

R&S® MMC3000

APPAREIL DE CRYPTAGE MULTIRÔLE ET MULTIMODE

Sécurité renforcée HF/VHF/UHF et SatCom
pour la voix et les données



Brochure produit
Version 05.00

ROHDE & SCHWARZ

Make ideas real



D'UN SEUL COUP D'ŒIL

Le R&S®MMC3000 est un appareil cryptographique tactique entièrement renforcé, utilisé pour crypter et décrypter les communications vocales et de données aux plus hauts niveaux de sécurité. Certifié TEMPEST, il est interopérable avec les équipements de communication radio HF/VHF/UHF, SatCom et filaire. Il est parfaitement adapté à une utilisation sur des plateformes stationnaires et mobiles dans des environnements terrestre, naval et aérien extrêmes.

Le R&S®MMC3000 repose sur l'ELCRODAT 4-2. L'ELCRODAT 4-2 est certifié pour les communications sensibles jusqu'au niveau COSMIC TOP SECRET (CTS) de l'OTAN. Il a fait ses preuves comme composant principal sur le terrain des communications hautement sécurisées et permet d'assurer l'interopérabilité entre les pays de l'OTAN. Le R&S®MMC3000 ne contient pas d'algorithmes de cryptage de l'OTAN, mais il est conforme aux normes exigeantes en matière de robustesse, de flexibilité et de sécurité.

Le R&S®MMC3000 prend en charge les modes simple, half-duplex et duplex, afin de répondre aux exigences du plus large éventail d'applications numériques et analogiques, à la fois en fonctionnement local et à distance.

Le R&S®MMC3000 peut être utilisé au moyen d'une unité de commande, ainsi qu'à l'aide du module MIL-bus. Un algorithme de cryptage personnalisable propose la singularité et l'exclusivité nécessaires pour les différents scénarios d'un pays ou d'une coalition.

En mode de cryptage de données, le dispositif s'intègre facilement dans les systèmes de transmission de données équipés d'interfaces militaires standardisées (la plupart des interfaces militaires sont prises en charge). Le vocodeur utilisé en mode vocal optimise la clarté de la voix même dans les transmissions bruyantes. La conception souple et évolutive incorpore un processus protégé de téléchargement du logiciel et un emplacement dédié pour une carte de cryptage supplémentaire permettant la mise à niveau de l'appareil, pour répondre aux besoins futurs.

Le R&S®MMC3000 possède de nombreux accessoires servant à intégrer l'appareil dans des infrastructures de communications complexes. Un système de gestion de la sécurité (R&S®SMS3000) est complété par un dispositif de chargement de données (DLD), un cadre support, une unité d'alimentation des composants dédiés au fonctionnement à distance de l'unité de commande.

Caractéristiques principales

- ▶ Cryptage voix / données avec des niveaux de sécurité élevés
- ▶ Protection des communications radio HF/VHF/UHF, SatCom et filaires
- ▶ Ultra-durci, inviolable, certifié TEMPEST
- ▶ Plusieurs accessoires prévus pour répondre aux besoins des installations fixes et mobiles dans toutes les branches des forces armées (terrestre, navale, aérienne)
- ▶ Algorithmes de cryptage personnalisables pour les besoins spécifiques de chaque client



CARACTÉRISTIQUES PRINCIPALES ET AVANTAGES

Interfaces de commande dédiées pour différentes applications

- ▶ Interface de gestion des systèmes logiciels de commande à distance
- ▶ Interface de gestion des systèmes de communications MIL-bus
- ▶ Interface utilisateur de l'unité de contrôle
- ▶ Interface micro-casque / intercom
- ▶ [page 4](#)

Protection complète grâce à un concept de sécurité très élaboré

- ▶ Environnement de production audité
- ▶ Séparation rouge-noir par matériel et protection contre le sabotage
- ▶ Génération et gestion sécurisées des clés
- ▶ [page 6](#)

Polyvalence à travers une multitude de modes de trafic/mode de fonctionnement et mode de transmission

- ▶ Modes de trafic en fonction des modes de fonctionnement et de transmission
- ▶ Modes de fonctionnement pour les transmissions voix / données
- ▶ Télétype pour les communications extrêmement fiables
- ▶ Prêt pour des transmissions via IP
- ▶ Transmissions synchrones et asynchrones via les interfaces rouge et noire
- ▶ [page 8](#)

Haute qualité de service et fonctionnement flexible grâce à une technologie de pointe

- ▶ Haute qualité de service
- ▶ Flexibilité de la configuration
- ▶ Évolutivité
- ▶ [page 10](#)

Algorithmes de cryptage personnalisables pour les besoins spécifiques de chaque client

- ▶ [page 10](#)

Une large sélection d'accessoires simplifie la mise en service et l'exploitation

- ▶ Un PC de configuration améliore l'efficacité et la précision du processus de chargement des préreglages
- ▶ Le cadre-support protège l'appareil dans des environnements physiquement exigeants
- ▶ Le chargeur de données R&S®GP3000 (DLD) permet de distribuer les clés aux unités géographiquement séparées
- ▶ Bloc d'alimentation externe à réglage continu (110 V / 240 V)
- ▶ [page 11](#)

INTERFACES DE COMMANDE DÉDIÉES POUR DIFFÉRENTES APPLICATIONS

Le R&S®MMC3000 propose une large gamme d'options d'interface prenant en charge différentes plateformes d'applications et divers scénarios.

