بسمه تعالی

شماره : ۱۱۰/۳۳۶
تاریخ : ۱۴۰۱/۰۹/۰۵
پیوست : ندارد

تولید، دانش‌بنیان و اشتغال‌آفرین
مقام معظم رهبری

مرکز مدیریت آمار و فناوری اطلاعات
وزارت بهداشت، درمان و آموزش پزشکی

مدیریت محترم آمار و فناوری اطلاعات دانشکده / دانشگاه علوم پزشکی و خدمات بهداشتی، درمانی سراسر کشور

مدیرعامل محترم شرکت/مجموعه توسعه دهنده سامانه اطلاعات بیمارستانی

مدیرعامل محترم شرکت/مجموعه توسعه دهنده سامانه اطلاعات آزمایشگاهی

موضوع : اخذ تاییدیه مطابقت با استانداردهای زیرساخت کلید عمومی کشور برای سامانه های اطلاعاتی حوزه سلامت

با سلام

احتراما، به استحضار می رساند با عنایت به آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیک و تصویب مدل سلسله مراتبی متشکل از شورای سیاست گذاری گواهی الکترونیکی به منظور رسمیت بخشیدن به امضای الکترونیکی در کشور، مرکز صدور گواهی الکترونیکی میانی سلامت زیر نظر مرکز دولتی صدور گواهی الکترونیکی ریشه، به عنوان مرجع صدور گواهی در حوزه سلامت کشور می باشد. با آغاز نظام نسخه نویسی الکترونیک، و مطرح شدن الزامات جدید در حفظ اصول امنیت در فضای تبادل الکترونیکی اطلاعات از جمله محرمانگی، جامعیت، انکارناپذیری و تصدیق هویت، استناد پذیری اسناد و داده پیام‌هایی که جایگزین اسناد و مکاتبات می گردند، بهره برداری از امضای الکترونیکی دارای الزام حقوقی بوده و آماده سازی سامانه های اطلاعاتی حوزه سلامت جهت مطابقت با استانداردهای زیرساخت کلید عمومی کشور اجتناب ناپذیر و پیش نیاز بهره برداری است.

با توجه به الزامات مذکور و پیرو کارگاه مورخ ۱۴۰۱/۰۸/۲۴ خواهشمند است دستور فرمائید اقدامات لازم جهت اخذ گواهینامه مطابقت با زیرساخت کلید عمومی کشور از آزمایشگاه ارزیابی نرم‌افزارهای مبتنی بر PKI مورد تایید مرکز دولتی صدور گواهی الکترونیکی ریشه برای کلیه سامانه‌های اطلاعاتی حوزه سلامت اعم از بیمارستانی، آزمایشگاهی و نسخه نویسی مورد استفاده انجام و تصویر گواهی مذکور به این مرکز ارسال گردد.

امین بیگلرخانی
رئیس مرکز مدیریت آمار و فناوری اطلاعات
وزارت بهداشت، درمان و آموزش پزشکی

رونوشت :

- معاون توسعه مدیریت و منابع (جناب آقای دکتر بهروز رحیمی)

جناب آقای مهندس حسن هاشمی رئیس محترم سازمان نظام صنفی رایانه ای کشور

ریاست محترم مرکز توسعه تجارت الکترونیکی

شهرک قدس، خیابان سیمای ایران، بین فلامک و زرافشان، ستاد مرکزی وزارت بهداشت، درمان و آموزش پزشکی، بلوک A، طبقه پنجم
تلفن: ۲-۸۱۴۵۳۶۰۱ نمابر: ۸۱۴۵۶۵۰۳ نشانی اینترنتی: it.behdasht.gov.ir نشانی پست الکترونیکی: it@behdasht.gov.ir

مرکز مدیریت آمار و فناوری اطلاعات
وزارت بهداشت، درمان و آموزش پزشکی

بسمه تعالی

شماره : د/۱۱۰/۱۶۳۳
تاریخ : ۱۴۰۲/۰۸/۱۳
پیوست : دارد

مهم-حائز اهمیت

مهار تورم و رشد تولید
((مقام معظم رهبری))

رؤسای محترم دانشگاه ها/دانشکده های علوم پزشکی و خدمات بهداشتی درمانی...

موضوع : تاکید بر اجرا و پیاده سازی دستورالعمل ها و یا سرویس های ابلاغی وزارت متبوع در سال ۱۴۰۲

با سلام واحترام

با عنایت به اولویت‌دهی و تاکید بر اجرایی‌سازی مجموعه وب‌سرویس‌های مبتنی بر عملکرد شامل کارانه بیمارستان، پرستاران و درآمد بیمارستانی و سند متحدالشکل گزارش سامانه‌های اطلاعات بیمارستانی و یا کلینیکی برای دستورالعمل پرداخت کارانه گروه پرستاری، موضوع ابلاغیه‌های شماره ۱۱۰/۲۲۶ مورخ ۱۴۰۲/۰۶/۱۱، ۱۱۰/۲۳۵مورخ ۱۴۰۲/۰۶/۲۱ و شماره ۱۱۰/۲۵۹مورخ ۱۴۰۲/۰۷/۰۵ به استحضار می‌رساند، عطف به نامه شماره ۲۱۳۰/ص ت۱۴۰۲ مورخ ۱۴۰۲/۰۷/۱۲ سازمان نظام صنفی رایانه‌ای کشور همکاری و پاسخگویی مناسبی در بیمارستان‌های دانشگاهی کشور جهت راه‌اندازی و صحت‌سنجی اجرای دستورالعمل مذکور صورت نگرفته است که این موضوع باعث تاخیر در اجرای سراسری سرویس کارانه پرستاری در بیمارستان‌های کشور در مهلت مقرر گردیده است.

لازم بذکر است با وجود تاکیدات بسیار بر اهمیت و اولویت اجرا و پیاده‌سازی دستورالعمل‌ها و یا سرویس‌های ابلاغی وزارت متبوع در سال ۱۴۰۲ (موضوع مکاتبه شماره ۱۱۰/۱۹۴ مورخ ۱۴۰۲/۰۶/۰۱ با سازمان نظام صنفی رایانه‌ای)، همچنان بازدیدها و بررسی‌های میدانی نشان‌دهنده عدم اجرای دستورالعمل‌ها و وب‌سرویس‌های مورد اشاره در مهلت مقرر می‌باشد که به عنوان نمونه در تبادل اطلاعات مصدومین ترافیکی و شناسه کروکی شرایط و الزامات اجرایی فنی برای اجرای وب‌سرویس توسط توسعه‌دهندگان سامانه‌های اطلاعات بیمارستانی در اکثر بیمارستان های کشور فراهم نشده است.

شهرک قدس، خیابان سیمای ایران، بین فلامک و زرافشان، ستاد مرکزی وزارت بهداشت، درمان و آموزش پزشکی، بلوک A، طبقه پنجم
تلفن: ۲-۸۱۴۵۳۶۰۱ نمابر: ۸۱۴۵۶۵۰۳ نشانی اینترنتی: it.behdasht.gov.ir نشانی پست الکترونیکی: it@behdasht.gov.ir

بسمه تعالی

مرکز مدیریت آمار و فناوری اطلاعات
وزارت بهداشت، درمان و آموزش پزشکی

شماره : د/۱۱۰/۱۶۳۳
تاریخ : ۱۴۰۲/۰۸/۱۳
پیوست : دارد

مهم-حائز اهمیت

مهار تورم و رشد تولید
((مقام معظم رهبری))

همچنین پیرو نامه سازمان بیمه سلامت ایران به شماره ۱۴۰۲/۱۹۹۰۱۹ مورخ ۱۴۰۲/۰۶/۰۵ و نامه‌های شماره ۴۰۰/۱۵۰۷۷د مورخ ۱۴۰۲/۰۶/۱۴ و شماره ۱۱۰/۱۱۵۳/د مورخ ۱۴۰۱/۰۶/۱۲ مبنی بر تخصیص اعتبار به دانشگاه‌های علوم‌پزشکی کشور، انتظار می‌رود نظارت جدی و مستمر بر موضوع اجرا و پیاده‌سازی سرویس‌ها و دستورالعمل‌های ابلاغی تا پایان سال ۱۴۰۲ و بویژه هزینه کرد دقیق مبالغ تخصیص داده شده به شرکت‌های توسعه‌دهنده سامانه‌های اطلاعات بیمارستانی طرف قرارداد مراکز تابعه آن دانشگاه (مستندات پیوست) انجام پذیرد و گزارش اقدامات صورت گرفته جهت پایش مستمر این موضوع حداکثر طی پنج روز کاری از تاریخ مکاتبه به این مرکز ارسال گردد.

دکتر سید رضا مظهری
رییس مرکز مدیریت آمار و فناوری اطلاعات

رونوشت :

- جناب آقای دکتر پورحسینی مشاور محترم وزیر و مدیر کل حوزه وزارتی
جناب آقای دکتر سعید کریمی معاون محترم درمان
جناب آقای دکتر محمد مهدی ناصحی مدیرعامل محترم سازمان بیمه سلامت
جناب آقای مهندس حسن هاشمی رئیس محترم سازمان نظام صنفی رایانه ای کشور
جناب آقای دکتر رحیم نیا مدیر کل محترم دفتر بازرسی، ارزیابی عملکرد و پاسخگویی به شکایات
جناب آقای دکتر حسین فرزانه رئیس محترم مرکز حراست وزارت بهداشت درمان و آموزش پزشکی
مدیران محترم آمار و فناوری اطلاعات دانشگاه ها/دانشکده های علوم پزشکی و خدمات بهداشتی درمانی سراسر کشور
جناب آقای مهندس علیرضا کشاورز جمشیدیان دبیر محترم سازمان نظام صنفی رایانه ای کشور
جناب آقای دکتر نیما اختردانش معاون محترم فنی مرکز مدیریت آمار و فناوری اطلاعات

شهرک قدس، خیابان سیمای ایران، بین فلامک و زرافشان، ستاد مرکزی وزارت بهداشت، درمان و آموزش پزشکی، بلوک A، طبقه پنجم
تلفن: ۲-۸۱۴۵۳۶۰۱ نمابر: ۸۱۴۵۶۵۰۳ نشانی اینترنتی: it.behdasht.gov.ir نشانی پست الکترونیکی: it@behdasht.gov.ir

مرکز مدیریت آمار و فناوری اطلاعات
وزارت بهداشت، درمان و آموزش پزشکی

بسمه تعالی

شماره : ۱۱۰/۳۷۹
تاریخ : ۱۴۰۲/۰۹/۰۸
پیوست : ندارد

پیگیری.حائز اهمیت

مهار تورم و رشد تولید
((مقام معظم رهبری))

رئیس/ سرپرست محترم دانشگاه/دانشکده علوم پزشکی و خدمات بهداشتی درمانی سراسر کشور

موضوع : الزام اخذ تأییدیه مطابقت با استانداردهای زیرساخت عمومی کشور برای سامانه های اطلاعات بیمارستانی(پیگیری)

با سلام و احترام

در راستای اجرایی سازی جزء (۴)، بند (س) تبصره (۱۷) قانون بودجه سال ۱۴۰۲ و پیرو مکاتبه شماره ۱۱۰/۱۶۳۳/د مورخ ۱۴۰۲/۰۸/۱۳ مبنی بر «تأکید بر اجرا و پیاده سازی دستورالعمل ها و یا سرویس‌های ابلاغی وزارت متبوع در سال ۱۴۰۲»، یکی از سرویس های اولویت دار مربوطه «پیاده‌سازی امضای دیجیتال(PKE شدن) با اولویت سامانه های نسخه نویسی الکترونیکی» می باشد که لازم است اعتبار مشوق متناظر با این موضوع پس از تحویل و نهایی سازی قابلیت مذکور و ارائه گواهینامه مرتبط با آن، به شرکت‌های توسعه دهنده سامانه های اطلاعات بیمارستانی طرف قرارداد مراکز تابعه آن دانشگاه/دانشکده پرداخت گردد.

در همین راستا با عنایت به ابلاغیه شماره ۱۱۰/۳۳۶ مورخ ۱۴۰۱/۰۹/۰۵ «الزام اخذ تأییدیه مطابقت با استانداردهای زیرساخت کلید عمومی کشور برای سامانه های اطلاعاتی حوزه سلامت» تأکید گردیده و عطف به آیین نامه اجرایی ماده ۳۲ قانون تجارت الکترونیک و تصویب مدل سلسله مراتبی متشکل از شورای سیاست گذاری گواهی الکترونیکی به منظور رسمیت بخشیدن به امضای الکترونیکی در کشور، مرکز صدور گواهی الکترونیکی میانی سلامت زیر نظر مرکز دولتی صدور گواهی الکترونیکی ریشه، به عنوان مرجع صدور گواهی در حوزه سلامت کشور می باشد.

با توجه به الزامات فعلی در حفظ اصول امنیت در فضای تبادل الکترونیکی اطلاعات از جمله محرمانگی، جامعیت، انکار ناپذیری و تصدیق هویت و استنادپذیری اسناد و داده پیام های جایگزین اسناد و مکاتبات، بهره برداری از امضای الکترونیکی دارای الزام حقوقی بوده و آماده سازی سامانه های اطلاعاتی بیمارستانی علی الخصوص به منظور امضای نسخ الکترونیک، فرم های بالینی و داده پیام‌های پرونده الکترونیک سلامت جهت مطابقت با استانداردهای زیرساخت کلید عمومی کشور اجتناب ناپذیر و پیش نیاز بهره‌برداری می باشد.

شهرک قدس، خیابان سیمای ایران، بین فلامک و زرافشان، ستاد مرکزی وزارت بهداشت، درمان و آموزش پزشکی، بلوک A، طبقه پنجم
تلفن: ۲-۸۱۴۵۳۶۰۱ نمابر: ۸۱۴۵۶۵۰۳ نشانی اینترنتی: it.behdasht.gov.ir نشانی پست الکترونیکی: it@behdasht.gov.ir

مرکز مدیریت آمار و فناوری اطلاعات
وزارت بهداشت، درمان و آموزش پزشکی

بسمه تعالی

شماره : ۱۱۰/۳۷۹
تاریخ : ۱۴۰۲/۰۹/۰۸
پیوست : ندارد

پیگیری.حائز اهمیت

مهار تورم و رشد تولید
((مقام معظم رهبری))

لذا خواهشمند است دستور فرمایید پیگیری لازم جهت اخذ گواهینامه مطابقت با زیرساخت کلید عمومی کشور از آزمایشگاه ارزیابی نرم افزارهای مبتنی بر PKI مورد تایید مرکز دولتی صدور گواهی الکترونیکی ریشه برای محصولات نرم افزاری مورد بهره برداری در آن مجموعه صورت پذیرفته و مراتب به این مرکز اعلام گردد.

