le choix a été fait de :
  - conserver une politique d'inscription sur la liste basée sur des exigences de premier niveau, pour le volet technique ;
  - viser un encadrement permanent et strict des prestations de certification, afin d'aboutir – à terme – à des prestations équitables (au niveau des décisions) et homogènes (en termes de qualité d'expertise).

# Nos besoins vis à vis des rapports (1)

- Un rapport de certification doit :
  - attester de la conformité et du niveau de sécurité de la plate-forme de jeu ;
  - présenter des niveaux d'analyse homogènes ;
  - proposer des conclusions/décisions équitables entre les différents opérateurs
    - indifféremment de l'organisme chargé de la certification ;
- → fort besoin d'encadrement, par l'ARJEL, des prestations effectuées par les certificateurs, afin d'assurer :
  - la pertinence du périmètre et des analyses ;
  - l'égalité de traitement entre les opérateurs, par l'homogénéisation des décisions :
    - un certificateur n'a pas la connaissance ou l'historique de toutes les décisions prises dans le cadre des certifications ;
    - une non-conformité rédhibitoire doit entraîner un refus de certification pour l'ensemble des opérateurs concernés :
      - ex, pour l'année 2011, l'absence de mise en coupure d'un capteur et la présence d'une vulnérabilité exploitable à distance ont constitué des motifs de non certification. Le défaut d'homologation des évolutions des logiciels de jeu n'a pas été retenu – mais il l'est en 2012 ;

# Nos besoins vis à vis des rapports (2)

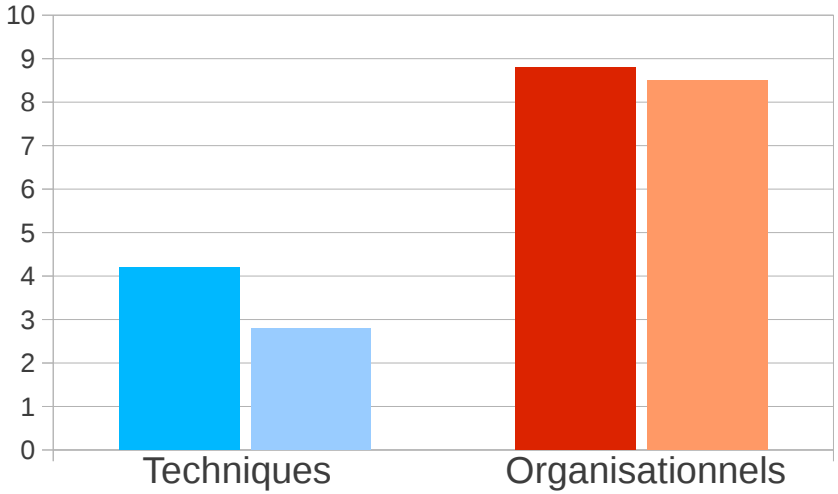
- Équité nécessaire vis à vis des opérateurs, et des certificateurs ;
- l'opérateur n'a pas forcément une équipe d'experts en sécurité :
  - les préconisations doivent être pertinentes et réalistes ;
  - l'objectif n'est pas de proposer plus de préconisations que la concurrence :
    - augmentation du risque d'erreur,
    - perte de pertinence,
    - doute sur le niveau d'expertise ;
- Au final, besoin d'une prestation à haute valeur ajoutée.

# Relation CV / qualité des livrables

- Profils consultants / experts technique relativement semblables (environ 200 profils ):
  - expérience de 1 à 10 ans,
  - moyenne générale à 3 ans ;
- certains signes peuvent alerter (faux positifs possibles) :
  - CV flous :
    - formation absente,
    - chronologie inexistante (nombre réel d'années d'expérience ?),
    - compétences non précisées (uniquement des expériences et références de clients),
    - références rarement vérifiables publiquement : articles publiés, conférences ou d'outils publiés, etc.
    - profils linkedin/viadeo souvent plus précis !
  - trop de mots clés antinomiques, pour un profil donné :
    - gestion de risques, ISO27001, expertise technique ;
- l'âge n'est pas forcément un critère déterminant :
  - composition de l'équipe primordiale,
    - l'encadrement (chef de projet, référent technique, validation des livrables …) est parfois la solution.
- importance de la politique commerciale de la société :
  - prestations médiocres réalisées, dans leur domaine, par des experts reconnus.

