FINANCES PUBLIQUES

CONCOURS INTERNE
POUR L'ACCÈS AU GRADE D'INSPECTEUR DES FINANCES PUBLIQUES
AFFECTÉ AU TRAITEMENT DE L'INFORMATION EN QUALITÉ D'ANALYSTE

ANNÉE 2023

_____

ÉPREUVE ÉCRITE D'ADMISSIBILITÉ N° 3

Durée : 1 heure 30 – Coefficient : 1

_____

Version anglaise à partir d'un texte issu d'une revue ou d'une documentation informatique

_____

Seuls sont pris en compte les points obtenus au-dessus de 10.

_____

Recommandations importantes

Le candidat trouvera au verso la manière de servir la copie dédiée.

Sous peine d'annulation, en dehors du volet rabattable d'en-tête, les copies doivent être totalement anonymes et ne comporter aucun élément d'identification tels que nom, prénom, signature, paraphe, localisation, initiale, numéro ou toute autre indication, même fictive, étrangère au traitement du sujet.

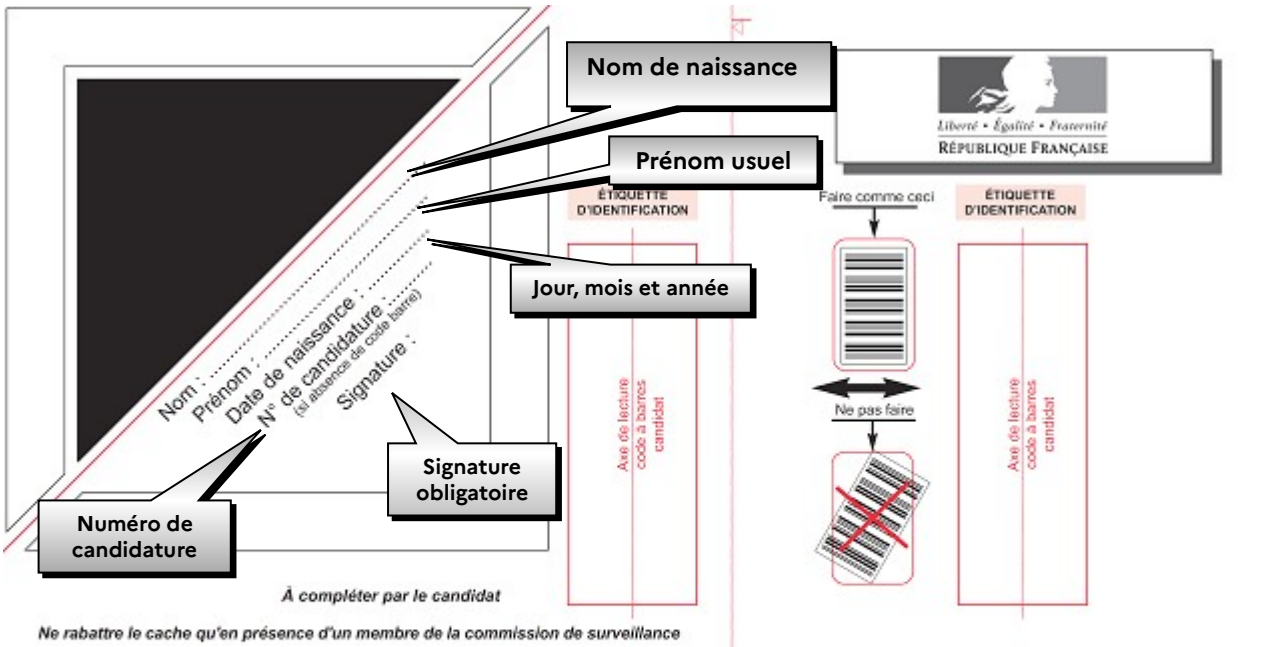
Sur les copies, les candidats devront écrire et souligner si nécessaire au stylo bille, plume ou feutre de couleur noire ou bleue uniquement. De même, l'utilisation de crayon surligneur est interdite.

