

Solutions d'authentification renforcée

Critères d'évaluation

État de l'art

Sommaire

1 Rappel JRSSI 2012 : Sécurité des accès périmétriques

2 Cas d'usage, besoins et contraintes utilisateurs

3 Critères d'évaluation et cas d'authentications renforcées

4 Conditions de réalisation et de mise en œuvre

Rappel JRSSI 2012 : Sécurité des accès périmétriques

Plusieurs niveaux de sécurité existent : Authentification **faible** (1/3)

- Quelle évaluation ?
- Définition : identifiant + authentifiant statique
- 1 seul facteur, « ce que je sais »
- Au regard des **avantages** :
- **Facilité de** déploiement,
 - **Simplicité** de mise en œuvre
 - **Coût** incomparable

Rappel JRSSI 2012 : Sécurité des accès périmétriques

- Au regard des **risques** forts (événements redoutés / probabilité) :
 - **Scénarios** de **compromission** des identifiants/mdp en forte **hausse**
 - Observation + keylogger (comment garantir qu'il n'y en a pas ?)
 - Phishing (hameçonnage) (de mieux en mieux conçus)
 - Compromission de bases (APT non détectées ou constatées après vol des bases)
 - **Réutilisation** aisée des « mots de passe compromis »
 - Mdp multi applications
 - Mdp à durée de vie (très) longue
 - Mdp peu robuste (social engineering)

Rappel JRSSI 2012 : Sécurité des accès périmétriques

- Au regard des **usages** :
 - Pour une authentification à **l'accès initial** et de ce qui en **dépend**

- Au regard de **l'impact** sur le SI :
 - La généralisation du SSO et/ou de la fédération d'identité **maximise** l'effet du vol
 - 1 authentification – N applications – P domaines – **NxP accès**

Rappel JRSSI 2012 : Sécurité des accès périmétriques

– Au regard des **Contre-mesures possibles** :

- Sensibilisation : nécessaire mais pas suffisante (<75% après plusieurs campagnes sur des populations choisies - JRSSI 2012)
- Mot de passe robuste : inutile contre une fuite en clair
- Obsolescence des mdp : réduit l'utilisation, inutile si la fuite est active
- Antivirus : limite la contagion mais donne un faux sentiment de sécurité

➤ *protection par mdp devenue inacceptable pour le SI et pourtant irremplaçable ?*

Rappel JRSSI 2012 : Sécurité des accès périmétriques

Plusieurs niveaux de sécurité existent : Authentification **forte** (2/3) :

- Quelle évaluation ?
- Définition : identifiant + au **moins** deux facteurs **indépendants**
- « ce que je sais » + « ce que je possède »
 - OTP = PIN + code affiché sur le support cryptographique physique
 - Certificats sur carte à puce = PIN + signature d'un aléa par la clé privée stockée dans le support cryptographique physique
- Au regard du nombre : 250 000 OTP + 3000 cartes à puce

Rappel JRSSI 2012 : Sécurité des accès périmétriques

- Au regard des **avantages** :
 - Inviolabilité
 - Sécurité à l'accès forte
 - Et donc **sécurité** sur **tout** le **périmètre** du SI rendue forte
 - Non répudiation (selon les cas : signature, chiffrement, etc.)
- Au regard des **risques** :
 - Contraintes de coût et modalités opérationnelles de déploiement qui jouent *en faveur du mot de passe*

Rappel JRSSI 2012 : Sécurité des accès périmétriques

Plusieurs niveaux de sécurité existent : Authentification **renforcée**
(3/3) : Quelle évaluation?

- Définition : identifiant + *au moins 1* facteur non statique
« ce que je sais » ...
- Au regard des **avantages** :
 - **Facilité** de déploiement
 - **Simplicité** de mise en œuvre
 - **Faible** coût
 - **Renforcement** de la sécurité à l'accès
- Au regard des **risques** :
 - Attention à une bonne adéquation aux besoins réels

Rappel JRSSI 2012 : Sécurité des accès périmétriques

Authentification **renforcée** les offres industrielles se multiplient et sont **très** différenciées :



Soft token



Empreinte numérique



Grille statique



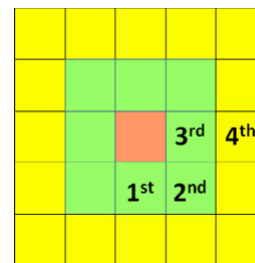
OTP via SMS



OTP « invisible token »



Grille dynamique



Biométrie



following

finding

Captcha

Rappel JRSSI 2012 : Sécurité des accès périmétriques

- **Question 1** : Mais comment réduire l'usage du mot de passe en tant qu'authentification à l'accès afin de la renforcer?
- **Question 2** : Comment choisir le bon niveau de sécurité, le bon moyen d'authentification adapté pour chaque usage et chaque usager?
- **Question 3** : Quel est le moyen d'authentification parfait (unique, pas cher, authentification forte, facile à déployer, pour tous les groupes d'utilisateurs) ?
- **Question 4** : Concrètement parlant, comment fait-on pour doter chaque usager rapidement et sans les difficultés habituelles de déploiement ?
- **Question 5** : Et comment accroche-t-on l'ensemble des applications du SI sur cette nouvelle authentification à l'accès tout en garantissant la continuité de fonctionnement du SI ?

Sommaire

1 **Rappel JRSSI 2012 : Sécurité des accès périmétriques**

2 **Cas d'usage, besoins et contraintes utilisateurs**

3 **Critères d'évaluation et cas d'authentications renforcées**

4 **Conditions de réalisation et de mise en œuvre**

Cas d'usage, besoins et contraintes utilisateurs (1/2)

Questions clés	Réponses type
Dans quel contexte et quel lieu ?	<ul style="list-style-type: none">• Domicile• Dans un espace public• En classe devant des étudiants, des élèves• En salle des professeurs, sur un système partagé (CDI, etc.)• En réunion• Sur le réseau administratif...
Avec quel matériel ?	<ul style="list-style-type: none">• Ordinateur professionnel / personnel• Téléphone mobile / tablette• Avec un projecteur...
A quel moment ?	<ul style="list-style-type: none">• Fréquence d'utilisation (quotidienne, hebdomadaire, mensuelle...)• Durée d'utilisation (quelques minutes, plusieurs heures...)
Sur quels types d'applications ?	<ul style="list-style-type: none">• Bureautique• Messagerie• Applications métier...
Sur quel type de données ?	<ul style="list-style-type: none">• Informations non confidentielles• Données nominatives (élèves...)• Budgets...
Avec qui ?	<ul style="list-style-type: none">• Avec des enseignants• Avec des élèves• Avec les parents• Avec le personnel administratif...

