

لوات

هوشمندی در مسیر مشتری

هویت دیجیتال

بر پایه هوش مصنوعی (AI)

API & SDK



هویت دیجیتال، کلید ورود به آینده

هویت دیجیتال یک نمایش دیجیتال از یک موجودیت است که از جزئیات کافی برای تمایز کردن آن موجودیت در یک بافتار دیجیتال برخوردار است. Digital Identity به عنوان مجموع خصیصه‌های موجودیت در قلمرو دیجیتال، به اندازه مفهوم هویت در دنیای فیزیکی حائز اهمیت است؛ چرا که علاوه بر حفظ ویژگی‌های ذاتی که هویت را به یک عامل تعیین‌کننده تبدیل می‌کند، به طور همزمان، این نوع هویت به عنوان یک عامل توانمندساز برای دولتها در دستیابی به شمول اجتماعی، تحول دیجیتال، بهبود کیفیت سرویس‌ها و غیره عمل می‌کند.

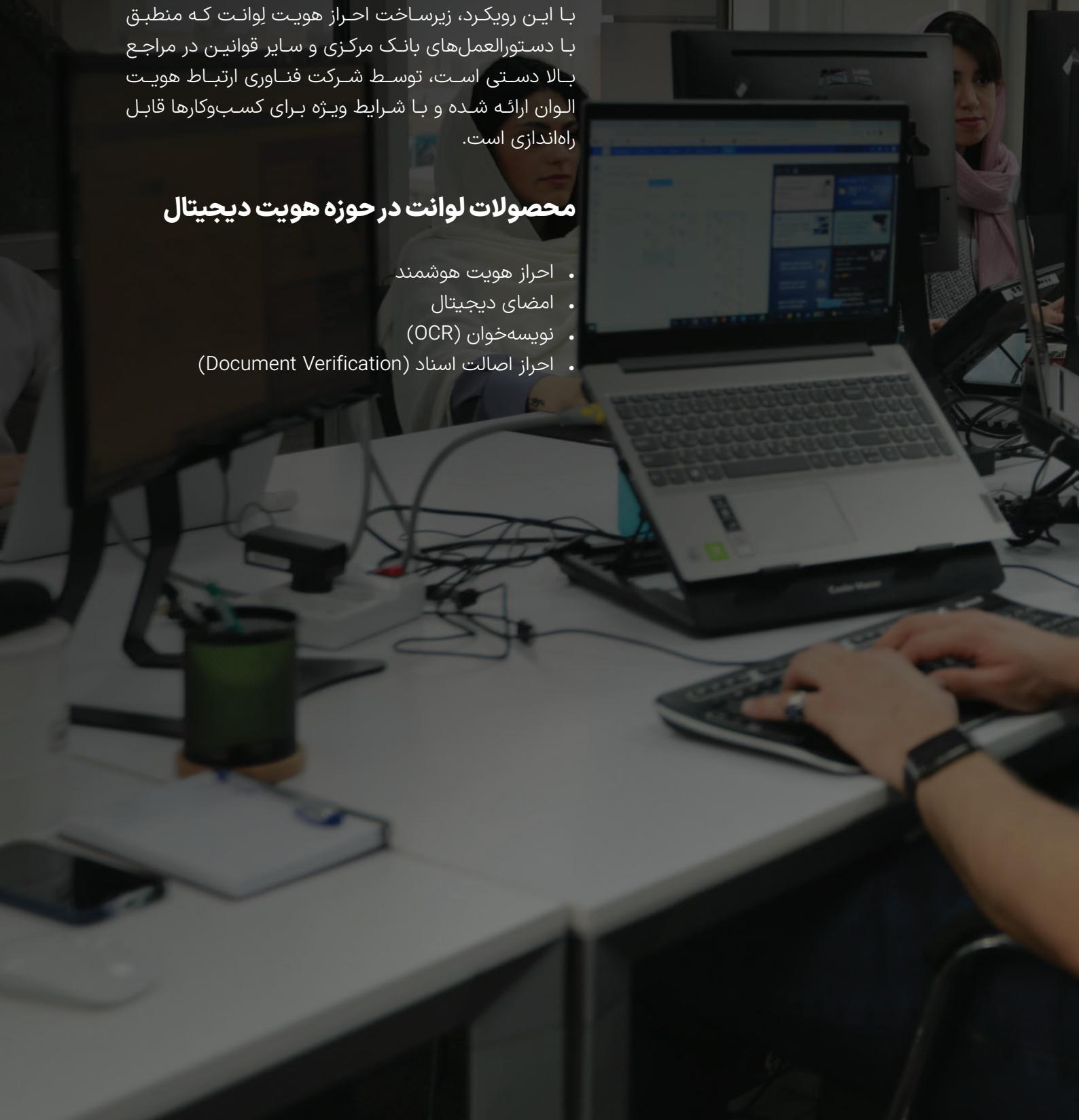
رویکرد لوانت

شرکت فناوری ارتباط هویت الوان با بهره‌مندی از کارشناسان مهندسی توسعه زیرساخت‌های مقیاس بزرگ نرم‌افزاری، و همچنین متخصصان زبان مالی، در تلاش است تا به عنوان یک سرویس دهنده و شریک تجاری در کنار سازمان‌هایی که علاقمندند به سرعت وارد بازارهای جدید مالی شوند، ایفای نقش کند.

با این رویکرد، زیرساخت احراز هویت لوانت که منطبق با دستورالعمل‌های بانک مرکزی و سایر قوانین در مراجع بالا دستی است، توسط شرکت فناوری ارتباط هویت الوان ارائه شده و با شرایط ویژه برای کسب‌وکارها قابل راه‌اندازی است.

محصولات لوانت در حوزه هویت دیجیتال

- احراز هویت هوشمند
- امضای دیجیتال
- نویسه‌خوان (OCR)
- احراز اصالت اسناد (Document Verification)





سرویس‌های احراز هویت لوانت

ارائه خدمات از طریق اینترنت، روز به روز بیشتر از گذشته می‌شود و کاربران، روز به روز با انواع روش‌های Fraud یا کلاهبرداری در فضای مجازی آشنا می‌شوند. رشد روزافزون مشتریان آنلاین، سرمایه‌گذاران و صاحبان کسب و کار را برای ادامه دادن مصمم‌تر از قبل کرده، اما در عین حال، از چالش‌های امنیتی نیز نمی‌توان به سادگی عبور کرد. مجموعه لوانت با تجربه مناسب و طولانی در زمینه احراز هویت به صورت هوشمند و در قالب اتوماسیون، ۶ راه حل اصلی خود در این زمینه را به صورت عمومی منتشر کرده و شرکتها می‌توانند با بهره‌برداری از آن‌ها، فرایندهای احراز هویت مشتریان خود را به سادگی انجام دهند.



