STRUCTURE COMMUNE DU PROGRAMME D'ENSEIGNEMENT ET CADRE D'ÉVALUATION

Répartition standardisée des unités et alignement technique sur le cadre DigComp pour la sécurité numérique des élèves du secondaire

Lot de travail 2. Activité 1.

Titre du projet	SONET : Bien-être et sécurité des seniors sur Internet
Programme	Erasmus+ KA220-ADU
Convention de subvention	2025-1-PL01-KA220-ADU-000364406

Co-funded by the European Union

Numéro de version	1.0
Numéro d'activité	WP2.A1_ CADRE PÉDAGOGIQUE
Partenaire chef de file	Institut de technologie de Karlsruhe (KIT), Allemagne
Date	juin 2026
Tâche	Tâche 2.1 : Élaboration du cadre pédagogique, de la carte des compétences et du programme d'études commun
Type de document	Livrable du projet / Rapport
Résumé	Dans le prolongement direct de la recherche de référence exhaustive et des conclusions transnationales présentées lors de la première phase, ce rapport met en œuvre ces connaissances empiriques en établissant l'architecture structurelle et le cadre d'évaluation du programme d'études commun SONET. Conçu pour combler le « déficit d'autonomie » chez les seniors, il détaille une charge de travail standardisée de 12 heures, divisée en quatre modules fondamentaux de 3 heures chacun (sécurité générale, cybersécurité, éducation aux médias et technologies d'assistance à l'autonomie à domicile). Chaque module intègre des ressources multimodales, des jeux de simulation interactifs en bac à sable et un cadre d'auto-évaluation quantitative composé de 15 questions. Enfin, ce cadre établit une correspondance systématique entre les 10 acquis d'apprentissage cibles et les normes officielles du Cadre européen des compétences numériques pour les citoyens (DigComp), afin de garantir la validité transfrontalière et la transférabilité institutionnelle au sein de l'UE.

Table des matières

Table des matières 2
1 3
2 6
3 7
3.1 7
3.2 10
3.3 15
3.4 16
3.5 17
3.6 17
3.7 18
3.8 18
3.9 18
4 20
4.1 20
4.2 20
5 24
6 25

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

1 RÉSUMÉ

S'appuyant directement sur la recherche de référence exhaustive et les conclusions transnationales présentées dans le livrable précédent, ce document transpose ces connaissances empiriques en un écosystème éducatif structuré et adapté aux seniors. Alors que les sociétés européennes sont confrontées à des défis parallèles liés à la numérisation totale des services et au vieillissement démographique accéléré, la recherche de référence a mis en évidence un grave « déficit d'autonomie », où la possession quasi universelle d'appareils numériques chez les personnes âgées se heurte à des compétences fonctionnelles fragiles. Pour combler ce fossé, ce cadre transforme la formation traditionnelle aux TIC en un parcours d'apprentissage accompagnant, au rythme lent et hautement répétitif, conçu pour favoriser la sécurité numérique et la souveraineté numérique à long terme à travers l'Europe.

Ce livrable formalise l'architecture structurelle, la répartition en unités et les paramètres d'évaluation du programme d'enseignement commun SONET. Le programme de formation s'articule autour de quatre modules thématiques principaux, chacun développé et animé par un partenaire dédié du projet :

Module 1 : Sécurité générale (dirigé par PARASOL) – Couvrant la prise de conscience de la situation, le fonctionnement de base des appareils et la prévention quotidienne des menaces.

Module 2 : Cybersécurité (dirigé par E-SENIORS) – Axé sur la protection des données personnelles, la gestion des mots de passe et la détection du hameçonnage.

Module 3 : Éducation aux médias (dirigé par BLSH) – Développement de l'esprit critique, détection des fausses informations et évaluation de l'IA et des deepfakes.

Module 4 : Technologies d'assistance à l'autonomie à domicile (AAD) (dirigé par KIT) – Présentation des capteurs de sécurité pour la maison connectée, des configurations SOS portables et des outils favorisant le vieillissement autonome à domicile.

Le programme établit un modèle de charge de travail standardisé et équilibré, d'exactement 3 heures par module, pour un programme de formation complet de 12 heures. Afin de répondre à la diversité des préférences d'apprentissage, chaque module intègre 1,5 heure de présentation structurée (environ 40 diapositives)

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

enrichie de composants multimédias, notamment un podcast audio d'expert de 20 minutes et une interview vidéo d'un spécialiste du domaine de 20 minutes. La consolidation active des compétences est renforcée par un jeu de simulation interactif de 30 minutes, hébergé sur la plateforme SONET E-Tool, adaptée aux seniors.

La rétention des connaissances et l'adaptation comportementale sont évaluées à l'aide d'un cadre d'auto-évaluation quantitatif rigoureux. Chaque module comporte exactement 15 questions à choix multiples formulées de manière positive (5 questions par unité) afin d'éviter toute confusion linguistique. Ce corpus d'évaluation est réparti de manière équilibrée entre trois niveaux de difficulté distincts : connaissances fondamentales (40 %), contexte des compétences appliquées (40 %) et tâches pratiques basées sur des scénarios (20 %), fournissant un retour explicatif immédiat pour renforcer les habitudes de sécurité en ligne.

