CyberBatiment Documentation

Release 1.0.3

ufrimag

Feb 04, 2019

Contents

Ce site regroupe l'ensemble des comptes rendus de réunion ayant eu lieu jusqu'à présent dans le cadre du projet iAccess. Ce projet concerne la sécurité de sites comme des usines, des lieux de cultes, des hopitaux, des sites sportifs, des complexes commerciaux, etc. L'objectif du projet consiste à développer le logiciel iAccess dans le cadre d'un consortium mettant en oeuvre différentes parties prenantes au sein de différentes organisations (à ce jour, IMAG, Batemis, Bissis et Competis).

CHAPTER 1

Comptes rendus de réunions

1.1 CR001 Réunion de lancement de iAccess

Date 02-01 08h-10h d

Type Réunion

Lieu Grenoble-AccessIT

PartiesPrenantes ABI, JDR, KWG, MPA, PSO, TNA, ZSH

Organisateur ABI

Rapporteur KWG

Presents ABI, JDR, KWG, MPA, PSO, TNA, ZSH

Objectifs Présentation des parties prenantes, grands objectifs

Attention: Ce compte rendu est un document de travail et n'est pas contractuel.

1. En ce début de projet, les parties prenantes sont les suivantes :
2. • Ahmed BLASI (ABI) – IM2AG, Grenoble
3. • Jean-Claude DUFOUR (JDR) - AccessIT, Grenoble
4. • Ken WONG (KWG) – IM2AG, Grenoble
5. • Mireille PALMA (MPA) – AccessIT, Lisbonne
6. • Paolo SANTIAGO SANCHEZ (PSO) – AccessIT, Caracas
7. • Hong SHI (HSI) – AccessIT, Zurich
8. • Tararya NARAMANATA (TNA) – AccessIT, Nantes
9. • Zork SWISH (ZSH) – AccessIT, Autriche

- Cassandra COHEN (CCN) - IM2AG, Grenoble

Le présent projet a été baptisé iAccess.

Les demandes de sécurisation de sites et de bâtiments se développent suite aux attentats des dernières années. Il s'agit d'une opportunité commerciale pour les sociétés de sécurité comme AccessIT.

La société AccessIT est spécialisée dans les systèmes de contrôle d'accès.

AccessIT ne produit pas les équipements de sécurité, mais les assemble et les installe.

Les logiciels contrôlant ces équipements sont développés par AccessIT à la demande pour chaque site.

L'équipe informatique de AccessIT est assez limitée actuellement.

Avec l'augmentation de la demande, AccessIT doit faire appel à des prestataires extérieurs pour répondre à ses clients.

La conception de certaines versions de iAccess sera donc confiée à l'UFR IM2AG.

Un certain nombre de contraintes techniques ont été déjà mentionnées :

- les développements devront se faire en Python 3.7 avec le framework Tornado.

Le choix de Python/Tornado est lié au fait que AccessIT utilise déjà ces technologies en interne.

Pour le matériel de sécurité, AccessIT a passé un accord avec Bissis.

Bissis est un constructeur proposant du matériel à la pointe de l'innovation.

En particulier AccessIT a décidé de se baser des bissas (sas à deux portes) pour toutes ses offres.

AccessIT et Bissis ont passé un accord pour mettre sur le marché des bissas le plus rapidement possible.

Bissis sera donc partie prenante pour le projet et fournira les bissas, avec leurs drivers.

Une prochaine réunion aura lieu dans les locaux de Bissis à Berlin pour étudier les bissas.

Différentes organisations ont déjà contacté AccessIT pour la mise en place de iAccess.

L'entreprise chimique Chimiotis désire sécuriser son site de Morrocoy pour octobre 2019.

Les sites des jeux olympiques de Tokyo doivent également être sécurisées pour 2020.

Plusieurs universités indiennes voudraient également migrer vers iAccess en 2019.

Les commerciaux de AccessIT prévoient une augmentation exponentielle des demandes au prochain trimestre.

Chaque version de iAccess sera conçue et développée de façon incrémentale, en commençant par les fonctionnalités les plus demandées par les clients.

AccessIT a décidé d'imposer l'utilisation d'UML pour la conception de ce projet (et d'autres projets).

Plus particulièrement un accord a été passé avec ModelioSoft-Paris pour des licences Modelio.

AccessIT utilisera une démarche agile pour s'assurer de l'adéquation du système avec les besoins des sites.

La conception de la version de iAccess pour Morrocoy a été confiée à l'IM2AG

La prochaine réunion aura lieu à Londres en présence de Competis.

En conclusion, il a été observé que ce consortium international ne pourrait fonctionner qui si toutes les parties prenantes parviennent à participer et à mettre en œuvre leur savoir-faire.

Les différentes parties prenantes sont toutes conscientes des opportunités commerciales apportées par ce nouveau contexte sécuritaire.

1.2 CR002 Réunion iAcces pour le stade Kasumigaoka de Tokyo

Date 01-05 08h-22h

Type Reunion

Lieu Tokyo

PartiesPrenantes ABI, JDR, PSO, AGO

Organisateur ABI

Rapporteur KWG

Presents ABI, JDR, PSO, AGO

Objectifs Attentes pour le stade Kasumigaoka de Tokyo

Attention: Ce compte rendu est un *document de travail* et n'est pas contractuel.