احراز هویت با اطلاعات بانکی و تلفن همراه



احراز هویت با عکس سلفی



احراز هویت ویدیویی



دریافت اطلاعات بانک



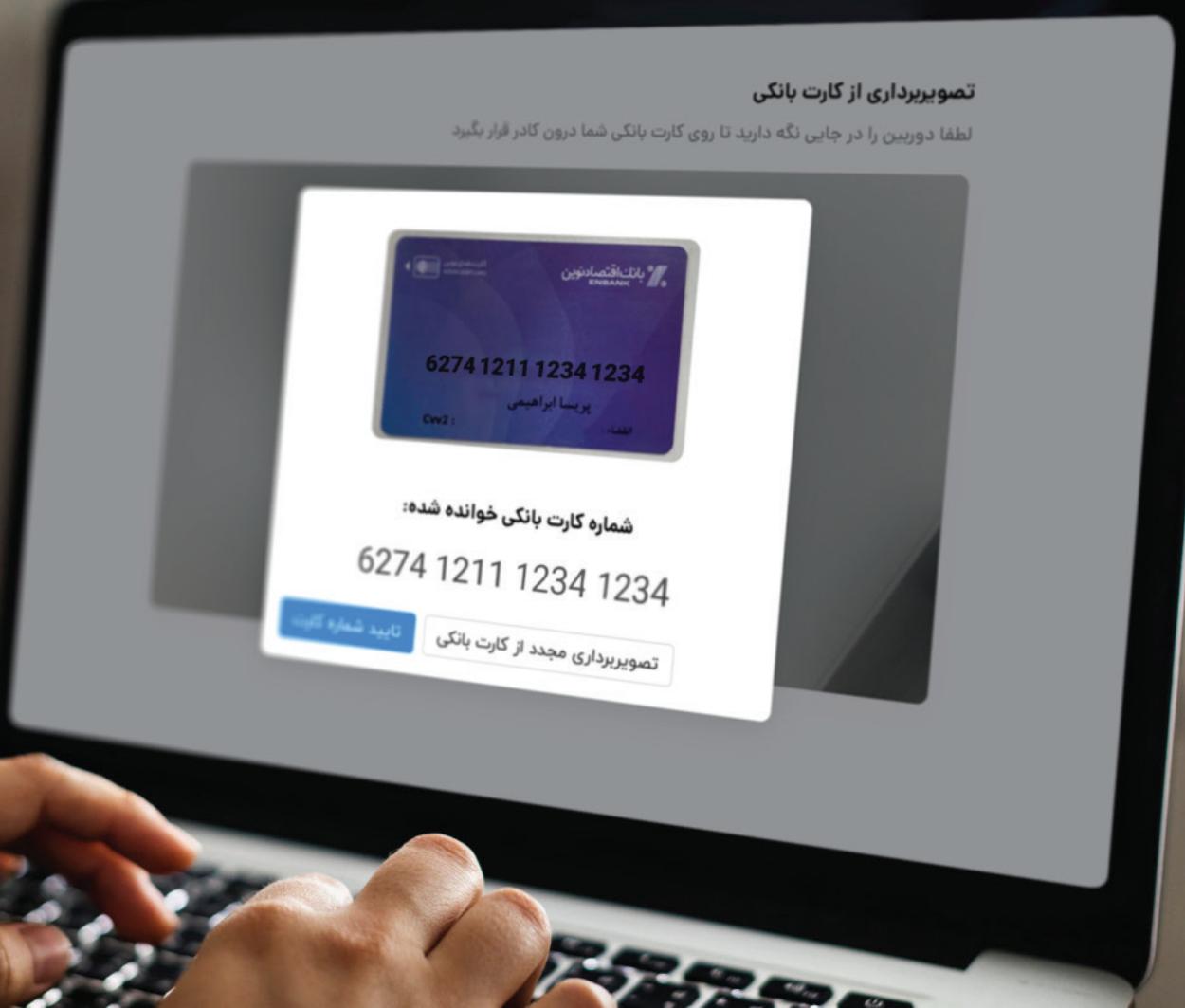
احراز هویت با کارت بانکی



احراز هویت با کارت ملی

تصویربرداری از کارت بانکی

لطفاً دوربین را در جایی نگه دارید تا روی کارت بانکی شما درون گادر قرار بگیرد



سرویس‌های هوش مصنوعی لوانت

با گسترش محصولات دیجیتال و شکل‌گیری روزافزون کسب‌وکارهای فناوری محور، امنیت و سرعت، بیش از بیش نقش کلیدی پیدا کرده‌اند؛ به گونه‌ای که اگر کسب‌وکاری به آن توجه نکند، به سادگی از چرخه رقابت خارج می‌شود. کسب‌وکارهایی که در شروع، مشکلات متاثر از حضور در بازارهای بزرگ را پیش‌بینی کرده و برای آن‌ها راه حل داشته باشند، در زمان‌هایی که در رقابت پیروز شده و سهم بازار خود را چند برابر کنند. احراز هویت مشتریان به صورت آنلاین و هوشمند در کنار خوانش مدارک و مستندات، قابلیت‌هایی هستند که «امنیت و سرعت» را به عنوان مزیت رقابتی استراتژیک برای کسب‌وکار فراهم می‌کنند.

مجموعه لوانت، برخی از سرویس‌های مبتنی بر هوش مصنوعی خود را با موضوع «احراز هویت آنلاین» و «خوانش متنون از تصاویر (OCR)» که می‌توانند در محصولات دیجیتال سایر شرکت‌ها مورد بهره‌برداری قرار بگیرند، با شرایط بسیار مناسب در اختیار کسب و کارهای متقاضی قرار می‌دهد.



تطبیق دو چهره



خوانش متن کارت ملی (OCR)



خوانش متن کارت بانکی (OCR)



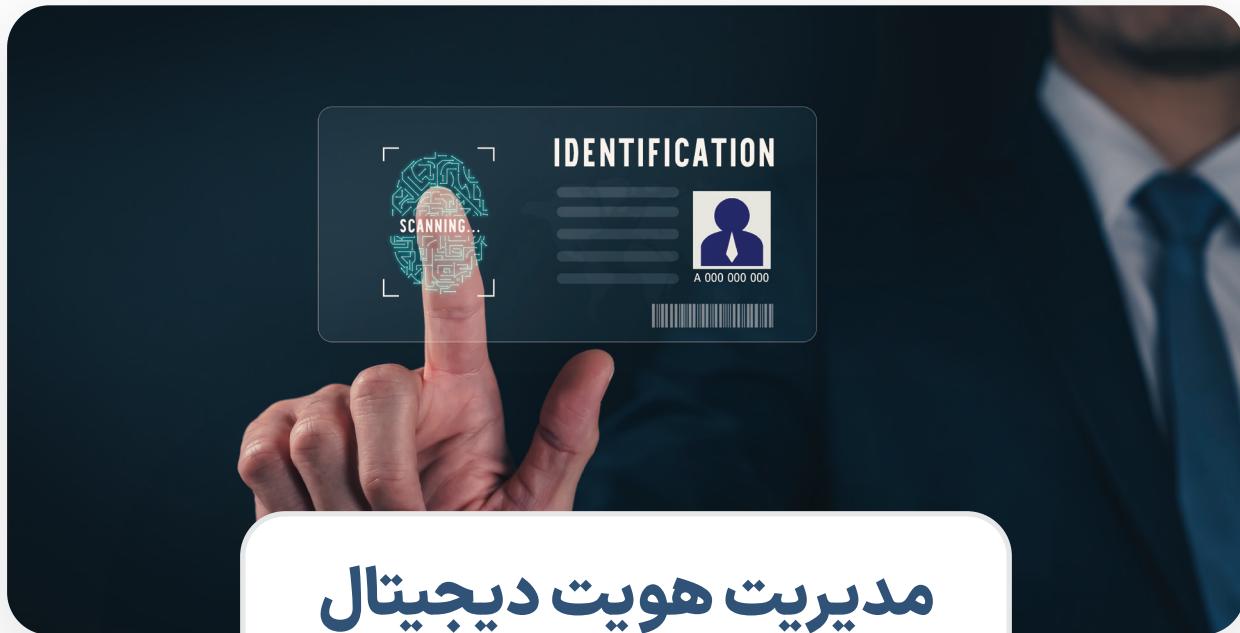
خوانش چک صیاد (OCR)



خوانش شناسنامه فرمات جدید (OCR)



بررسی زنده بودن (Liveness)



مدیریت هویت دیجیتال

بستر شکل‌گیری اعتماد دیجیتال

شتاب روزافزون تحولات دیجیتال در فضای سایبری و نقش آن در زندگی افراد، جذابیت‌های فراوانی را به همراه دارد. کاربردها و تأثیرات شگرف این تحولات، موجب سهولت و راحتی در زندگی افراد می‌شود و همین امر در چرخه‌ای که یک سوی آن نیازهای بشری و سوی دیگر آن پیشرفتهای تکنولوژیک قرار دارد، بهنوعی زمینه‌ساز توسعه فناوری‌ها و تقویت‌کننده نوآوری است.

اما این تحولات، روی دیگری نیز دارند و آن، سختتر شدن جلب اعتماد یا اعتمادسازی در فضای سایبریست. در حقیقت، در فضای سایبری به دلیل گستردگی، پیچیدگی و تنوع تحولات، جلب اعتماد و ایجاد اطمینان میان موجودیت‌ها از ابعاد گوناگون، بسیار دشوار شده است. بدون شک آرمان شهر یا مدینه فاضله در فضای سایبر، در بستر حفظ کارکردهای آن همراه با امنیت همه‌جانبه تحقق می‌یابد و این مهم صورت نمی‌پذیرد مگر زمانی که اعتماد میان بازیگران این اکوسیستم عظیم حاکم باشد. بهنحوی که کلیه تعاملات و تراکنش‌های میان افراد حقیقی، حقوقی، اشیاء و نظایر آن، به راحتی و با حداقل ریسک انجام شود.