Cas d'usage, besoins et contraintes utilisateurs (2/2)

Questions clés	Exemples de problématiques métiers
Gestion des sujets et remontées pour les examens et le post-bac ?	<ul style="list-style-type: none"> • Confidentialité élevée et accès restreints durant une période courte • Impact de divulgations de sujets
Applications financières en établissement ?	<ul style="list-style-type: none"> • Impact élevé d'une usurpation d'identité (à cause de l'impact élevé de l'usurpation de droits associés au compte)
Applications de gestion des personnels ?	
Contentieux juridiques possibles ?	<ul style="list-style-type: none"> • RGS
Applications de scolarité Second degré : Gestion des élèves ?	<p><i>Exemple – Logiciel de Notes :</i></p> <ul style="list-style-type: none"> • En salle des professeurs, un enseignant veut pouvoir utiliser l'ordinateur commun pour se connecter à l'application de saisie des notes de ses élèves
Gestion des notes-bulletins / compétences / vie scolaire ?	<p><i>Exemple – Logiciel de Notes :</i></p> <ul style="list-style-type: none"> • En conseil de classe, le chef d'établissement veut pouvoir se connecter à une application pour afficher sur grand écran devant les professeurs, les représentants de parents et les délégués d'élèves, les moyennes par matière et les commentaires des enseignants pour chacun des élèves

Cas d'usage, besoins et contraintes utilisateurs

En conclusion quel est l'état des lieux :

- Plusieurs niveaux de sécurité existent dans notre panoplie ministérielle :
 - Fort (OTP, carte à puce) ou Renforcée (certificat dans le magasin cryptographique MS)
 - Faible (mdp)
- Ils ont des inconvénients :
 - Certains sont trop chers
 - D'autres sont trop complexes à déployer : gérer le parc des clés, remplacement
 - Ou trop peu fiables (mdp)
 - Usages mal couverts par OTP/certificat : Parents ? Elèves ? Extérieurs ?
- Reste à explorer les nouveaux modes d'authentification (renforcés) et à les caractériser au regard de nos besoins

Sommaire

- 1 **Rappel JRSSI 2012 : Sécurité des accès périmétriques**
- 2 **Cas d'usage, besoins et contraintes utilisateurs**
- 3 **Critères d'évaluation et cas d'authentications renforcées**
- 4 **Conditions de réalisation et de mise en œuvre**

Critères d'évaluation & cas d'authentications renforcées

Plusieurs groupes de critères sont nécessaires pour construire les radars :

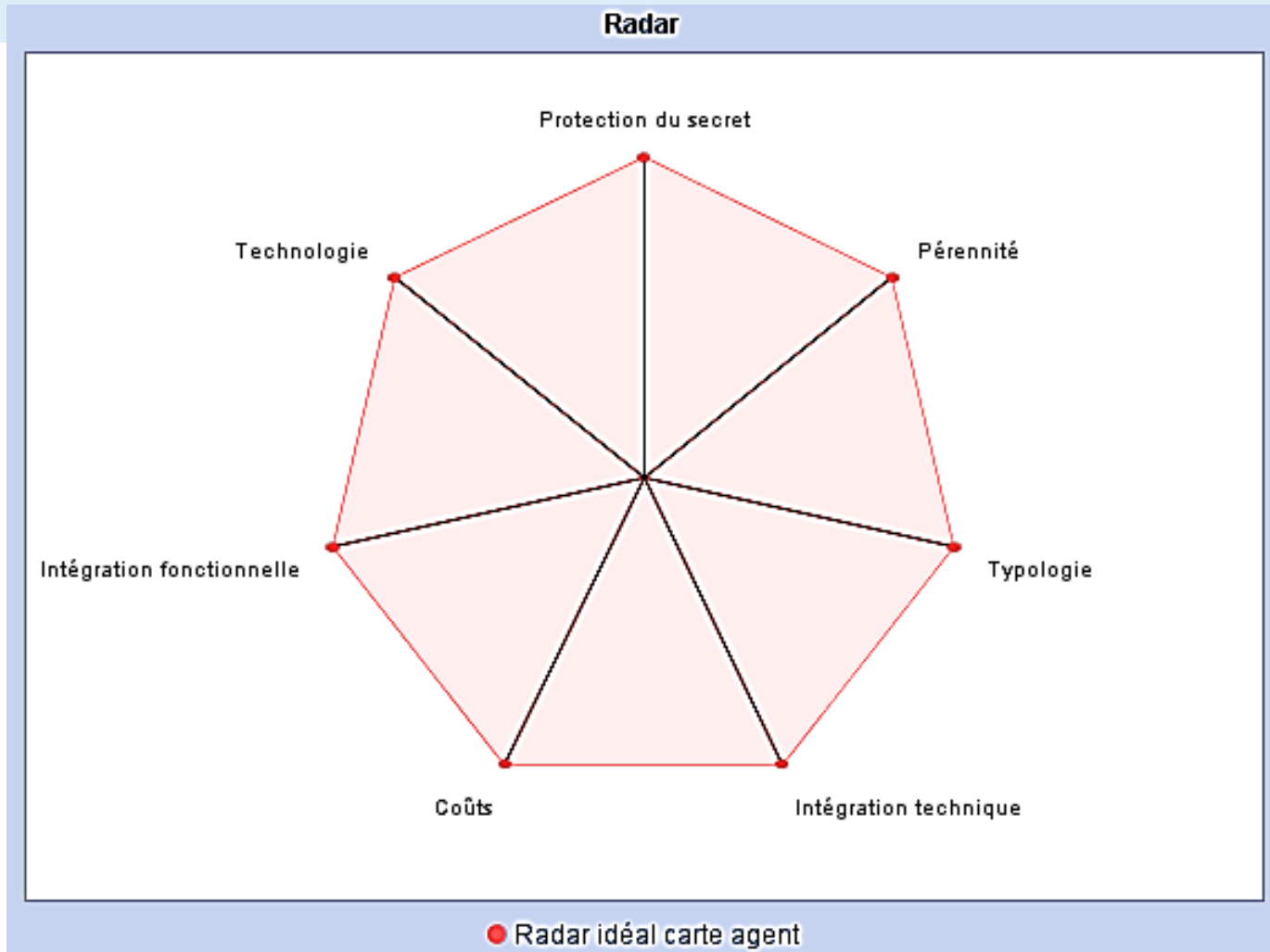
- Les classes de critères d'évaluation sont :
 - Typologie (forte/faible, nombre de facteurs, etc.)
 - Technologie (adhérence au SI, support cryptographique physique, etc.)
 - Protection du secret (sensibilité au vol, etc.)
 - Coût
 - Facilité d'intégration technique au SI (compatibilité avec les infrastructures, résilience, etc.)
 - Facilité d'intégration fonctionnelle (adaptation aux conditions de travail des agents, ALE, CRL, etc.)
 - Pérennité de la solution d'authentification