Afin de garantir la validité institutionnelle et une transférabilité transfrontalière sans heurts au sein de l'Union européenne, les 10 acquis d'apprentissage fondamentaux sont systématiquement mis en correspondance avec les normes officielles du Cadre européen des compétences numériques pour les citoyens (DigComp), contribuant directement au domaine 1 (maîtrise de l'information), au domaine 2 (communication), au domaine 4 (sécurité) et au domaine 5 (résolution de problèmes). En fin de compte, ce cadre offre un modèle pédagogique évolutif et validé qui transforme les formateurs d'adultes en « pilotes numériques » capables de dissiper l'anxiété liée à la technologie et d'assurer un vieillissement à domicile en toute sécurité.

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

Figure 1 : CADRE SONET

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

2 INTRODUCTION ET GRANDES TENDANCES

Dans les cinq pays européens partenaires participant au projet SONET, à savoir la Pologne, l'Espagne, la France, l'Allemagne et la Roumanie, les secteurs de la formation des adultes et de l'inclusion numérique sont actuellement remodelés par des macro-tendances convergentes. Celles-ci comprennent le vieillissement démographique rapide, la dématérialisation croissante des administrations publiques et la complexité grandissante des risques de sécurité hybrides, à la fois numériques et physiques. Dans ces cinq pays, la part de la population âgée de 65 ans et plus a déjà dépassé ou approche rapidement le seuil critique de 20 %.

Alors que les politiques nationales de transformation numérique visent universellement à favoriser l'inclusion sociale et civique, les personnes âgées sont contraintes de naviguer dans un environnement complexe caractérisé par des menaces sophistiquées en matière de cybersécurité, une fraude financière omniprésente et un isolement social profond.

Les conditions de mise en œuvre nationales, les cadres institutionnels et les écosystèmes culturels diffèrent structurellement au sein du consortium :

- La France privilégie une approche pilotée par l'État et médiatisée par des acteurs humains grâce à son réseau national de conseillers numériques, parallèlement à des réponses institutionnelles structurées face à l'« abus de faiblesse ».

- L'Allemagne aborde la transition numérique avec une culture profondément axée sur la protection des données (Datenschutz) et s'appuie considérablement sur son réseau très ancré d'associations (Vereine).

- L'Espagne évolue dans un contexte de forte pénétration des appareils mobiles mais de capacités fonctionnelles inégales, et lutte contre un volume élevé de cybercriminalité grâce à des cadres institutionnels solides tels que le Plan Mayor Seguridad.

- La Pologne s'appuie sur des structures familiales intergénérationnelles résilientes pour combler les lacunes en matière de compétences numériques, en déployant activement des campagnes citoyennes et institutionnelles pour lutter contre les escroqueries par ingénierie sociale largement répandues.

- La Roumanie est confrontée à d'importants défis structurels, notamment un taux de participation historiquement bas des adultes à la formation tout au long de la vie et un fossé marqué entre zones urbaines et rurales ; elle s'appuie fortement sur des interventions menées par des ONG pour atténuer les risques croisés liés à la fraude numérique et à la sécurité.

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

3 PROGRAMME D'ENSEIGNEMENT COMMUN, STRUCTURES DES UNITÉS ET CADRE D'ÉVALUATION

3.1 Architecture du programme d'études et paramètres de charge de travail

Le programme commun SONET est organisé de manière systématique en quatre modules thématiques, accessibles via une plateforme en ligne interactive (E-Tool) complétée par des ressources multimédias. Afin de répondre à la diversité des préférences d'apprentissage, chaque module comprend des présentations structurées (environ 40 diapositives par module), un épisode de podcast audio animé par un expert, un entretien enregistré avec un spécialiste de terrain (par exemple, un agent de prévention de la police, un analyste en cybersécurité), des quiz d'auto-évaluation et un jeu de simulation interactif dédié.

Le programme établit un modèle de charge de travail standardisé et équilibré afin de garantir une certaine flexibilité, qu'il s'agisse de formations courtes, de séries d'ateliers ou de parcours d'apprentissage mixte :

- Contenu pédagogique et lecture des présentations (1,5 heure par module)
- Écoute du podcast (20 minutes par module)
- Visionnage de l'entretien avec un expert (20 minutes par module)
- Jeu éducatif interactif (30 minutes par module)
- Quiz d'auto-évaluation et de réflexion (20 minutes par module)
- Cela représente une charge de travail estimée à **3 heures par module**, soit un total d'environ **12 heures pour l'ensemble du programme de formation**.