یکی از مهمترین کارکردهای مدیریت هویت دیجیتال، ایجاد اعتماد دیجیتال در فضای سایبر است. درواقع پایه و اساس مدیریت هویت دیجیتال، ایجاد اعتماد است. به همین دلیل است که رویکرد بسیاری از کشورها و پروژه‌های ملی در حوزه هویت دیجیتال، «ایجاد هویت قابل اعتماد است»؛ هویتی که مبنای ایجاد اعتماد در فضای سایبری است؛ بنابراین شاید بتوان گفت مدیریت هویت دیجیتال کلید دستیابی به اعتماد دیجیتال است. طبیعتاً تحقق امنیت سایبری نیز در گرو ایجاد اعتماد دیجیتال است. اعتمادسازی در فضای سایبری، شئون و ابعاد متعددی را در بر می‌گیرد. سه بُعد مهم آگاهی از بافتار، مدیریت ریسک و تحولات فناوری به عنوان مهمترین چالش‌های اعتمادسازی و مدیریت هویت دیجیتال شناخته می‌شوند.





فرآیند و مزیت‌های استفاده از هویت دیجیتال

سطح متفاوتی از احراز هویت در سازمان‌ها وجود دارد و خدمات سازمان‌ها بر همین اساس به مشتریان ارائه می‌شود. رایج‌ترین مدل سطح‌بندی احراز هویت شامل ۴ سطح «موجودیت گمنام»، «دارای اسم مستعار در یک یا چند وبسایت»، «تأیید هویت به صورت خوداظهاری یا به کمک اعضای شبکه»، «تأیید هویت شده به کمک هویت رسمی» است. در سرویس‌های احراز هویت لوانت ابزارهای متنوعی برای انجام کامل‌ترین سطح احراز هویت با کمک هویت رسمی در اختیار سازمان‌ها قرار داده‌ایم. سرویس‌هایی که می‌توانند از طریق اطلاعات ثبت‌شده افراد در سازمان ثبت‌احوال و تطبیق آن با اطلاعات دریافتی از مدارک، چهره و ویدئوی کاربر هویت وی را تصدیق کنند. علاوه بر این با استفاده از سرویس استعلام مالکیت تلفن همراه، می‌توان مالکیت خط تلفنی که سیستم از طریق آن با کاربر در ارتباط است را بررسی کرد.

پارامترهای مورد بررسی در فرآیند احراز هویت هوشمند لوانت

۱. مدارک آپلود شده
۲. تطبیق با ثبت‌احوال
۳. عکس سلفی
۴. بررسی زنده بودن ویدیوی سلفی (Liveness)
۵. بررسی آگاهی شخص در ویدیو (Awareness)
۶. استعلام مالکیت تلفن همراه

مزایای سمت کاربران

- افزایش اعتماد کاربران و جلوگیری از آسیب‌هایی مانند فیشینگ
- دسترسی به سیستم واحد احراز هویت برای دریافت بسیاری از خدمات
- راحتی احراز هویت و ارائه اطلاعات شناسایی به سازمان‌های مختلف
- امکان استفاده از شناسه واحد برای ورود به درگاه‌های مختلف
- از میان رفتن خطر گم شدن استناد کاغذی
- امکان کنترل هویت و اطلاعات کاربران توسط خود ایشان
- فرآگیری امضای دیجیتال و سهولت در امضا و پیگیری هویت امضا کنندگان استناد و قراردادها
- امکان افتتاح حساب و استفاده از خدمات بانکی به صورت غیر حضوری

مزایای سمت سازمان‌ها

- عدم فراموشی مشخصات ورود و احراز هویت و افزایش نرخ بازگشت کاربران
- کاهش هزینه‌های عملیاتی
- کاهش هزینه‌های مدیریت کاربران
- عدم نیاز به نگهداری استناد و مدارک کاغذی کاربران
- امکان تعامل و ارائه خدمات دیجیتال گستردگرتر به کاربران
- کاهش امکان جعل استناد و بهبود سطح اعتماد به اطلاعات دریافت شده از کاربر
- سهولت در دریافت و بهروزرسانی اطلاعات کاربران از قبیل آدرس و شماره تلفن
- افزایش موققیت و نطابق کاربران



قابلیت‌های احراز هویت هوشمند لوانت

با توجه به احراز هویت تمامی کاربران، ارائه خدمات مشخص در قالب نرم‌افزارها یا وبسایت‌های تأییدشده و همچنین استفاده از پروتکل‌های امن انتقال داده، کاربران می‌توانند با اطمینان خاطر از خدمات آنلاین تحت سیستم‌های احراز هویت و امضای دیجیتال لوانت استفاده کرده و تا حد زیادی از آسیب‌های احتمالی خدمات آنلاین از قبیل فیشینگ، در امان باشند.

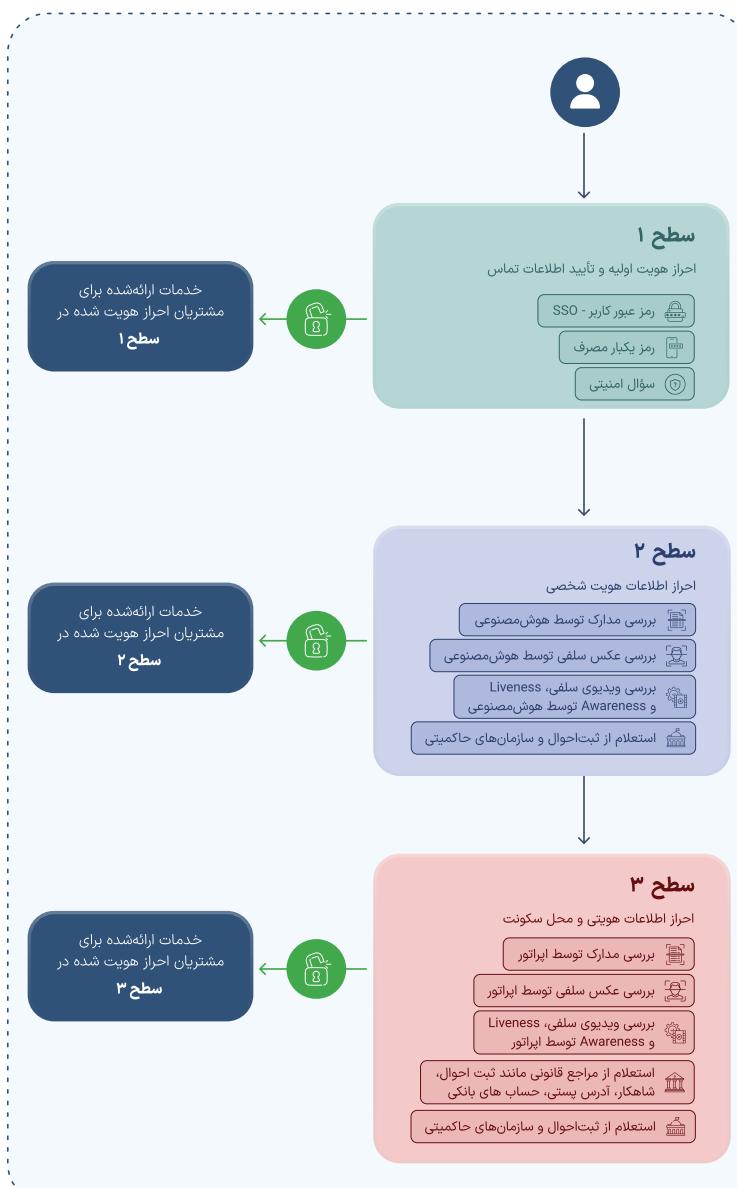
طی روند احراز هویت، قوانین، استانداردها و دستورالعمل‌های قانونی و حقوقی لحاظ شده و سوابق افراد به تناسب فعالیت‌های درخواستشده ایشان بررسی می‌گردد. این امر، توانایی پیشگیری از مواردی مانند پولشویی و جعل اسناد را به شدت تقویت کرده و به سازمان‌های استفاده کننده از سیستم‌های احراز هویت، امکان می‌دهد تا با اطمینان بیشتری به کاربران و مشتریان خود خدمات ارائه کنند.

