

Revendications

5

1. Procédé d'authentification mutuelle d'un dispositif (DE) électronique fonctionnel commandable et de son utilisateur (USER) comprenant une phase préliminaire de configuration (SDCP) du dispositif (DE) définissant les modalités de la vérification de son authenticité, l'utilisateur (USER) pouvant ensuite commander le dispositif (DE) afin qu'il lui procure un service déterminé (DS), le dispositif
10 (DE) contenant des données sensibles ou confidentielles (DA) et étant agencé de manière à - dans une phase opérationnelle (OP) déclenchée par l'utilisateur (USER) et incluant une étape préliminaire d'authentification de l'utilisateur (UAP) par le dispositif (DE) -, exécuter une opération spécifique (SO) appropriée pour procurer le service (DS), le procédé comportant, en outre, avant toute phase opérationnelle (OP), une phase préalable d'authentification du dispositif (SDAP) dans laquelle est
15 vérifiée l'authenticité du dispositif (ED), de sorte que :

- si à l'issue de la phase préalable d'authentification du dispositif (SDAP), le dispositif (DE) est avéré authentique, l'utilisateur (USER) peut exécuter la phase opérationnelle (OP),
- si à l'issue de la phase préalable d'authentification du dispositif (SDAP), le dispositif (ED) n'est pas avéré authentique, l'utilisateur (USER) peut empêcher l'exécution de la phase opérationnelle (OP),
20 en sorte que, d'abord le dispositif (DE), puis l'utilisateur (USER), sont authentifiés et que l'opération exécutée et le service (DS) procuré sont sécurisés.

25

2. Procédé selon la revendication 1, dans lequel la phase préalable d'authentification du dispositif (SDAP) est exécutée par l'utilisateur (USER).

3. Procédé selon l'une des revendications 1 et 2, qui comporte dans le temps plusieurs phases opérationnelles (OP), dans lequel une phase préalable d'authentification du dispositif (SDAP) est exécutée avant chaque phase opérationnelle (OP).

30 4. Procédé selon l'une des revendications 2 et 3 en ce qu'elle dépend de la revendication 2, dans lequel la phase préalable d'authentification du dispositif (SDAP) par l'utilisateur (USER), repose sur un processus d'authentification question-réponse, moyennant un secret d'authentification du dispositif (SDAS) qui est une question préalable (PQ) de l'utilisateur (USER) au dispositif (DE) et une réponse préalable (PA) du dispositif (DE) à l'utilisateur (USER) à la question préalable (PQ), la question
35 préalable (PQ) et la réponse préalable (PR) étant secrètes pour n'être connues ou accessibles que du seul utilisateur (USER) authentique, de sorte que l'authenticité du dispositif (DE) n'est avérée que si et seulement si l'utilisateur (USER) vérifie qu'il y a identité entre, d'une part, la réponse apportée (ADS) par le dispositif (DE) à la question préalable (PQ) et d'autre part la réponse préalable (PA).

5. Procédé selon l'une des revendications 1 à 4, dans lequel la phase préliminaire de configuration (SDCP) configure le dispositif (ED) avec le secret d'authentification du dispositif (SDAS).

5 6. Procédé selon la revendication 5, dans lequel la phase préliminaire de configuration (SDCP) du dispositif (DE) est exécutée par l'utilisateur (USER).

7. Procédé selon l'une des revendications 5 et 6 en ce qu'elle dépend de la revendication 5, tel que la configuration du dispositif (DE) avec la question préalable (PQ) et la réponse préalable (PA) est
10 exécutée à partir d'une question de l'utilisateur (USER), grâce à un processus générateur de question à réponse.

8. Procédé selon l'une des revendications 5 à 7 en ce qu'elles dépendent de la revendication 5, dans lequel la phase préalable d'authentification du dispositif (SDAP) est exécutée après que la phase
15 préliminaire de configuration (SDCP) a été exécutée, et sous la condition de l'absence d'exécution, entre temps, de toute autre phase préalable d'authentification du dispositif (SDAP) ou d'une phase opérationnelle (OP).

9. Procédé selon l'une des revendications 5 à 7 en ce qu'elles dépendent de la revendication 5, dans lequel la phase préalable d'authentification du dispositif (SDAP) est exécutée après que la phase
20 préliminaire de configuration (SDCP) a été exécutée, et sous la condition de l'exécution entre temps, d'une ou de plusieurs autres phases préalables d'authentification du dispositif (SADP) ou de phases opérationnelles (OP).