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

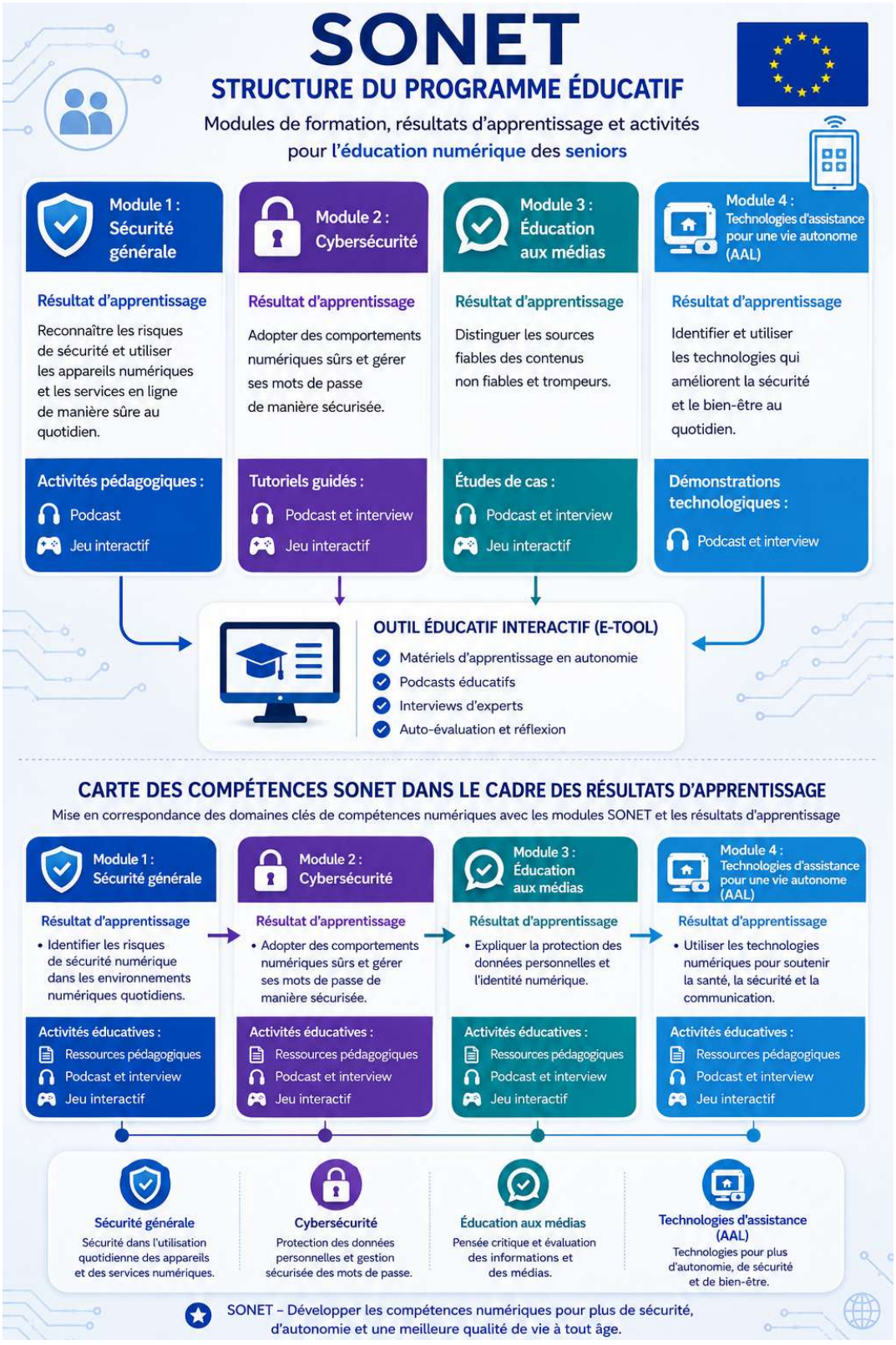

Figure 2 : *Structure du programme SONET et cadre de cartographie des compétences pour la formation numérique des seniors.*

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

MODULE	OBJECTIFS D'APPRENTISSAGE	ACTIVITÉS PÉDAGOGIQUES	COMPOSANTES MULTIMÉDIA	COMPOSANTE INTERACTIVE	RÉSULTATS D'APPRENTISSAGE	CHARGE DE TRAVAIL
Module 1 : Sécurité générale	Comprendre les risques liés à la sécurité dans les environnements numériques du quotidien.	Présentation pédagogique, discussion guidée, exercices pratiques.	Podcast avec un expert en sécurité, entretien avec un spécialiste de la prévention de la police.	Jeu interactif permettant d'identifier les fraudes et les communications suspectes.	Les apprenants identifient les risques liés à la sécurité et utilisent les appareils numériques en toute sécurité.	Environ 3 heures
Module 2 : Cybersécurité	Protection des données personnelles et de l'identité numérique.	Tutoriels étape par étape, exercices sur les mots de passe, démonstrations de connexion sécurisée.	Podcast avec un spécialiste de la cybersécurité, entretien avec un expert.	Jeu de simulation permettant de détecter les tentatives d'hameçonnage et de fraude.	Les apprenants adoptent un comportement numérique sûr et gèrent leurs mots de passe en toute sécurité	Environ 3 heures
Module 3 : Éducation aux médias	Évaluation des informations en ligne et identification des	Études de cas, discussions de groupe, analyse de contenus en ligne.	Podcast sur la désinformation et les médias numériques, entretien avec un expert.	Jeu permettant de distinguer les informations fiables de celles qui sont trompeuses.	Les apprenants distinguent les sources crédibles des contenus non fiables.	Environ 3 heures