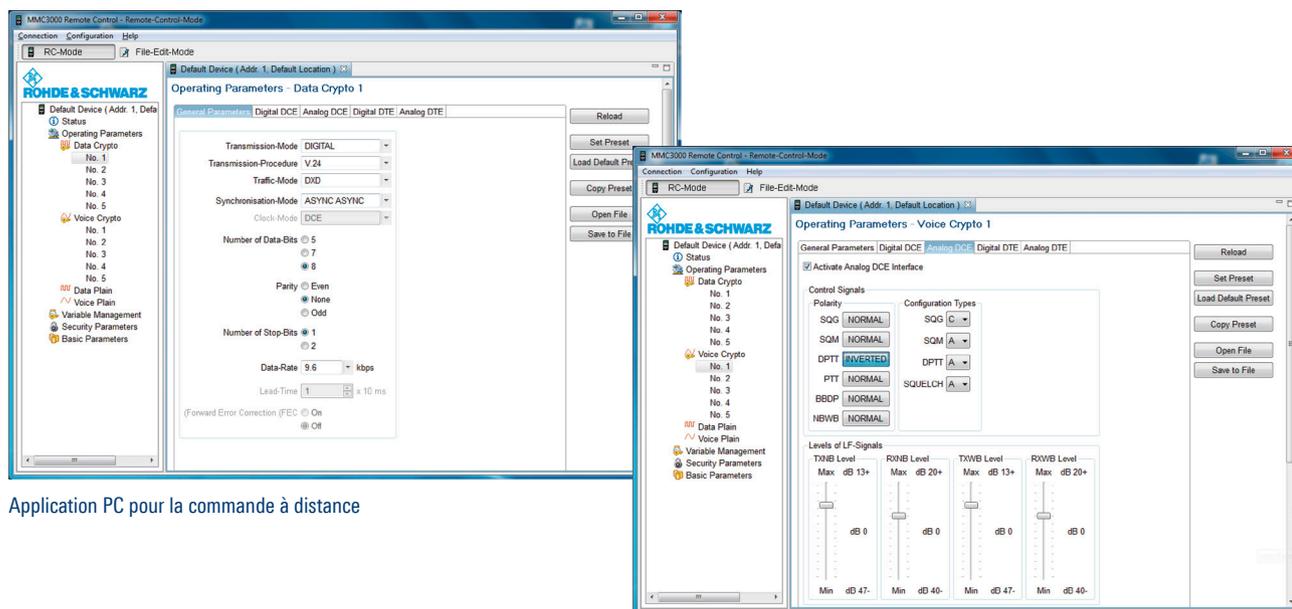
Interface de gestion du logiciel de commande à distance

Le contrôle à distance intégral dans un environnement logiciel défini permet de gérer des appareils dans des endroits inaccessibles, par exemple des locaux exigus au sein d'un avion ou dans un environnement naval. Cette application améliore la flexibilité, la précision et la vitesse dans la gestion d'un système complexe, car jusqu'à 31 R&S®MMC3000 peuvent être connectés à l'adaptateur série RS-485. Cette interface permet de réduire la probabilité d'erreur et d'économiser les ressources en copiant des réglages répétitifs ou en téléchargeant des réglages préconfigurés. Des préreglages afin qu'un grand nombre d'appareils puissent être stockés. Cette fonctionnalité est particulièrement utile dans les centres de commandement et de contrôle, ainsi qu'à bord des navires – deux scénarios de fonctionnement qui impliquent généralement un grand nombre d'émetteurs / récepteurs et d'appareils cryptographiques externes déportés.

L'application copie et télécharge également les paramètres préconfigurés (par exemple d'un appareil à l'autre). Les cinq vues de chaque appareil (état, paramètres de fonctionnement, gestion variable, paramètres de sécurité et

paramètres de base), ainsi que les activités de supervision, fournissent un aperçu complet et rapide de tous les appareils dans un groupe ou un aperçu de tous les réglages d'un appareil individuel d'un seul coup d'œil. Les profils de configuration existants peuvent être copiés et modifiés. Cela signifie que les nouveaux appareils que l'on prépare pour l'installation n'ont plus besoin d'être configurés individuellement – et laborieusement – à la main. La configuration peut se dérouler dans un environnement de gestion prédéfini. Pendant le fonctionnement, les configurations de l'appareil peuvent être laissées telles quelles ou, si nécessaire, être adaptées de manière dynamique.

Un document de contrôle d'interfaces (ICD) disponible auprès de Rohde&Schwarz SIT détaille l'interface pour le logiciel de contrôle à distance du R&S®MMC3000, permettant ainsi aux intégrateurs de développer un logiciel de contrôle à distance personnalisé. De ce fait, le R&S®MMC3000 s'intègre facilement au sein de systèmes de gestion haut de gamme. En plus, le logiciel de contrôle à distance du R&S®MMC3000 est exécutable sur des PC standards, ce qui facilite son intégration au sein d'environnements système existants.



