



جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران

Iranian National Standardization Organization



استاندارد ملی ایران

۱۸۹۷۸-۲

چاپ اول

۱۳۹۵

INSO

18978-2

1st.Edition

2017

Identical with
ISO 24102-2:2015

سامانه‌های حمل و نقل هوشمند (ITS)

– دسترسی ارتباطات سیار زمینی

(CALM) – مدیریت ایستگاه ITS

قسمت ۲: مدیریت از دور ITS-SCUها

Intelligent transport systems —
Communications access
for land mobiles (CALM) — ITS
station management —
Part 2:
Remote management of ITS-SCUs

ICS: 03.220.01;35.240.60

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج- ایران

تلفن: ۸-۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: <http://www.isiri.gov.ir>

Iranian National Standardization Organization (INSO)

No.1294 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: <http://www.isiri.gov.ir>

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک ماده ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانه صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادهای در کمیته ملی مرتبط با آن رشته طرح و در صورت تصویب، به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند در کمیته ملی طرح، بررسی و در صورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شماره ۵ تدوین و در کمیته ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)^۱، کمیسیون بین‌المللی الکتروتکنیک (IEC)^۲ و سازمان بین‌المللی اندازه‌شناسی قانونی (OIML)^۳ است و به عنوان تنها رابط^۴ کمیسیون کدکس غذایی (CAC)^۵ در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استانداردهای کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینه مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامه تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، واسنجی وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization

2- International Electrotechnical Commission

3- International Organization for Legal Metrology (Organisation Internationale de Metrologie Legals)

4- Contact point

5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« سامانه‌های حمل و نقل هوشمند (ITS) – دسترسی ارتباطات سیار زمینی (CALM) – مدیریت

ایستگاه ITS – قسمت ۲: مدیریت از دور ITS-SCU ها »

رئیس:

کدخدازاده، کیاندرخت

(کارشناسی ارشد عمران راه و ترابری)

سمت و / یا محل اشتغال

مرکز تدوین مقررات، ایمنی حمل و نقل، پدافند غیرعامل و مدیریت بحران معاونت حمل و نقل وزارت راه و شهرسازی

دبیر:

گل نواز، محدثه

(کارشناسی ارشد مدیریت اجرایی - استراتژیک)

سازمان ملی استاندارد ایران

اعضاء: (اسامی به ترتیب حروف الفباء)

احمدی فرد، مسعود

(کارشناسی مهندسی مکانیک)

شرکت پارس خودرو

رمضانی، یوسف

(کارشناسی ارشد مهندسی کامپیوتر)

گروه پژوهشی فناوری اطلاعات سازمان جهاد دانشگاهی صنعتی شریف

طاووسی، وحید

(کارشناسی ارشد مهندسی خودرو)

دانشگاه علم و صنعت ایران

طرفه نژاد، حمید

(کارشناسی ارشد مهندسی الکترونیک)

مرکز مدیریت راه‌های کشور سازمان راهداری و حمل‌ونقل جاده‌ای

عروجی، سید مهدی

(کارشناسی ارشد مدیریت فناوری اطلاعات)

سازمان تنظیم مقررات و ارتباطات رادیویی

سمت و/ یا محل اشتغال

اعضاء : (اسامی به ترتیب حروف الفباء)

کارشناس استاندارد

ملا احمدی، سیمین

(کارشناسی مهندسی مکانیک)

ویراستار

کارشناس استاندارد

طاووسی، وحید

(کارشناسی ارشد مهندسی خودرو)

فهرست مندرجات

صفحه	عنوان
ز	پیش‌گفتار
ح	مقدمه
۱	۱ هدف و دامنه کاربرد
۱	۲ مراجع الزامی
۲	۳ اصطلاحات و تعاریف
۳	۴ نمادها و اصطلاحات اختصاری
۴	۵ الزامات
۴	۶ معماری مدیریت از دور
۱۱	۷ واحدهای داده پروتکل مدیریت از دور
۱۳	۸ کارکردهای خدمت ابتدایی
۱۶	۹ رویه‌های مدیریت از دور
۲۲	۱۰ استفاده از FSAP
۲۳	پیوست الف (الزامی)، ماژول (پودمان)های ASN.1
۳۳	پیوست ب (آگاهی دهنده)، پارامترهای خدمت ارتباطی
۳۵	کتاب‌نامه

پیش‌گفتار

استاندارد «سامانه‌های حمل و نقل هوشمند (ITS) - دسترسی ارتباطات سیار زمینی (CALM)» - مدیریت ایستگاه ITS - قسمت ۲: مدیریت از دور ITS-SCUها» که پیش‌نویس آن در کمیسیون‌های مربوط بر مبنای پذیرش استانداردهای بین‌المللی/منطقه‌ای به عنوان استاندارد ملی ایران به روش اشاره شده در مورد الف، بند ۷، استاندارد ملی ایران شماره ۵ تهیه و تدوین شده، در سی و سومین اجلاس کمیته ملی استاندارد حمل و نقل مورخ ۱۳۹۵/۱۲/۲۱ تصویب شد. اینک این استاندارد به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شماره ۵ (استانداردهای ملی ایران - ساختار و شیوه نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، در هنگام تجدیدنظر در کمیسیون فنی مربوط، مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

این استاندارد ملی بر مبنای پذیرش استاندارد بین‌المللی زیر به روش «معادل یکسان» تهیه و تدوین شده و شامل ترجمه تخصصی کامل متن آن به زبان فارسی می‌باشد و معادل یکسان استاندارد بین‌المللی مزبور است:

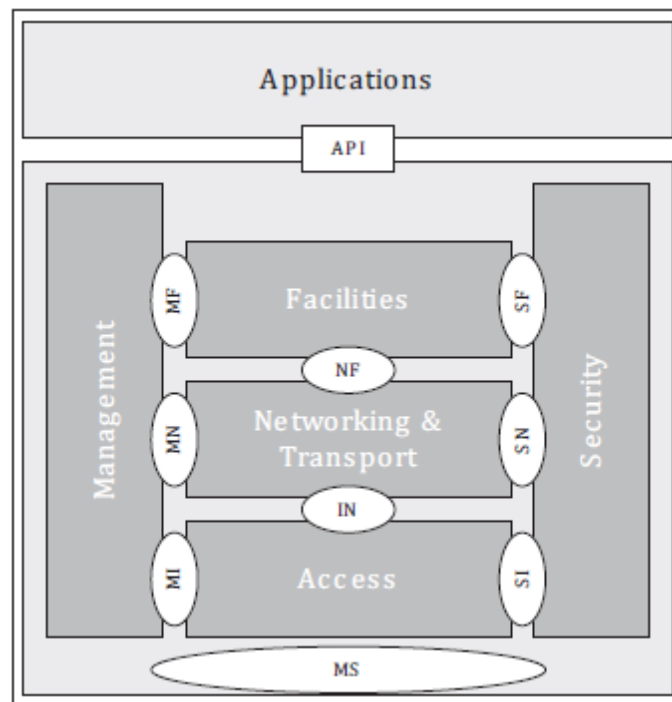
ISO 24102-2:2015, Intelligent transport systems — Communications access for land mobiles (CALM) — ITS station management — Part 2: Remote management of ITS-SCUs

مقدمه

این استاندارد، یکی از مجموعه استانداردهای ملی ایران شماره ۱۸۹۷۸ است. سایر قسمت های این مجموعه استاندارد به شرح زیر است:

- قسمت ۱: مدیریت محلی
- قسمت ۳: نقاط دسترسی خدمت
- قسمت ۴: ارتباطات مدیریت داخلی ایستگاه
- قسمت ۵: پروتکل اعلان خدمت سریع (FSAP)
- قسمت ۶: مدیریت مسیر و جریان

این استاندارد، مدیریت از دور یک واحد ایستگاه ITS (ITS-SU) به همراه ایستگاه ITS و معماری ارتباطی تعیین شده در استاندارد ISO 21217 که در شکل ۱ نشان داده شده است، را مشخص کرده، و در آن بعنوان یک حوزه امن مدیریت شده محدود (کران دار) عمل می شود.



شکل ۱- معماری مرجع ایستگاه ITS

سامانه‌های حمل و نقل هوشمند (ITS) - دسترسی ارتباطات سیار زمینی (CALM) - مدیریت ایستگاه ITS - قسمت ۲: مدیریت از دور ITS-SCUها

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، ارائه ویژگی‌هایی برای مدیریت ایستگاه سامانه‌های حمل و نقل هوشمند (ITS)، برای سازگاری با معماری مرجع ایستگاه ITS و مجموعه استانداردهای مرتبط با این موضوع در ISO/TC 204 است.

مدیریت از دور ایستگاه ITS، توسط واحدهای داده پروتکل (PDU)^۱، و روش‌های اجرای «پروتکل مدیریت از دور ایستگاه ITS» (RSMP)^۲ مربوط به موضوعات مدیریت شده در واحد ایستگاه ITS، تعیین می‌شود. بین واحدهای ایستگاه ITS مدیریت شده (مشتری (خدمت گیرنده-کارخواه) های مدیریت)، و واحدهای مدیریت کننده از دور ایستگاه ITS (سرور (خدمت دهنده - کارساز) های^۳ مدیریت) تفاوت وجود دارد.

۲ مراجع الزامی

در مراجع زیر ضوابطی وجود دارد که در متن این استاندارد به صورت الزامی به آن‌ها ارجاع داده شده است. بدین ترتیب، آن ضوابط جزئی از این استاندارد محسوب می‌شوند.

در صورتی که به مرجعی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن برای این استاندارد الزام‌آور نیست. در مورد مراجعی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی برای این استاندارد الزام‌آور است.

استفاده از مراجع زیر برای کاربرد این استاندارد الزامی است:

-
- 1- Protocol Data Units
 - 2 - Remote ITS Station Management Protocol
 - 3 - Management servers

2-1 ISO 21217, Intelligent transport systems — Communications access for land mobiles (CALM) — Architecture

2-2 ISO 24102-1, Intelligent transport systems — Communications access for land mobiles (CALM) — ITS station management — Part 1: Local management

2-3 ISO 24102-3, Intelligent transport systems — Communications access for land mobiles (CALM) — ITS station management — Part 3: Service access points

2-4 ISO 24102-4, Intelligent transport systems — Communications access for land mobiles (CALM) — ITS station management — Part 4: Station-internal management communications

2-5 ISO/IEC 7498-4, Information processing systems — Open Systems Interconnection — Basic Reference

یادآوری- استاندارد ملی ایران شماره ۴-۱۶۲۷۴: سال ۱۳۹۱، فناوری اطلاعات -اتصال متقابل سامانه های باز-مدل مرجع پایه -مدل پایه، با استفاده از استاندارد ISO/IEC 7498-4: 1989 تدوین شده است.

2-6 ISO/IEC 8825-2, Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules(PER)

یادآوری- استاندارد ملی ایران شماره ۲-۸۸۲۵: سال ۱۳۹۱، فناوری اطلاعات -قواعد کد بندی نشانه گذاری قاعده ی نحوی انتزاعی یک (ASN.1) ویژگی قواعد کد بندی فشرده (PER)، با استفاده از استاندارد ISO/IEC 8825-2: 2008 تدوین شده است.