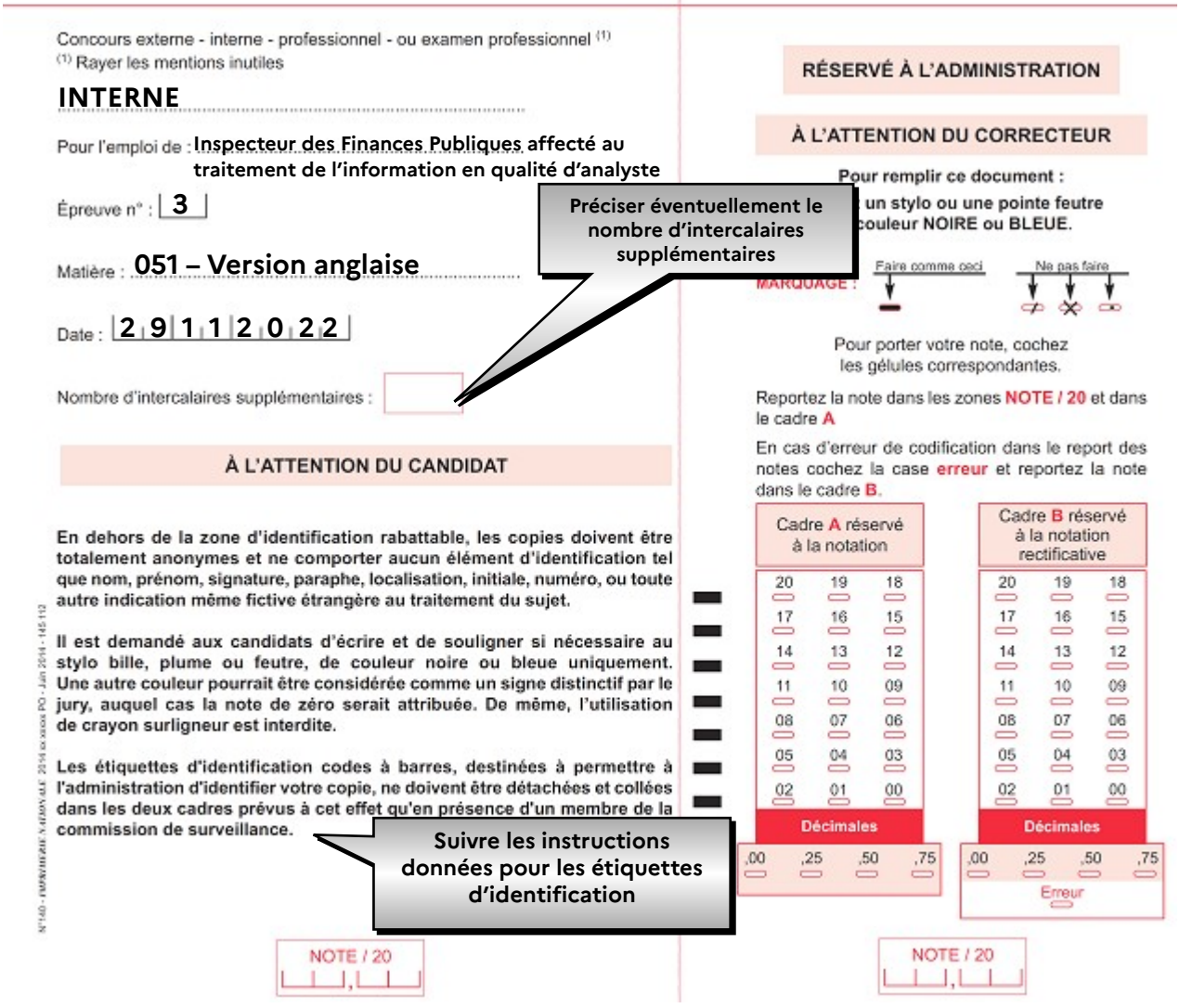
Il devra obligatoirement se conformer aux directives données.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Tournez la page S.V.P.

Le candidat complétera l'intérieur du volet rabattable des informations demandées et se conformera aux instructions données





EN AUCUN CAS, LE CANDIDAT NE FERMERA LE VOLET RABATTABLE AVANT D'Y AVOIR ÉTÉ AUTORISÉ PAR LA COMMISSION DE SURVEILLANCE

FINANCES PUBLIQUES

VERSION ANGLAISE À PARTIR D'UN TEXTE ISSU D'UNE REVUE OU D'UNE DOCUMENTATION INFORMATIQUE

Code matière : 051

Les candidates et les candidats peuvent avoir à leur disposition sur la table de concours le matériel d'écriture, une règle, un correcteur, des surligneurs.

In a remote-work world, a zero-trust revolution is necessary

[...]

Last summer, law enforcement officials contacted both Apple and Meta, demanding customer data in "emergency data requests." The companies complied. Unfortunately, the "officials" turned out to be hackers affiliated with a cyber-gang called "Recursion Team."

Roughly three years ago, the CEO of a UK-based energy company got a call from the CEO of the company's German parent company instructing him to wire a quarter of a million dollars to a Hungarian "supplier." He complied. Sadly, the German "CEO" was in fact a cybercriminal using deepfake audio technology to spoof the other man's voice.

One set of criminals was able to steal data, the other, money. And the reason was trust. The victims' source of information about who they were talking to was the callers themselves.

What is zero trust, exactly?

Zero trust is a security framework that doesn't rely on perimeter security. Perimeter security is the old and ubiquitous model that assumes everyone and everything inside the company building and firewall is trustworthy. Security is achieved by keeping people outside the perimeter from getting in.

A UK doctoral student at the University of Stirling named Stephen Paul Marsh coined the phrase "zero trust" in 1994. (Also called "de-perimeterization," the concept was thoroughly fleshed out in guidelines like Forrester eXtended, Gartner's CARTA and NIST 800-207).

Perimeter security is obsolete for a number of reasons, but mainly because of the prevalence of remote work. Other reasons include: mobile computing, cloud computing and the increasing sophistication of cyberattacks, generally. And, of course, threats can come from the inside, too.

In other words, there is no network edge anymore — not really — and even to the extent that perimeters exist, they can be breached. Once hackers get inside the perimeter, they can move around with relative ease.

Zero trust aims to fix all that by requiring each user, device, and application to individually pass an authentication or authorization test each time they access any component of the network or any company resources.

Tournez la page S.V.P.

Technologies are involved in zero trust. But zero trust itself is not a technology. It's a framework and, to a certain extent, a mindset. We tend to think of it as a mindset for network architects and security specialists. That's a mistake; it needs to be the mindset of all employees.

[...]

Computerworld, April 22, 2022