Application PC pour la commande à distance

Interface de gestion des systèmes de communications MIL-bus

Le contrôle électronique de l'interface MIL-bus du R&S®MMC3000 est logé dans un boîtier déporté qui peut être fixé à l'unité de base. Il est conforme à la norme MIL-STD-1553B et inclut un accès redondant. Le contrôle à distance est intégré dans une application de communications existante et destiné aux systèmes de communications complexes équipés de plusieurs appareils R&S®MMC3000 – principalement dans un environnement aéroporté, par exemple pour des hélicoptères ou des avions.

Le module MIL-bus du R&S®MMC3000 assure la pleine capacité opérationnelle, ainsi que les changements des pré-réglages et la réinitialisation logique.

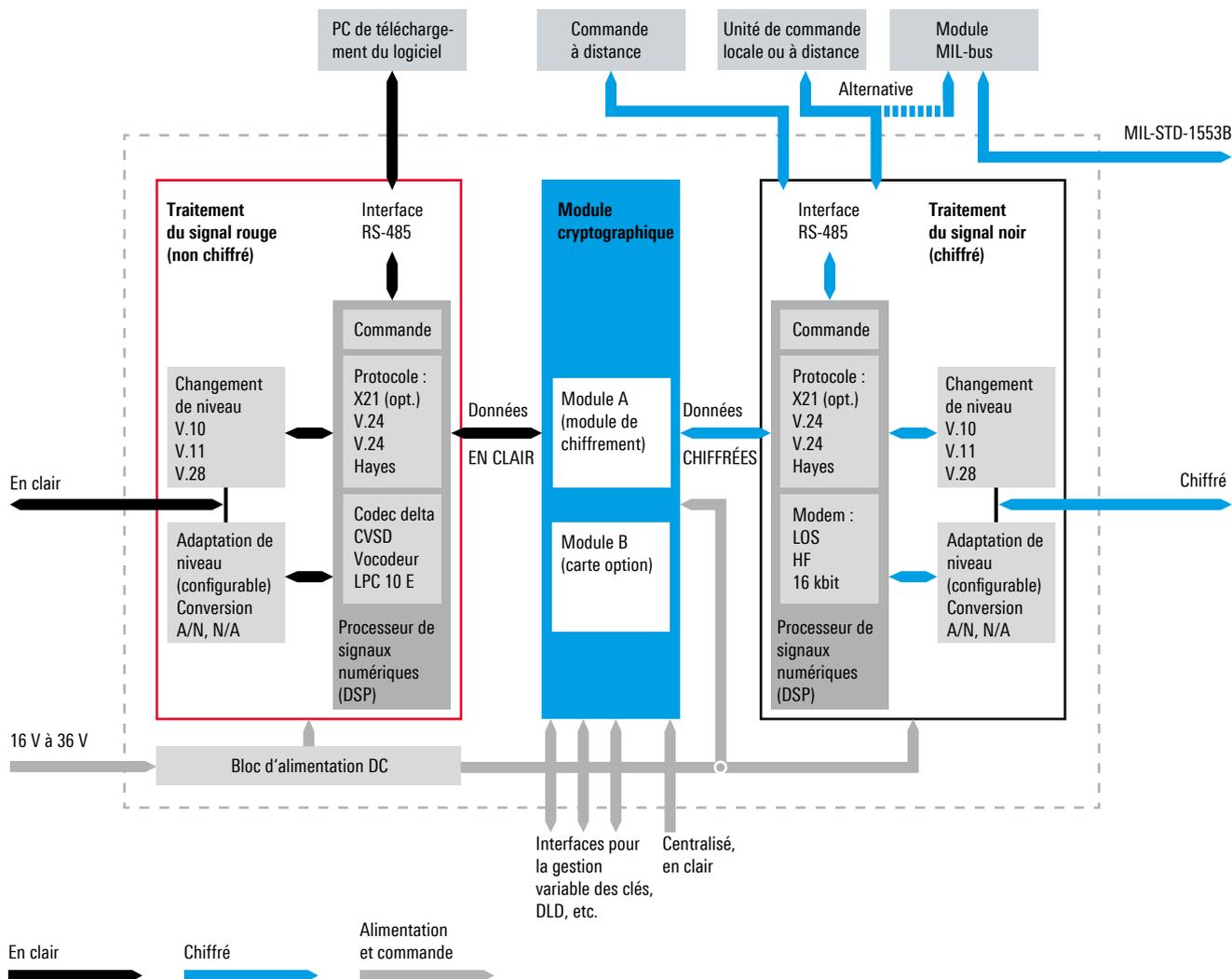
Interface utilisateur de l'unité de contrôle

L'unité de contrôle du R&S®MMC3000 est logée dans un boîtier déporté qui peut être fixé à l'unité de base. Elle est conçue pour les systèmes de communications simples avec un seul R&S®MMC3000, où elle permet à un utilisateur local de changer les pré-réglages et d'accéder à tous les paramètres logiques, physiques et de sécurité (tension, mise à zéro logique et physique, annulation de la mise à zéro, etc.). De plus, l'unité de contrôle peut être utilisée en mode déporté depuis l'unité de base via une liaison câble pouvant atteindre 50 m. Les composants de connexion de l'unité de contrôle déportée sont disponibles sur demande.

Interface micro-casque / intercom

L'interface micro-casque / intercom prend en charge les microphones actifs et passifs, ainsi que le squelch (silencieux) pour assurer une meilleure qualité vocale. Elle est généralement utilisée pour les communications d'urgence locales ou pour le dépannage et évite de devoir reconfigurer l'équipement connecté ou les applications.