۳ اصطلاحات و تعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف ارائه شده در استانداردهای ISO 21217، ISO 24102-1، ISO 24102-3، ISO 24102-4 و ISO/IEC 7498-4، اصطلاحات و تعاریف زیر به کار می‌رود:

۱-۳

مشتری (کارخواه-خدمت گیرنده) مدیریت از دور

remote management client

واحد ارتباطی ایستگاه ITS است که در آن مدیریت از دور ایستگاه ITS توسط سرور مدیریت از دور (۳-۲)، اجرا می‌شود.

سِرور (کارساز - خدمت‌دهنده) مدیریت از دور

remote management server

هستار^۱ اجرا کننده مدیریت از دور ایستگاه ITS، در واحد ارتباطی ایستگاه ITS است.

۴ نمادها و اصطلاحات اختصاری

در این استاندارد، علاوه بر اصطلاحات اختصاری ارائه شده در استانداردهای ISO 21217، ISO 24102-1، ISO 24102-3 و ISO/IEC 7498-4، اصطلاحات اختصاری زیر نیز بکار می‌رود.

BSME	Bounded Secured Managed Entity (from ISO 21217)	هستار امن مدیریت شده محدود (کران‌دار) (از استاندارد ISO 21217)
IICP	ITS station-Internal management Communications Protocol (from ISO 24102-4)	پروتکل ارتباطی مدیریت داخلی ایستگاه ITS (از استاندارد ISO 24102-4)
FSAP	Fast Service Advertisement Protocol (from ISO 24102-5)	پروتکل اعلان خدمت سریع (از استاندارد ISO 24102-5)
ITS	Intelligent Transport Systems	سامانه‌های حمل و نقل هوشمند
ITS-SCU	ITS Station Communication Unit (from ISO 21217)	واحد ارتباطی ایستگاه ITS (از استاندارد ISO 21217)
ITS-SCU-CMC	ITS-SCU Configuration Management Centre (from CEN/ISO/TS 17419)	مرکز مدیریت پیکربندی ITS-SCU (از استاندارد CEN/ISO/TS 17419)
ITS-SU	ITS Station Unit (from ISO 21217)	واحد ایستگاه ITS (از استاندارد ISO 21217)
RMC	Remote Management Client	مشتری مدیریت از دور
RMCH	Remote Management Communication Handler	اداره‌کننده ارتباط مدیریت از دور
RMPE	Remote Management Protocol Execution	اجرای پروتکل مدیریت از دور
RMS	Remote Management Server	سِرور مدیریت از دور
RSMP	Remote ITS station Management Protocol	پروتکل مدیریت از دور ایستگاه ITS

1 - Entity

۵ الزامات

هستار مدیریت ایستگاه ITS، باید قابلیت کارکردی تعیین شده در قسمت‌های قبلی این استاندارد را فراهم کند.

- ۱- قابلیت کارکردی مدیریت ایستگاه ITS محلی، در استاندارد ISO 24102-1 تعیین شده است،
 - ۲- قابلیت کارکردی مدیریت ایستگاه ITS از دور، در این استاندارد تعیین شده است،
 - ۳- قابلیت کارکردی نقاط دسترسی خدمت مدیریت، در استاندارد ISO 24102-3 تعیین شده است.
 - ۴- قابلیت کارکردی ارتباطات مدیریت داخلی ایستگاه ITS، در استاندارد ISO 24102-4 تعیین شده است،
 - ۵- قابلیت کارکردی «پروتکل اعلان خدمت سریع» (FSAP)، در استاندارد ISO 24102-5 تعیین شده است،
 - ۶- قابلیت کارکردی مدیریت مسیر و جریان، در استاندارد ISO 24102-6 تعیین شده است.
- ابزارهای ایجاد امنیت برای دسترسی به قابلیت کارکردی مدیریت، باید در مفهوم جهانی امنیت ITS، تعیین شود. جزئیات بیشتر، خارج از دامنه کاربرد این استاندارد است.
- جزئیات الزامات اجباری، در بندهای زیر، در این استاندارد، تعیین شده اند:
- بند ۶، معماری مدیریت از دور را ارائه می‌کند.
 - بند ۷، واحدهای داده پروتکل مدیریت از دور را تعیین می‌کند.
 - بند ۸، کارکردهای اولیه خدمت را تعیین می‌کند.
 - بند ۹، روش‌های اجرای مدیریت از دور را تعیین می‌کند.
 - بند ۱۰، جزئیات مورد نیاز برای پروتکل اعلان خدمت سریع (FSAP) را تعیین می‌کند.
 - پیوست الف، ماژول ASN.1 برای مدیریت از دور را تعیین می‌کند.
 - پیوست ب، تنظیمات پارامترهای خدمت ارتباطی مورد استفاده در انتخاب خودکار پروفیل‌های ارتباطی تعیین شده در استاندارد CEN/ISO/TS 17423 را پیشنهاد می‌کند.

۶ معماری مدیریت از دور

۱-۶ قابلیت کارکردی

- «پروتکل مدیریت از دور ایستگاه ITS» (RSMP) تعیین شده در این استاندارد، دارای اهداف زیر است:
- تنظیم، به روزرسانی و حذف اطلاعات پیکربندی و عملیات واحد ارتباطی ایستگاه ITS (ITS-SCU) در واحد ایستگاه ITS (ITS-SU) که در استاندارد ISO 21217 تعیین شده است، بعنوان مثال: اطلاعات در خصوص خط‌مشی‌ها و مقررات (استاندارد CEN/ISO/TS 17419)، اطلاعات مرتبط با امنیت، اطلاعات حسابداری، پارامترهای لایه دسترسی (به مرجع [1] کتاب‌نامه مراجعه کنید) و غیره.

- نصب، به‌روزرسانی و از نصب خارج کردن اطلاعات پایدار^۱ در ITS-SCU، بعنوان مثال: فرایندهای برنامه‌های کاربردی ITS-S، پروتکل‌های ارتباطی ITS-S، و
- اطلاع‌رسانی^۲ و بازیابی اطلاعات مدیریتی، مانند: فایل‌های گزارش رویدادها، اخطارهای تولید شده توسط ITS-SCU متعلق به ITS-SU.

به این ترتیب، پنج حوزه مدیریتی مشخص شده در استاندارد ISO/IEC 7498-4 پوشش داده می‌شود.

مدیریت از دور ایستگاه ITS، مجموعه‌ای از فرایندهای مدیریتی، که در آن، واحدهای ایستگاه ITS، بعنوان سرورهای مدیریت از دور (RMS) عمل می‌کنند، را پوشش می‌دهد و واحدهای ارتباطی ایستگاه ITS (-ITS SCU) متعلق به ITS-SUهای مدیریت شده که بعنوان مشتری‌های مدیریت از دور (RMC) عمل کرده را مدیریت می‌کند.

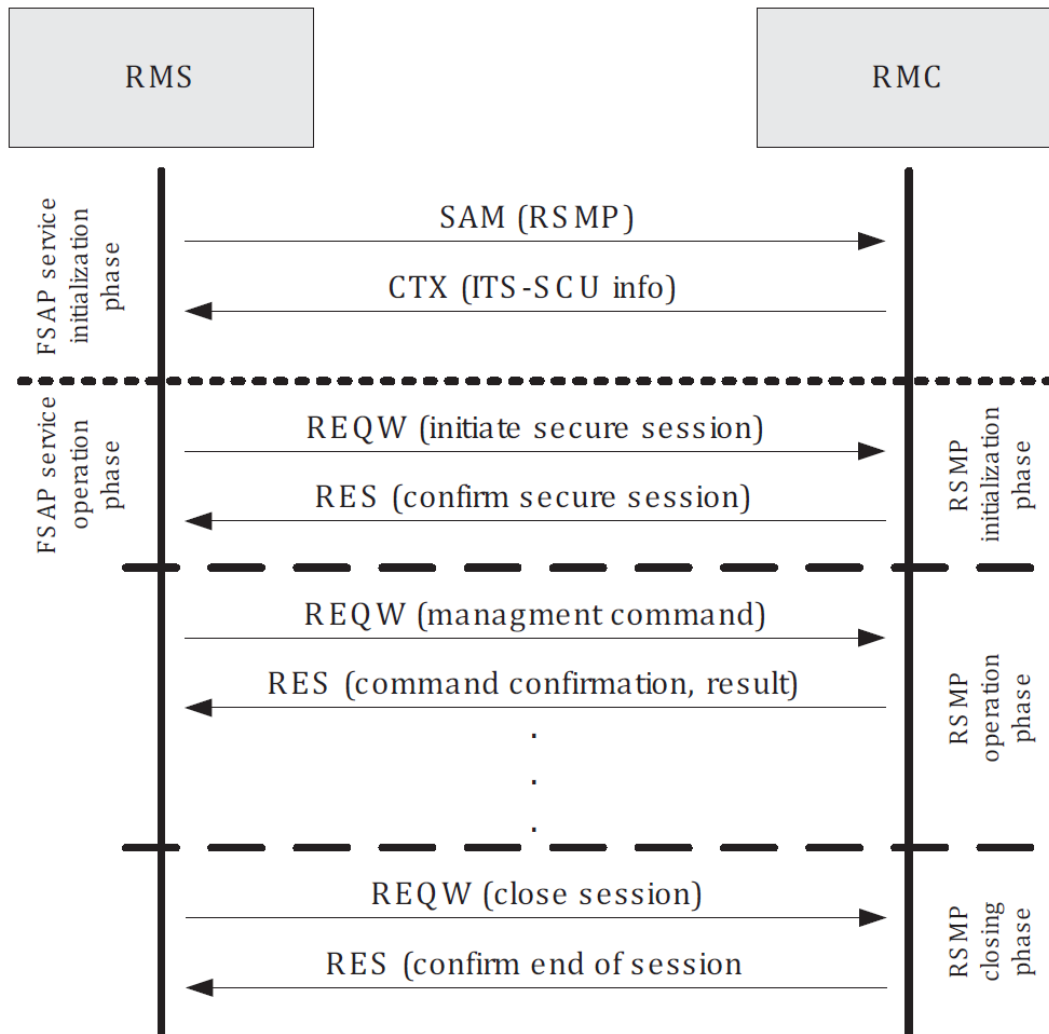
هر RMS مربوط به یک مرکز مدیریت پیکربندی ITS-SCU است که در CEN/ISO/ TS 17419 مشخص شده است. هر RMS می‌تواند، بعنوان مثال، در سامانه فرعی ITS کنار جاده‌ای، یا در سامانه فرعی ITS مرکزی اجرا شود.

مدیریت از دور ایستگاه ITS برای موضوعات مدیریت شده (طبق استاندارد ISO/IEC 7498-4) در نشست-های ارتباطی مدیریت از دور، بکار می‌رود. چنین نشست‌های ارتباطی می‌تواند در موارد زیر برپا شود:

- توسط RMS (نشست ارتباطی آغاز شده توسط سرور)، به عنوان مثال با استفاده از پروتکل اعلان خدمت سریع (FSAP) (به مرجع [۲] رجوع شود) یا با دسترسی مستقیم مبتنی بر IPv6، یا
- توسط RMC (نشست ارتباطی آغاز شده توسط مشتری)، عموماً با استفاده از ارتباطات IPv6، مطابق آنچه در شکل ۲ (نشست ارتباطی آغاز شده توسط سرور با استفاده از FSAP)، در شکل ۳ (نشست ارتباطی آغاز شده مستقیماً توسط سرور) و در شکل ۴ (نشست ارتباطی آغاز شده توسط مشتری) نشان داده شده است.