1. Nouvel intervenant :
2. _ Apito GUARACARUMBO (AGO) - Competis, Tokyo
3. La réunion a eu lieu sur le site du stade Kasumigaoka de Tokyo () guidé par AGO.
4. Le stade a été détruit et est actuellement reconstruit à neuf pour les jeux olympiques d'été de 2020.
5. Son accès doit être sécurisé pour fin 2019.
6. Grâce aux bissas, cette installation a été considérée comme viable par AccessIT.
7. AccessIT et Bissis seront les seuls à pouvoir équiper des sites avec des bissas.
8. Un plan des installations a été fourni par Competis.
9. A partir de la visite du site et de ce plan, un premier plan sécurité a été établi.
10. Les différents points d'accès et le nombre des bissas a été déterminé par AccessIT.
11. De même pour le positionnement des caméras et de la salle de contrôle.

12. Les différentes zones du site ont été représentées sur le plan sécurité.
13. Par contre les bâtiments, installations et autres espaces non sécurisés n'y sont pas.
14. De même pour les entrées de véhicules et autres entrées gérées par des vigiles.
15. Les différents types de bissas ont été choisis en fonction du niveau de sécurité à atteindre.
16. Il est rappelé qu'une présentation des bissas aura lieu à Berlin - Bissis.
17. Différents groupes de personnes autorisées devront être définis.
18. Par exemple les spectateurs auront des billets papier.
19. Ils ne pourront accéder qu'à la tribune correspondant à leur billet.
20. Cette autorisation n'est valide que pour la période correspondant à l'épreuve du billet.
21. Un exemple de billet a été fourni par Competis et reproduit ci-dessous.