Schéma fonctionnel de l'appareil de cryptage R&S®MMC3000



PROTECTION COMPLÈTE GRÂCE À UN CONCEPT DE SÉCURITÉ TRÈS ÉLABORÉ

Le R&S®MMC3000 est basé sur un concept de sécurité couvrant le cycle de vie cryptographique entier pour fournir une protection complète.

Environnement de production audité

Le concept de sécurité du R&S®MMC3000 commence dès la production, l'appareil étant entièrement fabriqué dans un environnement de haute sécurité au sein des usines auditées de Rohde&Schwarz en Allemagne.

Séparation rouge-noir par matériel et protection contre le sabotage

La séparation rouge-noir, réalisée au niveau du matériel, constitue la base de la sécurité de l'information au niveau physique.

Pendant les opérations, l'intégrité du R&S®MMC3000 est assurée par des mécanismes évolués de protection contre le sabotage et la violation d'accès. En cas d'urgence, le dispositif peut être mis à zéro automatiquement ou manuellement par l'une des interfaces physiques disponibles. Son équipement de test intégré (BITE) surveille toutes les fonctions en permanence et assure le bon fonctionnement du système. Sa conception certifiée TEMPEST élimine tout risque d'interception des communications.

Génération et gestion sécurisées des clés

Le R&S®MMC3000 propose une gestion moderne des variables cryptographiques noires, ainsi qu'un système haute performance de gestion de la sécurité. Après leur cryptage par le système de gestion de la sécurité R&S®SMS3000, les clés noires sont téléchargées en toute sécurité depuis le dispositif de chargement des données renforcé R&S®GP3000 (DLD) vers le R&S®MMC3000. La génération des clés se fait dans un R&S®KGE3000 dédié qui contient un générateur physique de bruit aléatoire véritable (TRNG – True Random Noise Generator) de très haute qualité.

Si aucune infrastructure de génération de clés n'est disponible, le R&S®MMC3000 peut générer des clés opérationnelles dans l'appareil de cryptage lui-même.



Vue arrière du
R&S®MMC3000

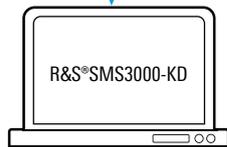
Génération et gestion des clés avec le R&S®MMC3000

Zone sécurisée
(par ex. homeland HQ)



Fourniture des clés

- Génération (chiffrée)
- Distribution (chiffrée)



POLYVALENCE À TRAVERS UNE MULTITUDE DE MODES DE TRAFIC/ MODES DE FONCTIONNEMENT ET MODES DE TRANSMISSION

La flexibilité des interfaces du R&S®MMC3000, avec des interfaces de communications analogiques et numériques, lui permet de prendre en charge plusieurs modes de trafic, de fonctionnement et de transmission.

Modes de trafic en fonction des modes de fonctionnement et de transmission

Le mode utilisé par le R&S®MMC3000 pour envoyer la voix et les données dépend du mode de fonctionnement sélectionné et du mode de transmission. Les modes disponibles sont le simplex, le half-duplex (HDX), le duplex, le double simplex (DX), l'entrée tardive (DX-LE) et le duplex avec accusé de réception (DXD).

Modes de fonctionnement pour les transmissions voix / données

L'appareil de cryptage R&S®MMC3000 propose quatre modes de fonctionnement selon le câblage des interfaces externes et du paramétrage. Les différents modes de fonctionnement sont paramétrés à travers l'unité de contrôle. Les paramètres réglés sont mémorisés dans l'unité de base du R&S®MMC3000. Ces modes de fonctionnement sont les suivants :

Données cryptées

En mode de données cryptées, le R&S®MMC3000 peut être intégré dans les systèmes de transmission de données équipés d'interfaces compatibles avec ITU-T V.24/ V.10/V.11/V.28 ou X.21/V.11 (en option). Les protocoles

de numérotation ou les commandes Hayes (commandes AT) sont utilisables. Après avoir identifié et vérifié les commandes Hayes envoyées par l'équipement terminal de traitement de données (ETTD), le R&S®MMC3000 transmet les commandes Hayes, se synchronise avec le poste demandé et active le mode de données cryptées. Si une interface analogique est utilisée, le modem LOS intégré (selon ITU-T V.26) ou le modem HF (selon STANAG 4197) sera utilisé.

Voix cryptée

En mode de voix cryptée, les signaux vocaux sont numérisés soit à travers le vocodeur LPC 10e, soit à travers le codec delta CVSD, en fonction du mode de trafic. Un modem HF (selon STANAG 4197), un modem LOS (selon ITU-T V.26) et le mode bande de base / diphase ou V.24 peuvent être sélectionnés suivant la méthode de numérisation vocale appliquée.

Voix en clair / données en clair

Plusieurs modes en clair sont disponibles pour la voix et les données en fonction des différentes applications (voix : modes HF, VHF, UHF; données; mode numérique V.24).

Divers champs d'application du R&S®MMC3000



Télétype pour les communications extrêmement fiables

Le télétype assure des communications extrêmement fiables dans des environnements où la largeur de bande est faible ou variable, mais il nécessite une adaptation flexible à des niveaux de faible tension.