موارد جرائم سایبری در سال‌های اخیر افزایش یافته است. سرقت اطلاعات هویتی اغلب در ارتباط با شرکت‌های بزرگ بین‌المللی مانند فیسبوک و اینستاگرام شنیده می‌شود. در نتیجه‌ی این روند، کسب‌وکارهای مختلف به یک سیستم امنیتی نیاز دارند که بتوانند به طور مؤثر از داده‌های هویتی مشتریان خود محافظت کنند. اینجاست که نقش فناوری‌های احراز هویت از جمله تشخیص زنده بودن ظاهر می‌شود. جعل هویت با استفاده از عکس‌ها، ویدئوها یا ماسک‌ها توسط هکرهایی انجام می‌شود که دائمًا به دنبال راههایی برای دسترسی به هویت افراد و درنتیجه کلاهبرداری و اخاذی از افراد مختلف هستند. از این جهت با توجه به دقیق و توان پاسخگویی سرویس احراز هویت هوشمند لوانت نسبت به سایر رقبا، در رتبه بالاتری قرار می‌گیرد. سرویس لوانت Print Attack، Replay Attack، و ... را تشخیص دهد.

متصل به سرویس‌های هوشمند اطلاعات			پشتیبانی از سرویس‌های هوشمند اطلاعات		
ثبت شرکت‌ها	اطلاعات بانکی	کدپستی و آدرس			
سجام و اطلاعات بورسی	شهرکار	ثبت احوال	تشخیص حالات چهره	تشخیص حرکات دست و سر	تشخیص و تطبیق چهره
پشتیبانی از OTP و 2FA به منظور ارتقاء امنیت کاربران					
پشتیبانی از امضا دیجیتال جهت انعقاد قراردادها و توافق‌ها به صورت آنلاین			Anti-Spoofing Liveness و تشخیص		
قابلیت تعریف فیلدهای سفارشی در پروفایل مشتریان					
پشتیبانی از OAuth و LDAP			امکان استخراج اطلاعات از تصویر مدارک (OCR)		

امکان سطح‌بندی مراحل احراز هویت براساس نیازهای سازمان

یکی از چالش‌های اساسی سازمان‌ها در خصوص امنیت اطلاعات، موضوع کنترل و مدیریت دسترسی (Access Control) به اطلاعات است. مدیران سازمانی همواره با این چالش مواجه‌اند که در چه سطحی باید به کاربران داخلی و یا نهادهای بیرونی دسترسی اعطای شود و چه اصولی برای آن باید رعایت شود. از یک سو باید حداقل دسترسی را به موجودیت‌های مختلف اعطا نمود و از سوی دیگر باید کاربران و نهادهای مختلف تا حدی دسترسی داشته باشند تا بتوانند نیازمندی و فعالیت‌های مورد انتظار خود را اجرا نمایند. سرویس‌های لوانت، از یک مازول جامع جهت مدیریت دسترسی کاربران به بخش‌های مختلف سیستم بهره می‌برند. با استفاده از این مازول می‌توان دسترسی به کلیه قسمت‌های سیستم را کنترل کرد. دسترسی به زیرسیستم‌ها، صفحات، حتی بخش‌هایی از صفحات یا ذکمه‌ها و یا جزیئرین بخش‌های سیستم از طریق مازول مدیریت سطح دسترسی قابل کنترل و مدیریت هستند. مازول مدیریت سطوح دسترسی در سرویس‌های لوانت، قابلیت‌هایی مانند ایجاد و حذف حساب کاربری، فرآیند اعطای دسترسی به کاربر، مدیریت اعطاء دسترسی سطح بالا (مدیران، راهبران و ...)، مدیریت اطلاعات احراز هویت کاربر، بازنگری حقوق دسترسی اعطاء شده و در نهایت حذف یا تغییر دسترسی موجود را در اختیار مدیر سیستم قرار می‌دهند.



هویت‌های تأیید شده

در حالت کلی می‌توان هویت دیجیتال را در دو دسته تأیید شده و تأیید نشده قرار دارد. هویت‌های دیجیتال تأیید شده فقط یکبار ایجاد شده و شامل تأیید (تصدیق) [اثبات اینکه هر فرد همان کسی است که ادعا می‌کند] از استناد رسمی هویتی مانند پاسپورت، گواهی‌نامه رانندگی، گواهی تولد و اسکن ویژگی‌های بیومتریک هستند. این دسته مورد اعتمادترین نوع هویت‌های دیجیتال بوده و می‌توانند برای دسترسی به طیف وسیعی از سرویس‌ها مورد استفاده قرار گیرند.

هویت تأیید نشده

هویت‌های دیجیتال تأیید نشده زمانی ایجاد می‌شوند که افراد با خصیصه‌های شخصی مانند نام، تاریخ تولد و دیگر جزییات شخصی در وب سایتی ثبت‌نام کنند. این وب‌سایتها معمولاً در گذر زمان یک پروفایل از سوابق کاربر ایجاد می‌کنند. این روش منجر به شکل‌گیری ردیاب آنلاین برای افراد می‌شود. ردیاب آنلاین در گذر زمان به ایجاد هویت آنلاین کاربران کمک می‌کند. هویت‌های دیجیتال تأیید نشده با ریسک بالای جعل، کلاهبرداری و سرقت روبه‌رو هستند. با توجه به مطالب ذکر شده می‌توان یک گستره برای تأیید هویت در نظر گرفت که از هویت بنام یا گمنام شروع شده و به هویت تأیید شده با بهره‌گیری از هویت رسمی ختم می‌شود.



احراز هویت هوشمند اشخاص حقوقی

اگر فرایند شناسایی و تأیید هویت صاحب یک کسبوکار، بررسی ساختار مالکیت و استناد و در نهایت شناسایی و تأیید هویت ذینفعان آن با روش‌های سنتی انجام شود، مستلزم صرف زمان و هزینه بالا است. به همین دلیل، شرکت‌هایی که می‌خواهند از مقررات AML پیروی کنند و در کنار آن از کسبوکار خود نیز محافظت کنند، از فرایند تأیید هویت الکترونیکی (eIDV) برای خودکار کردن احراز هویت استفاده می‌کنند. لوانت با زیرساخت‌های احراز هویت الکترونیکی، دسترسی آسان به انطباق با مقررات KYB را فراهم می‌کند.

پارامترهای مورد بررسی در فرایند احراز هویت هوشمند اشخاص حقوقی

استفاده از استعلام‌های دولتی، سوابق شرکت‌ها، دسترسی به پایگاه‌دادهای مختلف برای تجزیه و تحلیل ذینفعان نهایی و سهامداران استفاده می‌شود. علاوه بر این، نظارت مستمر و کنترل‌های خودکار تضمین می‌کند که کسبوکارها، سازگار با مقررات جلوگیری از پولشویی و تأمین مالی تروریسم هستند. در رویه‌های خودکار KYB، شرکت‌ها می‌توانند داده‌های رسمی ثبت تجاری را با استفاده از API، دریافت کرده و هویت کسبوکار متقاضی همکاری را تأیید کنند. همراه با شناسه ملی، سرویس دیجیتال KYB می‌تواند اطلاعات مهمی را در مورد هر کسبوکار جمع‌آوری کند.

شرکت‌ها فرایندهای KYB را توسعه می‌دهند تا با قوانینی مانند مقررات مبارزه با پولشویی (AML) و تأمین مالی تروریسم (CFT) مطابقت داشته باشند. رویه‌های KYC/KYB برای جلوگیری از جرایم احتمالی پولشویی شرکت‌ها یا خطر فعالیت‌های تروریستی انجام می‌شود و در نتیجه با مقررات بین‌المللی AML مطابقت دارد. مقررات KYB در جایی اعمال می‌شود که شرکت‌ها با هم تجارت می‌کنند و در تماس هستند و برای تحقق آن نیاز به جمع‌آوری و تجزیه و تحلیل داده‌های سایر شرکت‌ها وجود دارد:

۴. هویت مدیران و مالکان

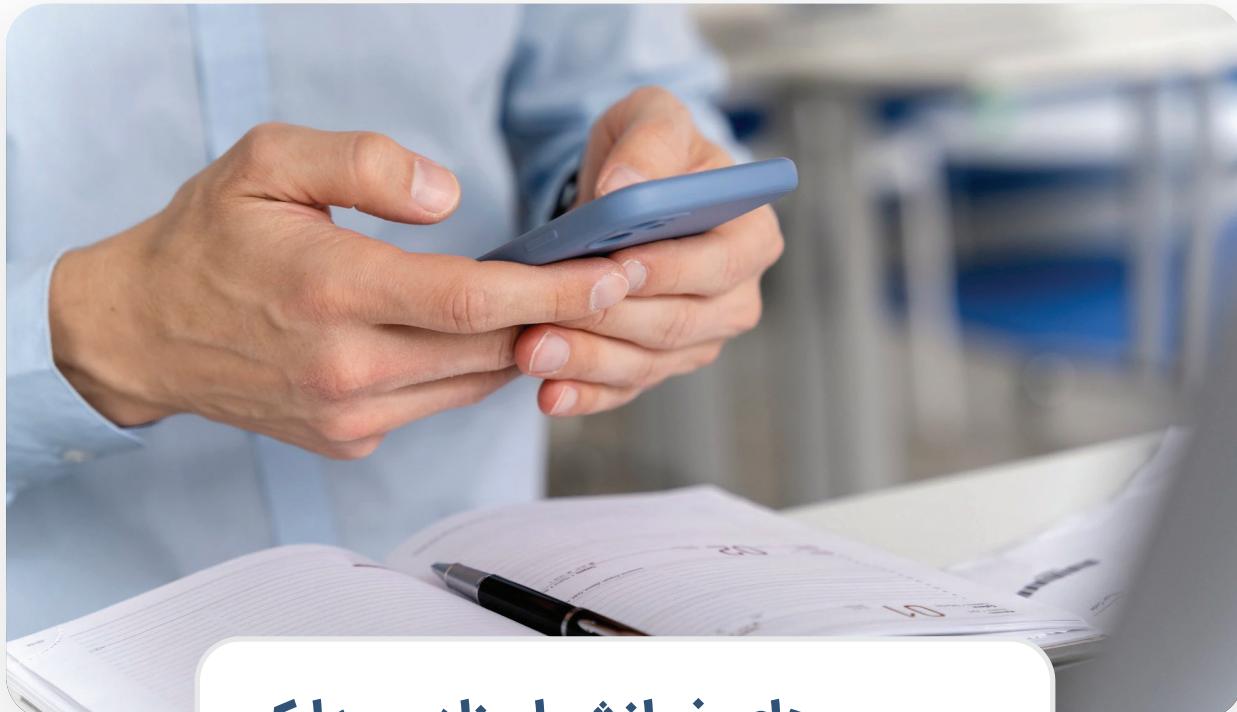
۳. استناد و مجوزها

۲. آدرس شرکت

۱. مدارک ثبتی

مؤسسات نیازمند KYB

همه مؤسسات مالی که انتقال پول انجام می‌دهند، مانند بانک‌ها، باید فرایند KYB را برای مشتریان حقوقی خود طی کنند. علاوه بر این، شرکت‌ها باید اطلاعات تجاری و مالی مشتریان حقوقی خود را حتی در سطح بین‌المللی تجزیه و تحلیل و تأیید کنند. به این ترتیب شرکت‌ها در برابر تقلب در استناد از خود محافظت می‌کنند و امنیت معاملات را تضمین می‌کنند. علاوه بر این، رویه‌های KYB باید به طور کامل انجام شود تا با مقررات جاری پولشویی مطابقت داشته باشد. مؤسسات مالی که با مقررات AML مطابقت دارند در برابر جرمیه و آسیب رسیدن به برنده‌شان مصون هستند.



سرویس‌های خوانش اسناد و مدارک

بررسی اسناد و مدارک ارائه شده توسط کاربران، اعم از اسناد هویتی و یا مالی، بخش مهمی از فرآیند احراز هویت و اعتبارسنجی کاربران محسوب می‌شود. لوانت، با استفاده از مدل‌های هوش مصنوعی و پردازش تصویر، سرویس‌هایی را به صورت اختصاصی برای همین منظور ارائه کرده تا امکان اسکن، خوانش و استخراج اطلاعات دارای اهمیت را از اسناد ارائه شده توسط مشتری، در اختیار سازمان‌ها قرار دهد. سرویس‌های خوانش اسناد و مدارک لوانت، شامل موارد زیر می‌شوند:

خوانش متن کارت بانکی

اگر در سایت یا اپلیکیشن خود به سرویسی نیاز دارید که تصاویر کارت‌های بانکی را از کاربر دریافت و اطلاعات مندرج بر روی آن را استخراج نماید، این سرویس با پروفورمنس بالا و خطای بسیار ناچیز، یکی از بهترین راهکارها محسوب می‌شود. «سرویس خوانش متن کارت بانکی (OCR)» لوانت، با توانایی خواندن فونت‌های متعدد فارسی، به سادگی کلیه متن‌های مندرج بر روی کارت‌های بانکی را استخراج و به صورت Text ارائه می‌دهد.

خوانش متن کارت ملی

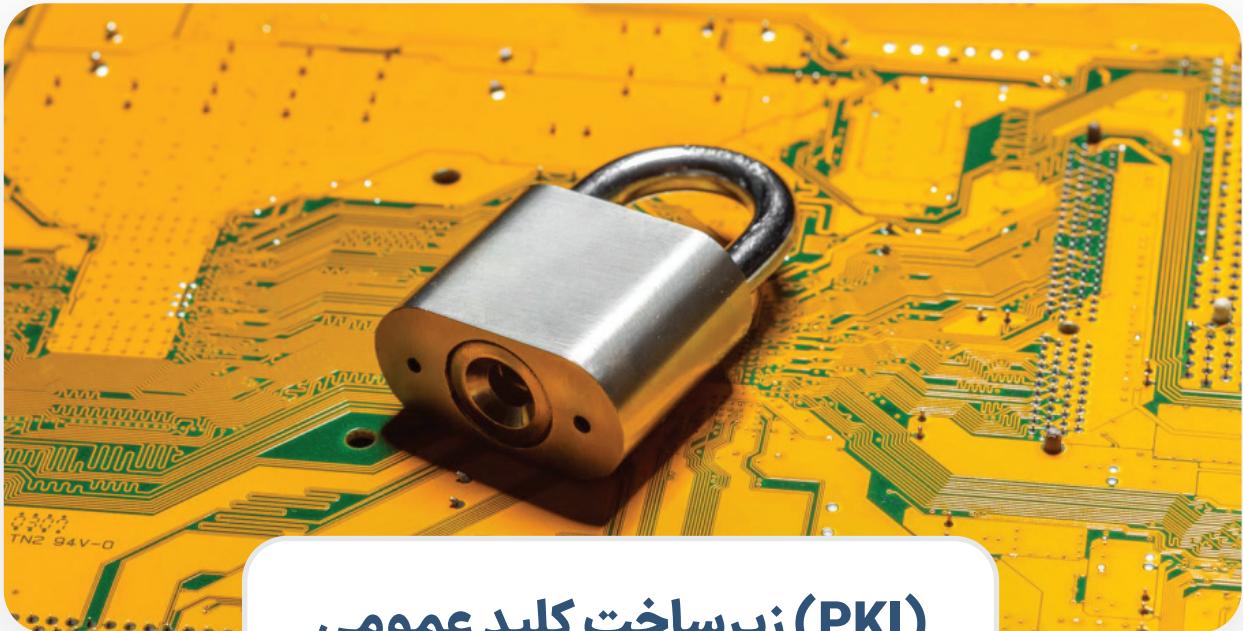
«سرویس خوانش متن کارت ملی (OCR)» لوانت، با استفاده از الگوهای پیشرفته هوش مصنوعی می‌تواند اطلاعات مندرج بر رو و یا پشت آن را به صورت Text استخراج نماید. این سرویس با پروفورمنس بالا و خطای بسیار پایین، قابلیت استخراج متون فارسی کارت ملی را هم دارد.

نویسه‌خوان چک صیاد

این سرویس، جهت خوانش اطلاعات درج شده بر روی چک صیادی طراحی شده است. در طراحی این سرویس از چندین مدل هوش مصنوعی استفاده شده است که ابتداء، به بررسی وجود یا عدم وجود چک صیادی در تصویر آپلود شده می‌پردازند. در صورت تشخیص وجود چک صیادی در تصویر، یک مدل هوش مصنوعی دیگر به استخراج اطلاعات موجود در چک پرداخته و این اطلاعات جهت خوانش هوشمند در اختیار یک مدل OCR قرار می‌گیرند.

