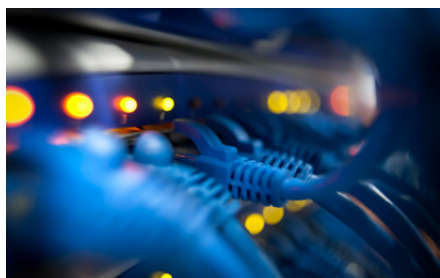


Sécurisation des flux et protection des réseaux



Trustway Chronos : une solution de chiffrement réseau jusqu'au niveau « *Confidentiel Défense* ».

Atos a développé une solution de haute sécurité pour protéger les communications et les échanges sur les réseaux.

La solution Trustway Chronos permet de couvrir les débits jusqu'à 10 Gbits/s en full duplex.

Le Trustway Chronos est une solution dédiée aux Opérateurs d'Importance Vitale (OIV) et industriels de l'armement, offrant une souplesse d'intégration et d'administration.

Une offre au coeur de la loi de Programmation Militaire (LPM)

La solution Trustway Chronos répond aux nouvelles exigences de la LPM et aux dispositions relatives à la protection des infrastructures vitales déclinées dans le Livre Blanc sur la Défense et la Sécurité Nationale (LBDSN) contre la cybermenace. Cofinancé par Atos et le Ministère de la Défense avec la participation de l'Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI), cette solution offre une protection des informations sensibles jusqu'au niveau de sécurité « *Confidentiel Défense* ».

Trustway Chronos : une gamme complète

Trustway Chronos se décline selon 3 versions parfaitement interopérables couvrant des débits allant de 250 Mbits/s à 10 Gbits/s :

- chiffreur « *Chronos* » : 2*250 Mbits/s
- chiffreur « *Hi Chronos* » : 2*900 Mbits/s
- chiffreur « *X Chronos* » : 2*8 Gbits/s.

Très haut niveau de sécurité

Le système fonctionne en mode « *encapsulé* » et fournit les services de sécurité suivants :

- le chiffrement des flux;
- le scellement des flux;
- la gestion de l'anti-rejeu;
- la sélection des adresses IP rouges et noires autorisées;
- la journalisation des événements.

Un déploiement sous contrôle étatique

Toute acquisition est soumise à l'accord préalable de l'ANSSI. Aussi l'Autorité Qualifiée responsable du Systèmes d'Information (AQSSI ou RSSI) doit engager sa demande vers l'ANSSI et informer l'autorité de tutelle, dont il dépend, de sa démarche.

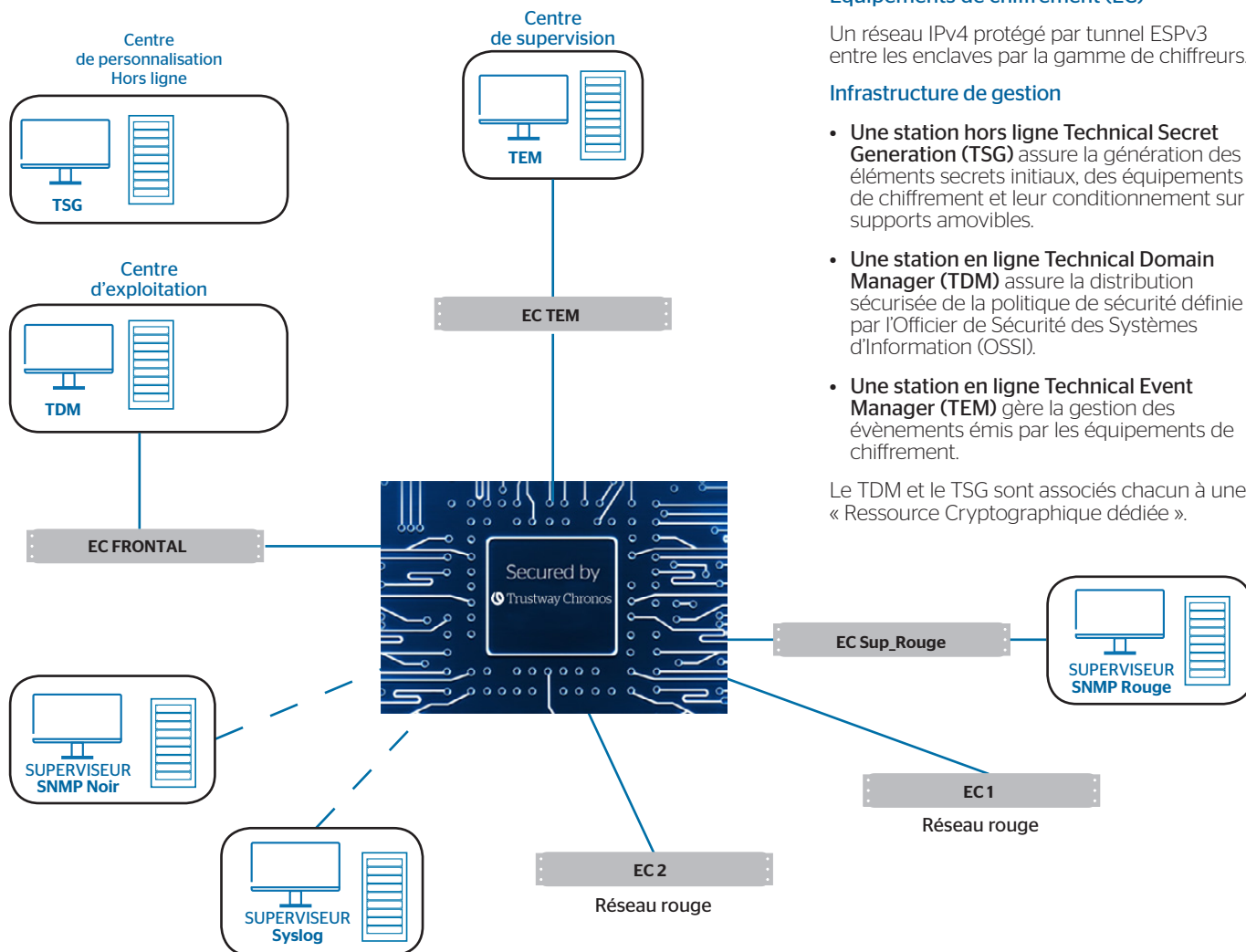
Le Ministère de la Défense et l'ANSSI instruisent conjointement le dossier et informent le demandeur, le Haut Fonctionnaire de Défense (HFDS) dont il dépend et Atos de la décision retenue.