Un débit binaire de 50 bit/s à 64 kbit/s permet la communication dans beaucoup de scénarios extrêmes et spéciaux, comme par exemple les bas débits dans les communications des hélicoptères ou les transmissions VHF/UHF.

L'interface micro-casque prend en charge les microphones actifs et passifs et le squelch pour assurer un meilleur discernement acoustique. L'appareil peut être configuré pour prendre en charge le canal de garde. Les communications d'urgence locales ainsi que le dépannage peuvent se faire via l'interface sans avoir besoin de reconfigurer les appareils connectés et les applications.

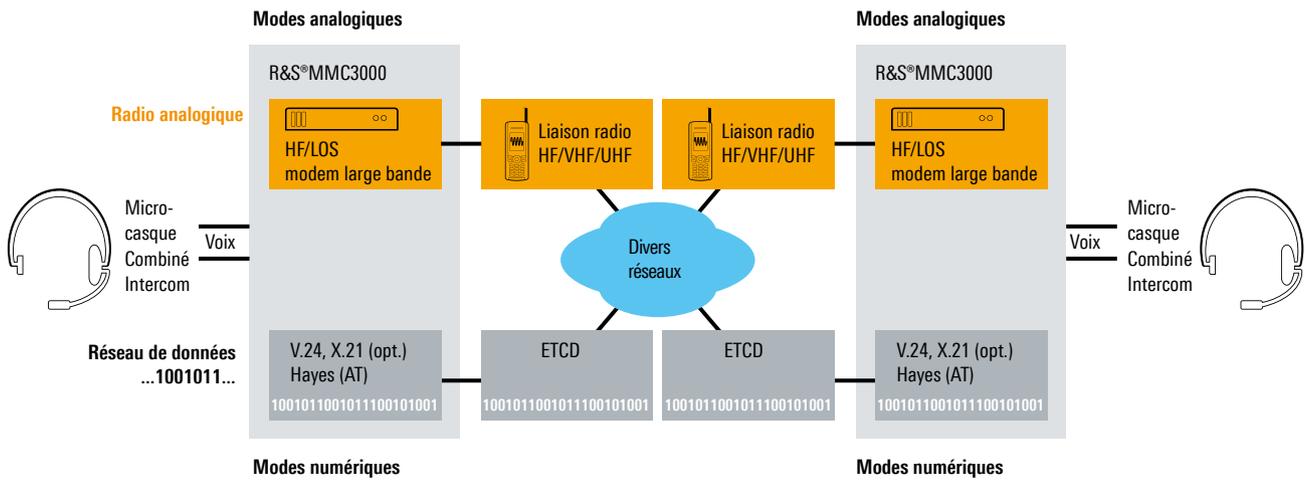
Prêt pour des transmissions via IP

Le passage aux trafic IP pour l'information est pris en charge pour les infrastructures Ethernet. Les données sont transmises via Ethernet en utilisant des convertisseurs standards, repoussant ainsi les restrictions de distance des transmissions séries.

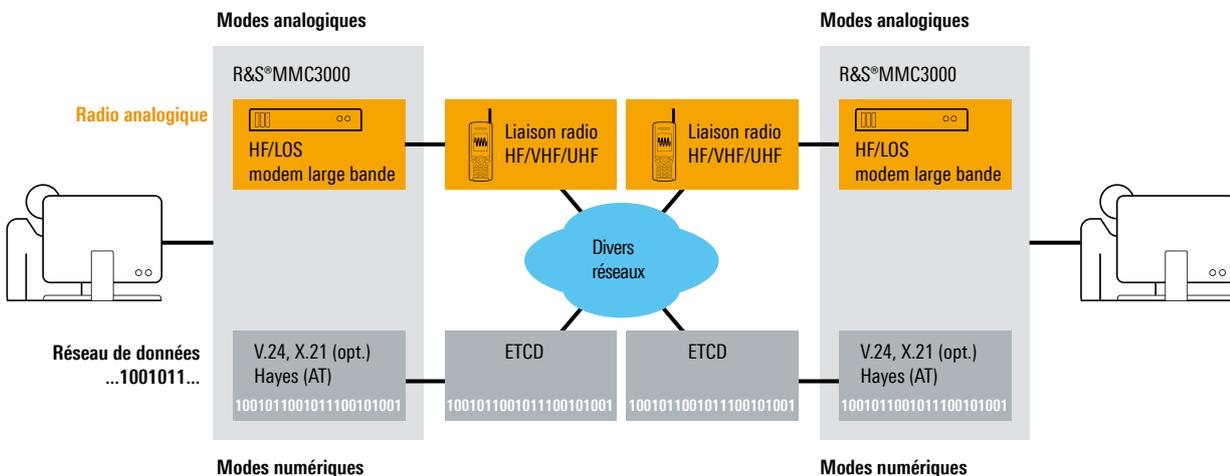
Transmissions synchrones et asynchrones via les interfaces rouge et noire

Toutes les combinaisons de transmissions synchrones et asynchrones sont prises en charge par l'interface noire, aussi bien que par l'interface rouge. Les différents modes de synchronisation sont respectés au sein de chaque réseau sans avoir besoin d'un équipement supplémentaire ou de modifier le réseau.