10. Procédé selon l'une des revendications 5 à 7 en ce qu'elles dépendent de la revendication 5, dans lequel à une phase préliminaire de configuration (SDCP) est associée de façon nécessaire et suffisante soit une seule phase préalable d'authentification du dispositif (SDAP) soit une pluralité préfixée de phases préalables d'authentification du dispositif (SDAP) successives soit une pluralité illimitée de phases préalables d'authentification du dispositif (SDAP) successives.
25

11. Procédé selon l'une des revendications 1 à 10, dans lequel l'étape préliminaire d'authentification de l'utilisateur (UAP) par le dispositif (DE) repose sur un secret d'authentification de l'utilisateur (UAS) qui est une réponse opérationnelle de l'utilisateur (OA) au dispositif (DE), secrète pour n'être connue et accessible que du seul utilisateur (USER) authentique, de sorte que l'authenticité de l'utilisateur
35 (USER) n'est avérée que si et seulement si le dispositif (DE) vérifie qu'il y a identité entre, d'une part, la réponse apportée par l'utilisateur (AU) et, d'autre part, la réponse opérationnelle (OA).

12. Procédé selon l'une des revendications 4 à 11 en ce qu'elles dépendent de la revendication 4, dans lequel la question préalable (PQ) et la réponse opérationnelle (OA) sont différentes.

13. Procédé selon l'une des revendications 1 à 12, qui comprend une étape de suppression des données sensibles ou confidentielles (DA) du dispositif (DE), exécutée automatiquement à l'issue d'un nombre
5 préfixé d'exécution de phases préalables d'authentification du dispositif (SDAP) successives où le dispositif (DE) n'est pas avéré authentique.

14. Procédé selon la revendication 13 dont l'étape de suppression des données sensibles ou confidentielles (DA) du dispositif (DE) efface également la question préalable (PQ) et la réponse
10 préalable (PA) lorsque à l'issue d'un nombre préfixé d'exécution de phases préalables d'authentification du dispositif ou du système SDAP successives, l'utilisateur USER a échoué à fournir la question préalable (PQ) correspondant à la réponse préalable (PA), de telle sorte le dispositif ED ou le système ES considérera que l'utilisateur n'est pas l'utilisateur authentique.

15. Procédé d'exploitation par un utilisateur (USER) d'un dispositif (DE) électronique fonctionnel commandable par l'utilisateur (USER) afin qu'il lui procure un service déterminé (DS), le dispositif (DE) contenant des données sensibles ou confidentielles (DA), dans lequel - dans une phase opérationnelle (OP) déclenchée par l'utilisateur (USER) et incluant une étape préliminaire d'authentification de l'utilisateur (UAP) par le dispositif (DE) -, le dispositif (DE) exécute une
20 opération spécifique (SO) appropriée pour procurer le service (DS), le procédé d'exploitation étant caractérisé en ce qu'il comporte, en outre, avant toute phase opérationnelle (OP), une phase préalable d'authentification du dispositif (SDAP) dans laquelle est vérifiée l'authenticité du dispositif (DE), de sorte que :

- si à l'issue de la phase préalable d'authentification du dispositif (SDAP), le dispositif (DE) est
25 avéré authentique, l'utilisateur (USER) peut exécuter la phase opérationnelle (OP),
- si à l'issue de la phase préalable d'authentification du dispositif (SDAP), le dispositif (DE) n'est pas avéré authentique, l'utilisateur (USER) peut empêcher l'exécution de la phase opérationnelle (OP), en sorte que, d'abord le dispositif (DE), puis l'utilisateur (USER), sont authentifiés et que l'opération exécutée et le service (DS) procuré sont sécurisés.

30

16. Dispositif (DE) électronique fonctionnel, commandable par un utilisateur (USER) en vue d'un service déterminé (DS), contenant des données sensibles ou confidentielles (DA), spécialement agencé pour la mise en œuvre du procédé d'authentification mutuelle selon l'une quelconque des revendications 1 à 13 et pour la mise en œuvre du procédé d'exploitation selon la revendication 15,
35 notamment pour exécuter une phase préalable d'authentification du dispositif (SDAP).

17. Dispositif (DE) selon la revendication 16, configuré à l'issue d'une phase préliminaire de configuration (SDCP) avec le secret d'authentification du dispositif (SDAS), qui est une question

préalable de l'utilisateur (PQ) au dispositif (DE) et une réponse préalable du dispositif (PA) à l'utilisateur (USER) à la question préalable (PQ).