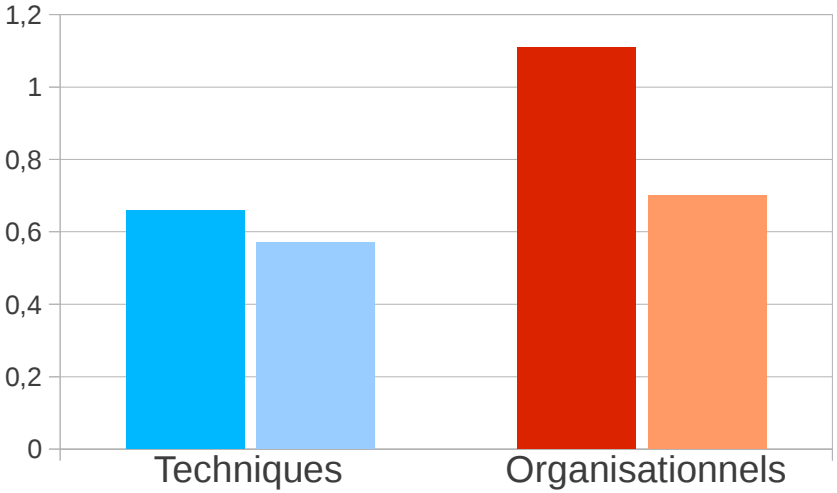
# Profils des certificateurs ARJEL (2011)

## Années d'expérience, par profil :




- profils organisationnels plus expérimentés que les profils techniques
- profils techniques :
  - dossiers de candidature : > 4 ans d'expérience ;
  - actifs : < 3 ans.
  - → des profils non présentés dans le dossier, et peu expérimentés, ont été introduits ;
  - → première tendance : l'expérience moyenne semble aller en diminuant et la taille des équipes en augmentant. Diminution légère de l'expérience due à l'introduction de nouveaux profils ;
- profils organisationnels : environ 9 ans d'expérience.