Critères d'évaluation & cas d'authentications renforcées

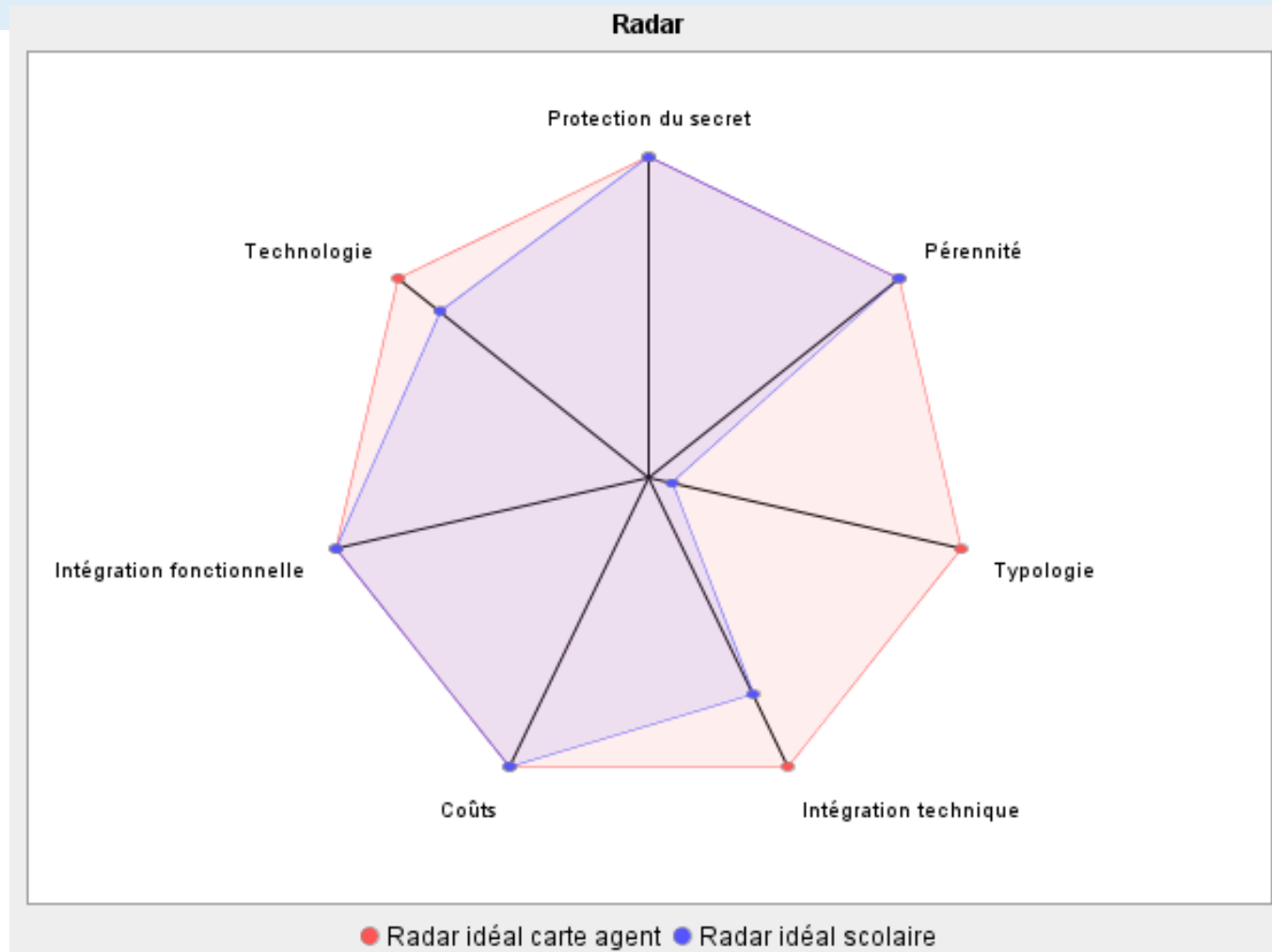
Ces groupes de critères mettent en lumière des catégories très différentes de moyens d'authentification:

- Un premier groupe basé sur la détention d'un **support** cryptographique **physique**
 - Problématique de non répudiation, difficulté de déploiement, prix
 - Un second groupe basé sur l'installation de **logiciel** sur un système physique non dédié tels que : pc, tablette, smartphone, etc.
 - Problématique de non maîtrise du support, difficulté de déploiement,
 - Un troisième groupe basé sur la virtualisation du moyen d'authentification, telle que les **grilles dynamiques**, les « invisible tokens », etc.
 - Problématique faible coût
- Le radar **idéal** serait le suivant :