22. Pendant les jeux olympiques, les athlètes accéderont au village sportif, au restaurant, et à leur bâtiment.

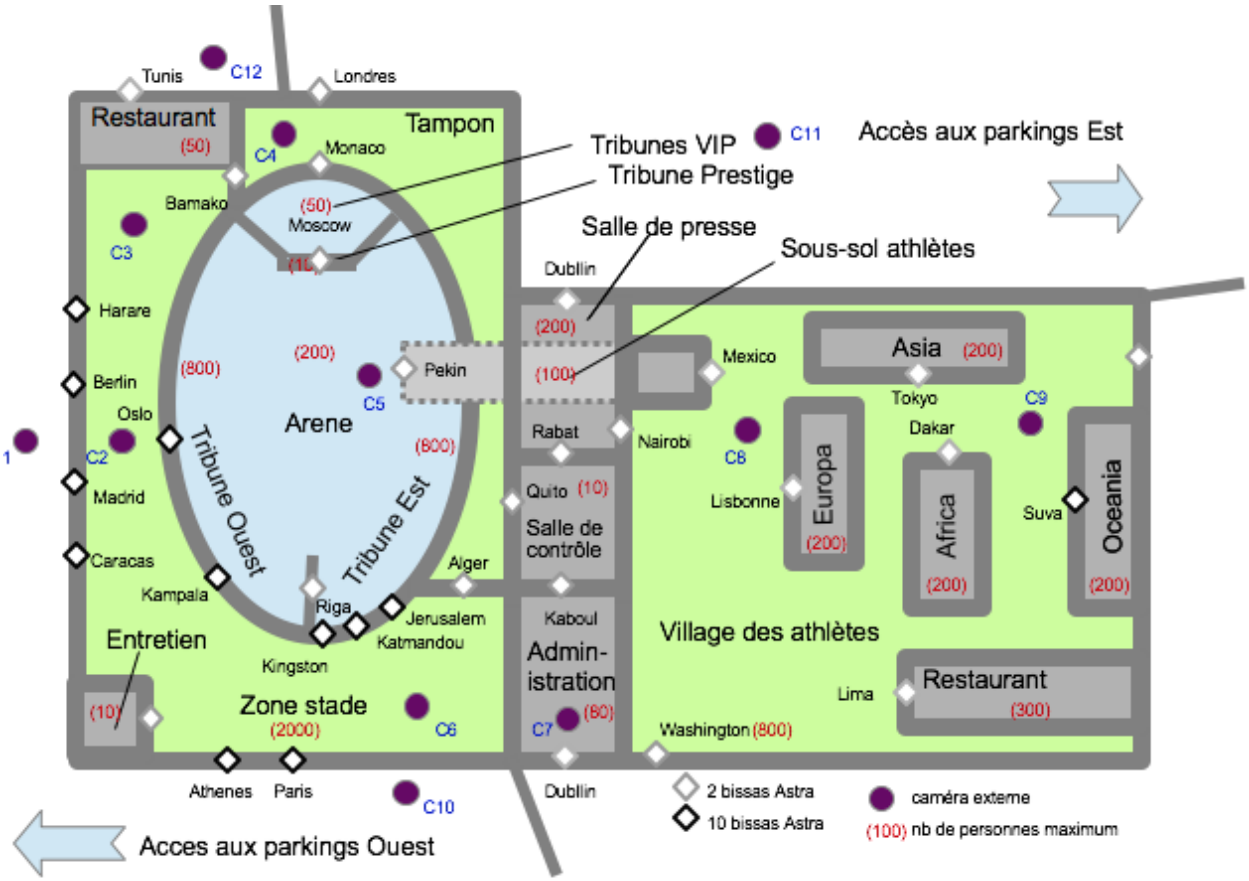

Fig. 1: Fig. 1 : Le nouveau stade Kasumigaoka

Fig. 2: Fig. 2 : Exemple de billet faisant office de badge grâce au QR code

23. Ils pourront aussi aller en salle de presse et à l'administration de 8h à 17h.
24. Par contre l'accès au sous-sol sportif et à l'arène ne leur sera pas autorisé tout le temps.
25. Ce sera uniquement le cas si une épreuve de leur discipline est en cours.
26. Différents autres groupes de badgeurs ont été évoqués dans ce cas d'étude.
27. Par exemple les administratifs et les journalistes ont chacun leurs zones.
28. Comme sur tous les sites, les gardiens peuvent aller dans toutes les zones dont la salle de contrôle.
29. Ils peuvent depuis leur smartphone débloquer l'accès ou la sortie d'une personne bloquée suite à un incident.
30. Même si différents groupes de badgeurs ont été identifiés, d'autres pourraient apparaître.
31. Un superviseur unique par site pourra créer des administrateurs pour ces groupes. Il leur donnera des droits sur la gestion d'une ou plusieurs zones.
32. Chaque groupe d'un site sera alors créé et géré par un administrateur et pas par le superviseur.
33. Par exemple les administrateurs des sportifs pourront éditer leurs badges et définir les zones auxquelles ils ont accès et à quels moments.
34. Les administrateurs de presse s'occuperont des badges des journalistes, etc.
35. Bien entendu les administrateurs de groupe ne pourront pas donner à un groupe l'accès à des zones dont il n'est pas chargé.
36. Les badges papiers pour les spectateurs seront émis par un système en ligne.
37. Dans une telle compétition, on attend en effet environ 100 000 spectateurs.
38. Plus de 400 000 billets seront sans doute émis (mais pas forcément utilisés).
39. Le système en ligne CyberCompetition (par Competis) sera en charge de l'émission des billets.
40. Pour les spectateurs les badges prendront la forme de QR codes sur leurs billets papiers (cf. *CR002Fig2*)
41. De façon générale des logiciels externes (e.g. CyberCompetition) devront pouvoir gérer les membres d'un groupe, comme ajouter des spectateurs à des compétitions pour lesquels des billets ont été émis par l'ERP CyberCompetition.
42. Pour la transmission par un logiciel à iAccess des informations de gestion d'un groupe, seules certaines informations seront nécessaires
43. Il a été convenu qu'un format XML soit utilisé dans ce cadre.
44. Le fichier d'exemple ci-dessous a été fourni par Competis.

45. La transmission des données entre CyberCompetition et iAccess devra se faire via un web service sécurisé.
46. En conclusion, la visite sur le site du stade olympique de Tokyo a été très instructive.
47. Il correspond bien aux fonctionnalités de base que devra permettre iAccess à terme.

1.3 CR003 Réunion iAcces pour Chimiotis

Date 02-17 15h-23h

Type Réunion

Lieu Morrocoy-Chimiotis

```
<sales transaction="8JH8HHDNKHJA7887787"  items="145" date="20141226">
 <sale>
  <firstName>Virginie</firstName>
  <lastName>Maris</lastName>
  <nationalId>P283728746</nationalId>
  <tickets type='internet' vendor='ticket4all.com' vendorid='4528'>
    <ticket id='879277246472">
      <product>Hockey B12</product>
      <period start='20150116T1100-0430' end='20150116T1800-0430/>
      <qrcode>UDH2846DHSQJ3JF ... GS73Z84DFHDFGSHSDG3657D</qrcode>
      <price amount="28" money="EUR"/>
      <seat>T23</seat>
      ...
...
```

Fig. 3: Fig. 3 : Exemple de fichier généré par Competis - Exemple Competis 01_05

PartiesPrenantes ABI, JDR, PSO, AGO

Organisateur ABI

Rapporteur KWG

Presents ABI, JDR, PSO, AGO,

Objectifs Cas d'étude Usine de Morrocoy

Attention: Ce compte rendu est un *document de travail* et n'est pas contractuel.

1. Nouvel intervenant, directeur de l'usine à Morrocoy :
2. _ Eliezer LAEMMEL (ELL) - Morrocoy, Chimiotis
3. Grâce aux contacts d'AGO, une visite du site chimique de Morrocoy a été organisée opportunément.
4. Chimiotis, la société gérante désire s'équiper de bissass pour son système d'accès sécurisé.
5. Il s'agit donc d'un prospect chaud pour iAccess.
6. Un premier plan sécurité a été créé à partir des informations fournies par Chimiotis.
7. Contrairement au stade de Tokyo, le site Morrocoy n'accueille pas de spectateurs.
8. Un élément important concerne les règles à appliquer en cas d'incendie dans une zone.
9. Tous les points d'accès doivent être ouverts automatiquement vers l'extérieur dans les zones dites "Incendie Libre" (IL).
10. Dans les autres zones, un incident est envoyé à tous les gardiens.
11. Chaque gardien signale qu'il a bien reçu l'incident et peut ensuite consulter si des personnes sont présentes dans la zone et débloquer tel ou tel point d'accès.
12. Il faudra donc prendre en compte les systèmes à incendie et les interfacer avec iAccess.
13. Par ailleurs à première vue le nombre de groupes est a priori plus faible à Morrocoy qu'à Tokyo.