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

	fausses informations.					
Module 4 : Technologies d'assistance à l'autonomie à domicile (AAL)	Utilisation des technologies favorisant l'autonomie.	Démonstrations de technologies d'assistance, exercices pratiques avec des appareils.	Podcast sur les technologies de santé numériques, entretien avec un spécialiste de l'AAL.	Simulation explorant la maison connectée et les appareils d'assistance.	Les apprenants identifient et utilisent des technologies qui améliorent la sécurité et le bien-être.	Environ 3 heures

Tableau 3 - Structure du module et correspondance des activités

3.2 Décomposition détaillée des unités et des thèmes

MODULE 1 : Sécurité générale (animé par le partenaire : PARASOL)

Introduction : ce module présente aux seniors les risques liés à la sécurité au quotidien, tant dans l'environnement physique que numérique. Il vise à renforcer la conscience situationnelle et les compétences en matière de sécurité personnelle, afin d'aider les seniors à réagir avec assurance face à des situations potentiellement risquées, à des comportements suspects et aux interactions avec des inconnus.

Unité 1 : Comprendre les risques liés à la sécurité au quotidien

Unité 2 : Utilisation sécurisée des appareils numériques

Unité 3 : Reconnaître les fraudes et les communications suspectes

UNITÉ	THÈMES ABORDÉS	CONTENU PRINCIPAL ET PORTÉE	ÉLÉMENT INTERACTIF
Unité 1	Risques courants pour la sécurité des personnes âgées ; Escroqueries ciblant les personnes âgées ; Situations suspectes dans la vie	Explication des escroqueries courantes ; Exemples de situations réelles ; Listes de contrôle de sécurité.	Discussion de scénarios : que feriez-vous dans cette situation ?

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

	quotidienne ; Conscience situationnelle.		
Unité 2	Sécurité de base des appareils ; utilisation sécurisée des smartphones et des tablettes ; connexion à des réseaux Wi-Fi sécurisés ; identification des sites web fiables.	Guides d'utilisation étape par étape ; Conseils pour une navigation sécurisée ; Bonnes pratiques en matière de messagerie.	Exercices pratiques sur les appareils
Unité 3	Escroqueries par téléphone ; Messages de hameçonnage ; SMS et e-mails frauduleux ; Tactiques de manipulation émotionnelle.	Exemples de communications suspectes ; Signes avant-coureurs d'une fraude ; Comment réagir en toute sécurité.	Jeu de simulation : « Sûr ou suspect ? »

Tableau 4.1 - Répartition détaillée des unités et des thèmes (Module 1)

**Modules complémentaires sur la sécurité hors ligne : traitent de l'utilisation sécurisée des distributeurs automatiques de billets physiques, de l'orientation dans les transports, des protocoles de sécurité à domicile, des contacts d'urgence et des réseaux de soutien communautaires locaux.)*

MODULE 2 : Cybersécurité (Animé par notre partenaire : E-SENIORS)

Introduction : ce module est axé sur la protection des données personnelles, de l'identité numérique et des comptes en ligne. Les seniors apprennent à gérer leurs mots de passe en toute sécurité, à reconnaître les tentatives d'hameçonnage et à naviguer en toute sécurité sur les services en ligne afin de renforcer leur confiance dans l'utilisation de ces outils.

Unité 1 : Données personnelles et identité numérique

Unité 2 : Sécurité des mots de passe et protection des comptes

Unité 3 : Utilisation sécurisée des services en ligne

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

UNITÉ	THÈMES ABORDÉS	CONTENU PRINCIPAL ET PORTÉE	ÉLÉMENT INTERACTIF
Unité 1	Qu'est-ce qu'une donnée à caractère personnel ? Risques liés au partage d'informations personnelles ; Protection de l'identité numérique.	Exemples d'informations sensibles ; Paramètres de confidentialité sur les plateformes en ligne.	Exercice : quelles informations doivent rester privées ?
Unité 2	Créer des mots de passe forts ; stratégies de gestion des mots de passe ; authentification à deux facteurs.	Exemples de mots de passe ; pratiques de sécurité.	Atelier de création de mots de passe
Unité 3	Sécurité des services bancaires en ligne ; Identification des sites web sécurisés ; Transactions en ligne sécurisées.	Reconnaître les sites web sécurisés (HTTPS) ; Éviter les liens suspects.	Jeu de simulation : « Repérez le message de hameçonnage ».

