

Durée : 1h — Documents non autorisés

- 1– a. Qu'est-ce que veut dire l'acronyme « DICP » ? (1pt)
3pts b. Donnez pour chaque terme, dont l'initial fait parti de cet acronyme, la ou les **opérations cryptographiques** qui y sont associées. (2pts)
- 2– Pourquoi les risques sont-ils plus importants dans un **réseau local** que sur **Internet** ?
2pts *Vous indiquerez quels sont les différents risques possibles et, pour chacun de ces risques, sur quelle étape d'une communication il intervient.*
- 3– a. Comment est construite la « **signature électronique** » d'un document ? (1pt)
4pts b. Pourquoi une **personne malveillante ne peut modifier**, ni le document, ni la signature associée, sans que cela ne se remarque lors de la vérification de cette signature ? (1pt)
c. Est-ce qu'une signature électronique est **recevable** lors d'un procès ? (1pt)
d. Est-ce que la signature électronique ne peut être **associée qu'à une personne** ? (1pt)
- 4– a. Pourquoi distingue-t-on deux sortes « **d'actifs** » ? (1pt)
5pts b. Qu'est-ce que l'on entend par « **réduction de risques** » ? (2pts)
Est-ce que cette réduction peut aller jusqu'à l'annulation complète du risque ?
c. Est-ce que tous les risques sont **traités de la même manière** par l'entreprise ? (1pt)
d. Comment déterminer des « **priorités** » pour le traitement des différents risques identifiés ? (1pt)
- 5– a. À partir de votre ordinateur, comment se déroule une communication suivant le « **protocole http** » ? (1pt)
4pts *Vous indiquerez quels sont les opérations réseau que réalise votre ordinateur pour établir la communication.*
b. Quelles opérations supplémentaires s'ajoutent lorsque l'on utilise une communication sécurisée suivant le protocole « **https** » ? (1pt)
c. Pourquoi la mise en place d'une communication sécurisée https peut **échouer** ? (1pt)
d. Est-ce que l'ordinateur que vous utilisez pour communiquer peut-être « **tracé** », c-à-d être suivi et vous identifier de manière certaine ? (1pt)
- 6– Qu'est-ce qu'apporte une **PKI** dans la gestion des risques pour un système d'information ?
2pts *Vous indiquerez ce qu'elle permet et ce sur quoi elle peut intervenir au niveau de l'analyse des risques.*