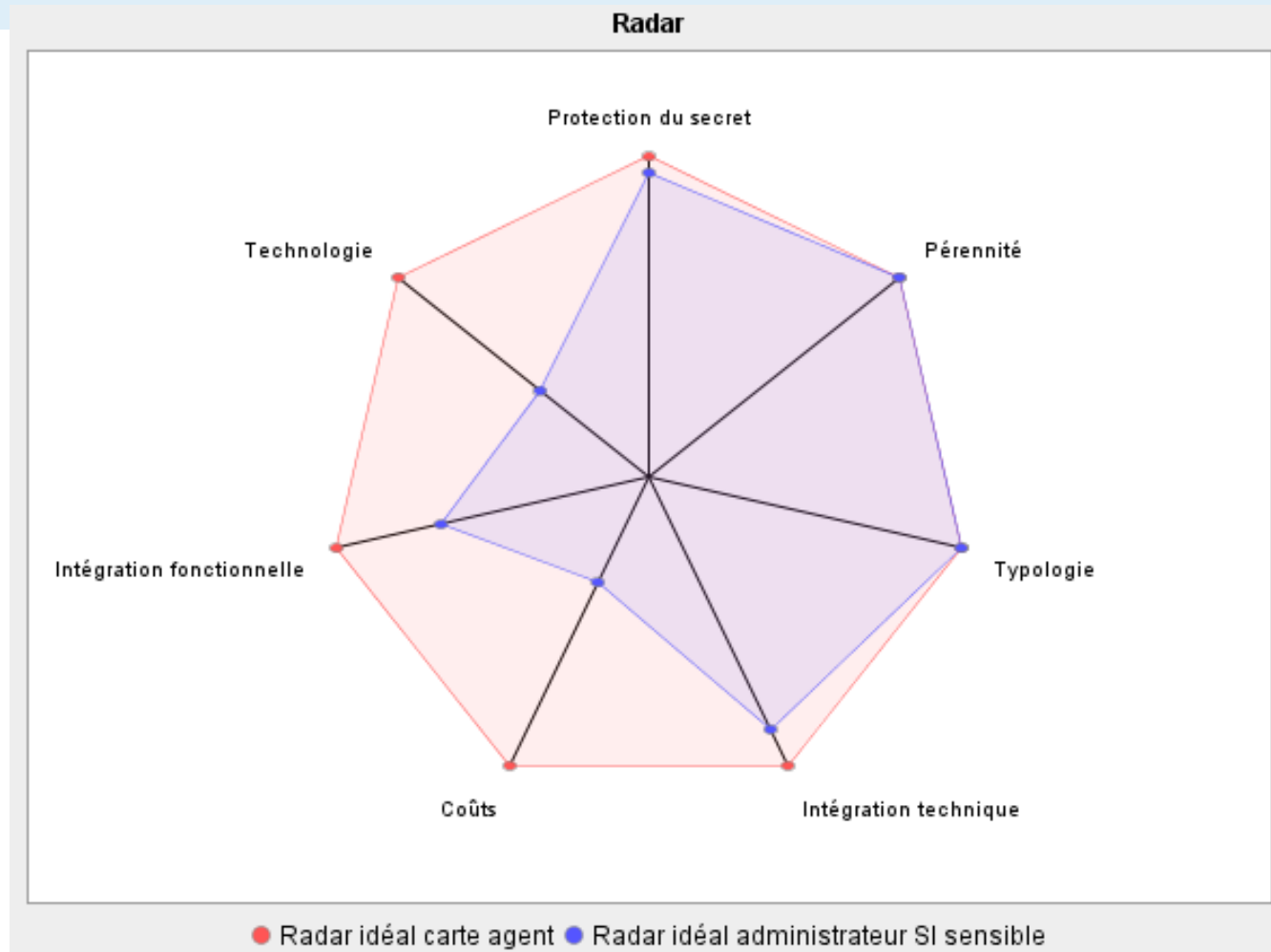
Cas d'authentications renforcées : Cas idéal



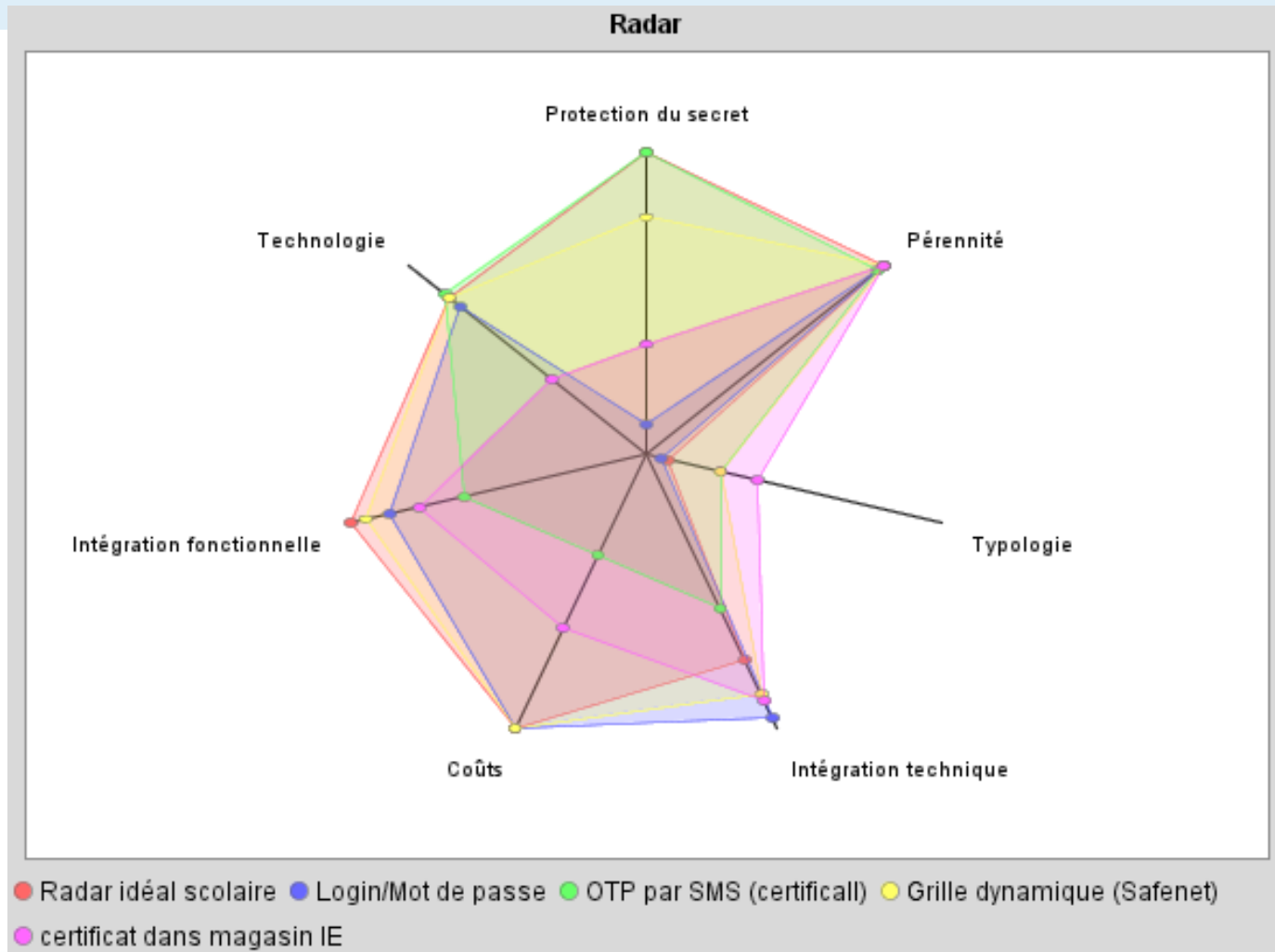
Cas d'authentications renforcées : Cas scolaire



Cas d'authentications renforcées : Cas Administrateur SI sensible



Cas d'authentications renforcées : Comparaison de plusieurs types



Sommaire

- 1 **Rappel JRSSI 2012 : Sécurité des accès périmétriques**
- 2 **Cas d'usage, besoins et contraintes utilisateurs**
- 3 **Critères d'évaluation et cas d'authentications renforcées**
- 4 **Conditions de réalisation et de mise en œuvre**

Conditions de réalisation et de mise en œuvre

De cette étude viennent plusieurs réponses aux questions initiales :

- **Question 3** : Quelle est l'authentification parfaite (pas chère, forte, facile à déployer, pour toutes les groupes d'utilisateurs) ?
- **Question 4** : Et comment fait-on pour doter chaque utilisateur rapidement et sans les difficultés habituelles de déploiement ?
- **Question 5** : Et comment accroche-t-on l'ensemble des applications du SI sur cette nouvelle authentification à l'accès tout en garantissant la continuité de fonctionnement ?