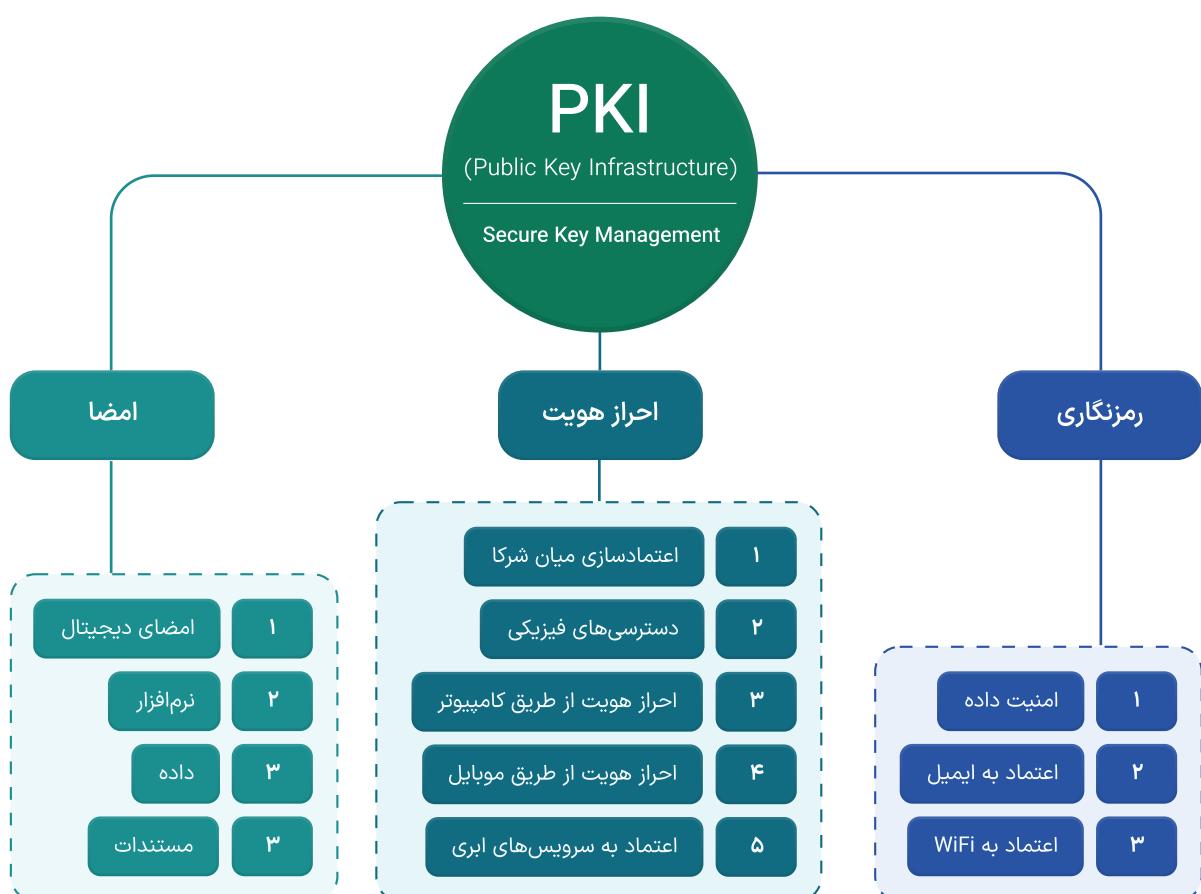
نویسه‌خوان شناسنامه فرمت جدید

این سرویس جهت خوانش اطلاعاتی نظری شماره ملی و تاریخ تولد در شناسنامه‌های با فرمت جدید طراحی شده است. تصویر مورد نظر خود را برای سرویس مذکور ارسال می‌کنید تا در مرحله اول، سیستم ارزیابی سند را انجام دهد. اگر تصویر ارسال شده، شناسنامه با فرمت جدید نباشد، سرویس پیام خطای ارسال می‌کند، اما در صورتی که تصویر شما یک شناسنامه با فرمت جدید باشد، اطلاعاتی نظری کد ملی و تاریخ تولد از آن استخراج شده و در پاسخ ارسال می‌شود.



زیرساخت کلید عمومی (PKI)

PKI یا زیرساخت کلید عمومی، یک ساختار رمزگاریست که شامل فرآیندها، استانداردها و فناوری‌های مورد نیاز برای صدور و مدیریت شناسه‌های معتبر دیجیتالی می‌شود. بسیاری از اسناد دیجیتالی و آنلاین افراد (از جمله امضای دیجیتال)، از طریق این زیرساخت، قابلیت صدور و احراز اصالت را دارند. تحت این زیرساخت، برای هر شخص کلیدهای دیجیتالی عمومی و شخصی تولید می‌شوند که منحصر به همان شخص خواهند بود. در فرآیند امضای دیجیتال، فایل سند مورد نظر کاربر، با استفاده از این دو کلید دیجیتالی رمزگاری شده و اسناد امضا شده، بهسادگی قابلیت رهگیری و احراز اصالت را از طریق کلید عمومی شخص امضاکننده خواهند داشت.

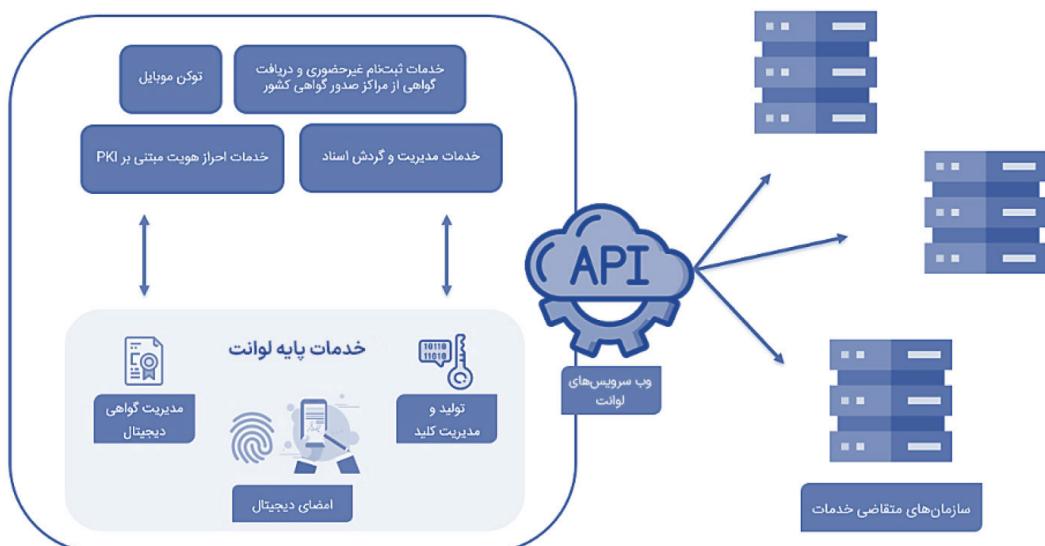




امضای دیجیتال

در جهت افزایش بهرهوری، کاهش هزینه و سرعت بیشتر، روال‌ها و خدمات اداری و سازمانی به صورت روزافزون در حال تغییر از مدل سنتی و کاغذی به سمت الکترونیکی و غیرحضوری شدن، هستند. مهم‌ترین چالش‌های ارایه خدمات به صورت الکترونیکی و راه دور، احراز هویت اشخاص و سیستم‌ها، فراهم نبودن بسترها غیرحضوری و حفظ اصالت تراکنش‌ها و اسناد الکترونیکی است. لذا، به کارگیری راهکارهای قانونی برای شناسایی و احراز هویت اشخاص به صورت الکترونیکی و غیرحضوری، امضای دیجیتال اسناد و تراکنش‌ها مطابق قوانین امضای الکترونیکی کشور، در راستای ارایه خدمات غیرحضوری و برشط، ضروری است. راهکارهای به نسبت قدیمی امضای دیجیتال اسناد و احراز هویت اشخاص مبتنی بر امضای دیجیتال، موانع و مخاطراتی در پیاده‌سازی و به کارگیری دارند. برخی از مشکلاتی که راهکار لوانت در راستای برطرف نمودن آن‌ها است، هزینه‌های بالای خرید و نگهداری تجهیزات رمزگاری شخصی و سازمانی از قبیل توکن‌های امضای دیجیتال و کارت‌های هوشمند با قابلیت رمزگاری نامتقارن، محدودیت سیستم‌های اشخاص در اتصال و به کارگیری این تجهیزات، عدم امکان استفاده از گواهی‌های الکترونیکی صادر شده برای یک راهکار بصورت مشترک در سایر خدمات و راهکارها، و عدم سازگاری راهکارهای قدیمی (توکن و کارت هوشمند) با فناوری‌های جدیدتر (امضای همراه یا ابری) می‌باشد.