دکتر سید رضا مظهری
رییس مرکز مدیریت آمار و فناوری اطلاعات

رونوشت :

- جناب آقای دکتر پورحسینی مشاور محترم وزیر و مدیر کل حوزه وزارتی
جناب آقای دکتر بهروز رحیمی معاون محترم توسعه مدیریت و منابع
جناب آقای دکتر سعید کریمی معاون محترم درمان
جناب آقای دکتر حسین فرشیدی معاون محترم بهداشت
جناب آقای دکتر عباس عبادی معاون محترم پرستاری
جناب آقای مهندس حسن هاشمی رئیس محترم سازمان نظام صنفی رایانه ای کشور
جناب آقای دکتر واعظی رئیس محترم مرکز مدیریت بیمارستانی و تعالی خدمات بالینی
جناب آقای دکتر طباطبایی لطفی مدیر کل محترم دفتر ارزیابی فناوری و تدوین استاندارد و تعرفه سلامت
جناب آقای دکتر محمودرضا محقق دولت آبادی دبیر محترم شورای عالی بیمه سلامت و مدیرکل دفتر برنامه ریزی و سیاستگذاری بیمه های سلامت
جناب آقای دکتر حسین فرزانه رئیس محترم مرکز حراست وزارت بهداشت درمان و آموزش پزشکی
جناب آقای دکتر رحیم نیا مدیر کل محترم دفتر بازرسی، ارزیابی عملکرد و پاسخگویی به شکایات
مدیران محترم آمار و فناوری اطلاعات دانشگاه ها/دانشکده های علوم پزشکی و خدمات بهداشتی درمانی سراسر کشور
جناب آقای ناصر شاکر حسینی رئیس محترم کمیسیون سلامت الکترونیک سازمان نظام صنفی رایانه ای کشور
جناب آقای دکتر نیما اختردانش معاون محترم فنی مرکز مدیریت آمار و فناوری اطلاعات
سرپرست محترم گروه تنظیم مقررات، صدور پروانه و نظارت

شهرک قدس، خیابان سیمای ایران، بین فلامک و زرافشان، ستاد مرکزی وزارت بهداشت، درمان و آموزش پزشکی، بلوک A، طبقه پنجم
تلفن: ۲-۸۱۴۵۳۶۰۱ نمابر: ۸۱۴۵۶۵۰۳ نشانی اینترنتی: it.behdasht.gov.ir نشانی پست الکترونیکی: it@behdasht.gov.ir

بسمه تعالی

مرکز مدیریت آمار و فناوری اطلاعات
وزارت بهداشت، درمان و آموزش پزشکی

شماره : ۱۱۰/۵۱۵
تاریخ : ۱۴۰۲/۱۲/۱۹
پیوست : دارد

فوری.حائز اهمیت

مهار تورم و رشد تولید
((مقام معظم رهبری))

رئیس/ سرپرست محترم دانشگاه/دانشکده علوم پزشکی و خدمات بهداشتی درمانی سراسر کشور
مدیرعامل محترم شرکت/مجموعه توسعه دهنده سامانه اطلاعاتی حوزه سلامت
موضوع : راهنمای فنی پیاده سازی سرویس امضای دیجیتال

با سلام

احتراما، پیرو نامه شماره ۱۱۰/۳۷۹ مورخ ۱۴۰۲/۰۹/۰۸ با موضوع الزام اخذ تاییدیه مطابقت با استانداردهای زیرساخت کلید عمومی کشور برای کلیه سامانه‌های اطلاعاتی حوزه سلامت و به منظور تسهیل در فرآیند استفاده از زیرساخت کلید عمومی وزارت متبوع در راستای تجهیز این سامانه‌ها به قابلیت امضای الکترونیک و مهر سازمانی با هدف ایجاد امکان استنادپذیری برای اسناد الکترونیک و داده پیام‌های حوزه سلامت، این مرکز اقدام به راه‌اندازی و ارائه سرویس DSS (Digital Sign Service) بر بستر درگاه یکپارچه تبادل اطلاعات سلامت (دیتاس) نموده است.

بدینوسیله به پیوست، راهنمای استفاده به همراه نمودار مراحل پیاده سازی سرویس‌های مرتبط با این موضوع جهت بهره برداری مقتضی ارسال می‌گردد.

دکتر سید رضا مظهری
رییس مرکز مدیریت آمار و فناوری اطلاعات

رونوشت :

- جناب آقای دکتر پورحسینی مشاور محترم وزیر و مدیر کل حوزه وزارتی
- جناب آقای دکتر رحیمی معاون محترم توسعه مدیریت و منابع
- جناب آقای دکتر کریمی معاون محترم درمان
- جناب آقای دکتر فرشیدی معاون محترم بهداشت
- جناب آقای دکتر عبادی معاون محترم پرستاری
- جناب آقای دکتر محمد مهدی ناصحی مدیرعامل محترم سازمان بیمه سلامت
- جناب آقای دکتر سید میرهاشم موسوی مدیرعامل محترم سازمان تامین اجتماعی
- جناب آقای دکتر امیر نوروزی رئیس محترم سازمان بیمه خدمات درمانی وزارت دفاع و پشتیبانی نیروهای مسلح
- جناب آقای دکتر احسان کیانخواه دبیر محترم شورای اجرایی فناوری اطلاعات کشور
- جناب آقای حسین فغفوری سرپرست محترم هیات حسابرسی دیوان محاسبات مستقر در وزارت بهداشت
- جناب آقای عباس شیرزاد رئیس محترم شعبه اول دادسرای دیوان محاسبات کشور
- جناب آقای مهندس حسن هاشمی رئیس محترم سازمان نظام صنفی رایانه ای کشور
- جناب آقای دکتر محمودرضا محقق دولت آبادی دبیر محترم شورای عالی بیمه سلامت و مدیرکل دفتر برنامه ریزی و سیاستگذاری بیمه های سلامت
- جناب آقای دکتر حسین فرزانه رئیس محترم مرکز حراست وزارت بهداشت درمان و آموزش پزشکی
- جناب آقای دکتر رحیم نیا مدیر کل محترم دفتر بازرسی، ارزیابی عملکرد و پاسخگویی به شکایات
- مدیران محترم آمار و فناوری اطلاعات دانشگاه ها/دانشکده های علوم پزشکی و خدمات بهداشتی درمانی سراسر کشور
- جناب آقای ناصر شاکر حسینی رئیس محترم کمیسیون سلامت الکترونیک سازمان نظام صنفی رایانه ای کشور
- جناب آقای دکتر نیما اختردانش معاون محترم فنی مرکز مدیریت آمار و فناوری اطلاعات

شهرک قدس، خیابان سیمای ایران، بین فلامک و زرافشان، ستاد مرکزی وزارت بهداشت، درمان و آموزش پزشکی، بلوک A، طبقه پنجم
تلفن: ۲-۸۱۴۵۳۶۰۱ نمابر: ۸۱۴۵۶۵۰۳ نشانی اینترنتی: it.behdasht.gov.ir نشانی پست الکترونیکی: it@behdasht.gov.ir

مرکز مدیریت آمار و فناوری اطلاعات

وزارت بهداشت، درمان و آموزش پزشکی

درگاه یکپارچه تبادل اطلاعات سلامت (دیتاس)

سرویس امضای دیجیتال

(سند راهنمای فنی پیاده‌سازی)

نگارش ۰,۱

تاریخ ویرایش سند
۱۴۰۲/۱۰/۰۹

شناسنامه سند

درگاه یکپارچه تبادل اطلاعات سلامت (دیتاس)	
نام سند :	سرویس امضای دیجیتال (سند راهنمای فنی پیاده‌سازی)
ارائه‌دهنده سرویس:	مرکز مدیریت آمار و فناوری اطلاعات، شرکت پندار کوشک ایمن
نام فایل :	DITAS_DigitalSignService_V0.1
تاریخ انتشار نگارش اولیه سند :	۱۴۰۲/۱۰/۰۹
تاریخ انتشار نگارش فعلی سند :	۱۴۰۲/۱۰/۰۹
شرح سند :	این سند برای بهره‌برداری از سرویس امضای دیجیتال تهیه شده است.
نویسندگان :	مرکز مدیریت آمار و فناوری اطلاعات وزارت بهداشت، درمان و آموزش پزشکی
فایل مرجع :	PKI-DSS-API-DG-v2.10.docx

تاریخچه ویرایش سند

نویسنده/ویراستار	تاریخ	نگارش	اقدامات
ابراهیم کشاورز صفری	۱۴۰۲/۱۰/۰۹	۰,۱	تدوین نسخه اولیه سند

تاریخچه بررسی و تایید سند

نویسنده/ویراستار	تاریخ	نگارش	وضعیت

فهرست مطالب

مقدمه

در این مستند راهنمایی‌های لازم جهت استفاده از توابع سرویس PKA به منظور انجام عملیات‌های اعتبارسنجی گواهی‌نامه‌ها و امضای اسناد و مهر زمانی و همچنین عملیات‌های صدور گواهینامه و همچنین ابطال گواهینامه و نیز تعلیق و فعال‌سازی گواهینامه ارائه شده است. خدماتی که این دسته از توابع ارائه می‌دهند، در ادامه مورد بررسی قرار خواهد گرفت. همچنین این راهنما به صورت اختصاصی برای برنامه‌نویسان و توسعه‌دهندگان نرم‌افزار تهیه شده است و قدر مسلم نیاز به دانش‌های اولیه برنامه‌نویسی دارد.

تعاریف

دیتاس (DITAS): به درگاه یکپارچه تبادل اطلاعات سلامت اطلاق می‌شود.

ارائه‌دهنده سرویس: معاونت/ سازمان/ مرکزی که سرویس الکترونیکی آن بر بستر دیتاس پیاده‌سازی شده باشد.

احراز هویت کاربر (Authorization): از این پارامتر جهت احراز هویت کاربران دیتاس استفاده می‌شود که به صورت OAuth2 می‌باشد.

شناسه سرویس[1] (PID): شناسه یکتای ارائه شده به کاربر برای فراخوانی سرویس.

نحوه احراز هویت کاربر دیتاس

باتوجه به اینکه تمامی خدمات ارائه شده نیازمند دسترسی به توکن خاص هر مرکز می باشد این تابع به منظور ارائه توکن مورد استفاده قرار می گیرد. توکن دریافت شده توسط این تابع در بخش Header درخواست‌ها ثبت می گردد. خروجی این تابع توکن دسترسی‌ای با تاریخ انقضاء مشخص می باشد.

دسترسی به خدمات

دسترسی به خدمات ارائه شده از طریق آدرس زیر امکان‌پذیر است:

[1] Package ID

```
Base Url:  Https://apigateway.behdasht.gov.ir
```

تمامی خدمات نیازمند توکن دسترسی هستند که در بخش هدر درخواست‌ها قرار می‌گیرند.

تابع دریافت توکن دیتاس[1]

این تابع با استفاده از ورودی‌های مخصوص به هر کاربر، توکن دسترسی‌ای با تاریخ انقضاء مشخص را برمی‌گرداند.

- قالب ورودی

```
POST /oauth/token HTTP/1.1
Host: apigateway.behdasht.gov.ir
Authorization: Basic {authorizationCode}
grant_type=password&username=yourusername&password=yourpassword
```

جدول ۱- پارامترهای ورودیHeader تابع دریافت توکن

ردیف	نام پارامتر	نوع داده	الزامی	توضیحات
۱	authorizationCode	basic auth	بله	شامل Client_Id:Client_Secret مخصوص به هر کاربر است که به صورت Base64 ارسال می‌شود.

جدول ۲- پارامترهای ورودیBody تابع دریافت توکن

ردیف	نام پارامتر	مقدار ورودی	الزامی	توضیحات
۱	grant_type	password	بله	مدل دسترسی
۲	username	Your username	بله	نام کاربری شما
۳	password	Your password	بله	رمز عبور شما

- نمونه خروجی موفق

```
{
    "access_token": "c8abceda-aa31-4a7e-95c0-213e5709e6b6",
    "token_type": "bearer",
    "refresh_token": "84dc3bf1-7342-4c5e-adc3-c2304583ae02",
    "expires_in": 763,
    "scope": "trust read write"
}
```

- نمونه خروجی ناموفق

```
{
    "error": "invalid_grant",
    "error_description": "Bad credentials"
}
```

[1] Get Token

جدول ۳- پارامترهای خروجی Body تابع دریافت توکن دیتاس

ردیف	نام پارامتر	نوع داده	توضیحات
۱	access_token	string	توکن دسترسی
۲	refresh_token	string	بروزرسانی توکن
۳	scope	string	محدوده دسترسی توکن
۴	token_type	string	نوع توکن
۵	expires_in	string	مقدار زمان باقیمانده تا منقضی شدن توکن (بر اساس ثانیه)

جدول ۴- پارامترهای خروجی Header تابع دریافت توکن

ردیف	نام پارامتر	نوع داده	توضیحات
۱	requestId	string	شناسه پیگیری برای رهگیری درخواست

پارامترهای خروجی Header همه توابع دیتاس مطابق جدول ۴ می‌باشد.

تابع بروزرسانی توکن دیتاس[۱]

این تابع، توکن دریافتی از *تابع دریافت توکن دیتاس* را بروزرسانی می‌کند. پارامترهای خروجی Header این تابع مطابق جدول ۴ می‌باشد.

- قالب ورودی

```
POST /oauth/token HTTP/1.1
Host: apigateway.behdasht.gov.ir
Authorization: Basic {authorizationCode}
grant_type=refresh_token&refresh_token={refreshToken}
```

جدول ۵- پارامترهای ورودی Header تابع بروزرسانی توکن دیتاس

ردیف	نام پارامتر	نوع داده	الزامی	توضیحات
۱	Authorization	basic auth	بله	شامل Client_Id:Client_Secret مخصوص به هر کاربر است که به صورت Base64 ارسال می‌شود.

- نمونه خروجی موفق

```
{
    "access_token": "529d80a1-e8af-44b2-9dac-565cff4258f1",
    "token_type": "bearer",
    "refresh_token": "f998a112-b166-4177-8e2e-c2d89fedb352",
    "expires_in": 899,
    "scope": "trust read write"
}
```

[۱] Refresh Token

- نمونه خروجی ناموفق

```
{
    "error": "invalid_grant",
    "error_description": "Bad credentials"
}
```

جدول ۶- پارامترهای خروجی Body تابع بروزرسانی توکن

ردیف	نام پارامتر	نوع داده	توضیحات
۱	accessToken	string	توکن دسترسی
۲	refreshToken	string	بروز رسانی توکن
۳	scope	string	محدوده دسترسی توکن
۴	tokenType	string	نوع توکن
۵	expiresIn	string	مقدار زمان باقیمانده تا انقضا شدن توکن (بر اساس ثانیه)

نحوه فراخوانی توابع سرویس امضای دیجیتال

پارامترهای ورودی Header توابع سرویس امضای دیجیتال

در تمامی توابع این سرویس، از پارامترهای جدول ۷ به عنوان ورودی Header استفاده می‌شود.