Conditions de réalisation et de mise en œuvre

- **Question 3** : Quelle est l'authentification parfaite (pas chère, forte, facile à déployer, pour toutes les groupes d'utilisateurs) ?

Conditions de réalisation et de mise en œuvre

Réponse 3

- En fonction de la **population** ciblée, les valorisations des critères ne sont pas les mêmes
- Il n'y a donc **pas** de type d'authentification idéal, **unique** pour tous les groupes d'utilisateurs
- Il y a plutôt un **bouquet** d'authentifications renforcées à mettre en œuvre, mettant en jeu plusieurs méthodes d'authentification, ouvrant sur des droits particuliers régis par une politique d'habilitation

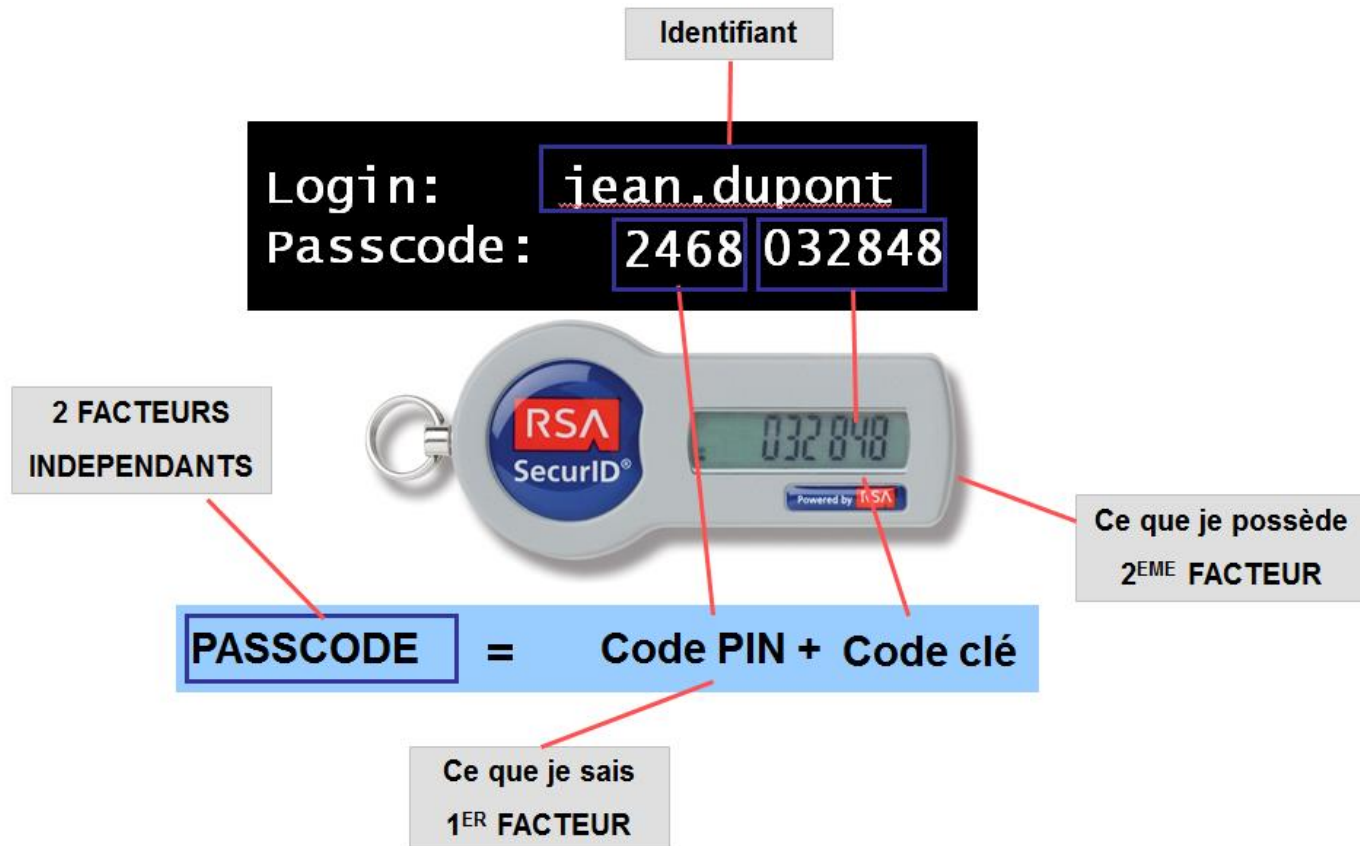


OTP physique

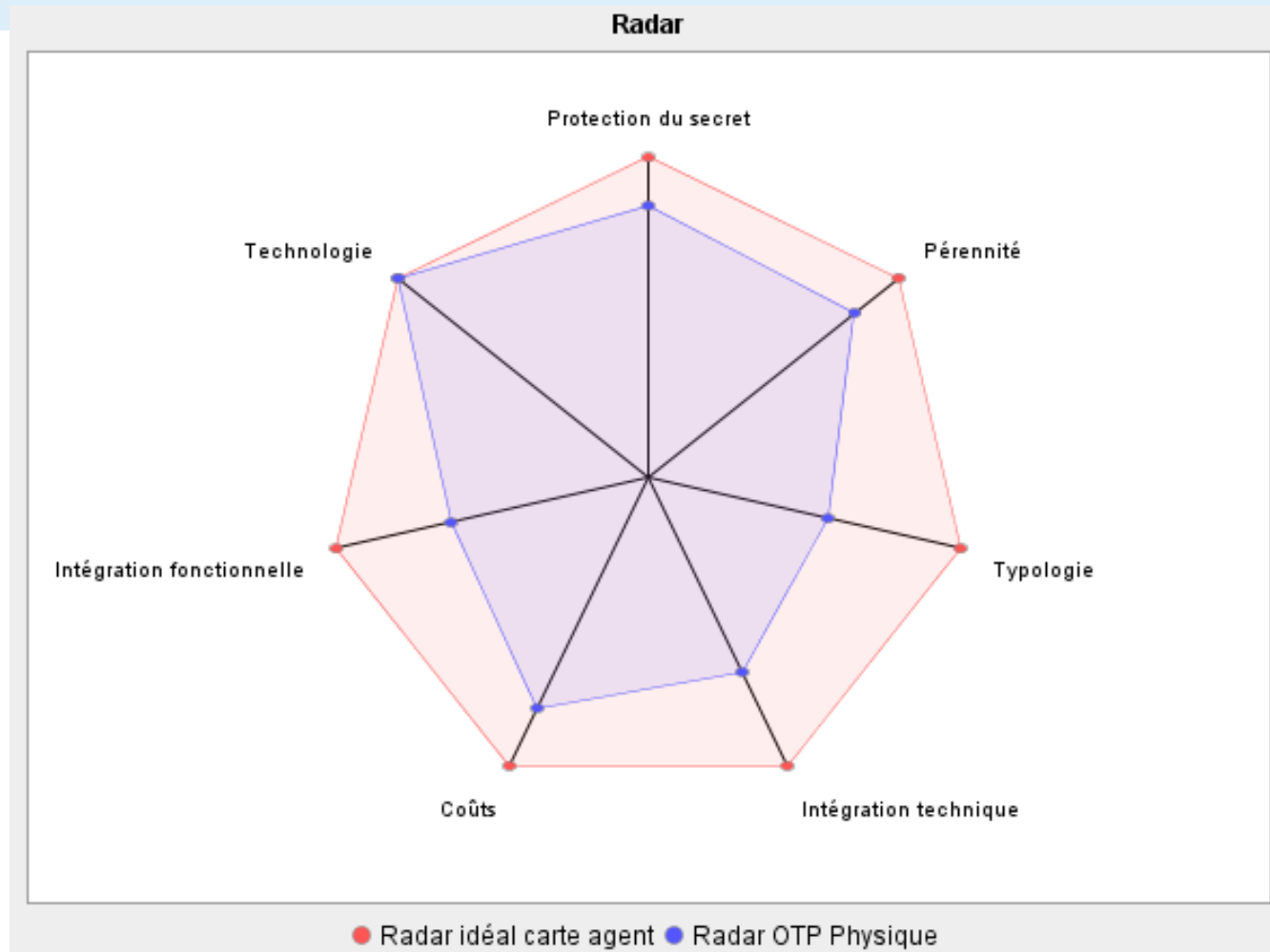
Conditions de réalisation et de mise en œuvre