Cryptage de la voix dans des réseaux de communication différents



Cryptage des données dans des réseaux de communication différents



HAUTE QUALITÉ DE SERVICE ET SOUPLESSE D'EXPLOITATION GRÂCE À UNE TECHNOLOGIE DE POINTE

Haute qualité de service

Le R&S[®]MMC3000 assure une haute qualité de service dans les conditions les plus diverses :

- ▶ Entrée tardive pour les communications cryptées très chargées et ininterrompues, même dans des conditions exigeantes pour le canal de transmission
- ▶ Codecs vocaux de haute qualité optimisés pour chaque type de transmission

Flexibilité de la configuration

Cinq pages de pré-réglages pour chaque mode de fonctionnement permettent une configuration rapide et souple.

Évolutivité

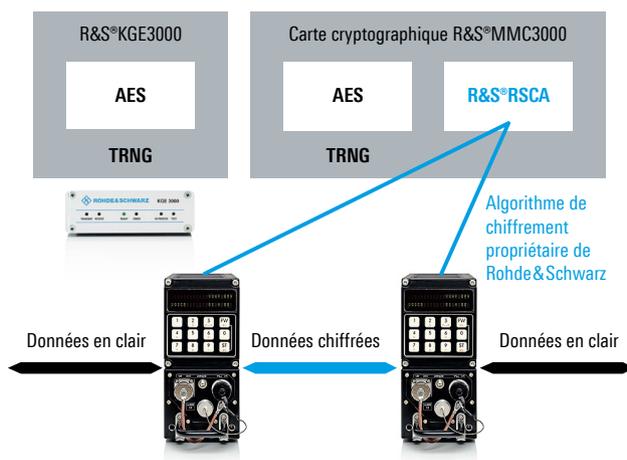
Le R&S[®]MMC3000 propose un emplacement supplémentaire pour l'installation d'une carte de cryptage répondant aux conditions futures. Le R&S[®]MMC3000 est mis à niveau moyennant le téléchargement sécurisé d'un logiciel avec un PC et un progiciel de mise à jour dédié. Ce mécanisme est sécurisé par un algorithme de cryptage spécifique à chaque client.

ALGORITHMES DE CRYPTAGE PERSONNALISABLES POUR LES BESOINS SPÉCIFIQUES DE CHAQUE CLIENT

Le cryptage dans le R&S[®]MMC3000 est basé sur le module cryptographique haute performance de Rohde&Schwarz SIT. Les exigences spécifiques des clients peuvent être satisfaites avec l'algorithme propriétaire R&S[®]RSCA et/ou par l'implémentation spécifique de l'algorithme AES 256. Le degré de personnalisation est tel qu'il peut s'adapter exactement aux exigences uniques des différents clients et applications.

Rohde&Schwarz SIT contrôle tous les aspects du cycle de vie cryptographique de sorte que tous les accessoires de l'appareil de cryptage, par exemple les conteneurs cryptographiques, les supports de clés, les clés de cryptage et les chargeurs de clés, soient configurés pour assurer l'intégration facile et cohérente des algorithmes mis en œuvre.

Technologies de sécurité du R&S[®]MMC3000



LA LARGE SÉLECTION D'ACCESSOIRES SIMPLIFIE LA MISE EN SERVICE ET L'EXPLOITATION

Un PC de configuration améliore l'efficacité et la précision du processus de chargement des préréglages

L'application pour (pré-)configurer les préréglages et les charger dans plusieurs appareils de cryptage R&S®MMC3000 évite de propager les erreurs humaines lors de la mise en service de l'appareil.

Le cadre-support protège l'appareil dans des environnements physiquement exigeants

Le cadre-support aux normes militaires permet de fixer l'appareil de cryptage R&S®MMC3000 solidement dans des environnements particulièrement sujets aux secousses, aux chocs et aux fortes vibrations, par exemple dans un hélicoptère.

Le chargeur de données R&S®GP3000 (DLD) permet de distribuer les clés aux unités géographiquement séparées

Le chargeur de données évite de devoir rassembler toutes les unités en un endroit à proximité de l'équipement ou du processus de génération des clés. Puisqu'il charge des clés noires dans le R&S®MMC3000, le dispositif de chargement de données est sécurisé même en cas de perte des chargeurs DLD.

Bloc d'alimentation externe à réglage continu (110 V/240 V)

La tension du bloc d'alimentation est de 16 V à 36 V. Le bloc est protégé contre les courants électriques et possède des options d'interface pour différentes prises.

Composants et accessoires du R&S®MMC3000



UTILISATION DU R&S[®]MMC3000 AVEC DIFFÉRENTES RADIOS

L'une des caractéristiques essentielles des communications modernes est l'interopérabilité avec les équipements existants. Ceci est vrai pour les émetteurs / récepteurs, ainsi que pour les appareils de cryptage.

Le R&S[®]MMC3000 a été testé avec beaucoup de radios différentes. Il forme une base solide d'interopérabilité pour les communications sécurisées avec les équipements de nombreux fournisseurs.

Les appareils de cryptage doivent être compatibles avec de nombreux dispositifs de cryptage existants et futurs, assurer plusieurs rôles et prendre en charge divers modes.