## Nombre de certifications, par profil :

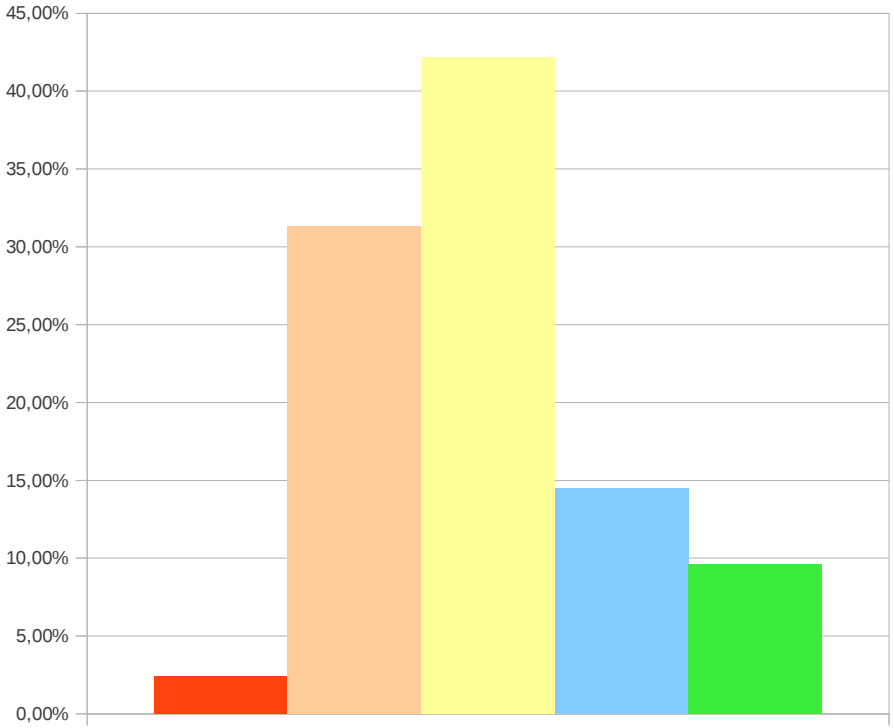



- profils organisationnels plus certifiés que les profils techniques
- profils techniques :
  - dossiers de candidature & actifs :
    - environ 0.6 certification par individu,
    - … mais seulement 20 % des individus actifs sont certifiés !
  - certifications principales : ISO (2700*), SANS, CISSP/CISA ;
- profils organisationnels :
  - 0.7 certification par individu, avec 46 % des individus certifiés ;
  - certifications principales : ISO (2700*), QSA ;
  - → les profils organisationnels affectés aux certifications ARJEL sont moins certifiés que les profils présentés : les prestations ARJEL étant peu organisationnelles, et non orientée ISO 2700*, les compétences sont donc finalement plutôt celles d'un chef de projet.

# Profils des certificateurs ARJEL (2011)

## Niveau des livrables

- Évaluation du niveau global des livrables reçus :
  - échelle entre 1 (très insuffisant) et 5 (très bon) ;
  - critères d'évaluation portant sur la qualité générale (pertinence et compréhension du périmètre, profondeur des analyses) des livrables, aussi bien que sur le nombre d'échanges avec l'ARJEL et le coût induit par le suivi du certificateur :
    - ex : un rapport correct obtenu après 5 itérations et 3 mois de délai n'obtient pas une note moyenne
  - répartition des évaluations des livrables :