Réponse 3

Revue des solutions industrielles : OTP physique



Critères d'évaluation et cas OTP physique



Grille dynamique OTP

Conditions de réalisation et de mise en œuvre

Réponse 3

Revue des solutions industrielles : Grille OTP dynamique

			3 rd	4 th
		1 st	2 nd	

1 Schéma secret

3	0	9	7	4
0	4	6	9	6
7	2	0	8	2
1	5	5	5	8
3	2	8	1	1

2 Grille aléatoire

3	0	9	7	4
0	4	6	9	6
7	2	0	8	2
1	5	5	5	8
3	2	8	1	1

3 OTP généré

Conditions de réalisation et de mise en œuvre

Réponse 3

Revue des solutions industrielles : Grille OTP dynamique

Login : gdupont

Mot de passe :

Conditions de réalisation et de mise en œuvre

Réponse 3

Revue des solutions industrielles : Grille OTP dynamique

Login : gdupont

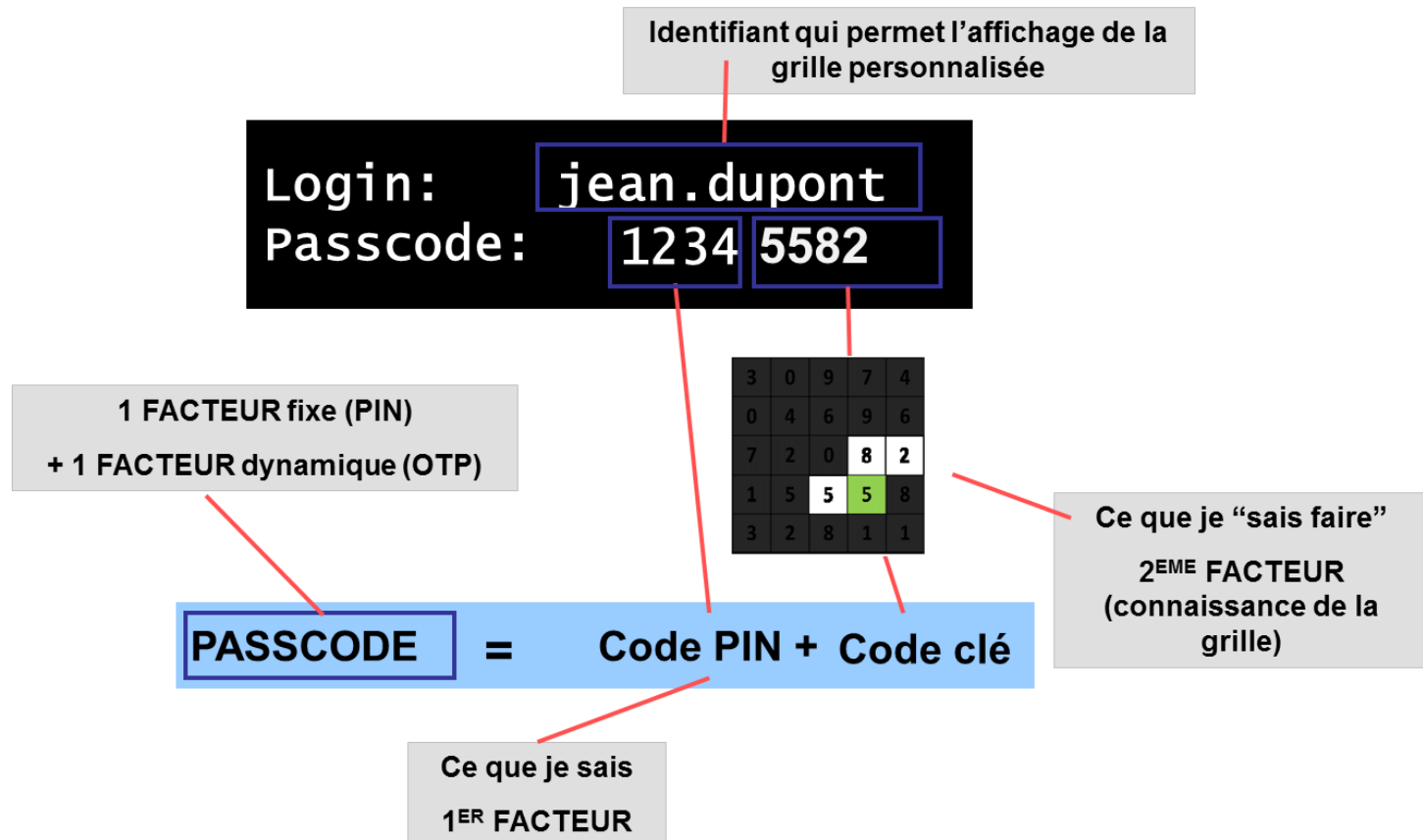
3	0	9	7	4
0	4	6	9	6
7	2	0	8	2
1	5	5	5	8
3	2	8	1	1