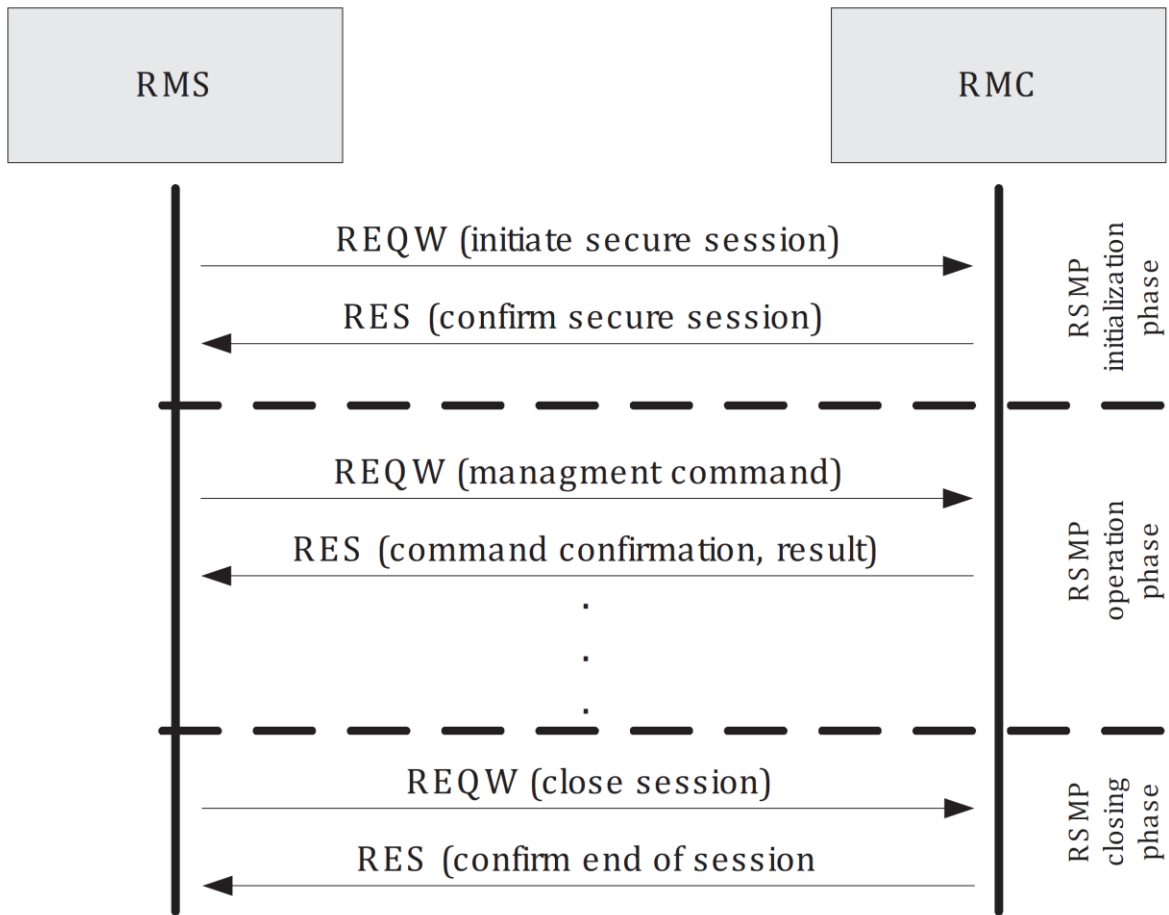
سازوکارهای تعیین شده در این استاندارد، ویژگی‌های بعدی مشخصات مدیریت از دور را در استانداردهای مجزا یا توسط ابزارهای ثبت، توانمند می‌کند.

1 - Persistent information
2 - Notification



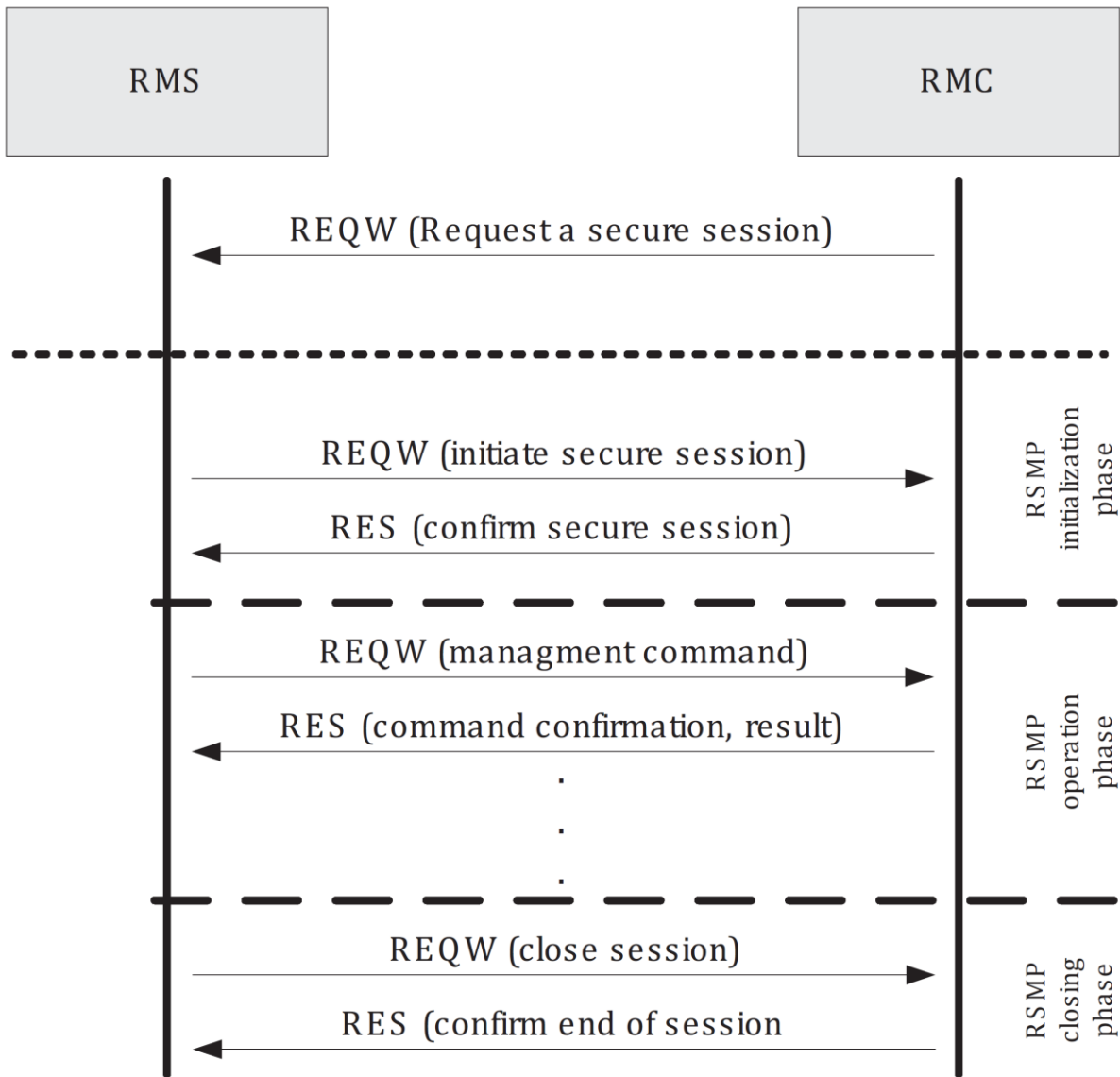
شکل ۲- نشست ارتباطی آغاز شده توسط سرور (مثالی با استفاده از FSAP)

SAM و CTX که در مرجع [2] کتاب‌نامه مشخص شده، و جزئیات آن‌ها در این استاندارد تعیین شده است، برای آماده سازی نشست ارتباطی مدیریتی امن، در مثال شکل ۲ این استاندارد بکار می‌رود. در طی فاز عملیاتی خدمت FSAP، ابتدا یک نشست ارتباطی امن از RMS درخواست می‌شود که توسط RMC تصدیق می‌شود. پس از استقرار موفق نشست ارتباطی با تصدیق متقابل RMS و RMC با توافق اختیاری در مورد رمزگذاری داده‌های مدیریتی که باید در نشست ارتباطی مبادله شود، RMS می‌تواند فرامین مدیریتی را بصورت متوالی ارسال کند، که هر یک از این فرامین توسط RMC تصدیق می‌شود که همچنین ارائه دهنده داده‌های نتایج اختیاری نیز است. در نهایت، RMS نشست ارتباطی را به اتمام می‌رساند که این امر نیز توسط RMC تصدیق می‌شود. متعاقب آن، هیچ داده مدیریتی نمی‌تواند مبادله شود.



شکل ۳- نشست ارتباطی آغاز شده مستقیماً توسط سرور

در مثال شکل ۳، یک RMS بطور مستقیم یک نشست ارتباطی امن را با یک RMC آغاز می‌کند. همان‌طور که در شکل فوق برای نشست ارتباطی آغاز شده مستقیماً توسط سرور نشان داده شده است، پس از تایید نشست ارتباطی امن توسط RMC، RMS نشست ارتباطی امن را اجرا کرده و پایان می‌دهد.



شکل ۴- نشست ارتباطی آغاز شده توسط مشتری

در مثال شکل ۴، به محض ورود یک رویداد به RMC، RMC نیاز برای نشست ارتباطی امن را به RMS اعلام می‌کند. سپس RMS نشست ارتباطی امن را شروع کرده، آن را اجرا می‌کند و سرانجام آن را پایان می‌دهد.

