روکارمز
رمزنگاری ایمیل سازمانی

سرویس رمزنگاری ایمیل روکا رمز

سرویس روکا رمز جهت رمزنگاری ایمیل های مهم سازمانی طراحی شده است. از قابلیت های این سرویس امکان احراز هویت کاربران برای تضمین دریافت ایمیل به صورت محرمانه و رمزنگاری شده توسط فرد گیرنده می باشد. همچنین این سرویس با قابلیت شناسایی کلمات کلیدی در محتویات موضوع یا محتوای ایمیل طراحی شده است و در صورتی که ایمیل حاوی کلمات کلیدی باشد ، به صورت اتوماتیک رمز نگاری خواهد شد. (کلمات کلیدی را کاربران هر سازمان از قبل تعریف نموده اند) قابلیت دیگر این سرویس(در صورت انتخاب یک ایمیل) امکان رمزنگاری دستی برای کاربران می باشد.

همچنین این امکان وجود دارد که رمزنگاری به صورت درون سازمانی و بدون هیچ گونه وابستگی به سرویس خارج از سازمان انجام شود و کلیه فرایند های امنیتی رمزنگاری در داخل سازمان انجام پذیرد. با توجه به اینکه اکثر سرویس های رمزنگاری در دنیا به صورت کلاد می باشند و کشور در وضعیت تحریم قرار گرفته است این ویژگی بسیار کاربردی خواهد بود.

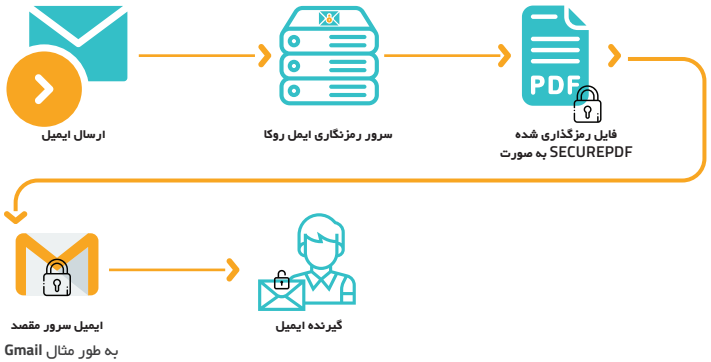
کاربران این اطمینان را خواهند داشت که ایمیل های ارسالی به دامین های خارجی نیز رمز نگاری شده اند. به طور مثال در صورت ارسال پیام بر روی سرور های Gmail، با استفاده از سرویس روکا رمز، امکان مشاهده محتویات ایمیل برای کمپانی Gmail امکان پذیر نمی باشد.

روکارمز
رمزنگاری ایمیل سازمانی

پروتکل
Secure PDF

Secure PDF

در این راهکار پیغام های ارسال شده توسط فرستنده، به همراه ضمیمه های آن تماماً به یک فایل **PDF** رمزشده تبدیل می شود و پسورد آن نیز بصورت **Hash** شده می باشد که قابل شکستن و رمزگشایی نمی باشد. کاربران با اعتبار سنجی و احراز هویت در سامانه روکا برای خود یک رمز تعریف می کنند و پس از آن تمامی فایل های دریافتی (که اکنون به فایل **PDF** تبدیل شدند)فقط با این رمز قابل رمزگشایی و خواندن می باشند.



روکارمز
رمزنگاری ایمیل سازمانی

پروتکل
WebMail

WebMail

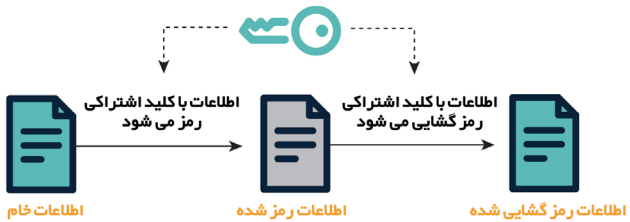
در این راهکار پیغام های ارسالی توسط دستگاه رمزنگار روکا رمزنگاری می شود و برای گیرنده یک اعلان با مضمون ایمیل رمزنگاری شده ارسال می شود. گیرنده پس از دریافت این پیغام به سامانه روکا وارد می شود و پس از اعتبار سنجی، پیغام رمز شده ی آن توسط سیستم از حالت رمز خارج می شود و به آن نمایش داده می شود.