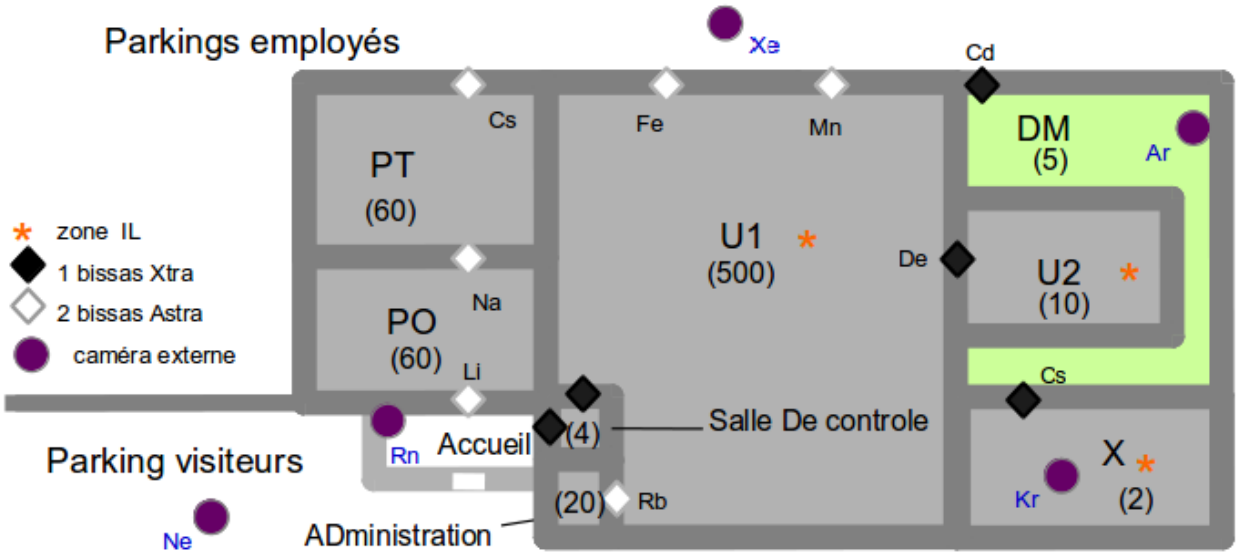

Fig. 4: Fig. 1 : Potentiel plan sécurité pour le site de Morrocoy

14. Le nombre de badgeurs par groupe va de 1 à 300 environ.
15. Les ouvriers font les 3 x 8 mais de manière relativement régulière.
16. Les membres de chaque groupe sont finalement assez stables.
17. En effet le personnel de l'usine ne change que rarement et les groupes sont basés sur des règles relativement stables dans chaque zone.
18. Ci-dessous le dernier plan d'autorisation fourni par l'administration de Chemiotis.

19. Les autorisations aux zones sont présentées pour chaque groupe à droite.
20. A gauche sont représentées les périodes liées à ces autorisations.
21. Après discussion avec l'administration il apparait qu'il s'agit d'une version très simplifiée.
22. En effet l'usine devant tourner 24h/24h, 365j/365, des groupes d'ouvriers sont ajoutés pour les jours fériés et les week-ends.
23. Ces groupes ne sont pas représentés sur le planning annuel montré en *CR003Fig2*.
24. Ce planning est représentatif de ce qui se passe chaque année.
25. Les groupes du planning annuel sont homogènes par rapport aux zones autorisées.
26. Autrement dit, pour une période un groupe peut accéder toujours aux mêmes zones (cf. *CR003Fig2*).
27. En réalité, et selon un exemple donné par ELL, certains groupes (e.g. GX et GY) peuvent accéder à la zone PT et PO en semaine de 8h à 12h pendant l'été.
28. Mais de plus GX peut en plus accéder à la zone X et DM le week-end de 16h à 23h de mars à avril.
29. Actuellement tous ces différents cas sont gérés de manière ad-hoc par les gardiens en poste aux points d'accès de chaque zone.
30. En pratique cette gestion est un peu aléatoire et se base sur le bon-vouloir des gardiens et des employés.
31. Il faudra absolument définir des autorisations plus fines dans iAccess pour représenter ce genre de périodes.