جدول ۷– پارامترهای ورودی Header توابع سرویس امضای دیجیتال

ردیف	نام پارامتر	نوع داده	الزامی	توضیحات
۱	Content-Type	String	بله	نوع محتوای ورودی
۲	Pid	String	بله	شناسه سرویس
۳	Authorization	String	بله	مقدار توکن بازگشتی از تابع دریافت یا بروزرسانی توکن

سرویس اعتبارسنجی[۱]

بررسی اعتبار امضای دیجیتال و تاریخ اعتبار گواهینامه

تابعی که این خدمت را ارائه می‌کند، گواهی ارائه‌شده را از نظر اعتبار آن در زمان کنونی و همچنین امضای دیجیتال صادرشده بر روی آن از طرف CA صادرکننده آن، مورد ارزیابی قرار می‌دهد. جزئیات این تابع به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/VAService_ValidateCertificateRaw	
ورودی‌ها	`Byte[] Base64Certificate`	گواهی مورد نظر جهت بررسی صحت اعتبار در قالب byte[]
خروجی	`bool`	نتیجه‌ی صحت اعتبار گواهی

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/VAService_ValidateCertificate	
ورودی‌ها	`string Bs64Certificate`	گواهی مورد نظر جهت بررسی صحت اعتبار در قالب Base64
خروجی	`bool`	نتیجه‌ی صحت اعتبار گواهی

[۱] VAService

بررسی اعتبار گواهینامه(ها) با لیست گواهی باطله (CRL)

یکی از استانداردهایی که در زمینه بررسی اعتبار گواهینامه موجود است، استاندارد CRL یا Certificate Revocation List می‌باشد. این استاندارد به منظور بررسی اعتبار گواهی، به صورت آفلاین مورد استفاده قرار می‌گیرد. در این تابع، ابتدا آدرس Crl از فایل گواهی واکشی می‌شود، در صورتی‌که این آدرس در فایل گواهی وجود نداشته باشد یا دسترسی به آن با خطا مواجه شود، از آدرس مربوط به Crl در vaProfile استفاده می‌شود. جزئیات این تابع به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateCertificateByCRLExRaw	

ورودی‌ها
ValidateRequest<byte[]>
{
Certificate,
vaProfile
}
	Byte[]
	Base64Certificate
		گواهی موردنظر جهت بررسی صحت اعتبار در قالب byte[]

	string vaProfile	نام پروفایل مورداستفاده(اختیاری)
خروجی	CRLRevocationResult <byte[]>	نتیجه‌ی بازگشتی از بررسی Crl، شامل وضعیت صحت گواهی، زمان ابطال و فایل گواهی

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateCertificateByCRLEx	

ورودی‌ها
ValidateRequest<string[]>
{
Certificate,
vaProfile
}
	string
	Base64Certificate
		گواهی موردنظر جهت بررسی صحت اعتبار

	string vaProfile	نام پروفایل مورداستفاده(اختیاری)
خروجی	CRLRevocationResult <string>	نتیجه‌ی بازگشتی از بررسی Crl، شامل وضعیت صحت گواهی، زمان ابطال و فایل گواهی

دو تابع قدیمی ذیل، جهت مطابقت با نسخه‌های قدیمی نگهداری می‌گردد، اما توصیه می‌شود از توابع بالا جهت اعتبارسنجی گواهی‌ها به صورت آفلاین استفاده گردد:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateCertificateByCRLRaw	

ورودی‌ها
ValidateRequest<byte[]>
{
Certificate,
vaProfile
}
	Byte[]
	Base64Certificate
		گواهی موردنظر جهت بررسی صحت اعتبار در قالب byte[]

	string vaProfile	نام پروفایل مورداستفاده(اختیاری)
خروجی	bool	نتیجه‌ی صحت گواهی

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateCertificateByCRL		

ورودی‌ها
ValidateRequest<string>
{
Certificate,
vaProfile
}
	string Base64Certificate	گواهی موردنظر جهت بررسی صحت اعتبار در قالب Base64	

	string vaProfile	نام پروفایل مورداستفاده(اختیاری)	
خروجی	bool	نتیجه‌ی صحت گواهی	

جهت بررسی وضعیت اعتبار فهرستی از گواهی‌ها، از توابع ذیل استفاده می‌شود، با توجه به این نکته که زنجیره‌ی فهرست گواهی‌ها باید یکسان باشد.

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateCertificateByCRLRaw		
ورودی‌ها ChainValidationRequest <byte[]> { Certificates, vaProfile }	IEnumerable<byte[]> Base64CertificateList	فهرست گواهی‌های موردنظر جهت بررسی صحت اعتبار درقالب byte[]	
	string vaProfile	نام پروفایل مورداستفاده(اختیاری)	
خروجی	IEnumerable <CRLRevocationResult <byte[]>>	فهرستی از نتایج بازگشتی از بررسی Crl، شامل وضعیت صحت گواهی، زمان ابطال و فایل گواهی	

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateCertificateListByCRL		
ورودی‌ها ChainValidationRequest <string> { Certificates, vaProfile}	IEnumerable<string> Base64CertificateList	فهرست گواهی‌های موردنظر جهت بررسی صحت اعتبار درقالب Base64	
	string vaProfile	نام پروفایل مورد استفاده(اختیاری)	
خروجی	IEnumerable <CRLRevocationResult <string>>	فهرستی از نتایج بازگشتی از بررسی Crl، شامل وضعیت صحت گواهی، زمان ابطال و فایل گواهی	

بررسی اعتبار گواهینامه با سرویس استعلام آنلاین وضعیت گواهینامه (OCSP)

استاندارد دیگری که برای اعتبارسنجی گواهینامه‌ها مورد استفاده قرار می‌گیرد، استاندارد OCSP یا Online Certificate Status Protocol می‌باشد. این استاندارد وضعیت اعتبار گواهی را به صورت آنلاین مورد بررسی قرار می‌دهد.

در این تابع ابتدا آدرس Ocsp از فایل گواهی واکشی می‌شود، در صورتی‌که این آدرس در فایل گواهی وجود نداشته باشد، اگر vaProfile ارسال شده باشد، از آدرس مربوط به Ocsp در vaProfile استفاده می‌شود. جزئیات این تابع به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateCertificateByOCSPExRaw	

ورودی‌ها
ValidateRequest<byte[]>
{
Certificate,
vaProfile
}
	byte[] Bs64Certificate	رشته‌ی گواهی مورد نظر جهت بررسی صحت اعتبار

	string vaProfile	نام پروفایل مورد استفاده(اختیاری)
خروجی	OCSPResponseStatus<byte[]>	نتیجه بازگردانده شده از طرف سرور OCSP شامل وضعیت گواهی، زمان ابطال، علت ابطال و گواهی

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateCertificateByOCSPEx	

ورودی‌ها
ValidateRequest<string>
{
Certificate,
vaProfile
}
	string Bs64Certificate	رشته‌ی گواهی مورد نظر جهت بررسی صحت اعتبار در قالب base64

	string vaProfile	نام پروفایل مورد استفاده(اختیاری)
خروجی	OCSPResponseStatus<string>	نتیجه بازگردانده شده از طرف سرور OCSP شامل وضعیت گواهی، زمان ابطال، علت ابطال و گواهی

دو تابع قدیمی ذیل، جهت مطابقت با نسخه‌های قدیمی نگهداری می‌گردد، اما توصیه می‌شود از توابع بالا جهت اعتبارسنجی گواهی‌ها به صورت آنلاین از توابع بالا استفاده گردد. تفاوت توابع قدیمی ذیل، با توابع بالا در نوع خروجی است که در توابع ذیل فقط وضعیت گواهی، برگردانده می‌شود.

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateCertificateByOCSPExRaw	

ورودی‌ها
ValidateRequest<byte[]>
{
Certificate,
vaProfile
}
	Byte[] Bs64Certificate	آرایه‌ی رشته‌ی گواهی مورد نظر جهت بررسی صحت اعتبار

	string vaProfile	نام پروفایل مورد استفاده(اختیاری)
خروجی	CertificateStatus	وضعیت بازگردانده شده از طرف سرور OCSP

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateCertificateByOCSPEx	

ورودی‌ها
ValidateRequest<string>
{
Certificate,
vaProfile
}
	string Bs64Certificate	گواهی مورد نظر جهت بررسی صحت اعتبار

	string vaProfile	نام پروفایل مورد استفاده(اختیاری)
خروجی	CertificateStatus	وضعیت بازگردانده شده از طرف سرور OCSP

مقادیر نتیجه بازگشتی(CertificateStatus):

```
Good = 0,
Revoked = 1,
Unknown = 2
```

جهت بررسی وضعیت اعتبار فهرستی از گواهی‌ها از توابع ذیل استفاده می‌گردد، با توجه به این نکته که زنجیره فهرست گواهی‌ها باید یکسان باشد.

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateCertificateListByOCSPRaw	
ورودی‌ها ChainValidationRequest<byte[]> { Certificates, vaProfile}	IEnumerable<byte[]> Base64CertificateList	فهرستی از گواهی های مورد نظر جهت بررسی صحت اعتبار در قالب Base64
	string vaProfile	نام پروفایل مورد استفاده(اختیاری)
خروجی	IEnumerable <OCSPResponseStatus <byte[]>>	فهرستی از نتایج وضعیت‌های بازگردانده شده از طرف سرور OCSP، زمان ابطال، دلیل ابطال و فایل گواهی

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateCertificateListByOCSP	
ورودی‌ها ChainValidationRequest<string> { Certificates, vaProfile}	IEnumerable<string> Base64CertificateList	فهرستی از گواهی‌های مورد نظر جهت بررسی صحت اعتبار در قالب Base64
	string vaProfile	نام پروفایل مورد استفاده(اختیاری)
خروجی	IEnumerable <OCSPResponseStatus <string>>	فهرستی از وضعیت‌های بازگردانده شده از طرف سرور OCSP، زمان ابطال، دلیل ابطال و فایل گواهی

مقادیر نتیجه بازگشتی(CertificateStatus):

```
Good = 0,
Revoked = 1,
Unknown = 2
```

بررسی اعتبار گواهینامه با موارد استفاده گواهی(Key Usage)

با استفاده از این تابع می‌توان کاربردهای یک گواهی را بررسی نمود.

در این تابع با استفاده از فهرست Keyusages که در تگ مربوطه در vaProfile مشخص شده است، کاربردهای گواهی بررسی می‌گردد.

کاراکتر جداکننده در این لیست علامت | می‌باشد. به‌طور مثال:

KeyUsages="DIGITALSIGNATURE | NONREPUDIATION"

لازم به توضیح است که در فیلد Keyusage، با توجه به نیاز، می‌توان هریک یا چندین مورد از اقلام ذیل را قرار داد:

```
EncipherOnly,
CrlSign,
KeyCertSign,
KeyAgreement,
DataEncipherment,
KeyEncipherment,
NonRepudiation,
DigitalSignature,
DecipherOnly
```

جزئیات تابع ارائه‌دهنده‌ی این خدمت در سرویس VAService به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateCertificateByKeyUsageRaw	
ورودی‌ها ValidateRequest<byte[]> { Certificate, vaProfile}	byte[] Bs64Certificate	گواهی مورد نظر جهت بررسی صحت اعتبار
	string vaProfile	نام پروفایل مورد استفاده
خروجی	bool	وضعیت تایید موارد استفاده (Keyusage) های موجود در گواهی

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateCertificateByKeyUsage	
ورودی‌ها ValidateRequest<string> { Certificate, vaProfile}	string Bs64Certificate	گواهی مورد نظر جهت بررسی صحت اعتبار
	string vaProfile	نام پروفایل مورد استفاده
خروجی	bool	وضعیت تایید موارد استفاده (Keyusage) های موجود در گواهی

با استفاده از این تابع می‌توان کاربردهای توسعه‌یافته یک گواهی را بررسی نمود. در این تابع با استفاده از فهرست ExtendedKeyUsage هایی که در تگ مربوطه در vaProfile مشخص شده است، کاربردهای توسعه‌یافته گواهی بررسی می‌گردد. کاراکتر جداکننده در این لیست علامت | می‌باشد. به‌طور مثال:

```
ExtendedKeyUsage="1.2.840.113583.1.1.5"
```

در فیلد ExtendedKeyUsage باید با توجه به نیاز، OID هر یک از کاربردها قرارداده شـــود. جزئیات این تابع به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateCertificateByKeyUsageExRaw	
ورودی‌ها ValidationByKeyUsageRequest<byte[]> { Certificate, KeyUsages, ExtendedKeyUsages}	`Byte[]` Bs64Certificate	گواهی مورد نظر جهت بررسی صحت اعتبار
	`IEnumerable<KeyUsage>` keyUsageList	موارد استفاده (keyUsage) های مورد نیاز برای بررسی
	`IEnumerable<string>` extendedKeyUsageList	لیستی از oId های مورد نیاز برای بررسی. این مقدار از فیلد Enhanced Key Usage گواهینامه استخراج می‌شود. بطور مثال: (1.3.6.1.4.1.311.20.2.2)
خروجی	`bool`	وضعیت تایید موارد استفاده(EnhancedKeyusage) های موجود در گواهی

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateCertificateByKeyUsageEx	

ورودی‌ها
ValidationByKeyUsageRequest<string>
{
Certificate,
KeyUsages,
ExtendedKeyUsages
}
	`string` Bs64Certificate	گواهی مورد نظر جهت بررسی صحت اعتبار

	`IEnumerable<KeyUsage>` keyUsages	موارد استفاده (EnhancedKeyusage) های مورد نیاز برای بررسی
	`IEnumerable<string>` extendedKeyUsages	لیستی از oId های مورد نیاز برای بررسی. این مقدار از فیلد EnhancedKeyusage گواهینامه استخراج می‌شود. بطور مثال: (1.3.6.1.4.1.311.20.2.2)
خروجی	`bool`	وضعیت تایید موارد استفاده (EnhancedKeyusage) های موجود در گواهی

بررسی کلی اعتبار گواهینامه

برای این روش دو تابع قدیمی و جدید پیاده‌سازی شده است. برای تطبیق‌پذیری با نسخه‌های قبلی، تابع قدیمی نیز وجود

دارد اما توصیه می‌شود که از تابع جدید برای بررسی کلی اقلام گواهی‌نامه استفاده گردد.