Mot de passe :

Conditions de réalisation et de mise en œuvre

Réponse 3

Revue des solutions industrielles : Grille OTP dynamique



Conditions de réalisation et de mise en œuvre

Réponse 3

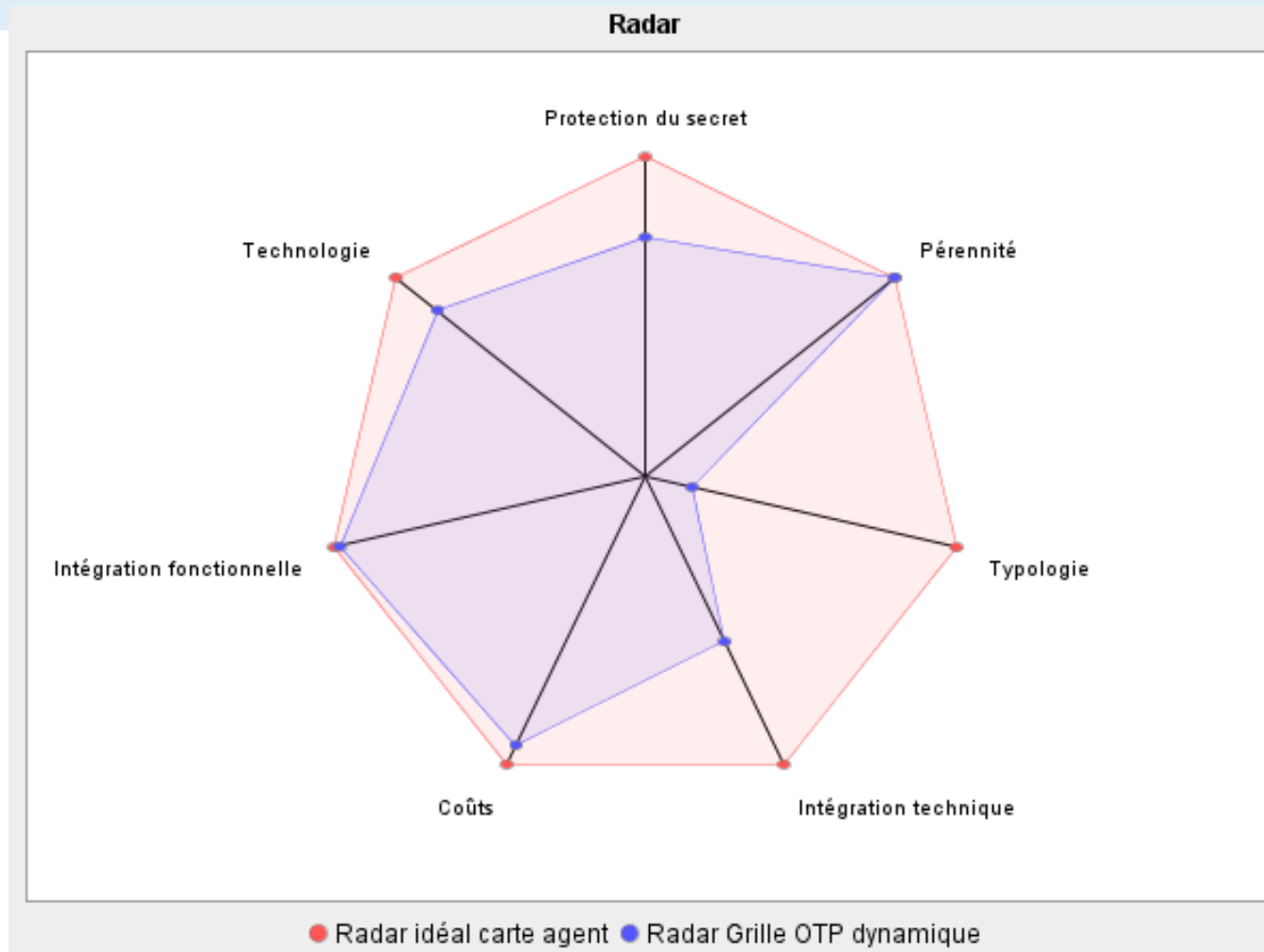
Revue des solutions industrielles : Grille OTP dynamique

Login : gdupont

3	0	9	7	4
0	4	6	9	6
7	2	0	8	2
1	5	5	5	8
3	2	8	1	1

Mot de passe : 1234 5582

Critères d'évaluation et cas Grille OTP dynamique



Carte multi services

Conditions de réalisation et de mise en œuvre

Réponse 3

Revue des solutions industrielles : Carte multiservices

Usage 1 : carte à puce, qualifiée RGS, pour l'authentification, la signature, le chiffrement



Conditions de réalisation et de mise en œuvre

Réponse 3

Revue des solutions industrielles : Carte multiservices

Usage 2 : accès
bâtiment Technologie
RFID 13.56MHz (MIFARE)



Conditions de réalisation et de mise en œuvre

Réponse 3

Revue des solutions industrielles : Carte multiservices

Usage 3 : accès en mode OTP pour l'authentification sans driver et avec saisie du code PIN déporté.