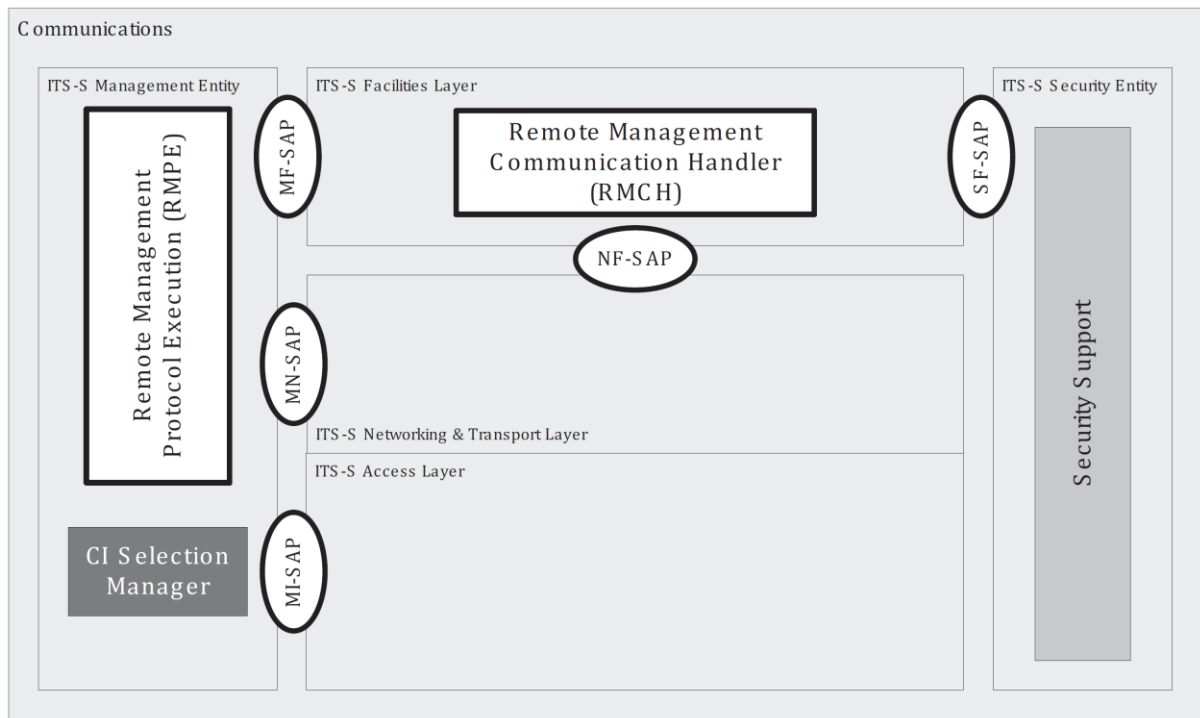
۲-۶ معماری ایستگاه ITS

«پروتکل مدیریت از دور ایستگاه ITS» (RSMP) شامل دو بلوک (بستک) کارکردی است، یعنی:

- فرایند برنامه کاربردی ITS-S، «اجرای پروتکل مدیریت از دور» (RMPE) با یک ITS-AID ثبت شده، و

- تسهیلات ITS-S «اداره‌کننده ارتباط مدیریت از دور» (RMCH) با استفاده از شماره درگاه ثبت شده مشخص PORT-RSM و شماره‌های درگاه ITS که بطور پویا اختصاص داده می‌شوند (به مرجع [3] کتاب‌نامه مراجعه کنید). مقدار PORT-RSM برابر ۳۲۷۶۳ است.

تخصیص این بلوک‌های کارکردی در معماری ایستگاه ITS، که در استاندارد ISO 21217 تعیین شده است، در شکل ۵ معرفی می‌شود. شناساگرهای منحصر بفرد بطور جهانی، در CEN/ISO/TS 17419 تعیین شده‌اند.



شکل ۵- بلوک‌های کارکردی RSMP

RMCH در لایه تسهیلات ایستگاه ITS واقع شده است.

RMPE در هستار مدیریت ایستگاه ITS واقع شده است.

RMCH و RMPE از طریق خدمات MF-SAP، MF-COMMAND و MF-REQUEST، با خدمت ابتدایی قابلیت‌های کارکردی تعیین شده در بند ۸ متصل می‌شوند.

۳-۶ اجرای توزیع شده یک ایستگاه ITS

«پروتکل مدیریت از دور ایستگاه ITS» (RSMP) اجراهای توزیع شده نقش‌های ITS-S، که در استاندارد ISO 21217 مشخص شده است، یعنی چندین ITS-SCU به ازای هر ITS-SU، را پشتیبانی می‌کند. بنابراین RMCH می‌تواند از طریق شبکه داخلی ایستگاه ITS، با یک ITS-SCU تامین کننده پیوند به واحد

ایستگاه ITS همتا^۱، ارتباط برقرار کند. جزئیات بیشتر، به پروتکل لایه شبکه و لایه انتقال ITS-S استفاده شده بستگی دارد و خارج از دامنه کاربرد این استاندارد است.

۴-۶ RMPE

«اجرای پروتکل مدیریت از دور» (RMPE)، فرایند برنامه کاربردی ITS-S است که در هستار مدیریت ITS-S قرار گرفته است. دو نمونه مجزا برای RMPE وجود دارد، یعنی نمونه سرور و نمونه مشتری. در هر ITS-SCU متعلق به یک ITS-SU دقیقاً یک نمونه RMPE وجود دارد. RMPE نمی‌تواند ITS-SCU هایی که در آن‌ها نمونه سازی انجام نشده است، را مدیریت کند.

یادآوری - برای اطلاعات بیشتر در مورد فرایندهای برنامه کاربردی ITS-S، به استاندارد ISO 21217 مراجعه کنید.

فعالیت‌های مدیریتی شامل موارد زیر است:

- به روز رسانی ثابت افزار در ITS-SCU،
- نگهداری فرایندهای برنامه کاربردی ITS-S،
- نصب‌های جدید،
- به روز رسانی‌های نصب‌های موجود،
- حذف نصب‌های موجود،
- نگهداری پروتکل‌های ارتباطی، مدیریتی، و امنیتی،
- نصب‌های جدید،
- به روز رسانی‌های نصب‌های موجود،
- حذف نصب‌های موجود،
- نگهداری از پارامترهای پیکربندی،
- تنظیم مقادیر پارامترها و سایر اطلاعات،
- بازیابی مقادیر پارامترها و سایر اطلاعات، مانند فایل سوابق رویدادها^۲،
- نگهداری امنیت مربوط به موارد مدیریت شده.

۵-۶ RMCH

«اداره‌کننده ارتباط مدیریت از دور» (RMCH) یک تسهیل ارتباطی است که در لایه تسهیلات ITS-S واقع شده است. RMCH:

- واحدهای داده خدمت را از ITS-SU های همتا دریافت می‌کند، که شامل «واحدهای داده پروتکل RMCH» (RMCH-PDU ها) است و در شکل ۷ نشان داده شده است،

1 - Peer ITS station
2 - Logfiles

- RMPE-PDU ها که در شکل ۷ نشان داده شده است را از طریق MF-SAP با RMPE مبادله می کند،
 - RMCH-PDU ها را به ITS-SU های همتا انتقال می دهد، و
 - از خدمات هستار امنیتی ITS-S از طریق خدمت ابتدایی SF-SAP، برای تایید هویت^۱ واحدهای ایستگاه ITS همتا، و برای پنهان سازی^۲ یا آشکار سازی^۳ اختیاری RMPE-PDU ها استفاده می کند.
- از درگاه ITS مشخص PORT_RSM (به مرجع [3] کتابنامه مراجعه کنید) به شرح زیر استفاده می شود:
- الف- یک RMS برای انتقال یک پیام
- بعنوان شماره درگاه مبداء، و
 - بعنوان شماره درگاه مقصد در مورد شروع نشست ارتباطی مستقیم، و فقط در پیام REQW (نشست ارتباطی امن ابتدایی) نشان داده شده در شکل ۳. با REQW (نشست ارتباطی امن ابتدایی) یک RMS از RMC ای، استفاده از یک شماره درگاه معین که بطور پویا تخصیص داده شده است را برای ارتباطات بعدی درخواست می کند.
- ب- یک RMC برای انتقال یک پیام
- بعنوان شماره درگاه مقصد در مورد شروع نشست ارتباطی مستقیم، و فقط در پیام «اعلام نیاز برای نشست ارتباطی امن» نشان داده شده در شکل ۴.
- نمونه سازی های مشتری، شماره های درگاه که بطور پویا تخصیص داده می شوند را بعنوان شماره درگاه مبداء استفاده می کند.

۷ واحدهای داده پروتکل مدیریت از دور

مدیریت از دور ایستگاه، از واحدهای داده پروتکل، عناصر داده، و عناصر امنیتی نشان داده شده در شکل های ۶، ۷، ۸، و ۹، استفاده می کند. معرفی ASN.1 مربوط به این PDU ها در پیوست الف تعیین شده است.

RMCH - Request/Response:

SecHeader	<i>OCTET STRING containing RSMP-Request or RSMP-Response optionally encrypted</i>	SecTrailer
-----------	---	------------

شکل ۶- واحدهای داده پروتکل RMCH

-
- 1 - Authenticate
 - 2 - Encrypt
 - 3 - Decrypt

پیام‌های RMCH-Request و RMCH-Response، پیام‌های RSMP-Request و RSMP-Response را به ترتیب در کپسولی، بین هدر (سرآیند) امنیتی^۱ و تریلر (دنباله) امنیتی^۲ قرار می‌دهد. پیام‌های RSMP-Request و RSMP-Response، همان‌طور که در بخش‌های SecHeader مشخص شده است، می‌توانند رمزنگاری شوند.

RSMP-Request:

SessionID	PDU-Counter	PDU-ID (0)	Length of remainder	Request Data
-----------	-------------	------------	---------------------	--------------

RSMP-Response:

SessionID	PDU-Counter	PDU-ID (1)	Length of remainder	Response Data
-----------	-------------	------------	---------------------	---------------

شکل ۷- واحدهای داده پروتکل RSMP، RSMP-Request و RSMP-Response

همان‌طور که در شکل ۴ نشان داده شده است، پیام‌های RSMP-Request مربوط به نوع ASN.1، **RSMPmessage**، توسط RMS ها و RMC ها برای درخواست نشست ارتباطی مدیریت از دور ارسال می‌شود. پیام‌های RSMP-Response مربوط به نوع ASN.1، **RSMPmessage** فقط توسط RMC ها ارسال می‌شود.

SessionID بطور منحصر بفرد یک نشست ارتباطی را برای ITS-SCU خاص و مرکز مدیریت خاص، شناسایی می‌کند. مقدار صفر، توسط RMC در پیام RSMP-Request برای درخواست شروع یک نشست ارتباطی امن توسط یک RMS، استفاده می‌شود.

PDU-Counter در یک نشست ارتباطی، PDU ها را بطور منحصر بفردی تشخیص می‌دهد. مقدار ارائه شده در یک RSMP-Request، در RSMP-Response متناظر استفاده می‌شود.

PDU-ID، پیام‌های RSMP-Request و RSMP-Response را تشخیص می‌دهد.

1 - Security header
2 - Security trailer

Request Data:

RqDataID	Length of RqData	RqData
----------	------------------	--------

Response Data:

RsData ID	Length of RsData	RsData	Error Status
-----------	------------------	--------	--------------

شکل ۸- عناصر داده درخواست و پاسخ، RequestData و ResponseData

RqDataID ها در نوع ASN.1، RefRSMPREQ و RsDataID ها در نوع ASN.1، RefRSMPRES داده می-شوند. این ID ها بطور منحصر بفردی RqData و RsData را به ترتیب شناسایی می کنند. ErrorStatus توسط نوع ASN.1، RSMPErrStatus داده می شود.

SecHeader:

SecHeadID	Length of SecHead	SecHead
-----------	-------------------	---------

SecTrailer:

SecTrailID	Length of SecTrail	SecTrail
------------	--------------------	----------

شکل ۹- هدر و تریلر امنیتی، SecHeader و SecTrailer

SecHeadID ها و SecTrailID ها در نوع ASN.1، RefSECRSMP داده می شوند. عدم استفاده از هرگونه امنیتی توسط مقدار ASN.1، c-noSecurity داده می شود، SecHead متناظر و SecTrail متناظر از نوع ASN.1، NullType هستند.

۸ کارکردهای خدمت ابتدایی

۸-۱ خدمات ابتدایی عمومی

خدمات ابتدایی MF-COMMAND.request، MF-COMMAND.confirm، MF-REQUEST.request، MF-REQUEST.confirm، SF-REQUEST.request و SF-REQUEST.confirm در استاندارد ISO 24102-3 تعیین شده اند. این استاندارد، کارکردهای خدمات ابتدایی عمومی قابل کاربرد برای RSMP را تعیین می کند.