تابع جدید، به این صورت است که ابتدا کاربردهای گواهی، زنجیره گواهی، سپس وضعیت گواهی با استفاده از Ocsp , Crl بررسی می‌شود، در نهایت تاریخ انقضای گواهی بررسی می‌گردد. و در صورتی‌که در بررسی یکی از این اقلام، اعتبارسنجی گواهی‌نامه انجام نگیرد، علت رد شدن گواهی در خروجی تابع منعکس می‌گردد. همینطور اگر علت رد شدن گواهی، ابطال آن باشد، تاریخ ابطال نیز در خروجی تابع قرار داده می‌شود.

لازم به ذکر است که ترتیب بررسی Ocsp و Crl به این صورت است که ابتدا با توجه به آدرس Ocsp داخل گواهی، بررسی صورت می‌گیرد و در صورت عدم وجود آدرس AIA در فایل گواهی، از آدرس Crl داخل فایل گواهی استفاده می‌شود. در صورتی‌که این آدرس نیز وجود نداشته باشد یا دسترسی به آن آدرس با خطا مواجه شود، اگر vaProfile ارسال شده باشد، ابتدا با توجه به آدرس تنظیم شده برای Ocp، و در صورت عدم موفقیت از آدرس تنظیم شده برای Crl استفاده می‌شود.

جزئیات تابع جدید ارائه‌دهنده‌ی این خدمت در سرویس VAService به صورت‌های زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateCertificateEntirelyExRaw	

ورودی‌ها
ValidateEntirelyRequest <byte[]>
{
Certificate,
vaProfile
}
	`byte[]` Base64Certificate	آرایه‌ی رشته‌ی Base64 گواهی مورد نظر جهت بررسی صحت اعتبار در قالب byte[]

	`string` vaProfile	نام پروفایل مورد استفاده(اختیاری)
خروجی	`CertificateValidationResult`	وضعیت اعتبارسنجی گواهینامه و تاریخ ابطال گواهی

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateCertificateEntirelyEx	

ورودی‌ها
ValidateEntirelyRequest <string>
{
Certificate,
vaProfile
}
	`string` Base64Certificate	رشته‌ی Base64 گواهی مورد نظر جهت بررسی صحت اعتبار

	`string` vaProfile	نام پروفایل مورد استفاده(اختیاری)
خروجی	`CertificateValidationResult`	وضعیت اعتبارسنجی گواهینامه و تاریخ ابطال گواهی

توابع قدیمی: در این توابع، فقط وضعیت گواهی در خروجی تابع منعکس می‌گردد.

/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateCertificateEntirelyRaw		نام تابع

گواهی مورد نظر جهت بررسی صحت اعتبار در قالب byte[]	byte[] Base64Certificate	**ورودی‌ها**
		ValidateEntirelyRequest <byte[]>
		{
		Certificate,
		vaProfile
		}

نام پروفایل مورد استفاده	string vaProfile	
وضعیت اعتبارسنجی گواهینامه	CertificateValidationStatus	**خروجی**

/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateCertificateEntirely		نام تابع

گواهی مورد نظر جهت بررسی صحت اعتبار	string Base64Certificate	**ورودی‌ها**
		ValidateEntirelyRequest <string>
		{
		Certificate,
		vaProfile
		}

نام پروفایل مورد استفاده	string vaProfile	
وضعیت اعتبارسنجی گواهینامه	CertificateValidationStatus	**خروجی**

مقادیر نتیجه بازگشتی(CertificateValidationResult)

```
CertificateValidationOK = 0,
PeriodValidationFailed = 1,
ChainValidationFailed = 2,
IntgrityValidationFailed = 3,
KeyUsageValidationFailed = 4,
OCSPValidationRevoked = 5,
OCSPValidationUnKnown = 6,
CRLValidationRevoked = 7,
CRLAndOCSPValidationError = 8,
OCSPValidationException = 9,
CRLValidationUnKnown = 10,
CRLAndOCSPValidationUnknown = 11
```

دانلود فایل CRL

استاندارد CRL یا Certificate Revocation List که در زمینه‌ی بررسی اعتبار گواهینامه موجود است، نیازمند بررسی سریال گواهینامه با فایل تولید شده توسط CA می‌باشد. تابع DownloadCRL جهت دانلود فایل CRL پیاده‌سازی شده است. جزئیات این تابع به صورت‌های زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/VAService_DownloadCRL	
ورودی‌ها	string crlUrl	آدرس فایل CRL
خروجی	byte[]	فایل دانلود شده CRL

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_DownloadCRLByCertificateRaw	
ورودی‌ها	byte[] base64certificate	گواهی مورد نظر جهت دریافت آدرس CRL
خروجی	byte[]	فایل دانلود شده CRL

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_DownloadCRLByCertificate	
ورودی‌ها	string base64certificate	گواهی مورد نظر جهت دریافت آدرس CRL
خروجی	byte[]	فایل دانلود شده CRL

بررسی اقلام استاندارد گواهی‌های میانی و ریشه

این تابع همه استانداردهای موجود، جهت بررسی اعتبار گواهینامه‌های میانی و ریشه‌ی گواهی ارسال شده را بررسی می‌کند. فرآیند بررسی این تابع، به این صورت است که صحت مقادیر BasicConstraint, Path Length, Subject Type = CA,

keyUsages ={CrlSign , KeyCerSign} های گواهی‌های میانی و ریشه‌ی یک گواهی بررسی می‌گردد.

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateBasicConstraintsRaw	
ورودی‌ها	byte[] base64certificate	آرایه‌ی رشته base64 گواهی مورد نظر جهت بررسی
خروجی	bool	نتیجه‌ی صحت بررسی گواهی

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /VAService_ValidateBasicConstraints	
ورودی‌ها	string base64certificate	رشته base64 گواهی مورد نظر جهت بررسی
خروجی	bool	نتیجه‌ی صحت بررسی گواهی

سرویس امضای اسناد الکترونیک[1]

سرویس DSService توابع مورد نیاز جهت ارسال سند مورد نیاز به سرور امضاکننده‌ی اسناد و همچنین استخراج سند

[1] DSService

امضا شده از پاسخ دریافتی سرور را ارائه می‌دهند. خدماتی که این دسته از توابع ارائه می‌دهند در ادامه مورد بررسی قرار خواهد گرفت.

درخواست امضای سند PDF

این تابع فرایند مورد نیاز جهت امضای سند PDF توسط سرور امضای اسناد را پیاده‌سازی می‌کند. جزئیات این تابع به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/DSService_PDFSignRaw	
ورودی‌ها SignRequest<byte[]> { Data, DSProfile }	Byte[] PDFBase64	رشته Base64 شامل سند PDF درخواستی جهت امضا توسط سرور امضای اسناد
	string DSProfile	نام پروفایل مورد استفاده
خروجی	Byte[]	آرایه ای از رشته Base64 شامل سند PDF امضا شده توسط سرور امضای اسناد

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/DSService_PDFSign	
ورودی‌ها SignRequest<string> { Data, DSProfile }	string PDFBase64	رشته Base64 شامل سند PDF درخواستی جهت امضا توسط سرور امضای اسناد
	string DSProfile	نام پروفایل مورد استفاده
خروجی	string	رشته Base64 شامل سند PDF امضا شده توسط سرور امضای اسناد

درخواست امضای سند CMS

این تابع فرایند مورد نیاز جهت امضای سند CMS توسط سرور امضای اسناد را پیاده‌سازی می‌کند.

جزئیات تابع ارائه‌دهنده‌ی این خدمت در سرویس DSService به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/DSService_CMSSignRaw	

ورودی‌ها
CMSSignRequest<byte[]>
{
Data,
DSProfile,
AttachData
}
	Byte[] Data	آرایه ای از رشته Base64 شامل سند CMS درخواستی جهت امضا توسط سرور امضای اسناد

	string DSProfile	نام پروفایل مورد استفاده
	bool AttachData	مقدار دودویی جهت انتخاب قرارگیری خود اطلاعات در قالب CMS خروجی.
خروجی	Byte[]	رشته Base64 شامل سند CMS امضا شده توسط سرور امضای اسناد

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/DSService_CMSSign		

ورودی‌ها
CMSSignRequest<string>
{
Data,
DSProfile,
AttachData
}
	string CMSBase64	رشته Base64 شامل سند CMS درخواستی جهت امضا توسط سرور امضای اسناد

	string DSProfile	نام پروفایل مورد استفاده
	bool AttachData	مقدار دودویی جهت انتخاب قرارگیری خود اطلاعات در قالب CMS خروجی.
خروجی	string	رشته Base64 شامل سند CMS امضا شده توسط سرور امضای اسناد

درخواست امضای RSA

این تابع فرایند مورد نیاز جهت امضای RSA توسط سرور امضای اسناد را پیاده‌سازی می‌کند:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/DSService_RSASignRaw		
ورودی‌ها SignRequest<byte[]> { Data, DSProfile }	Byte[] Data	رشته Base64 درخواستی جهت امضا توسط سرور امضای اسناد
	string DSProfile	نام پروفایل مورد استفاده
خروجی	Byte[]	آرایه ای از رشته Base64 امضا شده توسط سرور امضای اسناد

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/DSService_RSASign		
ورودی‌ها SignRequest<string> { Data, DSProfile }	string Data	رشته Base64 درخواستی جهت امضا توسط سرور امضای اسناد
	string DSProfile	نام پروفایل مورد استفاده
خروجی	string	رشته Base64 امضا شده توسط سرور امضای اسناد

درخواست امضای سند XML

این تابع فرایند مورد نیاز جهت امضای سند XML توسط سرور امضای اسناد را پیاده‌سازی می‌کند. جزئیات این تابع به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/DSService_XMLSign		
ورودی‌ها SignRequest<string> { Data,	string Data	سند XML درخواستی جهت امضا توسط سرور امضای اسناد
	string DSProfile	نام پروفایل مورد استفاده

DSProfile }		
خروجی	string	رشته XMLBase64 امضا شده توسط سرور امضای اسناد

سرویس مهر زمانی مطمئن[1]

سرویس TSAService توابع مورد نیاز جهت ارسال اطلاعات مورد نیاز جهت صدور مهر زمانی مطمئن بر روی آن به سرور TSA و همچنین دریافت پاسخ دریافتی از سرور را ارائه می‌دهند. خدماتی که این دسته از توابع ارائه می‌دهند در ادامه مورد بررسی قرار خواهد گرفت.

درخواست مهر زمانی مطمئن

این تابع فرآیند موردنیاز جهت صدور مهر زمانی مطمئن بر روی اطلاعات درخواستی توسط سرور TSA را پیاده‌سازی می‌کند. جزئیات تابع ارائه‌دهنده‌ی این خدمت در سرویس TSAService به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/TSAService_TSTSignRaw	
ورودی‌ها TSTSignRequest <byte[]> { Message, RequestCertificate, TSAProfile}	Byte[] Message	آرایه ای از رشته Base64 شامل اطلاعات درخواستی جهت صدور مهر زمانی مطمئن بر روی آن توسط سرور TSA
	bool RequestCertificate	مقدار دودویی جهت انتخاب قرار دهی گواهی سرور صادرکننده‌ی مهر زمانی در خروجی دریافتی از سرور
	string TSAProfile	نام پروفایل مورد استفاده.
خروجی	Byte[]	ارایه ای از رشته Base64 شامل مهر زمانی صادرشده بر روی اطلاعات

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/TSAService_TSTSign	

ورودی‌ها
TSTSignRequest
<string>
{
Message,
RequestCertificate,
TSAProfile
}
	string Message	رشته Base64 شامل اطلاعات درخواستی جهت صدور مهر زمانی مطمئن بر روی آن توسط سرور TSA

	bool RequestCertificate	مقدار دودویی جهت انتخاب قرار دهی گواهی سرور صادرکننده‌ی مهر زمانی در خروجی دریافتی از سرور
	string TSAProfile	نام پروفایل مورد استفاده.
خروجی	string	رشته Base64 شامل مهر زمانی صادرشده بر روی اطلاعات

[1] TSAService

سرویس رمزنگاری و رمزگشایی[1]

CryptoService توابع لازم برای رمزنگاری و رمزگشایی را در قالب یک وب سرویس ارائه می‌دهد. خدماتی که این دسته از توابع ارائه می‌دهند در ادامه مورد بررسی قرار خواهد گرفت.

مبدل رشته Base64 به Unicode

این تابع یک رشته را به فرمت Base64 دریافت کرده و به فرمت Unicode تبدیل می‌نماید.

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/CryptoService_Base64ToUnicode	
ورودی‌ها	`string b64Str`	رشته به فرمت Base64 برای تبدیل به فرمت Unicode
خروجی	`string`	رشته به فرمت Unicode تولید شده از رشته ورودی

مبدل رشته Unicode به Base64

این تابع یک رشته را به فرمت Unicode دریافت کرده و به فرمت Base64 تبدیل می‌نماید.

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/CryptoService_UnicodeToBase64	
ورودی‌ها	`string unicodeStr`	رشته به فرمت Unicode برای تبدیل به فرمت Base64
خروجی	`string`	رشته به فرمت Base64 تولید شده از رشته ورودی

استخراج گواهی از قالب CMS

به منظور دستیابی به گواهی‌هایی که در یک قالب CMS موجود می‌باشند و عملیات رمزنگاری با استفاده از آن‌ها انجام شده است، در کلاس Crypto تابع زیر در نظر گرفته شده است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_CmsExtractCertificatesRaw	
ورودی‌ها	`Byte[] messgaeSignatureCertificate`	آرایه‌ی رشته Base64 که حاوی یک قالب CMS است. این قالب در درون خود شامل گواهی استفاده شده جهت انجام عملیات رمزنگاری بر روی اطلاعات می‌باشد
خروجی	`IEnumerable<byte[]>`	آرایه‌ای از گواهی‌های استخراج‌شده از درون قالب CMS

[1] CryptoService

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_CmsExtractCertificates	
ورودی‌ها	string messgaeSignatureCertificate	رشته Base64 که حاوی یک قالب CMS است. این قالب در درون خود شامل گواهی استفاده شده جهت انجام عملیات رمزنگاری بر روی اطلاعات می‌باشد
خروجی	IEnumerable<string>	آرایه‌ای از گواهی‌های استخراج‌شده از درون قالب CMS

تصدیق امضای دیجیتال در قالب CMS

به منظور تصدیق امضای دیجیتالی که در قالب CMS قرار دارد، در کلاس Crypto دو تابع در نظر گرفته شده است. در صورتی که قالب CMS علاوه بر مقدار امضای دیجیتال، حاوی اصل محتوای اطلاعات امضا شده نیز باشد، در این صورت وجود خود قالب CMS برای تصدیق امضای صادرشده بر روی اطلاعات کفایت می‌نماید. تابعی که این خدمت را ارائه می‌دهد در جدول زیر آمده است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_CmsVerifyAttachRaw	
ورودی‌ها	Byte[] messgaeSignatureCertificate	آرایه ای از رشته Base64 که حاوی یک قالب CMS است. این قالب در درون خود شامل اطلاعات امضا شده، مقدار امضا و گواهی استفاده شده جهت صدور امضا بر روی اطلاعات می‌باشد.
خروجی	bool	مشخص‌کننده‌ی صحت امضای ارسال شده.

