



شرکت توانیر

تشریح پروژه واگذاری

CoRFP20-12



<p>عنوان پروژه:</p>	<p>طراحی و ساخت نمونه نیمه صنعتی رمزنگار داده، متناسب با پروتکل IEC60870-5-104 مورد استفاده در شبکه انتقال صنعت برق</p>
<p>عنوان طرح:</p>	<p>طرح توسعه فناوری های امنیتی در صنعت برق</p>
<p>واحد اجرایی:</p>	<p>مرکز توسعه فناوری امنیت اطلاعات، ارتباطات و تجهیزات صنعت برق</p>
<p>برآورد کلی مدت زمان اجرای پروژه: ۱۲ ماه</p>	
<p>تبیین و تشریح پروژه همراه با ذکر مراحل کلی:</p>	
<p>یکی از جنبه های امنیت، محرمانگی (Privacy) است که می تواند با استفاده از انواع روش های رمزنگاری به صورت تعبیه شده در سیستم و یا با استفاده از رمزنگارهای مجزا (Stand alone) تحقق یابد. از آنجا که در سیستم های مخابراتی و اسکادای موجود در صنعت برق این ویژگی امنیتی لحاظ نشده است، لذا استفاده از رمزنگارهای مجزا (Stand alone) تنها راه حل موجود برای حفظ محرمانگی داده می باشد.</p>	
<p>با توجه به اینکه رمزنگار متناسب با کاربردهای صنعت برق باید علاوه بر قدرت رمزنگاری و امنیت فیزیکی رمزنگار، ملاحظات خاص صنعتی را نیز مورد توجه قرار دهد، لذا استفاده از محصولات رمزنگار عمومی موجود در حوزه ICT عمومی به این منظور مناسب نمی باشد.</p>	
<p>همچنین اگرچه نمونه این محصولات در شرکت های خارجی طراحی و ساخته شده اند ولی به دلیل آنکه روش رمزنگاری این سیستم ها در اختیار آن شرکت ها می باشد، استفاده از این محصولات در ارتباطات زیرساخت های حیاتی صنعت برق کشور قابل اطمینان نیست. لذا طراحی رمزنگار داده در کشور می تواند در جهت ارتقای سطح امنیت ارتباطات در صنعت برق موثر واقع شود که در این تعریف پروژه به آن پرداخته می شود.</p>	
<p>در این تعریف پروژه، طراحی و ساخت رمزنگاری مدنظر می باشد که در طراحی آن به دو مورد زیر توجه شده باشد: مورد اول سطح امنیت رمزنگار می باشد. سطوح امنیتی مختلفی برای انواع رمزنگارها وجود دارد. استاندارد FIPS 140 سطوح امنیتی رمزنگاری را مشخص می کند که در واقع تعیین کننده قدرت رمزنگار در مقابله با انواع حملات می باشد. سطح مورد نظر در این پروژه سطح ۲ می باشد.</p>	
<p>مورد دوم ملاحظات خاص موجود در کاربردهای صنعت برق می باشد. همانطور که ذکر شد در طراحی رمزنگار متناسب با کاربردهای صنعت برق باید علاوه بر قدرت رمزنگاری و امنیت فیزیکی رمزنگار، ملاحظات خاص دیگری نیز مورد توجه قرار گیرد. از جمله این ملاحظات می توان به پشتیبانی از پیغام های تکراری، پشتیبانی از پیغام های بلادرنگ مدنظر در دیسپاچینگ، عدم تداخل با مکانیزم های تشخیص خطا در سیستم کنترلی صنعت برق، پشتیبانی از نرخ بیت پایین داده متناسب با کاربردهای دیسپاچینگ و ... اشاره نمود.</p>	
<p>با توجه به توضیحات فوق فعالیت های اصلی اجرای این پروژه شامل موارد زیر است:</p>	
<ul style="list-style-type: none"> • انجام مطالعات به منظور استخراج استانداردها، ملاحظات رمزنگار داده متناسب با کاربردهای دیسپاچینگ • طراحی الگوریتم رمزنگاری متناسب برای کاربرد دیسپاچینگ و شبیه سازی آن • انتخاب و پیاده سازی سخت افزار مناسب • پیاده سازی نرم افزار الگوریتم طراحی شده • طراحی بخش حفاظت فیزیکی سیستم • انجام آزمون های استاندارد امنیتی (فیزیکی و اطلاعاتی) مطابق مطالعات انجام شده 	



شرکت توانیر

تشریح پروژه واکذاری

CoRFP20-12



<p>عنوان پروژه:</p>	<p>طراحی و ساخت نمونه نیمه صنعتی رمزنگار داده، متناسب با پروتکل IEC60870-5-104 مورد استفاده در شبکه انتقال صنعت برق</p>
<p>عنوان طرح:</p>	<p>طرح توسعه فناوری های امنیتی در صنعت برق</p>
<p>واحد اجرایی:</p>	<p>مرکز توسعه فناوری امنیت اطلاعات، ارتباطات و تجهیزات صنعت برق</p>
<p>برآورد کلی مدت زمان اجرای پروژه: ۱۲ ماه</p>	
<p>مشخصات محصول نهایی (خروجی مورد انتظار):</p> <p>رمزنگار داده متناسب با کاربردهای دیسپاچینگ به صورت Stand alone با قابلیت های زیر:</p> <ul style="list-style-type: none"> - دارای سطح امنیتی ۲ استاندارد FIPS 140، تطابق با استاندارد AGA-12 و متناسب با استاندارد IEC 62351 - دارای مکانیزم کنترل دسترسی و سیستم مدیریت کلید مناسب - دارای الگوریتم های رمزنگاری AES 128bit، RSA 1024/2048 و HMAC SHA 256 - با قابلیت پشتیبانی از پروتکل های صنعتی IEC 60870-101/104 - با قابلیت پشتیبانی از پیغام های تکراری - با قابلیت پشتیبانی از نرخ بیت کانال های مخابراتی موجود از نرخ 300bps تا 115.2 kbps - پشتیبانی از پیغام های بلادرنگ (عملیات رمزنگاری دارای تاخیر ذاتی می باشد) - عدم تداخل با مکانیزم های تشخیص خطا در سیستم دیسپاچینگ - پشتیبانی از نرخ بیت های پایین داده متناسب با نیازهای دیسپاچینگ 	