

ANNEXE VII-1 : modèle d'attestation de respect du cahier des charges pour l'épreuve E4 (option SISR)

**BTS SERVICES INFORMATIQUES AUX ORGANISATIONS
Session 2019**

**CONTRÔLE DE L'ENVIRONNEMENT TECHNOLOGIQUE
Cahier des charges national concernant l'épreuve E4 « Conception et maintenance de solutions informatiques »
pour la session 2019 (identique à 2018) : Note de service n° 2017-012 du 19-1-2017 - BO N°7 du 16 février 2017**

<p>Nom et adresse du centre d'examen</p>	<p>Lycée Sidoine Apollinaire 20 rue Jean Richepin 63000 CLERMONT-FERRAND</p>	<p>Cachet et signature du responsable</p>  <p>P.CANTOURNET</p>	<p>SISR</p>
---	---	--	--------------------

Éléments communs obligatoires¹ pour les deux options

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation ²
Service d'authentification	- Microsoft Windows Server 2008 R2 (Active Directory)	
SGBD	- Mysql/phpMyadmin	
Accès sécurisé à Internet	- IPFire	
Environnement de travail collaboratif	- Dossier « partage » sur le serveur du LAN - Dropbox	

¹ Pour la partie commune aux deux spécialités, le cahier des charges national stipule que « 1.6 Lorsque les deux situations professionnelles [...] s'appuient sur deux contextes différents, chaque contexte [...] doit respecter les règles communes aux deux options ». **L'absence d'éléments obligatoires peut faire l'objet d'une sanction applicable aux candidats, pouvant aller jusqu'à -15 points.**

²⁷ enseigner pour les candidats passant l'épreuve sous forme ponctuelle.

Logiciel de gestion d'incidents	- GLPI	
Logiciel de gestion des configurations	- OCS	
Serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents	- Microsoft Windows Server 2008 R2 - Linux Debian - Centos (Eyes Of Network)	
Solution de sauvegarde	- Solution basée sur le serveur 2008	
Ressources dont l'accès est sécurisé et soumis à habilitation	- Mise en place d'une DMZ avec règles de filtrage - Accès Internet (Proxy, règles firewall) - Dossiers personnels (NTFS)	
Deux types de solution technique d'accès dont une mobile	- PC Fixes - PC Portables	

Éléments spécifiques à l'option SISR³

Rappel (extrait du cahier des charges national) : « 1.4 – Les logiciels de simulation ou d'émulation sont utilisés en réponse à des besoins de l'organisation. Ils ne peuvent se substituer à des équipements réels dans l'environnement technologique d'apprentissage. **Une solution d'infrastructure réduite à une simulation par un logiciel ne peut être acceptée.** »

Éléments de base obligatoires

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation ⁴
Un réseau comportant plusieurs périmètres de sécurité	<ul style="list-style-type: none">- LAN- DMZ- INTERNET	
Solution permettant l'administration à distance sécurisée de serveurs	<ul style="list-style-type: none">- Bureau à distance Microsoft avec règles spécifiques sur le firewall IPFire	
Logiciel d'analyse de trames	<ul style="list-style-type: none">- Wireshark	
Logiciel de supervision système et réseau	<ul style="list-style-type: none">- Solution Eyes Of Network	
Trois type de solution techniques d'accès dont une mobile	<ul style="list-style-type: none">- PC Fixes- PC Portables- Tablette	
Un service rendu à l'utilisateur final respectant un contrat de service	<ul style="list-style-type: none">- Mise en place du service Web dans la DMZ avec répartition de charge.	

³ Pour les éléments **spécifiques** à l'option, le cahier des charges national précise « 1.6 [...] Le respect des règles [...] est mesuré à partir du cumul des caractéristiques des deux environnements » (si les deux situations s'appuient sur des contextes différents). »

⁴ À renseigner pour les candidats passant l'épreuve sous forme ponctuelle.

Éléments complémentaires⁵ (au moins 3 parmi les 9)

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation ⁶
Solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet)	<ul style="list-style-type: none"> - Accès Internet (proxy, blacklist...) - Accès LAN depuis l'extérieur (Administrateur) - Accès serveur Web dans la DMZ 	
Solution garantissant la continuité d'un service	<ul style="list-style-type: none"> - Solution HAProxy pour continuité du service Web 	
Solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion	<ul style="list-style-type: none"> - Solution HAProxy assurant la tolérance de panne du serveur Web (avec un 2e serveur Web) 	
Solution permettant la connexion sécurisée entre deux sites distants	<ul style="list-style-type: none"> - OpenVPN 	
Solution permettant le déploiement des solutions techniques d'accès	<ul style="list-style-type: none"> - WDS 	
Solution gérée à l'aide de procédures automatisées écrites avec un langage de <i>scripting</i>	<ul style="list-style-type: none"> - Linux Debian 	
Solution permettant la supervision la qualité, de la sécurité et de la disponibilité des services avec remontées d'alertes	<ul style="list-style-type: none"> - Solution de supervision Eyes Of Network 	
Solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau	<ul style="list-style-type: none"> - Snort sous Pfsense 	
Solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion	<ul style="list-style-type: none"> - Solution HAProxy (répartition de charge paramétrable entre les 2 serveurs web) 	

⁵ 2.2 La structure et les activités de l'organisation s'appuient sur au moins trois solutions d'infrastructures opérationnelles [parmi les 9]

⁶ À renseigner pour les candidats passant l'épreuve sous forme ponctuelle.