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_CmsVerifyAttach	
ورودی‌ها	string messgaeSignatureCertificate	رشته Base64 که حاوی یک قالب CMS است. این قالب در درون خود شامل اطلاعات امضا شده، مقدار امضا و گواهی استفاده شده جهت صدور امضا بر روی اطلاعات می‌باشد.
خروجی	bool	مشخص‌کننده‌ی صحت امضای ارسال شده.

در صورتی که قالب CMS حاوی اطلاعات امضا شده نباشد، در این صورت به منظور تصدیق امضا موجود در این قالب، خود اطلاعات امضا شده نیز موردنیاز می‌باشد. به منظور تصدیق امضای دیجیتال در این شرایط، تابع زیر در کلاس Crypto در نظر گرفته شده است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/CryptoService_CmsVerifyRaw	

ورودی‌ها
CmsVerifyRequest
<byte[]>
{
Signature,
Message
}
	Byte[] Signiture	آرایه‌ای از رشته Base64 که حاوی یک قالب CMS است. این قالب در درون خود شامل مقدار امضا و گواهی استفاده شده جهت صدور امضا بر روی اطلاعات می‌باشد.

	Byte[] Message	آرایه‌ای از رشته‌ای که در قالب Base64 برای امضا ارسال شده است.
خروجی	bool	نتیجه‌ی صحت امضای ارسال شده.

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/CryptoService_CmsVerify	

ورودی‌ها
CmsVerifyRequest
<string>
{
Signature,
Message
}
	string Signiture	رشته Base64 که حاوی یک قالب CMS است. این قالب در درون خود شامل مقدار امضا و گواهی استفاده شده جهت صدور امضا بر روی اطلاعات می‌باشد.

	string Message	رشته‌ای که در قالب Base64 برای امضا ارسال شده است.
خروجی	bool	نتیجه‌ی صحت امضای ارسال شده.

تصدیق امضای دیجیتال در قالبCMS و اعتبار سنجی گواهی

به منظور تصدیق امضای دیجیتالی که در قالب CMS قرار دارد و نیز اعتبار سنجی گواهی امضاکننده، در کلاس Crypto توابعی در نظر گرفته شده است. تابعی که این خدمت را ارائه می‌دهد در جدول زیر آمده است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_CmsVerifyAndValidateCertificateAttachRaw	

ورودی‌ها
PdfVerifyAnd
ValidateRequest
<byte[]>
{
SignedData,
VaProfile
}
	Byte[] SignedData	رشته Base64 که حاوی یک قالب CMS است. این قالب در درون خود شامل اطلاعات امضا شده، مقدار امضا و گواهی استفاده شده جهت صدور امضا بر روی اطلاعات می‌باشد.

	string vaProfile	نام پروفایل مورد استفاده
خروجی	IEnumerable <VerificationResult>	آرایه‌ای از نوع VerificationResult که نتیجه تصدیق هر ردیف از امضا را برمی گرداند

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_CmsVerifyAndValidateCertificateAttach	

ورودی‌ها
PdfVerifyAnd
ValidateRequest
<string>
{
SignedData,
VaProfile
}
	string SignedData	رشته Base64 که حاوی یک قالب CMS است. این قالب در درون خود شامل اطلاعات امضا شده، مقدار امضا و گواهی استفاده شده جهت صدور امضا بر روی اطلاعات می‌باشد.

	string vaProfile	نام پروفایل مورد استفاده

خروجی	IEnumerable<VerificationResult>	آرایه ای از نوع VerificationResult که نتیجه تصدیق هر ردیف از امضا را برمی گرداند

نتایج بازگشتی(VerificationResult)

```
VerificationOK = 0,
CertPeriodValidationFailed = 1,
CertChainValidationFailed = 2,
CertIntgrityValidationFailed = 3,
CertKeyUsageValidationFailed = 4,
CertOCSPValidationRevoked = 5,
CertOCSPValidationUnKnown = 6,
CertCRLValidationRevoked = 7,
CertCRLAndOCSPValidationFailed = 8,
VerificationFailed = 9,
CMSDataNotAttached = 10,
CMSFromatIncorrect = 11,
CertPeriodAndTimeMismatch = 12,
SignitureNotFound=13,
InvalidSignDateTime = 14
```

در صورتی‌که قالب CMS حاوی اطلاعات امضا شده نباشد، در این صورت به منظور تصدیق امضا موجود در این قالب، خود اطلاعات امضا شده نیز موردنیاز می‌باشد. به منظور تصدیق امضای دیجیتال در این شرایط، تابع زیر در کلاس Crypto در نظر گرفته شده است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_CmsVerifyAndValidateCertificateRaw	
ورودی‌ها CmsVerifyAnd ValidateRequest <byte[]>{ Signature, Message, VaProfile }	Byte[] signature	رشته Base64 که حاوی یک قالب CMS است. این قالب در درون خود شامل مقدار امضا و گواهی استفاده شده جهت صدور امضا بر روی اطلاعات می‌باشد.
	Byte[] message	اطلاعات امضا شده به فرمت Base64 در ورودی تابع قرار میگیرد.
	string vaProfile	نام پروفایل مورداستفاده
خروجی	IEnumerable<VerificationResult>	آرایه ای از نوع VerificationResult که نتیجه تصدیق هر ردیف از امضا را برمی‌گرداند. مشخص‌کننده‌ی صحت امضای ارسال شده و اعتبار گواهی امضاکننده می‌باشد.
نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_CmsVerifyAndValidateCertificate	
ورودی‌ها CmsVerifyAnd ValidateRequest <string>{ Signature, Message, VaProfile }	string signature	رشته Base64 که حاوی یک قالب CMS است. این قالب در درون خود شامل مقدار امضا و گواهی استفاده شده جهت صدور امضا بر روی اطلاعات می‌باشد.
	string message	اطلاعات امضا شده به فرمت Base64 در ورودی تابع قرار میگیرد.
	string vaProfile	نام پروفایل مورداستفاده

خروجی	IEnumerable<VerificationResult>	آرایه ای از نوع VerificationResult که نتیجه تصدیق هر ردیف از امضا را برمی‌گرداند. مشخص‌کننده‌ی صحت امضای ارسال شده و اعتبار گواهی امضاکننده می‌باشد.

نتایج بازگشتی(VerificationResult)

```
VerificationOK = 0,
CertPeriodValidationFailed = 1,
CertChainValidationFailed = 2,
CertIntgrityValidationFailed = 3,
CertKeyUsageValidationFailed = 4,
CertOCSPValidationRevoked = 5,
CertOCSPValidationUnKnown = 6,
CertCRLValidationRevoked = 7,
CertCRLAndOCSPValidationFailed = 8,
VerificationFailed = 9,
CMSDataNotAttached = 10,
CMSFromatIncorrect = 11,
CertPeriodAndTimeMismatch = 12,
SignitureNotFound=13,
InvalidSignDateTime = 14
```

دریافت Policyهای گواهینامه

این تابع تمام Policy های یک گواهی‌نامه را به صورت لیستی از رشته‌ها استخراج می‌کند. جزئیات تابع ارائه‌دهنده‌ی این خدمت در کلاس Crypto به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_CertificatePoliciesRaw	
ورودی‌ها	Byte[] Base64Certificate	گواهینامه
خروجی	string[]	لیست policy های گواهینامه

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_CertificatePolicies	
ورودی‌ها	string Base64Certificate	گواهینامه
خروجی	String[]	لیست policy های گواهینامه

ایجاد Hash برای امضای یک پیام

به منظور امضای یک پیام، لازم است ابتدا Hash آن پیام به دست آید. در کلاس Crypto تابعی برای این کار در نظر گرفته شده است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/CryptoService_DigestRaw	

ورودی‌ها
DigestRequest<byte[]>
{
Message,
HashAlgorithm
}
	byte[] message	متن پیام به فرمت Base64 در ورودی تابع قرار می‌گیرد.

	HashAlgorithm hashAlgorithm	الگوریتم درهم سازی مورد استفاده.
خروجی	byte[]	آرایه‌ی رشته Base64 حاوی Hash پیام

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/CryptoService_Digest	
ورودی‌ها DigestRequest<string> { Message, HashAlgorithm}	string message	متن پیام به فرمت Base64 در ورودی تابع قرار می‌گیرد.
	HashAlgorithm hashAlgorithm	الگوریتم درهم سازی مورد استفاده.
خروجی	string	رشته Base64 حاوی Hash پیام

از توابع زیر برای گرفتن Hash پیام در قالب Cms استفاده می‌گردد:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_CmsDigestRaw	

ورودی‌ها
CmsDigestRequest<byte[]>
{
Message,
Certificate,
HashAlgorithm,
SignDate
}
	byte[] message	آرایه‌ی متن پیام به فرمت Base64 در قالب CMS

	byte[] Certificate	گواهی موردنظر
	HashAlgorithm hashAlgorithm	الگوریتم درهم سازی مورد استفاده.
	DateTime SignDate	زمان امضا
خروجی	byte[]	آرایه‌ی رشته Base64 حاوی Hash پیام

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_CmsDigest	

ورودی‌ها
CmsDigestRequest<string>
{
Message,
Certificate,
HashAlgorithm,
SignDate
}
	string message	متن پیام به فرمت Base64

	string Certificate	گواهی موردنظر
	HashAlgorithm hashAlgorithm	الگوریتم درهم سازی مورد استفاده.
	DateTime SignDate	زمان امضا
خروجی	string	رشته Base64 حاوی Hash پیام

نکته مهم: تمامی ورودی‌های مشترک در دو تابع CmsDigest و PutCmsSignature باید دارای مقادیر یکسان باشند.

مقادیر HashAlgorithm:

```
SHA1 = 0,
SHA256 = 1,
SHA384 = 2,
SHA512 = 3
```

قرار دادن Digest امضا در محتوای Cms

از این تابع به منظور قرار دادن مقدار Digest امضا شده در CMS استفاده می‌شود و محتوای امضا شده در قالب رشته Base64 بازگشت داده می‌شود.

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_PutCMSSignatureRaw	

ورودی‌ها
CMSSignature<byte[]>
{
Message,
Certificate,
HashAlgorithm,
SignDate,
Signature,
Encapsulate
}
	byte[] message	آرایه‌ی متن پیام به فرمت Base64 در قالب CMS

	byte[] Certificate	گواهی موردنظر
	HashAlgorithm hashAlgorithm	الگوریتم درهم سازی مورد استفاده.
	DateTime SignDate	زمان امضا
	byte[] Signature	آرایه‌ی رشته base64 امضا
	bool Encapsulate	محتوا در امضا کپسوله شود یا خیر
خروجی	byte[]	آرایه‌ی رشته Base64 حاوی Hash پیام

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_PutCMSSignature	

ورودی‌ها
CMSSignature<string>
{
Message,
Certificate,
HashAlgorithm,
SignDate,
Signature,
Encapsulate
}
	string message	متن پیام به فرمت Base64

	string Certificate	گواهی موردنظر
	HashAlgorithm hashAlgorithm	الگوریتم درهم سازی مورد استفاده.
	DateTime SignDate	زمان امضا
	string Signature	رشته base64 امضا
	bool Encapsulate	محتوا در امضا کپسوله شود یا خیر
خروجی	string	رشته Base64 حاوی Hash پیام

نکته مهم: تمامی ورودی‌های مشترک در دو تابع CmsDigest و PutCmsSignature باید دارای مقادیر یکسان باشند.

ایجاد Hash برای امضای یک سند PDF

به منظور امضای یک سند PDF، لازم است ابتدا Hash آن سند به دست آید. در کلاس Crypto تابعی برای این کار در نظر گرفته شده است:

نکته: در این تابع از الگوریتم SHA1 استفاده شده است. بنابراین برای امضای نتیجه این تابع نیز باید از الگوریتم SHA1 استفاده گردد.

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/CryptoService_PDFDigestRaw	

ورودی‌ها
PDFDigestRequest<byte[]>
{
PdfData,
Certificate,
DateTime,
ImageDataUrl,
CrProfile,
}
	byte[] pdfData	فایل pdf در قالب Base64 در ورودی تابع قرار میگیرد.

	byte[] certificate	گواهی مورد نظر جهت استفاده برای عملیات امضای دیجیتال.
	DateTime datetime	زمان امضا
	string ImageDataUrl	تصویر مورد استفاده در سند امضا شده
	string crProfile	نام پروفایل استفاده شده جهت امضای فایل pdf
خروجی	byte[]	آرایه‌ی رشته Base64 که حاوی hash فایل pdf

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/CryptoService_PDFDigest	

ورودی‌ها
PDFDigestRequest<byte[]>
{
PdfData,
Certificate,
DateTime,
ImageDataUrl,
CrProfile,
}
	string pdfData	فایل pdf در قالب Base64 در ورودی تابع قرار میگیرد.

	string certificate	گواهی مورد نظر جهت استفاده برای عملیات امضای دیجیتال.
	DateTime datetime	زمان امضا
	String ImageDataUrl	تصویر مورد استفاده در سند امضا شده
	string crProfile	نام پروفایل استفاده شده جهت امضای فایل pdf
خروجی	string	رشته Base64 که حاوی hash فایل pdf

ایجاد Hash برای امضاهای متعدد در یک سند PDF

به منظور امضاهای متعدد یک سند PDF، لازم است ابتدا Hash آن سند به دست آید. در کلاس Crypto دو تابع برای این‌کار در نظر گرفته شده است:

نام تابع	API/CryptoService/PDFDigestRaw	

ورودی‌ها
PDFDigestRequest
<byte[]>
{
PdfData,
Certificate,
CrProfile,
DateTime,
ImageDataUrl
}
	byte[] pdfData	فایل pdf در قالب Base64 در ورودی تابع قرار میگیرد.

	byte[] certificate	گواهی مورد نظر جهت استفاده برای عملیات امضای دیجیتال.
	string crProfile	نام پروفایل مورداستفاده
	DateTime datetime	زمان گرفتن Hash
	string ImageDataUrl	تصویر مورد استفاده
خروجی	byte[]	آرایه‌ی رشته Base64 که حاوی محتویات فایل pdf به صورت Hash شده می‌باشد.