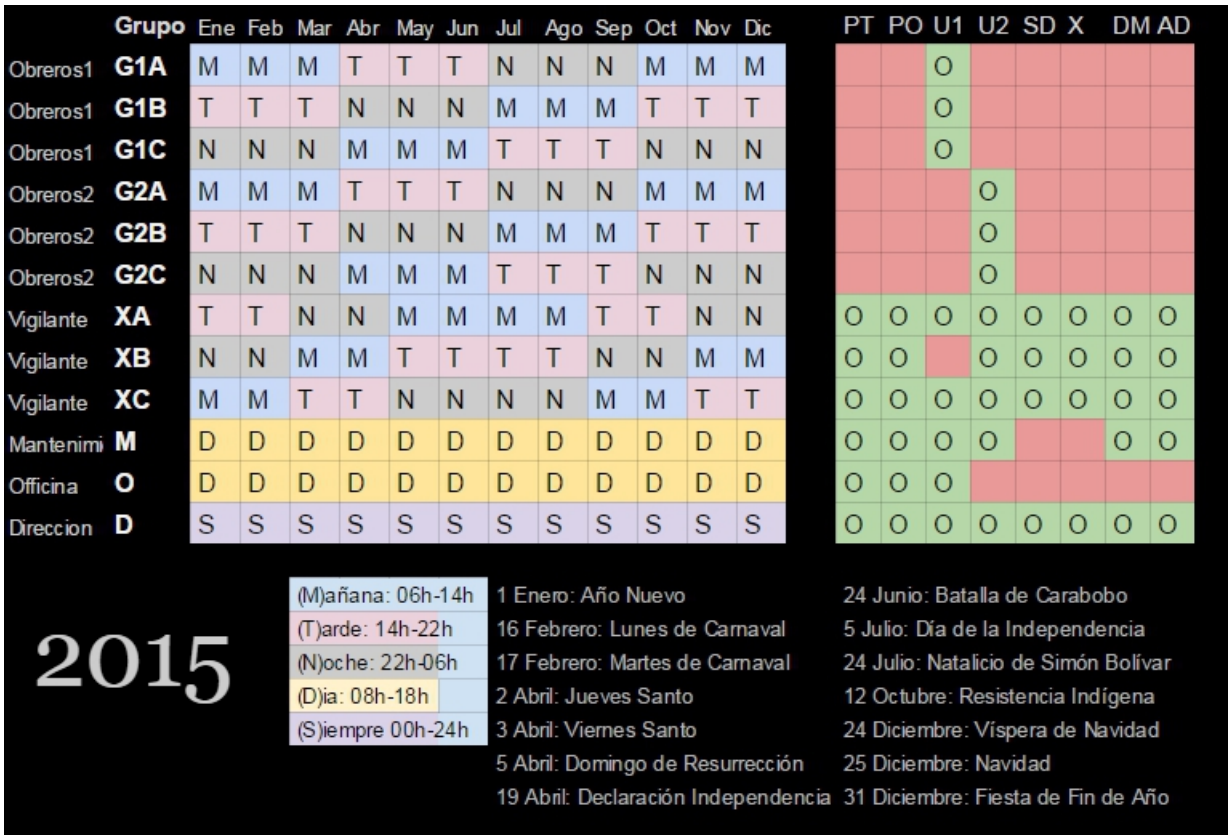

Fig. 5: Fig. 2 : Plan d'autorisation (simplifié) pour le site de Morrocoy

32. Une autorisation doit être un triplet (groupe(s), période, zone(s)).
33. Par exemple, en reprenant l'exemple donné par ELL, on doit pouvoir définir deux autorisations comme suit.

Table 1: Tab. 1 : Exemple ELL 01-06

Groupes	Période	Zones
GX, GY	xxxxxxJASxxx LMMJVxx 08:00-12:00	PT, PO
GX	xxMAxxxxxxxx xxxxxSD 16:00-23:00	X, DM

34. Les autorisations sous forme de triplets pourraient aussi convenir a priori pour le stade de Tokyo en 2020.
35. Il s'agit en effet d'une représentation générale et sans doute satisfaisante.
36. Il a été décidé de partir a priori sur ce modèle d'autorisation pour iAccess.
37. Dans le cas de Morrocoy, il semble qu'un seul administrateur pourrait gérer tous les groupes.
38. Cela contraste avec le site de Tokyo où plusieurs administrateurs devront gérer des groupes différents et inversement ou un même groupe pourra être géré par des administrateurs différents.
39. Actuellement l'usine est gardée par 60 gardiens, 24/24.
40. Avec iAccess on estime que 4 gardiens serait suffisant, d'où 12 en 3x8.
41. Comme pour les autres sites, le serveur de contrôle serait installé dans la salle de contrôle.
42. Chemiotis émet également le besoin de pouvoir recevoir des visiteurs via des badges courts.
43. Dans ce cas les badges courts pourraient être distribués en direct à la réception et utilisés immédiatement.
44. Actuellement il n'y a aucun système pour les badges courts à Morrocoy.
45. Il s'agit simplement d'un coup de téléphone donné aux gardiens, ce qui n'est évidemment pas sécurisé.
46. Chemiotis souhaiterait par contre disposer de l'historique d'accès.
47. Chemiotis voudrait contrôler les heures de présences dans l'usine des employés.
48. La conservation de l'historique des événements étant imposée par la réglementation du Venezuela, cette fonctionnalité devra être intégrée dans iAccess.
49. Un web service permettra à des systèmes externes (e.g. systèmes de paye / de contrôle de présence) d'importer les événements d'accès de iAccess (horaire d'entrée pour chaque point d'accès).
50. Ce web service devra être sécurisé pour des aspects de confidentialité mais aussi de sécurité (e.g. heures d'accès des gardiens, etc).
51. A Tokyo, le service web d'export sera utilisé entre autres par les services commerciaux pour déterminer les billets vendus n'ayant pas été utilisés.
52. Après discussion avec Competis, l'historique d'accès est également nécessaire pour Tokyo vu le grand niveau de sécurité attendu au Japon.
53. En conclusion, les besoins du site de Morrocoy sont tout à fait pertinents pour iAccess.
54. AccessIT confirme son intérêt de développer une version de iAccess pour ce site.
55. Cette version sera la première développée par l'IM2AG.
56. La prochaine réunion aura lieu comme prévu à Berlin - Bissis.

1.4 CR004 Matériels de contrôle d'accès

Date 03-15-07h-20h

Type Réunion

PartiesPrenantes KWG, CMS, YBI, MPA, ZSH

Lieu Berlin-Bissis

Organisateur KWG

Rapporteur KWG

Presents KWG, CMS, YBI, MPA, ZSH

Objectifs Architecture et discussions sur les fonctionnalités gardien

Attention: Ce compte rendu est un *document de travail* et n'est pas contractuel.