معماری لوانت



از جمله ویژگی‌های بارز سامانه امضای دیجیتال لوانت عبارتست از:

ارایه خدمات گردش اسناد و امضای دیجیتال اسناد و تراکنش‌ها

پشتیبانی از تولید و مدیریت بیش از ۳۰ روج کلید RSA و گواهی‌های الکترونیکی X509

امکان آرشیو اسناد و رکورد امضاهای دیجیتال به عنوان ادله اثبات دعوى

امکان ثبت‌نام و صدور گواهی از مراکز صدور گواهی میانی داخلی و بین‌المللی

ارایه وب‌سرویس‌های امضای همراه مبتنی بر گوشی هوشمند

امکان به‌کارگیری گواهی‌ها و کلیدهای روی موبایل بر روی PC و سرور، به عنوان توکن PKI

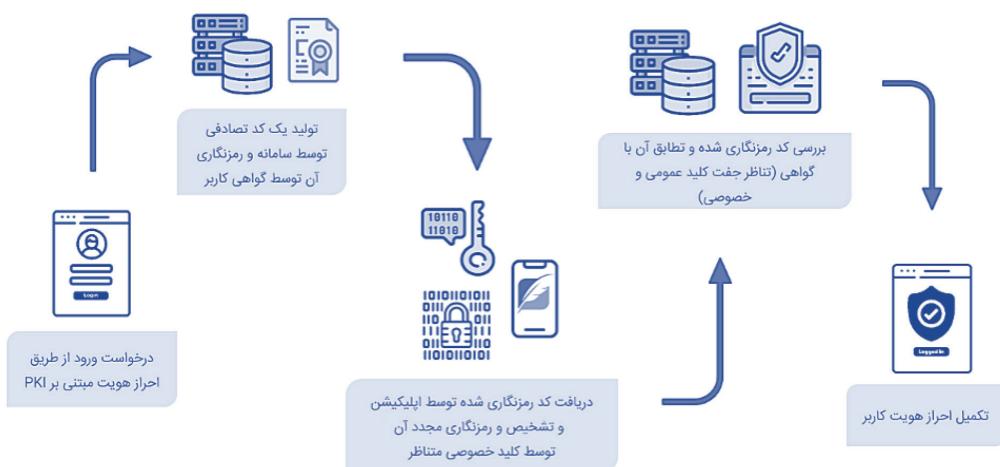
پشتیبانی از سیستم‌های قدیمی مجهز شده به رمزگاری کلید عمومی (PKE) بدون نیاز به تغییر سامانه

قابلیت تعریف و مدیریت کاربران و نقش‌های چندین سازمان در سامانه

سامانه جامع احراز هویت غیرحضوری و امضای دیجیتال شرکت فناوری ارتباط هویت‌الوان، با نام لوانت، علاوه بر ارایه سرویس‌های امضای دیجیتال همراه، مبتنی بر استانداردهای مورد تایید مراکز ریشه صدور گواهی الکترونیکی در کشور و استانداردهای بین‌المللی (ETSI TR 102 203)، یک راه حل کامل برای گردش‌کار تایید اسناد، امضای دیجیتال، ردیابی وضعیت سند و ارایه ادله قانونی است.

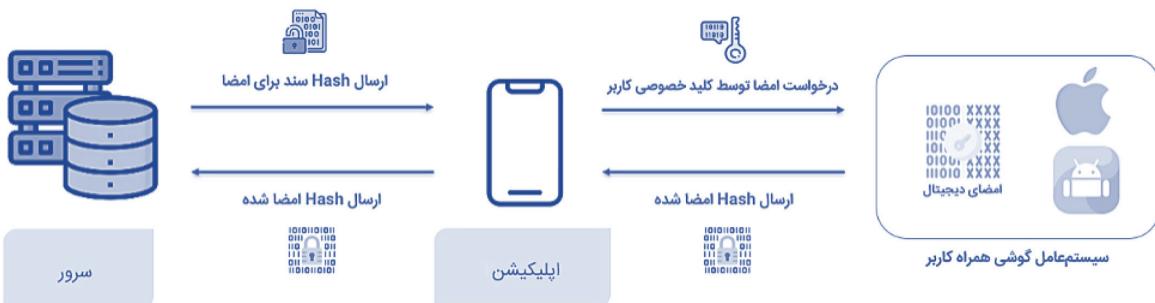
همچنین، این راهکار در راستای سازگاری با انواع سامانه‌هایی که قابلیت به‌کارگیری تجهیزات رمزگاری و گواهی الکترونیکی را از پیش دارد هستند، گوشی موبایل را به عنوان یک توکن PKI، به سیستم معرفی می‌کند و کاربر علاوه بر استفاده از خدمات آنلاین ثبت‌نام و صدور گواهی، امضای همراه اسناد و تراکنش‌ها توسط سامانه، امکان مراجعته به دفاتر ثبت‌نام و صدور گواهی فعلی (از قبیل دفاتر ثبت اسناد، دفاتر پیشخوان دولت یا RA های سازمانی) و دریافت گواهی الکترونیکی از تمامی مراکز میانی صدور گواهی را دارد.

مراحل احراز هویت مبتنی بر PKI



کاربر، بدون نیاز به ثبت‌نام در سامانه مرکزی لوانت نیز می‌تواند از توکن موبایل خود در سامانه ستاد ایران، ارائه اظهار نامه مالیاتی و مالیات ارزش افزوده، امنیت بانکداری الکترونیک، طرح شباب وزارت بازرگانی، امور بورس و اوراق بهادار، سامانه املاک و مستغلات، امضای استناد Word و PDF، ورود به سیستم (ویندوز، لینوکس و مک)، احراز هویت در VPN، احراز هویت در Two-Way SSL، ایمیل امن S/MIME و سایر کاربردهای زیرساخت کلید عمومی، استفاده نماید.

مراحل امضای دیجیتال



راهکار امضای دیجیتال استناد این شرکت، با بهره‌گیری از سرویس‌های هویت‌سنجی و استعلام معتبر کشور، از قبیل سرویس احراز مالکیت شماره تلفن همراه (شاھکار) سازمان تنظیم مقررات و ارتباطات رادیویی و سرویس‌های احراز اقلام هویتی و استعلام عکس اشخاص حقیقی سازمان ثبت احوال کشور، سرویس استعلامی انطباق‌سنجی کدپستی شرکت ملی پست، سرویس شبای بانک مرکزی و همچنین سرویس تشخیص چهره و زنده‌سنجی قبل از صدور گواهی، امکان احراز اینهمانی متقارضی را دارد.

سامانه لوانت دارای چندین زیرسیستم اصلی است که خدمات هر یک به واسطه وب‌سرویس (Web API) و واسط کاربری تحت وب (Web UI)، قابل استفاده توسط سازمان‌ها و اشخاص می‌باشد. این سامانه به صورت مایکروسرویس طراحی شده و امکان استقرار مولفه‌های مختلف سامانه به صورت توزیع شده وجود دارد، لذا بهروزرسانی لوانت با کمترین تاثیر بر روی عملکردهای سامانه انجام خواهد شد و مانیتورینگ این سامانه، با بالاترین استانداردها قابل انجام است.

مراحل دریافت گواهی امضا



لوانت با اخذ مجوزهای امنیتی و صلاحیتی لازم به عنوان یک مرکز ثبت‌نام برای دریافت گواهی‌های امضا قادر به ارائه خدمات است و به لطف سرویس خدمات پایه خود فرآیند ثبت‌نام و دریافت گواهی را نیز به صورت غیرحضوری و حضوری، و تنها با چند کلیک و پس از گرفتن اطلاعات لازم از متقارضی و اعتبارسنجی آنها از طریق وب‌سرویس‌های احراز هویت و احراز آیتم‌های بیومتریک و زنده‌سنجی انجام می‌دهد.