ANNEXE VII-2 : modèle d'attestation de respect du cahier des charges de l'épreuve E4 (option SLAM)

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS
Session 2019

CONTRÔLE DE L'ENVIRONNEMENT TECHNOLOGIQUE
Cahier des charges national concernant l'épreuve E4 « Conception et maintenance de solutions informatiques »
pour la session 2019 (identique à 2018) : Note de service n° 2017-012 du 19-1-2017 - BO N°7 du 16 février 2017

<p>Nom et adresse du centre d'examen</p>	<p>Lycée Sidoine Apollinaire 20 rue Jean Richepin 63000 CLERMONT-FERRAND</p>	<p>Cachet et signature du responsable</p>  <p>P.CANTOURNET</p>	<p>SLAM</p>
---	---	--	--------------------

Éléments communs obligatoires⁷ pour les deux options

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation ⁸
Service d'authentification	- Microsoft Windows Server 2008 R2 (Active Directory)	
SGBD	- Mysql/phpMyadmin	
Accès sécurisé à Internet	- IPFire	

⁷ Pour la partie commune aux deux spécialités, le cahier des charges national stipule que « 1.6 Lorsque les deux situations professionnelles [...] s'appuient sur deux contextes différents, chaque contexte [...] doit respecter les règles communes aux deux options ». **L'absence d'éléments obligatoires peut faire l'objet d'une sanction applicable aux candidats, pouvant aller jusqu'à -15 points.**

⁸ À renseigner pour les candidats passant l'épreuve sous forme ponctuelle.

Environnement de travail collaboratif	<ul style="list-style-type: none"> - Dossier « partage » sur le serveur du LAN - Dropbox 	
Logiciel de gestion d'incidents	<ul style="list-style-type: none"> - GLPI 	
Logiciel de gestion des configurations	<ul style="list-style-type: none"> - OCS 	
Serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents	<ul style="list-style-type: none"> - Microsoft Windows Server 2008 R2 - Linux Debian - Centos (Eyes Of Network) 	
Solution de sauvegarde	<ul style="list-style-type: none"> - Solution basée sur le serveur 2008. 	
Ressources dont l'accès est sécurisé et soumis à habilitation	<ul style="list-style-type: none"> - Mise en place d'une DMZ avec règles de filtrage - Accès Internet (Proxy, règles firewall) - Dossiers personnels (Permissions NTFS) 	
Deux types de solution technique d'accès dont une mobile	<ul style="list-style-type: none"> - PC Fixes - PC Portables 	

Éléments spécifiques au option SLAM⁹

Rappel (extrait du cahier des charges national) : « 1.4 – Les logiciels de simulation ou d’émulation sont utilisés en réponse à des besoins de l’organisation. Ils ne peuvent se substituer à des équipements réels dans l’environnement technologique d’apprentissage. **Une solution d’infrastructure réduite à une simulation par un logiciel ne peut être acceptée.** »

Éléments obligatoires

Éléments	Description de l’implantation dans le centre d’examen (nom du service ou de l’outil et caractéristiques techniques)	Remarques de la commission d’interrogation ¹⁰
Environnement(s) de développement : - Un ou deux environnements de développement - disposant d’ outils de gestion de tests , - supportant un <i>framework</i> - et au moins deux langages	<ul style="list-style-type: none">- Framework.net- IDE Visual Studio 2015 Professionnel- Netbeans pour JAVA	
Bibliothèque de composants logiciels	<ul style="list-style-type: none">- Framework.net	
SGBD avec langage de programmation associé	<ul style="list-style-type: none">- MySQL- SQL Server 2012	
Logiciel de gestion de versions	<ul style="list-style-type: none">- GIT- TFS	

⁹ Pour les éléments **spécifiques** à l’option, le cahier des charges national précise « 1.6 [...] Le respect des règles [...] est mesuré à partir du cumul des caractéristiques des deux environnements » (si les deux situations s’appuient sur des contextes différents). »

¹⁰ À renseigner pour les candidats passant l’épreuve sous forme ponctuelle.

Éléments complémentaires¹¹

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Code exécuté sur ¹²				Remarques de la commission d'interrogation ¹³
		3.2.1 le système d'exploitation d'une STA fixe	3.2.2 un navigateur <i>web</i>	3.2.3 le système d'exploitation d'une STA mobile	3.2.4 le système d'exploitation d'un serveur	
Solution applicative N° 1						
Solution applicative N°2						
...						

¹¹ Extrait du cahier des charges : « 3.2 Les activités de l'organisation cliente s'appuient sur **au moins deux solutions applicatives opérationnelles** permettant d'offrir un accès sécurisé à des données hébergées sur un site distant. Au sein des architectures de ces solutions applicatives, doivent figurer l'exploitation de mécanismes d'appel à des services applicatifs distants et au moins trois des situations ci-dessous :

3.2.1 du code exécuté sur le système d'exploitation d'une solution technique d'accès fixe (type client lourd) ;

3.2.2 du code exécuté dans un navigateur *web* (type client léger ou riche, *applet*, etc.) ;

3.2.3 du code exécuté sur le système d'exploitation d'une solution technique d'accès mobile ;

3.2.4 du code exécuté sur le système d'exploitation d'un serveur (*servlet*, procédure cataloguée, etc.).

3.3 Une solution applicative peut être issue d'un développement spécifique ou de la modification du code d'un logiciel (*open source* par exemple).

3.4 **Les solutions applicatives présentes dans le contexte sont opérationnelles et leur code source est accessible dans un environnement de développement opérationnel au moment de l'épreuve.** »

¹² Indiquer une croix si la solution mise en œuvre intègre le type de code indiqué

¹³ À renseigner pour les candidats passant l'épreuve sous forme ponctuelle.