Tableau 4.2 - Répartition détaillée des unités et des thèmes (modules 2)

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

MODULE 3 : Éducation aux médias (animé par le partenaire : BLSH)

Introduction : ce module aide les seniors à développer leur esprit critique lorsqu'ils consultent des informations en ligne. Les participants apprennent à évaluer les sources, à reconnaître les fausses informations et à comprendre comment les contenus générés par l'IA et les médias manipulés peuvent influencer la perception du public.

Unité 1 : Comprendre l'information en ligne

Unité 2 : Reconnaître la désinformation et les fausses informations

Unité 3 : Contenus générés par l'IA et manipulation des médias

UNITÉ	THÈMES ABORDÉS	CHAMP D'APPLICATION DU CONTENU PRINCIPAL	ÉLÉMENT INTERACTIF
Unité 1	Comment l'information se diffuse en ligne ; les différents types de sources médiatiques ; les informations fiables et non fiables.	Exemples de sources fiables ; Introduction aux outils de vérification des faits.	Exercice de comparaison des sources
Unité 2	Caractéristiques des fausses informations ; titres et images manipulés ; manipulation émotionnelle dans les médias.	Exemples de désinformation virale ; pratiques de partage responsables.	Jeu : « Repérez les fausses informations ».
Unité 3	Images et textes générés par l'IA ; Deepfakes ; Comment repérer les contenus manipulés.	Exemples de contenus générés par l'IA ; comment vérifier les informations.	Exercice : Images réelles vs images générées par l'IA

Tableau 4.3 - Répartition détaillée des unités et des thèmes (Module 3)

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

MODULE 4 : Technologies d'assistance à l'autonomie à domicile (animé par le partenaire : KIT)

Introduction : Ce module présente aux seniors les technologies qui favorisent l'autonomie, la surveillance de la santé et la sécurité à domicile, en renforçant leur confiance dans l'utilisation des technologies d'assistance pour améliorer leur sécurité et leur autonomie.

Unité 1 : Introduction aux technologies d'assistance

Unité 2 : Technologies de sécurité pour la maison connectée

Unité 3 : Outils numériques pour la santé et la communication

UNITÉ	THÈMES ABORDÉS	CONTENU PRINCIPAL ET PORTÉE	ÉLÉMENT INTERACTIF
Unité 1	Qu'est-ce que l'assistance à l'autonomie à domicile (AAD) ? Avantages des technologies d'assistance ; exemples d'appareils destinés aux personnes âgées.	Présentation des technologies de la maison connectée ; outils de suivi de la santé.	Discussion : Comment la technologie peut-elle améliorer la vie quotidienne ?
Unité 2	Systèmes d'alerte d'urgence ; technologies de détection des chutes ; capteurs de sécurité domestique.	Exemples de solutions pour la maison connectée.	Étude de cas : concevoir un environnement domestique plus sûr
Unité 3	Applications de suivi de la santé ; services de télésanté ; technologies de communication.	Utilisation d'applications pour le suivi de la santé ; outils numériques pour la communication familiale.	Jeu de simulation : « Smart Home Safety Builder ».

Tableau 4.4 – Répartition détaillée des unités et des thèmes (modules 4)

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

3.3 Cadre de répartition des questions d'auto-évaluation

Afin de garantir une couverture équilibrée, le système établit un ensemble strict d'exigences quantitatives pour la conception des quiz : chaque module doit comporter exactement 15 questions à choix multiples, réparties de manière égale à raison de 5 questions par unité, afin d'assurer une représentation complète de tous les thèmes.

BLOC D'UNITÉS THÉMATIQUES	NOMBRE DE QUESTIONS VISÉ
Unité 1 (Compréhension conceptuelle)	5 questions
Unité 2 (Mise en œuvre des compétences tactiques)	5 questions
Unité 3 (Scénario d'identification des menaces)	5 questions
Nombre total de questions par module	**15 questions**

Tableau 5 - Cadre de répartition des questions d'auto-évaluation

** Exemple de formulation de question selon le cadre standardisé :

Vous recevez un message vous informant que votre compte bancaire a été bloqué et vous demandant de cliquer sur un lien pour vérifier vos informations. Que devez-vous faire ?

Options de réponse : A. Cliquer immédiatement sur le lien

B. Contacter la banque via son numéro de téléphone officiel

C. Répondre en indiquant votre numéro de compte

D. Transférer le message à des amis.

Réponse correcte : B

Texte d'explication du système : Les banques ne demandent jamais d'informations personnelles par le biais de messages contenant des liens. Contactez toujours la banque par les canaux officiels.

- Restrictions linguistiques :

  Les questions doivent être simples, concrètes et directement liées au contenu. Les formulations négatives ou prêtant à confusion (par exemple : « Laquelle de ces options n'est PAS sûre ? ») doivent être évitées au profit de formulations directes et positives (par exemple : « Quelle est l'action la plus sûre ? »).

- Répartition des niveaux de difficulté :

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

Les questions doivent présenter un niveau de difficulté modéré, incitant à la réflexion, sans être piégeuses ni utiliser de formulations trompeuses.