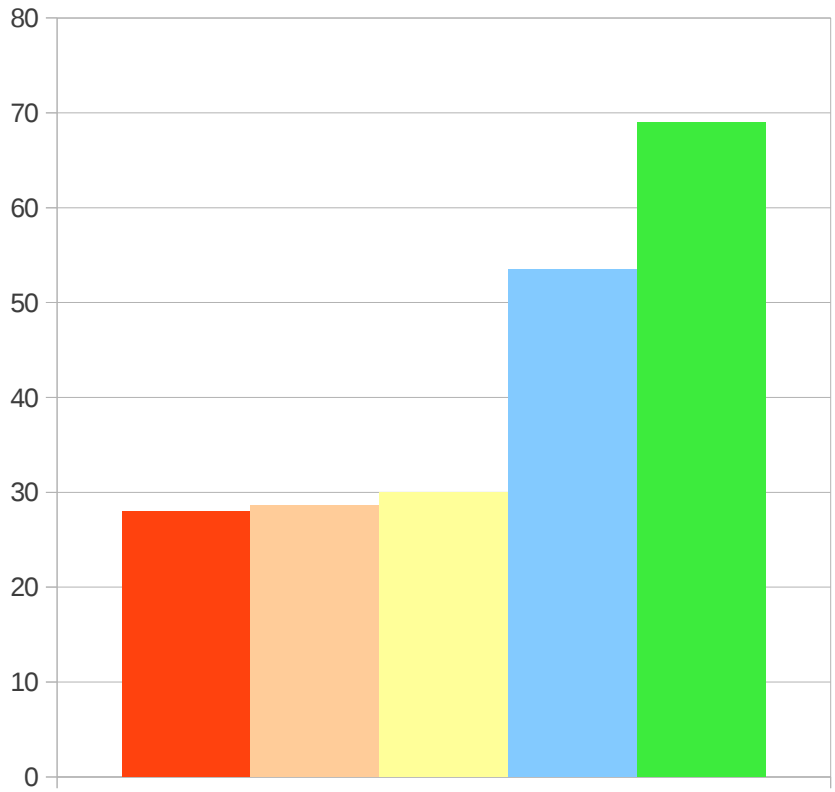

- 2/3 des prestations ont un niveau de qualité correct, bon ou très bon ;
  - 10 % des prestations ont un très bon niveau, et correspondent à :
    - pour l'une d'elle, une prestation totalement refaite après une prestation jugée insuffisante ;
    - une prestation réalisée sur une plate-forme en marque blanche, au profit de plusieurs opérateurs ;
- 1/3 des prestations ont un niveau de qualité jugé insuffisant ou très insuffisant :

→ en général, il s'agit de prestations dont le rendu est correct mais après de nombreux retours effectués aux organismes certificateur.

# Profils des certificateurs ARJEL (2011)

## Corrélation évaluation/charge déclarée

- Corrélation avec la charge déclarée (j.h) :
  - … et non les jours facturés ;
  - estimation donnée par agrément :
    - information déclarative,
    - forte mutualisation :
      - intra-opérateur (multi-agréments),
      - inter-opérateurs (marques blanches),
    - pas de distinction entre :
      - certification unique à 6 mois,
      - certification annuelle initiale,
      - → remarque : pas de prise en compte des premières certifications annuelles (2012),

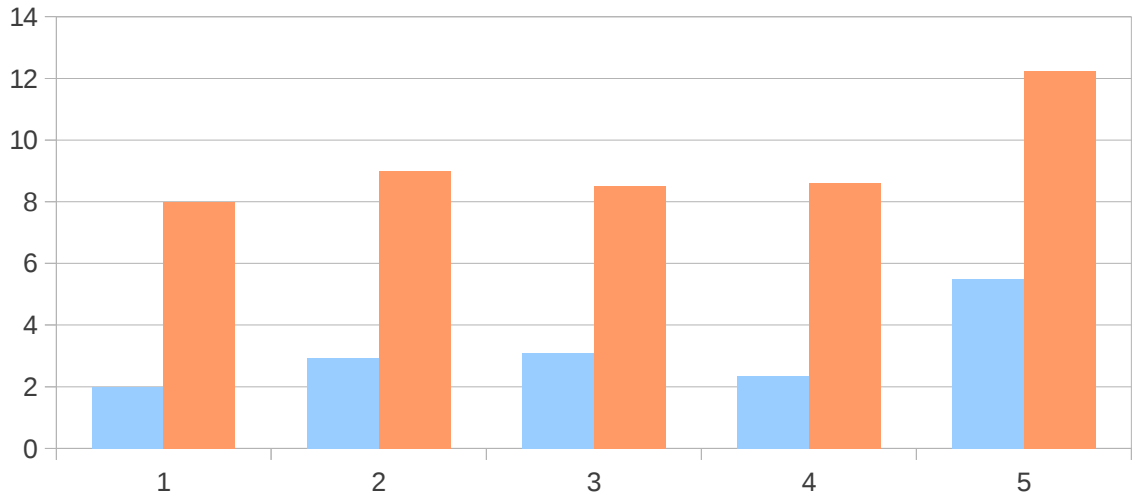



    - moyenne de 36 j.h par agrément
  - → charge en augmentation pour les certifications annuelles.