1. Nouvelles parties prenantes :
2. _ Clarissa Maris (CMS) - Bissis, Berlin
3. _ Yohav El Benali (YBI) - Bissis, Berlin
4. La réunion a eu lieu dans les locaux de Bissis.
5. Bissis est sur le point de commercialiser des sas de sécurité révolutionnaires.
6. Ces systèmes physiques seront prochainement commercialisés sous le nom de *Bissas*.
7. Bissis souhaite accélérer la mise sur le marché des bissas et souhaite donc intégrer le consortium pour participer à l'élaboration de iAccess.
8. Il est entendu que Bissis fournira ces Bissas et pour chaque modèle un driver logiciel pour l'intégrer à iAccess
9. Par contre un problème est vite apparu pendant la réunion.
10. Il sera impossible de voir les bissas avant au moins deux mois, et cela pour des problèmes de confidentialité.
11. Vu les très nombreuses innovations, de multiples brevets sont en court d'acquisition et ce procédé est long.
12. La direction ne souhaite prendre aucun risque de fuites et même en interne seuls certains employés (e.g. YBI) ont une vision globale des bissas tel qu'ils seront présentés dans quelques mois.
13. Après quelques échanges et discussions animées, il est apparu que ce ne devrait cependant pas être un problème pour iAccess.
14. Bissis fournira des simulateurs pour que puissent commencer les tests lorsque nécessaires.
15. Toutes les parties logicielles sur le serveur applicatif pourront être réalisées en amont grâce à la simulation des bissas et des caméras pilotées par les drivers à installer sur le serveur de contrôle.
16. AccessIT, qui travaille depuis longtemps avec Bissis, est confiant dans cette démarche.
17. L'utilisation d'une spécification UML a été soulignée comme un point essentiel dans ce contexte tendu.
18. Il a été convenu que l'IM2AG fournirait rapidement des scénarios qui serviront à écrire les tests de la version pour Morrocoy.
19. Il s'agit non seulement de tester les scénarios de passage sans incident, mais aussi les scénarios générant des alarmes envoyées aux gardiens.

20. En ce qui concerne les fonctionnalités des bissas, Bissis a proposé une illustration via l'étude d'un système proposé par un de ses concurrents.
21. Les bissas ressembleront *par certains côtés* au système "Cilindro Bibussola" de AllUserIndustrie:

22. Le Bibussola n'est là qu'à titre d'illustration ; les bissas ont de nombreuses différences.
23. Des groupes de 2 à 16 bissas peuvent être alignés par point d'accès.
24. Le matériel est extrêmement performant (à condition que les contrôles logiciels suivent).
25. Ceci permet des flux importants à un même point d'accès (jusqu'à 100 passages/mn).
26. Les bissas sont symétriques
27. Ils possèdent systématiquement des lecteurs sur les deux faces (contrairement aux Bibussolas).
28. Ils peuvent ainsi contrôler à la fois l'entrée et la sortie.
29. Ce qui permet à tout moment être capable de savoir qui est dans une zone.
30. Cette fonction est nécessaire entre autres pour ne pas dépasser le nombre maximum de personnes autorisées par zone.
31. Si une zone est pleine, une alerte devra être générée pour qu'un affichage le signale et que les gardiens soient prévenus de venir expliquer la situation.
32. Les lecteurs des bissas sont polyvalents et permettent plusieurs types d'identification.
33. Ils lisent différents types de badges papier, par exemple des QR codes.
34. Ils peuvent lire également des cartes classiques ou sans contact (jusqu'à 1m).
35. Quel que soit le type de badge, les informations envoyées par le driver du bissas au serveur de contrôle sont toujours identiques.
36. La première information est le numéro du point d'accès dans le site.
37. La seconde information est le numéro du bissas dans ce point d'accès
38. La troisième information est la face sur laquelle le badge a été lu (A ou B).
39. La dernière information est le "bCode" (code badge) lu par le lecteur de badge.
40. Les lecteurs sont équipés de deux leds (une rouge et verte).
41. Deux détecteurs de chaque côté permettent au bissas de signaler lorsqu'une porte arrive en position ouverte ou en position fermée.
42. Tout comme le Cilindro Bibussola, les bissas possèdent un détecteur de présence à l'intérieur du sas.
43. **A chaque fois qu'une porte est refermée, il détecte l'absence ou la présence d'une personne et si du métal est présent en re**

44. En fait les bissas sont entièrement contrôlés par le driver fourni par Bissis.
45. Ces drivers seront installés sur le serveur de contrôle.
46. Chaque bissas sera connecté au panneau de brassage du serveur de contrôle par une connexion RFC 821
47. Bissis propose deux types de bissas, les bissas Astra et les bissas Xtra.
48. Les bissas Astra sont destinés à recevoir un public important.
49. C'est pour cela que AccessIT préconise leur utilisation au stade de Tokyo.
50. Les bisas Xtra sont écartés car leur débit est insuffisant.