روکارمز
رمزنگاری ایمیل سازمانی

پروتکل
Initiated Encryption

Automated or User Initiated Encryption

رمزنگاری ایمیل ها به طرق مختلفی امکان پذیرند. به عنوان مثال، کاربر می تواند کلمه یا کلماتی را بر روی سرویس تعریف نماید و در صورتی که عنوان و یا محتوای ایمیل شامل یکی از این کلمات بود، ایمیل به صورت خودکار رمزنگاری شود. همچنین این امکان وجود دارد که گیرندگان و فرستندگان خاصی بر روی سرویس تعریف شوند و بدین شکل در صورت ارسال و یا دریافت ایمیل از این اشخاص، عملیات رمزنگاری خود به خود انجام شود. در صورتی که کلمه و یا شخصی (به عنوان فرستنده و گیرنده) تعریف نشده باشد، کاربر می تواند به صورت دستی رمزنگاری را انجام دهد.



پنهان کردن آدرس فرستنده ایمیل:

در سرویس روکا رمز کاربران علاوه بر امکان رمزنگاری ایمیل ها، از این قابلیت نیز برخوردارند که به عنوان فرستنده ایمیل، نام کاربری خود را مخفی نمایند. همچنین سازمان می تواند تمامی ایمیل های ارسالی از بخش های مختلف سازمان را تحت عنوان یک نام واحد ارسال کند.

روکارمز
رمزنگاری ایمیل سازمانی

پروتکل
PGP

Pretty Good Privacy به معنای حریم خصوصی کامل:

در این پروتکل، یک متن که شامل محتوای کاملا قابل درک می باشد، به متن رمزنگاری (داده‌های غیرقابل خواندن) تبدیل می‌شود. بدین شکل که محتوا با یک کلید تصادفی رمزگذاری می‌شود، که به عنوان کلید جلسه شناخته می‌شود. این کلید به طور تصادفی از طریق استفاده از رمزنگاری متقارن تولید می‌شود. در این مرحله این کلید با اتفاده از تکنولوژی الگوریتم های نامتقارن به دست گیرنده می رسد. سپس گیرنده با استفاده از همین کلید و متن رمزنگاری شده می تواند به اطلاعات دست یابد.

S/MIME(Secure/Multipurpose Internet Mail Extensions)

در این راهکار رمز نگاری بصورت **End-to-End** انجام می شود. فرستنده و گیرنده هر کدام کلید های عمومی یکدیگر را دارند و کلید های خصوصی نزد خود نگه داشته می شوند. فرستنده پیام را با کلید عمومی گیرنده رمز می کند و این پیام رمز شده فقط با کلید خصوصی مربوط به گیرنده (که فقط نزد خودش می باشد)، امکان بازگشایی دارد. در واقع این راهکار مشابه پی جی پی بوده با این تفاوت که نیاز به ساخت کلید تصادفی نمی باشد.

روکارمز
رمزنگاری ایمیل سازمانی

پروتکل
DKIM

DomainKeys Identified Mail(DKIM)

این سرویس یک راهکار برای تصدیق و احراز هویت ایمیل می باشد. این مکانیزم امکانی را فراهم می کند که میل سرور های گیرنده ایمیل بررسی کنند که ایمیل دریافتی از **Domain** مربوطه توسط مدیریت دامنه تائید شده باشد. این متد در زمان ارسال ایمیل مشخصاتی از قبیل نام فرستنده ، نام دامنه ، موضوع ایمیل و... را به عنوان امضای الکترونیکی در هدر ایمیل (**Header**) قرار داده تا زمانی که گیرنده ایمیل را دریافت کرد ، بتواند اطلاعاتی چون اعتبار ایمیل و دامنه ، عدم هرزنامه بودن و ... را بررسی کرده و سپس ایمیل را به دست گیرنده برساند. همچنین در این متد ،کلید خصوصی را فقط و فقط فرد فرستنده در دست داشته و می تواند پیغام ها را طوری رمزنگاری که فقط توسط همان کلید در **DNS** باز شود.