# Profils des certificateurs ARJEL (2011)

## Corrélation évaluation/paramètres divers

- Années d'expérience des profils techniques/organisationnels, par niveau d'évaluation :




- en termes de certification :
  - profils organisationnels :
    - 50 % des profils du groupe 5 sont certifiés QSA (aucune certification ISO 2700*),
    - 50 % des profils du groupe 1 sont certifiés ISO 2700* (aucune certification QSA) ;
  - profils techniques :
    - 25 % des profils du groupe 5 sont certifiés CISSP,
    - aucun profil du groupe 1 n'est certifié ;
- remarques :
  - l'intégralité des profils du groupe 5 sont issus d'une formation bac+5 (école d'ingénieurs, ou assimilé) ;
  - la majorité des profils techniques du groupe 1 sont issus de cursus universitaires courts (bac+2 ou bac+4), dans des domaines non liés à l'informatique et à la sécurité ;
  - le profil moyen est issu d'une formation bac+5 (ingénieur à 56 %, universitaire à 44 %), éventuellement complété par un mastère (11%).

# Bilan des certifications
## retour des certifications 6 mois / 1 an (2010 / 2011)

- Premières prestations très hétérogènes entre les différents certificateurs :
  - concernant le périmètre des analyses :
    - qualification : certains équipements ou fonctionnalités d'applications – critiques – ont découverts par l'ARJEL lors des (premiers) entretiens collaboratifs ;
    - l'opérateur ou un sous-traitant a refusé l'accès à sa plate-forme, ou met à disposition le code source de son application dans des conditions inadaptées à un audit technique (ex : via RDP) :
      - première exigence du référentiel de conformité,
      - … que le certificateur a des scrupules à faire jouer face à son client ;
  - concernant la qualité des analyses et des livrables :
    - rapports ne fournissant aucune trace technique ;
    - analyses contredisant les traces techniques présentées dans la même page du rapport ;
    - vulnérabilités sans aucune conséquence sérieuse ;
    - conclusions techniquement fausses ;
  - concernant la charge et la facturation des prestations :
    - très fortes disparités constatées...
    - … mais une politique commerciale qui relève de la stratégie du certificateur.

# Bilan des certifications

## retour des certifications 6 mois / 1 an (2010 / 2011)

- Forte disparité des coûts liés à la certification ;
  - cependant, un faible coût n'est pas synonyme de faible qualité,
    - tout comme un coût élevé n'est pas non plus synonyme de bonne qualité ;
- comment expliquer une telle différence de prix ?
  - incompréhension des attentes de l'ARJEL ?
  - tentative d'offrir à moindre coût des prestations de faible qualité ?
  - stratégie commerciale
    - afin de capter des opérateurs en vue des certifications récurrentes à venir, et de pérenniser l'activité de certification
- risques/conséquences immédiates :
  - retours négatifs de certains organismes certificateurs :
    - questionnement sur la stratégie à adopter :
      - révision des prix à la baisse,
      - adaptation du niveau de qualité des prestations,
    - mise en sommeil de l'activité de certification :
      - repli vers les activités de conseil...
      - … indirectement soumises au même niveau d'exigences, lorsqu'elles sont en rapport avec l'ARJEL !
  - risque que les opérateurs s'orientent vers le ou les certificateurs les moins-disants :
    - certification pour la certification ?
  - risque d'une production de livrables sans plus-value, et déconnectés de la réalité technique.

# Assurance qualité
## retour des certifications 6 mois / 1 an (2010 / 2011)

- Comment homogénéiser la qualité des prestations ?
  - pas de volonté d'interférer dans la stratégie commerciale des certificateurs :
    - contrairement à une CSPN, le nombre de jours dédiés à une analyse n'est pas fixé ;
  - des intérêts difficilement conciliables :
    - une qualité élevée des livrables attendue par l'ARJEL,
    - une réduction des coûts souhaitée par les opérateurs,
    - une amélioration de la rentabilité des prestations souhaitée par les certificateurs ;
- Solution :
  - analyse approfondie, par l'ARJEL, de l'ensemble des rapports livrés par les certificateurs :
    - analyse approfondie initiée après la vague de certifications de l'été 2011 ;
  - révision à la hausse le niveau de détails de la méthodologie et du contenu des livrables :
  - → « norme ARJEL » (Annexe DET 1.2), portée à la connaissance des certificateurs et des opérateurs :
    - http://www.arjel.fr/IMG/pdf/annexe.pdf
  - réalisation, par l'ARJEL, d'analyses techniques en profondeur des systèmes d'information des opérateurs
  - → finalement, utilisation des leviers juridiques prévus par le règlement d'inscription, afin de remédier aux insuffisances répétées : suspension voire retrait de l'inscription à la liste des certificateurs.