زیرسیستم‌ها (ماژول‌ها) سامانه لوانت

ماژول امضای همراه (MSSP)

ماژول گردش و امضای استناد

ماژول RA حضوری و غیرحضوری

ماژول مدیریت، احراز هویت و مجوزدهی کاربران

ماژول مدیریت و پیکربندی سامانه

ماژول ممیزی و مانیتورینگ



قانون تجارت الکترونیکی در ایران، امضای دیجیتال را با داشتن شرایطی، معادل امضای دستی (خیس یا کاغذی) می‌داند، همچنین مرکز دولتی صدور گواهی الکترونیکی ریشه بر طبق آیین‌نامه ماده ۳۲ قانون تجارت الکترونیکی، مسئول مجوز ایجاد، امضاء، صدور و ابطال گواهی الکترونیکی مراکز صدور گواهی الکترونیکی میانی در زیرساخت کلید عمومی کشور می‌باشد. لذا لوانت، منطبق با قوانین و استانداردهای مرکز دولتی صدور گواهی الکترونیکی ریشه کشور و با بررسی کاستی‌های راهکارهای موجود در کشور و مزایای راهکارهای نوین بین‌المللی، طراحی و توسعه داده شده است. در این راهکار از گوشی هوشمند کاربر به عنوان تجهیز رمزگاری استفاده شده است و زوج کلیدهای خصوصی و عمومی اشخاص، بر روی گوشی ایشان تولید و نگهداری می‌شوند و امکان ثبت‌نام و صدور گواهی بصورت حضوری و غیرحضوری از تمامی مراکز میانی داخلی و بین‌المللی (که خدمات صدور و مدیریت گواهی را به‌واسطه API ارایه می‌کنند)، توسط این راهکار، فراهم شده است. لذا کاربر با در دست داشتن گوشی هوشمند، امکان اثبات هویت خود مبتنی بر امضای دیجیتال و گواهی الکترونیکی در سامانه‌های ارایه خدمات الکترونیکی برخی، و امضای دیجیتال استناد و تراکنش‌ها به‌صورت شخصی و سازمانی، خواهد داشت. این راهکار با برخورداری از معماری پیمانهای و استفاده از واسطه‌های استاندارد، قابلیت اتصال به سایر تجهیزات رمزگاری شخصی از قبیل توکن‌ها و کارت‌های هوشمند و تجهیزات سیستمی از قبیل انواع HSM با رابط #11 PKCS برای امضای استناد و تراکنش‌ها توسط اشخاص، یا سیستم‌ها برای امضای استناد و تراکنش‌ها به‌صورت سازمانی را دارد.

نمای کلی از خدمات گردش اسناد لوانت

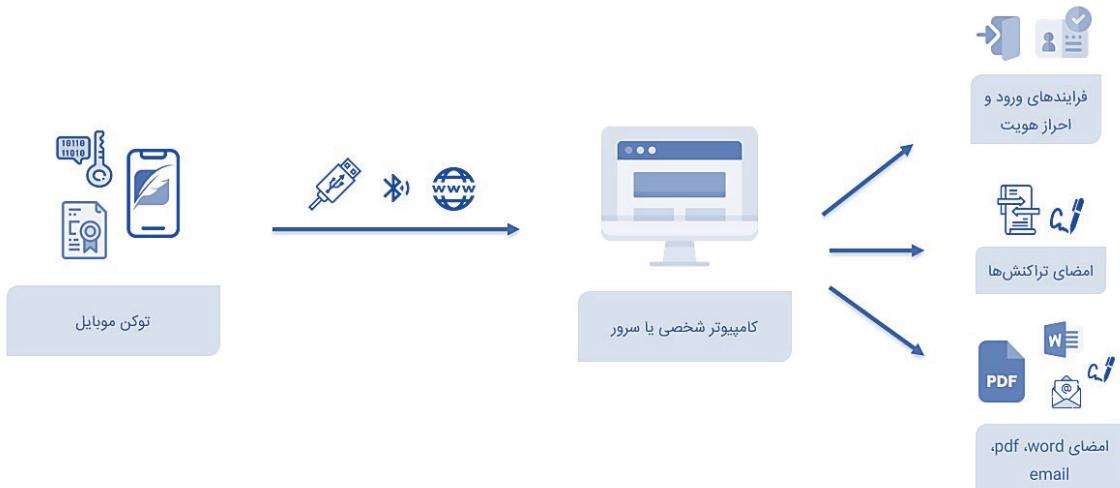




توكن موبایل

سامانه لوانت که هم برای اندروید و هم iOS طراحی شده است، علاوه بر اینکه به عنوان بخشی از راهکار امضای همراه می‌تواند مورد استفاده گیرد، بلکه بدون نیاز به ثبت نام و ارتباط با سرور مرکزی لوانت، این امکان را به مالک گوشی می‌دهد که از گوشی همراهش به عنوان توکن PKI استفاده کند و مشابه توکن‌های USB مورد استفاده در کشور، کاربر می‌تواند کلیدها و گواهی‌های روی توکن را مدیریت کند و در کامپیوتر شخصی یا سرور اقدام به امضای استناد یا ایمیل‌های خود نماید.

کاربرد توكن موبایل



با استفاده از این قابلیت، کاربر بدون نیاز به ثبت‌نام در سامانه مرکزی لوانت نیز می‌تواند از توكن موبایل خود در سامانه ستاد ایران، ارائه اظهارنامه مالیاتی و مالیات ارزش افزوده، امنیت بانکداری الکترونیک، طرح شباب وزارت بازرگانی، امور بورس و اوراق بهادار، سامانه املاک و مستغلات، امضای استناد Word و PDF، ورود به سیستم (ویندوز، لینوکس و مک)، احراز هویت در VPN، احراز هویت در Two-Way SSL، ایمیل امن S/MIME و سایر کاربردهای زیرساخت کلید عمومی، استفاده نماید.

استانداردها

محصول لوانت بر اساس استانداردهای داخلی و خارجی طراحی و پیاده‌سازی شده است.
برخی از استانداردهای محصول در ادامه ارائه می‌شود.

مرکز توسعه تجارت الکترونیکی ایران و سازمان استاندارد

۱۳۹۳/۱۰/۳۰

الزامات پروتکل درخواست گواهی در
زیرساخت کلید عمومی ایران

۱۳۹۴/۳/۱۸

الزامات پروتکل احراز هویت در زیرساخت
کلید عمومی ایران

۱۳۹۴/۳/۱۸

الزامات تشکیل و اعتبارسنجی مسیر گواهی
دیجیتالی

۱۳۹۲/۱۲/۱۱

الزامات برنامه‌های کاربردی مجهز به
زیرساخت کلید عمومی ایران

۱۳۹۲/۱۲/۱۱

الزامات امنیتی پودمان‌های رمزگاشتنی
زیرساخت کلید عمومی

۱۳۹۲/۱۲/۱۱

الزامات ساختار نحوی پیام‌های رمزگاشتنی
در زیرساخت کلید عمومی ایران

استانداردهای سری ETSI

ETSI TR 102 206

الزامات امنیتی

ETSI TS 102 204

واسطه‌های وب امضای همراه

ETSI TR 102 203

الزامات عملکردهای تجاری

استانداردهای سری PKCS

PKCS #10

درخواست گواهی الکترونیکی X509

PKCS #7

قالب نگهداری پیام‌های امضای گواهیها

PKCS #1

کلیدها و امضای RSA

PKCS #13

کلیدها و امضای ECC

PKCS #11

رابط ارتباطی با HSM و توکن

استانداردهای اتحادیه اروپا

ETSI EN 319 162

Associated Signature Containers

ETSI EN 319 142

PDF Advanced Electronic Signature Profiles

ETSI EN 319 122

CMS Advanced Electronic Signatures

ETSI TS 119 612 v2.1.1

Electronic Signatures and Infrastructures (ESI); Trusted Lists

استانداردهای سری ANSI

X9.31:1998

Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (DSA)

X9.30 Part 2:1997

Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry, Part 2: The Secure Hash Algorithm

X9.30 Part 1:1997

Public Key Cryptography Using Irreversible Algorithm: Digital Signature Algorithm (DSA)

X9.57:1997

Public Key Cryptography for the Financial Services Industry: Certificate Management

X9.55:1997

Certificate Extensions for Multi-Domain Operations

X9.42:2003

Public Key Cryptography for Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography

X9.68 Part 2:2001

Digital Certificates for High Transaction Volume Financial Systems

X9.63:2001

Key Agreement and Key Management Using Elliptic Curve-Based Cryptography

X9.62:1998

Public Key Cryptography: The Elliptic Curve Digital Signature Algorithm (ECDSA)

X9.79:2001

PKI Practices and Policy Framework for the Financial Services Industry

X9.73:2003

Cryptographic Message Syntax

X9.69:1998

Framework for Key Management Extensions



تهران، میدان آرژانتین، خیابان الوند، پلاک ۱۹، طبقه ۵

www.levants.io