نام تابع	API/CryptoService/PDFDigest	

ورودی‌ها
PDFDigestRequest
<string>
{
PdfData,
Certificate,
CrProfile,
DateTime,
ImageDataUrl
}
	string pdfData	فایل pdf در قالب Base64 در ورودی تابع قرار میگیرد.

	string certificate	گواهی مورد نظر جهت استفاده برای عملیات امضای دیجیتال.
	string crProfile	نام پروفایل مورداستفاده
	DateTime datetime	زمان گرفتن Hash
	string ImageDataUrl	تصویر مورد استفاده
خروجی	string	رشته Base64 که حاوی محتویات فایل pdf به صورت Hash شده می‌باشد.

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_PDFDigestForMultiSignRaw	
ورودی‌ها MultiSignPdfDigest Request <byte[]> { PdfData, HashAlgorithm, CertificationLevel, DateTime DateTime, SignerCertificate, ImageDataUrl, Location, LowerLeftX, LowerLeftY, UpperRightX, UpperRightY, Page, Reason, SignatureFieldName }	byte[] pdfData	آرایه‌ی فایل pdf در قالب Base64 .
	HashAlgorithm HashAlgorithm	الگوریتم درهم سازی استفاده شده در عملیات امضای دیجیتال.
	CertificationLevel certificationLevel	نوع امضای برروی pdf NOT_CERTIFIED = 0, CERTIFIED_NO_CHANGES_ALLOWED = 1, CERTIFIED_FORM_FILLING = 2, CERTIFIED_FORM_FILLING_AND_ANNOTATION = 3,
	DateTime datetime	زمان Hash
	byte [] signatureCertificate	گواهی مورد نظر جهت استفاده برای عملیات امضای دیجیتال در قالب Base64
	string ImageDataUrl	تصویر مورد استفاده در سند امضا شده
	string Location	نام موقعیت مکانی
	int LowerLeftX	مختصاتی که تصویر امضا در آنجا قرار داده می‌شود.
	int LowerLeftY	مختصاتی که تصویر امضا در آنجا قرار داده می‌شود.
	int UpperRightX	مختصاتی که تصویر امضا در آنجا قرار داده می‌شود.
	int UpperRightY	مختصاتی که تصویر امضا در آنجا قرار داده می‌شود.
	int Page	صفحه‌ای که تصویر امضا در آن قرار داده شود
	string Reason	متن دلیل امضا
	string signatureFieldName	نام فیلد امضا در pdf
خروجی	Byte[]	آرایه‌ی رشته Base64 که حاوی Hash فایل pdf

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_PDFDigestForMultiSign	
ورودی‌ها MultiSignPdfDigest Request <string> { PdfData, HashAlgorithm, CertificationLevel, DateTime DateTime, SignerCertificate, ImageDataUrl, Location, LowerLeftX, LowerLeftY, UpperRightX, UpperRightY, Page, Reason, SignatureFieldName }	string pdfData	فایل pdf در قالب Base64 .
	HashAlgorithm HashAlgorithm	الگوریتم درهم سازی استفاده شده در عملیات امضای دیجیتال.
	CertificationLevel certificationLevel	نوع امضای برروی pdf NOT_CERTIFIED = 0, CERTIFIED_NO_CHANGES_ALLOWED = 1, CERTIFIED_FORM_FILLING = 2, CERTIFIED_FORM_FILLING_AND_ANNOTATION = 3,
	DateTime datetime	زمان Hash
	string signatureCertificate	گواهی مورد نظر جهت استفاده برای عملیات امضای دیجیتال در قالب Base64
	string ImageDataUrl	تصویر مورد استفاده در سند امضا شده
	string Location	نام موقعیت مکانی
	int LowerLeftX	مختصاتی که تصویر امضا در آنجا قرار داده می‌شود.
	int LowerLeftY	مختصاتی که تصویر امضا در آنجا قرار داده می‌شود.
	int UpperRightX	مختصاتی که تصویر امضا در آنجا قرار داده می‌شود.
	int UpperRightY	مختصاتی که تصویر امضا در آنجا قرار داده می‌شود.
	int Page	صفحه‌ای که تصویر امضا در آن قرار داده شود
	string Reason	متن دلیل امضا
	string signatureFieldName	نام فیلد امضا در pdf
خروجی	string	رشته Base64 که حاوی Hash فایل pdf

استخراج گواهینامه‌ها از فایل PDF

این تابع تمامی گواهینامه‌هایی که به منظور امضای فایل PDF مورد استفاده قرار گرفته‌اند را از فایل استخراج می‌کند.

جزئیات تابع ارائه‌دهنده‌ی این خدمت در کلاس Crypto به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_PdfExtractCertificatesRaw	
ورودی‌ها	byte[] signedPdf	آرایه‌ی رشته Base64 که حاوی یک فایل PDF امضا شده می‌باشد
خروجی	IEnumerable<byte[]	آرایه‌ای از گواهی‌های استخراج‌شده از درون فایل PDF

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_PdfExtractCertificates	
ورودی‌ها	string signedPdf	رشته Base64 که حاوی یک فایل PDF امضا شده می‌باشد
خروجی	IEnumerable<string>	آرایه‌ای از گواهی‌های استخراج‌شده از درون فایل PDF

استخراج اطلاعات امضاها از فایل PDF

این تابع اطلاعات تمامی امضاهای موجود در فایل PDF را استخراج می‌کند. جزئیات تابع ارائه‌دهنده‌ی این خدمت در کلاس Crypto به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_PDFExtractSignerInfoRaw	
ورودی‌ها	`Byte[] signedPdf`	آرایه‌ی رشته Base64 که حاوی یک فایل PDF امضا شده می‌باشد
خروجی	`IEnumerable<SignerInfo<byte[]>>`	آرایه‌ای از اطلاعات امضاهای موجود در گواهی

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_PDFExtractSignerInfo	
ورودی‌ها	`string signedPdf`	رشته Base64 که حاوی یک فایل PDF امضا شده می‌باشد
خروجی	`IEnumerable<SignerInfo<string>>`	آرایه‌ای از اطلاعات امضاهای موجود در گواهی

تصدیق امضای دیجیتال PDF

این تابع به منظور تصدیق امضای دیجیتال صادرشده بر روی یک فایل PDF مورد استفاده قرار می‌گیرد. جزئیات تابع ارائه‌دهنده‌ی این خدمت در کلاس Crypto به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/CryptoService_PDFVerifyRaw	
ورودی‌ها	`Byte[] signedPdf`	آرایه‌ی رشته Base64 که حاوی یک فایل PDF امضا شده می‌باشد.
خروجی	`bool`	مشخص‌کننده‌ی صحت امضای صادرشده بر روی فایل PDF

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/CryptoService_PDFVerify	
ورودی‌ها	`string signedPdf`	رشته Base64 که حاوی یک فایل PDF امضا شده می‌باشد.
خروجی	`bool`	مشخص‌کننده‌ی صحت امضای صادرشده بر روی فایل PDF

تصدیق امضای دیجیتال PDF و اعتبارسنجی گواهی‌های امضا

این تابع به منظور تصدیق امضای دیجیتال صادرشده بر روی یک فایل PDF مورد استفاده قرار می‌گیرد. همچنین در این روش همه استانداردهای موجود جهت بررسی اعتبار گواهینامه‌های موجود در امضا بررسی می‌شود. جزئیات تابع ارائه‌دهنده‌ی این خدمت در کلاس Crypto به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_PDFVerifyAndValidateCertificateRaw	
ورودی‌ها PdfVerifyAnd ValidateRequest <byte[]> { SignedData, VaProfile }	Byte[] signedData	آرایه‌ی رشته Base64 که حاوی یک فایل PDF امضا شده می‌باشد.
	string vaProfile	نام پروفایل مورد استفاده(اختیاری)
خروجی	IEnumerable <VerificationResult>	خروجی شامل وضعیت اعتبارسنجی گواهینامه‌ها

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_PDFVerifyAndValidateCertificate	
ورودی‌ها PdfVerifyAnd ValidateRequest <string> { SignedData, VaProfile }	string signedData	رشته Base64 که حاوی یک فایل PDF امضا شده می‌باشد.
	string vaProfile	نام پروفایل مورد استفاده(اختیاری)
خروجی	IEnumerable <VerificationResult>	خروجی شامل وضعیت اعتبارسنجی گواهینامه‌ها

نتایج بازگشتی(VerificationResult)

```
VerificationOK = 0,
CertPeriodValidationFailed = 1,
CertChainValidationFailed = 2,
CertIntgrityValidationFailed = 3,
CertKeyUsageValidationFailed = 4,
CertOCSPValidationRevoked = 5,
CertOCSPValidationUnKnown = 6,
CertCRLValidationRevoked = 7,
CertCRLAndOCSPValidationFailed = 8,
VerificationFailed = 9,
CMSDataNotAttached = 10,
CMSFromatIncorrect = 11,
CertPeriodAndTimeMismatch = 12,
SignitureNotFound = 13,
InvalidSignDateTime = 14
```

قرار دادن امضا در سند PDF

از این تابع به منظور قرار دادن مقدار Digest امضا شده در سند PDF (منطبق با استاندارد#PKCS7) استفاده می‌شود و سند امضا شده در قالب رشته Base64 بازگشت داده می‌شود.

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_PutPDFSignatureRaw	

ورودی‌ها
PDFSignature<byte[]>
{
PdfData,
Signature,
Certificate,
DateTime,
ImageDataUrl,
CrProfile
}
	byte[] pdfData	فایل pdf در قالب Base64 در ورودی تابع قرار میگیرد.

	byte[] Signature	مقدار Digest امضا شده
	byte[] certificate	گواهی مورد نظر جهت استفاده برای عملیات امضای دیجیتال
	DateTime datetime	زمان امضا
	string ImageDataUrl	تصویر مورد استفاده در سند امضا شده
	string crProfile	نام پروفایل استفاده شده جهت امضای فایل pdf
خروجی	byte[]	آرایه‌ی رشته Base64 حاوی محتویات فایل pdf

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_PutPDFSignature	

ورودی‌ها
PDFSignature<string>
{
PdfData,
Signature,
Certificate,
DateTime,
ImageDataUrl,
CrProfile
}
	string pdfData	فایل pdf در قالب Base64 در ورودی تابع قرار میگیرد.

	String Signature	مقدار Digest امضا شده
	string certificate	گواهی مورد نظر جهت استفاده برای عملیات امضای دیجیتال
	DateTime datetime	زمان امضا
	string ImageDataUrl	تصویر مورد استفاده در سند امضا شده
	string crProfile	نام پروفایل استفاده شده جهت امضای فایل pdf
خروجی	string	رشته Base64 حاوی محتویات فایل pdf

نکته مهم: تمامی ورودی‌های مشترک در دو تابع PdfDigest و PutPDFSignature باید دارای مقادیر یکسان باشند.

قرار دادن امضاهای متعدد در سند PDF

از این تابع به منظور قرار دادن مقدار Digest امضا شده در یک سند PDF (منطبق با استاندارد#PKCS7) استفاده می‌شود که دارای امضاهای متعددی است. سند امضا شده در قالب رشته Base64 بازگشت داده می‌شود.

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_PutPDFSignatureForMultiSignRaw	

ورودی‌ها
MultiSignPdfDigest Request
<byte[]>
{
PdfData,
HashAlgorithm,
CertificationLevel,
DateTime DateTime,
SignerCertificate,
ImageDataUrl,
Location,
LowerLeftX,
LowerLeftY,
UpperRightX,
UpperRightY,
Page,
Reason,
SignatureFieldName
}
	Byte[] pdfData	فایل pdf در قالب Base64 .

	HashAlgorithm HashAlgorithm	الگوریتم درهم سازی استفاده شده در عملیات امضای دیجیتال.
	CertificationLevel certificationLevel	نوع امضای برروی pdf NOT_CERTIFIED = 0, CERTIFIED_NO_CHANGES_ALLOWED = 1, CERTIFIED_FORM_FILLING = 2, CERTIFIED_FORM_FILLING_AND_ANNOTATION= 3,
	DateTime datetime	زمان Hash
	Byte[] signatureCertificate	گواهی مورد نظر جهت استفاده برای عملیات امضای دیجیتال در قالب Base64
	string ImageDataUrl	تصویر مورد استفاده در سند امضا شده
	string Location	نام موقعیت مکانی
	int LowerLeftX	مختصاتی که تصویر امضا در آنجا قرار داده می‌شود.
	int LowerLeftY	مختصاتی که تصویر امضا در آنجا قرار داده می‌شود.
	int UpperRightX	مختصاتی که تصویر امضا در آنجا قرار داده می‌شود.
	int UpperRightY	مختصاتی که تصویر امضا در آنجا قرار داده می‌شود.
	int Page	صفحه‌ای که تصویر امضا در آن قرار داده شود
	string Reason	متن دلیل امضا
	string signatureFieldName	نام فیلد امضا در pdf
خروجی	Byte[]	رشته Base64 که حاوی محتویات فایل pdf به صورت امضا شده می‌باشد.

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_PutPDFSignatureForMultiSign	

ورودی‌ها
MultiSignPdfDigest Request <string>
{
PdfData,
HashAlgorithm,
CertificationLevel,
DateTime DateTime,
SignerCertificate,
ImageDataUrl,
Location,
LowerLeftX,
LowerLeftY,
UpperRightX,
UpperRightY,
Page,
Reason,
SignatureFieldName
}
	string pdfData	فایل pdf در قالب Base64 .

	HashAlgorithm HashAlgorithm	الگوریتم درهم سازی استفاده شده در عملیات امضای دیجیتال.
	CertificationLevel certificationLevel	نوع امضای برروی pdf NOT_CERTIFIED = 0, CERTIFIED_NO_CHANGES_ALLOWED = 1, CERTIFIED_FORM_FILLING = 2, CERTIFIED_FORM_FILLING_AND_ANNOTATION= 3,
	DateTime datetime	زمان Hash
	string signatureCertificate	گواهی مورد نظر جهت استفاده برای عملیات امضای دیجیتال در قالب Base64
	string ImageDataUrl	تصویر مورد استفاده در سند امضا شده
	string Location	نام موقعیت مکانی
	int LowerLeftX	مختصاتی که تصویر امضا در آنجا قرار داده می‌شود.
	int LowerLeftY	مختصاتی که تصویر امضا در آنجا قرار داده می‌شود.
	int UpperRightX	مختصاتی که تصویر امضا در آنجا قرار داده می‌شود.
	int UpperRightY	مختصاتی که تصویر امضا در آنجا قرار داده می‌شود.
	int Page	صفحه‌ای که تصویر امضا در آن قرار داده شود
	string Reason	متن دلیل امضا
	string signatureFieldName	نام فیلد امضا در pdf
خروجی	string	رشته Base64 که حاوی محتویات فایل pdf به صورت امضا شده می‌باشد.

نکته مهم: تمامی ورودی های مشترک در تابع PDFDigestForMultiSign و در تابع PutPDFSignatureForMultiSign باید دارای مقادیر یکسان باشند.