Liste des appareils testés avec le R&S[®]MMC3000

Constructeur	Désignation	Mode vocal
BARRETT	890 HF	HF
DICOM	RF13	HF et VHF/UHF
HARRIS	PRC 117F	VHF/UHF
HARRIS	FALCON II RF-5800H	HF et LOS
HARRIS	FALCON II RF-5800U	VHF/UHF
ICOM	IC-M700 Pro	HF
ICOM	IC-706 Pro	HF
Kenwood	TM 241	HF
Kenwood	TS 870	HF
Motorola	URC-200	VHF/UHF
Motorola	MICOM	HF
Raytheon	ARC-232	VHF/UHF
Raytheon	ACU1000	HF et LOS
Rockwell Collins	TALON 8105	VHF/UHF
Rockwell Collins	TALON 8110	VHF/UHF
Rockwell Collins	ARC210	VHF/UHF
Rohde & Schwarz	R&S [®] M3SRXT4410	VHF/UHF
Rohde & Schwarz	R&S [®] XK2100	HF
Rohde & Schwarz	R&S [®] XK4100	HF
Rohde & Schwarz	R&S [®] XM6923	VHF/UHF
Rohde & Schwarz	R&S [®] M3AR	VHF/UHF
Rohde & Schwarz	R&S [®] M3TR	HF et VHF/UHF
Rohde & Schwarz	R&S [®] XT622P1	VHF/UHF
Rohde & Schwarz	R&S [®] XT6923L	VHF/UHF
Tait	TB7100	HF et LOS
THALES	TRM6110	HF
THALES	TRM6021	VHF/UHF
THALES	TRG3031C	VHF/UHF
THALES	TRG6031C	VHF/UHF
THALES	TRA6031C	VHF/UHF
THALES	PRC 148	VHF

Remarque : Cette liste donne une indication sur la flexibilité du R&S[®]MMC3000; les tests ont été réalisés sur des appareils individuels avec des versions de firmware spécifiques et des applications spécifiques. Pour les informations détaillées, veuillez vous adresser à Rohde & Schwarz SIT.

SPÉCIFICATIONS

Spécifications

Données opérationnelles

Modes de fonctionnement		voix EN CLAIR / CRYPTÉE, données EN CLAIR / CRYPTÉE
Modes de trafic		semi-duplex (voix), simplex, half-duplex (HDX), double simplex (DX), duplex avec accusé de réception (DXD), entrée tardive (DX-LE)

Interface analogique

Audio		
Interface audio / intercom universelle à 4 fils		
niveau		-47 dB à +13 dB, ajustable par pas de 1 dB
Impédance		600 Ω
Casque		interface de micro-casque
Radio		bande étroite / large bande
niveau		-40 dB à +20 dB, ajustable par pas de 1 dB
Impédance		600 Ω
Mode de trafic		half-duplex
Méthode de transmission		BANDE DE BASE / DIPHASE, modem LOS (V.26), modem HF (STANAG 4197)
Traitement de la voix		codec delta (CVSD) 16 kbit/s, LPC 10E (2,4 kbit/s) selon STANAG 4198

Interface numérique

V.24		50 bit/s à 57,6 kbit/s (5/7/8 bits) en mode asynchrone, 50 bit/s à 19,2 kbit/s (5/7/8 bits) en mode asynchrone / synchrone, 50 bit/s à 64 kbit/s en mode synchrone, compatible avec les commandes Hayes
------	--	--

Autres interfaces

Chargement des clés		RS-485 (DLD)
Effacement d'urgence des clés (mise à zéro)		commutateur, effacement centralisé
MIL-bus		MIL-STD-1553B
Contrôle à distance par application PC	pour 31 appareils R&S®MMC3000 au max.	RS-485

Paramètres de service et de stockage

Température de service		-30°C à +70°C
Température de stockage		-40°C à +85°C
Fuite RF		testé
CEM		MIL-STD-461C catégorie A1b, 2e partie

Données générales

Dimensions	L x H x P	90,4 mm x 193,5 mm x 200 mm (3.56 in x 7.62 in x 7.87 in)
Poids		3,8 kg (8.4 lb)
Alimentation		28 V (16 V à 36 V) DC
Alimentation	entrée	100 V à 240 V AC, 50 Hz à 60 Hz
	sortie	24 V DC
Consommation de courant		< 15 VA
MTBF		> 8000 h

RÉFÉRENCES DE COMMANDE

Désignation	Type	N° de commande
Unité de base		
(incluant l'unité de base, l'unité de commande, le cadre-support, le guide utilisateur compact)		
Appareil de cryptage multimode, multirôle	R&S®MMC3000	3566.2805.02
Manuel	R&S®MMC3000	3566.1344.32
Manuel de l'intégrateur	R&S®MMC3000	3566.2811.32
Manuel du contrôle à distance	R&S®MMC3000	5401.1635.32
Accessoires		
Module MIL-bus	R&S®MMC3000	3545.0603.03
Unité de commande	R&S®MMC3000	3545.0003.03
Cadre-support	R&S®MMC3000	3544.5330.04
Alimentation électrique AC	R&S®MMC3000	3566.0290.00
Unité de commande déportée	R&S®MMC3000	3566.2811.02
Logiciel de contrôle à distance	R&S®MMC3000-RC	5401.1635.00
Chargeur de données (avec câble de connexion)	R&S®GP3000	3566.2792.02
Système de gestion des clés (incluant R&S®KGE3000)	R&S®SMS3000-KGM	3566.2705.02

VOUS AGISSEZ. NOUS PROTÉGEONS.