۲-۸ کارکردهای خدمت ابتدایی MF-SAP

۱-۲-۸ درخواست انتقال RSMP-Request و RSMP-Response

خدمت ابتدایی MF-COMMAND.request استفاده می‌شود. انواع و مقادیر ASN.1، برای کارکرد قابل کاربرد، باید مطابق با جدول ۱، با جزئیات ASN.1 تعیین شده در پیوست الف، تعیین شده باشد.

جدول ۱- درخواست انتقال RSMP-Request و RSMP-Response

MF-Command-request		
&mxref	&MXParam	توضیحات
c-rsmpMessageTX =13	RSMPmessageTX	درخواست انتقال RSMP-Request و RSMP-Response به یک ایستگاه همتا خاص
MF-Command-confirm		
&mxref	&MXParam	توضیحات
c-rsmpMessageTXconf =13	NullType	چنانچه در استاندارد ISO 24102-3 تعیین شده است، MF-Command-request، RSMPmessageTX باید با NullType و با ErrStatus تایید شود.

۲-۲-۸ اعلام دریافت RSMP-Request و RSMP-Response

خدمت ابتدایی MF-REQUEST.request استفاده می‌شود. انواع و مقادیر ASN.1، برای کارکردهای قابل کاربرد، باید مطابق جدول ۲، با جزئیات ASN.1 تعیین شده در پیوست الف، تعیین شده باشد.

جدول ۲- اعلام دریافت RSMP-Request

MF-Request-request		
&mxref	&MXParam	توضیحات
c-rsmpMessageRX =15	RSMPmessageRX	اعلام دریافت RSMP-Request و RSMP-Response از ایستگاه همتا خاص
MF-Request-confirm		
&mxref	&MXParam	توضیحات
c-rsmpMessageRXconf =15	NullType	چنانچه در استاندارد ISO 24102-3 تعیین شده است، درخواست RSMPmessageRX باید با NullType و با ErrStatus تایید شود.

۳-۸ کارکردهای خدمت ابتدایی SF-SAP

۱-۳-۸ رویه امنیتی بکار رفته برای RSMP-Request و RSMP-Response

خدمت ابتدایی SF-REQUEST.request استفاده می‌شود. انواع و مقادیر ASN.1، برای کارکردهای قابل کاربرد، باید مطابق جدول ۳، با جزئیات ASN.1 تعیین شده در پیوست الف، تعیین شده باشد.

جدول ۳- رویه امنیتی بکار رفته برای RSMP-Request

SF-Request-request		
&mxref	&MXParam	توضیحات
c-secRSMPmessageTX =2	SecRSMPmessageTX	درخواست RSMP-Request امن، نسبت به انتقال به ایستگاه همتا خاص اولویت دارد
SF-Request-confirm		
&mxref	&MXParam	توضیحات
c-secRSMPmessageTXConf =2	RMCHmessage	چنانچه در استاندارد ISO 24102-3 تعیین شده است، SF-Request-request SecRSMPmessageTX باید با یک کپی امن از RSMP-Request، یعنی RMCH-Request و با ErrStatus تایید شود.

۲-۳-۸ رویه امنیتی بکار رفته برای RSMP-Response و RMCH-Request

خدمت ابتدایی SF-Request.request استفاده می‌شود. انواع و مقادیر ASN.1، برای کارکردهای قابل کاربرد، باید مطابق جدول ۴، با جزئیات ASN.1 تعیین شده در پیوست الف، تعیین شده باشد.

جدول ۴- رویه امنیتی بکار رفته برای RMCH response و RMCH-Request

SF-Request-request		
&mxref	&MXParam	توضیحات
c-secRMCHrX =3	SecRMCHrX	درخواست برای امن کردن RMCH-Request دریافت شده از یک ایستگاه همتا خاص، نسبت به ارسال به RMPE اولویت دارد
SF-Request-confirm		
&mxref	&MXParam	توضیحات
c-secRMCHrXConf =3	RSMPmessage	چنانچه در استاندارد ISO 24102-3 تعیین شده است، SF-Request-request باید با یک کپی امن از RMCH-Request، یعنی RSMP-Request و با ErrStatus تایید شود.

۹ رویه‌های مدیریت از دور

۱-۹ شروع نشست ارتباطی مدیریت از دور

۱-۱-۹ شروع توسط سرور

یک RMS می‌تواند یک نشست ارتباطی مدیریت از دور را بر اساس هدف شروع کند. برای شروع یک نشست ارتباطی مدیریت از دور، RMS باید RSMP-Request (rmsInitSession) را به RMC در ITS-SCU مورد نظر ارسال کند.

به محض دریافت RSMP-Request (rmsInitSession)، RMC باید درخواست را با RSMP-Response (rmsInitSessionRs) تصدیق کند.

۲-۱-۹ شروع توسط مشتری

یک RMC می‌تواند یک نشست ارتباطی مدیریت از دور را بر اساس هدف شروع کند. برای درخواست شروع یک نشست ارتباطی مدیریت از دور، RMC باید RSMP-Request (`rmsInitSession`) را به مرکز مدیریت مورد نظر ارسال کند. تا زمانی که RMC یک RSMP-Request (`rmsInitSession`) را از RMS منتخب شروع کننده نشست ارتباطی درخواست شده، دریافت کند، این درخواست می‌تواند تکرار شود.

به محض دریافت RSMP-Request (`rmsInitSession`)، RMC باید درخواست را با RSMP-Response (`rmsInitSessionRs`) تصدیق کند.

۳-۱-۹ شناساگر نشست ارتباطی RSMP

هر نشست ارتباطی مدیریت از دور، توسط یک «شناساگر نشست ارتباطی RSMP» `SessionID` مربوط به نوع 1.ASN، `RsmSessionID` تخصیص داده شده توسط RMC، شناسایی می‌شود. مقادیر `SessionID` برای RMC داده شده، باید منحصر بفرد باشد. در پیام RSMP-Request درخواست کننده شروع یک نشست ارتباطی امن توسط یک RMS، مقدار صفر باید توسط RMC مورد استفاده قرار گیرد، همان‌طور که در بند ۷ تعیین شده است.

۴-۱-۹ امنیت نشست ارتباطی RSMP

جزئیات تدابیر (طرح‌واره‌های) امنیتی^۱ باید برای یک نشست ارتباطی مدیریت از دور، بکار رود، می‌تواند بین RMS و RMC مورد مذاکره قرار گیرد. این مذاکره با استفاده از RSMP-Request و PDU های RSMP-Request تعیین شده در بند ۷ اجرا می‌شود. جزئیات این PDU ها در ویرایش بعدی این استاندارد تعیین خواهد شد.

۲-۹ خاتمه نشست ارتباطی مدیریت از دور

۱-۲-۹ خاتمه فعال

به محض اینکه فعالیت‌های بیشتری از مدیریت از دور، در یک نشست ارتباطی مدیریت از دور نیاز نباشد، RMS باید نشست ارتباطی را به اتمام رساند. خاتمه نشست ارتباطی مدیریت از دور باید توسط RMS بوسیله ارسال RSMP-Request (`rmsCloseSession`) به RMC مشخص شود.

1 - Security schemes

به محض دریافت RSMP-Request (`RMScloseSession`)، RMC باید درخواست را با RSMP-Response (`rmsCloseSessionRs`)، تصدیق کرده و باید نشست ارتباطی مدیریت از دور را پایان یافته تلقی کند.

۲-۲-۹ وقفه^۱

در شرایطی که RMC، در طی یک نشست ارتباطی مدیریت از دور باز، RSMP-Requests را از RMS، برای یک نشست زمانی بیشتر از زمان مشخص شده در پارامتر مدیریتی `RSMPTimeout` مربوط به نوع ASN.1، `RSMPTimeout` دریافت نکند، RMC باید خودش به تنهایی نشست ارتباطی مدیریت از دور را به اتمام برساند.

برای حفظ نمودن نشست ارتباطی، RMS می‌تواند بطور نشست‌ای RSMP-Request `Ping-command` را که با داده مطلق که باید توسط RMS با `RMS` Response `Ping-command` (`pingRs`)، عودت دهنده داده مطلق دریافتی، تصدیق شود، ارسال کند.

۳-۲-۹ نشست ارتباطی غیرفعال

تا زمانی که RMC در یک نشست ارتباطی مدیریت از دور فعال با RMS نباشد، باید همه پیام‌های RSMP-Request، بجز یک پیام برای شروع یک نشست ارتباطی مدیریت از دور و بطور اختیاری یک RSMP-Request (`rmsCloseSession`) تکرار شده، را نادیده بگیرد.

۳-۹ به روز رسانی ثابت افزار

به روز رسانی جزئی یا کامل ثابت افزار یک ITS-SCU می‌تواند توسط RMS از طریق ارسال پیام RSMP-Request (`firmwareUpdate`) درخواست شود. به محض دریافت پیام RSMP-Request (`firmwareUpdate`)، ابتدا RMC باید دریافت پیام RSMP-Request (`firmwareUpdate`) را از طریق ارسال پیام RSMP-Response (`firmwareUpdateRs`) تصدیق کند، و سپس باید به روز رسانی درخواست شده ثابت افزار را هماهنگ با الزامات عملیات امن پلتفرمی (طرح زیربنایی)^۲ که در آن ITS-SCU نصب شده است، اجرا کند. به محض شروع مجدد خودکار ITS-SCU، پس از به روز رسانی ثابت افزار، برای تایید موفقیت عملیات و برای به اتمام رساندن صحیح نشست ارتباطی، ITS-SCU باید یک نشست ارتباطی مدیریت از دور را در RMS درخواست کند.

تا زمانی که نشست ارتباطی به روز رسانی ثابت افزار فعال است، سایر نشست‌های ارتباطی مدیریتی ممنوع است.

1 - Timeout
2 - Platform

۴-۹ نگهداری از پروتکل‌های ITS-S

پروتکل‌های ITS-S پروتکل‌هایی متفاوت با پروتکل‌های فرایندهای برنامه کاربردی ITS-S هستند که در لایه دسترسی ITS-S، لایه شبکه و انتقال ITS-S، لایه تسهیلات ITS-S، هستار مدیریت ITS-S، و هستار امنیتی ITS-S قرار دارند.

نگهداری از یک پروتکل ITS-S می‌تواند با RSMP-Request (ProtMaintenance) با ایجاد تمایز در سه نوع از عملیات نگهداری، اجرا شود.

الف- نصب یک پروتکل جدید ITS-S درخواست شده با نوع ASN.1، ProtMgmtInstallRq.

ب- به روز رسانی یک پروتکل موجود ITS-S درخواست شده با نوع ASN.1، ProtMgmtUpdateRq، پروتکل موجود ITS-S با نوع ASN.1، ProtocolID ارائه شده توسط RSC در تصدیق نصب ابتدایی، شناسایی می‌شود.

پ- حذف یک پروتکل موجود ITS-S درخواست شده با نوع ASN.1، ProtMgmtDeleteRq، پروتکل موجود ITS-S با نوع ASN.1، ProtocolID ارائه شده توسط RSC در تصدیق نصب ابتدایی، شناسایی می‌شود.