استخراج گواهی از مهر زمانی

این تابع به منظور استخراج گواهینامه از مهر زمانی صادرشده مورد استفاده قرار می‌گیرد. جزئیات تابع ارائه‌دهنده‌ی این خدمت در کلاس Crypto به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_TstExtractCertificatesRaw	
ورودی‌ها	Byte[] tst	رشته Base64 که حاوی مهر زمانی صادرشده می‌باشد.
خروجی	IEnumerable<string>	آرایه‌ای از گواهی‌های استخراج‌شده از مهر زمانی.

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_TstExtractCertificates	
ورودی‌ها	string tst	رشته Base64 که حاوی مهر زمانی صادرشده می‌باشند.
خروجی	IEnumerable<string>	آرایه‌ای از گواهی‌های استخراج‌شده از مهر زمانی.

استخراج زمان از مهر زمانی

این تابع به منظور استخراج زمان از مهر زمانی صادرشده مورد استفاده قرار می‌گیرد. جزئیات تابع ارائه‌دهنده‌ی این خدمت در کلاس Crypto به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/CryptoService_TstExtractTimeRaw	
ورودی‌ها	Byte[] tst	آرایه‌ی رشته Base64 که حاوی مهر زمانی صادرشده می‌باشد.
خروجی	DateTime	زمان استخراج‌شده از درون مهر زمانی.

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/CryptoService_TstExtractTime	
ورودی‌ها	string tst	رشته Base64 که حاوی مهر زمانی صادرشده می‌باشند.
خروجی	DateTime	زمان استخراج‌شده از درون مهر زمانی.

تصدیق مهر زمانی

این تابع به منظور تصدیق مهر زمانی صادرشده مورد استفاده قرار می‌گیرد. جزئیات تابع ارائه‌دهنده‌ی این خدمت در کلاس Crypto به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_TstVerifyRaw	

ورودی‌ها
TimestampVerifyRequest<byte[]>
{
Message,
Certificate,
Timestamp
}
	Byte[] message	رشته Base64 که مهر زمانی بر روی آن صادرشده است.

	Byte[] cerificate	رشته Base64 گواهینامه که در صورتیکه ارسال نشود از گواهینامه‌ی موجود در رشته امضا شده حاوی مهر زمانی استفاده می‌کند.
	string tst	رشته Base64 که حاوی مهر زمانی صادرشده می‌باشند.
خروجی	bool	مشخص‌کننده‌ی صحت مهر زمانی

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_TstVerify	

ورودی‌ها
TimestampVerifyRequest<string>
{
Message,
Certificate,
Timestamp
}
	String message	رشته Base64 که مهر زمانی بر روی آن صادرشده است.

	String cerificate	رشته Base64 گواهینامه که در صورتیکه ارسال نشود از گواهینامه‌ی موجود در رشته امضا شده حاوی مهر زمانی استفاده می‌کند.
	string tst	رشته Base64 که حاوی مهر زمانی صادرشده می‌باشند.

خروجی	`bool`	مشخص‌کننده‌ی صحت مهر زمانی

امضای الکترونیک

این تابع جهت امضای پیام استفاده می‌شود. تعریف تابع ارائه‌دهنده‌ی این خدمت به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/CryptoService_SignRaw	
ورودی‌ها `CryptoSignRequest <byte[]> { Data, Certificate, HashAlgorithm }`	`byte[]` Data	آرایه‌ی حاوی رشته Base64 که برای انجام امضای الکترونیک
	`Byte[]` certificate	گواهی موردنظر جهت استفاده برای امضای دیجیتال
	`HashAlgorithm` hashAlgorithm	الگوریتم درهم‌سازی موردنظر برای امضای دیجیتال
خروجی	`byte[]`	آرایه‌ی رشته Base64 حاوی مقدار امضای الکترونیکی

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/CryptoService_Sign	
ورودی‌ها `CryptoSignRequest <string> { Data, Certificate, HashAlgorithm }`	`string` Data	حاوی رشته Base64 که برای انجام امضای الکترونیک
	`string` certificate	گواهی مورد نظر جهت استفاده برای امضای دیجیتال
	`HashAlgorithm` hashAlgorithm	الگوریتم درهم‌سازی موردنظر برای امضای دیجیتال
خروجی	`string`	رشته Base64 حاوی مقدار امضای الکترونیکی

بررسی امضای الکترونیک

این تابع جهت تصدیق امضای صادرشده بر روی اطلاعات مشخص شده استفاده می‌شود. تعریف تابع ارائه‌دهنده‌ی این خدمت به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/CryptoService_VerifyRaw	
ورودی‌ها `VerifyRequest<byte[]> { Data, Certificate, Signature, HashAlgorithm }`	`Byte[]` data	رشته Base64 که امضای الکترونیک بر روی آن صورت گرفته است.
	`Byte[]` certificate	گواهی مورد نظر جهت استفاده برای عملیات تصدیق امضای دیجیتال.
	`string` signature	رشته Base64 حاوی مقدار امضای صادرشده بر روی اطلاعات.
	`HashAlgorithm` hashAlgorithm	الگوریتم درهم سازی استفاده شده در عملیات امضای دیجیتال.
خروجی	`bool`	مشخص‌کننده‌ی صحت امضای ارسال شده.

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/CryptoService_Verify		

ورودی‌ها
VerifyRequest<string>
{
Data,
Certificate,
Signature,
HashAlgorithm
}
	string data	رشته Base64 که امضای الکترونیک بر روی آن صورت گرفته است.

	string certificate	گواهی مورد نظر جهت استفاده برای عملیات تصدیق امضای دیجیتال.
	string signature	رشته Base64 حاوی مقدار امضای صادرشده بر روی اطلاعات.
	HashAlgorithm hashAlgorithm	الگوریتم درهم سازی استفاده شده در عملیات امضای دیجیتال.
خروجی	bool	مشخص‌کننده‌ی صحت امضای ارسال شده.

اعتبار سنجی سند XML امضا شده

یک سند XML که امضا شده باشد را به کمک تابع XMLVerify می توان اعتبارسنجی کرد.

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/CryptoService_XMLVerify	
ورودی‌ها	Stream signedXML	سند XML امضا شده به صورت Stream
خروجی	bool	مشخص کننده صحت امضای سند XML

رمزگذاری

این تابع جهت رمزگذاری اطلاعات مشخص شده استفاده می‌شود. تعریف تابع ارائه‌دهنده‌ی این خدمت به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/CryptoService_EncryptRaw	

ورودی‌ها
CryptoRequest<byte[]>
{
Certificate,
Cipher
}
	Byte[] Certificate	رشته Base64 گواهینامه برای عملیات رمزگذاری

	Byte[] Cipher	رشته موردنظر برای عملیات رمزگذاری
خروجی	Byte[]	رشته Base64 رمزگذاری شده

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/CryptoService_Encrypt	
ورودی‌ها CryptoRequest<string>	string Certificate	رشته Base64 گواهینامه برای عملیات رمزگذاری

{ Certificate, Cipher }	`string` Cipher	رشته موردنظر برای عملیات رمزگذاری
خروجی	`Byte[]`	رشته Base64 رمزگذاری شده

رمزگشایی

این تابع جهت رمزگشایی اطلاعات مشخص شده استفاده می‌شود. تعریف تابع ارائه‌دهنده‌ی این خدمت به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/CryptoService_DecryptRaw	
ورودی‌ها	`Byte[]` message	رشته Base64 رمزگذاری شده
خروجی	`Byte[]`	آرایه‌ی رشته Base64 رمزگشایی شده

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/CryptoService_Decrypt	
ورودی‌ها	`string` message	رشته Base64 رمزگذاری شده
خروجی	`string`	رشته Base64 رمزگشایی شده

رمزگذاری متقارن

این تابع جهت رمزگذاری متقارن اطلاعات مشخص شده استفاده می‌شود. تعریف تابع ارائه‌دهنده‌ی این خدمت به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_SymmetricEncryptRaw	
ورودی‌ها SymmetricDecryptRequest <byte[]> { Key, IV, SymmetricAlgorithm, Data }	`Byte[]` key	کلید رمزگذاری
	`Byte[]` IV	بردار آغازین
	`SymmetricAlgorithms` SymmetricAlgorithm	الگوریتم استفاده شده در عملیات رمزگذاری AES_CBC128, AES_CBC256, AES_CBC192, AES_ECB128, AES_ECB256, AES_ECB192,
	`Byte[]` Data	رشته موردنظر برای عملیات رمزگذاری
خروجی	`Byte[]`	رشته Base64 رمزگذاری شده

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_SymmetricEncrypt	

ورودی‌ها
SymmetricDecryptRequest <string>
{
Key,
IV,
SymmetricAlgorithm,
Cipher
}
	strng key	کلید رمزگذاری

	string IV	بردار آغازین
	SymmetricAlgorithms SymmetricAlgorithm	الگوریتم استفاده شده در عملیات رمزگذاری AES_CBC128, AES_CBC256, AES_CBC192, AES_ECB128, AES_ECB256, AES_ECB192,
	string data	رشته موردنظر برای عملیات رمزگذاری
خروجی	string	رشته Base64 رمزگذاری شده

رمزگشایی متقارن

این تابع جهت رمزگشایی متقارن اطلاعات مشخص شده استفاده می‌شود. جزئیات این تابع به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_SymmetricDecryptRaw	

ورودی‌ها
SymmetricDecryptRequest <byte[]>
{
Key,
IV,
SymmetricAlgorithm,
Cipher
}
	Byte[] key	کلید رمزگشایی

	Byte[] IV	بردار آغازین
	SymmetricAlgorithms SymmetricAlgorithm	الگوریتم استفاده شده در عملیات رمزگذاری AES_CBC128, AES_CBC256, AES_CBC192, AES_ECB128, AES_ECB256, AES_ECB192,
	Byte[] cipher	رشته Base64 رمزگذاری شده
خروجی	Byte[]	رشته Base64 رمزگشایی شده

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_SymmetricDecrypt	

ورودی‌ها
SymmetricDecryptRequest <string>
{
Key,
IV,
SymmetricAlgorithm,
Cipher
}
	strng key	کلید رمزگشایی

	string IV	بردار آغازین
	SymmetricAlgorithms SymmetricAlgorithm	الگوریتم استفاده شده در عملیات رمزگذاری AES_CBC128, AES_CBC256, AES_CBC192, AES_ECB128, AES_ECB256, AES_ECB192,
	string cipher	رشته Base64 رمزگذاری شده
خروجی	string	رشته Base64 رمزگشایی شده

استخراج پیام از قالب CMSAttached

به منظور دستیابی به پیام که در یک قالب CMS موجود می‌باشد و عملیات رمزنگاری با استفاده از آن انجام شده است، در کلاس Crypto تابع زیر در نظر گرفته شده است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_CmsExtractAttachedMessageRaw	
ورودی‌ها	Byte[] messgaeSignatureCertificate	آرایه‌ی رشته Base64 که حاوی یک قالب CMS است. این قالب در درون خود شامل پیام استفاده شده جهت انجام عملیات رمزنگاری بر روی اطلاعات می‌باشد
خروجی	byte[]	آرایه‌ی پیام استخراج‌شده از درون قالب CMS

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_CmsExtractAttachedMessage	
ورودی‌ها	string messgaeSignatureCertificate	رشته Base64 که حاوی یک قالب CMS است. این قالب در درون خود شامل پیام استفاده شده جهت انجام عملیات رمزنگاری بر روی اطلاعات می‌باشد
خروجی	string	رشته Base64 پیام استخراج‌شده از درون قالب CMS

استخراج Thumbprint از فایل گواهی

به منظور دستیابی به فیلد Thumbprint که در فایل گواهی موجود می‌باشد، در کلاس Crypto تابع زیر در نظر گرفته شده است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_CertificateThumbprintRaw	
ورودی‌ها	Byte[] Base64Certificate	آرایه‌ی رشته Base64 که حاوی یک فایل گواهی است.
خروجی	byte[]	آرایه‌ی رشته Base64 از فیلد Thumbprint فایل گواهی

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /CryptoService_CertificateThumbprint	
ورودی‌ها	String Base64Certificate	رشته Base64 که حاوی یک فایل گواهی است.
خروجی	string	رشته Base64 از فیلد Thumbprint فایل گواهی

سرویس ورود به سیستم[1]

سرویس Login به منظور دسته‌بندی توابع مورد نیاز جهت اجرای روال شناسایی کاربر و ورود به سیستم، ایجاد شده

[1] LoginSrvice

است. توابع موجود در این سرویس ، توابع مورد نیاز جهت تولید رشته Challenge و تصدیق هویت کاربر می‌باشد.

در فرآیند تشخیص هویت کاربر، سرور با استفاده از تابعLoginChallenge از کلاس Login یک رشته تصادفی را در قالب Base64 تولید نموده و به سمت کاربر ارسال می‌نماید. در سمت کاربر رشته مربوطه با استفاده ازکلید خصوصی موجود در توکن کاربر امضا شده و رشته نهایی که امضای دیجیتال کاربر نیز در آن وجود دارد برای سرور ارسال خواهد شد. سپس سرور بر اساس کلید عمومی موجود در امضای الصاقی به رشته دریافت شده از سمت کاربر، هویت وی را تشخیص داده و در صورت تایید با توجه به سطوح دسترسی تعریف شده در سیستم، ورود کاربر را به سیستم میسر ساخته و منابع مورد درخواست را در اختیار وی قرار خواهد داد.

دریافت رشته کاراکتر تصادفی

این تابع مسئول تولید یک رشته تصادفی در قالب Base64 می‌باشد.

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/LoginService_LoginChallengeRaw	
ورودی‌ها	ندارد	
خروجی	Byte[]	آرایه رشته تصادفی در قالب Base64

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/LoginService_LoginChallenge	
ورودی‌ها	ندارد	
خروجی	string	رشته تصادفی در قالب Base64

دریافت فایل تنظیمات XML

این تابع مسئول دریافت فایل تنظیمات XML می‌باشد.

جزئیات تابع ارائه‌دهنده‌ی این خدمت در کلاس LoginService به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/LoginService_CurrentConfig	
ورودی‌ها	ندارد	
خروجی	object	فایل XML در قالب درخواست شده

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/LoginService_CurrentConfigAsXML	
ورودی‌ها	ندارد	
خروجی	string	رشته‌ی حاوی فایل XML

تصدیق هویت کاربر

این تابع با استفاده از رشته تولید شده در تابع LoginChallenge و رشته امضا شده دریافتی از سمت کاربر، هویت کاربر را بررسی و نتیجه تصدیق هویت را به همراه گواهی استخراج شده از امضای کاربر در خروجی باز می‌گرداند.