# Assurance qualité
## retour des certifications 6 mois / 1 an (2010 / 2011)

- Pourquoi une telle différence de qualité au final ?
- très difficile à évaluer …
- … quelques pistes :
  - profil des consultants :
    - quelques (très rares) erreurs de casting,
    - certaines sociétés privilégient des profils d'experts :
      - pas adaptés à tous les types de missions, (ex : audit de code vs. audit de configuration) ;
  - absence de vision globale,
    - manque de recul ou d'expérience technique :
      - certificateur capable d'auditer le système Linux d'un serveur syslog derrière n niveaux de filtrage réseau, mais qui omet un back-office métier accessible depuis l'internet ;
    - manque général de recul sur les aspects métiers :
      - ne pas remarquer qu'un pari peut être posé alors que la rencontre est terminée,
      - exercice difficile …
  - un niveau d'exigence inhabituel ?
    - mais doit-on se contenter, en 2012, de vulnérabilités sur l'utilisation du protocole SSLv2, sur la méthode TRACE, sur les cookies non « secure » et « httponly », et sur les empreintes de mots de passe MD5 (« à passer en SHA256 parce que MD5 est vulnérable ») ?

# Premiers résultats : côté opérateurs

- Les premiers audits et certifications portent leurs fruits :
  - amélioration sensible du niveau de sécurité ;
    - attitude plus pro-active des opérateurs face aux problèmes de sécurité ;
    - amélioration du niveau de maturité des opérateurs :
      - au niveau des plates-formes techniques, intégration notable des procédures de gestion de correctifs,
      - au niveau logiciel, intégration du processus d'homologation aux cycles de développement ;
  - conformité technique progressivement acquises sur l'ensemble des exigences :
    - en priorité :
      - respect des exigences règlementaires,
      - correction des vulnérabilités exploitables à distance,
    - à plus long terme :
      - fourniture et respect d'un plan d'action,
      - prestations et suivi qui s'inscrivent dans la durée.

# Premiers résultats : côté certificateurs

- Les premiers résultats sont également encourageants :
  - certains organismes, dont les livrables étaient perfectibles, semblent avoir arrêté la certification ;
    - malheureusement, il en est de même pour certains organismes ayant un bon niveau de production ;
  - certains ont notablement amélioré la qualité de leur production :
    - il ne s'agissait donc que d'un problème de méthodologie ;
  - → les certifications annuelles 2012 sont plus exhaustives, et révèlent plus de vulnérabilités ;

- mais cela amène à un constat inquiétant :
  - le niveau de détail exigé a parfois étonné les certificateurs :
    - cette expertise n'était généralement pas demandée par les clients ;
  - la remontée de nouvelles vulnérabilités, sur des plates-formes auditées à de multiples reprises, a elle-même inquiété certains opérateurs, s'interrogeant sur la pertinence des audits jusque-là réalisés.

# Conclusion

- Questions ouvertes :
  - d'une manière générale beaucoup d'audits (de complaisance?), sont-ils effectués par souci de conformité et non de sécurité ?
    - analyses peu poussées, peu ou pas de vulnérabilités sérieuses remontées ;
  - doit-on s'inquiéter du niveau d'expertise et d'encadrement actuel des prestataires ?
    - pas d'envie de découvrir les problèmes ?
    - pas l'expertise côté client pour évaluer la qualité des prestations ?
  - manque-t-il une véritable expertise technique aux clients de ces prestations (RSSI en première ligne) ?

# Questions ?