- Mécanisme de retour d'information :
  Immédiatement après qu'un apprenant a soumis sa réponse, la plateforme doit afficher une brève explication renforçant le comportement sûr.

Les questions sont réparties sur trois niveaux distincts afin d'équilibrer la compréhension et la mise en pratique (voir tableau 10).

NIVEAU DE DIFFICULTÉ VISÉ	RÉPARTITION EN POURCENTAGE
Facile (connaissances de base)	40 %
Moyen (contexte d'application des compétences)	40
Tâches pratiques basées sur des scénarios	20 %

Tableau 6 – Répartition des niveaux de difficulté dans l'auto-évaluation

3.4 Tableau récapitulatif des objectifs et des résultats du module

Le tableau suivant résume la répartition quantitative globale des éléments pédagogiques ciblés développés par le partenariat dans l'ensemble du cadre global.

MODULE THÉMATIQUE DE BASE	OBJECTIFS D'APPRENTISSAGE	RÉSULTATS D'APPRENTISSAGE
Sécurité générale (Module 1)	3	3
Cybersécurité (Module 2)	3	3
Éducation aux médias (Module 3)	2	2
Vie quotidienne assistée par l'environnement (Module 4)	2	2
Architecture globale du cadre	10	10

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

Tableau 7 - Tableau récapitulatif des quantités stratégiques du cadre

3.5 Composantes d'apprentissage multimédia

Chaque module comprend divers formats d'apprentissage afin de répondre aux différentes préférences d'apprentissage et de renforcer l'engagement des apprenants seniors :

- Présentations pédagogiques :
  Chaque organisation partenaire élabore environ 40 diapositives de contenu pédagogique par module, présentant les concepts clés liés aux compétences de manière claire, accessible et structurée.

- Podcasts :
  Chaque module comprend un épisode de podcast audio, au cours duquel des experts du domaine abordent des sujets très pertinents tels que les menaces de cybersécurité, la sécurité numérique ou les technologies d'assistance, afin de répondre aux besoins des apprenants auditifs.

- Entretiens avec des experts :
  Chaque module intègre une interview vidéo enregistrée avec un spécialiste (par exemple, des experts en cybersécurité, des spécialistes de la prévention policière, des professionnels de l'inclusion numérique ou des spécialistes des technologies de santé) afin d'apporter des informations pratiques et des exemples concrets.

3.6 Jeux éducatifs interactifs et simulations

Afin de renforcer l'engagement des utilisateurs et de consolider l'acquisition de compétences pratiques, chaque module propose un jeu éducatif interactif conçu pour simuler des situations numériques réelles, permettant ainsi aux seniors de s'exercer à la prise de décision stratégique et à la résolution de problèmes dans un environnement de test sécurisé :

- Module « Sécurité générale » :
  Un jeu de simulation dans lequel les apprenants identifient les risques potentiels pour la sécurité et les signes de fraude dans des situations quotidiennes.

- Module sur la cybersécurité :
  Un scénario interactif dans lequel les apprenants doivent repérer les e-mails de hameçonnage, les liens suspects et les tentatives complexes d'usurpation d'identité.

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

- Module sur l'éducation aux médias :

  Une activité ludique qui met les apprenants au défi de distinguer activement les sources fiables des fausses informations trompeuses diffusées en ligne.

- Module « Ambient Assisted Living » :

  Une simulation numérique montrant comment les technologies d'assistance peuvent être configurées concrètement pour améliorer la sécurité et l'autonomie à domicile.

3.7 Spécifications de la plateforme SONET E-Tool

Toutes les ressources pédagogiques, les canaux médiatiques et les acquis d'apprentissage sont intégrés de manière structurée dans **l'outil en ligne** officiel **SONET**. Cette plateforme numérique interactive est minutieusement conçue pour respecter les directives d'accessibilité web adaptées aux seniors. Le portail héberge de manière exhaustive tous les modules d'apprentissage, les présentations multimédias, les podcasts d'experts, les entretiens vidéo, les scénarios d'apprentissage simulés, les fiches de référence téléchargeables et les quiz interactifs d'auto-évaluation. L'E-Tool offre un environnement d'apprentissage intuitif et accessible, dans lequel les seniors peuvent accéder aux ressources de manière autonome ou sous la supervision en présentiel de formateurs adultes.

3.8 Rôle des partenaires dans l'élaboration du programme d'études

Le programme d'enseignement commun est élaboré selon une matrice hautement collaborative dans laquelle chaque partenaire du projet assume la responsabilité structurelle de composantes fondamentales spécifiques :

- Module 1 (Sécurité générale) : élaboré et piloté par PARASOL.
- Module 2 (Cybersécurité) : élaboré et piloté par E-SENIORS.
- Module 3 (Éducation aux médias) : élaboré et piloté par BLSH.
- Module 4 (Vie quotidienne assistée par l'environnement) : élaboré et piloté par KIT.