درخواست نگهداری باید توسط یک RMC با RSMP-Response (protMaintenanceRs) با ایجاد تمایز در سه نوع از عملیات نگهداری، تصدیق شود.

الف- تصدیق نصب یک فرایند جدید (یک نمونه از) برنامه کاربردی ITS-S با نوع ASN.1، ProtMgmtInstallRs تامین کننده شناساگر منحصر بفرد برنامه کاربردی از نوع ASN.1، ProtocolID از این نمونه از فرایند برنامه کاربردی ITS-S در صورت شکست، ProtInstance باید حاوی مقدار صفر باشد، در غیر این صورت باید حاوی مقدار موجود در ProtMgmtInstallRq شود.

ب- تصدیق به روز رسانی یک پروتکل موجود ITS-S با نوع ASN.1، ProtMgmtUpdateRs در صورت شکست، ProtocolID، ProtInstance موجود در ProtMgmtUpdateRs باید حاوی مقدار صفر باشد، در غیر این صورت باید حاوی مقدار موجود در ProtMgmtUpdateRq شود.

پ- تصدیق حذف یک پروتکل موجود ITS-S با نوع ASN.1، ProtMgmtDeleteRs در صورت موفقیت، ProtocolID، ProtInstance موجود در ProtMgmtDeleteRs باید حاوی مقدار صفر باشد، در غیر این صورت باید حاوی مقدار موجود در ProtMgmtDeleteRq شود.

وضعیت بازگشت نوع ASN.1، RSMPErrStatus موجود در تصدیق باید مقادیر را مطابق جدول ۵، ارائه کند.

جدول ۵- وضعیت نتیجه نگهداری پروتکل

مقدار وضعیت در RSMPErrStatus	نصب	به روز رسانی	حذف
rsmpeErrSuccess	نصب موفق	به روز رسانی موفق	حذف موفق
rsmpeErrRejected	به دلایل نامشخص، درخواست توسط RSC رد می‌شود		
rsmpeErrAppUnknown	موجود نمی‌باشد	درخواست رد می‌شود زیرا پروتکل مرجع ITS-S داده شده در نوع ASN.1، ProtocolID، در RSC ناشناخته است.	
rsmpeErrUnspecFailure	به دلایل نامشخص، درخواست شکست می‌خورد		

۵-۹ نگهداری از فرایندهای برنامه کاربردی ITS-S

نگهداری از یک فرایند برنامه کاربردی ITS-S می‌تواند با RSMPErrStatus (appMaintenance) با ایجاد تمایز در سه نوع از عملیات نگهداری، اجرا شود.

الف- نصب یک فرایند جدید (یک نمونه از) برنامه کاربردی ITS-S درخواست شده با نوع ASN.1،

AppMgmtInstallRq

ب- به روز رسانی یک فرایند موجود برنامه کاربردی ITS-S درخواست شده با نوع ASN.1، AppMgmtUpdateRq فرایند موجود برنامه کاربردی ITS-S با نوع ASN.1، ApplicationID ارائه شده توسط RSC در تصدیق نصب ابتدایی، شناسایی می‌شود.

پ- حذف یک فرایند موجود برنامه کاربردی ITS-S درخواست شده با نوع ASN.1، AppMgmtDeleteRq فرایند موجود برنامه کاربردی ITS-S با نوع ASN.1، ApplicationID ارائه شده توسط RSC در تصدیق نصب ابتدایی، شناسایی می‌شود.

درخواست نگهداری باید توسط RMC با RSMPErrStatus (appMaintenanceRs) با ایجاد تمایز در سه نوع از عملیات نگهداری، اجرا شود.

الف- تصدیق نصب یک فرایند جدید (یک نمونه از) برنامه کاربردی ITS-S با نوع ASN.1، AppMgmtInstallRs تامین کننده شناساگر منحصر بفرد برنامه کاربردی از نوع ASN.1، ApplicationID از این نمونه از فرایند برنامه کاربردی ITS-S. در صورت شکست، ApplicationID.AppInstance باید حاوی مقدار صفر باشد، در غیر اینصورت باید حاوی مقدار موجود در AppMgmtInstallRq شود.

ب- تصدیق به روز رسانی یک فرایند موجود برنامه کاربردی ITS-S با نوع ASN.1، **AppMgmtUpdateRs**، در صورت شکست، **ApplicationID.AppInstance** موجود در **AppMgmtUpdateRs** باید حاوی مقدار صفر باشد، در غیر این صورت باید حاوی مقدار موجود در **AppMgmtUpdateRq** شود.

پ- تصدیق حذف یک فرایند موجود برنامه کاربردی ITS-S با نوع ASN.1، **AppMgmtDeleteRs**، در صورت موفقیت، **ApplicationID.AppInstance** موجود در **AppMgmtDeleteRs** باید حاوی مقدار صفر باشد، در غیر این صورت باید حاوی مقدار موجود در **AppMgmtDeleteRq** شود.

وضعیت بازگشت نوع ASN.1، **RSMPErrStatus** موجود در تصدیق باید مقادیر را مطابق جدول ۶، ارائه کند.

جدول ۶- وضعیت نتیجه نگهداری برنامه کاربردی

مقدار وضعیت در RSMPErrStatus	نصب	به روز رسانی	حذف
rsmpErrSuccess	نصب موفق	به روز رسانی موفق	حذف موفق
rsmpErrRejected	به دلایل نامشخص، درخواست توسط RSC رد می شود		
rsmpErrAppUnknown	موجود نمی باشد	درخواست رد می شود زیرا نصب مرجع فرایند برنامه کاربردی ITS-S داده شده در نوع ASN.1، ApplicationID در RSC ناشناخته است.	
rsmpErrUnspecFailure	به دلایل نامشخص، درخواست شکست می خورد		

۶-۹ نگهداری اطلاعات پیکربندی

به منظور قرائت مقدار یک یا چند پارامتر مدیریتی (M-Params تعیین شده در استاندارد 1-ISO 24102)، یک RMS باید پیام **RSMP-Request (getMparams)** را ارسال کند. به محض دریافت پیام **RSMP-Response Request (getMparams)**، RMC باید اطلاعات درخواستی را در پیام **RSMP-Response (getMparamsRs)** برگرداند. در صورتی که مقدار پارامتر نتواند ارائه شود، باید در **RSMP-Response (getMparamsRs)** حذف شود.

به منظور نوشتن مقدار یک یا چند پارامتر مدیریتی (M-Params تعیین شده در استاندارد 1-ISO 24102)، یک RMS باید پیام **RSMP-Request (setMparams)** را ارسال کند. به محض دریافت **RSMP-Response (setMparams)**، RMC باید تنظیمات پارامتر درخواستی را در صورتی که خطای عدم دسترسی رخ دهد، اجرا کند و باید موفقیت یا شکست را در **RSMP-Response (setMparamsRs)** گزارش کند. در صورتی که تنظیمات همه پارامترهای درخواستی بتواند اجرا شود، وضعیت نتایج جهانی باید به مقدار

«rsmpErrSuccess» تنظیم شود. در غیر این صورت، وضعیت نتایج جهانی باید به مقدار «rsmpErrSetErrorGeneral» تنظیم شود و جزئیات وضعیت نتایج برای هر شکستی که رخ می‌دهد برگردانده شود.

۱۰ استفاده از FSAP

۱-۱۰ کلیات

«پروتکل اعلان خدمت سریع» (FSAP) در مرجع [2] کتاب‌نامه تعیین شده است. این استاندارد بخشی از استفاده از FSAP یا RSMP را تعیین می‌کند. سایر قسمت‌های استاندارد ISO 24102 برای ویژگی‌های خاص دیگر در نظر گرفته شده است.

۱۰-۲ SAM

ITS-AID ارائه شده در یک «پیام اعلان خدمت» (SAM)^۱ باید برابر مقدار ثبت شده ۱۳۴ از RMPE باشد. فیلد serverPort در یک SAM باید عدد ثبت شده مشخص ۳۲۷۶۳ از PORT_RSM را نشان دهد (به مرجع [3] کتاب‌نامه مراجعه کنید).

فیلد serviceData در یک SAM می‌تواند حاوی شناساگر منحصر بفرد نوع ASN.1، ItsScuCmcID از ITS-SCU-CMC تعیین شده در استاندارد CEN/ISO/TS 17419 که مدیریت از دور ایستگاه را پیشنهاد می‌دهد، باشد. در صورتی که ITS-SCU-CMC های متفاوتی در دسترس باشند، فیلد serviceData باید خالی باشد.

۱۰-۳ CTX

ITS-AID ارائه شده در یک «پیام محتوی خدمت» (CTX)^۲ باید برابر با مقدار ثبت شده ۱۳۴ از RMPE باشد.

فیلد clientPort باید حاوی شماره درگاه از RMC باشد که بصورت پویا تخصیص داده شده است، همان‌طور که در مراجع [2] و [3] کتاب‌نامه تعیین شده است.

فیلد contextData باید حاوی شناساگر منحصر بفرد نوع ASN.1، ItsScuCmcID از ITS-SCU-CMC مناسب تعیین شده در CEN/ISO/TS 17419 باشد.

1 - Service Advertisement Message

2 - Service Context Message

پیوست الف

(الزامی)

ماژول (پودمان) های ASN.1

الف- ۱ نمای کلی

ماژول ASN.1 که در ادامه آمده، در این پیوست تعیین شده است:

ITSSremoteMgmt { ISO (1) standard (0) calm-management (24102) remote (2) asnm-1 (1)}
 به روز رسانی‌های بر خط این ماژول ASN.1، خصوصاً اصلاحیه‌های مربوط به نمونه‌های انواع CLASS، در وبسایت نگهداری ISO به نشانی <http://standards.iso.org/iso/24102/-2> منتشر خواهد شد.

الف-۲ ماژول ITSSremoteMgmt

این ماژول، تعاریف نوع ASN.1 به همراه تعاریف مقدار مفید ASN.1 را تعیین می‌کند.

برای این ماژول ASN.1، قوانین گدگشایی بسته‌ای غیرمنظم (PER)^۱، چنانچه در استاندارد ISO/IEC 8825-2 تعیین شده است، باید بکار رود.