- 5 18.Dispositif (DE) selon la revendication 16, comprenant, d'une part, le secret d'authentification du dispositif (SDAS) et, d'autre part, le secret d'authentification de l'utilisateur (UAS).

- 10 19.Procédé d'authentification mutuelle d'un système (ES) électronique fonctionnel, commandable par un utilisateur (USER) en vue d'un service déterminé (DS), contenant des données sensibles ou confidentielles (DA), comprenant une pluralité de dispositifs (DE) électroniques associés fonctionnellement entre eux, agencé de manière à - dans une phase opérationnelle (OP) déclenchée par l'utilisateur (USER) et incluant une étape où le système (ES) authentifie l'utilisateur (USER) -, exécuter une opération (SO) ou une série d'opérations (SO) spécifique appropriée pour procurer le service (DS), le procédé comportant, en outre, avant toute phase opérationnelle (OP), une phase
15 préalable d'authentification du système (ES), dans laquelle est vérifiée l'authenticité de tout ou partie de la pluralité des dispositifs (DE) que le système (ES) comprend, moyennant la mise en œuvre, pour chaque dispositif (DE) vérifié, du procédé d'authentification selon l'une des revendications 1 à 13.

- 20 20.Procédé selon la revendication 19, avec une pluralité de dispositifs (DE) électroniques formant une ou plusieurs chaînes fonctionnelles avec un ou des dispositifs (DE) amont et un ou des dispositifs (DE) aval, dans lequel :
- si à l'issue de la phase préalable d'authentification d'un dispositif (DE) amont d'une chaîne de dispositifs (DE), ce dispositif (DE) est avéré authentique, il est procédé à l'authentification du ou des dispositifs (DE) aval de la même chaîne de dispositifs (DE),
 - 25 - si à l'issue de la phase préalable d'authentification d'un dispositif (DE) amont d'une chaîne de dispositifs (DE), ce dispositif (DE) n'est pas avéré authentique, il n'est pas procédé à l'authentification du ou des dispositifs (DE) aval de la même chaîne de dispositifs (DE), le système (ES) étant avéré non authentique.

- 30 21.Procédé d'exploitation par un utilisateur (USER) d'un système (ES) électronique fonctionnel commandable par l'utilisateur (USER) afin qu'il lui procure un service déterminé (DS), le système (ES) contenant des données sensibles ou confidentielles (DA), comprenant une pluralité de dispositifs (DE) électroniques associés fonctionnellement entre eux, dans lequel - dans une phase opérationnelle (OP) déclenchée par l'utilisateur (USER) et incluant une étape préliminaire d'authentification de l'utilisateur (UAP) par le système (ES) -, le système (ES) exécute une opération (SO) ou une série
35 d'opérations (SO) spécifique appropriée pour procurer le service (DS), le procédé d'exploitation étant caractérisé en ce qu'il comporte, en outre, avant toute phase opérationnelle (OP), une phase préalable d'authentification du système (SDAP) dans laquelle est vérifiée l'authenticité de tout ou partie de la pluralité des dispositifs (DE) que le système (ES) comprend, moyennant la mise en œuvre, pour

chaque dispositif (DE) vérifié, du procédé d'authentification selon l'une des revendications 1 à 13, de sorte que :

- si à l'issue de la phase préalable d'authentification du système (ES), le système (ES) est avéré authentique, l'utilisateur (USER) peut exécuter la phase opérationnelle (OP),
- si à l'issue de la phase préalable d'authentification du système (ES), le système (ES) n'est pas avéré authentique, l'utilisateur (USER) peut empêcher l'exécution de la phase opérationnelle (OP), en sorte que d'abord le système (ES) puis l'utilisateur (USER) sont authentifiés et que l'opération exécutée (SO) et le service (DS) procuré sont sécurisés.

10

22. Système (ES) électronique fonctionnel, commandable par un utilisateur (USER) en vue d'un service déterminé (DS), contenant des données sensibles ou confidentielles (DA), comprenant une pluralité de dispositifs (DE) électroniques associés fonctionnellement entre eux, selon l'une des revendications 16 à 18, spécialement agencé pour la mise en œuvre du procédé d'authentification mutuelle selon l'une des revendications 19 et 20 et pour la mise en œuvre du procédé d'exploitation selon la revendication 21, notamment pour exécuter une phase préalable d'authentification (SDAP) de tout ou partie de la pluralité des dispositifs (DE) que le système (ES) comprend.

20