



USA-3SC

Universal Server of Automated Services for Secured Storages and Communications

Universal

Complètement développé avec, et pour WINDEV, le système "GHOST PROTECT" peut être installé sur tous types de configuration. Ses composants peuvent être intégrés dans tous les développements.

Server

Installé directement comme le serveur "Master", il peut gérer les demandes de toutes les applications connectées qui constituent son réseau de partenaires.

L'intégration du composant "GhostFunction" dans tout développement indépendant WINDEV ou autre, le rend « Partenaire » ou, si nécessaire, permet de le transformer en serveur "Privé" le rendant capable de fournir à ses propres « Partenaires », l'accès à l'ensemble des services « GHOST PROTECT ». Sans aucune réduction de la sécurité ou des services rendus.

Automated

Pour son installation, comme pour son utilisation, le système serveur est totalement automatique, indépendant et ne requière aucune intervention ou décision humaine.

Aucune connaissance ou formation particulière n'est nécessaire à son utilisation.

Toutes les fonctions demandées par les applications "Partenaires" sont gérées sans aucune intervention complémentaire extérieure et en utilisant le paramétrage du langage WINDEV.

Tous les comptes-rendus des opérations demandées sont communiqués en temps réel aux demandeurs.

Services

Le serveur "GHOST PROTECT" fourni en exclusivité tous les services demandés par les applications "Partenaires", à partir du moment où elles s'y sont connectées.

Les applications "Partenaires" disposent automatiquement, d'une identification unique, permanente et invisible qui protège indéfiniment leurs informations et leurs échanges de toute divulgation.

Afin de faciliter, pour les réalisateurs de programmes informatiques, l'accès des applications "Partenaires" aux services disponibles, ceux-ci sont déclenchés par l'appel de fonctions dont le paramétrage est totalement identique à celui des fonctions équivalentes WINDEV de base.

Ces fonctions sont juste identifiées par la présence de la lettre "G" en tête de leurs noms.



Secured

La sécurité maximale des données stockées et de leurs échanges est assurée par la mise en oeuvre d'algorithmes dédiés et de clés individualisées, inaccessibles, totalement générées et gérées par le système.

Ces informations sont donc garanties inaccessibles de l'extérieur, même par désassemblage.

De ce fait, chaque système dispose d'une protection particulière interdisant la pénétration des hackers par itération ou répétition.

L'éventuelle découverte de l'accès à une donnée ne peut donc pas être utilisé pour une autre donnée, du même site ou, encore moins, d'un autre site.

Storage

Le stockage sécurisé des données est la mission principale du système "GHOST PROTECT".

Il assure cette mission par la multiplication, la dispersion, la segmentation, le salage et le cryptage de toutes les informations qui lui sont confiées. Tous les répertoires sont auto-générés, propre à chaque site, et les fichiers protégés sont masqués.

De plus, la configuration matérielle et le stockage des données sont surveillés en permanence, entraînant la signalisation et le blocage instantané de toute tentative d'accès non souhaité.

Afin de compliquer le travail des « Hackers », le traitement des accès frauduleux va, en fonction de la gravité, de la simple signalisation à la destruction totale des processus responsables.

Communications

La sécurité des données est complétée par la protection totale de leurs échanges en utilisant des algorithmes autonomes indépendants, au-dessus des systèmes de codage / cryptage connus.

Tous les moyens physiques de communication avec le monde extérieur sont inventoriés et mémorisés au premier lancement. Ils sont surveillés en permanence. Toute modification de la configuration système en cours de fonctionnement entraîne une réaction graduée, fonction de la gravité de la pénétration, allant de la simple signalisation du changement à... Si nécessaire l'arrêt, voir la destruction totale du système, hors bases de données du serveur.

Toutes les voies de communication extérieures, qu'elles soient... Par sockets, par emails, par SMS, par disques, par clés USB... Sont protégées au même niveau..

Comme pour le stockage, la garantie de confidentialité des communications est assurée par des solutions indépendantes qui permettent, entre autres, la mise en place de messageries à codification variable imprévisible, et individualisées. Elles sont donc impossibles à pénétrer et à généraliser.

Même en possession d'un échantillon de données décodé, il est impossible de décoder les autres parties des messages échangés ou des zones de leur stockage.