برای به روز رسانی این ماژول ASN.1، به وبسایت نگهداری ISO به نشانی <http://standards.iso.org/iso/24102/-2> مراجعه کنید.

```
ITSSremoteMgmt { iso (1) standard (0) calm-management (24102) remote (2) asnm-1
    ((1
DEFINITIONS AUTOMATIC TAGS ::= BEGIN
IMPORTS
NullType, Time48IAT, Lat, Lon FROM CALMllsap {iso(1) standard(0) calm-ll-sap(21218)
asnm-1
{()
MPARAM, RefMPARAM, Param24102No, Param24102, ApplicationID FROM CALMmanagement {
iso (1(
standard (0) calm-management (24102) local (1) asnm-1 (1{(
SFSAP-RR, RefSFSAP-RR, SFSAP-RC, RefSFSAP-RC, MFSAP-RC, RefMFSAP-RC, MFSAP-RR,
RefMFSAP-RR, MFSAP-CC, RefMFSAP-CC, MFSAP-CR, RefMFSAP-CR, MIconmand, MNcommand,
MFcommand, MIconmand, MScommand FROM CALMmsap { iso (1) standard (0) calm-
management
(۲۶)۰۲)msap (3) asnm-1 (1{(
ITSScuID, ItsScuCmcID, ITSaid, ITSSapPrPr, ITSSapdID, ITSSpPr, ITSaoID, ITSpID,
```

¹ - Packed encoding rules

```

ITSSpdID, ITSpdID, ProtocolID FROM CITSapplMgmtApplReg {iso(1) standard(0) cits-
applMgmt
  (\۷۴\۹)applRegistry (2{(
;
--End of IMPORTS
--Types
--Security header and trailer--
SECRSMP::=CLASS}
&ref RefSECRSMP, -- security type identifier
&SecRSMP
{
RefSECRSMP::=INTEGER}
c-noSecurity (0,(
c-octString (1(
)(0..255)
SecRSMPs SECRSMP::={noSecurity | octString, ...}
noSecurity SECRSMP::={&ref c-noSecurity, &SecRSMP NullType}
octString SECRSMP::={&ref c-octString, &SecRSMP OctStringSec}
OctStringSec::=OCTET STRING (SIZE(0..65535))
SecHeader::=SEQUENCE{
secRef SECRSMP.&ref({SecRSMPs}),
secHead SECRSMP.&SecRSMP({SecRSMPs}{@secRef})
}
SecTrailer::=SEQUENCE{
secRef SECRSMP.&ref({SecRSMPs}),
secTrail SECRSMP.&SecRSMP({SecRSMPs}{@secRef})
}
-- RSMP-Request and RSMP-Response common parts
-- RSMP PDU-ID
RsmppDUCounter::=INTEGER(0..65535) -- cyclic counter
RsmppSessionID::=INTEGER(0..65535) -- cyclic counter
RSMPPDU::=CLASS{
&ref RefRSMPPDU, -- management request type identifier
&RSMPPdu
}
RefRSMPPDU::=INTEGER{
c-requestPDU (0),
c-responsePDU (1)
} (0..255)
RSMPPdus RSMPPDU::={requestPDU | responsePDU, ...}
requestPDU RSMPPDU::={&ref c-requestPDU, &RSMPPdu RequestData}

```



```

responsePDU RSMPPDU::={&ref c-responsePDU, &RSMPPdu ResponseData}
RSMPPmessage::=SEQUENCE{
  sessionID RsmppSessionID,
  pduCounter RsmppPDUcounter,
  pduID RSMPPDU.&ref({RSMPPdus}),
  pdu RSMPPDU.&RSMPPdu({RSMPPdus}{@pduID})
}
-- RSMP-Request
RSMPPREQ::=CLASS{
  &ref RefRSMPREQ, -- management request type identifier
  &RSMPPrequest
}
-- RqDataIDs
RefRSMPREQ::=INTEGER{
  c-pingRq (0),
  c-rmcReqSession (1),
  c-rmsInitSession (2),
  c-rmsCloseSession (3),
  c-getMparams (4),
  c-setMparams (5),
  c-firmwareUpdate (6),
  c-protMaintenance (7),
  c-appMaintenance (8)
} (0..255)
RSMPPrequests RSMPPREQ::={pingRq | rmcReqSession | rmsInitSession | rmsCloseSession |
getMparams | setMparams | firmwareUpdate | protMaintenance | appMaintenance, ...}
pingRq RSMPPREQ::={&ref c-pingRq, &RSMPPrequest RSMPPping}
rmcReqSession RSMPPREQ::={&ref c-rmcReqSession, &RSMPPrequest RMCreqSession}
rmsInitSession RSMPPREQ::={&ref c-rmsInitSession, &RSMPPrequest RMSinitSession}
rmsCloseSession RSMPPREQ::={&ref c-rmsCloseSession, &RSMPPrequest RMScloseSession}
getMparams RSMPPREQ::={&ref c-getMparams, &RSMPPrequest GetMparams}
setMparams RSMPPREQ::={&ref c-setMparams, &RSMPPrequest SetMparams}
firmwareUpdate RSMPPREQ::={&ref c-firmwareUpdate, &RSMPPrequest FirmwareUpdate}
protMaintenance RSMPPREQ::={&ref c-protMaintenance, &RSMPPrequest ProtMaintenance}
appMaintenance RSMPPREQ::={&ref c-appMaintenance, &RSMPPrequest AppMaintenance}
RSMPPping::=OCTET STRING (SIZE(0..255))
-- RMC request for secure session initiation
-- Class to indicate reason for session initiation request by RMC
RMCREQREASON::=CLASS{
  &ref RefRMCREQREASON, -- reason identifier
  &RMCreqReason
}

```

```

}
-- IDs of reasons for session initiation request by RMC
RefRMCREQREASON::=INTEGER{
c-rmcRqNoReason (0), -- maybe RMS has news?
c-rmcRqExceptLogFile (1), -- exception occurred. RMS should read logfile.
c-rmcRqRegulUpdate (2) -- need regulatory info update.
} (0..255)

RMCCreqReasons      RMCREQREASON:={rmcRqNoReason      |      rmcRqExceptLogFile      |
rmcRqRegulUpdate, ...}

rmcRqNoReason RMCREQREASON:={&ref c-rmcRqNoReason, &RMCCreqReason NullType}

rmcRqExceptLogFile RMCREQREASON:={&ref c-rmcRqExceptLogFile, &RMCCreqReason
ExceptionID}

rmcRqRegulUpdate RMCREQREASON:={&ref c-rmcRqRegulUpdate, &RMCCreqReason
RegulUpdateRq}

ExceptionID::=INTEGER{
exceptUnknown (0)
}

RegulUpdateRq::=SEQUENCE{
-- ID of regulatory issue
lat Lat, -- latitude of RMC position
lon Lon -- longitude of RMC position
}

RMCCreqReas::=SEQUENCE{
rmcRqReasonRef RMCREQREASON.&ref({RMCCreqReasons}),
reason RMCREQREASON.&RMCCreqReason({RMCCreqReasons}{@rmcRqReasonRef})
RMCCreqSession::=SEQUENCE{
itsscuID ITSScuID, -- ITS-SCU-ID
itsScuCmcID ItsScuCmcID, -- unique ID of intended RMS
reqReas RMCCreqReas, -- reason for session request
prevSessionID RsmppSessionID -- previous sessionID with intended RMS
}

RMSinitSession::=SEQUENCE{
itsScuCmcID ItsScuCmcID, -- unique ID of RMS
itsscuID ITSScuID -- ITS-SCU-ID
}

RMScloseSession::=SEQUENCE{
itsScuCmcID ItsScuCmcID, -- unique ID of intended RMS
itsscuID ITSScuID -- ITS-SCU-ID
}

GetMparams::=SEQUENCE OF Param24102No
SetMparams::=SEQUENCE OF Param24102
FirmwareUpdate::=SEQUENCE{

```

```

firmware OCTET STRING -- specific to management centre
}
PROTMNT:=CLASS{
  &ref RefMNT,
  &PROTmntc
}
ProtMaintenance:=SEQUENCE{
  protMntRef PROTMNT.&ref({ProtMntRqs}),
  protMgmtTask PROTMNT.&PROTmntc({ProtMntRqs}{@protMntRef})
}
RefMNT:=INTEGER{
  c-MntInstall (0),
  c-MntUpdate (1),
  c-MntDelete (2)
}
ProtMntRqs PROTMNT:={installProtRq | updateProtRq | deleteProtRq, ...}
installProtRq PROTMNT:={&ref c-MntInstall, &PROTmntc ProtMgmtInstallRq}
updateProtRq PROTMNT:={&ref c-MntUpdate, &PROTmntc ProtMgmtUpdateRq}
deleteProtRq PROTMNT:={&ref c-MntDelete, &PROTmntc ProtMgmtDeleteRq}
ProtMgmtInstallRq:=SEQUENCE{
  protID ITSprotID, -- ITS protocol identifier
  itspoID ITSpID, -- ITS protocol owner
  itsspdID ITSSpdID, -- ITS-S protocol developer
  itsspPr ITSSpPr, -- ITS-S protocol provisioner
  protCode ProtCode -- software to be installed
}
ProtCode:=OCTET STRING
ProtMgmtUpdateRq:=SEQUENCE{
  protI ProtocolID, -- of ITS-S protocol to be updated
  itspoID ITSpID, -- ITS protocol owner
  itsspdID ITSSpdID, -- ITS-S protocol developer
  itsspPr ITSSpPr, -- ITS-S protocol provisioner
  protPackage ProtCode -- software to be installed
}
ProtMgmtDeleteRq:=ProtocolID -- of ITS-S protocol to be deleted
APPMNT:=CLASS{
  &ref RefMNT,
  &APPmntc
}
AppMaintenance:=SEQUENCE{
  appMntRef APPMNT.&ref({AppMntRqs}),

```

```

appMgmtTask APPMNT.&APPmntc({AppMntRqs}{@appMntRef})
}
AppMntRqs APPMNT::={installAppRq | updateAppRq | deleteAppRq, ...}
installAppRq APPMNT::={&ref c-MntInstall, &APPmntc AppMgmtInstallRq}
updateAppRq APPMNT::={&ref c-MntUpdate, &APPmntc AppMgmtUpdateRq}
deleteAppRq APPMNT::={&ref c-MntDelete, &APPmntc AppMgmtDeleteRq}
AppMgmtInstallRq::=SEQUENCE{
itsAID ITSaid, -- ITS application identifier
itsaooID ITSaooID, -- ITS application object owner
itssapdID ITSSapdID, -- ITS-S application process developer
itssapPrPr ITSSapPrPr, -- ITS-S application process provisioner
appPackage OCTET STRING -- software to be installed
}
AppMgmtUpdateRq::=SEQUENCE{
appID ApplicationID, -- of ITS-S application process to be updated
itsaooID ITSaooID, -- ITS application object owner
itssapdID ITSSapdID, -- ITS-S application process developer
itssapPrPr ITSSapPrPr, -- ITS-S application process provisioner
appCode AppCode -- software to be installed
{
AppCode::=OCTET STRING
AppMgmtDeleteRq::=ApplicationID -- of ITS-S application process to be deleted
RequestData::=SEQUENCE}
rsmpRqRef RSMPREQ.&ref({RSMPRequests,({
request RSMPREQ.&RSMPrequest({RSMPRequests){@rsmpRqRef({
{
--RSMP-Response
RSMPPRES::=CLASS}
&ref RefRSMPRES, -- management response type identifier
&RSMPresponse
{
--RsDataIDs
RefRSMPRES::=INTEGER}
c-pingRs (0,(
c-nullResponse (1,(
c-rmsInitSessionRs (2,(
c-rmsCloseSessionRs (3,(
c-getMparamsRs (4,(
c-setMparamsRs (5,(
c-firmwareUpdateRs (6,(
c-protMaintenanceRs (7,(