Fig. 6: Fig. 1 : *"CILINDRO BIBUSSOLA"* par AllUserIndustrie (cf `VideoBibussola`)

Fig. 7: Fig. 2 : Incident de « piggybacking (cf `VideoBibussola` seconde 52)

51. Les bissas Astra permettent entre autres d'organiser des files d'attentes uniques par point d'accès.
52. Ils sont munis d'un feu visible depuis la file indiquant l'état du bissas (disponible = vert, rouge = utilisé, orange = bientôt libre).
53. Ce feu tricolore permet de montrer le prochain bissas Astra disponible (voyant orange).
54. Pour cela, un détecteur de présence à l'intérieur fait passer le feu à l'orange lorsqu'un badgeur est entré dans le bissas et que la seconde porte s'ouvre.
55. En fait, une fois de plus, ce genre de fonctionnalités est prédéfini et intégré au bissas et ne sont pas commandés par le driver de Bissas depuis le serveur de contrôle.
56. AccessIT insiste de nouveau sur le fait que différents scénarios devront donner lieu à des incidents envoyés aux gardiens.
57. C'est le cas par exemple si un badgeur ne sort pas du sas au bout de 8 secondes.
58. C'est également le cas si quelqu'un bloque une porte (avec un pied ou autre).
59. Bissis propose aussi des bissas haute sécurité, les bissas Xtra.
60. Ces bissas sont préconisés par AccessIT pour l'usine de Morrocoy.
61. Ils permettent d'être sûr (à 98%) que le badgeur est bien la personne associée au badge.
62. La personne ne peut en effet sortir du sas qu'après avoir effectué une identification physique.
63. Cette identification physique se fait à l'intérieur du sas, après l'identification badge à l'entrée.
64. L'identification physique est une empreinte digitale
65. Si la personne n'est pas autorisée un incident système sera généré par le bissas Xtra.

66. Il en sera de même si le détecteur de métaux intégré dans les Xtra se déclenche.
67. Le badgeur sera alors bloqué dans le sas et devra attendre qu'un gardien vienne le débloquer.
68. Une fois de plus Bissis propose le matériel pour permettre cela, mais les fonctions devront être réalisées sur le serveur de contrôle en fonction des informations émises par les bissas.
69. Evidemment les digitCodes transmis par le lecteur d'empreinte digitale devront être comparés aux données disponibles sur le serveur applicatif.
70. Dans iAccess ce sont les administrateurs de groupes qui seront chargés, en plus de la délivrance des badges selon la procédure normale, de collecter les empreintes digitales des badgeurs.
71. L'identification physique des badgeurs dans un Xtra devra se faire en moins de 5 secondes.
72. L'identification des badges et surtout le calcul des autorisations lors d'un passage de badge devra toujours pouvoir être faite en moins de 2 secondes.
73. Sachant que l'on envisage plus de 200 entrées ou sorties simultanément un soin tout particulier devra être apporté à cet aspect.
74. Bissis propose également d'autres éléments matériels pour la sécurité.
75. Des caméras directionnelles C800 pourront être installées comme option d'iAccess.
76. Les gardiens devront pouvoir à tout moment les réorienter à distance.
77. Les plans de sécurité proposés par AccessIT pour Morrocoy et Tokyo sont déjà basés sur l'utilisation de ce matériel.
78. Cependant pour des raisons de délai, les caméras ne seront pas connectées à iAccess pour la première version du logiciel
79. Les bissas doivent être reliés au serveur de contrôle du site via des liaisons "RFC 321"; les caméras via des liaisons "RFC 821".
80. Le matériel et les protocoles associés sont en cours d'être brevetés par Bissis.
81. Il doit y avoir une salle de contrôle par site ; elle contient le serveur de contrôle.
82. Il s'agit d'un matériel spécialisé quasi temps réel auquel de multiples câbles sont connectés sur un panneau de brassage (jusqu'à des centaines sur certains sites).
83. Ce serveur de contrôle devra être connecté au serveur applicatif via une liaison TCP/IP sécurisée.
84. Seuls les gardiens doivent avoir accès à la salle de contrôle.
85. En conclusion de cette réunion (longue), il apparaît clairement que les technologies innovantes proposées par Bissis en font un partenaire idéal.
86. De plus, le matériel n'étant pas disponible à ce jour, il est essentiel de préparer les scénarios à prendre en compte et de les spécifier de manière rigoureuse.
87. Bissis fournira des simulateurs matériels pilotables par le driver fourni.
88. Dans un premier temps des tests seront ainsi effectués à partir des scénarios fournis par IM2AG.
89. Une réunion est prévue (03-18) pour discuter des points non abordés jusque-là et notamment de l'architecture de déploiement.

1.5 CR005 Architecture et contraintes techniques

Date 03-18 12h-17h

Type Réunion

PartiesPrenantes ABI, HSI, KWG, MPA, PSO

Lieu Paris-AccessIT

Organisateur ABI

Rapporteur KWG

Presents ABI, HSI, KWG, MPA

Objectifs Définir l'architecture et revenir sur les fonctions associées à chaque noeud.

Attention: Ce compte rendu est un *document de travail* et n'est pas contractuel.