Tous les partenaires contribuent activement à l'élaboration de supports pédagogiques standardisés ; à la préparation de ressources multimédias adaptées au contexte local, d'auto-évaluations, de podcasts et d'entretiens ; à la création de modèles de scénarios de jeux interactifs ; et à la participation aux évaluations de validation menées à l'échelle du consortium. Afin de garantir une accessibilité et une équité totales au niveau local, l'ensemble des supports finaux est traduit dans les langues des partenaires.

3.9 Impact attendu du cadre

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

La méthodologie pédagogique commune et le programme d'études conjoint visent à atteindre les résultats stratégiques à long terme suivants à l'échelle européenne :

- Renforcer la confiance des seniors dans le numérique, leur sentiment d'efficacité personnelle et leur autonomie fonctionnelle.
- Améliorer la sensibilisation à la cybersécurité et les habitudes quotidiennes en matière de protection des données.
- Soutenir une participation citoyenne sûre et autonome dans la société numérique.
- Promouvoir un vieillissement actif et en bonne santé à domicile grâce au déploiement de technologies d'assistance.

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

4 ALIGNEMENT TECHNIQUE SUR LE CADRE EUROPÉEN DigComp

4.1 Domaines de compétences DigComp couverts

Afin de garantir la validité institutionnelle et de faciliter la transférabilité transfrontalière au sein de l'Union européenne, le cadre SONET contribue directement à quatre domaines de compétences fondamentaux définis par le Cadre européen des compétences numériques pour les citoyens (DigComp) :

Domaine DigComp	Axe du projet SONET
Domaine 1 – Culture de l'information et des données	Évaluation des informations en ligne, suivi des rumeurs et vérification des sources de contenu.
Domaine 2 – Communication et collaboration	Utilisation d'outils de communication numériques pour le soutien familial et la connectivité en matière de soins.
Domaine 4 – Sécurité	Mise en œuvre de la cybersécurité, prévention de la fraude et gestion de la confidentialité des données personnelles.
Domaine 5 – Résolution de problèmes	Utilisation des technologies d'assistance pour favoriser le bien-être personnel et l'autonomie.

Tableau 8 – Axes prioritaires du SONET dans les domaines de compétence du DigComp

4.2 Mise en correspondance systématique des acquis d'apprentissage SONET avec la norme DigComp

Afin de garantir la validité institutionnelle et de faciliter la transférabilité transfrontalière au sein de l'Union européenne, les 10 acquis d'apprentissage du SONET sont alignés sur le **Cadre européen des compétences numériques pour les citoyens (DigComp)**.

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

MODULE	OBJECTIF D'APPRENTISSAGE VISÉ	RÉSULTAT D'APPRENTISSAGE MESURABLE	DOMAINE DIGCOMP	CORRESPONDANCE SPÉCIFIQUE AVEC LE DIGCOMP
Sécurité générale	Sensibiliser davantage aux risques généraux en matière de sécurité.	Identifier les risques courants en matière de sécurité dans les environnements numériques et réels du quotidien.	Domaine 4 : Sécurité	4.1 Protection des appareils et des données personnelles.
Sécurité générale	Utilisation sécurisée des appareils numériques et des technologies du quotidien.	Utiliser en toute sécurité des appareils numériques de base et se connecter à des services Internet.	Domaine 1 : Compétences de base	1.1 Parcourir, rechercher et naviguer parmi les données, les informations et les contenus.
Sécurité générale	Améliorer sa capacité à reconnaître les communications frauduleuses.	Identifier les signes avant-coureurs de la fraude en ligne, du phishing et des tentatives d'usurpation d'identité.	Domaine 4 : Sécurité	4.2 Protection des données personnelles et de la vie privée.
Cybersécurité	Améliorer la compréhension de la protection des données à	Expliquer les principes fondamentaux de la confidentialité en ligne et identifier les données sensibles.	Domaine 4 : Sécurité	4.2 Gestion des données à caractère personnel et

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

	caractère personnel.			de la vie privée.
Cybersécurité	Adopter des habitudes sûres en matière de gestion des mots de passe et des comptes.	Créer de manière autonome des mots de passe forts et appliquer les mesures de sécurité standard.	Domaine 4 : Sécurité	4.1 Protection des appareils.
Cybersécurité	Renforcer la sécurité de la navigation sur les plateformes de services en ligne.	Démontrer comment se connecter et utiliser en toute sécurité les sites web à enjeux élevés.	Domaine 4 : Sécurité	4.1 Protection des appareils et de l'identité numérique.
Éducation aux médias	Développer un esprit critique vis-à-vis des informations en ligne.	Distinguer les sources fiables des sources non fiables à l'aide d'indicateurs.	Domaine 1 : Compétences de base	1.2 Évaluation des données, des informations et des contenus numériques.
Éducation aux médias	Améliorer la capacité à identifier les fausses informations	Identifier des exemples concrets de fausses informations et expliquer en quoi elles sont trompeuses.	Domaine 1 : Culture générale	1.2 Évaluer la crédibilité des informations .