مقدار برگردانده شده برای AuthenticationResult می‌تواند شامل موارد زیر باشد:

```
UnKnown = 0,
Athenticated = 1,
SignatureVerificationError = 2,
CertificateValidationError = 3,
CertificateCrlCheckError = 4,
CertificateOcspCheckError = 5,
CertificateKeyUsageError = 6,
CertificateEnhancedKeyUsageError = 7
```

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /LoginService_AuthenticateRaw	

ورودی‌ها
AuthRequest<byte[]>
{
Random,
CmsSignature,
LoginProfile
}
	Byte[] random	رشته تصادفی ارسال شده سمت کاربر در قالب Base64

	Byte[] cmsSignature	امضای دریافت شده از سمت کاربر
	string loginProfile	نام تنظیمات پیکربندی کلاس Login در فایل pktb.xml
خروجی	AuthResponse<byte[]>	مقدار داده شمارشی مشخص کننده نتیجه تصدیق هویت کاربر

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /LoginService_Authenticate	

ورودی‌ها
AuthRequest<string>
{
Random,
CmsSignature,
LoginProfile
}
	string random	رشته تصادفی ارسال شده سمت کاربر در قالب Base64

	string cmsSignature	امضای دریافت شده از سمت کاربر
	string loginProfile	نام تنظیمات پیکربندی کلاس Login در فایل pktb.xml
خروجی	AuthResponse<string>	مقدار داده شمارشی مشخص‌کننده نتیجه تصدیق هویت کاربر

سرویس ارتباط با مخزن یا دایرکتوری کلید عمومی[1]

در PKDService توابعی به منظور دسته‌بندی توابع موردنیاز جهت برقراری ارتباط با دایرکتوری کلید عمومی قرار داده شده است. توابع موجود در این سرویس، توابع مورد نیاز جهت دریافت گواهی خاص از دایرکتوری کلید عمومی و یا

[1] PKDSrvice

قراردهی گواهینامه بر روی این دایرکتوری را ارائه می‌دهند.

دریافت گواهینامه از مخزن

این تابع به منظور دریافت گواهی خاص از دایرکتوری کلید عمومی مورد استفاده قرار می‌گیرد. جزئیات تابع ارائه‌دهنده این خدمت در کلاس PKDService به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /PKDService_DownloadCertificate	

ورودی‌ها
PKDClientRequest
{
Path,
PkdProfile
}
	`string` path	مقدار SubjectDN گواهینامه‌ی مورد درخواست

	`string` pkdProfile	نام پروفایل مورد استفاده
خروجی	`IEnumerable<byte[]>`	آرایه‌ای از گواهی‌های دریافت‌شده از دایرکتوری کلید عمومی

نام تابع	/api/client/apim/v1/mohmeservices/gwDss /PKDService_DownloadCertificateAsBase64	

ورودی‌ها
PKDClientRequest
{
Path,
PkdProfile
}
	`string` path	مقدار SubjectDN گواهینامه‌ی مورد درخواست

	`string` pkdProfile	نام پروفایل مورد استفاده
خروجی	`IEnumerable<string>`	آرایه‌ای از گواهی‌های دریافت‌شده از دایرکتوری کلید عمومی در قالب base64

دریافت CRL از مخزن

این تابع به منظور دریافت CRL یا Certificate Revocation List از دایرکتوری کلید عمومی مورد استفاده قرار می‌گیرد. جزئیات تابع ارائه‌دهنده‌ی این خدمت در کلاس PKDService به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/PKDService_DownloadCRL	

ورودی‌ها
PKDClientRequest
{
Path,
PkdProfile
}
	`string` path	مقدار SubjectDN گواهینامه‌ی crl مورد درخواست

	`string` pkdProfile	نام پروفایل مورداستفاده
خروجی	`byte[]`	آرایه‌ی فایل CRL دریافت شده از مخزن PKD

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/PKDService_DownloadCRLAsBase64	

ورودی‌ها
PKDClientRequest
{
Path,
PkdProfile
}
	string path	مقدار SubjectDN گواهینامه‌ی crl مورد درخواست

	string pkdProfile	نام پروفایل مورداستفاده
خروجی	string	رشته Base64 فایل CRL دریافت شده از مخزن PKD

دریافت لیست دایرکتوری

این تابع به منظور دریافت لیست دایرکتوری‌های موجود در یک مسیر LDAP پیاده‌سازی شده است. جزئیات تابع ارائه‌دهنده‌ی این خدمت به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/PKDService_SubDirectoryList	

ورودی‌ها
PKDClientRequest
{
Path,
PkdProfile
}
	string rootDirectoryPath	مقدار SubjectDN گواهینامه‌ی مورد درخواست

	string pkdProfile	نام پروفایل مورداستفاده
خروجی	String[]	آرایه ای از مسیر های موجود در دایرکتوری آرایه ای از مسیر های موجود در دایرکتوری

دریافت فایل تنظیمات

جزئیات تابع ارائه‌دهنده‌ی این خدمت به صورت زیر است:

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/PKDService_CurrentConfig	
ورودی‌ها	ندارد	
خروجی	Configuration	فایل تنظیمات در قالب Tag base configuration

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/PKDService_CurrentConfigAsXML	
ورودی‌ها	ندارد	
خروجی	string	رشته فایل تنظیمات در قالب XML

سرویس دریافت نسخه[1]

دریافت نسخه

جزئیات تابع ارائه‌دهنده‌ی این خدمت به صورت زیر است:

این تابع به صورت Get عمل کرده و روی مرورگر هم قابل اجراست.

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/ApiVersion_GetVersion	
ورودی‌ها	ندارد	
خروجی	string	رشته حاوی نسخه‌ی اپلیکیشن

این تابع به صورت Post عمل می‌کند.

نام تابع	/api/client/apim/v1/mohmeservices/gwDss/ApiVersion_Version	
ورودی‌ها	ندارد	
خروجی	string	رشته حاوی نسخه‌ی اپلیکیشن

[1] ApiVersion

پیوست‌ها

پیوست ۱- ساختار خروجی فراخوانی توابع دیتاس

فراخوانی هر یک از توابع دیتاس (به استثناء توابع دریافت و بروزرسانی توکن دیتاس)، منجر به دریافت خروجی با قالب زیر می‌شود:

```
{
    "result": {
        "data": {obj},
        "status": {
            "statusCode": XXX
        }
    },
    "status": {
        "statusCode": XXX,
        "message": "message"
    }
}
```

جدول ۸- ساختار خروجی Body توابع دیتاس

ردیف	نام پارامتر	نوع داده	توضیحات
۱	result.data	Object	پارامتر(های) خروجی تابع فراخوانی شده (به توضیحات مربوط به هر تابع در متن سند مراجعه نمایید.)
۲	result.status.statusCode	Integer	کد وضعیت پاسخ مربوط به سرویس‌دهنده
۳	status	Object	وضعیت پاسخ دیتاس نسبت به فراخوانی تابع، شامل کد وضعیت (statusCode) و پیام (message) مطابق جدول ۹

پیوست ۲- کدهای وضعیت پاسخ دیتاس نسبت به فراخوانی توابع

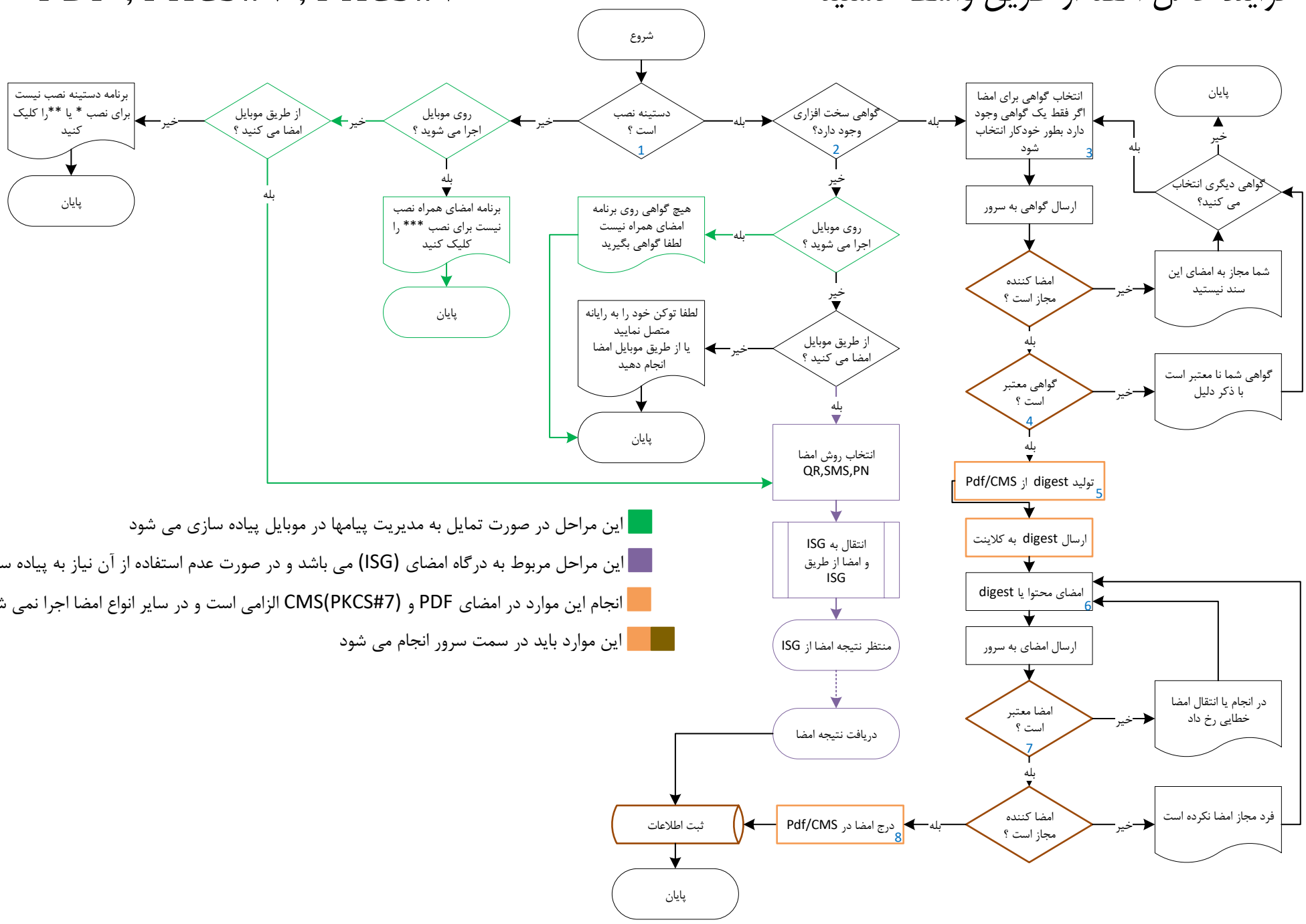
در جدول زیر فهرست کدهای وضعیت پاسخ دیتاس نسبت به فراخوانی توابع، متن پیام و توضیحات مربوطه آمده است.

جدول ۹- کدهای وضعیت پاسخ دیتاس نسبت به فراخوانی توابع

ردیف	کد وضعیت	پیام	توضیحات
۱	۲۰۰	OK!	عملیات با موفقیت انجام شد.
۲	۲۰۲	Accepted!	درخواست شما دریافت شد.
۳	۴۰۰	Bad request.	خطایی در داده‌های ورودی وجود دارد.
۴	۴۰۱	Credential is not valid!	نام‌کاربری و یا کلمه‌عبور نادرست است.
۵	۴۰۳	Your origin IP is permanently blocked!	آی پی شما قبلا اعلام نشده و مجاز به اتصال نیست.
۶	۴۰۴	Not Found!	پاسخی برای درخواست مورد نظر یافت نشد.
۷	۴۱۰	All resources are moved permanently to the HTTP secure protocol(HTTPS)!	برای دسترسی به خدمات از HTTPS استفاده نمایید.
۸	۴۲۹	Too many requests or Access denied!	درخواست‌ها بیش‌از حد مجاز است / مجوز استفاده از سرویس صادر نشده است
۹	۴۹۹	Client Closed Request!	در هنگام پردازش، کاربر ارتباط را قطع کرده است.
۱۰	۵۰۰	Internal server error!	بروز خطا در انجام عملیات توسط سرور.
۱۱	۵۰۳	Service provider error!	بروز خطا در انجام عملیات توسط فراهم‌کننده سرویس.
۱۲	۵۰۴	Backend timeout!	سرویس‌دهنده پاسخ‌گو نیست.
۱۳	۵۲۰	Unknown error!	خطای نامشخص.

فرایند کامل امضا از طریق واسطه دستینه

PDF , PKCS#۱ , PKCS#۷



این مراحل در صورت تمایل به مدیریت پیامها در موبایل پیاده سازی می شود

این مراحل مربوط به درگاه امضای (ISG) می باشد و در صورت عدم استفاده از آن نیاز به پیاده سازی ندارد

انجام این موارد در امضای PDF و CMS(PKCS#7) الزامی است و در سایر انواع امضا اجرا نمی شود

این موارد باید در سمت سرور انجام می شود

*نصب نرم افزار دستینه نسخه ویندوز
https://healthca.behdasht.gov.ir/uploads/502/softwares/
DastineInstaller.msi

**نصب نرم افزار دستینه نسخه موبایل
https://healthca.behdasht.gov.ir/uploads/502/
softwares/mkeyone.apk

***نصب نرم افزار امضای همراه
https://healthca.behdasht.gov.ir/uploads/502/
softwares/Behdasht-2.5.0-40.apk

****فایلهای جاوااسکریپت دستینه: بخشهای ۱ و ۲ و ۳ و ۶
https://healthca.behdasht.gov.ir//uploads/502/
softwares/DastineSample.rar

Functions name in /api/client/apim/v1//mohmeservices/gwDss

1- Dastine.IsInstalled ****
2- Dastine.FindCertificate ****
3- Dastine.SelectCertificateFromTokenByUI ****
4,1-VAService_ValidateCertificateEntirelyEx
4,2-VAService_ValidateCertificateEntirelyExRaw
5.1- CryptoService_PDFDigestForMultiSign
5,2- CryptoService_PDFDigestForMultiSignRaw
5.3- CryptoService_CmsDigest
5,4 CryptoService_CmsDigestRaw
6- Dastine.Sign ****
7.1- CryptoService_PDFVerify
7,2- CryptoService_PDFVerifyRaw
7.2- CryptoService_CmsVerify
7,3- CryptoService_CmsVerifyRaw
7.3- CryptoService_Verify
7,4- CryptoService_VerifyRaw
8.1- CryptoService_PutPDFSignatureForMultiSign
8,2- CryptoService_PutPDFSignatureForMultiSignRaw
8,3- CryptoService_PutCmsSignature
8.4- CryptoService_PutCmsSignatureRaw