Des conditions d'emploi adaptées

Le marquage des équipements défini par l'agrément offre une gestion adaptée et cohérente avec le niveau de protection couvert par la solution.



Caractéristiques



Equipements de chiffrement (EC)

Un réseau IPv4 protégé par tunnel ESPv3 entre les enclaves par la gamme de chiffreurs.

Infrastructure de gestion

- Une station hors ligne **Technical Secret Generation (TSG)** assure la génération des éléments secrets initiaux, des équipements de chiffrement et leur conditionnement sur supports amovibles.
- Une station en ligne **Technical Domain Manager (TDM)** assure la distribution sécurisée de la politique de sécurité définie par l'Officier de Sécurité des Systèmes d'Information (OSSI).
- Une station en ligne **Technical Event Manager (TEM)** gère la gestion des événements émis par les équipements de chiffrement.

Le TDM et le TSG sont associés chacun à une « Ressource Cryptographique dédiée ».

Interfaces

- 2 x10/100/1000 BaseT Ethernet
- Interface Optique 10G (équipements « X chronos »)
- 300 VPN simultanés.

Effacement d'urgence

Mécanisme de désensibilisation « d'urgence » du chiffreur.

Protection contre le rayonnement

Conformité à la norme « SDIP 27 Level B » en conduction et rayonnement.

Mode de redémarrage

Deux modes de redémarrage possibles :

- un mode de redémarrage manuel nécessitant la présence de l'OSSI
- un mode de redémarrage automatique.

Périmètre de l'agrément

Agrément conforme à la protection des informations classifiées :

- « Défense » jusqu'au niveau « Confidentiel Défense » et ses équivalents interalliés :
- « Confidentiel OTAN »
- « Confidentiel UE/EU »
- « Confidentiel EUROCOR ».

Agrément conforme à la protection des informations :

- « Diffusion Restreinte » et ses équivalents interalliés :
- « Diffusion Restreinte OTAN »,
- « Diffusion Restreinte UE/EU »
- « Diffusion Restreinte EUROCOR ».

Protocoles

Les boîtiers de chiffrement traitent les datagrammes du protocole IPv4 unicast.



Veuillez trouver plus d'information sur atos.net/fr/produits/cybersecurite/chiffrement-donnees/chiffrement-reseaux-sensibles-trustway-chronos

© Atos septembre 2018 - Toutes les marques déposées sont la propriété de leurs propriétaires respectifs. Atos, le logo Atos logo, Atos Codex, Atos Consulting, Atos Worldgrid, Bull, Canopy, equensWorldline, Unify, Worldline et Zero Email sont des marques déposées du groupe Atos. Atos se réserve le droit de modifier ce document à tout moment sans préavis. Certaines offres ou parties d'offres décrites dans ce document peuvent ne pas être disponibles localement. Veuillez contacter votre bureau local Atos pour obtenir des informations concernant les offres disponibles dans votre pays. Ce document ne constitue pas un engagement contractuel.