ROHDE & SCHWARZ SIT

Cryptage et sécurité informatique



Industrie

Les idées de produit, les processus de fabrication, les brevets et les données financières d'une organisation représentent environ 70 pour cent de ses actifs incorporels. Ces secrets commerciaux et

d'affaires sont essentiels à la capacité de l'organisation à créer de la valeur ajoutée et nécessitent une protection spécifique. Les solutions de sécurité informatique de Rohde&Schwarz SIT protègent des entreprises du monde entier contre l'espionnage et la manipulation des données. Les produits combinent une protection maximale avec un effort administratif minimal, et proposent aux utilisateurs un rapport prix / performance optimal. La gamme de produits Rohde&Schwarz SIT comprend des solutions de cryptage dédiées à la protection de la transmission de données au sein des réseaux publics et privés, des pare-feu de dernière génération pour assurer une utilisation sécurisée des clouds et d'internet, ainsi que des solutions flexibles pour les appels vocaux à l'abri des écoutes.



Infrastructures sensibles

Les infrastructures sensibles assurent le bon fonctionnement de notre société et de notre économie. Les tentatives de manipulations des infrastructures sur lesquelles comptent les fournisseurs d'énergie, les

opérateurs de transport, les services d'urgence et le secteur financier, pourraient représenter une sérieuse menace pour la sécurité publique. Rohde&Schwarz SIT propose aux opérateurs des infrastructures sensibles des produits de sécurité informatique intelligents, afin de sécuriser les réseaux de contrôle et de communications entre les centrales électriques, les tours d'aiguillage, les péages, les mâts radio et les nœuds réseau. En plus de solutions de cryptage pour les réseaux et les communications du début à la fin, des modules de sécurité matérielle (HSM) au sein des principales infrastructures publiques protègent les campus et les installations des entreprises contre les accès non autorisés.



Gouvernement

Les relations politiques internes d'un pays couvrent un large éventail de thèmes sensibles, y compris les affaires économiques et fiscales ou la politique énergétique. Les communications internes entre les déci-

deurs, les autorités gouvernementales, ainsi que les organismes de sécurité publique (PSS) doivent rester confidentielles. Depuis plus de 20 ans, Rohde&Schwarz SIT fournit des solutions hautement sécurisées qui garantissent une confidentialité absolue à tous les niveaux de classification de sécurité. Afin de sauvegarder leur souveraineté, les pays peuvent utiliser leurs propres algorithmes cryptographiques nationaux. La gamme de produits Rohde&Schwarz SIT intègre des produits de cryptage dédiés à tous les niveaux de classification afin de protéger les réseaux et les communications du début à la fin. Les produits destinés au gouvernement sont approuvés par le bureau fédéral allemand de la sécurité des technologies de l'information (BSI) et par l'UE et l'OTAN (jusqu'aux niveaux de classification de sécurité top secret et CTS (cosmic top secret)).



Forces armées

Les opérations lancées pour protéger les sociétés comportent des risques graves. Des renseignements précis et exacts sont nécessaires pour le commandement stratégique des opérations telles que le mainti-

en de la paix, l'aide humanitaire et les secours en cas de catastrophes naturelles. Le maintien de la supériorité de l'information est une priorité absolue. Rohde&Schwarz SIT, un partenaire de sécurité informatique de la République Fédérale d'Allemagne depuis 2004, participe à divers programmes d'équipements de l'OTAN. La société fournit des solutions dédiées à la protection efficace de la voix, des données, des images et des vidéo transmises à l'aide de réseaux fixes, de relais radio et de liaisons satellite. Rohde&Schwarz SIT est synonyme de disponibilité à long terme des produits et de l'interopérabilité des solutions avec les équipements existants. Les produits destinés à l'armée sont approuvés par le bureau fédéral allemand de la sécurité des technologies de l'information (BSI), ainsi que par l'OTAN et l'UE (jusqu'aux niveaux de classification de sécurité top secret et CTS (cosmic top secret)).

Service à valeur ajoutée

- ▶ Mondial
- ▶ Local et personnalisé
- ▶ Spécifique du client et flexible
- ▶ Qualité sans compromis
- ▶ Fiabilité à long terme

Rohde & Schwarz

Groupe spécialisé en électronique, Rohde & Schwarz offre des solutions innovantes dans les domaines d'activité suivants : test et mesure, broadcast et médias, communications sécurisées, cybersécurité, surveillance et test des réseaux. Fondée il y a plus de 80 ans, l'entreprise indépendante dont la maison mère est installée en Allemagne, à Munich, est présente dans plus de 70 pays avec un réseau étendu de vente et de service.

www.rohde-schwarz.com

Conception durable des produits

- ▶ Compatibilité environnementale et empreinte écologique
- ▶ Efficacité énergétique et faibles niveaux d'émission
- ▶ Longévité et coût total de possession optimisé

Certified Quality Management

ISO 9001

Certified Environmental Management

ISO 14001

Rohde & Schwarz training

www.training.rohde-schwarz.com

Service client Rohde & Schwarz

www.rohde-schwarz.com/support