Conditions de réalisation et de mise en œuvre

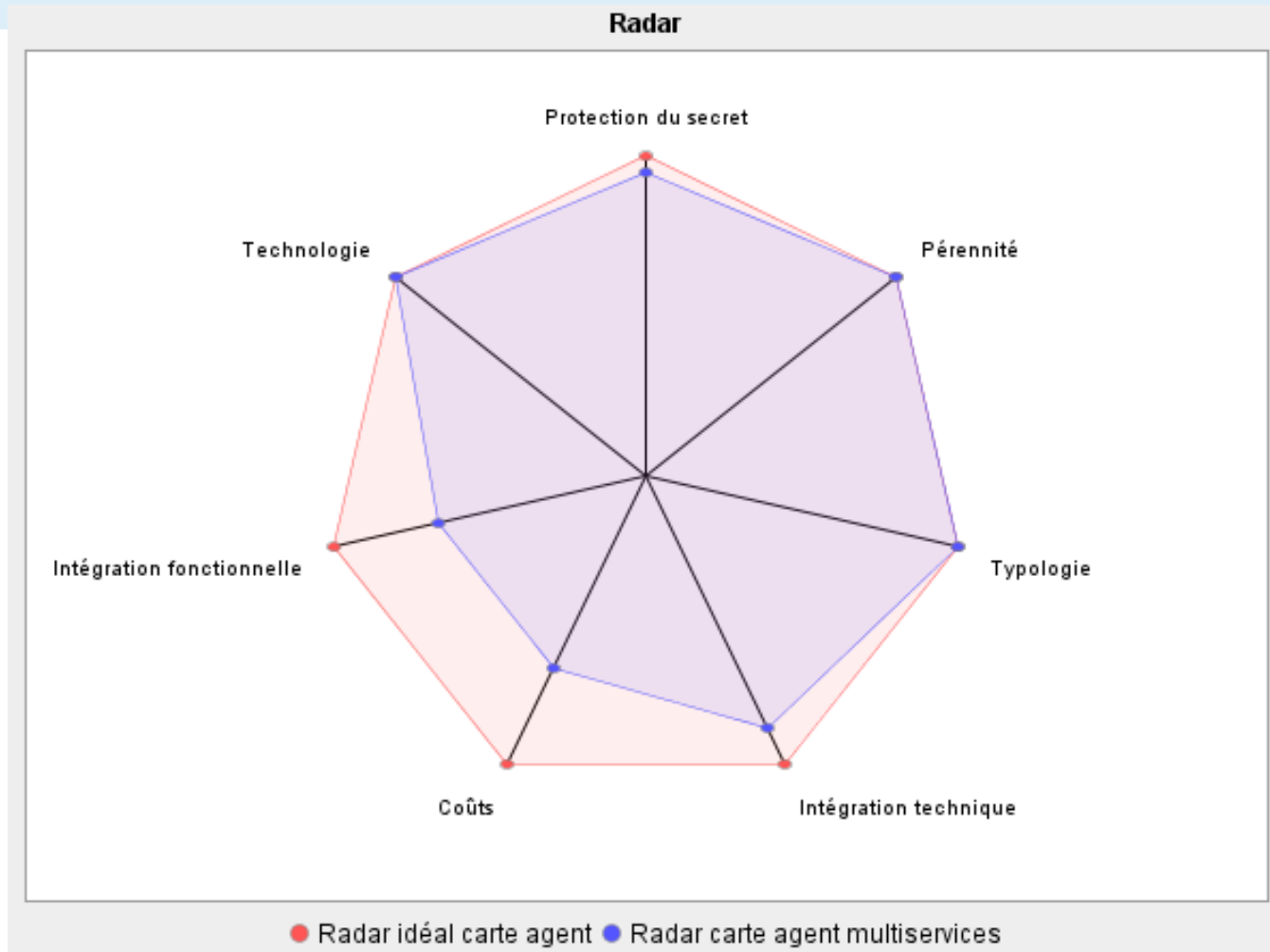
Réponse 3

Revue des solutions industrielles : Carte multiservices

Usage 4 : usages autres –
piste magnétique au verso.
Un numéro de série peut
également être gravé.



Critères d'évaluation et cas carte physique multiservices



Conditions de réalisation et de mise en œuvre

- **Question 5** : Et comment accroche-t-on l'ensemble des applications du SI sur cette nouvelle authentification à l'accès tout en garantissant la continuité de fonctionnement ?

Conditions de réalisation et de mise en œuvre

De cette étude viennent plusieurs enseignements de mise en œuvre:

- Remarque 1 : La mise en place de ce mode d'authentification renforcée ne peut pas se faire en destruction/remplacement de l'existant (mdp, OTP, etc.)
 - Il est quantitativement trop important (250 000 OTP, des millions de mdp)
 - Il rend un service opérationnel en production (OTP = protection des bases élèves)
 - La maîtrise de l'authentification à l'accès passe par le maintien de l'existant en particulier de l'authentification forte
- Remarque 2 : Une architecture duale « authentification renforcée/ authentification traditionnelle » doit donc être mise en place pour effectuer la migration

Conditions de réalisation et de mise en œuvre

- Remarque 3 : Cas d'architecture RADIUS
 - Cette architecture à deux portes, l'une faible, l'autre renforcée, peut permettre de substituer progressivement des applications de même niveau de sensibilité (politique d'habilitation) vers l'authentification renforcée
- Remarque 4 : Cas d'architecture SSO et Fédération d'identité
 - Il suffit d'ajouter une instance de fournisseur d'identité basé sur l'authentification renforcée à côté de la base des mots de passe sur le même périmètre de fédération : les deux portes sont valables tant que les deux bases contiennent les comptes
 - Dans ce cas les remarques 1 et 2 sont respectées

Conditions de réalisation et de mise en œuvre

- **Question 4** : Et comment fait-on pour doter chaque usager rapidement et sans les difficultés habituelles de déploiement pour tout le périmètre applicatif des SI ?
 - Usagers : 13 millions d'étudiants ou d'élèves, 20 millions de référents, 1 million d'enseignants, 300 000 ingénieurs
 - SI : ENT, bases élèves, applications Concours & Examens, bases RH, paye, etc.

Conditions de réalisation et de mise en œuvre

- Des pistes à explorer :
 - Des solutions techniques d'authentification à développer
 - Des lacunes des offres industrielles à combler
 - D'autres techniques à qualifier
 - Par exemple

Pistes à explorées : Grille OTP dynamique revue

			3 rd	4 th
		1 st	2 nd	

1 Schéma secret de gdupont

3	0	9	7	4
0	4	6	9	6
7	2	0	8	2
1	5	5	5	8
3	2	8	1	1

2 Grille aléatoire

3	0	9	7	4
0	4	6	9	6
7	2	0	8	2
1	5	5	5	8
3	2	8	1	1

3 OTP généré

	1 st	2 nd	3 rd	4 th

1 Schéma secret de jdurant

3	0	9	7	4
0	4	6	9	6
7	2	0	8	2
1	5	5	5	8
3	2	8	1	1

2 Grille aléatoire

3	0	9	7	4
0	4	6	9	6
7	2	0	8	2
1	5	5	5	8
3	2	8	1	1

3 OTP généré

Pistes à explorées : Grille OTP dynamique revue

Site web1 de la grille dynamique
(commune à tous)

3	0	9	7	4
0	4	6	9	6
7	2	0	8	2
1	5	5	5	8
3	2	8	1	1

Site web institutionnel 1

Login : gdupont

Mot de passe : 5582

Site web institutionnel 2

Login : jdurant

Mot de passe : 4696

Conclusion :

Des perspectives semblent ouvertes ...

Merci de votre attention