1. AccessIT rappelle l'architecture classique des applications déjà mises en place par leur soin.
2. Il n'y a aucune raison a priori de changer d'architecture sachant qu'elle fonctionne bien dans différents contextes.
3. Les matériels sécurité (bissas, caméras, etc.) sont toujours connectés directement au serveur de contrôle.
4. Ce serveur permet de gérer en temps réel les matériels en les commandant par leur driver
5. Le serveur d'applications doit être plus ou moins puissant selon le volume de données à gérer et le nombre de transactions à mettre en œuvre.
6. Pour les sites de Tokyo ou de Morrocoy, il n'y aura a priori pas de soucis, mais AccessIT a déjà eu affaire à des sites avec plus de 800 points d'accès, 80 000 badgeurs, avec des historiques à conserver sur 5 ans (base militaire en Sibérie).
7. De tels clients devront pouvoir être gérés avec iAccess.
8. Contrairement aux architectures traditionnelles, il n'y aura pas de poste fixe pour les gardiens.
9. Les gardiens seront équipés de smartphones pour gérer les incidents.
10. C'est un grand changement car jusque-là des appareils spécialisés ou des postes fixes étaient utilisés.
11. Les applis des smartphones des gardiens seront connectées au serveur applicatif via une connexion sécurisée https et un réseau wifi interne sécurisé.
12. AccessIT mentionne qu'il est possible d'installer des systèmes de brouillage et bien d'autres choses, qui rendent ce réseau à la fois sûr et fiable.

Fig. 8: Fig. 1 : Smartphones des gardiens

13. Les incidents doivent être localisés (e.g. bissas, point d'accès et/ou zone) et gardés dans l'historique.
14. Lorsqu'un gardien prend un incident, celui change d'état ("nouveau"->"affecté").

15. En fonction des cas, et la plupart du temps après s'être rendu sur place, le gardien peut agir sur l'incident pour l'ignorer ou le régler.
16. Un incident ignoré ou réglé est considéré comme fermé mais peut encore être commenté, en lui associant du texte, des photos ou de l'audio/vidéo.
17. Le règlement d'un incident dépend des cas.
18. En cas d'incident d'accès, le gardien peut fermer ou ouvrir une des portes du bissas (ou les deux) depuis sa tablette.
19. En cas d'incident d'incendie, le gardien peut déverrouiller un ou plusieurs bissas dans le sens de la sortie.
20. Quand le bissas est déverrouillé, la simple détection d'une personne devant le bissas l'ouvre le bissas et il est refermé une fois qu'elle est passée.
21. En situation de crise, le temps de réaction des gardiens peut devenir essentiel.
22. Pour améliorer la rapidité d'intervention des gardiens, iAccess fournira dans une seconde version un paramétrage avec des types d'incidents prédéfinis.
23. C'est le rôle des superviseurs de les définir et cela se fait généralement lors de la définition du plan sécurité initial en fonction des caractéristiques du site.
24. Assez souvent on découvre par la suite de nouveaux types liés à des situations répétitives (e.g. "tuyau percé" dans une usine, "malaise dans un bissas" dans un hôpital, "cartable coincé dans un bissas" dans une école, etc.).
25. Les gardiens peuvent alors sélectionner les types d'incidents correspondant à la situation.
26. Evidemment si nécessaire les gardiens peuvent utiliser la fonction téléphone de leur smartphone pour appeler les services compétents (urgences, police, armée, etc.)
27. La discussion sur le rôle des gardiens s'est achevée sur la conclusion suivante.
28. L'IHM des gardiens doit être particulièrement ergonomique vu le contexte d'utilisation à la fois quotidien et potentiellement intensif.
29. _
30. En ce qui concerne le poste superviseur (toujours un seul, pour des raisons de sécurité) et les postes administrateurs (autant que nécessaire), ceux-ci seront également connectés au serveur applicatif par une liaison Ethernet, avec un client lourd utilisant le protocole https.
31. Il s'agit dans les deux cas de PCs sous LINUX.
32. _
33. Les administrateurs gèrent non seulement les inscriptions des badgeurs, mais aussi les problèmes liés à la perte d'un badge.
34. Lorsqu'un badge est perdu, volé (y compris via agression), le badgeur est tenu d'en informer immédiatement le centre de sécurité.
35. Cela ne concerne pas les tickets avec des badges papier, qui sont gérés directement par la société qui les vend.
36. Quel que soit le type de badge, un badge est toujours associé à une seule personne à la fois et une personne ne peut posséder qu'un badge (pour un site) à un moment donné.
37. Les badgeurs sont connus au minimum par leur nom et leur prénom et un numéro d'identité national (NIN).
38. Le NIN utilisé dépend des personnes et des pays considérés.
39. Ce peut être le numéro de passeport, le numéro de carte d'identité ou tout autre document selon le pays.
40. Un mail et deux numéros de téléphone peuvent également être renseignés lors de l'enregistrement.

41. A chaque fois qu'un badge est donné à quelqu'un, qu'il est annulé suite à une perte ou un vol, l'opération doit être enregistrée dans l'historique.
42. Toutes ces opérations sont effectuées par les administrateurs de groupes.
43. Lorsqu'un badgeur appartient à plusieurs groupes, et si ces groupes sont gérés par différents administrateurs, n'importe quel de ces administrateurs peut gérer la perte du badge.
44. Finalement, le serveur applicatif est le seul élément de iAccess a être connecté à internet via tcp-ip.
45. C'est lui qui gèrera les web-services mentionnés auparavant.
46. _
47. Il est fait état d'un démarrage éminent de la phase de collecte des exigences.
48. Les spécifications UML seront faites par le groupe M1 MIAGE au sein de l'IM2AG à partir des comptes rendus de réunions réalisés jusque-là.
49. Les personnels de la société AccessIT ne seront pas disponibles dans les semaines qui viennent.
50. Il risque d'en être de même des membres IM2AG ayant participé à ces réunions, un voyage en Russie puis en Irlande étant prévu pour le prochain mois.

Ce contenu est disponible sur le site http://CyberBatiment.readthedocs.org