```

```

c-appMaintenanceRs (8(
(۲۵۵..۰){
RSMPPresponses RSMPRES:={pingRs | nullResponse | rmsInitSessionRs |
rmsCloseSessionRs|
getMparamsRs | setMparamsRs | firmwareUpdateRs | protMaintenanceRs |
appMaintenanceRs{... ,
pingRs RSMPRES:={&ref c-pingRs, &RSMPPresonse RSMPPing{
nullResponse RSMPRES:={&ref c-nullResponse, &RSMPPresonse NullType{
rmsInitSessionRs RSMPRES:={&ref c-rmsInitSessionRs, &RSMPPresonse
RMSinitSessionRs{
rmsCloseSessionRs RSMPRES:={&ref c-rmsCloseSessionRs, &RSMPPresonse
RMScloseSessionRs{
getMparamsRs RSMPRES:={&ref c-getMparamsRs, &RSMPPresonse GetMparamsRs{
setMparamsRs RSMPRES:={&ref c-setMparamsRs, &RSMPPresonse SetMparamsRs{
firmwareUpdateRs RSMPRES:={&ref c-firmwareUpdateRs, &RSMPPresonse
FirmwareUpdateRs{
protMaintenanceRs RSMPRES:={&ref c-protMaintenanceRs, &RSMPPresonse
ProtMaintenanceRs{
appMaintenanceRs RSMPRES:={&ref c-appMaintenanceRs, &RSMPPresonse
AppMaintenanceRs{
RMSinitSessionRs:=SEQUENCE}
itsScuCmcID ItsScuCmcID, -- unique ID of RMS
itsscuID ITSscuID, -- ITS-SCU-ID
resultStatus RSMPErrStatus -- (success / rejected(
{
RMScloseSessionRs:=SEQUENCE}
itsScuCmcID ItsScuCmcID, -- unique ID of intended RMS
itsscuID ITSscuID, -- ITS-SCU-ID
resultStatus RSMPErrStatus -- (success / rejected(
{
GetMparamsRs:=SEQUENCE OF Param24102
SetMparamsRs:=SEQUENCE}
globalStat RSMPErrStatus, -- success or setErrorGeneral
detailStat DetailStatusSetMparams -- present in case of errors
{
DetailStatusSetMparams:=SEQUENCE (SIZE(0..255)) OF SetMparamStatus
SetMparamStatus:=SEQUENCE}
paramNo Param24102No,
resultCode RSMPErrStatus
}
FirmwareUpdateRs:=SEQUENCE{
resultStatus RSMPErrStatus -- (success / rejected)
}

```

```

ProtMaintenanceRs ::= SEQUENCE {
    protMntRef PROT MNT . &ref ({ProtMntRss}),
    protMgmtTask PROT MNT . &PROT mntc ({ProtMntRss} {@protMntRef}),
    resultStatus RSMPErrStatus -- (success / accessViolation/protUnknown)
}

ProtMntRss PROT MNT ::= {installProtRs | updateProtRs | deleteProtRs, ...}
installProtRs PROT MNT ::= {&ref c-MntInstall, &PROT mntc ProtMgmtInstallRs}
updateProtRs PROT MNT ::= {&ref c-MntUpdate, &PROT mntc ProtMgmtUpdateRs}
deleteProtRs PROT MNT ::= {&ref c-MntDelete, &PROT mntc ProtMgmtDeleteRs}
ProtMgmtInstallRs ::= ProtocolID -- with instance = 0 in case of failure
ProtMgmtUpdateRs ::= ProtocolID -- with instance = 0 in case of failure
ProtMgmtDeleteRs ::= ProtocolID -- with instance = 0 in case of success
AppMaintenanceRs ::= SEQUENCE {
    appMntRef APP MNT . &ref ({AppMntRqs}),
    appMgmtTask APP MNT . &APP mntc ({AppMntRqs} {@appMntRef}),
    resultStatus RSMPErrStatus -- (success / accessViolation/appUnknown)
}

AppMntRqs APP MNT ::= {installAppRs | updateAppRs | deleteAppRs, ...}
installAppRs APP MNT ::= {&ref c-MntInstall, &APP mntc AppMgmtInstallRs}
updateAppRs APP MNT ::= {&ref c-MntUpdate, &APP mntc AppMgmtUpdateRs}
deleteAppRs APP MNT ::= {&ref c-MntDelete, &APP mntc AppMgmtDeleteRs}
AppMgmtInstallRs ::= ApplicationID -- with instance = 0 in case of failure
AppMgmtUpdateRs ::= ApplicationID -- with instance = 0 in case of failure
AppMgmtDeleteRs ::= ApplicationID -- with instance = 0 in case of success
ResponseData ::= SEQUENCE {
    rsmprRsRef RSM PRES . &ref ({RSMPresponses}),
    response RSM PRES . &RSM response ({RSMPresponses} {@rsmprRsRef}),
    error RSMPErrStatus
}

-- Error Status in RSM P - share values with ErrStatus in ISO 24102-3
RSMPErrStatus ::= INTEGER {
    rsmprErrSuccess (0), -- = accepted
    rsmprErrUnspecFailure (1),
    rsmprErrParamNoUnknown (2),
    rsmprErrAccessViolation (3),
    rsmprErrRejected (64),
    rsmprErrPduUnknown (65),
    rsmprErrSetErrorGeneral (66),
    rsmprErrAppUnknown (67),
    rsmprErrProtUnknown (68)
} (0..255)

```

```

-- Complements CALMmsap SAP functions
-- { iso (1) standard (0) calm-management (24102) msap (3) asnm-1 (1)}
-- MF-SAP Command.request --
-- send an RSMP message
rsmpMessageTX MFSAP-CR:={&mxref c-rsmpMessageTX, &MXParam RSMPmessageTX}
c-rsmpMessageTX RefMFSAP-CR:=13
RSMPmessageTX:=SEQUENCE{
rsmpRequest RSMPmessage
}
-- MF-SAP Command.confirm --
rsmpMessageTXconf MFSAP-CC:={&mxref c-rsmpMessageTXconf, &MXParam NullType}
c-rsmpMessageTXconf RefMFSAP-CC:=13
-- MF-SAP Request.request --
-- receive an RSMP message
rsmpMessageRX MFSAP-RR:={&mxref c-rsmpMessageRX, &MXParam RSMPmessageRX}
c-rsmpMessageRX RefMFSAP-RR:=15
RSMPmessageRX:=SEQUENCE{
rsmpRequest RSMPmessage
}
-- MF-SAP Request.confirm --
rsmpMessageRXconf MFSAP-RC:={&mxref c-rsmpMessageRXconf, &MXParam NullType}
-- could be omitted
c-rsmpMessageRXconf RefMFSAP-RC:=15
-- SF-SAP Request.request --
secRSMPmessageTX SFSAP-RR:={&mxref c-secRSMPmessageTX, &MXParam SecRSMPmessageTX}
secRMChRX SFSAP-RR:={&mxref c-secRMChRX, &MXParam SecRMChRX}
c-secRSMPmessageTX RefSFSAP-RR:=2
c-secRMChRX RefSFSAP-RR:=3
SecRSMPmessageTX:=SEQUENCE{
rsmpRequestTX RSMPmessageTX
}
SecRMChRX:=SEQUENCE{
rmchRX RMChmessage -- something is received
}
RMChmessage:=SEQUENCE{
header SecHeader,
rmchMsg OCTET STRING, -- result of security procedure
trailer SecTrailer
}
-- SF-SAP Request.conf -

```

```
secRSMPmessageTXConf SFSAP-RC::={&mxref c-secRSMPmessageTXConf, &MXParam
RMCHmessage{
secRMCHrxConf SFSAP-RC::={&mxref c-secRMCHrxConf, &MXParam RSMPmessage{
c-secRSMPmessageTXConf RefSFSAP-RC::=2
c-secRMCHrxConf RefSFSAP-RC::=3
--Management parameters Param24102--
-- extends ASN.1 module from ISO 24102-1
c-RSMPTIMEOUT RefMPARAM::=12
rsmpTimeout MPARAM::={&paramRef c-RSMPTIMEOUT, &Parameter RSMPTimeout}
RSMPTimeout::=INTEGER(0..65535) -- time in milliseconds
/*
The ASN.1 specification has been checked for conformance to the ASN.1
standards by OSS ASN.1 Syntax Checker, and by OSS ASN-1STEP
*/
END
```


پیوست ب

(آگاهی دهنده)

پارامترهای خدمت ارتباطی

جدول ب-۱ پارامترهای خدمت ارتباطی تعیین شده در استاندارد CEN/ISO/TS 17423 که برای RSMP در مُد (حالت) شروع مستقیم سرور و مُد شروع مشتری قابل کاربرد است را نشان می‌دهد. پارامترهای خدمت ارتباطی قابل کاربرد برای شروع سرور مبتنی بر FSAP، مواردی هستند که برای FSAP تعیین شده در مرجع [2] کتاب‌نامه تعیین شده است.

جدول ب-۱- پارامترهای خدمت ارتباطی

پارامتر خدمت ارتباطی	مقدار	توضیح
پارامترهای خدمت ارتباطی عملیاتی		
CSP_LogicalChannelType	rsmPLCH	کانال مدیریت پیکربندی ITS-SCU
CSP_ContConnect	{duration TimeDurationValue, interrupt TRUE}	اتصال پیوسته مورد نیاز برای نشست ارتباطی مدیریتی. مدت زمانی بستگی به وظیفه مدیریتی دارد. نشست ارتباطی ممکن است قطع شود.
CSP_NxPepeat	موجود نمی باشد	عدم تکرار
CSP_StoreAndForward	موجود نمی باشد	عدم نیاز به قابلیت ذخیره یا ارسال
CSP_FlowType	موجود نمی باشد	عدم ارائه نوع جریان مشخص
پارامترهای خدمت ارتباطی مقصد		
CSP_DestinationType	[0]:2	بر مبنای نشانی، تک پخشی
CSP_DestinationDomain	۸	جهانی
CSP_CommDistance	موجود نمی باشد	
CSP_Directivity	موجود نمی باشد	
پارامترهای خدمت ارتباطی اجرایی		
CSP_Resilience	مورد نیاز	کامل بودن پیام
CSP_MinThP	موجود نمی باشد	
CSP_MaxLat	موجود نمی باشد	
CSP_MaxADU	<حداکثر اندازه پیام>	بستگی به وظیفه مدیریتی دارد. ممکن است برای اطمینان از تکه تکه شدن کامل، نیاز به تکه تکه سازی و پروتکل انتقال TCP-like باشد.
پارامترهای خدمت ارتباطی امنیتی		
CSP_DataConfidentiality	موجود نمی باشد	اجرا شده توسط RMCH
CSP_DataIntegrity	موجود نمی باشد	اجرا شده توسط RMCH
CSP_NonPepudiation	موجود نمی باشد	اجرا شده توسط RMCH
CSP_SourceAuthentication	موجود نمی باشد	اجرا شده توسط RMCH
پارامترهای خدمت ارتباطی پروتکل		
CSP_Protocol	موجود نمی باشد	

کتابنامه

- [1] ISO 21218, Intelligent transport systems — Communications access for land mobiles (CALM) — Access technology support
- [2] ISO 24102-5, Intelligent transport systems — Communications access for land mobiles (CALM) —ITS station management — Part 5: Fast service advertisement protocol (FSAP)
- [3] ISO 29281-1, Intelligent transport systems — Communication access for land mobiles (CALM) —Non-IP networking — Part 1: Fast networking & transport layer protocol (FNTP)
- [4] CEN/ISO/TS 17419, Intelligent Transport Systems — Cooperative Systems — Classification and management of ITS applications in a global context
- [5] CEN/ISO/TS 17423, Intelligent Transport Systems — Cooperative Systems — Application requirements for selection of communication profiles