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

	et les rumeurs.			
Technologies AAL	Sensibiliser davantage aux technologies intelligentes d'assistance.	Identifier des outils d'assistance spécifiques favorisant une vie autonome en toute sécurité.	Domaine 5 : Résolution de problèmes	5.2 Identifier les besoins numériques et les solutions technologiques.
Technologies AAL	Développer l'utilisation opérationnelle des technologies d'assistance.	Démontrer avec succès l'utilisation opérationnelle de base d'un outil AAL.	Domaine 2 : Communication	2.1 Interagir grâce aux technologies numériques.

Tableau 9 - Mise en correspondance systématique des acquis d'apprentissage SONET avec les normes DigComp

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

5 CONCLUSIONS

La méthodologie pédagogique commune et le programme d'études conjoint élaborés dans le cadre du lot de travail 2 visent à atteindre les résultats suivants à un niveau global dans l'ensemble des régions partenaires européennes participantes :

- Renforcer la confiance et l'autonomie des seniors dans le domaine du numérique :

  Éliminer activement l'anxiété liée à la technologie et la peur du « pas à franchir » grâce à des cadres d'apprentissage géragogiques encourageants et à une validation positive.

- Améliorer les habitudes en matière de cybersécurité et de protection des données :

  Doter les apprenants seniors de routines comportementales concrètes, durables et sûres pour détecter efficacement les tentatives d'hameçonnage, résister aux manœuvres d'urgence psychologique et gérer leurs mots de passe en toute sécurité.

- Favoriser une participation civique et sociale en toute sécurité :

  Donner aux seniors les moyens d'interagir de manière autonome avec les registres publics numériques, les plateformes administratives en ligne (telles que Cl@ve, BundID, France Connect), les systèmes de santé et les canaux de communication familiaux.

- Promouvoir un vieillissement actif et en bonne santé :

  Optimiser la sécurité physique à domicile et l'autonomie à long terme en intégrant des technologies d'assistance (solutions d'assistance à l'autonomie à domicile, alertes SOS portables, capteurs intelligents) dans la vie quotidienne.

En combinant une infrastructure de prestation de services au niveau local (bibliothèques publiques, associations de seniors, clubs) avec un système de mise en relation entre bénévoles et des plateformes interactives multimodales d'outils numériques, le cadre SONET offre un modèle éducatif complet, durable et hautement reproductible pour l'inclusion numérique des seniors à travers l'Europe.

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

6 Références

1. Office central des statistiques (GUS), La société de l'information en Pologne en 2025, Varsovie, Pologne, 2026.
2. Conseil des ministres de la République de Pologne, Programme pour le développement des compétences numériques, 2023.
3. Cour des comptes (NIK), Exclusion numérique – Rapport d'audit, Varsovie, Pologne, 2025.
4. Instituto Nacional de Estadística (INE), Enquête sur l'équipement et l'utilisation des TIC dans les ménages 2025, Madrid, Espagne, 2025.
5. R. Tirado-Morueta et al., « L'inclusion numérique des personnes âgées en Espagne : les services d'accompagnement technologique destinés aux seniors comme facteur prédictif », Ageing & Society, 2023.
6. E. M. García-Jáñez, « Conception et développement de services dans les bibliothèques publiques pour l'inclusion numérique des personnes âgées », Revista General de Información y Documentación, 2024.
7. Agence nationale de la cohésion des territoires (ANCT), France Numérique Ensemble (2023–2027) : Stratégie nationale pour l'inclusion numérique, Paris, France, 2023.
8. INSEE et ministère de l'Intérieur, de la Sécurité et de la Société, Paris, France, 2021.
9. Office fédéral des statistiques (Destatis), « Une population en mutation : 15e projection démographique coordonnée », Wiesbaden, Allemagne, 2023.
10. Initiative D21 e.V., « D21-Digital-Index 2024/2025 : état des lieux annuel de la société numérique », Berlin, Allemagne, 2025.
11. N. Döring et S. Hellwig, « Géragogie et médias numériques : exigences pour une didactique adaptée à l'âge », Zeitschrift für Weiterbildungsforschung, vol. 47, n° 1, p. 45-62, 2023.
12. OCDE, Examens des politiques sociales et du marché du travail : Roumanie 2025, Paris : Éditions de l'OCDE, 2025.
13. Reveal Marketing Research, « 61 % des Roumains vivant en zone urbaine ont été la cible de tentatives de fraude en ligne », Bucarest, Roumanie, 2025.
14. Agence des droits fondamentaux de l'Union européenne, « Le vieillissement dans les sociétés numériques : facteurs favorables et obstacles à l'accès des personnes âgées aux services numériques », juin 2022.

Co-funded by the European Union

Financé par l'Union européenne. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenues pour responsables.

Consortium

FUNDACJA PARASOL

Acufade

eseniors

KIT Karlsruher Institut für Technologie

BRIDGE EDUCATION

Co-funded by
the European Union